Actividad Colaborativa - Unidad 3

Presentado Por:
Frank Alexander Sánchez Triana. Código: 1.061.047.409
Beatriz Elena Castillo Gómez. Código: 34.673.338
Jacqueline Muñoz Anacona. Código: 25.296.208
Luis Eyder Ortiz Collazos. Código: 76.332.853
Danny Yerfis Ducuara. Código: 10.189.373

Presentado A:
Ing. Nancy Amparo Guaca

Diplomado de profundización CISCO (diseño e implementación de soluciones Integradas LAN / WAN) (Opción de grado)
Grupo: 203092_29

Universidad Nacional Abierta y a Distancia – UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería
30 de Abril de 2017

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Tabla de contenido

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Introducción

La tecnología ha avanzado aceleradamente, y actualmente poder comunicarse y tener una información oportuna marca la diferencia; es por eso que es tan importante el uso de las redes en todas las áreas de nuestra vida, el impacto del internet está en todos los campos de la sociedad; permitiendo que exista una comunicación sin barreras en forma eficiente, con el internet todo está a nuestro alcance; como estudiantes de Ingeniería de sistemas necesitamos conocer en una forma más detallada el funcionamiento de las redes.

Con el presente trabajo colaborativo pretendemos aplicar los conocimientos adquiridos en cuanto a la Configuración de Sistemas de red soportados en VLANs (Unidad 3), del diplomado de profundización CISCO, desarrollando los ejercicios planteados para mejorar las estrategias de aprendizaje en cuanto a introducción a redes conmutadas, configuración y conceptos básicos de Switching, VLANs, Conceptos de Routing, Enrutamiento entre VLANs , Enrutamiento Estático.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Objetivos

- Examinar los modelos actuales de diseño de red y el modo en que los switches LAN crean tablas de reenvío y usan la información de direcciones MAC para conmutar datos entre los hosts de forma eficaz.
- Analizar las opciones de configuración básica de switch que se requieren para mantener un entorno LAN conmutado seguro y disponible.
- Configurar los puertos de switch para cumplir con los requisitos de red.
- Configurar la característica de seguridad de puertos para restringir el acceso a la red.
- Describir cómo configurar y administrar VLAN y enlaces troncales de VLAN, así como resolver problemas relacionados.
- Analizar cuestiones y estrategias de seguridad relacionadas con las VLAN y los enlaces troncales, así como las prácticas recomendadas para el diseño de VLAN.
- Utilizar herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.
- Configurar parámetros básicos en un router mediante la CLI para crear una ruta entre dos redes conectadas directamente.
- Explicar el proceso de encapsulación y desencapsulación que utilizan los routers para el switching de paquetes entre interfaces.
- Explicar las entradas de la tabla de routing de las redes conectadas directamente.
- Analizar los métodos utilizados para la implementación del routing entre VLAN. Incluyendo configuraciones para el uso de un router y un switch de capa 3.
- Describir los problemas que se encuentran al implementar routing entre VLAN y técnicas estándar de resolución de problemas.
- Configurar el enrutamiento entre VLAN con router-on-a-stick.
- Configurar rutas estáticas IPV4 e IPV6 especificando una dirección del siguiente salto.
- Configurar rutas IPV4 e IPV6 predeterminadas.
- Configurar una dirección de red resumida IPV4 e IPV6, a fin de reducir el número de actualizaciones de la tabla de routing.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Desarrollo de la actividad

Informe 1: 2.1.1.6 Lab - Configuring Basic Switch Settings

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

Topología

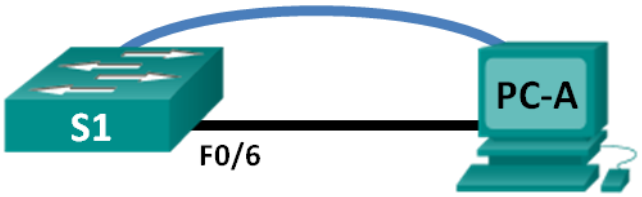


Tabla de direccionamiento

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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

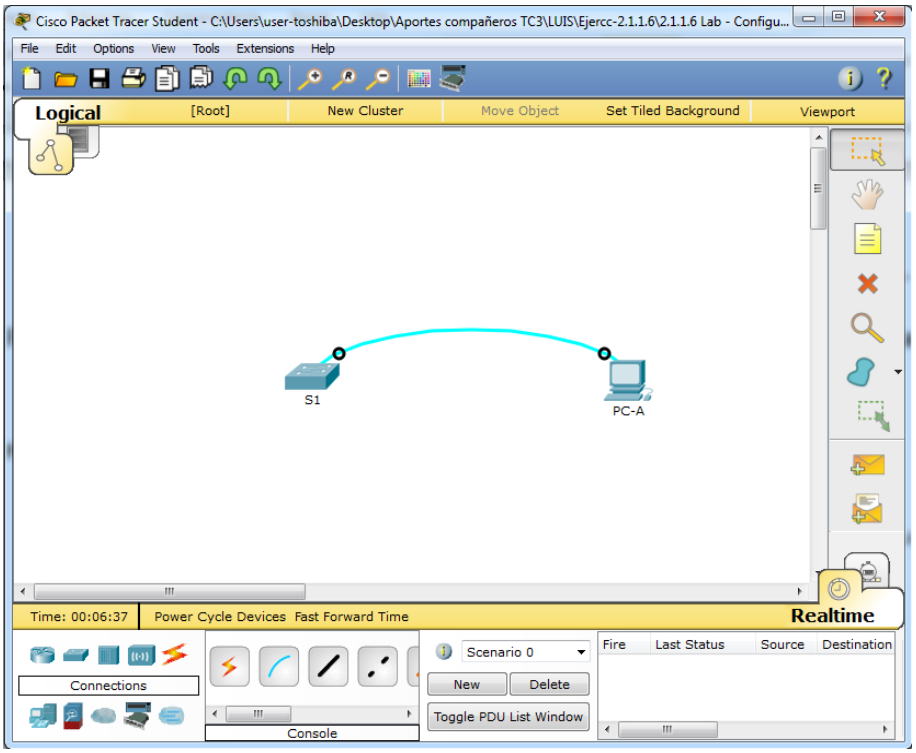
Parte 1: tender el cableado de red y verificar la configuración predeterminada del switch

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

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

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

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



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

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

No se configuran todavía parámetros de direccionamiento IP. Un conmutador Cisco 2960 puesto en servicio por primera vez no tiene ninguna configuración de red.

Paso 2. Verificar la configuración predeterminada del switch.

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

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

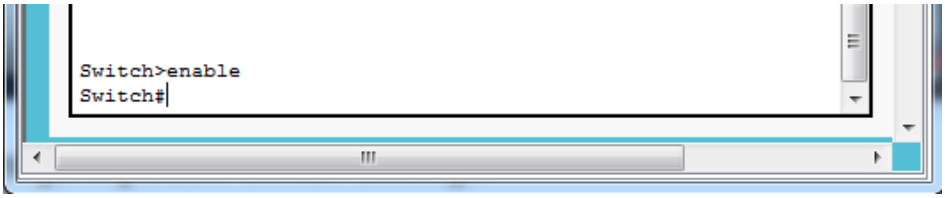
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

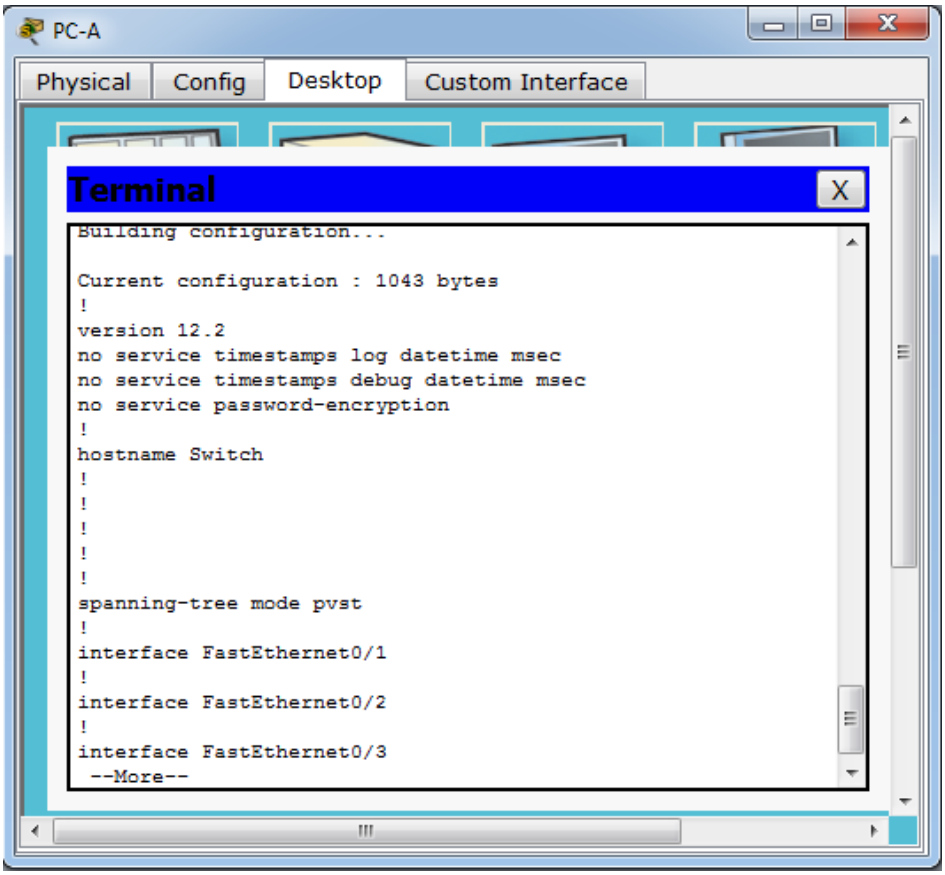
```
Switch> enable
Switch#
```

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.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

b. Examine el archivo de configuración activa actual.

`Switch# show running-config`

¿Cuántas interfaces FastEthernet tiene un switch 2960? 24

```
!
interface FastEthernet0/24
!
```

¿Cuántas interfaces Gigabit Ethernet tiene un switch 2960? 2

```
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
```

¿Cuál es el rango de valores que se muestra para las líneas vty? 0-4 and 5-15 or 0-15

```
line vty 0 4
 login
line vty 5 15
```

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

`Switch# show startup-config`

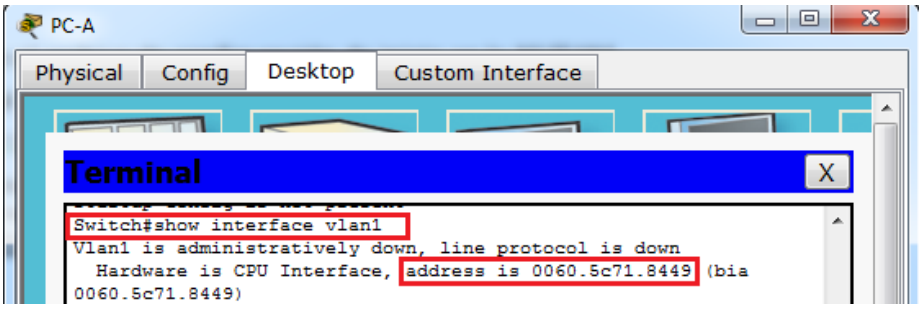
`startup-config is not present`

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

¿Por qué aparece este mensaje? No se han guardado configuraciones en NVRAM.

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

`Switch# show interface vlan1`



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

¿Cuál es la dirección MAC de esta SVI? Las respuestas varían. 0060.5c71.8449

¿Está activa esta interfaz? Vlan1 administrativamente caída

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

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

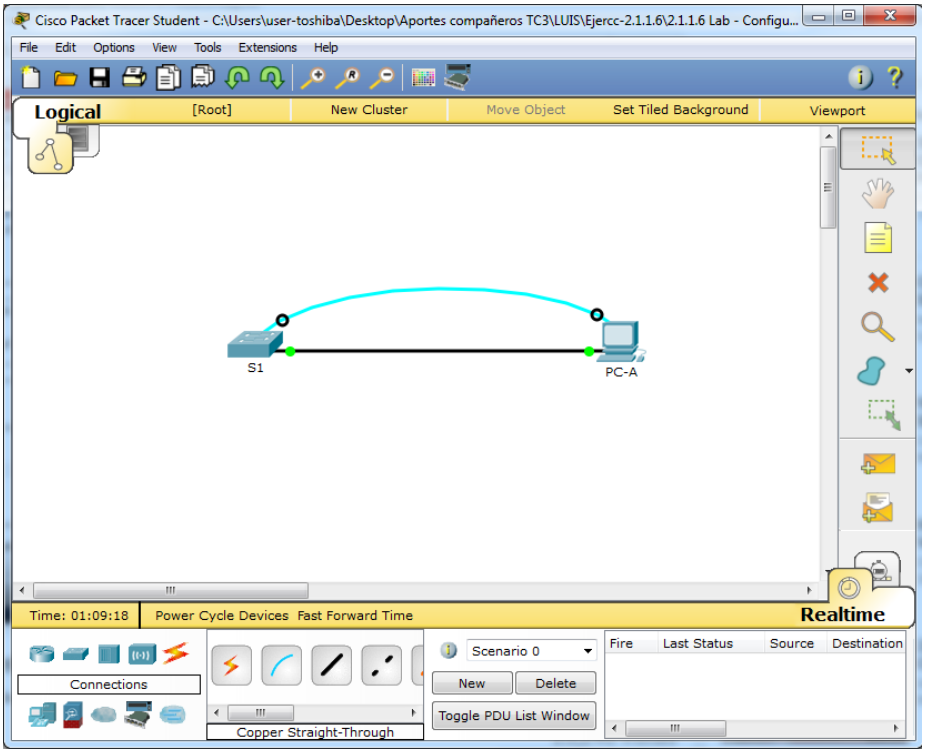
¿Qué resultado ve?

Vlan1 is administratively down, line protocol is down

Internet protocol processing disabled

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

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




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

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

¿Qué resultado ve?

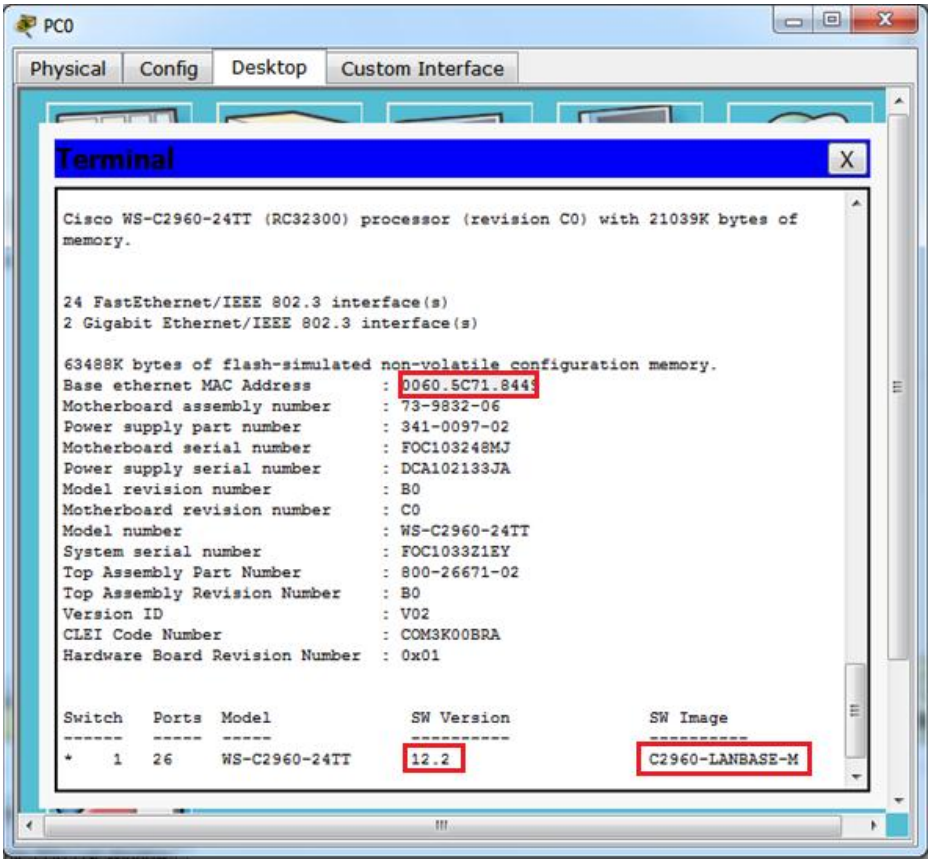
Vlan1 is administratively down, line protocol is down

Internet protocol processing disabled

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

```
Switch# show version
```



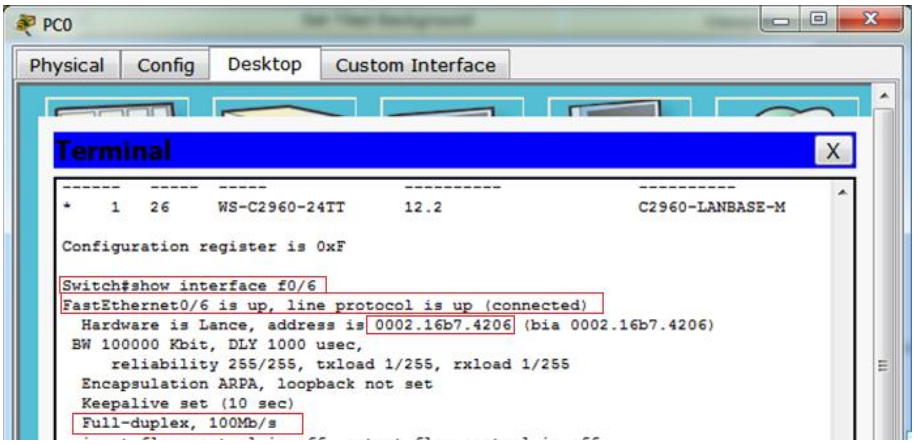
¿Cuál es la versión del IOS de Cisco que está ejecutando el switch? 12.2

¿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. 0060.5C71.8449

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

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

¿La interfaz está activa o desactivada? Interfaz levantada línea de protocolo levantada

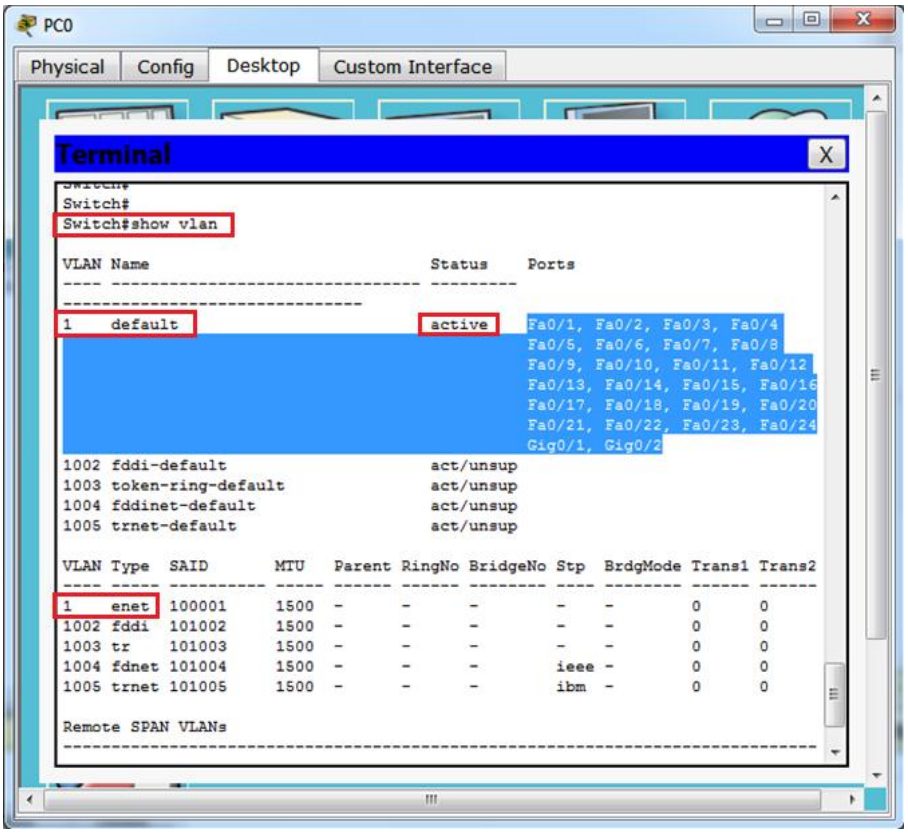
¿Qué haría que una interfaz se active? Conectar un host

¿Cuál es la dirección MAC de la interfaz? 0002.16b7.4206

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

i. Examine la configuración VLAN predeterminada del switch.

`Switch# **show vlan**`



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

¿Qué puertos hay en esta VLAN? 26

¿La VLAN 1 está activa? Si

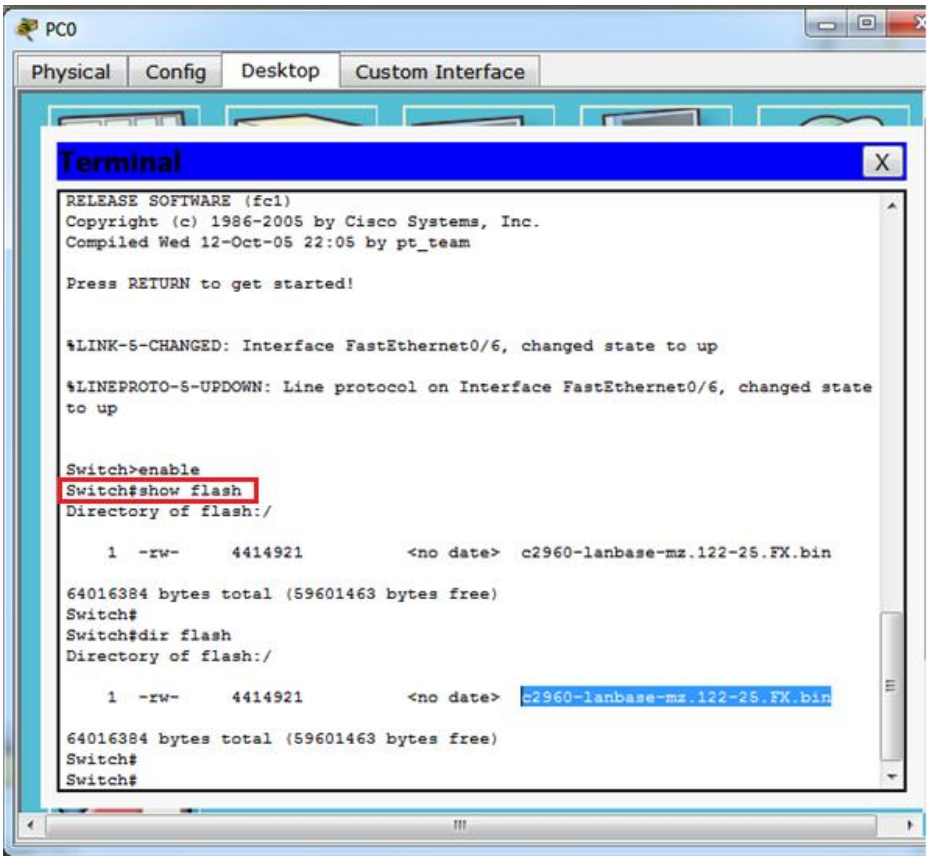
¿Qué tipo de VLAN es la VLAN predeterminada? enet (Ethernet)

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

j. Examine la memoria flash.

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

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



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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

Paso 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#
```

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#SERVICE pass
S1(config)#SERVICE password-encryption
S1(config)#enable secret class
S1(config)#no ip domai
S1(config)#no ip domain-loo
S1(config)#no ip domain-lookup
```

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.

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#SERVICE pass
S1(config)#SERVICE password-encryption
S1(config)#enable secret class
S1(config)#no ip domai
S1(config)#no ip domain-loo
S1(config)#no ip domain-lookup
```

c. Asigne el nombre de host del switch.

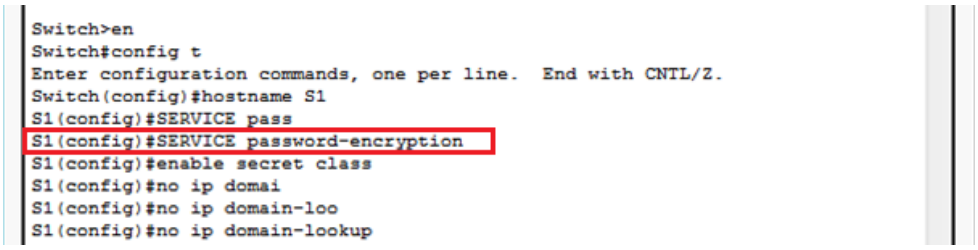
```
Switch(config)# hostname S1
S1(config)#
```

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#SERVICE pass
S1(config)#SERVICE password-encryption
S1(config)#enable secret class
S1(config)#no ip domai
S1(config)#no ip domain-loo
S1(config)#no ip domain-lookup
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

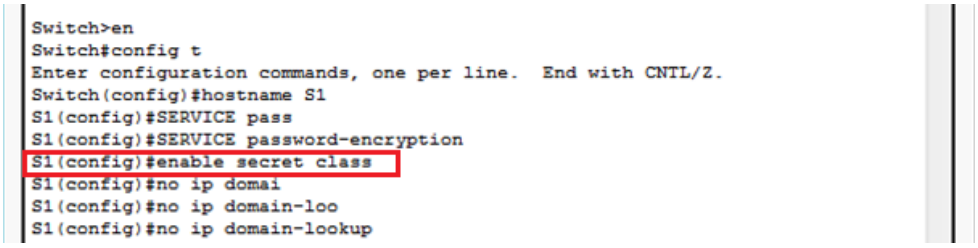
d. Configurar la encriptación de contraseñas.

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



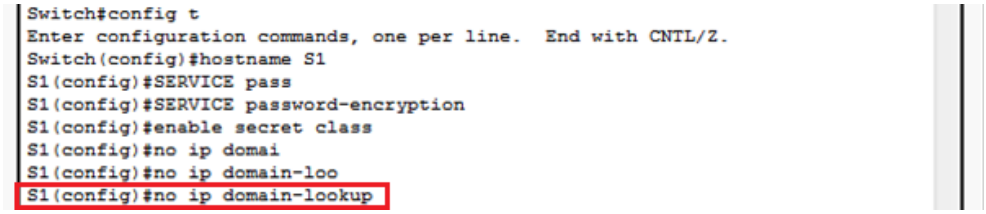
e. Asigne **class** como contraseña secreta para el acceso al modo EXEC privilegiado.

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



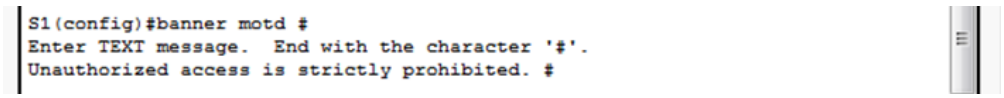
f. Evite las búsquedas de DNS no deseadas.

```
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. #
```



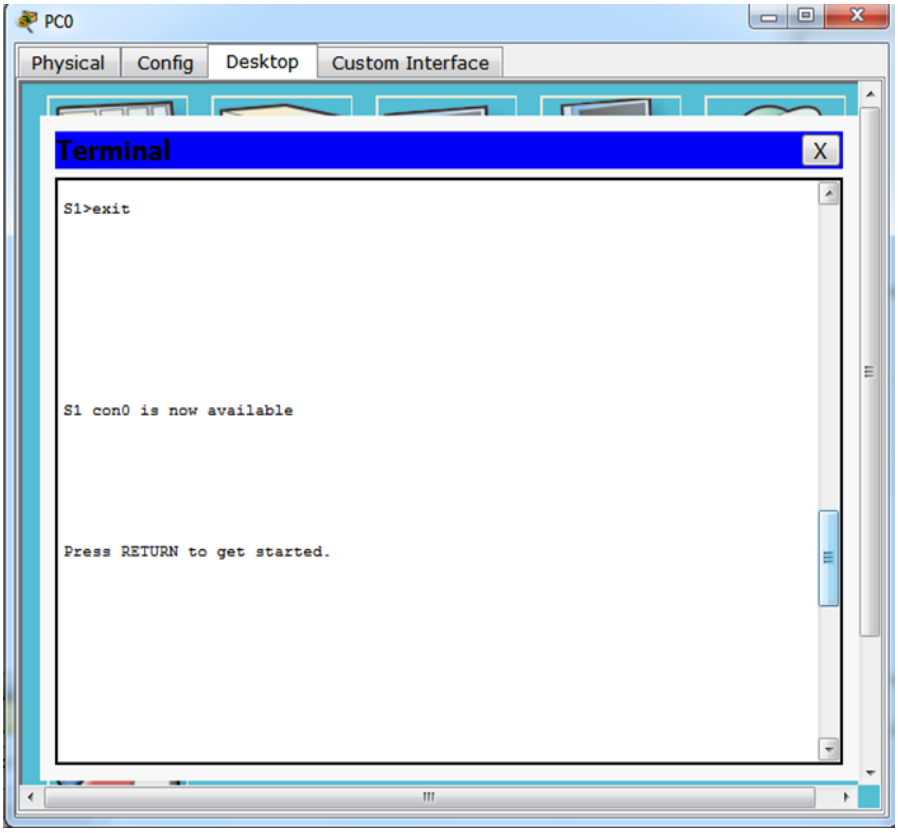
h. Para verificar la configuración de acceso, alterne entre los modos.

```
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
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
Press RETURN to get started.

Unauthorized access is strictly prohibited.
S1>
```

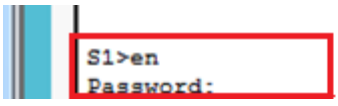
¿Qué teclas de método abreviado se usan para ir directamente del modo de configuración global al modo EXEC privilegiado? Ctrl + z



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.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

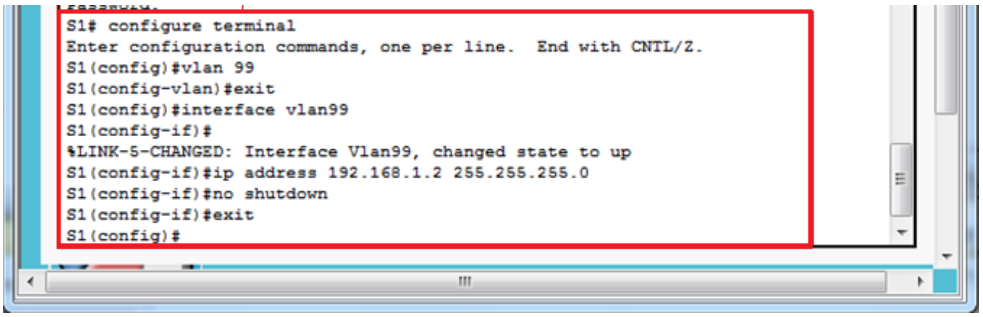
Antes de poder administrar el S1 en forma remota desde la PC-A, debe asignar una dirección IP al switch. El switch está configurado de manera predeterminada para que la administración de este se realice a través de VLAN 1. Sin embargo, la práctica recomendada para la configuración básica del switch es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

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

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

```
S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)#
```

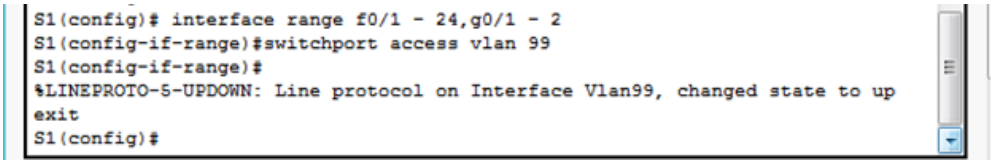
Observe que la interfaz VLAN 99 está en estado down, aunque haya introducido el comando **no shutdown**. Actualmente, la interfaz se encuentra en estado down debido a que no se asignaron puertos del switch a la VLAN 99.



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

```
S1(config)# interface range f0/1 – 24,g0/1 - 2
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

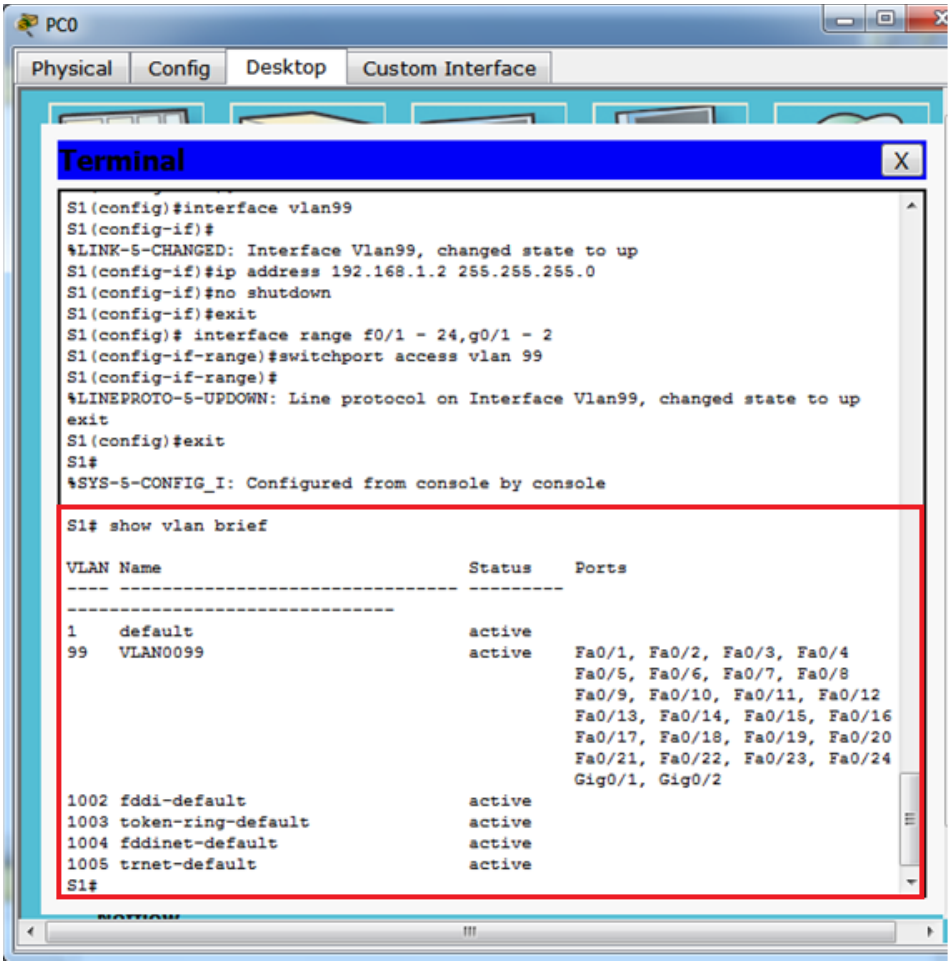
Para establecer la conectividad entre el host y el switch, los puertos que usa el host deben estar en la misma VLAN que el switch. Observe que, en el resultado de arriba, la interfaz VLAN 1 queda en estado down porque no se asignó ninguno de los puertos a la VLAN 1. Después de unos segundos, la VLAN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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

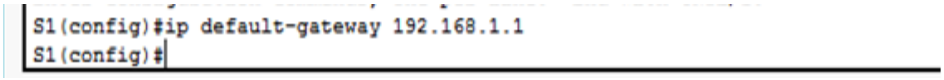
```
S1# show vlan brief

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
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

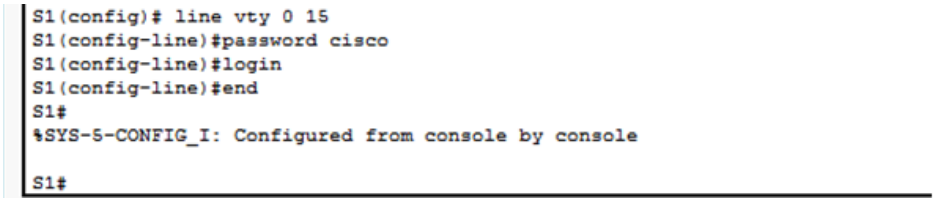


n. También se debe restringir el acceso del puerto de consola. La configuración predeterminada permite todas las conexiones de consola sin necesidad de introducir una contraseña. Para evitar que los mensajes de consola interrumpan los comandos, use la opción **logging synchronous**.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit
S1(config)#
```

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

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```



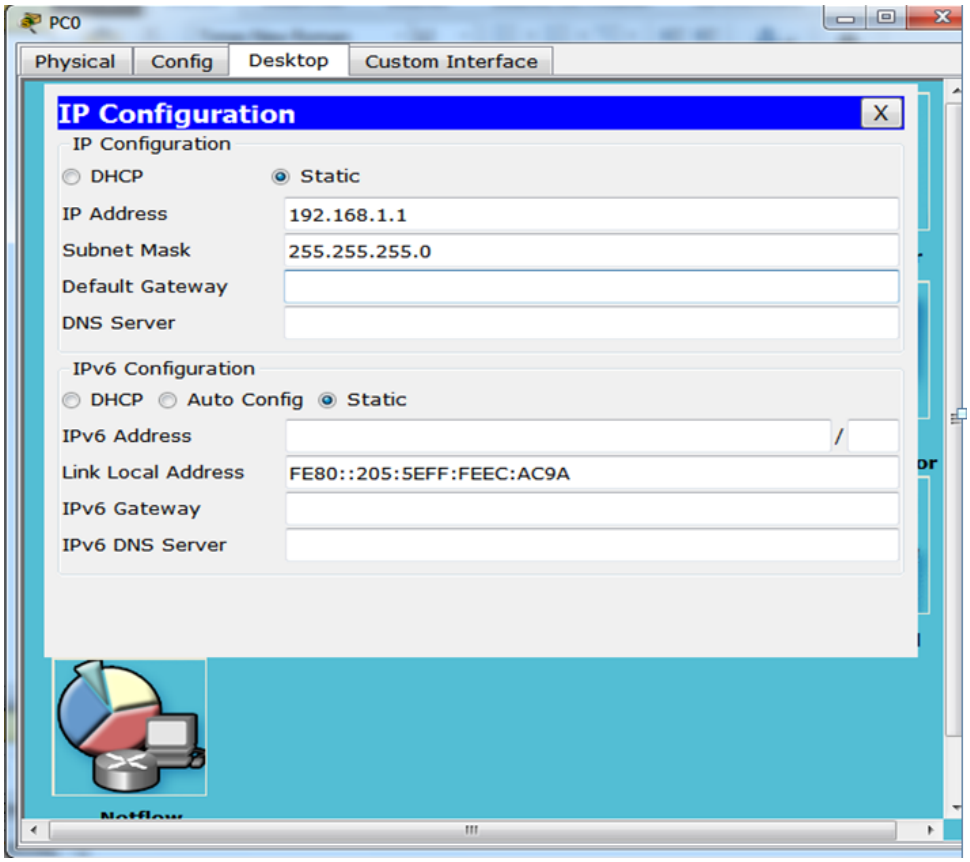
¿Por qué se requiere el comando **login**?
Porque sin el login el switch no mostrará la petición de password

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 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.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 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.

Paso 1. mostrar la configuración del switch.

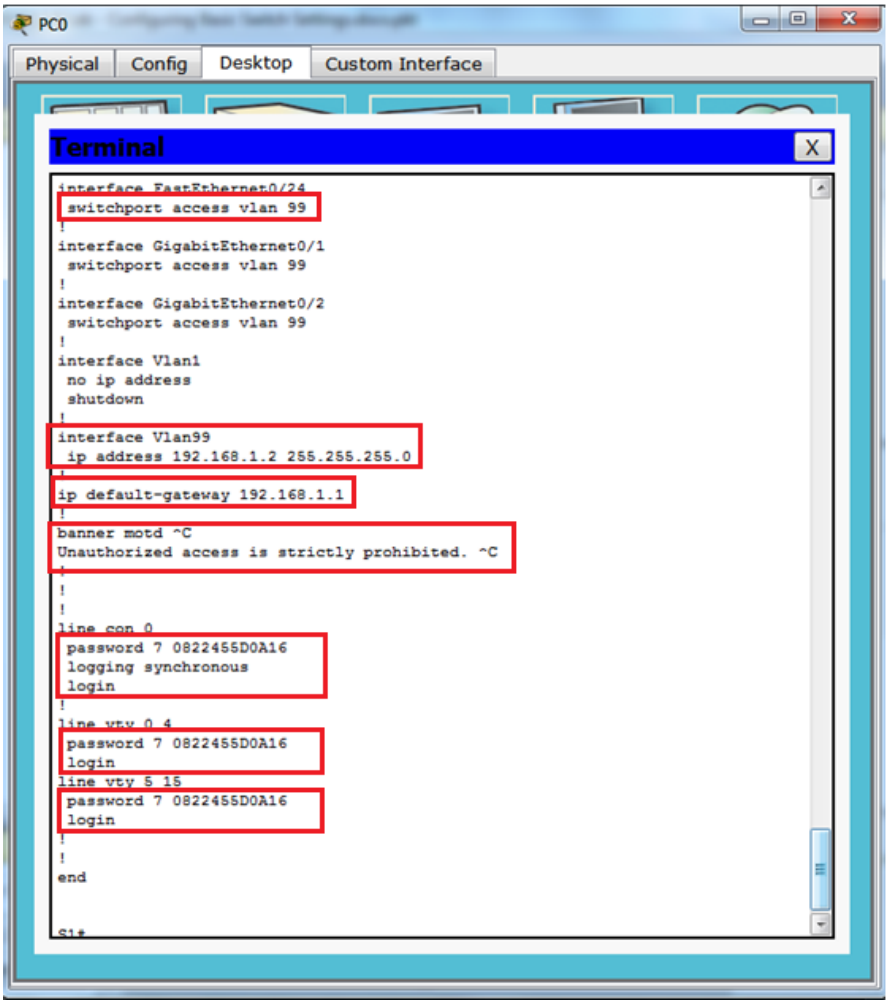
Desde la conexión de consola en la PC-A, muestre y verifique la configuración del switch. El comando **show run** muestra la configuración en ejecución completa, de a una página por vez. Utilice la barra espaciadora para avanzar por las páginas.

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

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

Current configuration : 2206 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<output omitted>
!
interface FastEthernet0/24
 switchport access vlan 99
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

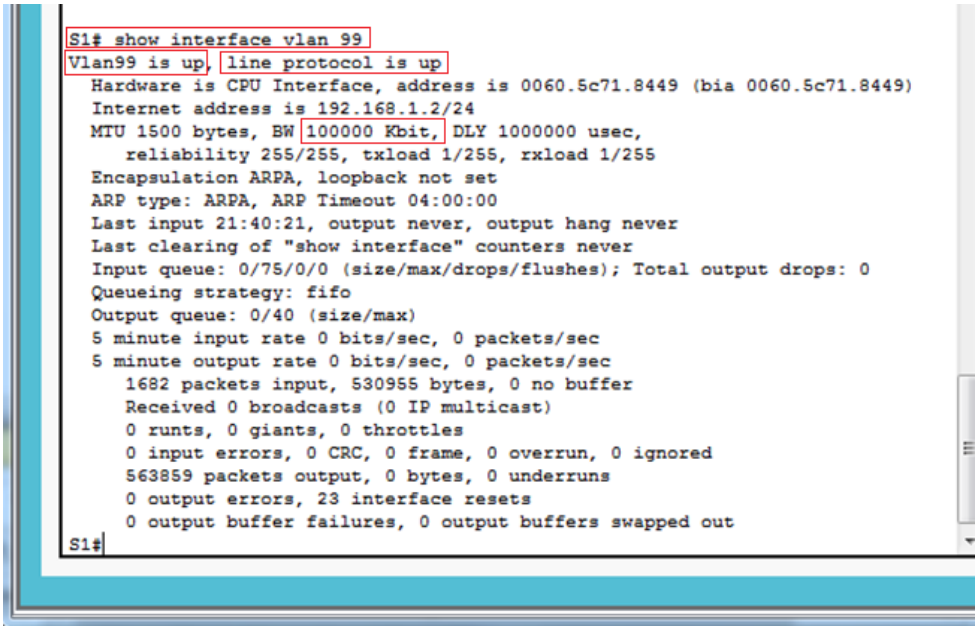
```
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password 7 104D000A0618
 logging synchronous
 login
line vty 0 4
 password 7 14141B180F0B
 login
line vty 5 15
 password 7 14141B180F0B
 login
!
end

S1#
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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
```



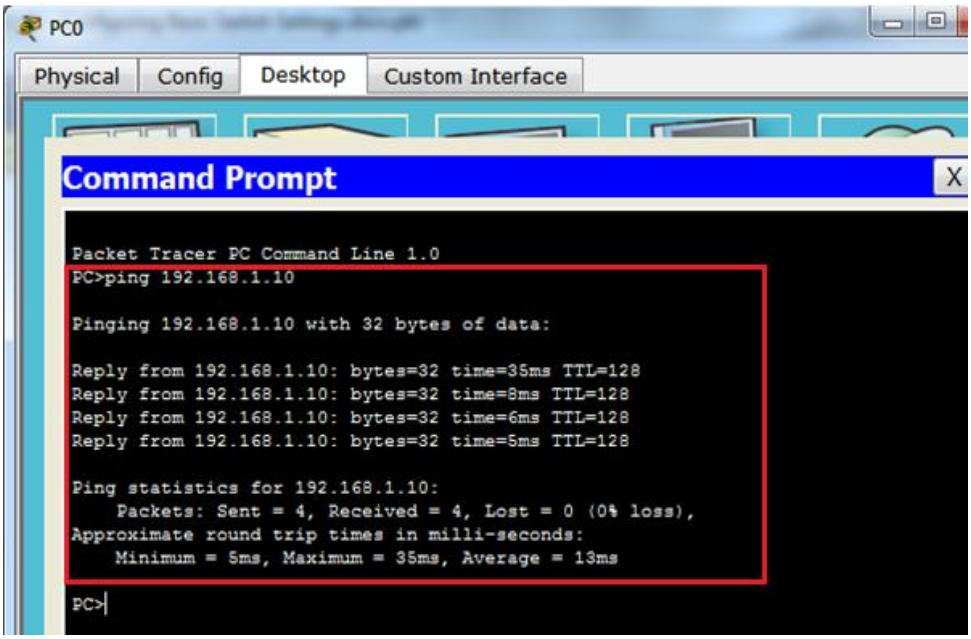
¿Cuál es el ancho de banda en esta interfaz? 1000000 Kb/s (1 Gb/sec)
¿Cuál es el estado de la VLAN 99? up
¿Cuál es el estado del protocolo de línea? Up

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

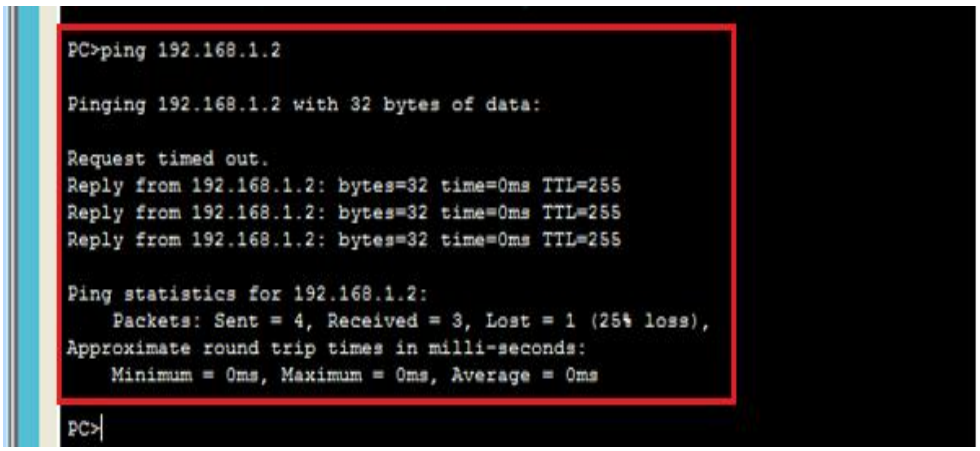
`C:\Users\User1>` **`ping 192.168.1.10`**



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

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

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 3. probar y verificar la administración remota del S1.

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

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

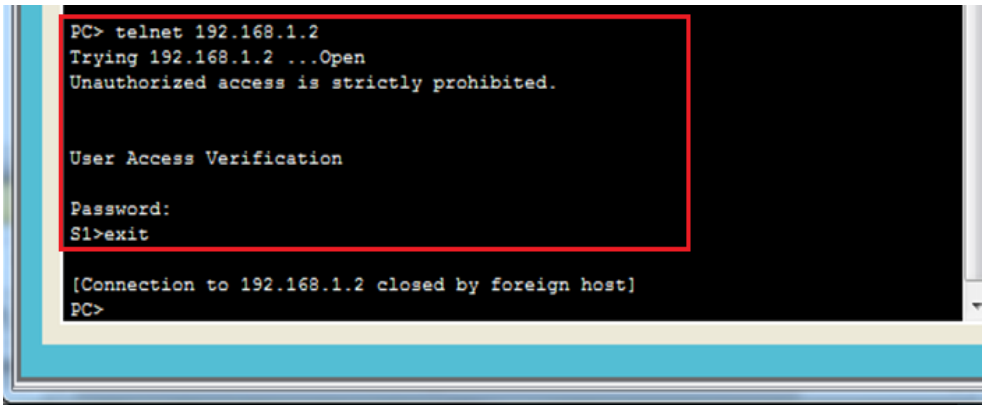
```
C:\Users\User1> pkgmgr /iu:"TelnetClient"
```

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

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

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

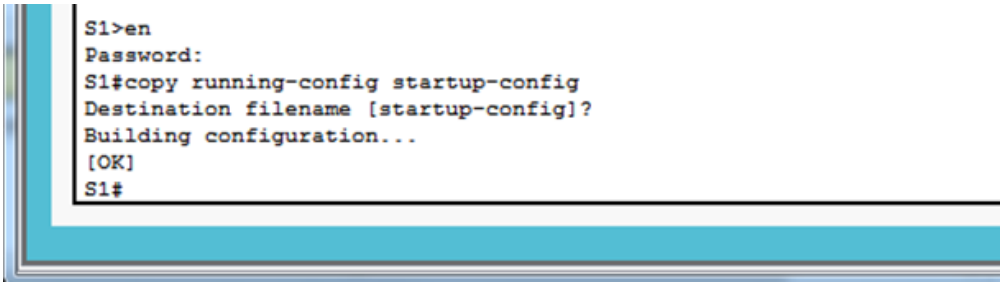
c. Escriba **exit** para finalizar la sesión de Telnet.



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

Guarde la configuración.

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

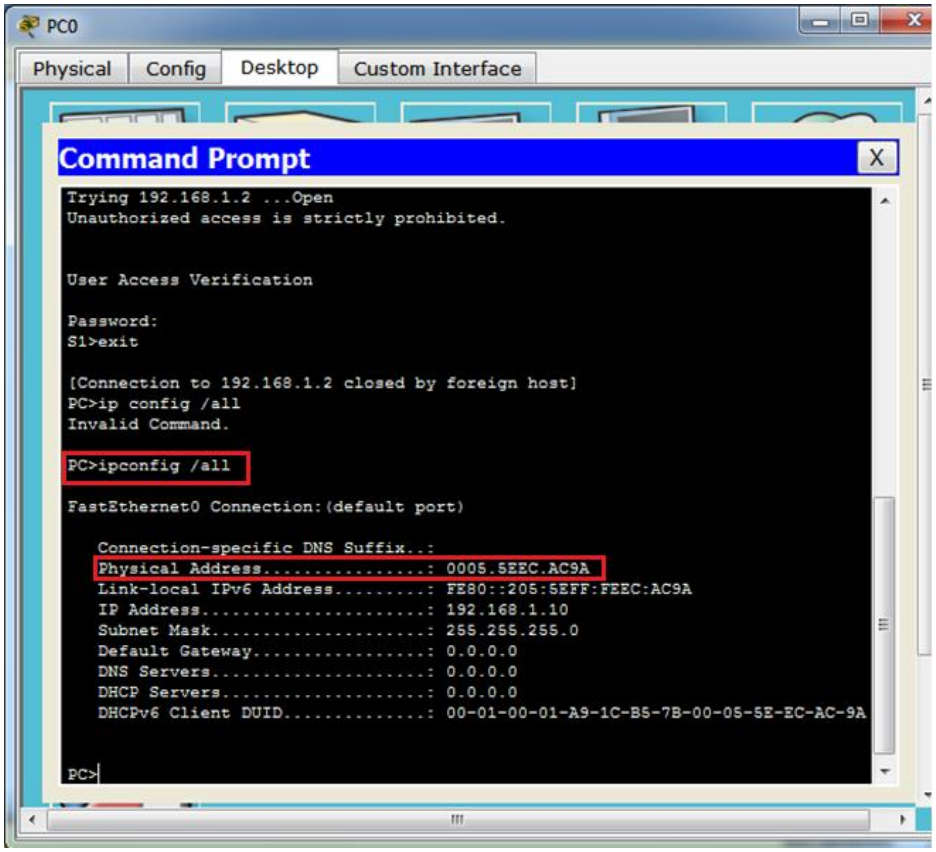
Parte 4: Administrar la tabla de direcciones MAC

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.

Paso 1. registrar la dirección MAC del host.

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

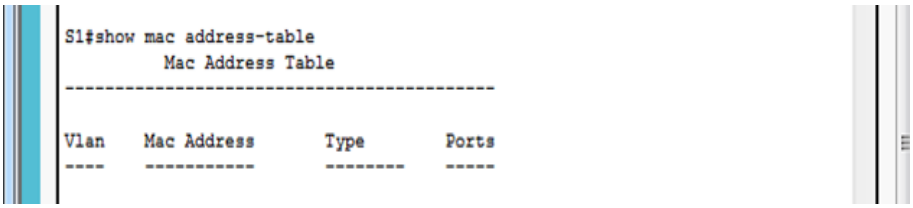
PC-A: 005.SEEC.AC9A



Paso 2. Determine las direcciones MAC que el switch ha aprendido.

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

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



¿Cuántas direcciones dinámicas hay? 1

¿Cuántas direcciones MAC hay en total? 1

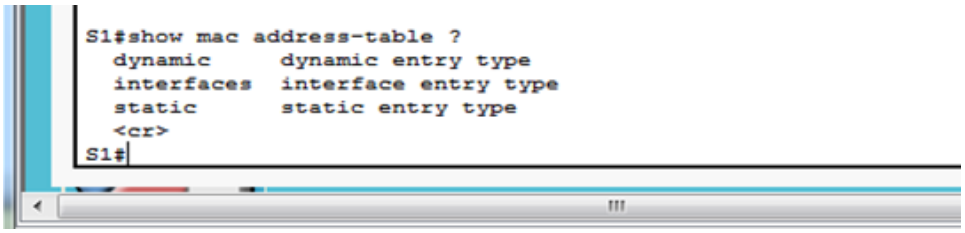
¿La dirección MAC dinámica coincide con la dirección MAC de la PC-A? Si

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

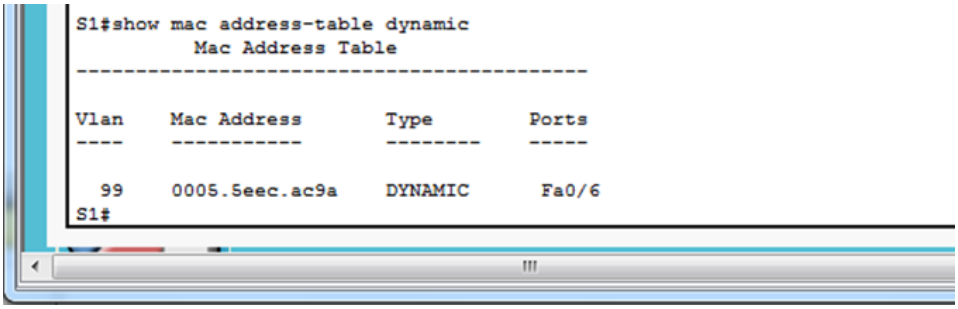
```
S1# show mac address-table ?
```



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

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

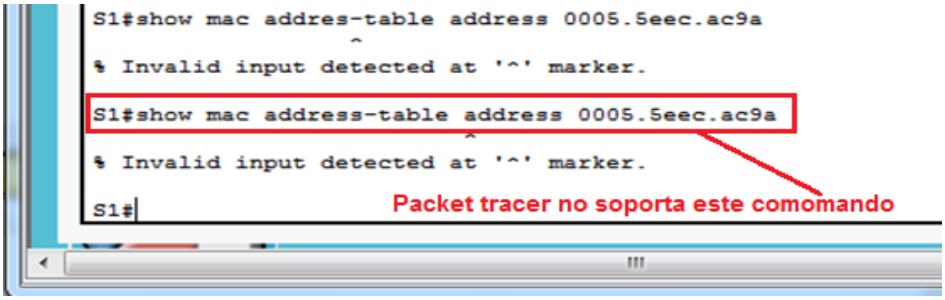
```
S1# show mac address-table dynamic
```



¿Cuántas direcciones dinámicas hay? 1

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

```
S1# show mac address-table address 0005.5eec.ac9a
```



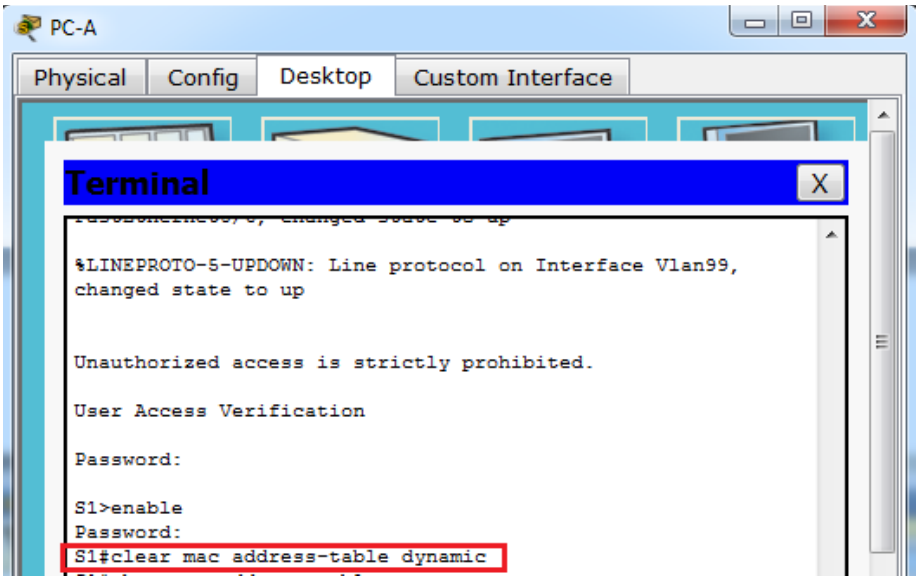
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 4. Configure una dirección MAC estática.

a. limpie la tabla de direcciones MAC.

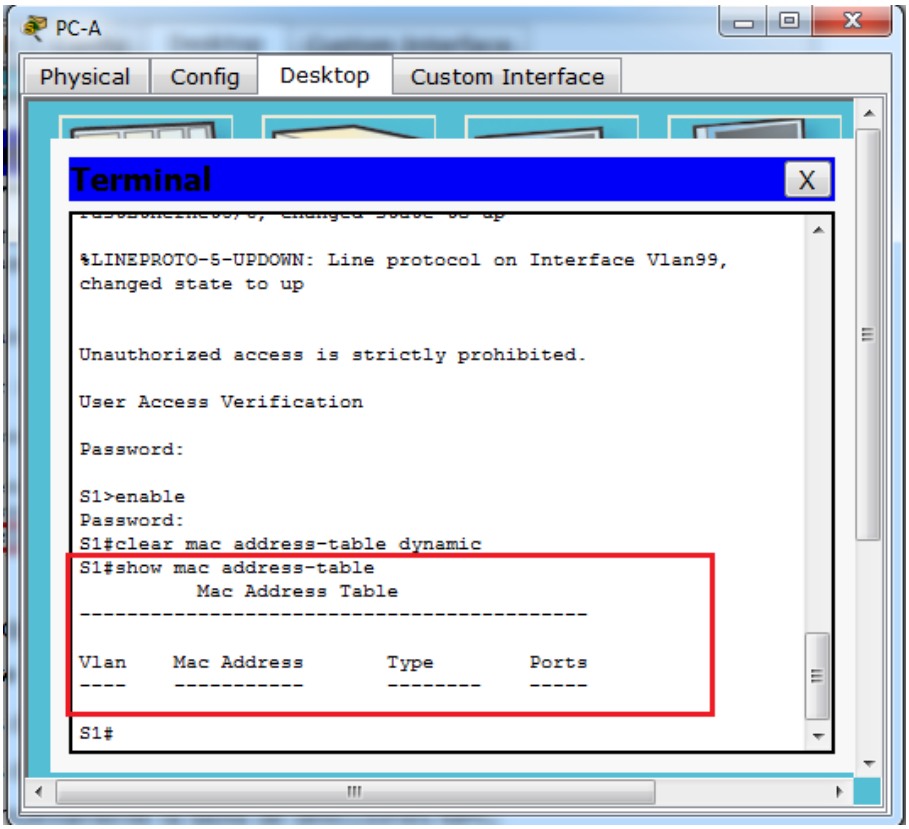
Para eliminar las direcciones MAC existentes, use el comando **clear mac address-table** del modo EXEC privilegiado.

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



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

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

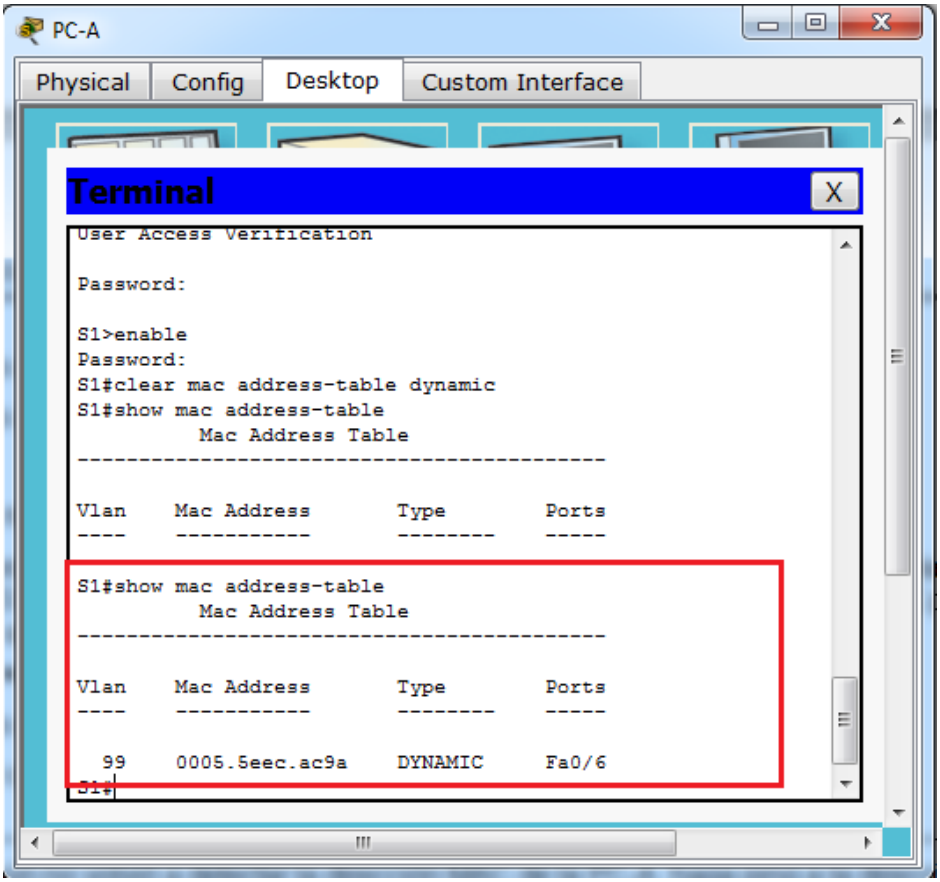
¿Cuántas direcciones MAC estáticas hay? 0

¿Cuántas direcciones dinámicas hay? 0

c. Examine nuevamente la tabla de direcciones MAC

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

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



¿Cuántas direcciones dinámicas hay? 1

¿Por qué cambió esto desde la última visualización? Porque el switch aprende la dirección MAC de la pc

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**.

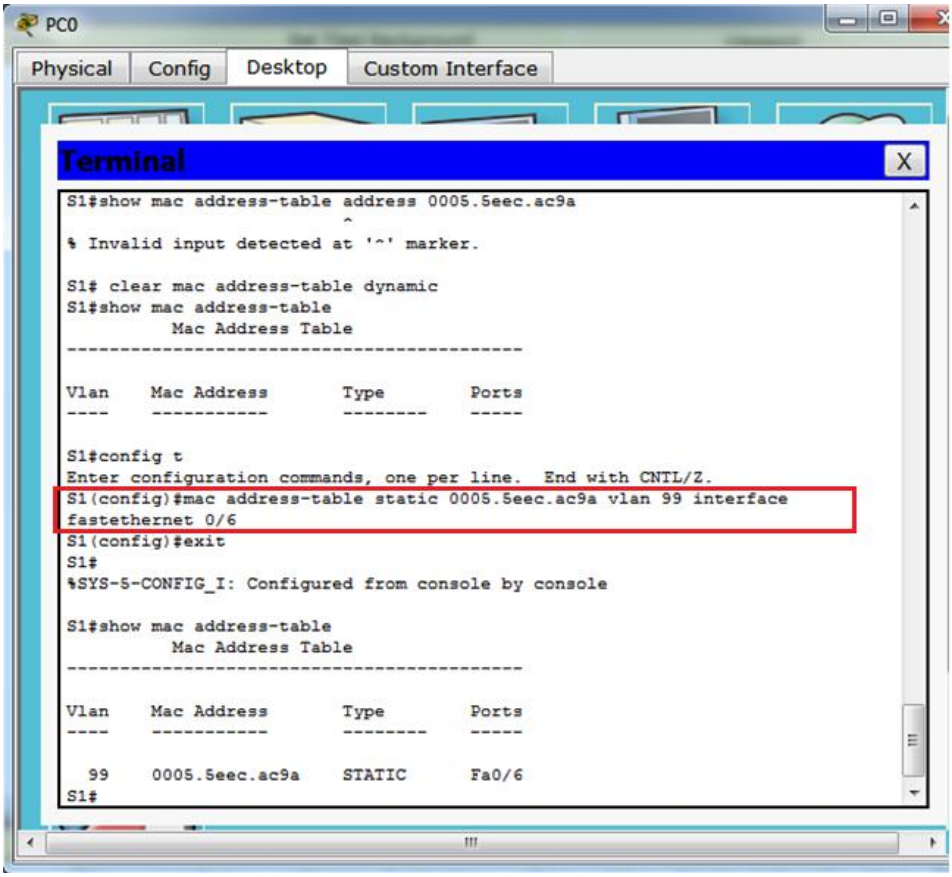
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

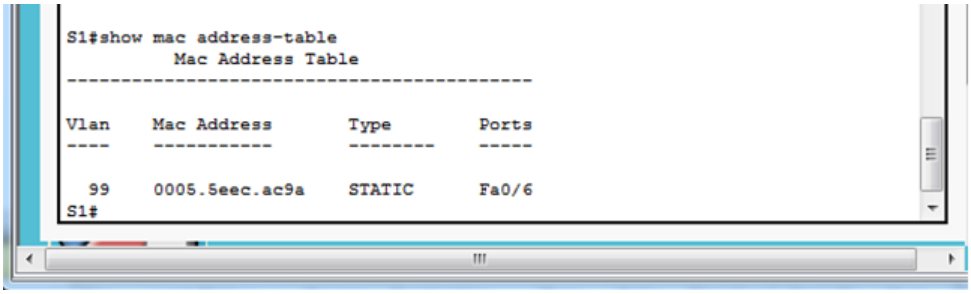
Configure una dirección MAC estática en F0/6 con la dirección que se registró para la PC-A en la parte 4, paso 1. La dirección MAC 0050.56BE.6C89 se usa solo como ejemplo. Debe usar la dirección MAC de su PC-A, que es distinta de la del ejemplo.

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



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

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



¿Cuántas direcciones MAC hay en total? 1

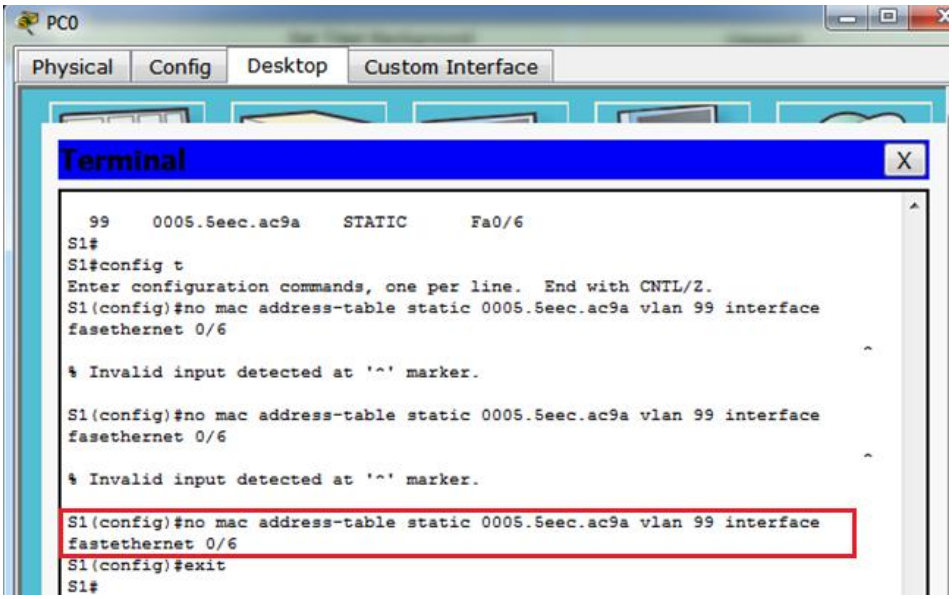
¿Cuántas direcciones estáticas hay? 1

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

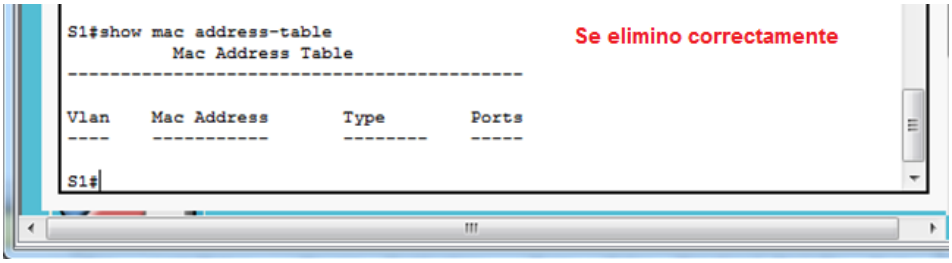
Nota: la dirección MAC 0050.56BE.6C89 se usa solo en el ejemplo. Use la dirección MAC de su PC-A.

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



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

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



¿Cuántas direcciones MAC estáticas hay en total? 0

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Reflexión

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

   Porque si no se configura el password en las vty no se podrá hacer tlenet al switch

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

   Para tener mejor seguridad

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

   Con el comando password-encryption

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

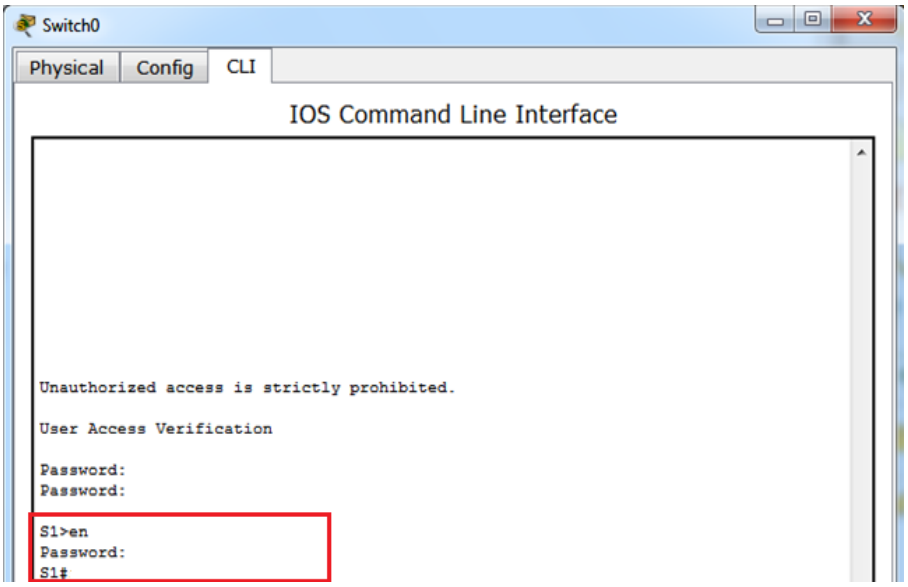
   Para especificar a qué puertos se debe conectar una computadora

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

Paso 1. Inicializar y volver a cargar el switch.

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

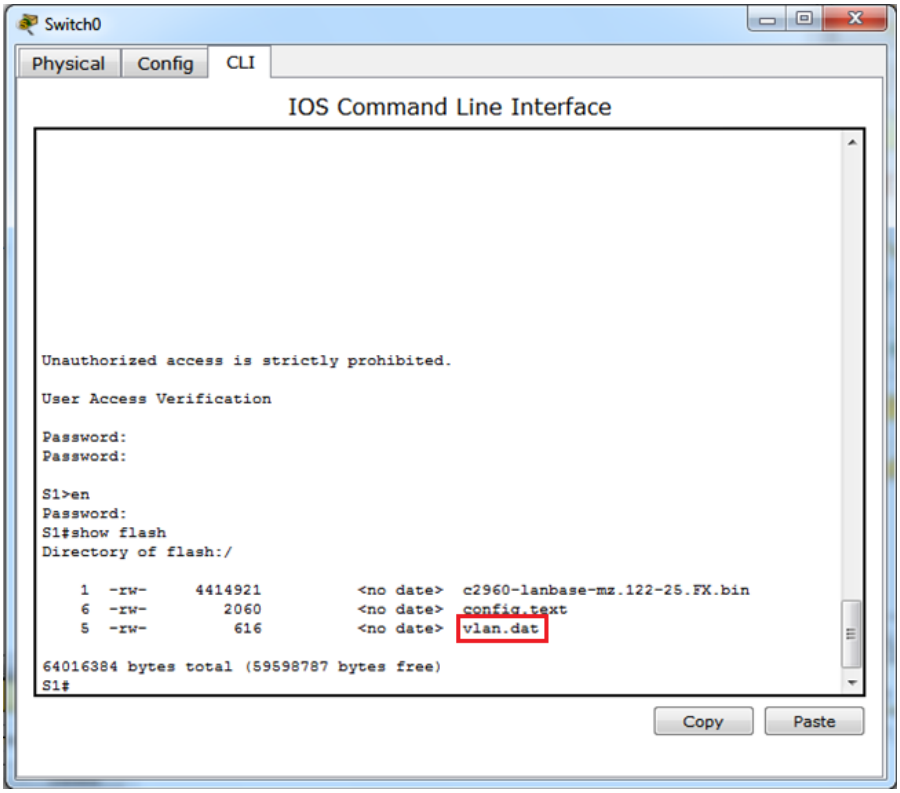
```
Switch> enable
Switch#
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

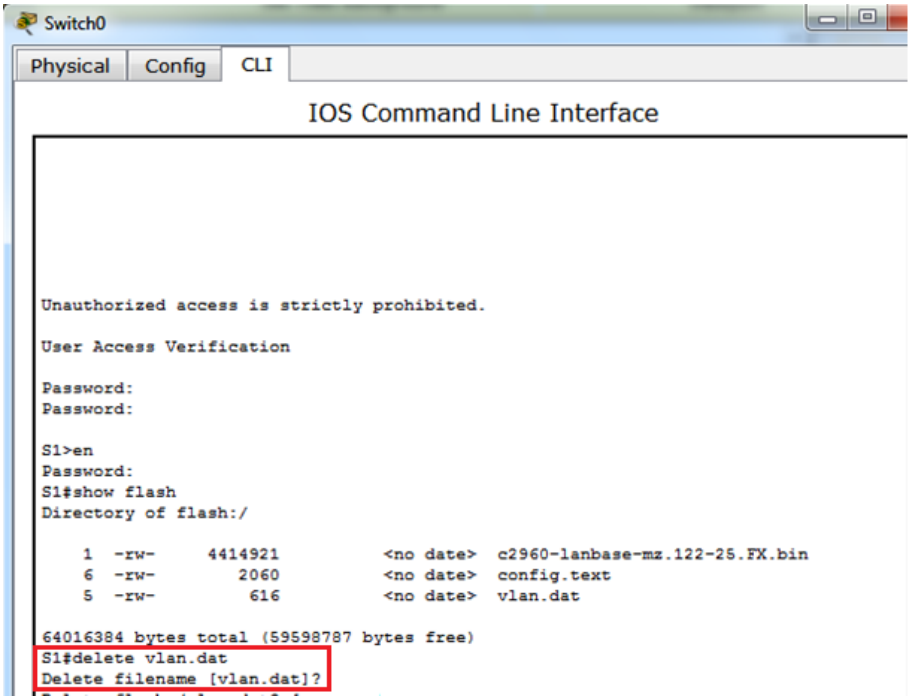
```
Switch# show flash
Directory of flash:/

    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#
```



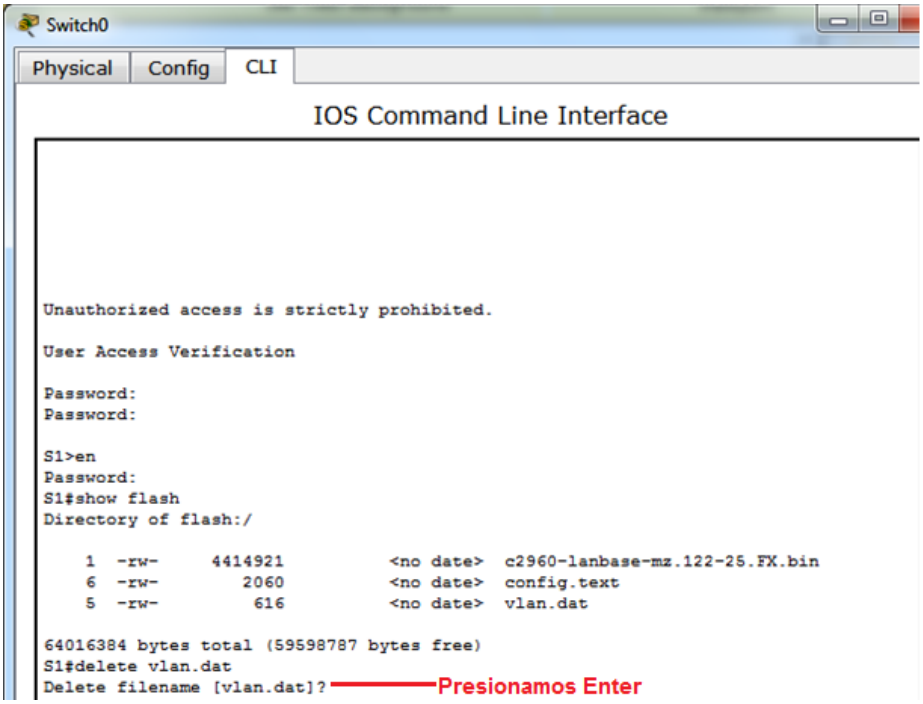
c. Si se encontró el archivo **vlan.dat** en la memoria flash, elimínelo.

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



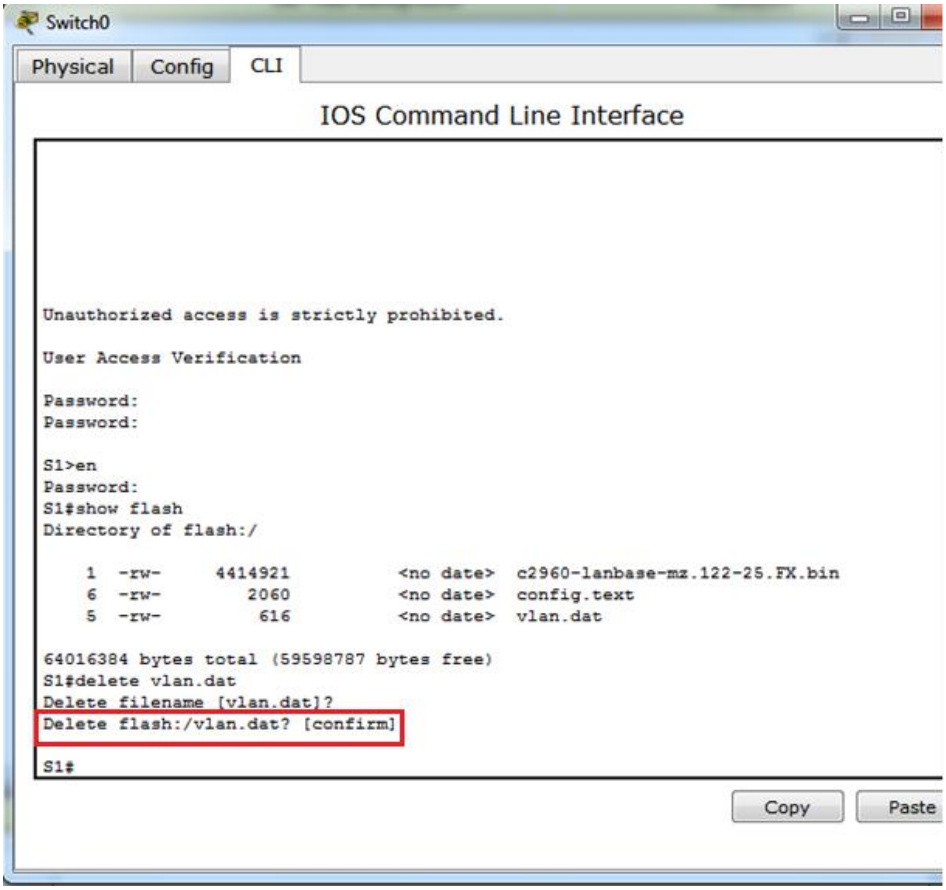
d. Se le solicitará que verifique el nombre de archivo. Si introdujo el nombre correctamente, presione Enter; de lo contrario, puede cambiar el nombre de archivo.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

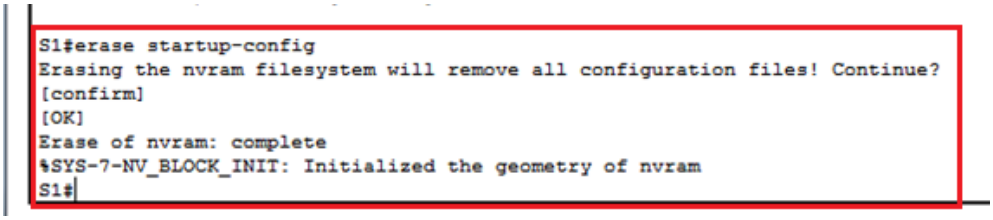
e. Se le solicita que confirme la eliminación de este archivo. Presione Intro para confirmar.

```
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 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#
```



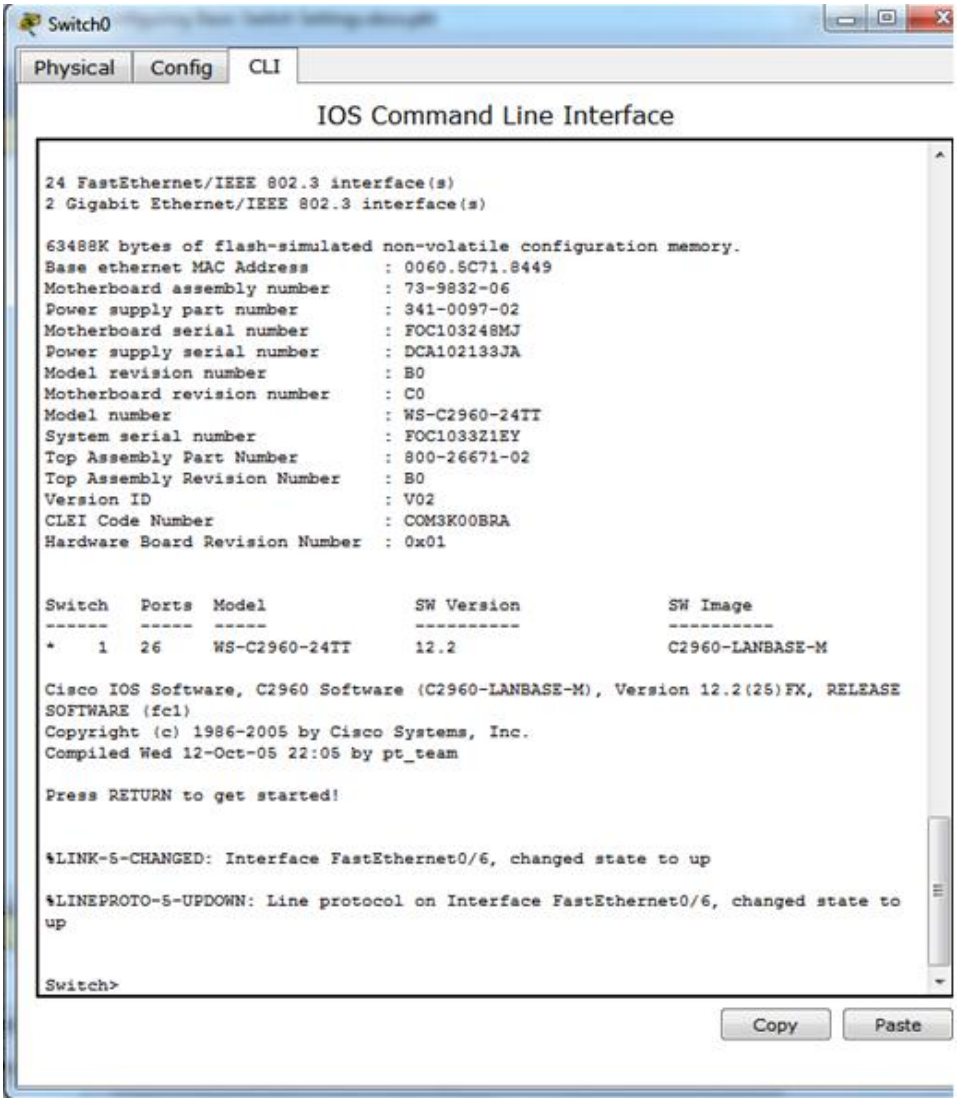
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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>
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

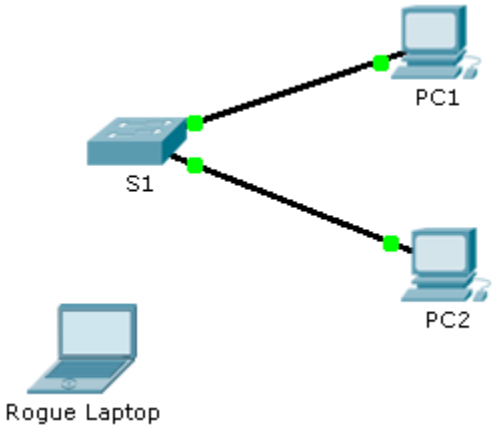
Conclusiones informe 1

- Por medio de la anterior práctica realizamos el tendido de cableado de red, verificamos la configuración del switch, configurando los parámetros básicos necesarios de los dispositivos de red, verificamos y probamos la conectividad de red, mostrando, probando las capacidades, guardamos los archivos, administramos las tablas de direcciones MAC, registramos y determinamos las direcciones MAC, y aprendemos diferentes comandos de configuración desde la consola.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 2: 2.2.4.9 Packet Tracer - Configuring Switch Port Security

Topology



Addressing Table

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

Objective

Part 1: Configure Port Security
Part 2: Verify Port Security

Background

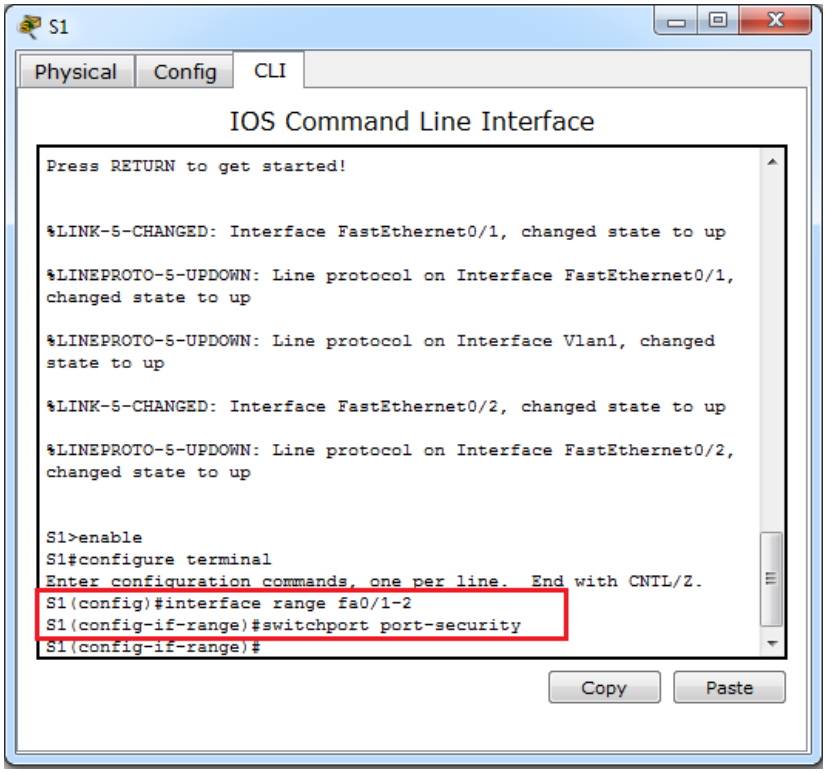
In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

Part 1: Configure Port Security

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

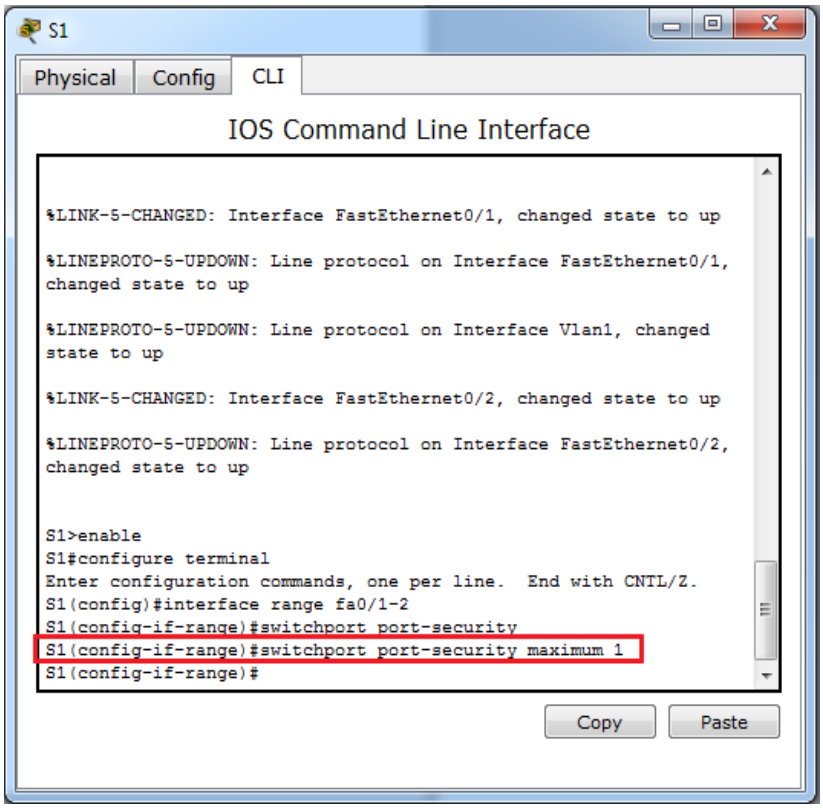
```
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# switchport port-security
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



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

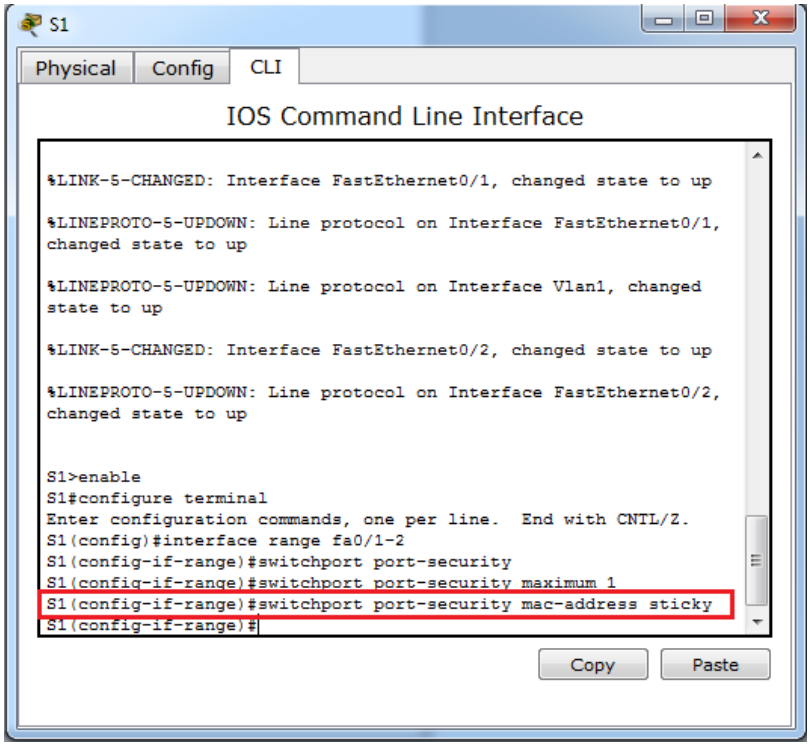
```
S1(config-if-range)# switchport port-security maximum 1
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

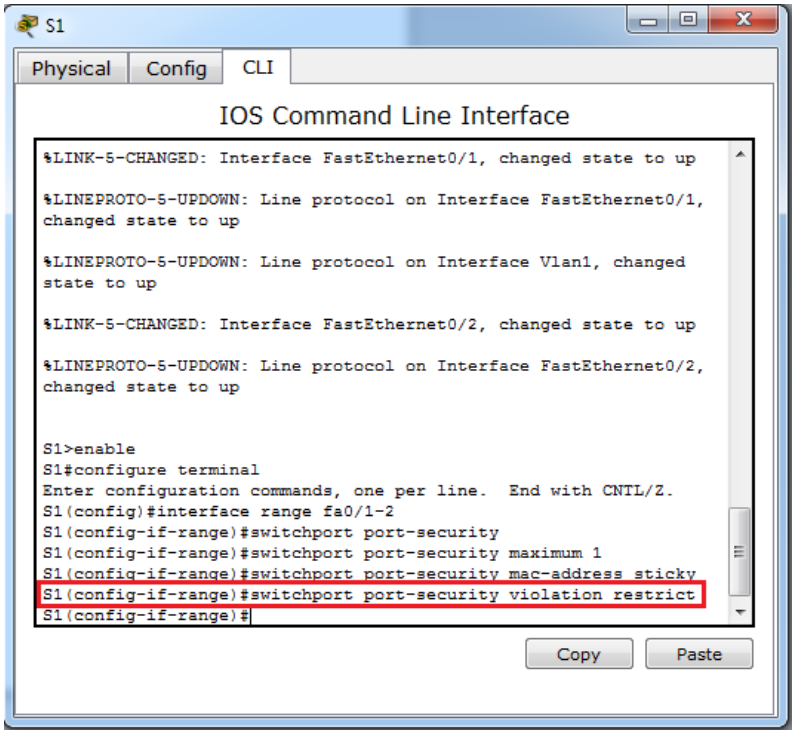
c. Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

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



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

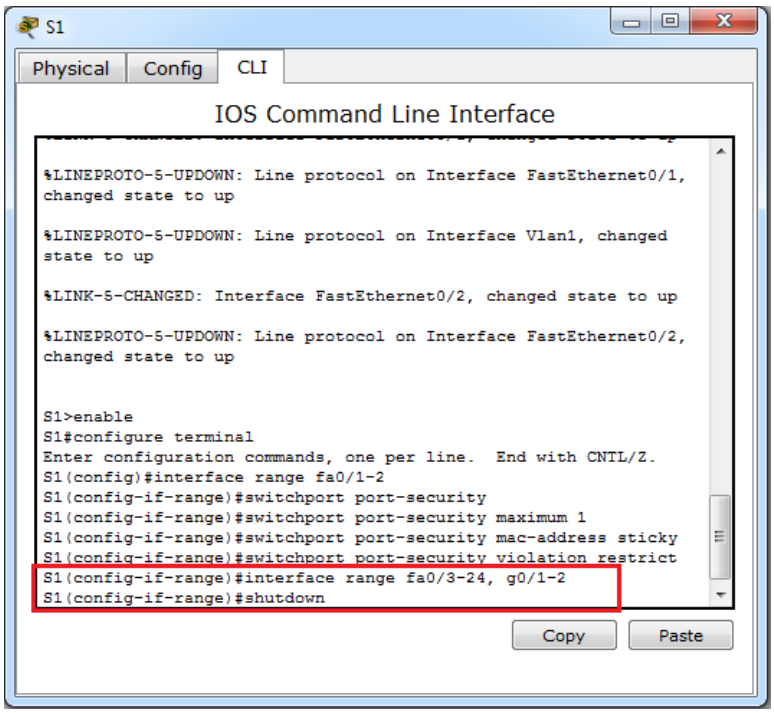
```
S1(config-if-range)# switchport port-security violation restrict
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

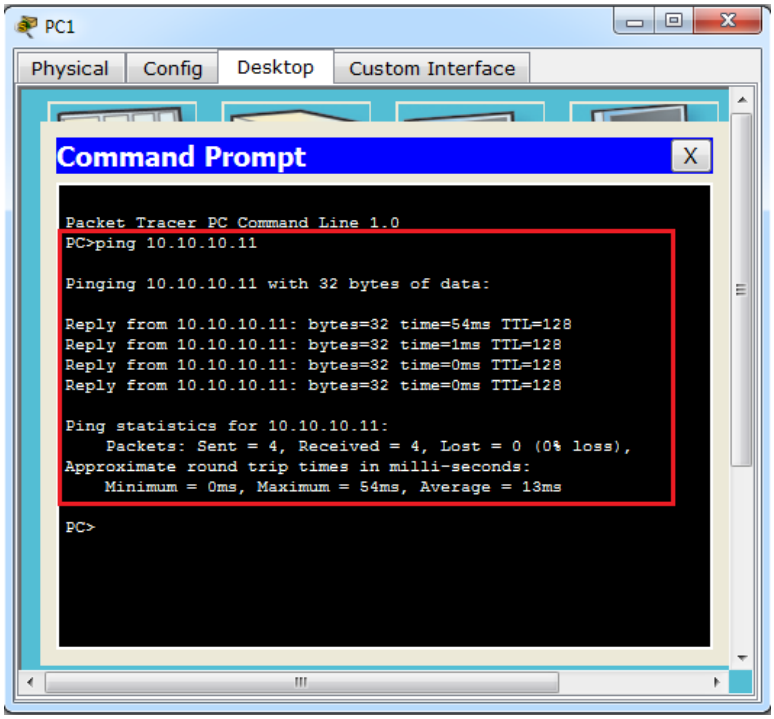
e. Disable all the remaining unused ports. Hint: Use the **range** keyword to apply this configuration to all the ports simultaneously.

```
S1(config-if-range)# interface range fa0/3 - 24 , g0/1 - 2
S1(config-if-range)# shutdown
```



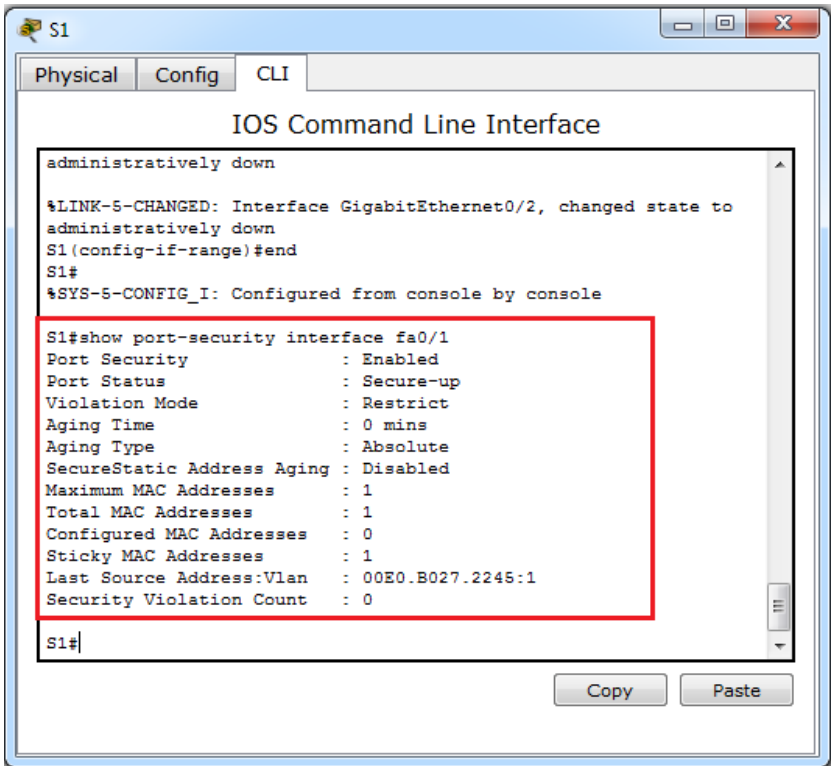
Part 2: Verify Port Security

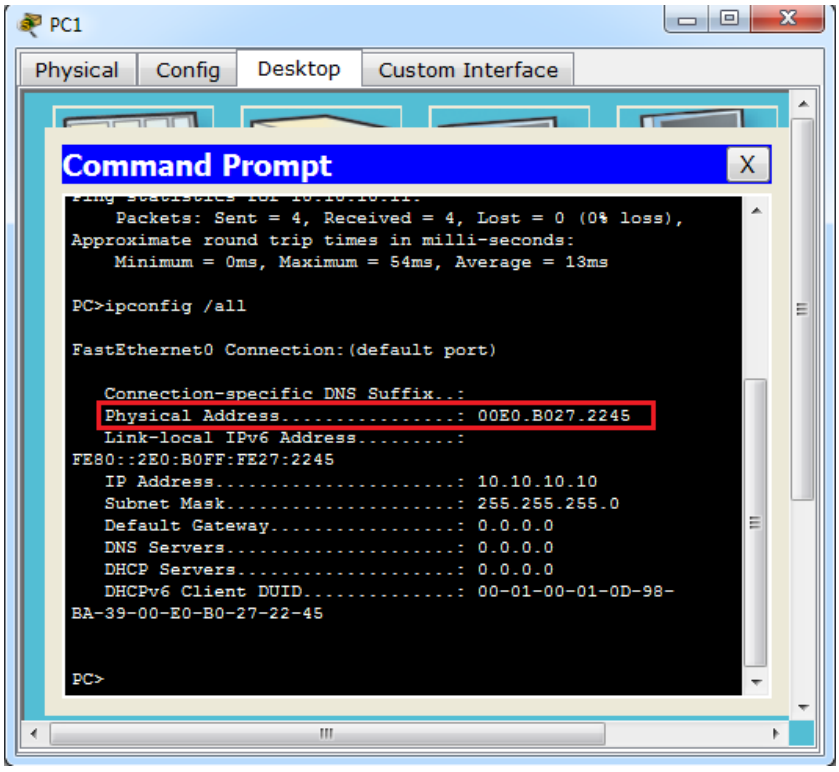
a. From **PC1**, ping **PC2**.



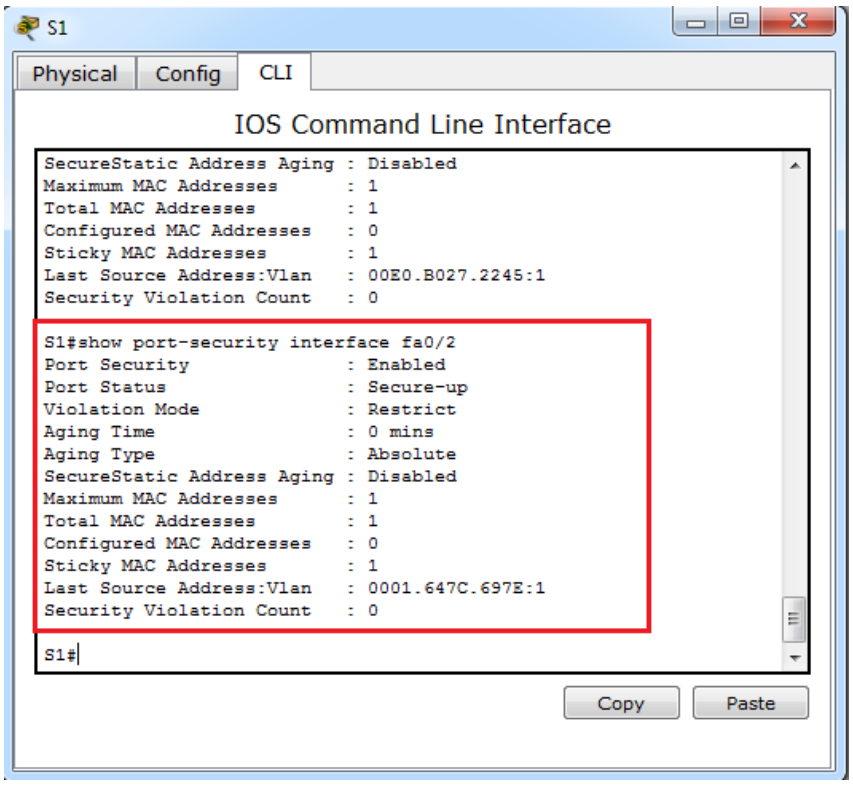
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

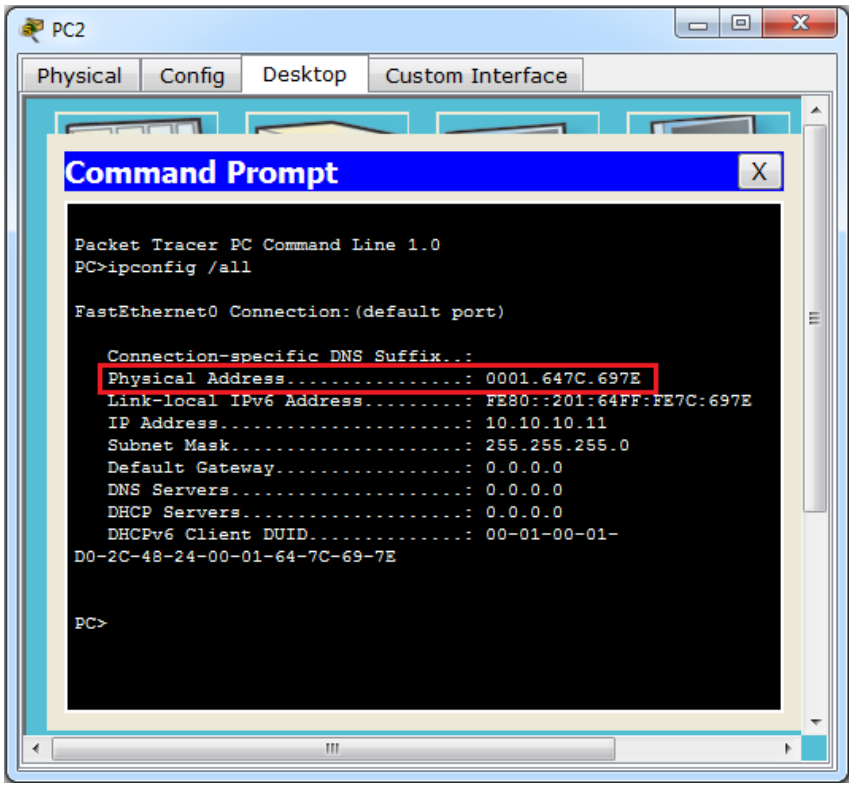
b. Verify port security is enabled and the MAC addresses of **PC1** and **PC2** were added to the running configuration.





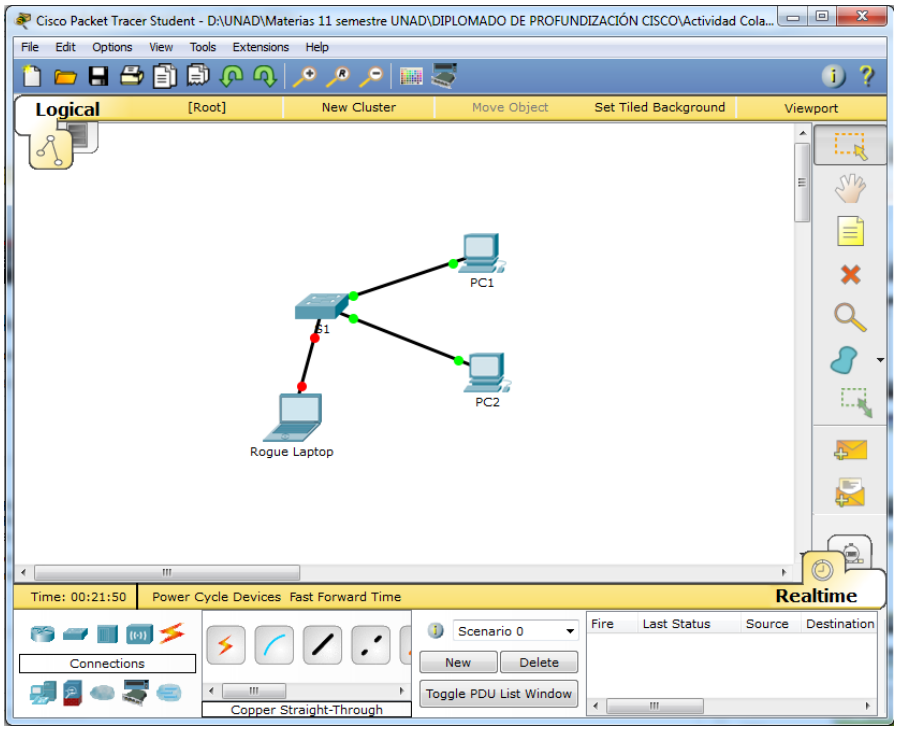
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



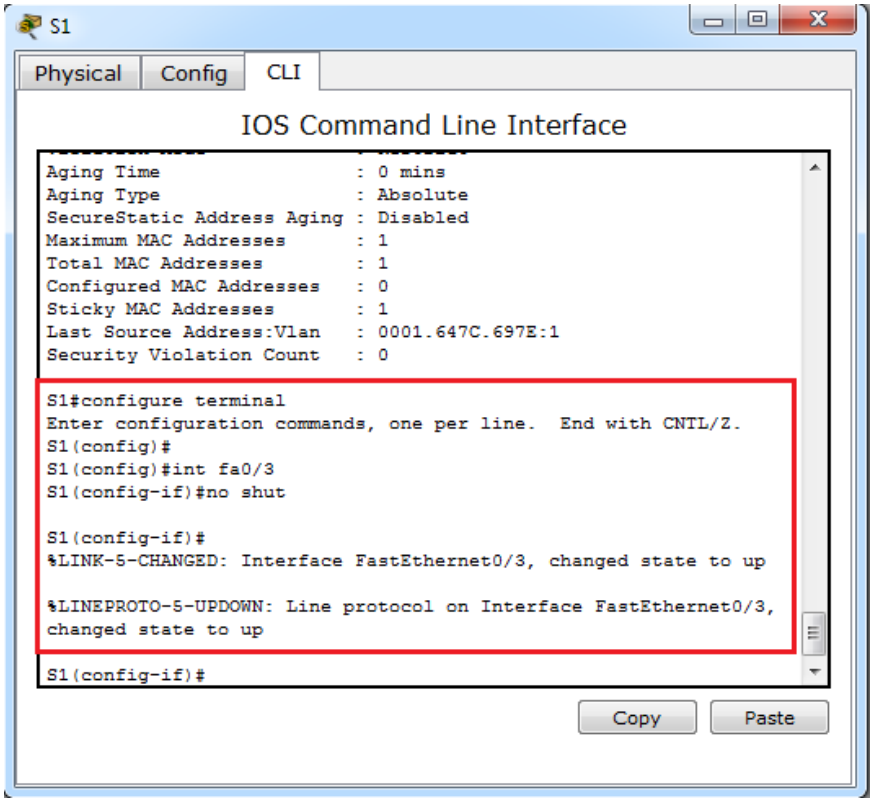


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

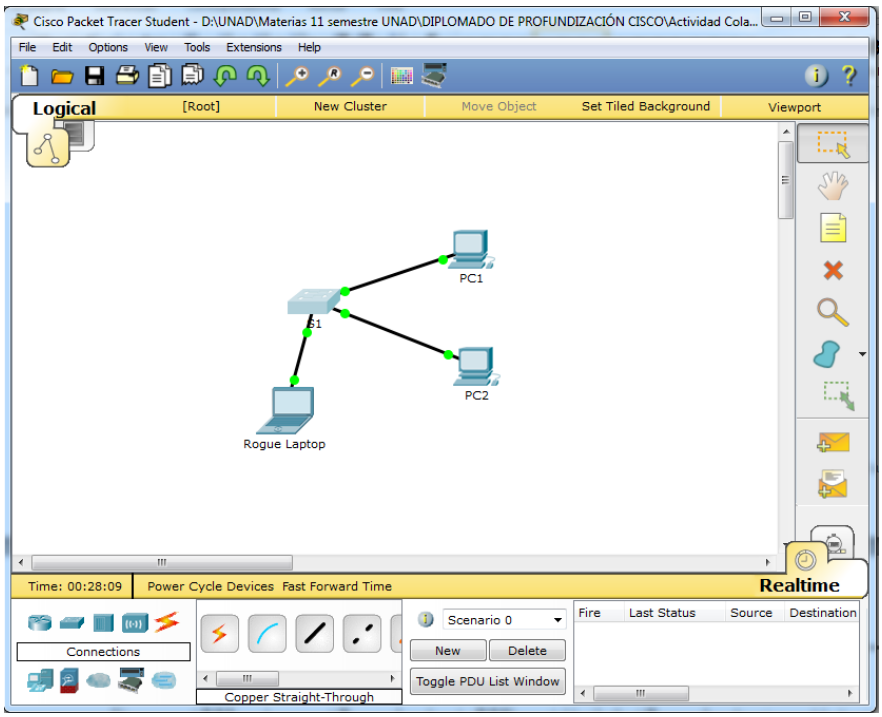
c. Attach **Rogue Laptop** to any unused switch port and notice that the link lights are red.



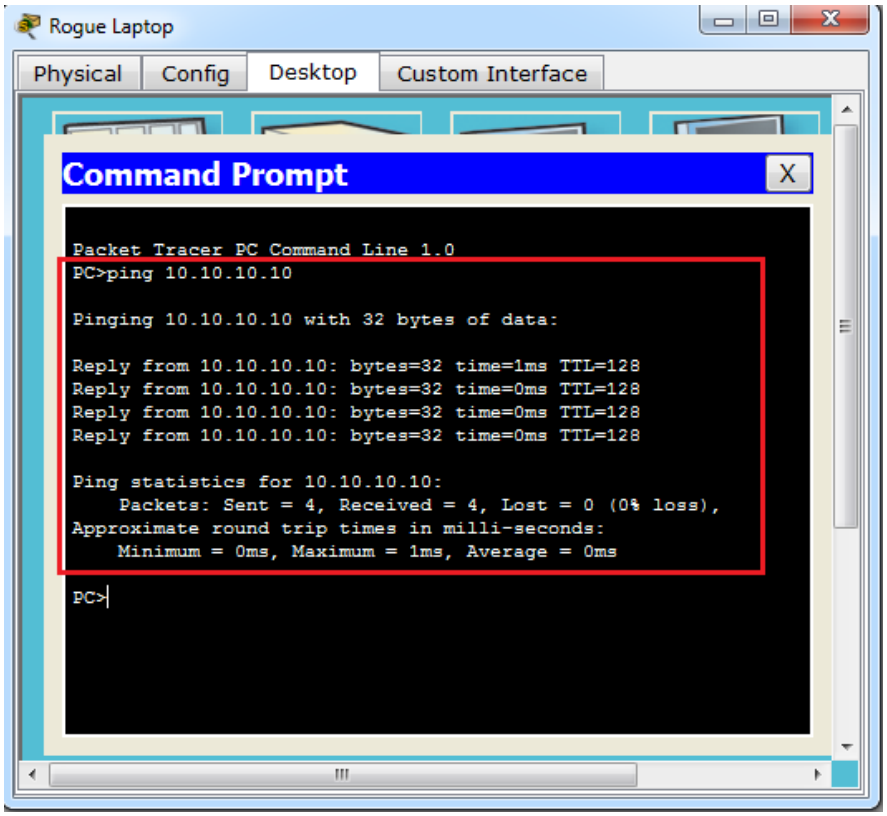
d. Enable the port and verify that **Rogue Laptop** can ping **PC1** and **PC2**. After verification, shut down the port connected to **Rogue Laptop.**



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

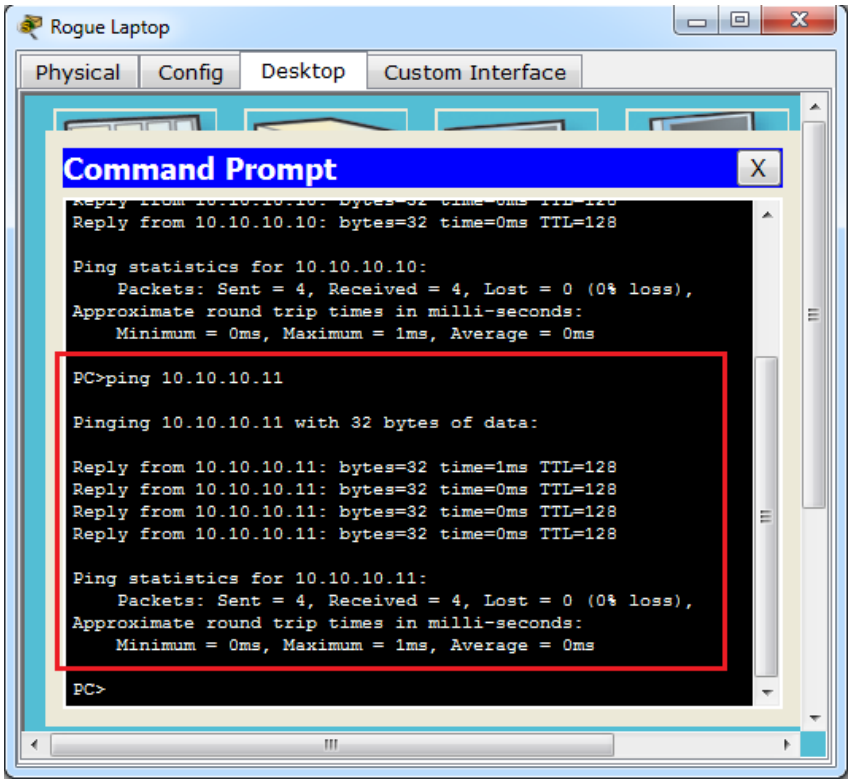


Ping de Rogue Laptop a la PC1

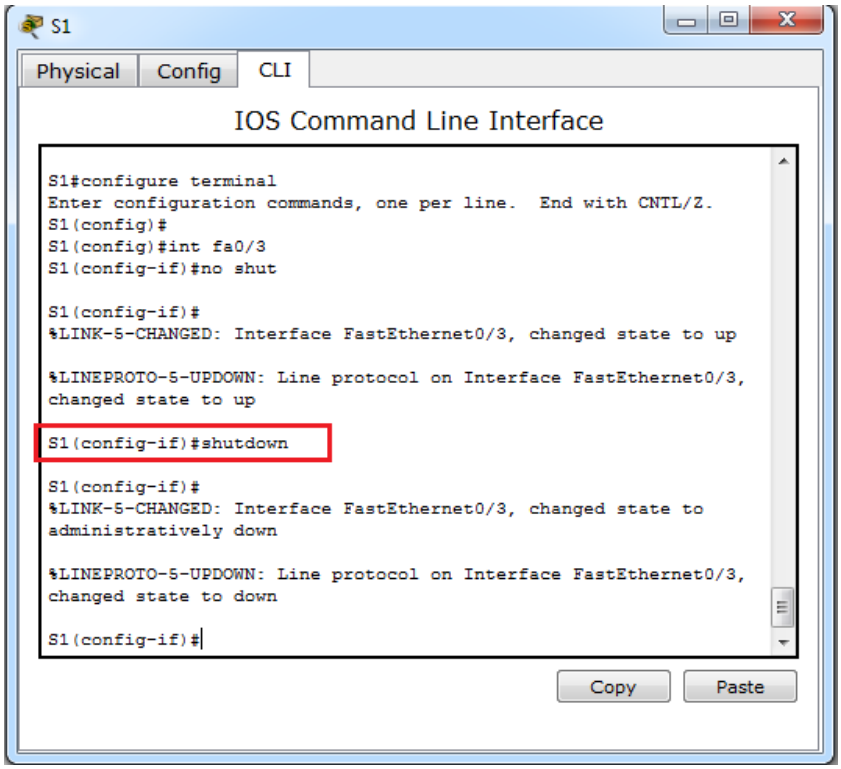


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

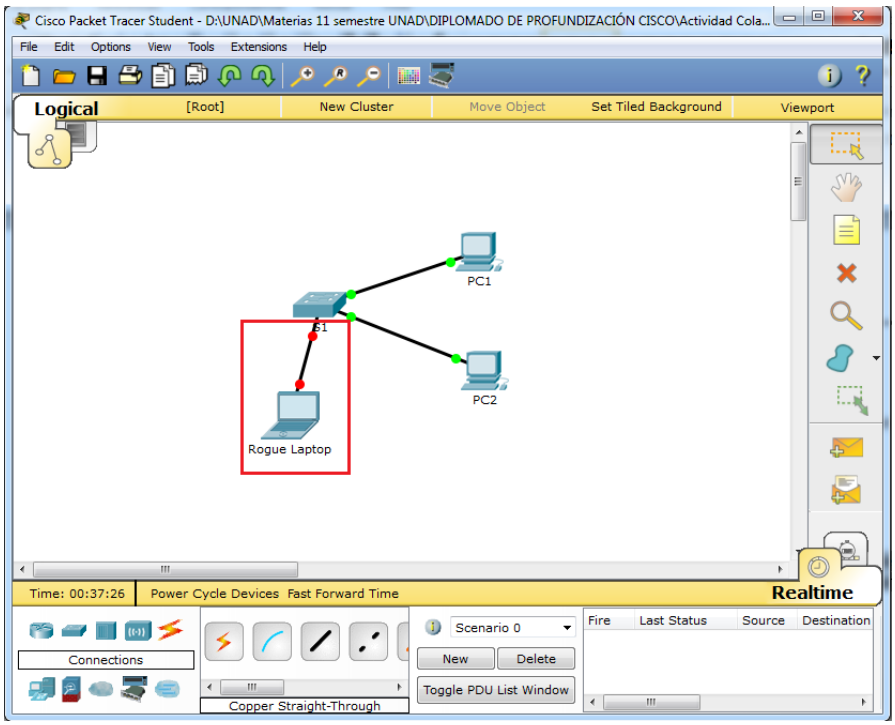
Ping de Rogue Laptop a la PC2



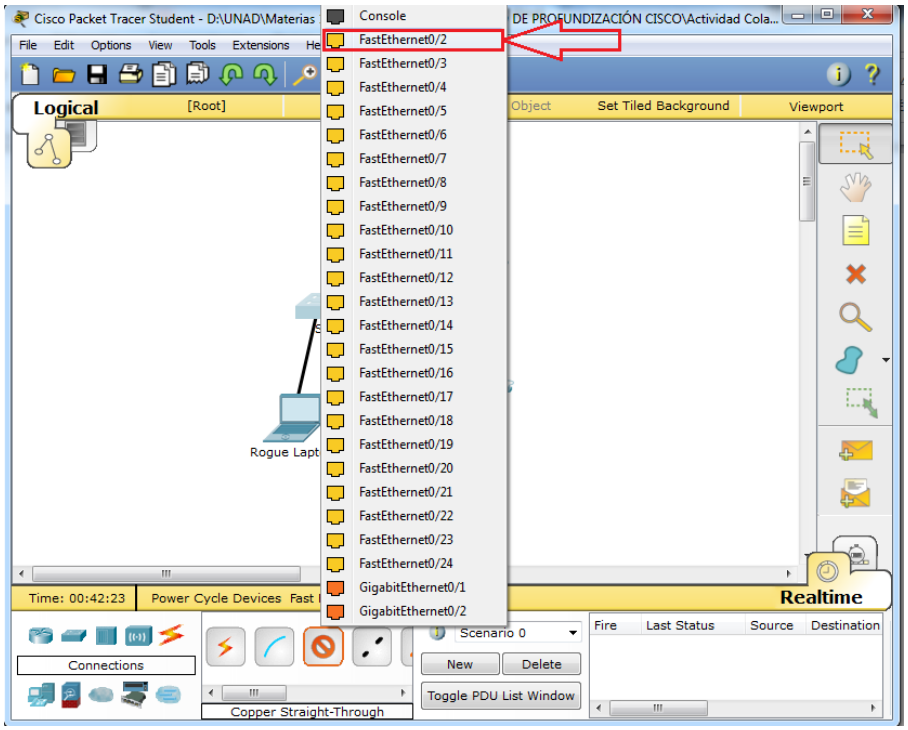
Desconectamos el puerto con shutdown



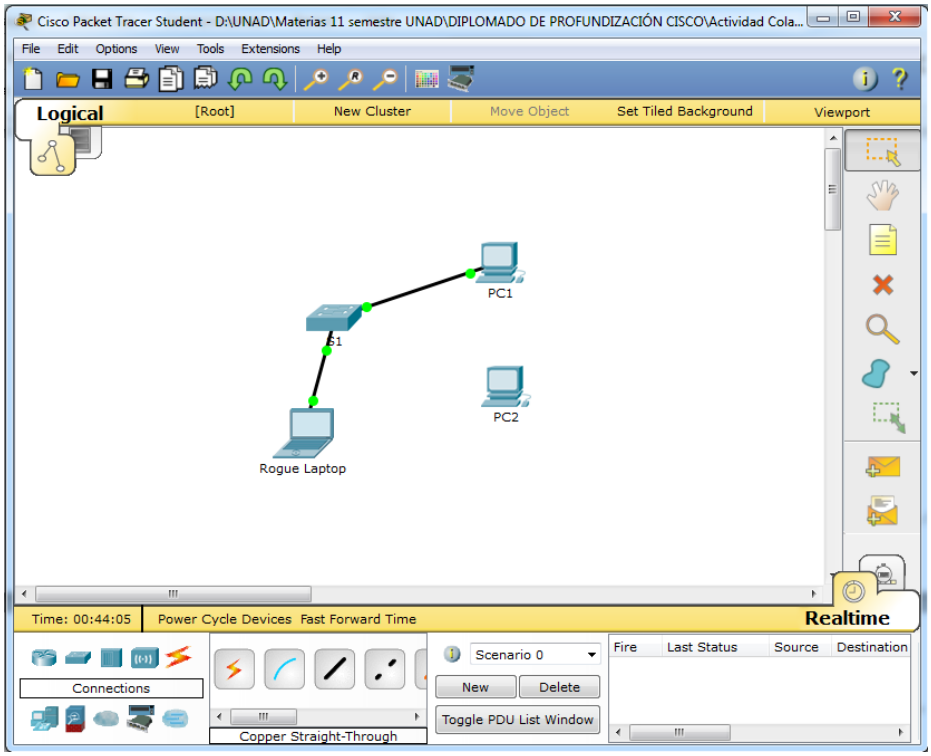
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



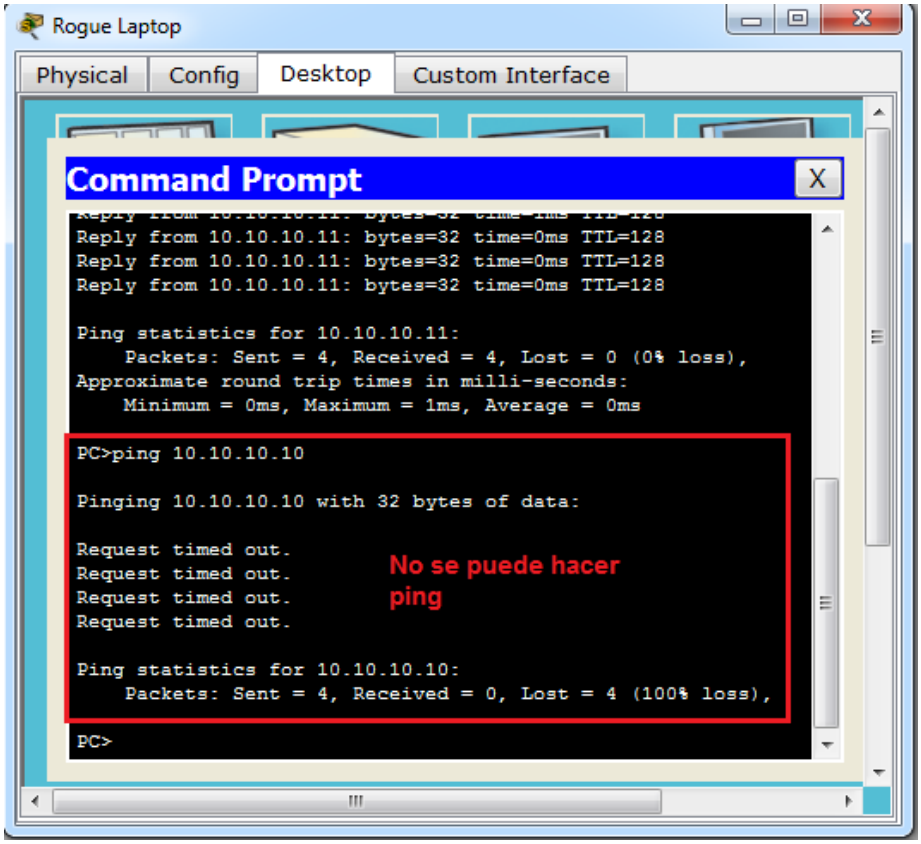
e. Disconnect **PC2** and connect **Rogue Laptop** to **PC2's** port. Verify that **Rogue Laptop** is unable to ping **PC1**.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



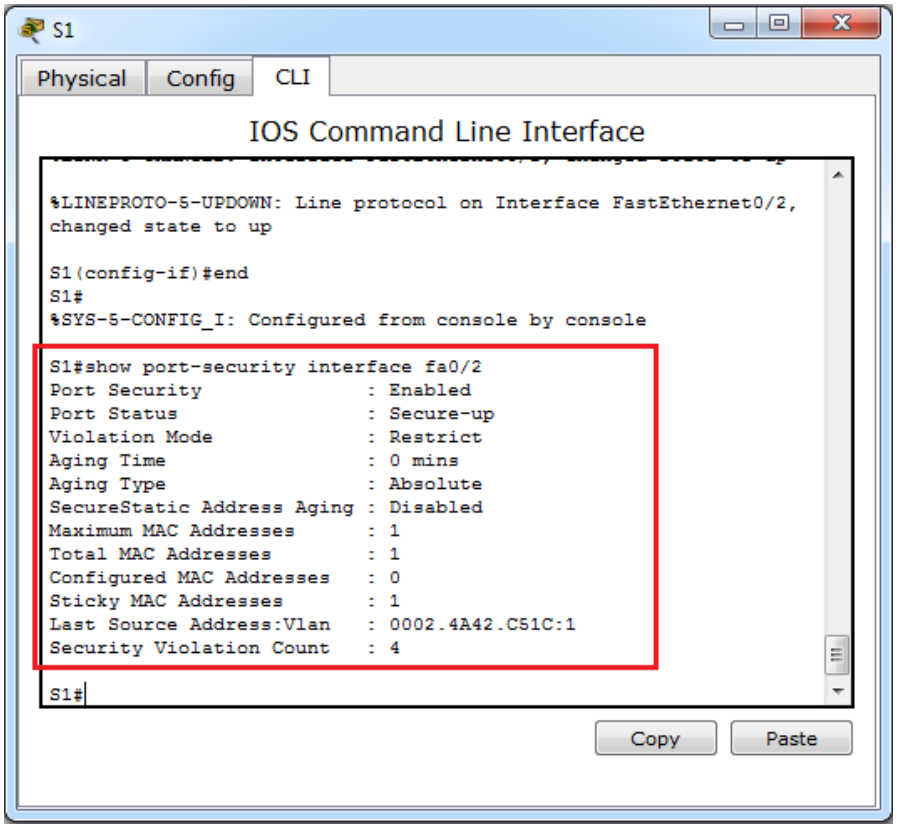
Ping de Rogue Laptop a la PC1



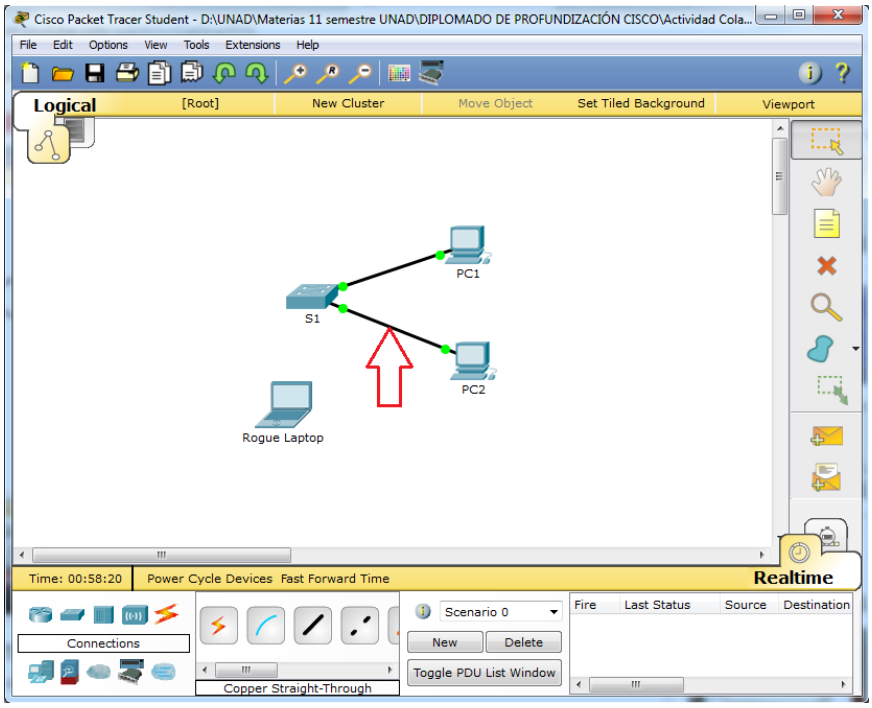
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

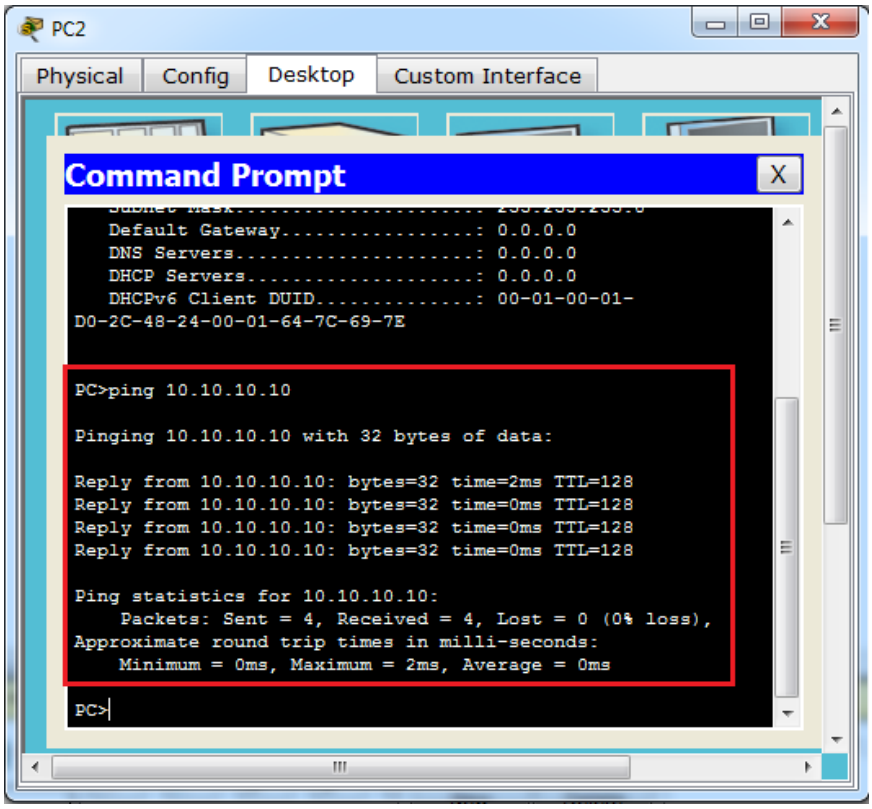


g. Disconnect **Rouge Laptop** and reconnect **PC2**. Verify **PC2** can ping **PC1**.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Ping de PC2 a PC1

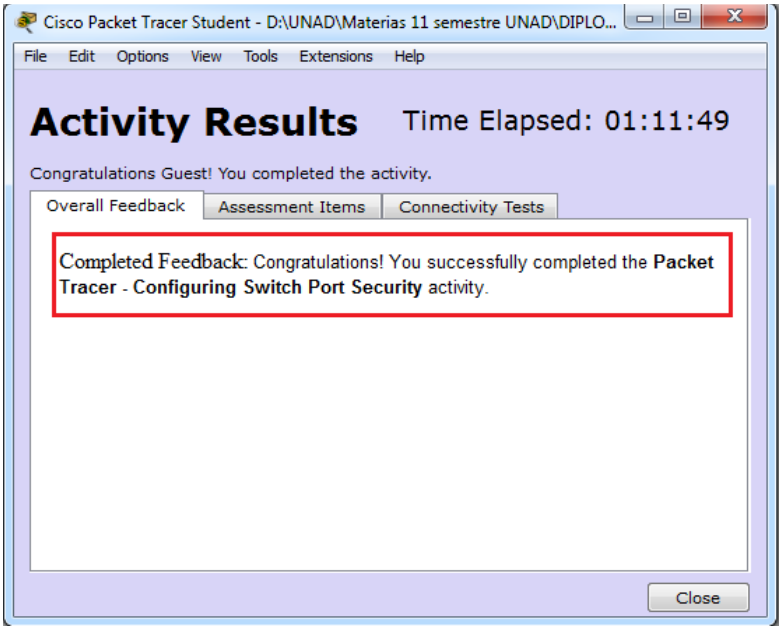


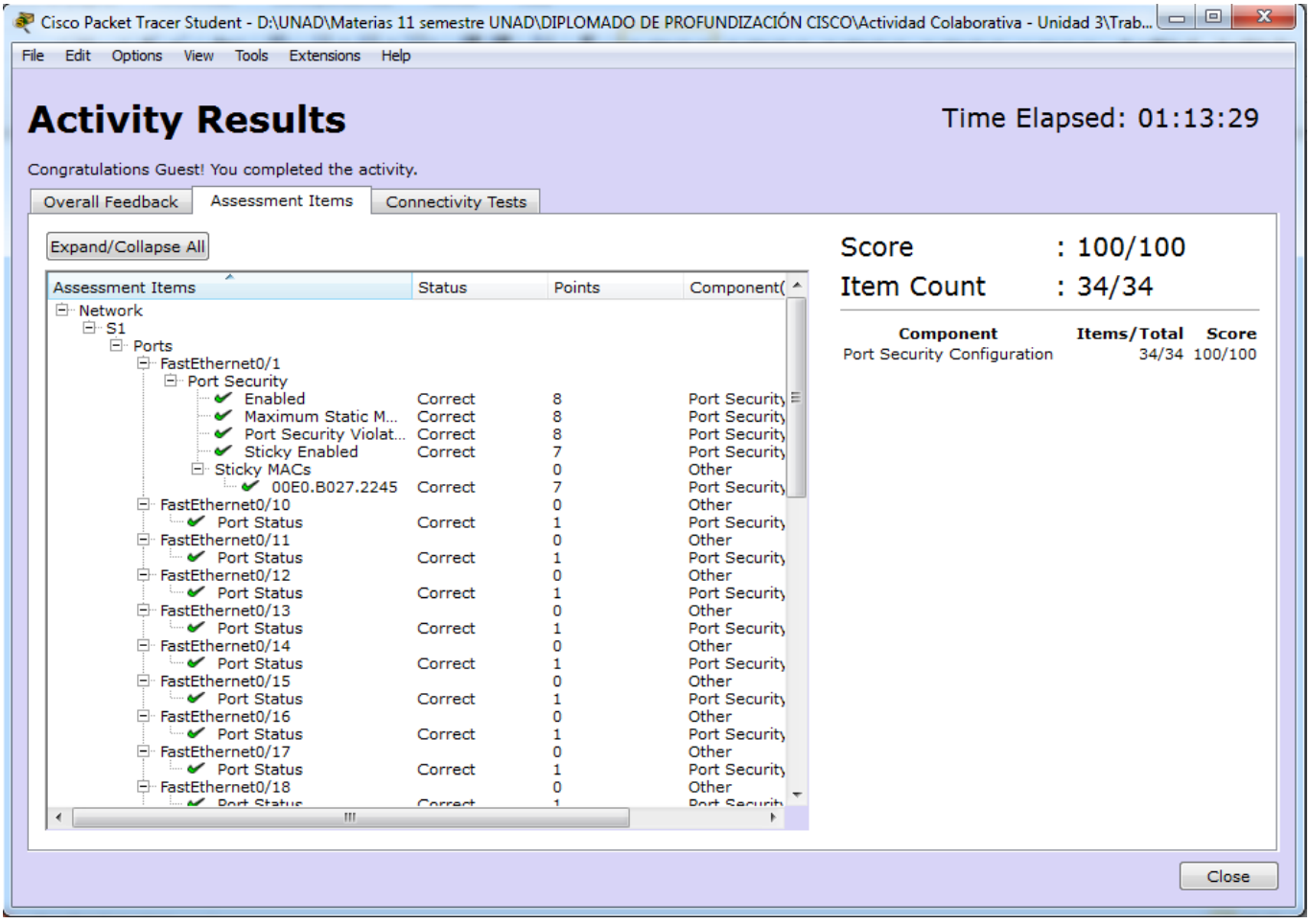
h. Why is **PC2** able to ping **PC1**, but the **Rouge Laptop** is not? The port security that was enabled on the port only allowed the device, whose MAC was learned first, access to the port while preventing all other devices access.

La seguridad del puerto que se habilitó permite acceder solo a un dispositivo, el dispositivo del cual se prendió primero su dirección MAC y se impide el acceso a otros dispositivos.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Resultados de la actividad:





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 2

- Con esta actividad se logró configurar la seguridad del puerto en un switch.
- Se logró verificar la seguridad del puerto.
- Conocimos que la seguridad de los puertos permite restringir el tráfico de entrada de un puerto al limitar las direcciones MAC que pueden enviar tráfico al puerto.
- Comprobamos que la seguridad del puerto estaba habilitada y que las direcciones MAC de los PC1 y PC2 se agregaron a la configuración en ejecución.
- Se comprobó que al habilitar el puerto para Rogue Laptop se pueda hacer ping a PC1 y PC2.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 3: 2.2.4.11 Lab - Configuring Switch Security Features

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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

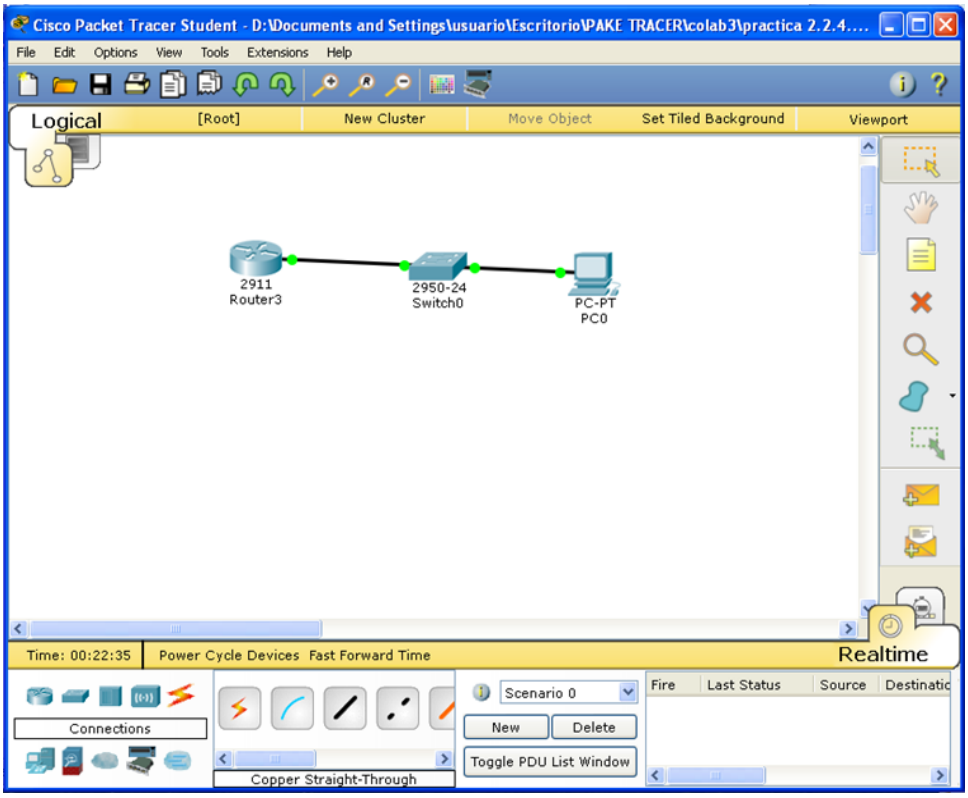
- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 1. Establecer la topología e inicializar los dispositivos

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

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



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

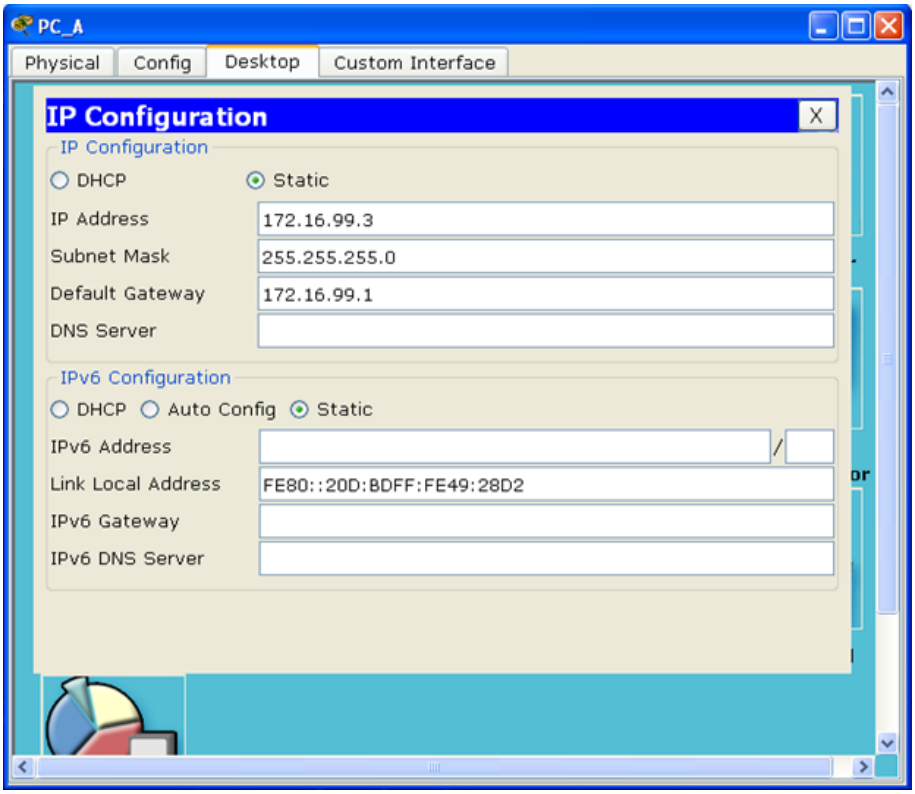
Si los archivos de configuración se guardaron previamente en el router y el switch, inicialice y vuelva a cargar estos dispositivos con los parámetros básicos.

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

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

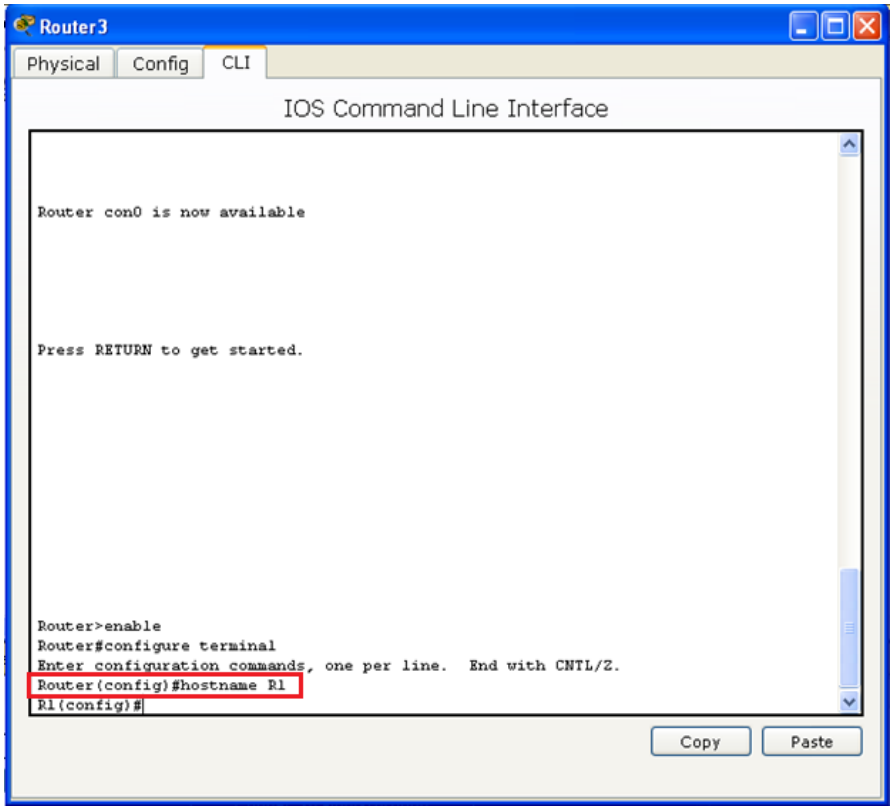
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



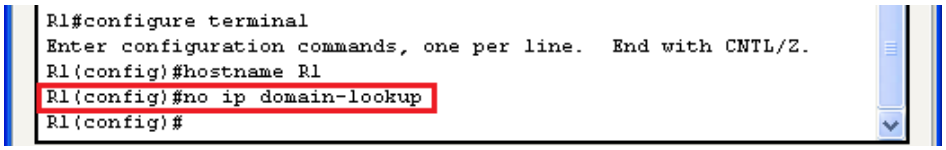
Paso 2. Configurar los parámetros básicos en el R1.

a. Configure el nombre del dispositivo.

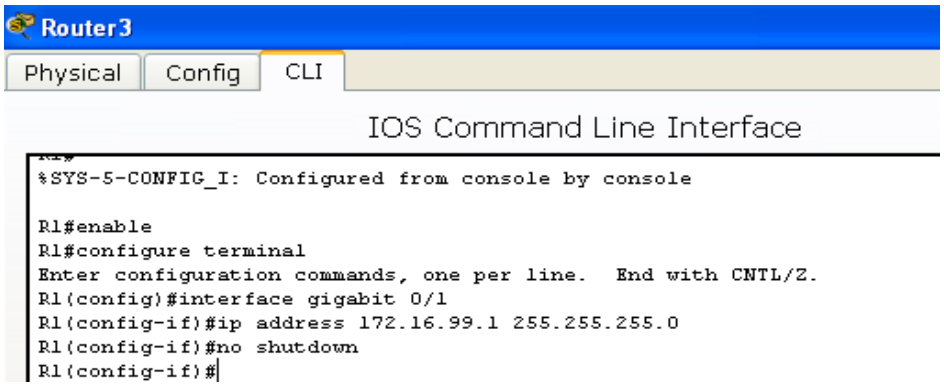


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

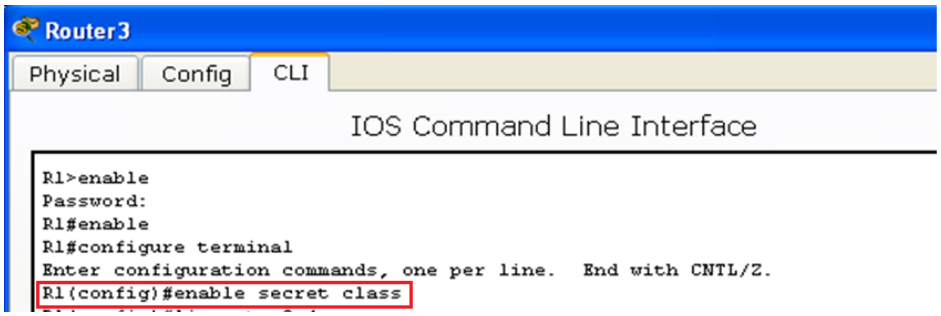
b. Desactive la búsqueda del DNS.



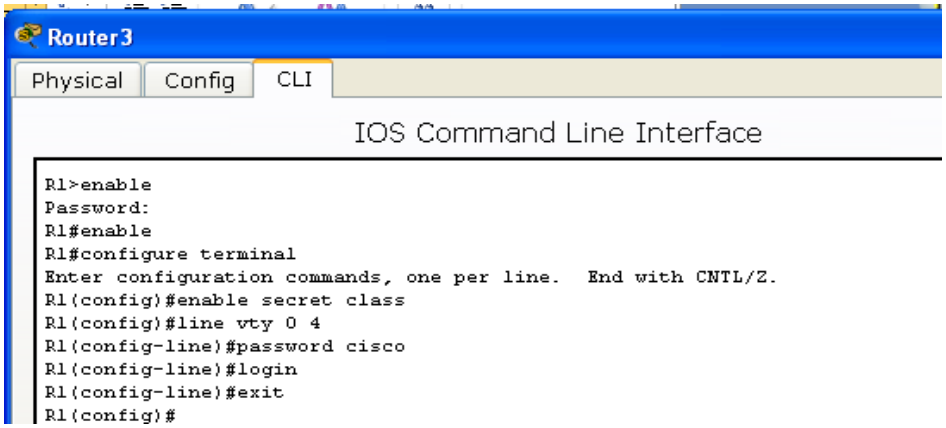
c. Configure la dirección IP de interfaz que se muestra en la tabla de direccionamiento.



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

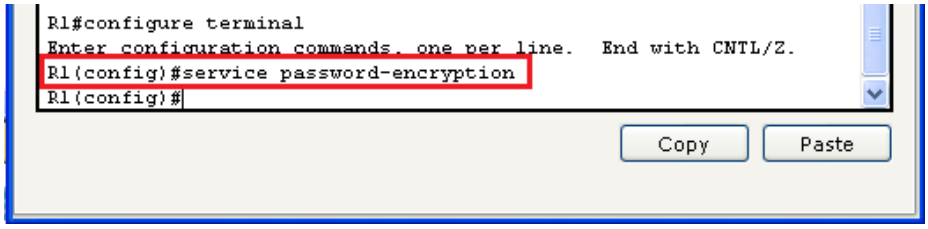


e. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.

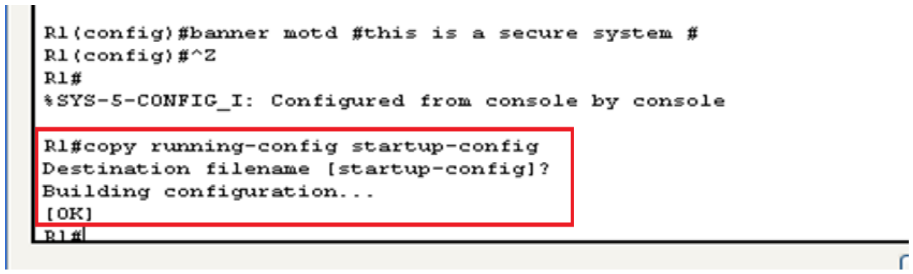


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

f. Cifre las contraseñas de texto no cifrado.



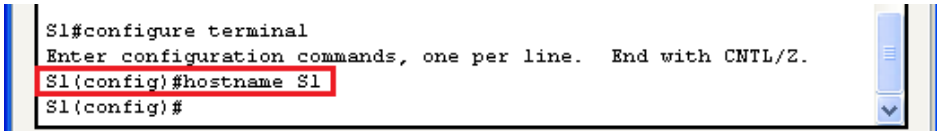
g. Guarde la configuración en ejecución en la configuración de inicio.



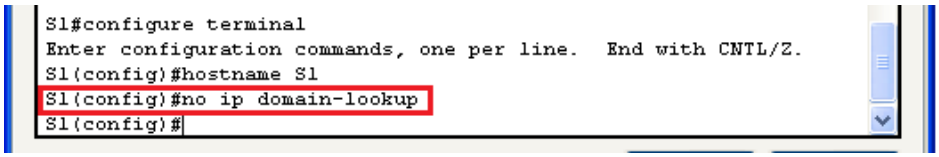
Paso 3. Configurar los parámetros básicos en el S1.

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

a. Configure el nombre del dispositivo.



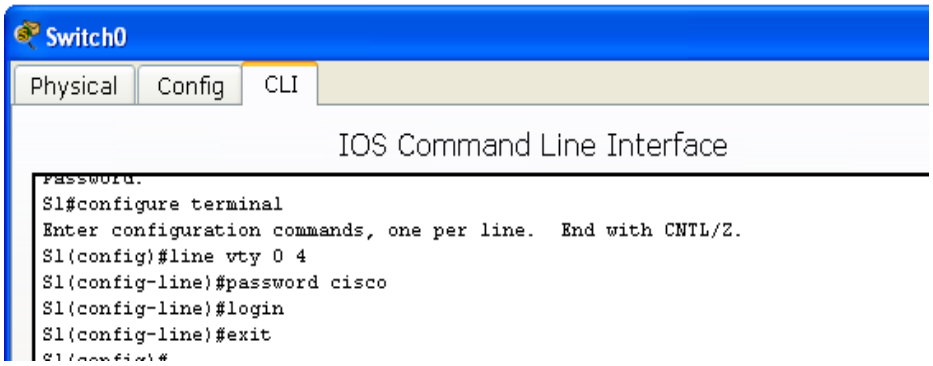
b. Desactive la búsqueda del DNS.



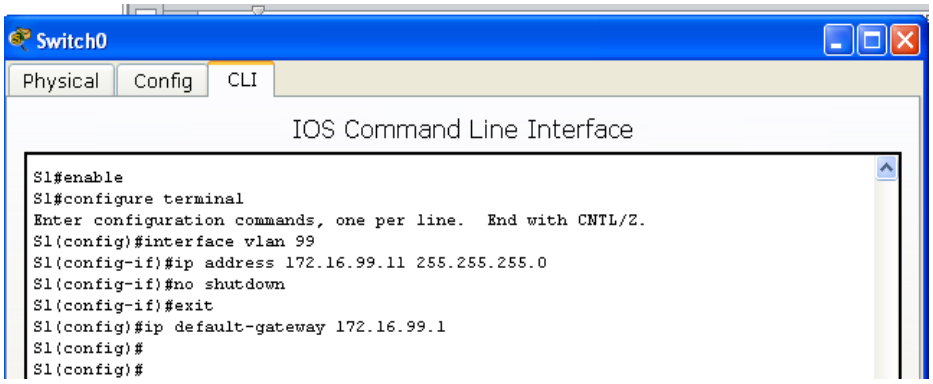
c. Asigne **class** como la contraseña del modo EXEC privilegiado**.**

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

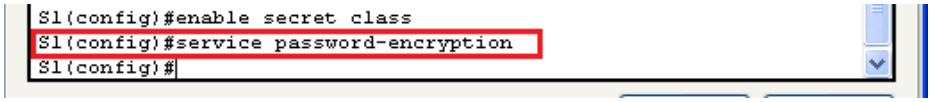
d. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y luego habilite el inicio de sesión.



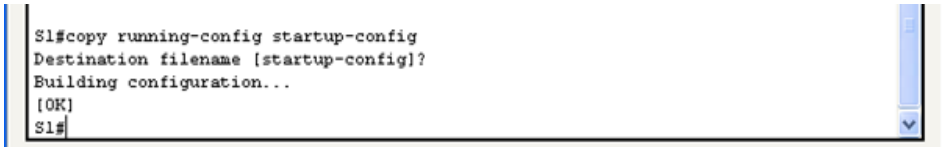
e. Configure un gateway predeterminado para el S1 con la dirección IP del R1.



f. Cifre las contraseñas de texto no cifrado.



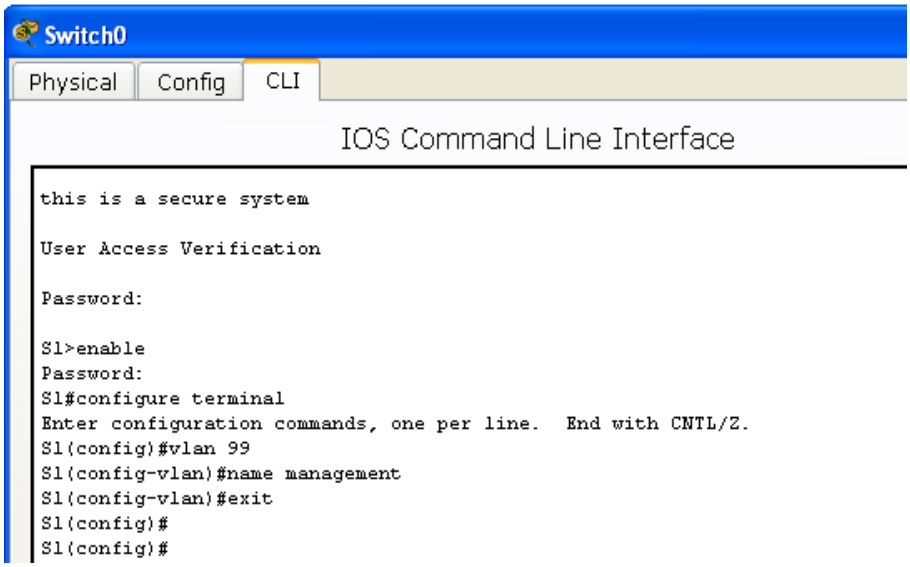
g. Guarde la configuración en ejecución en la configuración de inicio.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

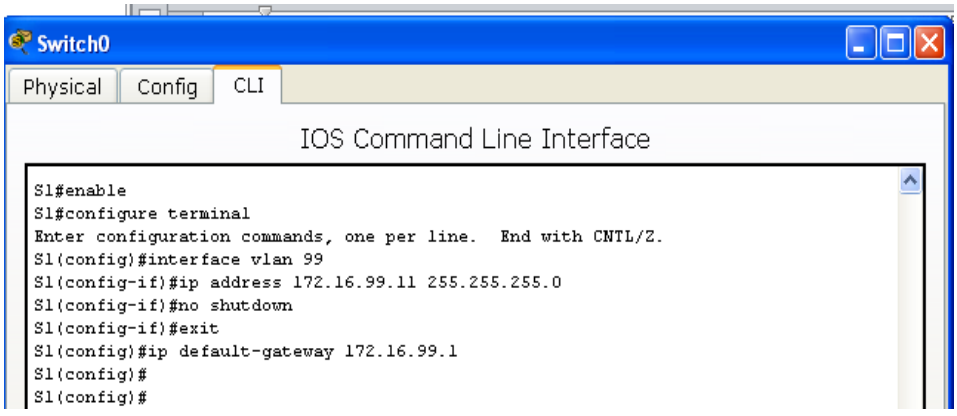
h. Cree la VLAN 99 en el switch y asígnele el nombre **Management**.

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



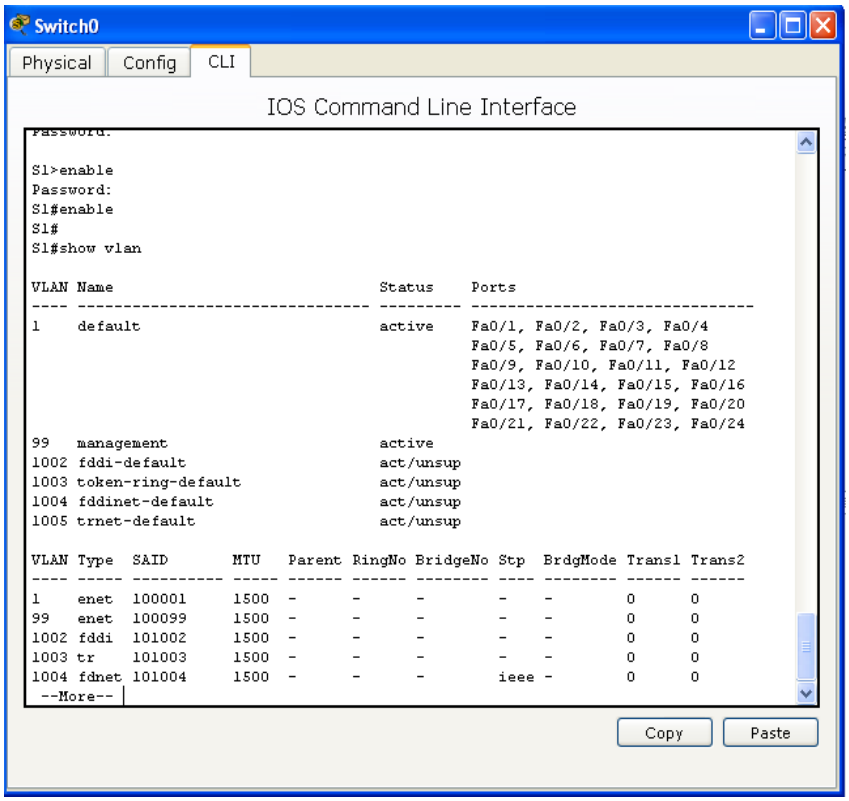
i. Configure la dirección IP de la interfaz de administración VLAN 99, tal como se muestra en la tabla de direccionamiento, y habilite la interfaz.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

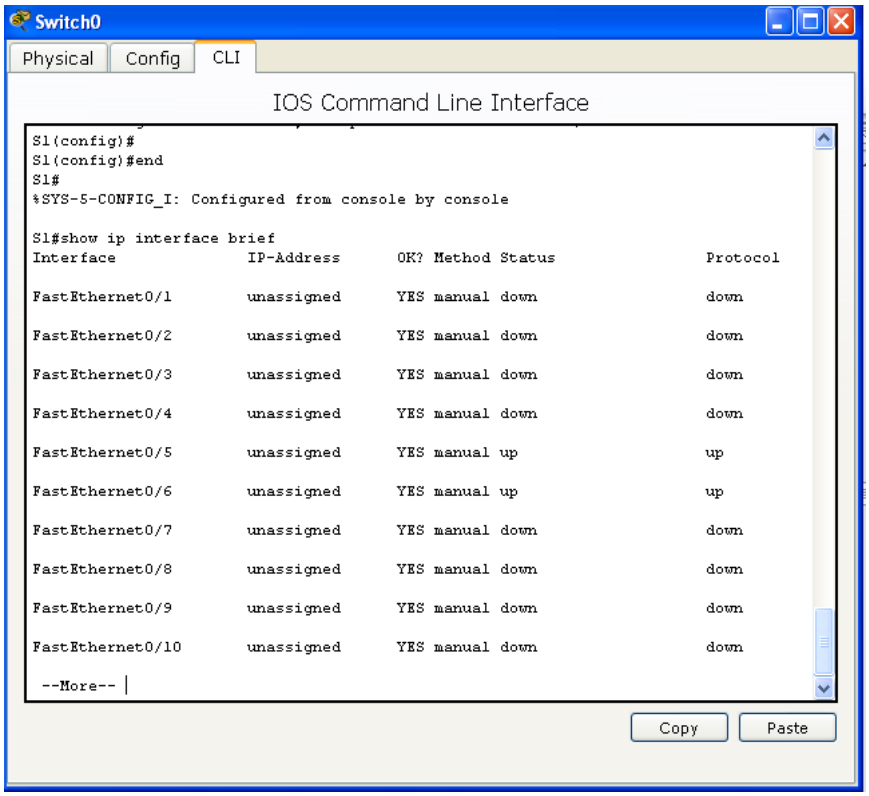


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

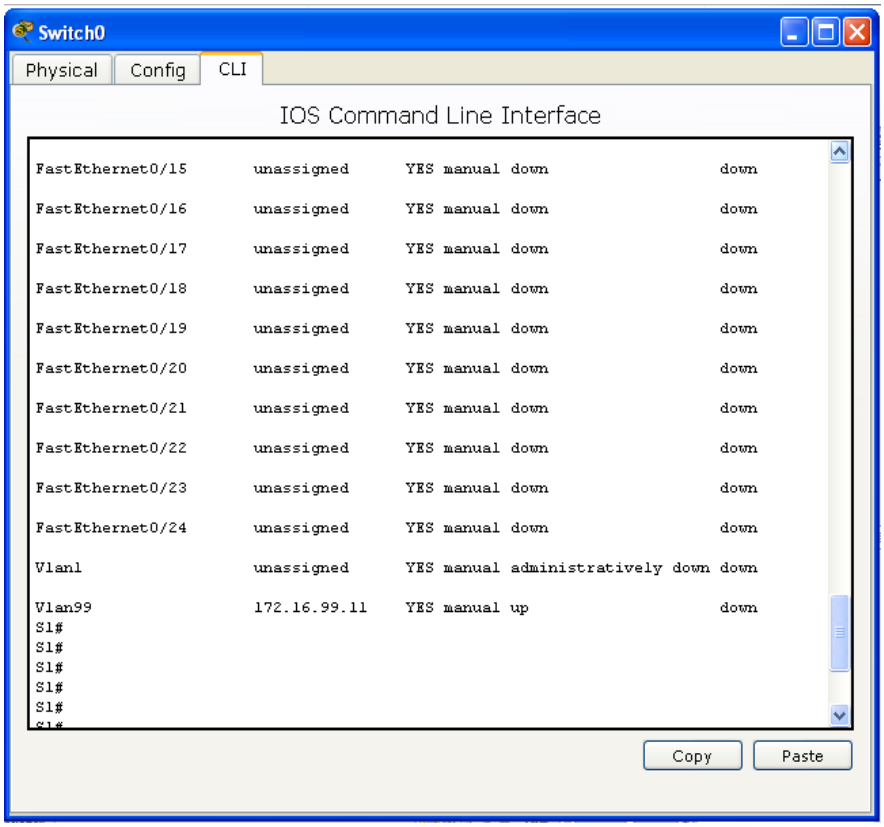
j. Emita el comando **show vlan** en el S1. ¿Cuál es el estado de la VLAN 99? Activa



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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



¿Por qué el protocolo figura como down, a pesar de que usted emitió el comando **no shutdown** para la interfaz VLAN 99? Porque no se asignaron puertos físicos en el switch a la interfaz VLAN 99

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

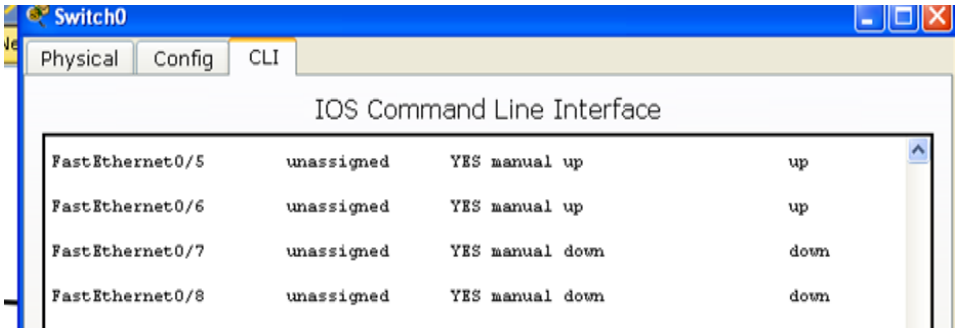
```
S1# config t
S1(config)# interface f0/5
S1(config-if)#  switchport  mode  access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)#  switchport  mode  access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

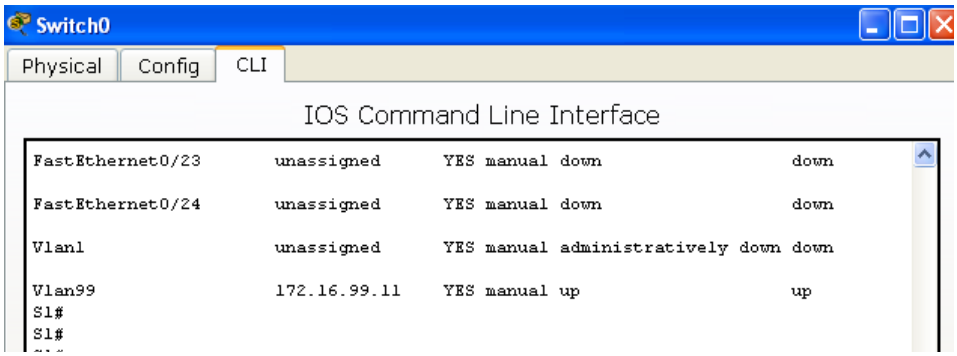
```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface   f 0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 99
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#interface   f 0/6
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
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

m. Emita el comando **show ip interface brief** en el S1. ¿Cuál es el estado y el protocolo que se muestra para la interfaz VLAN 99? Estado: UP y protocolo: UP

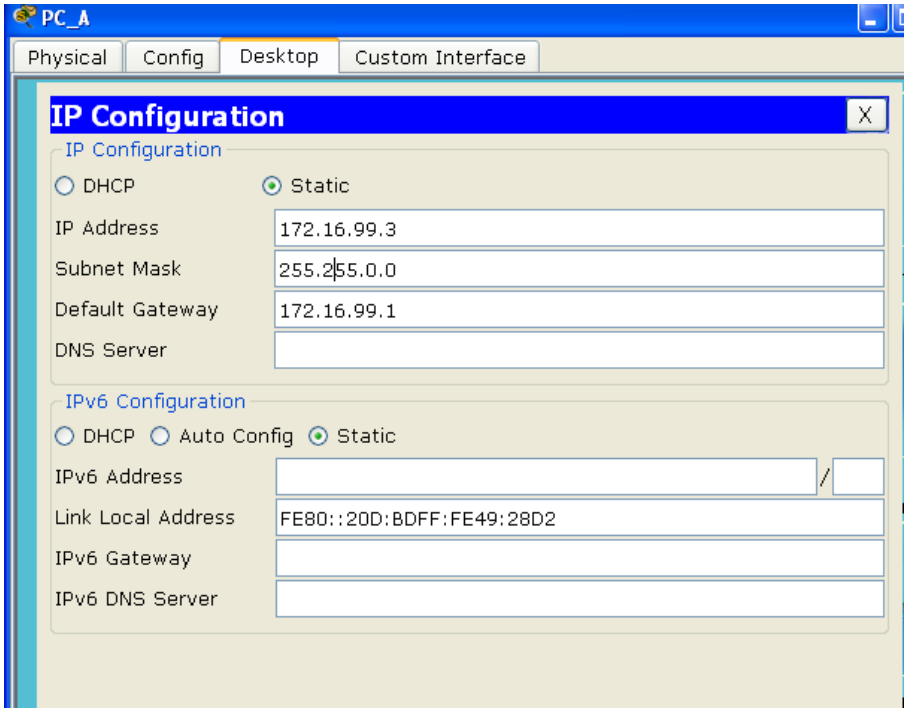
Nota: puede haber una demora mientras convergen los estados de los puertos.



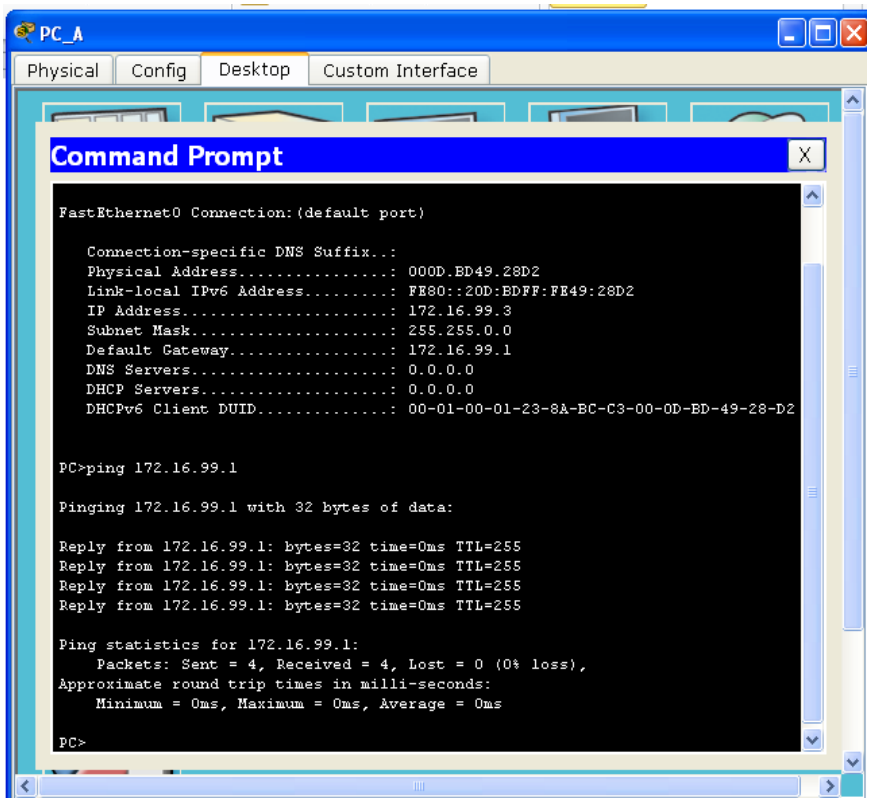


Paso 4. Verificar la conectividad entre los dispositivos.

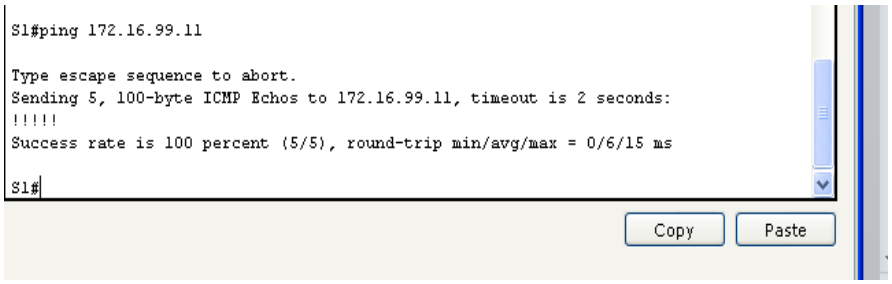
a. En la PC-A, haga ping a la dirección de gateway predeterminado en el R1. ¿Los pings se realizaron correctamente? Si



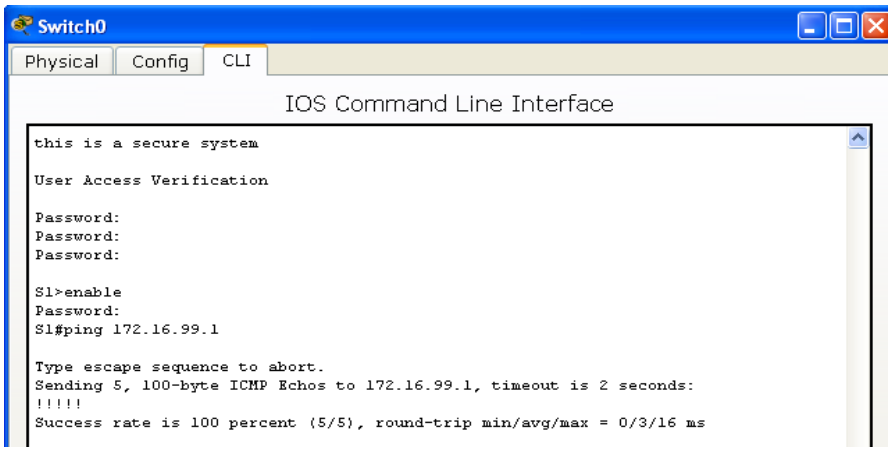
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



b. En la PC-A, haga ping a la dirección de administración del S1. ¿Los pings se realizaron correctamente? Si



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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

En un switch real si se puede acceder a la interfaz web, pero en un switch en packet tracer no se puede.

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

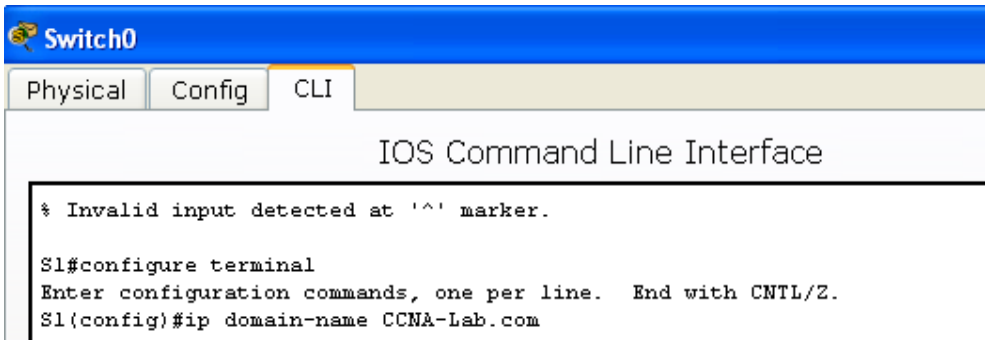
Nota: la interfaz web no segura (servidor HTTP) en un switch Cisco 2960 está habilitada de manera predeterminada. Una medida de seguridad frecuente es deshabilitar este servicio, tal como se describe en la parte 4.

Parte 3. Configurar y verificar el acceso por SSH en el S1

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

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

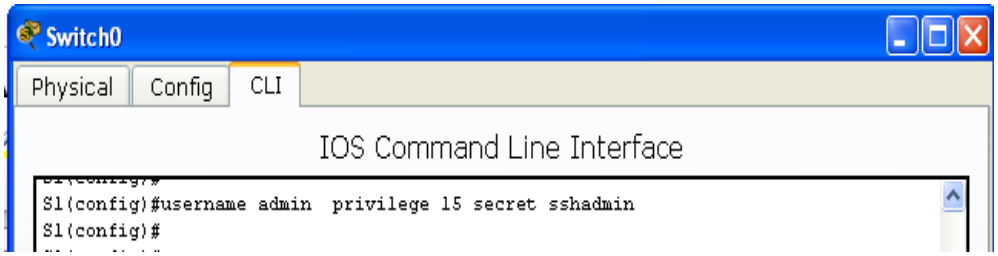
```
S1(config)# ip domain-name CCNA-Lab.com
```



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

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

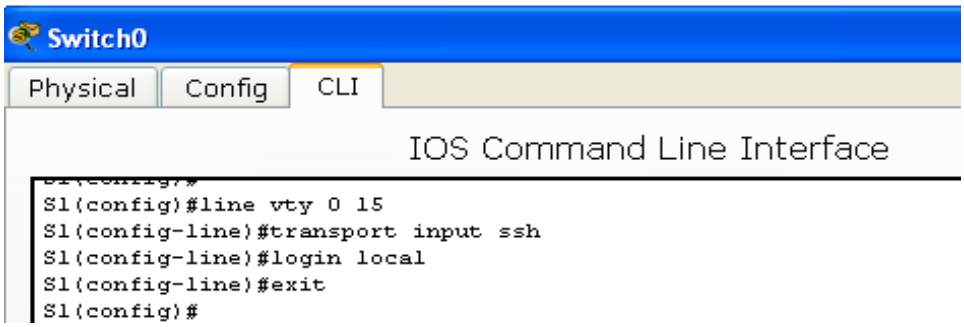
```
S1(config)# username admin privilege 15 secret sshadmin
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

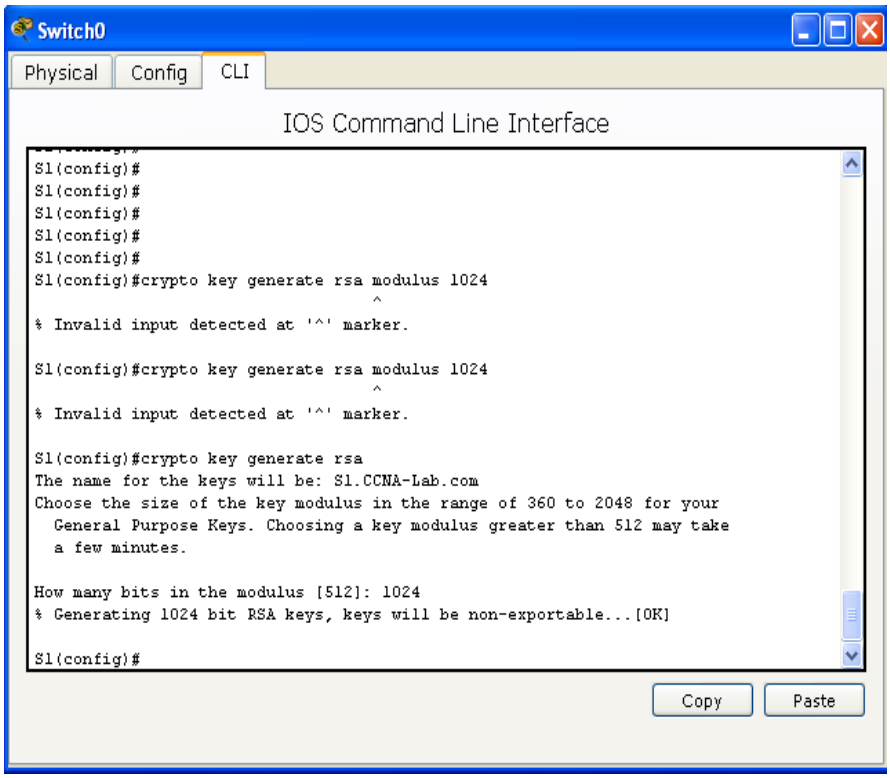
c. Configure la entrada de transporte para que las líneas vty permitan solo conexiones SSH y utilicen la base de datos local para la autenticación.

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



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

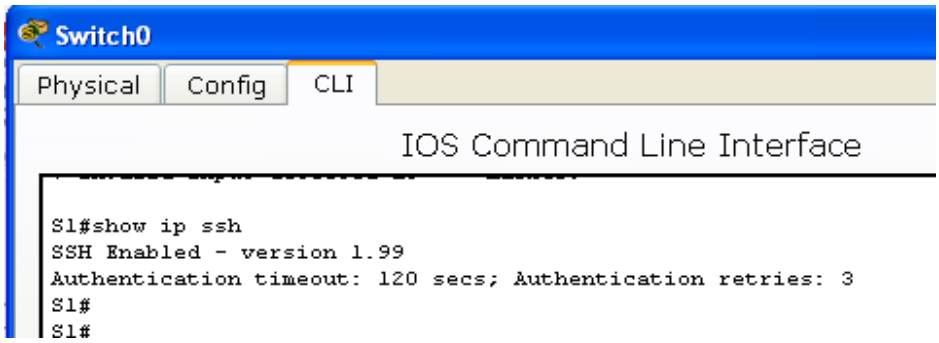
```
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

S1(config)#
S1(config)# end
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

```
S1# show ip ssh
```



¿Qué versión de SSH usa el switch? 1.99

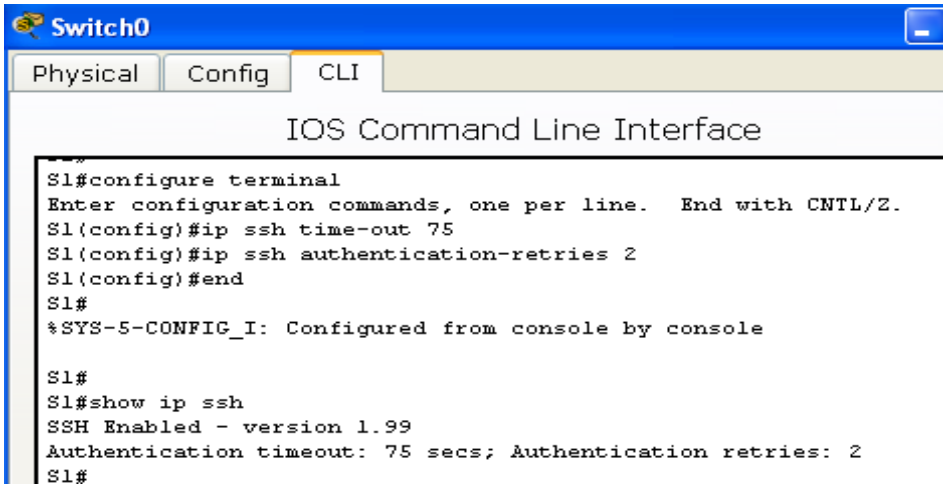
¿Cuántos intentos de autenticación permite SSH? 3

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

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

Modifique la configuración predeterminada de SSH.

```
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
```



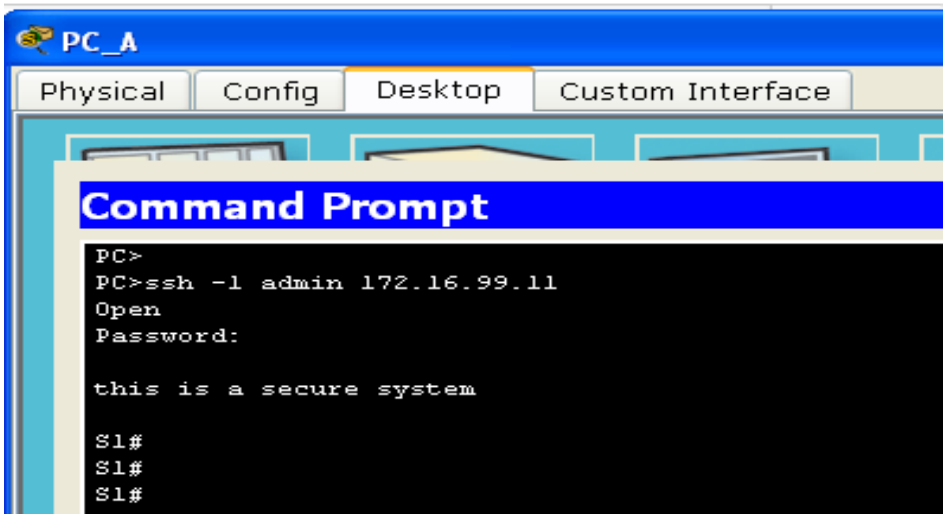
¿Cuántos intentos de autenticación permite SSH? 2

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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



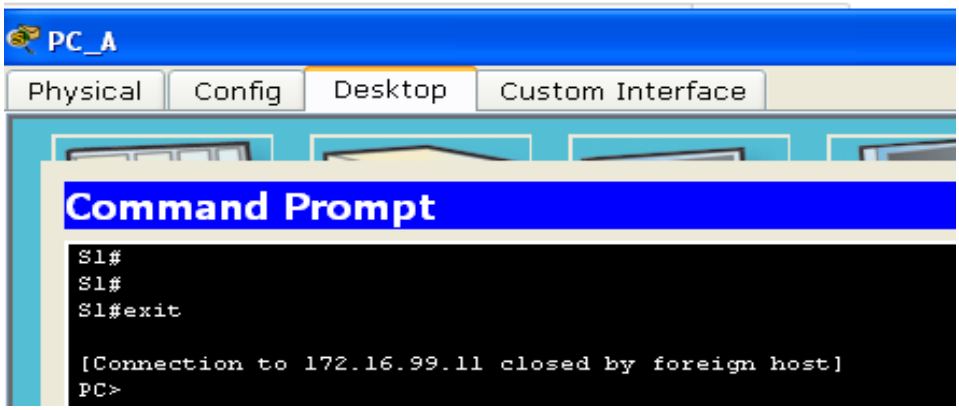
¿La conexión se realizó correctamente? Se hizo correctamente

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

Se hizo una petición de entrada SSH, porque entramos a una sección SSH a través de la ip del interfaz VLAN99, el nombre de usuario admin y la contraseña: sshadmin.

Me está mostrando el promt del sistema en el modo EXEC privilegiado.

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



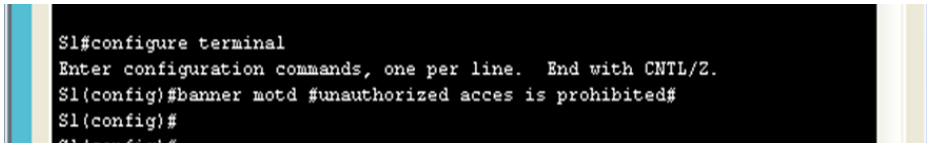
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

En la parte 4, desactivará los puertos sin utilizar, desactivará determinados servicios que se ejecutan en el switch y configurará la seguridad de puertos según las direcciones MAC. Los switches pueden estar sujetos a ataques de desbordamiento de la tabla de direcciones MAC, a ataques de suplantación de direcciones MAC y a conexiones no autorizadas a los puertos del switch. Configurará la seguridad de puertos para limitar la cantidad de direcciones MAC que se pueden detectar en un puerto del switch y para deshabilitar el puerto si se supera ese número.

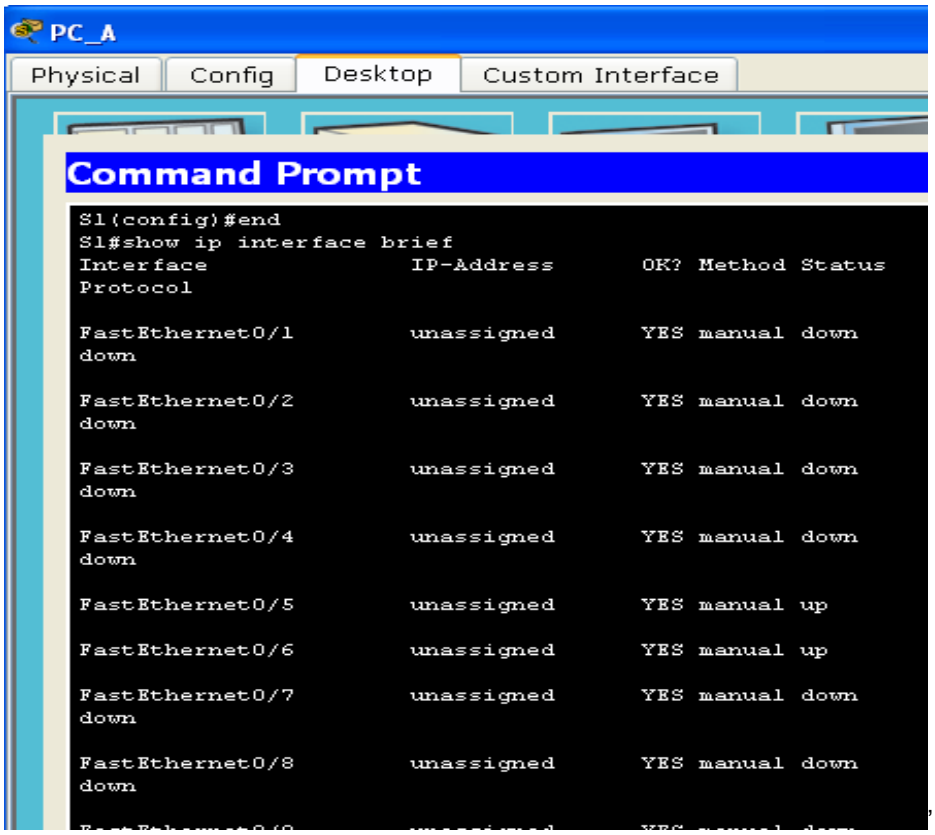
Paso 1. Configurar las características de seguridad general en el S1.

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



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

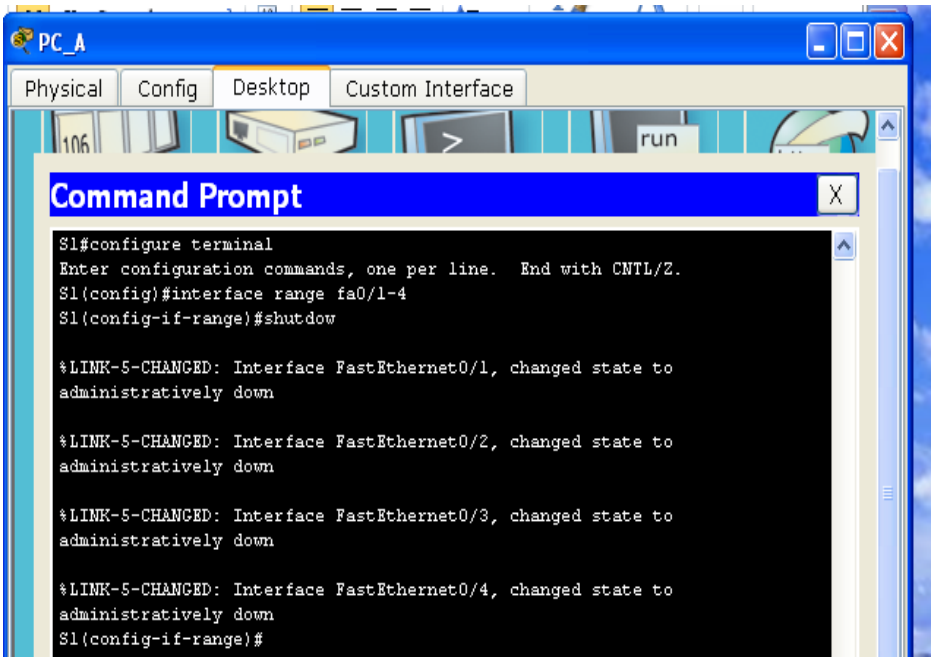
Están activos los puertos f0/5 y f0/6

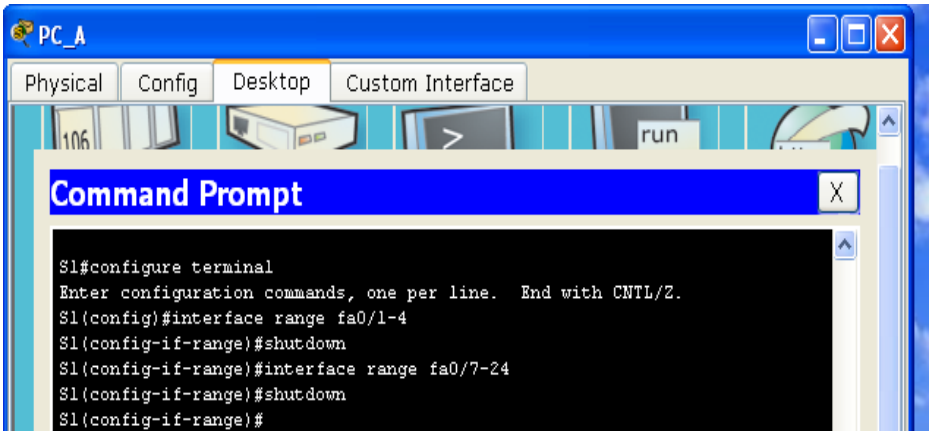


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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#
```

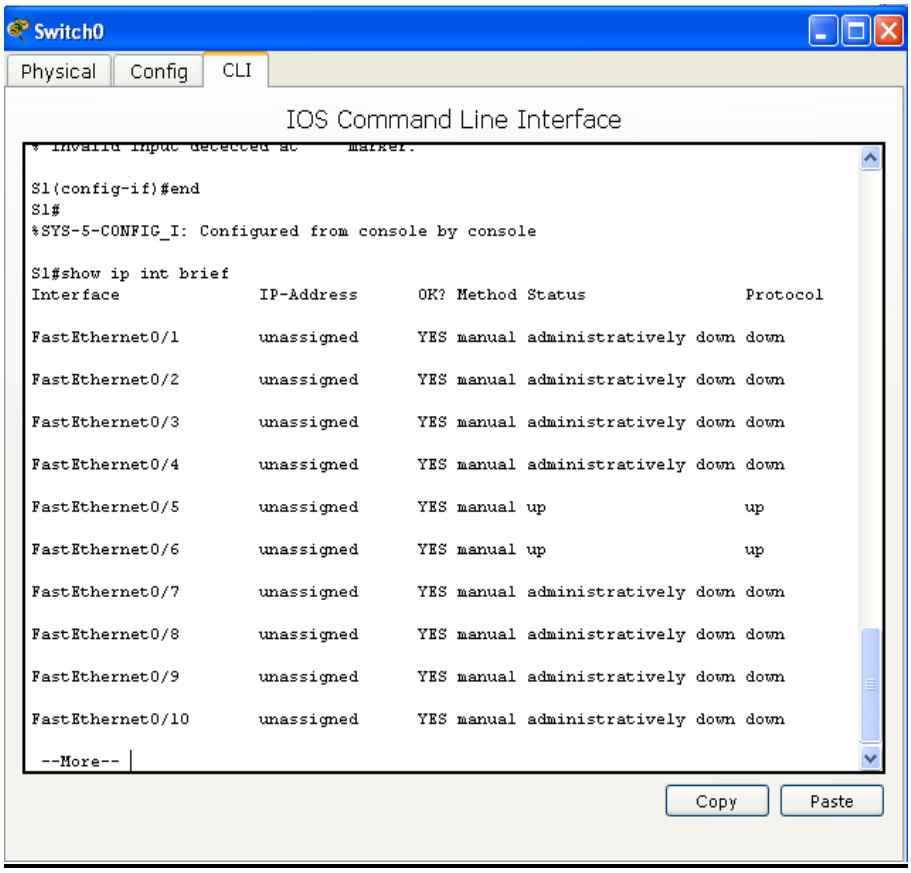




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

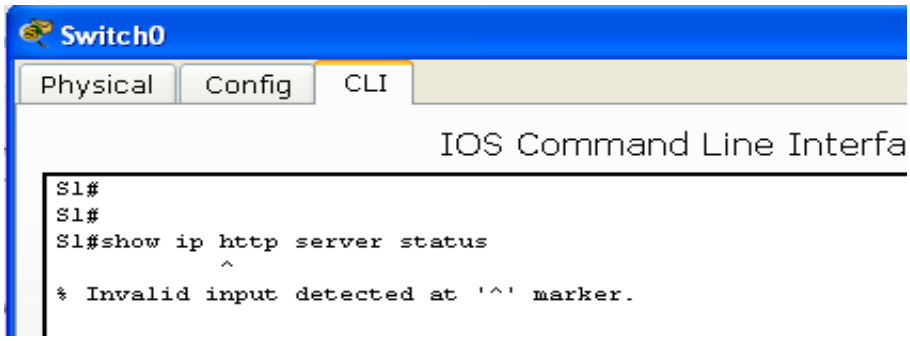
d. Emita el comando **show ip interface brief** en el S1. ¿Cuál es el estado de los puertos F0/1 a F0/4?

Administrativamente caído



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

No lo soporta este comando en esta versión de packet tracert



¿Cuál es el estado del servidor HTTP? Activado por defecto

¿Qué puerto del servidor utiliza? El puerto 80 por defecto

¿Cuál es el estado del servidor seguro de HTTP? Activado por defecto

¿Qué puerto del servidor seguro utiliza? El puerto 443 por defecto

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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
```

Packet tracert no soporta este comando

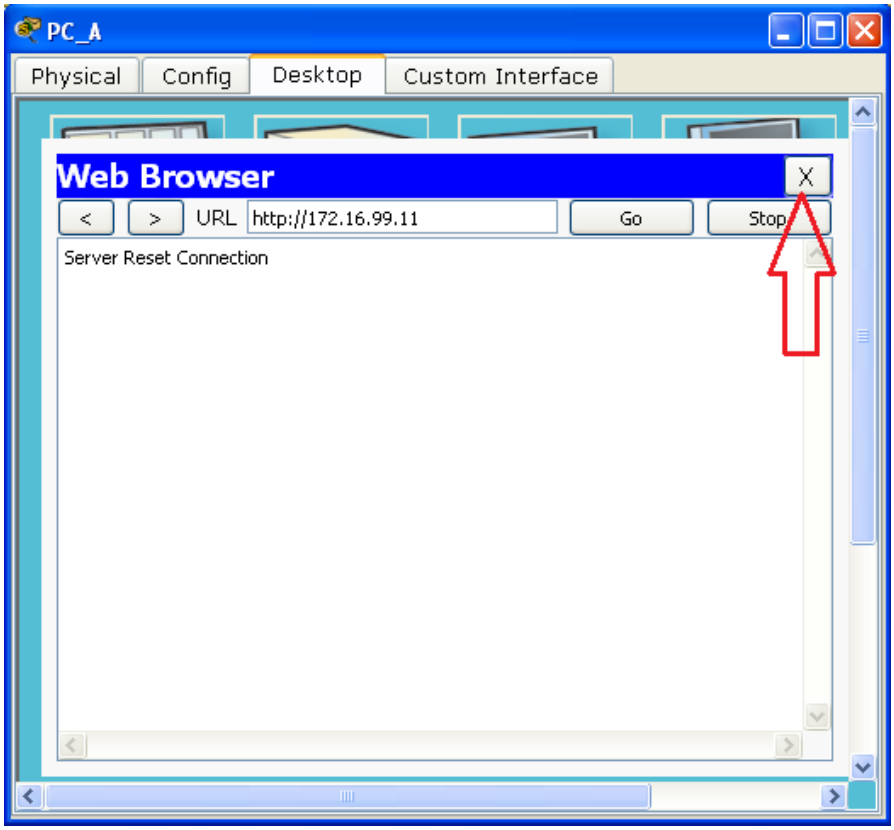
g. En la PC-A, abra una sesión de navegador web a http://172.16.99.11. ¿Cuál fue el resultado?

Como se desactiva el servidor http, la página web no se cargará. HTTP rechaza las conexiones desde S1

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?

En un switch real la sesión de navegador web sería satisfactoria

i. Cierre la sesión web en la PC-A.

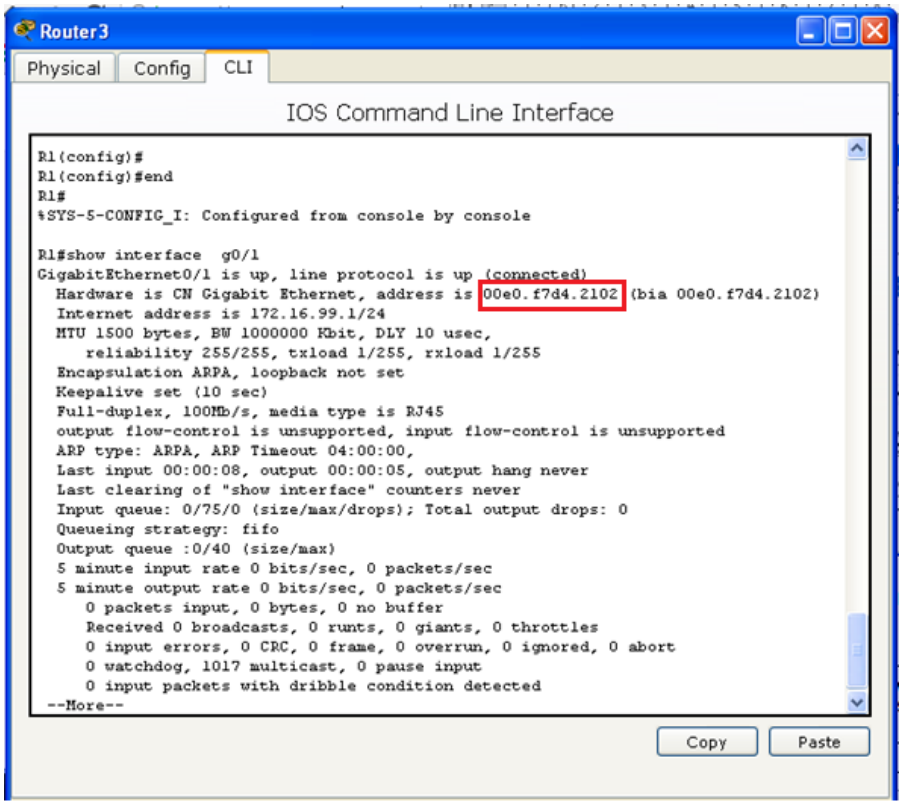


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

a. 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 00e0.f7d4.2102 (bia
00e0.f7d4.2102)
```



¿Cuál es la dirección MAC de la interfaz G0/1 del R1? 00e0.f7d4.2102

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

Dirección MAC de F0/5: 00e0.f7d4.2102

Dirección MAC de F0/6: 000d.bd49.28d2

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

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

  99    000d.bd49.28d2    DYNAMIC     Fa0/6
  99    00e0.f7d4.2102    DYNAMIC     Fa0/5
S1#
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

c. 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
```

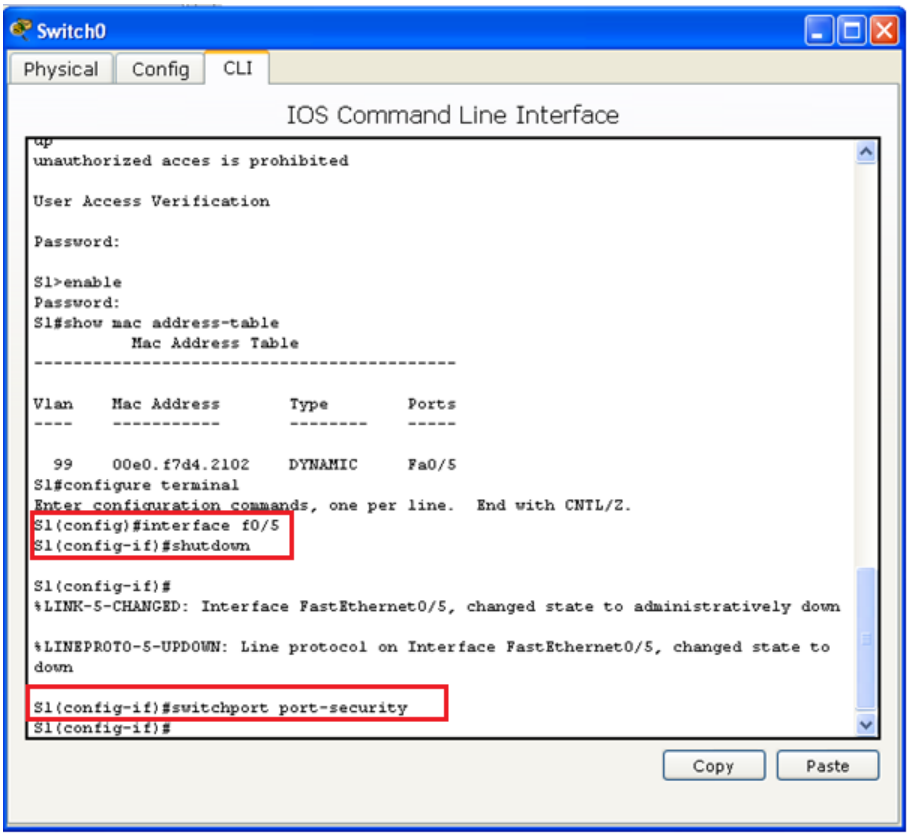
2) Desactive el puerto.

```
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.



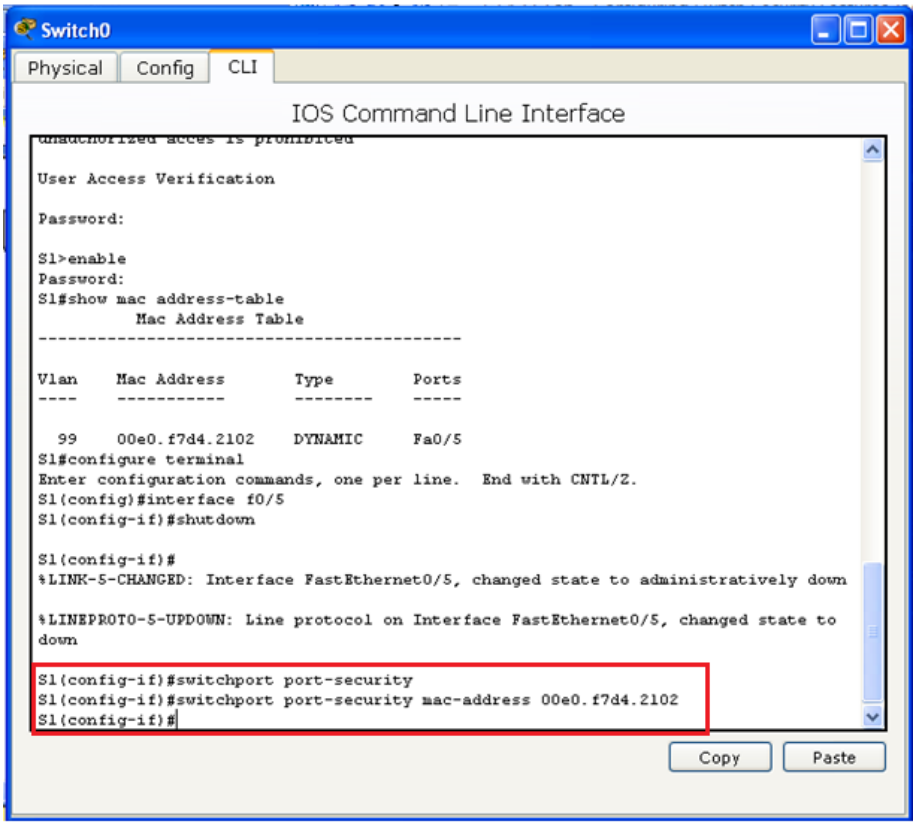
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

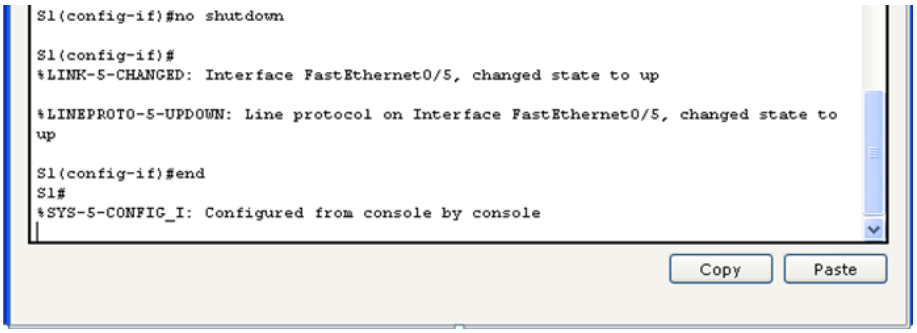
(xxxx.xxxx.xxxx es la dirección MAC real de la interfaz G0/1 del router)

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



5) Habilite el puerto del switch.

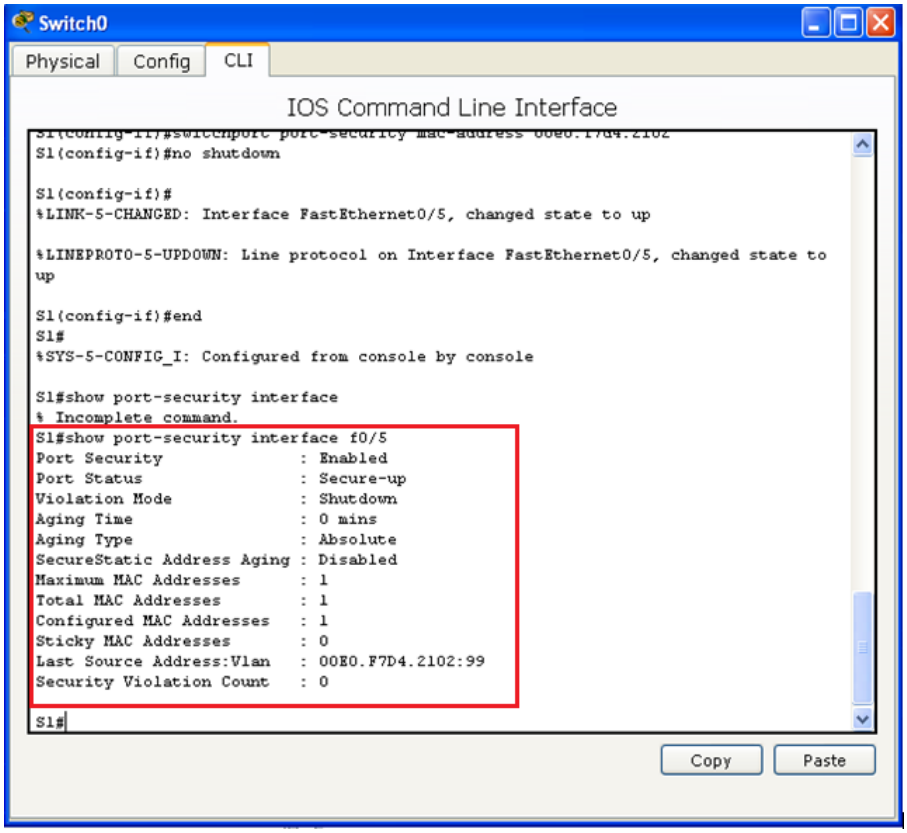
```
S1(config-if)# no shutdown
S1(config-if)# end
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

d. 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
```

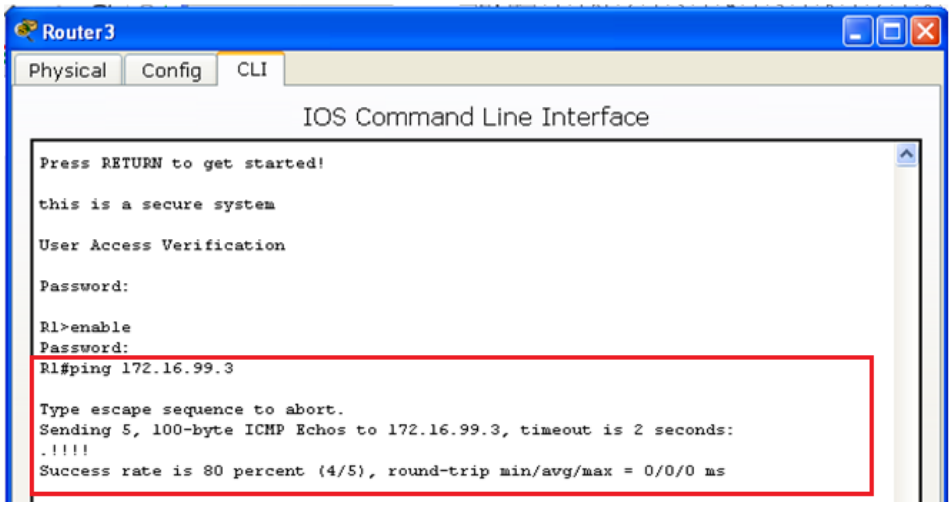


¿Cuál es el estado del puerto de F0/5? Secure-up

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

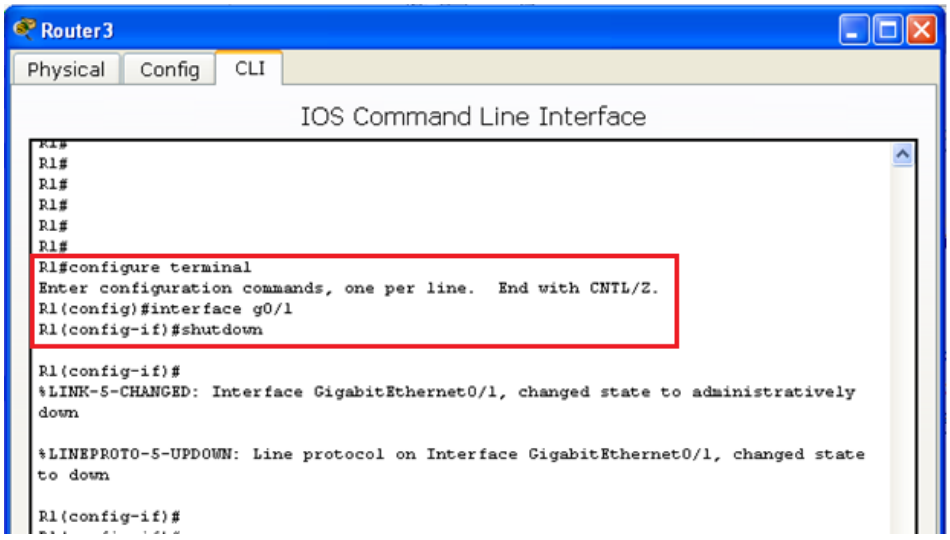
e. En el símbolo del sistema del R1, haga ping a la PC-A para verificar la conectividad.

```
R1# ping 172.16.99.3
```



f. 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.

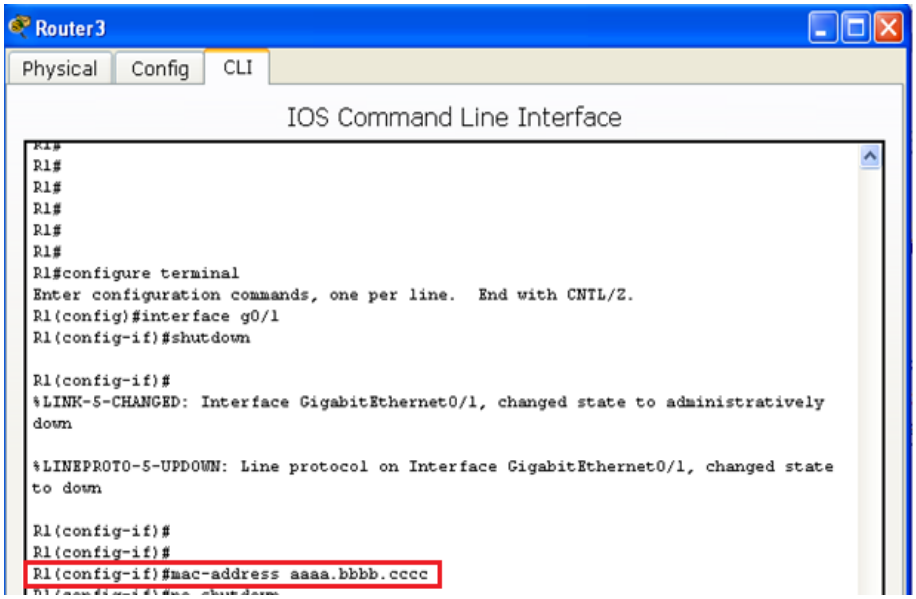
```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

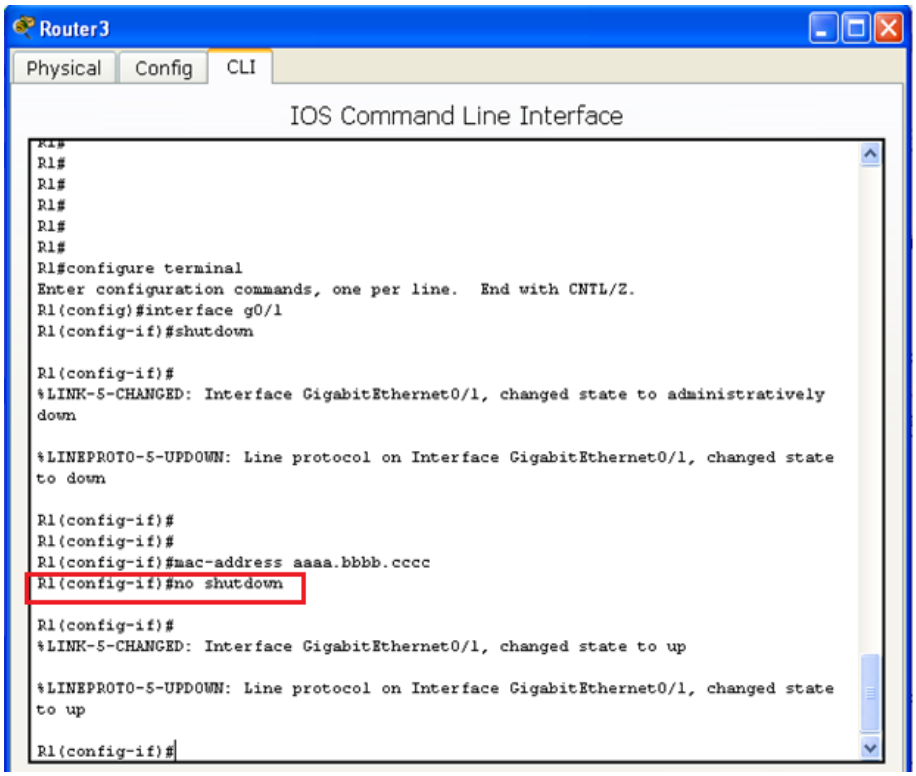
g. Configure una nueva dirección MAC para la interfaz, con la dirección **aaaa.bbbb.cccc**.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```



h. 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
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

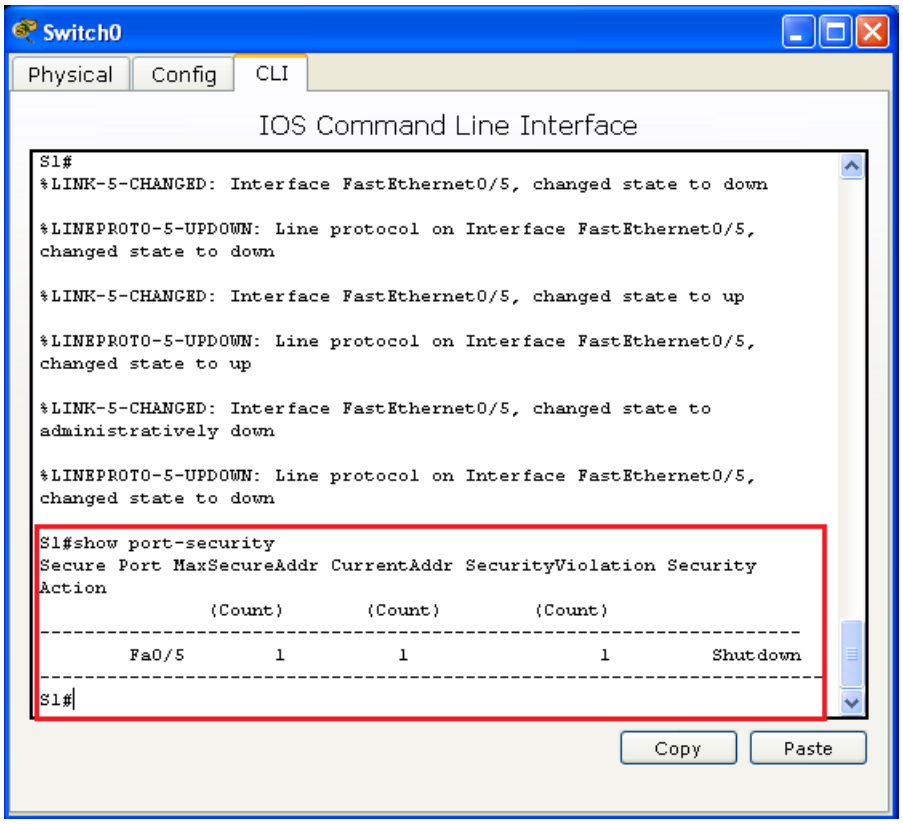
i. En el modo EXEC privilegiado del R1, haga ping a la PC-A. ¿El ping se realizó correctamente? ¿Por qué o por qué no?

El ping falla. Porque se ha violado la seguridad.

```
R1#ping 172.16.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

R1#
```

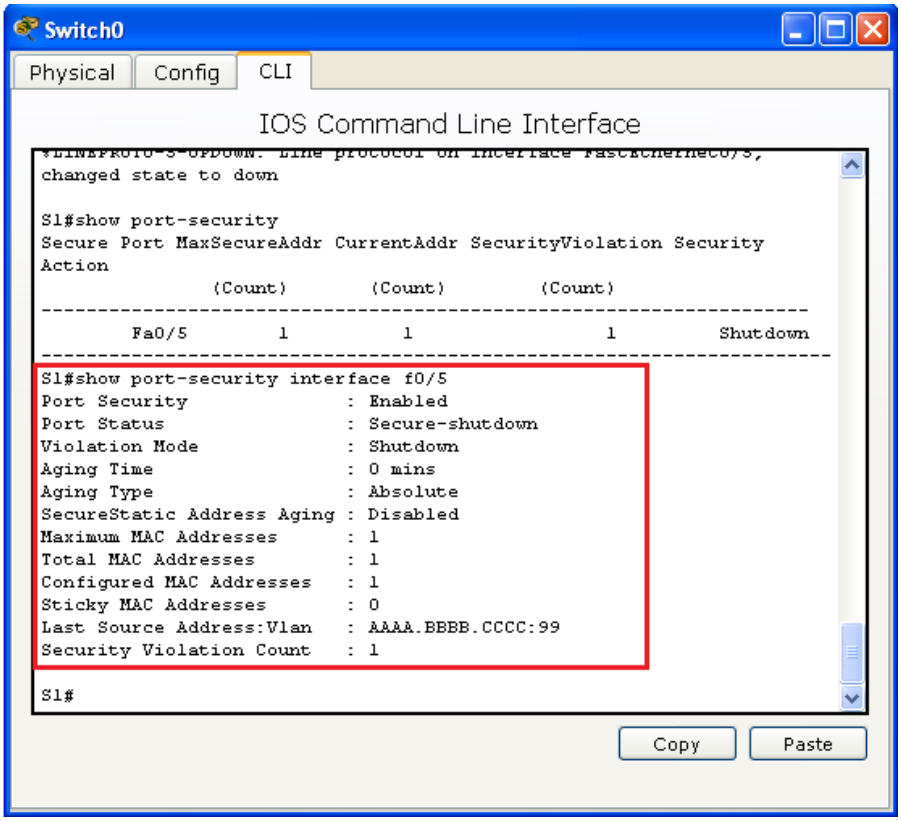
j. En el switch, verifique la seguridad de puertos con los comandos que se muestran a continuación.

```
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
```



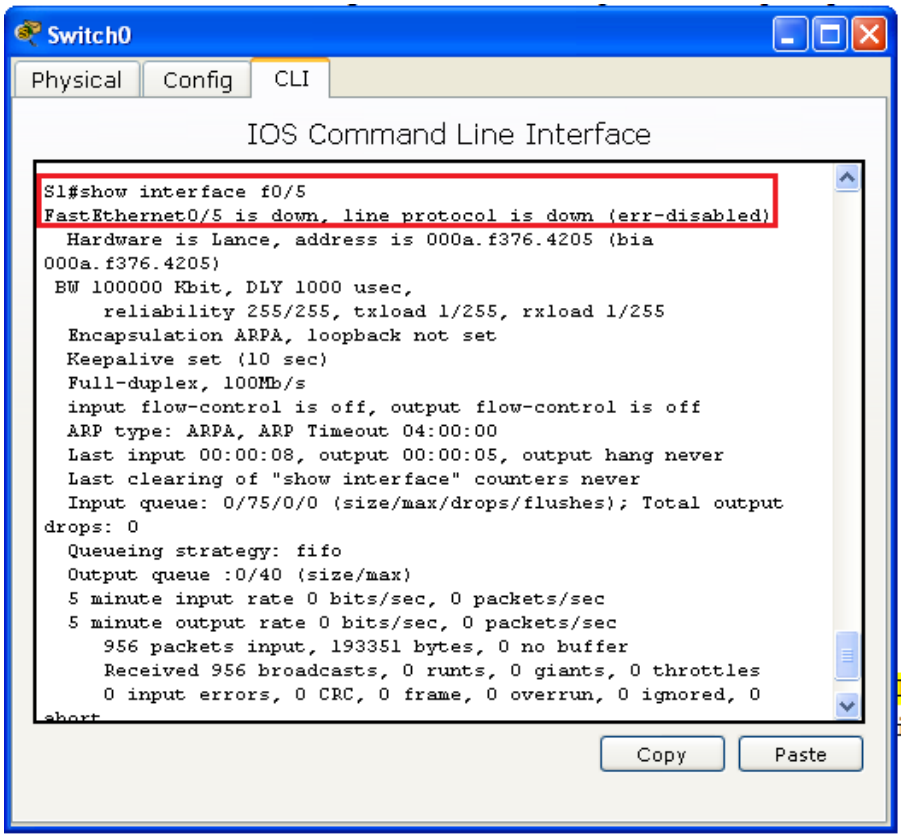
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

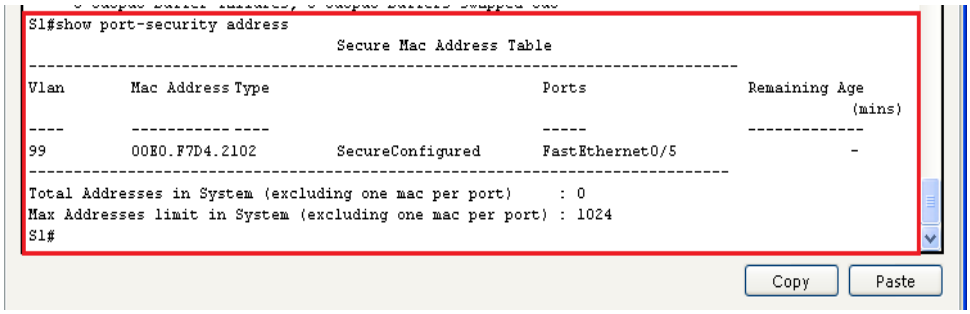



```
S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



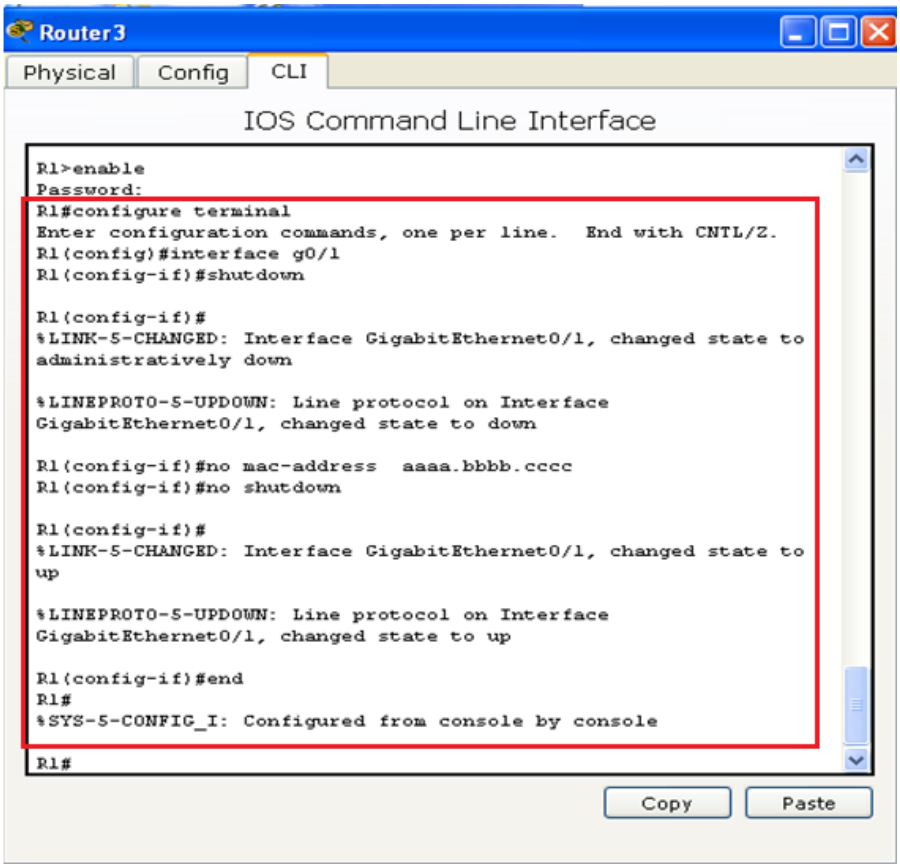

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                  Ports      Remaining Age
                                                           (mins)
----    -----------   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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

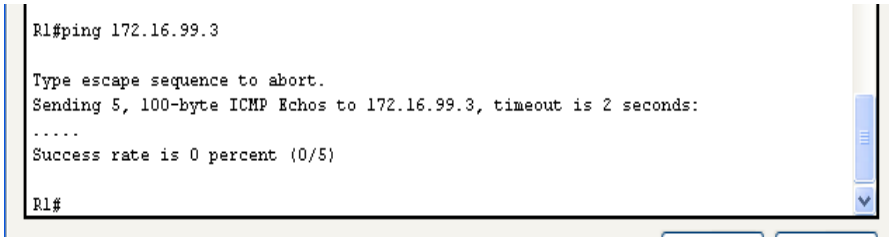
k. En el router, desactive la interfaz G0/1, elimine la dirección MAC codificada de forma rígida del router y vuelva a habilitar la interfaz G0/1.

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



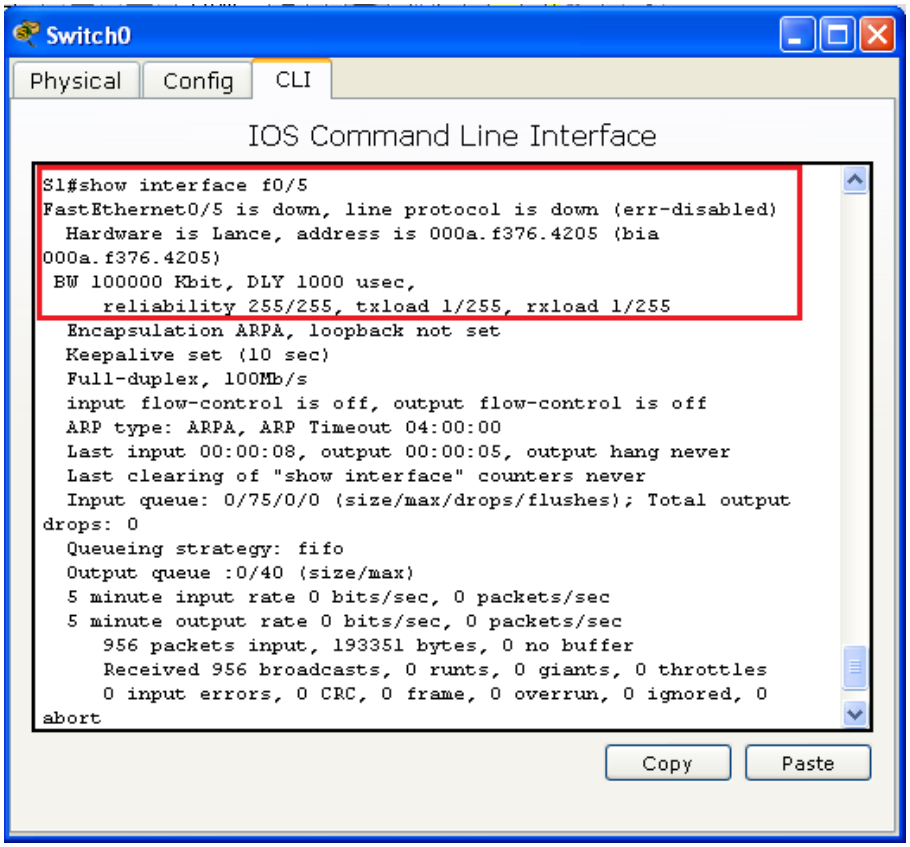
l. Desde el R1, vuelva a hacer ping a la PC-A en 172.16.99.3. ¿El ping se realizó correctamente?

No se realiza el ping correctamente



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

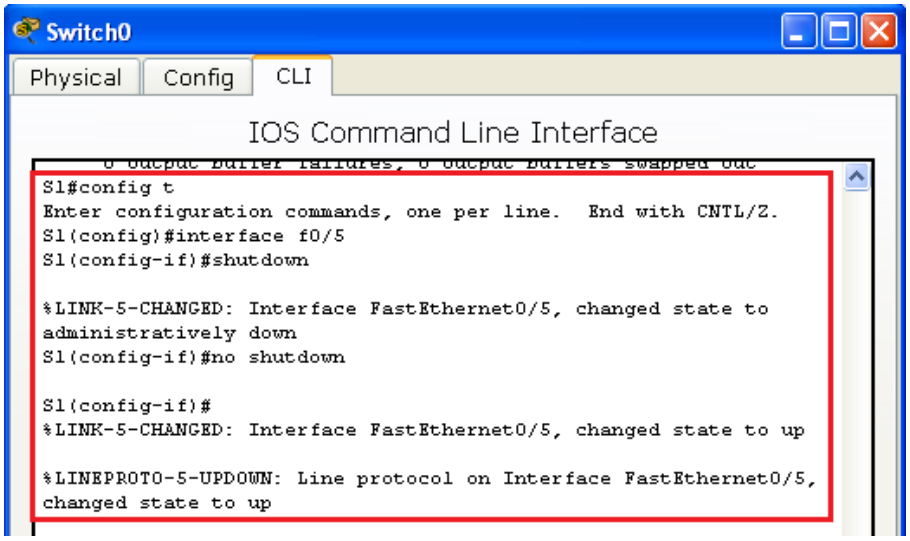
m. Emita el comando **show interface f0/5** para determinar la causa de la falla del ping. Registre sus conclusiones. El puerto F0 / 5 en S1 todavía está en un estado de error deshabilitado.



n. 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
```

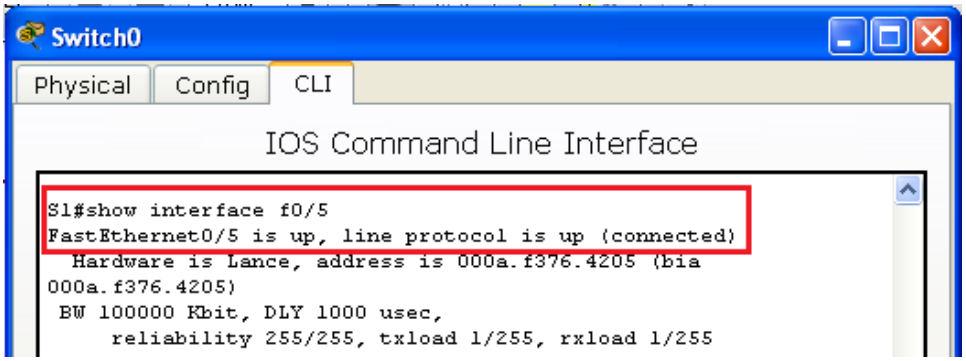
Nota: puede haber una demora mientras convergen los estados de los puertos.



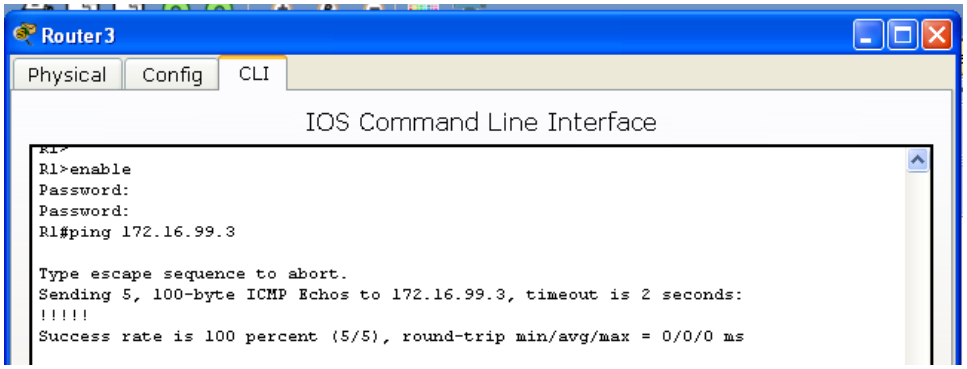
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

o. 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
```



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



Reflexión

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

   Esto ayuda a prevenir el acceso no autorizado de dispositivos a nuestra red.

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

   Los puertos sin uso deben ser desactivados porque un usuario podría conectarse al switch y acceder a la red LAN en cualquiera de los puertos sin uso

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

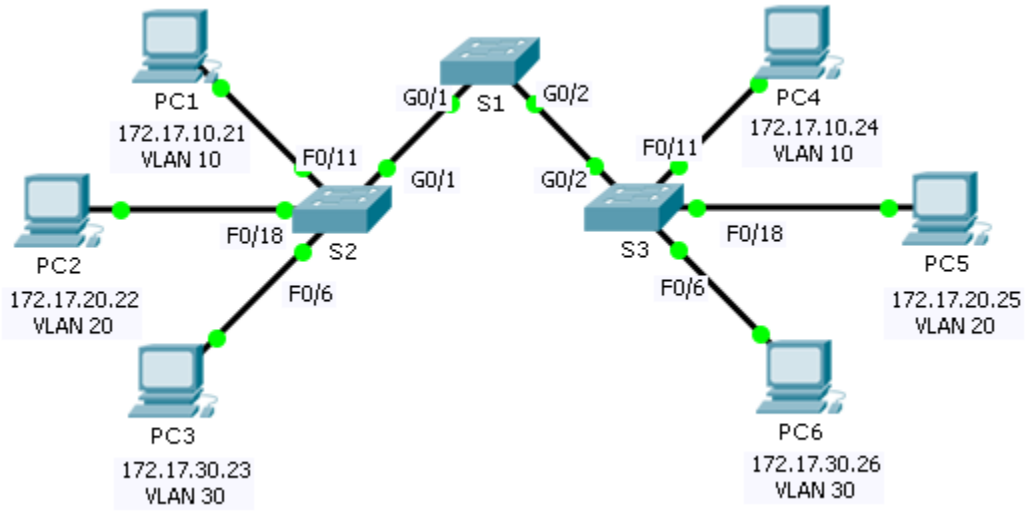
Conclusiones informe 3

- Es necesarios deshabilitar los puertos no utilizados en un switch, ya que un usuario podría acceder a la red de a través de los puertos sin uso que están habilitados.
- 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, se configuro características de seguridad en switches LAN y también se configuro y verifico la seguridad de puertos para bloquear cualquier dispositivo con una dirección MAC que el switch no reconozca.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 4: 3.2.1.7 Packet Tracer - Configuring VLANs

Topology



Addressing Table

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

Objectives

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

Background

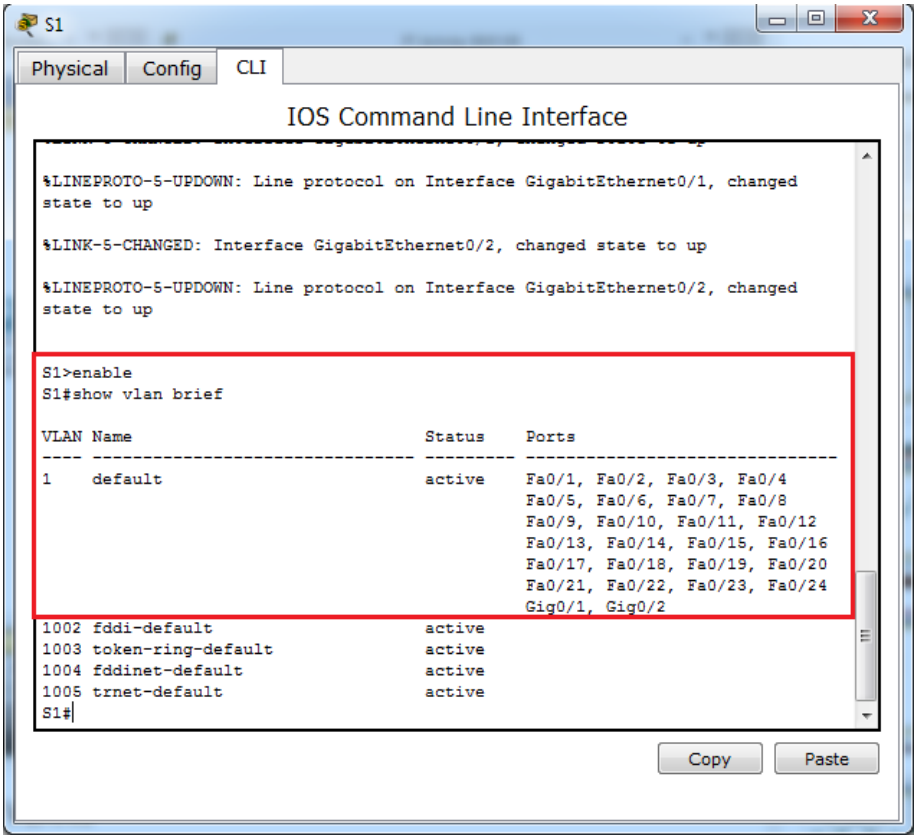
VLANs are helpful in the administration of logical groups, allowing members of a group to be easily moved, changed, or added. This activity focuses on creating and naming VLANs, and assigning access ports to specific VLANs.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

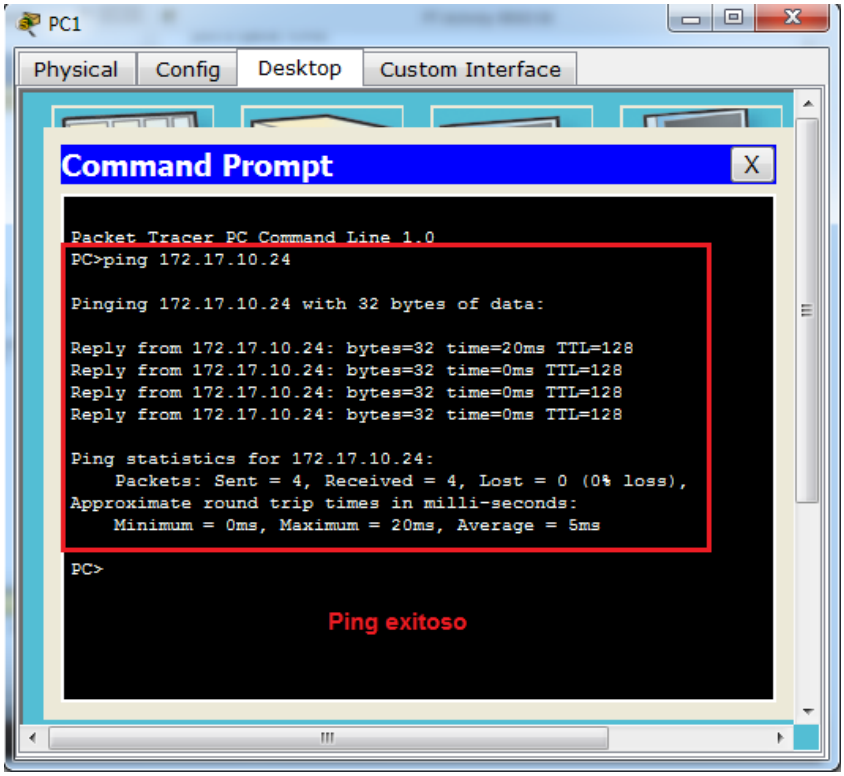


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

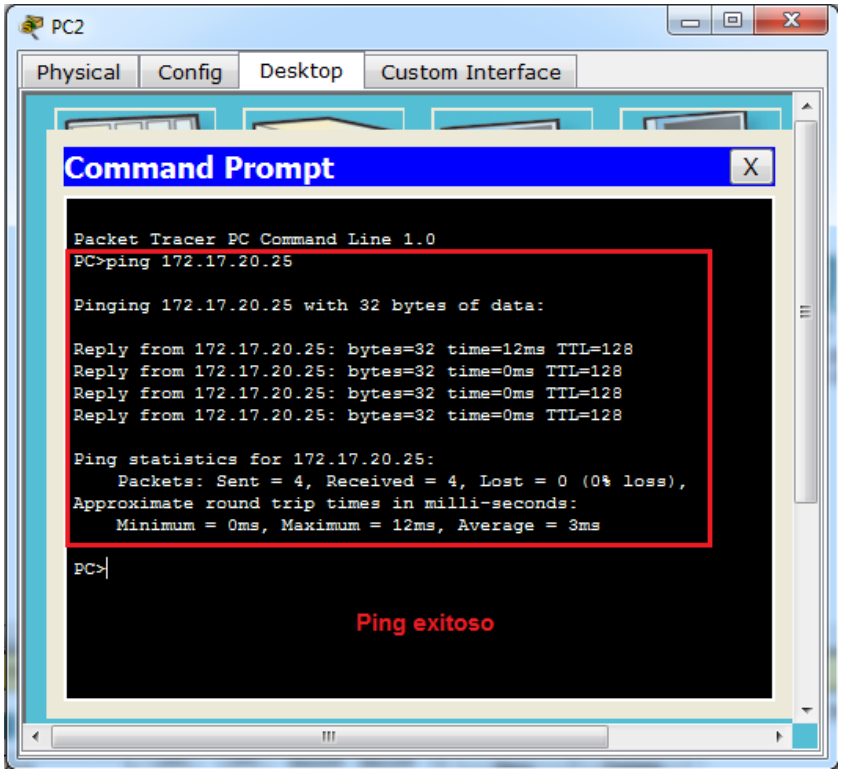
Step 2: Verify connectivity between PCs on the same network.

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

- PC1 can ping PC4

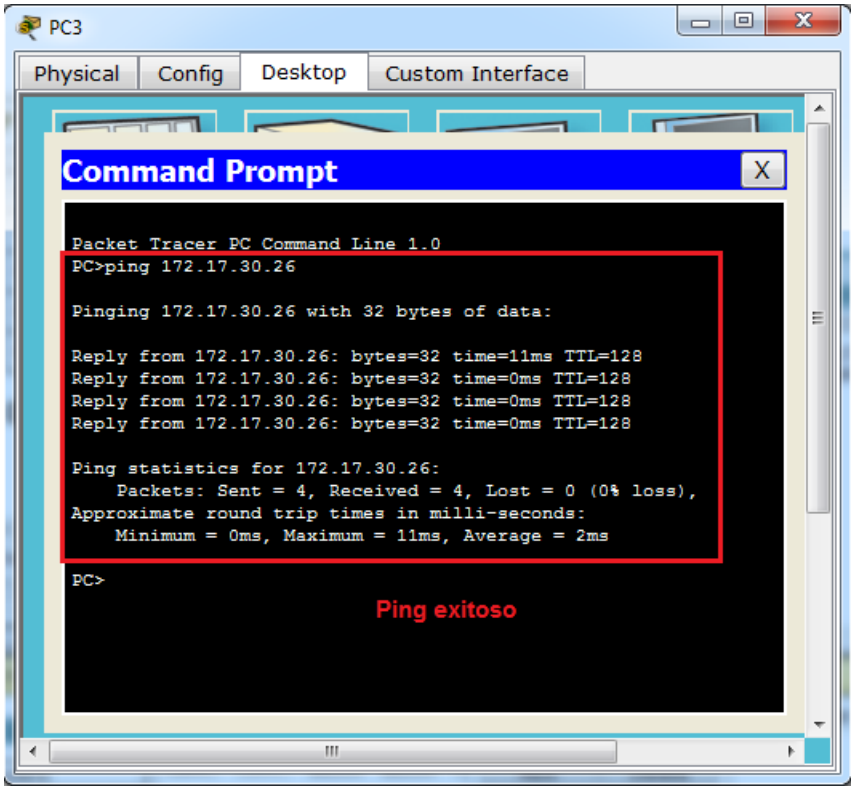


- PC2 can ping PC5

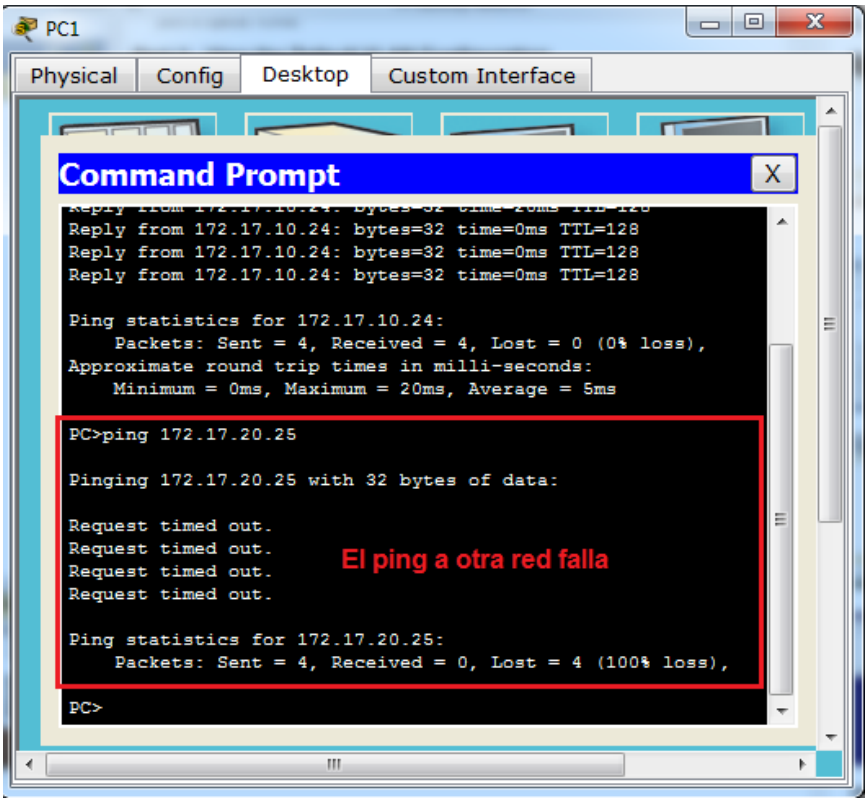


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

- PC3 can ping PC6



Pings to PCs in other networks fail. Para este caso se realizó ping al del PC1 a PC5



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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: seguridad, reducción de costes, rendimiento superior, mitigación de tormentas de difusión, mejora de la eficiencia del personal de TI y gestión más sencilla de proyectos y aplicaciones.

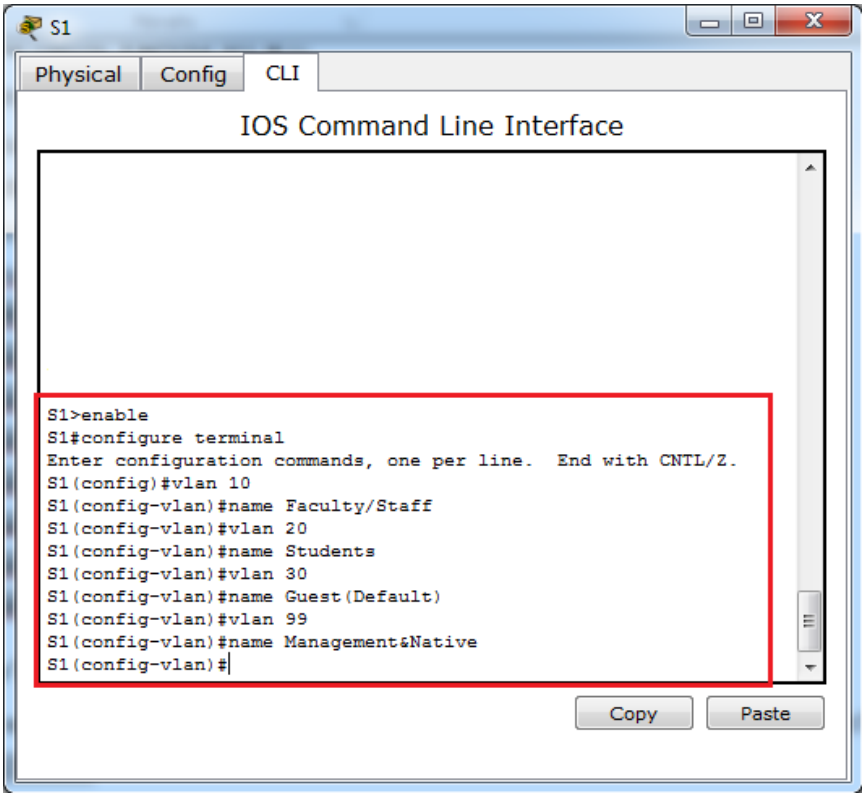
Part 2: Configure VLANs

Step 1: Create and name VLANs on S1.

Create the following VLANs. Names are case-sensitive:

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

```
S1#(config)# vlan 10
S1#(config-vlan)# name Faculty/Staff
S1#(config-vlan)#    vlan    20
S1#(config-vlan)# name Students
S1#(config-vlan)# vlan 30
S1#(config-vlan)# name Guest(Default)
S1#(config-vlan)# vlan 99
S1#(config-vlan)# name Management&Native
```

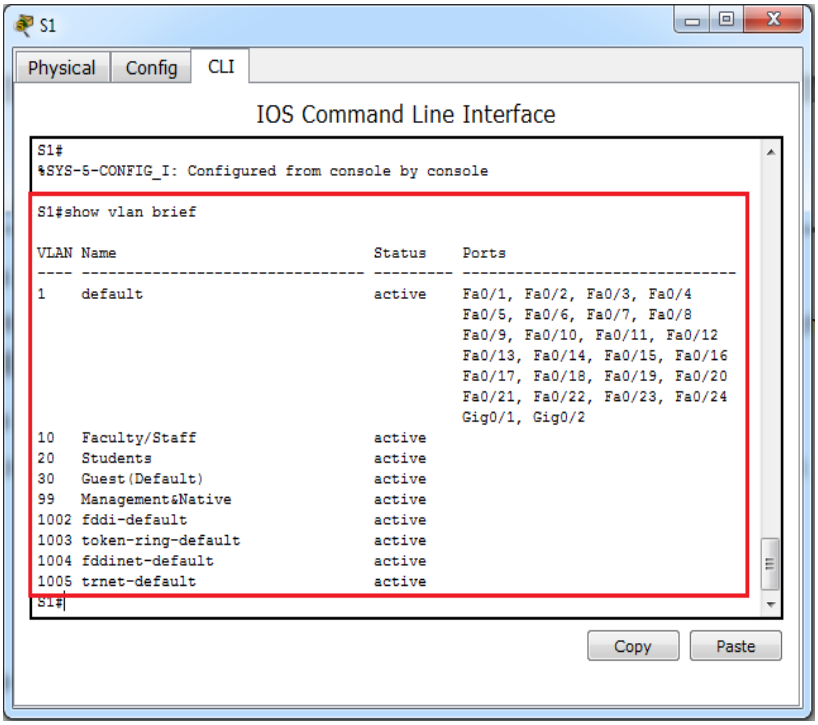


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Step 2: Verify the VLAN configuration.

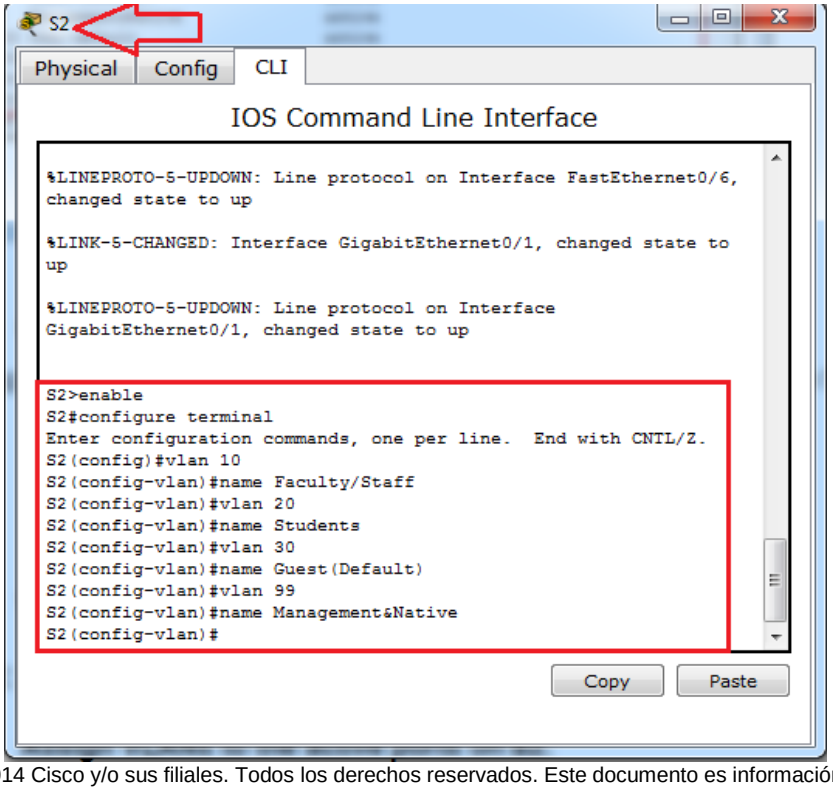
Which command will only display the VLAN name, status, and associated ports on a switch?

`S1# show vlan brief`

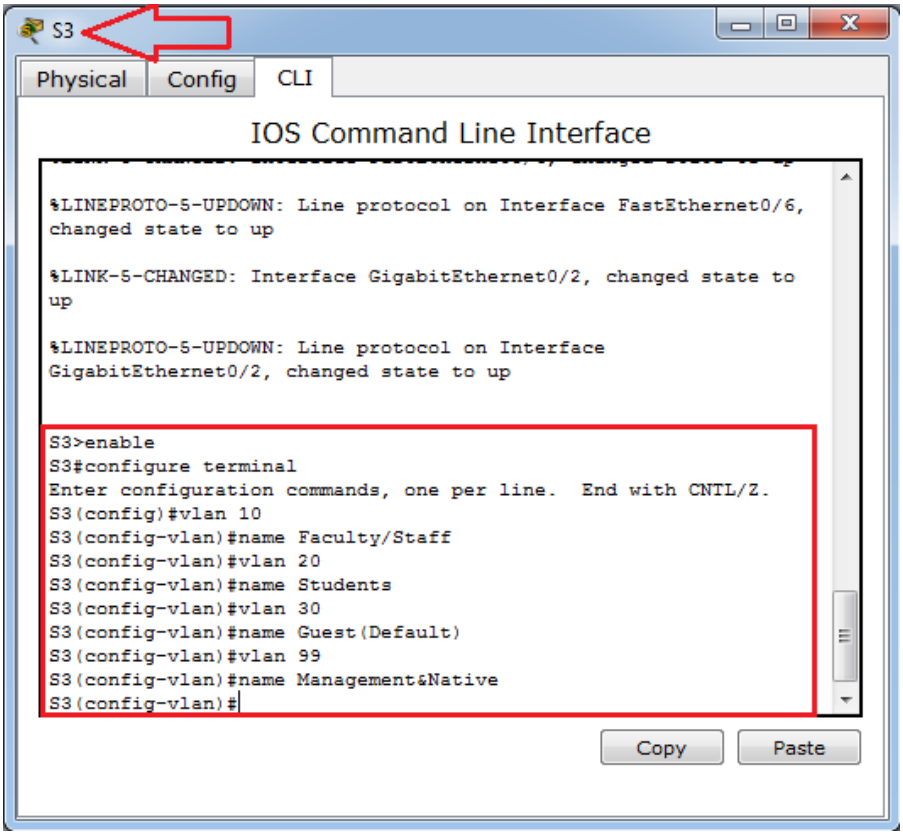


Step 3: Create the VLANs on S2 and S3.

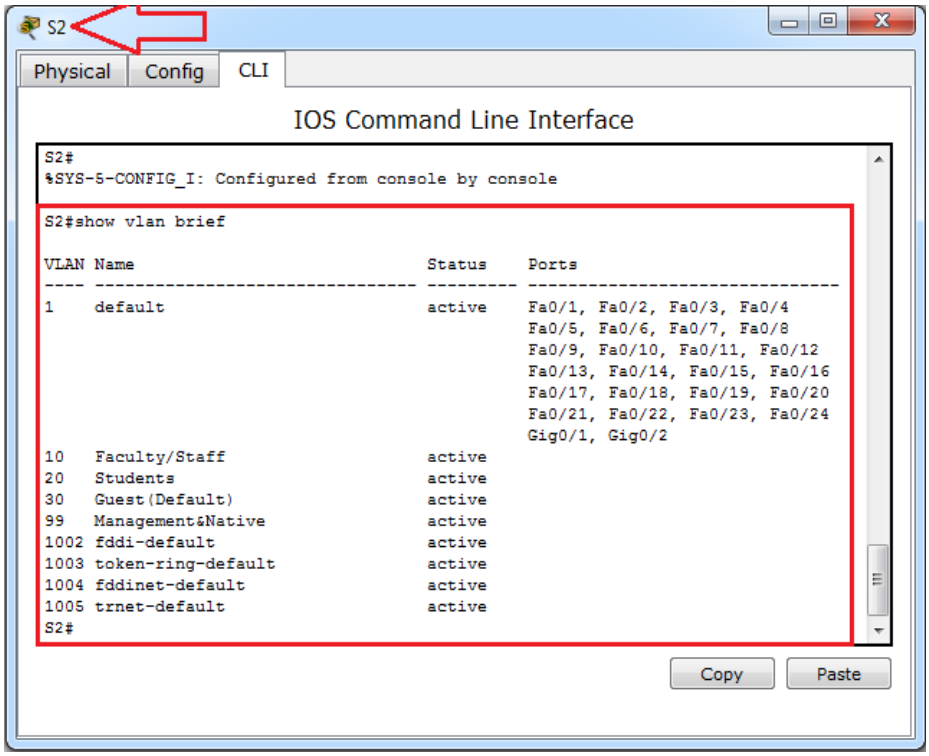
Using the same commands from Step 1, create and name the same VLANs on S2 and S3.



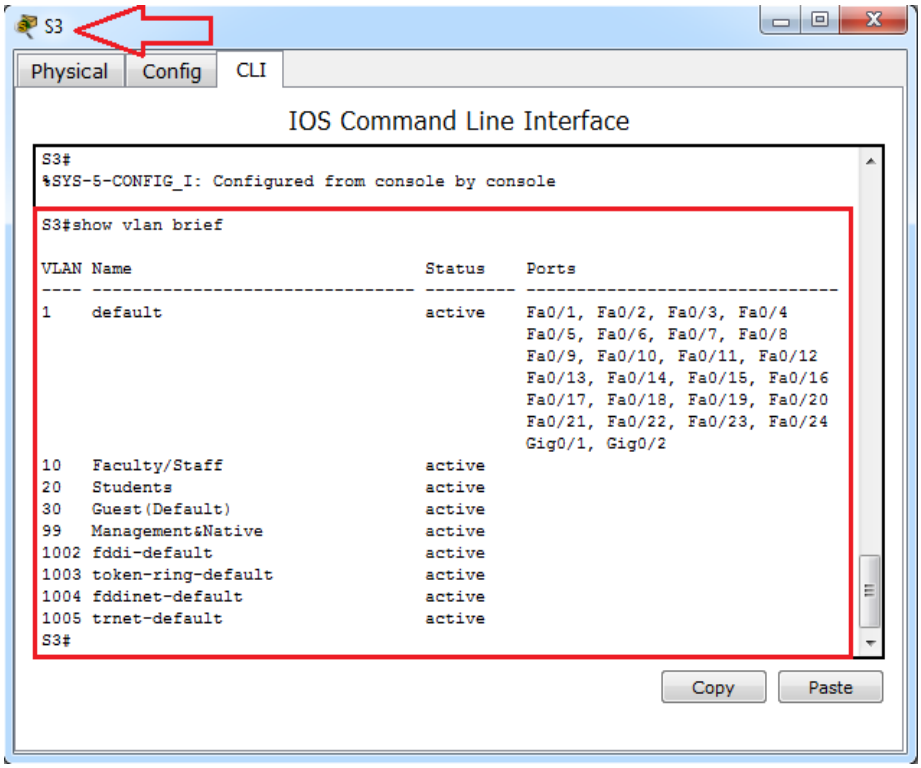
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



Step 4: Verify the VLAN configuration.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



Part 3: Assign VLANs to Ports

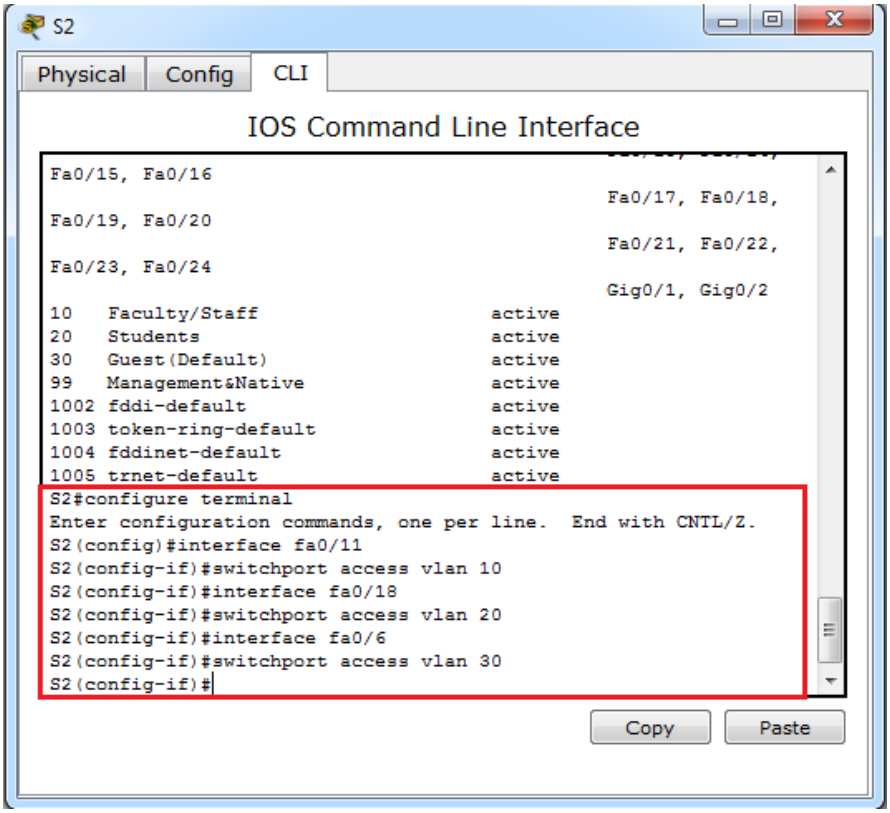
Step 1: Assign VLANs to the active ports on S2.

Assign the VLANs to the following ports:

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

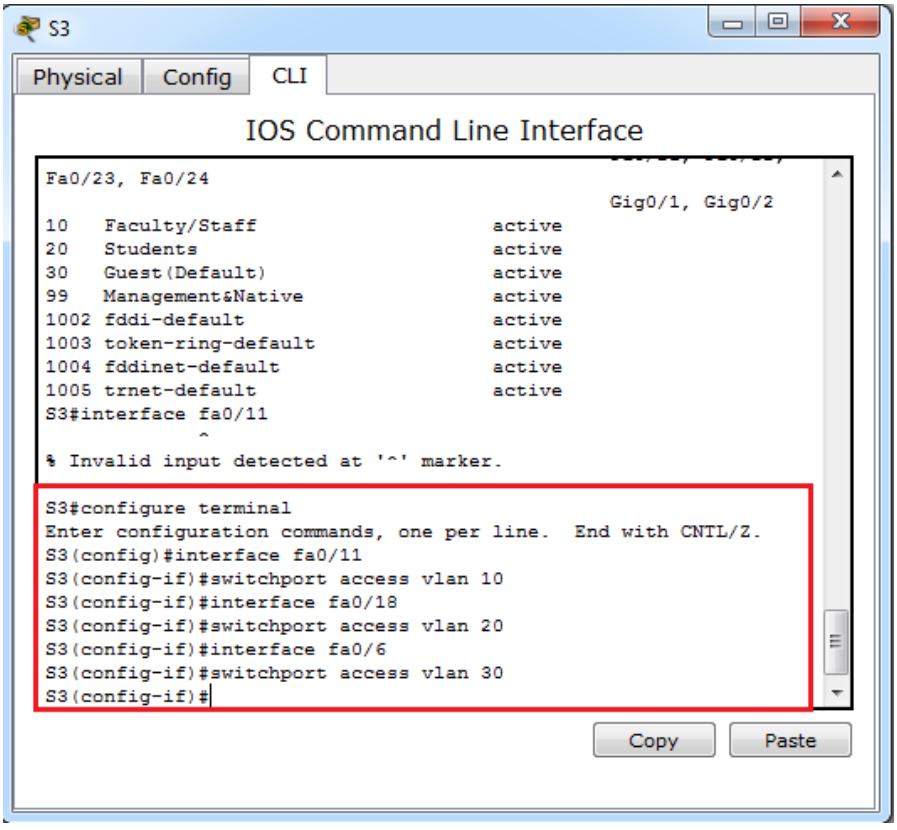
```
S2(config)# interface fa0/11
S2(config-if)# switchport access vlan 10
S2(config-if)#      interface      fa0/18
S2(config-if)# switchport access vlan 20
S2(config-if)# interface fa0/6
S2(config-if)# switchport access vlan 30
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



Step 2: Assign VLANs to the active ports on S3.

S3 uses the same VLAN access port assignments as S2.

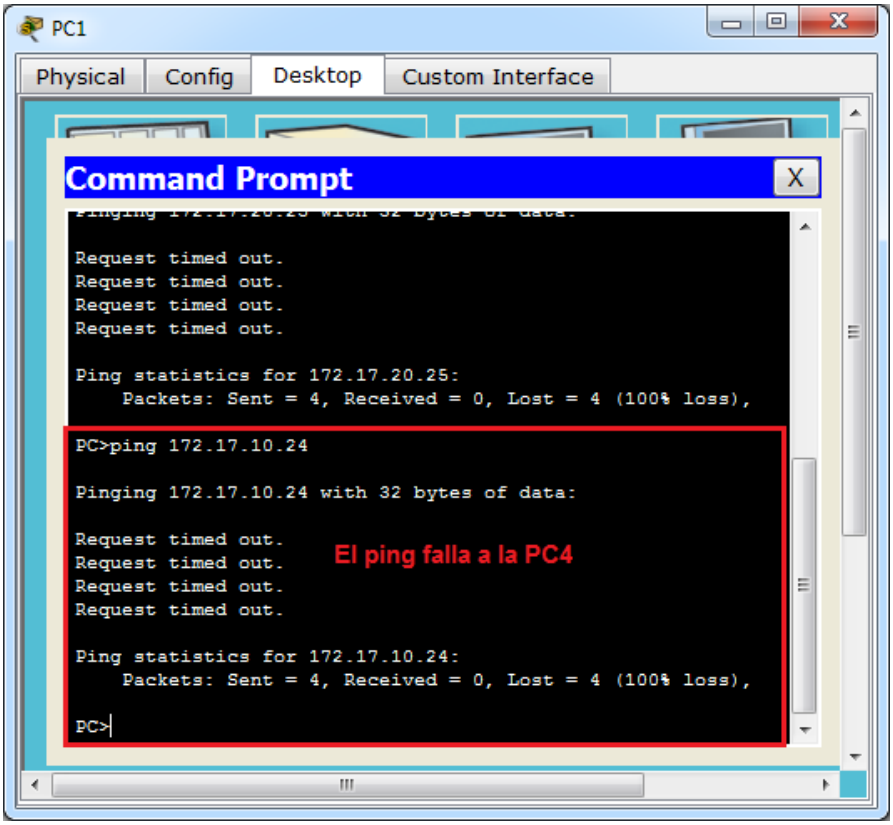


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

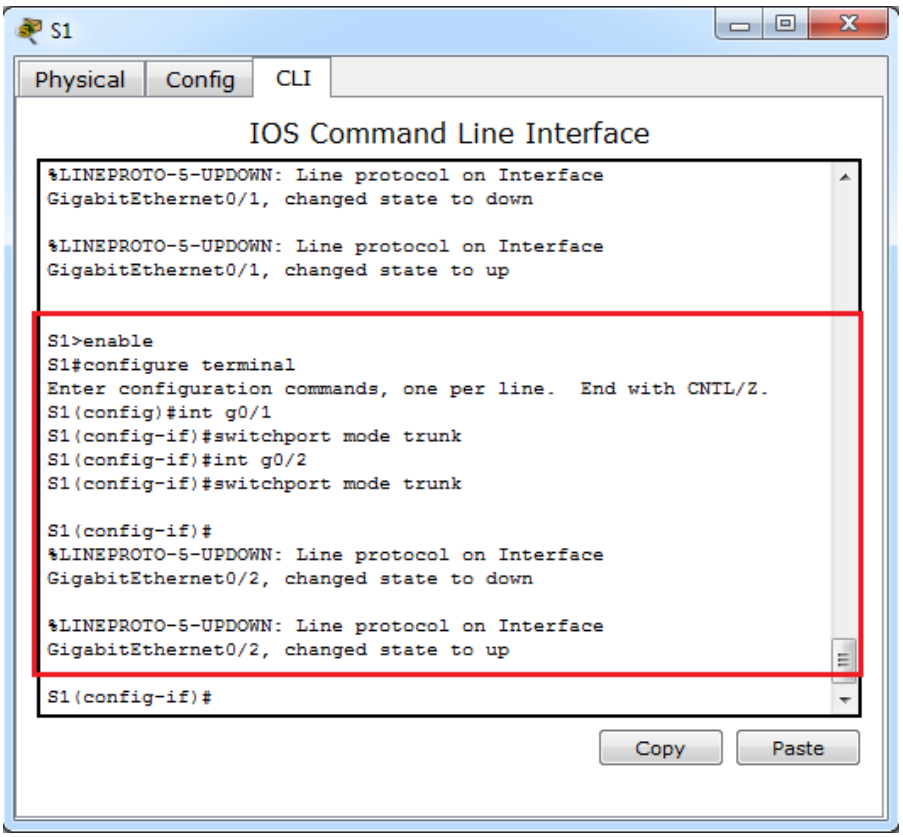
Los pings fallaron porque los puertos entre los switches están en VLAN 1 y PC1 y PC4 están en VLAN 10.

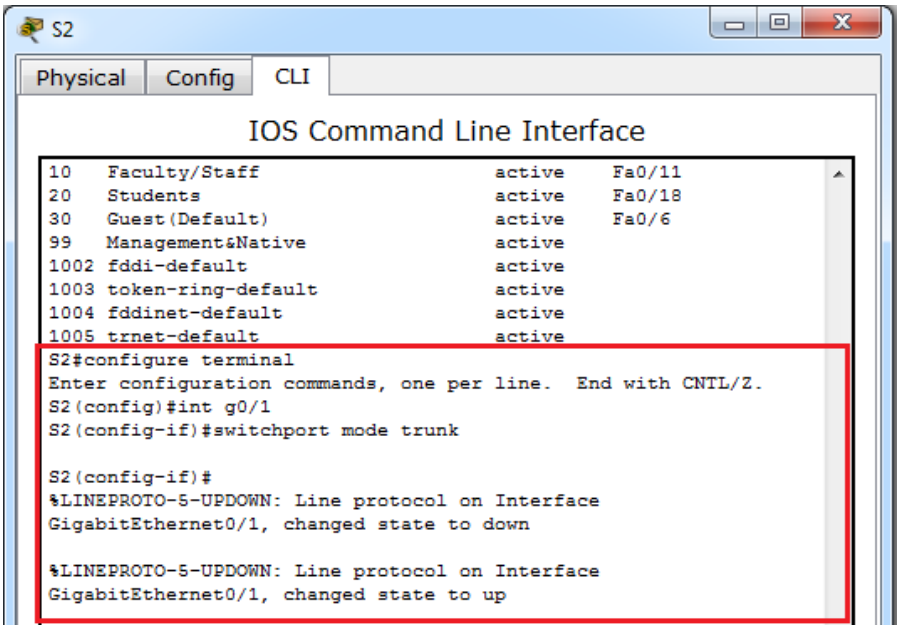


What could be done to resolve this issue? Configure the ports between the switches as trunk ports.

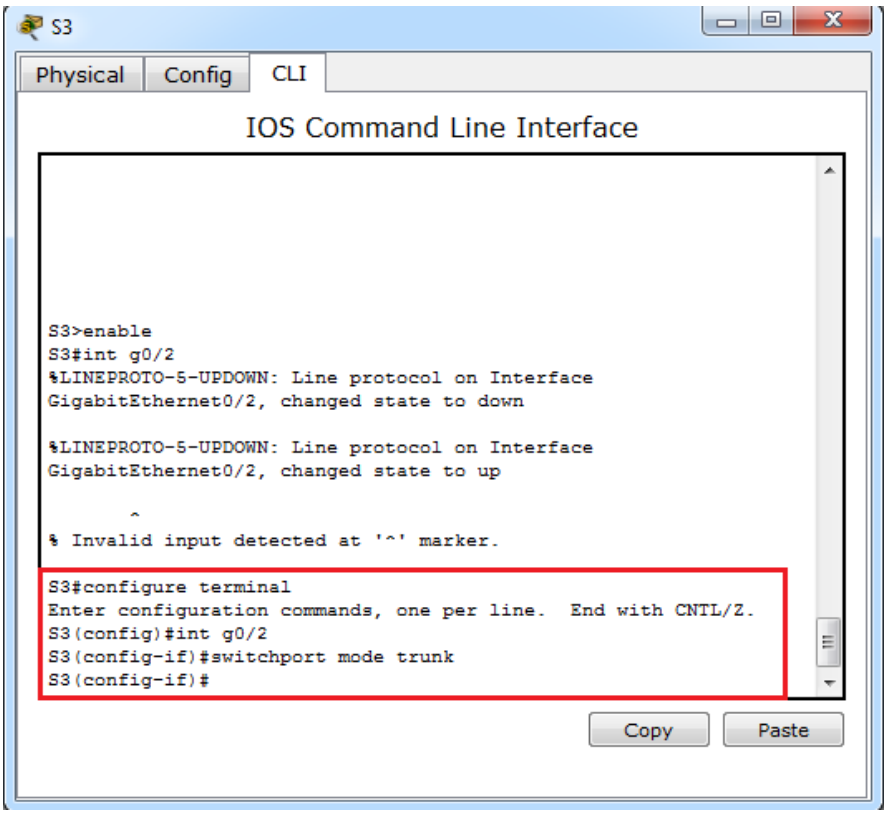
Configuramos los puertos entre los switches como puertos troncal.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

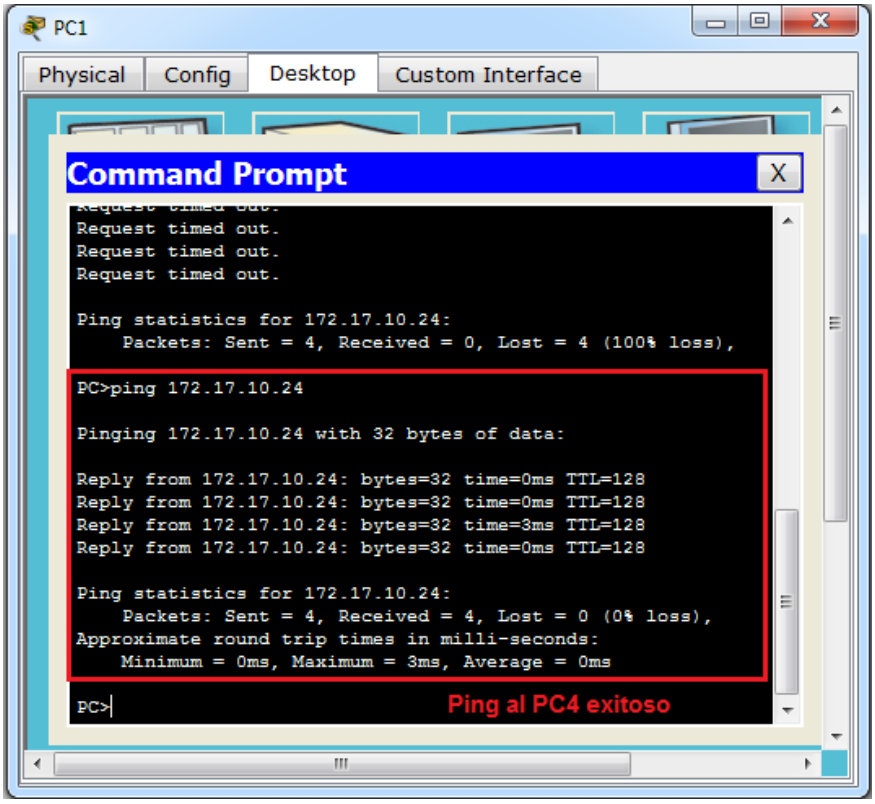




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

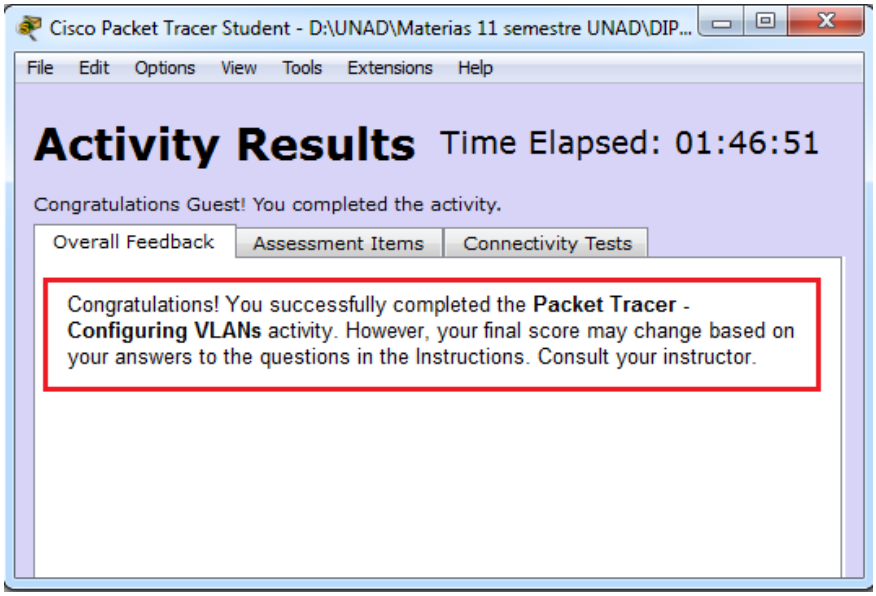


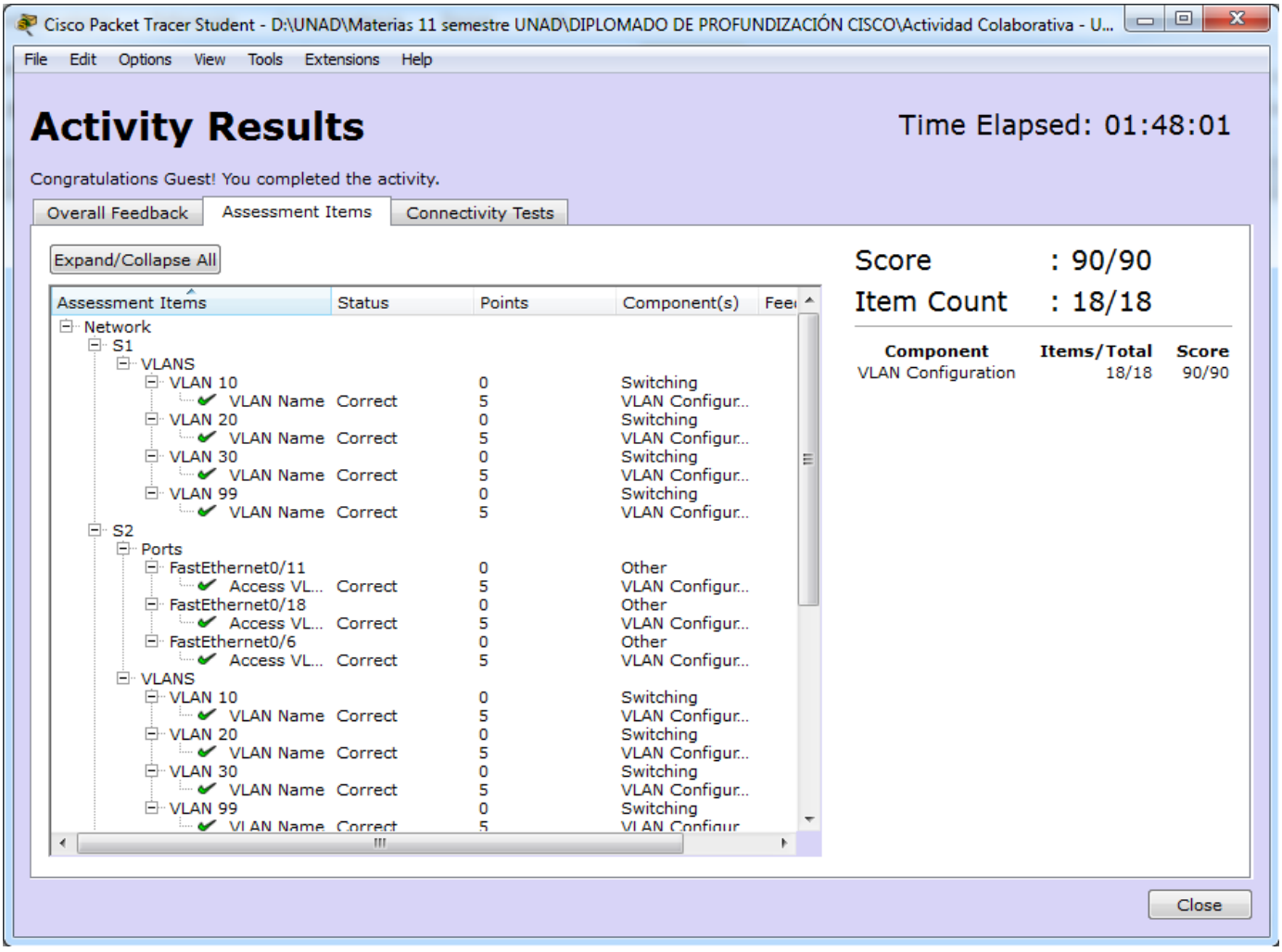
Volvemos a realizar ping al PC4 y nos muestra que el ping es exitoso



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Resultados de la actividad:





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

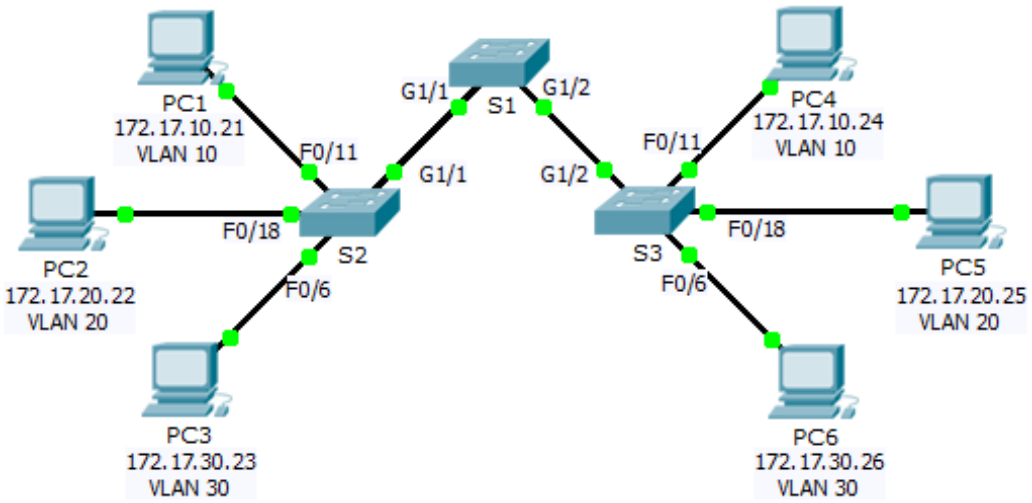
Conclusiones informe 4

- Con esta actividad se logró configurar las VLANs
- Se comprobó de manera correcta la configuración de VLAN predeterminada.
- Creamos y nombramos VLANs y se asignaron los respectivos puertos de acceso a VLANs específicas.
- Verificamos la conectividad entre los PCs en la misma red.
- Se dio a conocer los principales beneficios del uso de VLAN entre ellos están la seguridad, reducción de costes, mejor rendimiento.
- Se creó y configuro las VLANs en S1, S2 y S3.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 5: 3.2.2.4 Packet Tracer - Configuring Trunks

Topology



Addressing Table

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

Objectives

Part 1: Verify VLANs

Part 2: Configure Trunks

Background

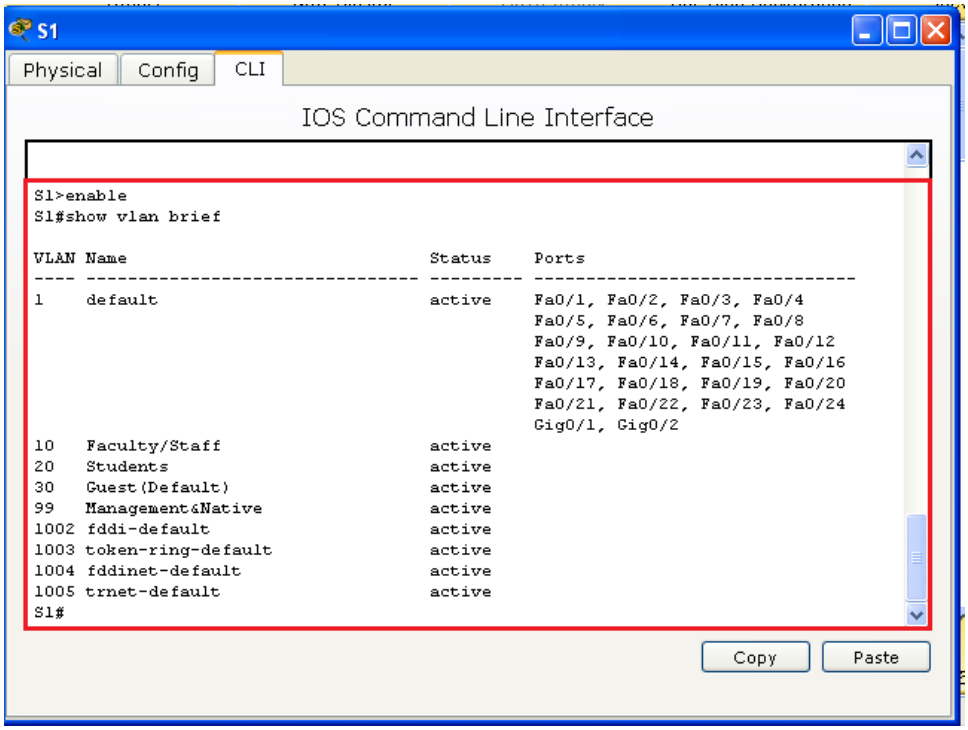
Trunks are required to pass VLAN information between switches. A port on a switch is either an access port or a trunk port. Access ports carry traffic from a specific VLAN assigned to the port. A trunk port by default is a member of all VLANs; therefore, it carries traffic for all VLANs. This activity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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

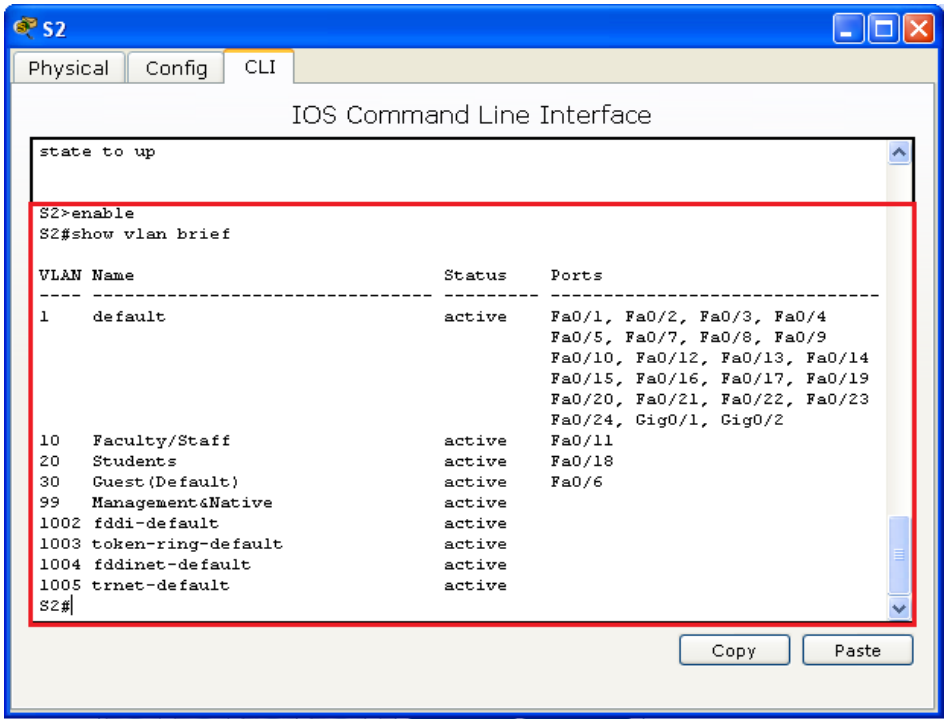
Part 1: Verify VLANs

Step 1: Display the current VLANs.

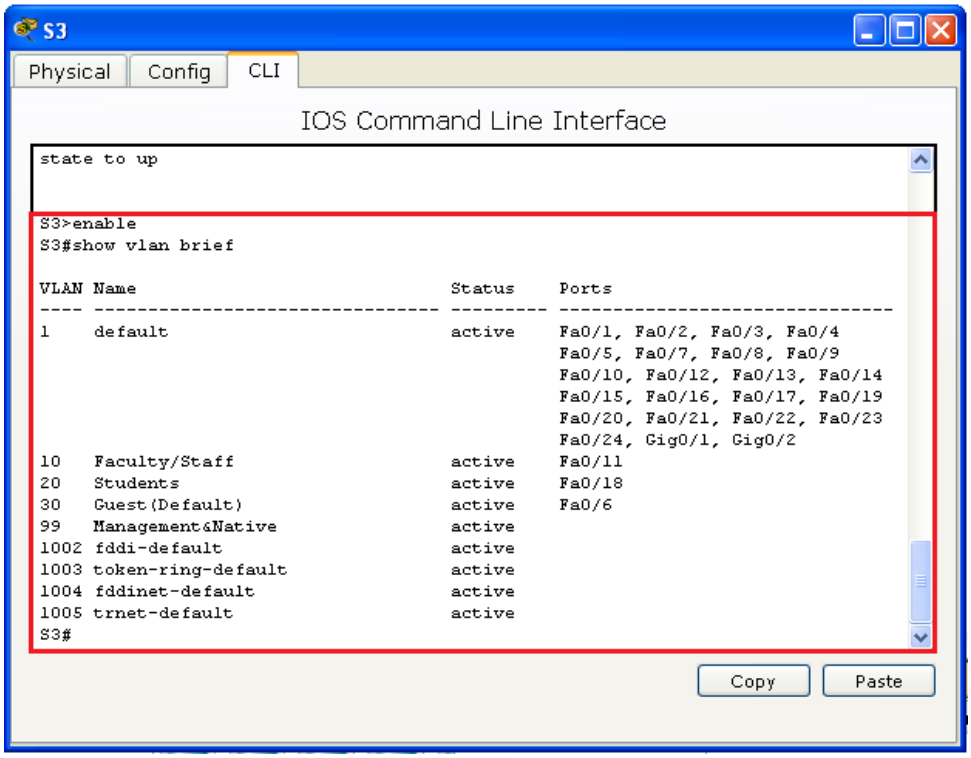
a. On **S1**, issue the command that will display all VLANs configured. There should be 9 VLANs in total. Notice how all 26 ports on the switch are assigned to one port or another.



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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

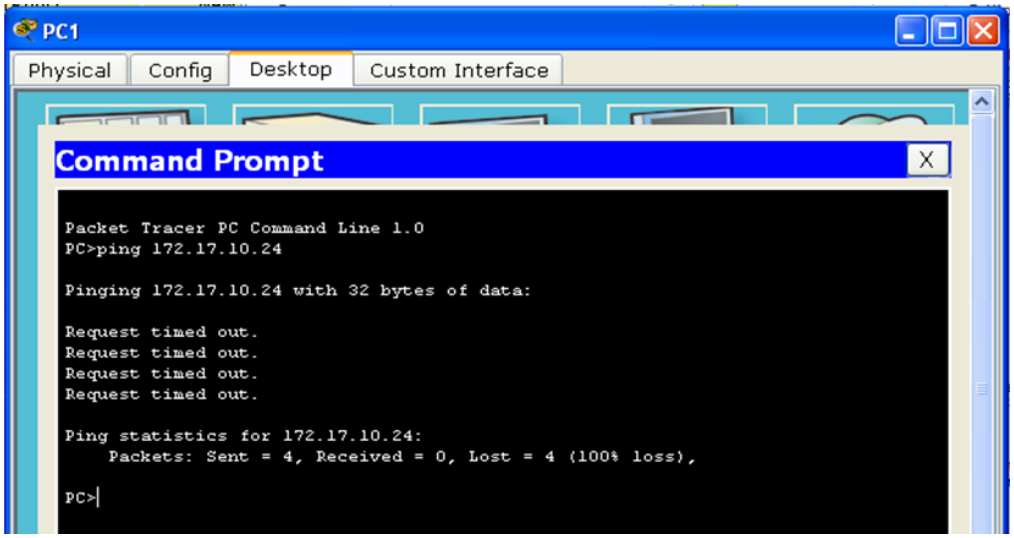


Step 2: Verify loss of connectivity between PCs on the same network.

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

PC1>ping 172.17.10.24

No hay conectividad. Están en la VLAN10 utilizan el Puerto f0/11



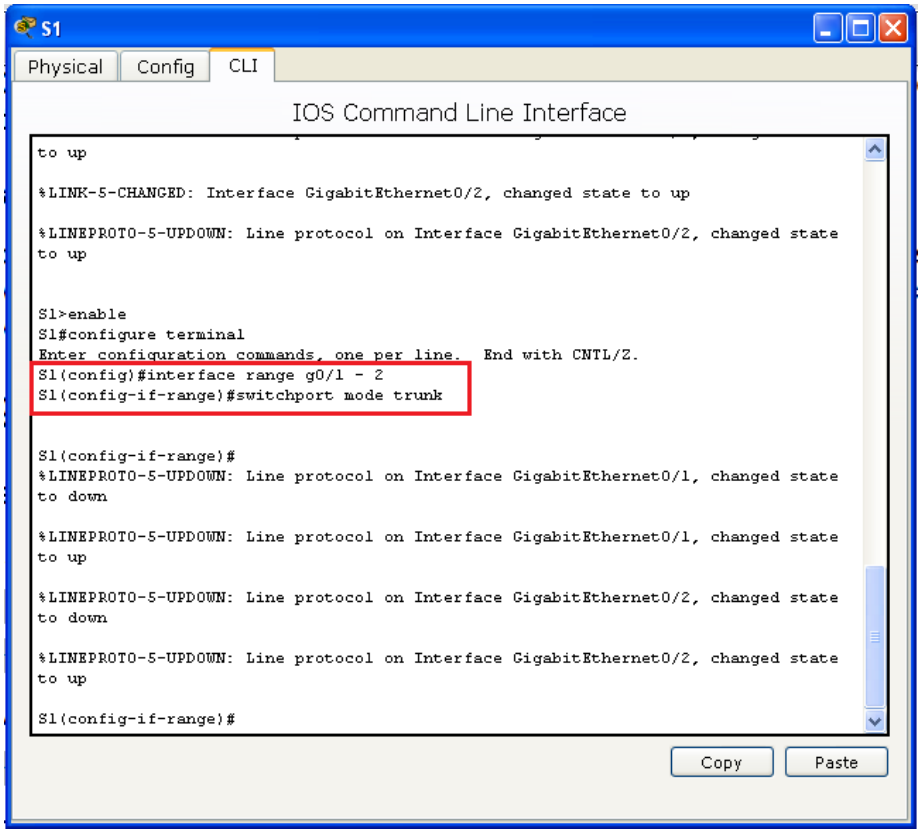
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Part 2: Configure Trunks

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

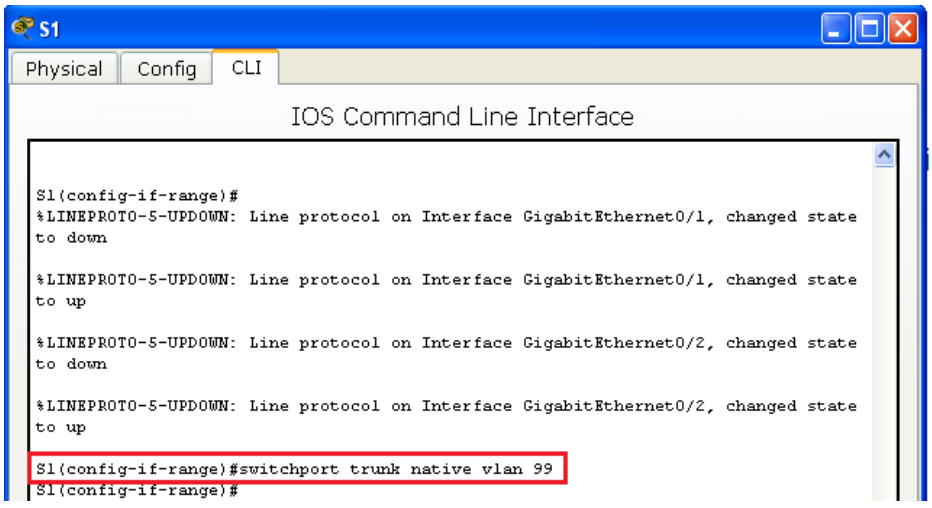
a. Configure G1/1 and G1/2 interfaces on S1 for trunking.

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



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

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

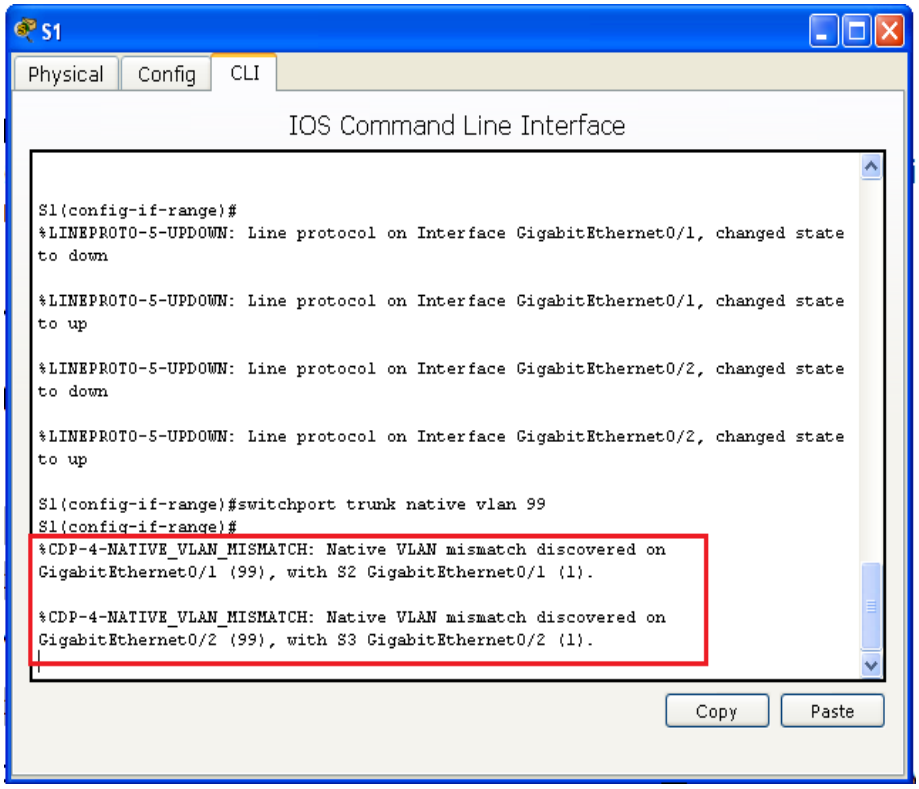
The trunk port takes about a minute to become active due to Spanning Tree which you will learn in the proceeding chapters. Click **Fast Forward Time** to speed the process. After the ports become active, you will periodically receive the following syslog messages:

```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/2
(99), with S3 GigabitEthernet1/2 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/1
(99), with S2 GigabitEthernet1/1 (1).
```

You configured VLAN 99 as the native VLAN on S1. However, the S2 and S3 are using VLAN 1 as the default native VLAN as indicated by the syslog message.

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

Los Pings tienen éxito porque el trunking se ha habilitado en S1. Dynamic Trunking Protocol (DTP) ha negociado automáticamente el otro lado de los enlaces troncal. En este caso, S2 y S3 han configurado automáticamente los puertos conectados a S1 como puertos de enlace.



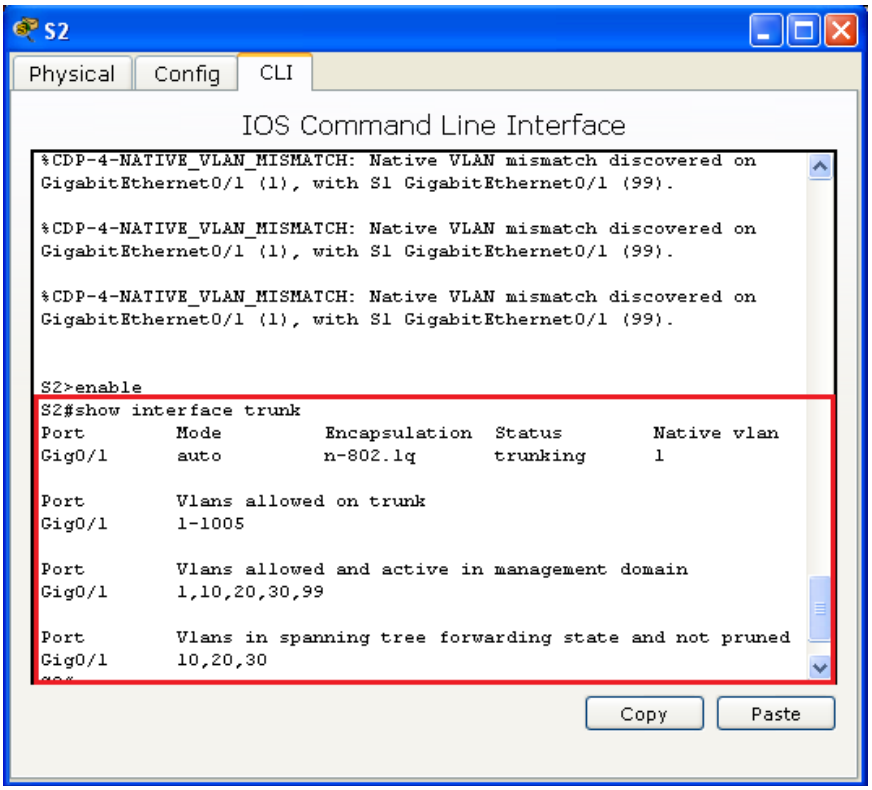
Con esto se busca que Los puertos g0/1-2 sean Troncales en la VLAN 99 Nativa, en S1. Pero se observa que no hay una coincidencia en las VLANs, ya que el S1 es la VLAN99 y en S2 y S3 es la VLAN1

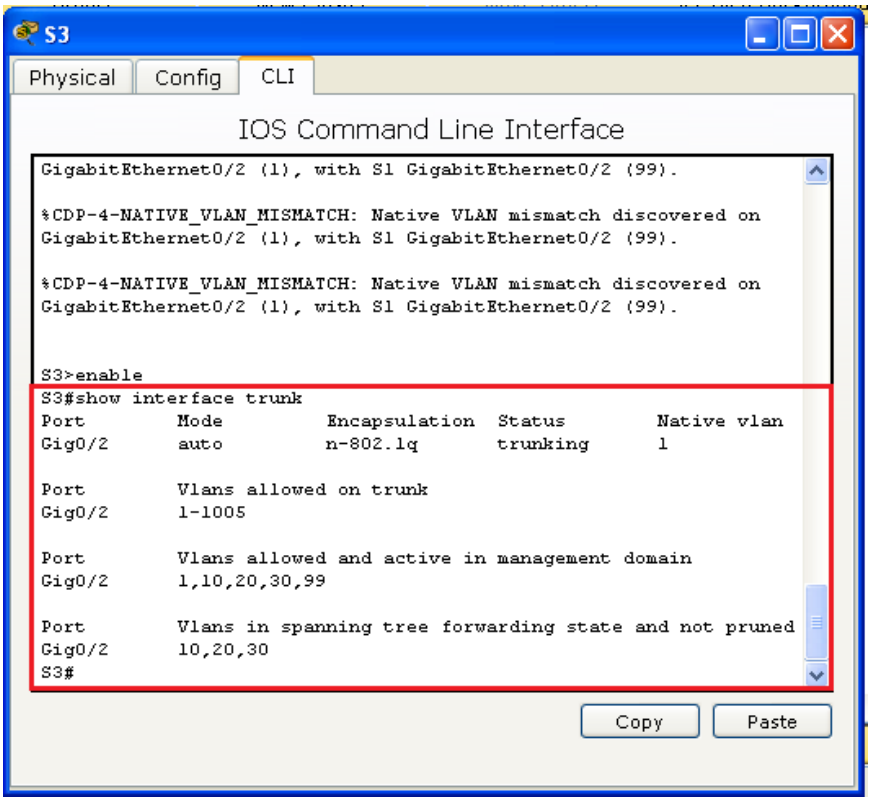
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

On **S2** and **S3**, issue the **show interface trunk** command to confirm that DTP has successfully negotiated trunking with S1 on S2 and S3. The output also displays information about the trunk interfaces on S2 and S3.

Which active VLANs are allowed to across the trunk? 1, 10, 20, 30, and 99.

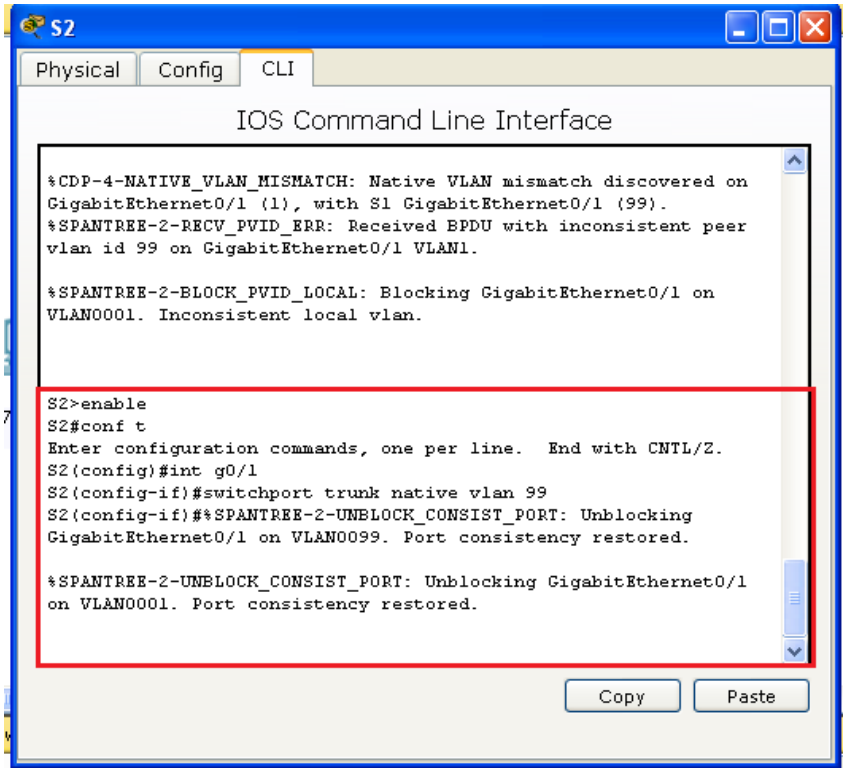


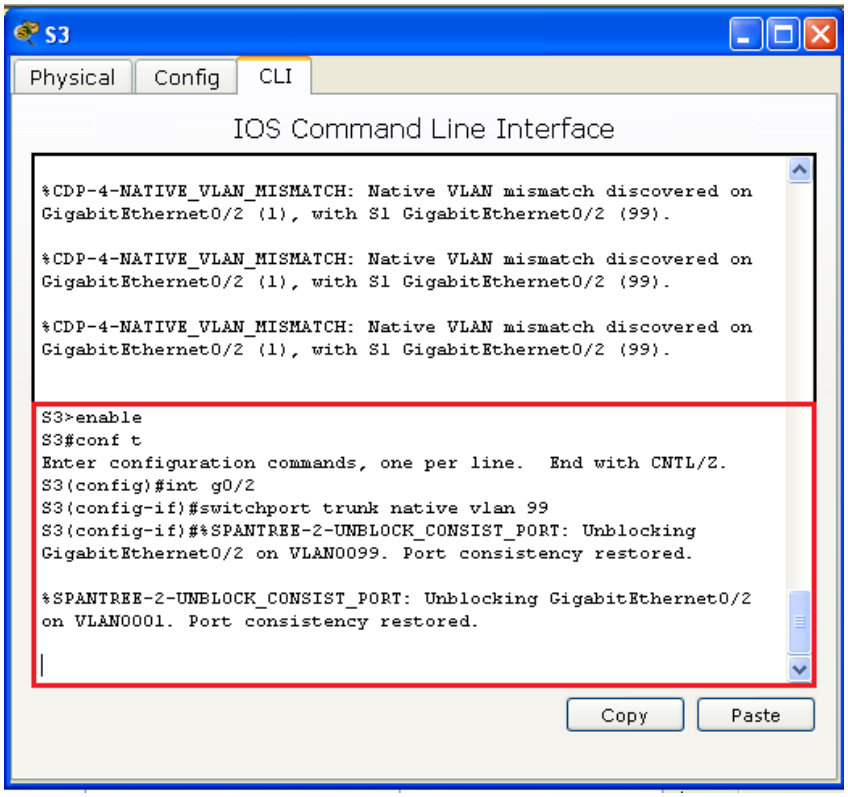


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

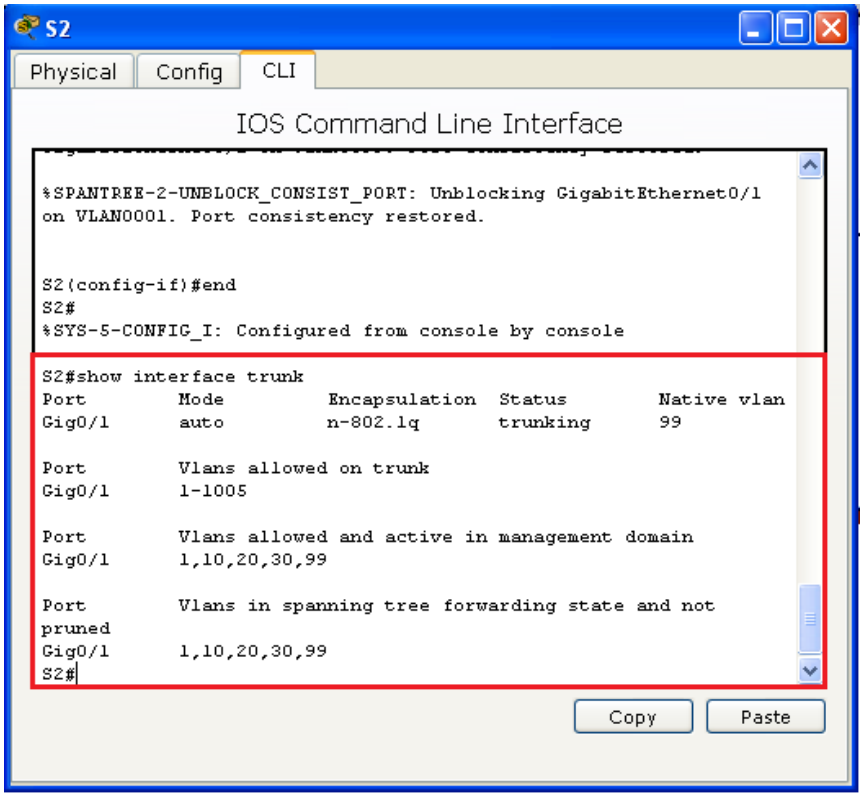
a. Configure VLAN 99 as the native VLAN for the appropriate interfaces on S2 and S3.

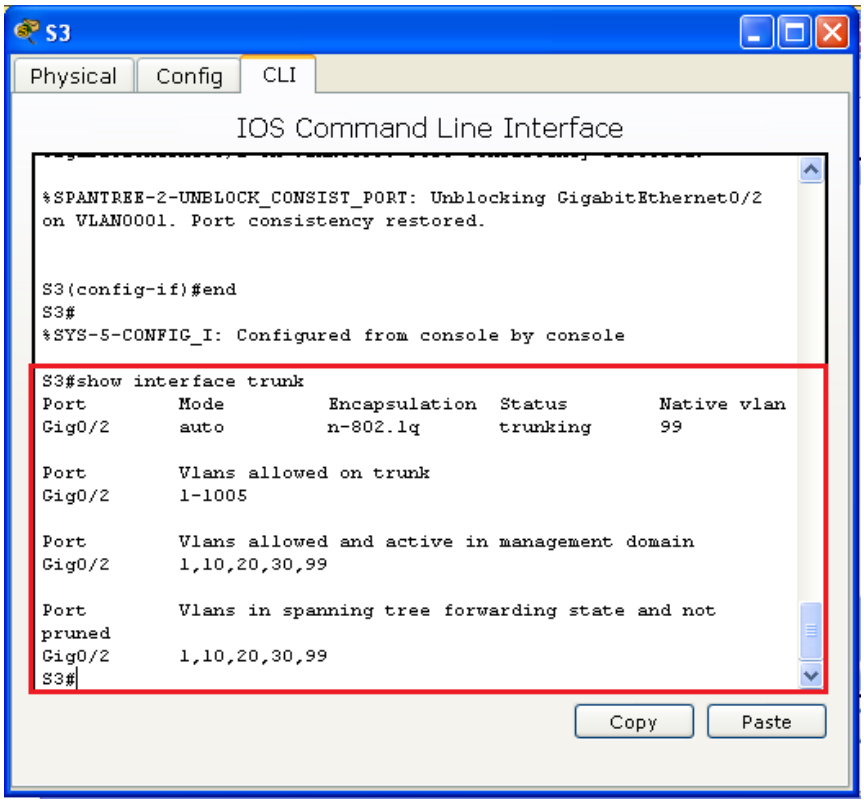




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

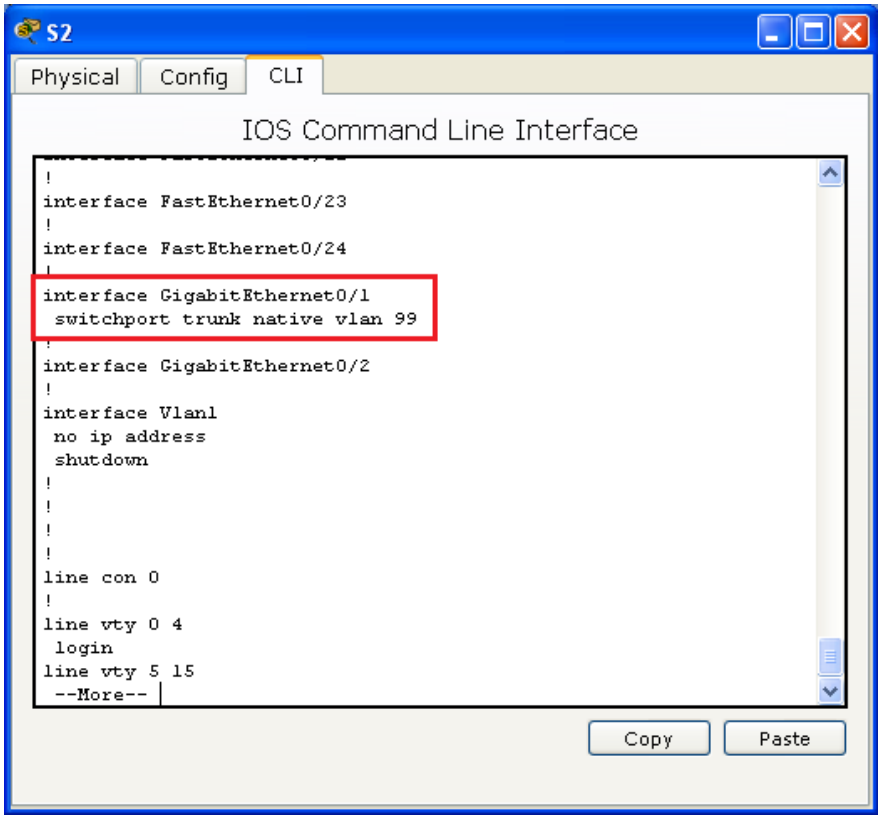


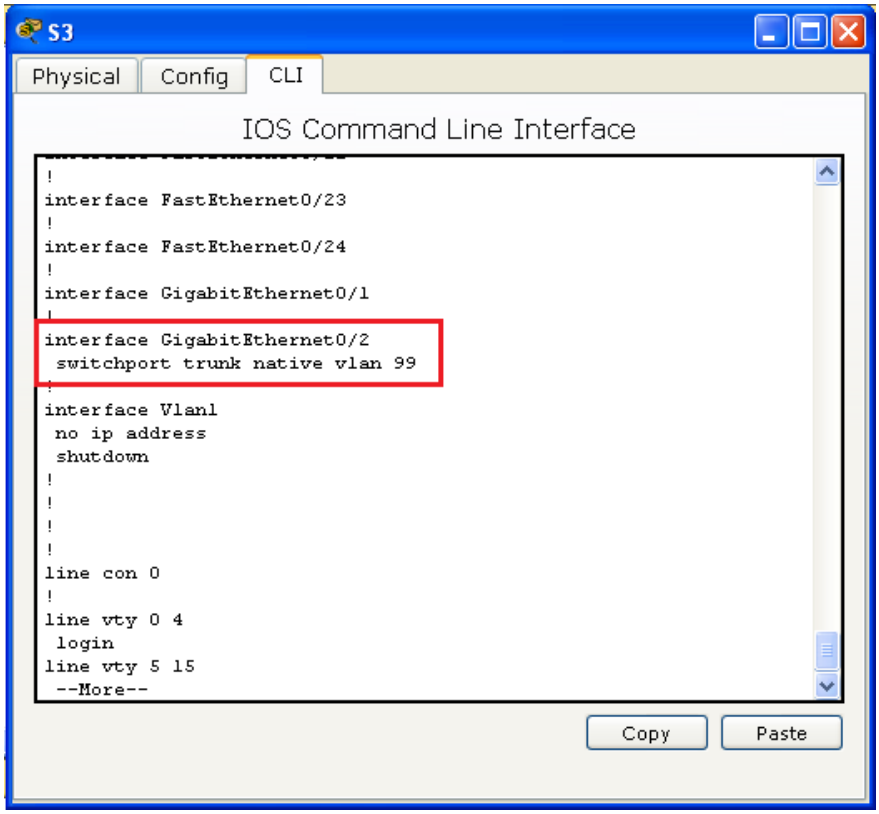


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Step 4: Verify configurations on S2 and S3.

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

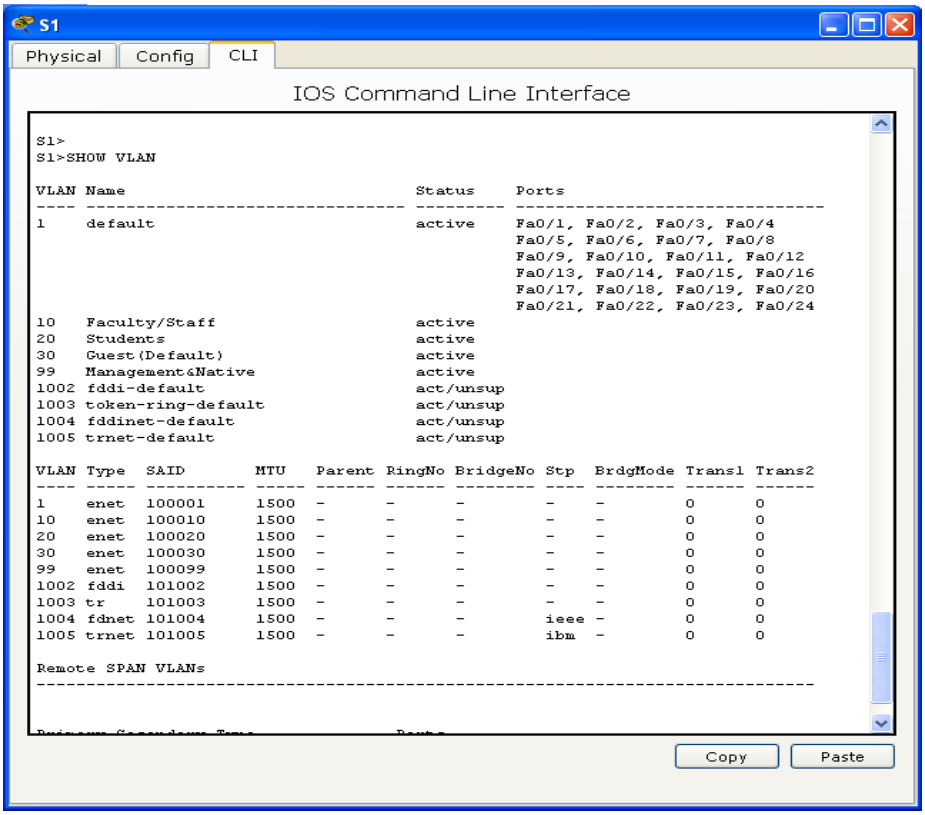


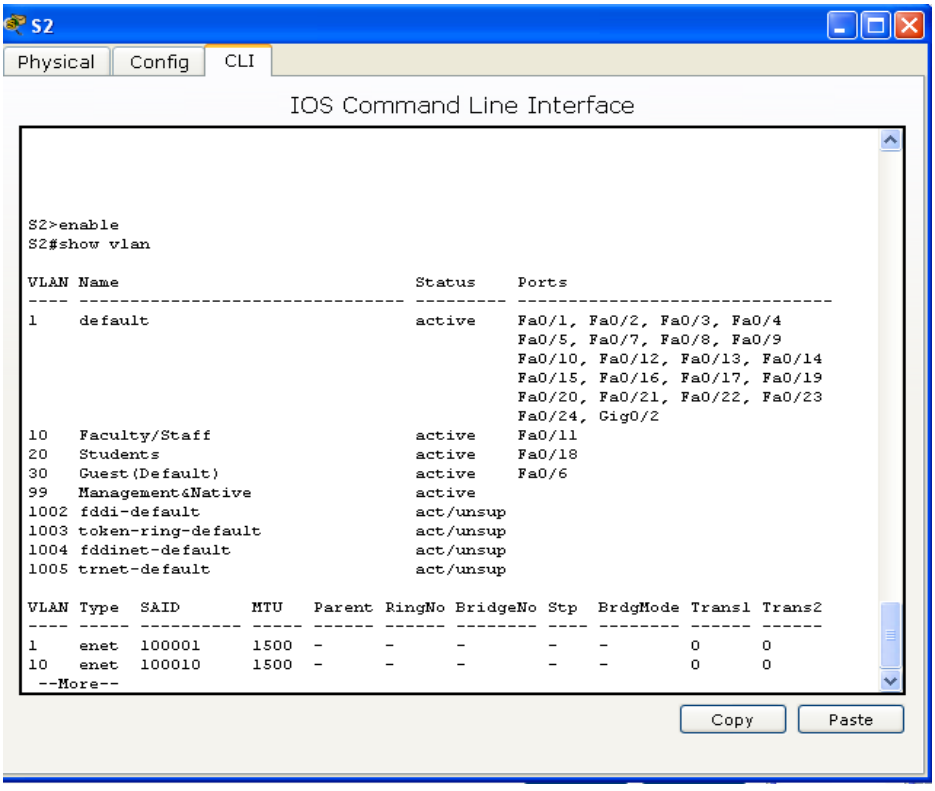


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

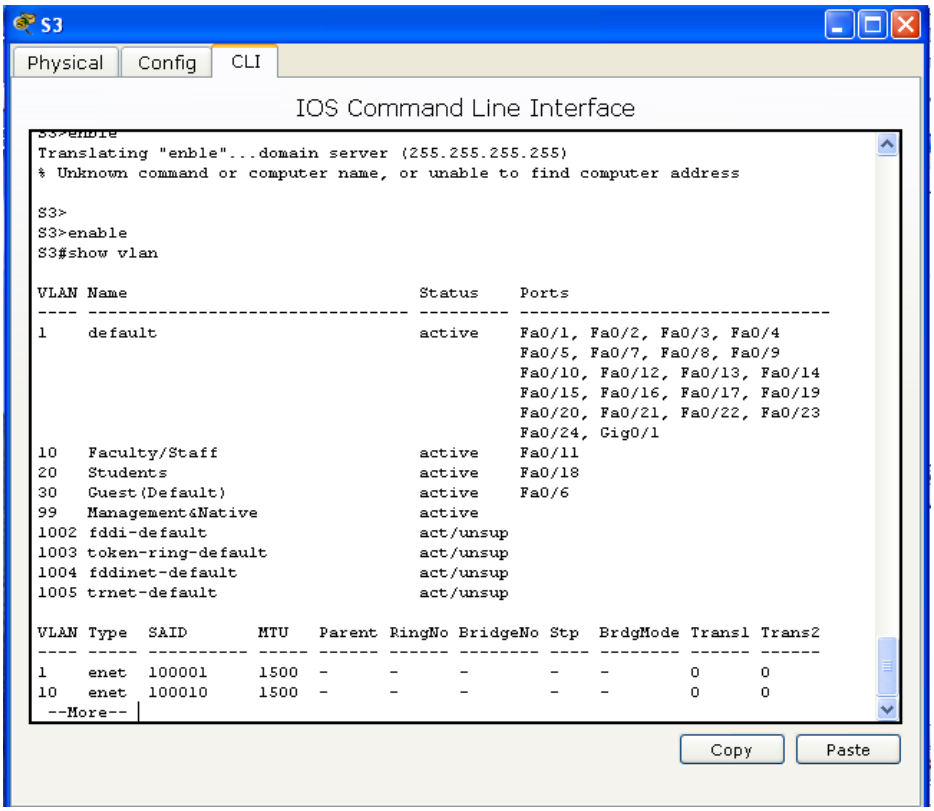
b. Use the **show vlan** command to display information regarding configured VLANs. Why is port G1/1 on S2 no longer assigned to VLAN 1? Port G0/1 is a trunk port and trunks ports are not displayed.

El puerto G0/1 es un puerto troncal y los puertos troncales no se muestran.

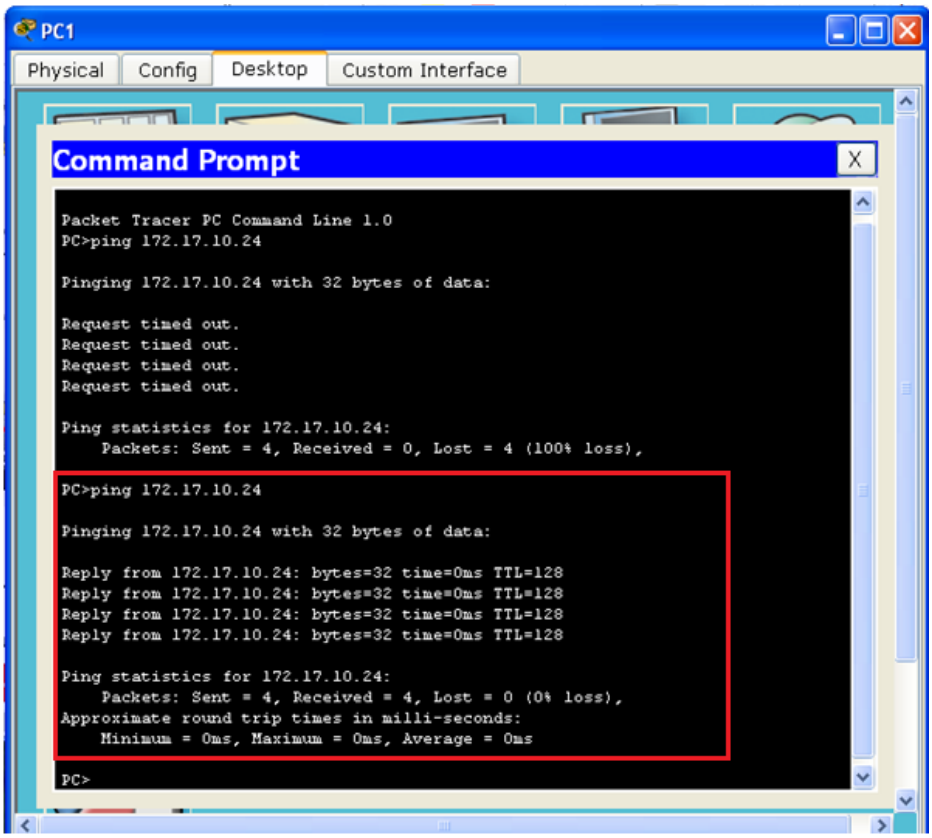




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



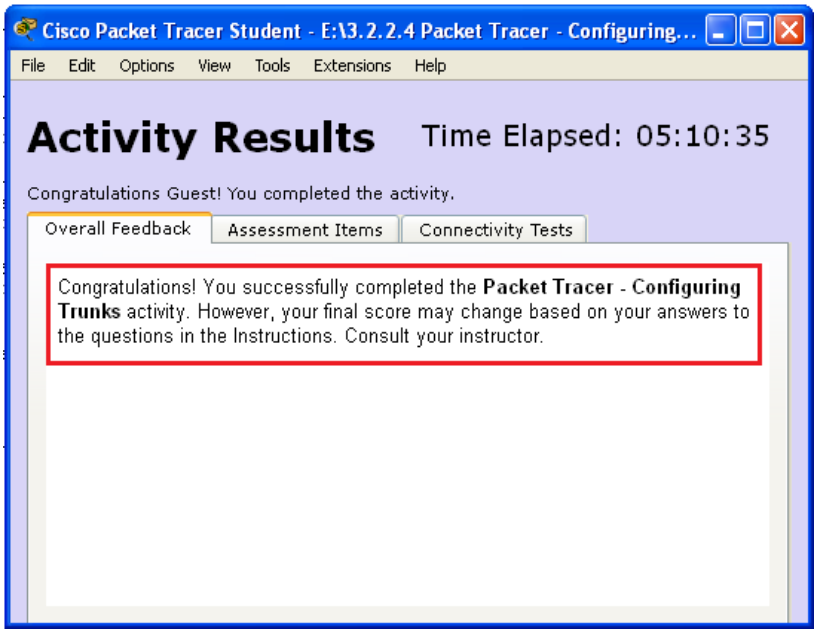
Ahora el ping de la pc1 a la pc4 es satisfactorio

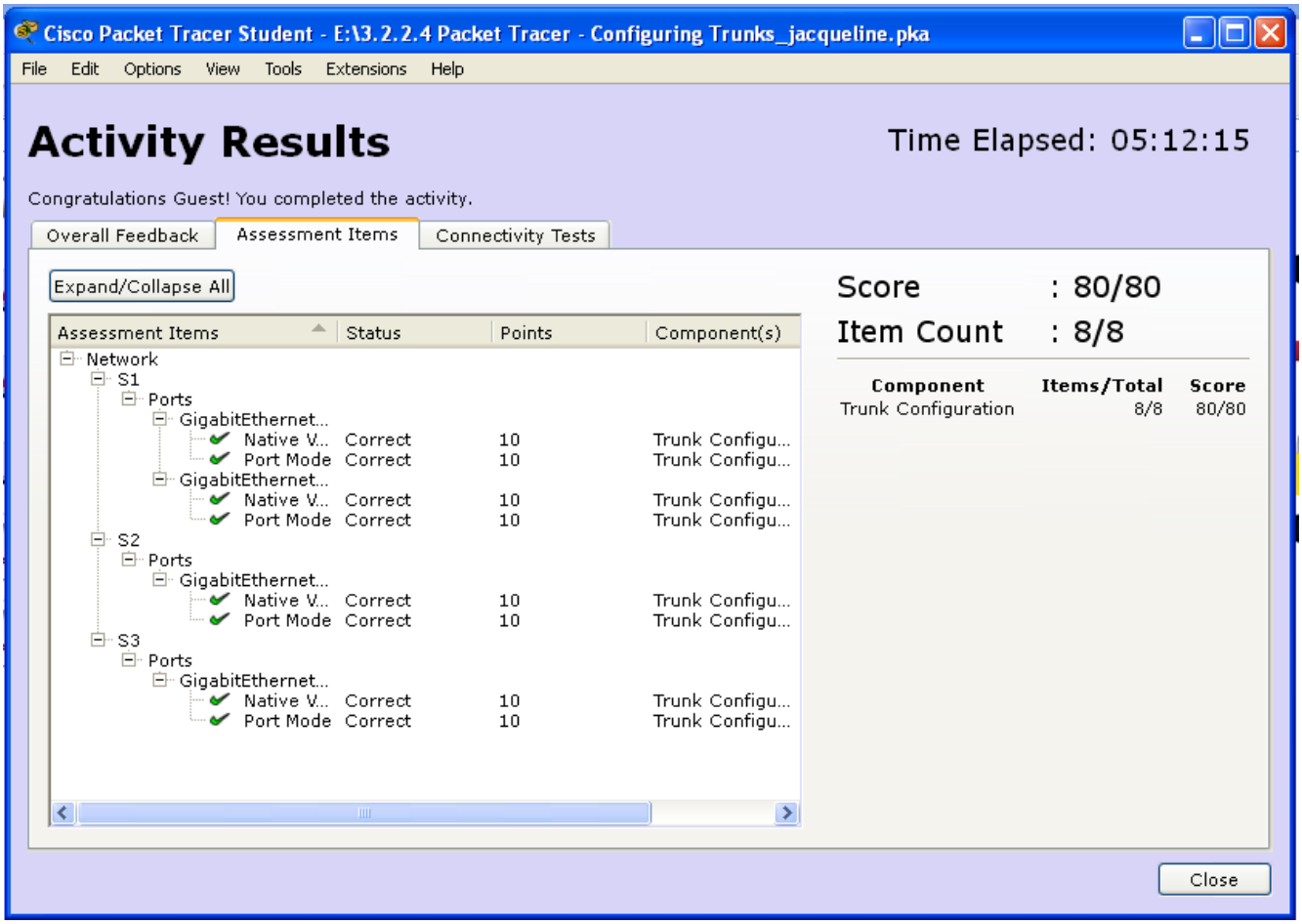


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Suggested Scoring Rubric

Packet Tracer scores 80 points. The three questions in Step 1, 2 and 4 are worth 20 points.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 5

- Es muy importante tener en cuenta que dentro del concepto de las VLANs, se puede configurar la VLAN 99 como nativa, la cual debe configurarse como troncal en cada uno de los switches que estarán conectados y de acuerdo a los puertos g0/1 o g0/2 según el caso. Esto permite la comunicación entre ordenadores que pertenezcan a una determinada VLAN y un puerto físico asignado del switch respectivo.
- Esta actividad se centró en crear puertos troncales y asignarlos a una VLAN nativa distinta de la predeterminada.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 6: 3.2.2.5 Lab - Configuring VLANs and Trunking

Práctica de laboratorio: configuración de redes VLAN y enlaces troncales

Topología

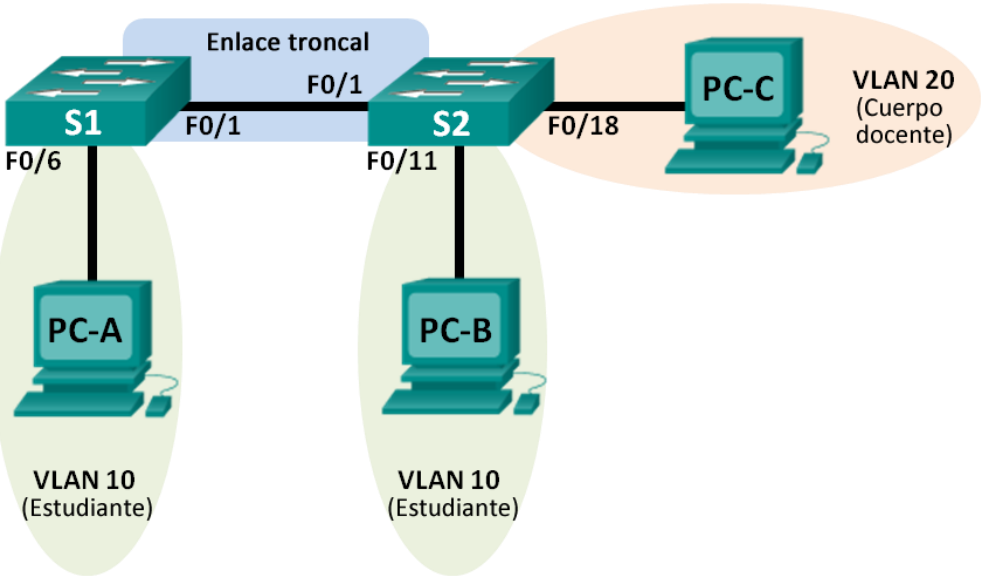


Tabla de direccionamiento

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

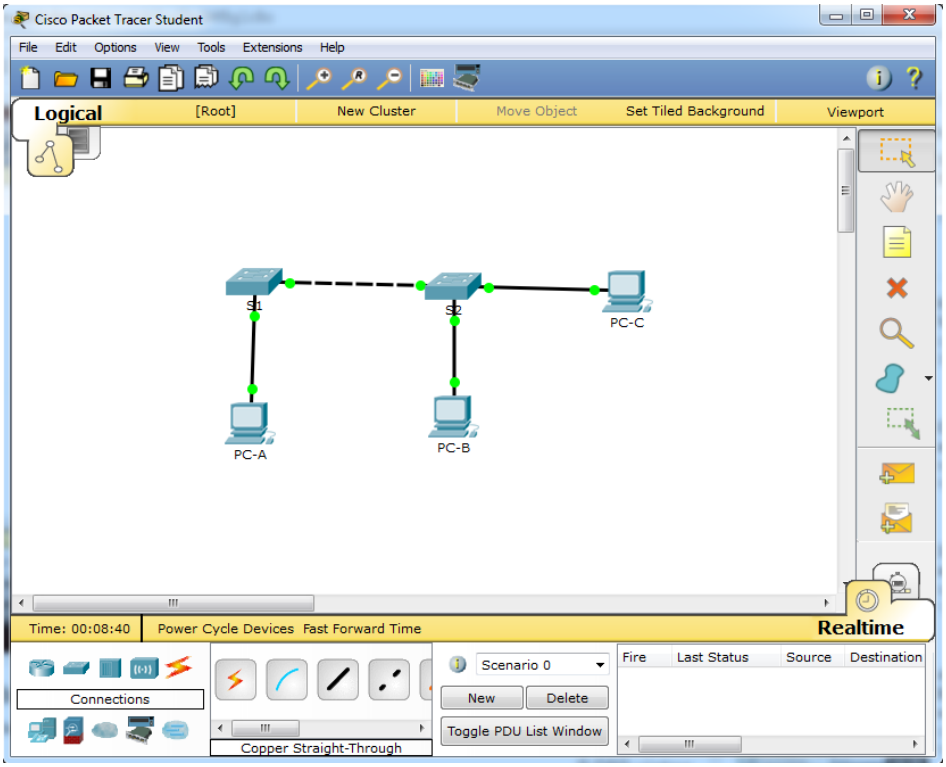
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

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

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



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

Paso 3. Configurar los parámetros básicos para cada switch.

a. Desactive la búsqueda del DNS.

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

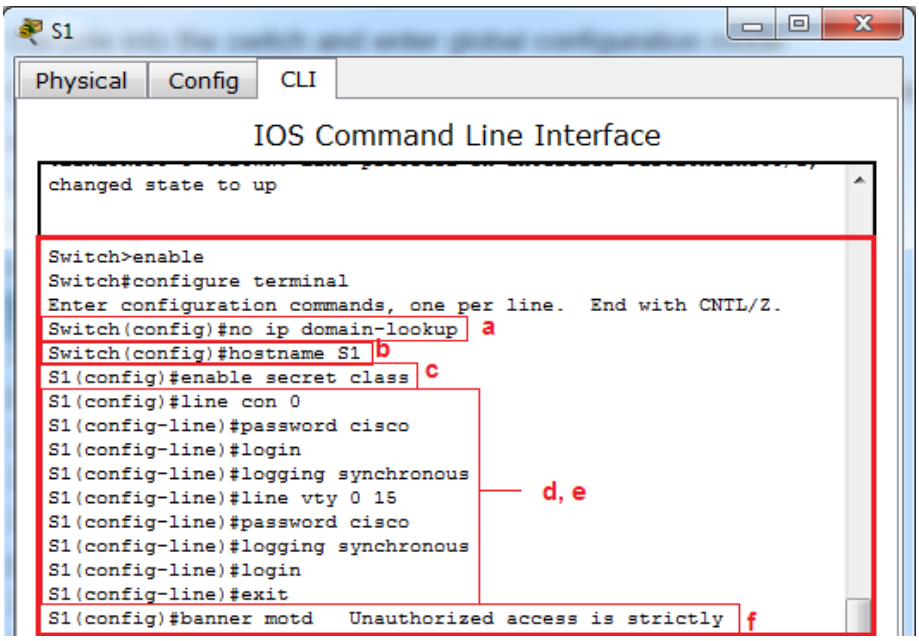
c. Asigne **class** como la contraseña del modo EXEC privilegiado.

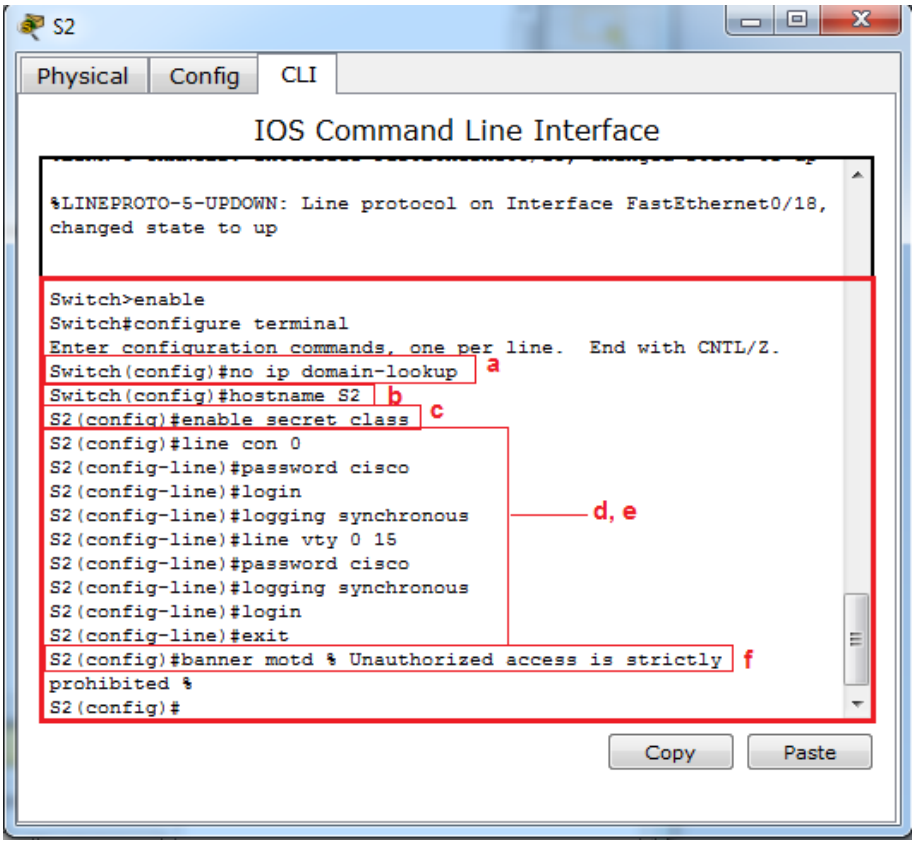
d. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión para las líneas de vty y de consola.

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

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

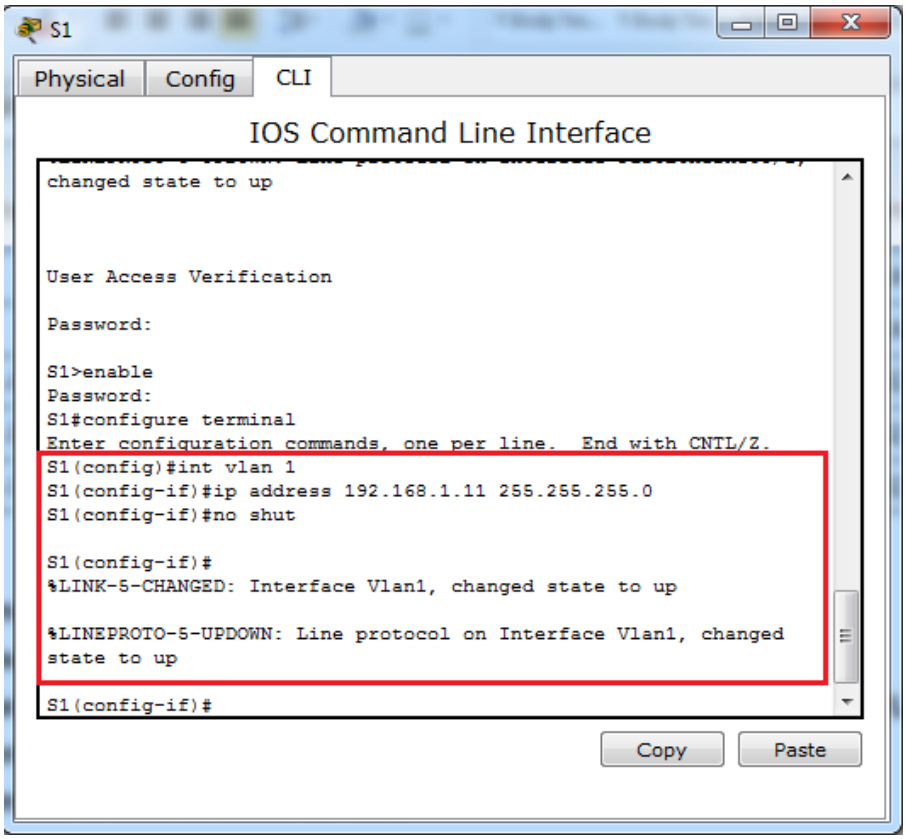
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

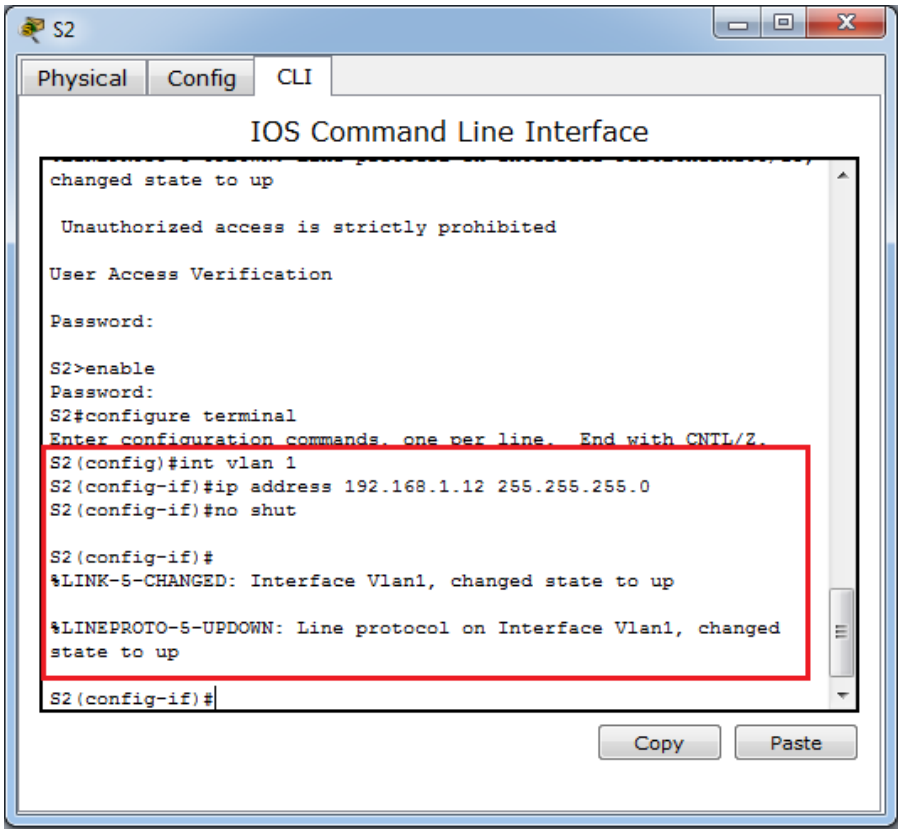




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

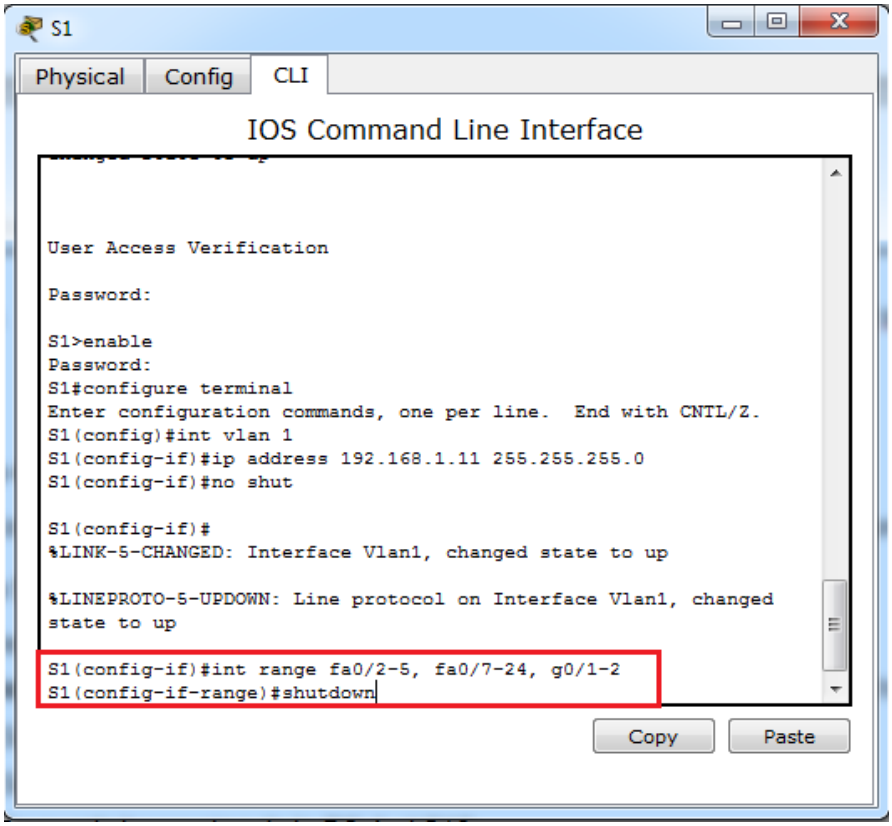
g. Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.

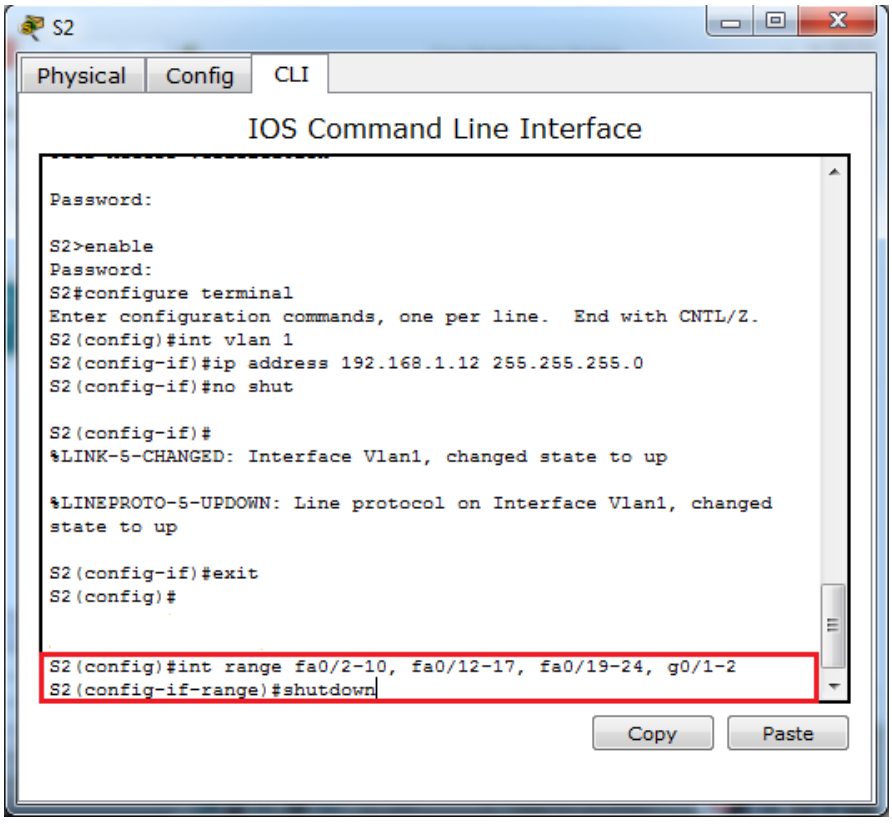




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

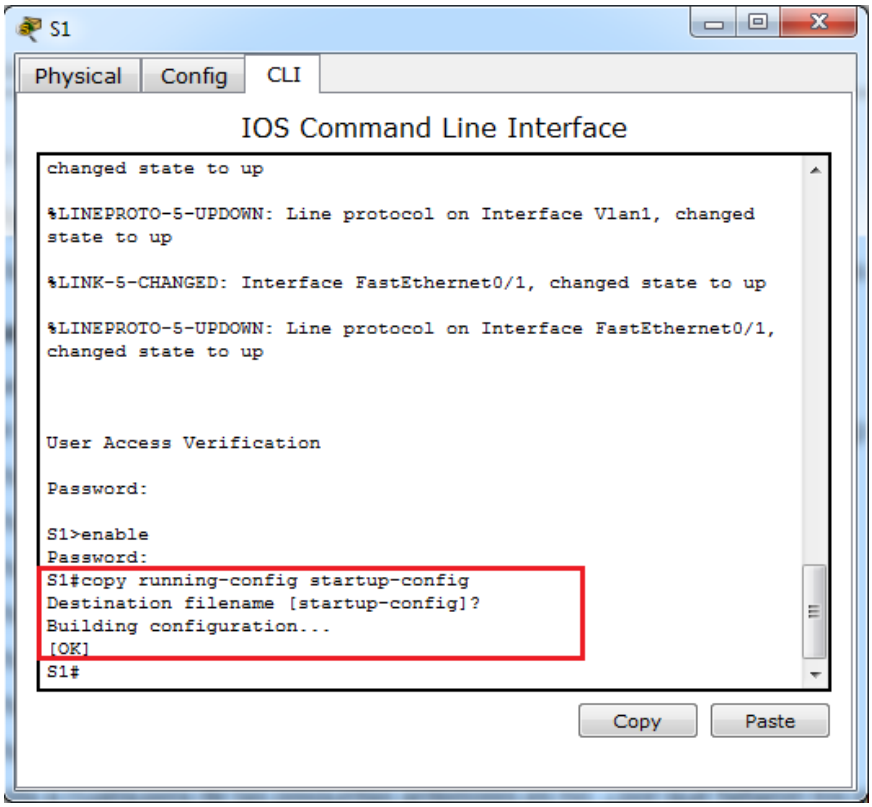
h. Desactive administrativamente todos los puertos que no se usen en el switch.

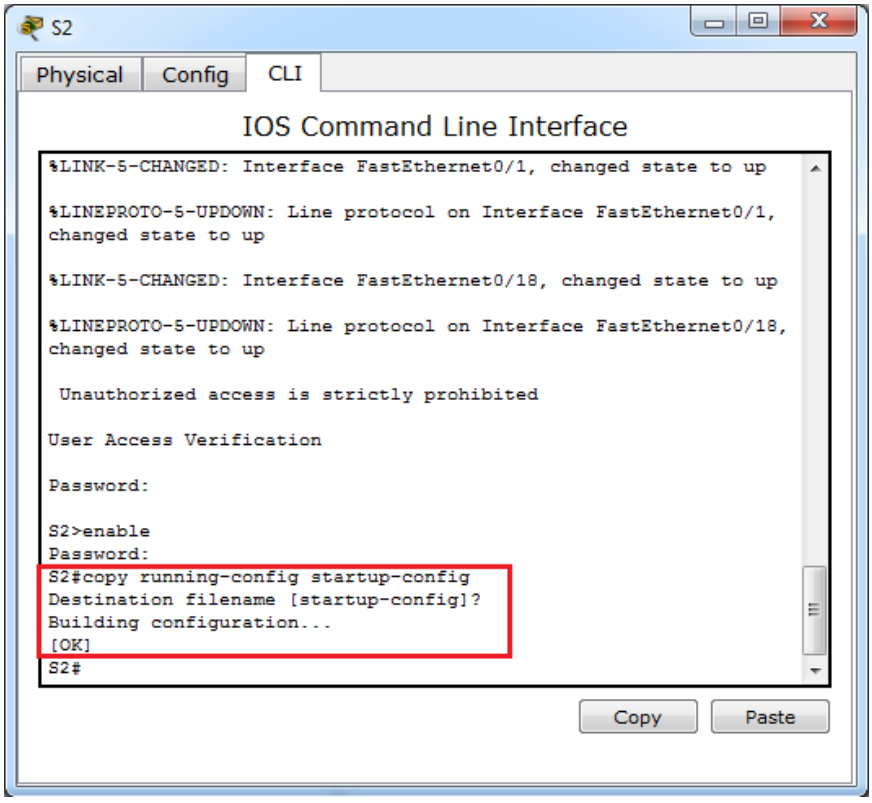




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

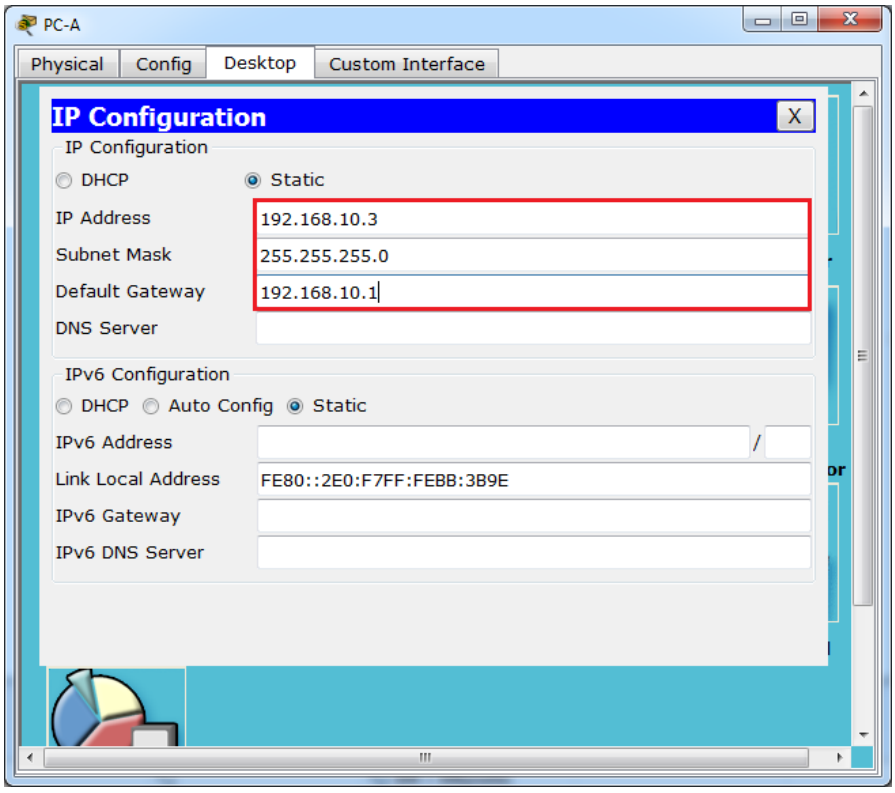


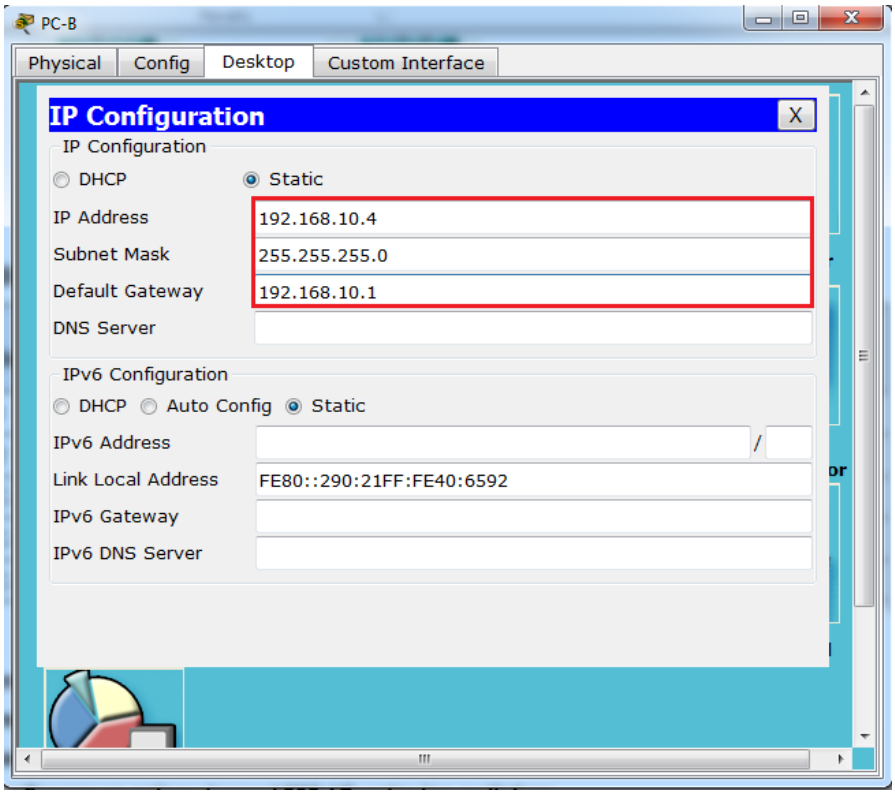


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

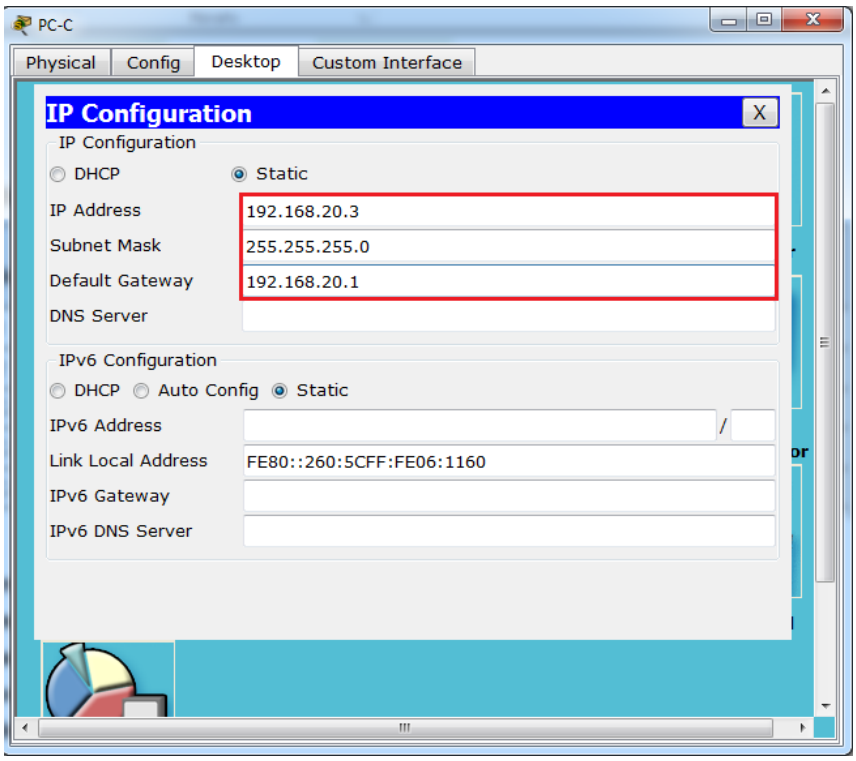
Paso 4. Configurar los equipos host.

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





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

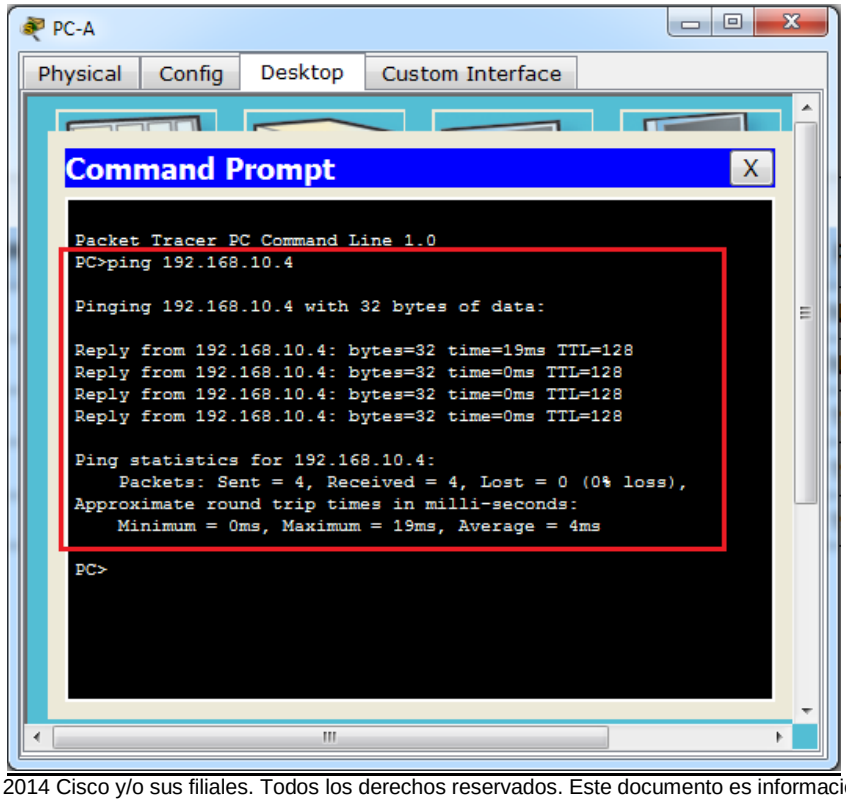


Paso 5. Probar la conectividad.

Verifique que los equipos host puedan hacer ping entre sí.

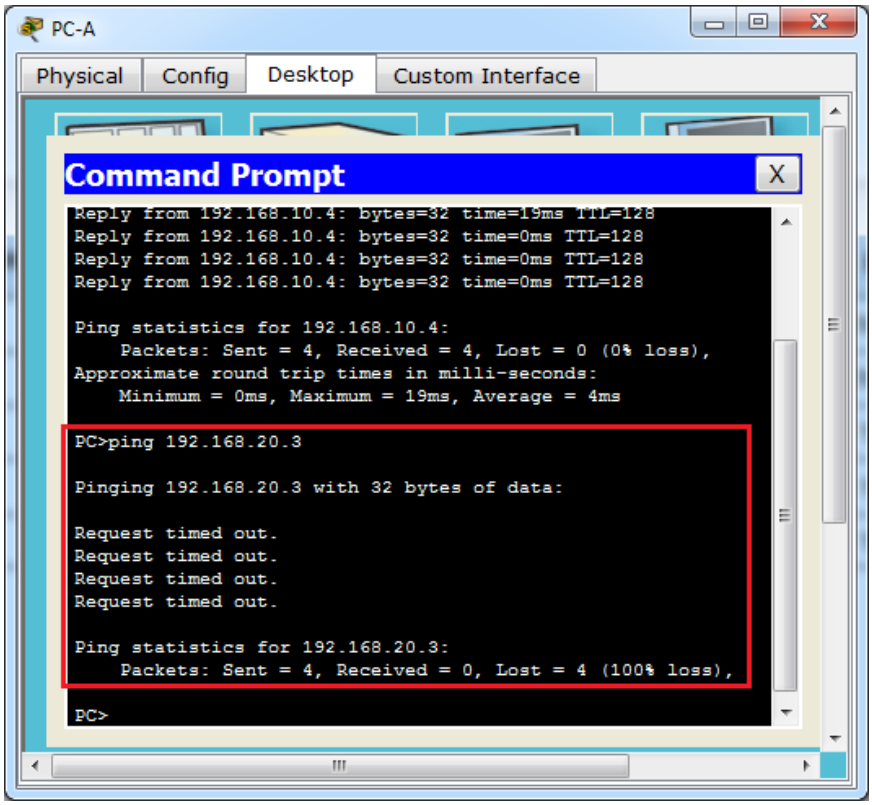
Nota: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

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

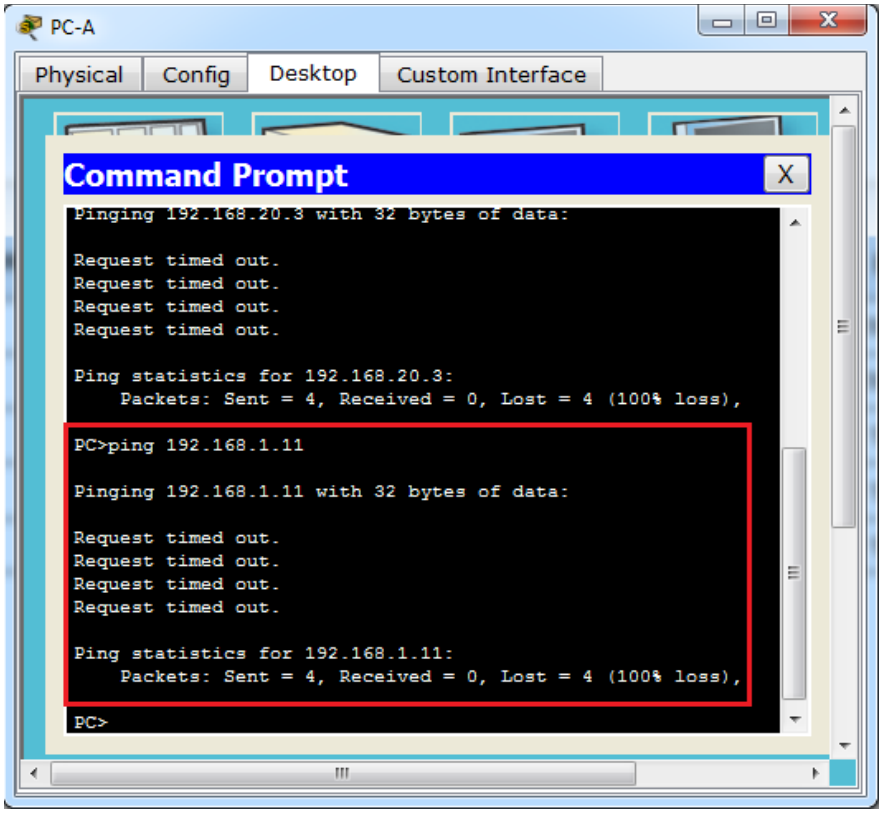


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

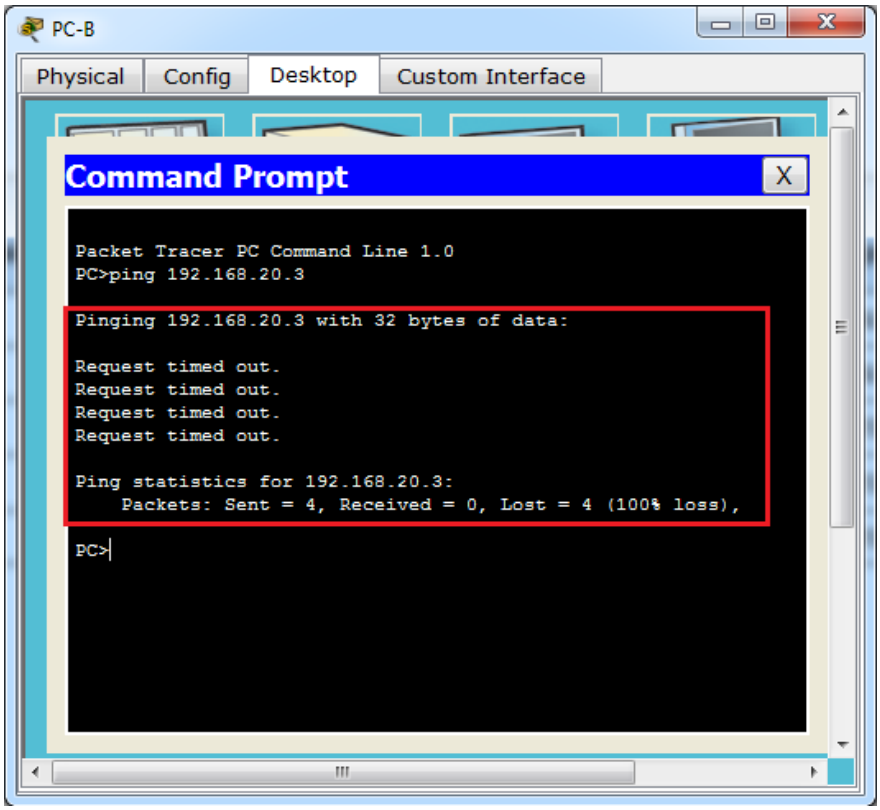


¿Se puede hacer ping de la PC-A al S1? No

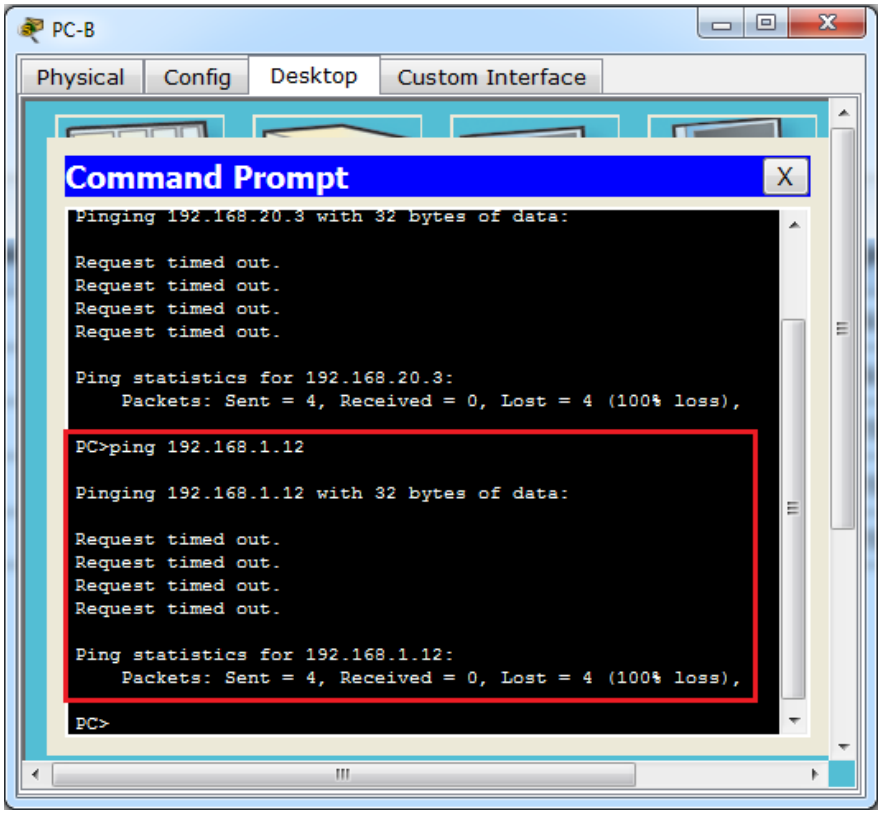


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

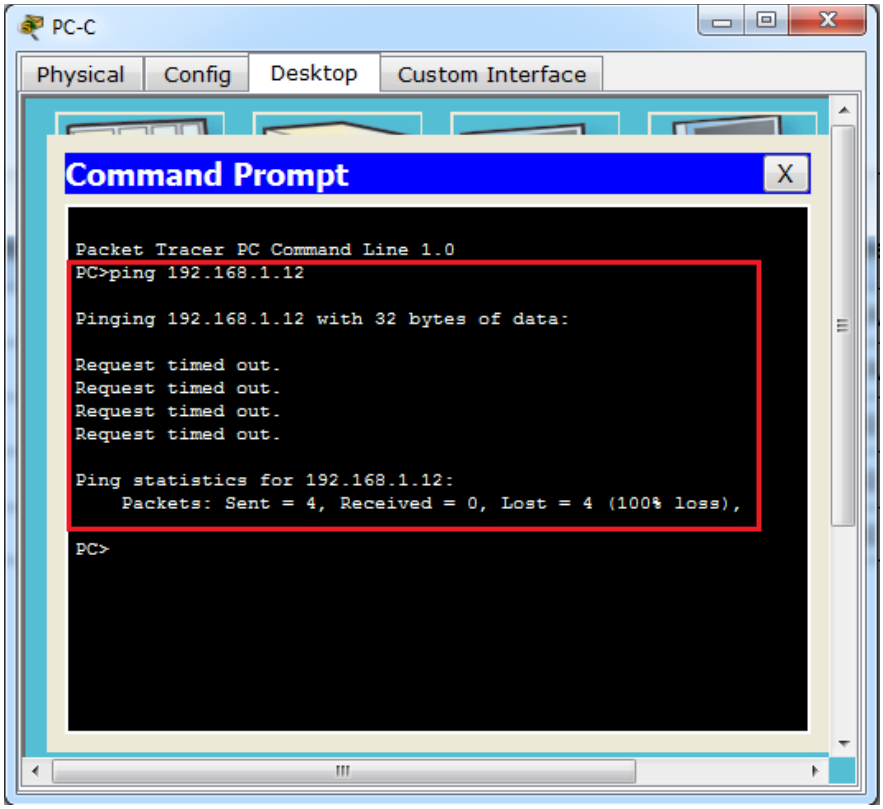


¿Se puede hacer ping de la PC-B al S2? No

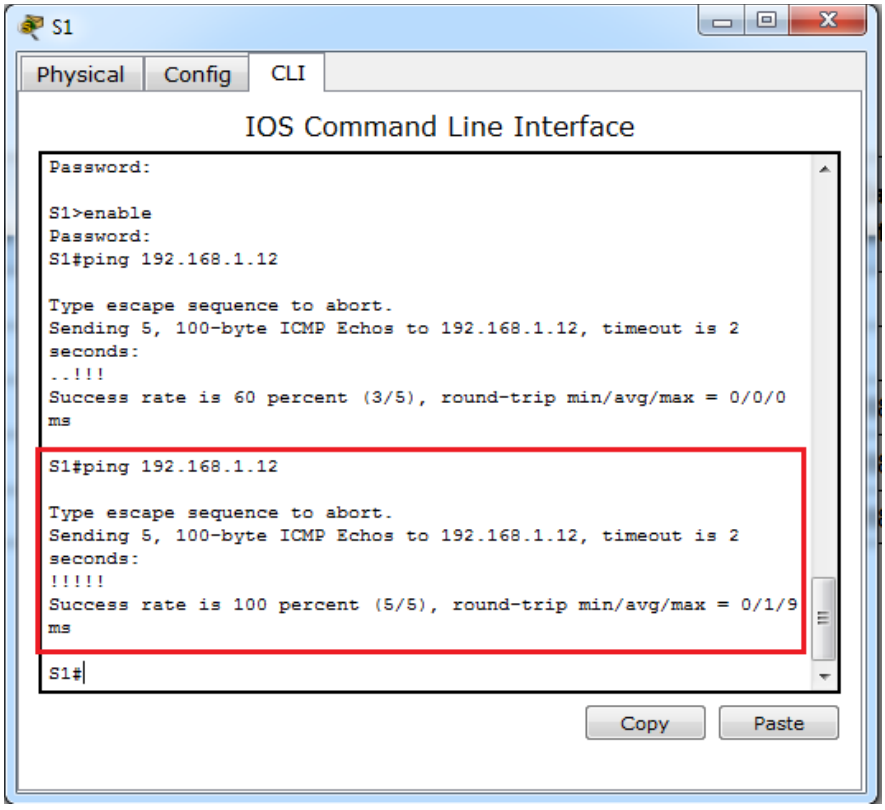


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



¿Se puede hacer ping del S1 al S2? Si



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

Los Pings no tuvieron éxito al intentar hacer ping a un dispositivo en una subred diferente. Para que estos pings tengan éxito, debe existir una puerta de enlace predeterminada para en rutar el tráfico de una subred a otra.

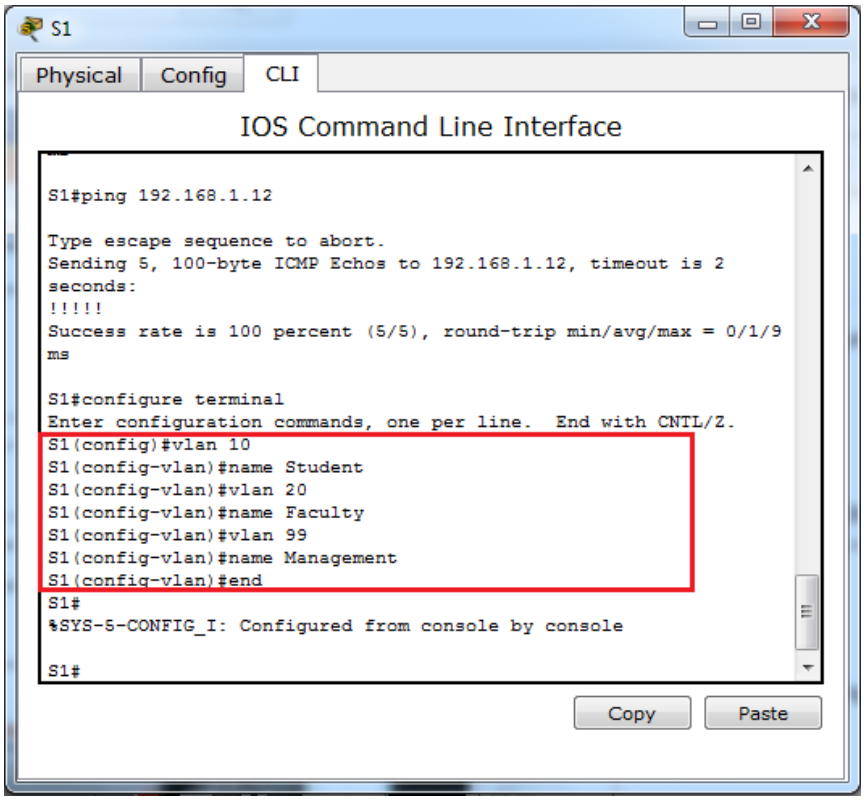
Parte 2. Crear redes VLAN y asignar puertos de switch

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

Paso 1. crear las VLAN en los switches.

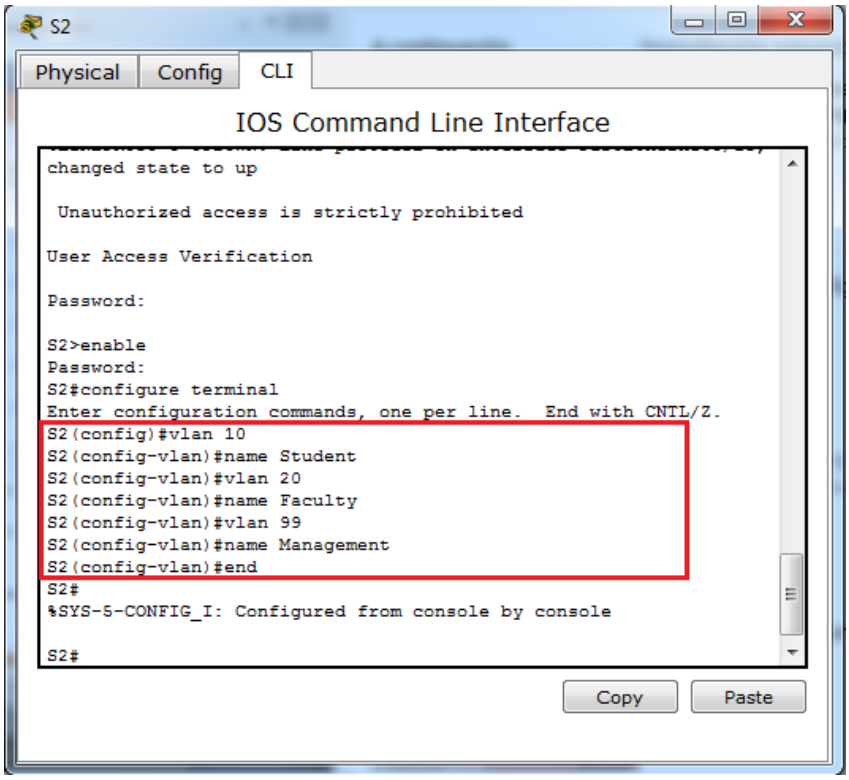
a. Cree las VLAN en S1.

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

b. Cree las mismas VLAN en el S2.

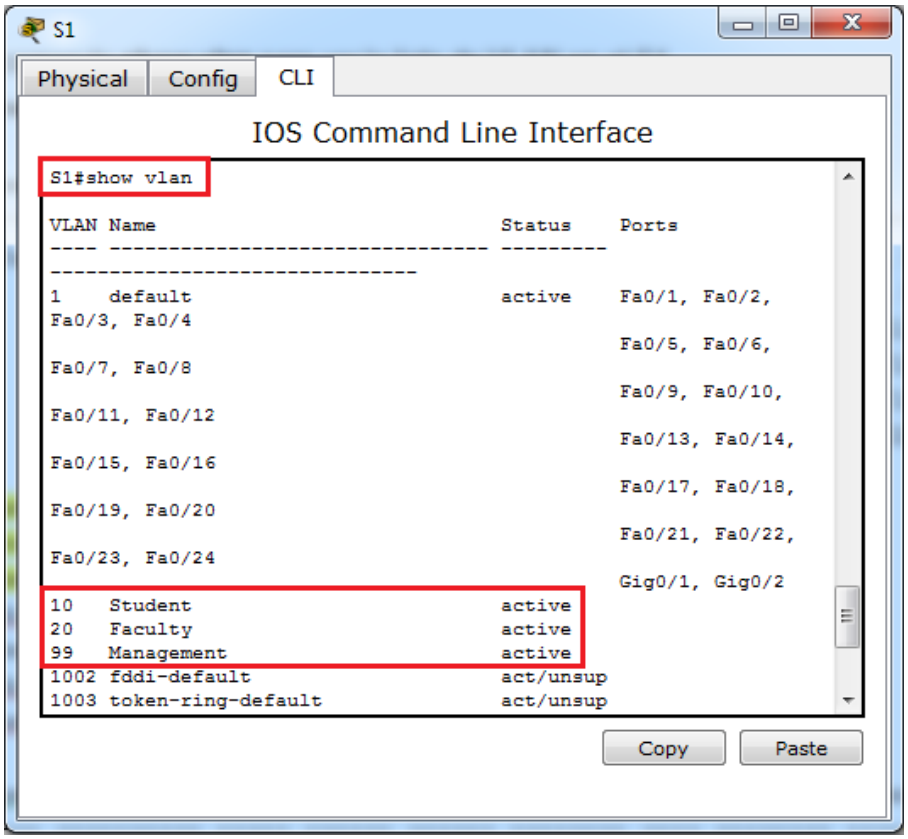


c. Emita el comando **show vlan** para ver la lista de VLAN en el S1.

```
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
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
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? VLAN 1

¿Qué puertos se asignan a la VLAN predeterminada?

Todos los puertos del switch están asignados a la VLAN 1 de forma predeterminada.

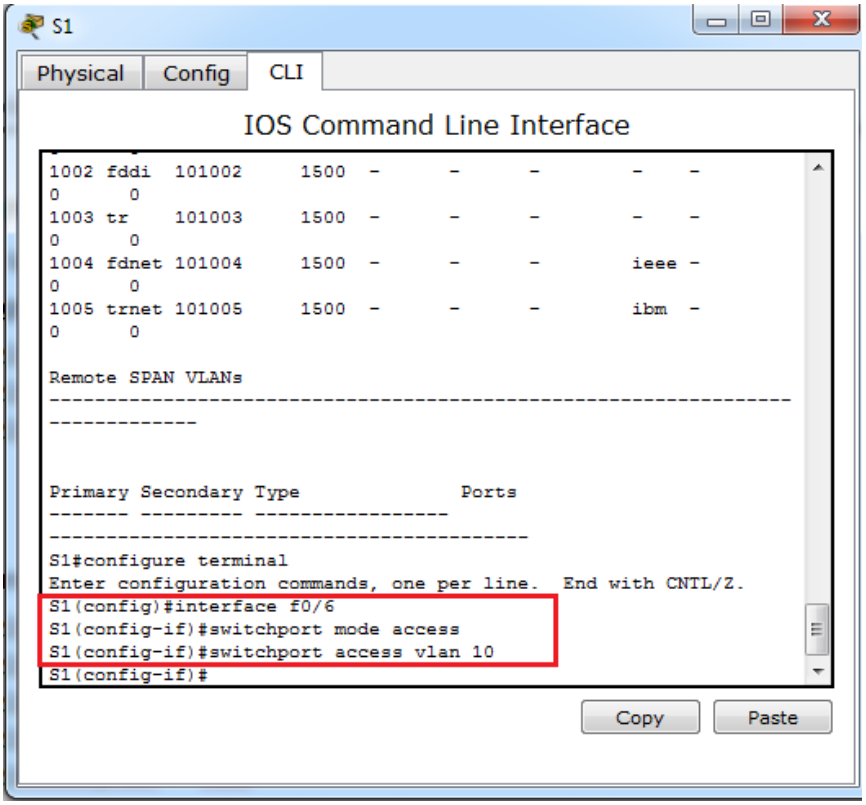
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

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

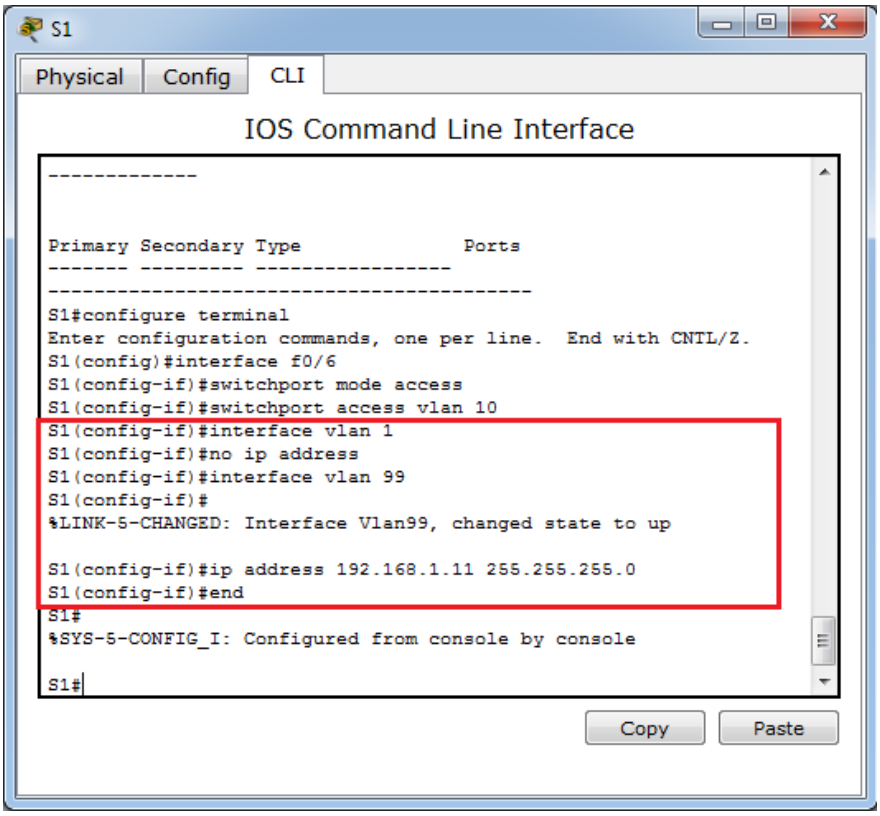
```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```



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

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

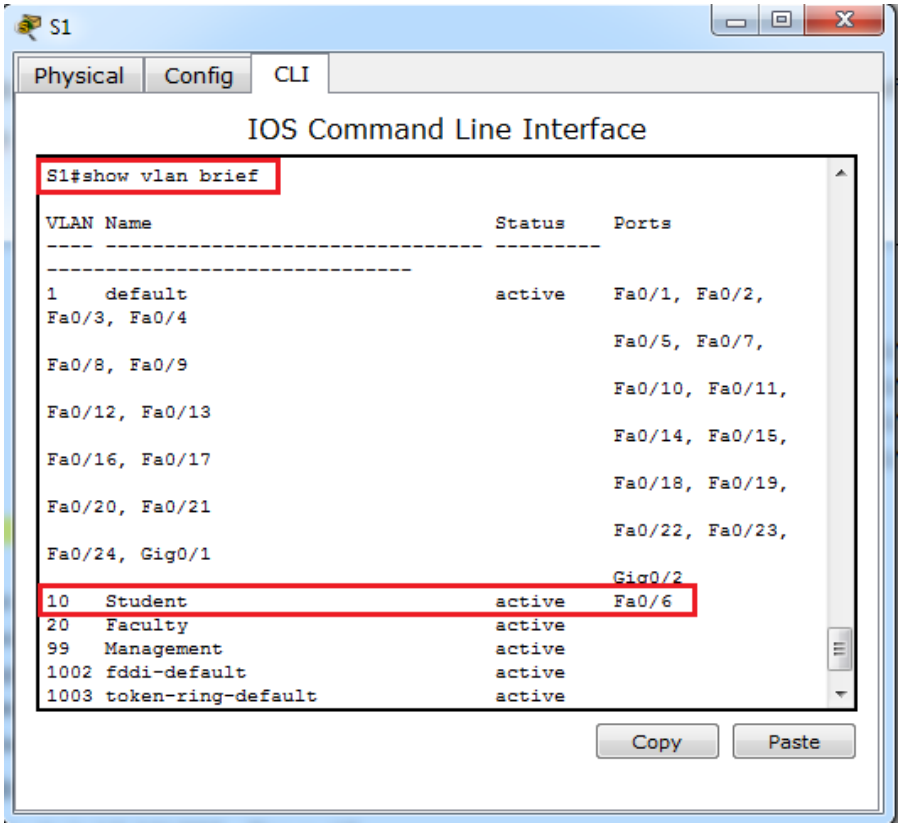
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



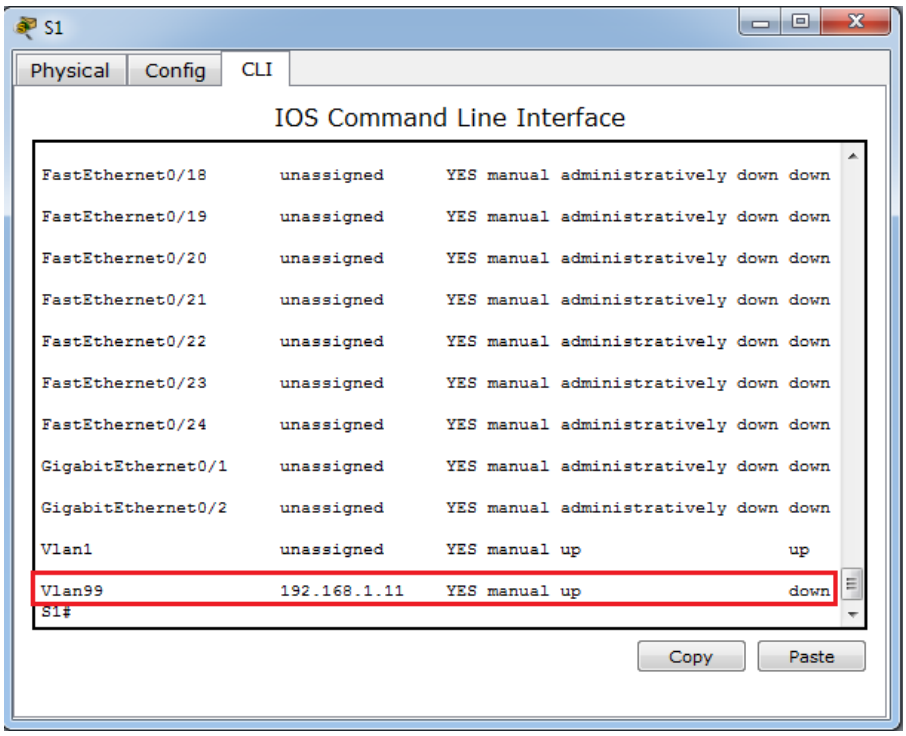
b. Emita el comando **show vlan brief** y verifique que las VLAN se hayan asignado a las interfaces correctas.

```
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
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



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

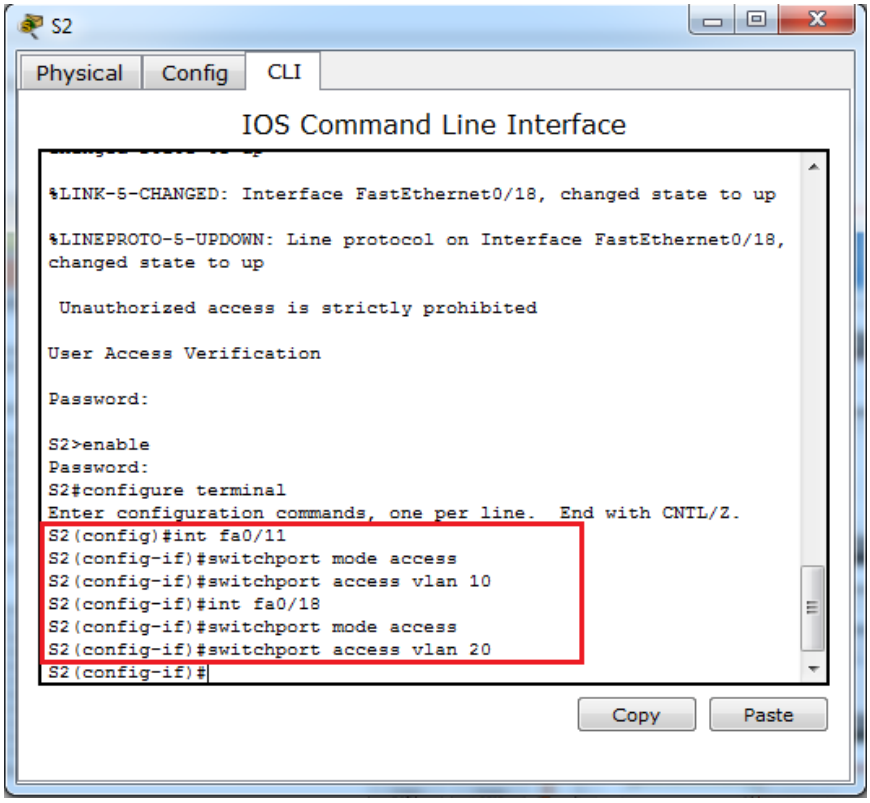


¿Cuál es el estado de la VLAN 99? ¿Por qué?

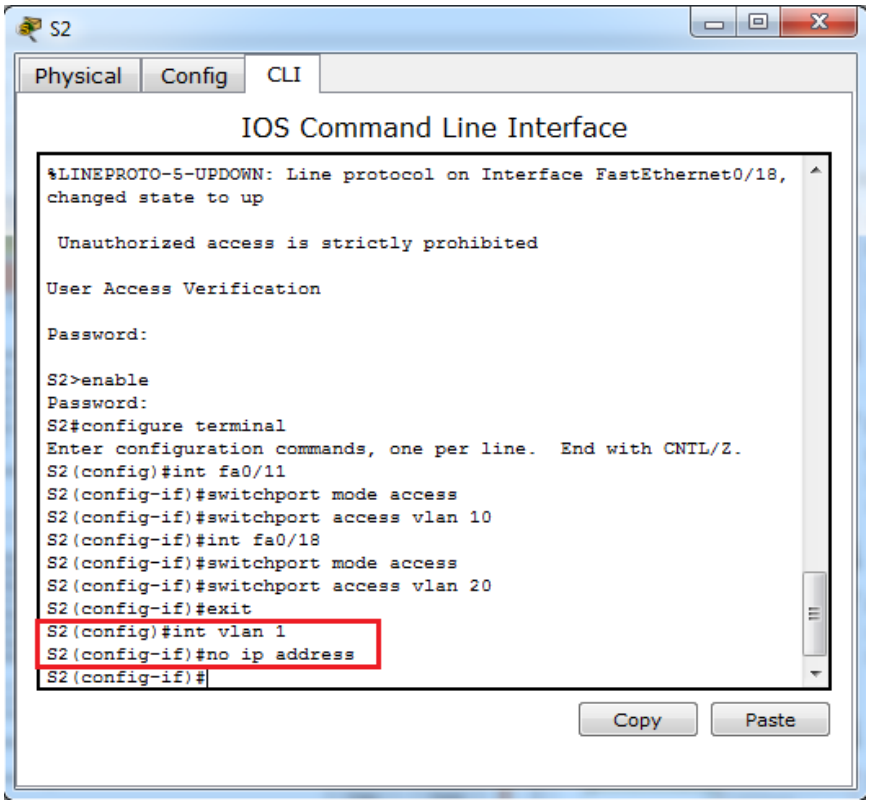
El estado de la VLAN 99 es up/down, porque aún no se ha asignado a un puerto activo.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

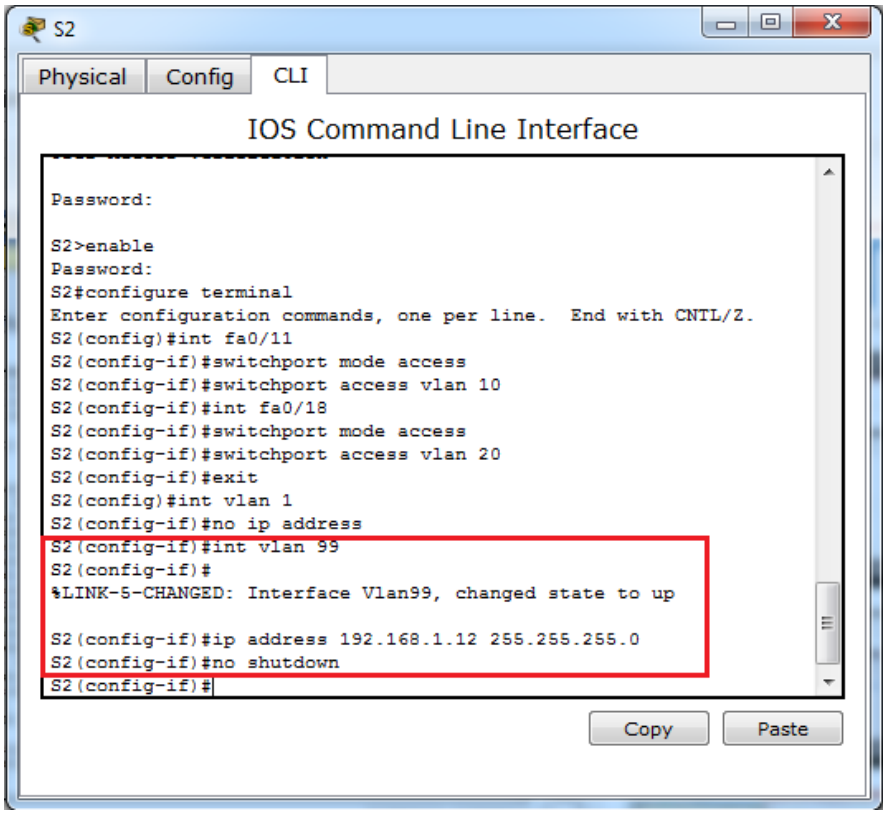


e. Elimine la dirección IP para la VLAN 1 en el S2.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

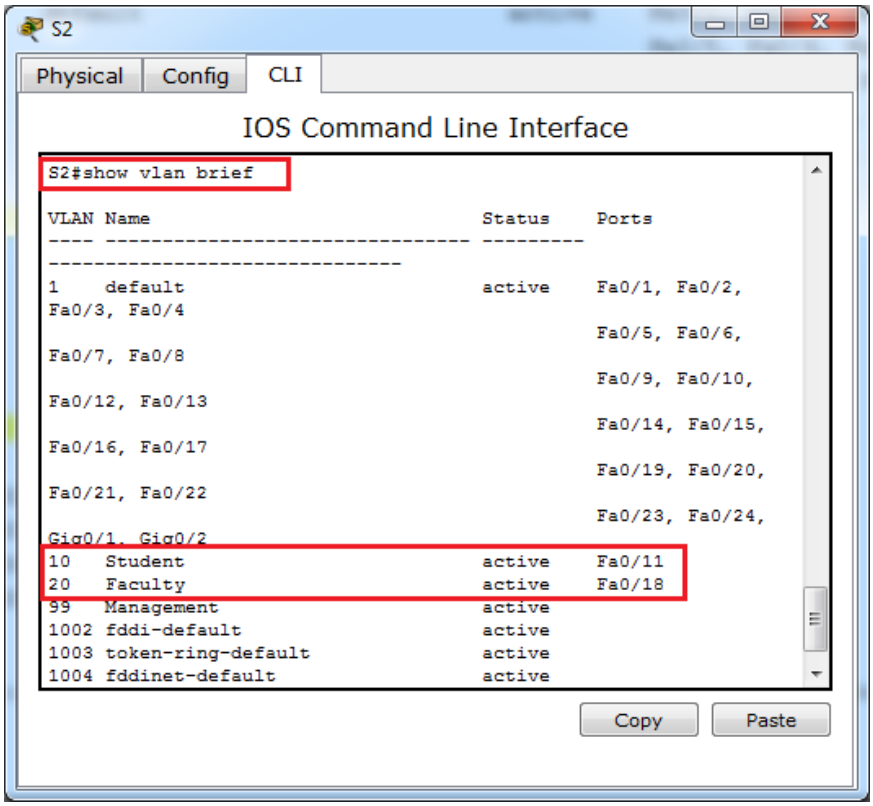
f. Configure una dirección IP para la VLAN 99 en el S2 según la tabla de direccionamiento.



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

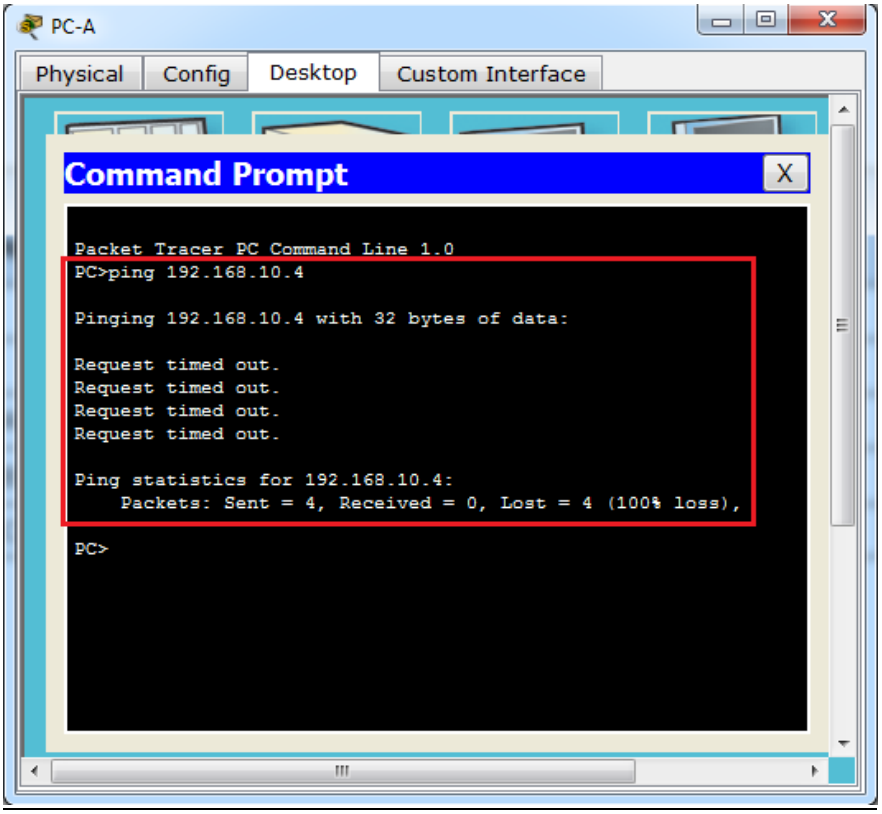
```
S2# show vlan brief

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
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



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

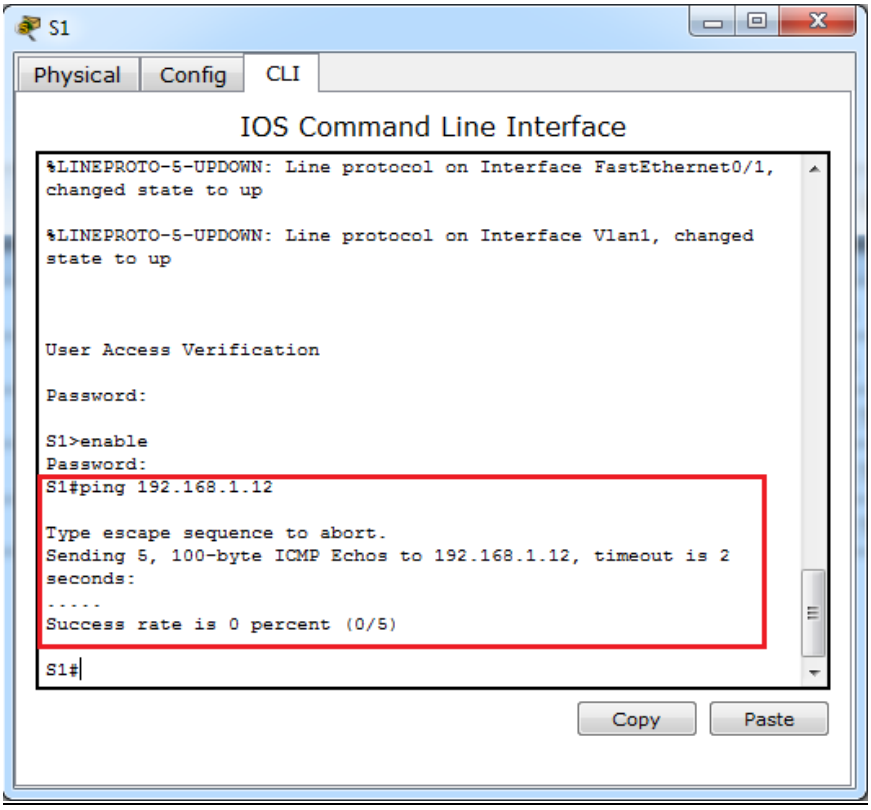
No. La interfaz F0/1 no está asignada a la VLAN 10, por lo que el tráfico de la VLAN 10 no se enviará a través de ella.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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



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

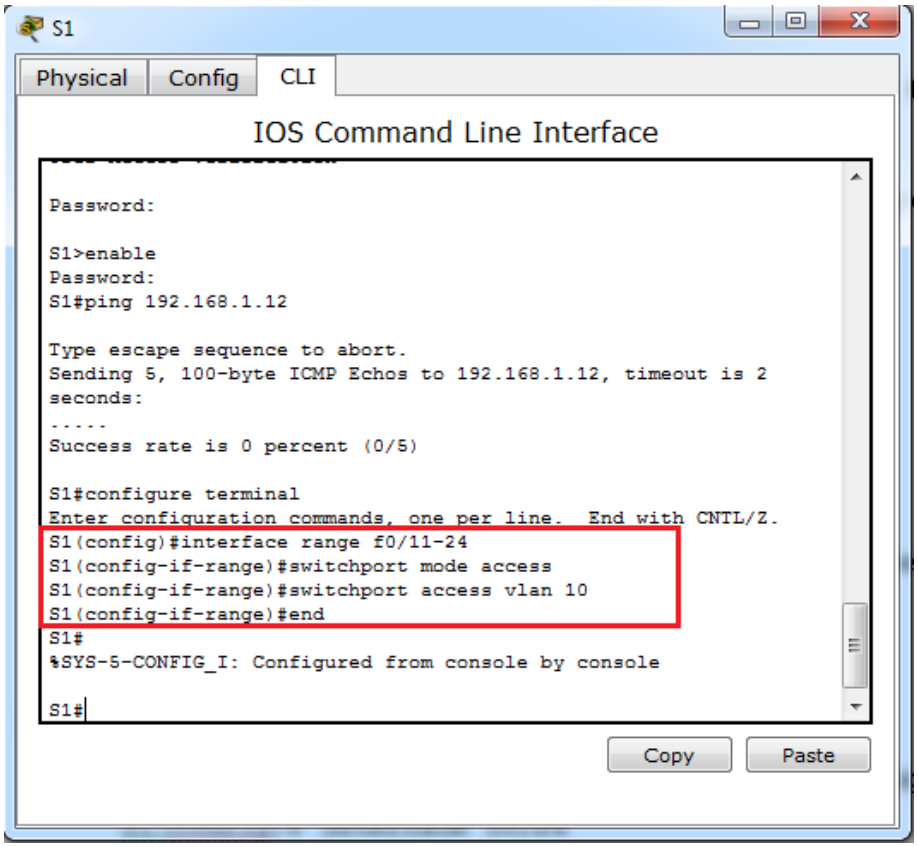
En la parte 3, cambiará las asignaciones de VLAN a los puertos y eliminará las VLAN de la base de datos de VLAN.

Paso 1. Asignar una VLAN a varias interfaces.

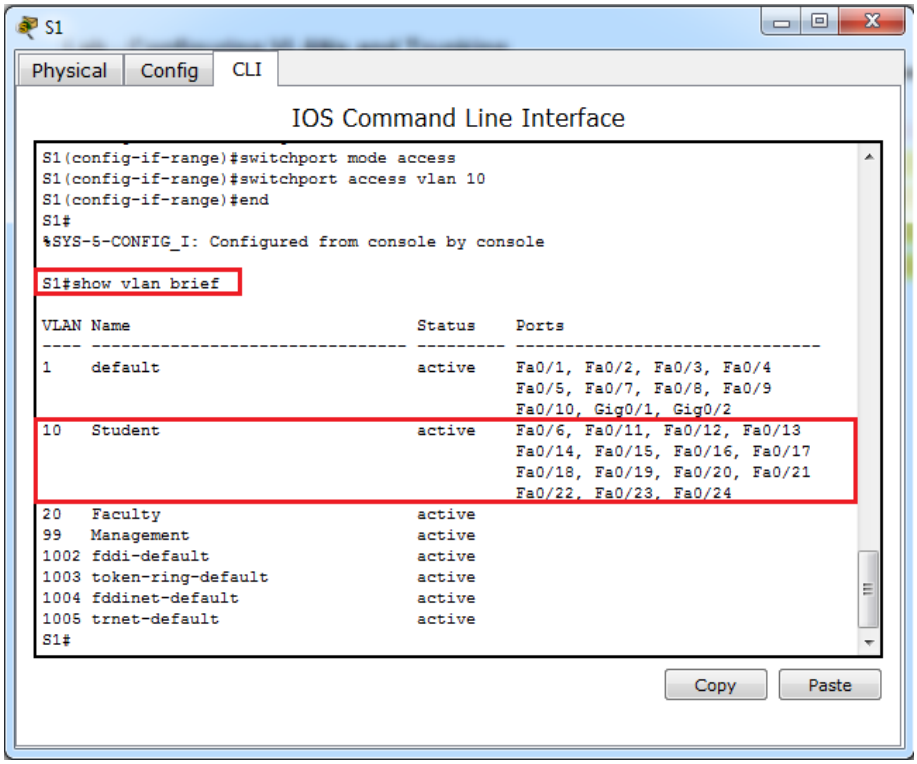
a. En el S1, asigne las interfaces F0/11 a 24 a la VLAN 10.

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

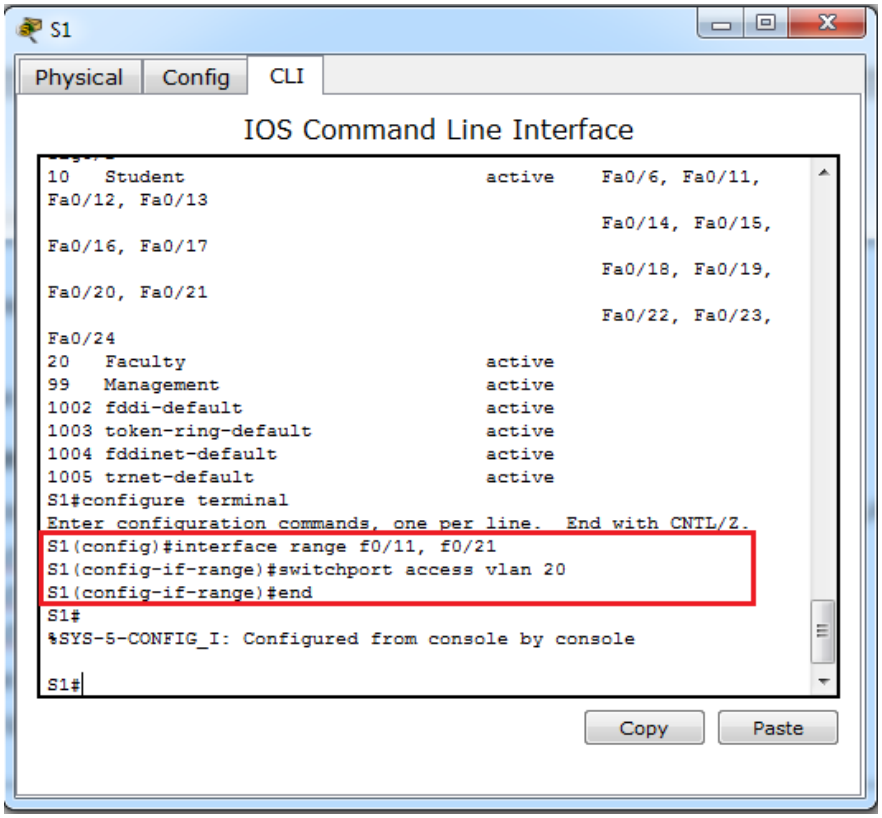


b. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN.

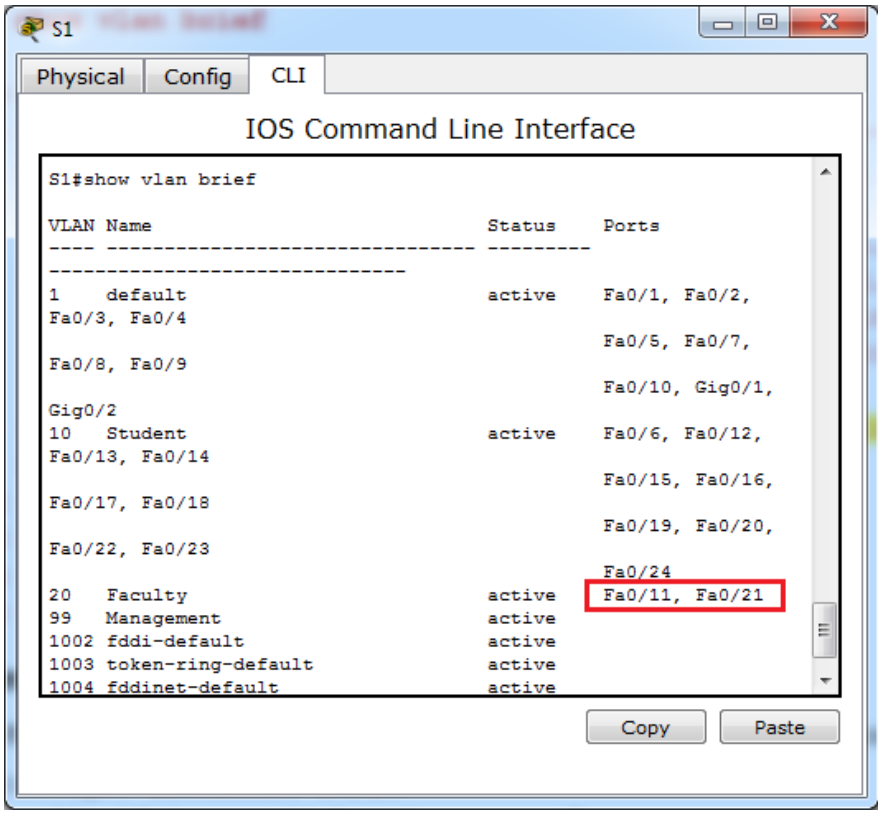


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



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

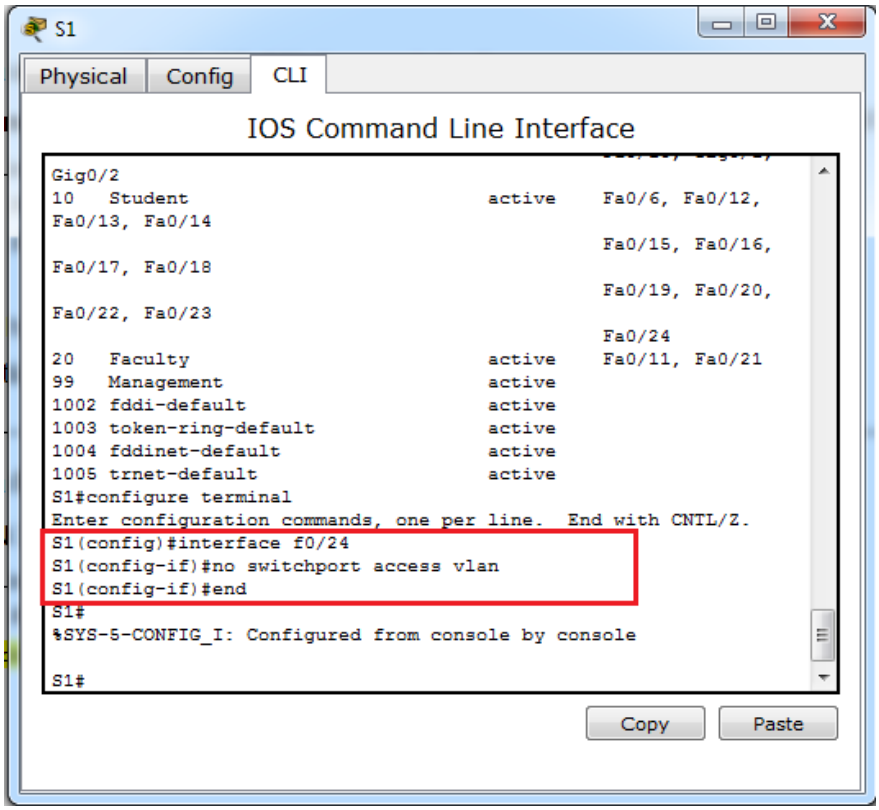


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

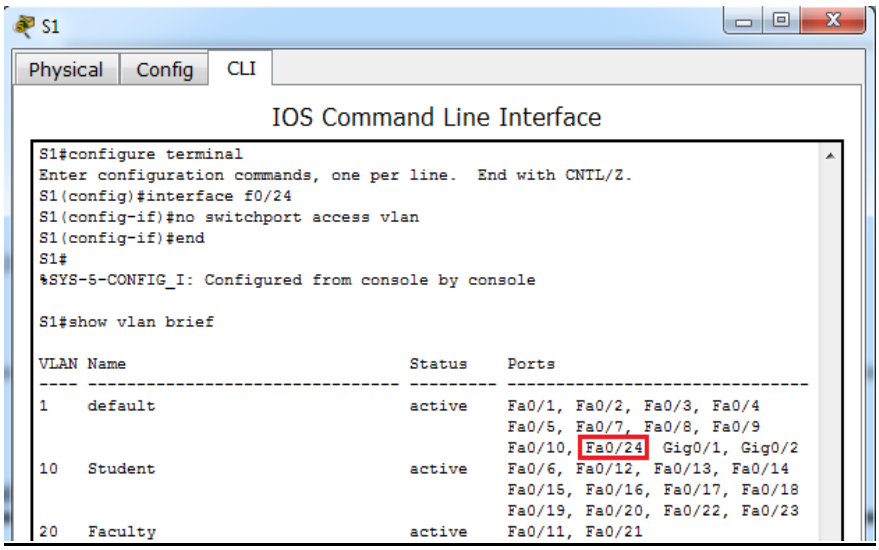
```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```



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

¿A qué VLAN está asociada ahora F0/24?

VLAN 1, la VLAN predeterminada.

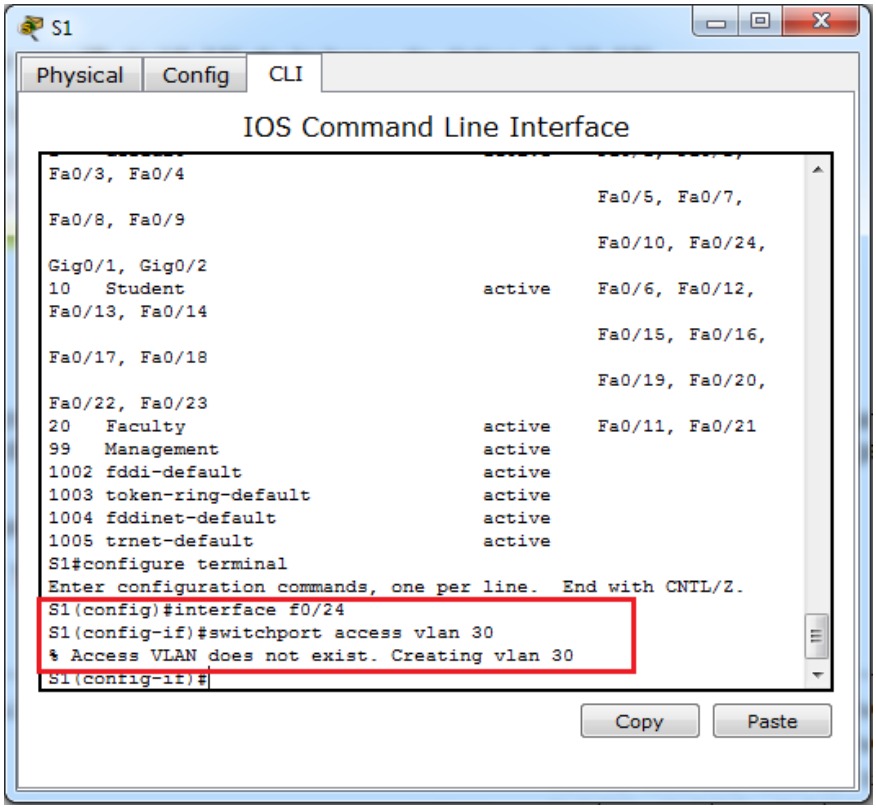


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

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

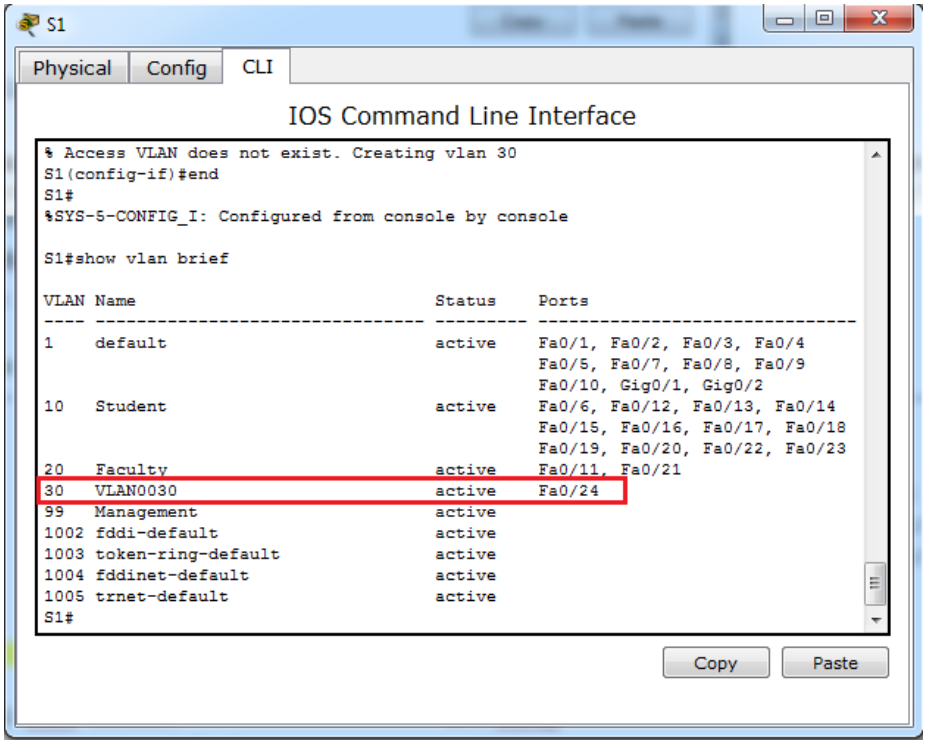


Nota: la tecnología de switches actual ya no requiere la emisión del comando **vlan** para agregar una VLAN a la base de datos. Al asignar una VLAN desconocida a un puerto, la VLAN se agrega a la base de datos de VLAN.

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

```
S1# show vlan brief
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
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

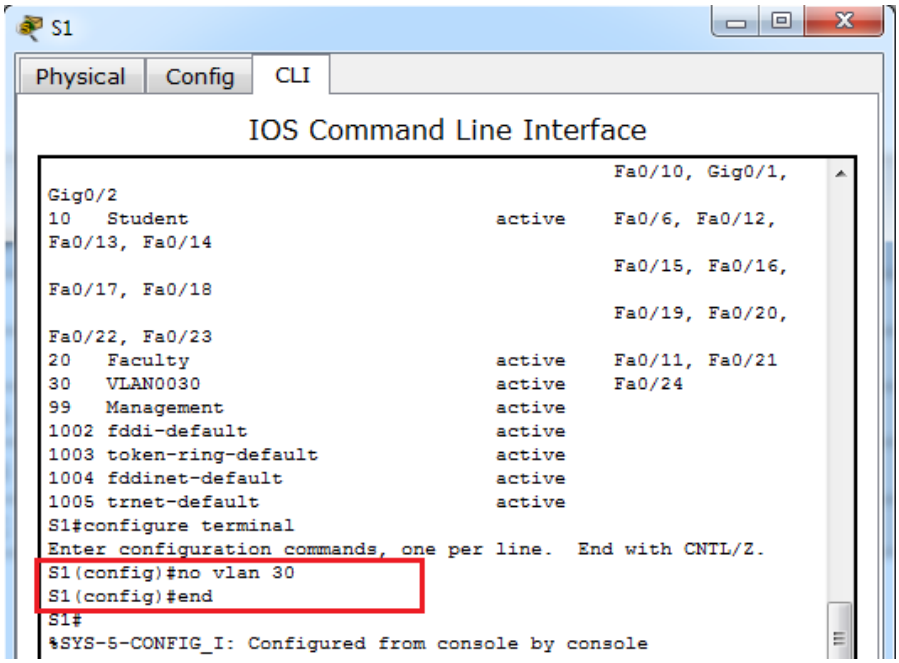


¿Cuál es el nombre predeterminado de la VLAN 30?

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
```



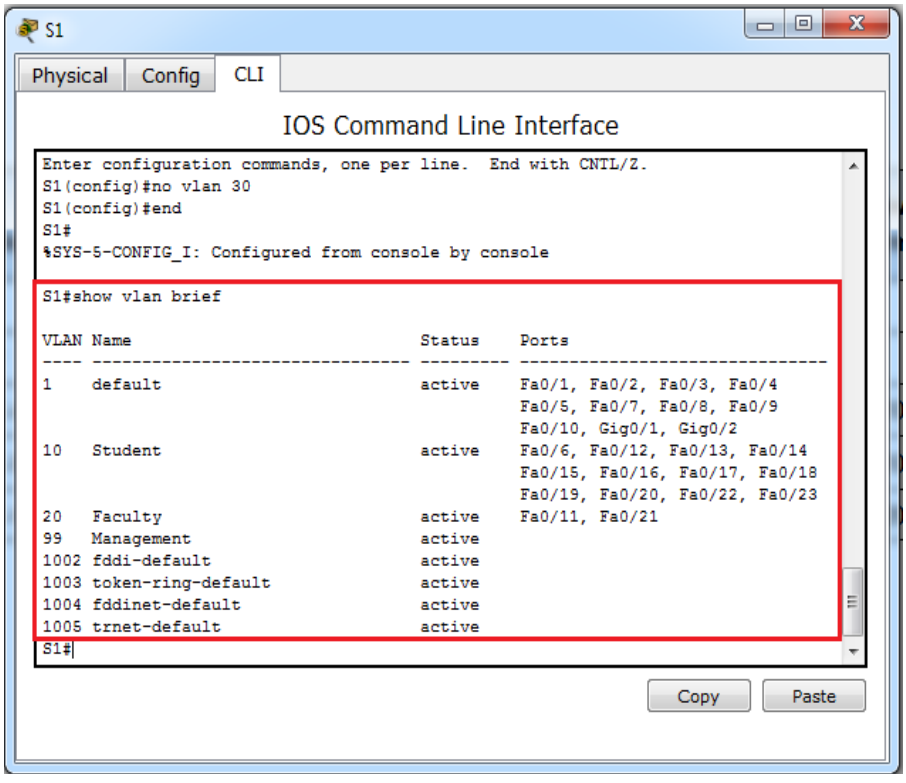
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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?

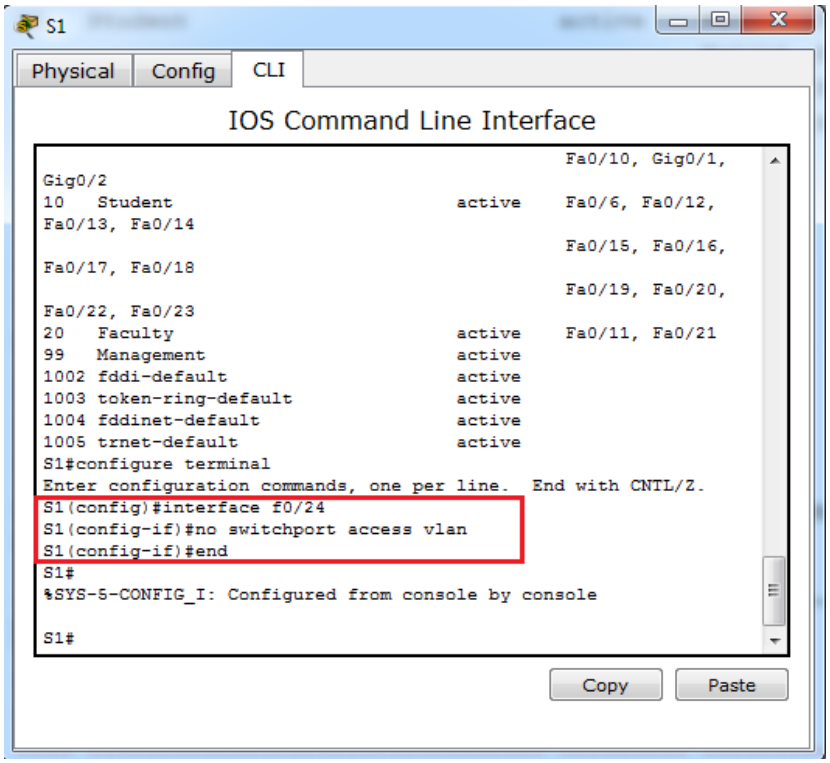
El puerto F0/24 no está asignado a ninguna VLAN. Este puerto no transferirá ningún tráfico.

```
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
```



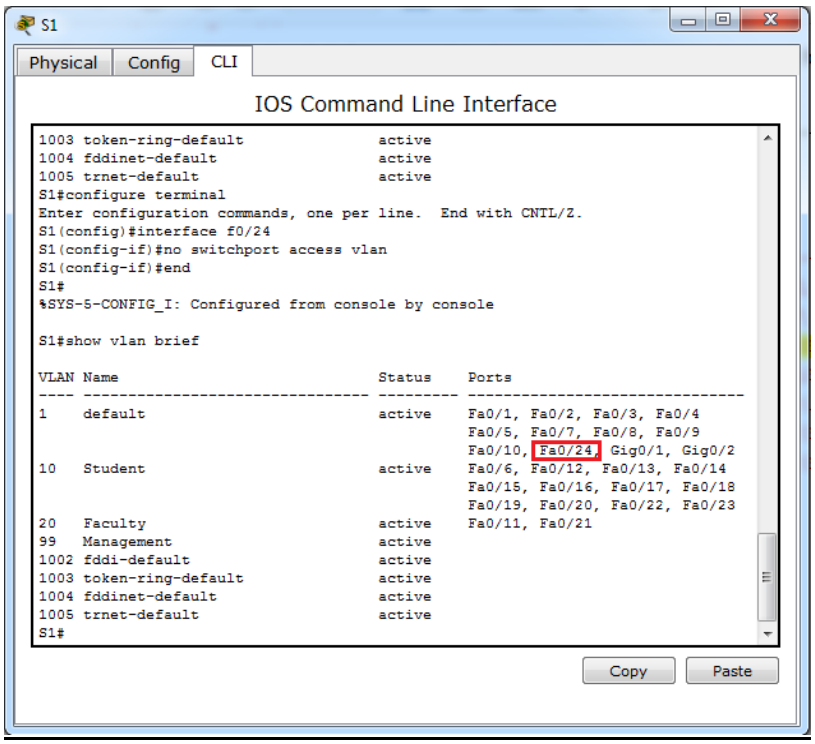
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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 elimina de la base de datos VLAN no están disponibles para su uso hasta que se reasigne a otra VLAN. Esto puede ser algo complicado para solucionar problemas, ya que las interfaces troncales no aparecen en la lista de puertos.

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

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

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

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

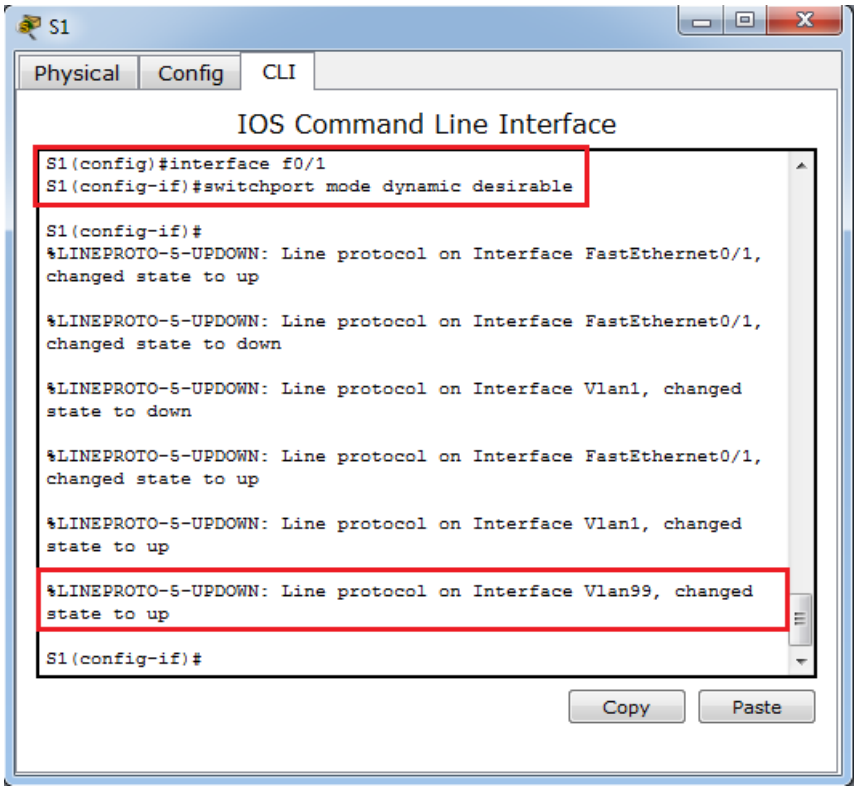
a. Establezca F0/1 en el S1 en modo de enlace troncal.

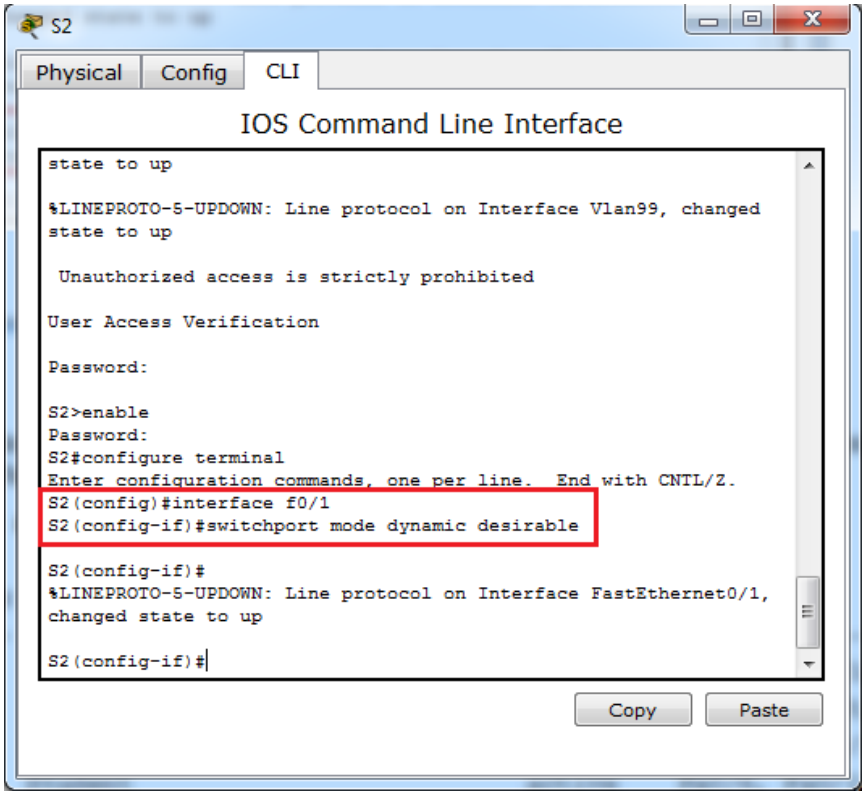
```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar  1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar  1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S1(config-if)#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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

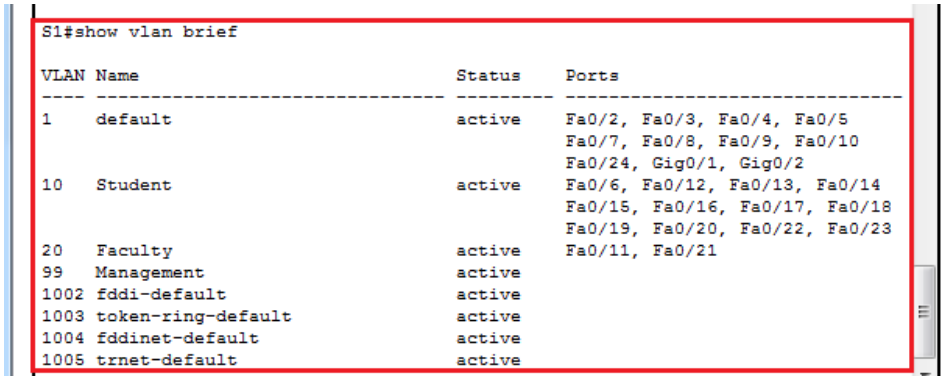




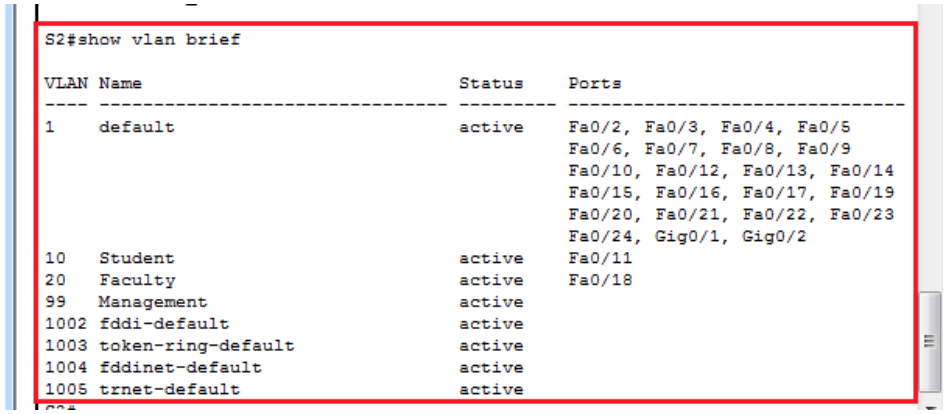
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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
```



```
S1#show vlan brief

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

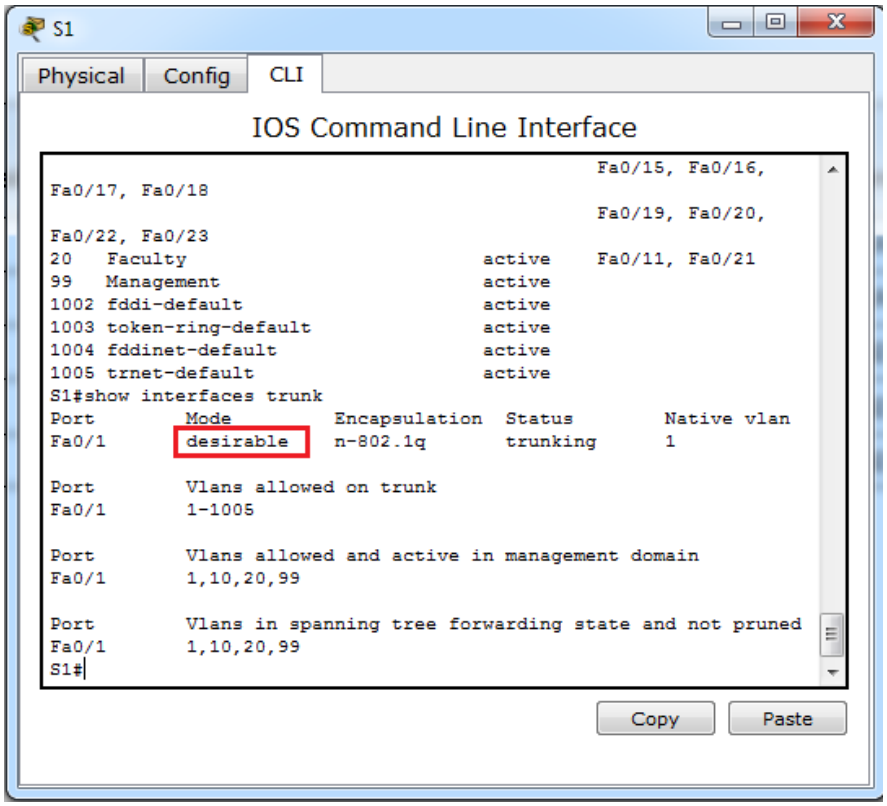


```
S2#show vlan brief

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

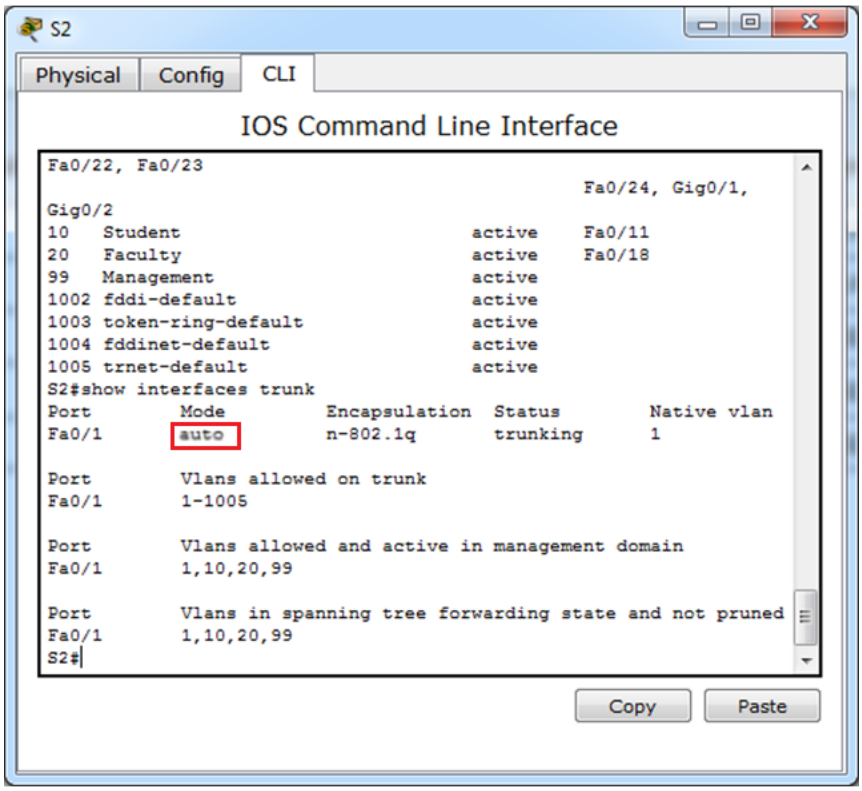
c. Emita el comando **show interfaces trunk** para ver las interfaces de enlace troncal. Observe que el modo en el S1 está establecido en deseado, y el modo en el S2 en automático.

```
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
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
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
```

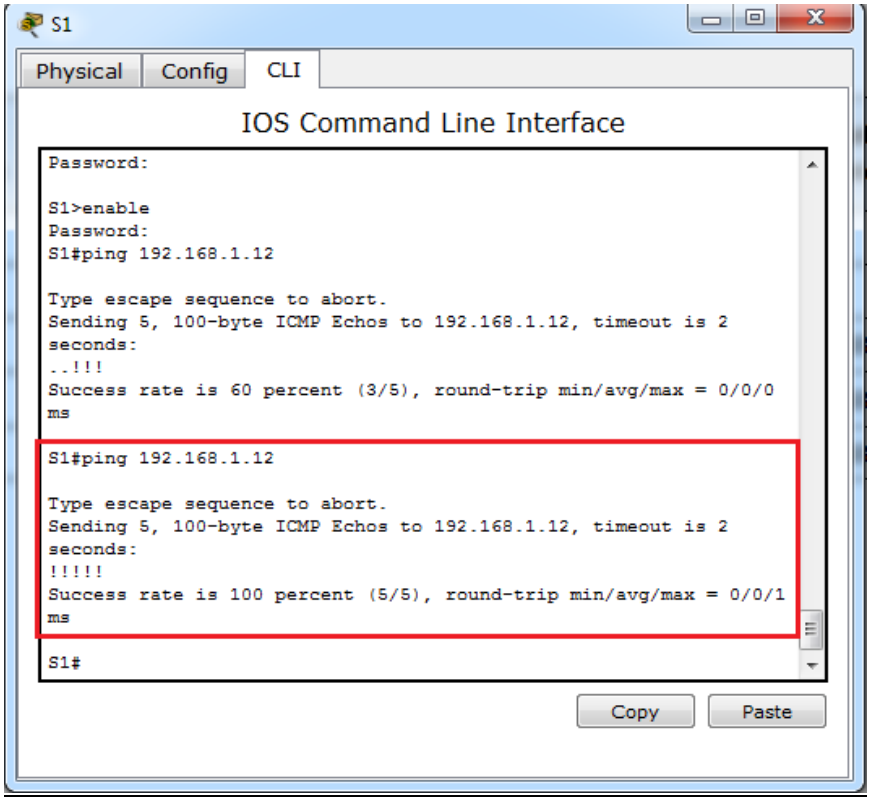


Nota: de manera predeterminada, todas las VLAN se permiten en un enlace troncal. El comando **switchport trunk** le permite controlar qué VLAN tienen acceso al enlace troncal. Para esta práctica de laboratorio, mantenga la configuración predeterminada que permite que todas las VLAN atraviesen F0/1.

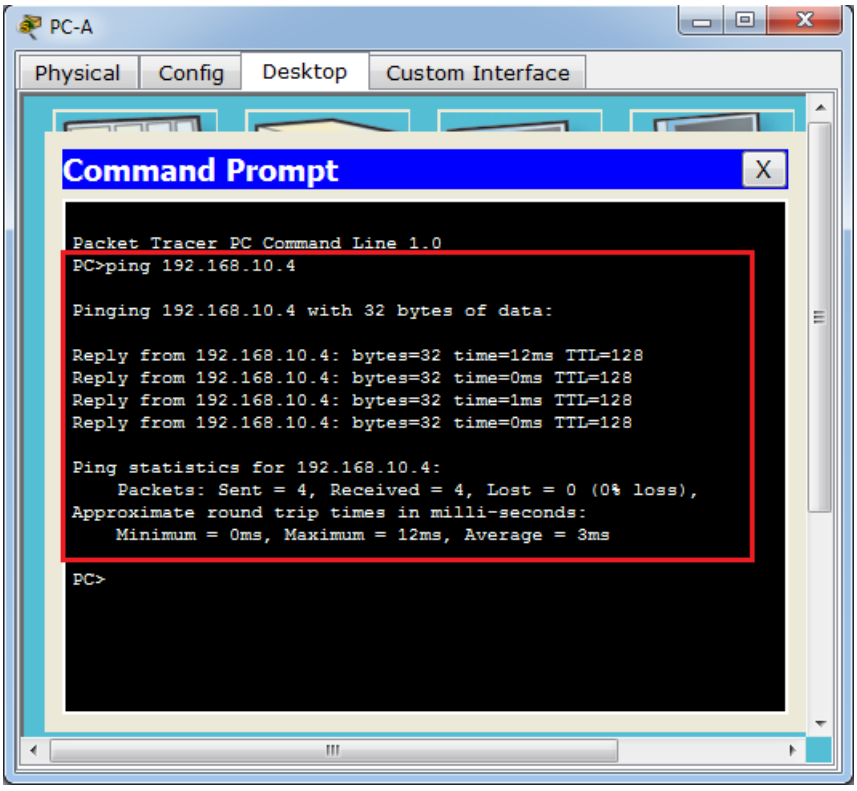
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

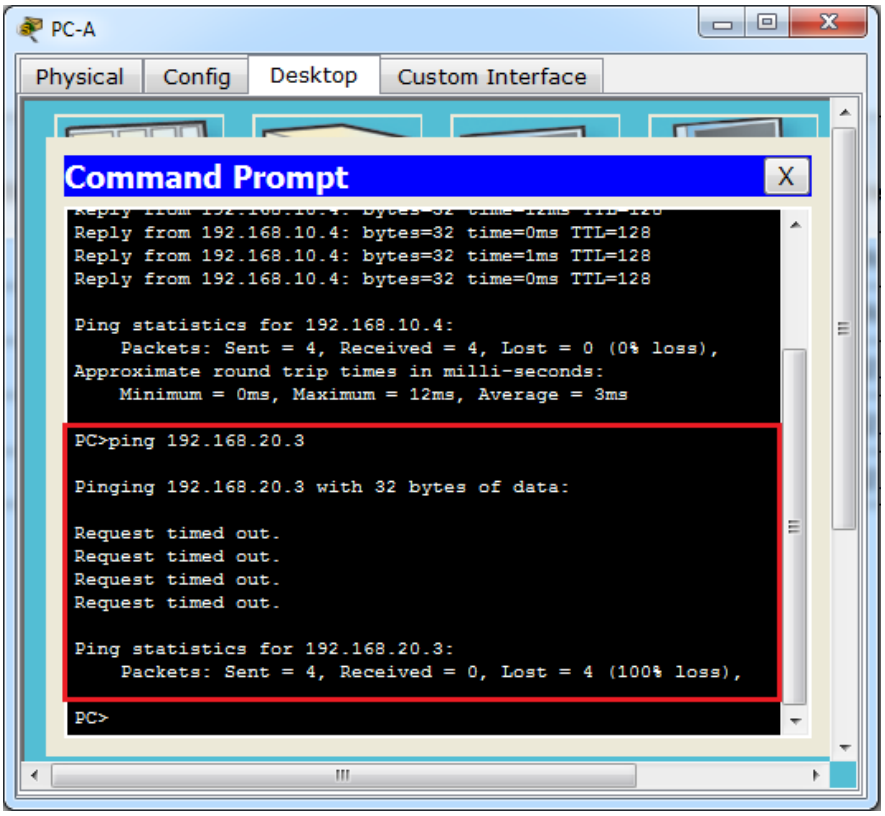


¿Se puede hacer ping de la PC-A a la PC-B? Si

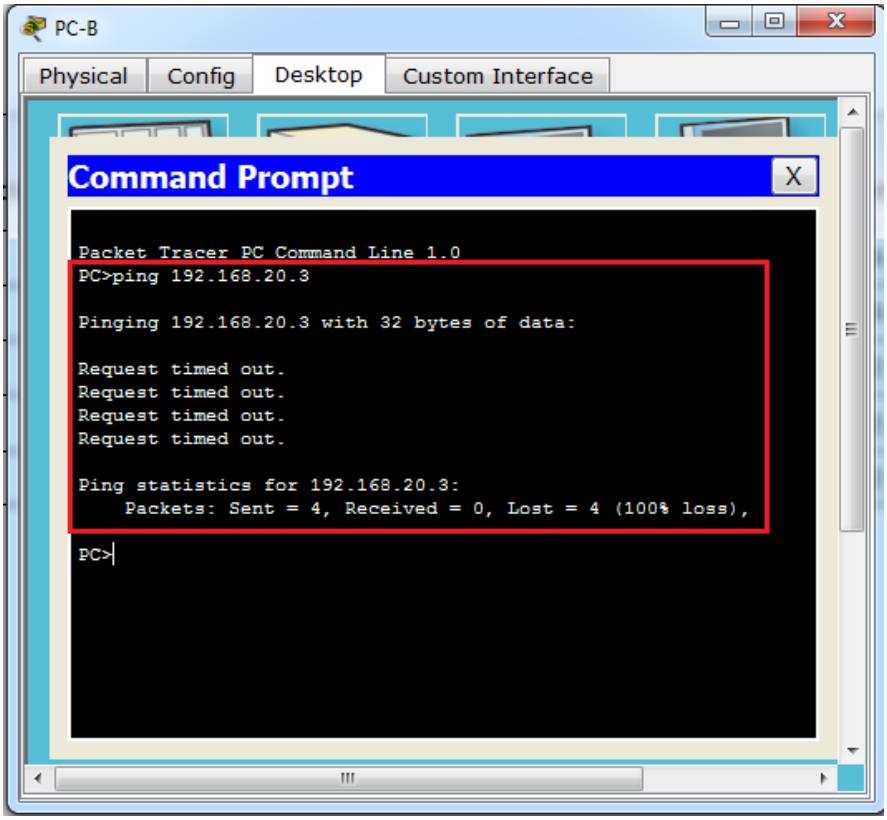


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

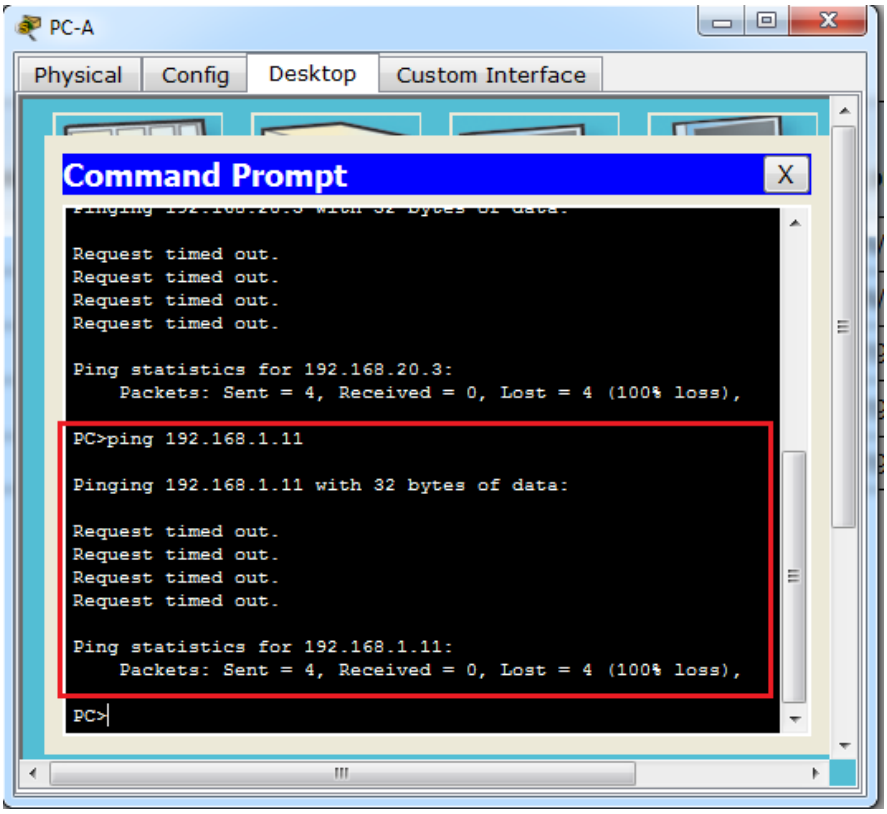


¿Se puede hacer ping de la PC-B a la PC-C? No

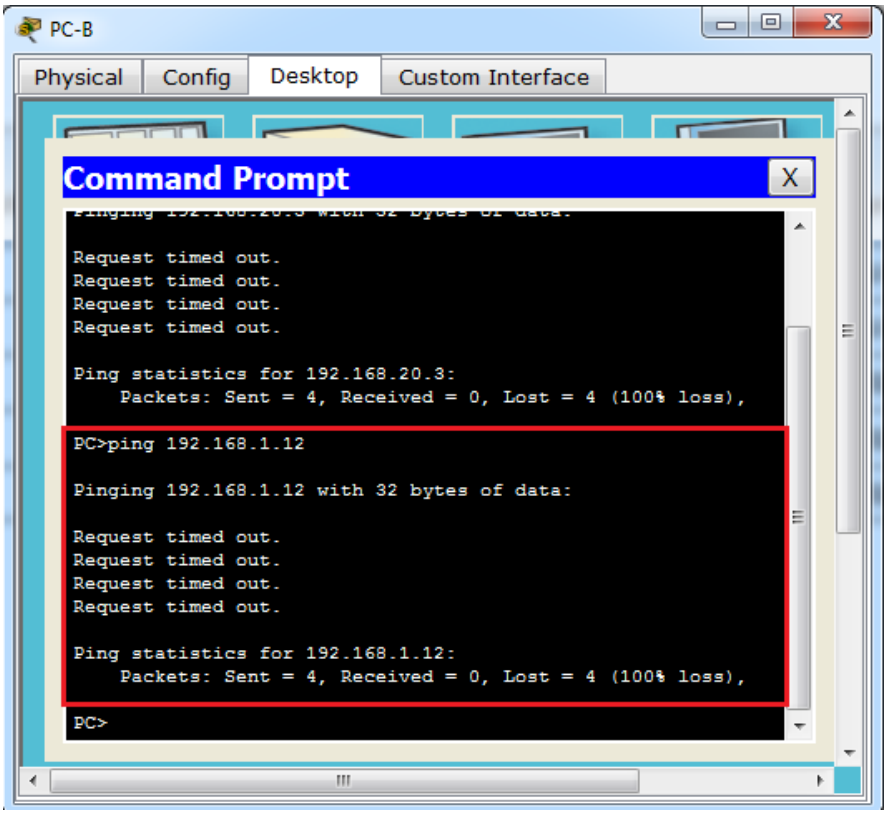


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

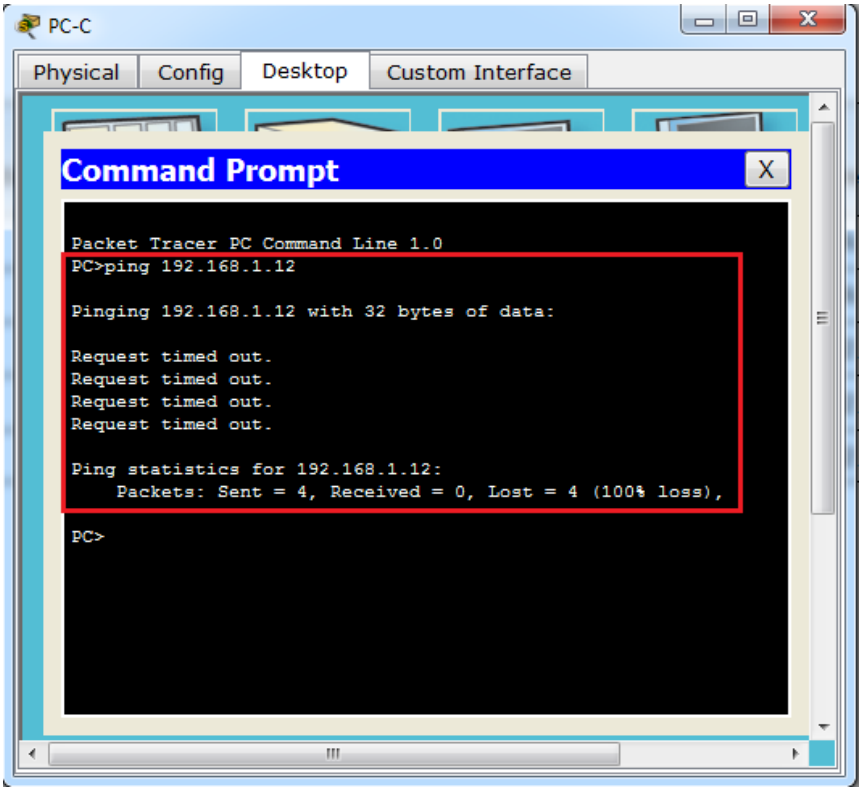


¿Se puede hacer ping de la PC-B al S2? No



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

¿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.

PC-C no puede hacer ping a PC-A y PC-B porque PC-C está en una VLAN diferente. Los switches están en diferentes VLAN que las PCs; Por lo tanto, los pings no tuvieron éxito.

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

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

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

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

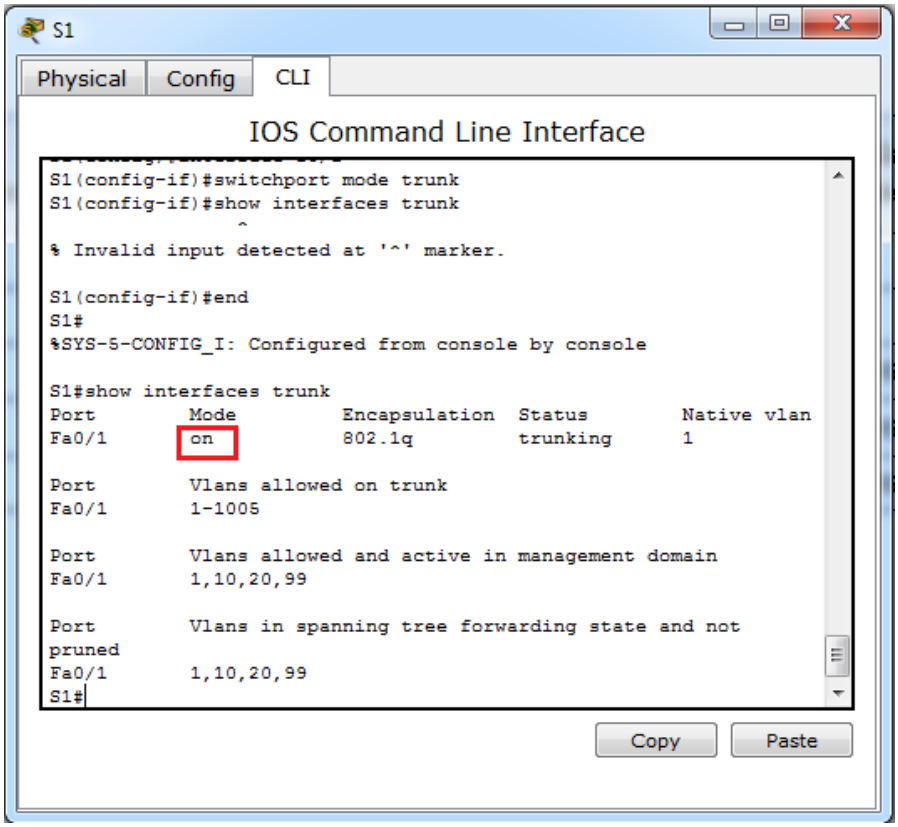
```
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#
```

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

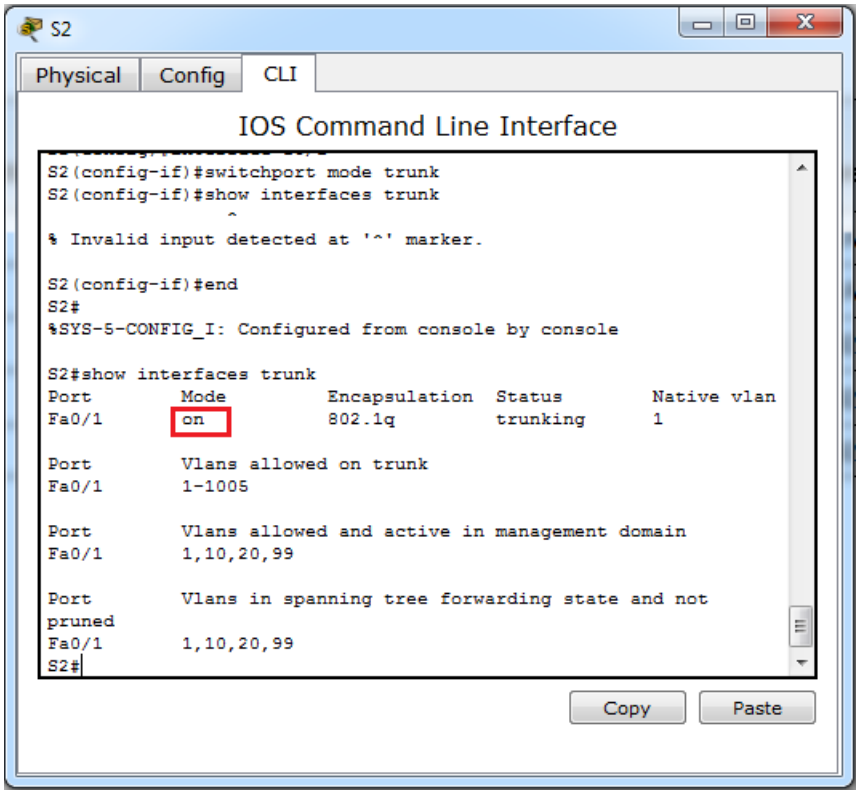
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



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

No todos los equipos utilizan DTP. El uso del comando switchport mode trunk asegura que el puerto se convierta como troncal independientemente del tipo de equipo conectado al otro extremo del enlace.

Parte 5. Eliminar la base de datos de VLAN

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

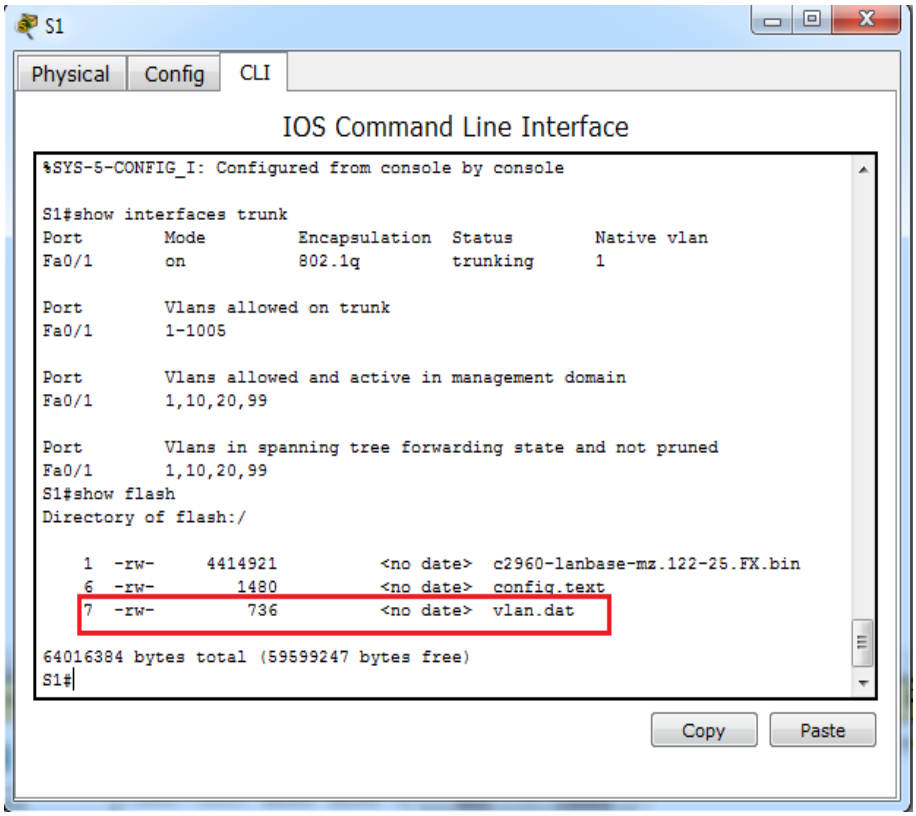
Paso 1. Determinar si existe la base de datos de VLAN.

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

```
S1# show flash

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.

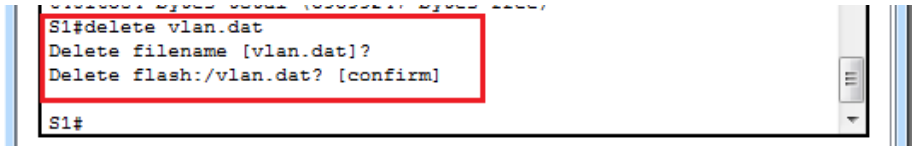
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



Paso 2. Eliminar la base de datos de VLAN.

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

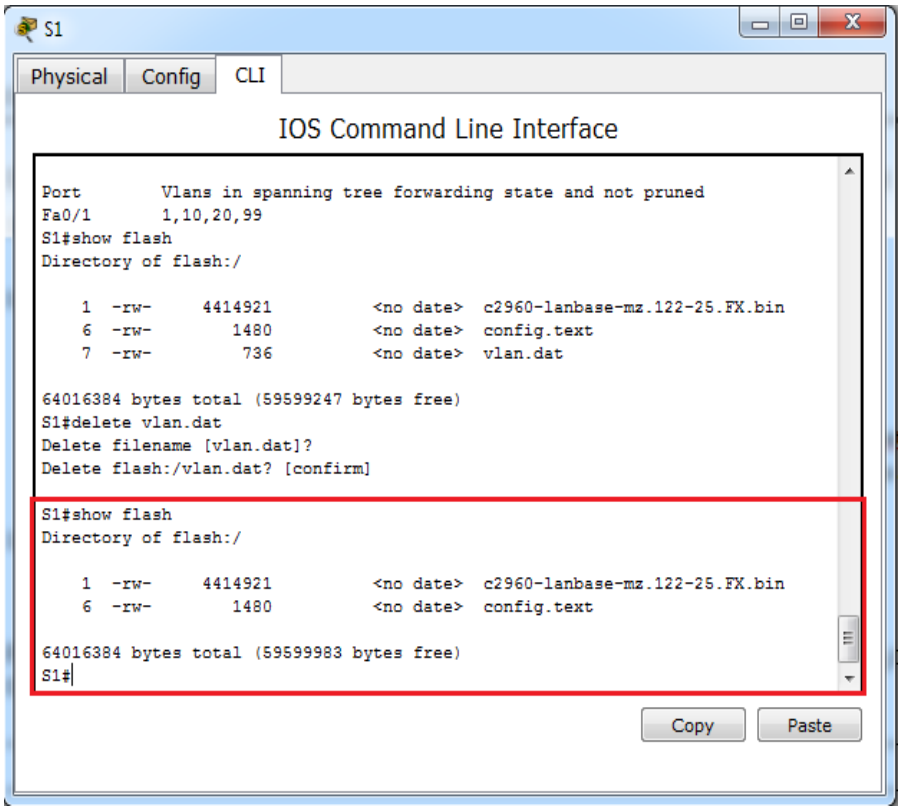
```
S1# delete vlan.dat
Delete    filename    [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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 inicializar un switch a su configuración predeterminada, los comandos serian **erase startup-config** y **reload** y deben ser emitidos después del comando **delete vlan.dat.**

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Reflexión

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

   Se necesita un switch o un router de capa 3 para enrutar el tráfico entre la VLAN.

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

   Los beneficios de VLAN incluyen: mejor seguridad, ahorro de costes (uso eficiente del ancho de banda y enlaces ascendentes), mayor rendimiento (menores dominios de broadcast), menores tormentas de broadcast, mejora la eficiencia del personal de TI, gestión más sencilla de proyectos y aplicaciones.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 6

- Con esta actividad se logró armar la red y configurar los parámetros básicos de los dispositivos
- Realizamos el cableado de red en packet tracer tal como se muestra en la topología de la guía.
- Configuramos los parámetros básicos para el switch S1 y S2.
- Configurar los equipos host de acuerdo a la tabla de direccionamiento de la guía.
- Probamos la conectividad entre los PCs y switch.
- Creamos las redes VLAN y asignamos puertos de switch.
- Configuramos un enlace troncal 802.1Q entre los switches.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 7: 3.3.2.2 Lab - Implementing VLAN Security

Práctica de laboratorio: implementación de seguridad de VLAN

Topología

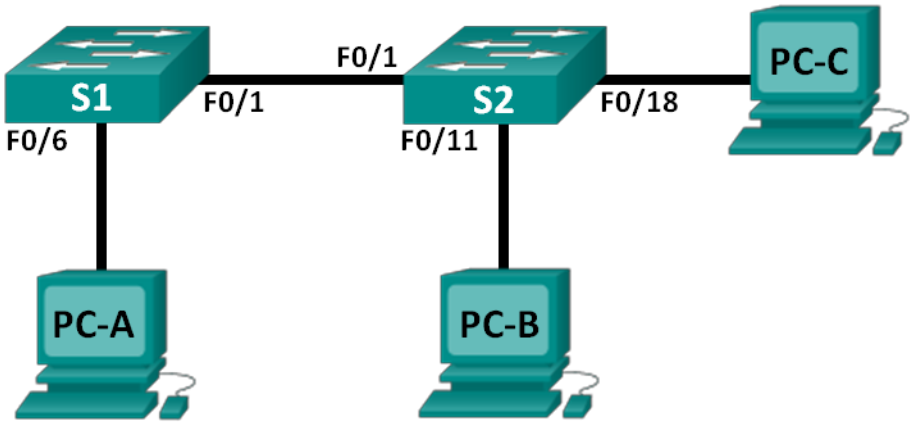


Tabla de direccionamiento

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

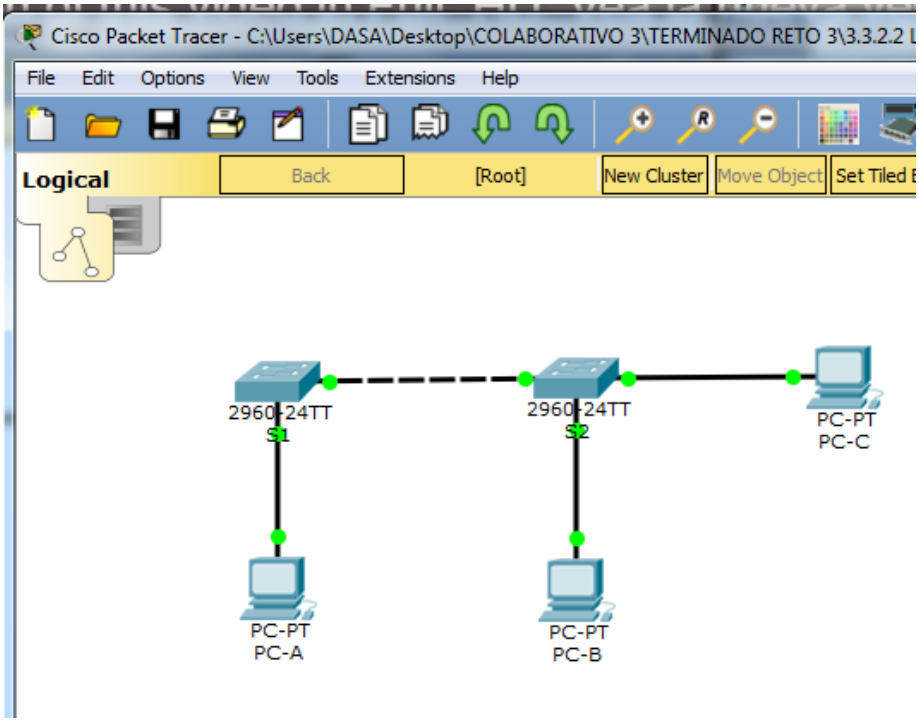
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet,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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

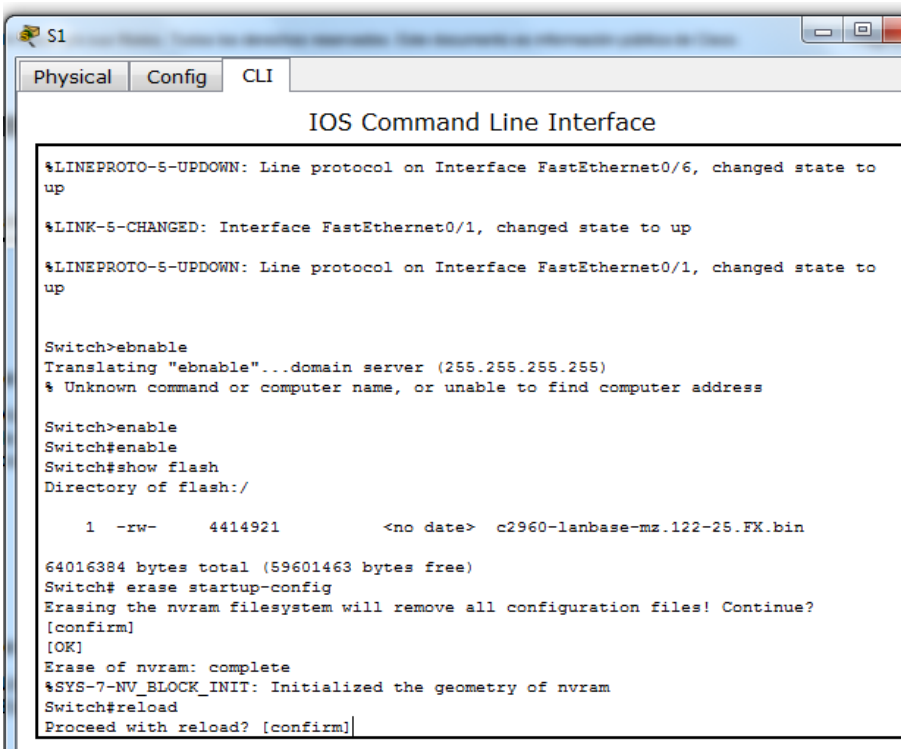
En la parte 1, configurará los parámetros básicos en los switches y las computadoras. Consulte la tabla de direccionamiento para obtener información sobre nombres de dispositivos y direcciones.

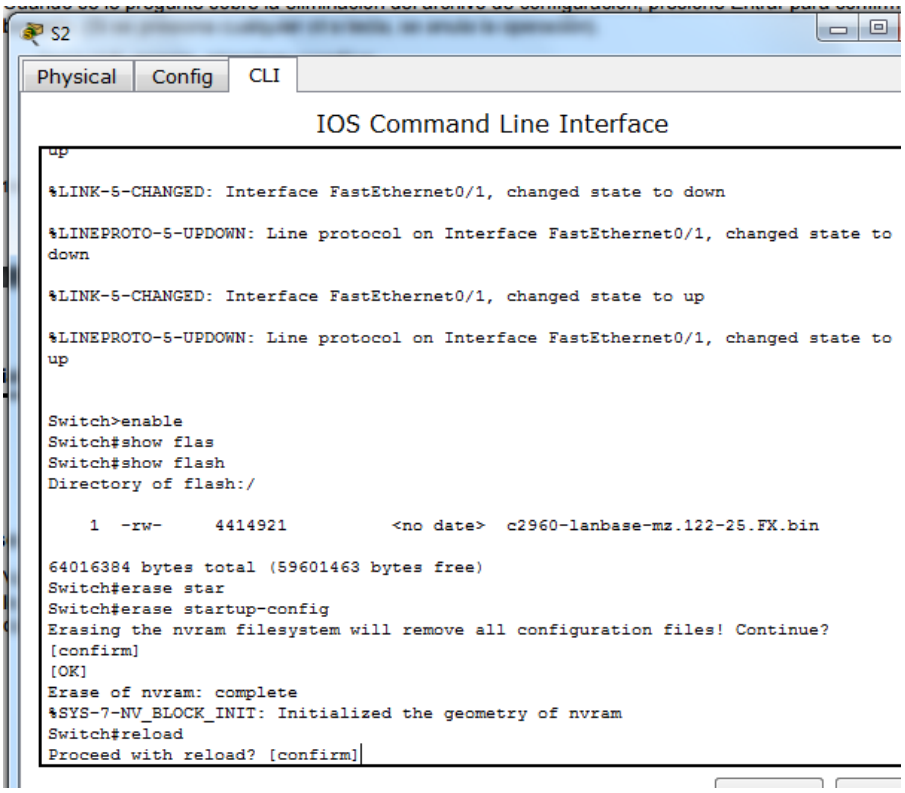
Paso 1. Realizar el cableado de red tal como se muestra en la topología.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 2. Inicializar y volver a cargar los switches.

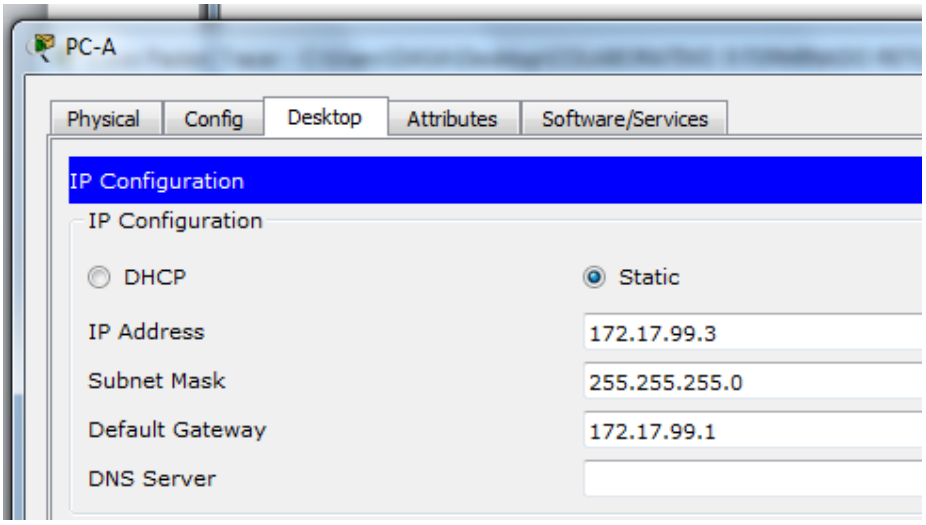


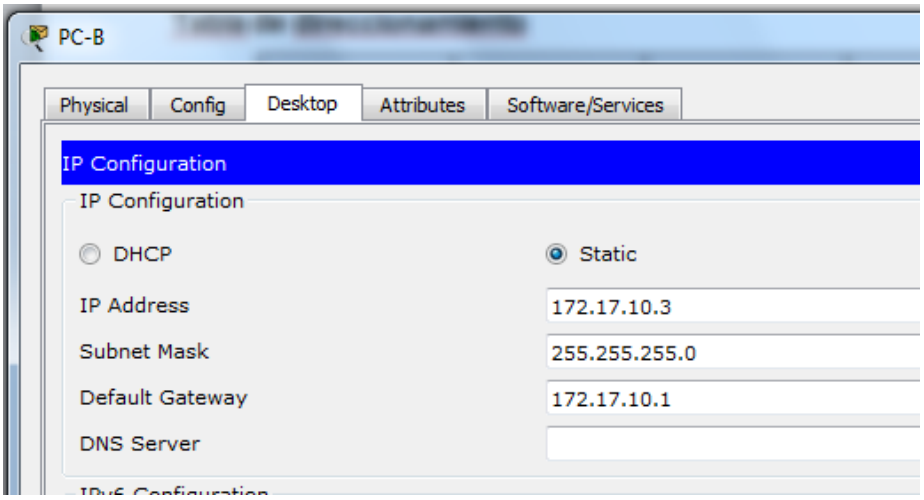


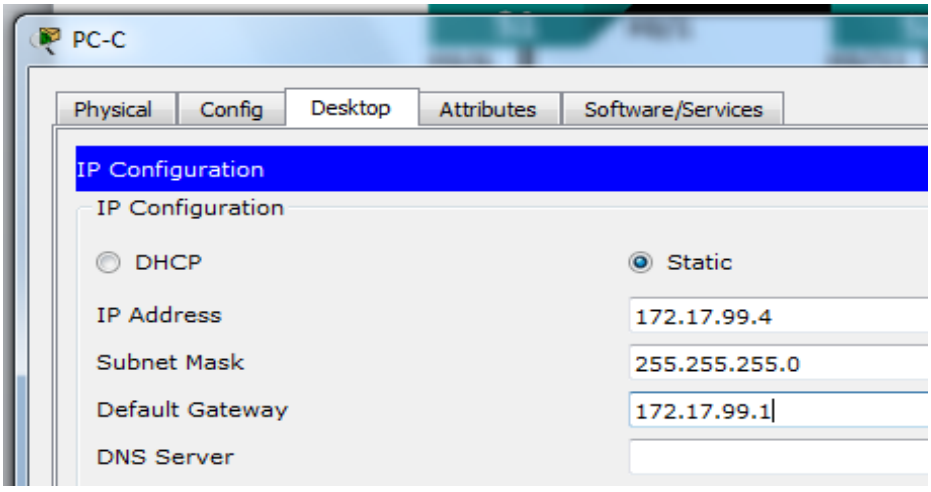
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.







© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 4. Configurar los parámetros básicos para cada switch.

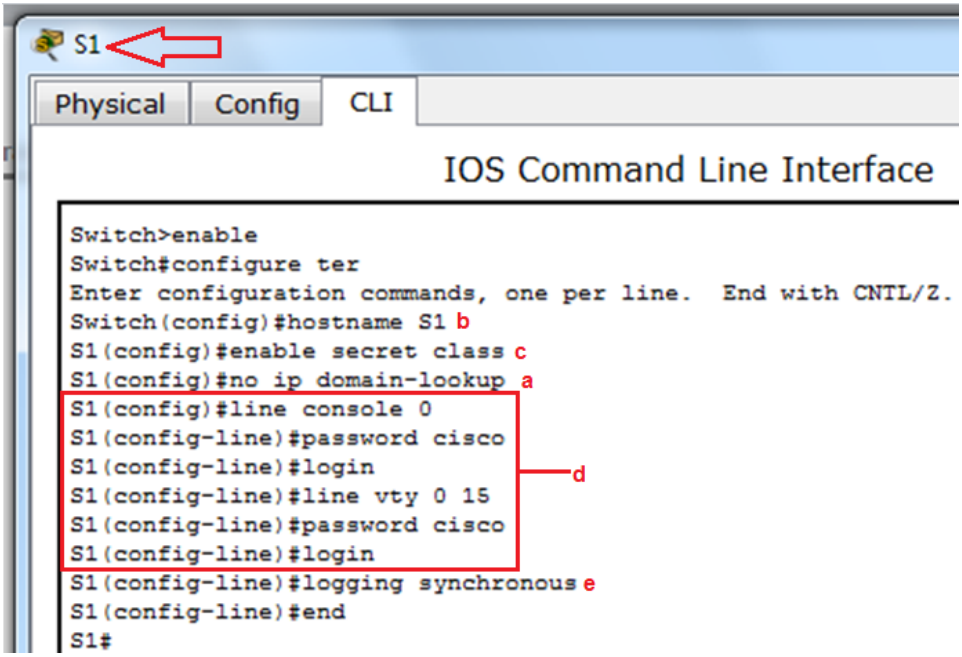
a. Desactive la búsqueda del DNS.

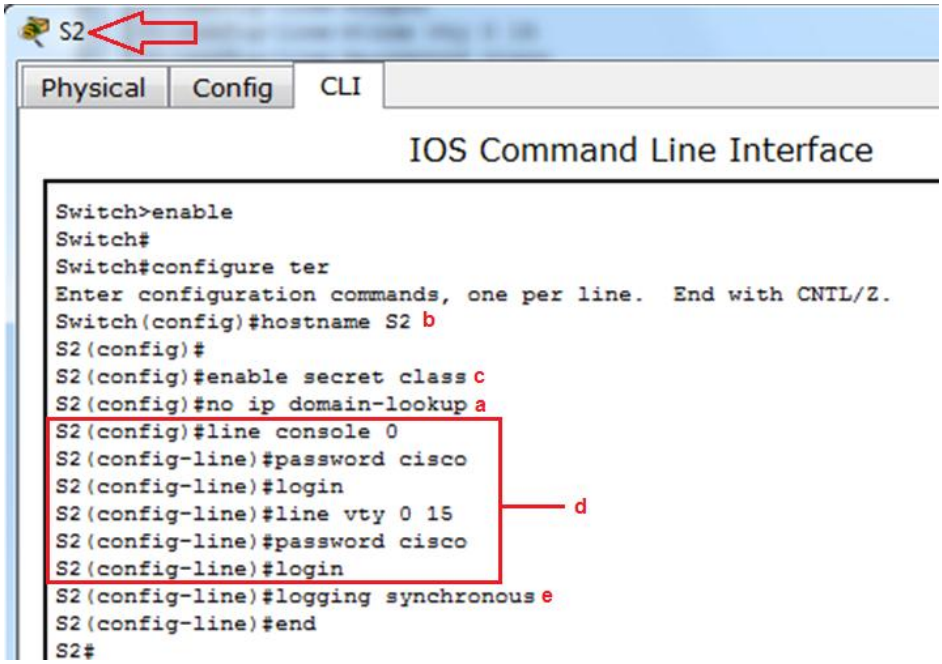
b. Configure los nombres de los dispositivos como se muestra en la topología.

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.

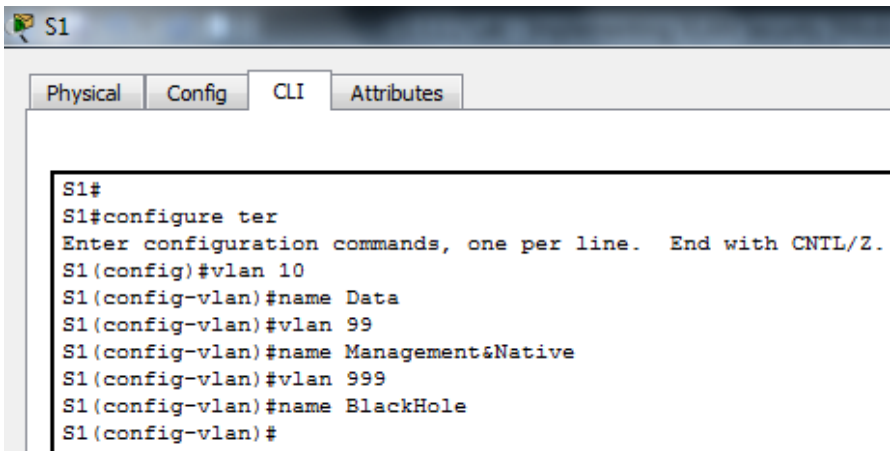


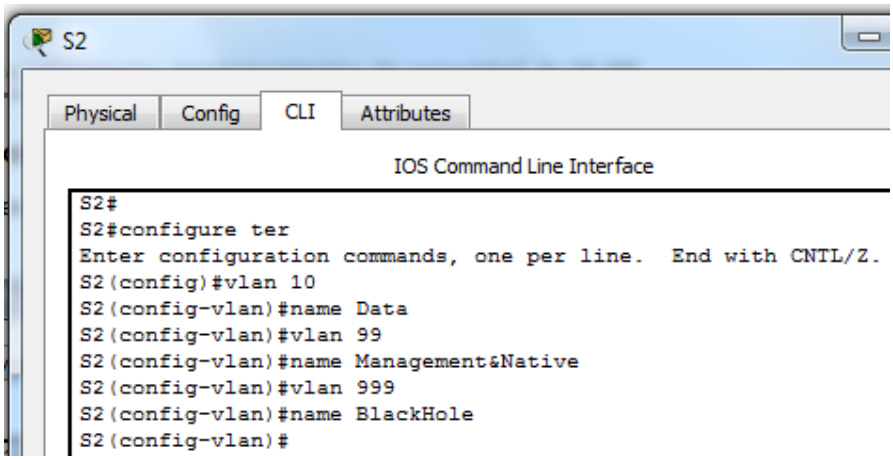


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

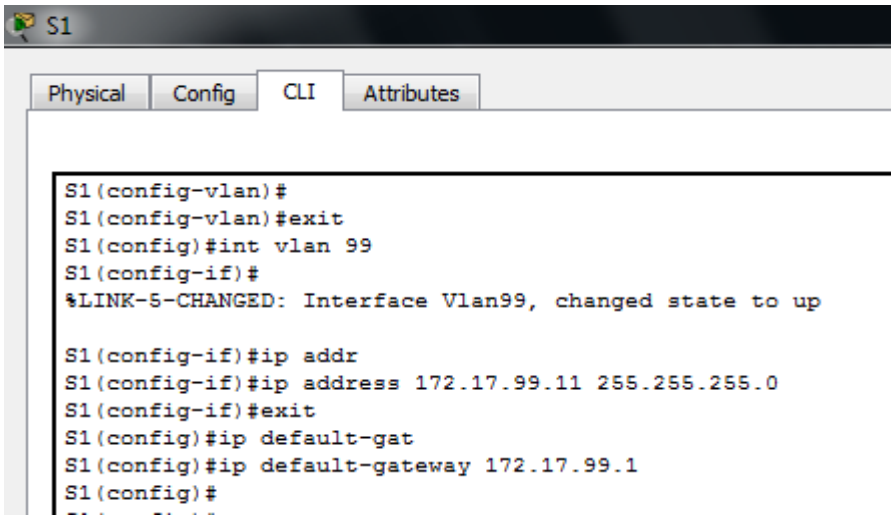
Paso 5. Configurar las VLAN en cada switch.

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

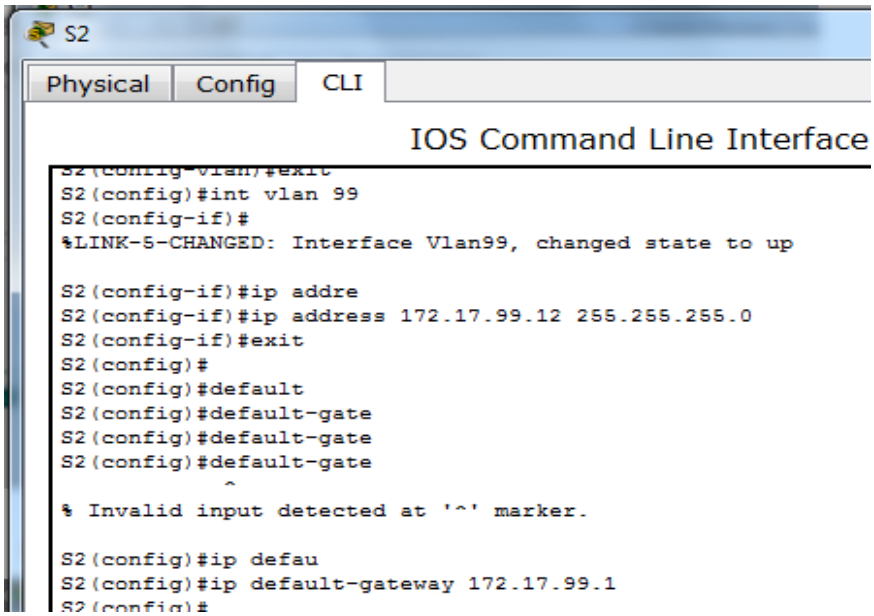




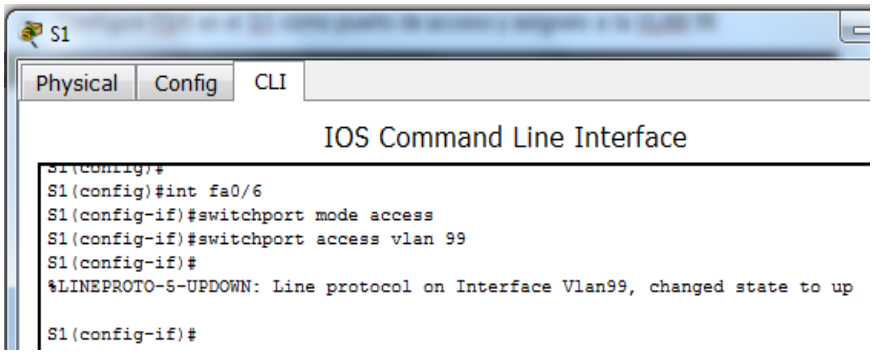
b. Configure la dirección IP que se indica para la VLAN 99 en la tabla de direccionamiento en ambos switches.



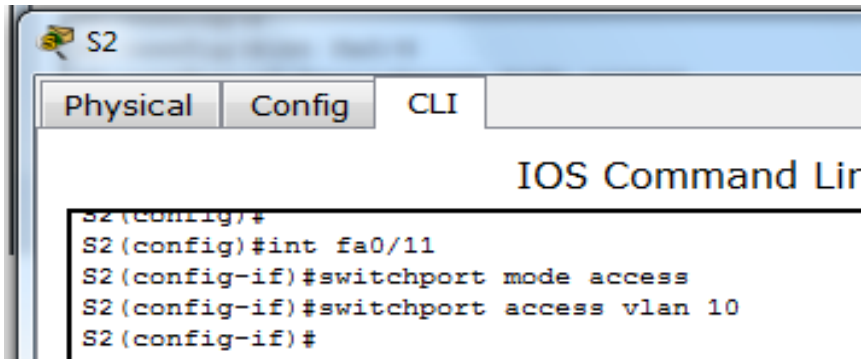
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



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

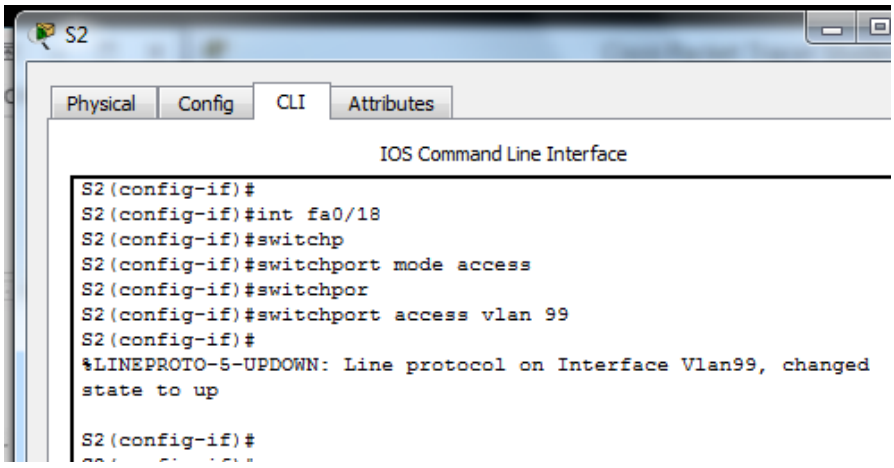


d. Configure F0/11 en el S2 como puerto de acceso y asígnelo a la VLAN 10.

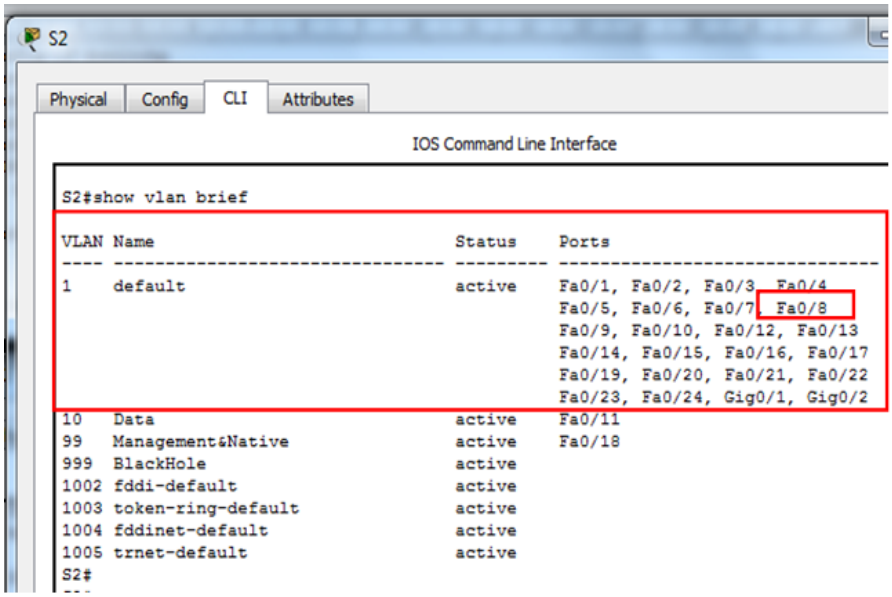


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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?

Se puede observar en la gráfica que dicho puerto como F0/8 pertenecería a la VLAN 1 por defecto. Así mismo, se observa que todos los puertos son asignados a la VLAN 1.

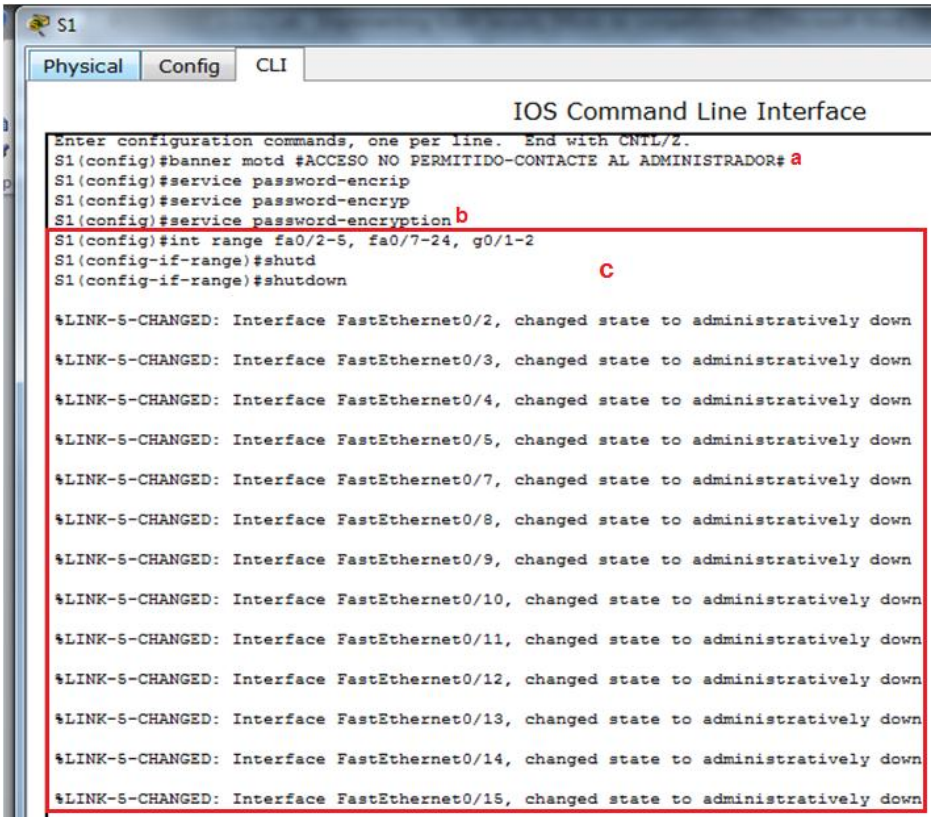
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

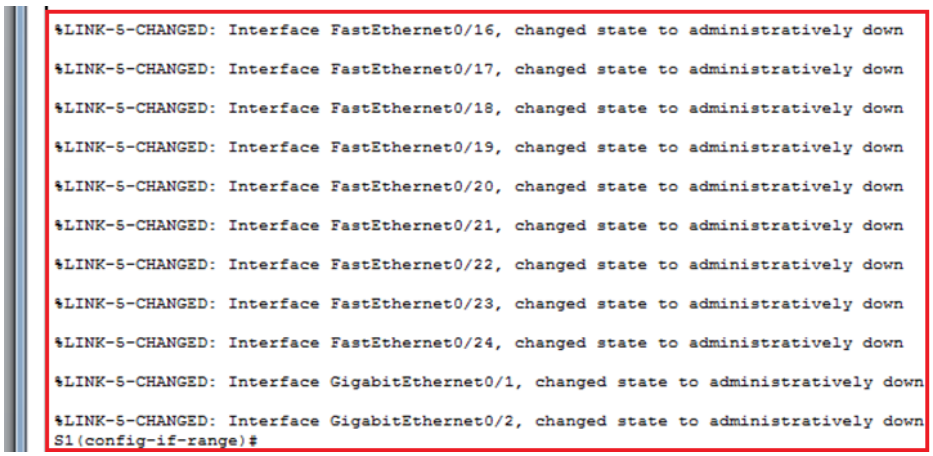
Paso 6. Configurar la seguridad básica del switch.

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

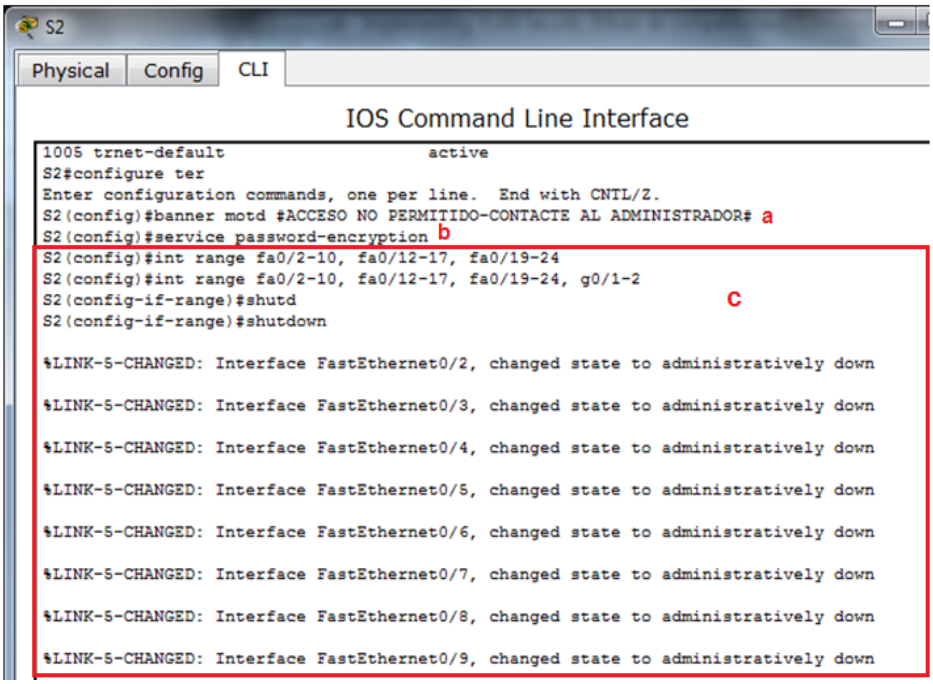
b. Encripte todas las contraseñas.

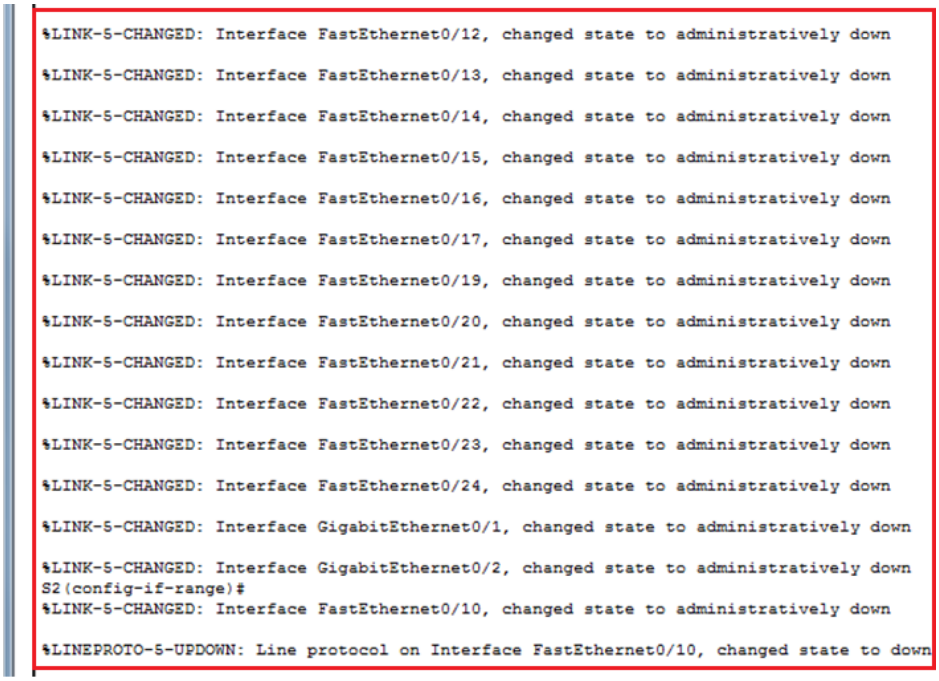
c. Desactive todos los puertos físicos sin utilizar.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

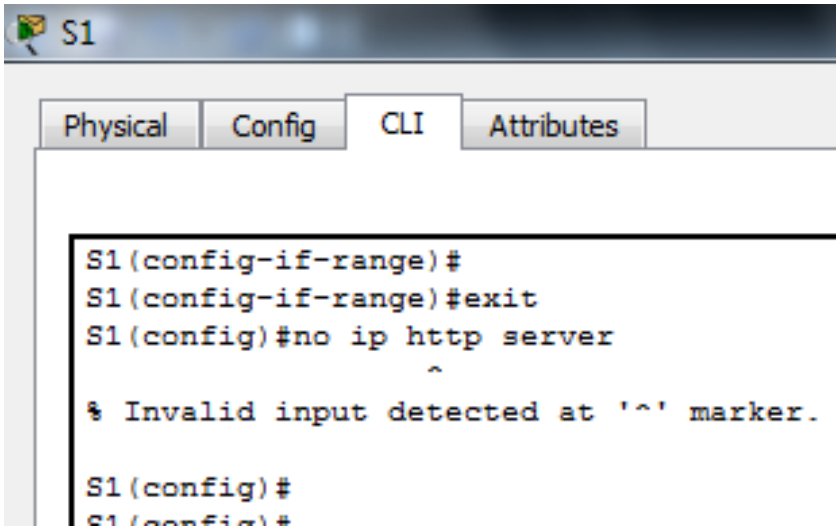


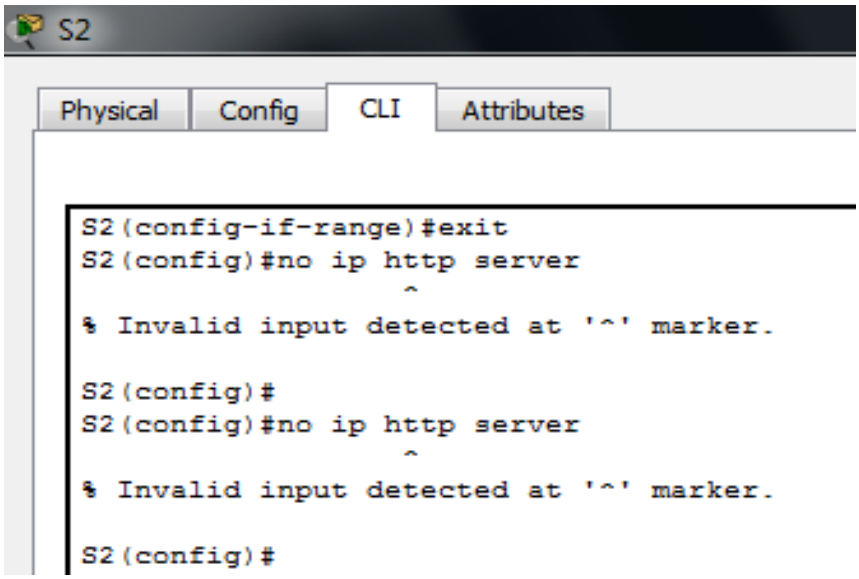


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

d. Deshabilite el servicio web básico en ejecución.

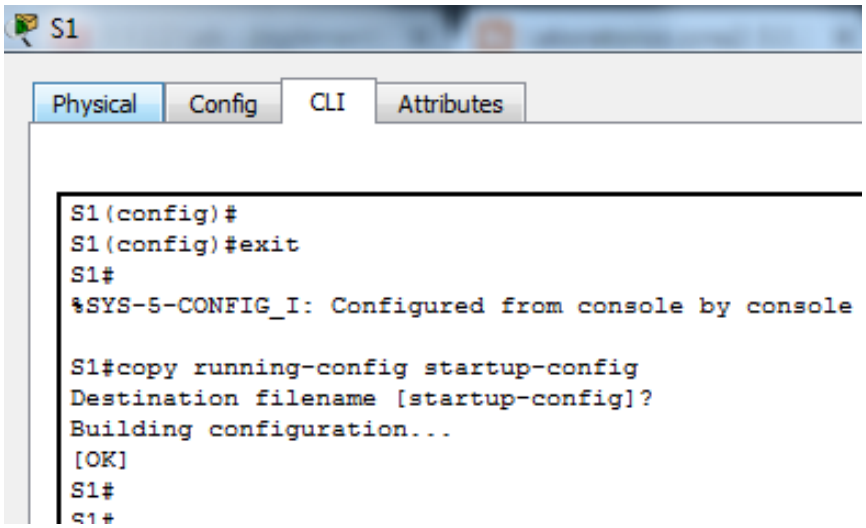
```
S1(config)# no ip http server
S2(config)# no ip http server
```

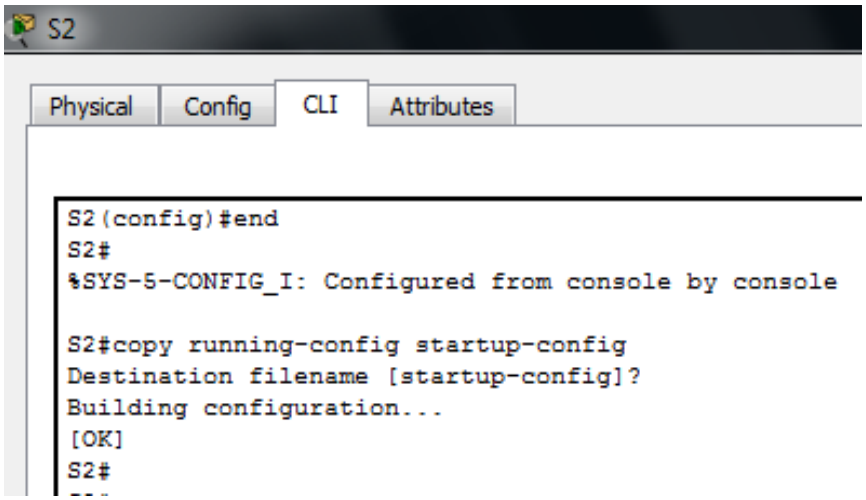




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



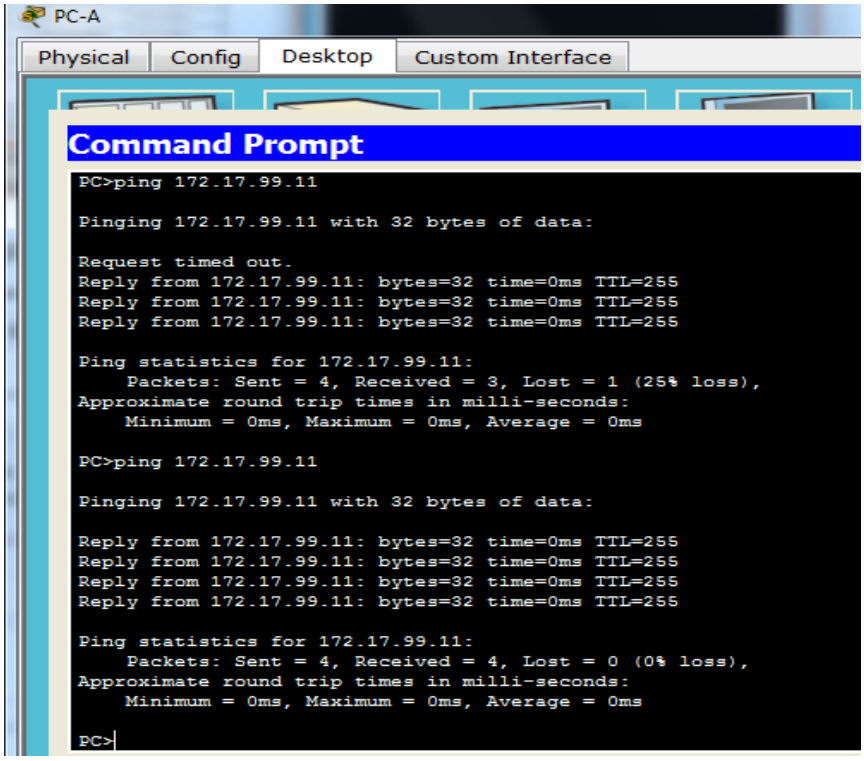


Paso 7. Verificar la conectividad entre la información de VLAN y los dispositivos.

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

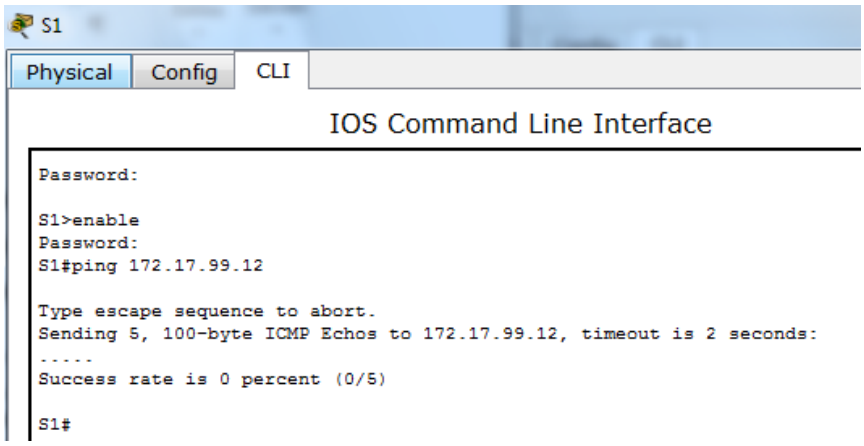
Se consiguió una conectividad con ping exitoso, ya que la PC-A se encuentra en la misma VLAN que la administración de administrador del switch.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



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

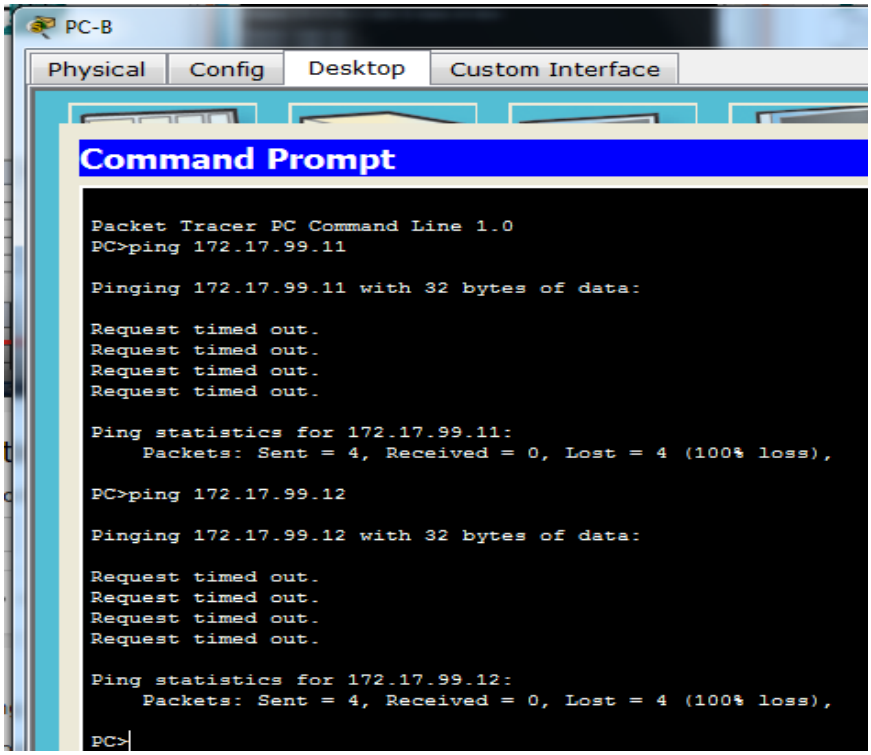
El ping fue fallido, se puede detallar que la dirección administrativa se haya en el Switch S1 y S2 se encuentran en la misma VLAN, no obstante la interface f0/1 en cada uno de los dispositivos, no está configurado como un puerto troncal.

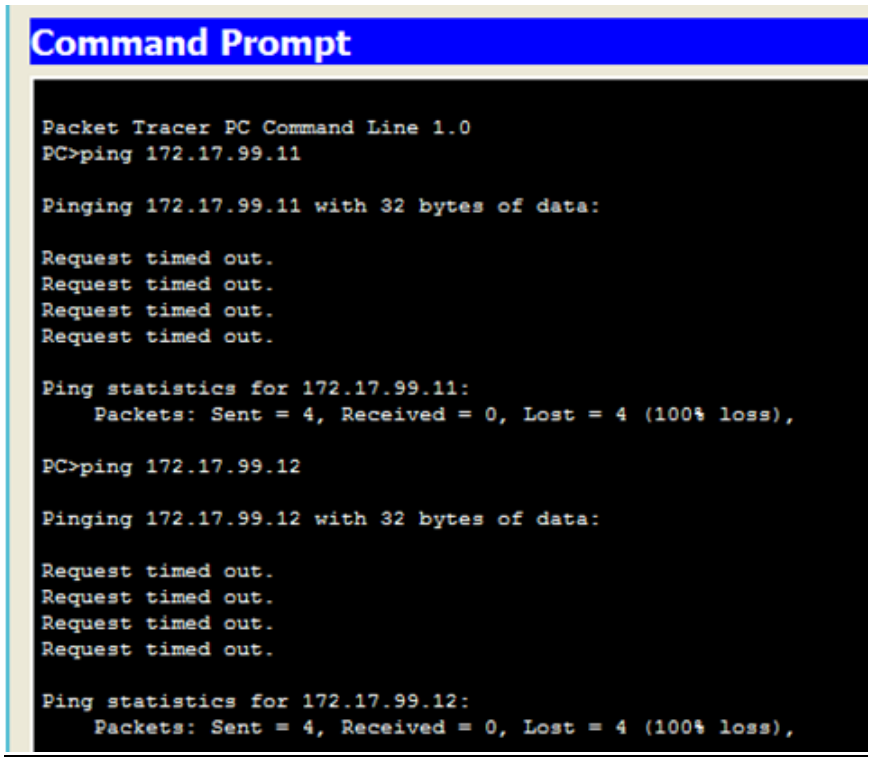


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

c. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué?

Los ping no fueron satisfactorios, ya que por ejemplo en ping desde la PC-B hacia S1, S2, PC-A y PCC. Ya que PC-B está sobre la VLAN 10 y S1, S2, PC-A Y PC-C se haya sobre la VLAN 99. No existe en el diagrama que permitan hacer el procedimiento de ruteo entre las redes.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
PC>ping 172.17.99.3

Pinging 172.17.99.3 with 32 bytes of data:

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

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

PC>ping 172.17.99.4

Pinging 172.17.99.4 with 32 bytes of data:

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

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

PC>
```

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

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

El ping realizado al S1 falló. Hay que tener en cuenta que la PC-C se encuentra en la misma VLAN que S1 y S2, sin embargo la PC-C está en capacidad de realizar ping a la dirección de S2, más no a la dirección administrativo de S1, ya que el enlace troncal no se ha configurado entre S1 y S2.

```
PC>ping 172.17.99.12

Pinging 172.17.99.12 with 32 bytes of data:

Reply from 172.17.99.12: bytes=32 time=0ms TTL=255
Reply from 172.17.99.12: bytes=32 time=0ms TTL=255
Reply from 172.17.99.12: bytes=32 time=0ms TTL=255
Reply from 172.17.99.12: bytes=32 time=0ms TTL=255

Ping statistics for 172.17.99.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

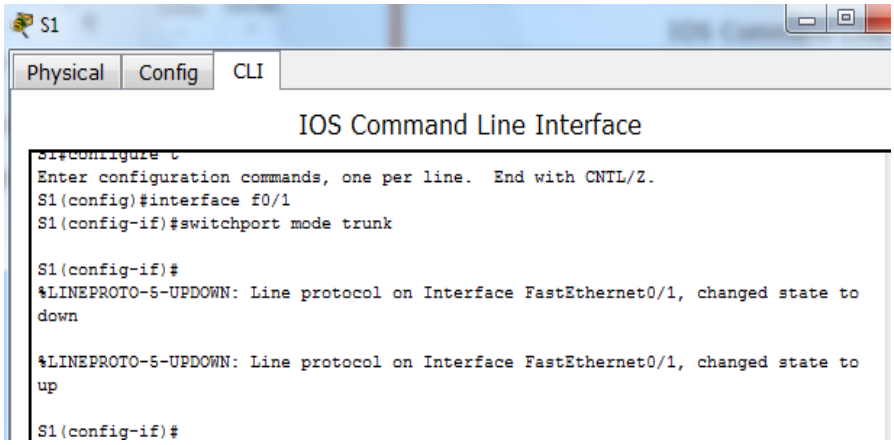
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 2. Implementar seguridad de VLAN en los switches

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

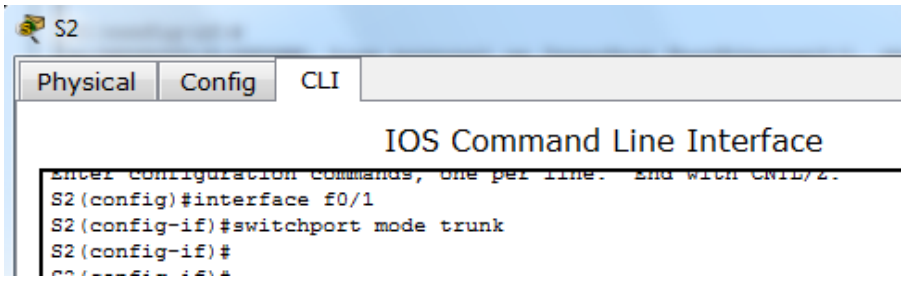
a. Configure el puerto F0/1 en el S1 como puerto de enlace troncal.

```
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.

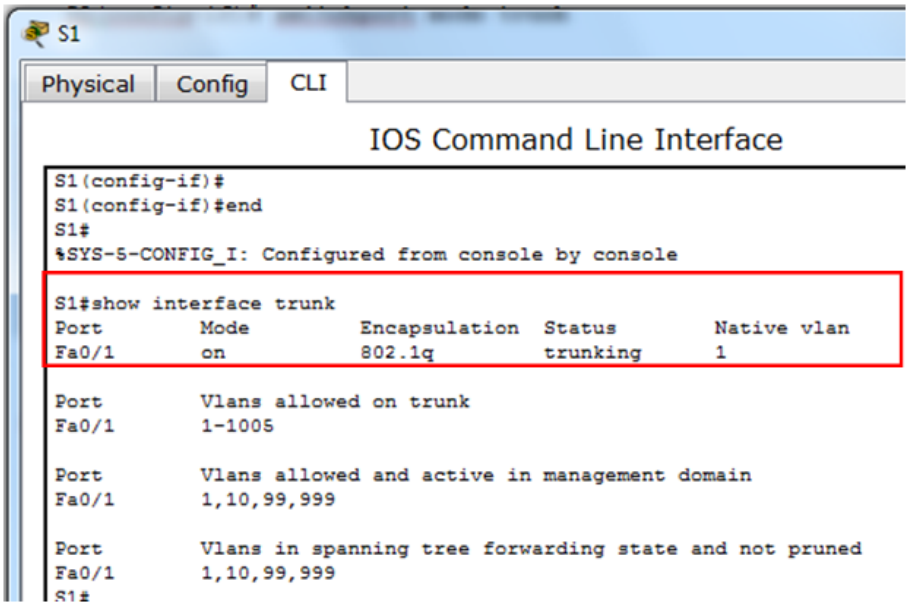
```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

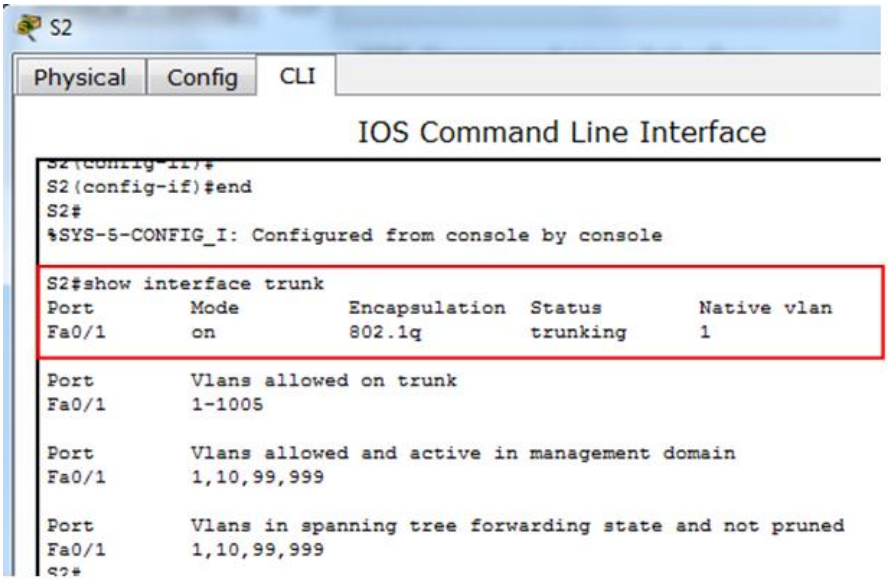


c. Verifique los enlaces troncales en el S1 y el S2. Emita el comando **show interface trunk** en los dos switches.

```
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
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.





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

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

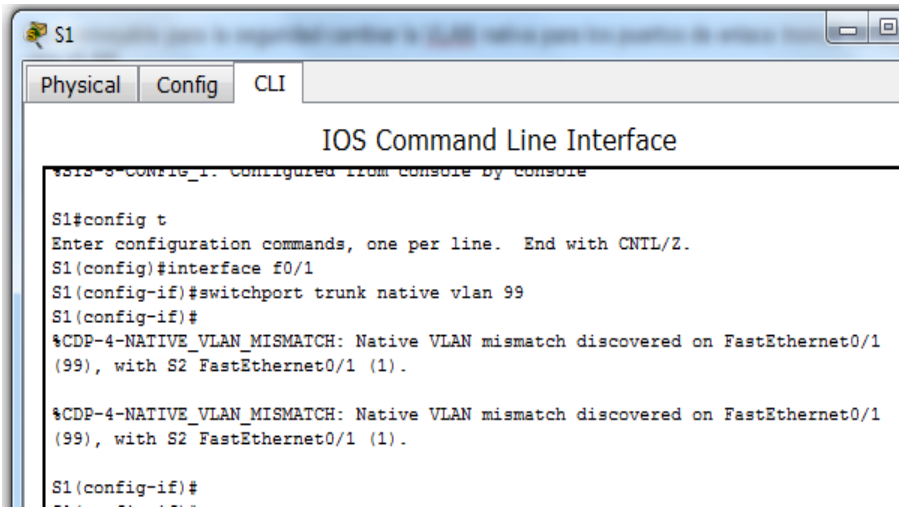
a. ¿Cuál es la VLAN nativa actual para las interfaces F0/1 del S1 y el S2?

La VLAN nativa actual es la VLAN1 para las interfaces F0/1 del S1 y S2.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

b. Configure la VLAN nativa de la interfaz de enlace troncal F0/1 del S1 en la VLAN 99 Management&Native.

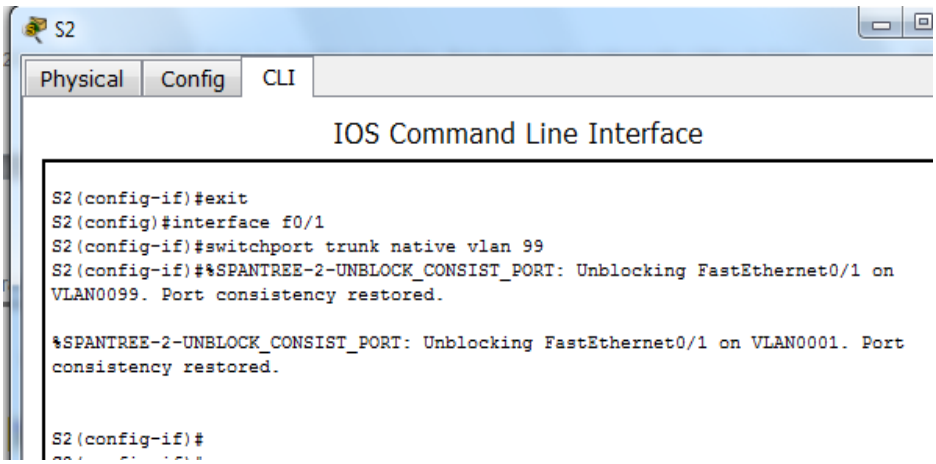
```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```



c. Espere unos segundos. Debería comenzar a recibir mensajes de error en la sesión de consola del S1. ¿Qué significa el mensaje %CDP-4-NATIVE_VLAN_MISMATCH:?
Dicho mensaje significa que S1 y S2 tienen sus VLANS nativas no concordantes. S2 tiene la VLAN en la VLAN 1 y S1 tiene la VLAN nativa a la VLAN 99.

d. Configure la VLAN 99 como VLAN nativa de la interfaz de enlace troncal F0/1 del S2.

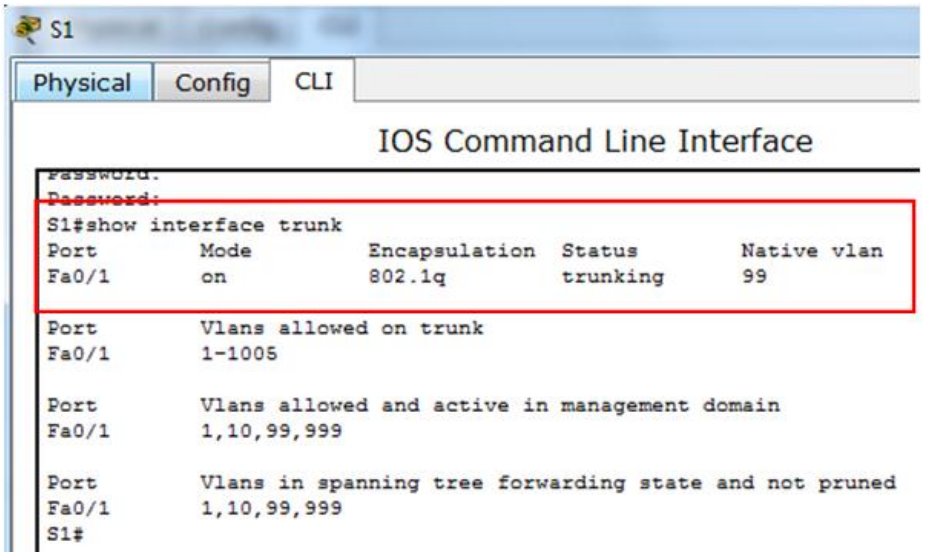
```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

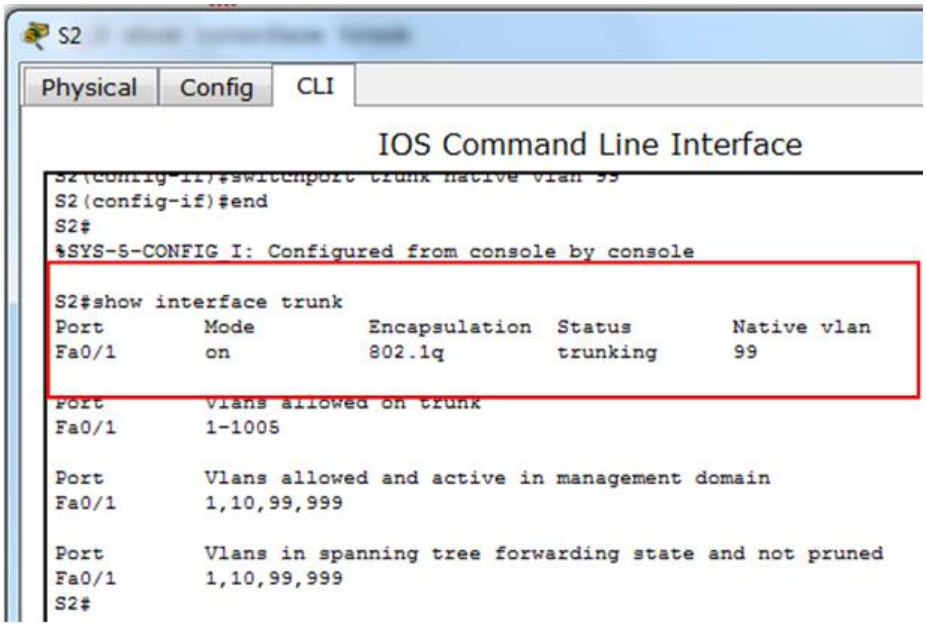


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

```
S1# show interface trunk

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
```



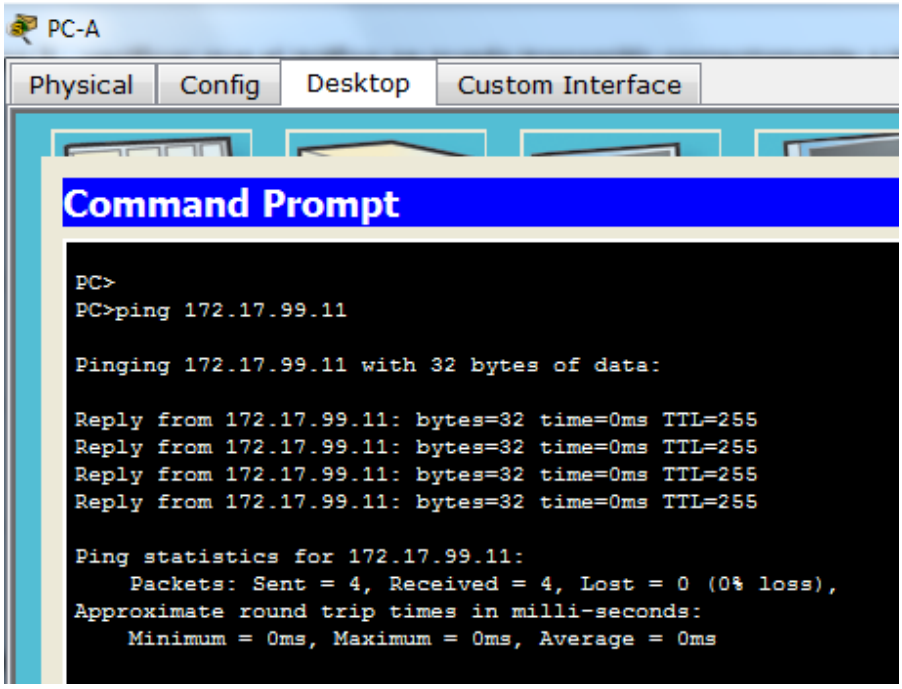


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

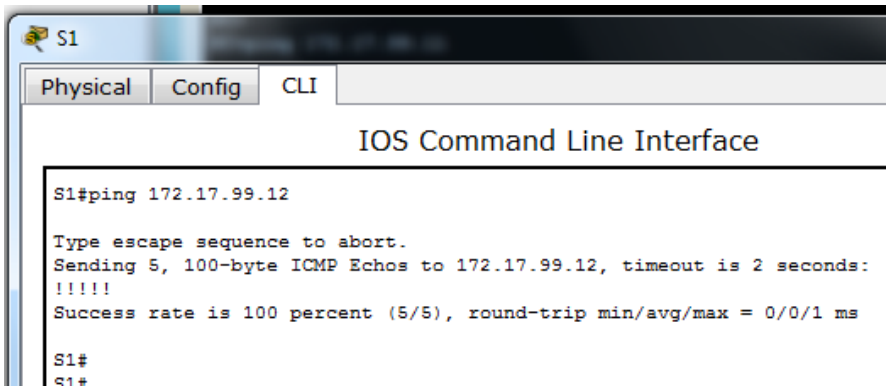
a. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué?

Fue satisfactorio, ya que PC-A se encuentra en la misma VLAN de la fase administrativa del swtiche.



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

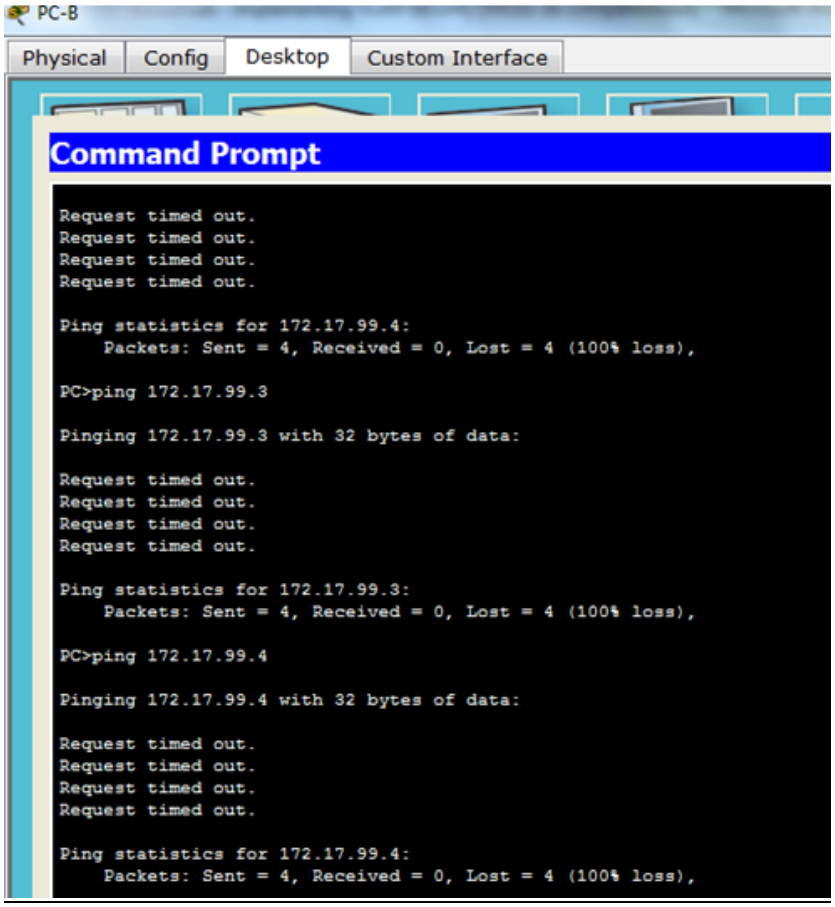
Fue satisfactorio, ya que los puertos troncales se configuraron correctamente, además los swtiches se encuentran en la misma VLAN 99.

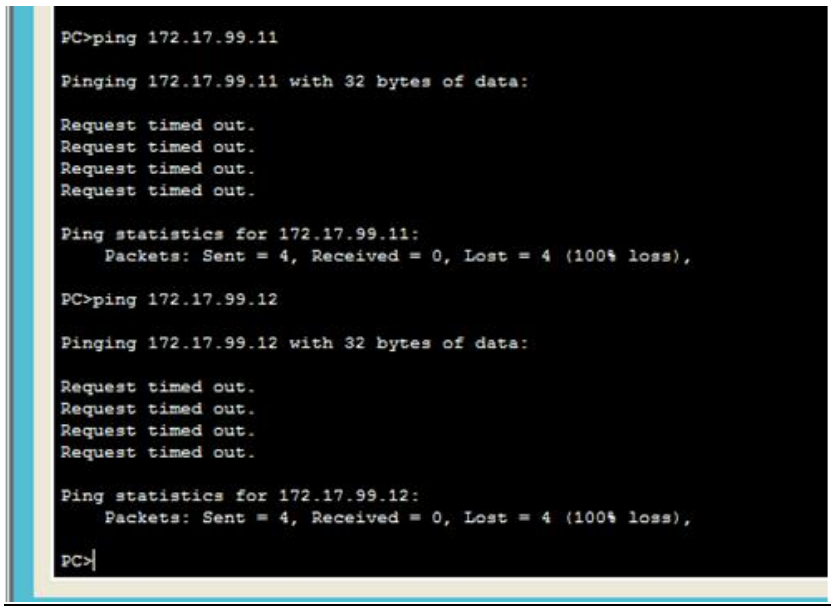


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

c. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué?

Los pines a S1, S2 y PC-A desde la PC-B no es satisfactorio, ya que la PC-B se encuentra en la VLAN1 y S1, S2, PC-A y PC-C están sobre la VLAN 99 y no existe un dispositivo que permita rotear desde las redes.

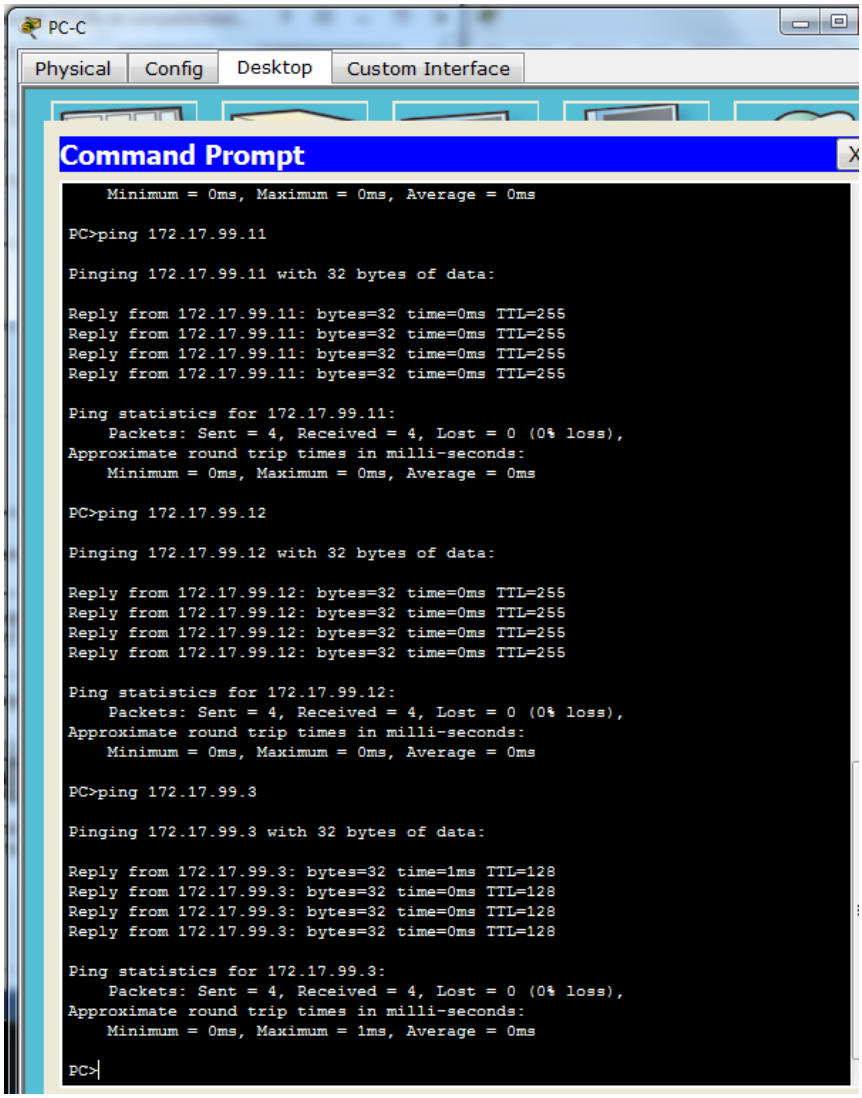




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

Todos los pines fueron satisfactorios porque PC-C está en la misma VLAN que S1, S2 y PC-A.

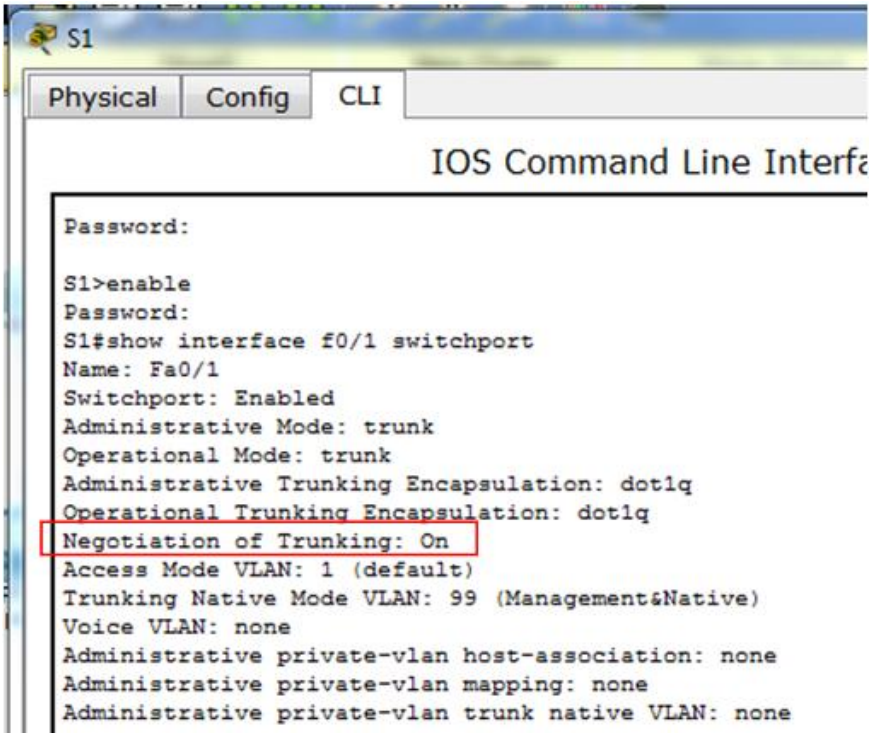


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 4. Impedir el uso de DTP en el S1 y el S2.

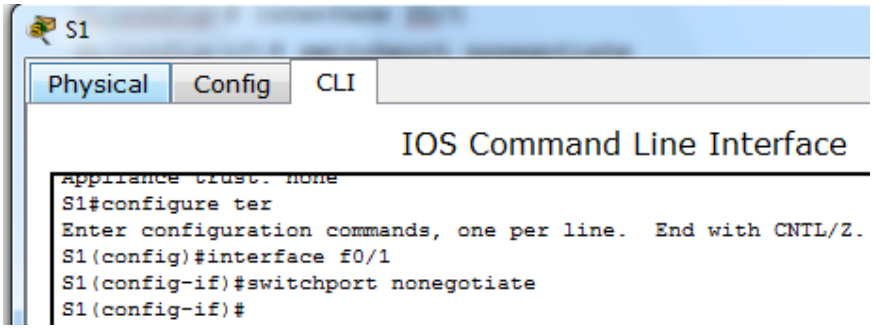
Cisco utiliza un protocolo exclusivo conocido como “protocolo de enlace troncal dinámico” (DTP) en los switches. Algunos puertos negocian el enlace troncal de manera automática. Se recomienda desactivar la negociación. Puede ver este comportamiento predeterminado mediante la emisión del siguiente comando:

```
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>
```



a. Desactive la negociación en el S1.

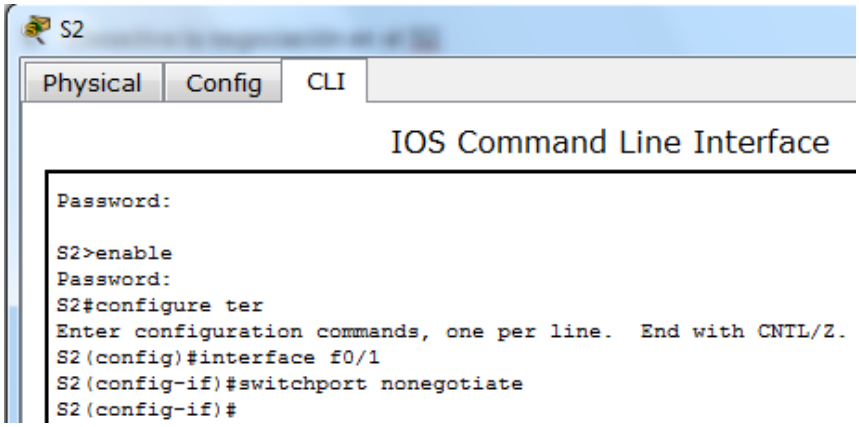
```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

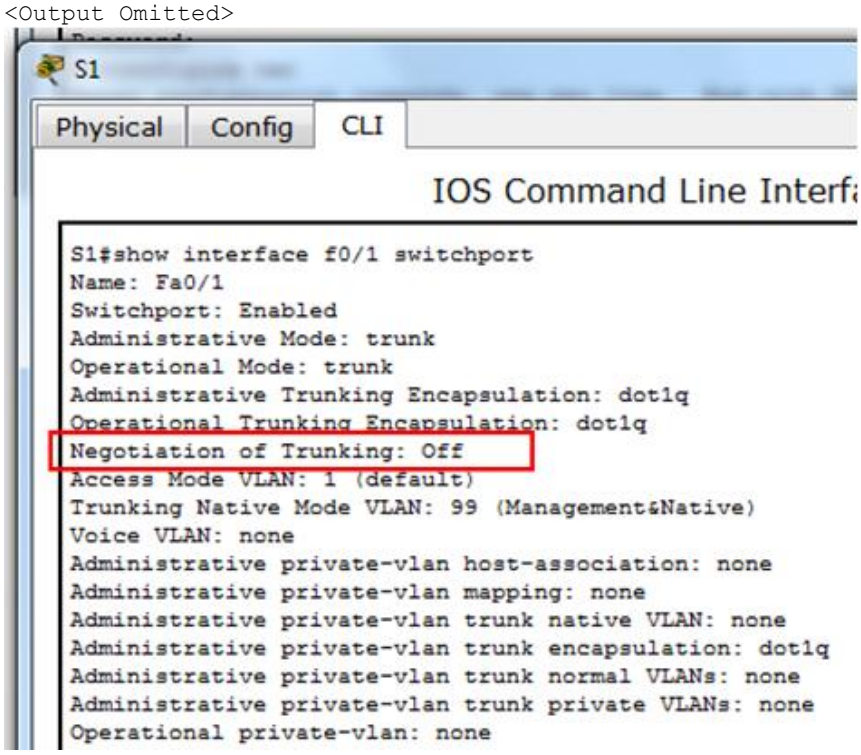
b. Desactive la negociación en el S2.

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

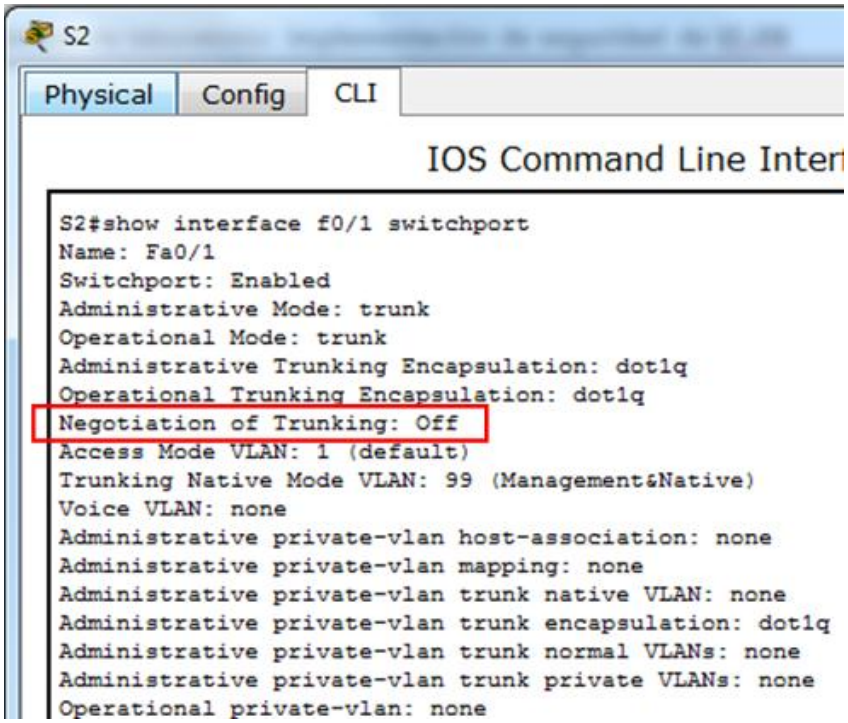


c. Verifique que la negociación esté desactivada mediante la emisión del comando **show interface f0/1 switchport** en el S1 y el S2.

```
S1# show interface f0/1 switchport
Name:          Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational  Trunking  Encapsulation:  dot1q
Negotiation of Trunking: Off
<Output Omitted>
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



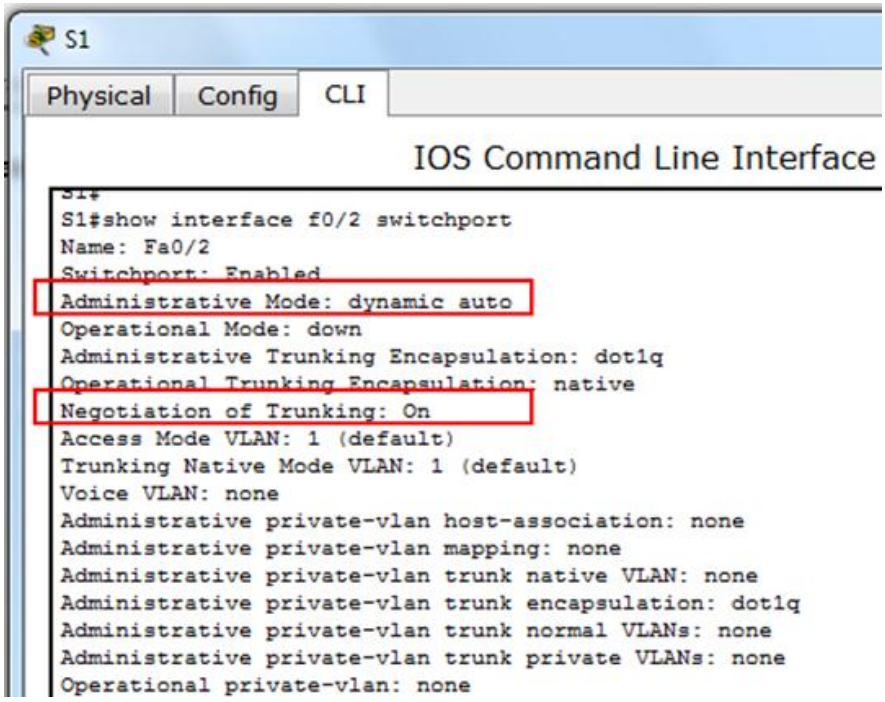
Paso 5. Implementar medidas de seguridad en los puertos de acceso del S1 y el S2.

Aunque desactivó los puertos sin utilizar en los switches, si se conecta un dispositivo a uno de esos puertos y la interfaz está habilitada, se podría producir un enlace troncal. Además, todos los puertos están en la VLAN 1 de manera predeterminada. Se recomienda colocar todos los puertos sin utilizar en una VLAN de “agujero negro”. En este paso, deshabilitará los enlaces troncales en todos los puertos sin utilizar. También asignará los puertos sin utilizar a la VLAN 999. A los fines de esta práctica de laboratorio, solo se configurarán los puertos 2 a 5 en ambos switches.

a. Emita el comando **show interface f0/2 switchport** en el S1. Observe el modo administrativo y el estado para la negociación de enlaces troncales.

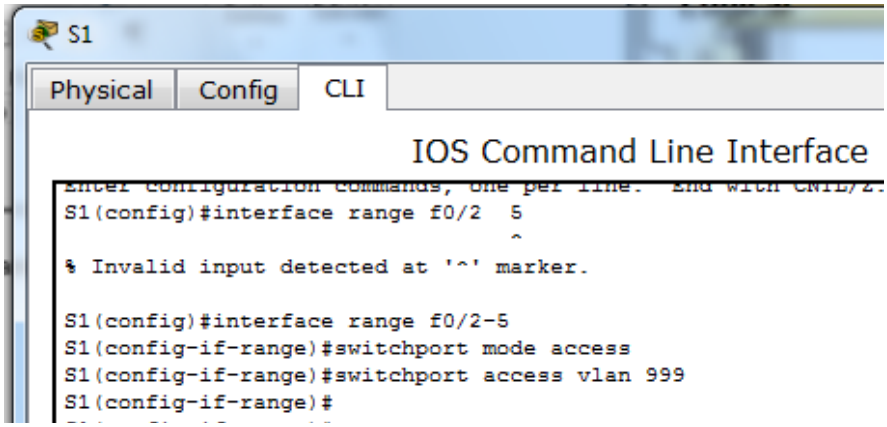
```
S1# show interface f0/2 switchport
Name:          Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

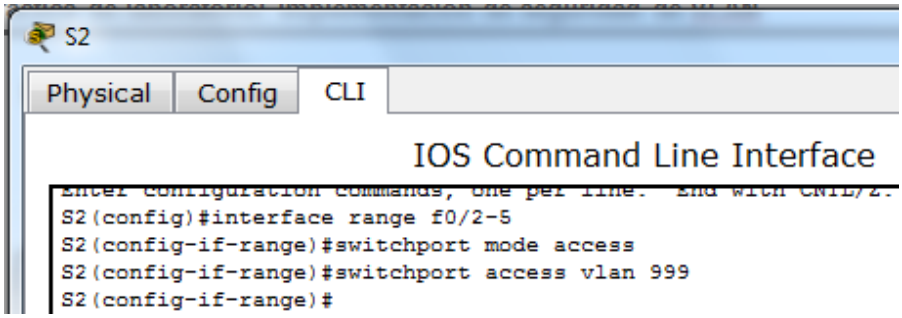


b. Deshabilite los enlaces troncales en los puertos de acceso del S1.

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



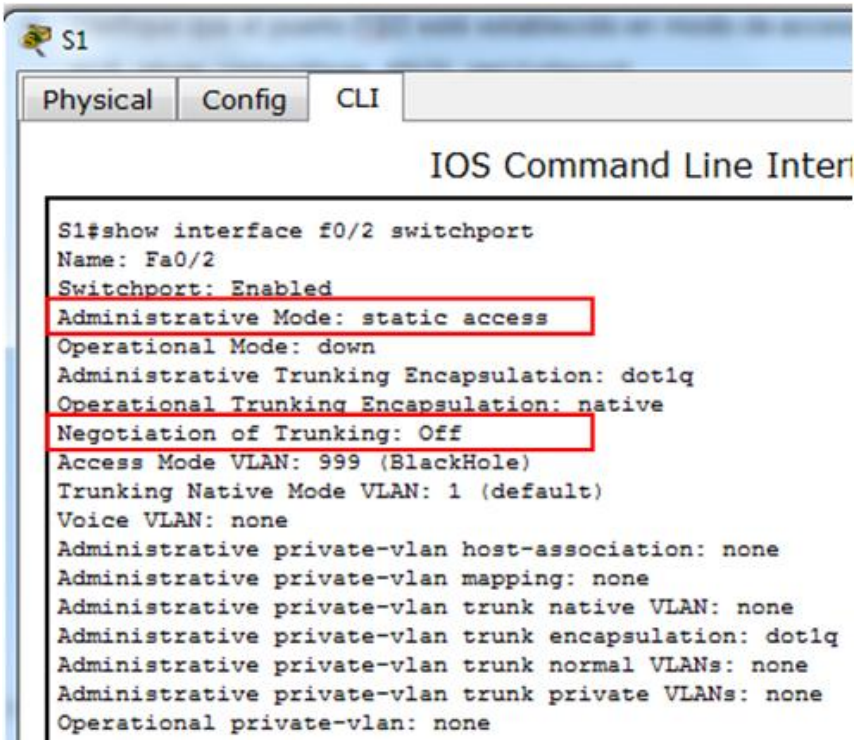
c. Deshabilite los enlaces troncales en los puertos de acceso del S2.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

d. Verifique que el puerto F0/2 esté establecido en modo de acceso en el S1.

```
S1# show interface f0/2 switchport
Name:          Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access  Mode  VLAN:  999  (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Output Omitted>
```



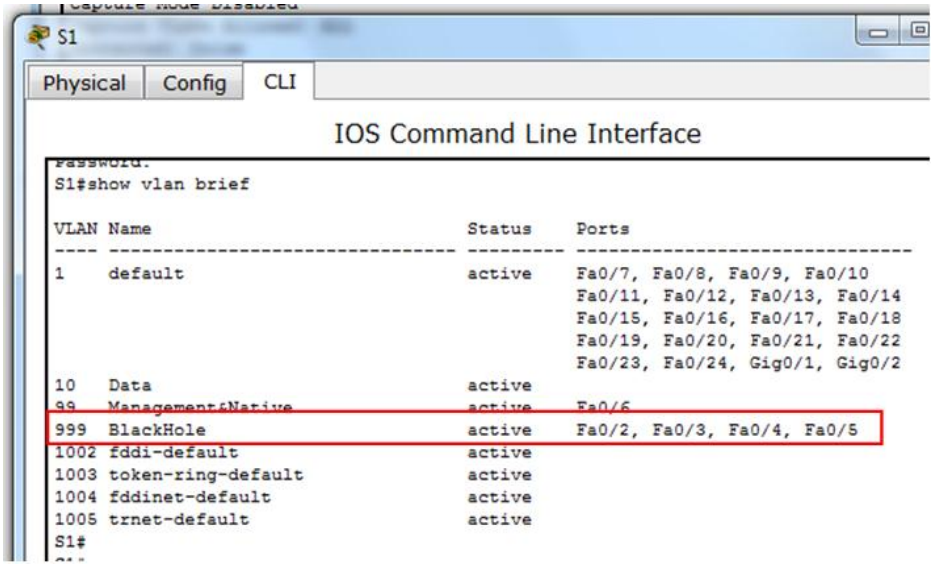
e. Verifique que las asignaciones de puertos de VLAN en ambos switches sean las correctas. A continuación, se muestra el S1 como ejemplo.

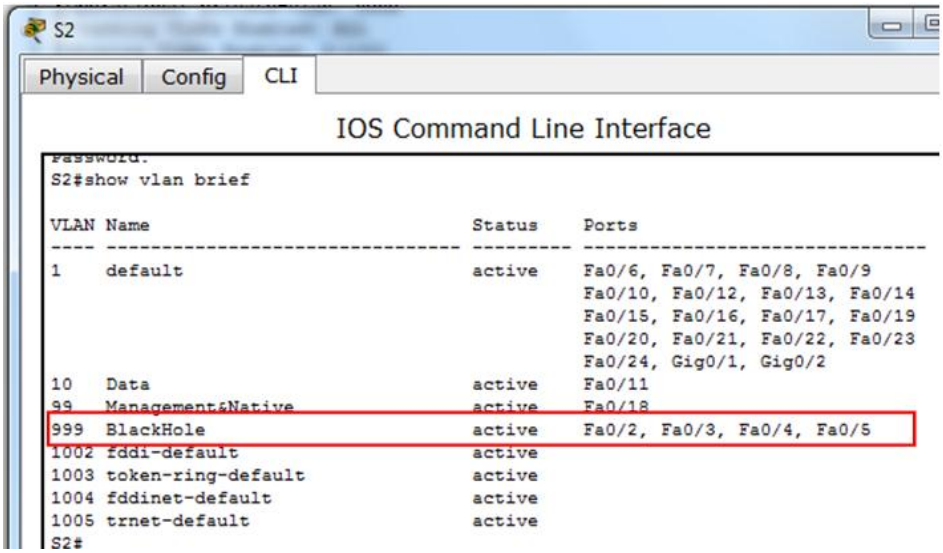
```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7,  Fa0/8,  Fa0/9,  Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
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.

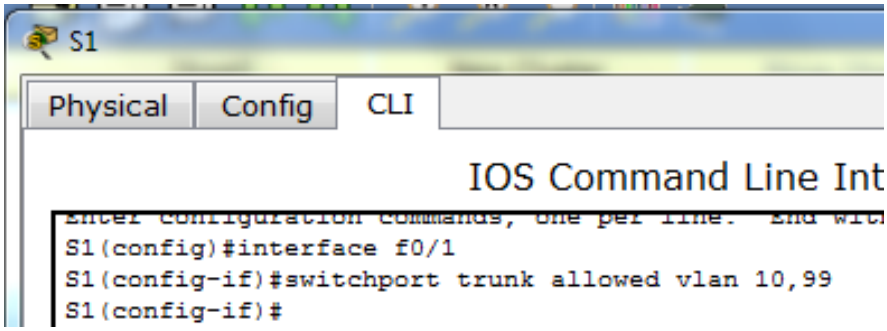




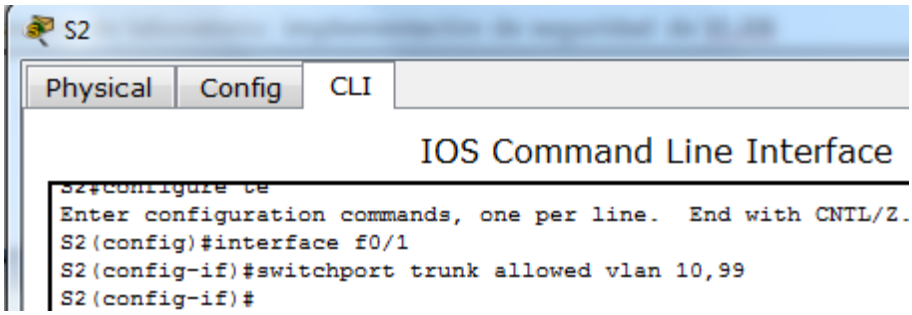
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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



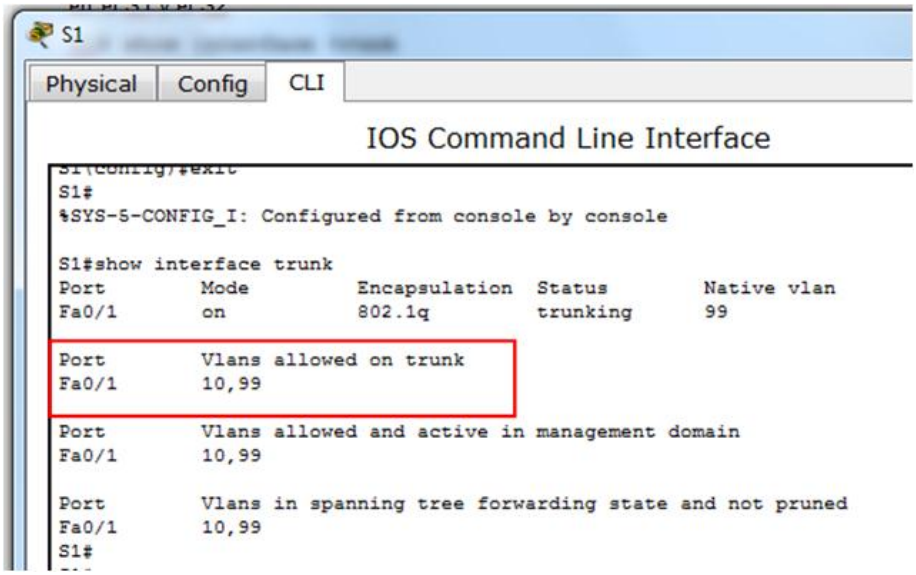
g. Restrinja el puerto de enlace troncal F0/1 en el S2 para permitir solo las VLAN 10 y 99.

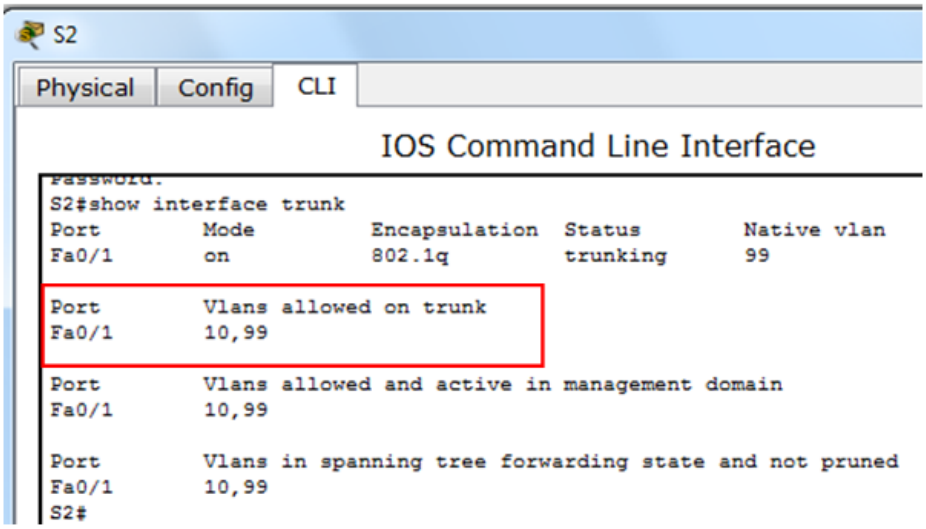


h. Verifique las VLAN permitidas. Emita el comando **show interface trunk** en el modo EXEC privilegiado en el S1 y el S2

```
S1# show interface trunk

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

Port        Vlans allowed on trunk
Fa0/1       10,99

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

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.





¿Cuál es el resultado?

Se puede evidenciar que únicamente las VLAN 10 y la VLAN 99 están permitidas sobre el enlace troncal, entre los switches S1 y S2.

Reflexión

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

Es claro que todos los puertos fueron asignados a la VLAN 1 por defecto, convirtiéndose en un problema de seguridad. En muchos Switches las líneas troncales se encuentran modo iniciación, y estas troncales pueden ser encendidas sin autorización, lo que es de cuidado en efectos de seguridad. Existe así mismo, un problema en encriptación de password, al estar en texto plano.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 7

- Configuramos los parámetros básicos de seguridad para los puertos de enlace troncal y de acceso en los switches, con el fin de protegerlos contra los ataques de VLAN.
- Utilizamos varios comandos show para analizar la forma en que se comportan los switches Cisco. Luego de esto aplicamos medidas de seguridad.
- Armamos la red y configuramos los parámetros básicos de los dispositivos.
- Implementamos seguridad de VLAN en los switches.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 8: 4.1.4.6 Lab - Configuring Basic Router Settings with IOS CLI

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

Topología

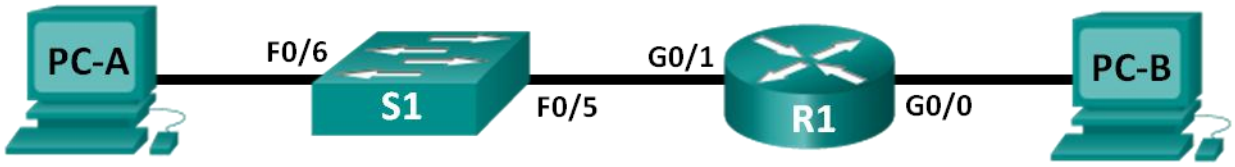


Tabla de direccionamiento

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

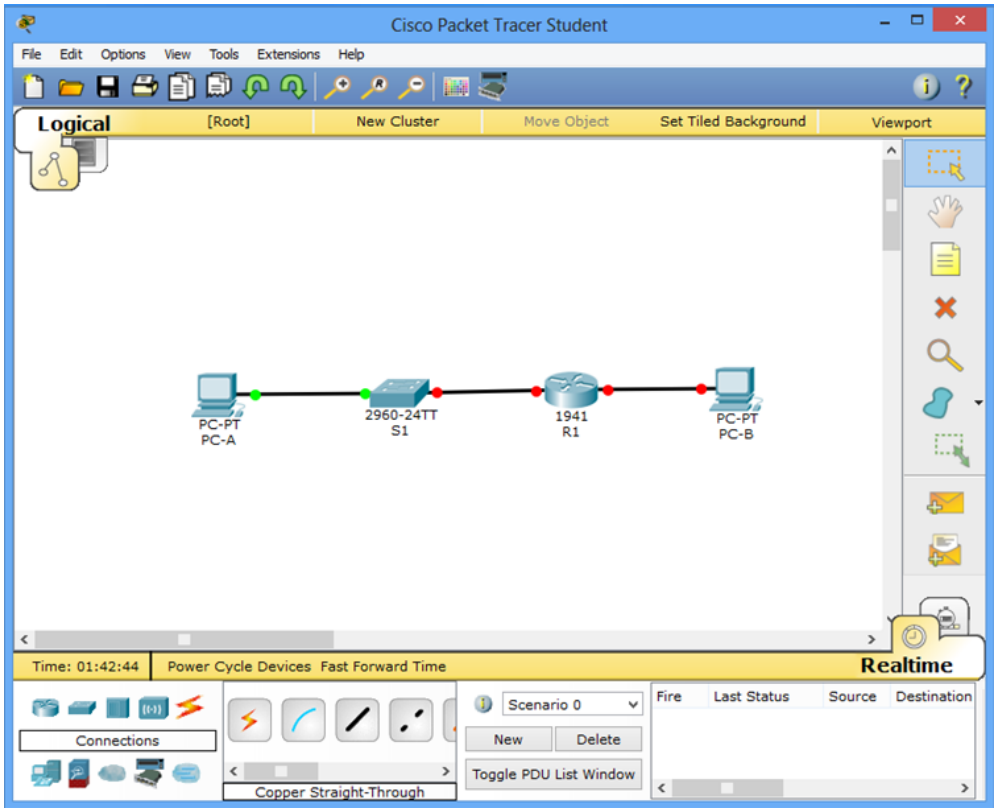
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 1: establecer la topología e inicializar los dispositivos

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

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

b. Encienda todos los dispositivos de la topología.



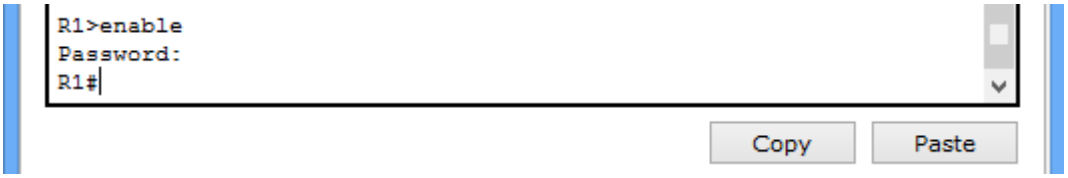
Paso 2. Inicializar y volver a cargar el router y el switch.

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

Inicializar y volver a cargar el router.

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

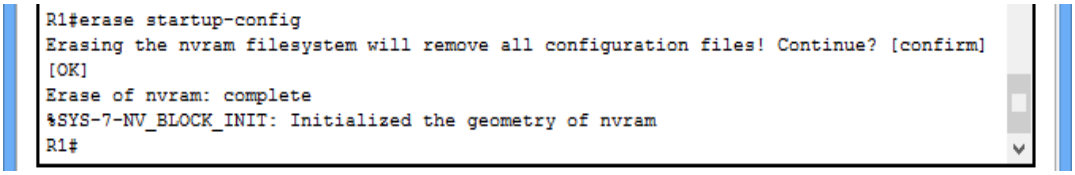
```
Router> enable
Router#
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

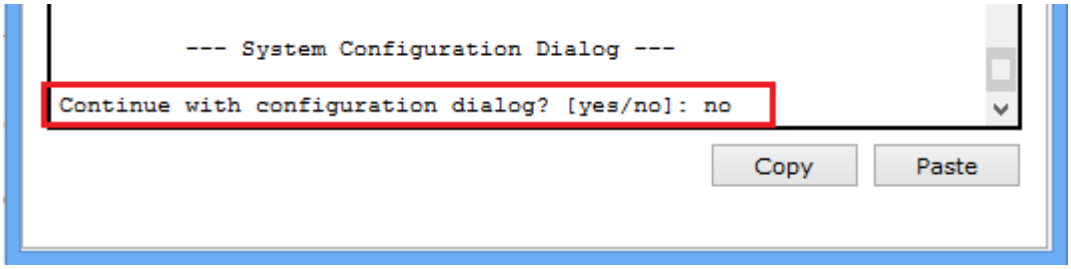


c. Emita el comando **reload** para eliminar una configuración antigua de la memoria. Cuando reciba el mensaje **Proceed with reload** (Continuar con la recarga), presione Enter para confirmar. (Si presiona cualquier otra tecla, se cancela la recarga).

```
Router# reload
Proceed with reload? [confirm]
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.
```

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

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

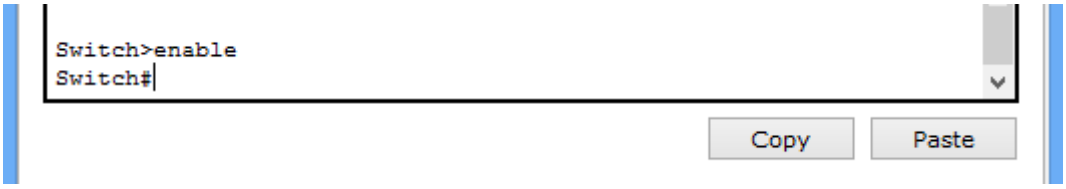


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Inicializar y volver a cargar el switch.

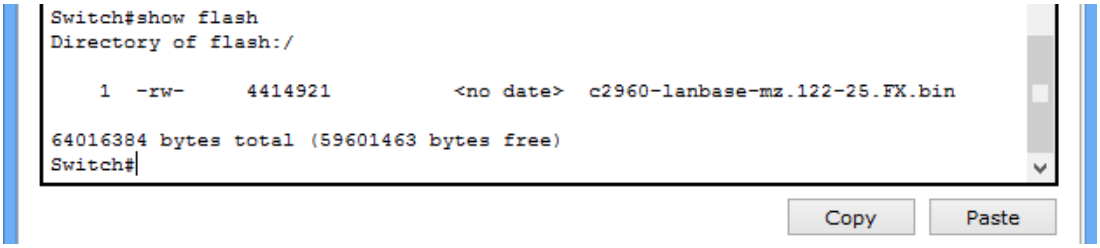
a. Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.

```
Switch> enable
Switch#
```



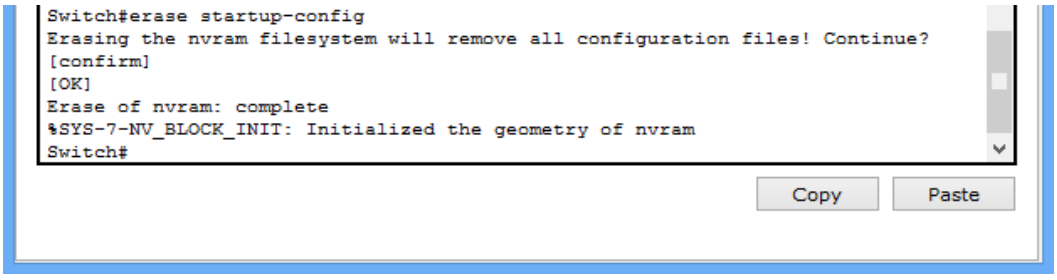
b. Utilice el comando **show flash** para determinar si se crearon VLAN en el switch.

```
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. 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).

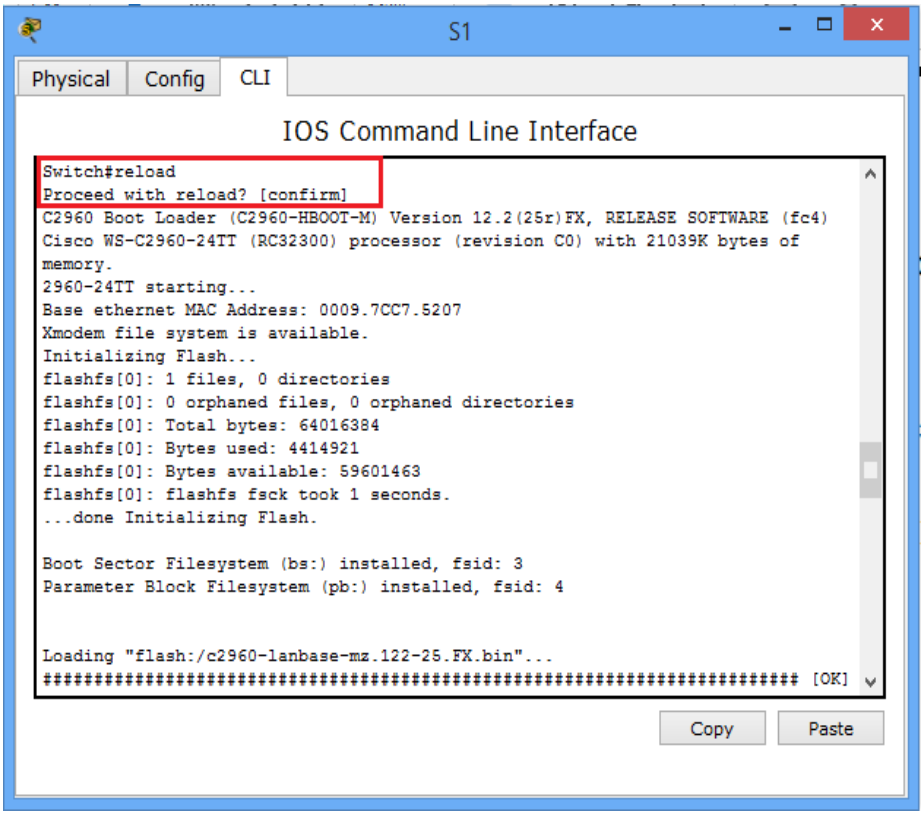
```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

d. 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.

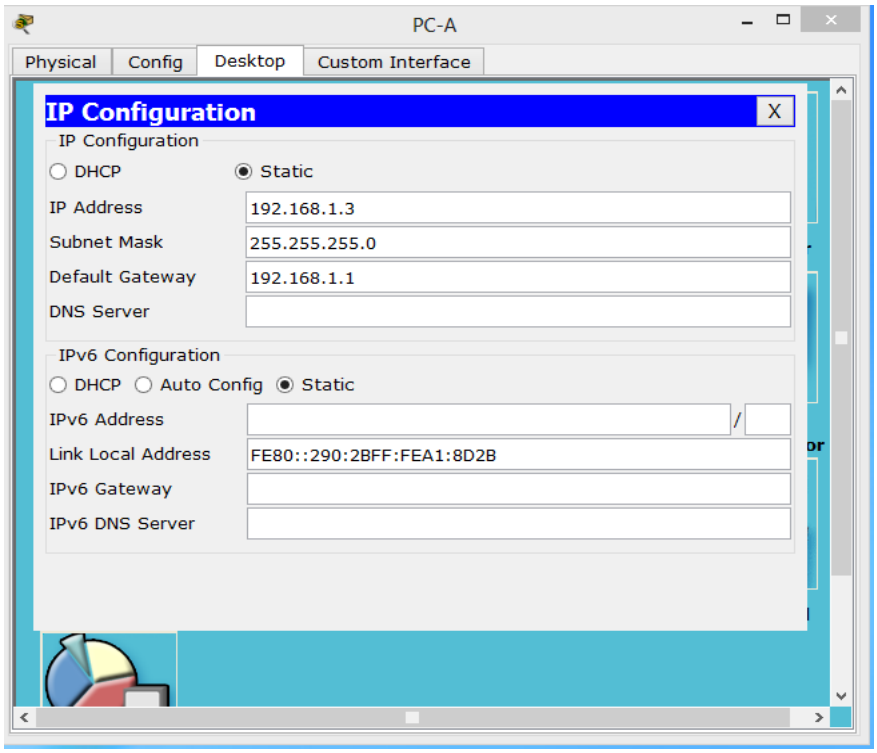
```
System configuration has been modified. Save? [yes/no]: no
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

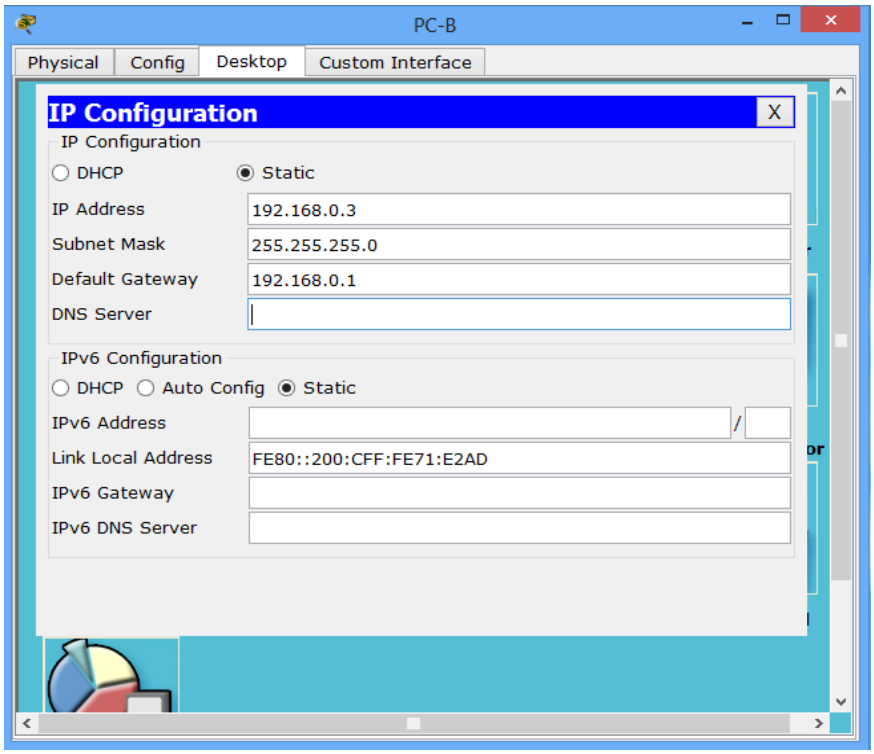
Parte 2: Configurar dispositivos y verificar la conectividad

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.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 2. Configurar el router.

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

```
Router> enable
Router#
```

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 10
```

b. Ingrese al modo de configuración global.

```
Router# config terminal
Router(config)#
```

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 10
```

c. Asigne un nombre de dispositivo al router.

```
Router(config)# hostname R1
```

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 10
```

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
```

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 10
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 10
```

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

Usando letras mayúsculas, números, caracteres especiales en todos los passwords

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

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

```
R1(config)#enable secret cisco12345
R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
```

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)#
```

```
R1(config)#enable secret cisco12345
R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#exec-timeout 5 0
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exit
```

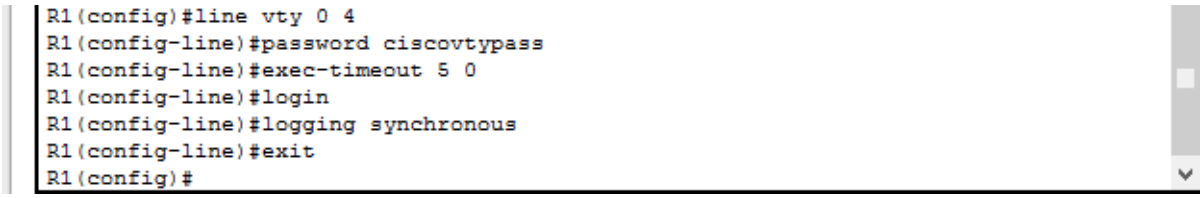
Para el comando **exec-timeout**, ¿qué representan el **5** y el **0**?

La sesión expira en 5 minutos y 0 segundos

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

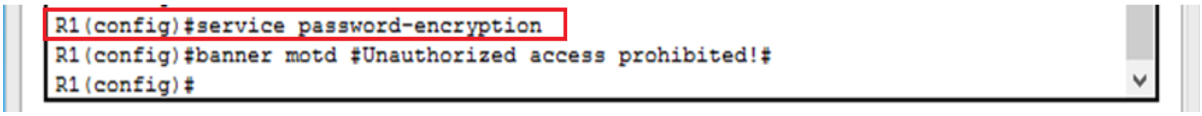
h. Asigne **ciscovtypass** como la contraseña de vty, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous**.

```
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)#
```



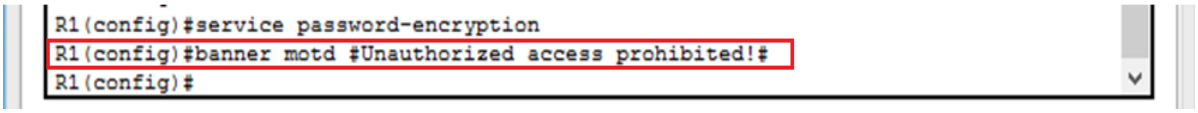
i. Cifre las contraseñas de texto no cifrado.

```
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.

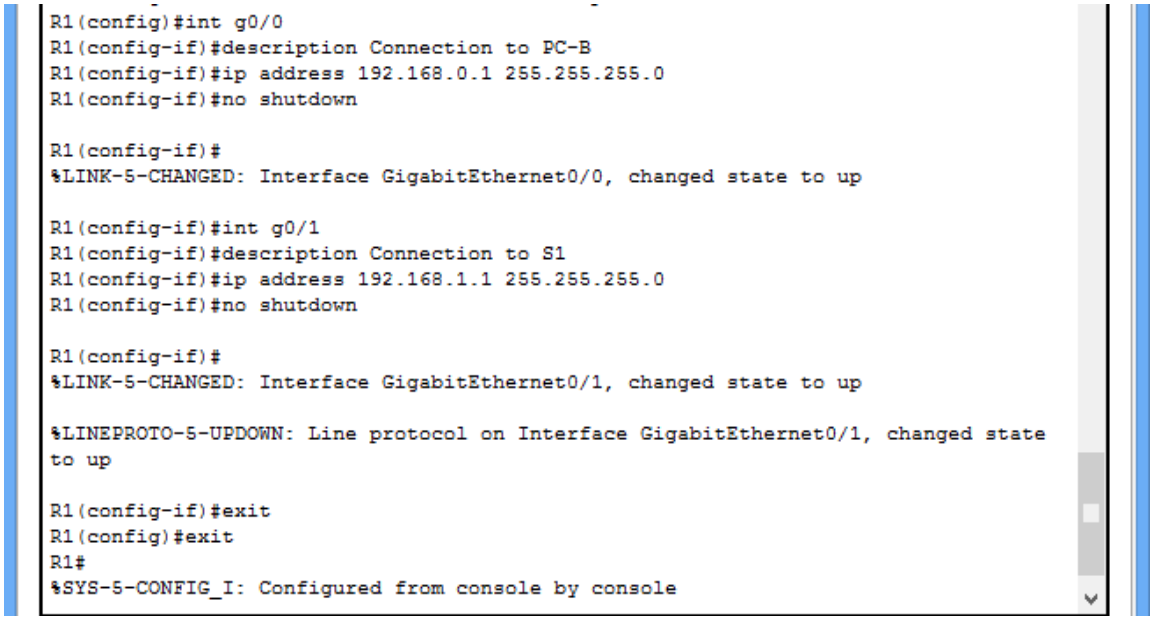
```
R1(config)# banner motd #Unauthorized access prohibited!#
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

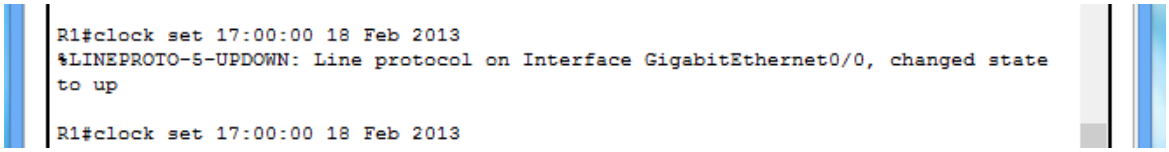
```
R1(config)# int g0/0
R1(config-if)#  description  Connection  to  PC-B
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# int g0/1
R1(config-if)#  description  Connection  to  S1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown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



```
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)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

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

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

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

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

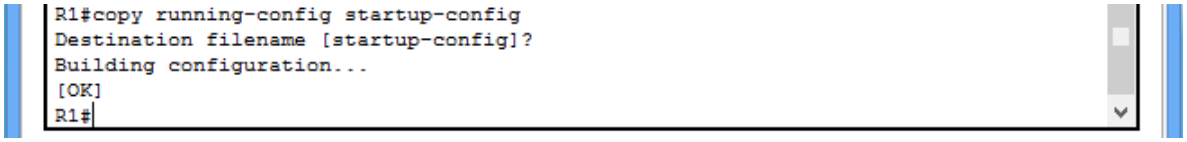


```
R1#clock set 17:00:00 18 Feb 2013
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state
to up

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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#
```

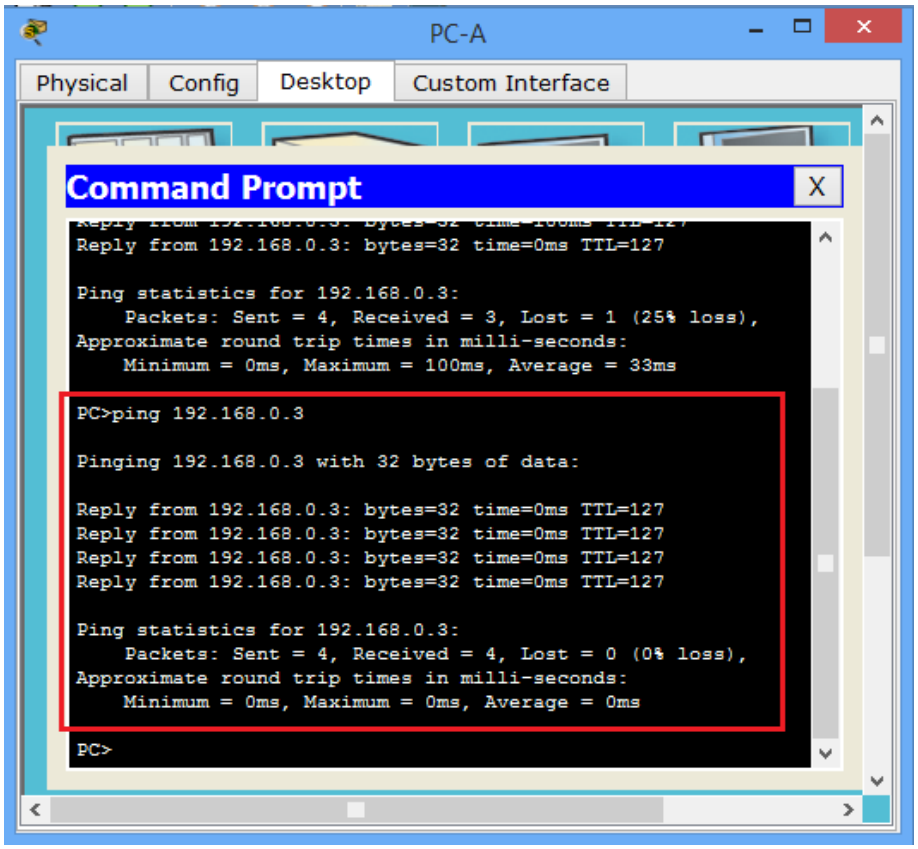


¿Qué resultado obtendría al volver a cargar el router antes de completar el comando **copy running-config startup-config**?

Si no guardamos lo de la RAM en la NVRAM, al reiniciar el router se perdería todo, porque ésta se borra al a pagar o reiniciar le router.

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

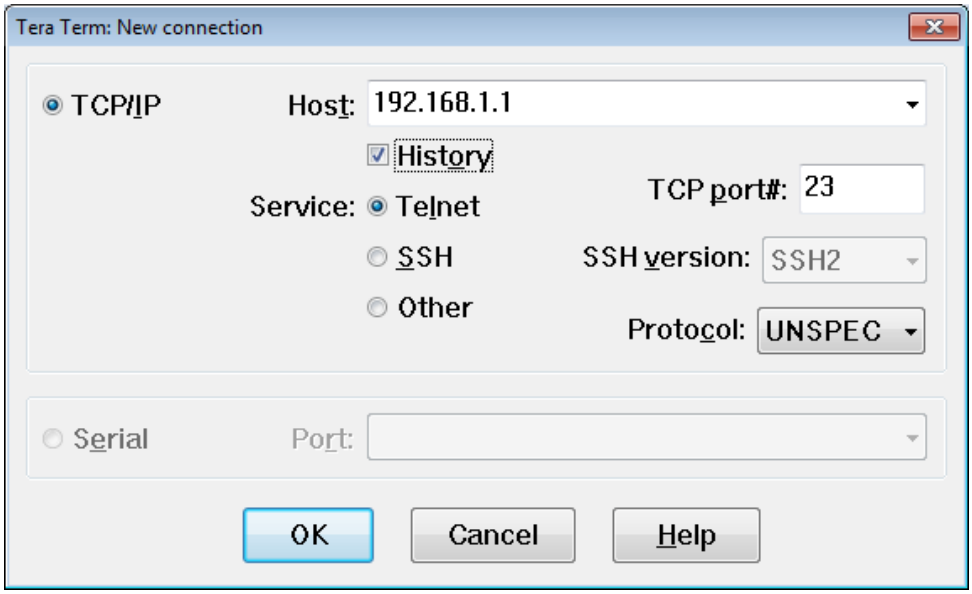
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

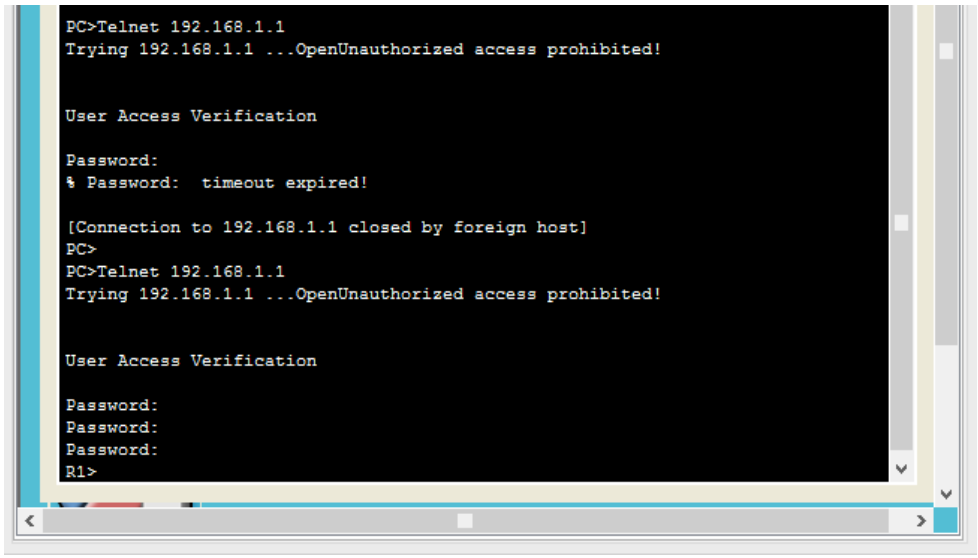
Después de completar esta serie de comandos, ¿qué tipo de acceso remoto podría usarse para acceder al R1?

Es decir el router como se configura a las dos interfaces ya puede conectar las dos redes. Mediante el cliente de Telnet de Tera Term.

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?

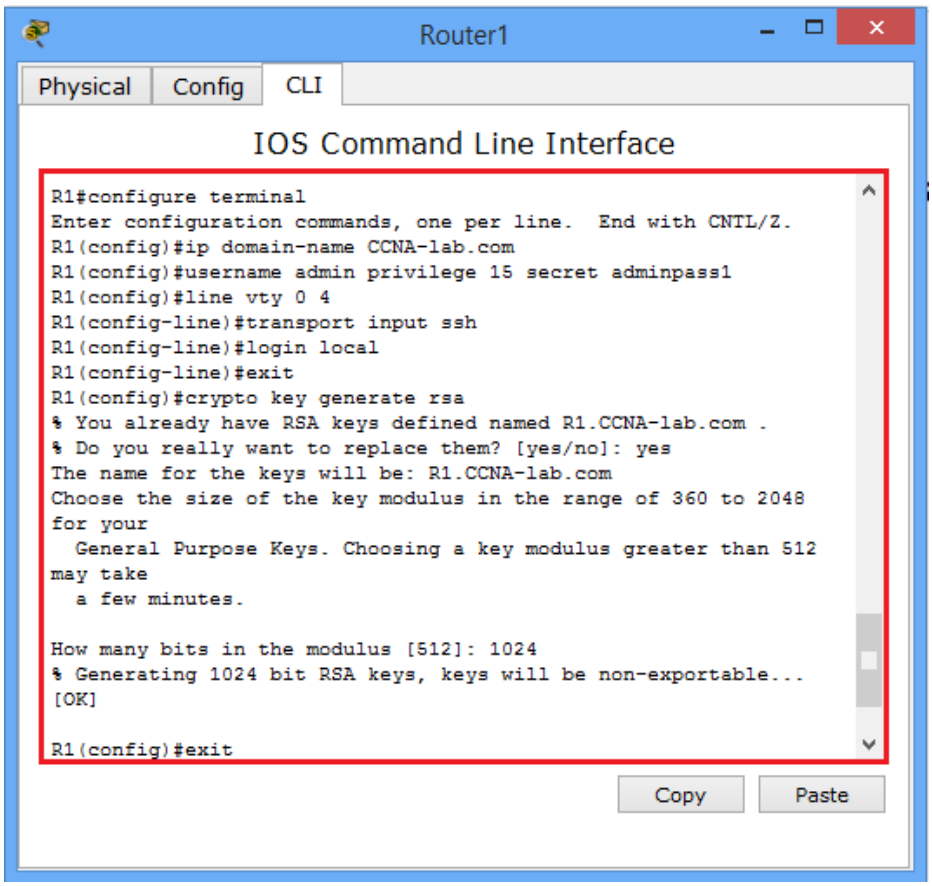
Una sesión Telnet se puede ver en texto plano. No está encriptada. Las contraseñas se pueden ver fácilmente usando un paquete sniffer.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

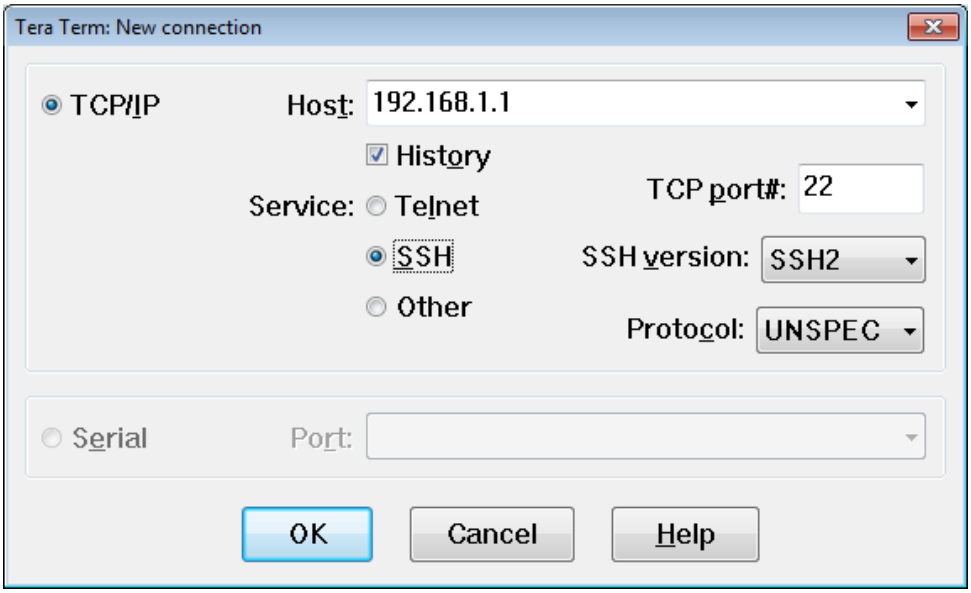
```
R1# configure terminal
R1(config)# ip domain-name CCNA-lab.com
R1(config)# username admin privilege 15 secret adminpass1
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)#     login     local
R1(config-line)# exit
R1(config)# crypto key generate rsa modulus 1024
R1(config)#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

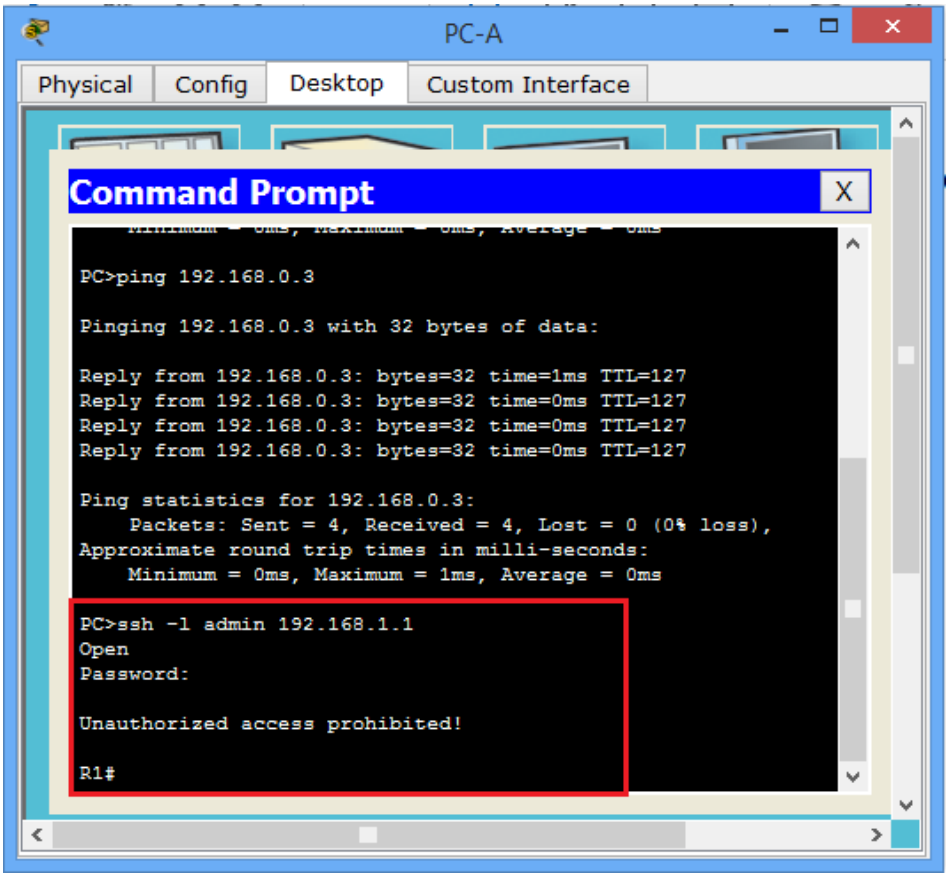


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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? Si

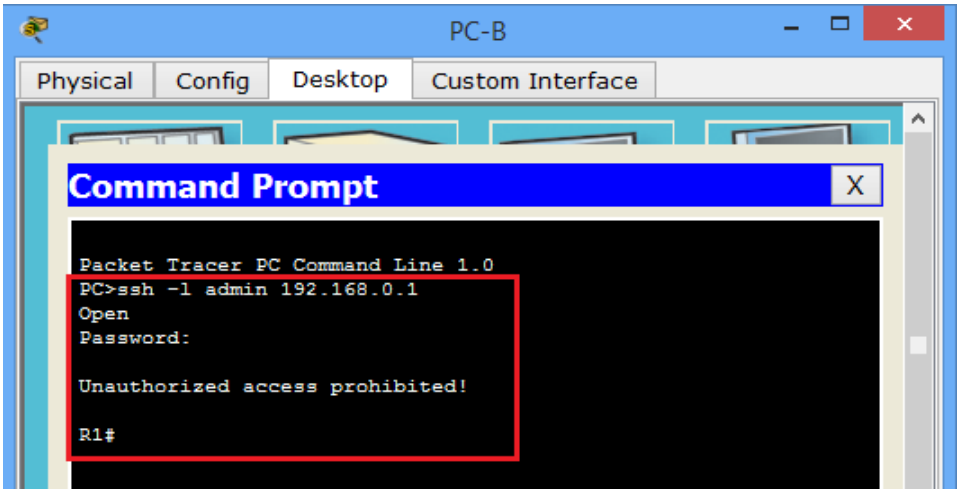
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 3: mostrar la información del router

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

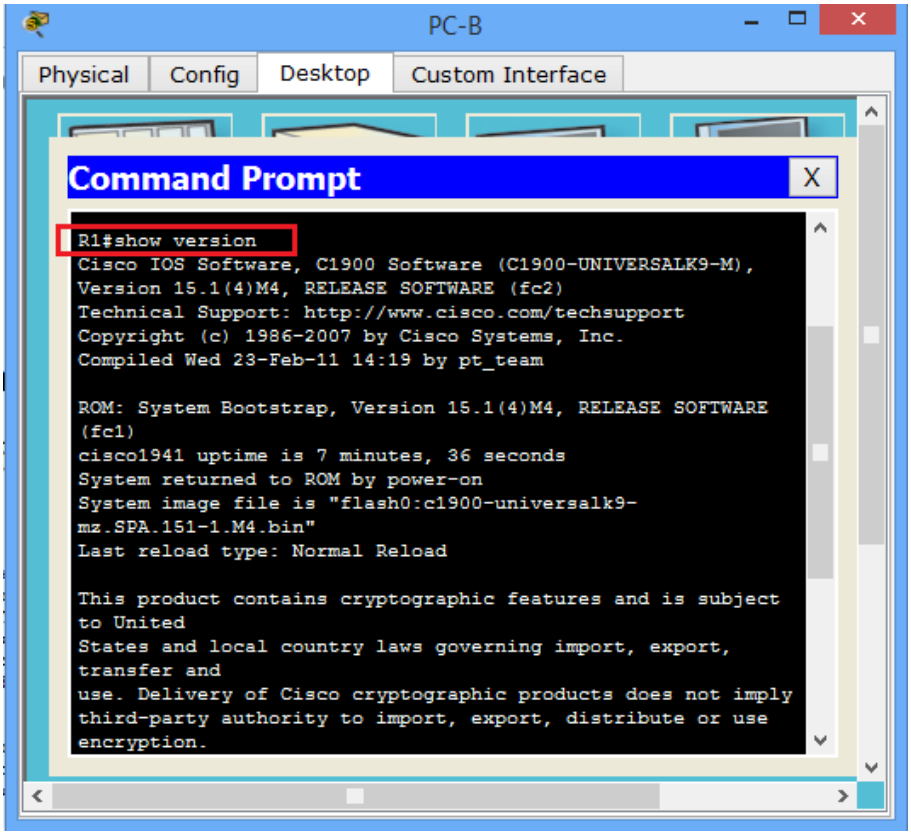
Paso 1. establecer una sesión SSH para el R1.

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.

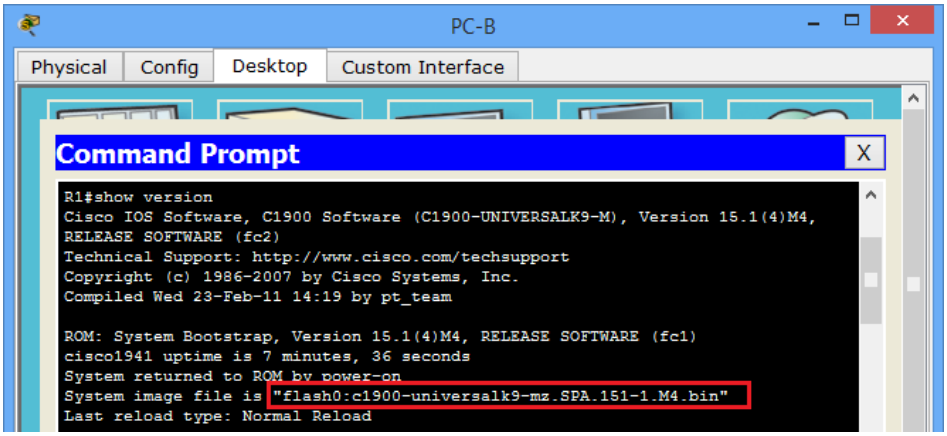
a. Use el comando **show version** para responder preguntas sobre el router.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

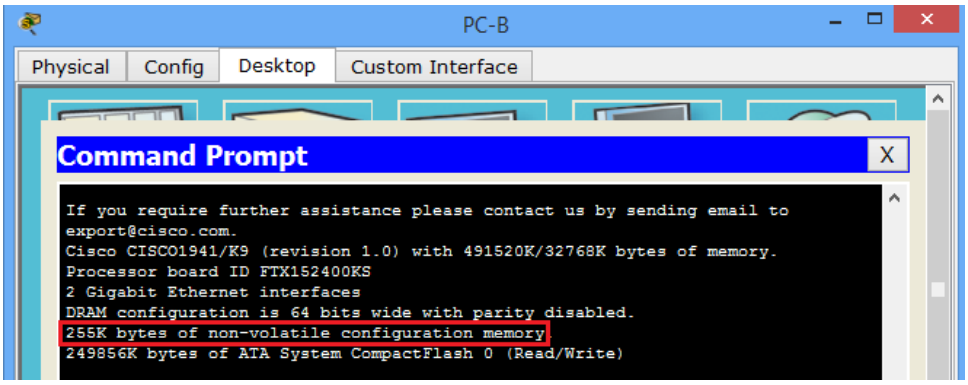
¿Cuál es el nombre de la imagen de IOS que el router está ejecutando?

flash0:c1900-universalk9-mz.SPA.151-1.M4.bin



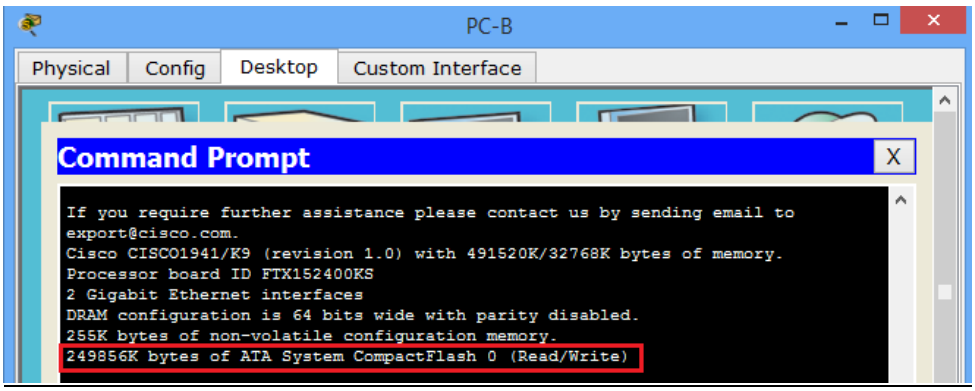
¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) tiene el router?

255K bytes of non-volatile configuration memory



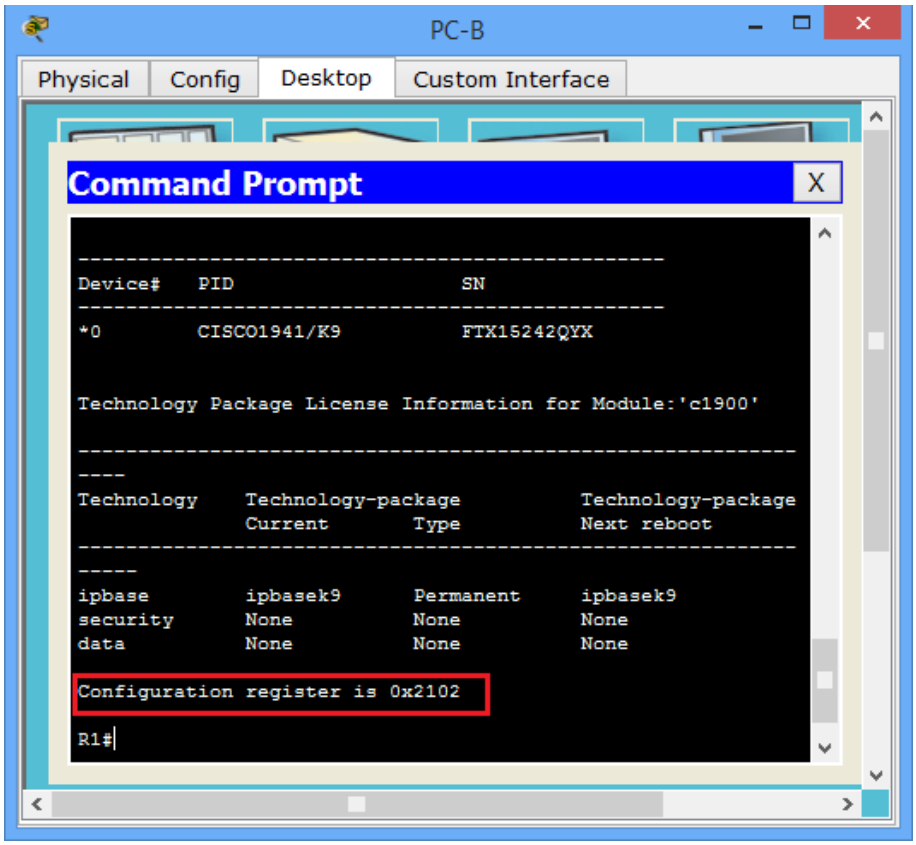
¿Cuánta memoria flash tiene el router?

249856K bytes of ATA System CompactFlash



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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?

En la mayoría de los casos (0x2102), el enrutador experimentará un arranque normal, carga el IOS de la desde la memoria Flash y carga la configuración de inicio de la NVRAM. Si el registro de configuración es 0x2142, el enrutador omitirá la configuración de inicio y comenzará en el símbolo del sistema de modo de usuario. Si falla el arranque inicial, el enrutador pasa al modo ROMMON.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

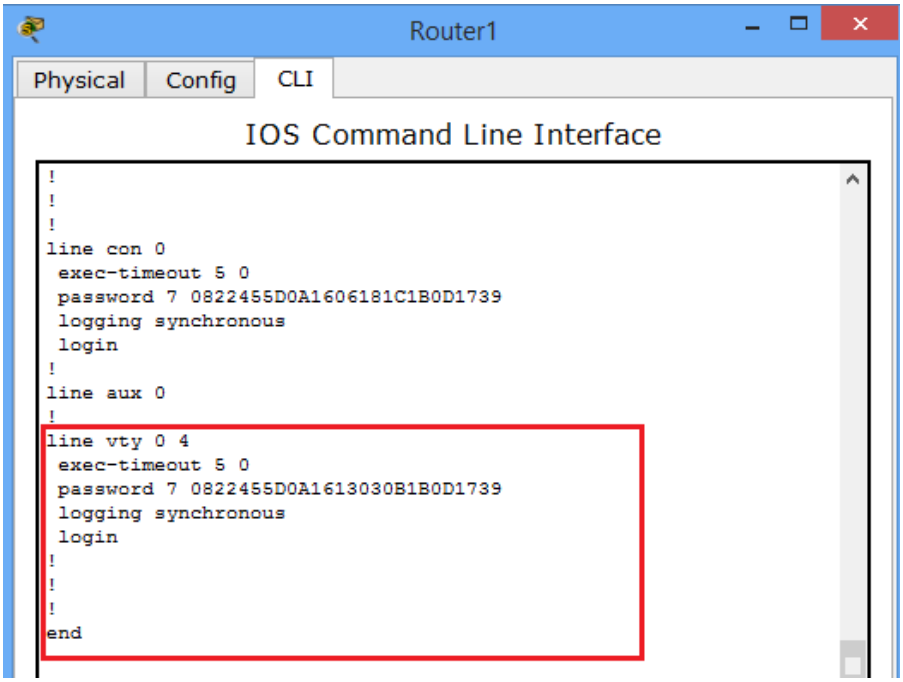
Paso 3. Mostrar la configuración de inicio.

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

¿De qué forma figuran las contraseñas en el resultado?

Están todos los passwords encriptados por lo que aparecen caracteres de símbolo, letras y números.

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



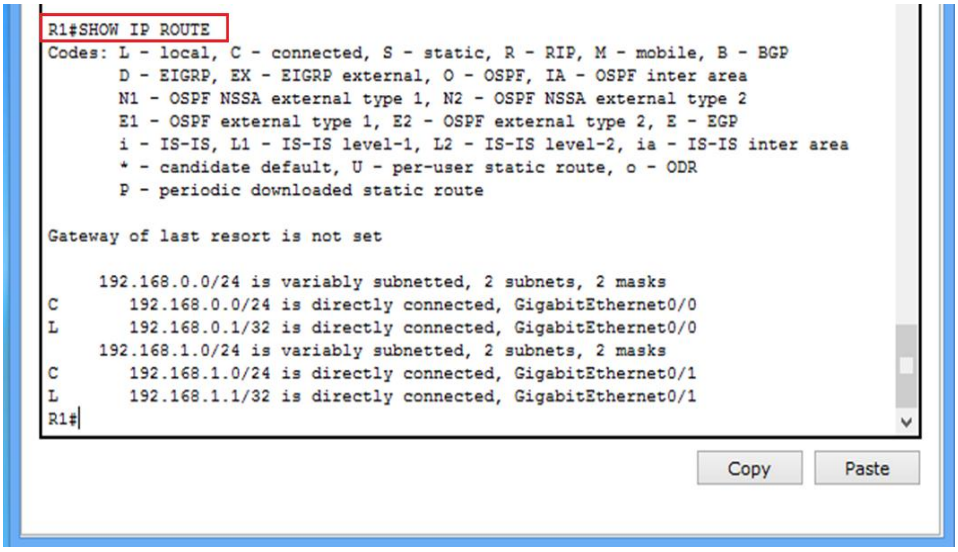
¿Qué resultado se obtiene al usar este comando?

El usuario recibe la configuración de inicio que comienza con la línea que incluye la primera instancia de expresión de filtrado

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

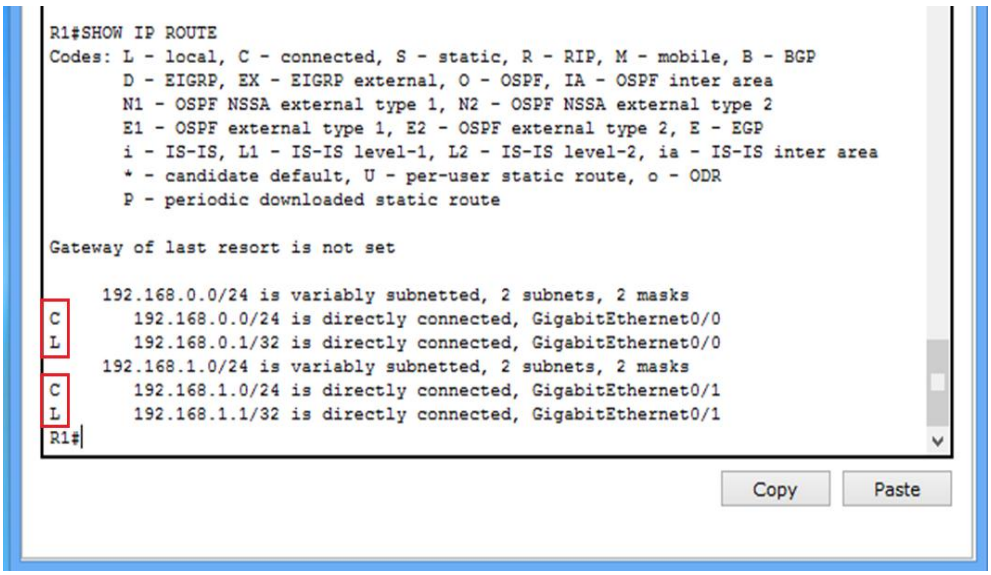
Paso 4. Mostrar la tabla de routing en el router.

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



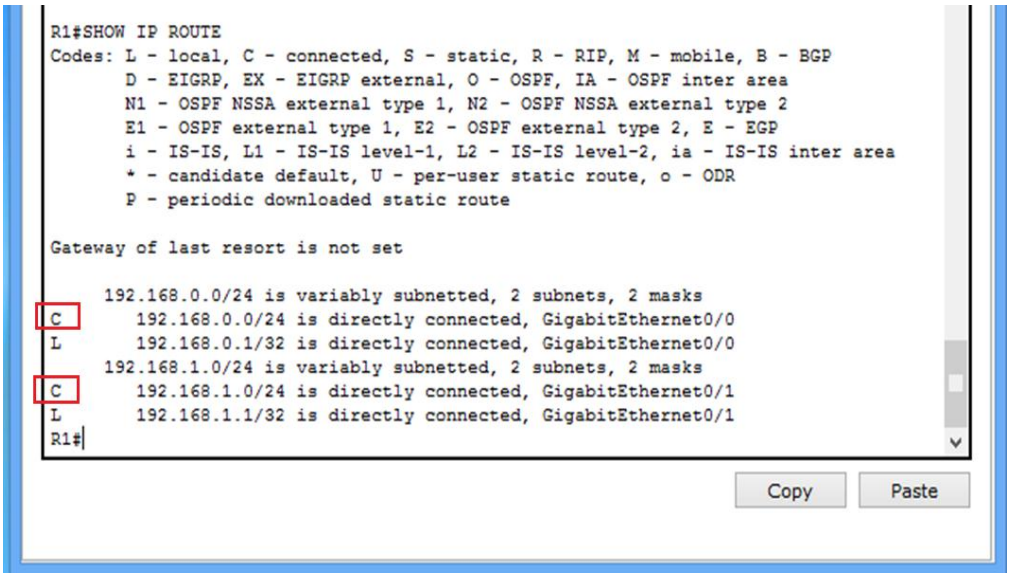
¿Qué código se utiliza en la tabla de routing para indicar una red conectada directamente?

La C designa una subred conectada directamente. La L designa una interfaz local.



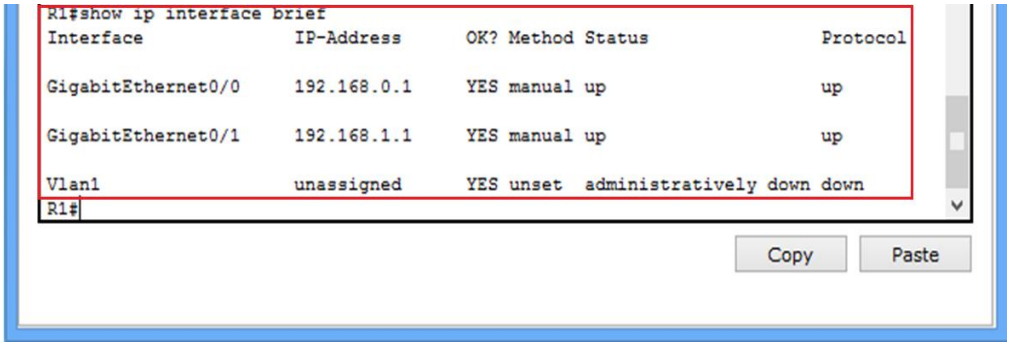
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

¿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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

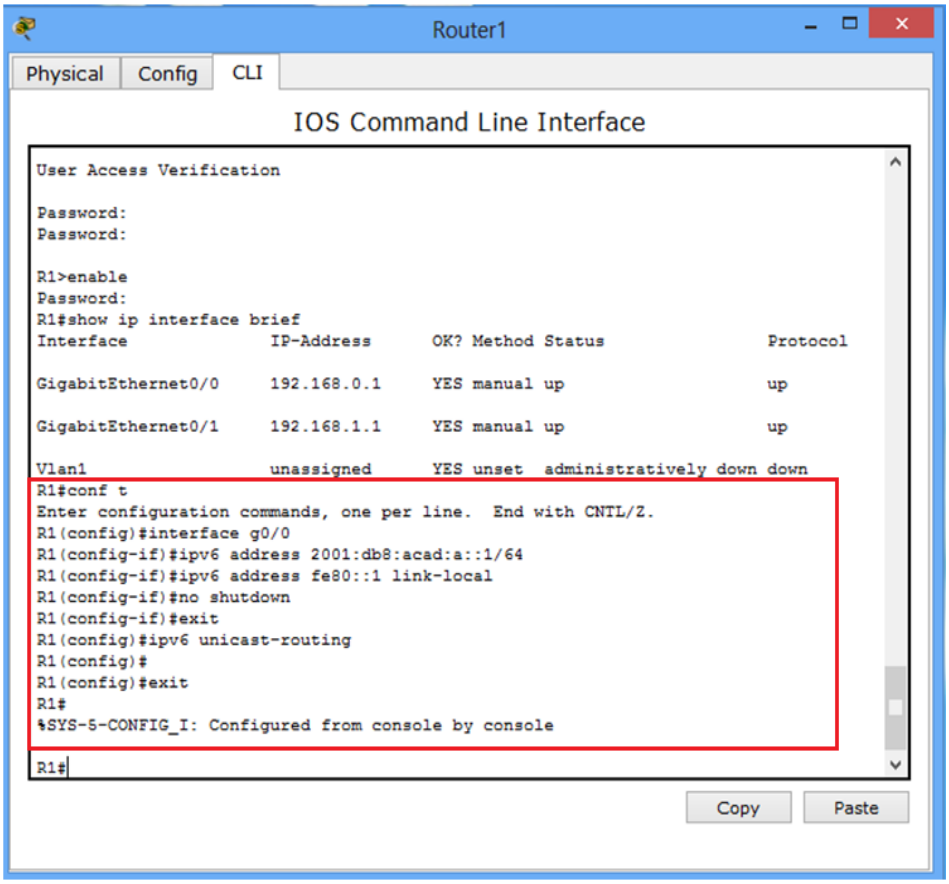
Parte 4: configurar IPv6 y verificar la conectividad

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
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

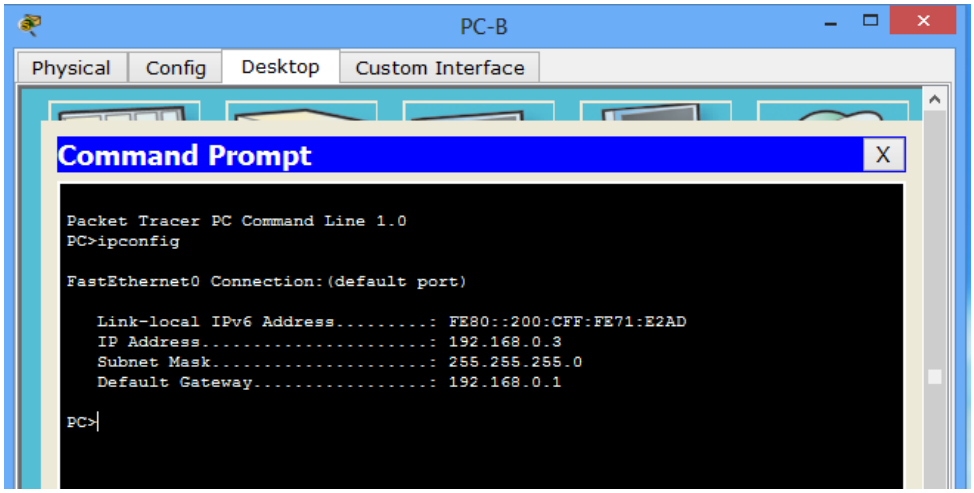
Si no se asignó una dirección IPv6 a la G0/1, ¿por qué se indica como [up/up]?

El estado [up / up] refleja el estado de Capa 1 y Capa 2 de la interfaz y no refleja el estado de la Capa 3.

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

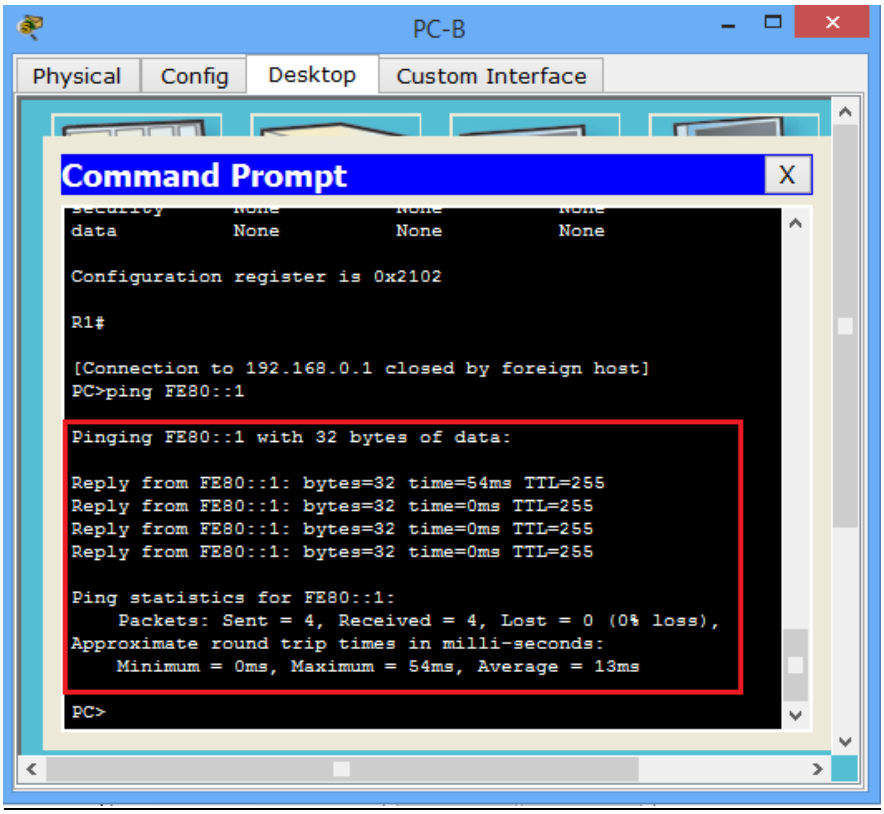
¿Cuál es la dirección IPv6 asignada a la PC-B? FE80::200:CFF:FE71:E2AD

¿Cuál es el gateway predeterminado asignado a la PC-B? 192.168.0.1

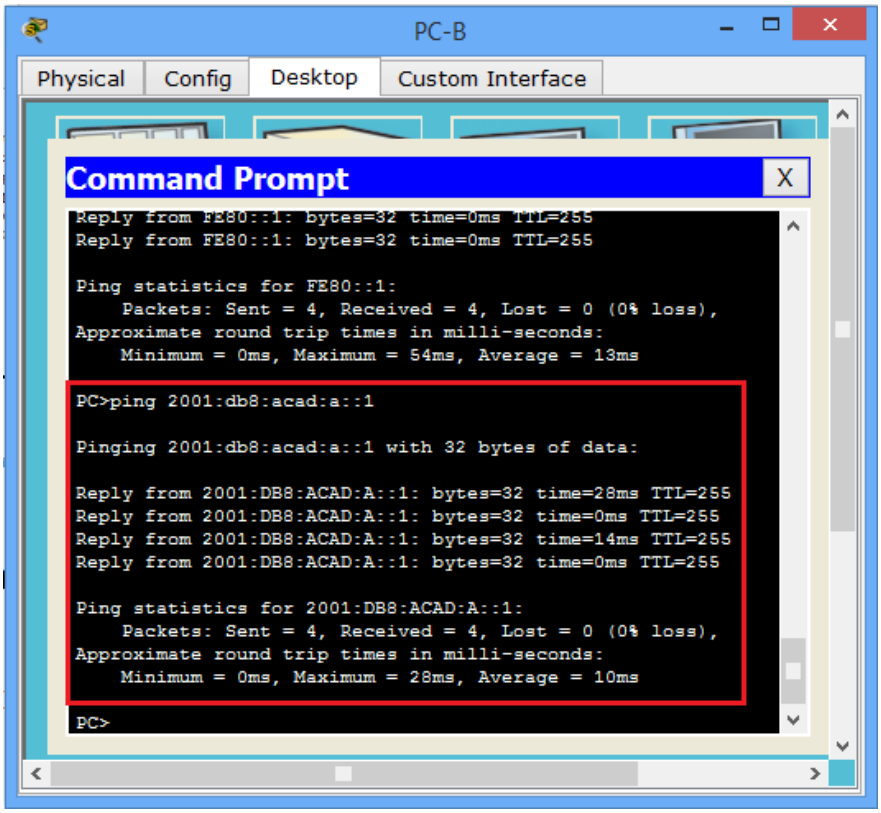


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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? Si



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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 proporcionaría la información.

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 startup-config o show running-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?

   El ping fallaría porque la interfaz R1 G0/1 no estaba configurada con IPv6 y PC-A sólo tiene una dirección 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.				

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 8

- Configuración de los parámetros básicos del router con la CLI del IOS.
- Con el desarrollo de ésta actividad se logró practicar y reconocer los procesos necesarios para establecer la topología e inicializar los dispositivos, de igual forma asignar su configuración, verificando el estado de la conectividad.
- Gracias a la práctica de esta actividad realizamos un reconocimiento de los comandos necesarios para mostrar la información del router; así como la configuración ipv6, verificando su conectividad.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

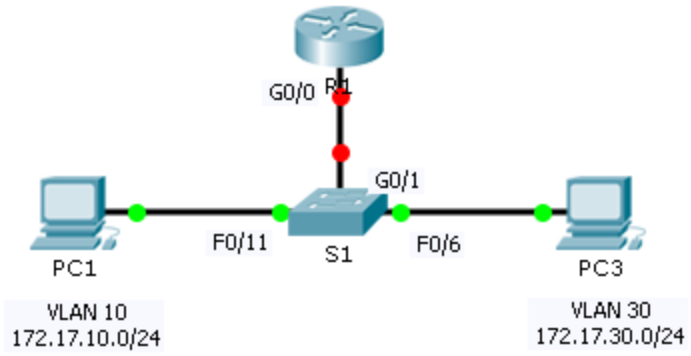
Informe 9: 4.1.4.7 Lab - Configuring Basic Router Settings with CCP

No se realiza de acuerdo a sugerencia de la tutora.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 10: 5.1.3.6 Packet Tracer - Configuring Router-on-a-Stick Inter-VLAN Routing

Topology



Addressing Table

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

Objectives

Part 1: Test Connectivity without Inter-VLAN Routing

Part 2: Add VLANs to a Switch

Part 3: Configure Subinterfaces

Part 4: Test Connectivity with Inter-VLAN Routing

Scenario

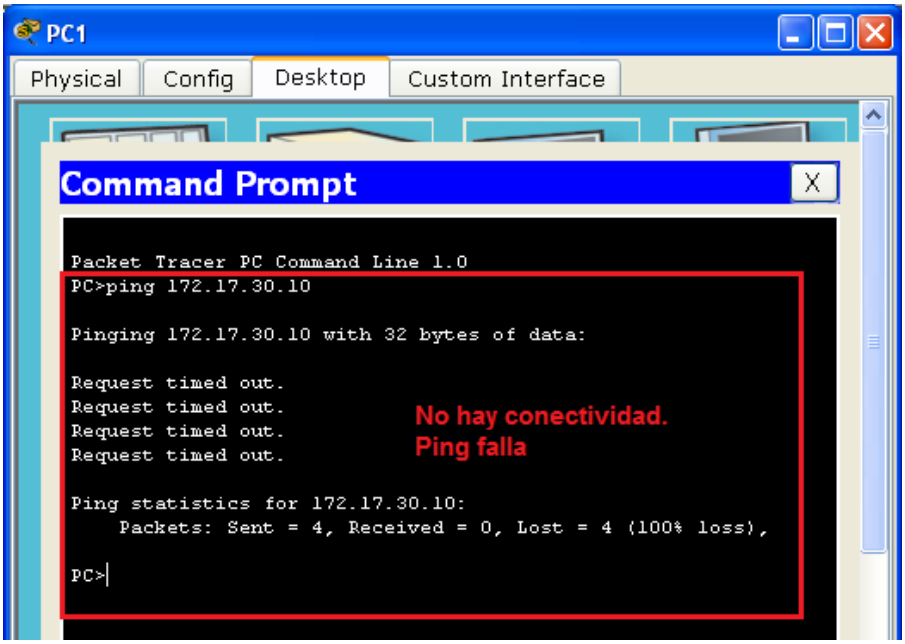
In this activity, you will check for connectivity prior to implementing inter-VLAN routing. You will then configure VLANs and inter-VLAN routing. Finally, you will enable trunking and verify connectivity between VLANs.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Part 1: Test Connectivity Without Inter-VLAN Routing

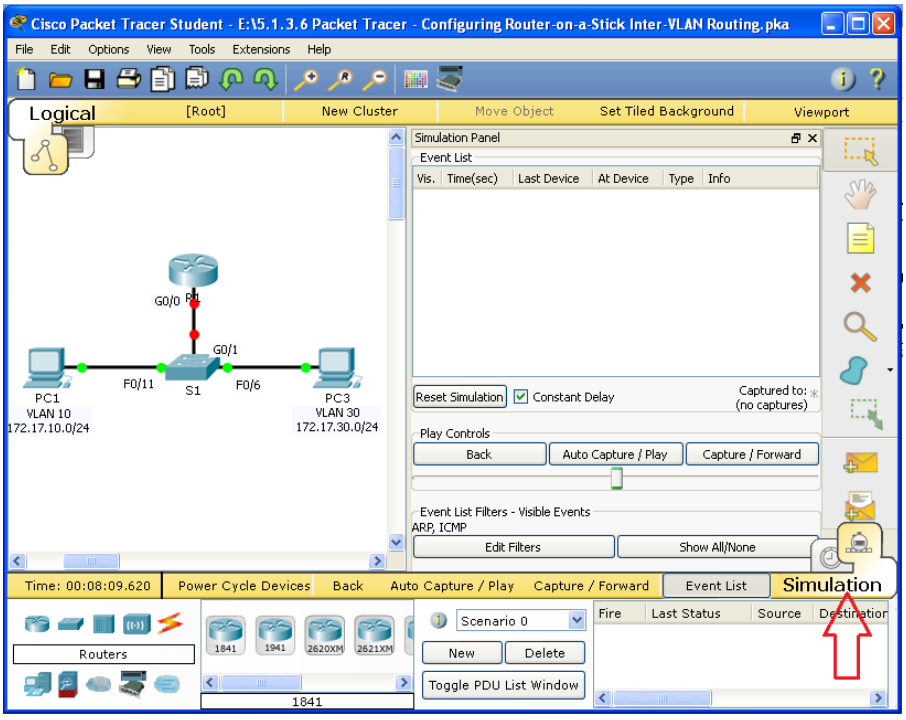
Step 1: Ping between PC1 and PC3.

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



Step 2: Switch to Simulation mode to monitor pings.

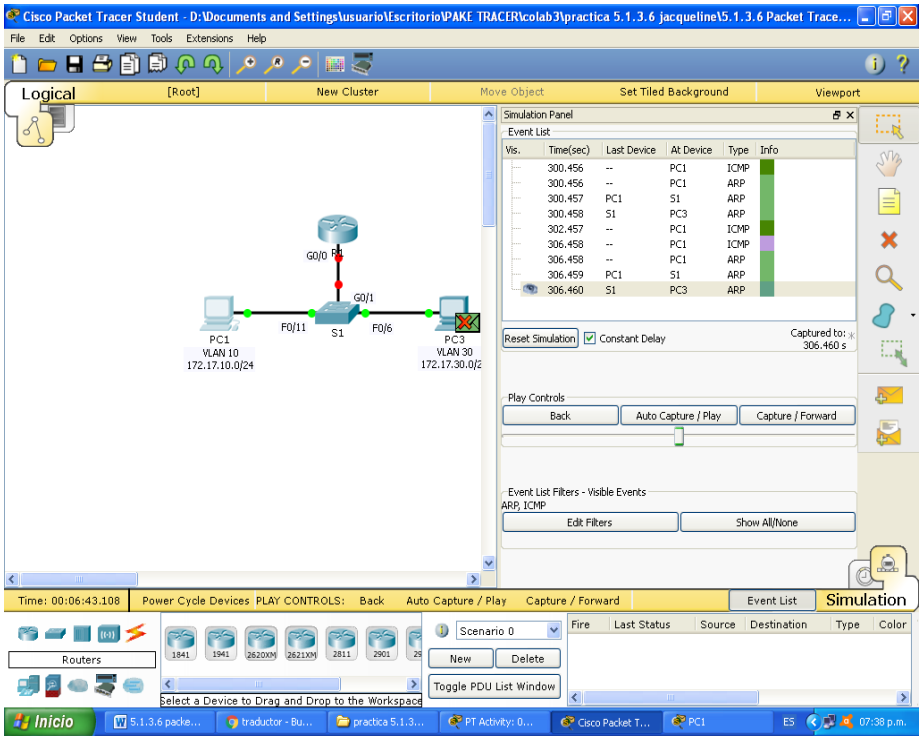
a. Switch to Simulation mode by clicking the **Simulation** tab or pressing **Shift+S**.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**. Notice how the ping never leaves **PC1**. What process failed and why? The ARP process failed because the ARP request was dropped by PC3. PC1 and PC3 are not on the same network, so PC1 never gets the MAC address for PC3. Without a MAC address, PC1 cannot create an ICMP echo request.

PC1 está en la VLAN10 Y PC3 está en la VLAN30. El proceso ARP falló porque la solicitud ARP se cayó en PC3. PC1 y PC3 no están en la misma red. PC1 nunca obtiene la dirección MAC para PC3. Sin una dirección MAC, PC1 no puede crear una solicitud de eco ICMP.

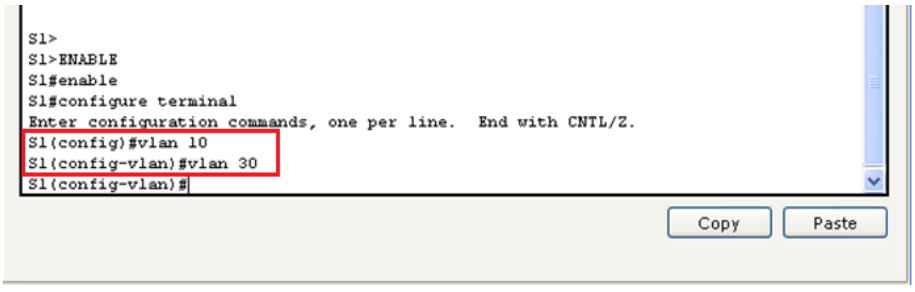


Part 2: Add VLANs to a Switch

Step 1: Create VLANs on S1.

Return to **Realtime** mode and create VLAN 10 and VLAN 30 on **S1**.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
```



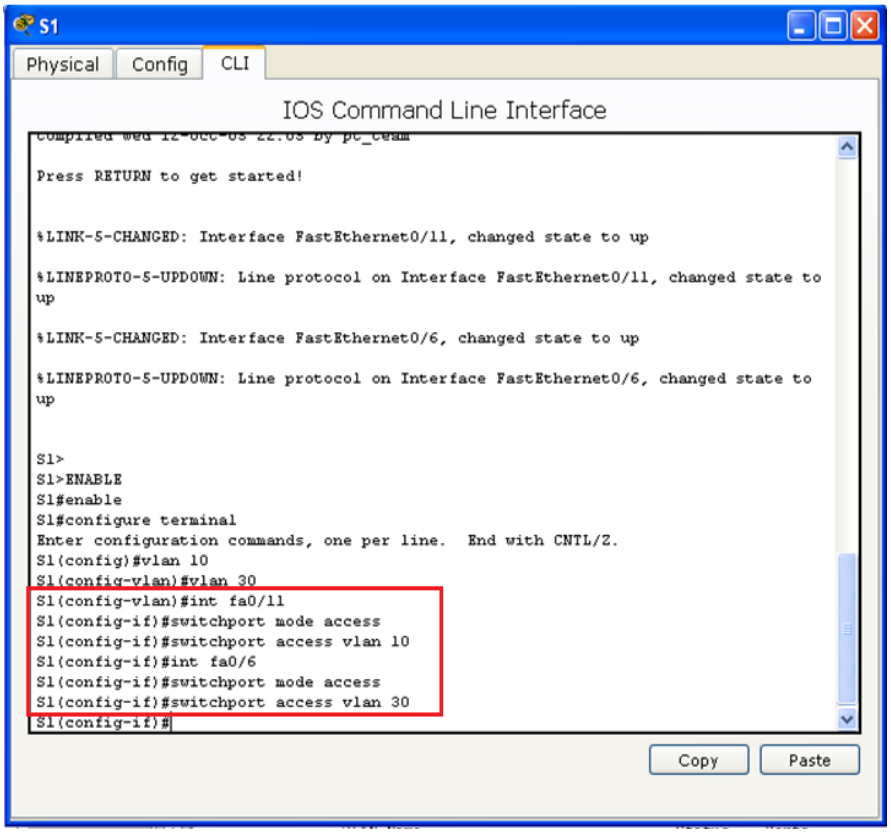
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Step 2: Assign VLANs to ports.

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

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

```
S1(config-vlan)# int fa0/11
S1(config-if)#  switchport  mode  access
S1(config-if)# switchport access vlan 10
S1(config-if)# int fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 30
```

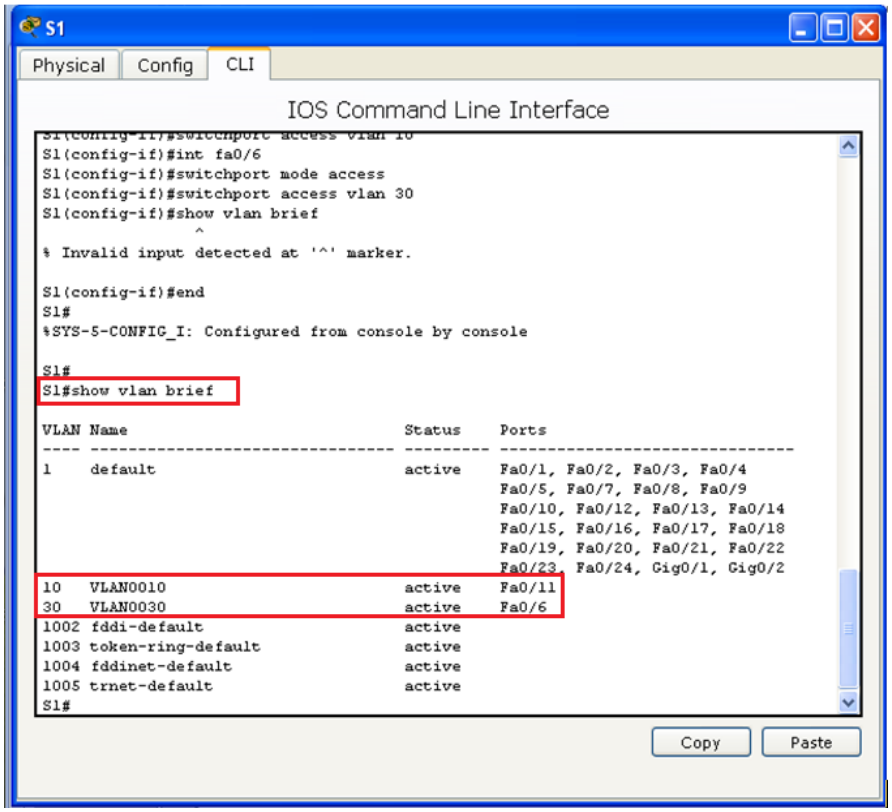


b. Issue the **show vlan brief** command to verify VLAN configuration.

```
S1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                                 Fa0/5,  Fa0/7,  Fa0/8,  Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/11
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

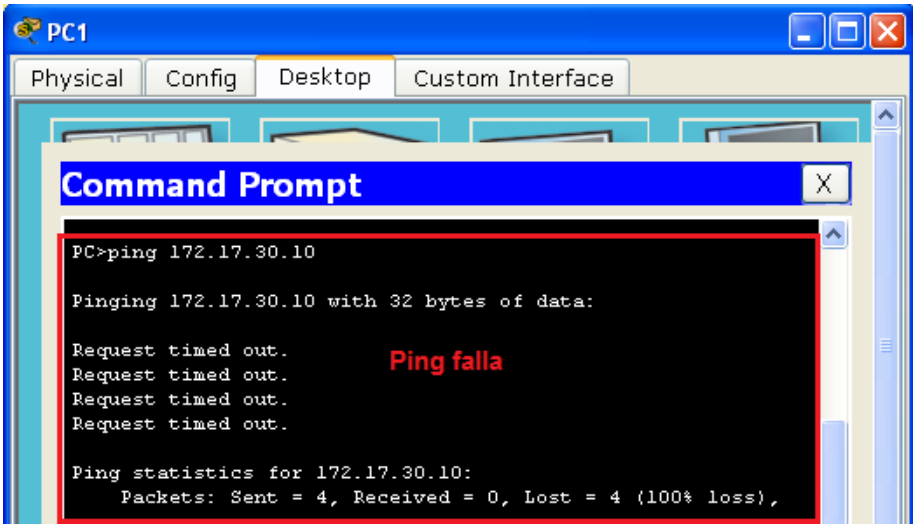
```
30   VLAN0030                         active    Fa0/6
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```



Step 3: Test connectivity between PC1 and PC3.

From **PC1**, ping **PC3**. The pings should still fail. Why were the pings unsuccessful? Each VLAN is a separate network and requires a router or a layer 3 switch to provide communication between them.

Cada VLAN es una red separada y requiere un router o un switch de capa 3 para proporcionar comunicación entre ellos.



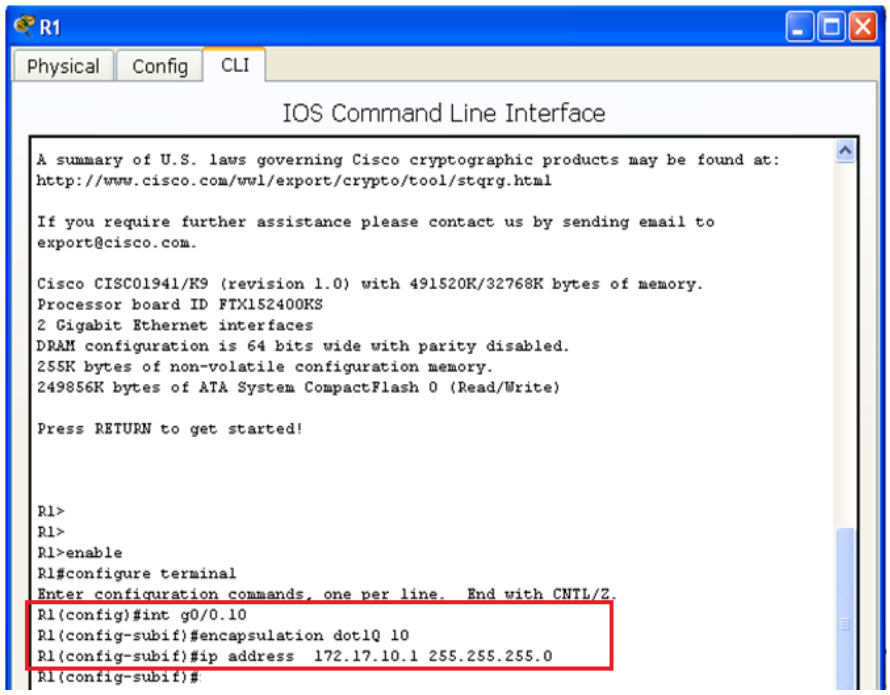
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Part 3: Configure Subinterfaces

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

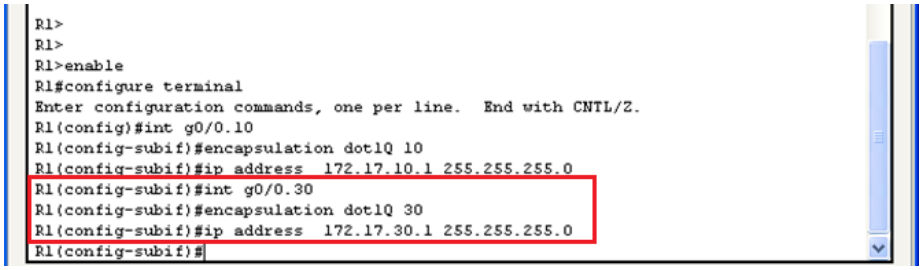
a. Create the subinterface G0/0.10.

- Set the encapsulation type to 802.1Q and assign VLAN 10 to the subinterface.
- Refer to the **Address Table** and assign the correct IP address to the subinterface.



b. Repeat for the G0/0.30 subinterface.

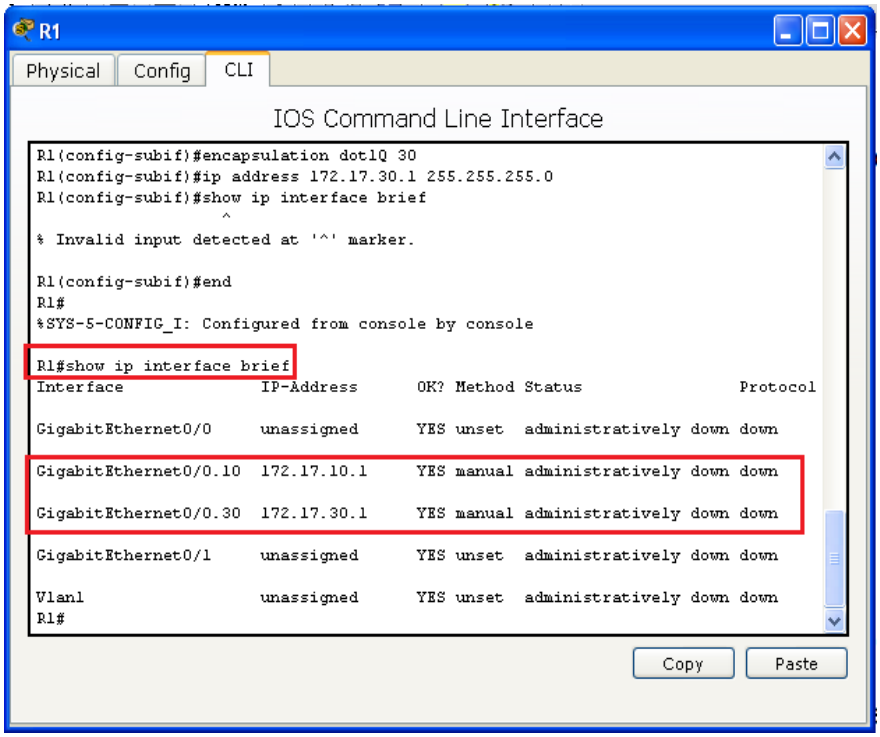
```
R1(config)# int g0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# int g0/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
```



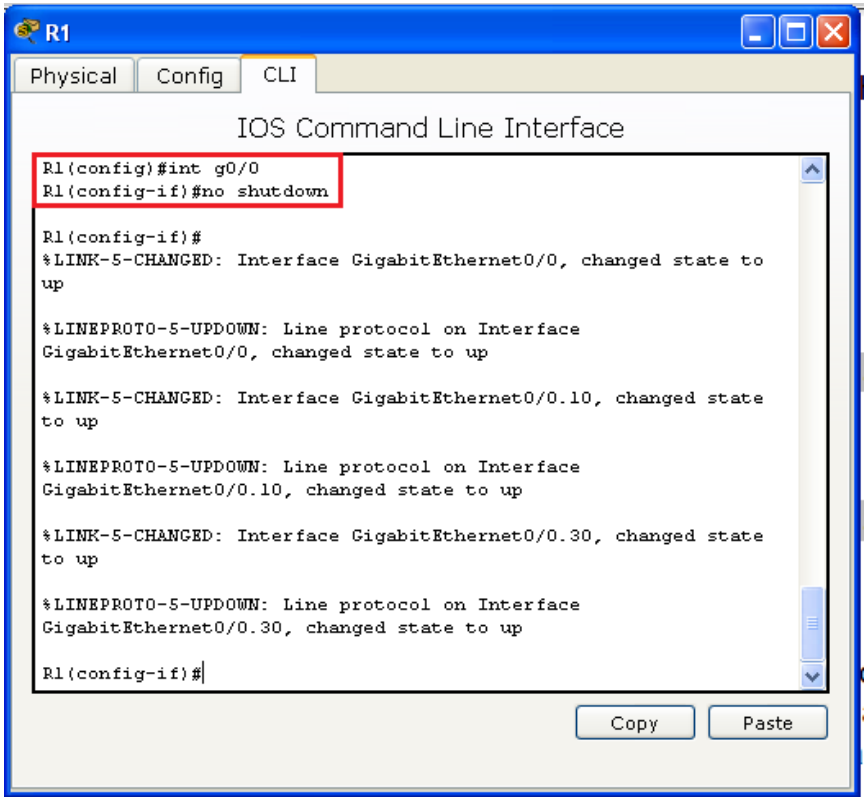
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Step 2: Verify Configuration.

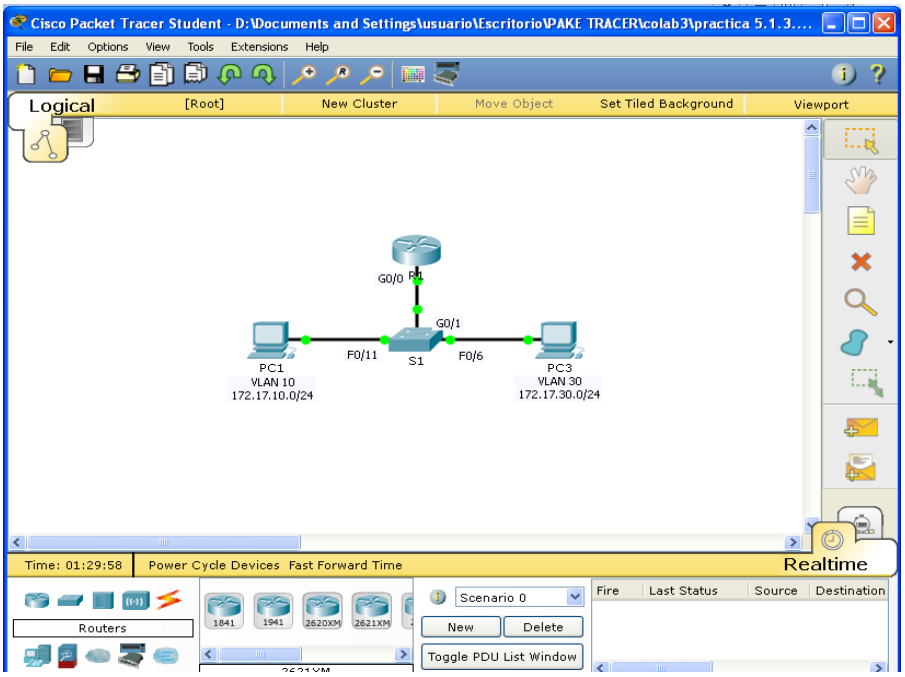
a. Use the **show ip interface brief** command to verify subinterface configuration. Both subinterfaces are down. Subinterfaces are virtual interfaces that are associated with a physical interface. Therefore, in order to enable subinterfaces, you must enable the physical interface that they are associated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



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



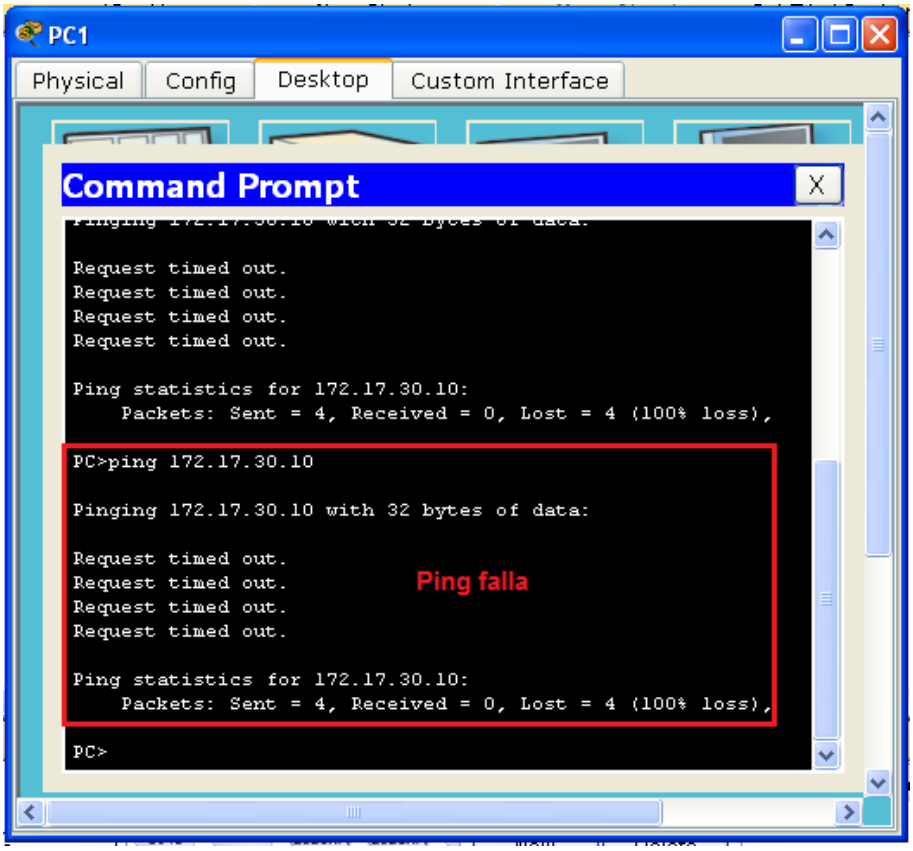
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



Part 4: Test Connectivity with Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

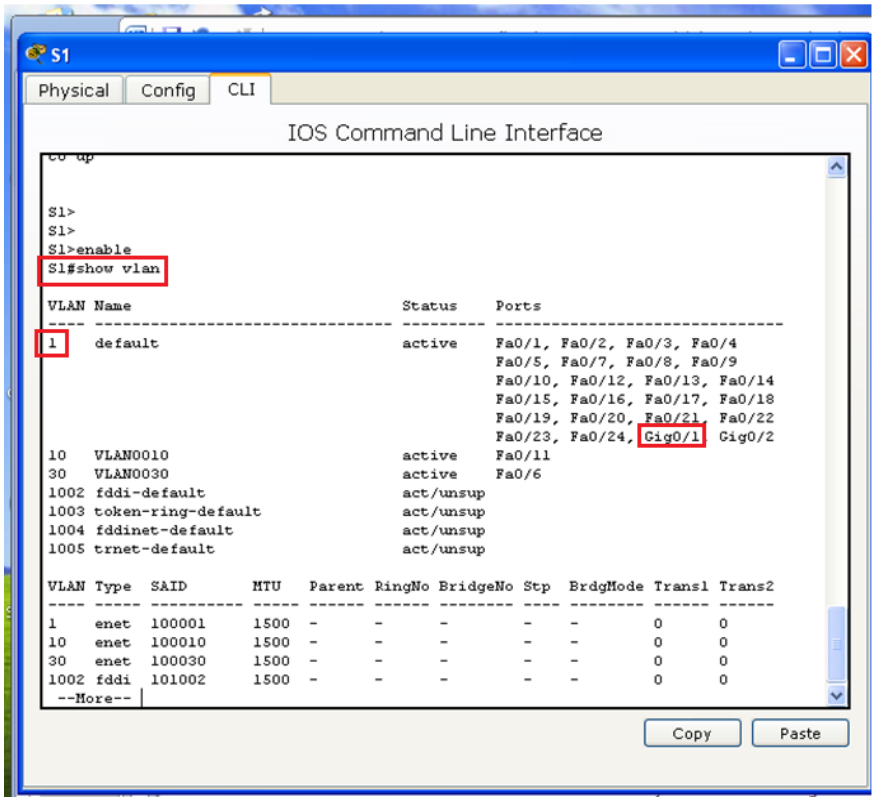
From **PC1**, ping **PC3**. The pings should still fail.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

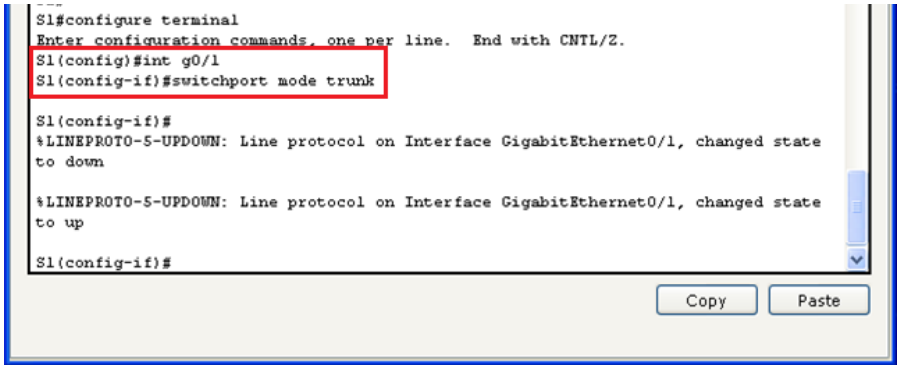
Step 2: Enable trunking.

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



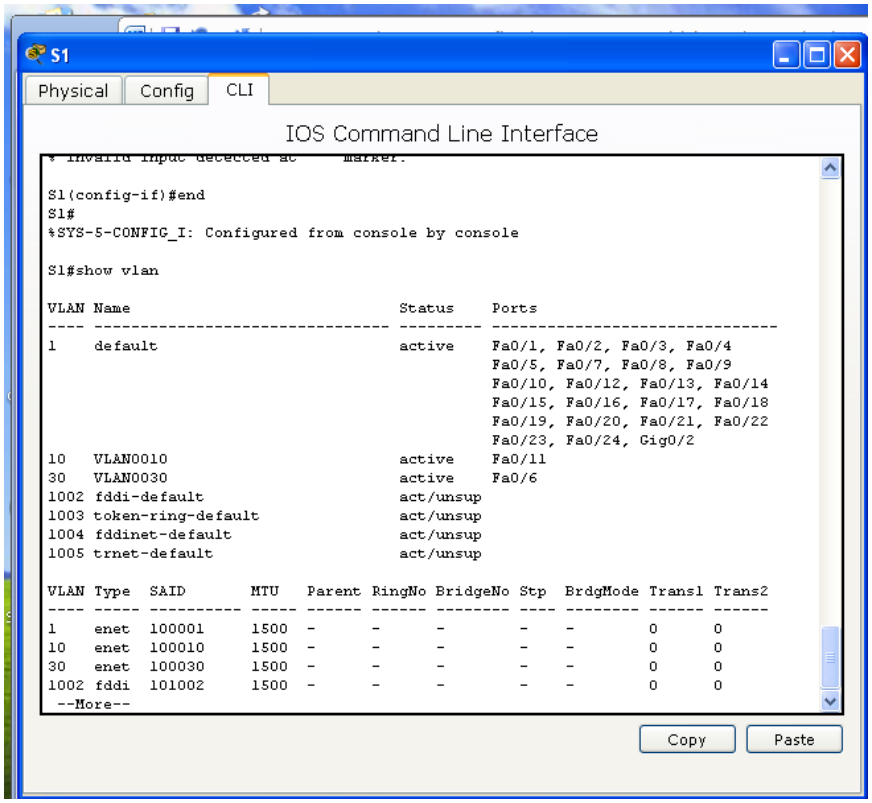
b. Because the router was configured with multiple subinterfaces assigned to different VLANs, the switch port connecting to the router must be configured as a trunk. Enable trunking on interface G0/1.

```
S1(config-if)# int g0/1
S1(config-if)# switchport mode trunk
```

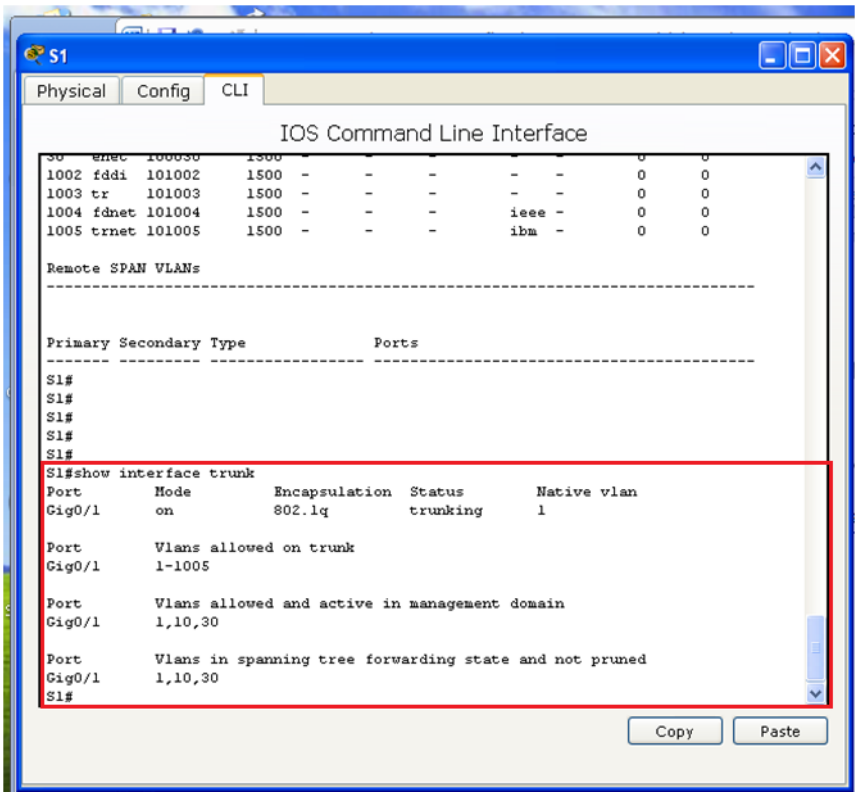


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

c. How can you determine that the interface is a trunk port using the **show vlan** command? The interface is no longer listed under VLAN 1. La interfaz ya no aparece en la VLAN 1.



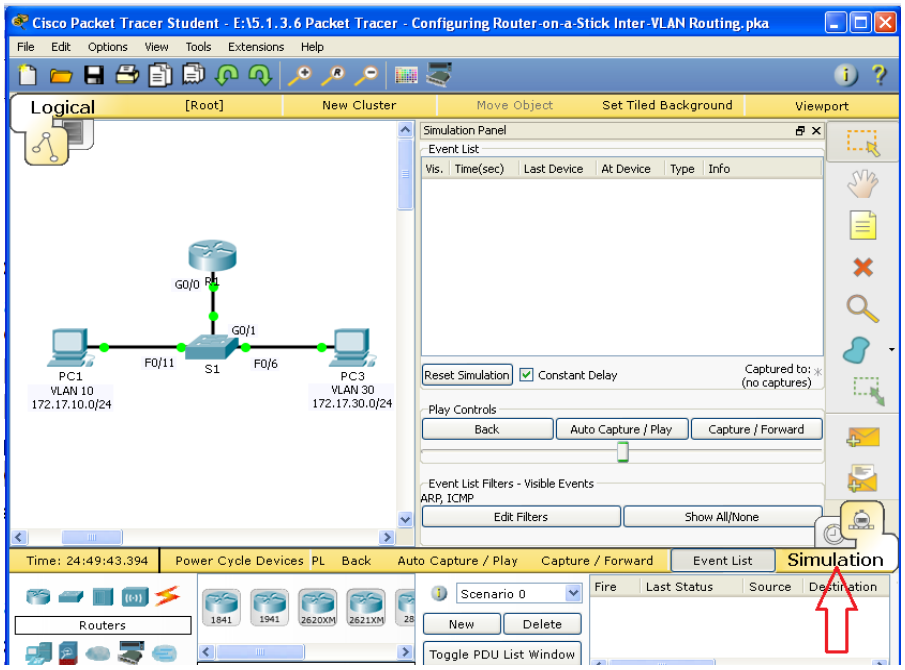
d. Issue the **show interface trunk** command to verify the interface is configured as a trunk.



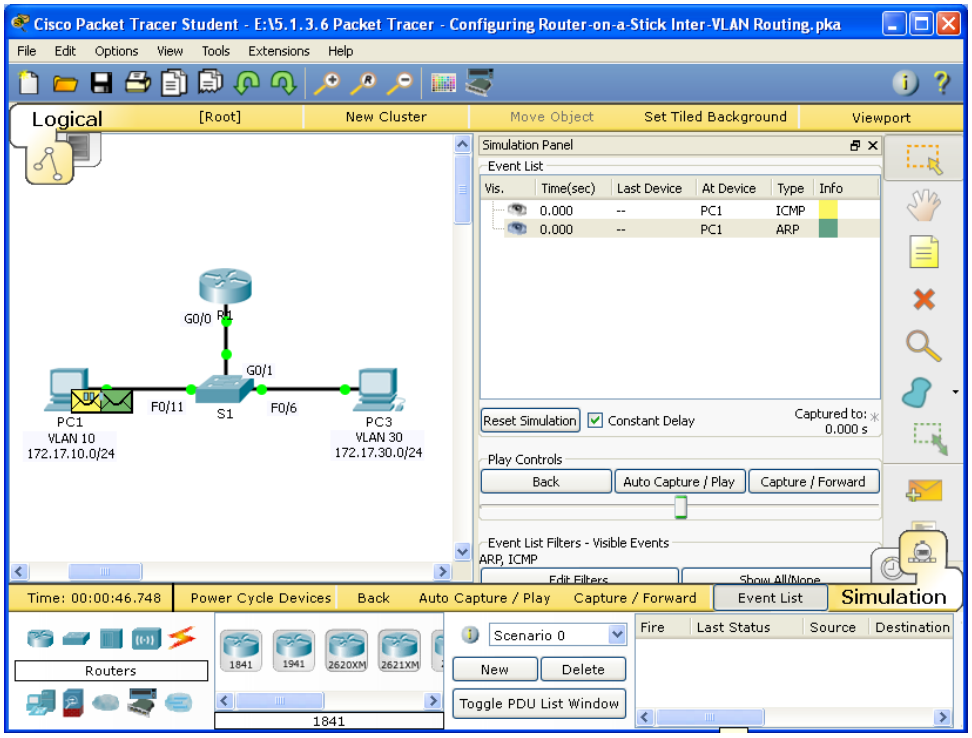
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Step 3: Switch to Simulation mode to monitor pings.

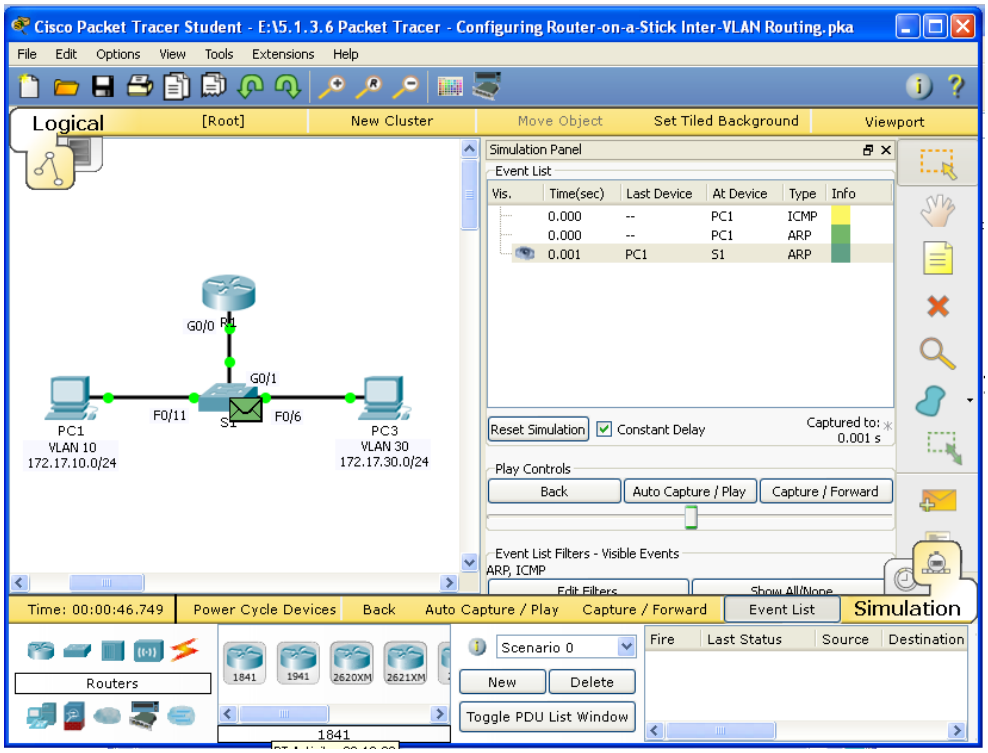
a. Switch to **Simulation** mode by clicking the **Simulation** tab or pressing **Shift+S**.

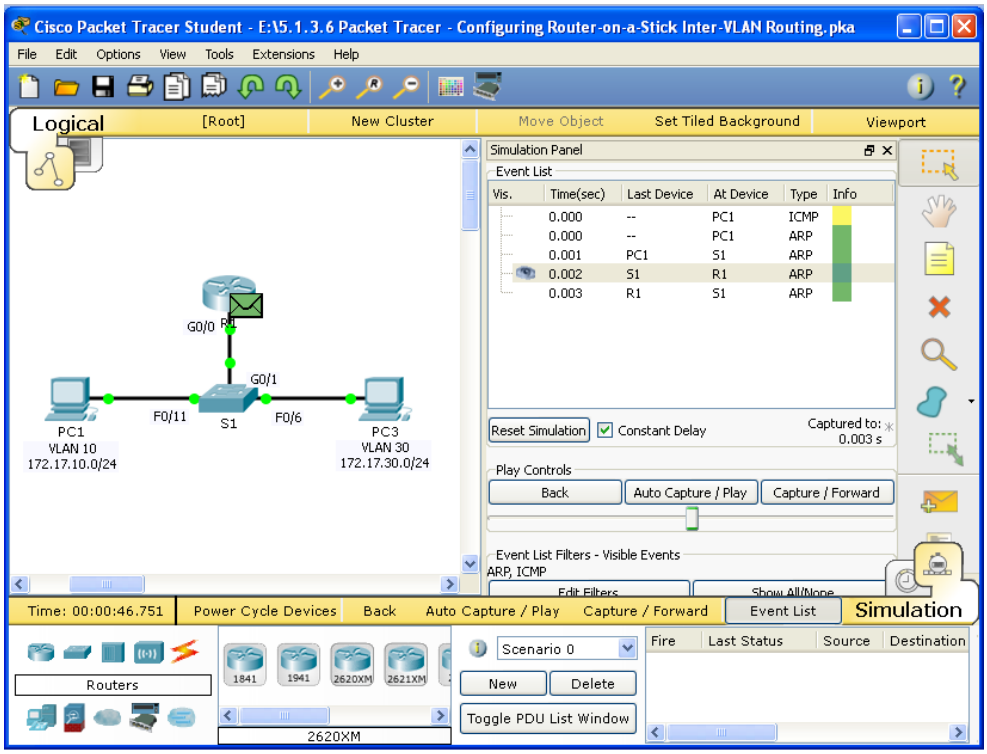


b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**.

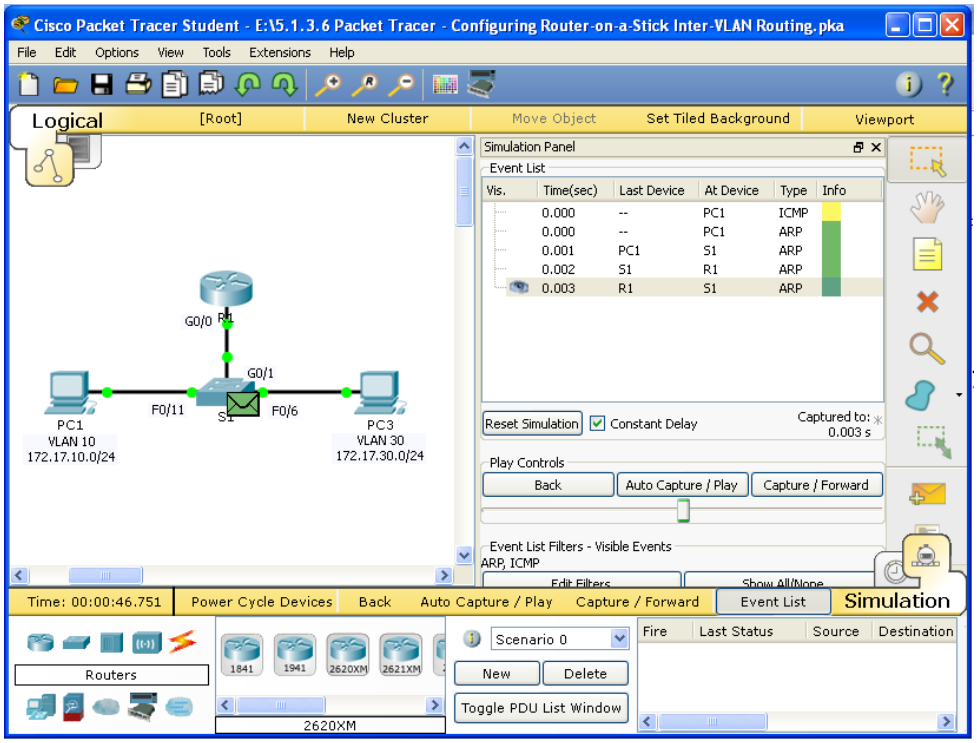


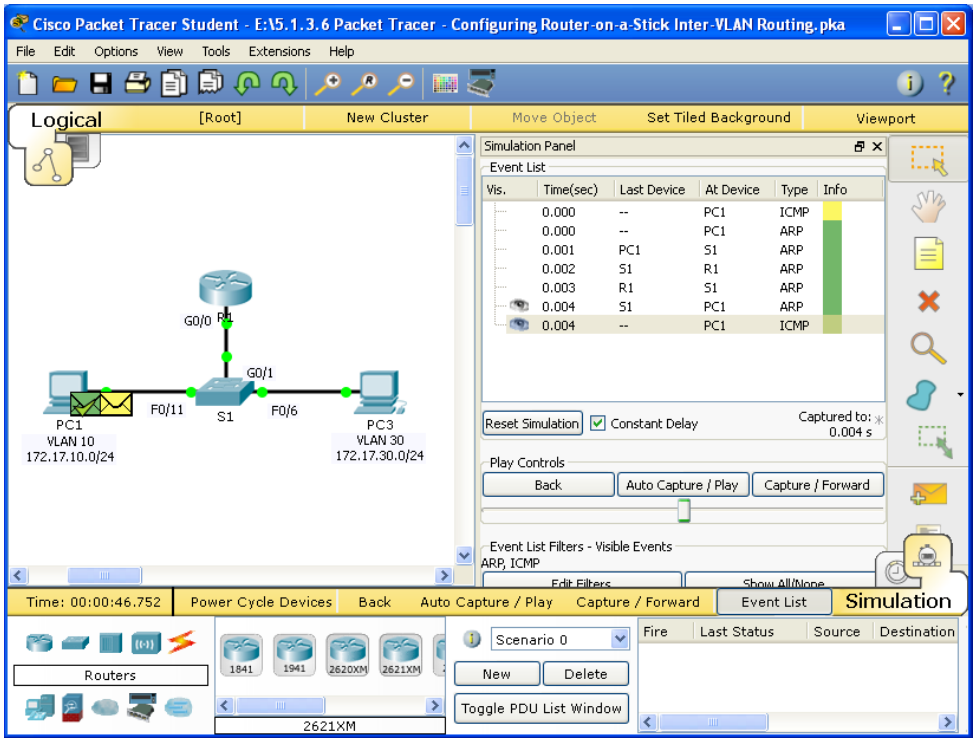
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

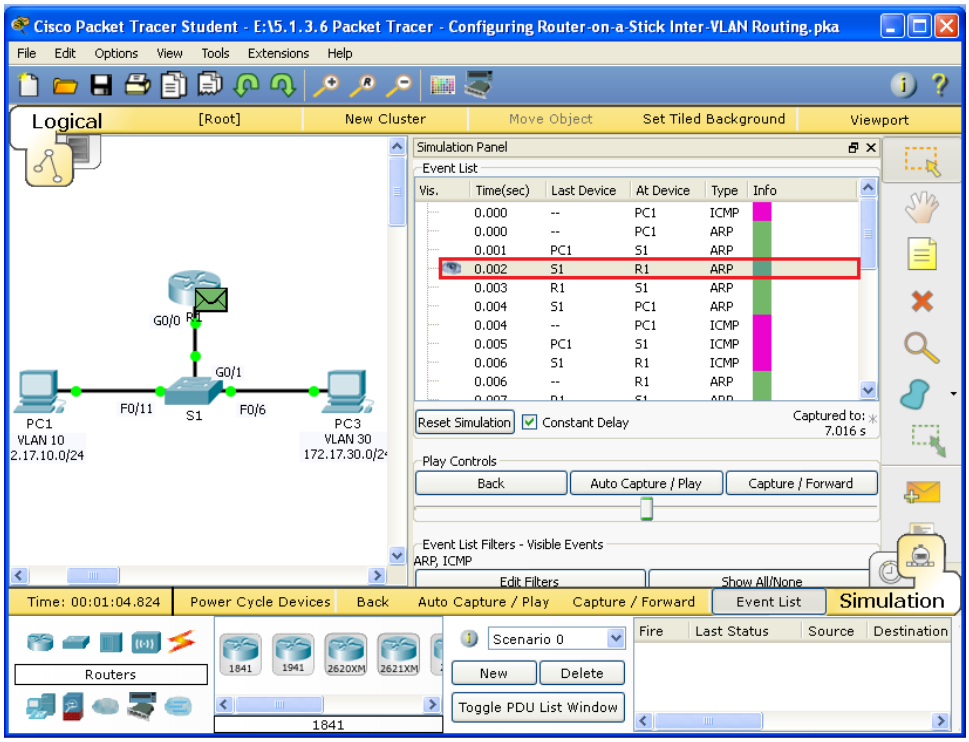




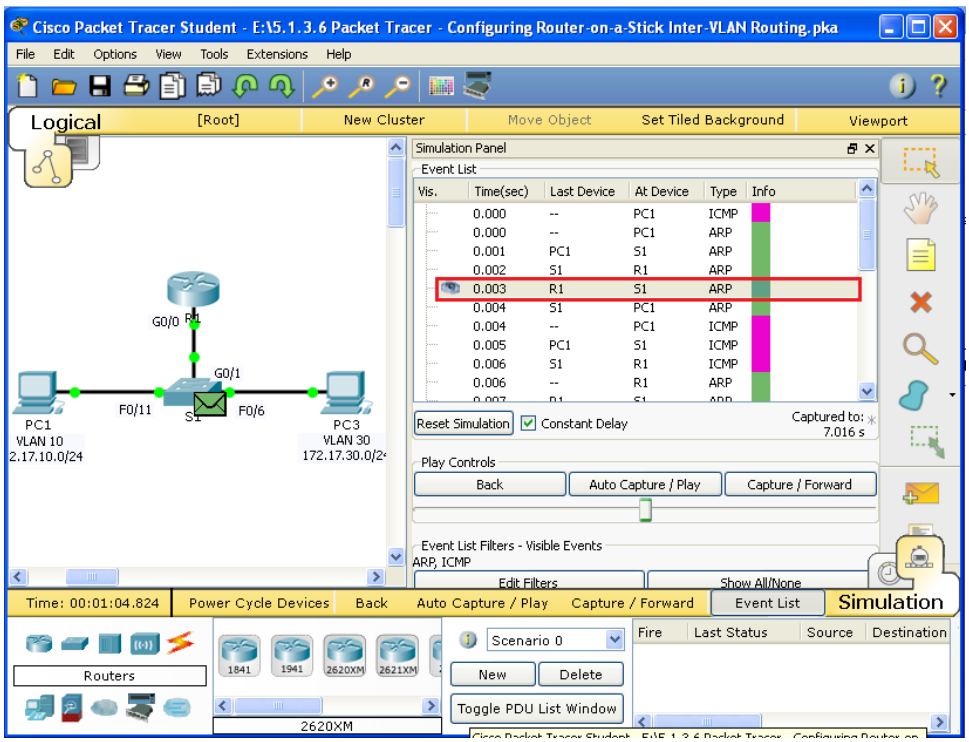
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

Solicitud ARP y respuestas entre S1 y R1

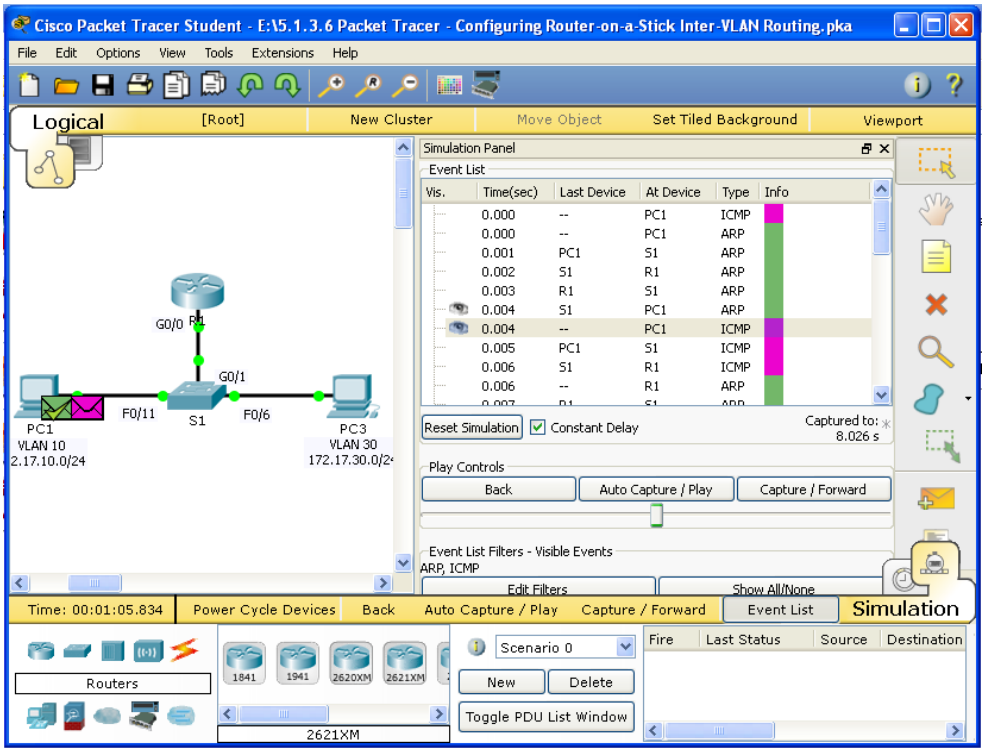


ARP solicita y responde entre R1 y S1

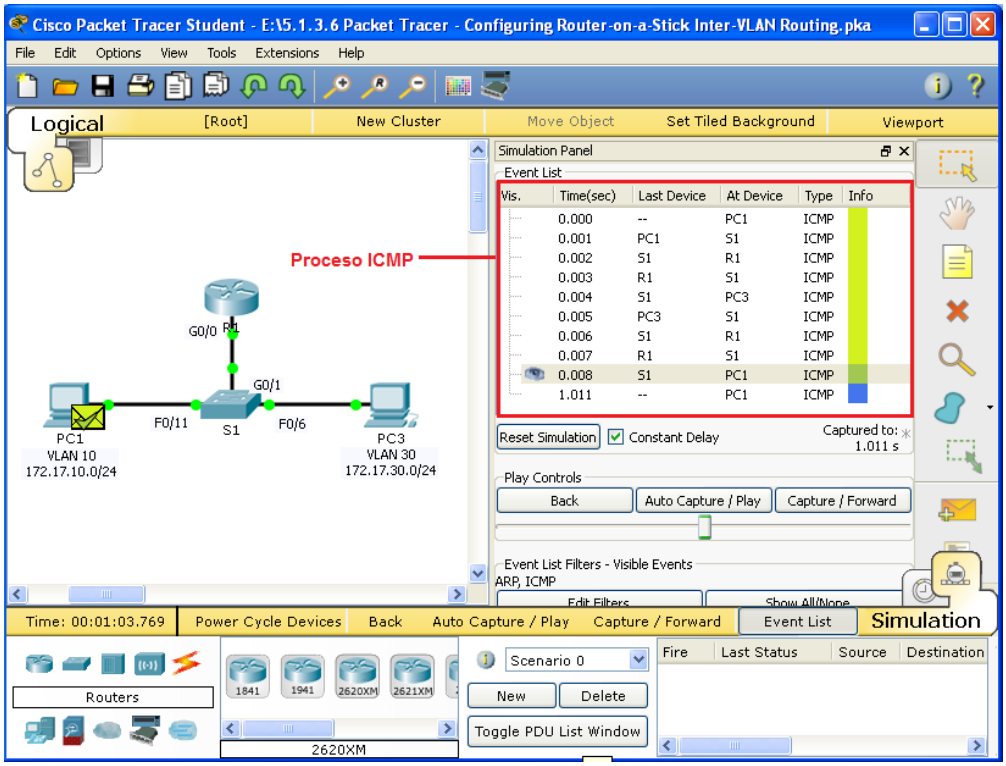


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

PC1 puede encapsular una solicitud ICMP.



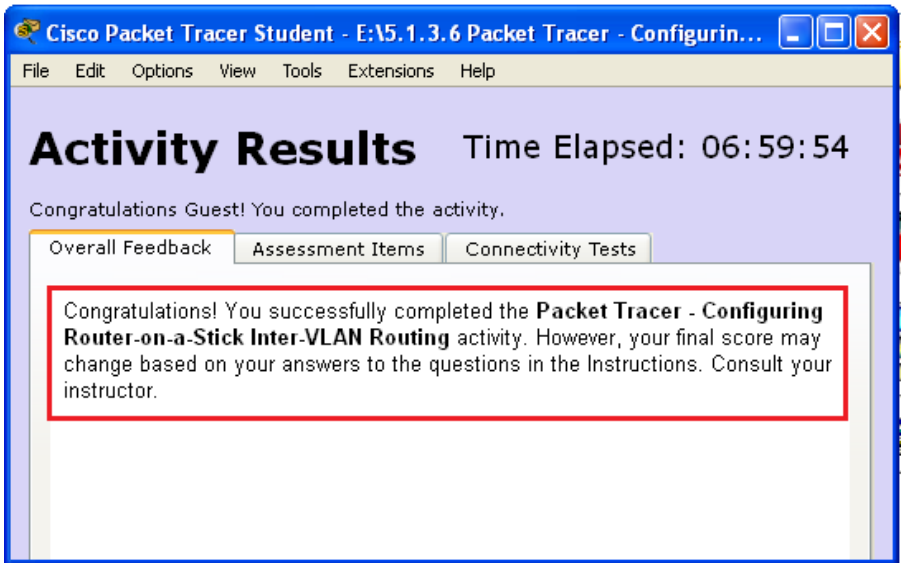
Note: After the ARP process finishes, you may need to click Reset Simulation to see the ICMP process complete.

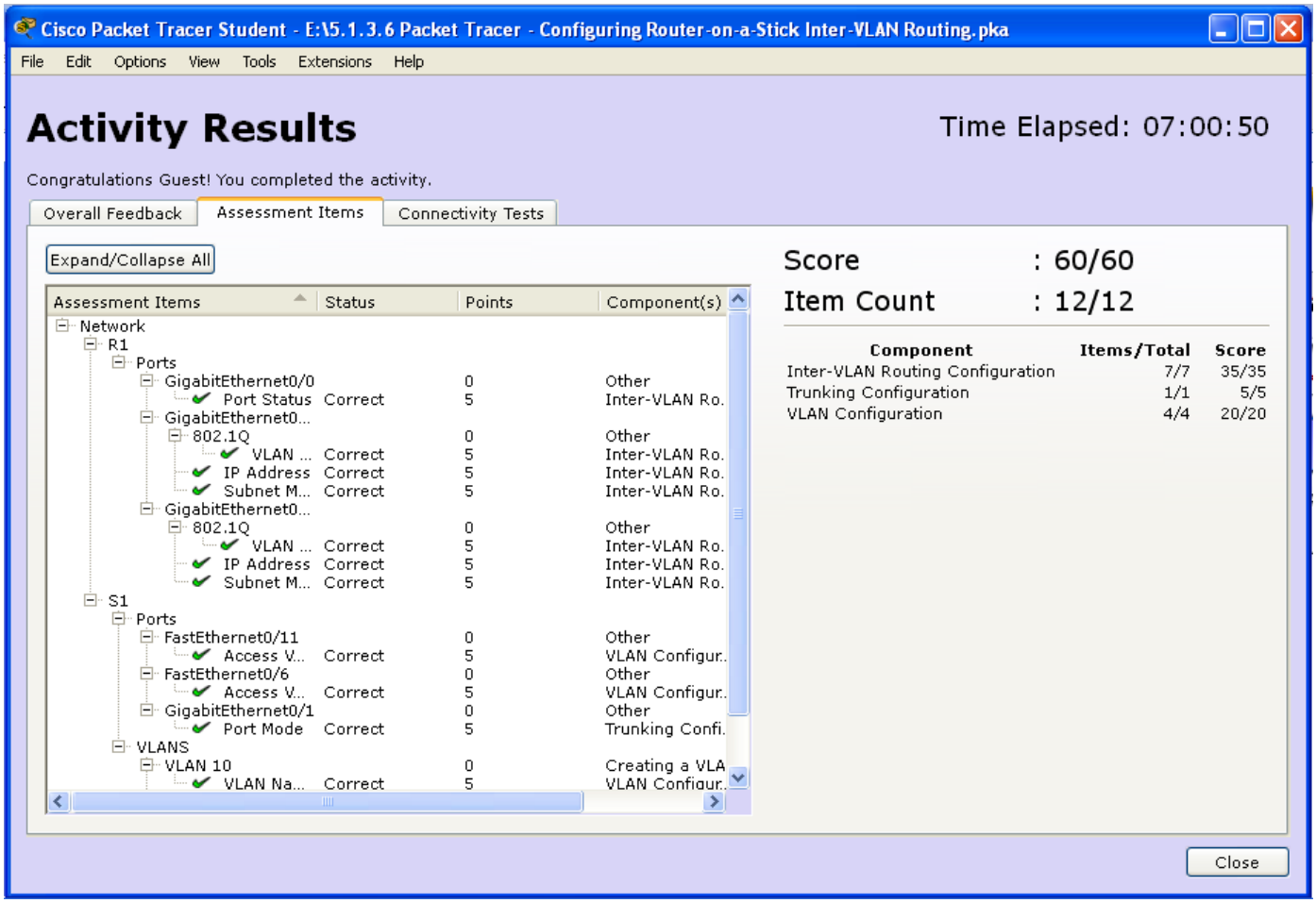


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Suggested Scoring Rubric

Packet Tracer scores 60 points. The four questions are worth 10 points each.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 10

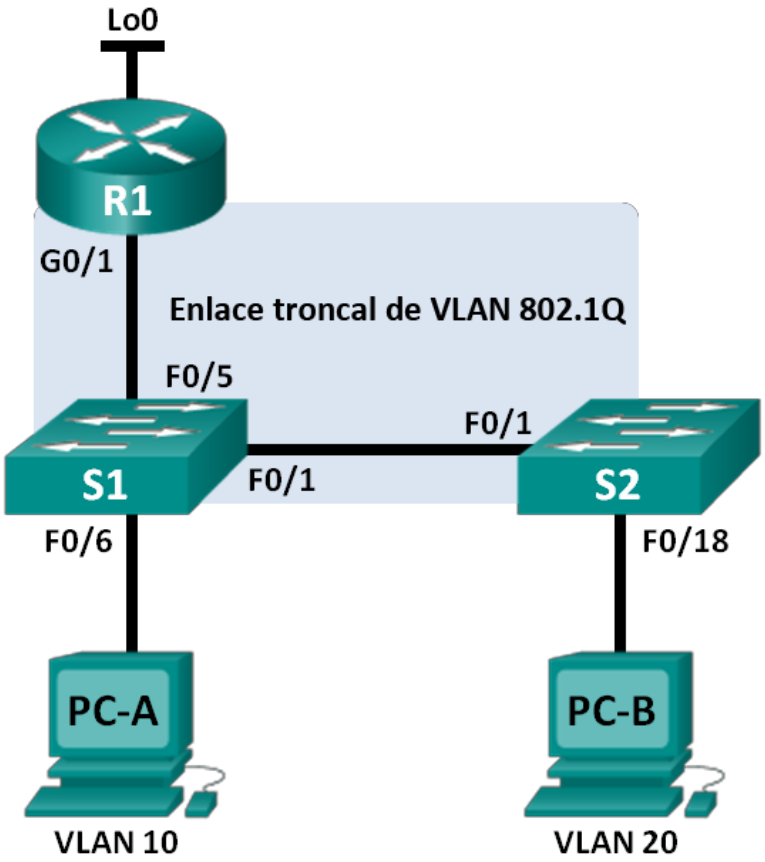
- A través de este trabajo se logra comprender cuales son los pasos y los mandos que se deben utilizar para crear VLANs en S1, configurar VLANS y sub-interfaces en R1 y habilitar la troncal en R1.
- Algo muy importante para establecer conectividad en equipos finales de comunicación como PC1 y PC3, los cuales están conectados a través de VLANS.
- En esta actividad, comprobamos la conectividad antes de implementar el enrutamiento entre VLAN.
- Configuramos las VLAN y el enrutamiento entre VLAN y finalmente, habilitamos trunking y verificamos la conectividad entre VLANs.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 11: 5.1.3.7 Lab - Configuring 802.1Q Trunk-Based Inter-VLAN Routing

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

Topología



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

Consulte la tabla Resumen de interfaces del router que se encuentra al final de 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.

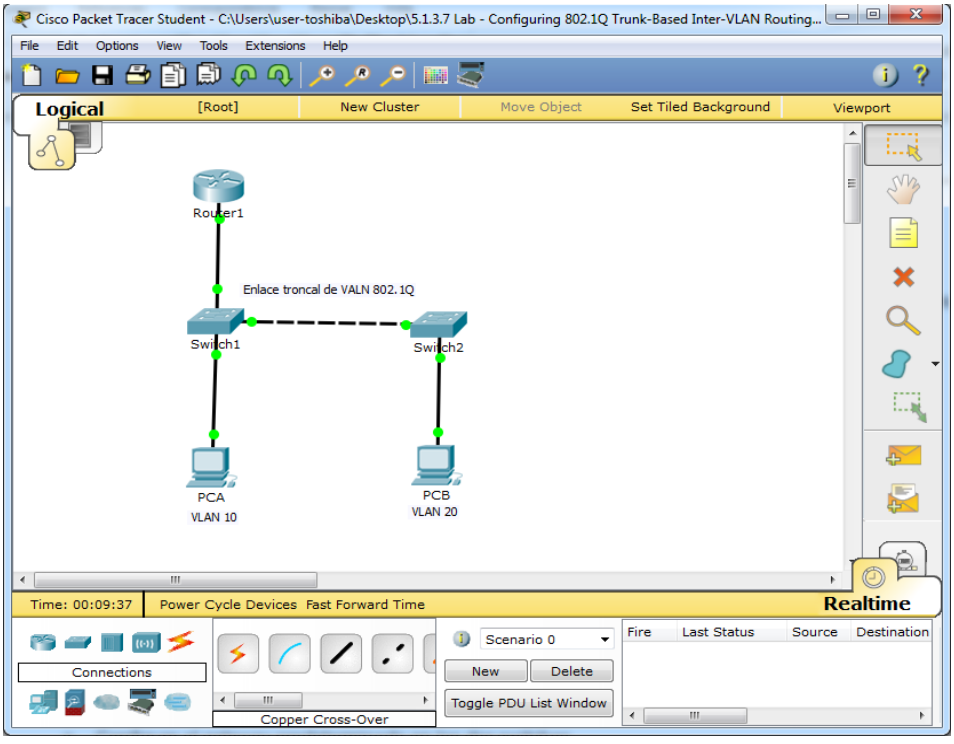
Recursos necesarios

- 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

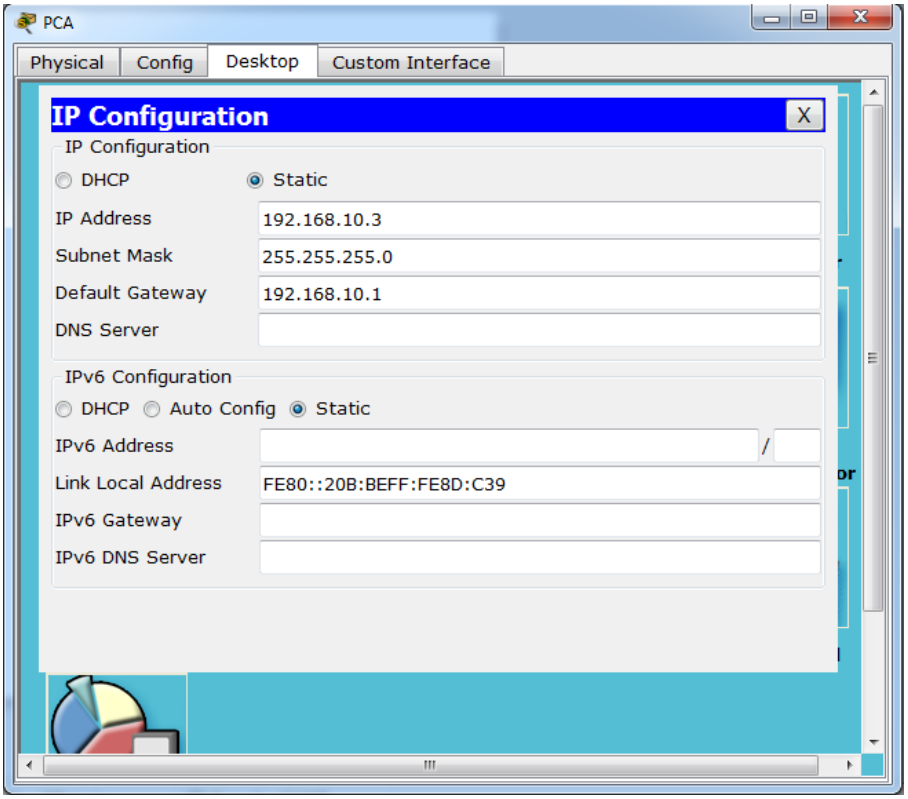
En la parte 1, configurará la topología de la red y configurará los parámetros básicos en los equipos host, los switches y el router.

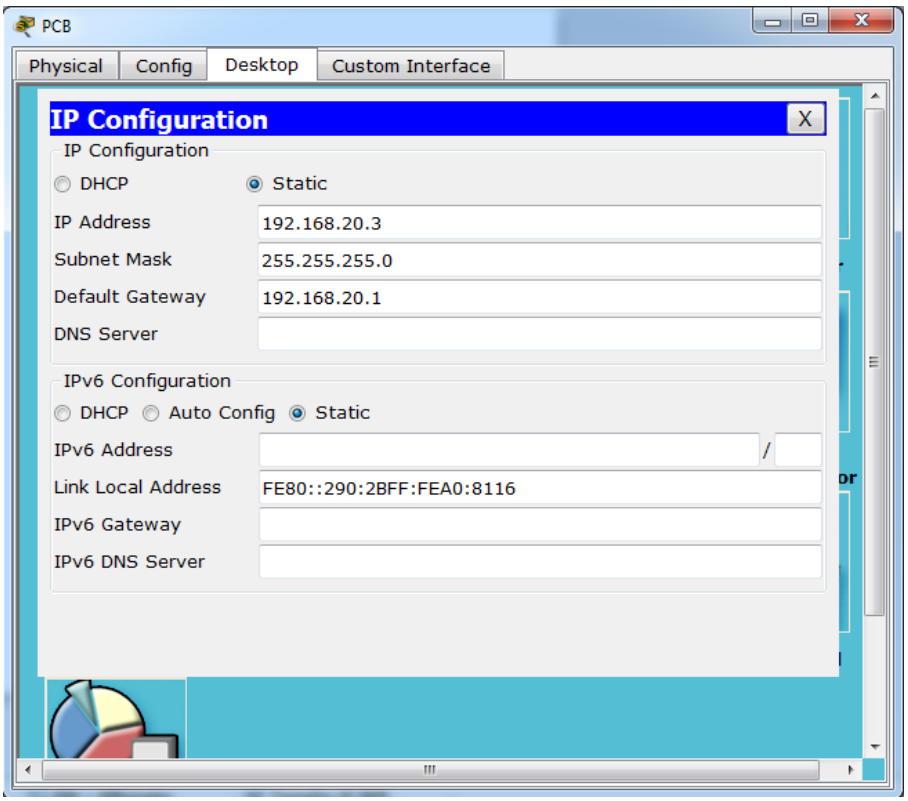
Paso 1. Realizar el cableado de red tal como se muestra en la topología.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 2. Configurar los equipos host.



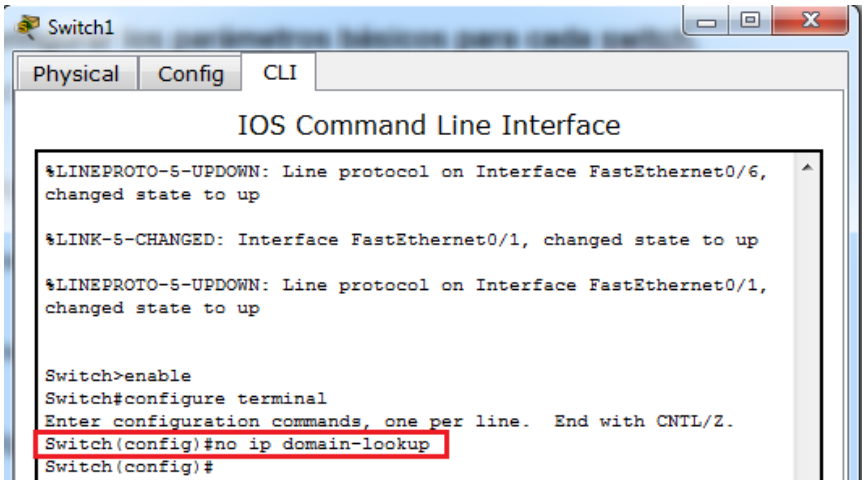


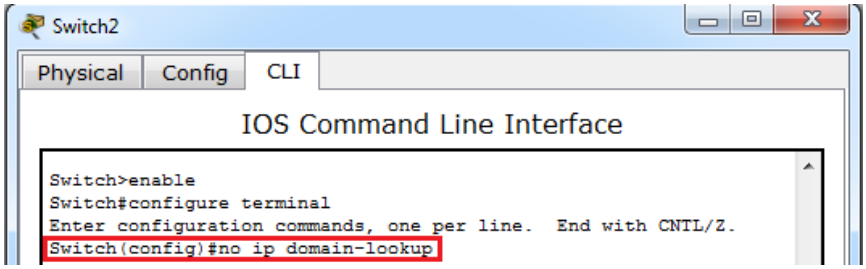
Paso 3. Inicializar y volver a cargar los routers y switches, según sea necesario.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

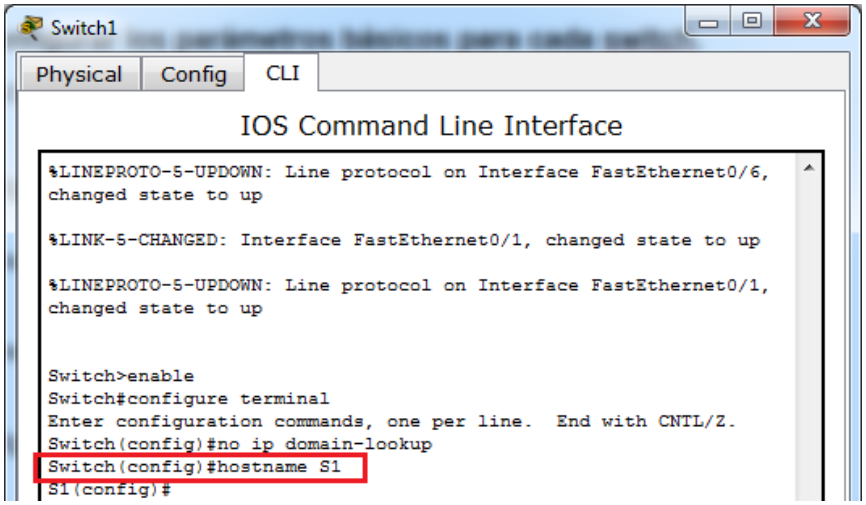
Paso 4. Configurar los parámetros básicos para cada switch.

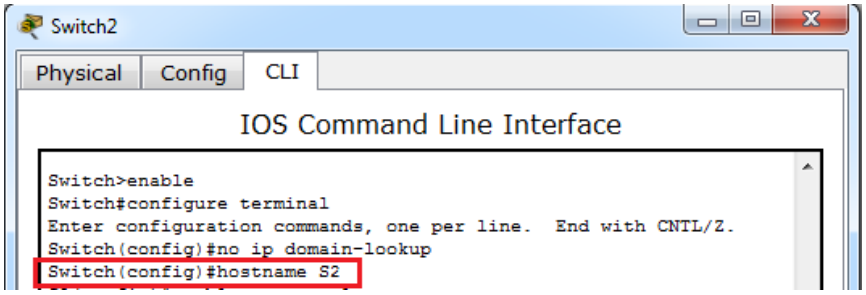
a. Desactive la búsqueda del DNS.





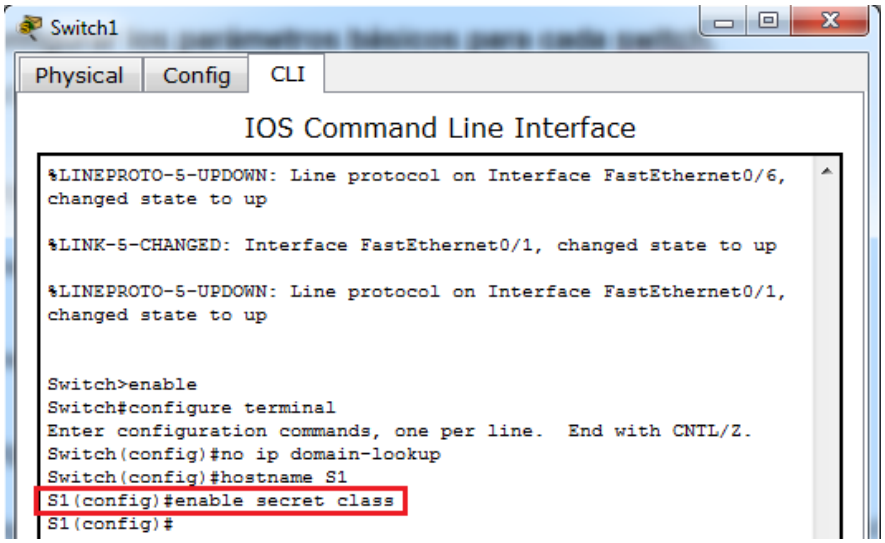
b. Configure los nombres de los dispositivos como se muestra en la topología.

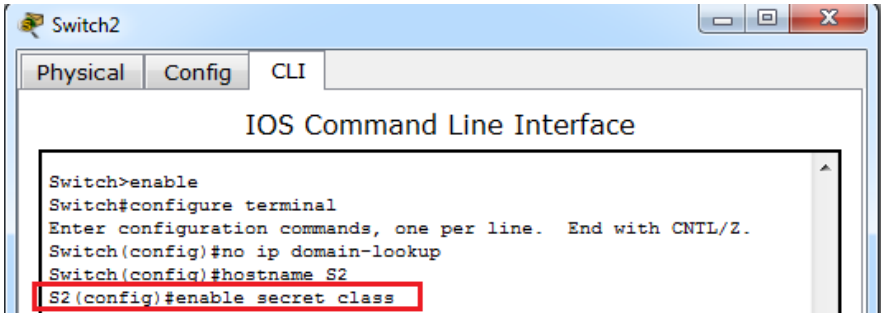




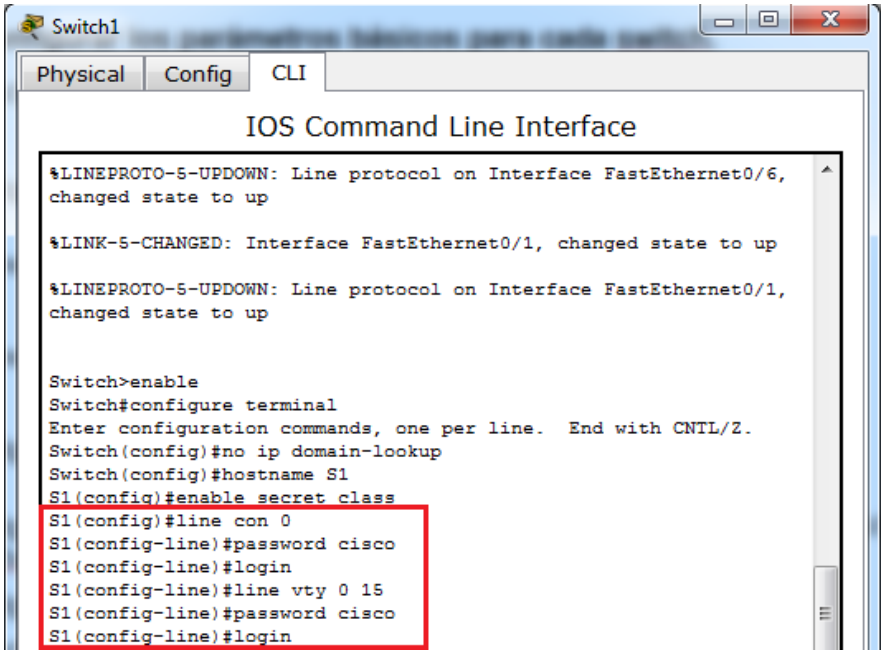
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

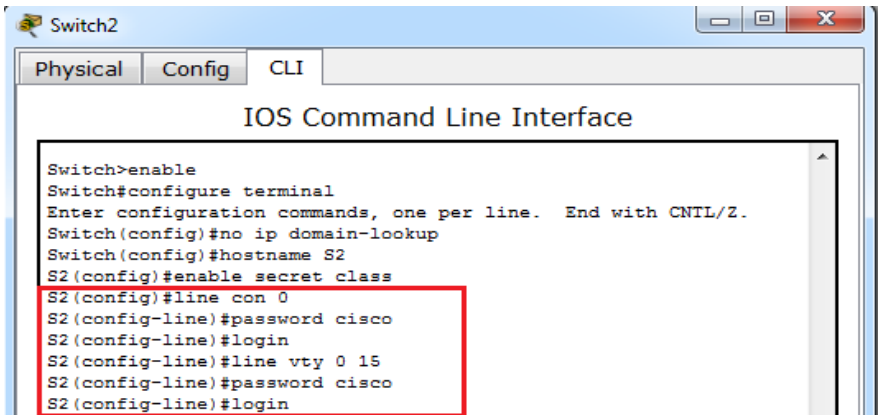




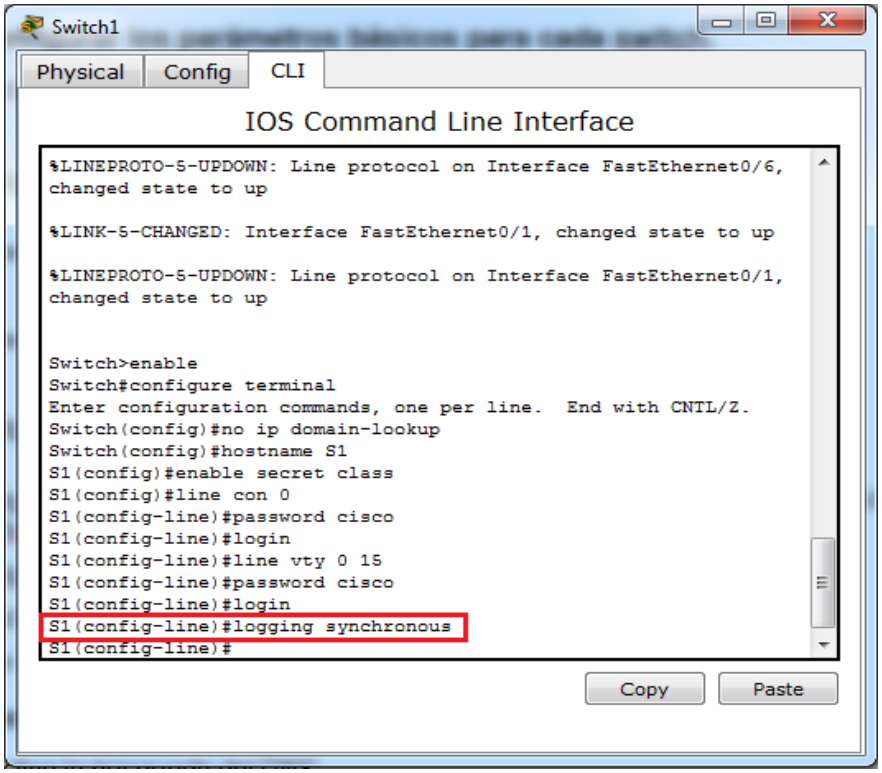
d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.

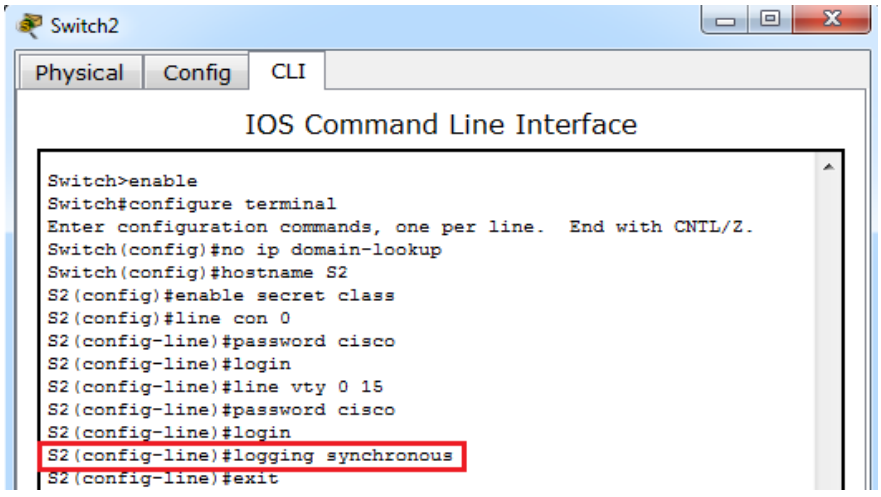


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



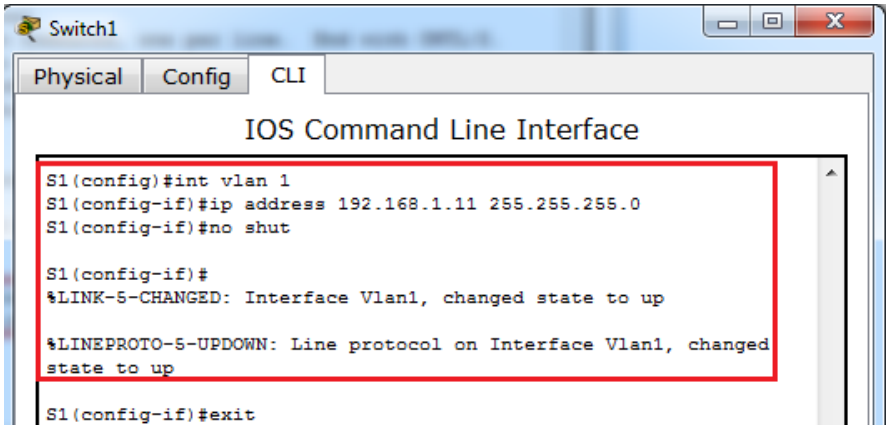
e. Configure **logging synchronous** para la línea de consola.

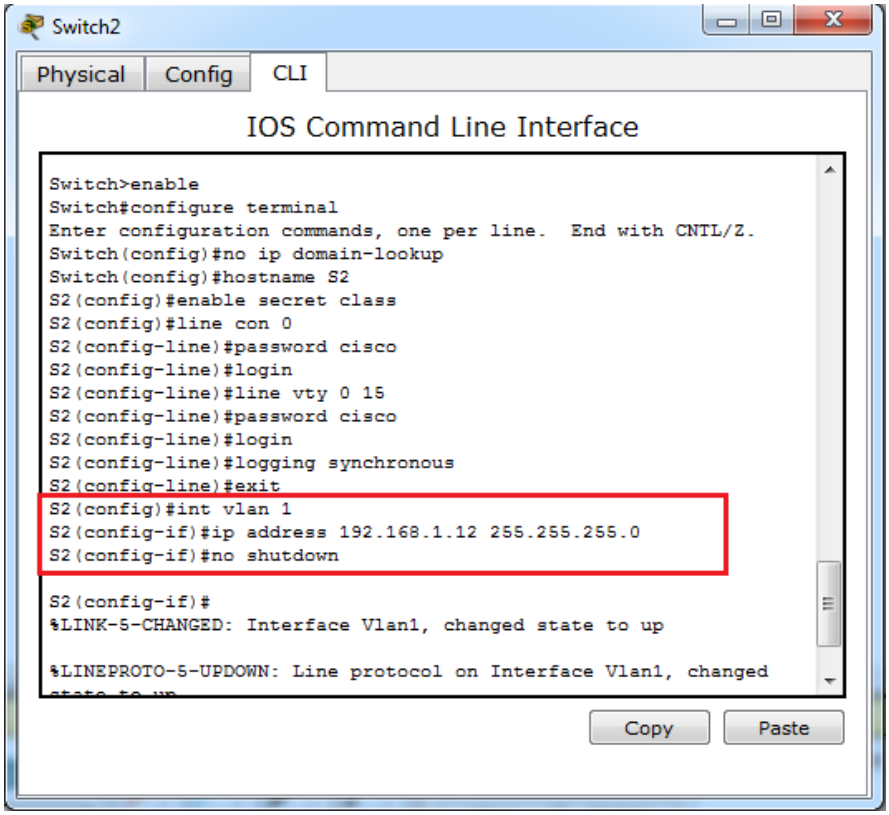




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

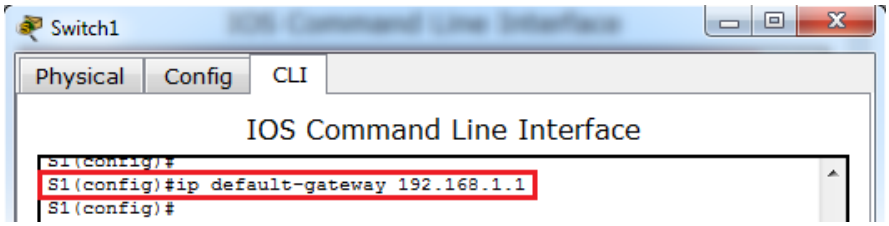
f. Configure la dirección IP que se indica en la tabla de direccionamiento para la VLAN 1 en ambos switches.

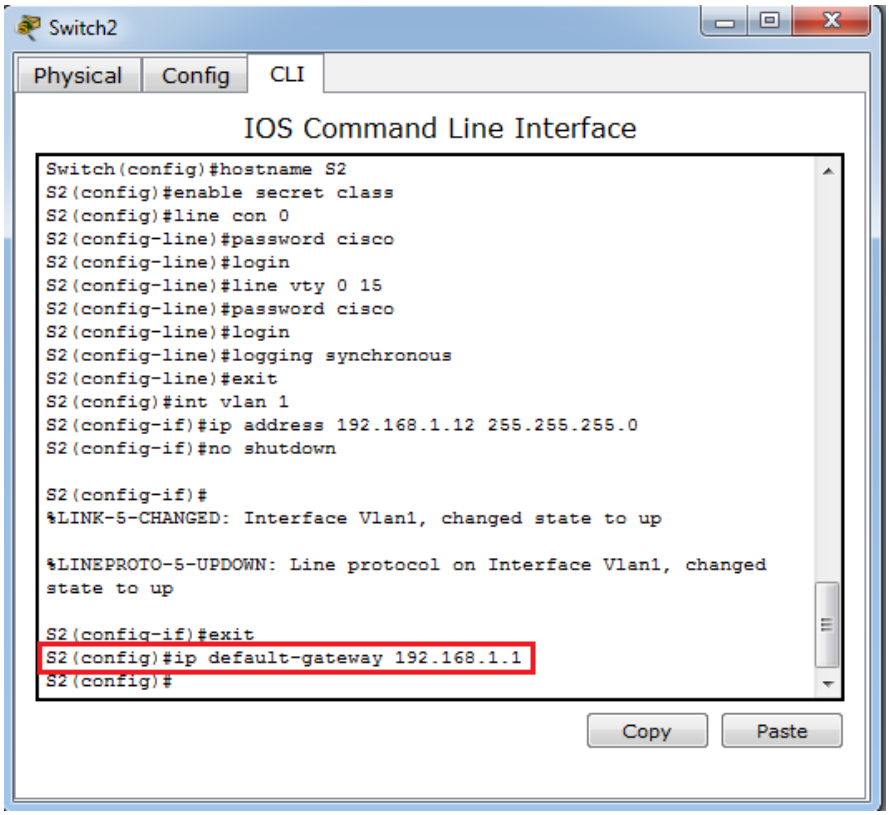




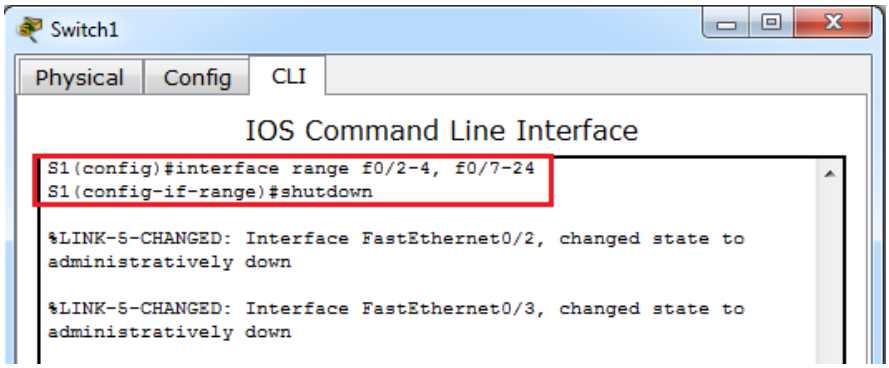
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

g. Configure el gateway predeterminado en los dos switches.

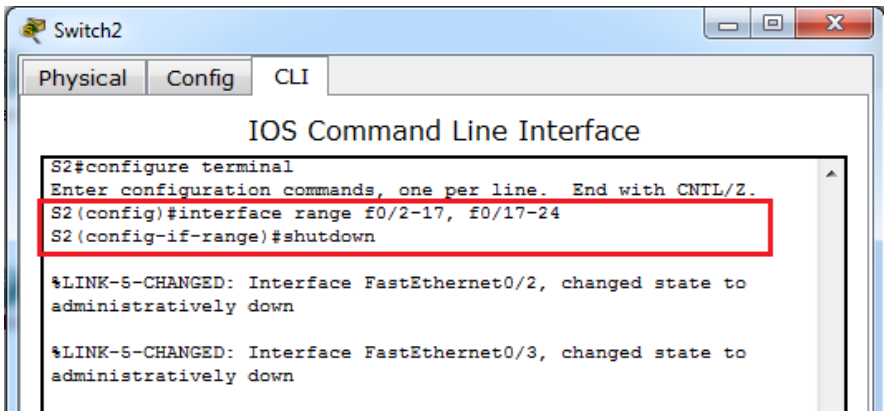




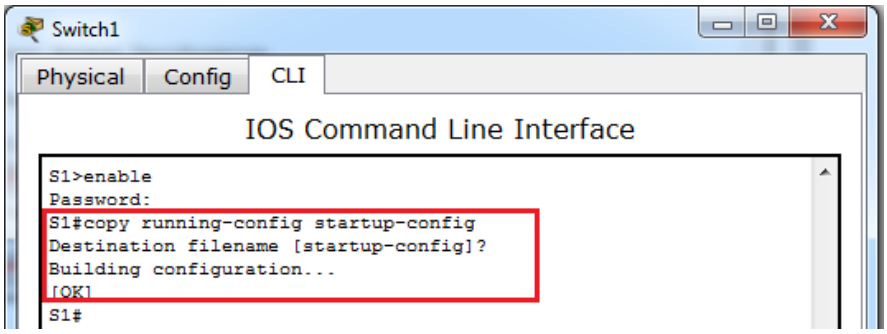
h. Desactive administrativamente todos los puertos que no se usen en el switch.

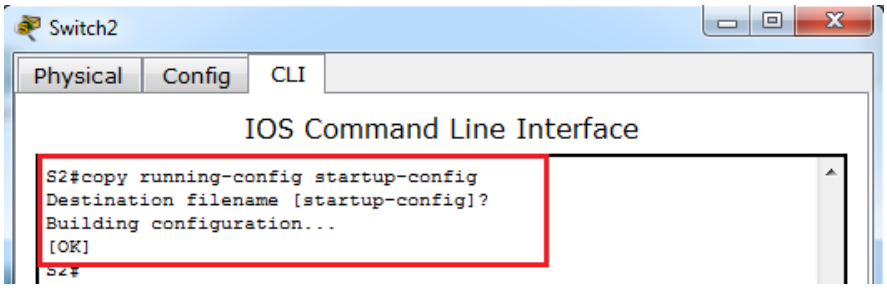


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



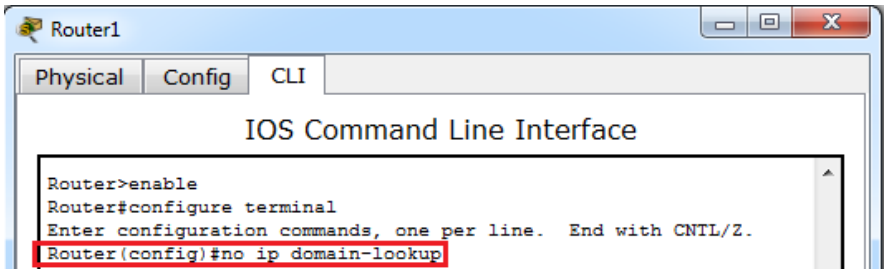
i. Copie la configuración en ejecución en la configuración de inicio





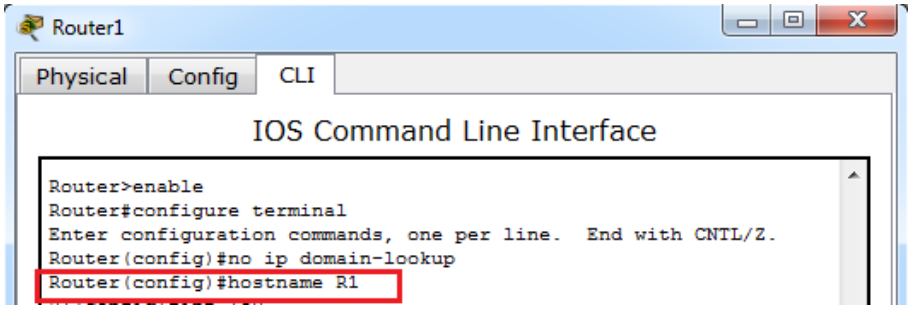
Paso 5. Configurar los parámetros básicos para el router.

a. Desactive la búsqueda del DNS.

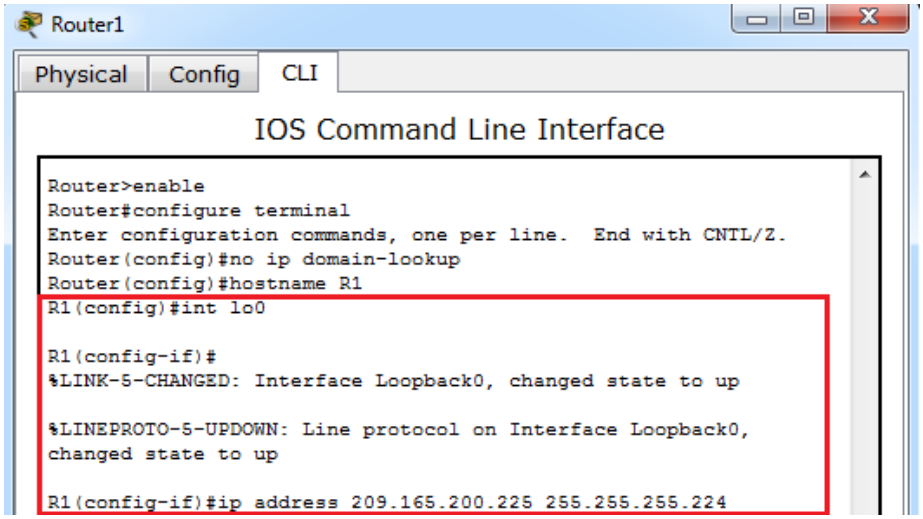


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

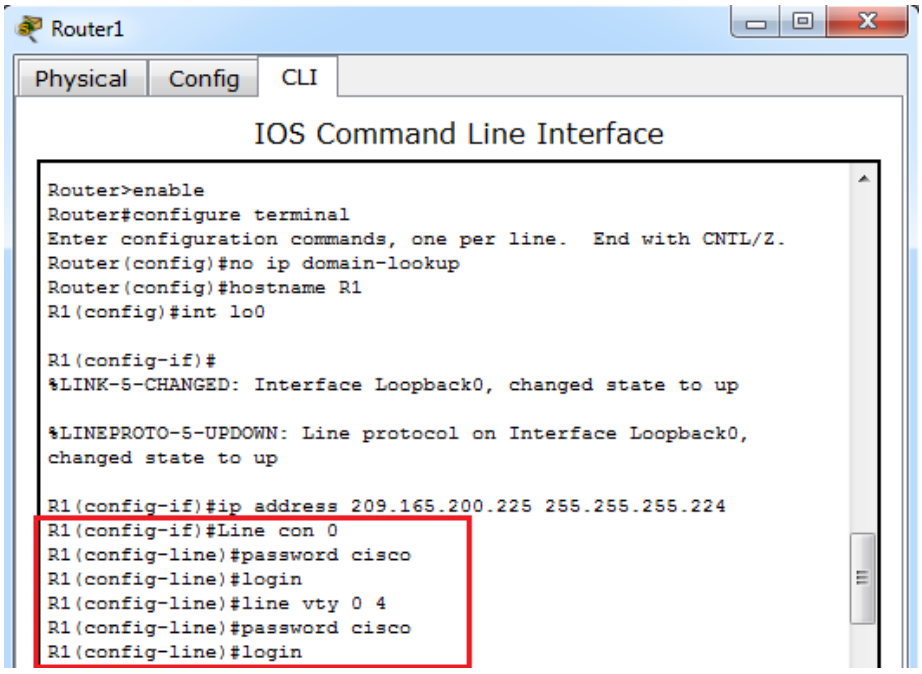
b. Configure los nombres de los dispositivos como se muestra en la topología.



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



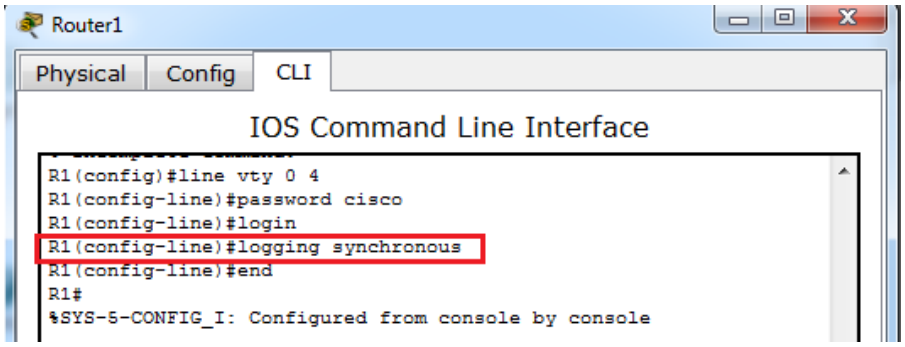
d. Asigne **cisco** como la contraseña de consola y la contraseña de vty.



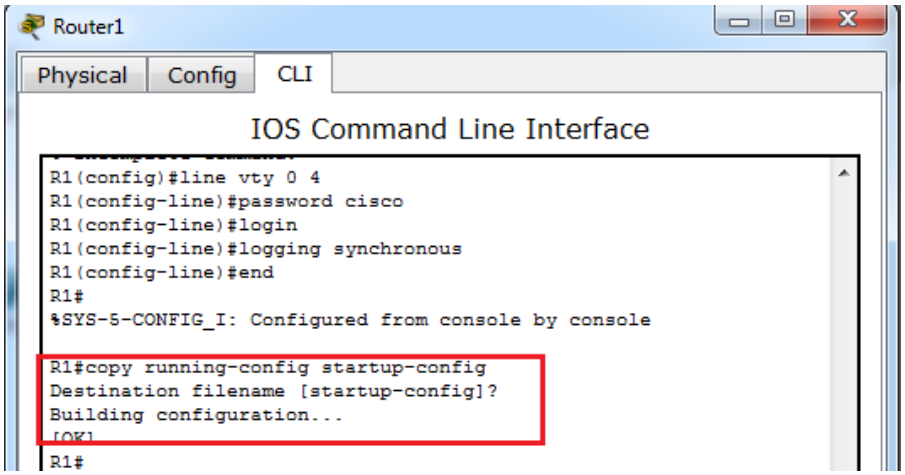
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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



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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

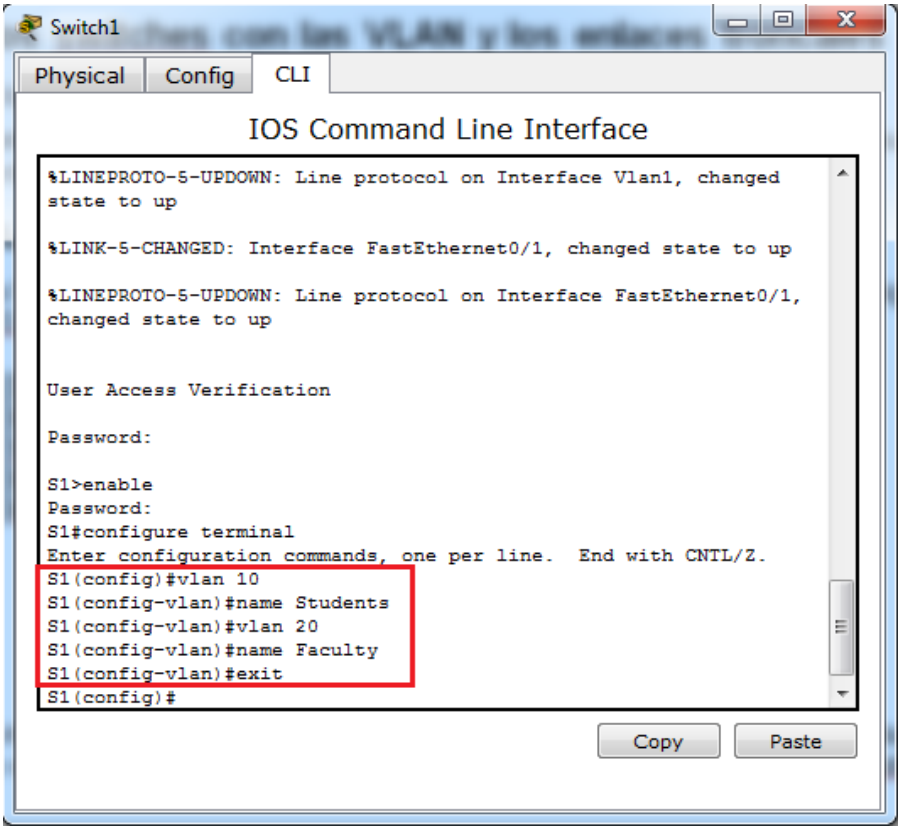
En la parte 2, configurará los switches con las VLAN y los enlaces troncales.

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

Paso 1. Configurar las VLAN en S1.

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

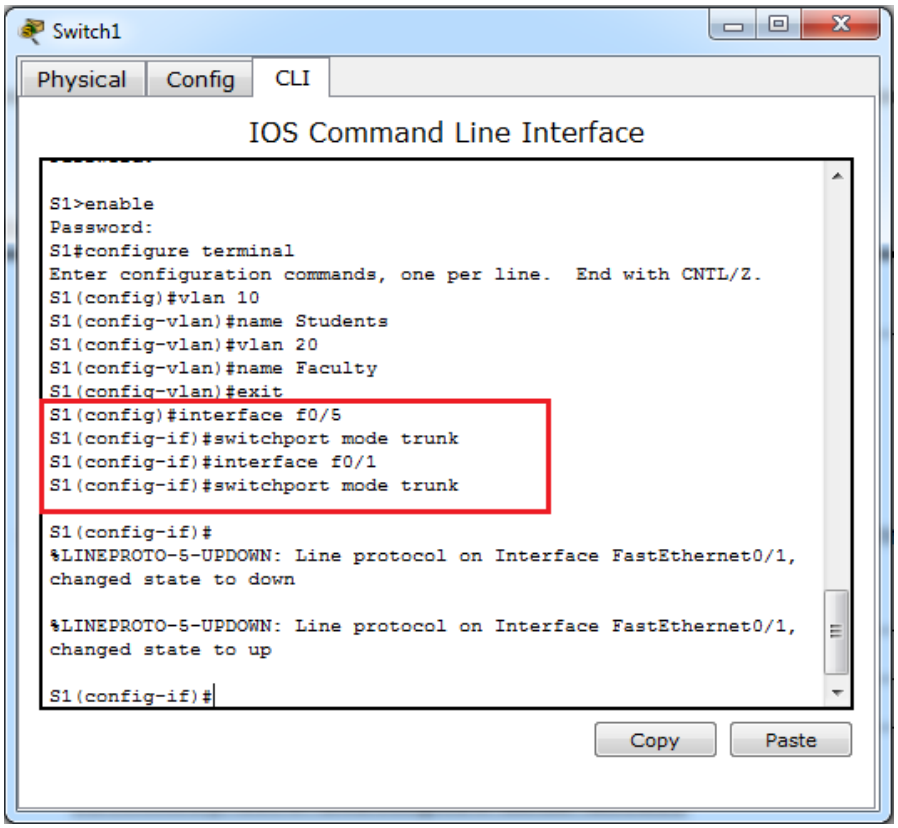
```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# exit
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

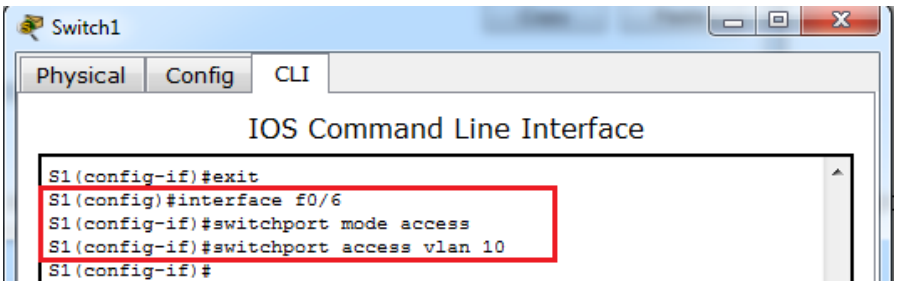
b. En el S1, configure la interfaz conectada al R1 como enlace troncal. También configure la interfaz conectada al S2 como enlace troncal. En el espacio proporcionado, escriba los comandos que utilizó.

```
S1(config)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/1
S1(config-if)# switchport mode trunk
```



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

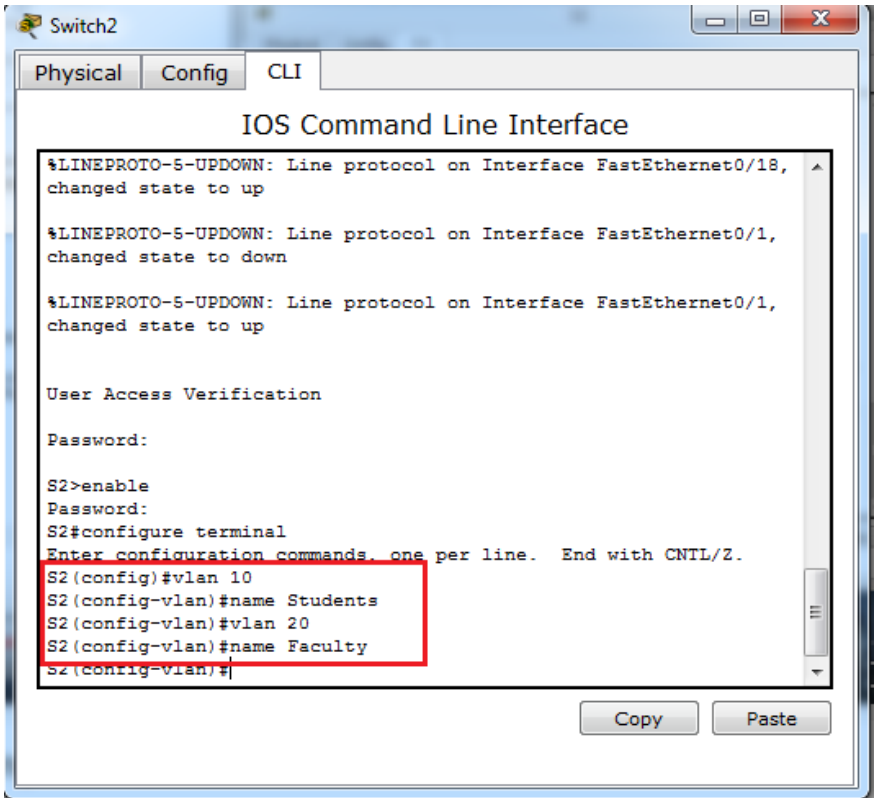
```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

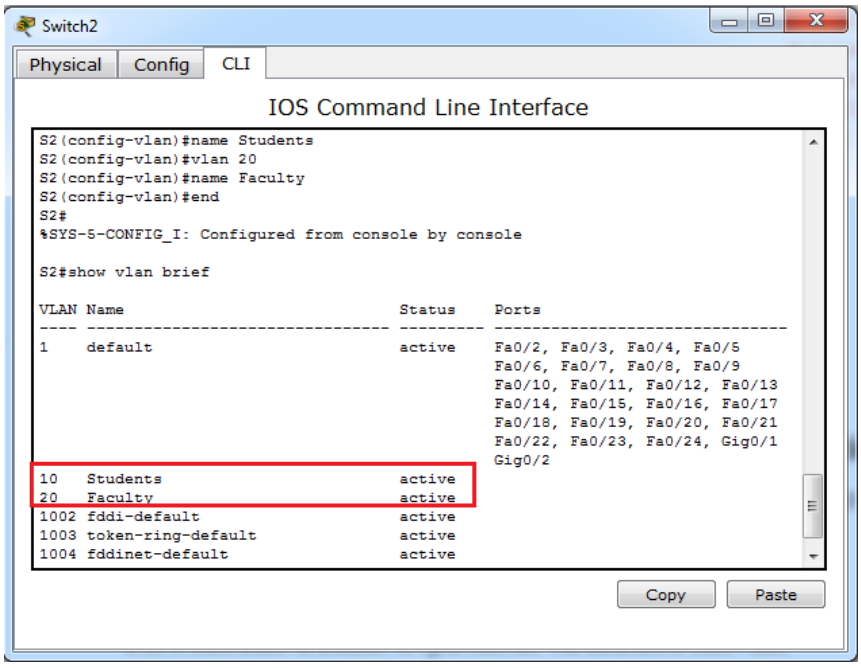
Paso 2. Configurar las VLAN en el switch 2.

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



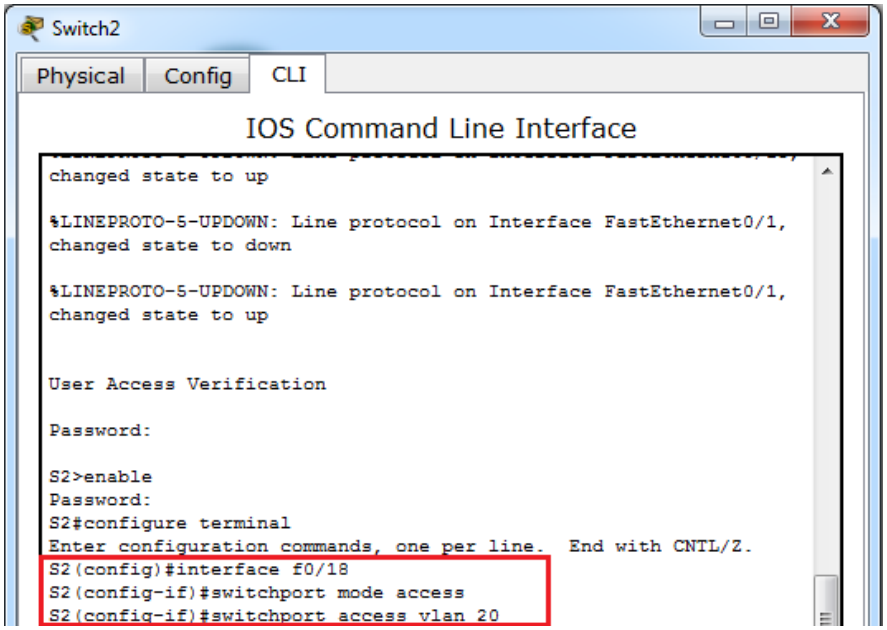
b. En el S2, verifique que los nombres y números de las VLAN coincidan con los del S1. En el espacio proporcionado, escriba el comando que utilizó.

```
S2# show vlan brief
```

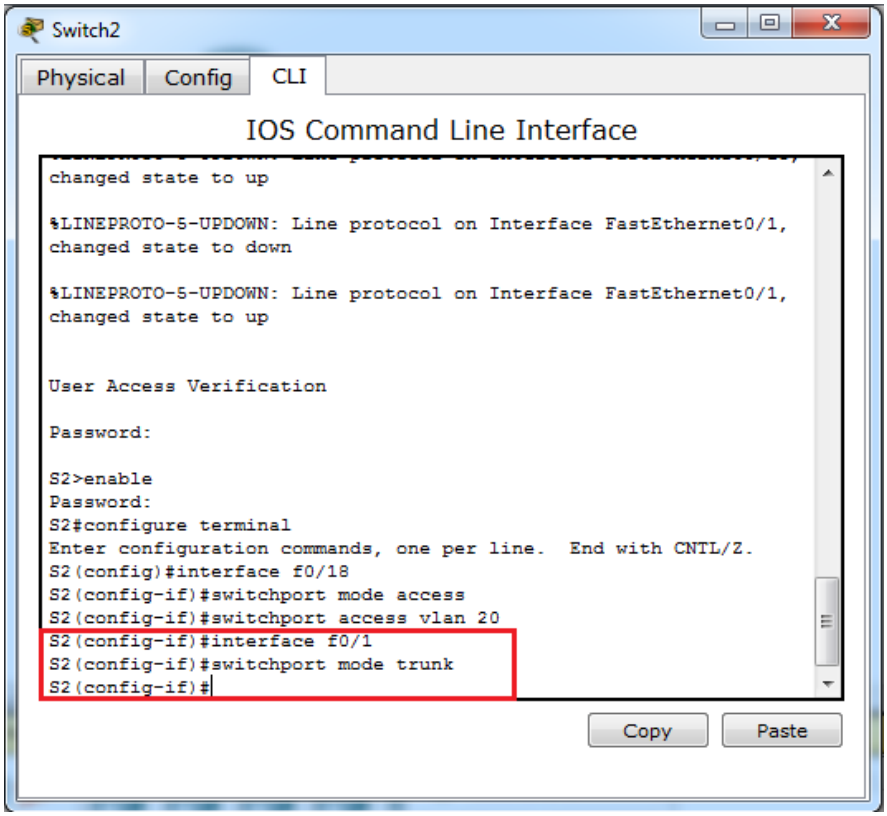


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 3: configurar routing entre VLAN basado en enlaces troncales

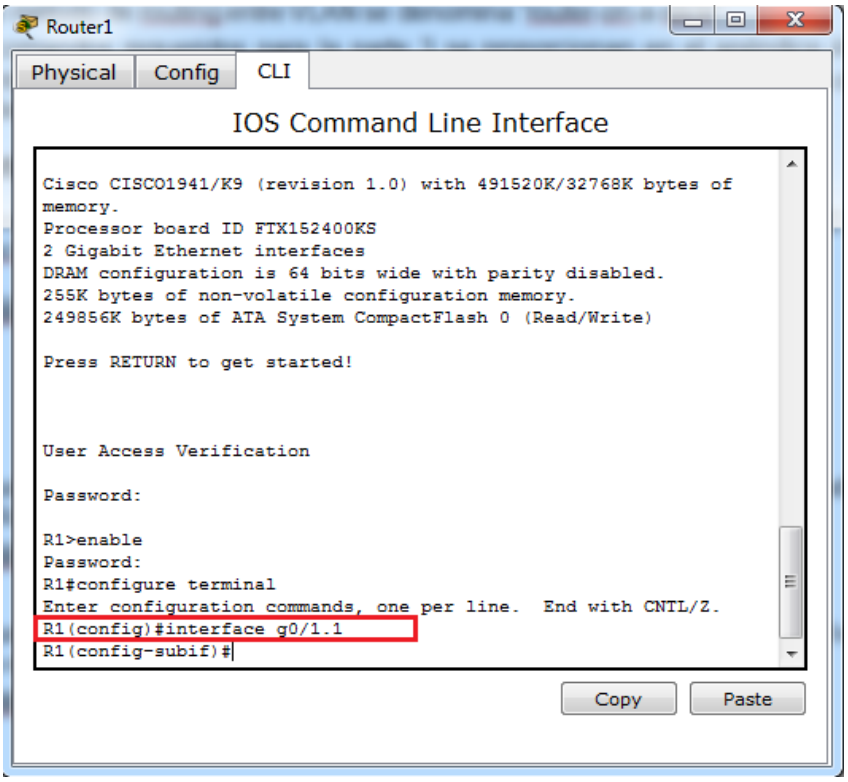
En la parte 3, configurará el R1 para enrutar a varias VLAN mediante la creación de subinterfaces para cada VLAN. Este método de routing entre VLAN se denomina “router-on-a-stick”.

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

Paso 1. Configurar una subinterfaz para la VLAN 1.

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

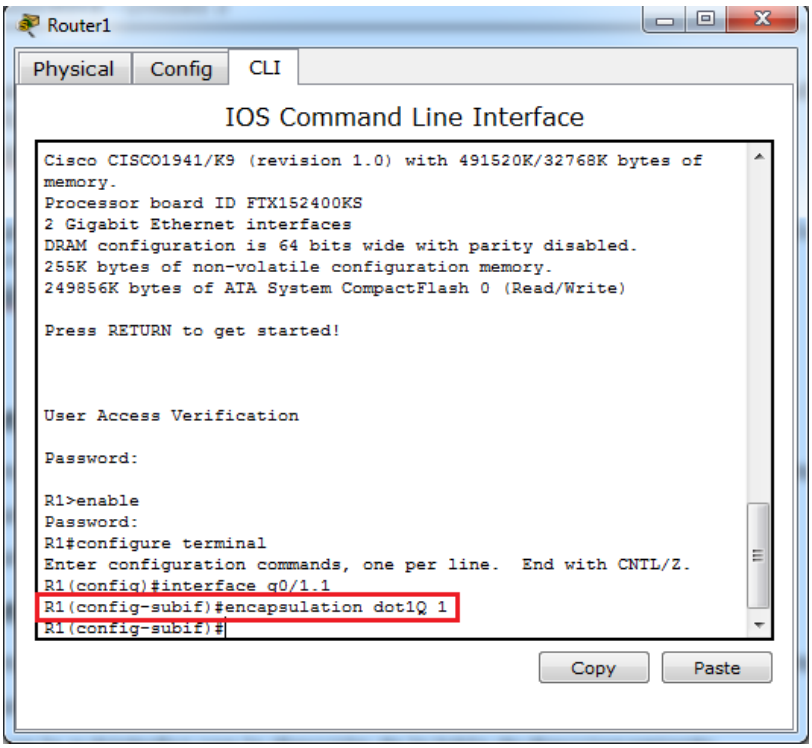
```
R1(config)# interface g0/1.1
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

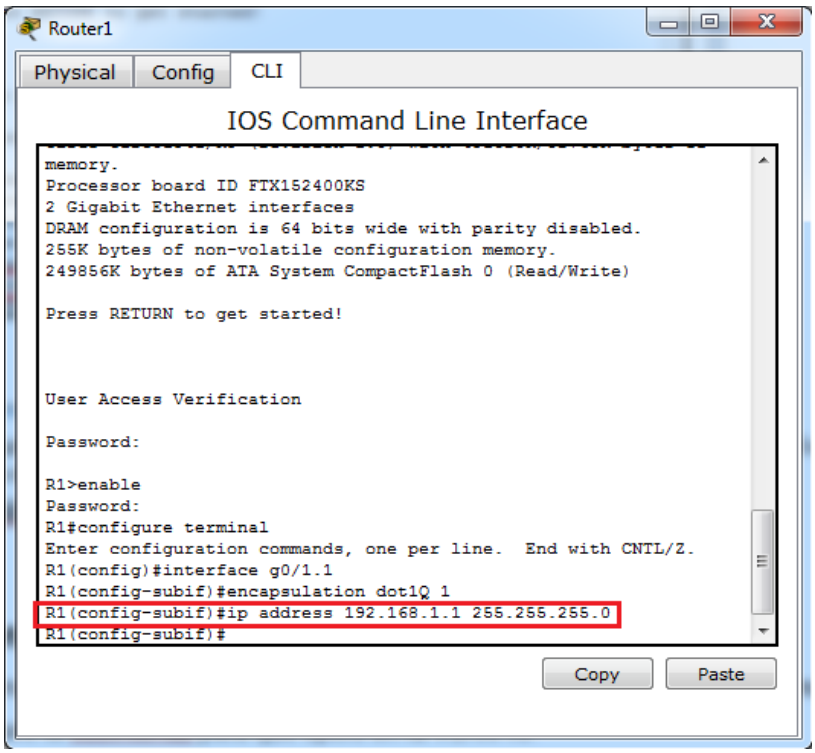
b. Configure la subinterfaz para que opere en la VLAN 1. En el espacio proporcionado, escriba el comando que utilizó.

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



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

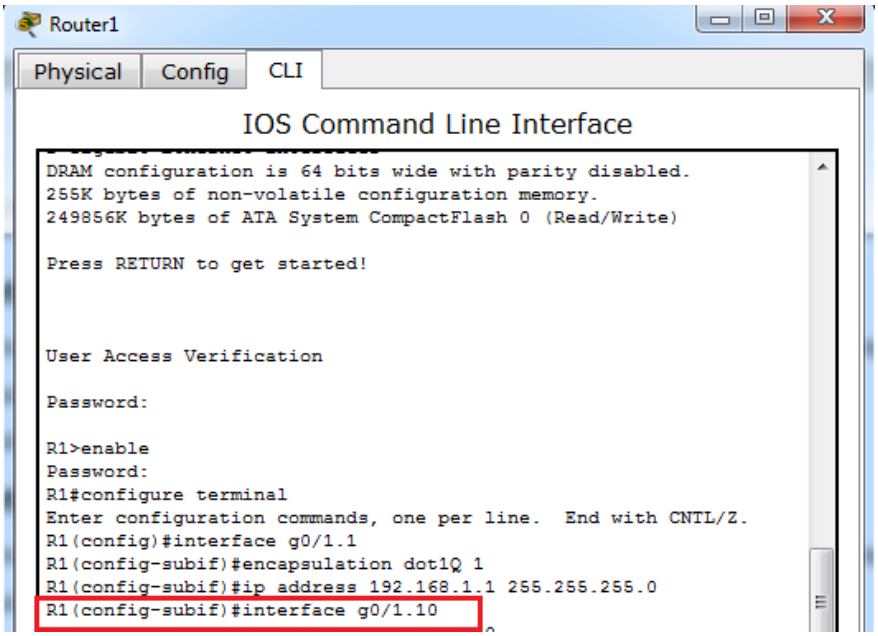
```
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
```



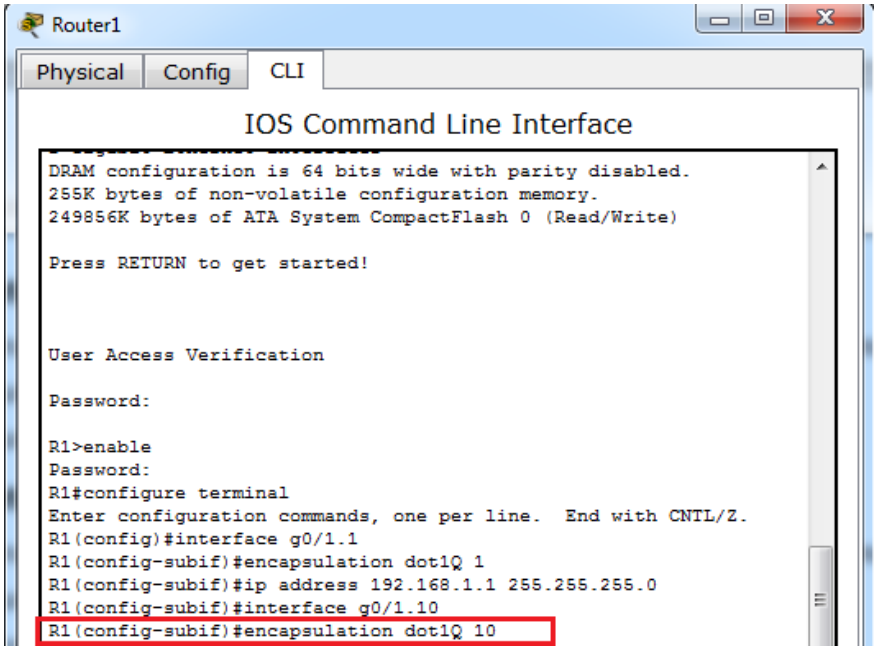
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 2. Configurar una subinterfaz para la VLAN 10.

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

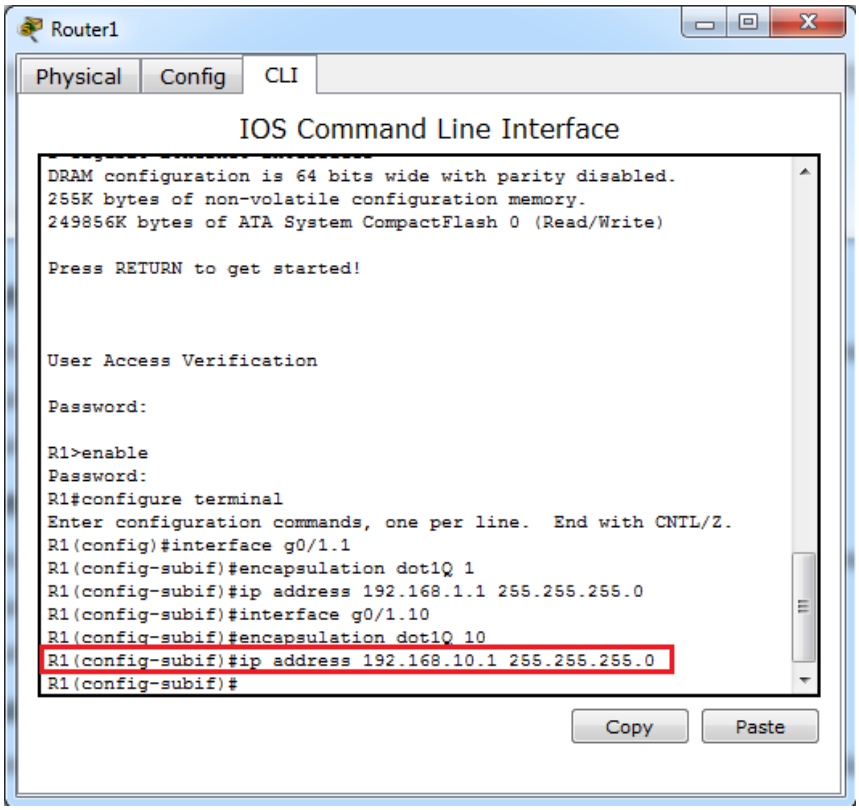


b. Configure la subinterfaz para que opere en la VLAN 10.



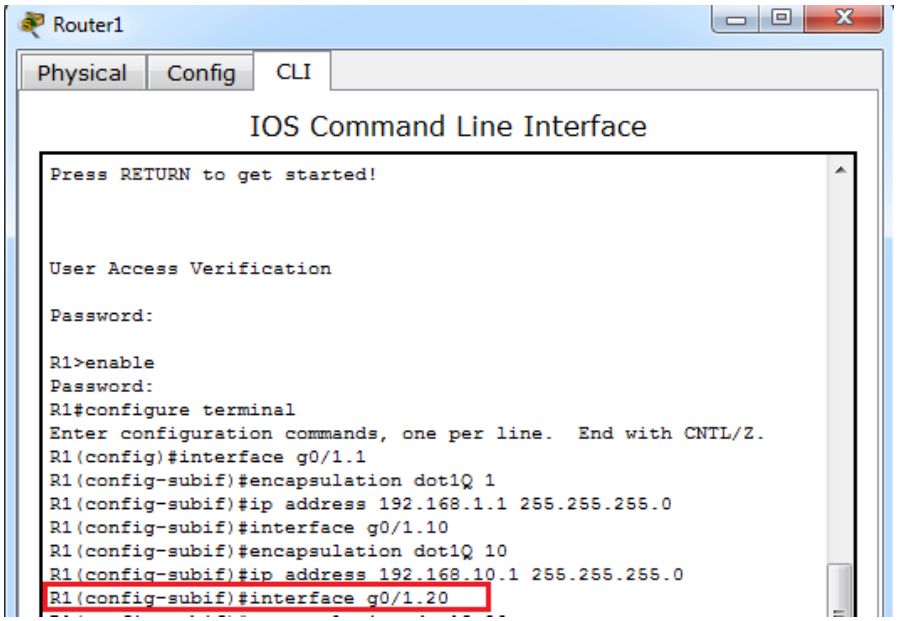
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



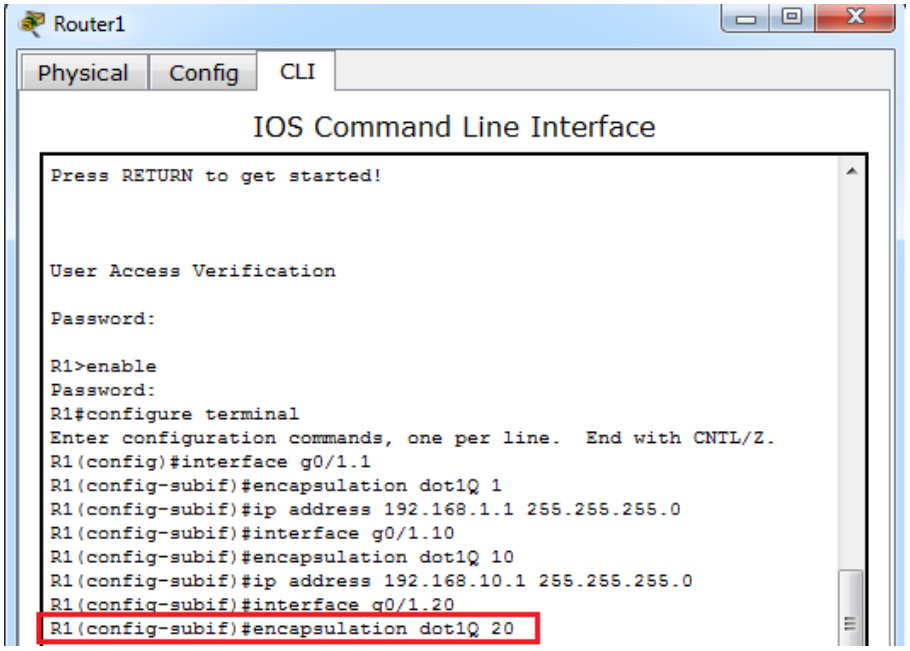
Paso 3. Configurar una subinterfaz para la VLAN 20.

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

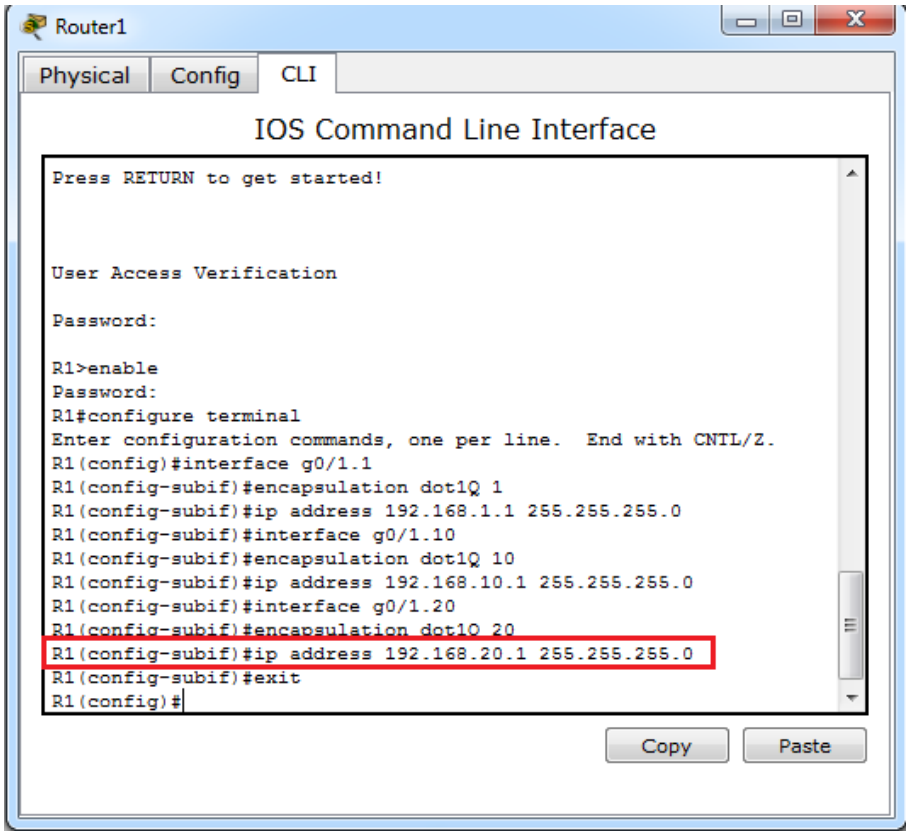


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



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

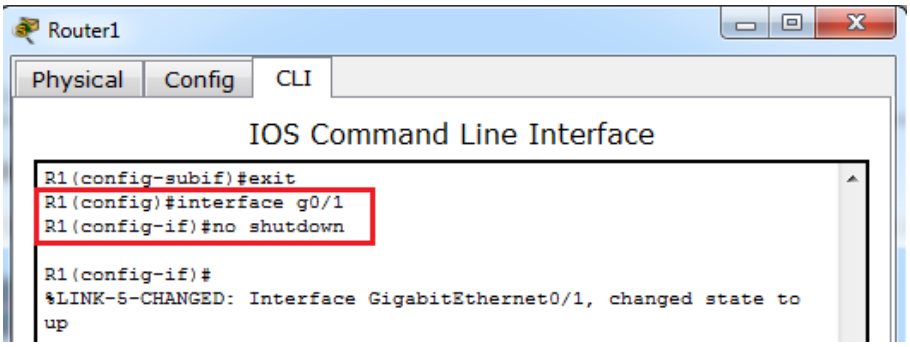


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 4. Habilitar la interfaz G0/1.

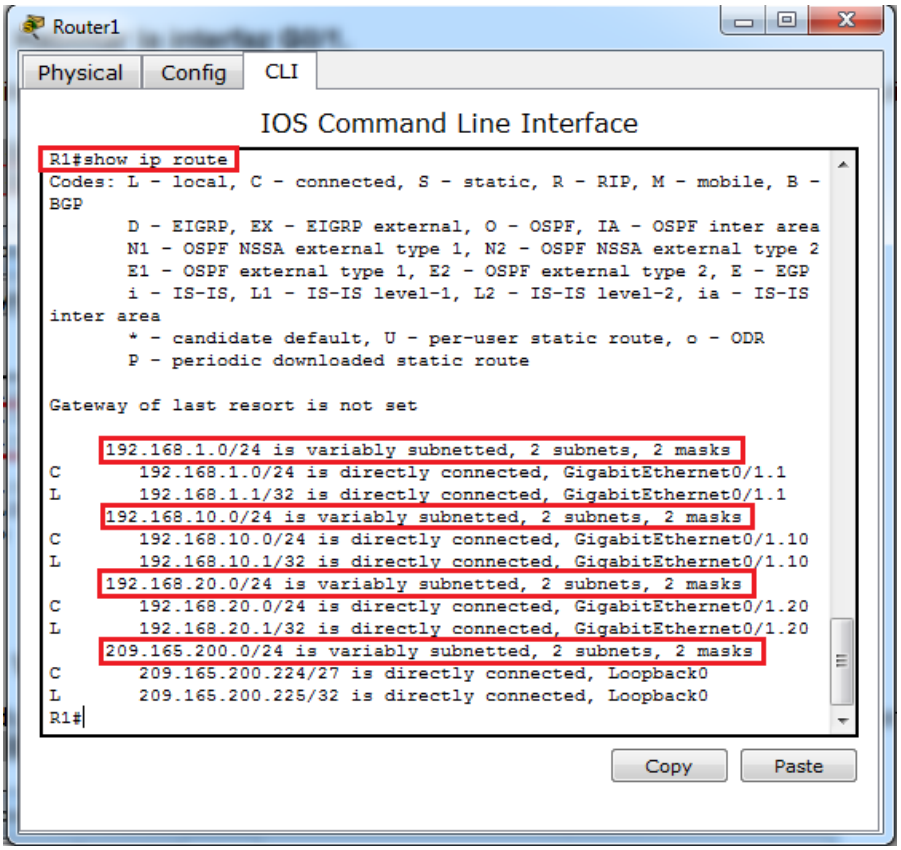
Habilite la interfaz G0/1. En el espacio proporcionado, escriba los comandos que utilizó.

```
R1(config)# interface g0/1
R1(config-if)# no shutdown
```



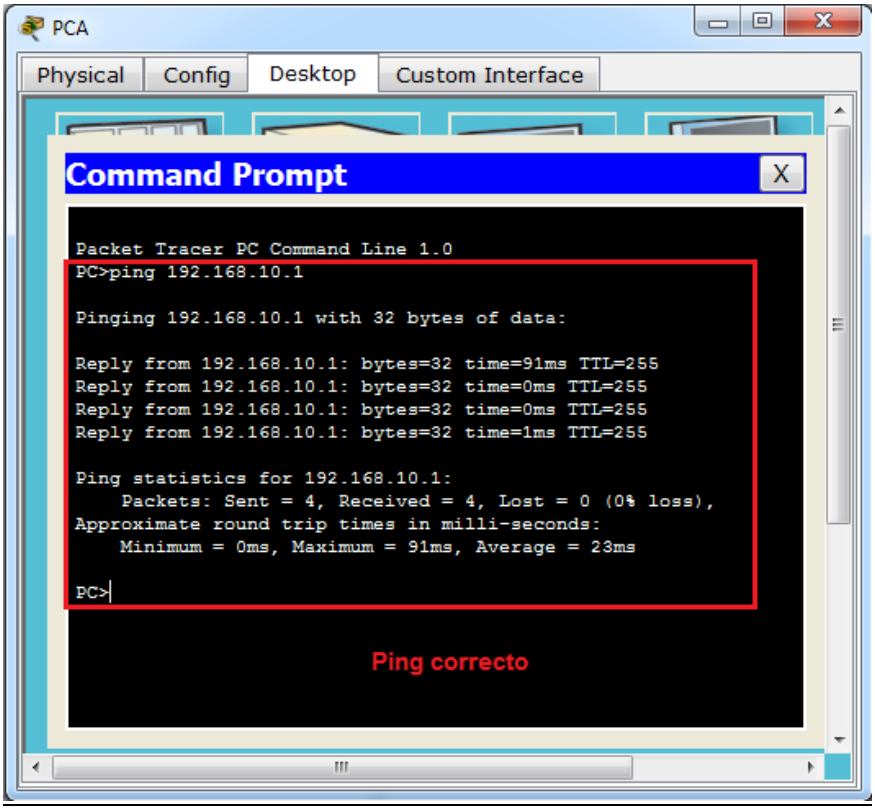
Paso 5. Verifique la conectividad.

Introduzca el comando para ver la tabla de routing en el R1. ¿Qué redes se enumeran?
192.168.1.0, 192.168.10.0, 192.168.20.0, y 209.165.200.224

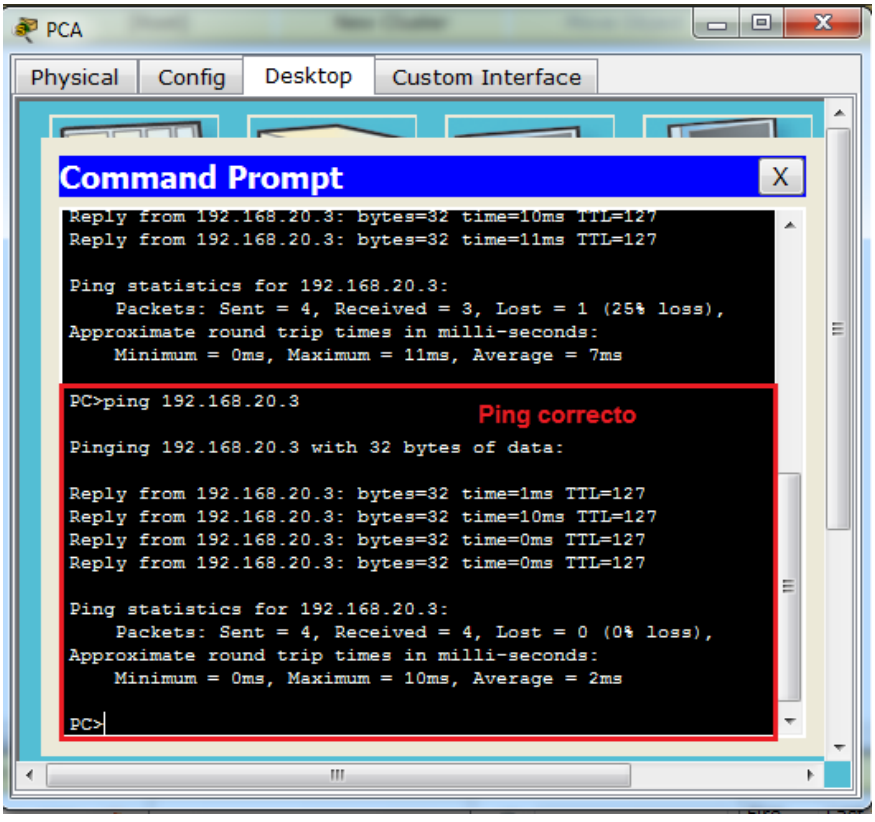


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

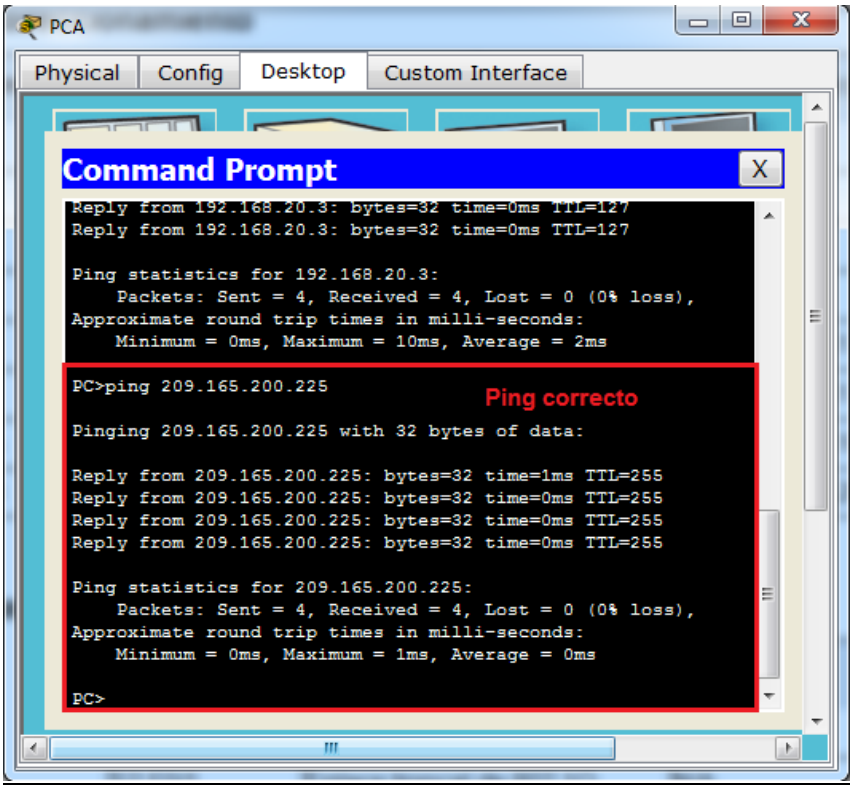


¿Es posible hacer ping de la PC-A a la PC-B? Si

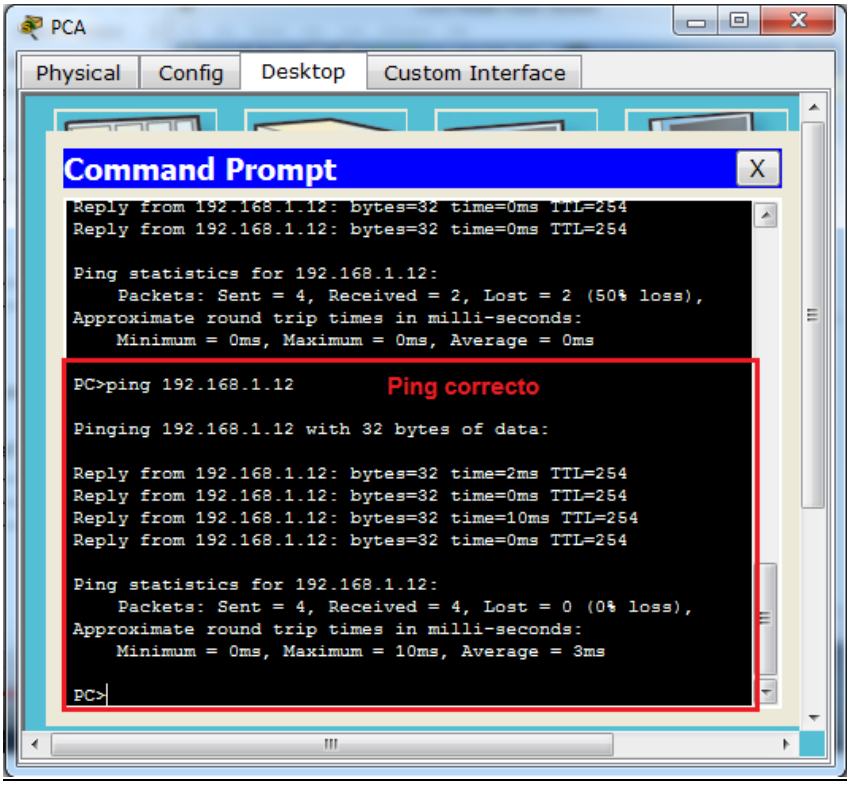


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

¿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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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 enrutamiento inter-VLAN en un Router-on-a-stick permite que una interfaz se dirija a VLANs múltiples a diferencia del método inter-VLAN 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.				

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 11

- En la práctica realizada se hacen las prácticas para poder armar primero, la red y configurar los parámetros básicos de los dispositivos, el router, los dos switches, y los dos pcs, luego se configuran igualmente los switches con vlan y enlaces troncales. Para finalizar la práctica configuramos el routing entre vlan y lo basamos en enlaces troncales.
- Aprendimos a conectar los equipos entre si verificando esas conexiones con el programa de simulación Packet Tracer.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 12: 6.2.2.5 Lab - Configuring IPv4 Static and Default Routes

Práctica de laboratorio: configuración de rutas estáticas y predeterminadas IPv4

Topología

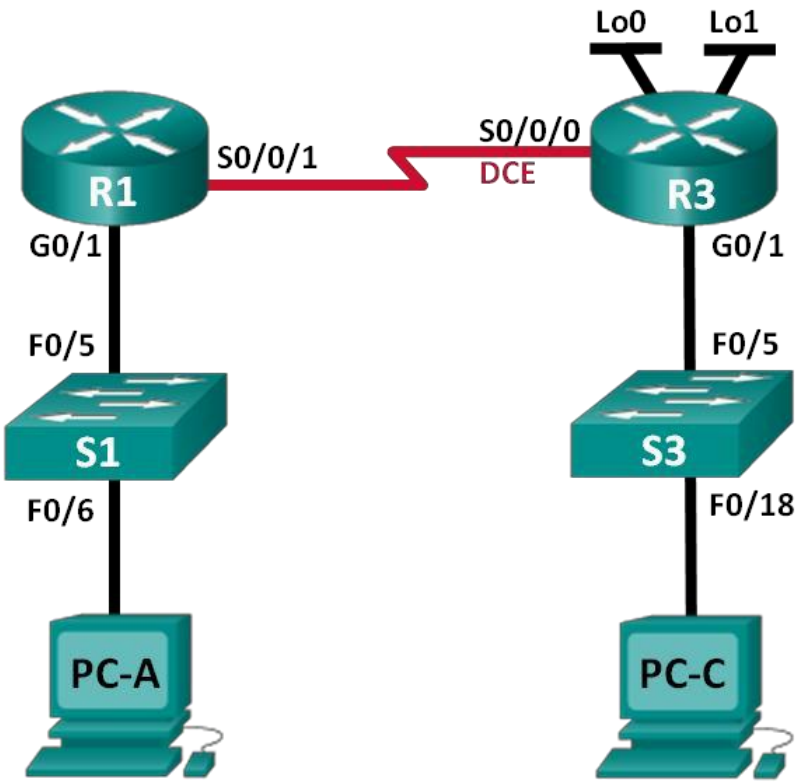


Tabla de direccionamiento

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

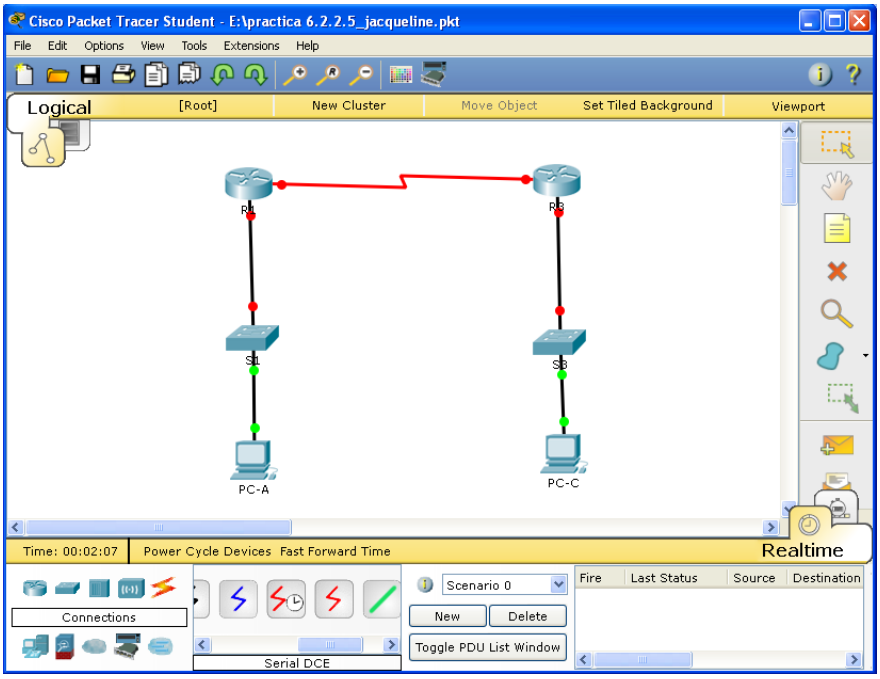
Recursos necesarios

- 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

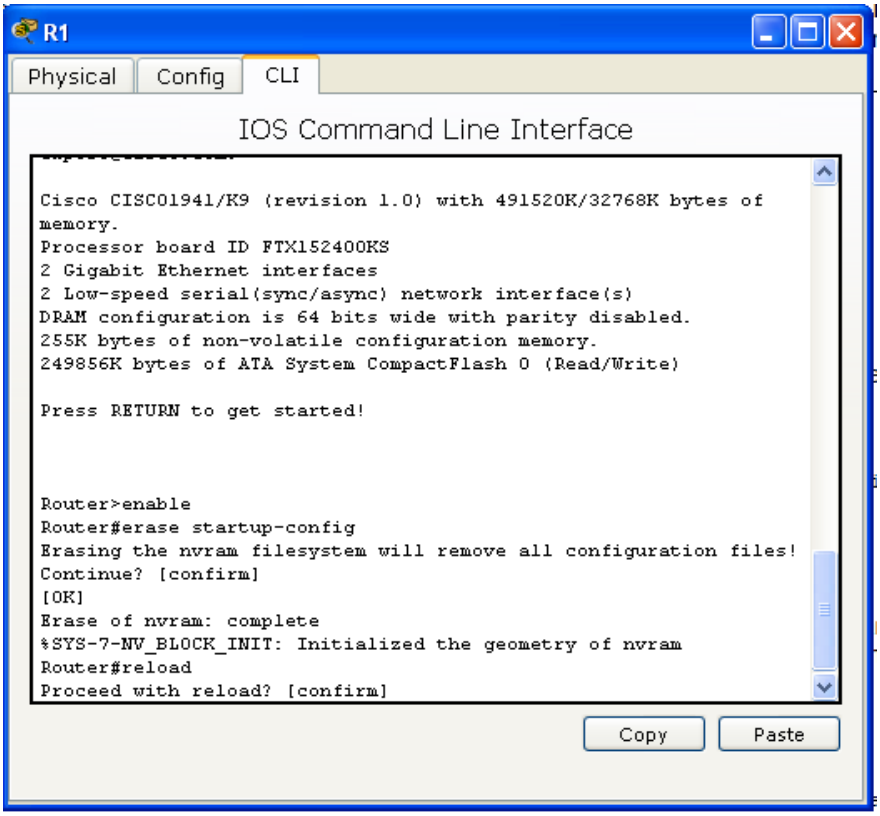
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 1. Establecer la topología e inicializar los dispositivos

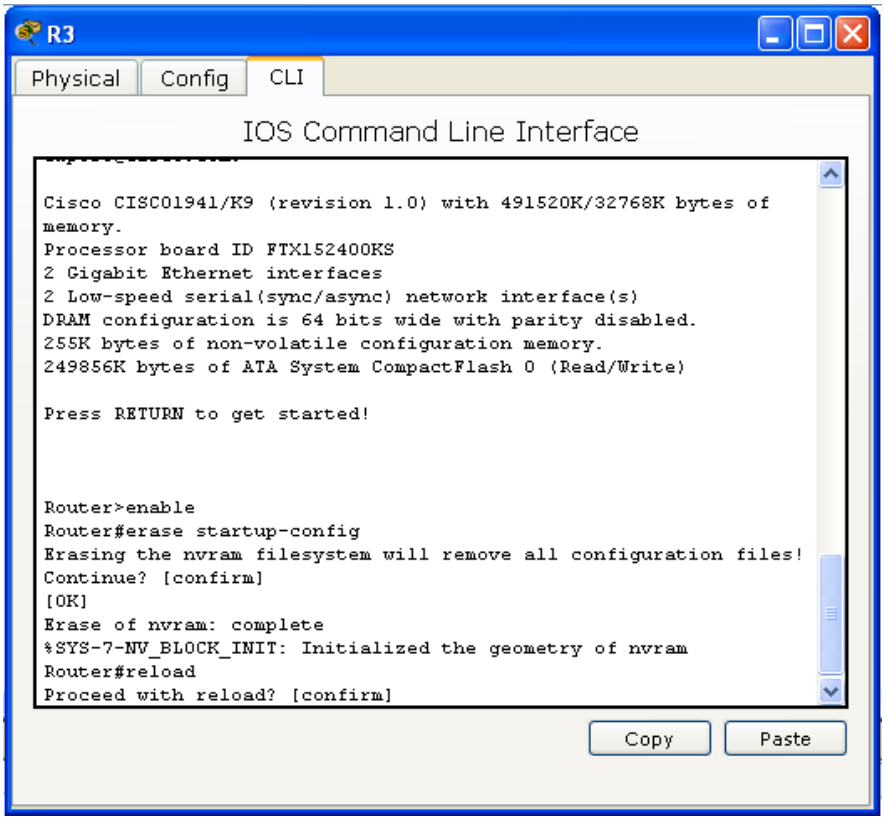
Paso 1. Realizar el cableado de red tal como se muestra en la topología.

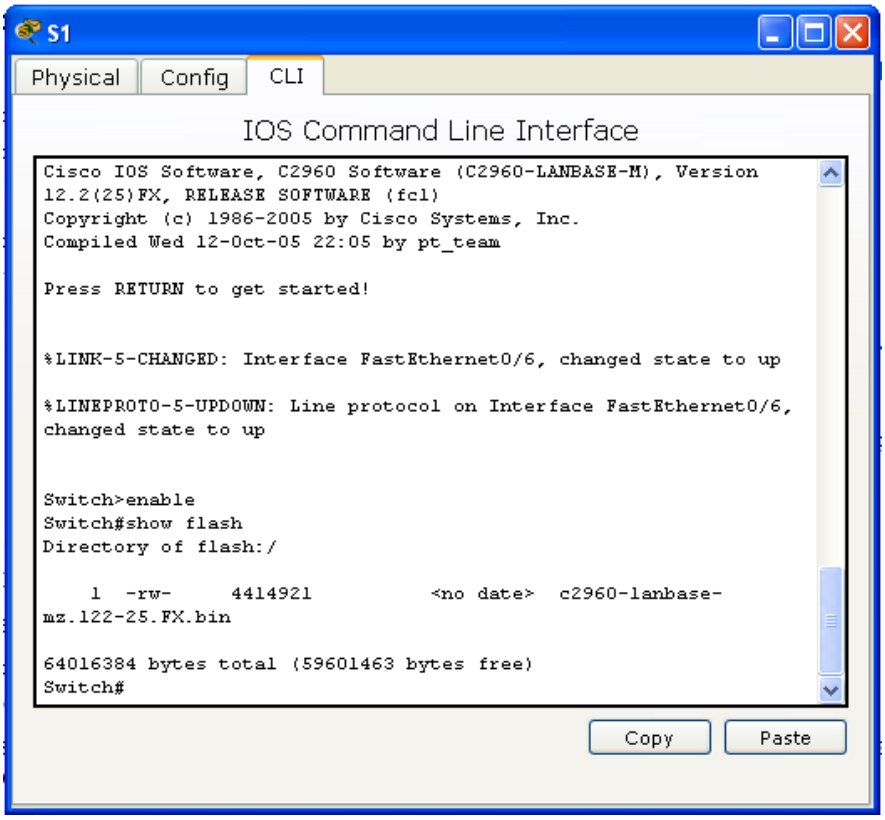


Paso 2. Inicializar y volver a cargar el router y el switch.

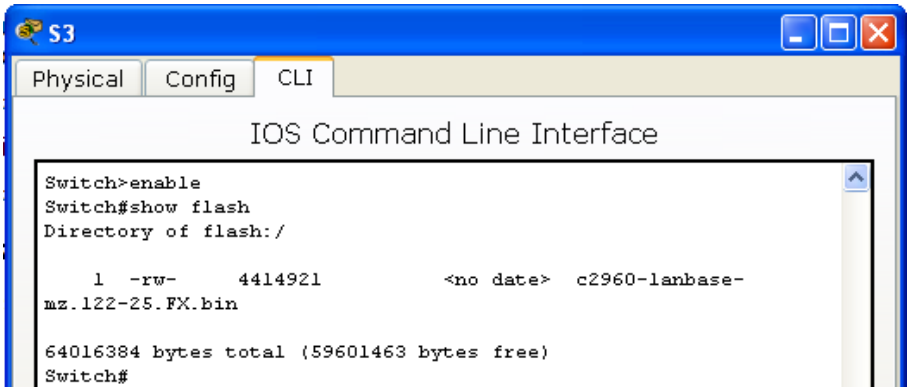


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.





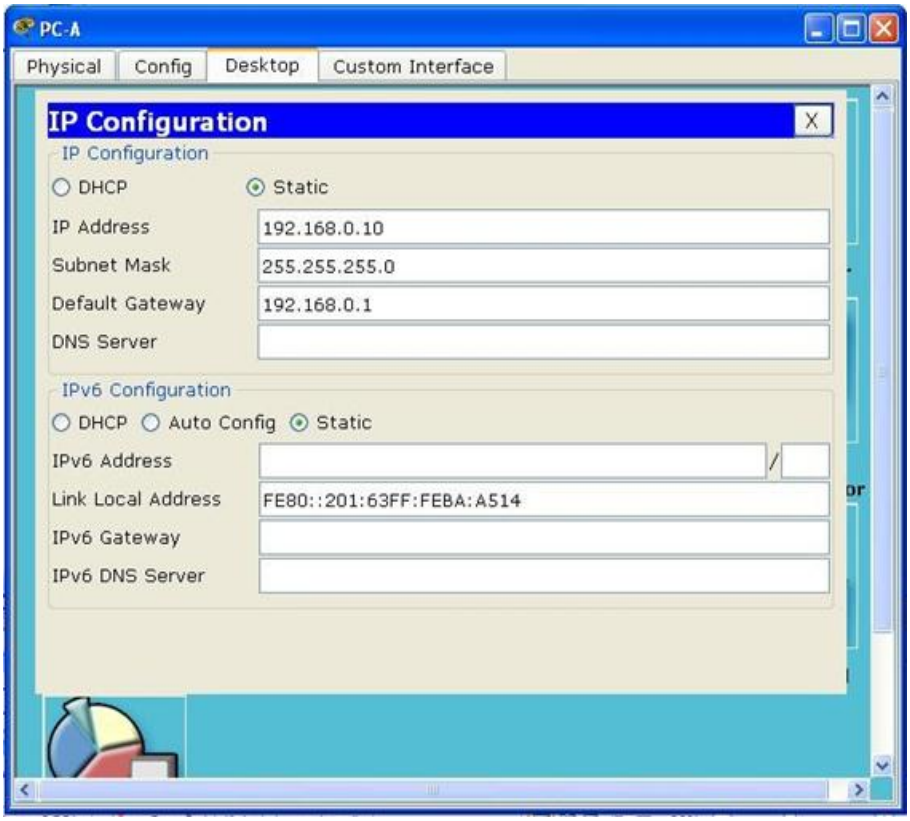
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



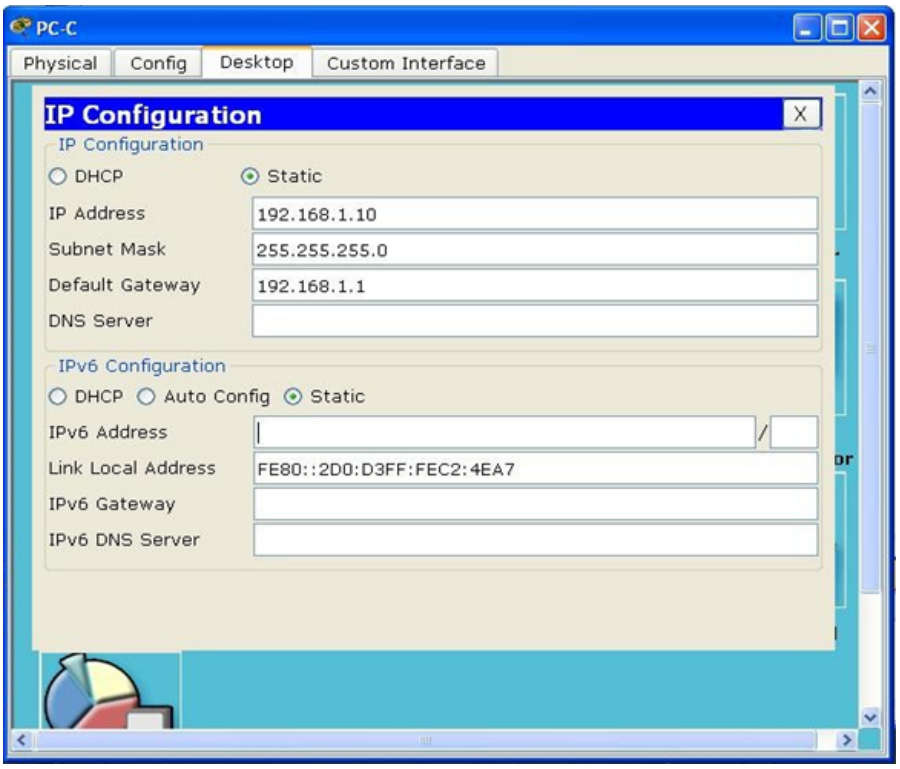
Parte 2. Configurar los parámetros básicos de los dispositivos y verificar la conectividad

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.

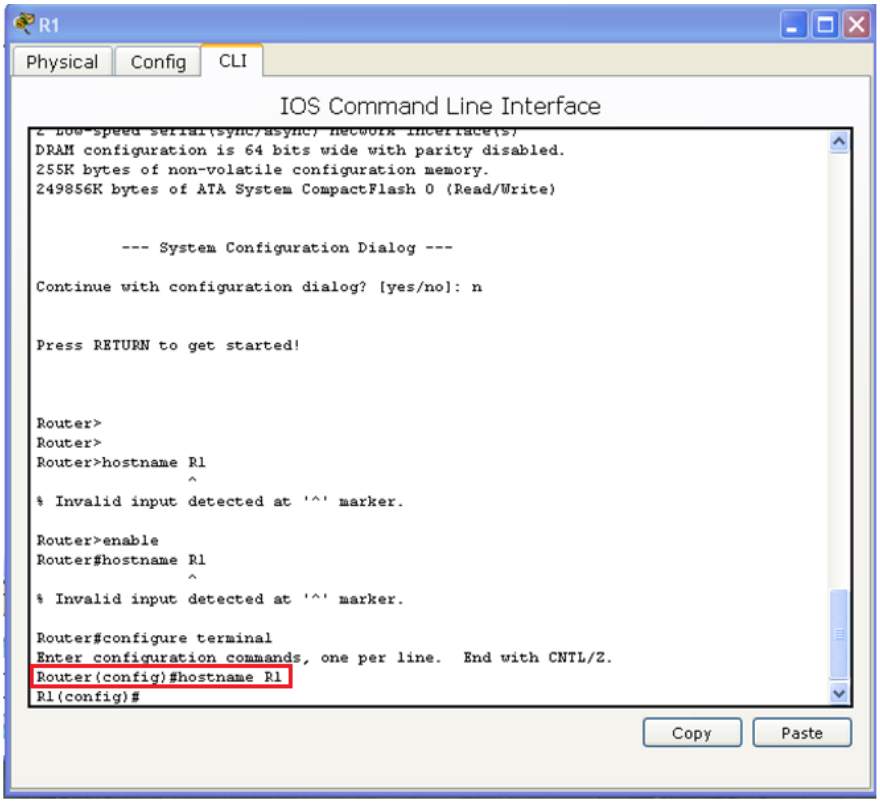


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

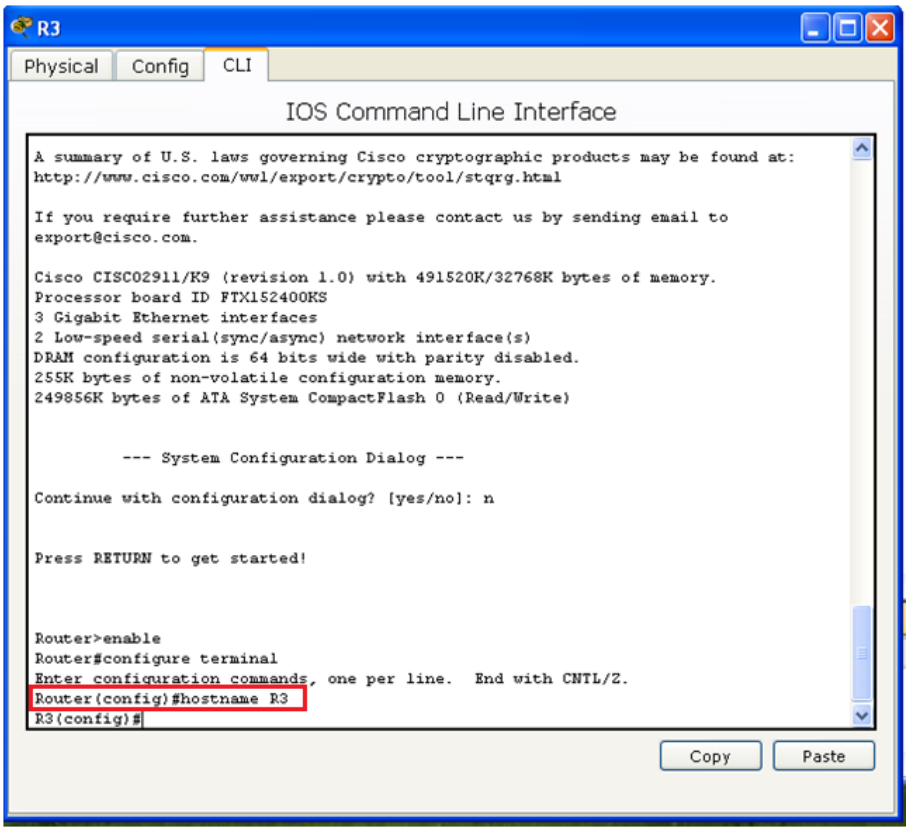


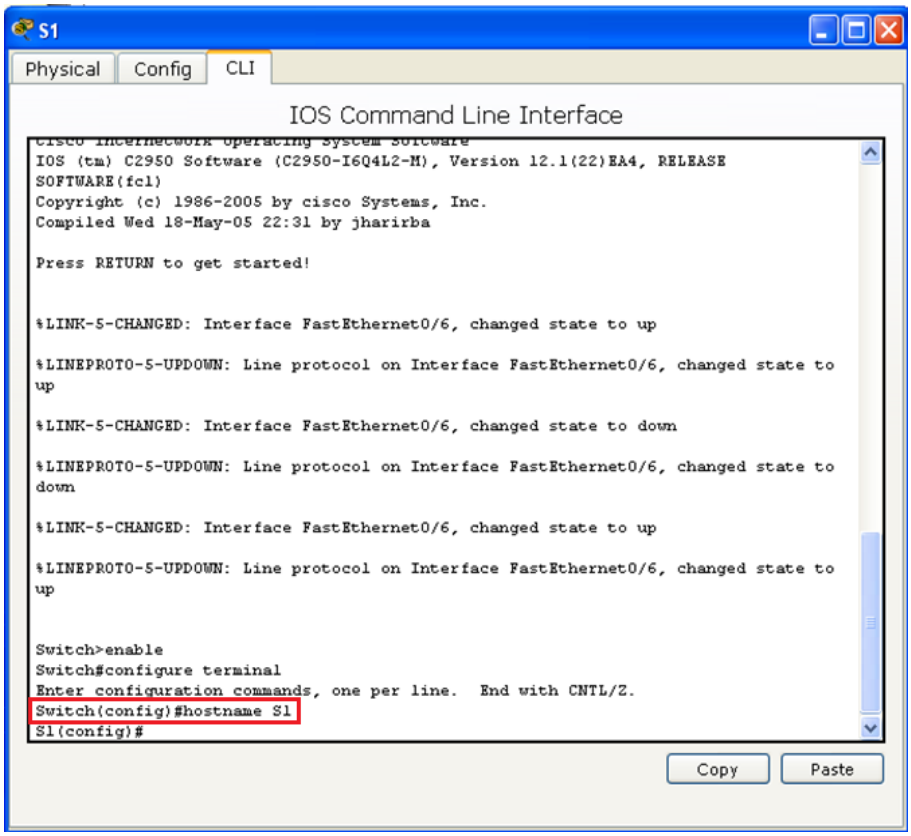
Paso 2. Configurar los parámetros básicos en los routers.

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

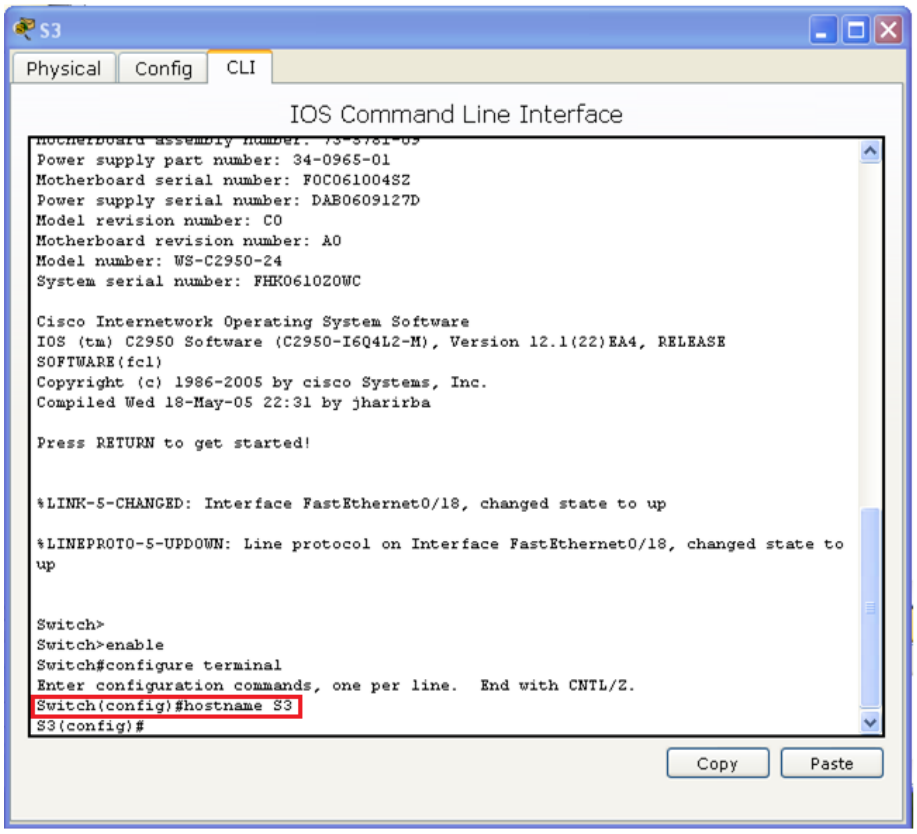


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

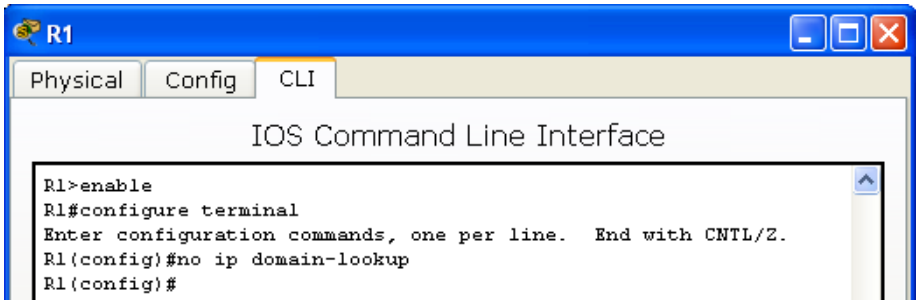


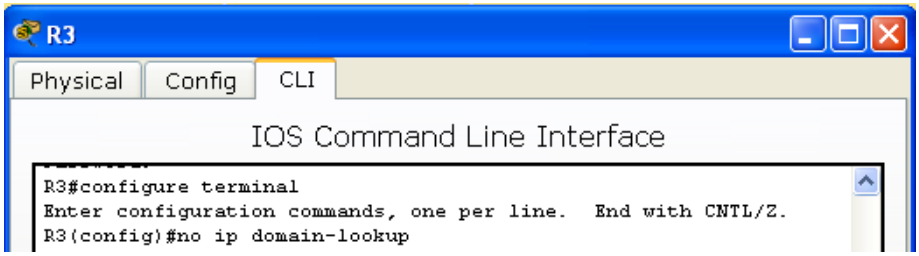


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

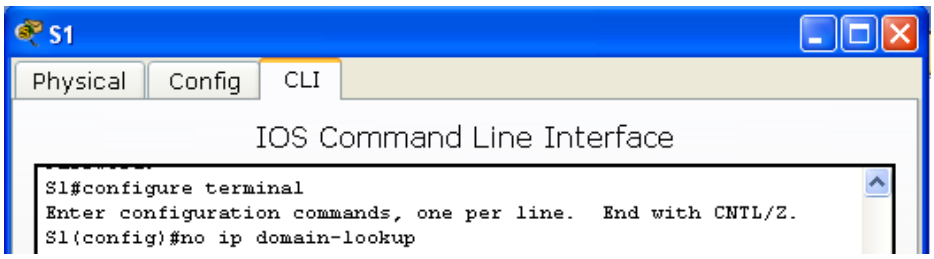


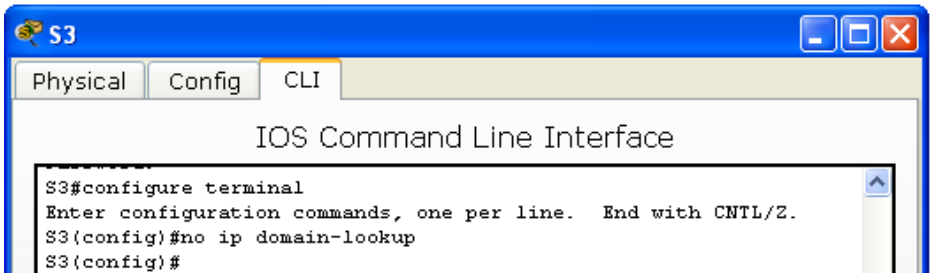
b. Desactive la búsqueda del DNS.



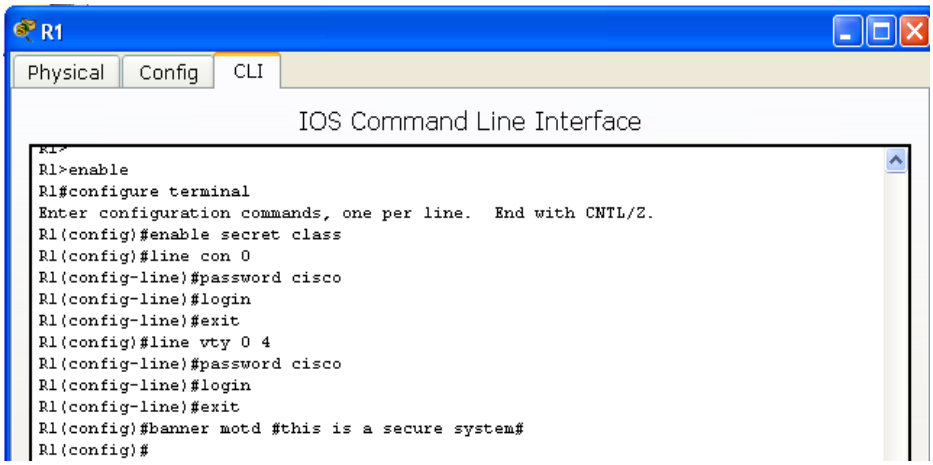


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

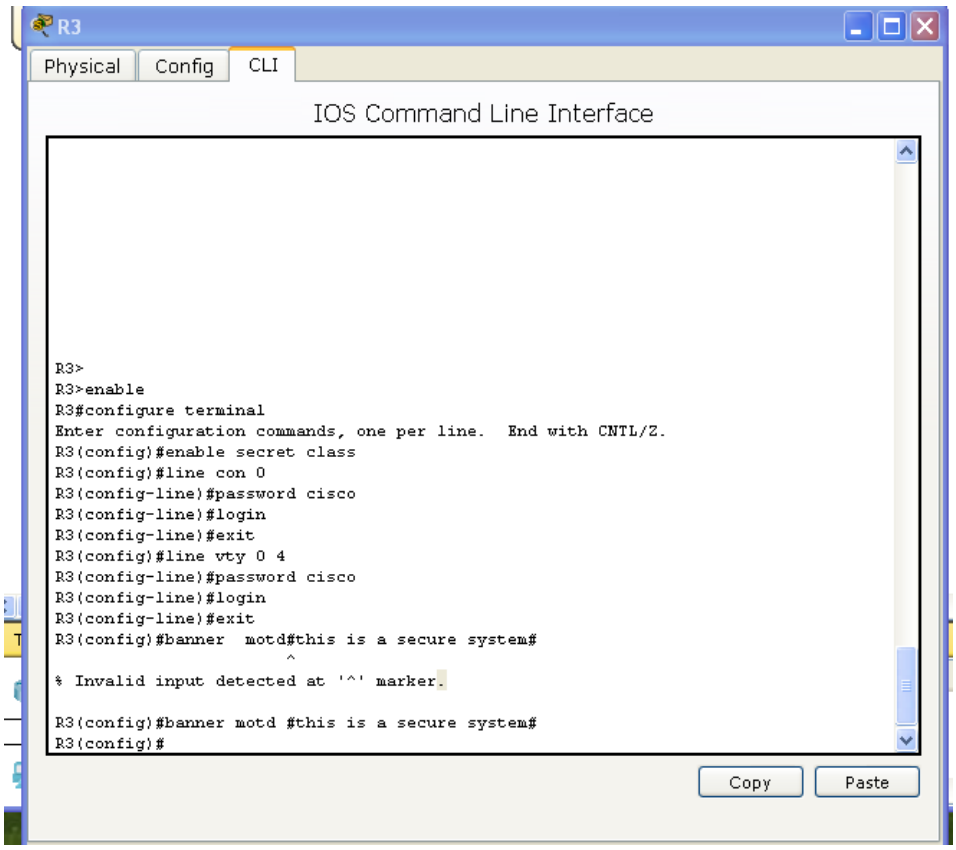


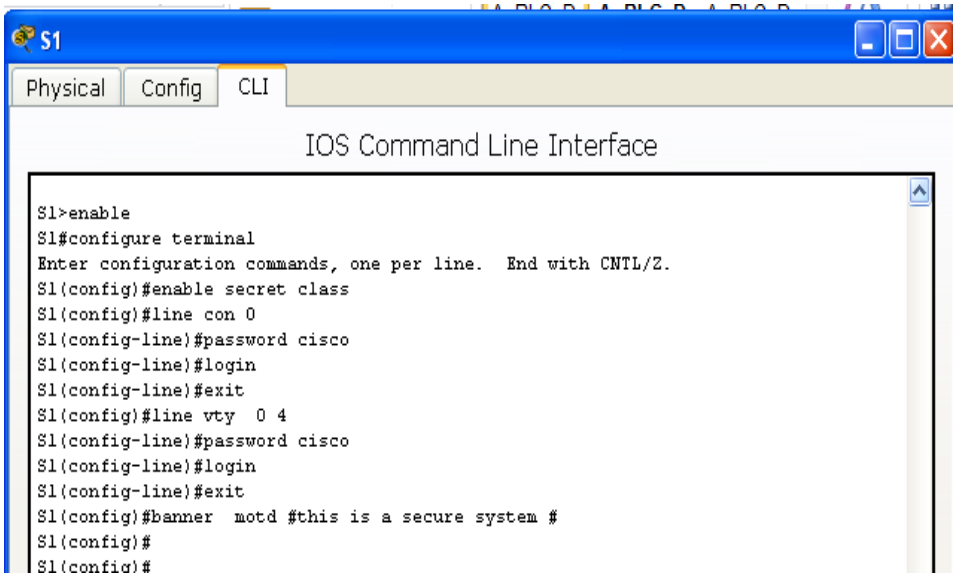


c. Asigne **class** como la contraseña de enable y asigne **cisco** como la contraseña de consola y la contraseña de vty.

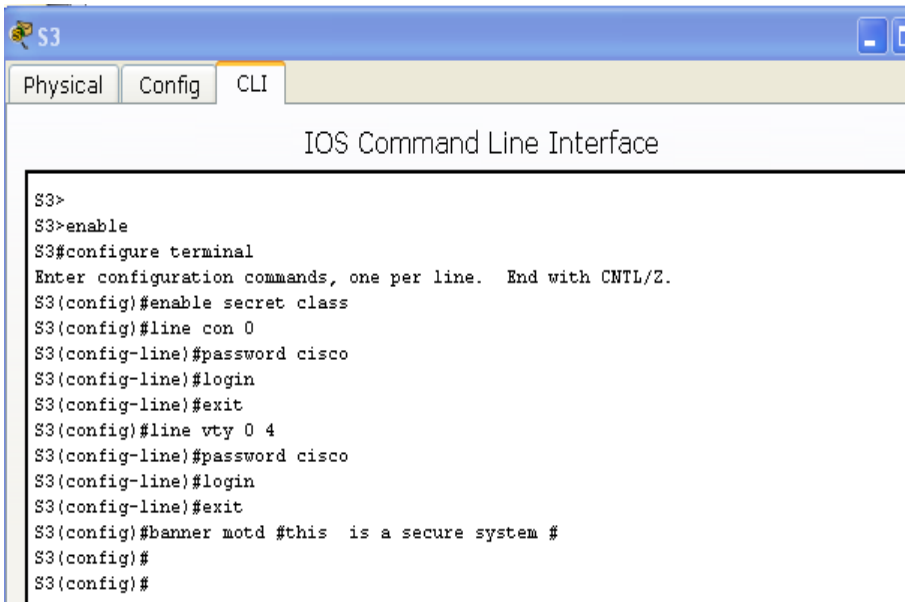


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

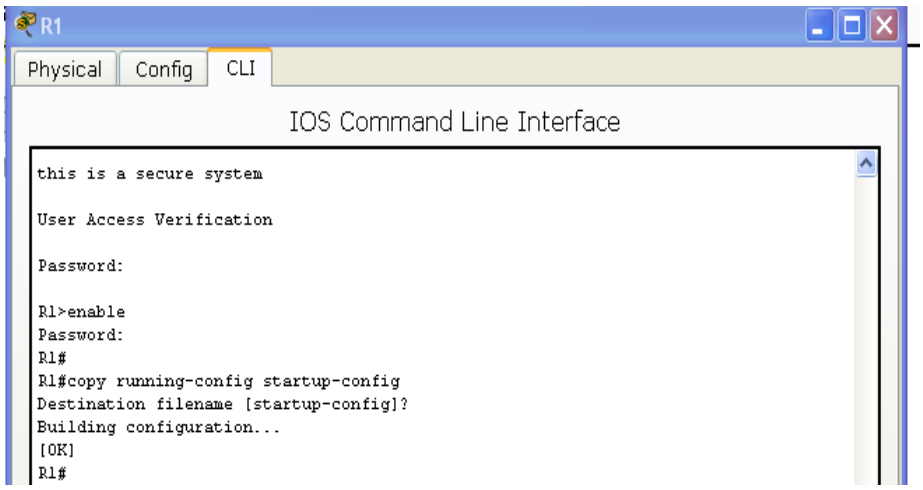


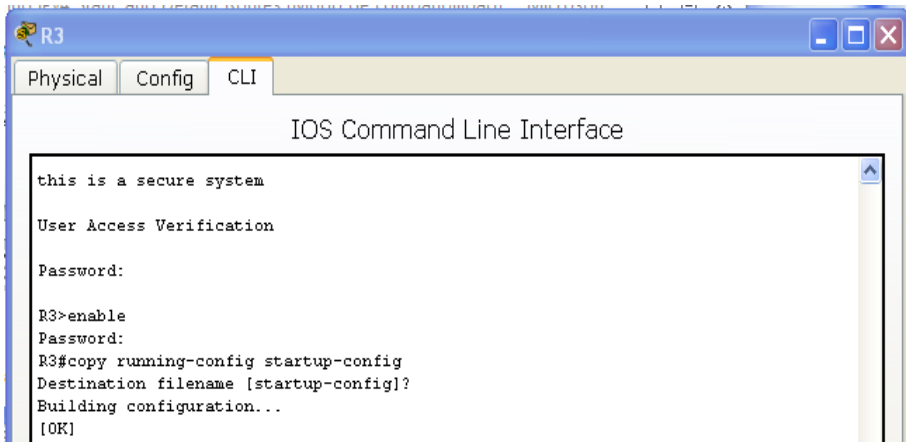


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

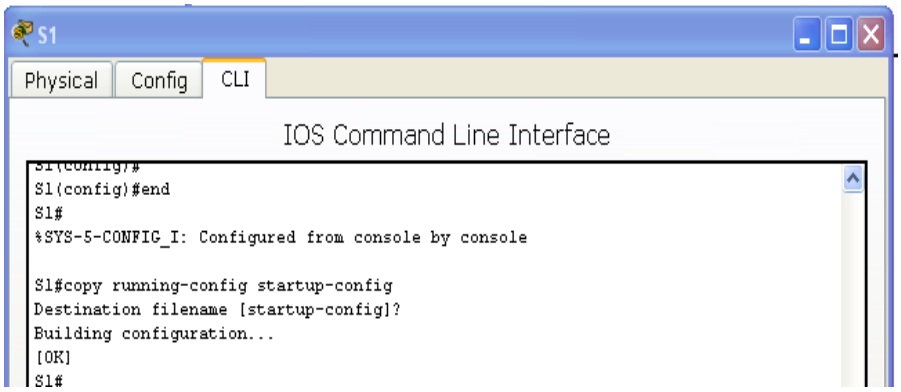


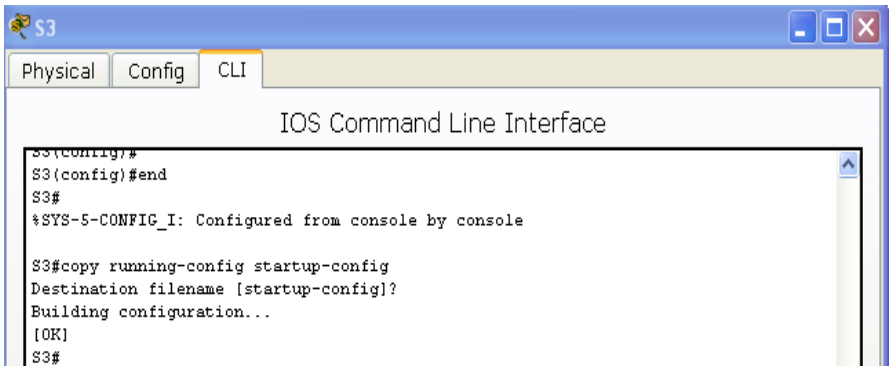
d. Guarde la configuración en ejecución en el archivo de configuración de inicio.





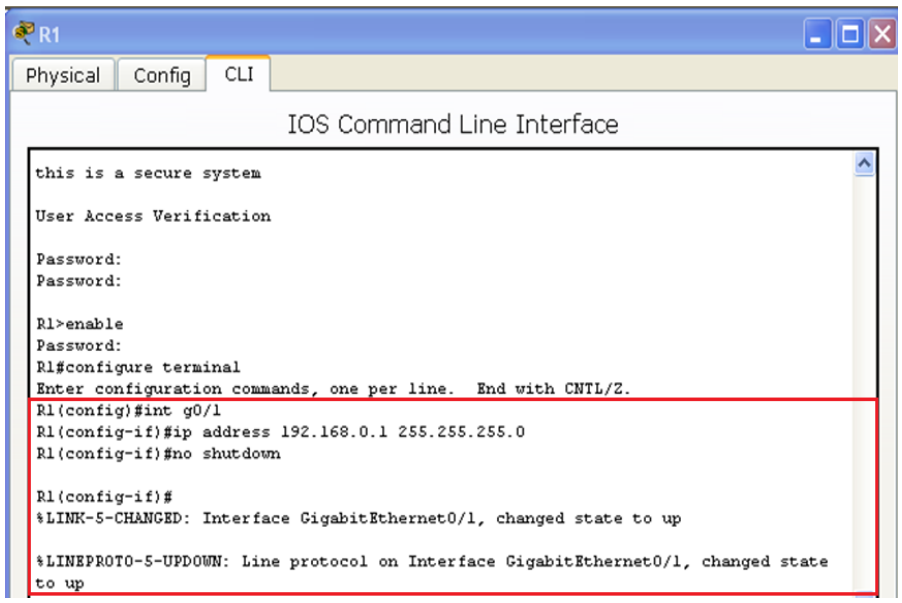
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



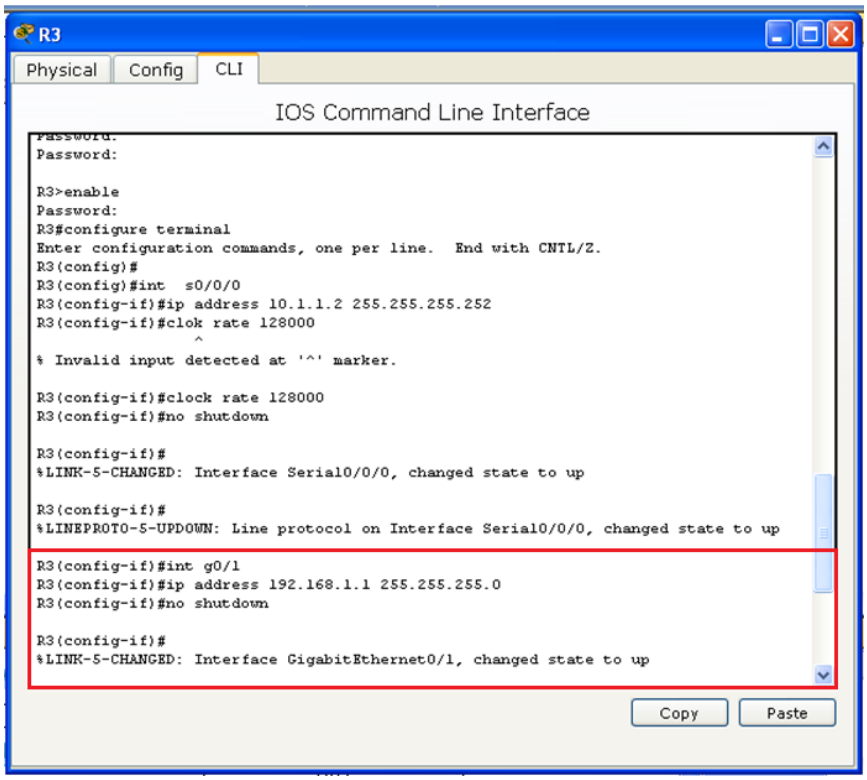


Paso 3. Configurar los parámetros IP en los routers.

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

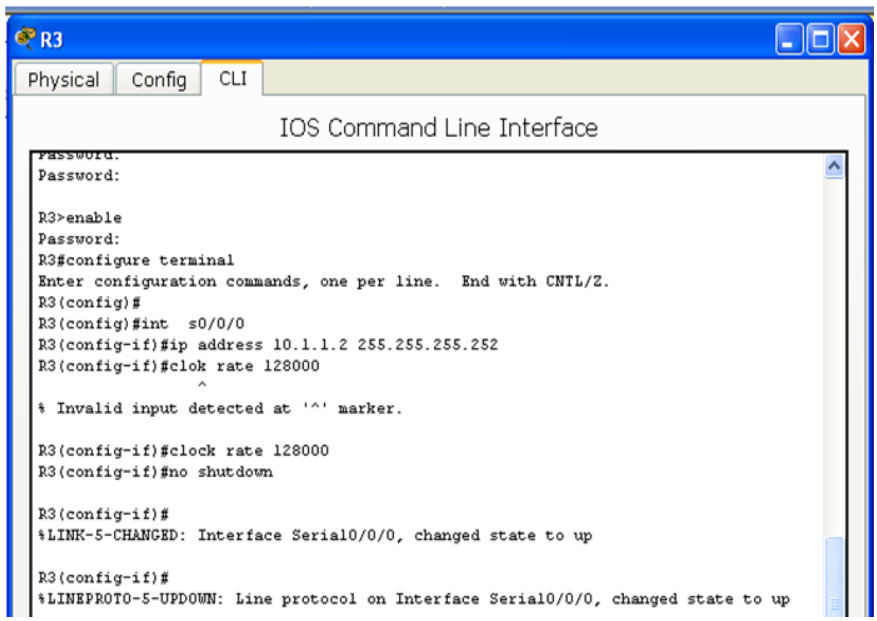


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



b. 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
```

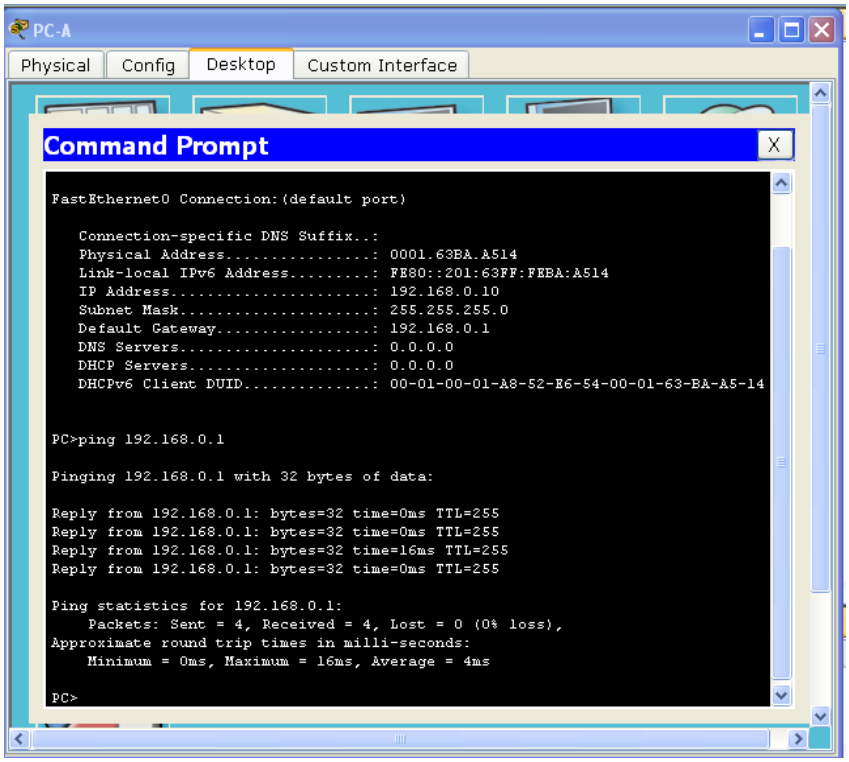


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

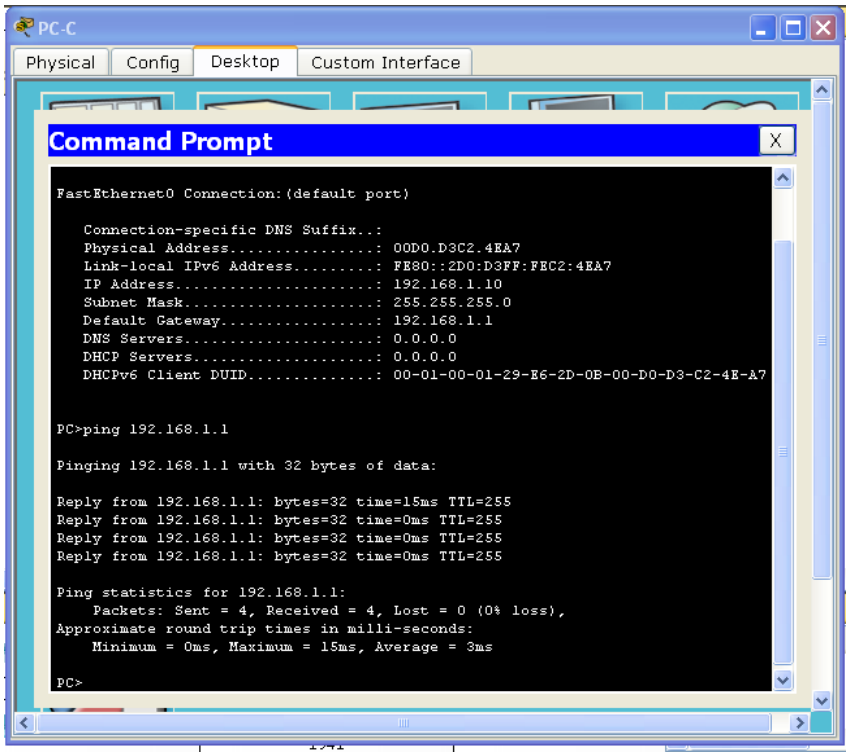
Paso 4. Verificar la conectividad de las LAN.

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



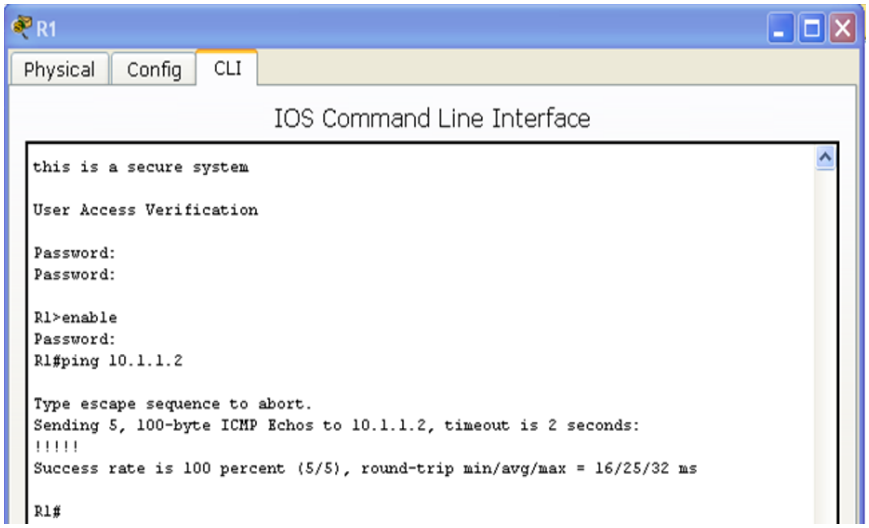
¿Es posible hacer ping de la PC-C al gateway predeterminado? Si



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

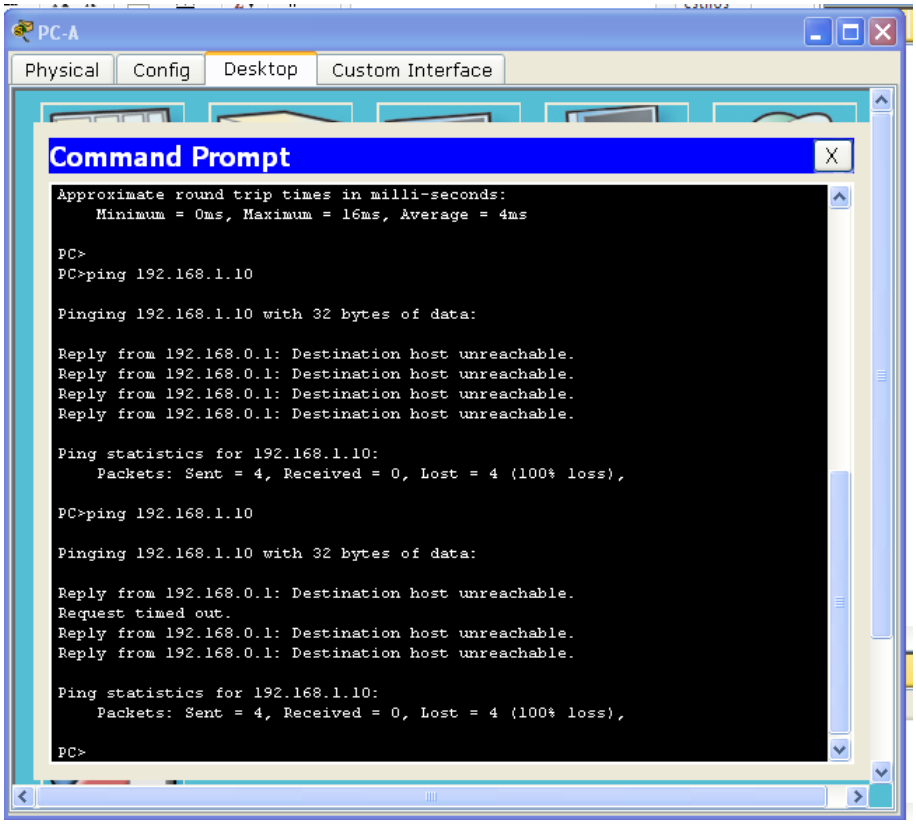
¿Es posible hacer ping del R1 a la interfaz S0/0/0 del R3? Si



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

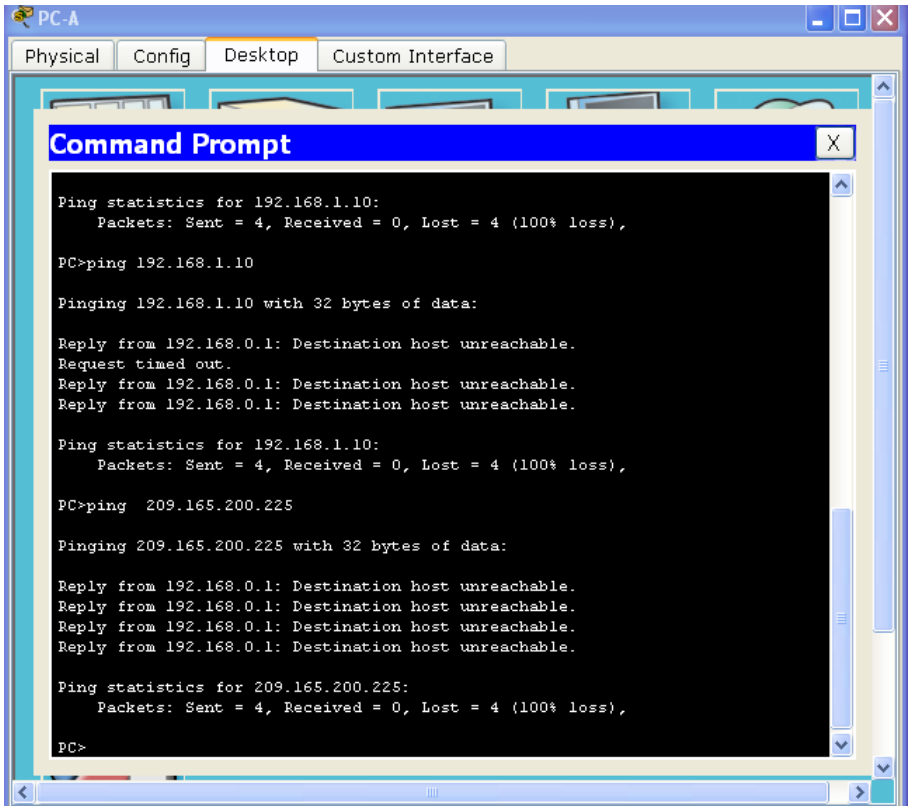
c. Pruebe la conectividad entre los dispositivos que no están conectados directamente.

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

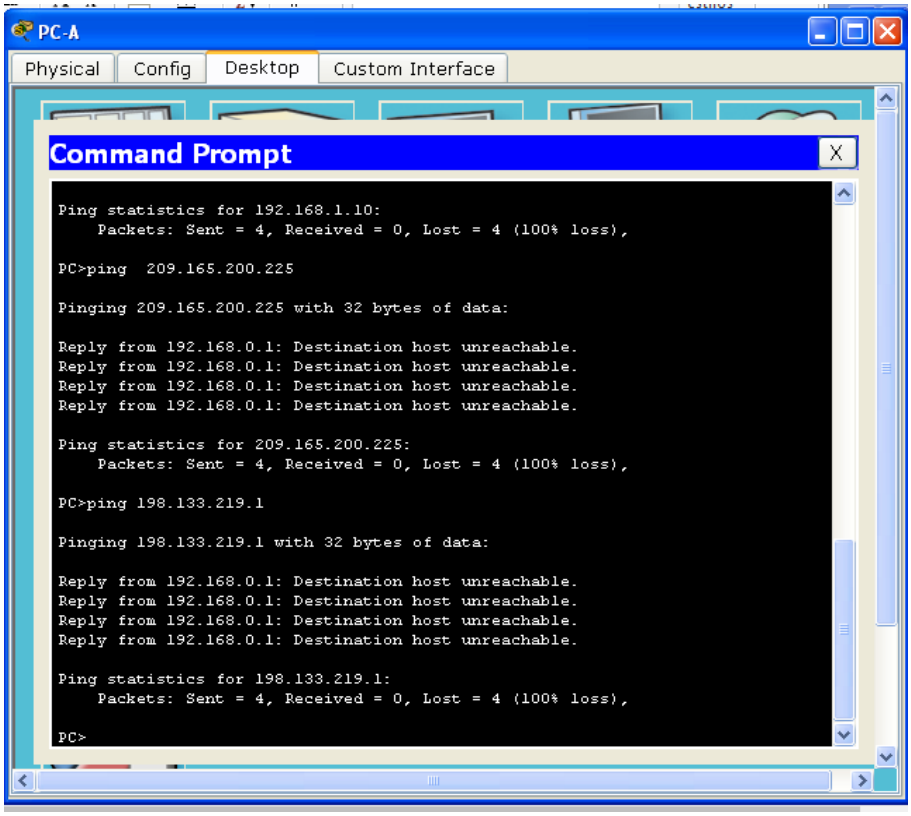


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

¿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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

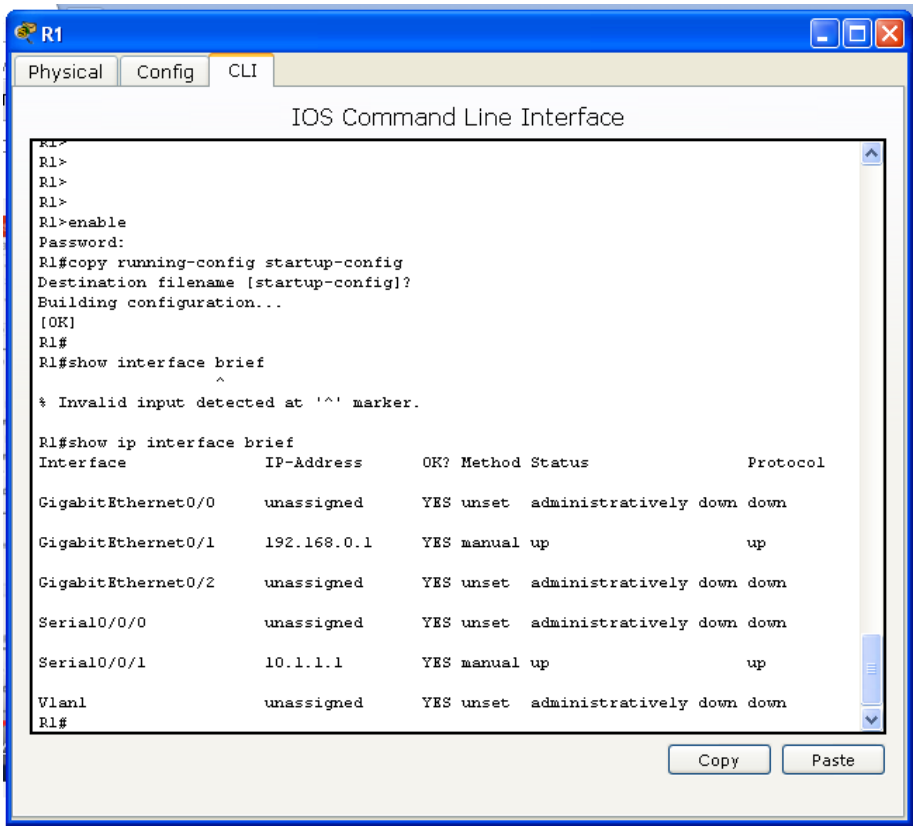
¿Los pings eran correctos? ¿Por qué o por qué no?

No hay comunicación porque el router no tiene rutas hacia redes distantes

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

Paso 5. Reunir información.

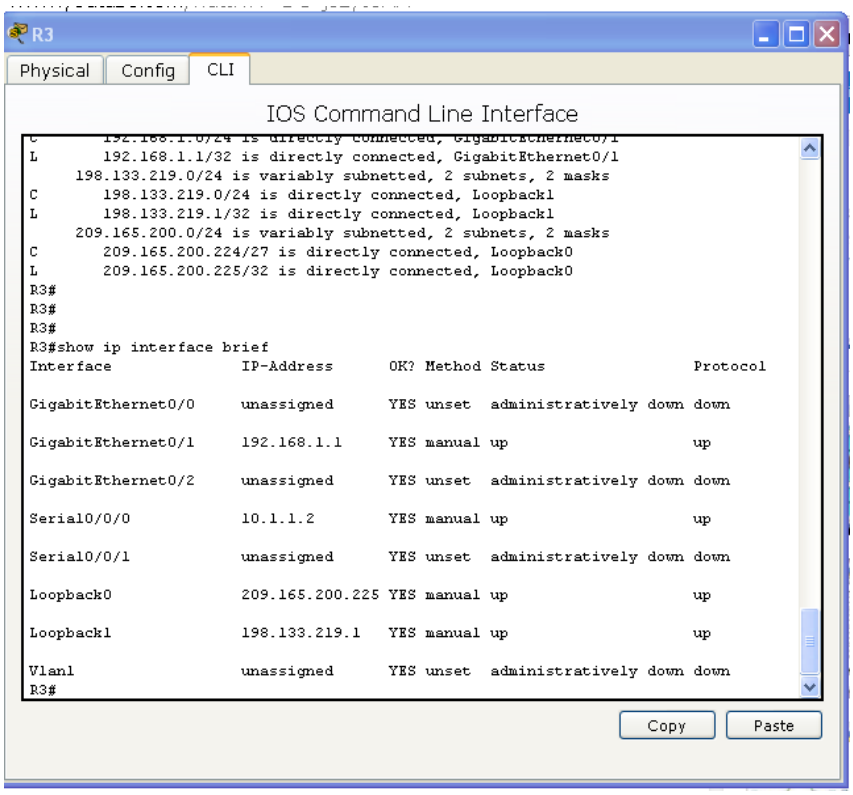
a. Revise el estado de las interfaces en el R1 con el comando **show ip interface brief**.



¿Cuántas interfaces están activadas en el R1? 2

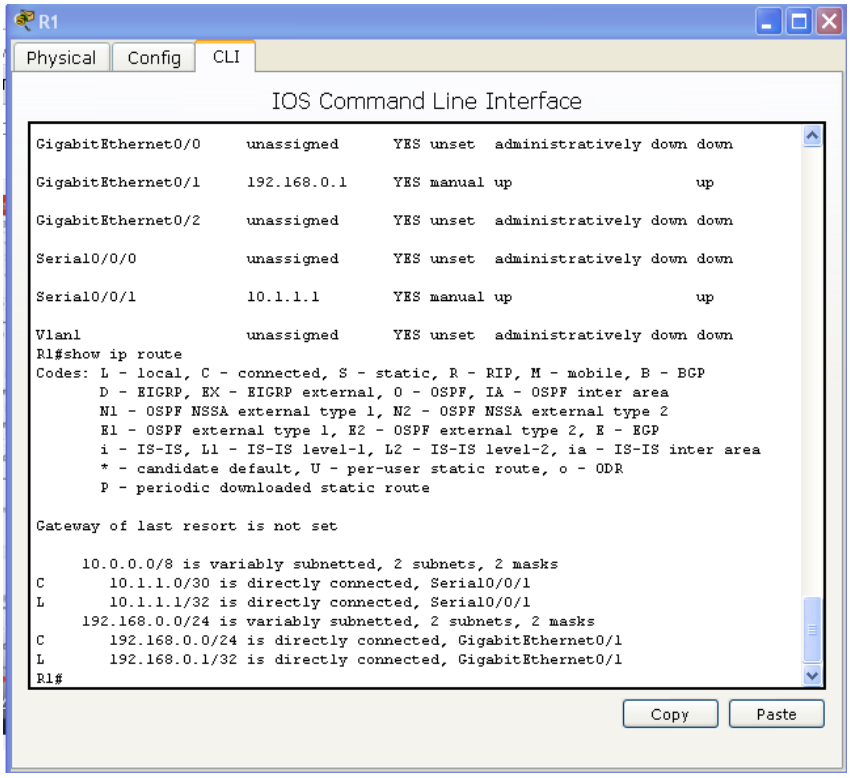
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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**.

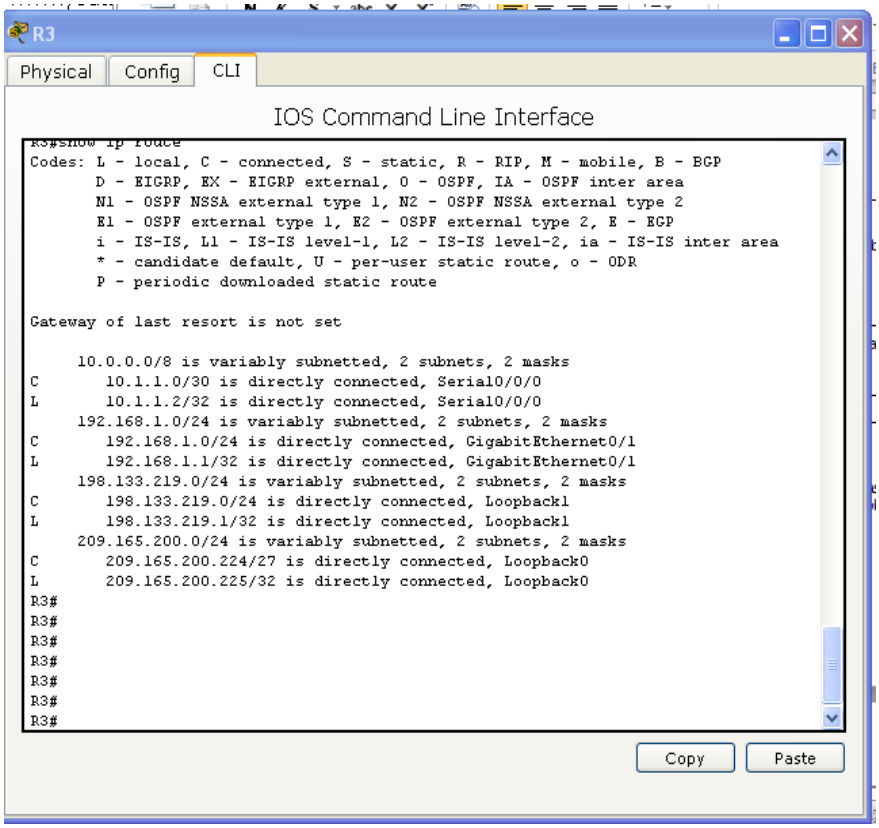


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

192.168.1.0, 198.133.219.0, 209.165.200.224

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 no están configurados con un protocolo de ruteo estático o dinamico y solo conocen sus redes directamente conectadas.

Parte 3. 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.

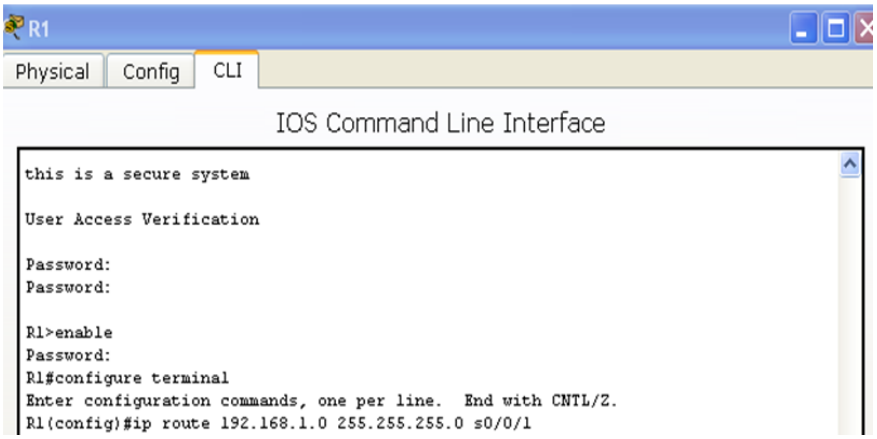
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 1. Configure una ruta estática recursiva.

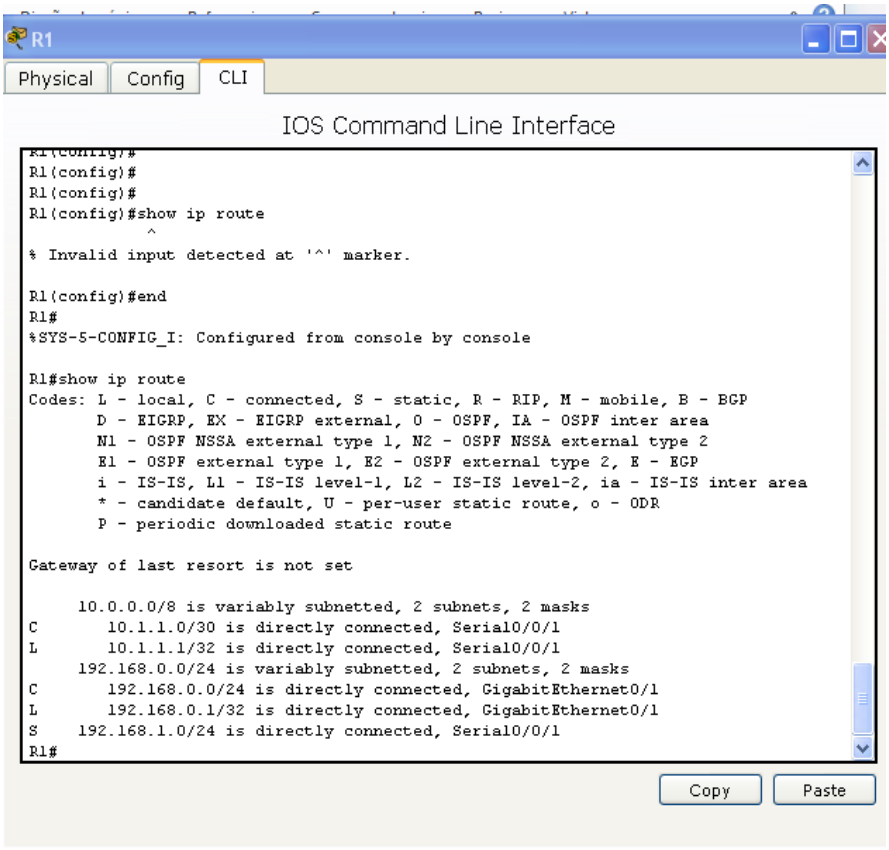
Con una ruta estática recursiva, se especifica la dirección IP del siguiente salto. Debido a que solo se especifica la IP de siguiente salto, el router tiene que hacer varias búsquedas en la tabla de routing antes de reenviar paquetes. Para configurar rutas estáticas recursivas, utilice la siguiente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

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

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



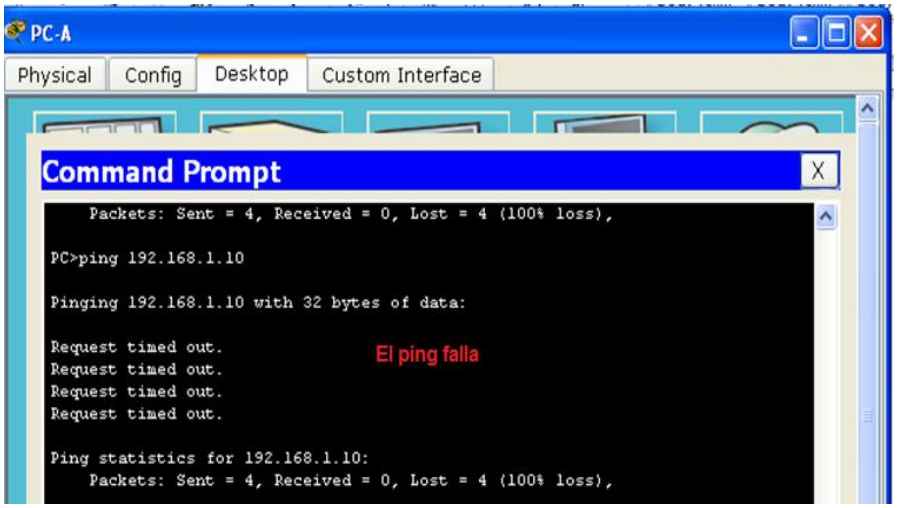
b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

¿Cómo se indica esta ruta nueva en la tabla de routing?
La red 192.168.0.0/24 está directamente conectada a través del puerto serial 0/0/0 del R3. Se debe configurar el R1 y R3 con una rutas estáticas respectivamente., para que hayan rutas de retorno cuando el pc destino envía su respuesta.

¿Es posible hacer ping del host PC-A host a al host PC-C? No



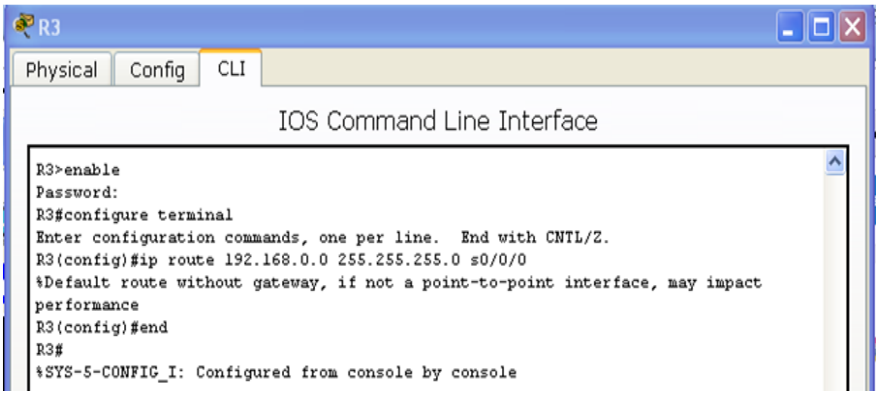
Estos pings deben fallar. Si la ruta estática recursiva se configuró correctamente, el ping llega a la PC-C. La PC-C envía un ping de respuesta a la PC-A. Sin embargo, este ping se descarta en el R3, porque el R3 no tiene una ruta de retorno a la red 192.168.0.0 en la tabla de routing.

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.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

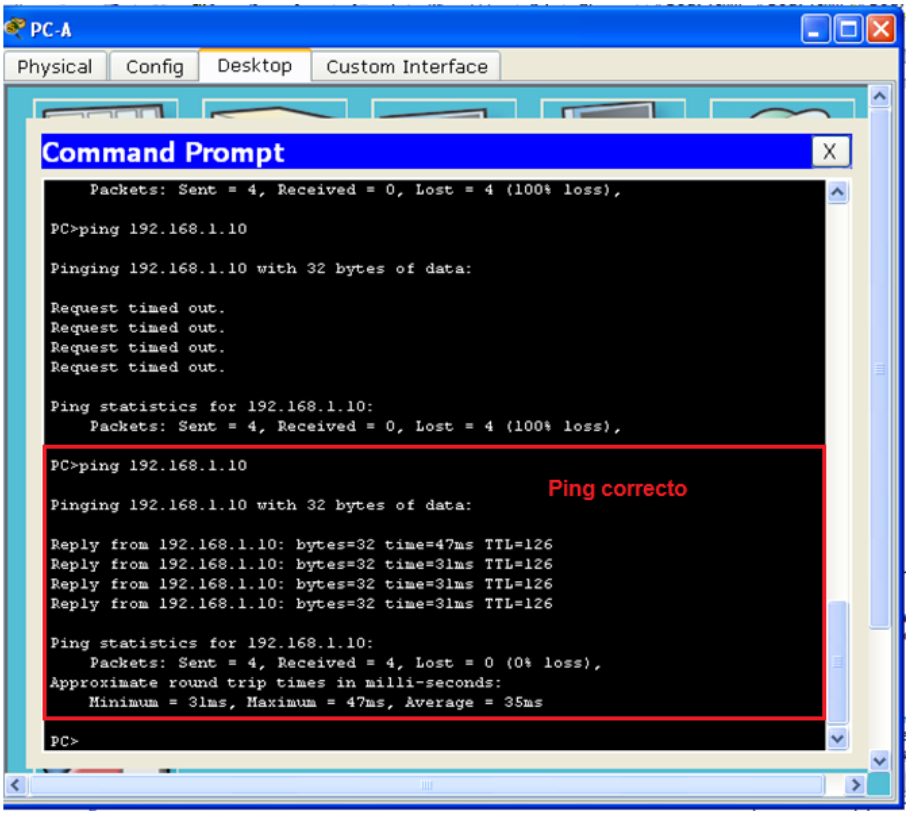
b. Observe la tabla de enrutamiento para verificar la entrada de la nueva ruta estática.

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
S    192.168.0.0/24 is directly connected, Serial0/0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
     198.133.219.0/24 is variably subnetted, 2 subnets, 2 masks
C       198.133.219.0/24 is directly connected, Loopback1
L       198.133.219.1/32 is directly connected, Loopback1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback0
L       209.165.200.225/32 is directly connected, Loopback0
R3#
```

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

La red 192.168.0.0/24 está directamente conectada a través del puerto serial 0/0/0 del R3. Se debe configurar el R1 y R3 con una rutas estáticas respectivamente., para que hayan rutas de retorno cuan do el pc destino envía su respuesta.

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

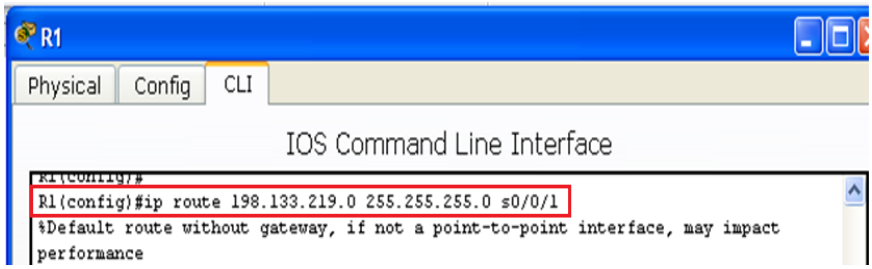


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 3. Configurar una ruta estática.

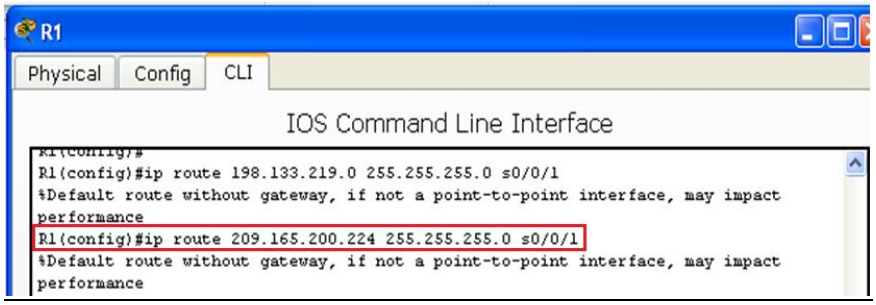
a. En el router R1, configure una ruta estática a la red 198.133.219.0 utilizando una de las opciones de configuración de ruta estática de los pasos anteriores. En el espacio proporcionado, escriba el comando que utilizó.

R1(config)# ip route 198.133.219.0 255.255.255.0 S0/0/1

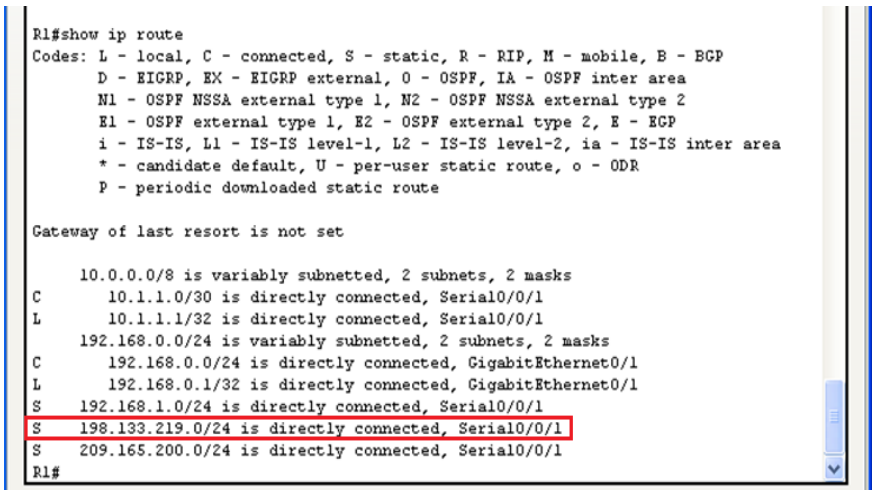


b. En el router R1, configure una ruta estática a la red 209.165.200.224 en el R3 utilizando la otra opción de configuración de ruta estática de los pasos anteriores. En el espacio proporcionado, escriba el comando que utilizó.

R1(config)# ip route 209.165.200.224 255.255.255.224 S0/0/1



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



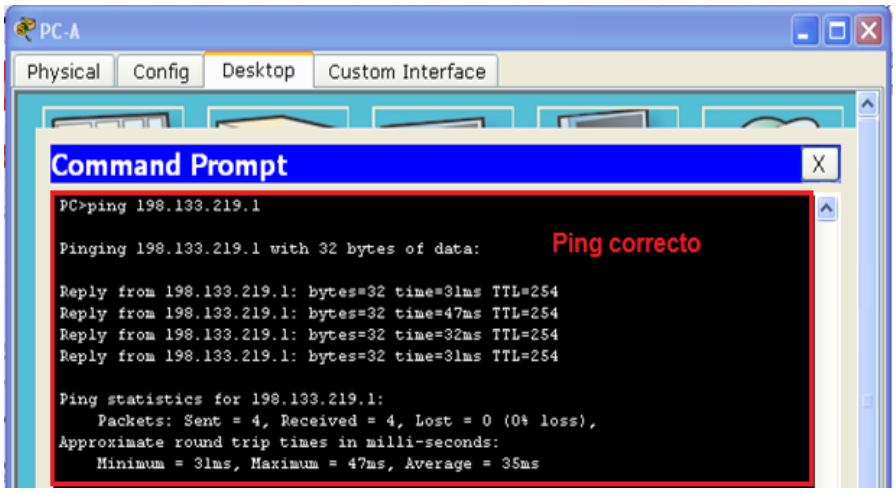
¿Cómo se indica esta ruta nueva en la tabla de routing?

S 198.133.219.0/24 is directly connected, Serial0/0/1

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

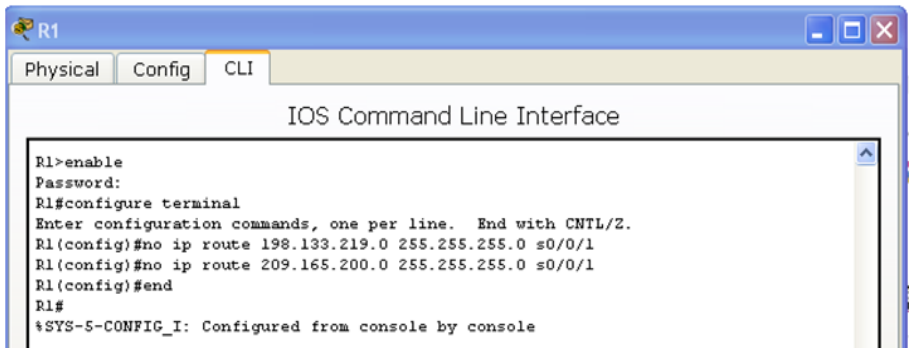
Este ping debe tener éxito.



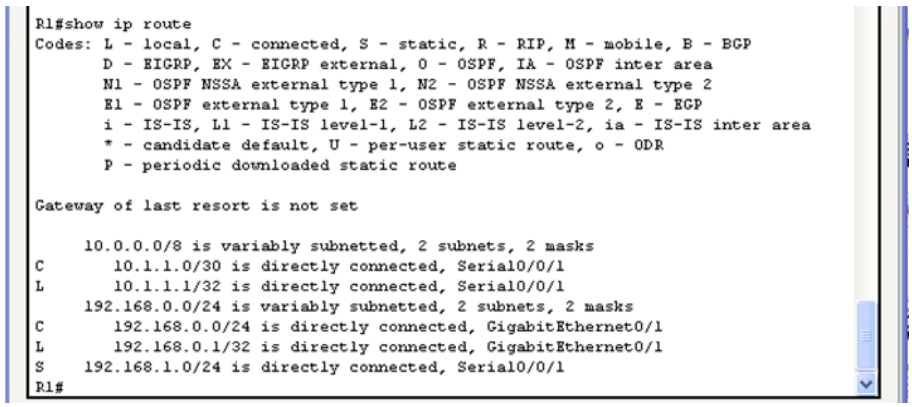
Paso 4. Elimine las rutas estáticas de las direcciones de loopback.

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.

```
R1(config)# no ip route 209.165.200.0 255.255.255.0 S0/0/1
R1(config)# no ip route 198.133.219.0 255.255.255.0 S0/0/1
```



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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

¿Cuántas rutas de red se indican en la tabla de routing del R1? 3

¿El gateway de último recurso está establecido? No

Parte 4. 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.

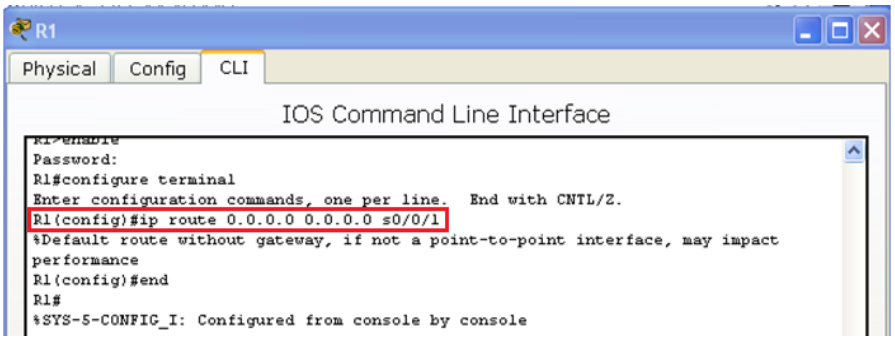
Una ruta predeterminada identifica el gateway al cual el router envía todos los paquetes IP para los que no tiene una ruta descubierta o estática. Una ruta estática predeterminada es una ruta estática con 0.0.0.0 como dirección IP y máscara de subred de destino. Comúnmente, esta ruta se denomina “ruta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

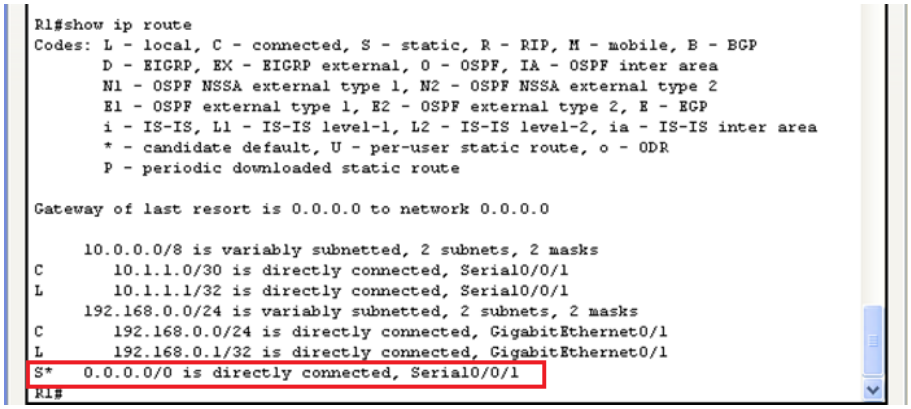
```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address or exit-intf}
```

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.

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



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



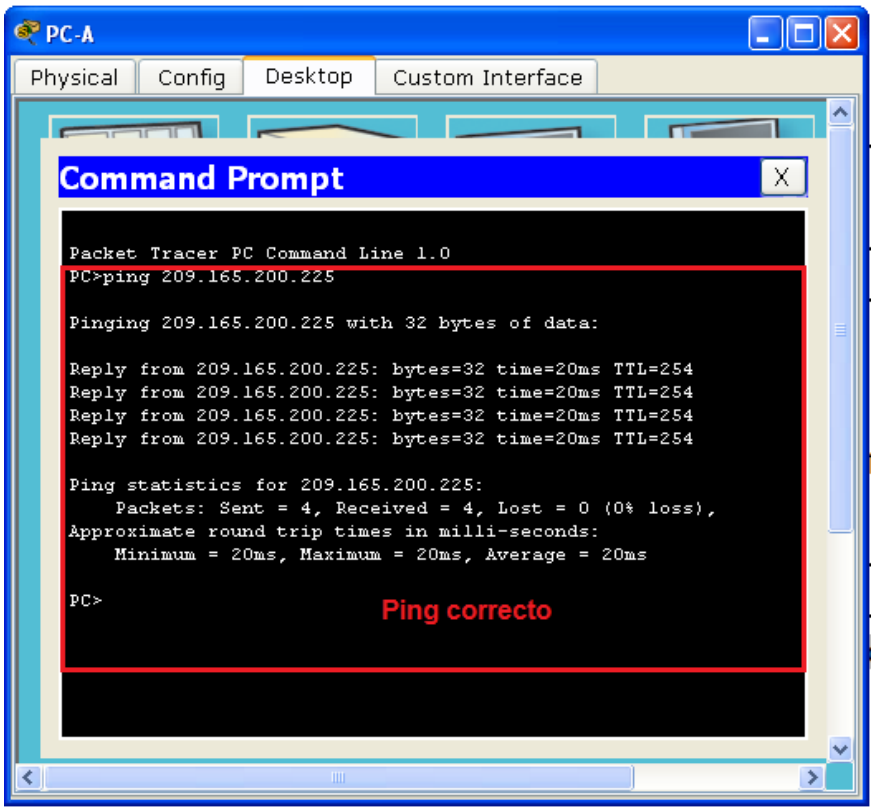
¿Cómo se indica esta ruta nueva en la tabla de routing?

```
S* 0.0.0.0/0 is directly connected, Serial0/0/1
```

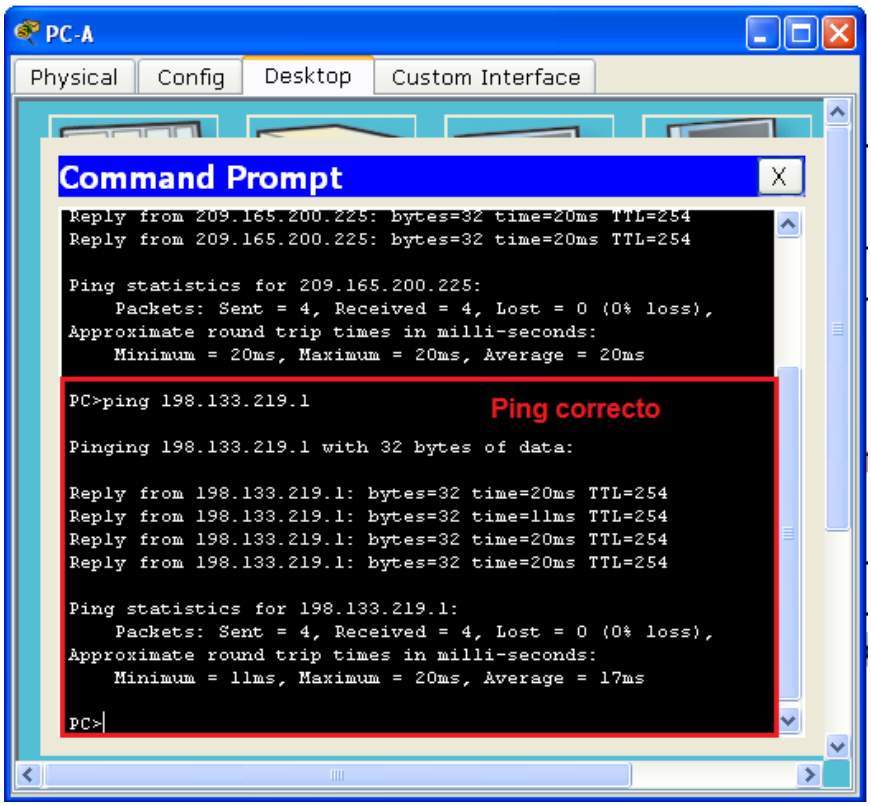
¿Cuál es el gateway de último recurso?
0.0.0.0/0 es el gateway de último recurso

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Reflexión

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

   R3(config)#ip route 192.168.0.3 255.255.255.0 s0/0/0

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

   El beneficio es que cuando se utiliza una ruta estática directamente conocida o conectada directamente, la interface de salida se resuelve en una sola búsqueda; mientras que en una ruta estática recursiva, se necesitan dos búsquedas para resolver la interface de salida.

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

   Una ruta predeterminada en un router permite enviar paquetes hacia redes desconocidas.

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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 12

- En una ruta estática directamente conectada la interface de salida se resuelve en una sola búsqueda. En una ruta estática recursiva se necesitan dos búsquedas para resolver la interface de salida.
- Una ruta predeterminada permite enviar paquetes hacia otras redes desconocidas.
- En esta actividad se aprende a configurar rutas estáticas y predeterminadas en routers, configurar contraseñas de seguridad en routers y switches.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 13: 6.2.4.5 Lab - Configuring IPv6 Static and Default Routes

Práctica de laboratorio: configuración de rutas estáticas y predeterminadas IPv6

Topología

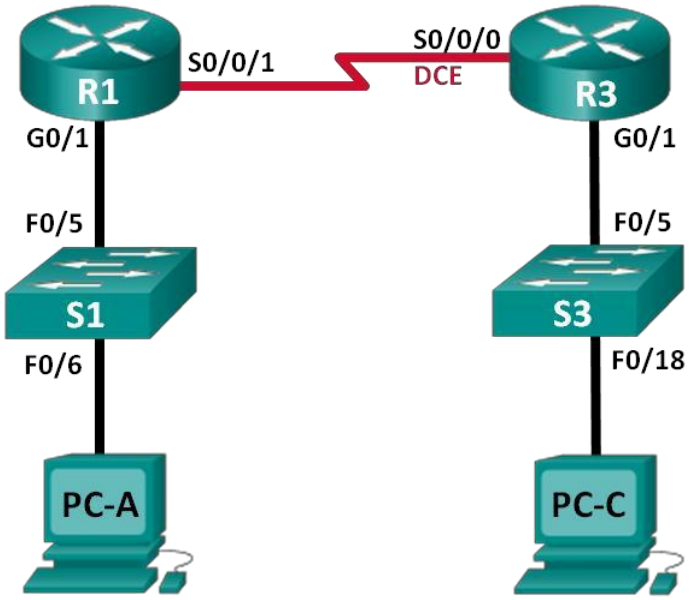


Tabla de direccionamiento

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

Objetivos

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

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 2: configurar rutas estáticas y predeterminadas IPv6

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

Información básica/situación

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

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

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

Recursos necesarios

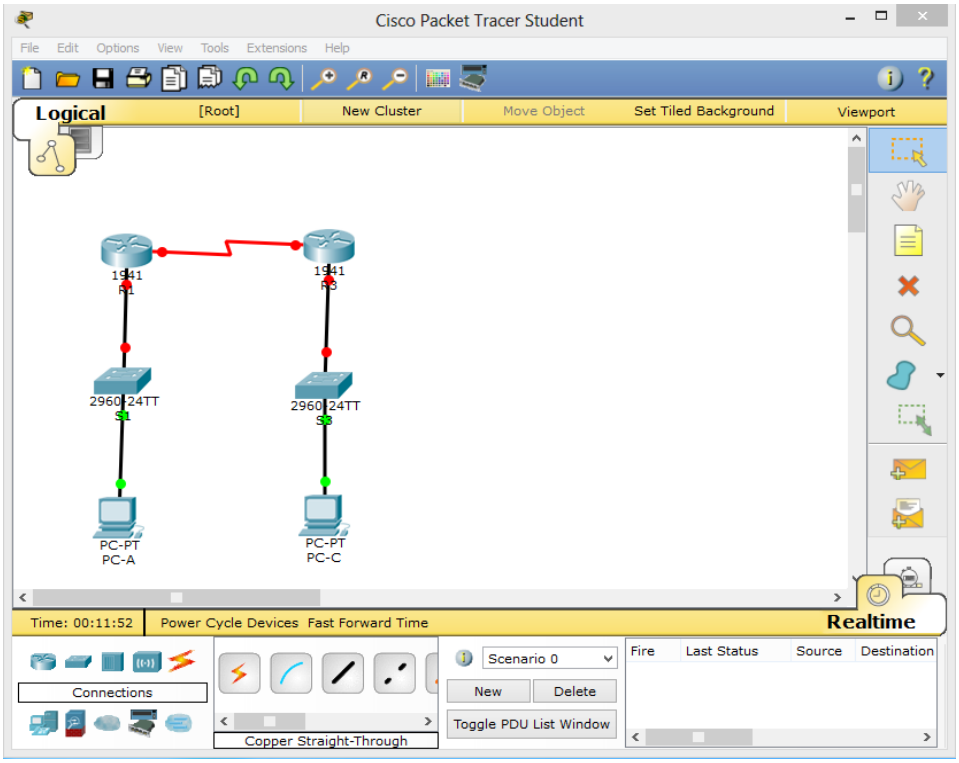
- 2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)
- 2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

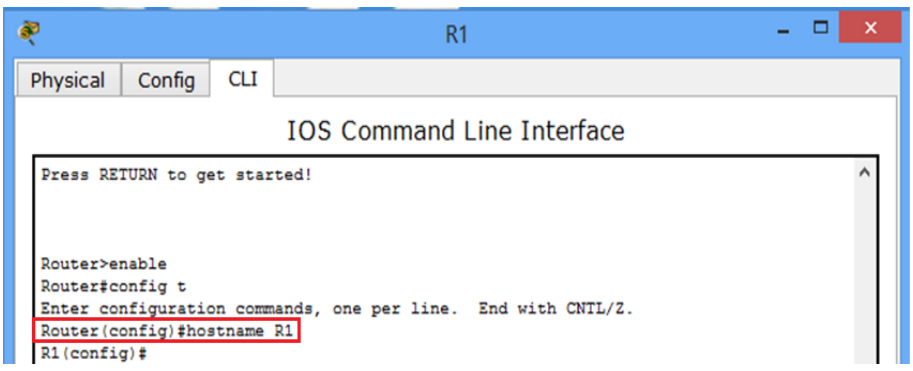
Paso 1. Realice el cableado de red tal como se muestra en el diagrama de topología.



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

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

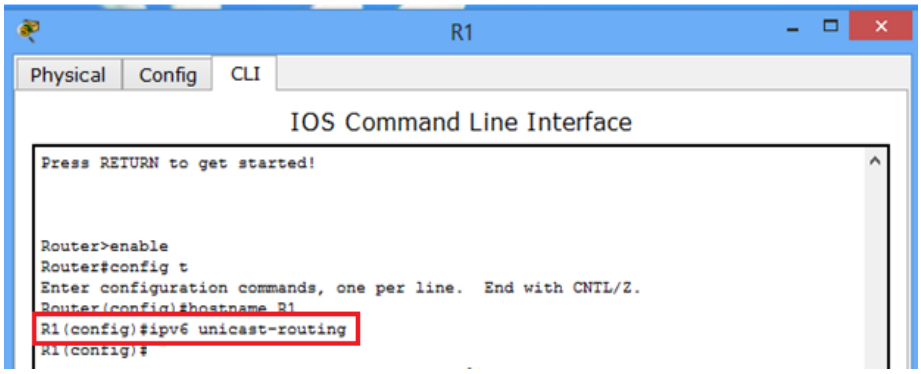
a. Mediante Tera Term, acceda al router etiquetado R1 en el diagrama de la topología mediante el puerto de consola y asígnele el nombre R1.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

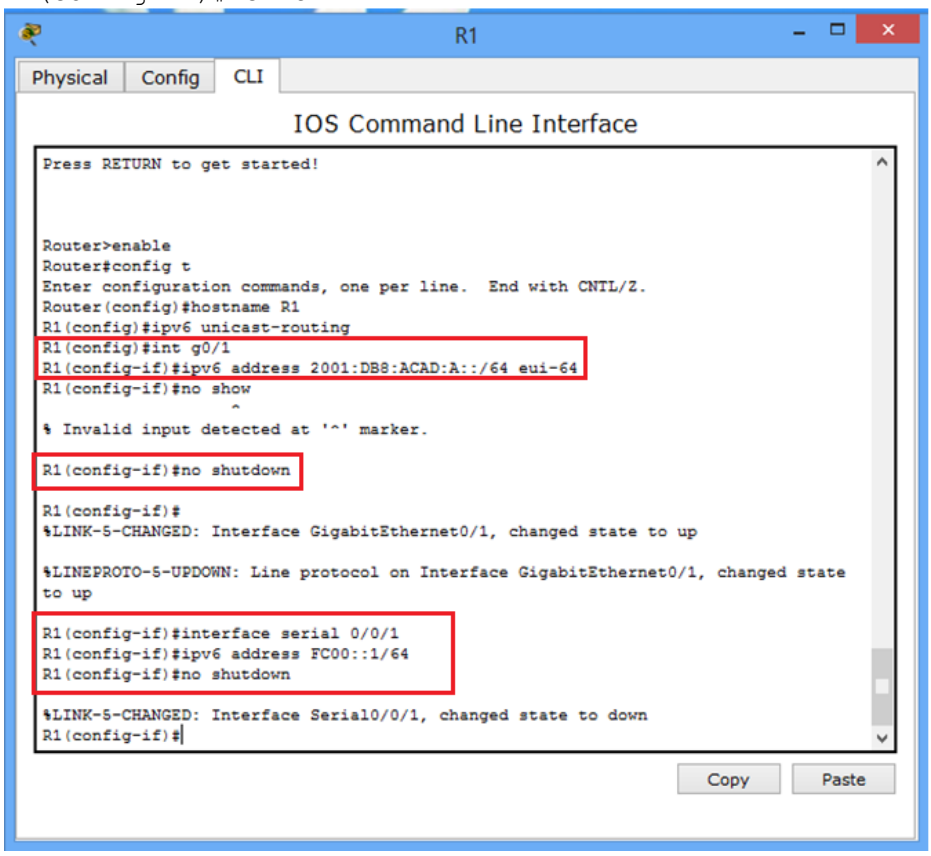
b. En el modo de configuración global, habilite el routing IPv6 en el R1.

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



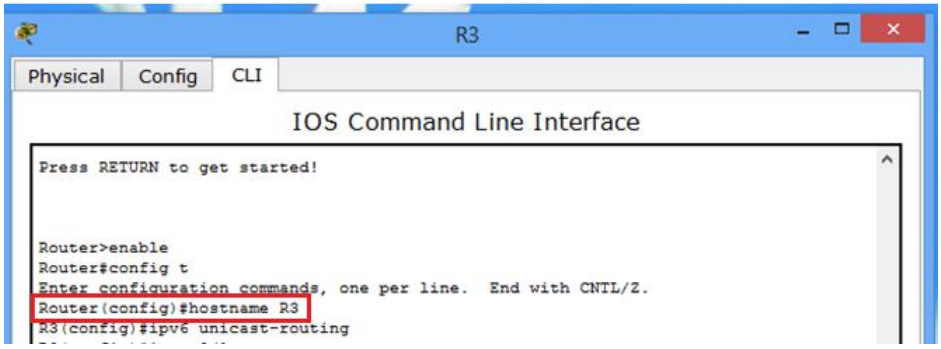
c. Configure las interfaces de red en el R1 con direcciones IPv6. Observe que IPv6 está habilitado en cada interfaz. La interfaz G0/1 tiene una dirección de unidifusión enrutable globalmente, y se utiliza EUI-64 para crear la porción del identificador de la interfaz de la dirección. La interfaz S0/0/1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

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



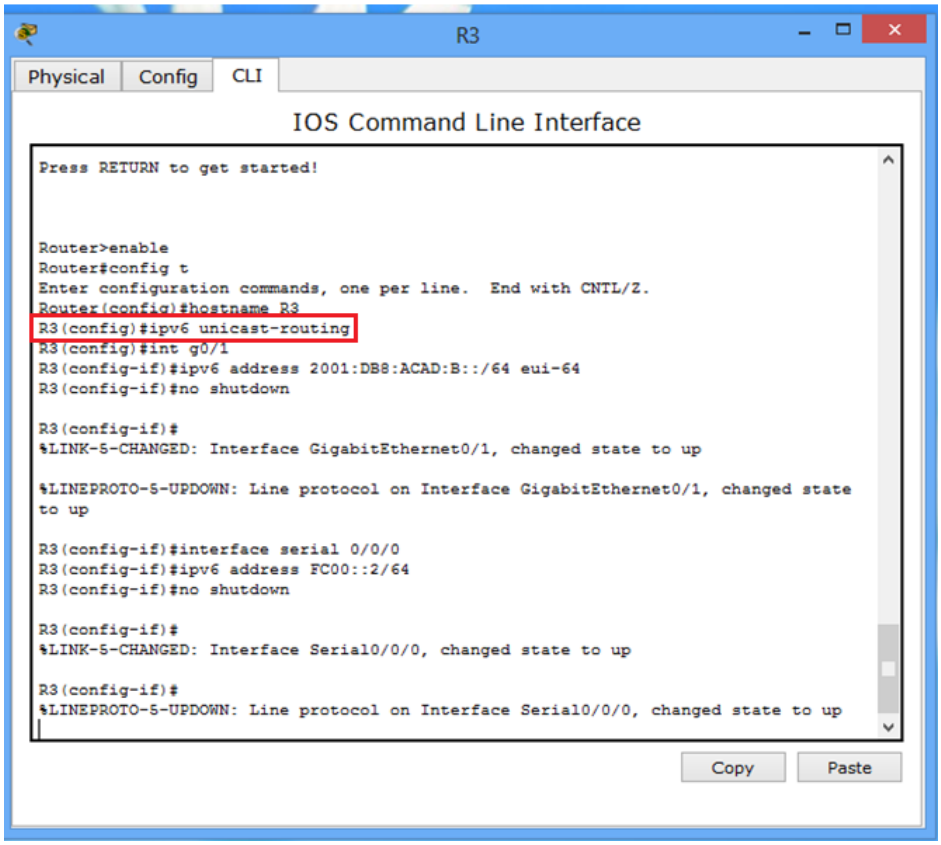
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

d. Asigne un nombre de dispositivo al router R3.



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

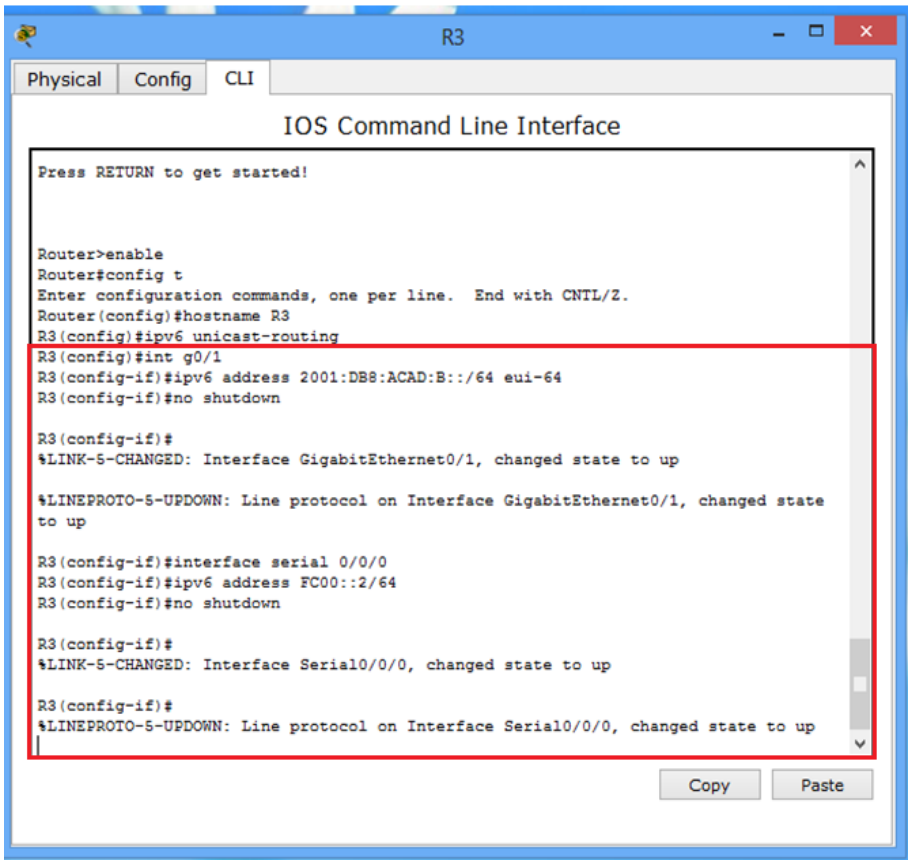
```
R3(config)# ipv6 unicast-routing
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

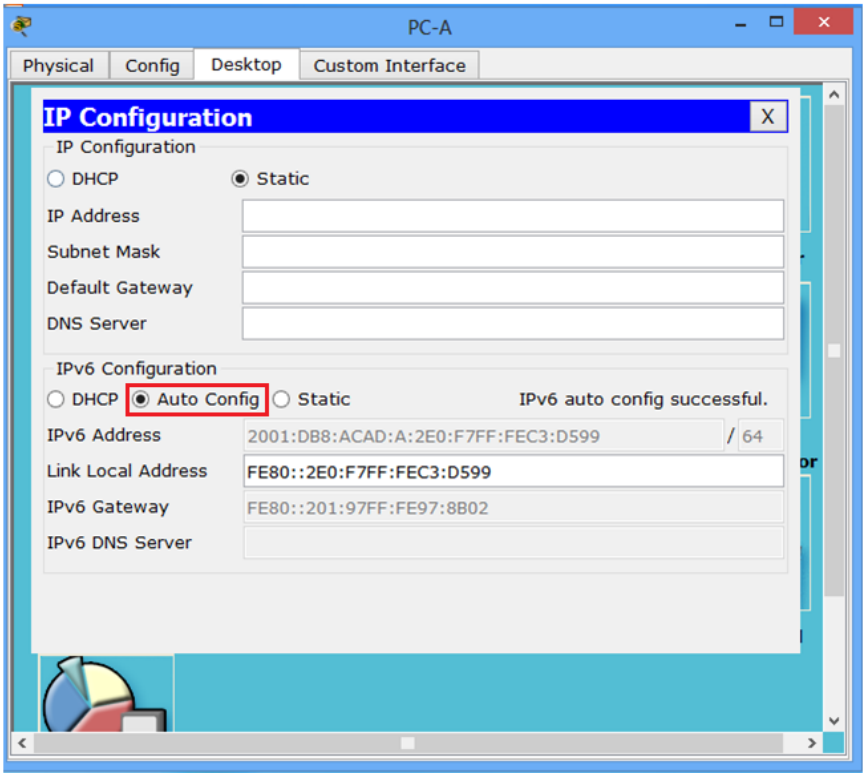
```
R3(config)# interface gigabit 0/1
R3(config-if)# ipv6 address 2001:DB8:ACAD:B::/64 eui-64
R3(config-if)# no shutdown
R3(config-if)# interface serial 0/0/0
R3(config-if)# ipv6 address FC00::2/64
R3(config-if)#   clock   rate   128000
R3(config-if)# no shutdown
R3(config-if)# exit
```

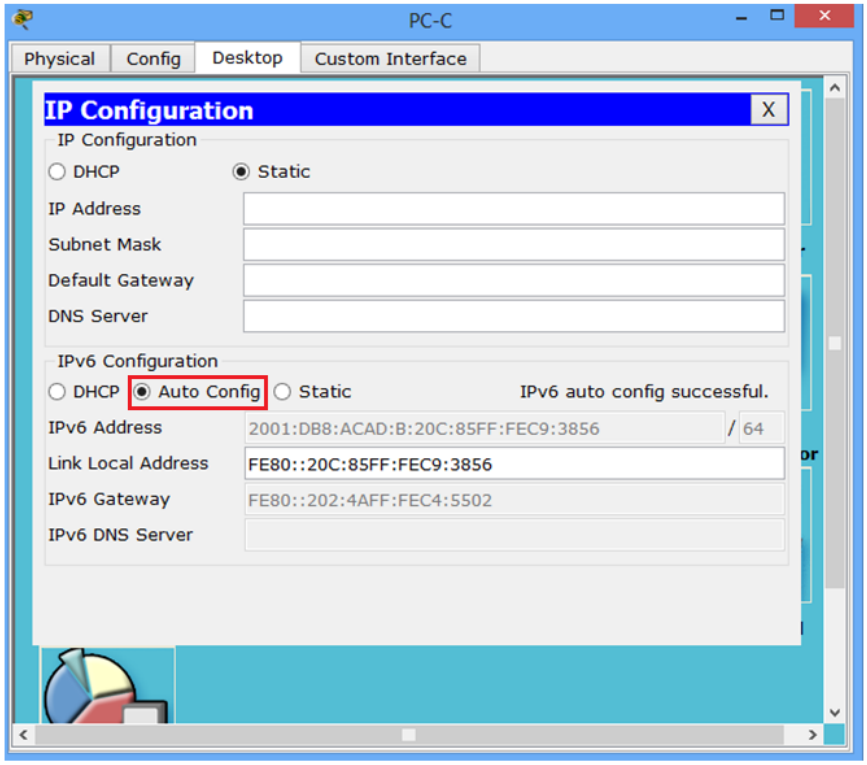


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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



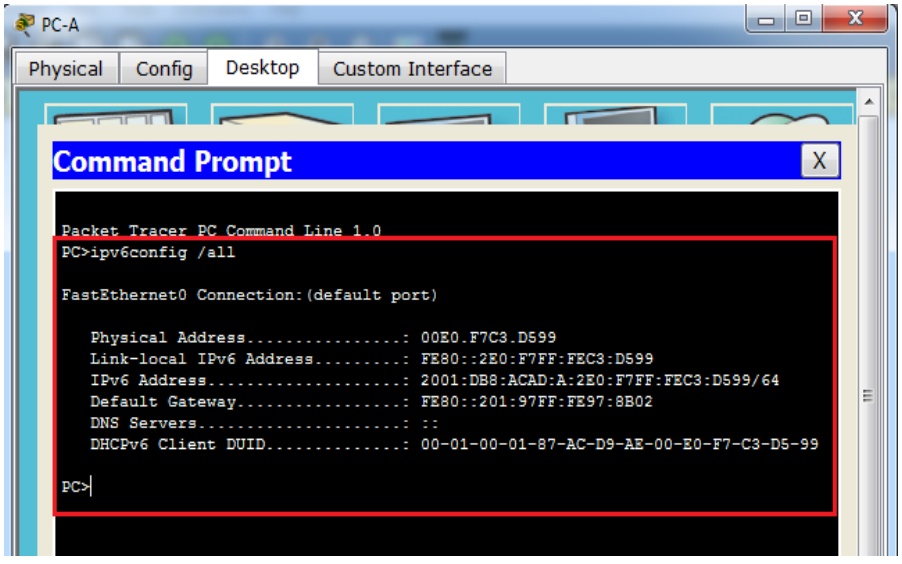


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

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

Ethernet adapter Local Area Connection:

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

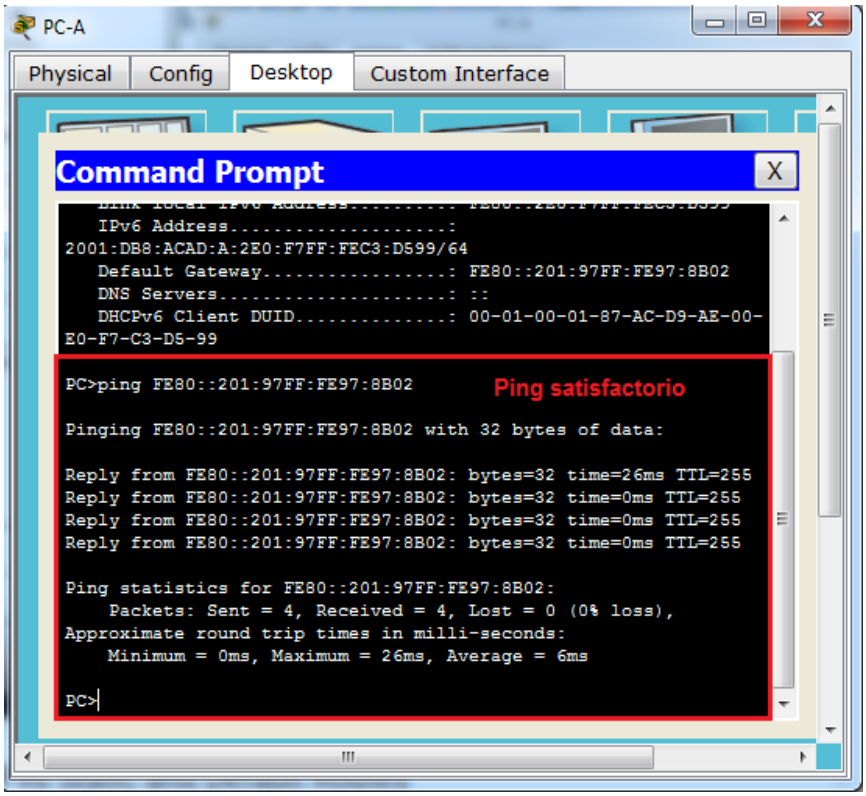
b. ¿Cuál es la dirección IPv6 de unidifusión global de la PC-A? 2001:DB8:ACAD:A:2E0:F7FF:FEC3:D599

c. ¿Cuál es la dirección IPv6 link-local de la PC-A? FE80::2E0:F7FF:FEC3:D599

d. ¿Cuál es la dirección IPv6 de gateway predeterminado de la PC-A? FE80::201:97FF:FE97:8B02

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

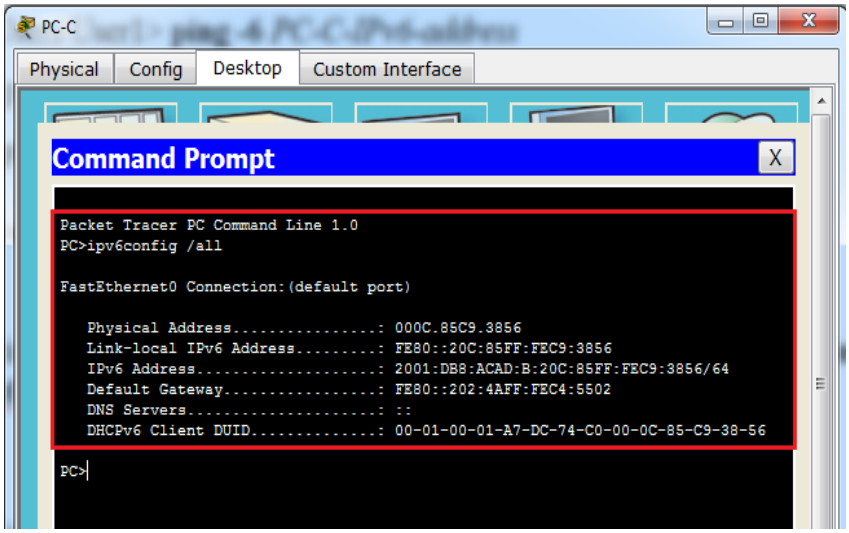
```
C:\Users\User1> ping -6 <default-gateway-address>
```



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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



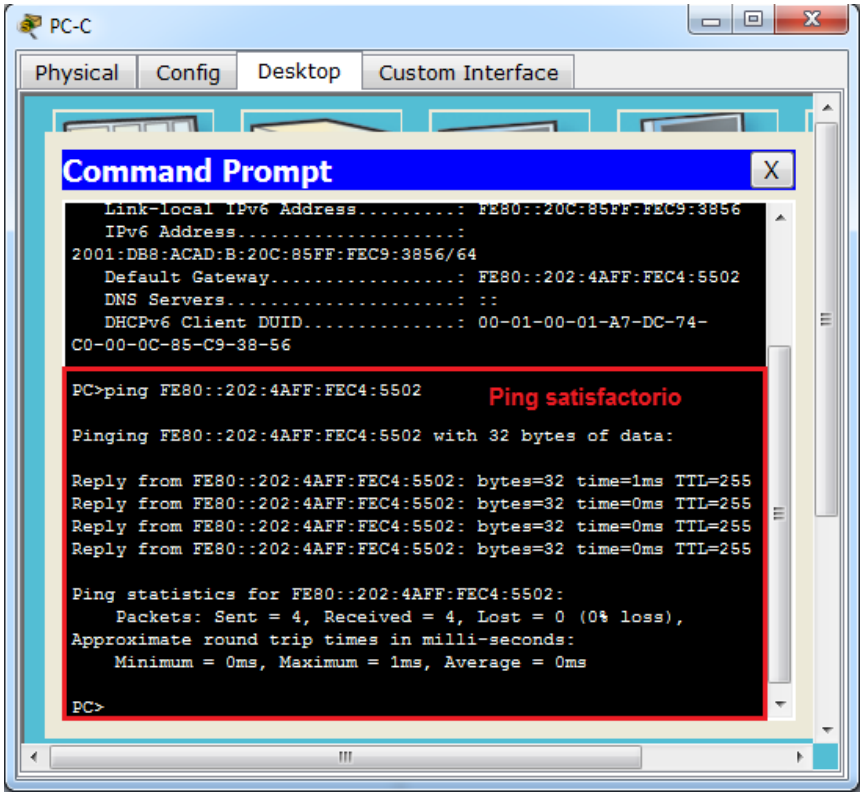
¿La PC-C recibió información de direccionamiento IPv6 del R3? Si

g. ¿Cuál es la dirección IPv6 de unidifusión global de la PC-C? 2001:DB8:ACAD:B:20C:85FF:FEC9:3856

h. ¿Cuál es la dirección IPv6 link-local de la PC-C? FE80::20C:85FF:FEC9:3856

i. ¿Cuál es la dirección IPv6 de gateway predeterminado de la PC-C? FE80::202:4AFF:FEC4:5502

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

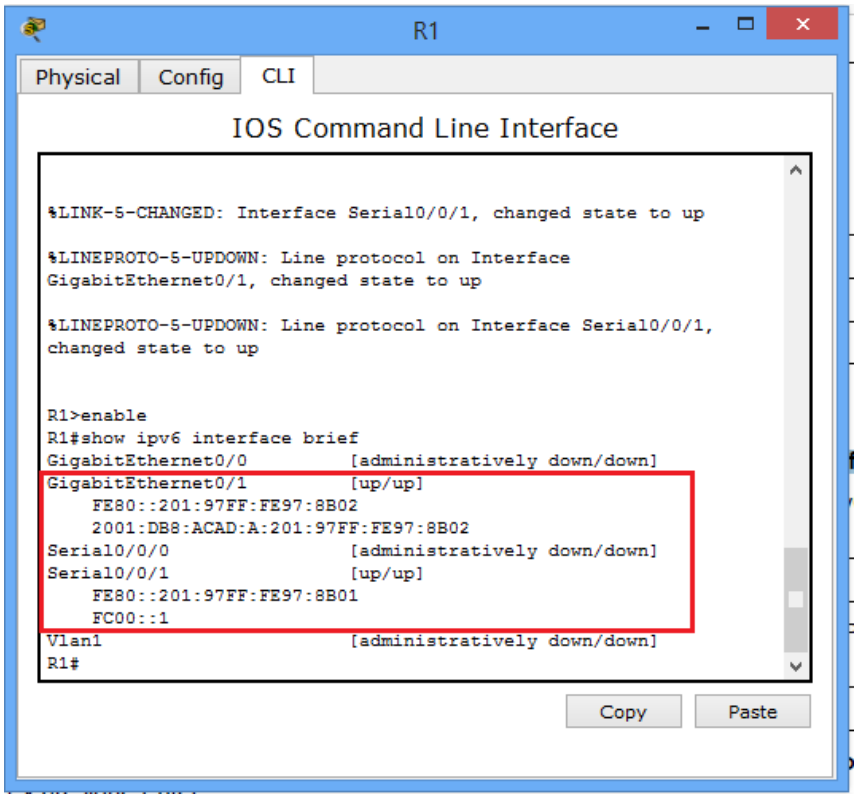
```
C:\Users\User1> ping -6 PC-C-IPv6-address
```

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

No se realizó correctamente porque los routers no han sido configurados con enrutamiento estático o dinámico y solo conocen las redes conectadas directamente. Sin las rutas adecuadas, los routers soltarán paquetes destinados a redes desconocidas.

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

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



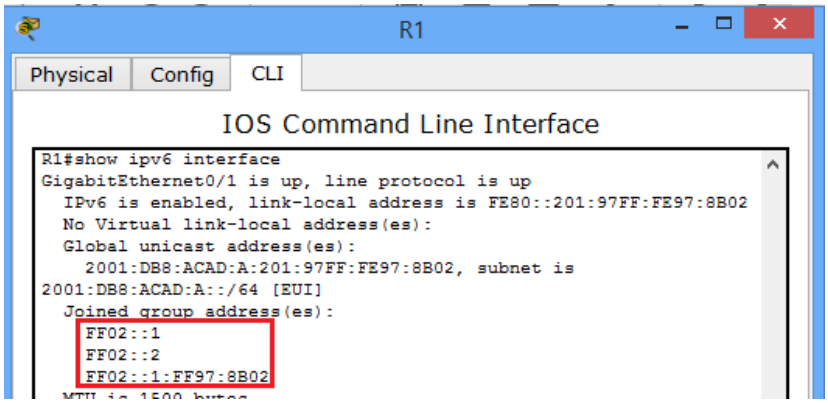
¿Cuáles son las dos direcciones IPv6 de la interfaz G0/1 y qué tipo de direcciones IPv6 son?

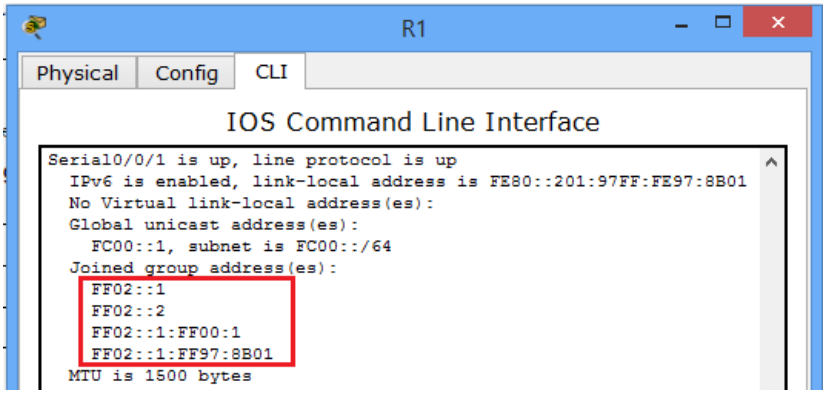
Una dirección link-local FE80::201:97FF:FE97:8B02 y una dirección global unicast 2001:DB8:ACAD:A:201:97FF:FE97:8B02

¿Cuáles son las dos direcciones IPv6 de la interfaz S0/0/1 y qué tipo de direcciones IPv6 son?
Una dirección link-local FE80::201:97FF:FE97:8B01 y una dirección unique-local FC00::1

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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





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

FF02::1, FF02::2, FF02::1:FF97:8B02

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

FF02::1, FF02::2, FF02::1:FF00:1, FF02::1:FF97:8B01

¿Para qué se usa la dirección de multidifusión FF02::1? Para comunicarse con los nodos

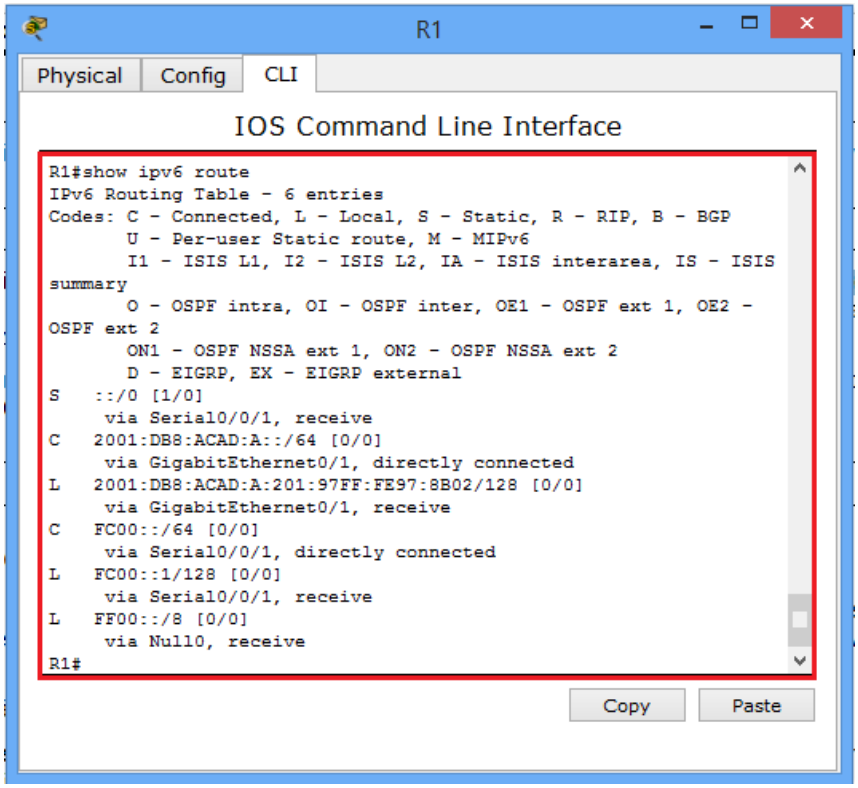
¿Para qué se usa la dirección de multidifusión FF02::2? Para comunicarse con los segmentos

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

Direcciones de multidifusión de nodos solicitados. Cada interfaz unicast o dirección anycast tiene que tener una dirección de multidifusión de nodo solicitada para resolver direcciones vecinas en el enlace local.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



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

No hay ping porque no hay rutas; el router dice que ese destino es inalcanzable, ya que el Router 1 conoce sus redes que están conectadas pero no conoce una red que está a un salto más lejos.

Parte 2. Configurar rutas estáticas y predeterminadas IPv6

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

Configurará tres tipos de rutas estáticas IPv6:

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

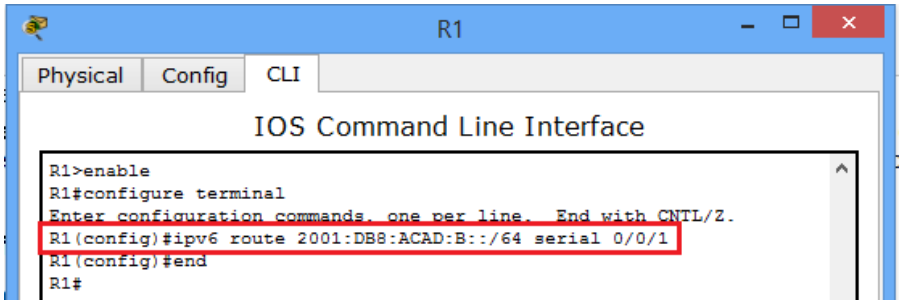
Paso 1. Configurar una ruta estática IPv6 conectada directamente.

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

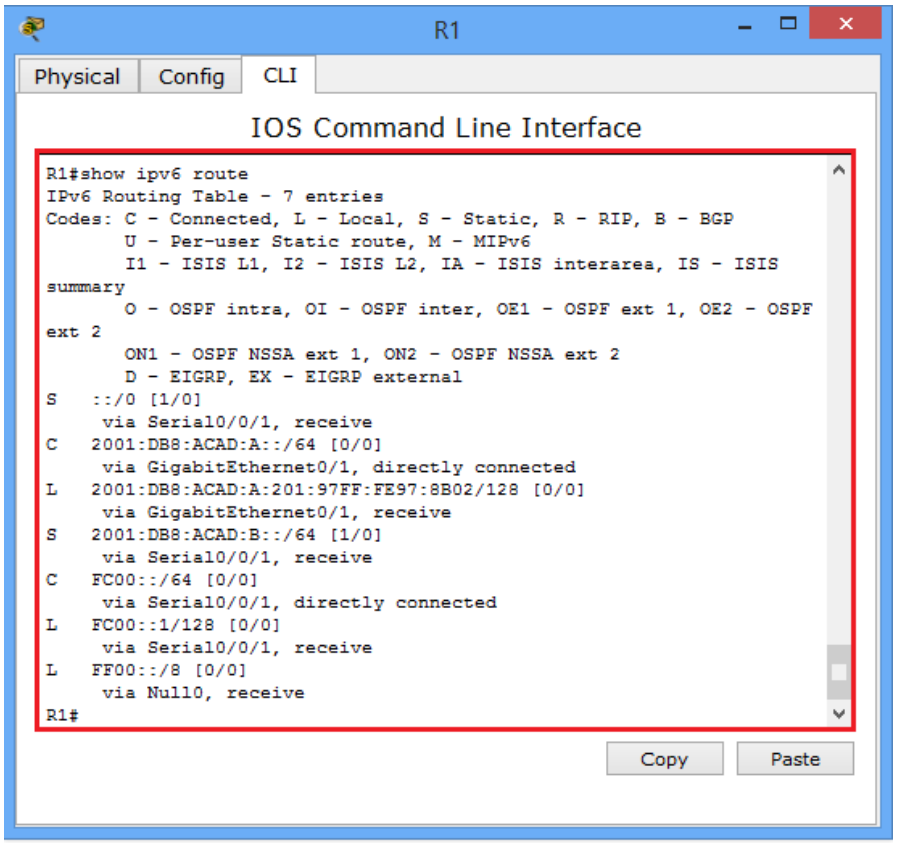
```
Router(config)# ipv6 route <ipv6-prefix/prefix-length> <outgoing-interface-type> <outgoing-interface-number>
```

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

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



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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

```
S 2001:DB8:ACAD:B::/64 [1/0]
via Serial0/0/1, directly connected
```

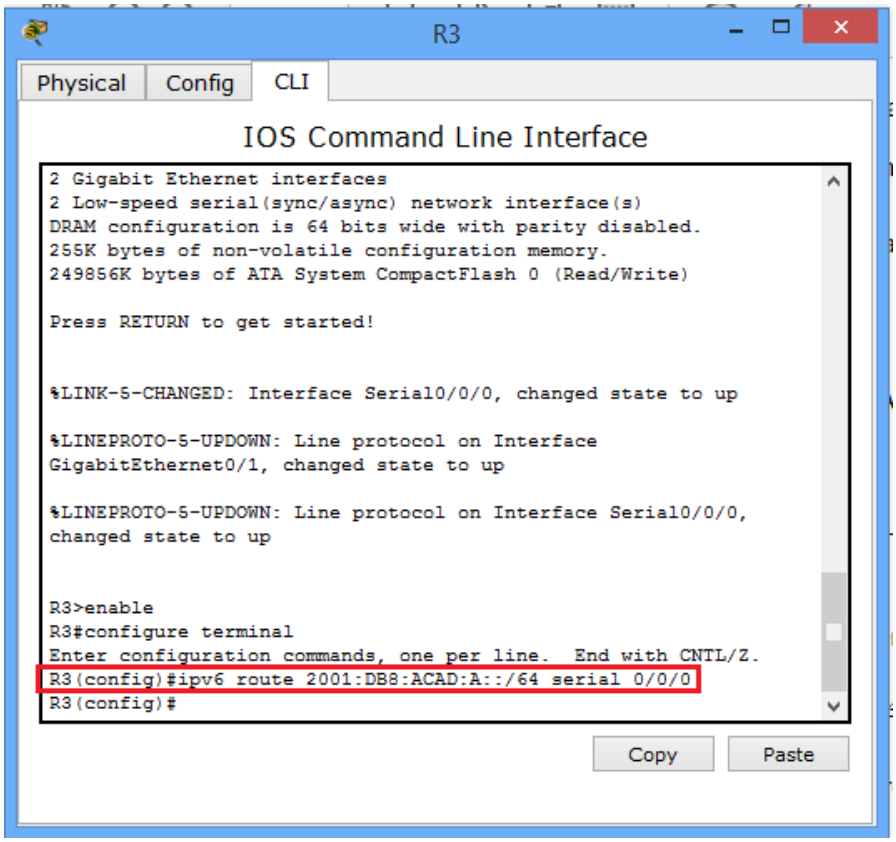
c. Ahora que la ruta estática se configuró en el R1, ¿es posible hacer ping de la PC-A al host PC-C?

No, todavía 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, ese ping se descarta en el R3, porque el R3 no tiene una ruta de retorno a la red 2001:DB8:ACAD:A::/64 en la tabla de routing. Para hacer ping correctamente a través de la red, también debe crear una ruta estática en el R3.

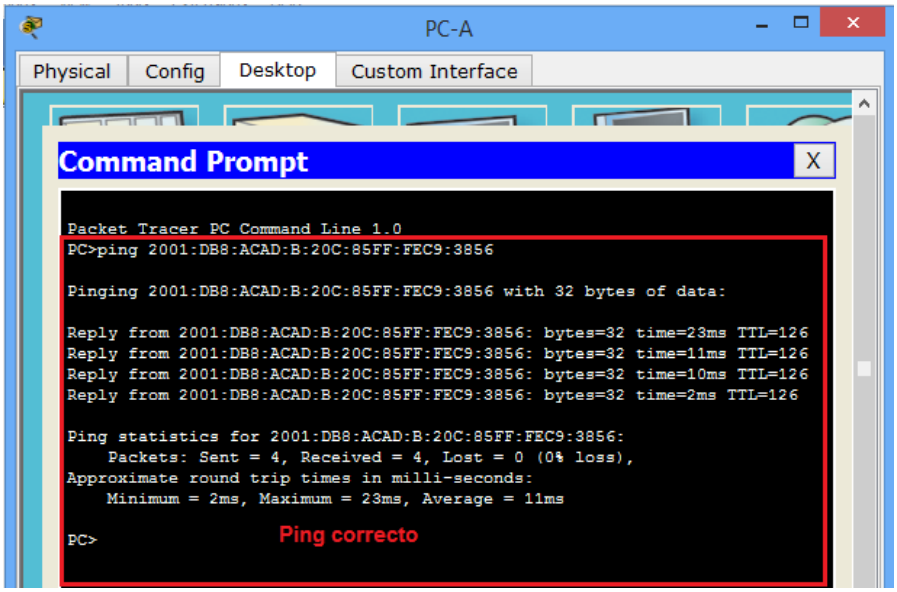
d. En el router R3, configure una ruta estática IPv6 a la red 2001:DB8:ACAD:A::/64, mediante la interfaz de salida S0/0/0 del R3.

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



¿El ping se realizó correctamente? ¿Por qué?

Si porque ya se configuraron los router 1 y 3; ya están las dos rutas una ruta de ida y la otra de vuelta.

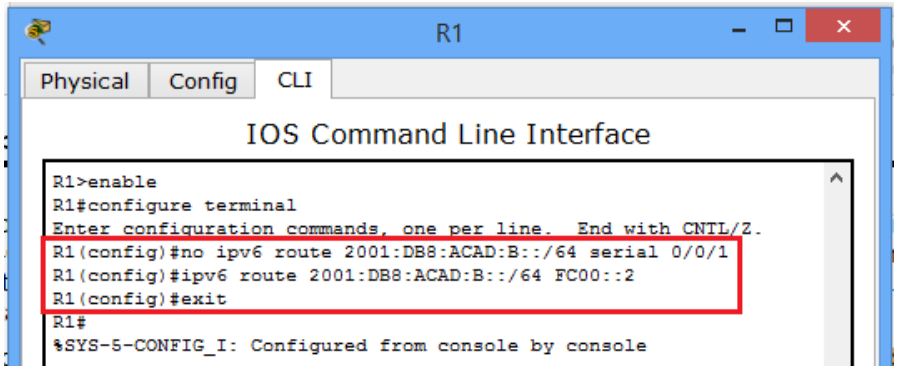
Paso 2. Configurar una ruta estática IPv6 recursiva.

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

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

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

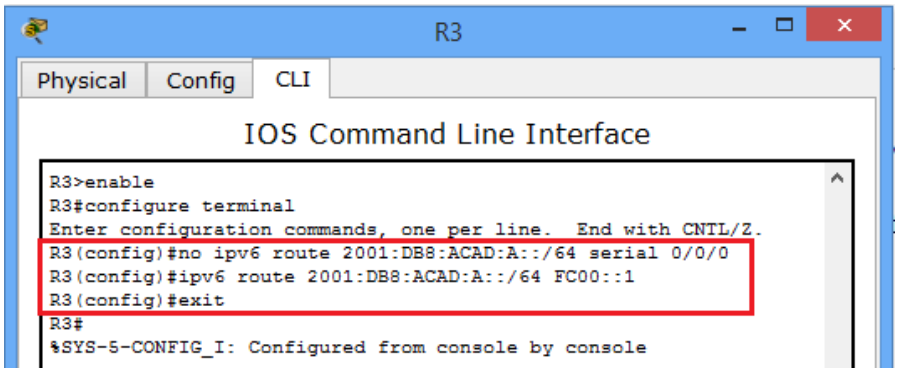
```
R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1
R1(config)#   ipv6   route   2001:DB8:ACAD:B::/64   FC00::2
R1(config)# exit
```



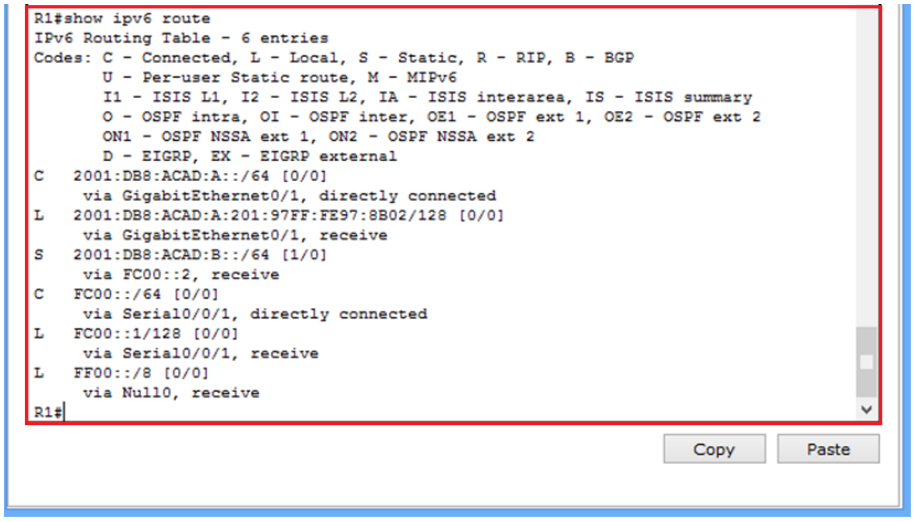
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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



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



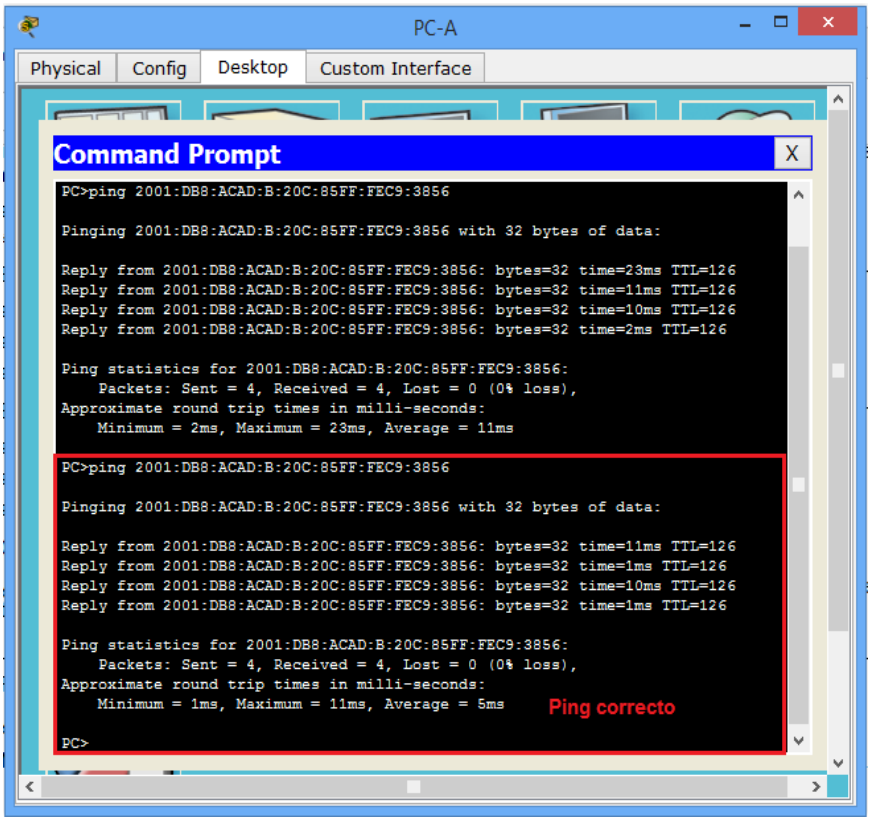
¿Cuál es la letra de código y la entrada de la tabla de routing de la ruta que se agregó recientemente a la tabla de routing?

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

`via FC00::2`

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



¿El ping se realizó correctamente? Si

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

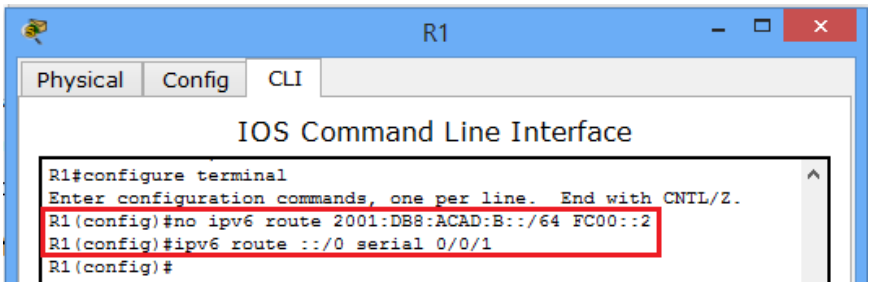
Paso 3. Configurar una ruta estática predeterminada IPv6.

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

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

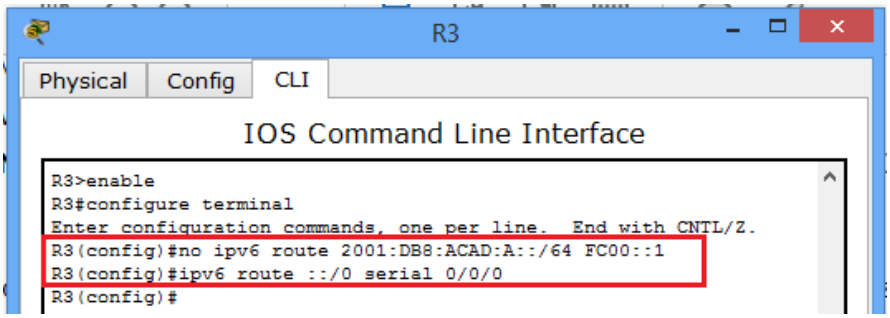
a. En el router R1, elimine la ruta estática recursiva y agregue una ruta estática predeterminada.

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

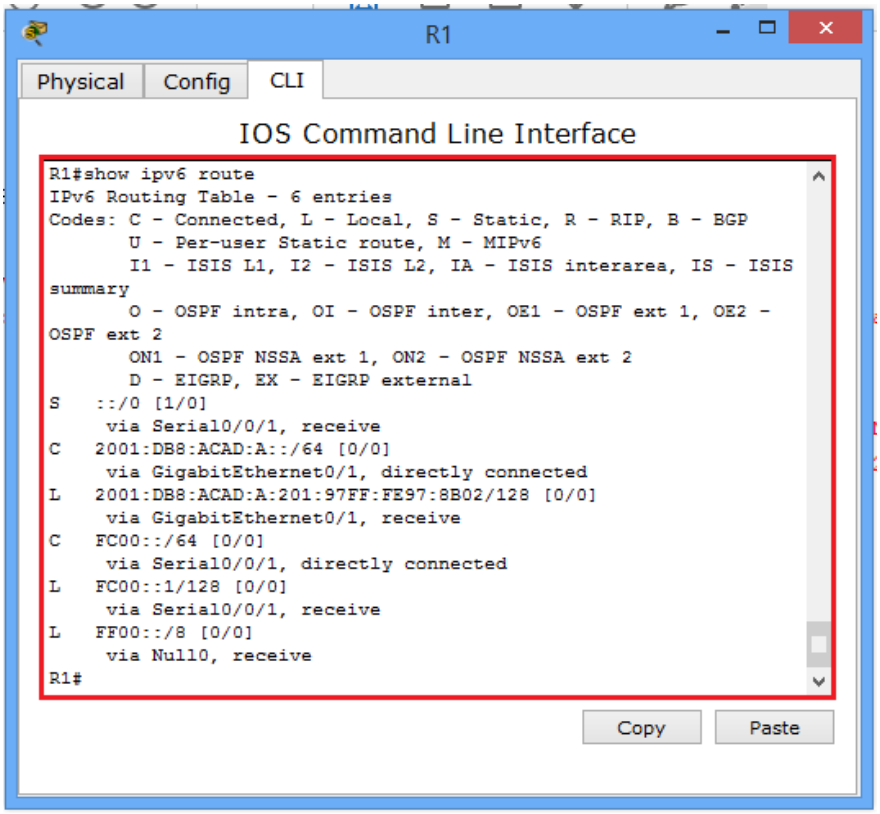


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



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



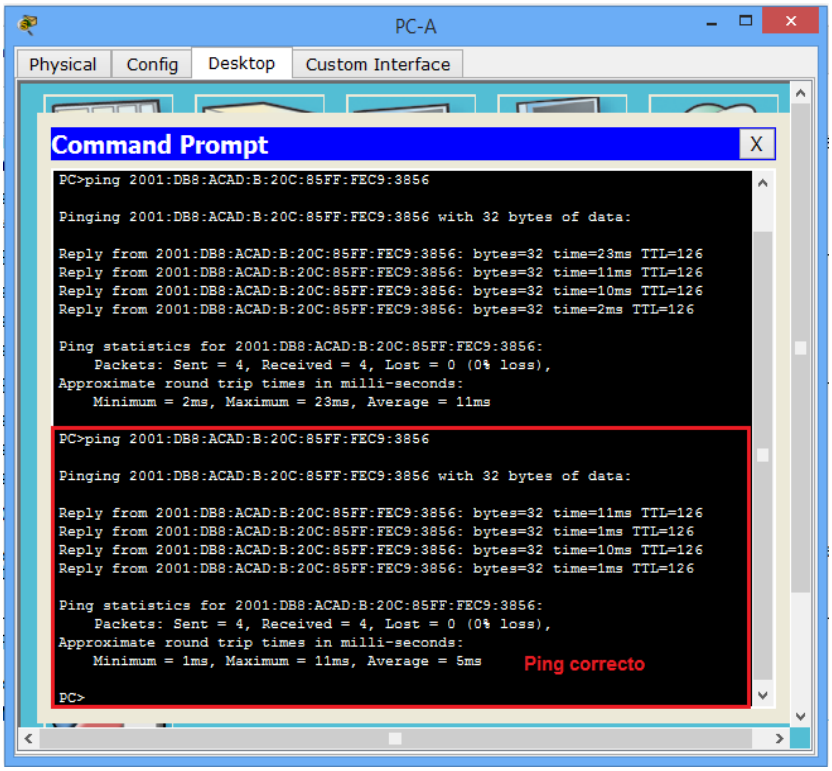
¿Cuál es la letra de código y la entrada de la tabla de routing de la ruta predeterminada que se agregó recientemente a la tabla de routing?

`S ::/0 [1/0]`

`via Serial0/0/1, receive`

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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



¿El ping se realizó correctamente? Si

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

Reflexión

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

   Si hay una transición podríamos usar ipv6 e ipv4 al mismo tiempo hasta que solamente se use la 6, hay muchas redes que utilizan la 6 pero para que aún tenga comunicación con sus clientes que aún usan versión 4, mantienen las dos al mismo tiempo.

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

   Al configurar una ruta IPv6 estática, se utiliza el comando **ipv6 route** en lugar del comando **ip route**. Otra diferencia importante es la necesidad de utilizar el comando **show ipv6 route** para ver la tabla de enrutamiento IPv6 en comparación con la tabla de enrutamiento IPv4 con el comando **show ip route.**

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 13

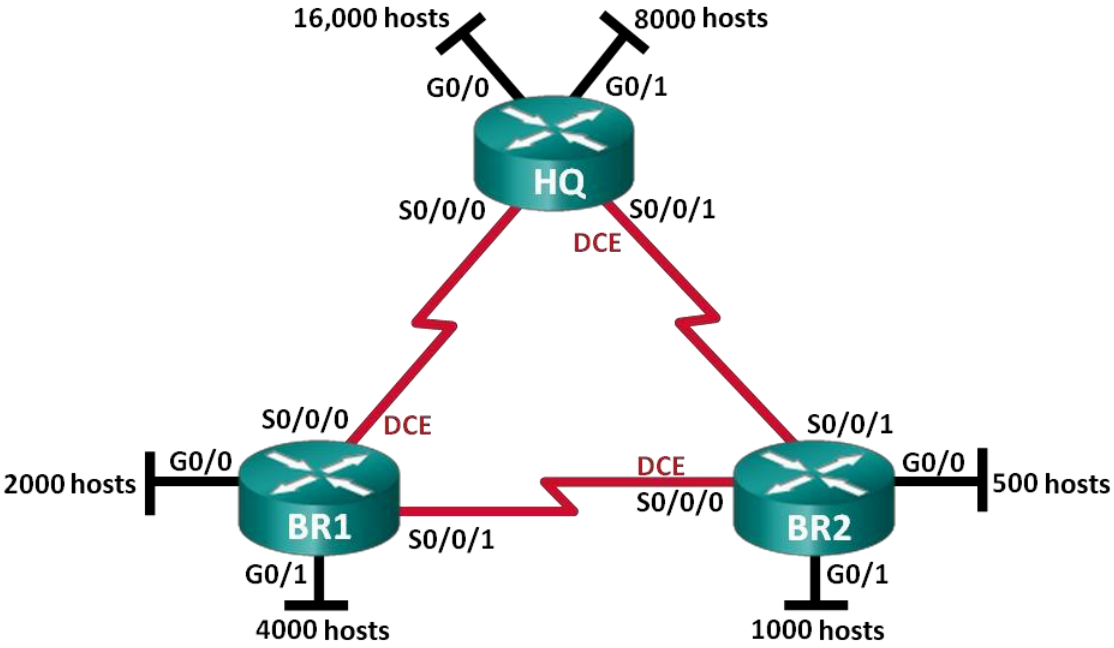
- Con el desarrollo de ésta actividad, aplicamos los conocimientos adquiridos en la unidad 3, en cuanto a los pasos necesarios para configurar toda una red que permita la comunicación con direccionamiento IPv6, también aprendimos como aplicar la configuración automática de dirección sin estado (SLAAC) y así configurar las direcciones IPv6 para los hosts.
- En la actividad también se realizó la configuración de rutas estáticas y predeterminadas IPv6 en los routers para habilitar la comunicación con redes remotas que no están conectadas directamente.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 14: 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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). 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)

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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? 32766

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

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

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

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

¿Cuántas direcciones IP se necesitan en la subred más grande? 16000

¿Cuál es la subred más pequeña que admite esa cantidad de direcciones? /18 o 255.255.192.0

¿Cuántas direcciones host admite esa subred? 16382

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

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

172.16.128.0/18

172.16.192.0/18

Utilice la primera dirección de red para esta subred.

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

Descripción de la subred HQ GO/1 LAN

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

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

¿Cuántas direcciones host admite esa subred? 8190

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

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

172.16.192.0/19

172.16.224.0/19

Utilice la primera dirección de red para esta subred.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

Descripción de la subred BR1 G0/1 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? 4000

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

¿Cuántas direcciones host admite esa subred? 4094

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

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

172.16.224.0/20

172.16.240.0/20

Utilice la primera dirección de red para esta subred.

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

Descripción de la subred BR1 G0/0 LAN

¿Cuántas direcciones IP se necesitan para la siguiente subred más grande? 2000

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

¿Cuántas direcciones host admite esa subred? 2046

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

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

172.16.240.0/21

172.16.248.0/21

Utilice la primera dirección de red para esta subred.

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

Descripción de la subred BR2 G0/1 LAN

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

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

¿Cuántas direcciones host admite esa subred? 1022

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

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

172.16.248.0/22

172.16.252.0/22

Utilice la primera dirección de red para esta subred.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

Descripción de la subred BR2 G0/0 LAN

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

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

¿Cuántas direcciones host admite esa subred? 510

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

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

172.16.252.0/23

172.16.254.0/23

Utilice la primera dirección de red para esta subred.

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

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

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

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

   172.16.254.0/24

   172.16.255.0/24

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

   172.16.254.0/30

   172.16.254.4/30

   172.16.254.8/30

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

   Enlace Serial HQ- BR1

   Enlace Serial HQ- BR2

   Enlace Serial BR1- BR2

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 2: diseñar el esquema de direcciones VLSM

Paso 1. Calcular la información de subred.

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

Descripción de la subred	Cantidad de hosts necesarios	Dirección de red/CIDR	Primera dirección de host	Dirección de broadcast
HQ G0/0	16 000	172.16.128.0/18	172.16.128.1/18	172.16.191.255/18
HQ G0/1	8 000	172.16.192.0/19	172.16.192.1/19	172.16.223.255/19
BR1 G0/1	4 000	172.16.224.0/20	172.16.224.1/20	172.16.239.255/20
BR1 G0/0	2 000	172.16.240.0/21	172.16.240.1/21	172.16.247.255/21
BR2 G0/1	1.000	172.16.248.0/22	172.16.248.1/22	172.16.251.255/22
BR2 G0/0	500	172.16.252.0/23	172.16.252.1/23	172.16.253.255/23
HQ S0/0/0-BR1 S0/0/0	2	172.16.254.0/30	172.16.254.1/30	172.16.254.3/30
HQ S0/0/1-BR2 S0/0/1	2	172.16.254.4/30	172.16.254.5/30	172.16.254.7/30
BR1 S0/0/1-BR2 S0/0/0	2	172.16.254.8/30	172.16.254.9/30	172.16.254.11/30

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

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

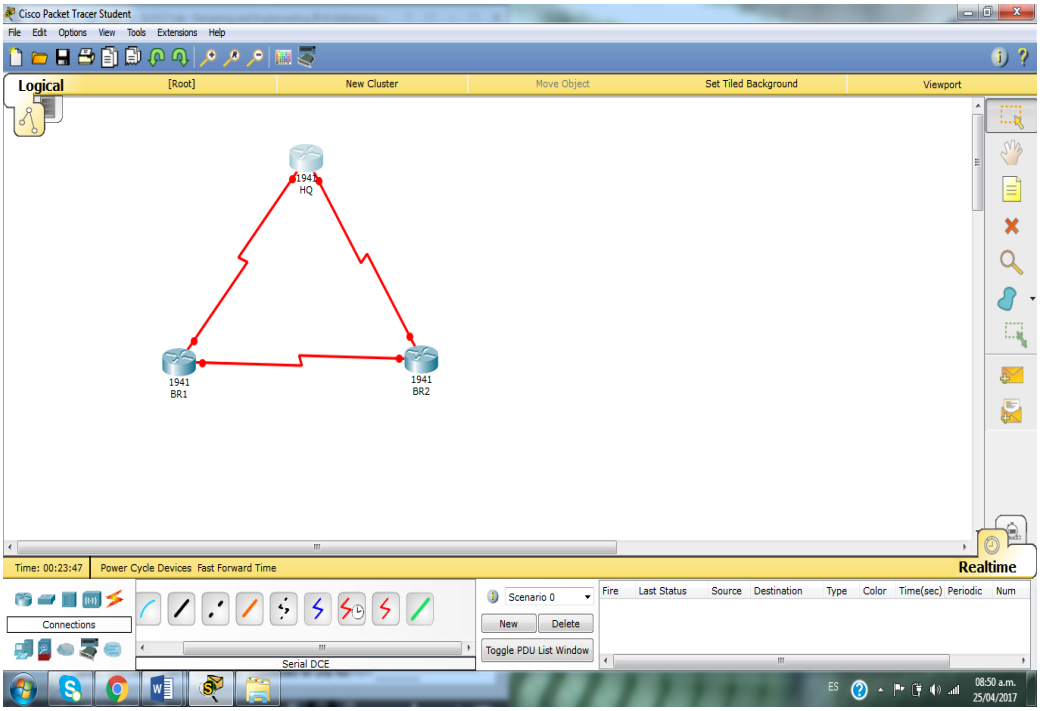
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Interfaz del dispositivo
HQ	G0/0	172.16.128.1	255.255.192.0	LAN de 16 000 hosts
	G0/1	172.16.192.1	255.255.224.0	LAN de 8000 hosts
	S0/0/0	172.16.254.1	255.255.255.252	BR1 S0/0/0
	S0/0/1	172.16.254.5	255.255.255.252	BR2 S0/0/1
BR1	G0/0	172.16.240.1	255.255.248.0	LAN de 2000 hosts
	G0/1	172.16.224.1	255.255.240.0	LAN de 4000 hosts
	S0/0/0	172.16.254.2	255.255.255.252	HQ S0/0/0
	S0/0/1	172.16.254.9	255.255.255.252	BR2 S0/0/0
BR2	G0/0	172.16.252.1	255.255.254.0	LAN de 500 hosts
	G0/1	172.16.248.1	255.255.252.0	LAN de 1000 hosts
	S0/0/0	172.16.254.10	255.255.255.252	BR1 S0/0/1
	S0/0/1	172.16.254.6	255.255.255.252	HQ S0/0/1

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 3: realizar el cableado y configurar la red IPv4

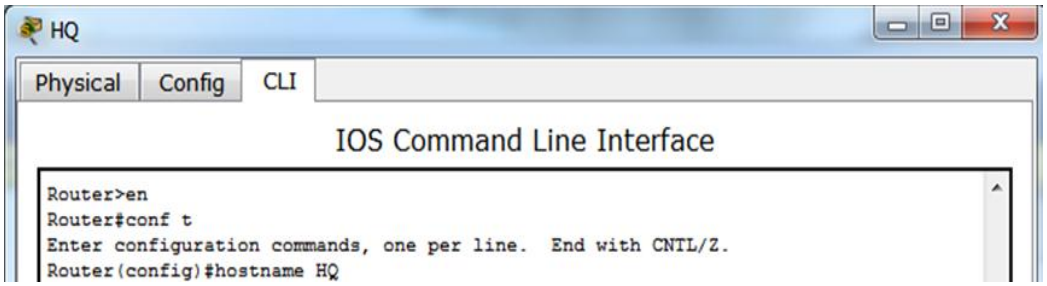
En la parte 3, realizará el cableado de la topología de la red y configurará los tres routers con el esquema de direcciones VLSM que elaboró en la parte 2.

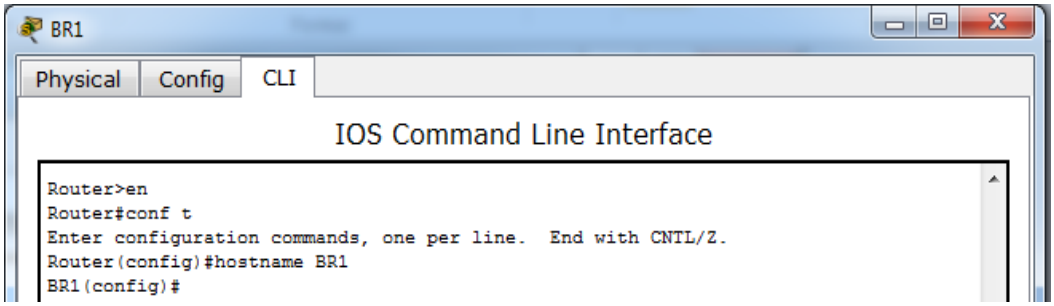
Paso 1. Realizar el cableado de red tal como se muestra en la topología.



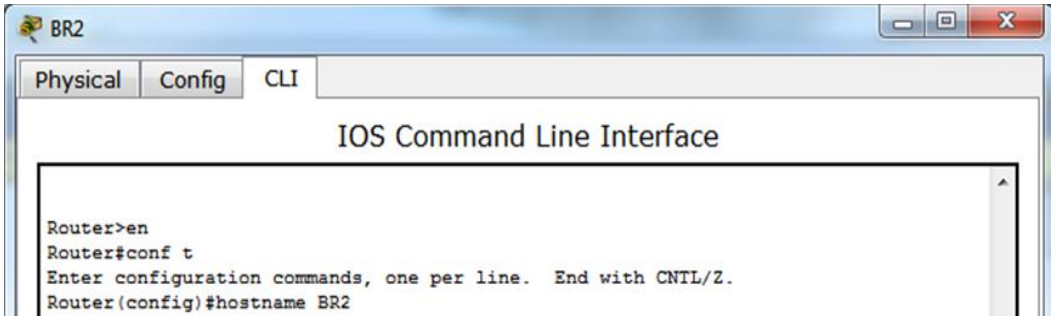
Paso 2. Configurar los parámetros básicos en cada router.

a. Asigne el nombre de dispositivo al router.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



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

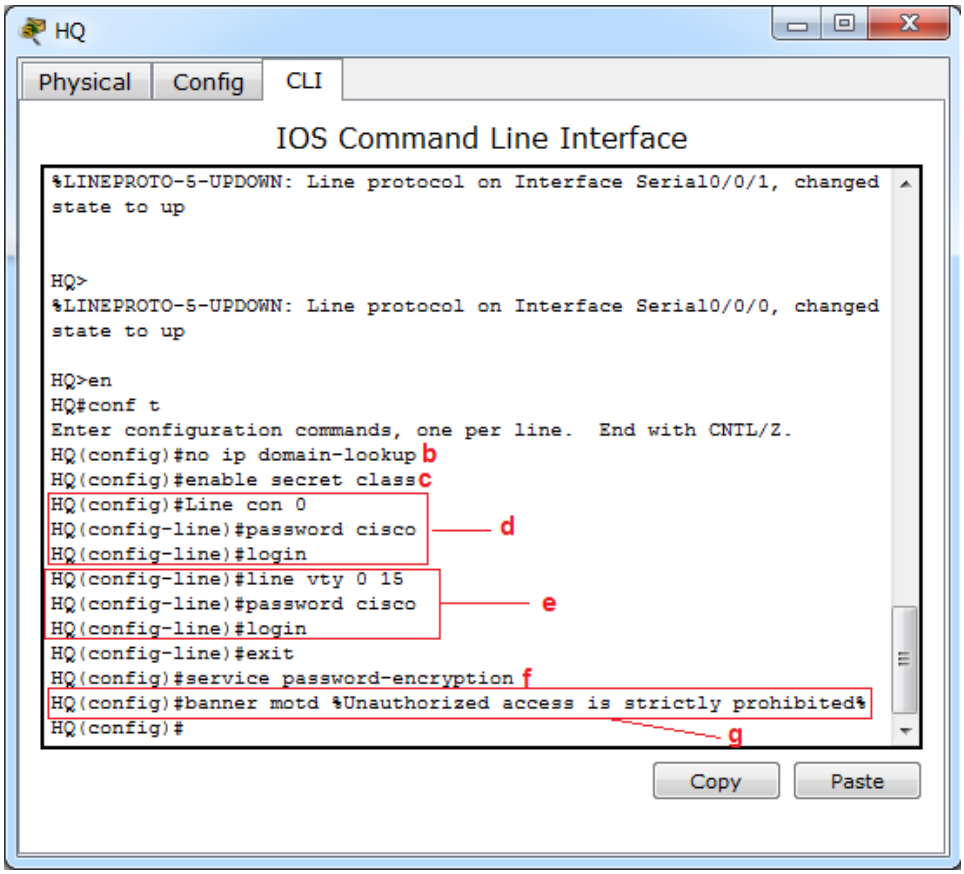
c. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

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

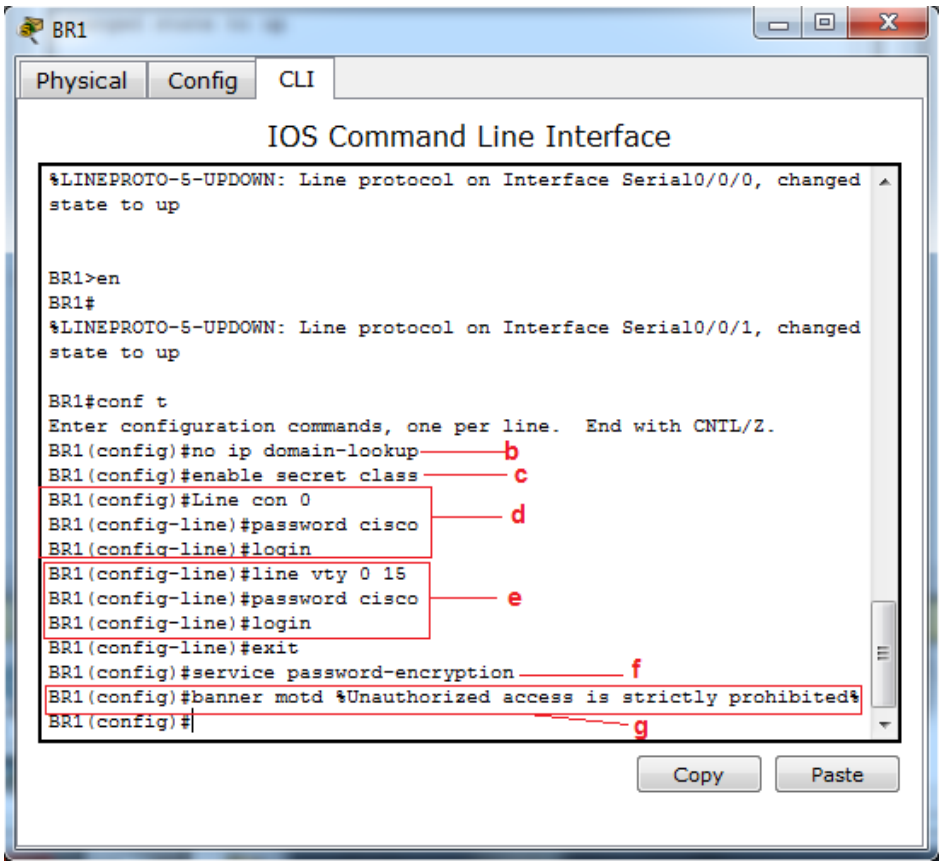
e. Asigne **cisco** como la contraseña de vty y habilite el inicio de sesión.

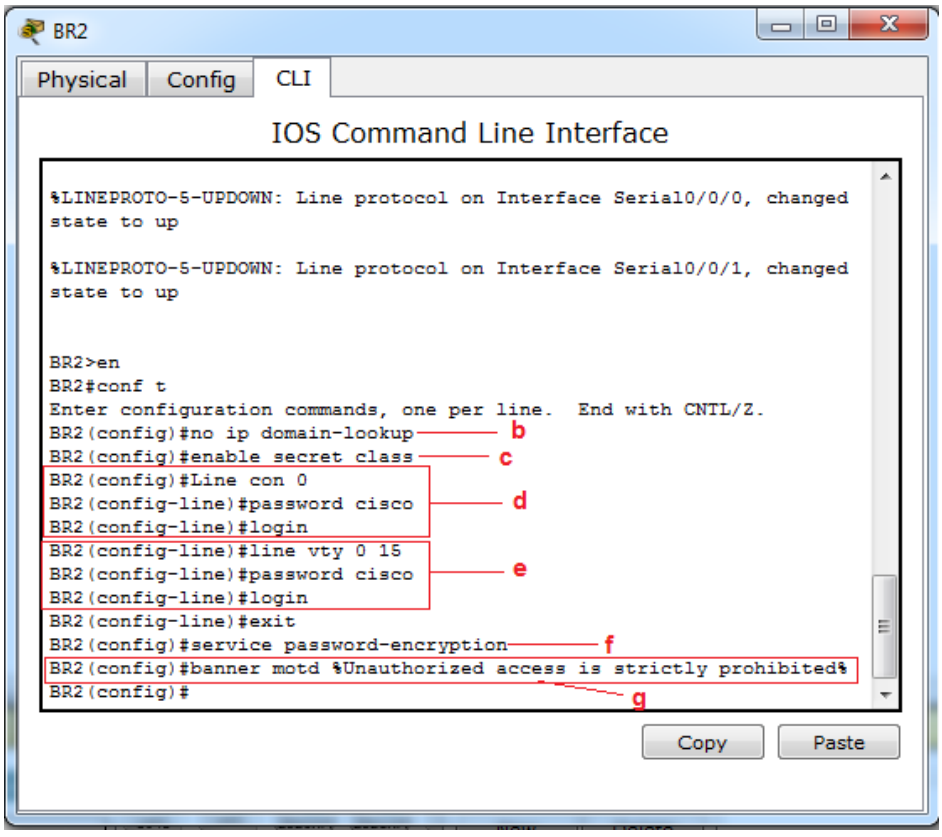
f. Cifre las contraseñas de texto no cifrado.

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



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Paso 3. Configurar las interfaces en cada router.

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

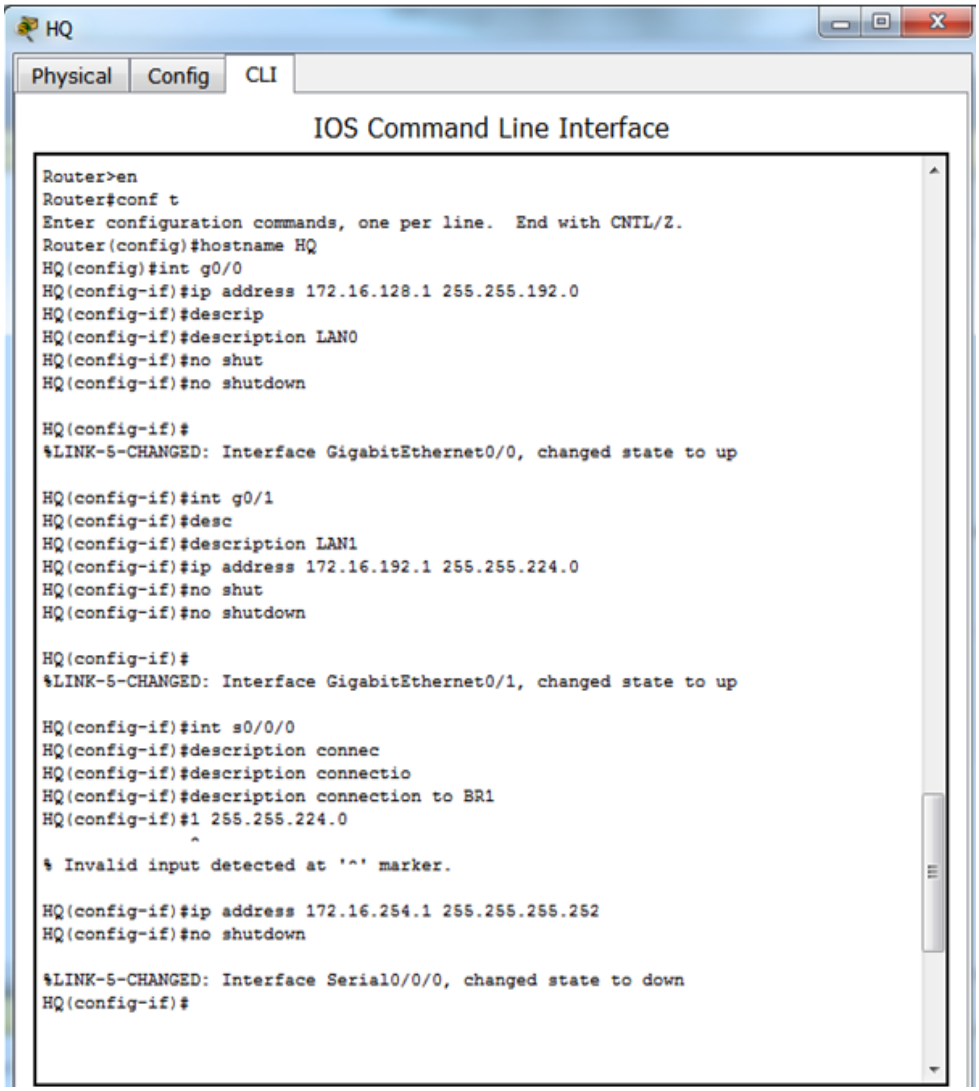
b. Configure una descripción de interfaz para cada interfaz.

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

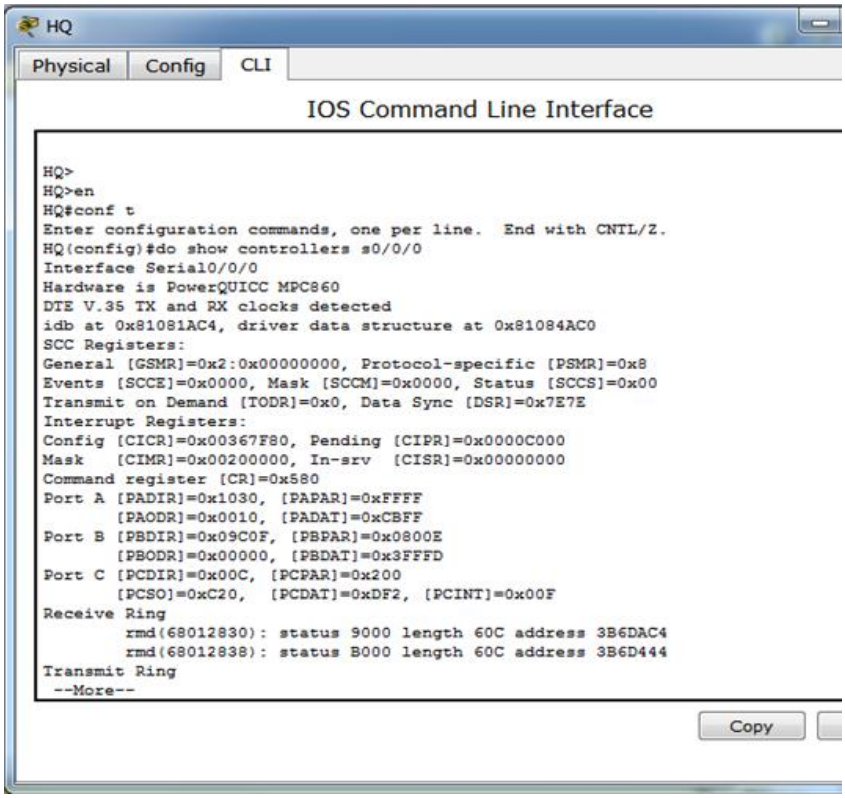
```
HQ(config-if)# clock rate 128000
```

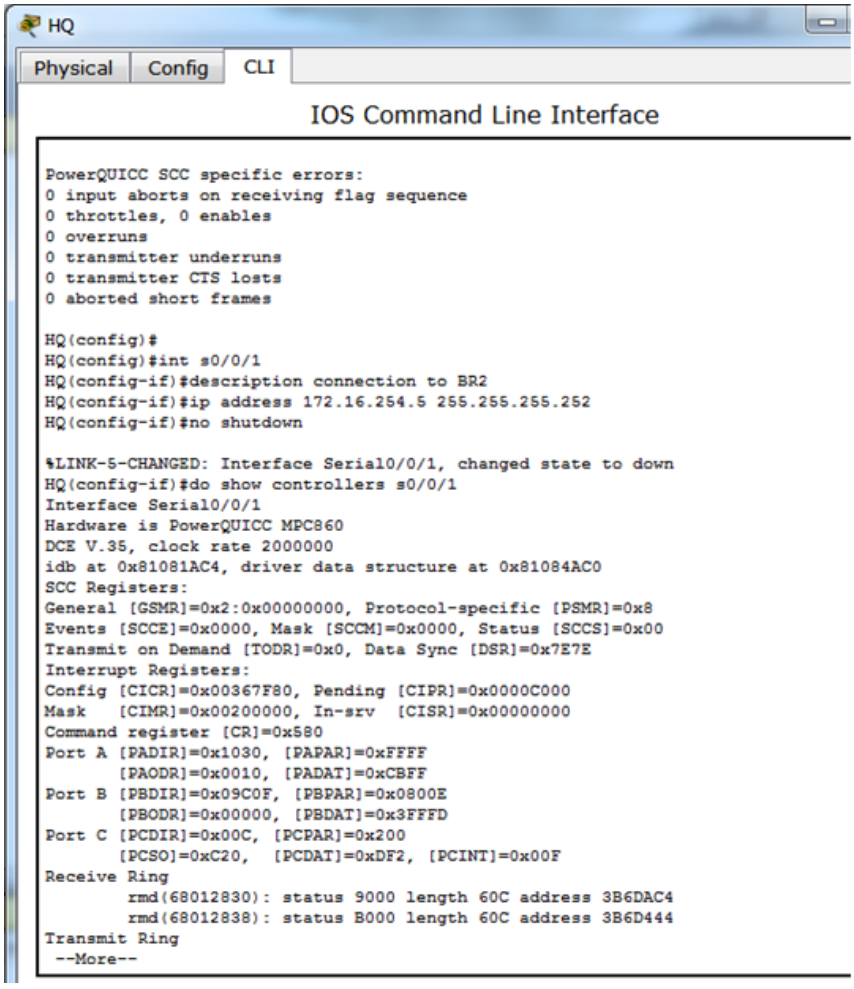
d. Active las interfaces.

Configuramos el Router HQ

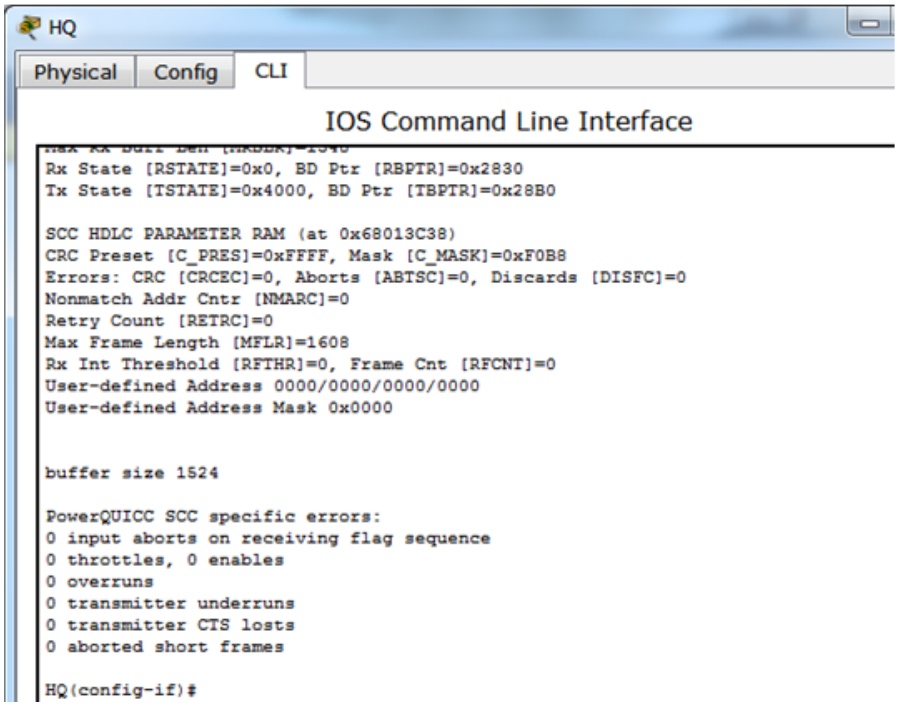


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

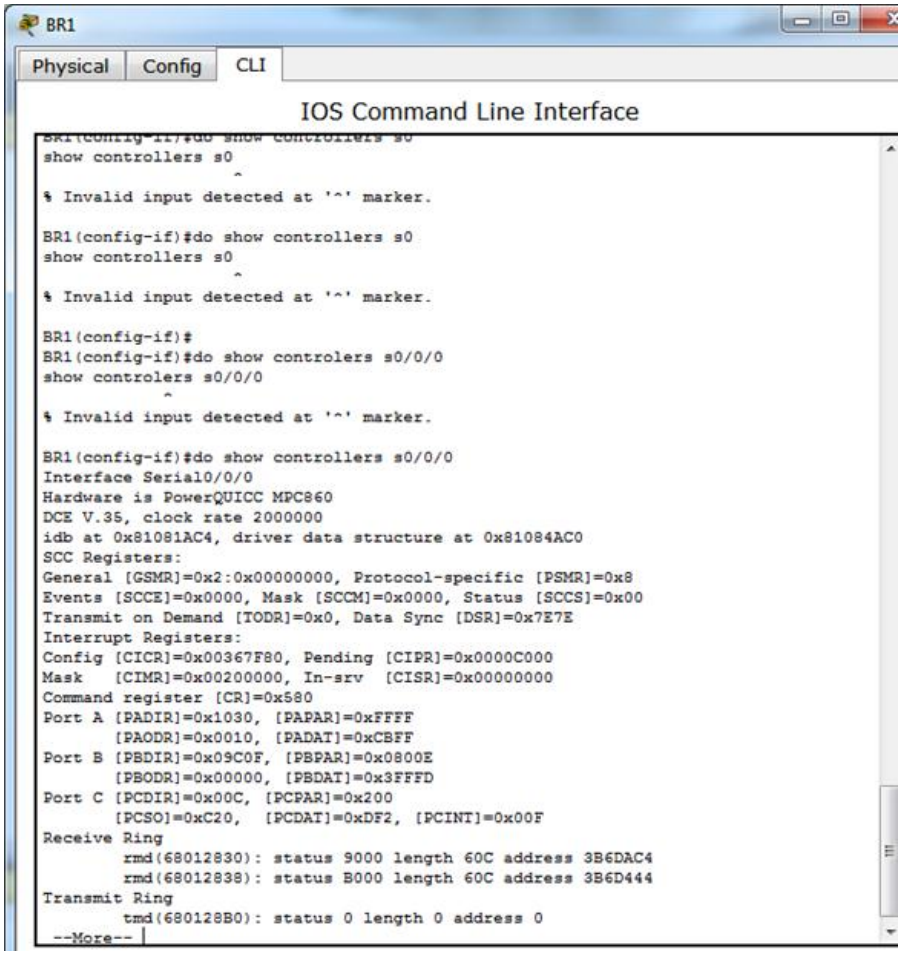




© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

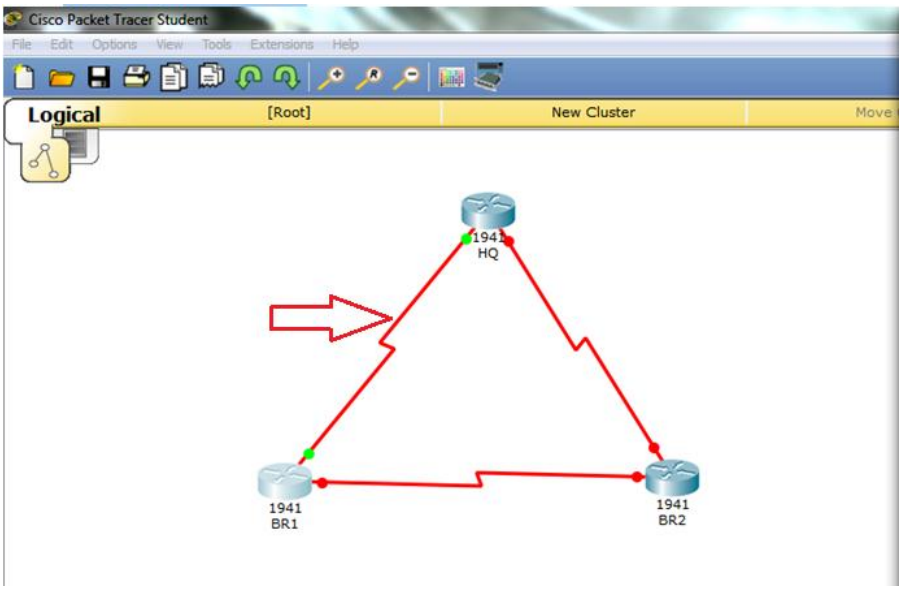


Configuramos el Router BR1



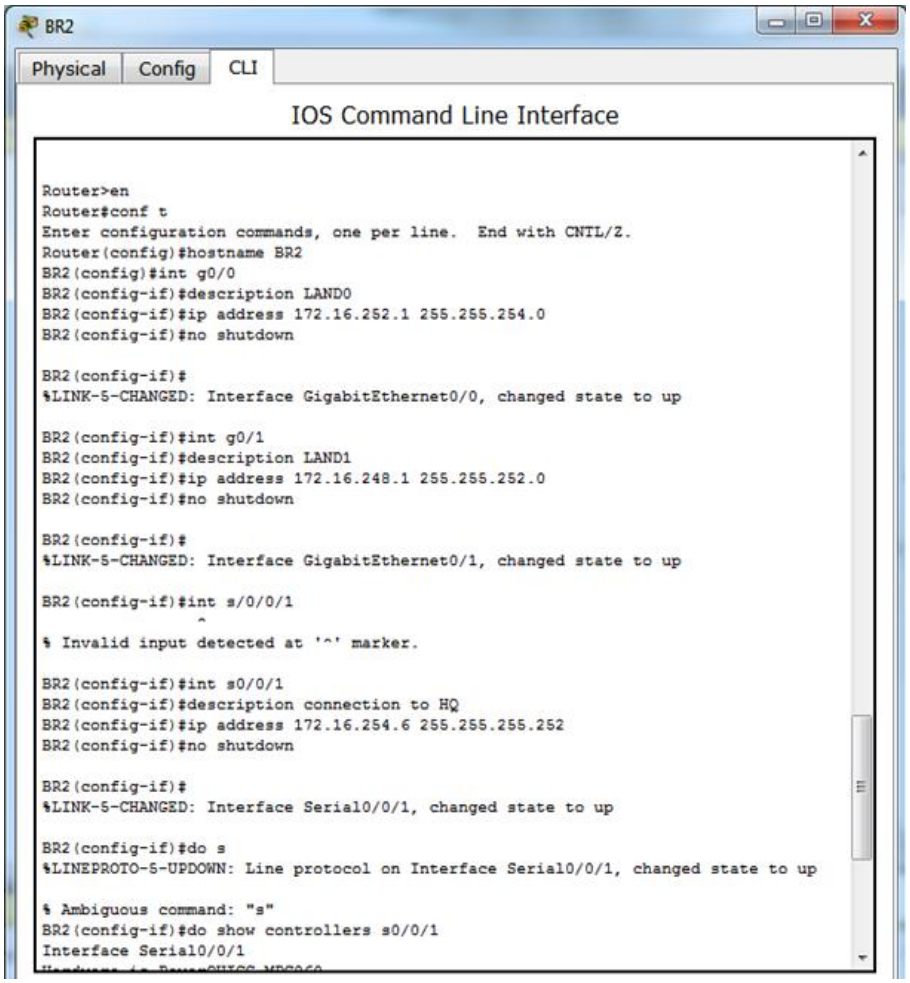
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Coneccion de BR1 con HQ

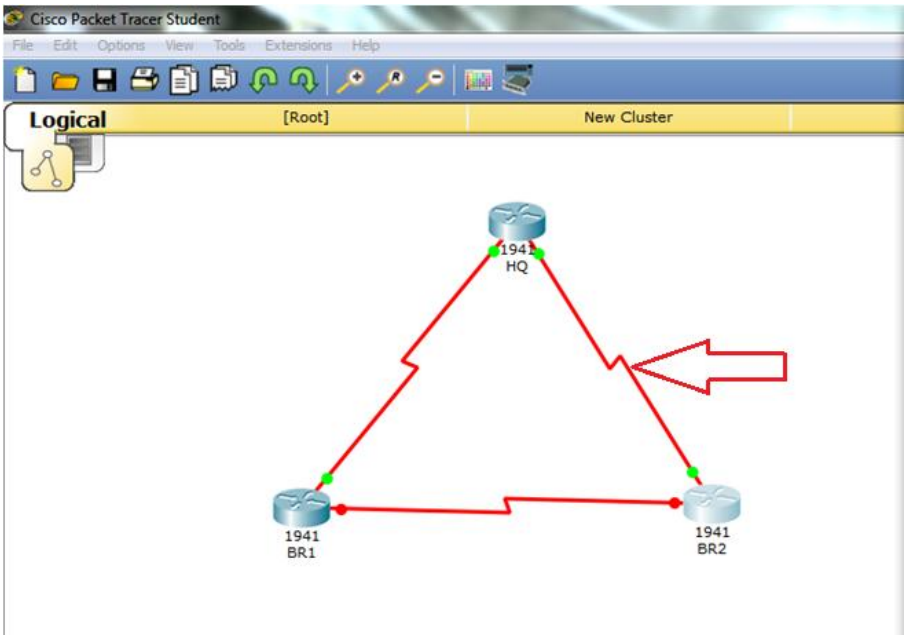


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

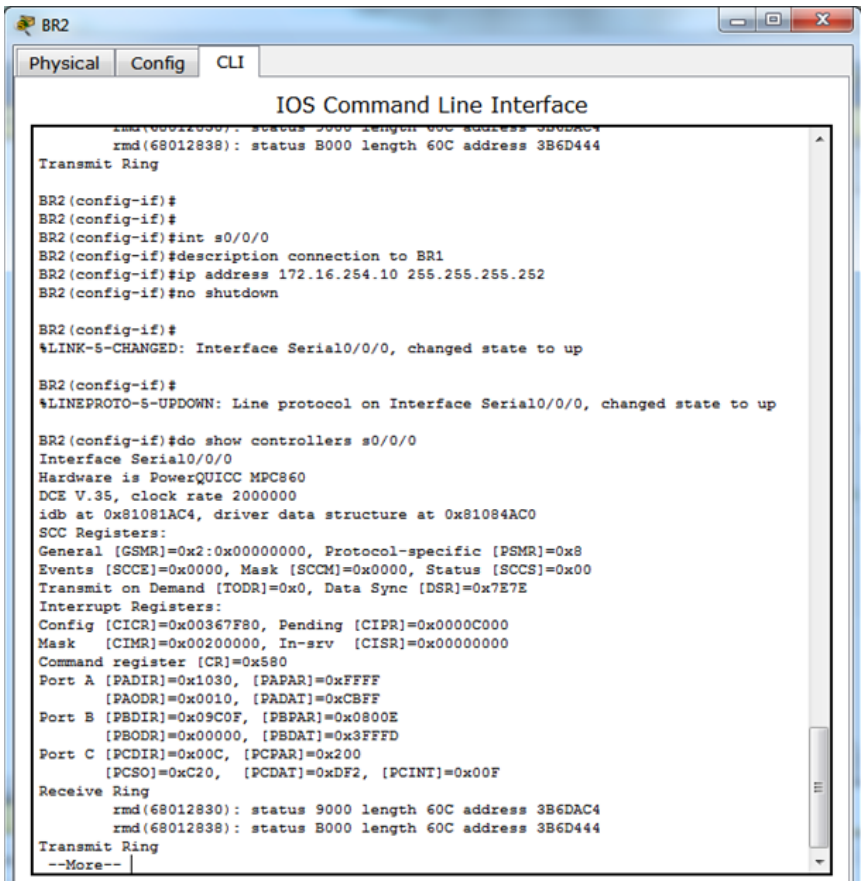
Configuramos el Router BR2

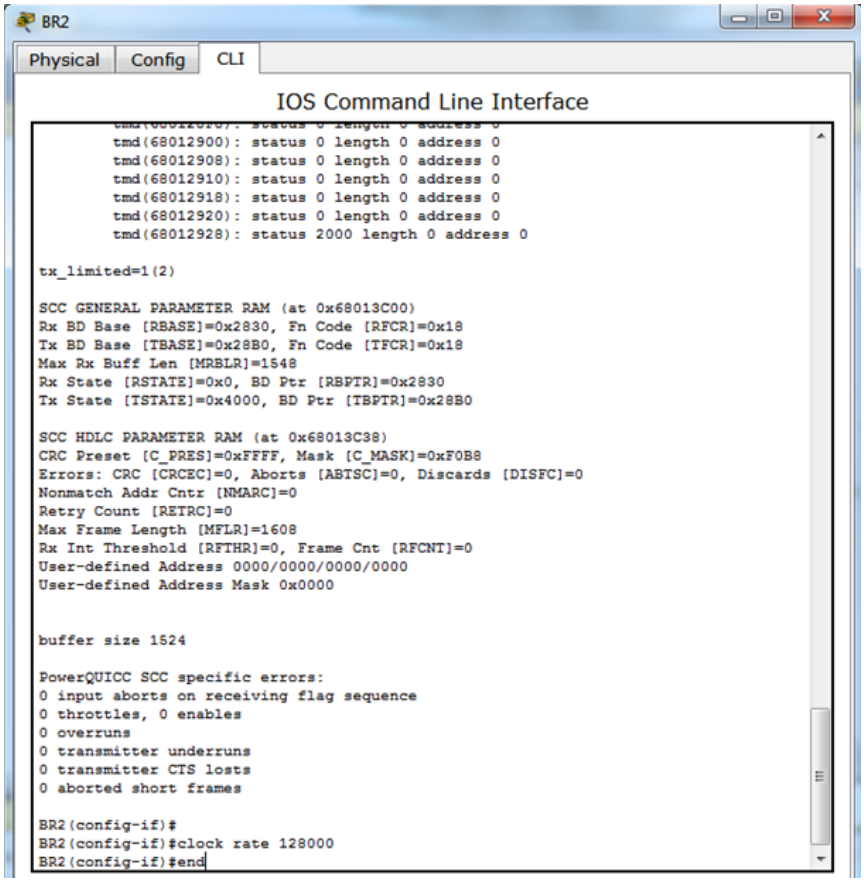


Coneccion de BR2 con HQ



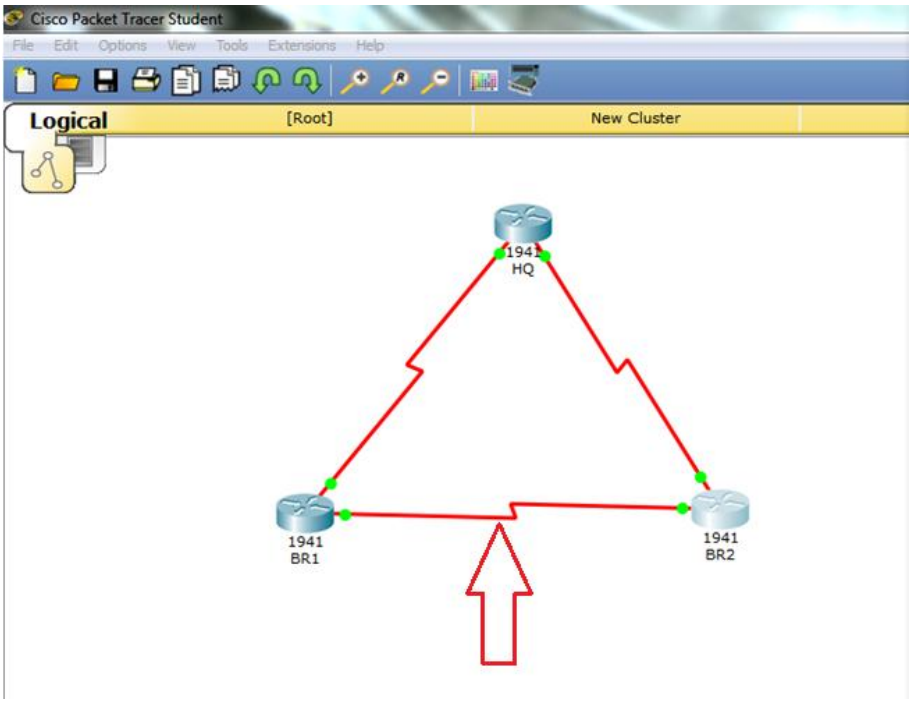
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

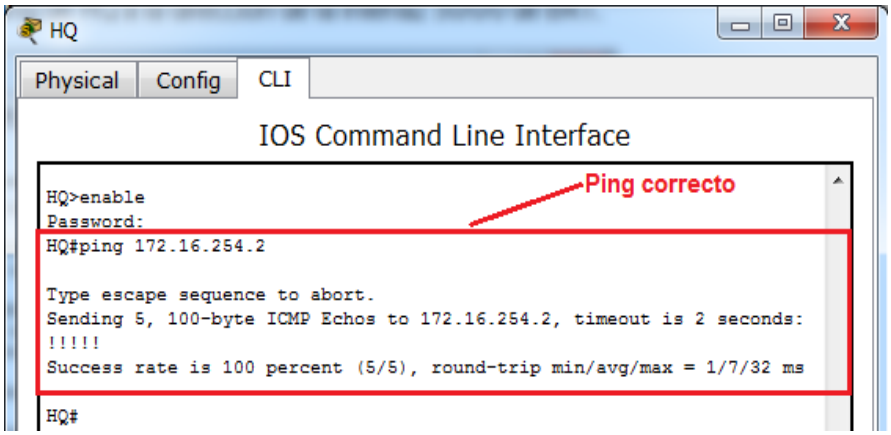
Coneccion de BR2 con BR1



Paso 4. Guardar la configuración en todos los dispositivos.

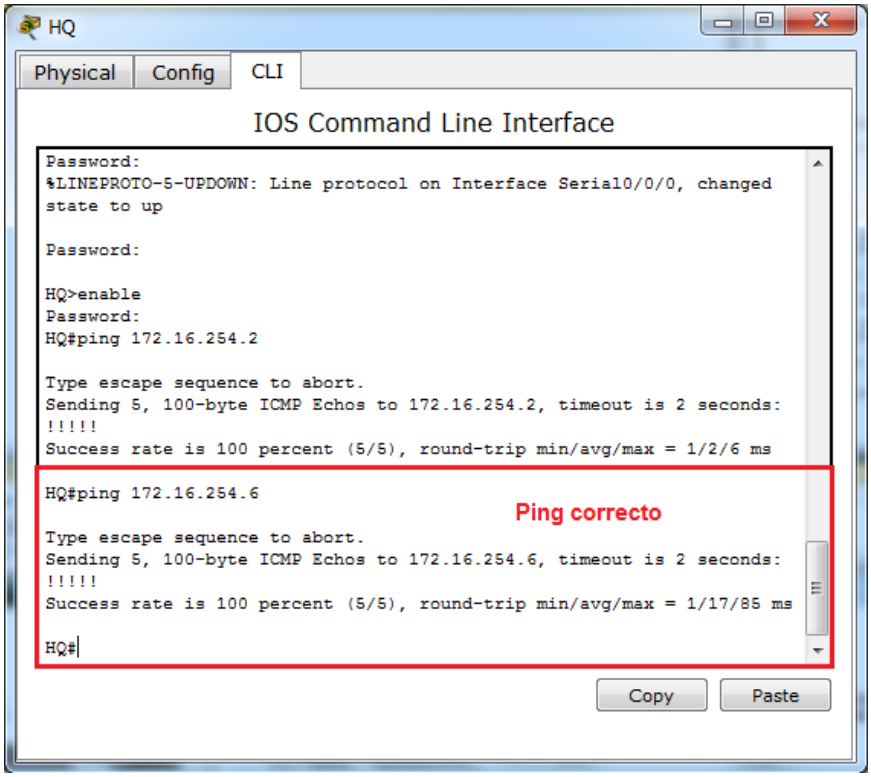
Paso 5. Probar la conectividad

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

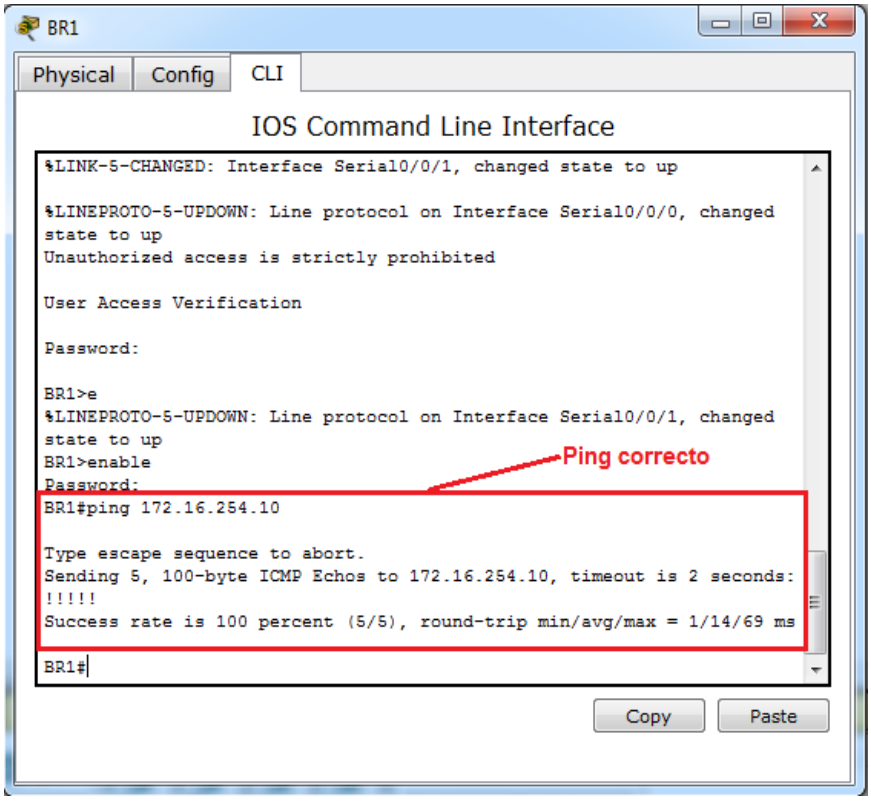


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

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

Reflexión

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

Una red con máscara de subred 30, tiene 4 espacios para direcciones, la dirección de red, dos direcciones por host, y una dirección de broadcast, podría ser tomando la dirección de red de la dirección previa y agregarle cuatro al último obteto.

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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 14

- En la práctica anterior se examinan los requisitos de red, siguiendo normalmente con las indicaciones y ayuda de los tutoriales, diseñamos el esquema de direcciones VLSM y también aprendemos a realizar el cableado y configuramos la red IPv4.
- Las prácticas realizadas nos llenan de mucho de conceptos, apreciaciones y comandos adecuados al momento de hacer las configuraciones adecuadas.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 15: 6.4.2.5 Lab - Calculating Summary Routes with IPv4 and IPv6

Topología

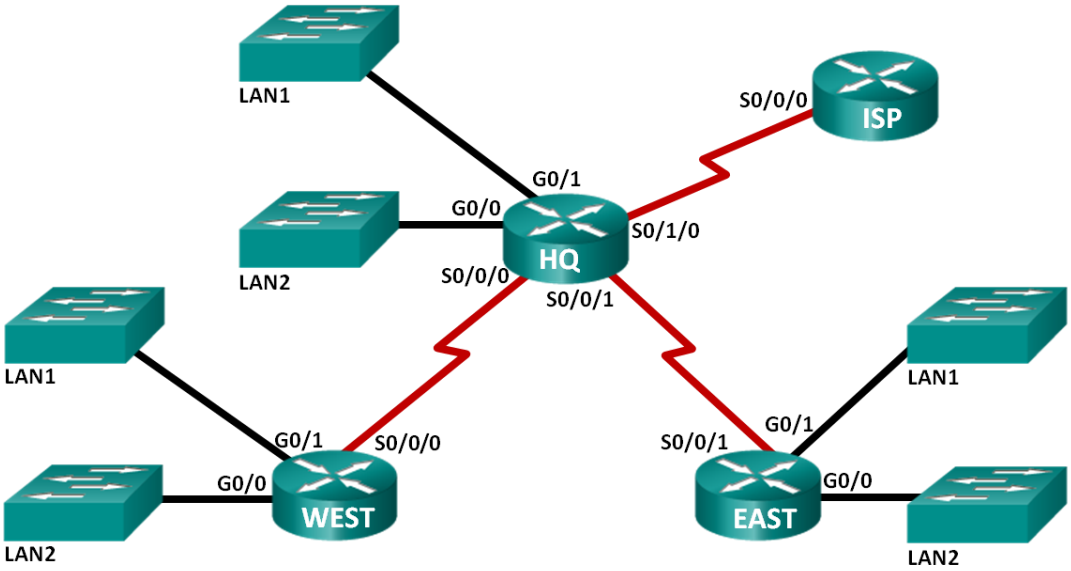


Tabla de direccionamiento

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

Objetivos

Parte 1: calcular rutas resumidas IPv4

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 1. Calcular rutas resumidas IPv4

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

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

LAN1 de HQ: 255.255.254.0

LAN1 de HQ: 255.255.254.0

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

LAN1 de HQ: 11000000.10101000. 01000000. 00000000

LAN1 de HQ: 11000000.10101000. 01000010. 00000000

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

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.

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

LAN1 de HQ 11000000.10101000.0100000.00000000

LAN2 de HQ 11000000.10101000.0100000.00000000

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

11000000.10101000.01000000.00000000

c. Indique las direcciones de red resumidas en formato decimal. 192.168.64.0

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

LAN1 de EAST: 255.255.255.0

LAN2 de EAST: 255.255.255.0

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

LAN1 de EAST: 11000000.10101000.01000100.00000000

LAN2 de EAST: 11000000.10101000.01000101.00000000

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

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

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

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

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

LAN1 de EAST: 11000000.10101000.0100010.00000000

LAN2 de EAST: 11000000.10101000.0100010.00000000

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

11000000.10101000.01000100.00000000

c. Indique las direcciones de red resumidas en formato decimal. 192.168.68.0

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

LAN1 de WEST: 255.255.255.128

LAN2 de WEST: 255.255.255.128

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

LAN1 de WEST: 11000000.10101000.01000110.00000000

LAN2 de WEST: 11000000.10101000.01000110.00000000

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

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

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

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

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

LAN1 de WEST: 11000000.10101000.01000110.00000000

LAN2 de WEST: 11000000.10101000.01000110.00000000

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

11000000.10101000.01000110.00000000

c. Indique las direcciones de red resumidas en formato decimal. 192.168.70.0

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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

HQ: 192.168.64.0 255.255.252.0

EAST: 192.168.68.0 255.255.254.0

WEST: 192.168.70.0 255.255.255.0

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

HQ: 11000000.10101000.01000000.00000000

EAST: 11000000.10101000.01000100.00000000

WEST: 11000000.10101000.01000110.00000000

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

a. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las tres redes? 21

b. 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.

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

HQ: 11000000.10101000.01000.00000000

EAST: 11000000.10101000.01000.00000000

WEST: 11000000.10101000.01000.00000000

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

11000000.10101000.01000000.00000000

c. Indique las direcciones de red resumidas en formato decimal. 192.168.64.0

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Parte 2. Calcular rutas resumidas IPv6

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

Topología

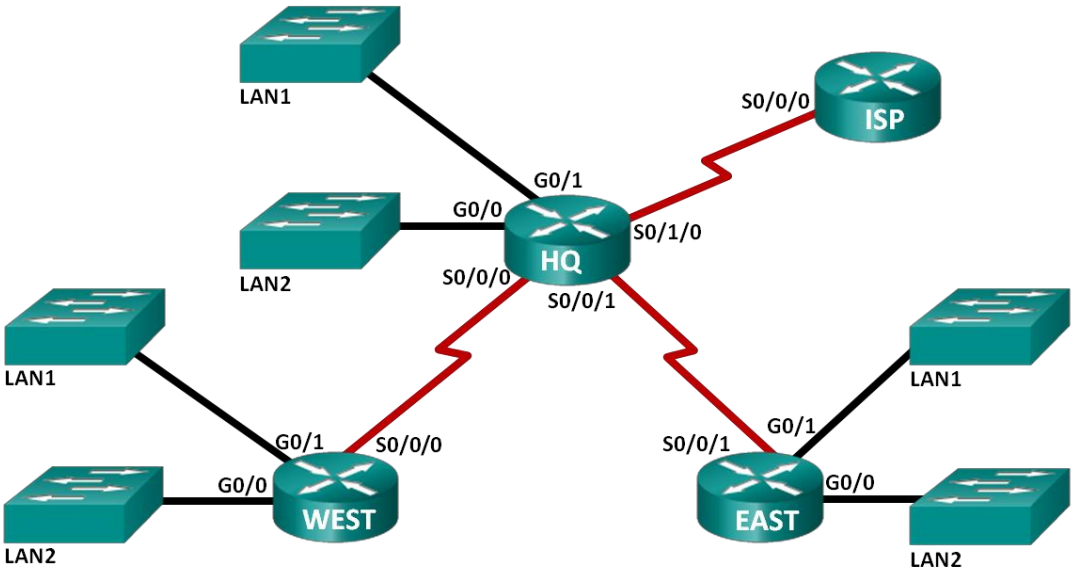


Tabla de direccionamiento

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

LAN1 de HQ: FFFF:FFFF:FFFF:FFFF

LAN2 de HQ: FFFF:FFFF:FFFF:FFFF

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

LAN1 de HQ: 0000000000001110

LAN2 de HQ: 0000000000001111

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. FFFF:FFFF:FFFF:FFFE

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

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

LAN1 de HQ: 000000000000111

LAN2 de HQ: 000000000000111

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

0000000000001110

c. Indique las direcciones de red resumidas en formato decimal. 2001:DB8: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	FFFF:FFFF:FFFF:FFFF	0000000000001110
LAN2 de HQ	2001:DB8:ACAD:F::/64	FFFF:FFFF:FFFF:FFFF	0000000000001111
Dirección de resumen de las LAN de HQ	2001:DB8:ACAD:E::/63	FFFF:FFFF:FFFF:FFFE	0000000000001110

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

LAN1 de EAST: FFFF:FFFF:FFFF:FFFF

LAN2 de EAST: FFFF:FFFF:FFFF:FFFF

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

LAN1 de EAST: 0000000000000001

LAN2 de EAST: 0000000000000010

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

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

b. Indique la máscara de subred de los primeros 64 bits de la ruta resumida. FFFF:FFFF:FFFF:FFFC

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

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

LAN1 de EAST: 00000000000000

LAN2 de EAST: 00000000000000

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

0000000000000000

c. Indique las direcciones de red resumidas en formato decimal. 2001:DB8:ACAD::/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	FFFF:FFFF:FFFF:FFFF	0000000000000001
LAN2 de EAST	2001:DB8:ACAD:2::/64	FFFF:FFFF:FFFF:FFFF	0000000000000010
Dirección de resumen de las LAN ESTE	2001:DB8:ACAD::/62	FFFF:FFFF:FFFF:FFFC	0000000000000000

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

LAN1 de WEST: FFFF:FFFF:FFFFF:FFFF

LAN2 de WEST: FFFF:FFFF:FFFFF:FFFF

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

LAN1 de WEST: 0000000000001001

LAN2 de WEST: 0000000000001010

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

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

b. Indique la máscara de subred de los primeros 64 bits de la ruta resumida. FFFF:FFFF:FFFFF:FFFC

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

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

LAN1 de WEST: 00000000000010

LAN2 de WEST: 00000000000010

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

0000000000001000

c. Indique las direcciones de red resumidas en formato decimal. 2001:DB8: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	FFFF:FFFF:FFFFF:FFFF	0000000000001001
LAN2 de WEST	2001:DB8:ACAD:A::/64	FFFF:FFFF:FFFFF:FFFF	0000000000001010
Dirección de resumen de las LAN OESTE	2001:DB8:ACAD:8::/62	FFFF:FFFF:FFFFF:FFFC	0000000000001000

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

HQ: FFFF:FFFF:FFFF:FFFE

EAST: FFFF:FFFF:FFFF:FFFC

WEST: FFFF:FFFF:FFFF:FFFC

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

HQ: 0000000000001110

EAST: 0000000000000000

WEST: 0000000000001000

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

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

b. Indique la máscara de subred de los primeros 64 bits de la ruta resumida. FFFF:FFFF:FFFF:FFF0

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

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

HQ: 000000000000

EAST: 000000000000

WEST: 000000000000

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

0000000000000000

c. Indique las direcciones de red resumidas en formato decimal. 2001:DB8:ACAD::/60

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Reflexión

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

   La diferencia es que ipv4 tiene 32 bits y ipv6 tiene 128 bits, también en ipv4 se convierte decimal a binario y en ipv6 se convierte de hexadecimal a binario.

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

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

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

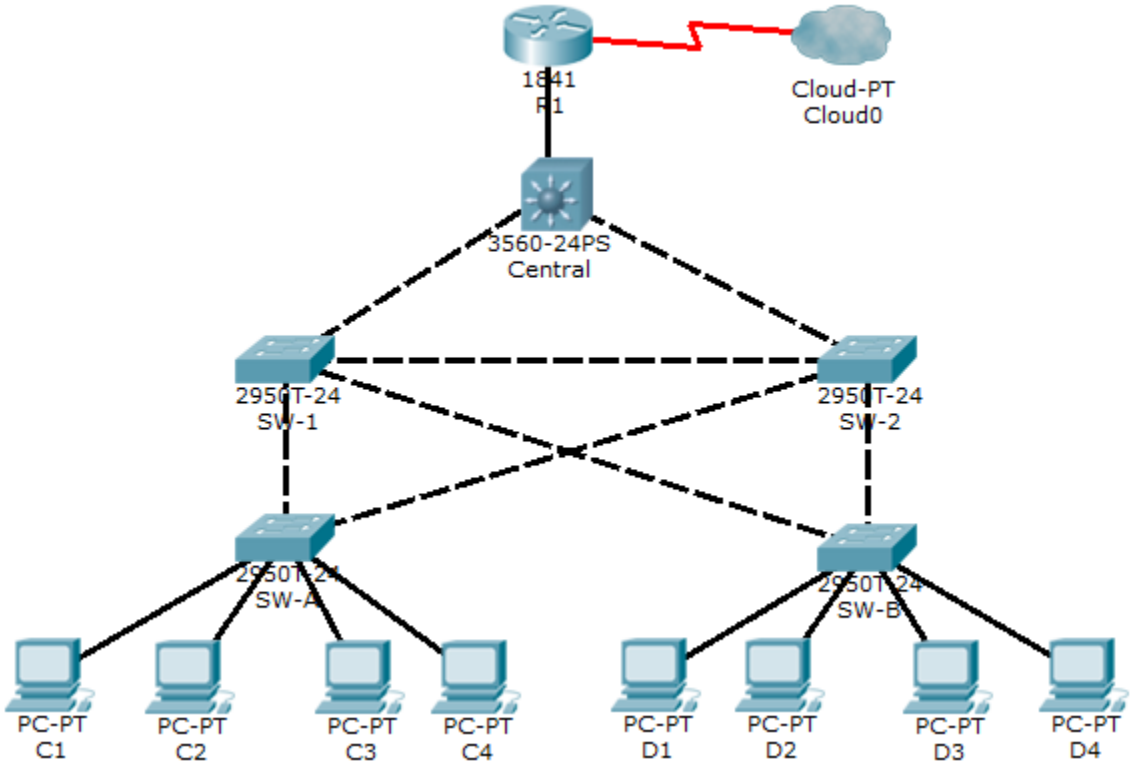
Conclusiones informe 15

- Con esta actividad se logró demostrar que 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.
- Se dio a conocer que con este proceso se disminuye los requisitos de memoria del router.
- Conocimos que se puede usar una sola ruta estática para representar unas pocas rutas o miles de rutas.
- Con esta práctica de laboratorio, determinamos las rutas resumidas de diferentes subredes de una red.
- Determinamos la ruta resumida de toda la red.
- Determinamos las rutas resumidas para direcciones IPv4 e IPv6.
- Debido a que IPv6 usa valores hexadecimales, convertimos los valores hexadecimales en valores binarios.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 16: 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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

All switch devices have been preconfigured with the following:

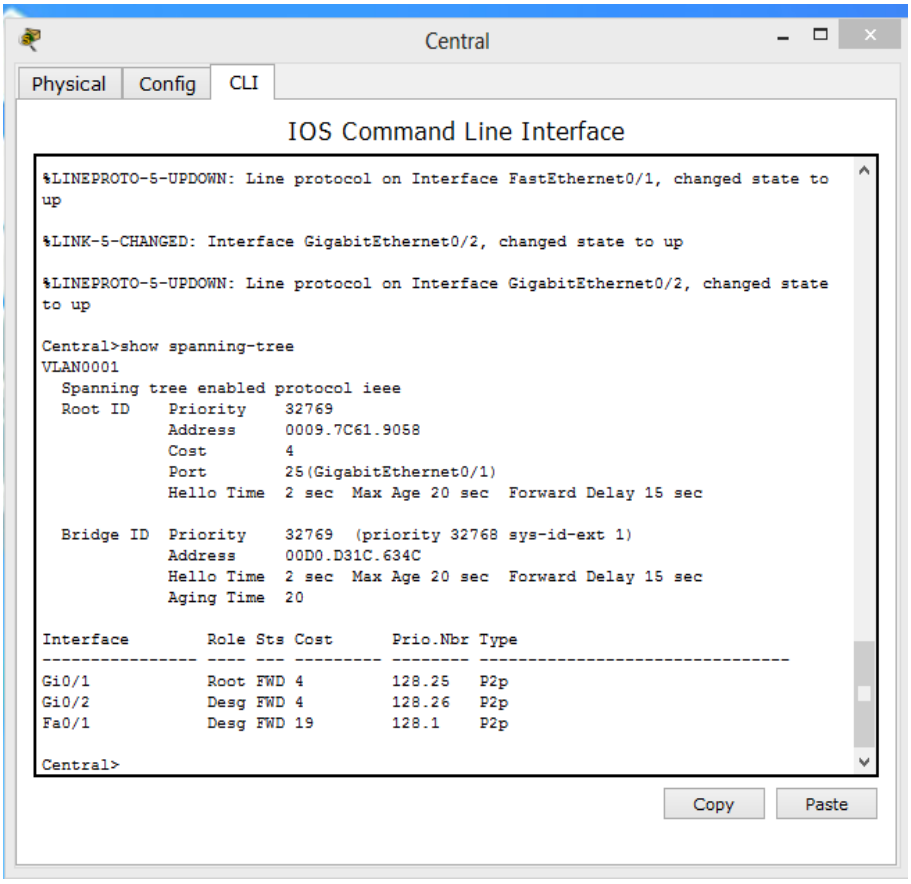
- Enable password: **ciscoenpa55**
- Console password: **ciscoconpa55**
- VTY line password: **ciscovtypa55**

Part 1: Configure Root Bridge

Step 1: Determine the current root bridge.

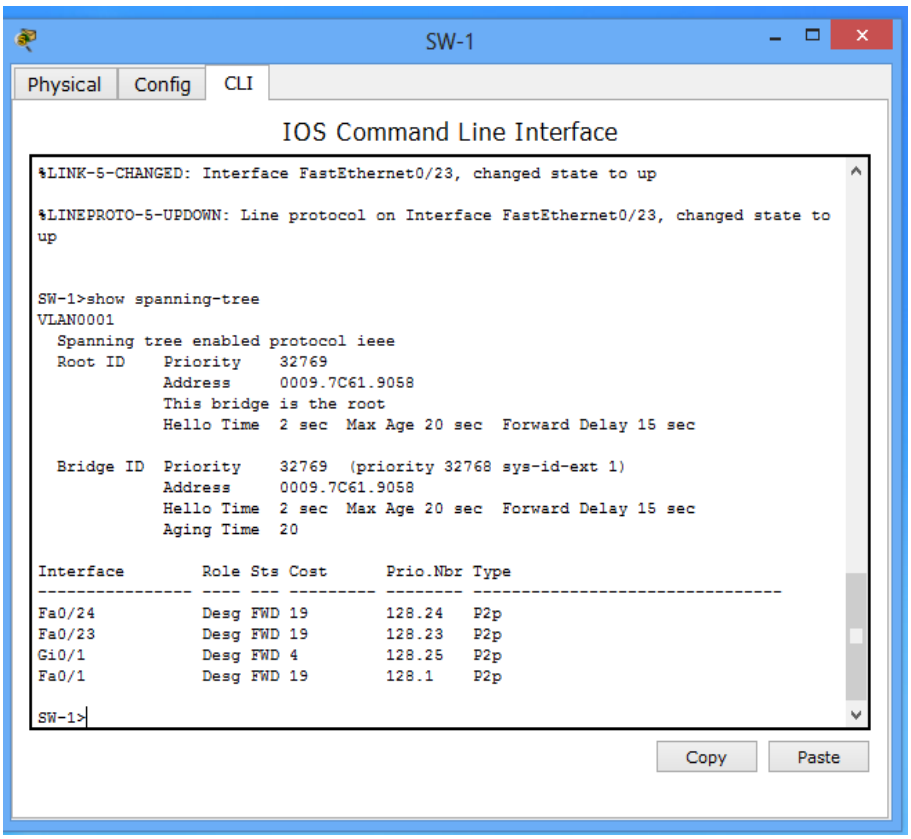
From **Central**, issue the **show spanning-tree** command to determine the current root bridge and to see the ports in use and their status.

Which switch is the current root bridge?



La raíz actual es SW-1

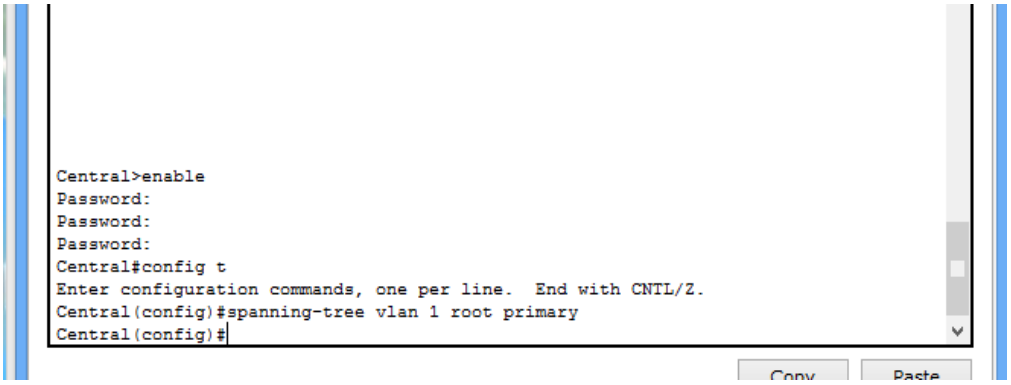
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



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
```

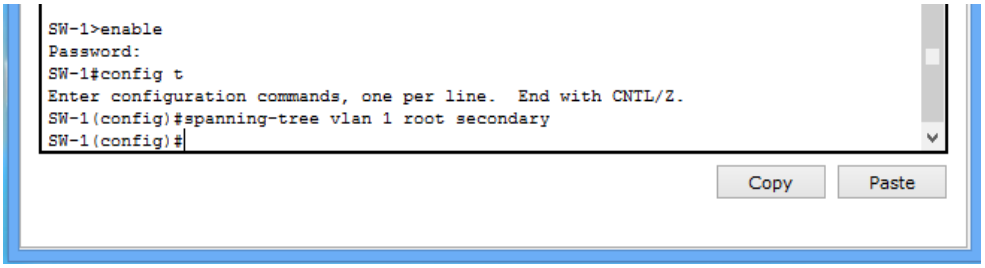


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

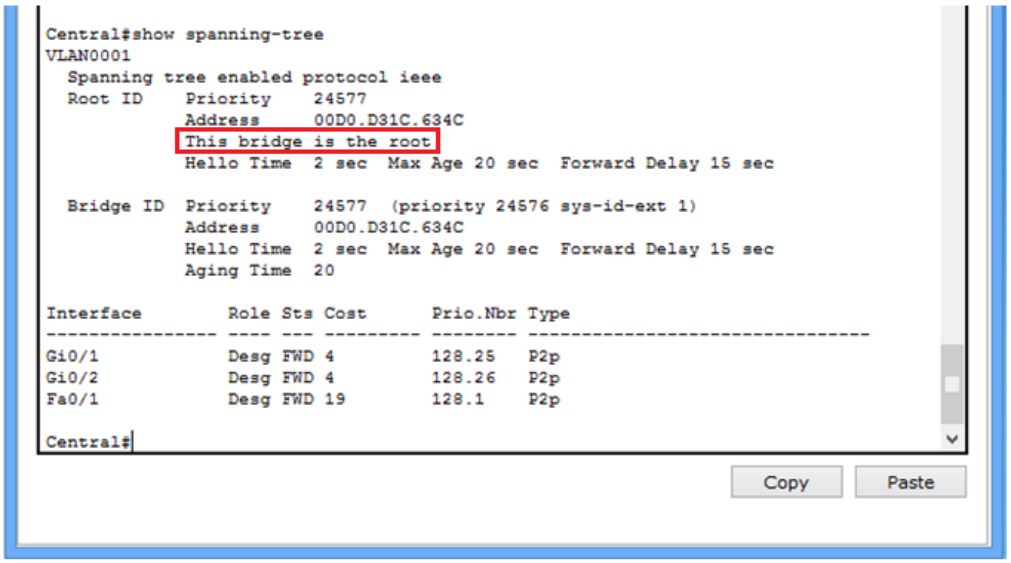
```
SW-1(config)# spanning-tree vlan 1 root secondary
```



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?



La raíz actual es Central

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

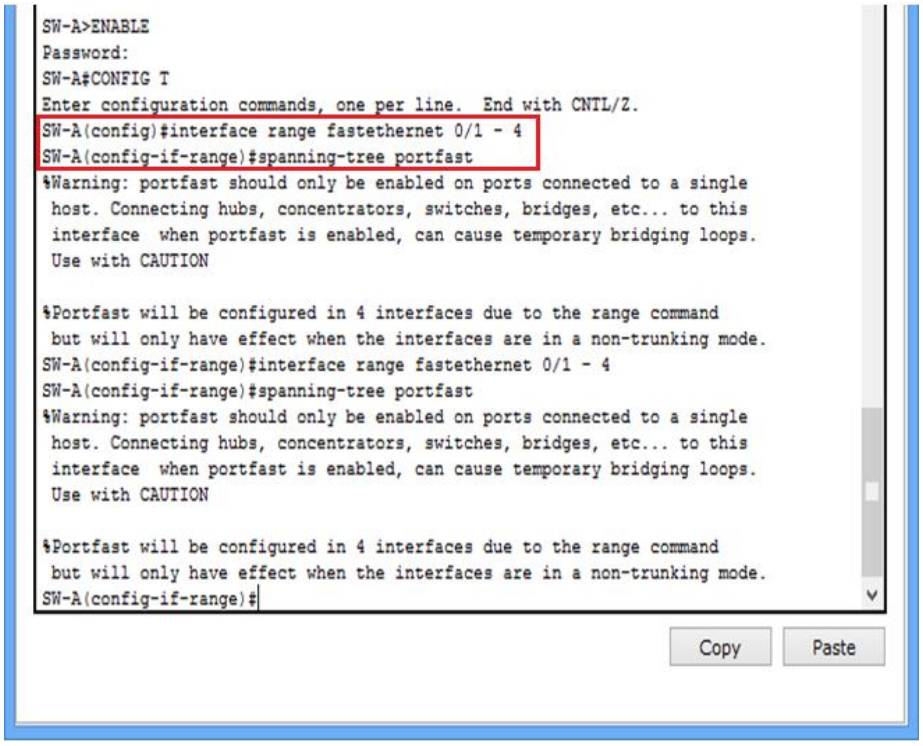
Part 2: Protect Against STP Attacks

Secure the STP parameters to prevent STP manipulation attacks.

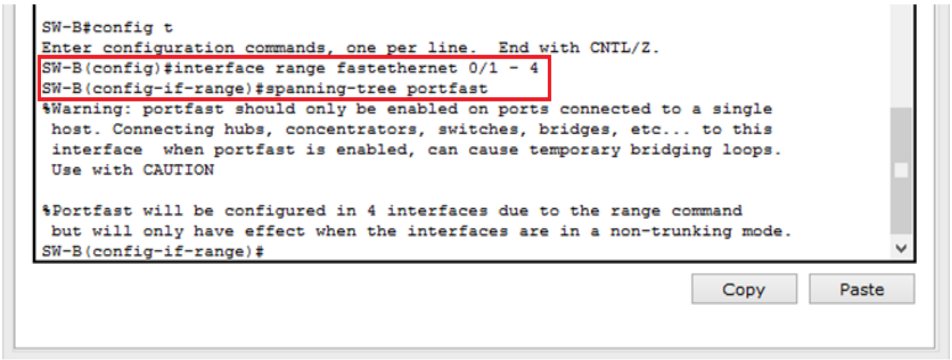
Step 1: Enable PortFast on all access ports.

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.

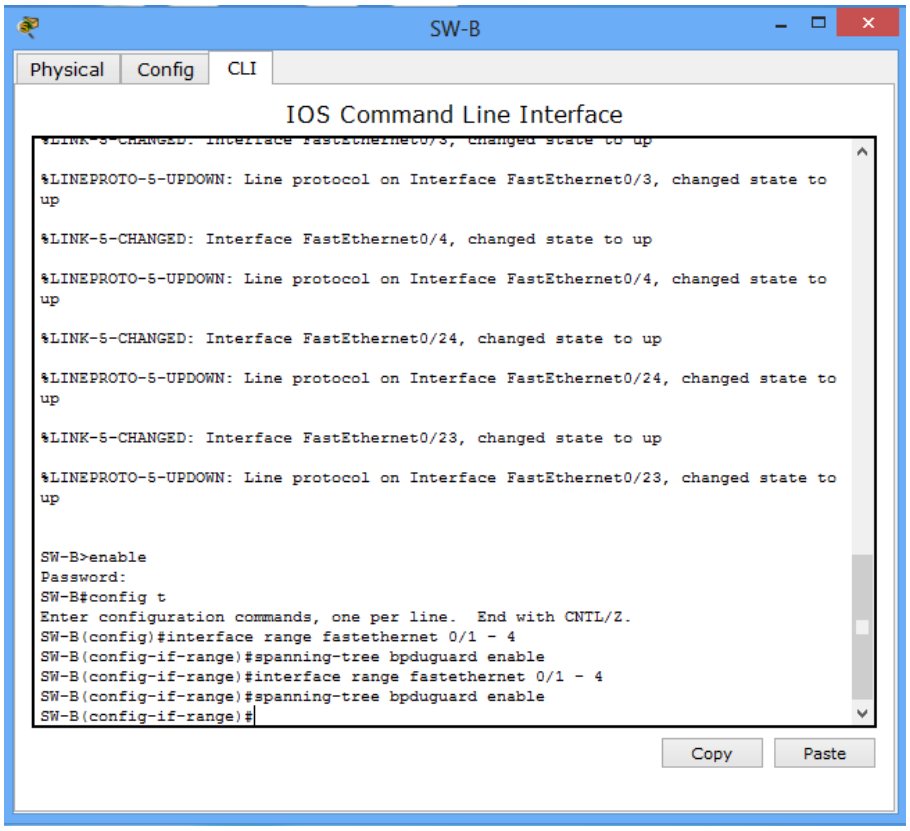
```
SW-A(config)# interface range fastethernet 0/1 - 4
SW-A(config-if-range)# spanning-tree portfast
```




```
SW-B(config)# interface range fastethernet 0/1 - 4
SW-B(config-if-range)# spanning-tree portfast
```



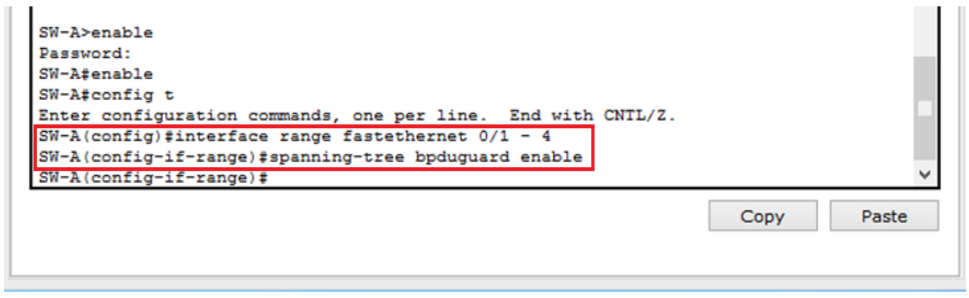
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



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)# interface range fastethernet 0/1 - 4
SW-A(config-if-range)# spanning-tree bpduguard enable
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
SW-B(config)# interface range fastethernet 0/1 - 4
SW-B(config-if-range)# spanning-tree bpduguard enable
```

```
SW-B>enable
Password:
SW-B#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-B(config)#interface range fastethernet 0/1 - 4
SW-B(config-if-range)#spanning-tree bpduguard enable
SW-B(config-if-range)#interface range fastethernet 0/1 - 4
SW-B(config-if-range)#spanning-tree bpduguard enable
SW-B(config-if-range)#
```

Note: Spanning-tree BPDU guard can be enabled on each individual port using the **spanning-tree bpduguard 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.

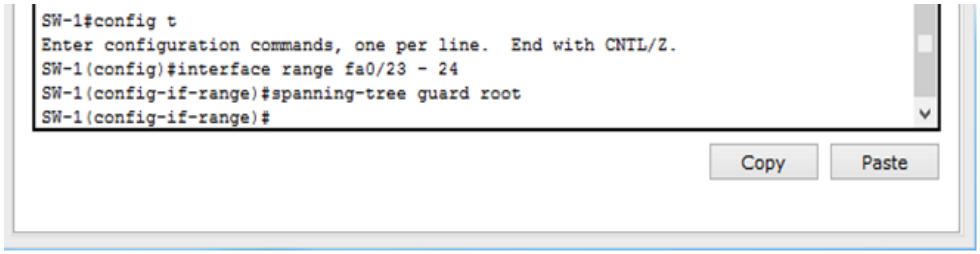
On **SW-1**, enable root guard on ports Fa0/23 and Fa0/24. On **SW-2**, enable root guard on ports Fa0/23 and Fa0/24.

```
SW-1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00D0.D31C.634C
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28673  (priority 28672 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
---------------- ---- --- --------- -------- --------------------------------
Fa0/24           Desg FWD 19        128.24   P2p
Fa0/23           Desg FWD 19        128.23   P2p
Gi0/1            Root FWD 4         128.25   P2p
Fa0/1            Desg FWD 19        128.1    P2p

SW-1#
```

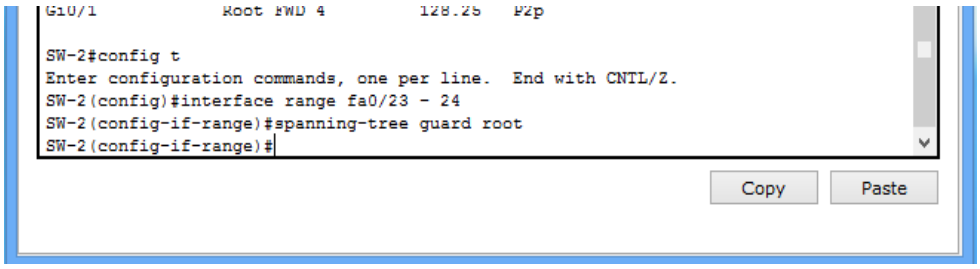
```
SW-2>enable
Password:
SW-2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00D0.D31C.634C
              Cost        4
              Port        25(GigabitEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000A.41B2.574A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p
Gi0/1            Root FWD 4         128.25   P2p

SW-2#
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
SW-1(config)# interface range fa0/23 - 24
SW-1(config-if-range)# spanning-tree guard root
```




```
SW-2(config)# interface range fa0/23 - 24
SW-2(config-if-range)# spanning-tree guard root
```

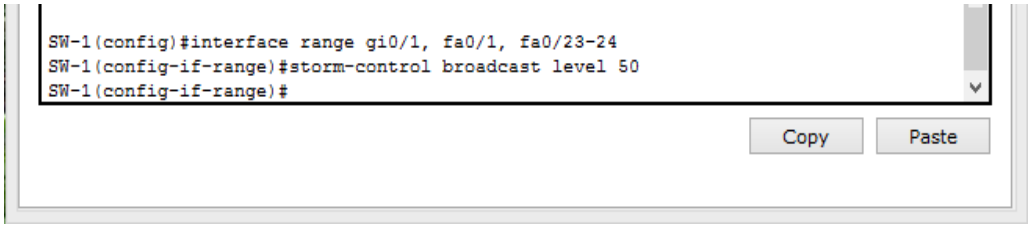


Part 3: Enable Storm Control

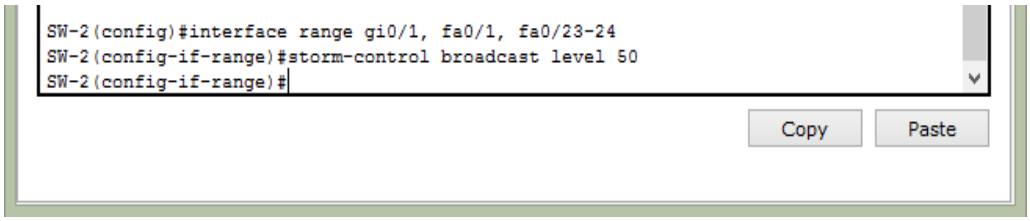
Step 1: Enable storm control for broadcasts.

a. 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)# interface range gi1/1 , fa0/1 , fa0/23 - 24
SW-1(config-if)# storm-control broadcast level 50
```




```
SW-2(config)# interface range gi1/1 , fa0/1 , fa0/23 - 24
SW-2(config-if)# storm-control broadcast level 50
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
Central(config-if)# interface range gi0/1 , gi0/2 , fa0/1
Central(config-if)# storm-control broadcast level 50
```

```
Central>enable
Password:
Central#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Central(config)#interface range gi0/1 , gi0/2 , fa0/1
Central(config-if-range)#storm-control broadcast level 50
Central(config-if-range)#
```

Copy Paste

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**.

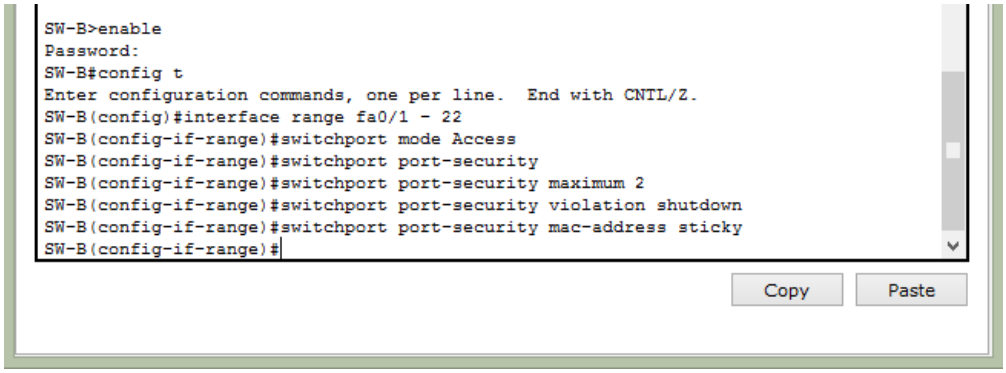
Note: A switch port must be configured as an access port to enable port security.

```
SW-A(config)# interface range fa0/1 - 22
SW-A(config-if-range)# switchport mode access
SW-A(config-if-range)# switchport port-security
SW-A(config-if-range)# switchport port-security maximum 2
SW-A(config-if-range)# switchport port-security violation shutdown
SW-A(config-if-range)# switchport port-security mac-address sticky
```

```
SW-A>enable
Password:
SW-A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)#interface range fa0/1 - 22
SW-A(config-if-range)#switchport mode access
SW-A(config-if-range)#switchport port-security
SW-A(config-if-range)#switchport port-security maximum 2
SW-A(config-if-range)#switchport port-security violation shutdown
SW-A(config-if-range)#switchport port-security mac-address sticky
SW-A(config-if-range)#
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
SW-B(config)# interface range fa0/1 - 22
SW-B(config-if-range)# switchport mode access
SW-B(config-if-range)# switchport port-security
SW-B(config-if-range)# switchport port-security maximum 2
SW-B(config-if-range)# switchport port-security violation shutdown
SW-B(config-if-range)# switchport port-security mac-address sticky
```



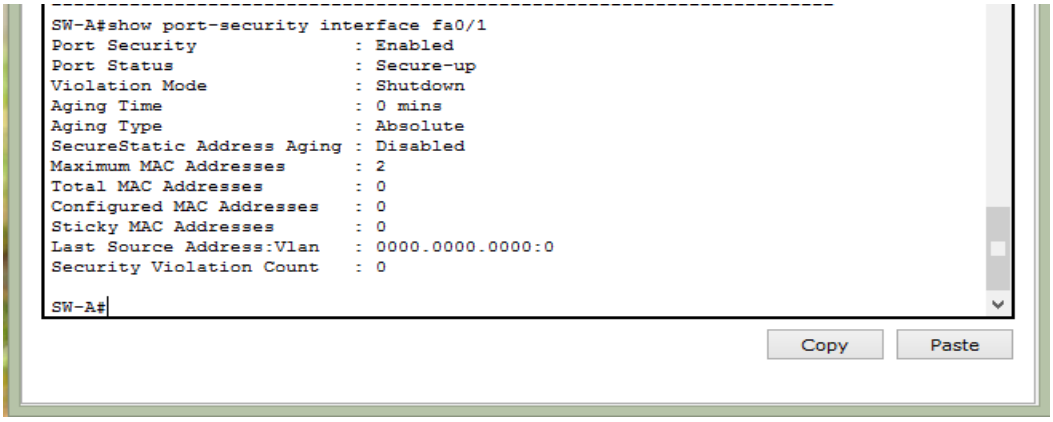
Why would you not want to enable port security on ports connected to other switches or routers?

Ports connected to other switch devices and routers can, and should, have a multitude of MAC addresses learned for that single port. Limiting the number of MAC addresses that can be learned on these ports can significantly impact network functionality.

Porque los puertos conectados a otros dispositivos de conmutación y enrutadores pueden y deben tener una multitud de direcciones MAC aprendidas para ese único puerto. Limitar el número 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.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Step 3: Disable unused ports.

Disable all ports that are currently unused.

```
SW-A(config)# interface range fa0/5 - 22
SW-A(config-if-range)# shutdown
```

```
SW-A>enable
Password:
SW-A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-A(config)#interface range fa0/5  22
                                    ^
% Invalid input detected at '^' marker.

SW-A(config)#interface range fa0/5-22
SW-A(config-if-range)#shutdown

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

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

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively
down
```

Copy Paste

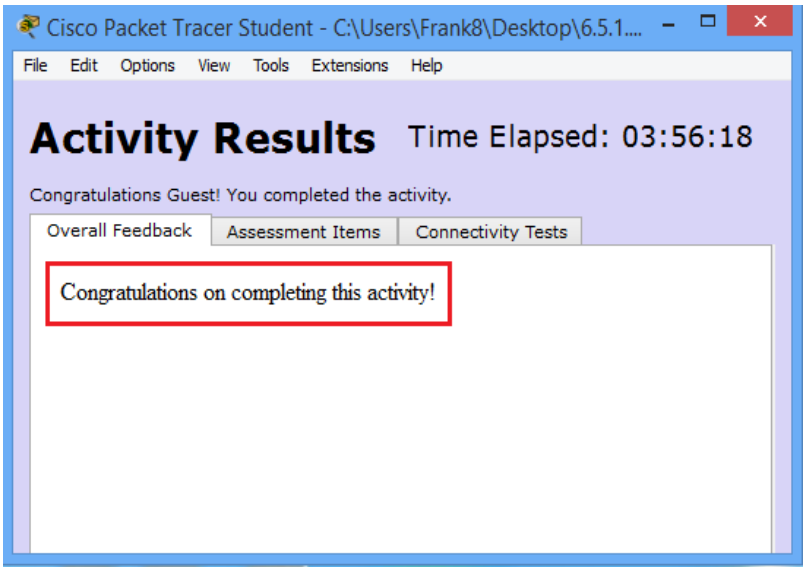
```
SW-B(config)# interface range fa0/5 - 22
SW-B(config-if-range)# shutdown
```

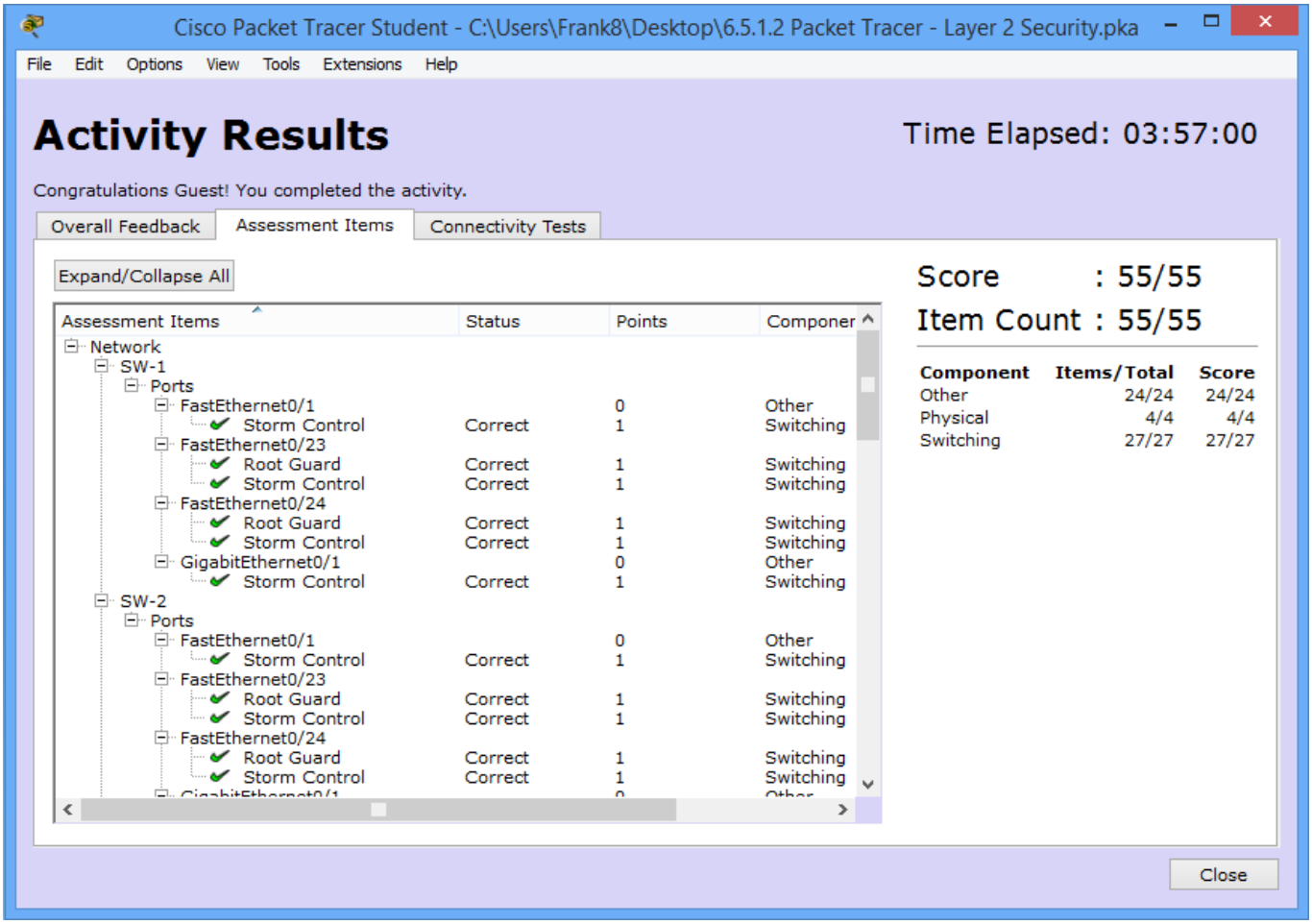
```
SW-B(config)#interface range fa0/5-22
SW-B(config-if-range)#shutdown

%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 FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively
down
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

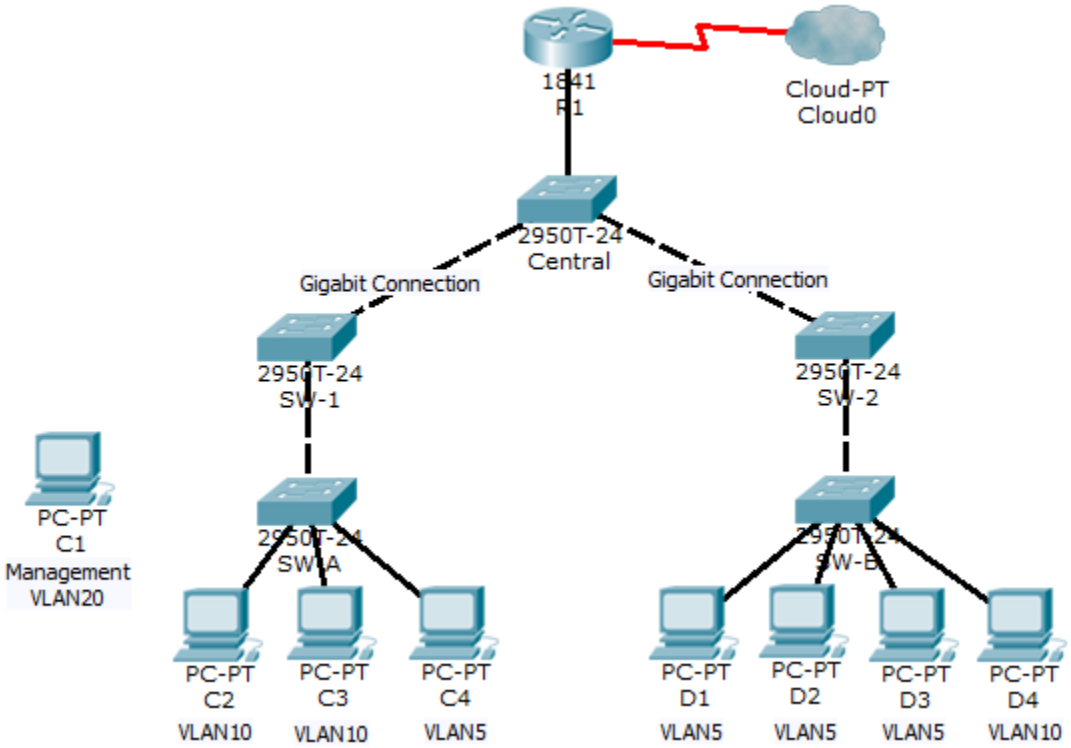
Conclusiones informe 16

- Con el desarrollo de esta actividad aprendí a asignar el interruptor central como el puente raíz.
- Conocimos los procedimientos necesarios para proteger los parámetros del árbol de expansión para evitar ataques de manipulación de STP.
- Conocimos los comandos necesarios para habilitar el control de tormentas para evitar tormentas de radiodifusión y habilitar la seguridad del puerto y así evitar ataques de desbordamiento de la tabla de direcciones MAC.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Informe 17: 6.5.1.3 Packet Tracer - Layer 2 VLAN Security

Topology



Objectives

- Connect a new redundant link between SW-1 and SW-2.
- Enable trunking and configure security on the new trunk link between SW-1 and SW-2.
- Create a new management VLAN (VLAN 20) and attach a management PC to that VLAN.
- Implement an ACL to prevent outside users from accessing the management VLAN.

Background / Scenario

A company's network is currently set up using two separate VLANs: VLAN 5 and VLAN 10. In addition, all trunk ports are configured with native VLAN 15. A network administrator wants to add a redundant link between switch SW-1 and SW-2. The link must have trunking enabled and all security requirements should be in place.

In addition, the network administrator wants to connect a management PC to switch SW-A. The administrator would like to allow the management PC to be able to connect to all switches and the router, but does not want any other devices to connect to the management PC or the switches. The administrator would like to create a new VLAN 20 for management purposes.

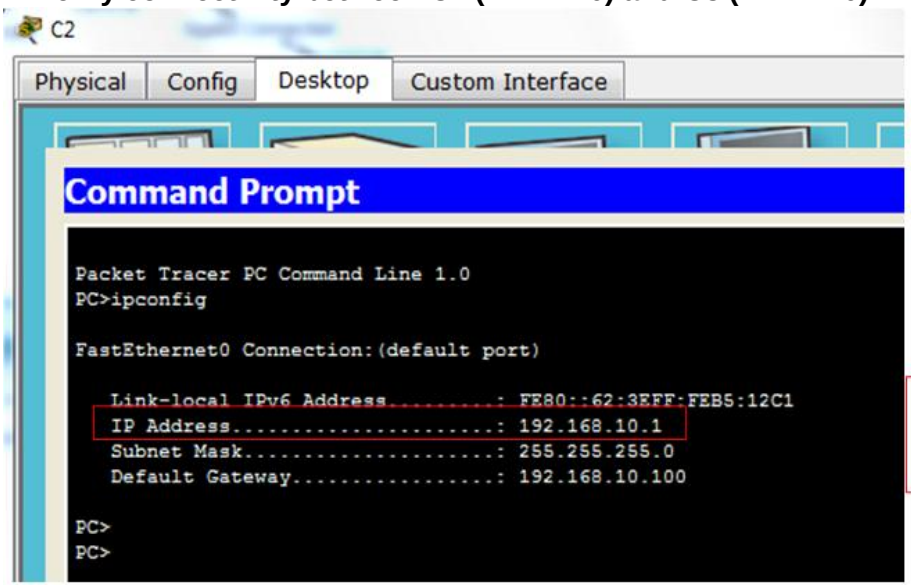
All devices have been preconfigured with:

- Enable secret password: **ciscoenpa55**
- Console password: **ciscoconpa55**
- VTY line password: **ciscovtypa55**

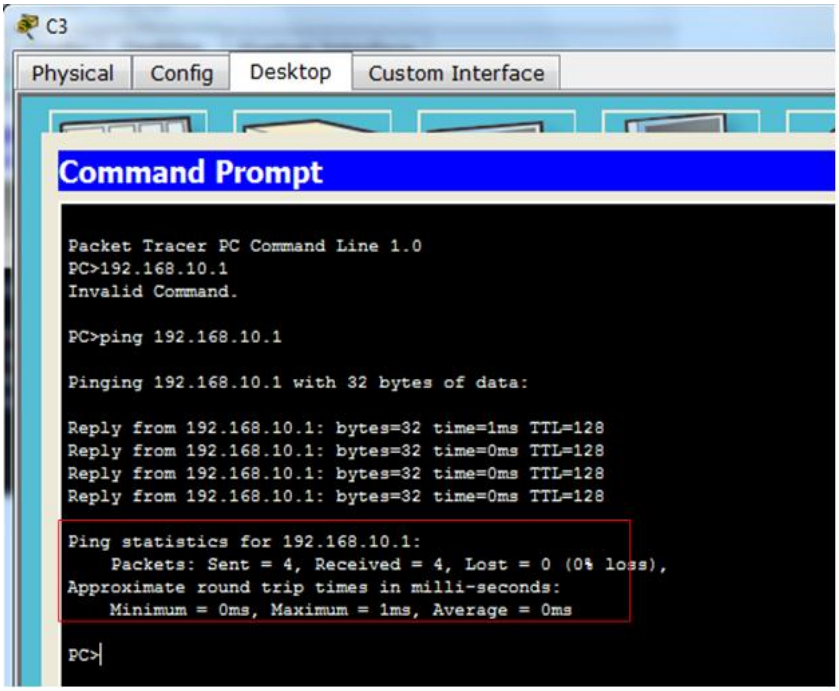
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Part 1: Verify Connectivity

Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).



Identificamos la ip de PC-PT C2

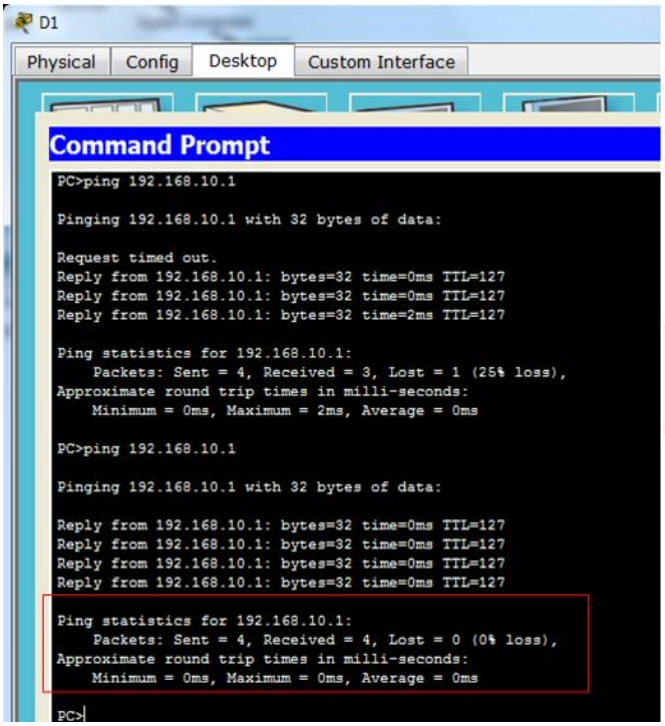


La conectividad se está dando fluidamente

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.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

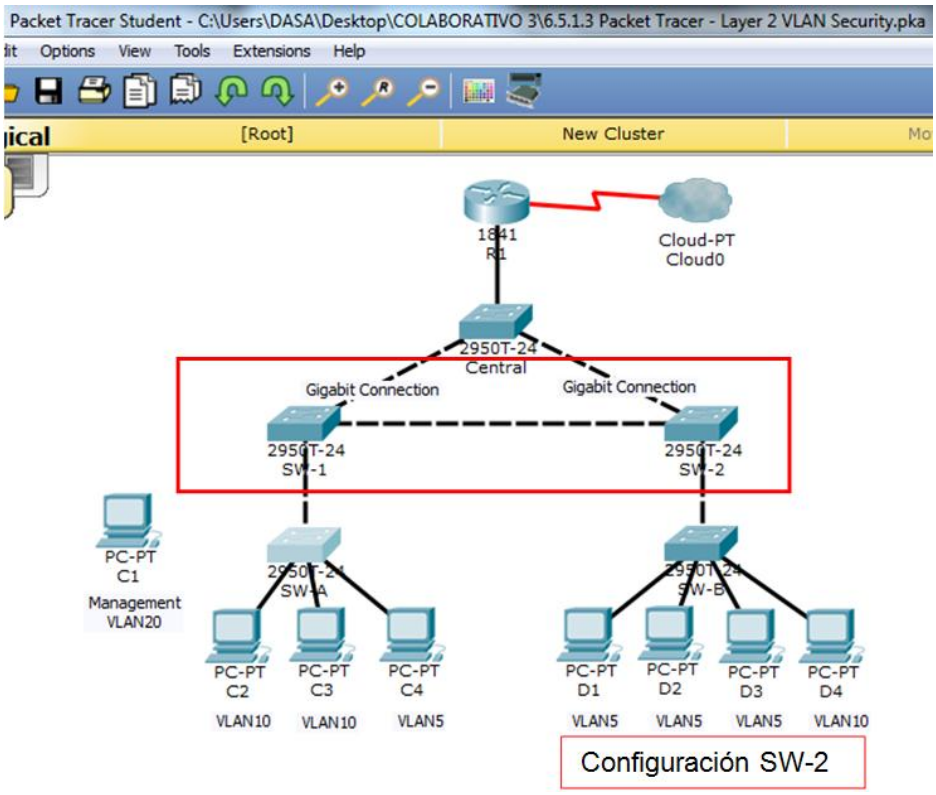


Existe conectividad entre los dos dispositivos

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**.



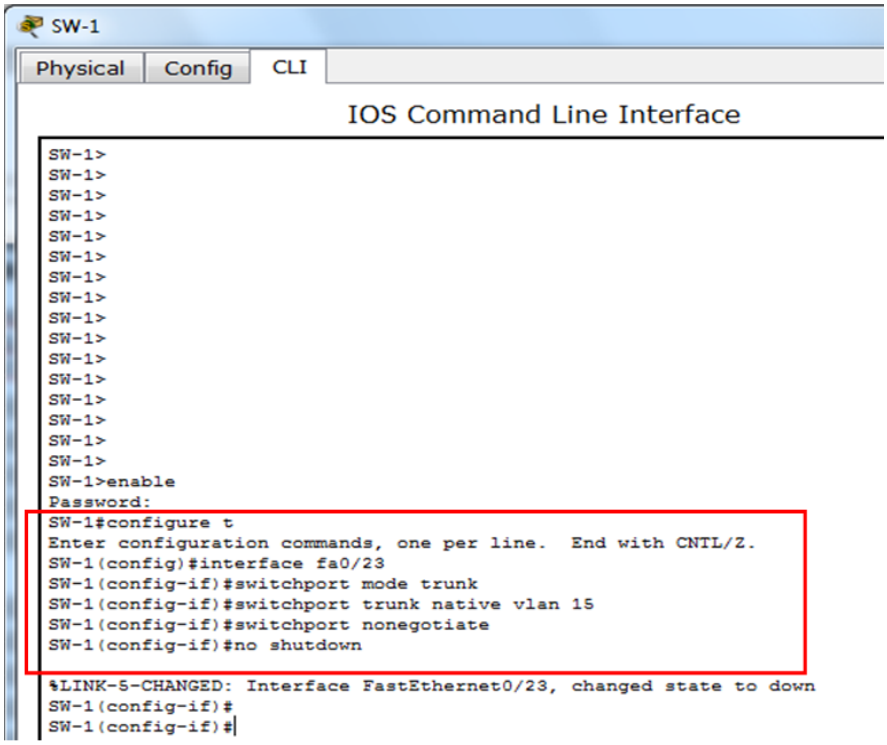
Configuración SW-2

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

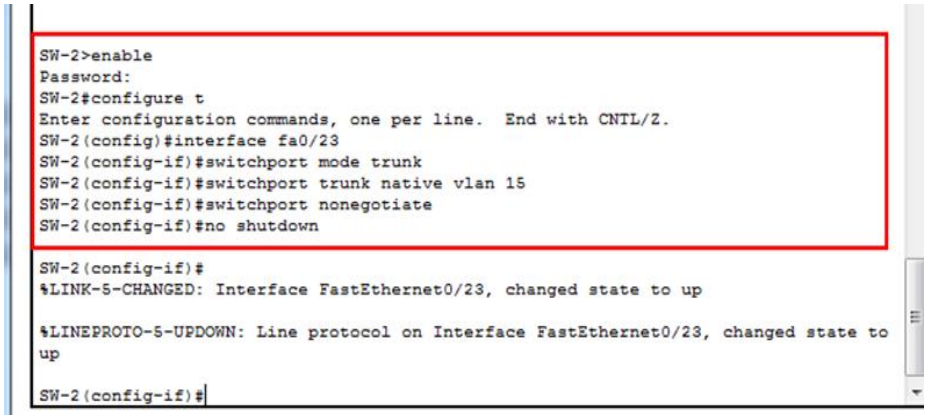
Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.

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
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

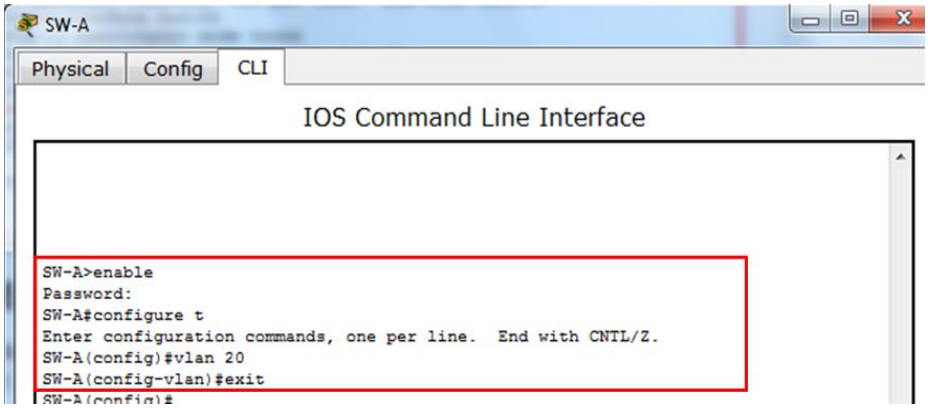
Part 3: Enable VLAN 20 as a Management VLAN

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.

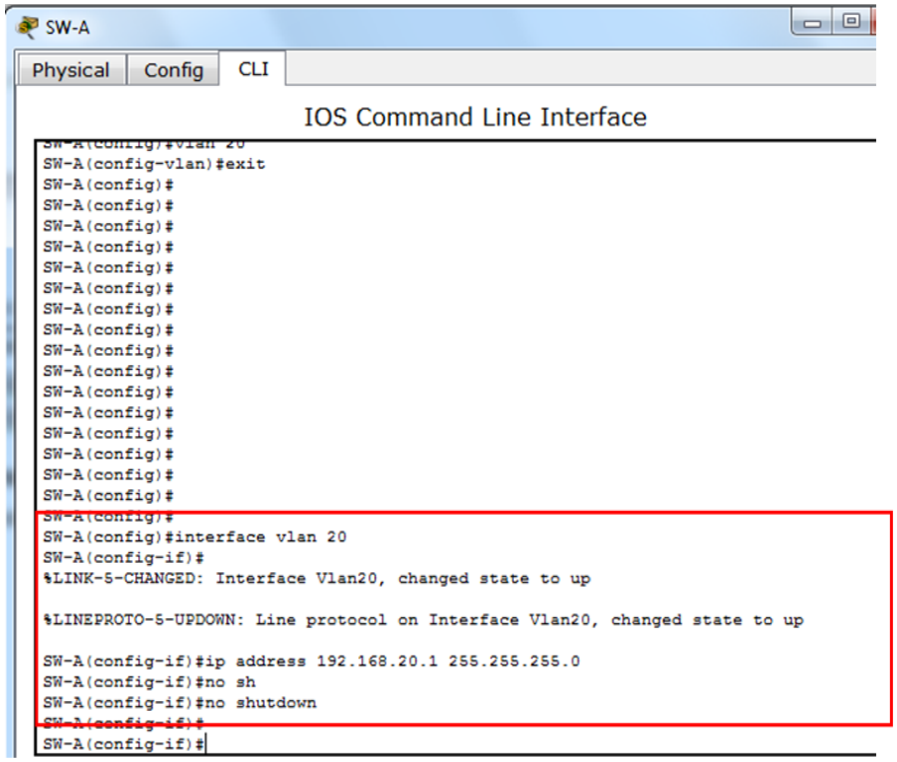
a. Enable VLAN 20 on **SW-A**.

```
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
```

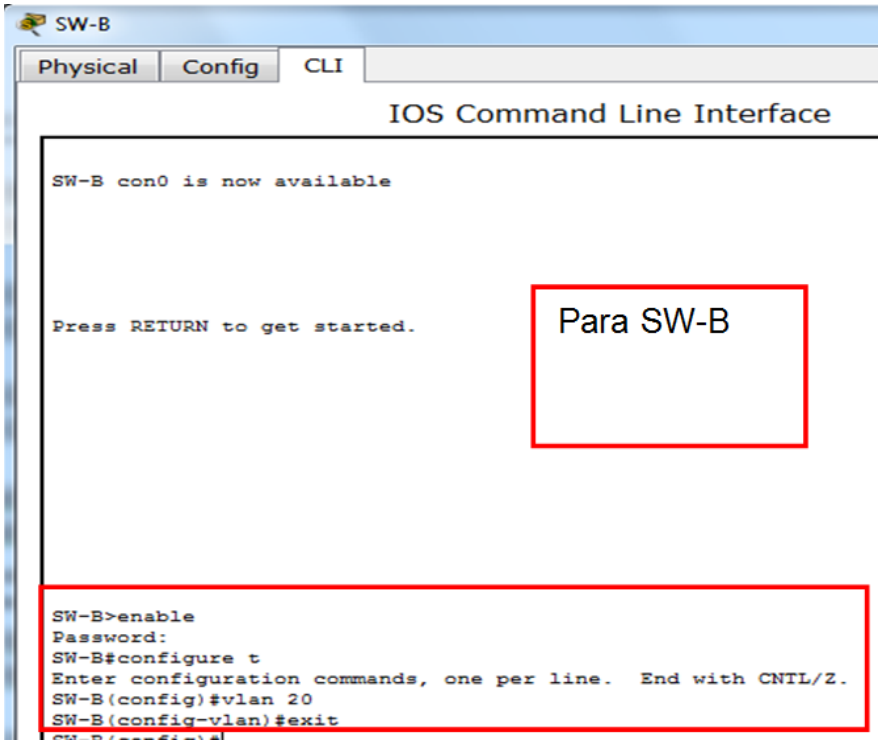


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

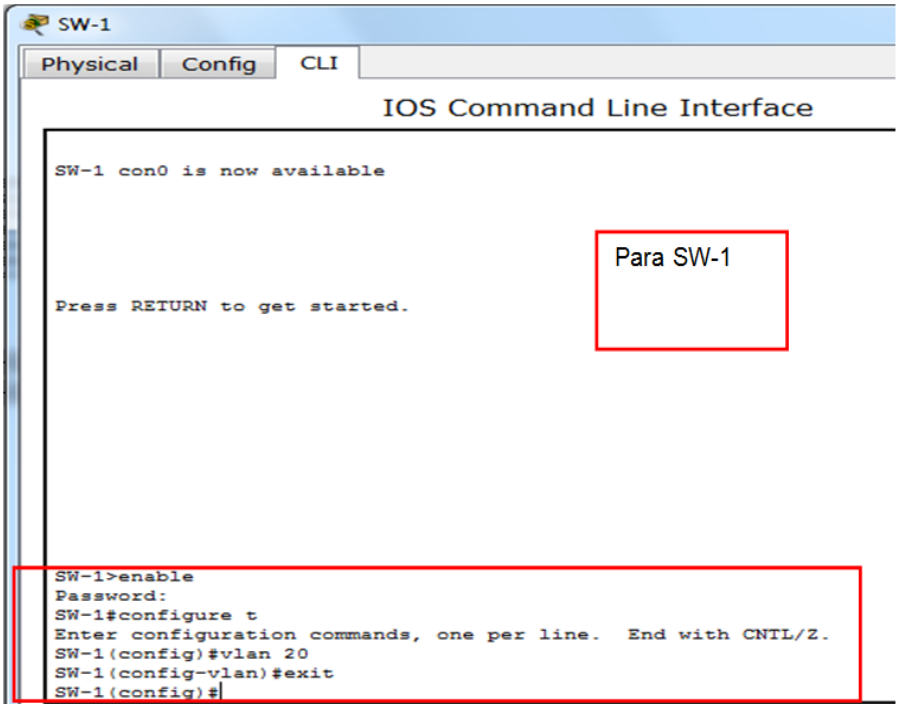
Step 2: Enable the same management VLAN on all other switches.

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
```

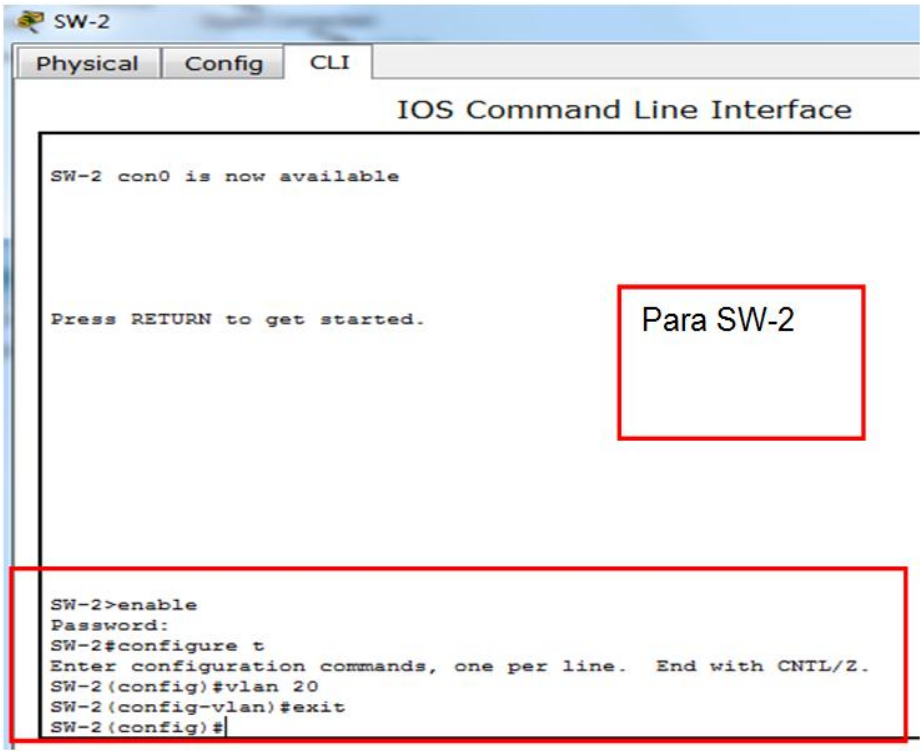



```
SW-1(config)# vlan 20
SW-1(config-vlan)# exit
```

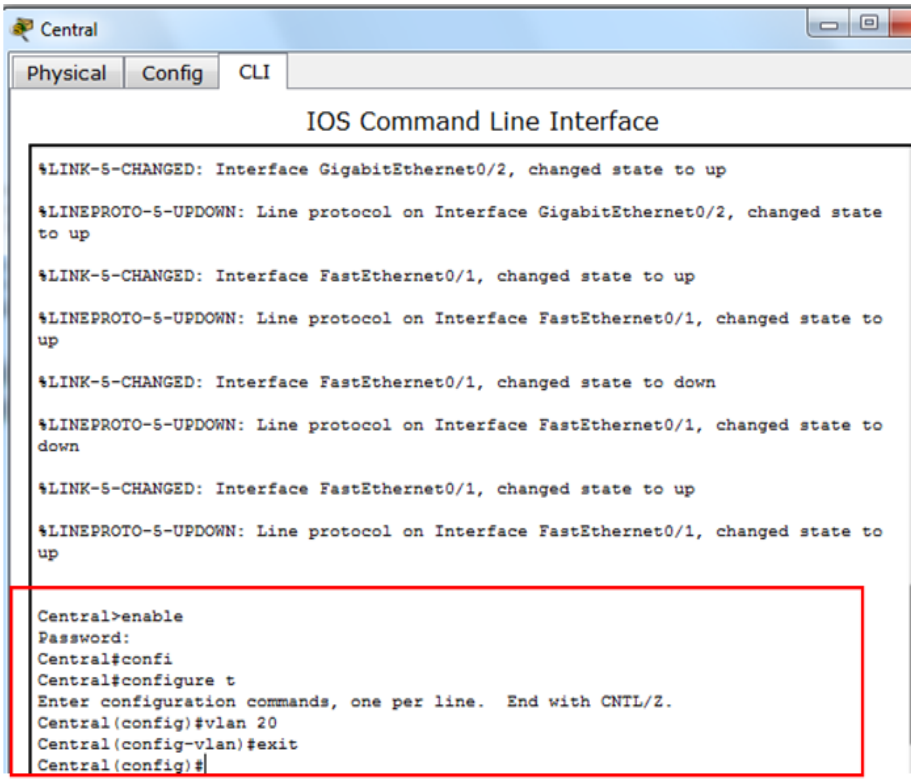


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
SW-2(config)# vlan 20
SW-2(config-vlan)# exit
```



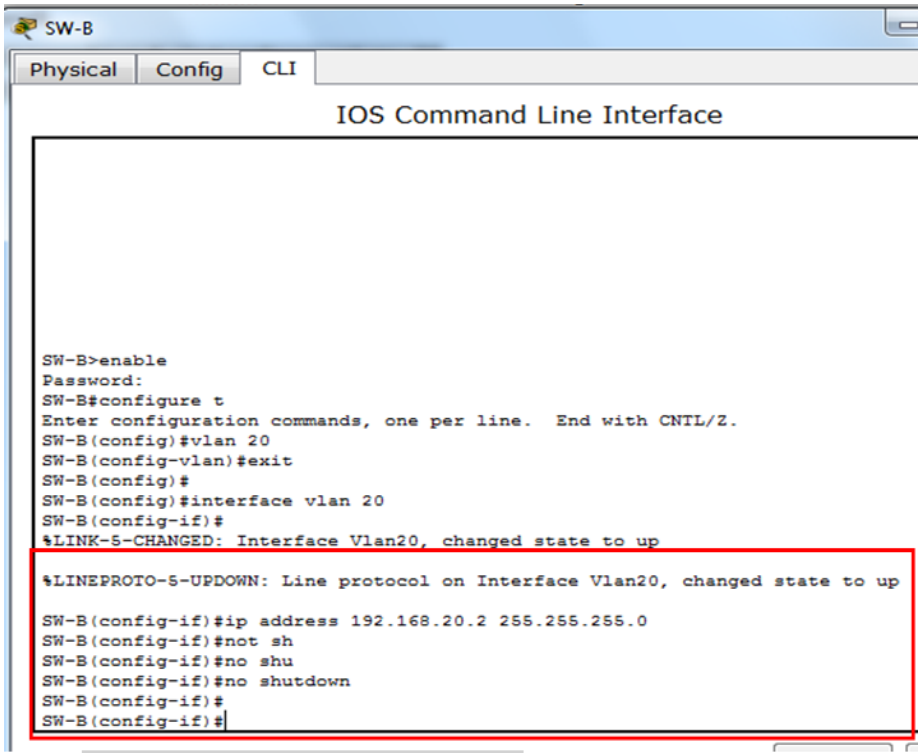

```
Central(config)# vlan 20
Central(config-vlan)# exit
```



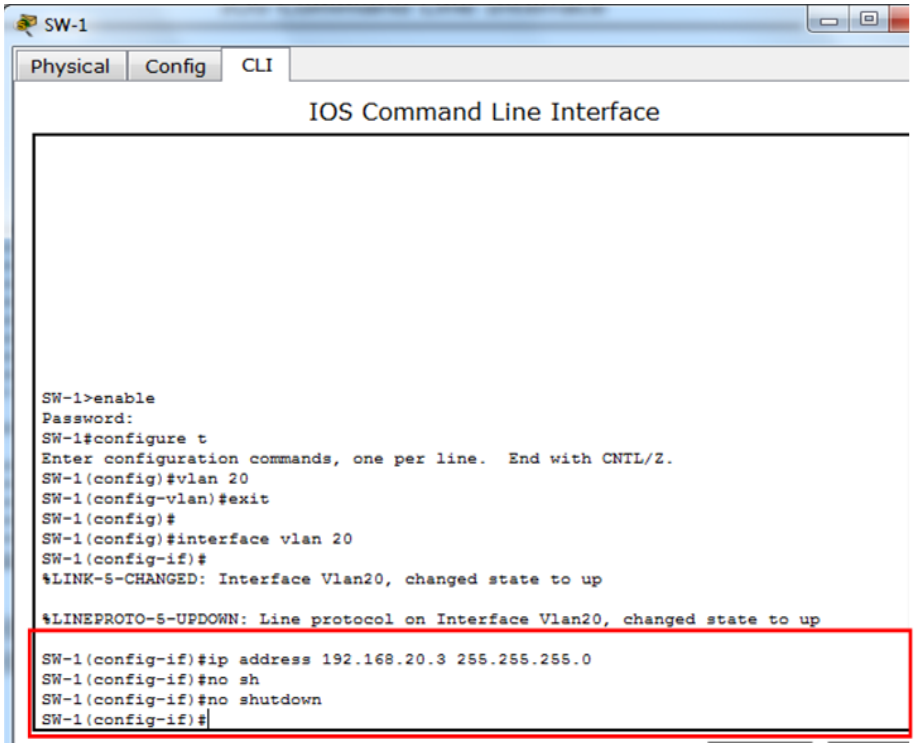
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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
```

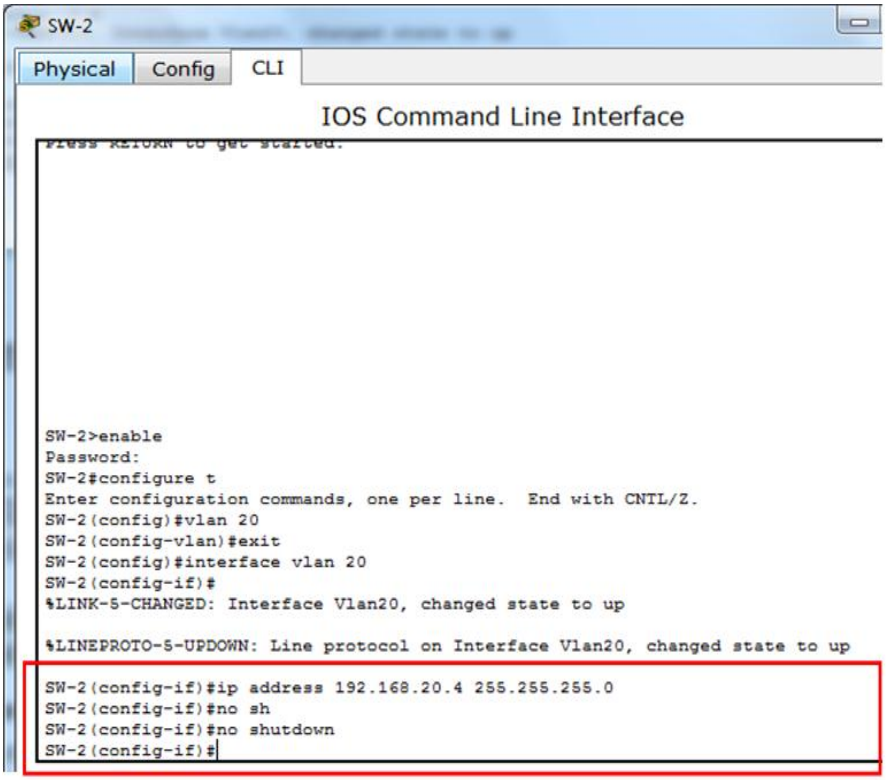



```
SW-1(config)# interface vlan 20
SW-1(config-if)# ip address 192.168.20.3 255.255.255.0
```

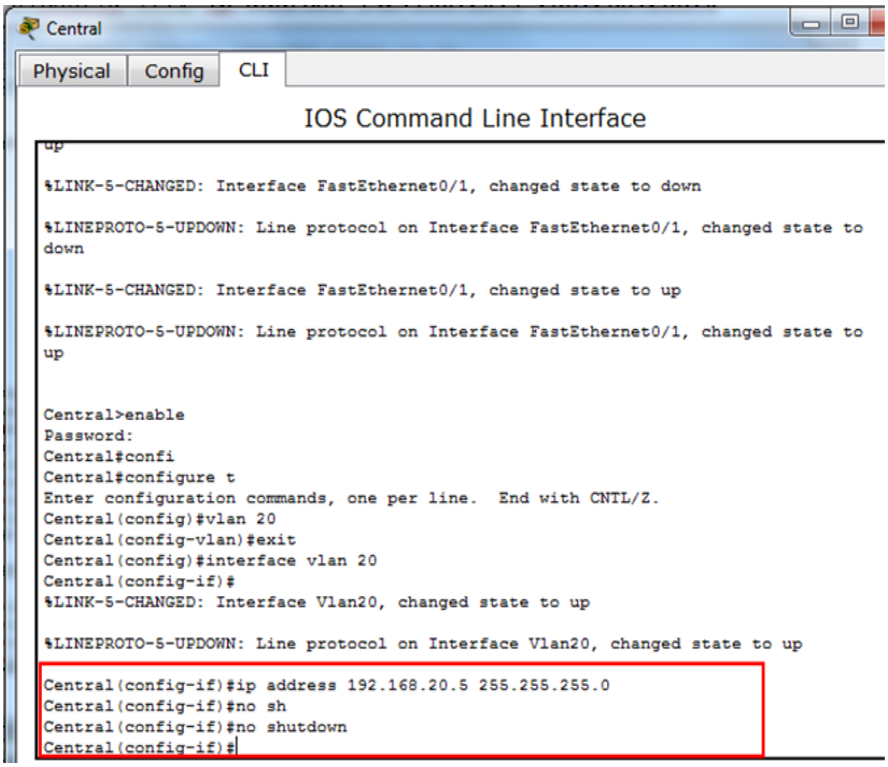


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

```
SW-2(config)# interface vlan 20
SW-2(config-if)# ip address 192.168.20.4 255.255.255.0
```



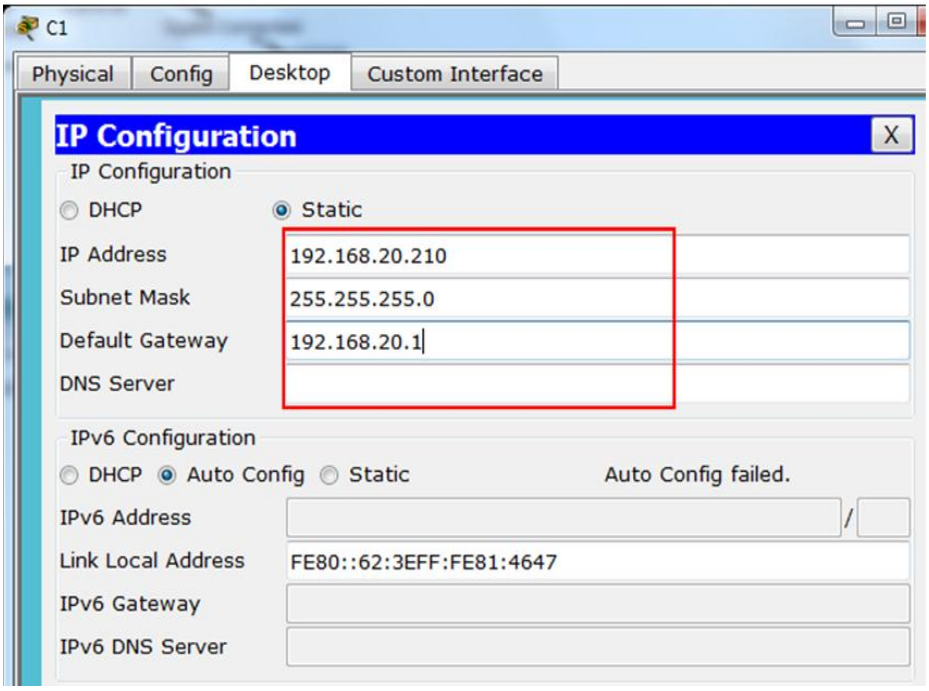

```
Central(config)# interface vlan 20
Central(config-if)# ip address 192.168.20.5 255.255.255.0
```

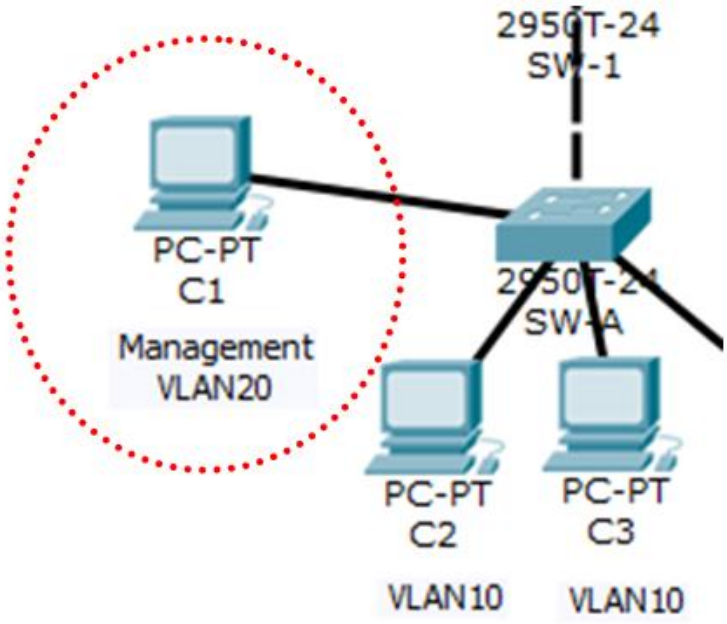


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.



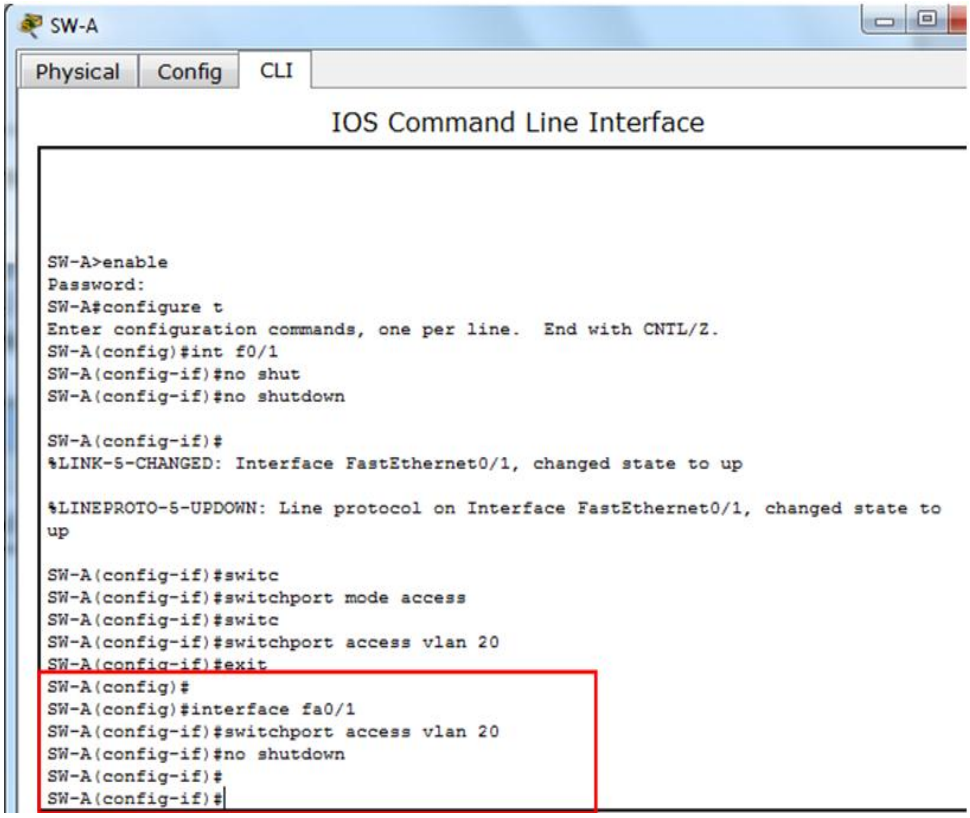


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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**.

Nota: Como se observó en la videoconferencia del día 19 de abril, existe un error en el archivo entregado para la práctica, ya que no establece conexión del management PC con los switches. Se realizó el ejercicio presente, sin poder entablar la comunicación en esta fase.

Part 4: Enable the Management PC to Access Router R1

Step 1: Enable a new subinterface on router R1.

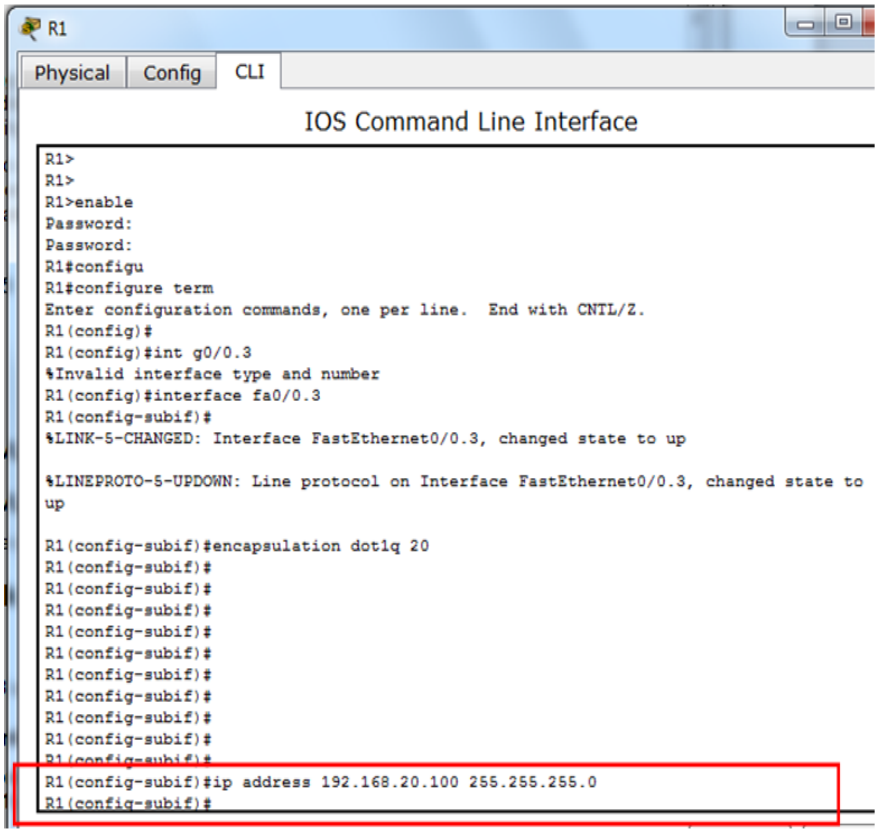
a. Create subinterface Fa0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20.

```
R1(config)# interface fa0/0.3
R1(config-subif)# encapsulation dot1q 20
```

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

b. Assign an IP address within the 192.168.20.0/24 network.

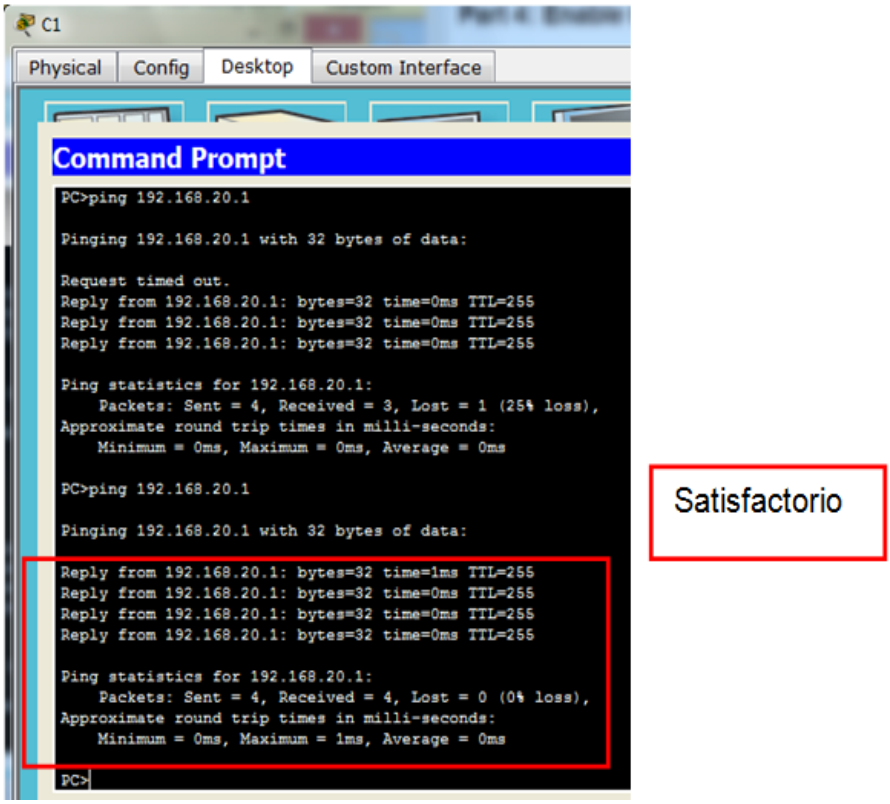
```
R1(config)# interface fa0/0.3
R1(config-subif)# ip address 192.168.20.100 255.255.255.0
```



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.



Satisfactorio

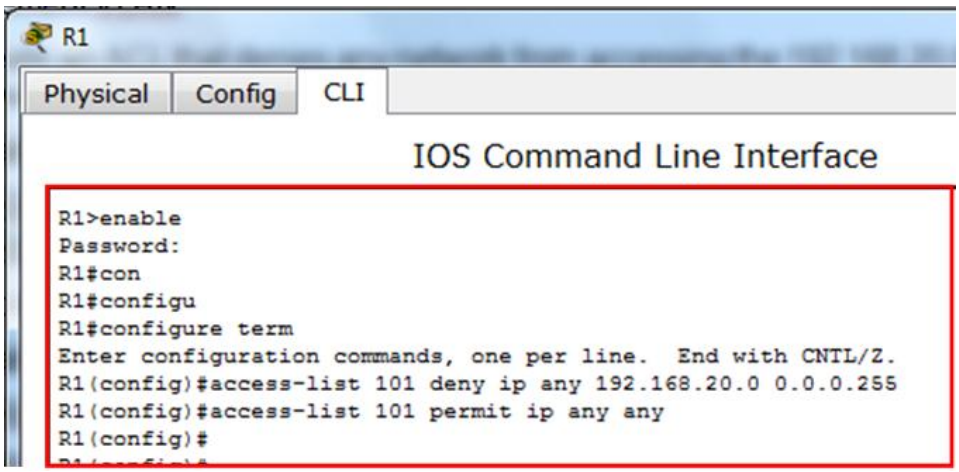
Step 3: Enable security.

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
```

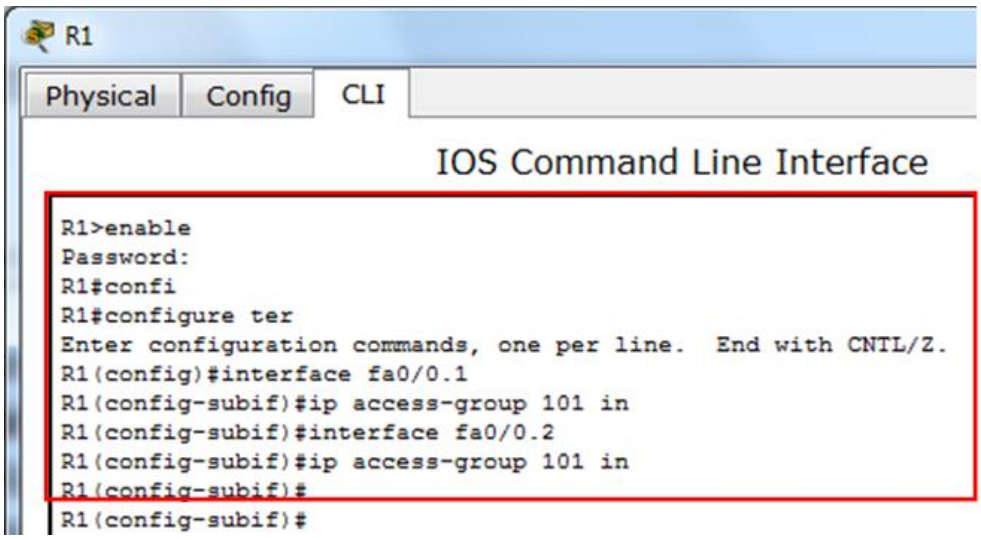


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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
```



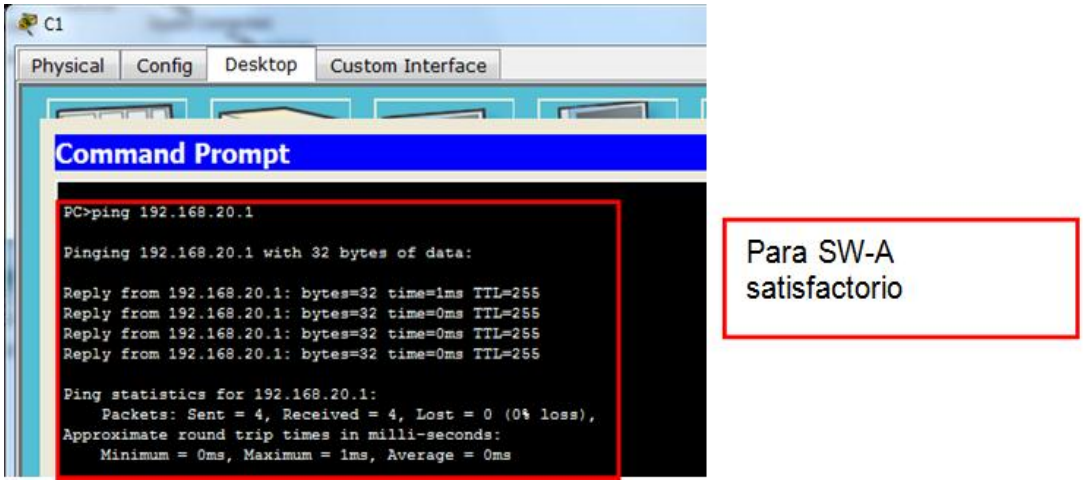
Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

Step 4: Verify security.

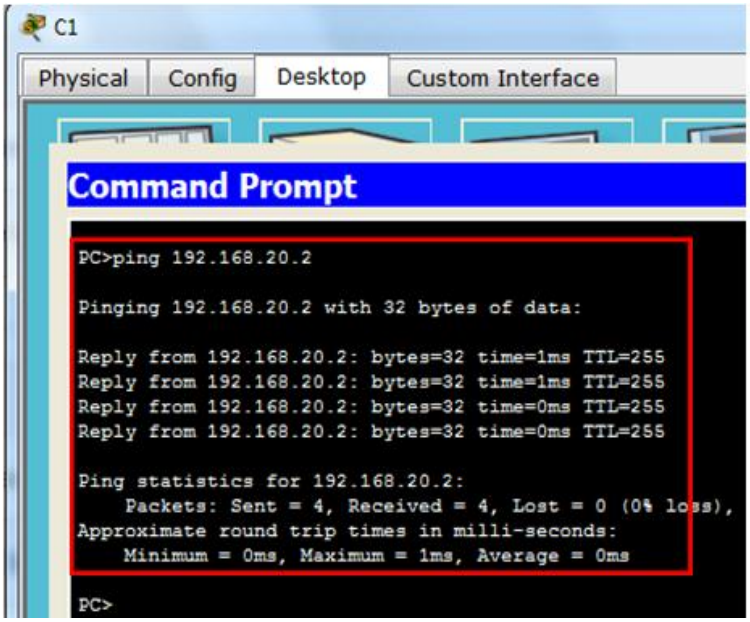
a. From the management PC, ping **SW-A**, **SW-B**, and **R1**. Were the pings successful? Explain.

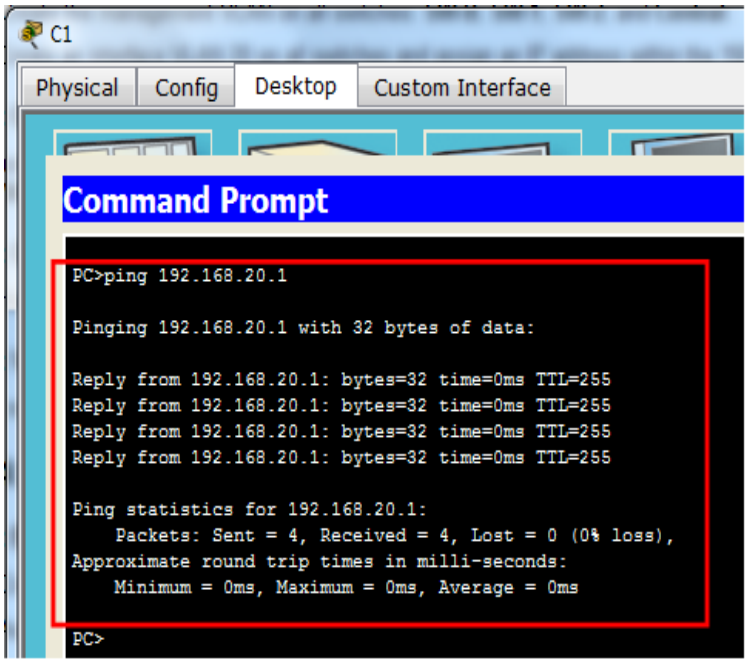
The pings should have been successful because all devices within the 192.168.20.0 network should be able to ping one another. Devices within VLAN20 are not required to route through the router.

Los pings deberían haber tenido éxito porque todos los dispositivos dentro de la red 192.168.20.0 deberían ser capaces de hacer ping uno al otro. Los dispositivos dentro de VLAN20 no son necesarios para la ruta a través del Router.



© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.



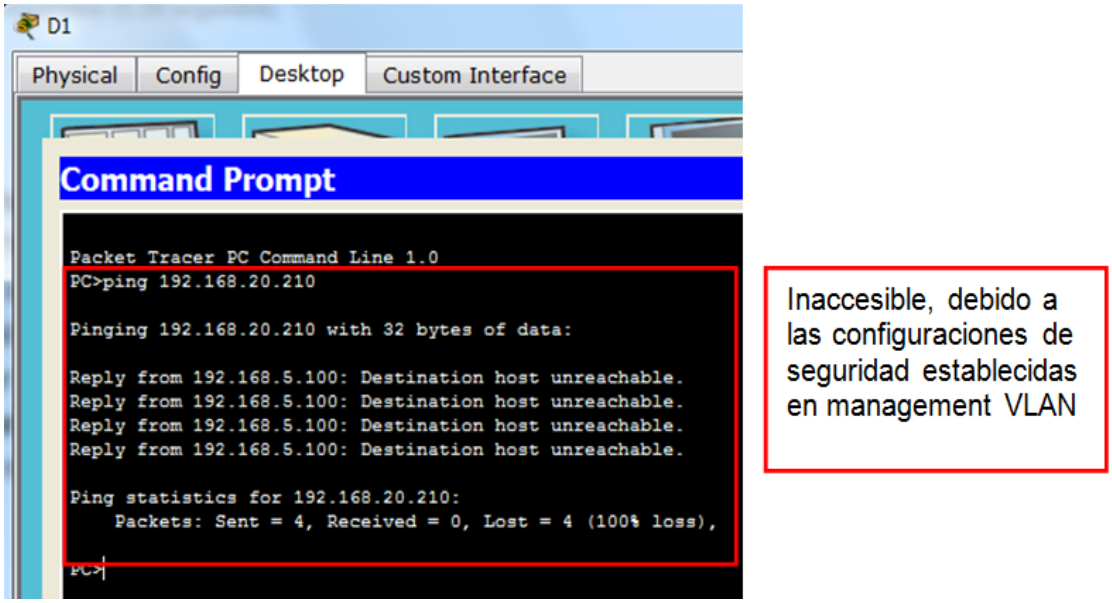


© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.

El ping debería haber fallado. Esto se debe a que para que un dispositivo dentro de una VLAN diferente pueda hacer ping exitosamente a un dispositivo dentro de VLAN20, debe ser enrutado. El router tiene una ACL que impide que todos los paquetes accedan a la red 192.168.20.0.

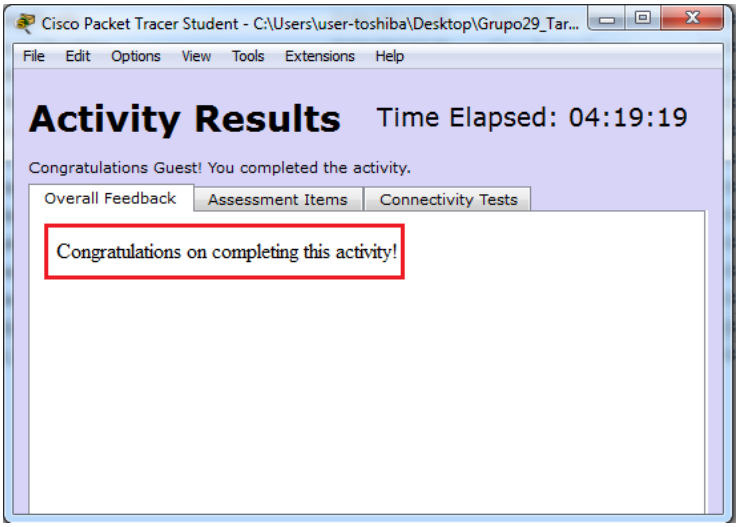


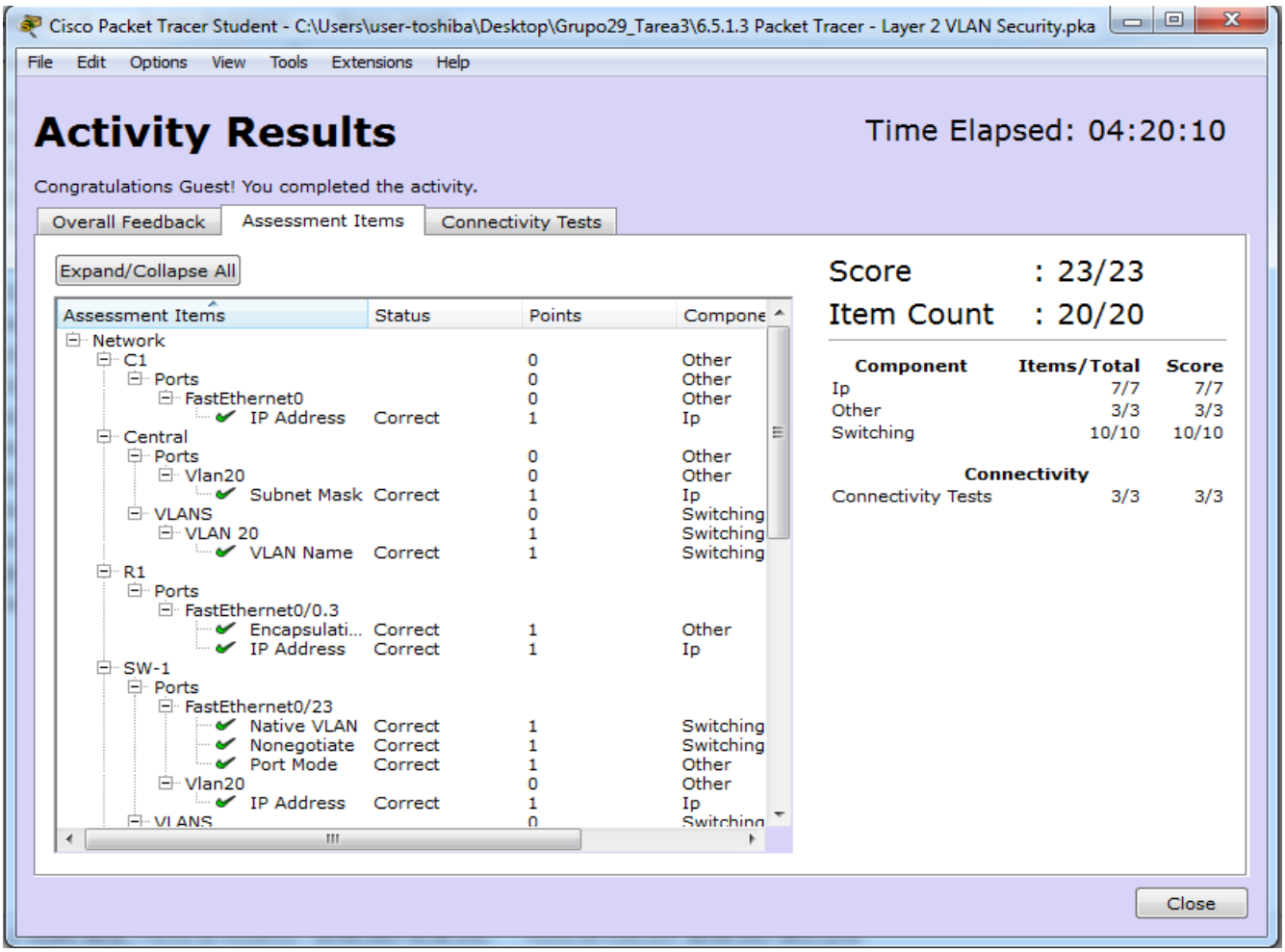
© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

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.





© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones informe 17

- Conectamos un enlace redundante entre SW-1 y SW-2, a continuación habilitamos trunking y configuramos la seguridad en el nuevo enlace troncal.
- Creamos una nueva VLAN de administración (VLAN 20) y conectamos una PC de administración a esa VLAN.
- Se implementó una ACL para evitar que usuarios externos accedan a la VLAN de administración.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Conclusiones

- Se fortalecio los conocimientos necesarios para el diseño de redes escalables mediante el uso del modelo jerárquico de tres niveles, con el fin de optimizar el rendimiento de la red e incorporar de manera adecuada el uso de tecnologías y protocolos de conmutación mejorados tales como: VLAN, Protocolo de enlace troncal de VLAN (VTP), Protocolo rápido de árbol de expansión (Rapid Spanning Tree Protocol - RSTP), Protocolo de árbol de expansión por VLAN (Spanning Tree per VLAN - PVSTP) y encpasulamiento por 802.1q.
- Configuramos, verificamos y resolvimos problemas de las VLAN, enlaces troncales de los switches Cisco, el enrutamiento entre VLAN, VTP y RSTP.
- Comprendimos la necesidad de establecer modelos de arquitecturas de comunicación estratificadas por niveles.
- Describimos tecnologías de conmutación mejoradas tales soportadas en el uso de VLANs y el Protocolo Spanning Tree.
- Se diseñó y configuro soluciones soportadas en el uso de dispositivos de conmutación acorde con las topologías de red requeridas bajo el uso de protocolos basados en STP y VLANs bajo una arquitectura jerárquica.
- Desarrollamos la capacidad de configurar y administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación, mediante el estudio del modelo OSI, la arquitectura TCP/IP, y el uso de recursos y herramientas en función de los protocolos y servicios de la capa física como soporte de las comunicaciones a través de las redes de datos estableciendo alternativas a problemas de interconectividad.
- Establecimos niveles de seguridad básicos, mediante la definición de criterios y políticas de seguridad aplicadas a diversos escenarios de red, bajo el uso de estrategias hardware y software, con el fin de proteger la integridad de la información frente a cualquier tipo de ataque que se pueda presentar en un instante de tiempo determinado; en especial en soluciones de red que involucren el uso de aplicaciones cliente-servidor.
- Desarrollamos la capacidad de configurar y verificar operaciones básicas de enrutamiento de Gateway interior mediante el uso de comandos específicos del IOS con el fin identificar y resolver problemas de conectividad y actualización de tablas de enrutamiento.
- Se utilizó herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento, evaluando el comportamiento de enrutadores, mediante el uso de comandos de administración de tablas de enrutamiento, bajo el uso de protocolos de vector distancia y estado enlace.
- Configuramos esquemas de conmutación soportadas en Switches, mediante el uso de protocolos basados en STP y VLANs en escenarios corporativos y residenciales, con el fin de comprender el modo de operación de las VLAN y la bondades de administrar dominios de broadcast independientes, en escenarios soportados a nivel de capa 2 al interior de una red jerárquica convergente.

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.

Bibliografía

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

UNAD (2014). Configuración de Switches y Routers [OVA]. Recuperado de: https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

Amberg, E. (2014). CCNA 1 Powertraining : ICND1/CCENT (100-101). Heidleberg: MITP. Recuperado de: http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=979032&lang=es&site=ehost-live

Lammle, T. (2008). Todd Lammle's CCNA IOS Commands Survival Guide. Indianapolis, Ind: Sybex. Recuperado de: http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=218603&lang=es&site=ehost-live

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de: http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de: http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de: http://gonda.nic.in/swangonda/pdf/ccna1.pdf

© 2014 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información pública de Cisco.