Diplomado de profundización CISCO

(Configuración de Sistemas de red soportados en VLANs)

Grupo: 203092-41

Actividad colaborativa: Unidad 3

Presentado por:

Astrid Manosalba Cañizarez

Jorge Humberto Lopez Aguirre

Nancy Liliana Satoba

Nubia Jesus Hernandez

Edison Correa Gómez

Tutor:

Juan Carlos Vesga

Universidad Nacional Abierta y a Distancia (UNAD)

30 / Abril / 2017

TABLA DE CONTENIDO

CAPITULOS **PÁGINAS**

INTRODUCCION

En este trabajo la función principal es desarrollar temas relacionados con las LAN virtuales (VLANs) que son las que se han colocado como una de las soluciones tecnológicas incorporadas en los equipos para redes conmutadas.

La tecnología de VLAN, es una manera económica y eficiente de agrupar usuarios de la red en grupos de trabajo virtuales, sin importar su ubicación física en la red y proporciona reducción de costos de administración, brinda seguridad de grupo de trabajo y de red y controla la actividad de broadcast.

En ello se trata principalmente la actividad de familiarizarse con los conceptos teóricos y practicos del curso sobre el funcionamiento de las redes a travez de switching y routing.

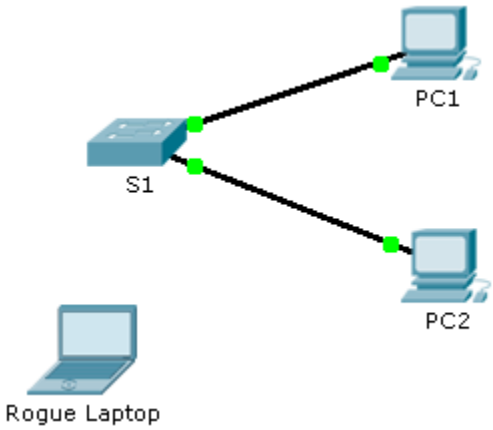
OBJETIVOS

- ✓ Aumentar los conocimientos en la configuración de switches Cisco.
- ✓ Desarrollar una serie de ejercicios para explicar paso a paso el proceso de configuración.
- ✓ Apoyar el aprendizaje a través de la descripción del proceso de configuración de redes de área local virtuales (VLANs) en switches Cisco.
- ✓ Configurar redes pequeñas y medianas utilizando el simulador, y tener las competencias necesarias para configurar y resolver fallos de equipos de Red.

Informe No. 1 (VLANS)

2.2.4.9. Packet Tracer - Configuring Switch Port Security

Topology



Addressing Table

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

Objective

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

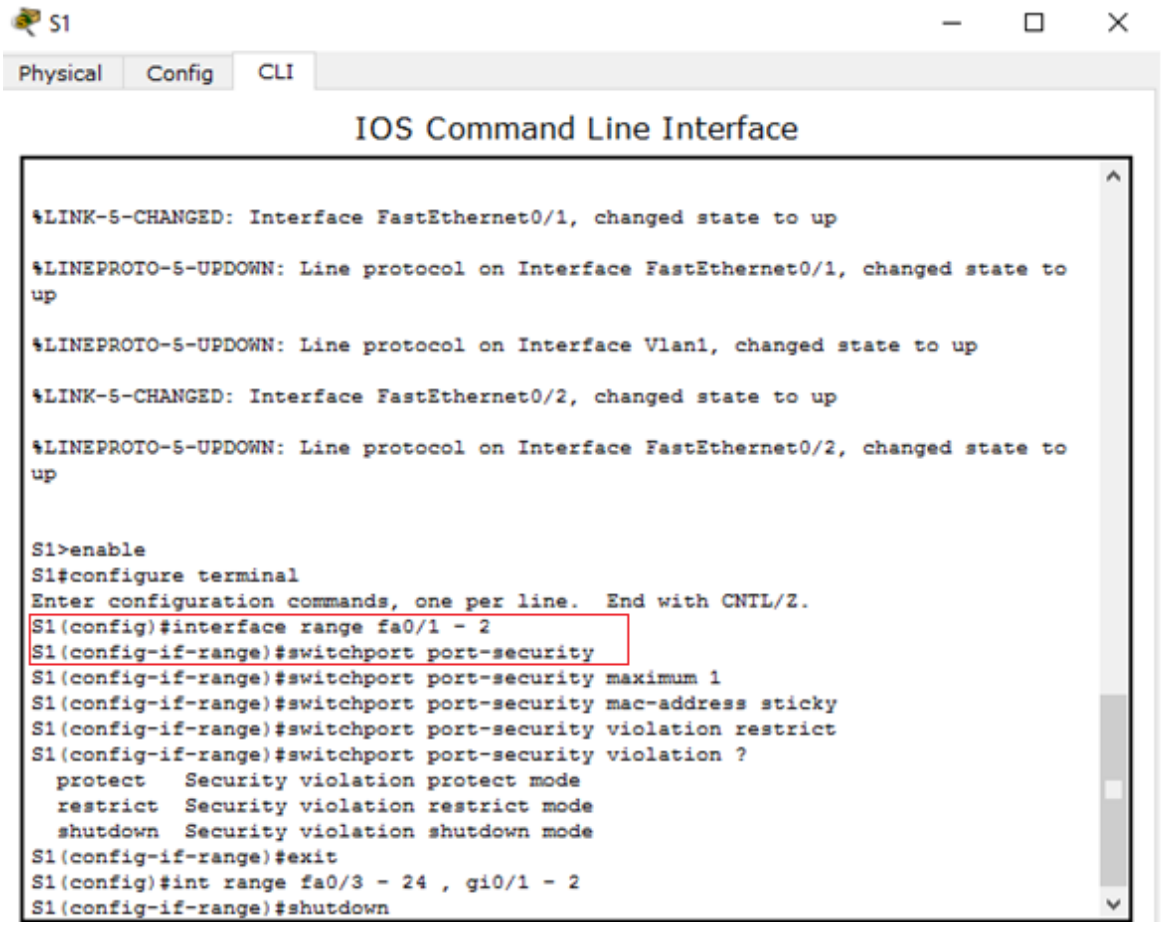
Background

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

Part 1: Configure Port Security

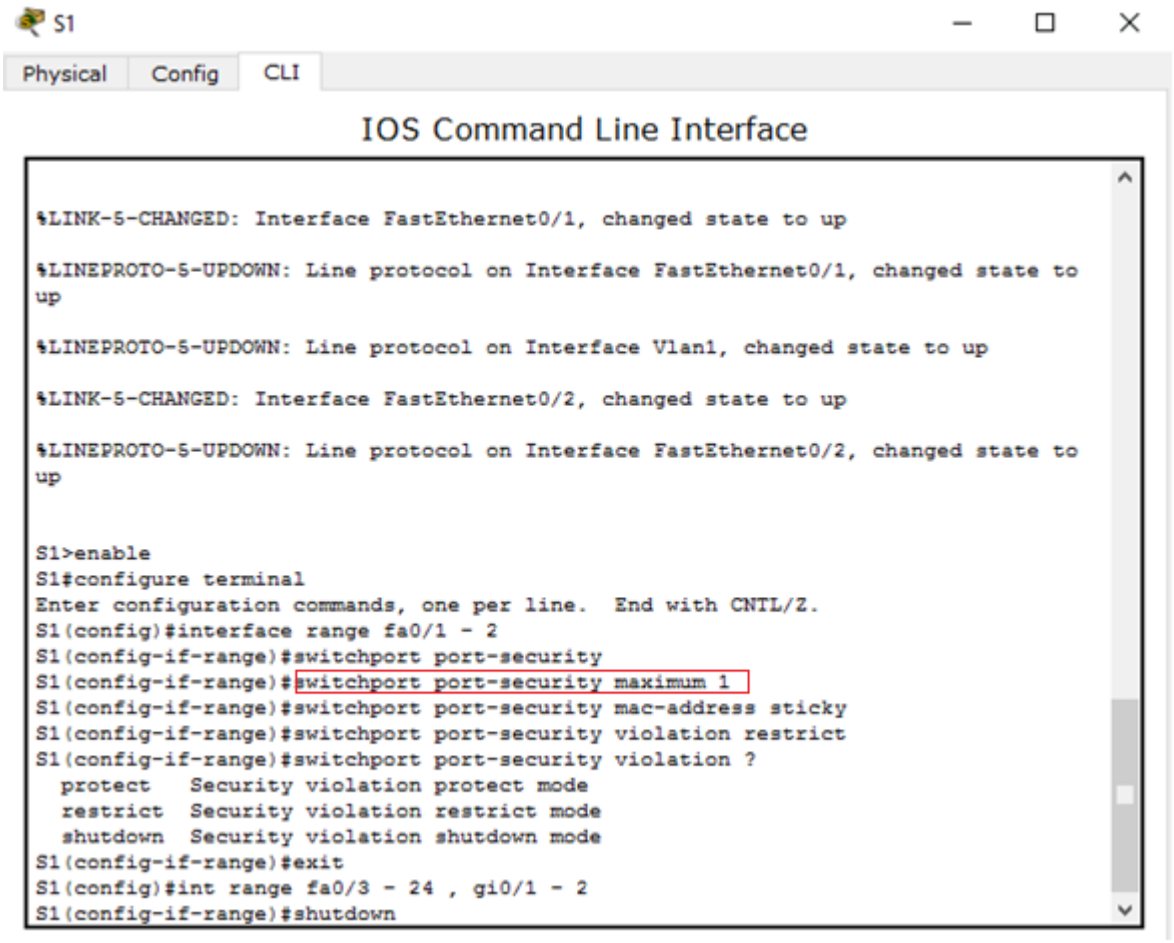
a. Access the command line for S1 and enable port security on Fast Ethernet ports 0/1 and 0/2.

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



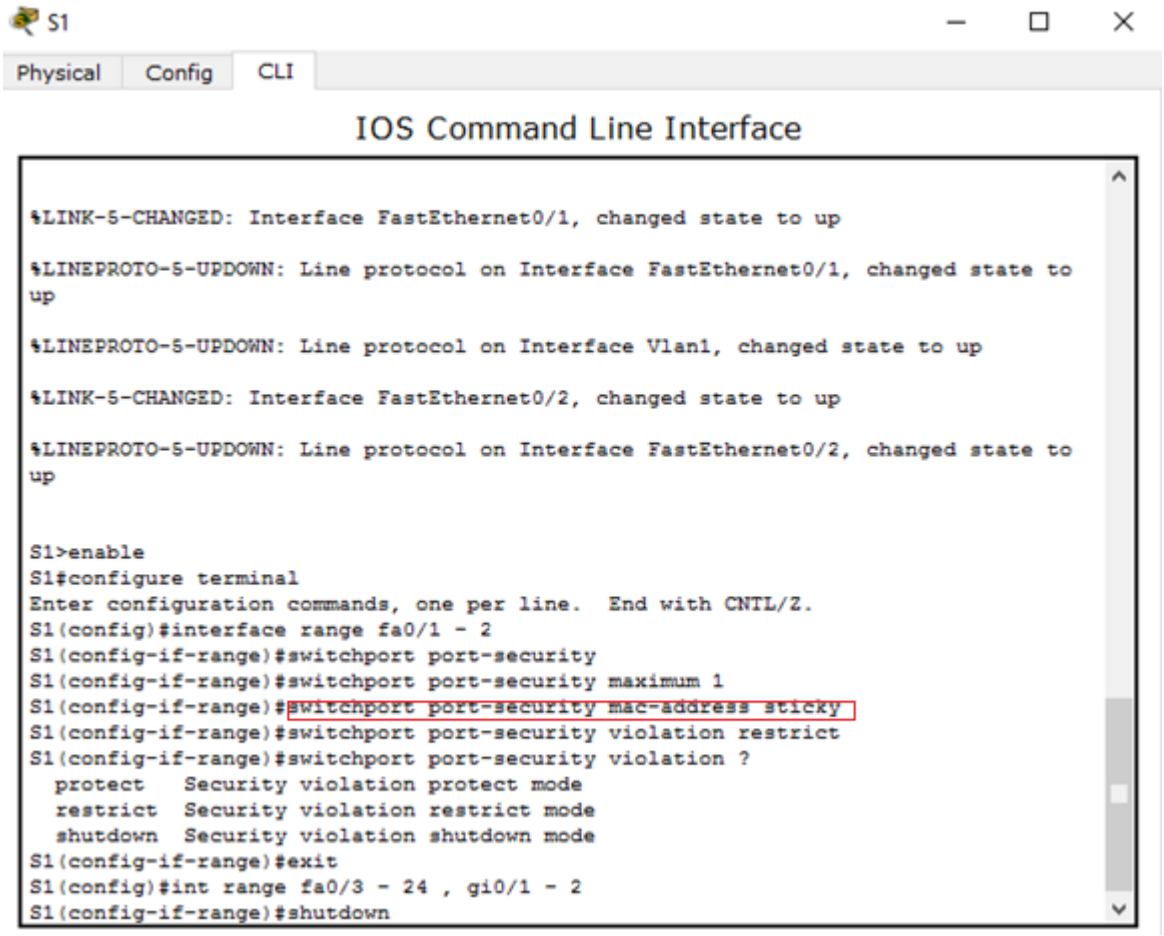
b. Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

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



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

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



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

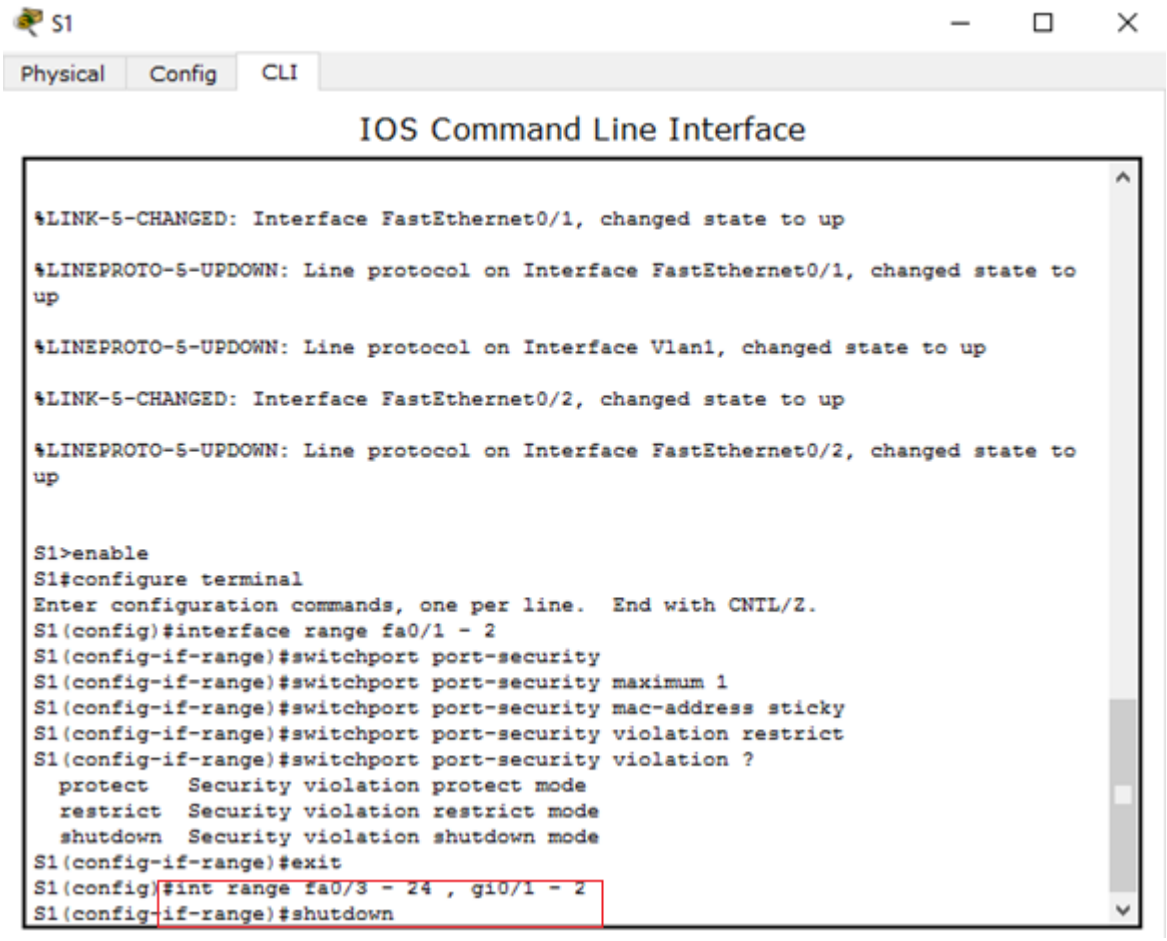
S1(config-if-range)# switchport port-security violation restrict

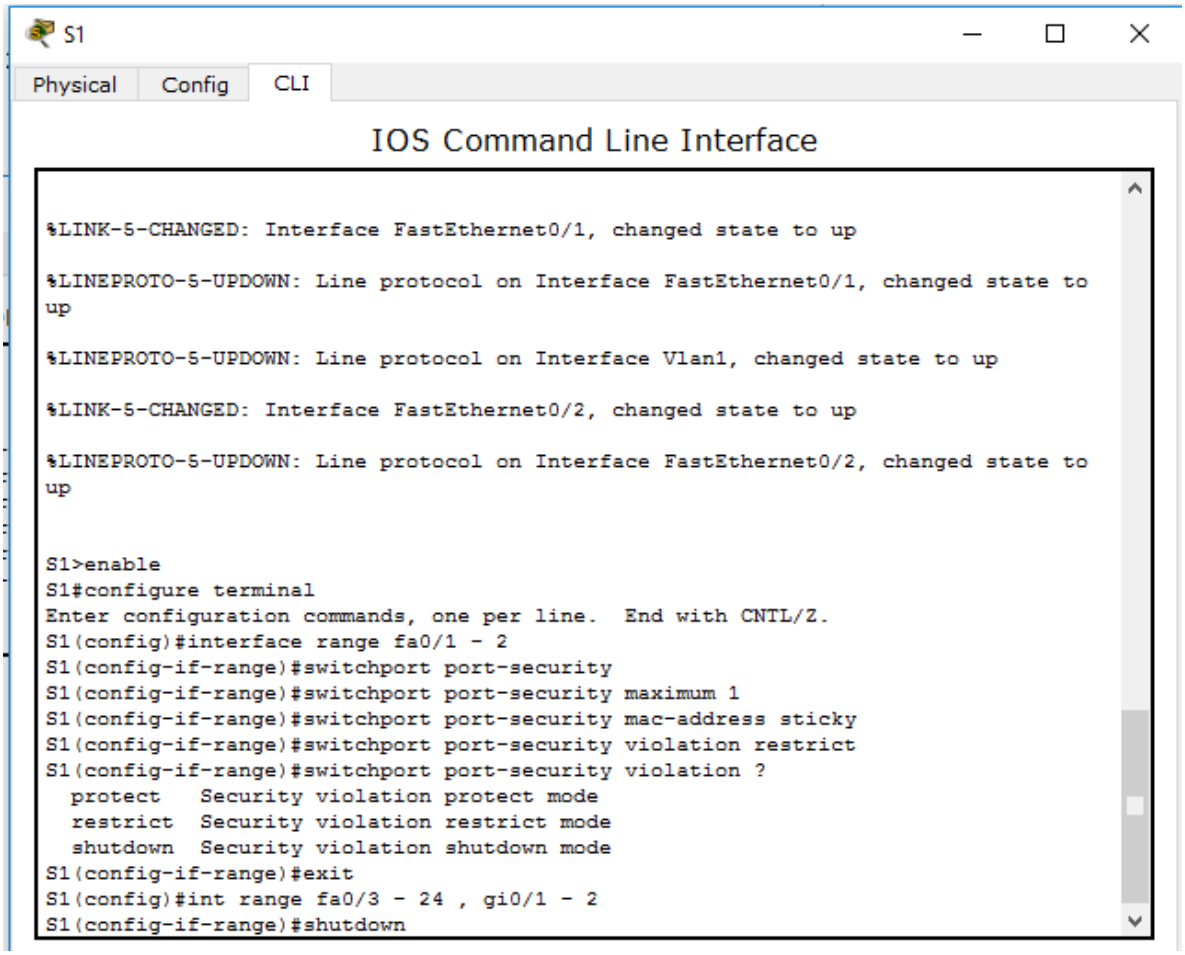
```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

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

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to
up


S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range fa0/1 - 2
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation restrict
S1(config-if-range)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
S1(config-if-range)#exit
S1(config)#int range fa0/3 - 24 , gi0/1 - 2
S1(config-if-range)#shutdown
```

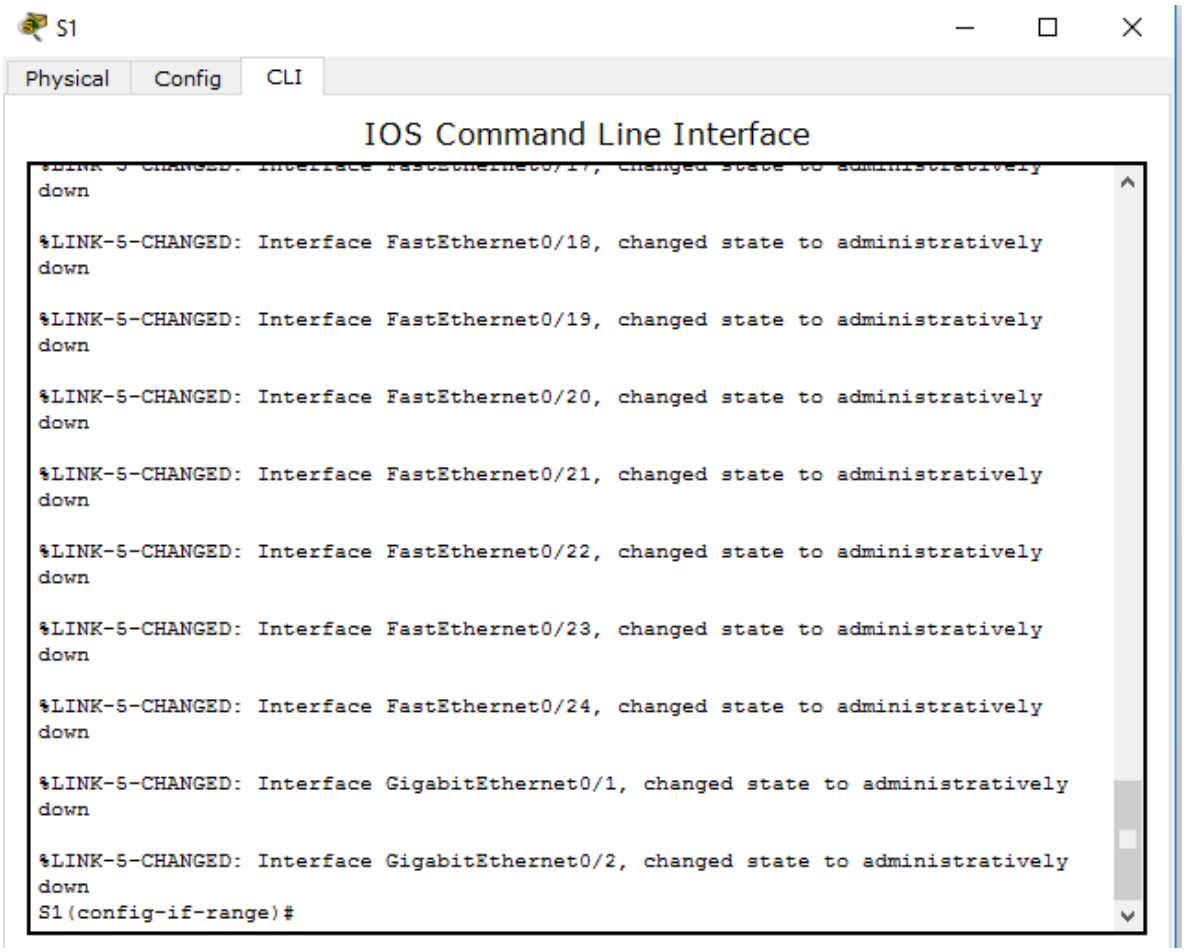
e. Disable all the remaining unused ports. Hint: Use the range keyword to apply this configuration to all the ports simultaneously.

S1(config-if-range)# interface range fa0/3 - 24 , gi1/1 - 2

S1(config-if-range)# shutdown


S1
Physical
Config
CLI
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
S1>enable
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range fa0/1 - 2
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation restrict
S1(config-if-range)#switchport port-security violation ?
protect Security violation protect mode
restrict Security violation restrict mode
shutdown Security violation shutdown mode
S1(config-if-range)#exit
S1(config)#int range fa0/3 - 24 , gi0/1 - 2
S1(config-if-range)#shutdown

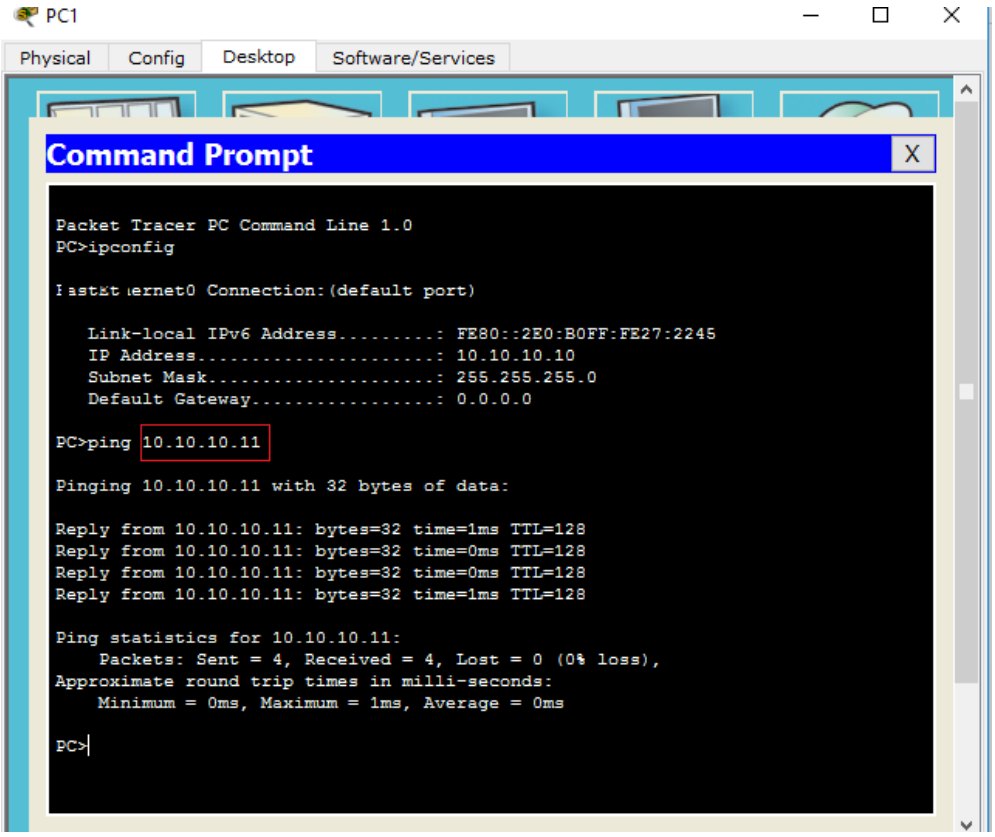

S1
Physical
Config
CLI
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
S1>enable
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range fa0/1 - 2
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation restrict
S1(config-if-range)#switchport port-security violation ?
protect Security violation protect mode
restrict Security violation restrict mode
shutdown Security violation shutdown mode
S1(config-if-range)#exit
S1(config)#int range fa0/3 - 24 , gi0/1 - 2
S1(config-if-range)#shutdown



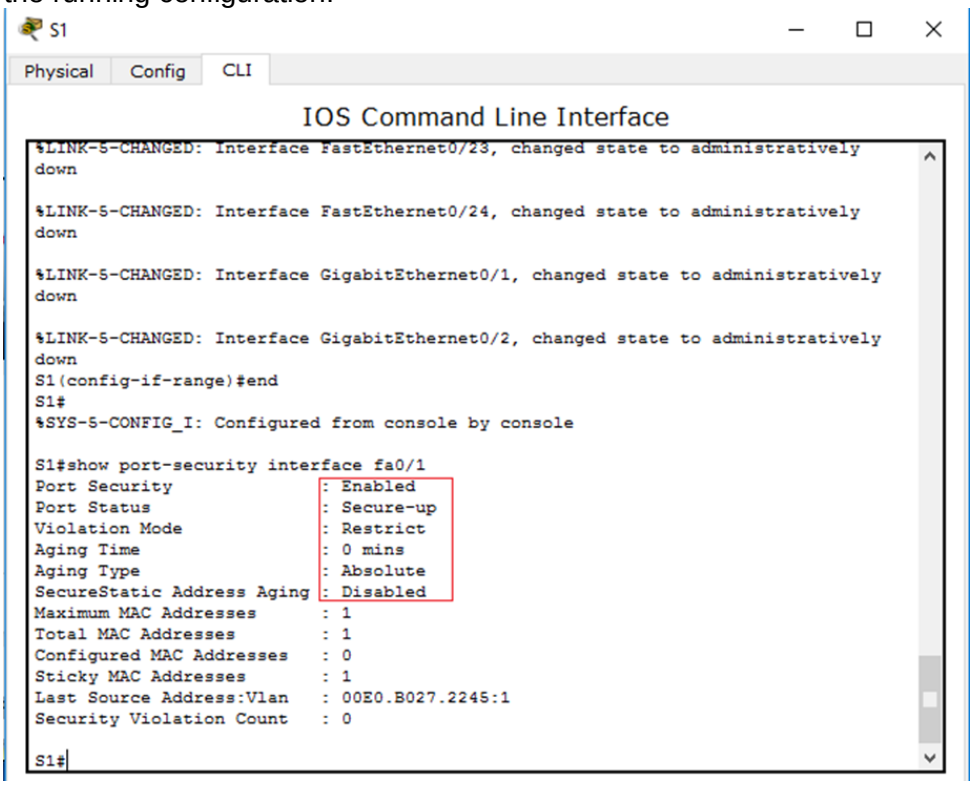

```
S1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down

 --More--
```

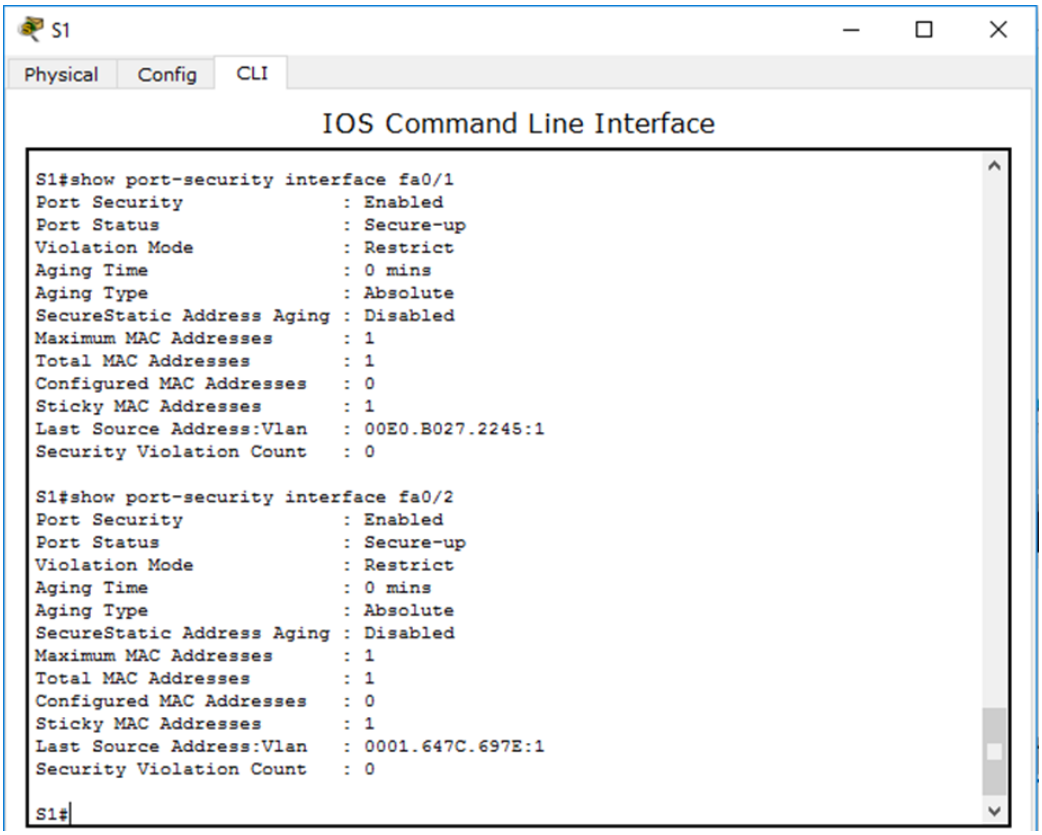
Part 2: Verify Port Security

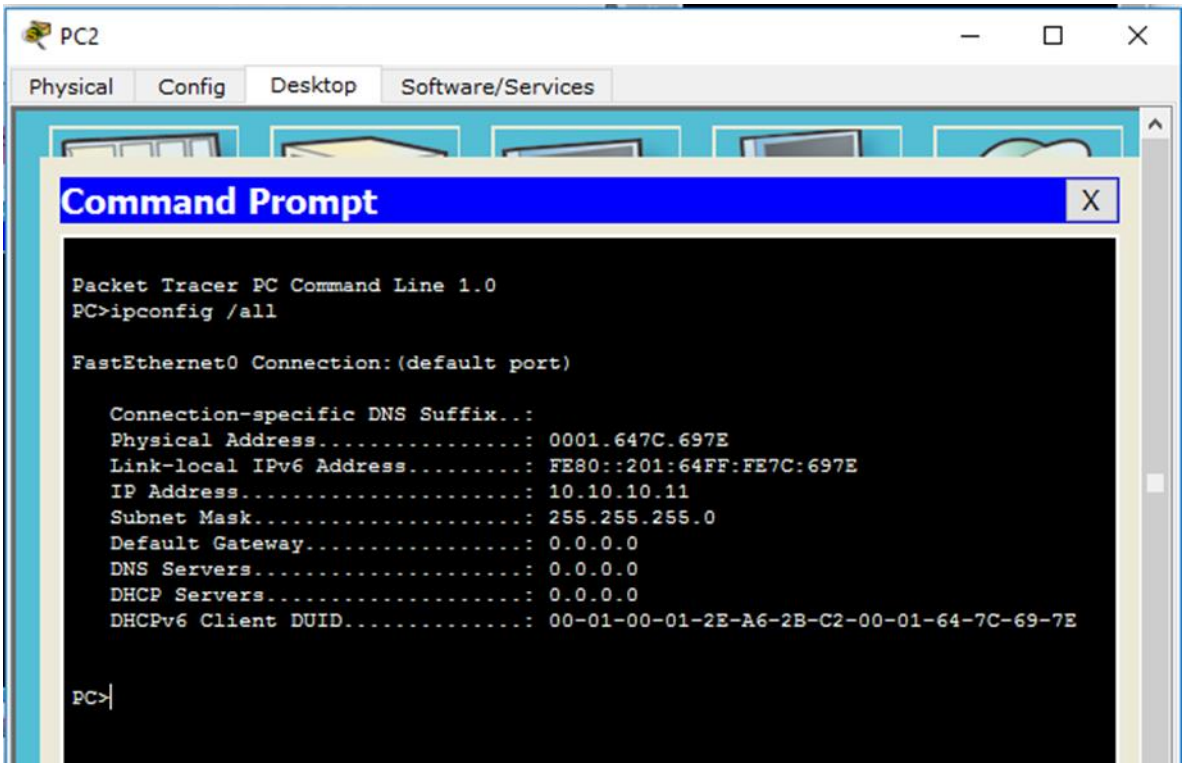
a. From PC1, ping PC2.



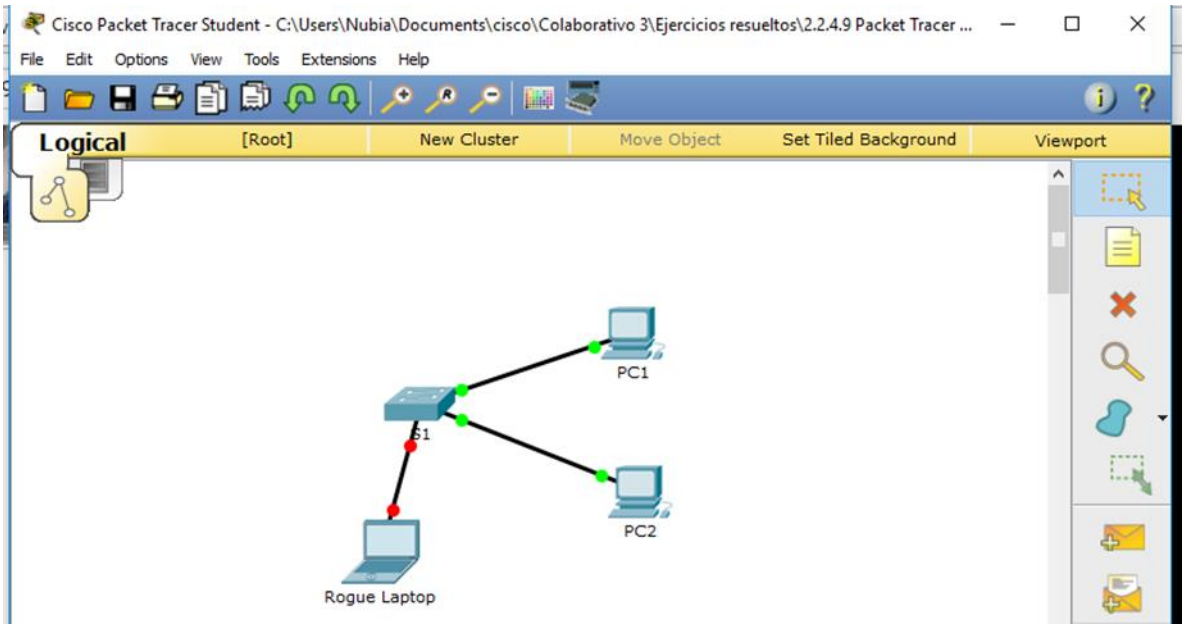
b. Verify port security is enabled and the MAC addresses of PC1 and PC2 were added to the running configuration.



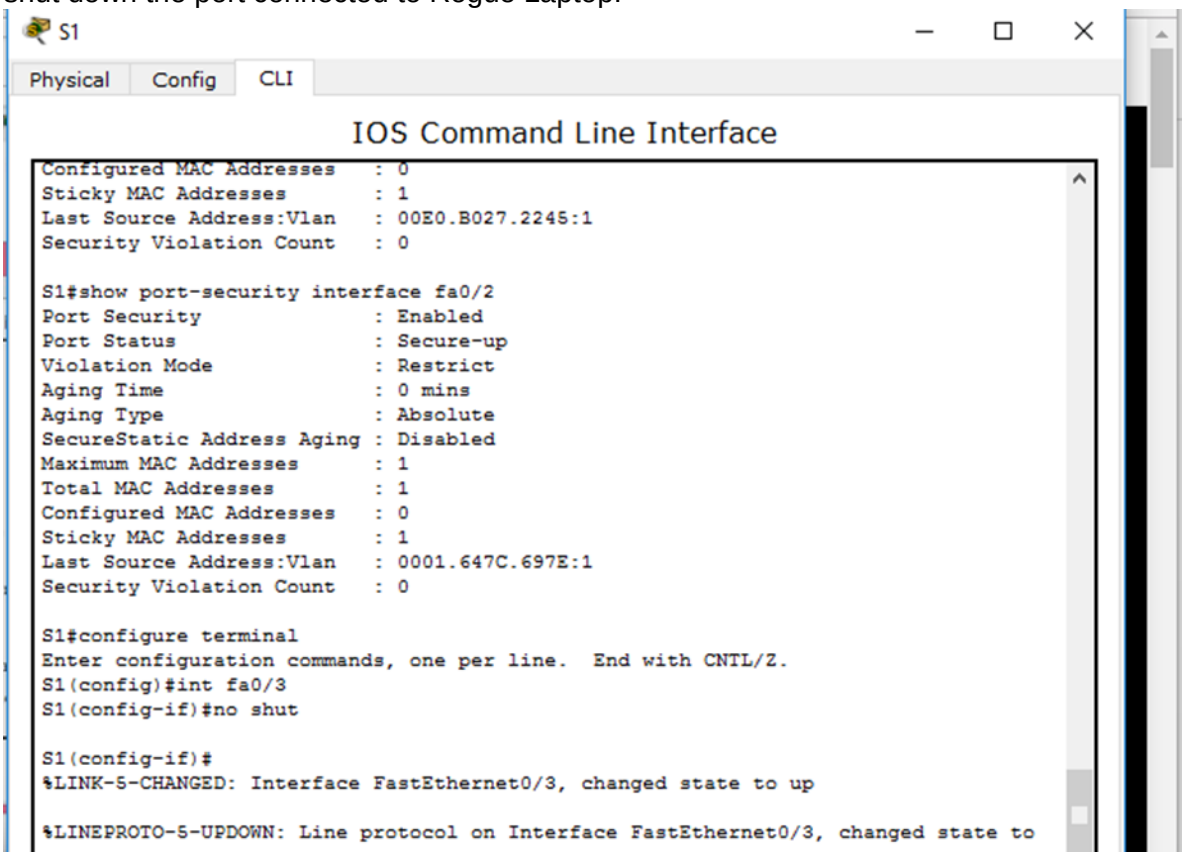


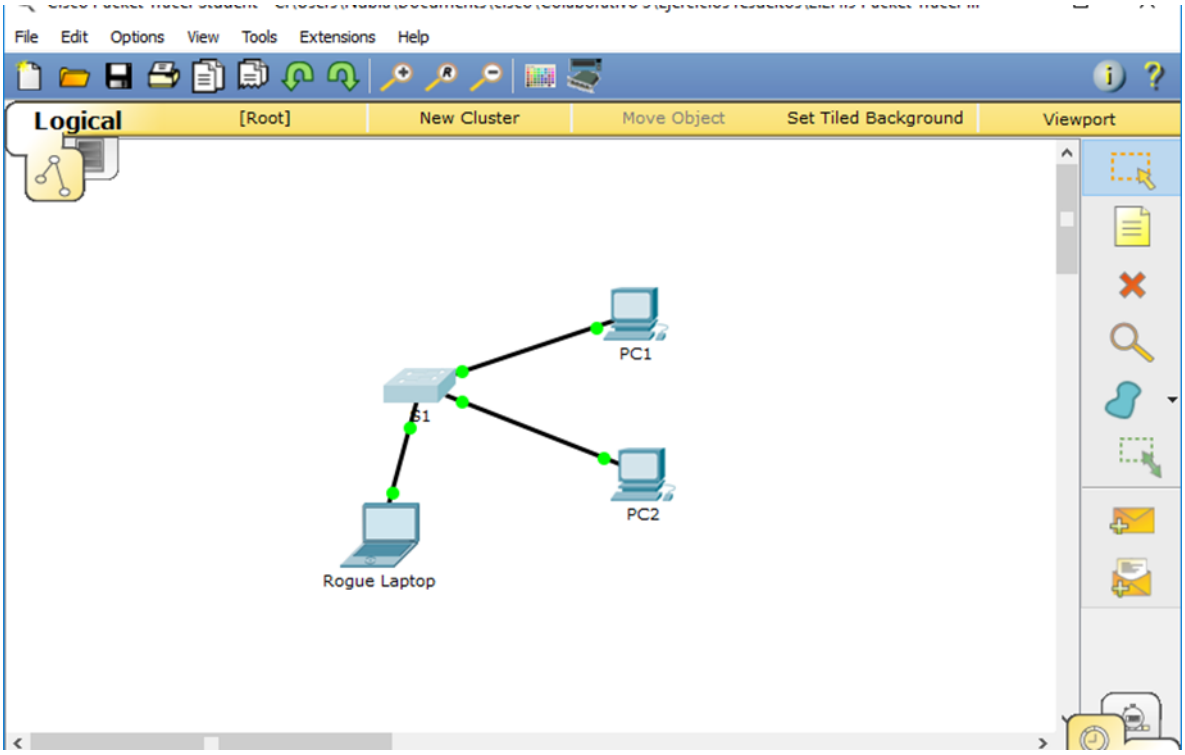


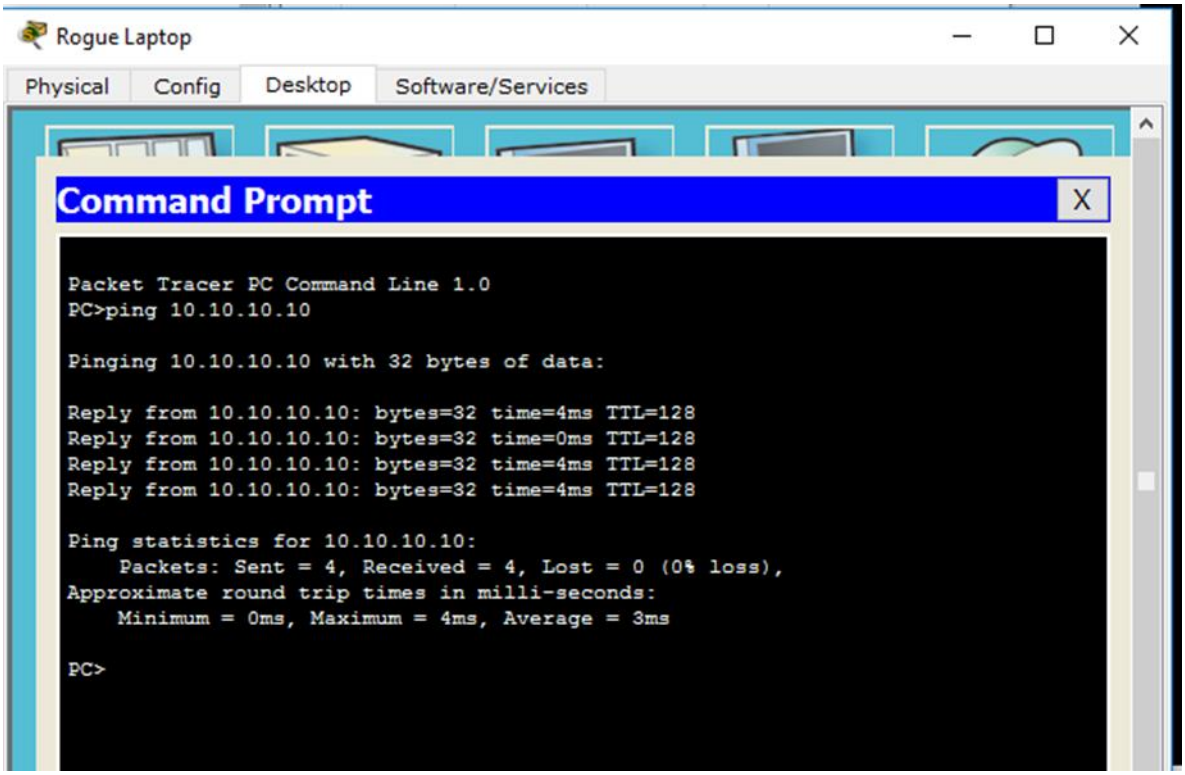
c. Attach Rogue Laptop to any unused switch port and notice that the link lights are red.

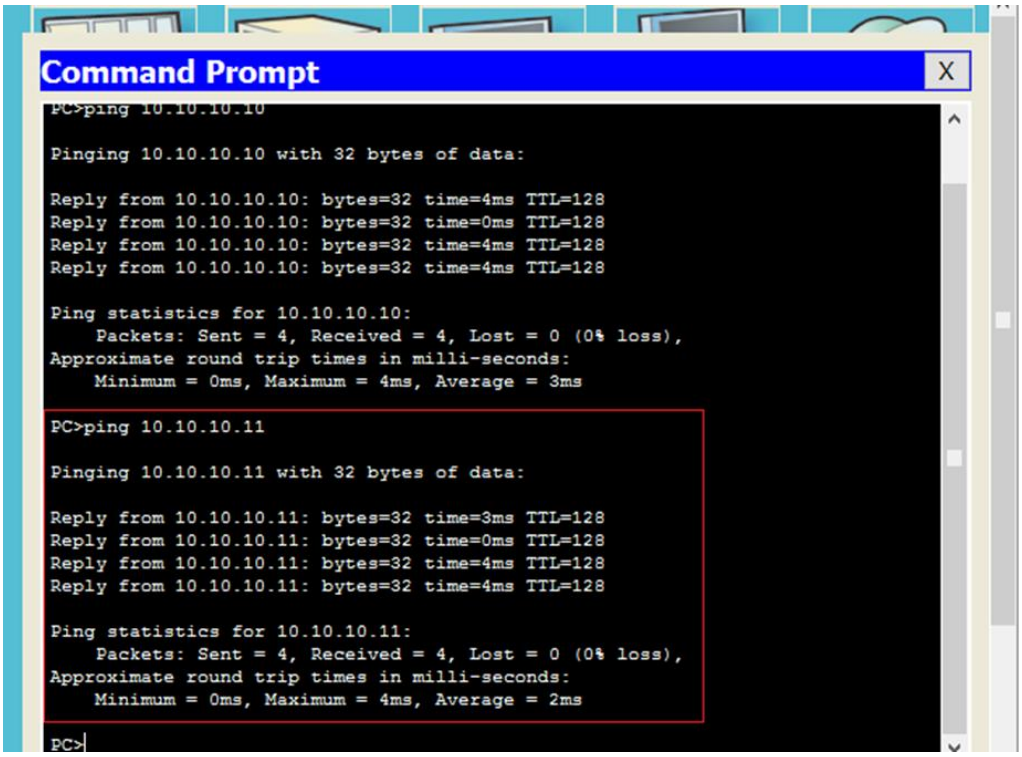


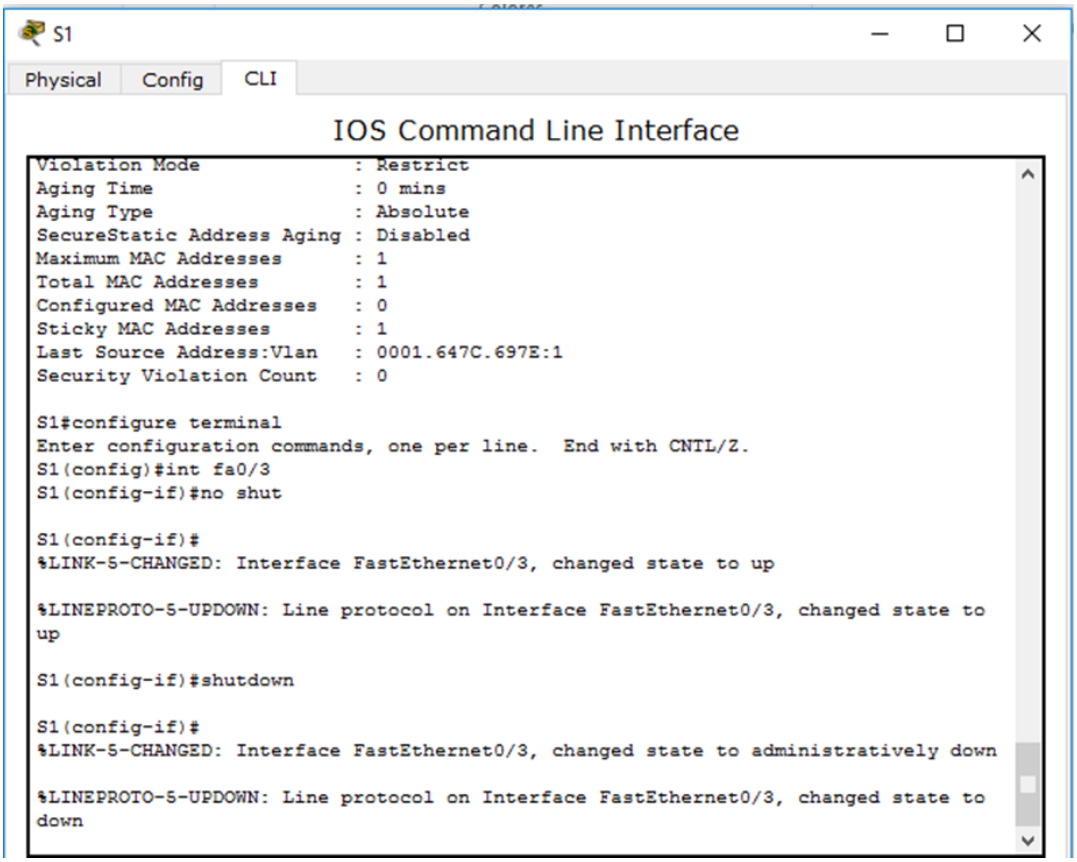
d. Enable the port and verify that Rogue Laptop can ping PC1 and PC2. After verification, shut down the port connected to Rogue Laptop.



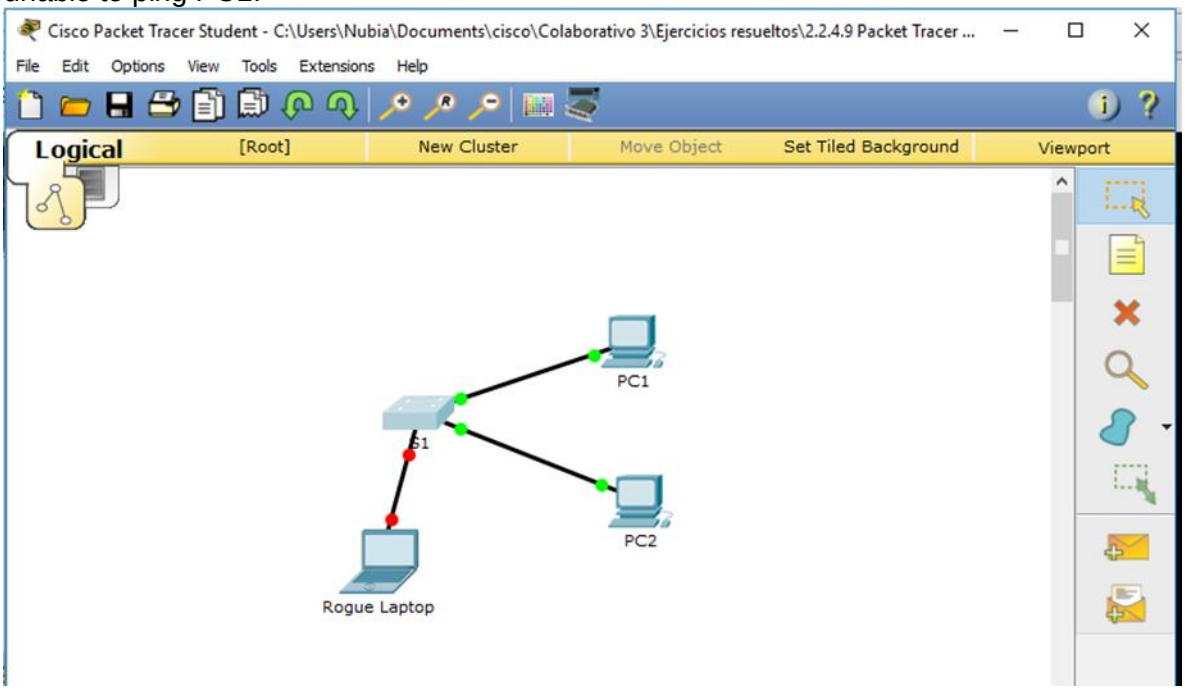

File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC1
PC2
Rogue Laptop

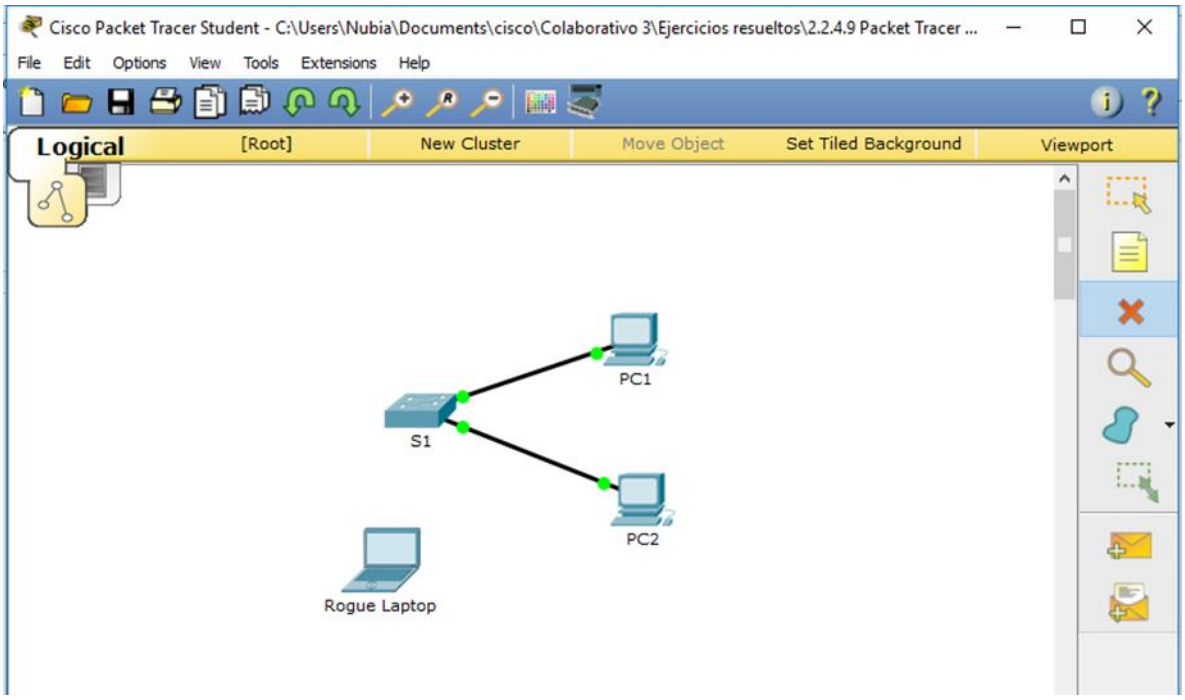

Rogue Laptop
Physical
Config
Desktop
Software/Services
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 10.10.10.10
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=4ms TTL=128
Reply from 10.10.10.10: bytes=32 time=0ms TTL=128
Reply from 10.10.10.10: bytes=32 time=4ms TTL=128
Reply from 10.10.10.10: bytes=32 time=4ms TTL=128
Ping statistics for 10.10.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 4ms, Average = 3ms
PC>


Command Prompt
X
PC>ping 10.10.10.10
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=4ms TTL=128
Reply from 10.10.10.10: bytes=32 time=0ms TTL=128
Reply from 10.10.10.10: bytes=32 time=4ms TTL=128
Reply from 10.10.10.10: bytes=32 time=4ms TTL=128
Ping statistics for 10.10.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 4ms, Average = 3ms
PC>ping 10.10.10.11
Pinging 10.10.10.11 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time=3ms TTL=128
Reply from 10.10.10.11: bytes=32 time=0ms TTL=128
Reply from 10.10.10.11: bytes=32 time=4ms TTL=128
Reply from 10.10.10.11: bytes=32 time=4ms TTL=128
Ping statistics for 10.10.10.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 4ms, Average = 2ms
PC>


S1
Physical
Config
CLI
IOS Command Line Interface
Violation Mode : Restrict
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0001.647C.697E:1
Security Violation Count : 0
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int fa0/3
S1(config-if)#no shut
S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
S1(config-if)#shutdown
S1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

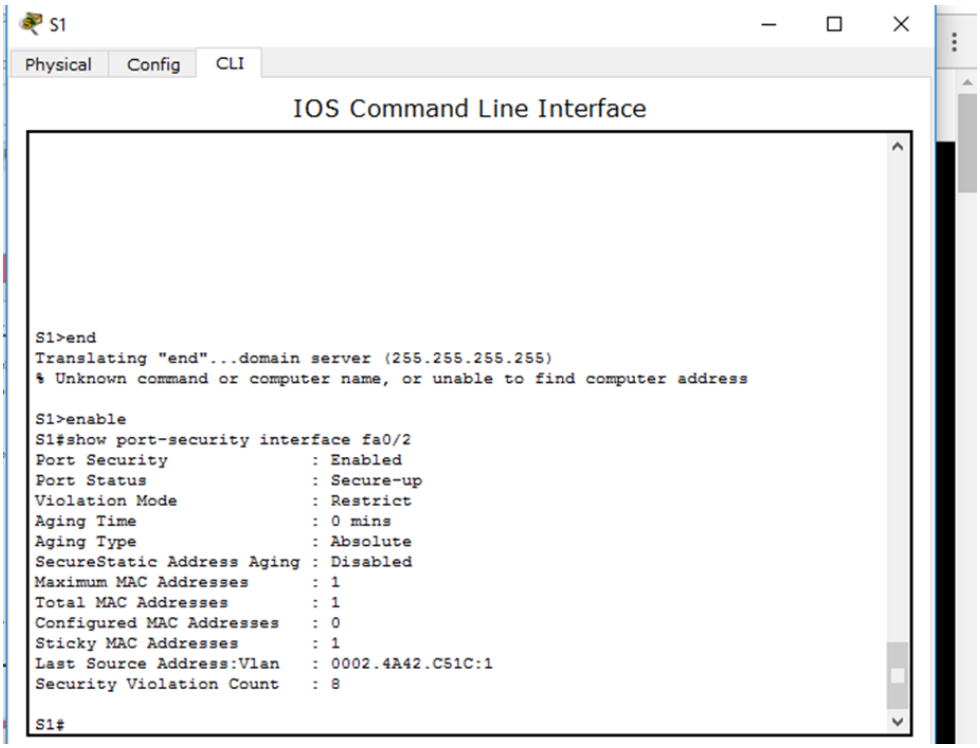
e. Disconnect PC2 and connect Rogue Laptop to PC2's port. Verify that Rogue Laptop is unable to ping PC1.



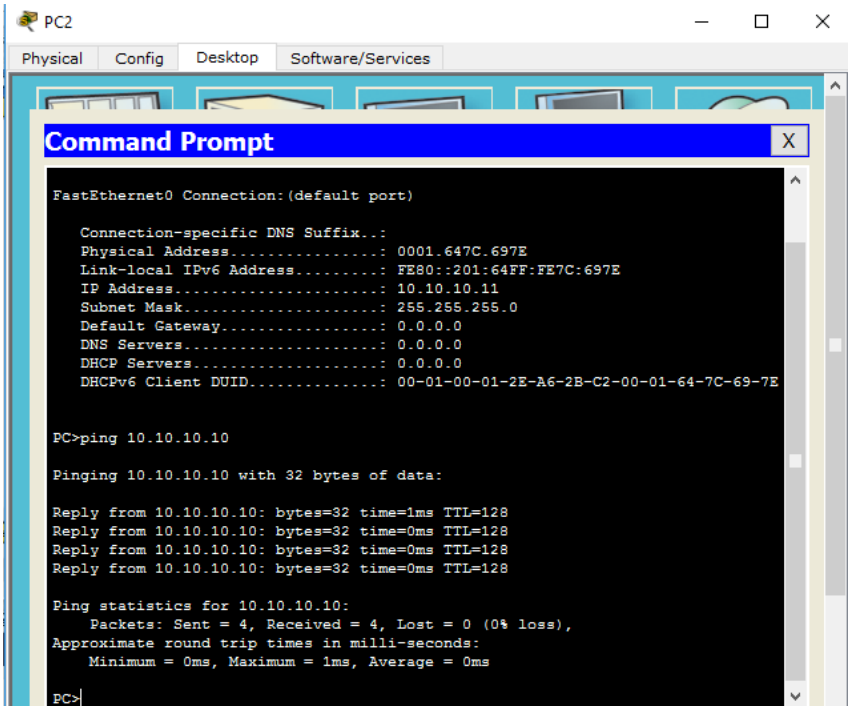


f. Display the port security violations for the port Rogue Laptop is connected to.

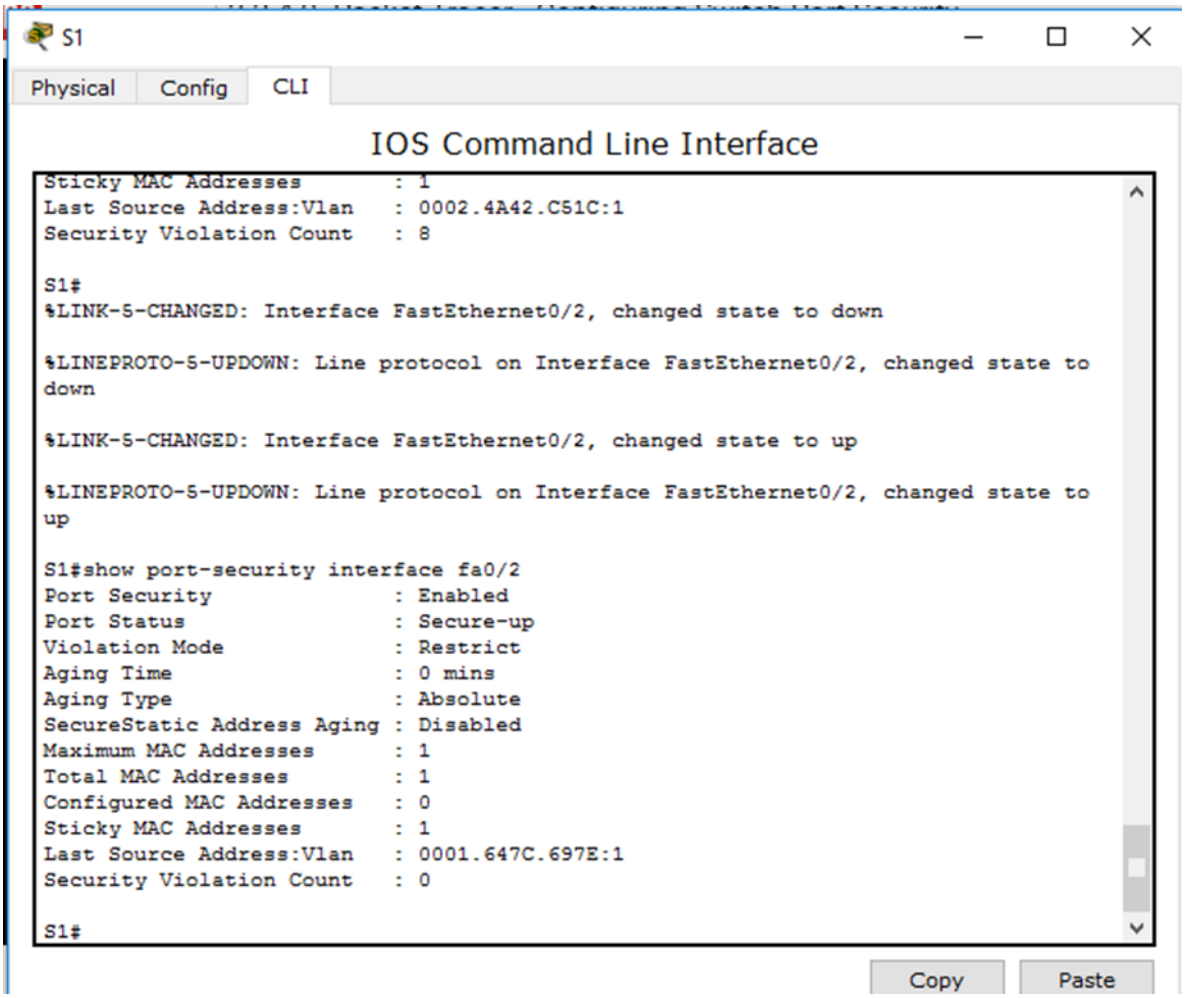
S1# show port-security interface fa0/2

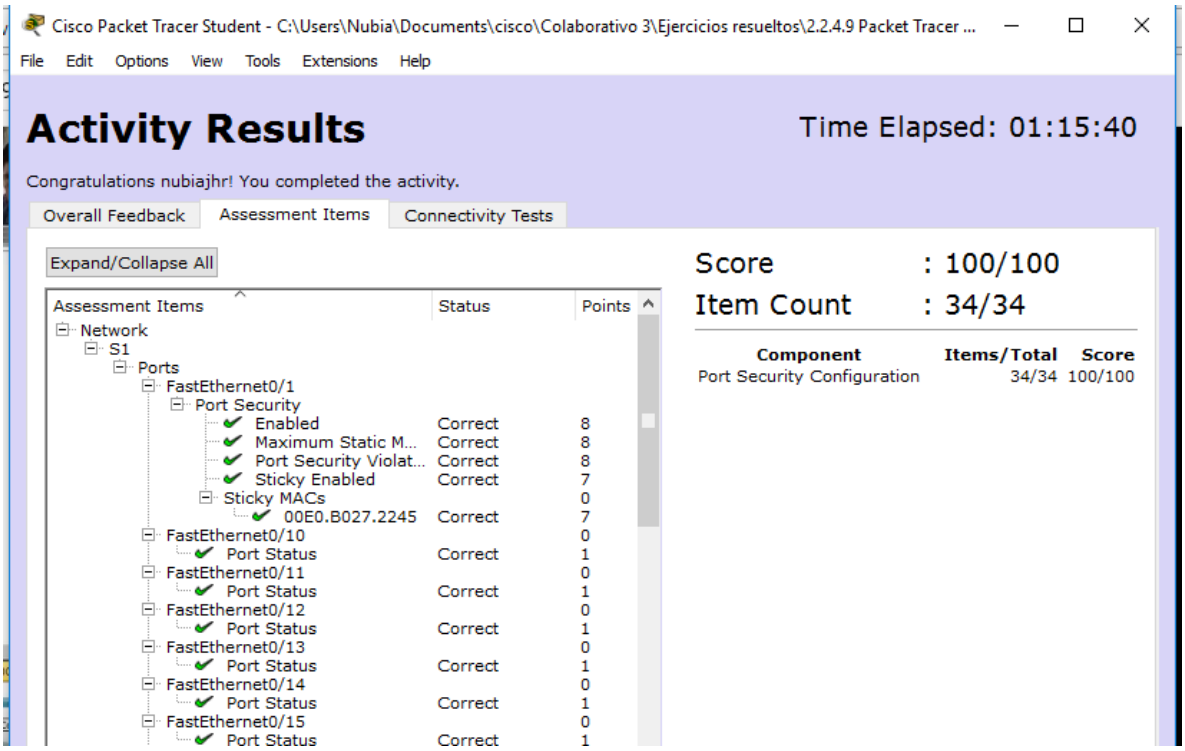


g. Disconnect Rouge Laptop and reconnect PC2. Verify PC2 can ping PC1.



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

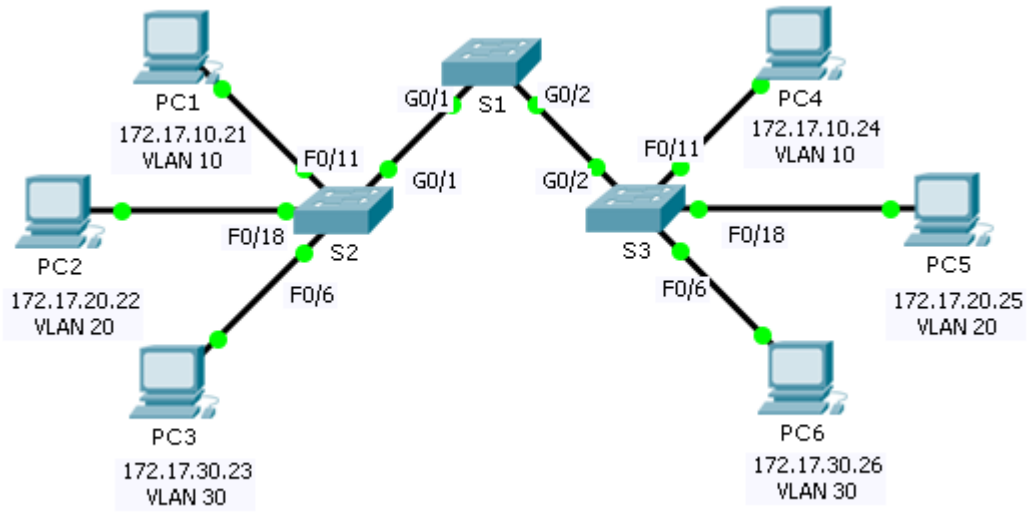



Cisco Packet Tracer Student - C:\Users\Nubia\Documents\cisco\Colaborativo 3\Ejercicios resueltos\2.2.4.9 Packet Tracer ...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 01:15:40
Congratulations nubiajhr! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Network
S1
Ports
FastEthernet0/1
Port Security
Enabled Correct 8
Maximum Static M... Correct 8
Port Security Violat... Correct 8
Sticky Enabled Correct 7
Sticky MACs 0
00E0.B027.2245 Correct 7
FastEthernet0/10 0
Port Status Correct 1
FastEthernet0/11 0
Port Status Correct 1
FastEthernet0/12 0
Port Status Correct 1
FastEthernet0/13 0
Port Status Correct 1
FastEthernet0/14 0
Port Status Correct 1
FastEthernet0/15 0
Port Status Correct 1
Score : 100/100
Item Count : 34/34
Component
Items/Total
Score
Port Security Configuration
34/34
100/100

Informe No. 2

3.2.1.7. Packet Tracer – Configuring VLANs

Topology



Addressing Table

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

Objectives

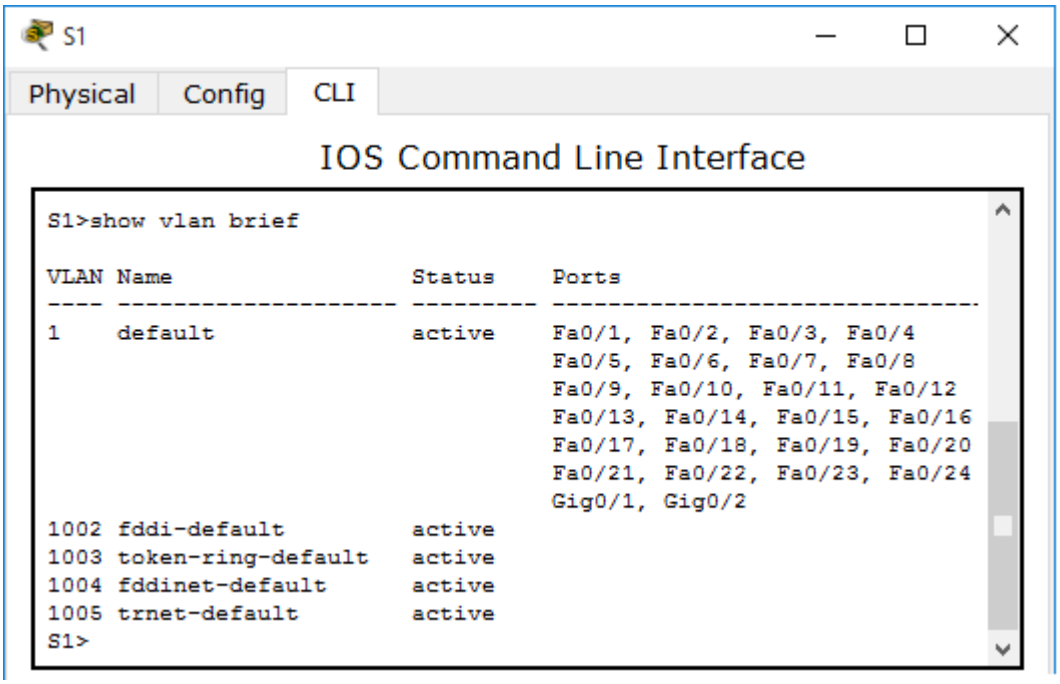
Part 1: Verify the Default VLAN Configuration
Part 2: Configure VLANs
Part 3: Assign VLANs to Ports

Background

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

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

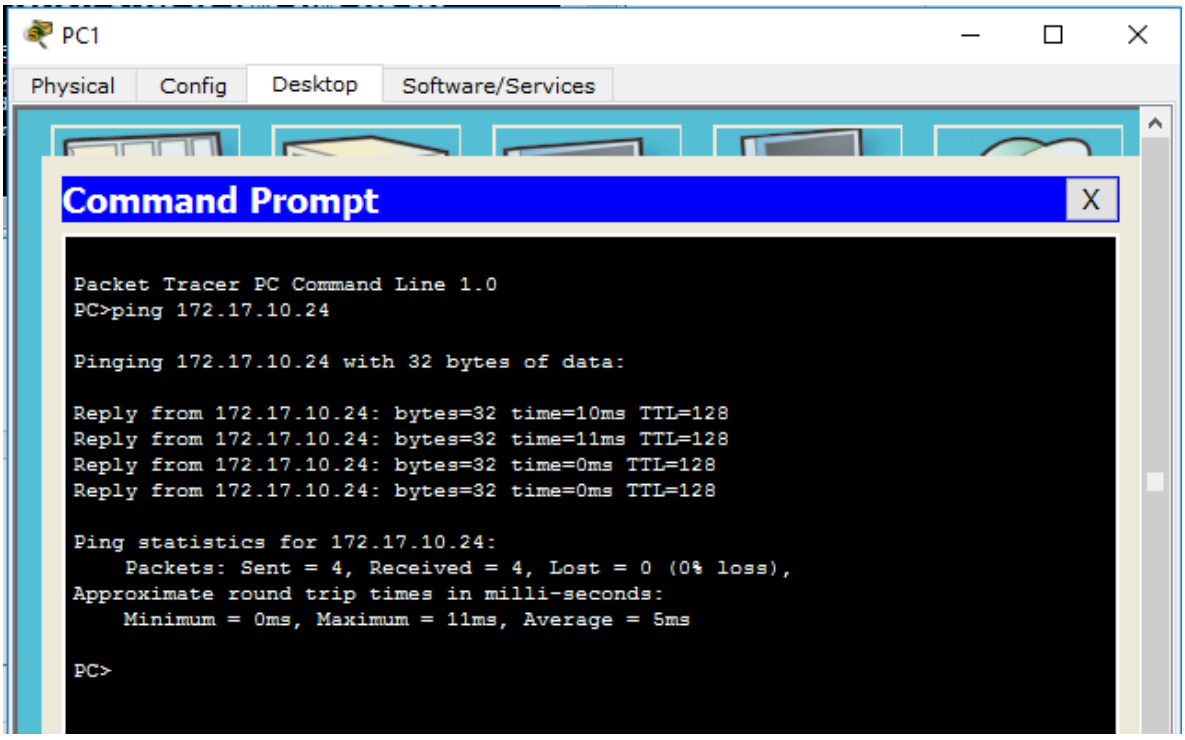
On S1, issue the command that displays all VLANs configured. By default, all interfaces are assigned to VLAN 1.



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

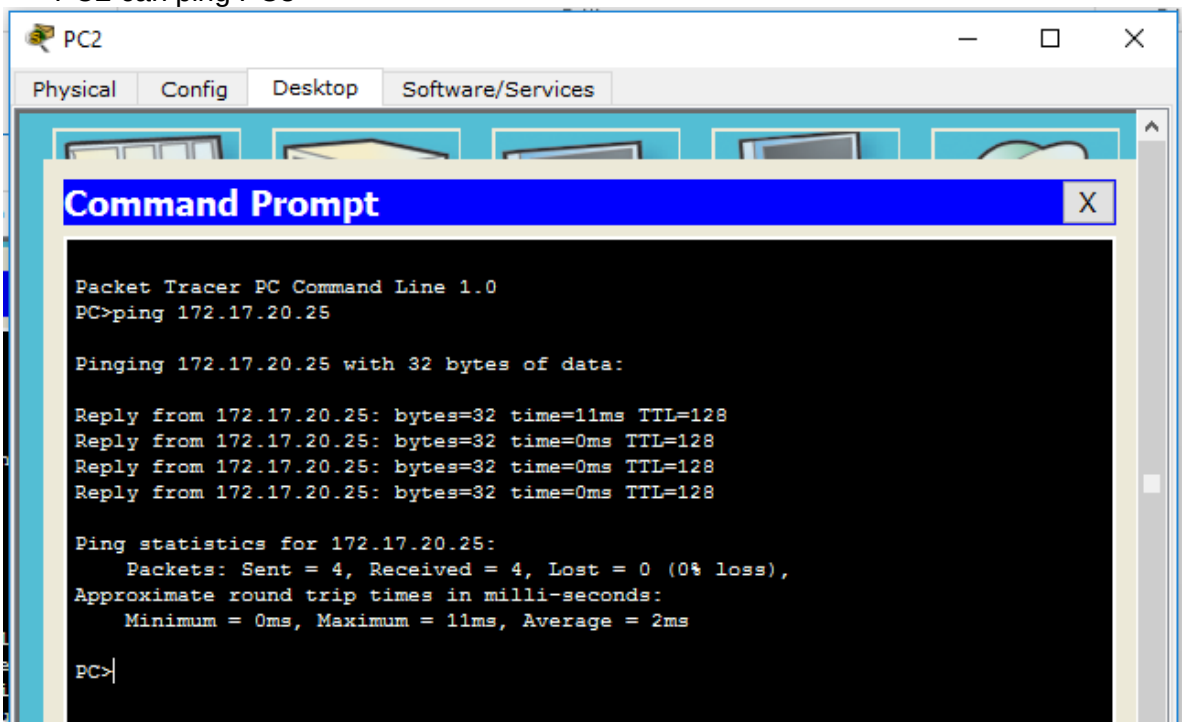
Notice that each PC can ping the other PC that shares the same network.

- PC1 can ping PC4



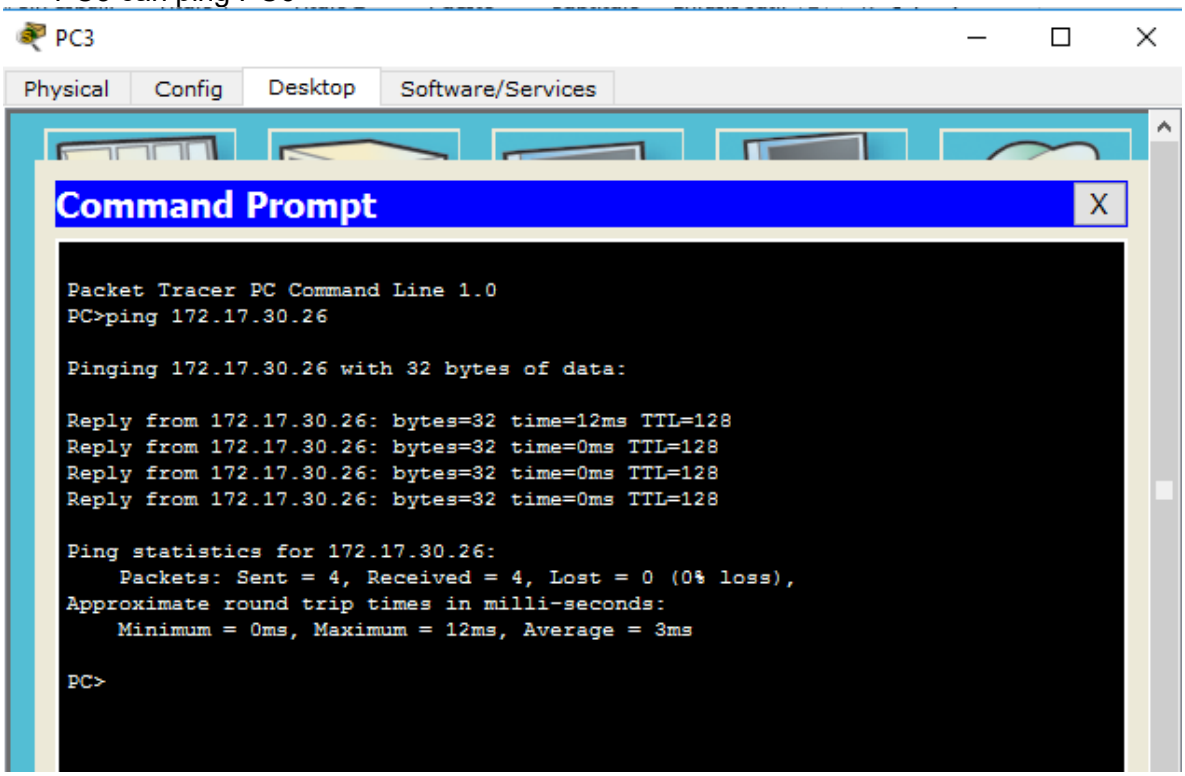
Ping exitoso

- PC2 can ping PC5



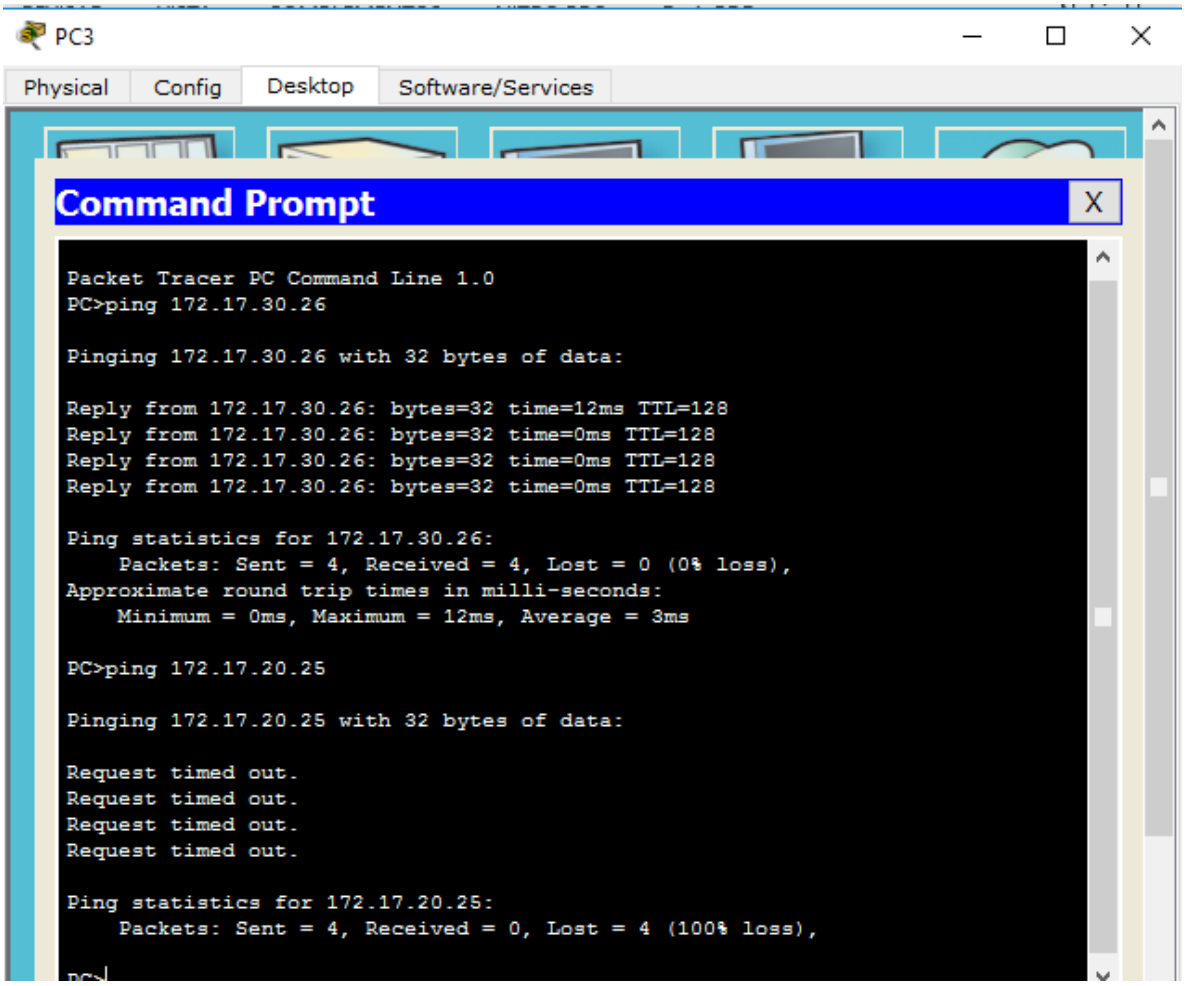
Ping exitoso

- PC3 can ping PC6



Pings to PCs in other networks fail.

Se comprueba fallo en la respuesta entre el PC3 y el PC 5.



Ping fallido

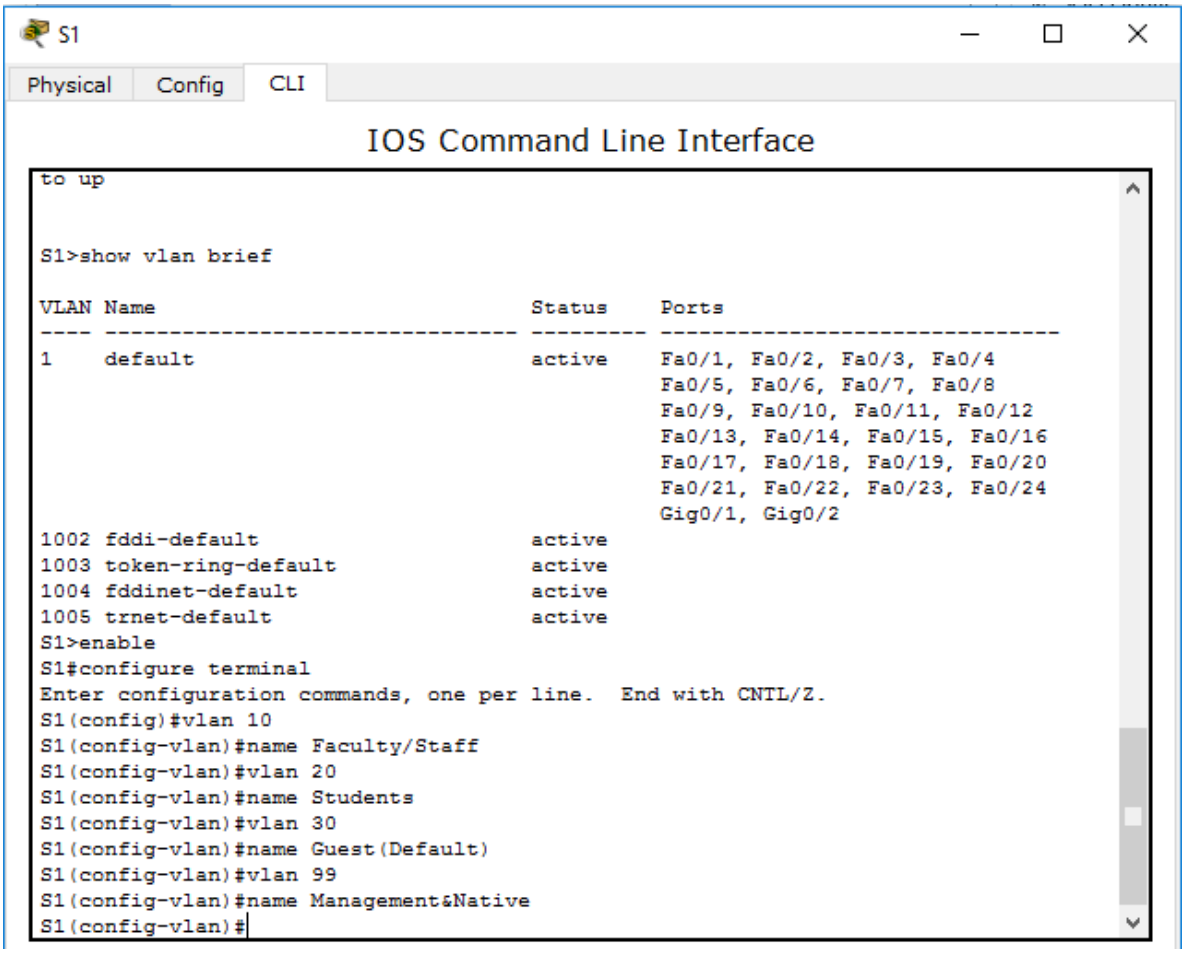
What benefit will configuring VLANs provide to the current configuration? The primary benefits of using VLANs are as follows: security, cost reduction, higher performance, broadcast storm mitigation, improved IT staff efficiency, and simpler project and application management.

Part 2: Configure VLANs
Step 1: Create and name VLANs on S1.

Create the following VLANs. Names are case-sensitive:

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

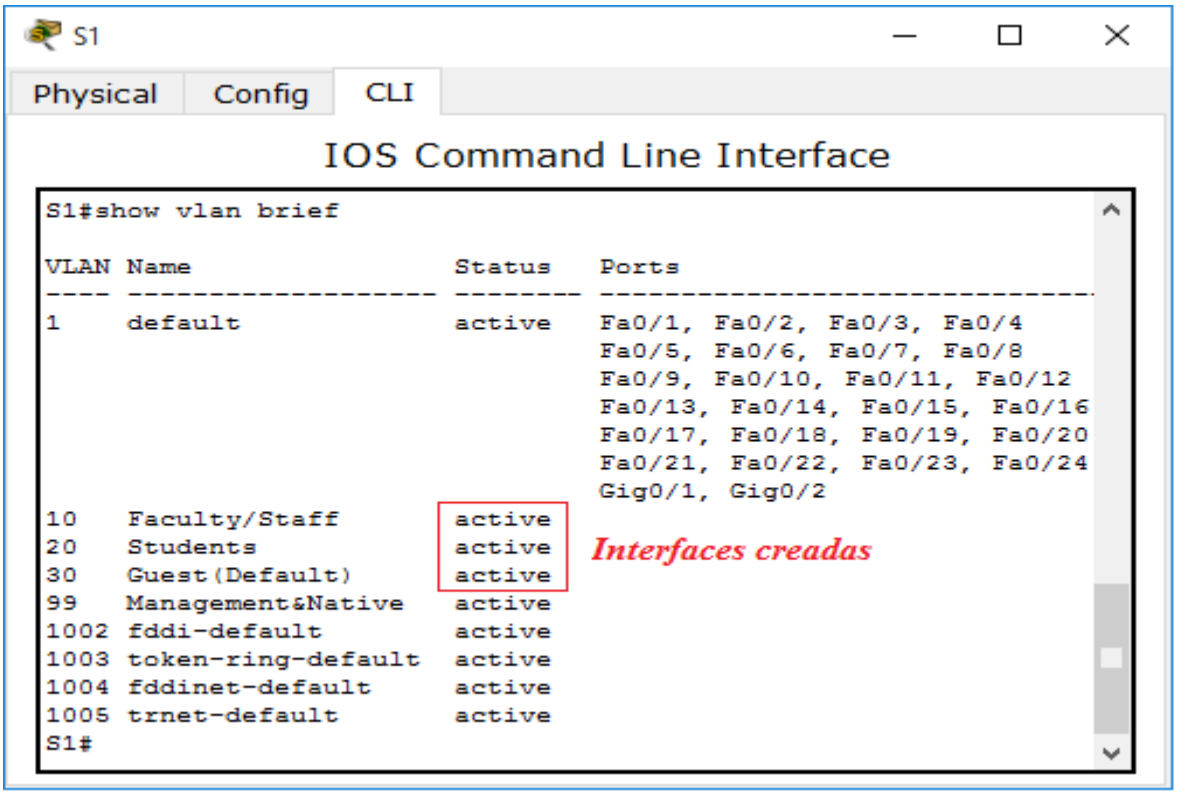
S1#(config)# vlan 10
S1#(config-vlan)# name Faculty/Staff
S1#(config-vlan)# vlan 20
S1#(config-vlan)# name Students
S1#(config-vlan)# vlan 30
S1#(config-vlan)# name Guest(Default)
S1#(config-vlan)# vlan 99
S1#(config-vlan)# name Management&Native

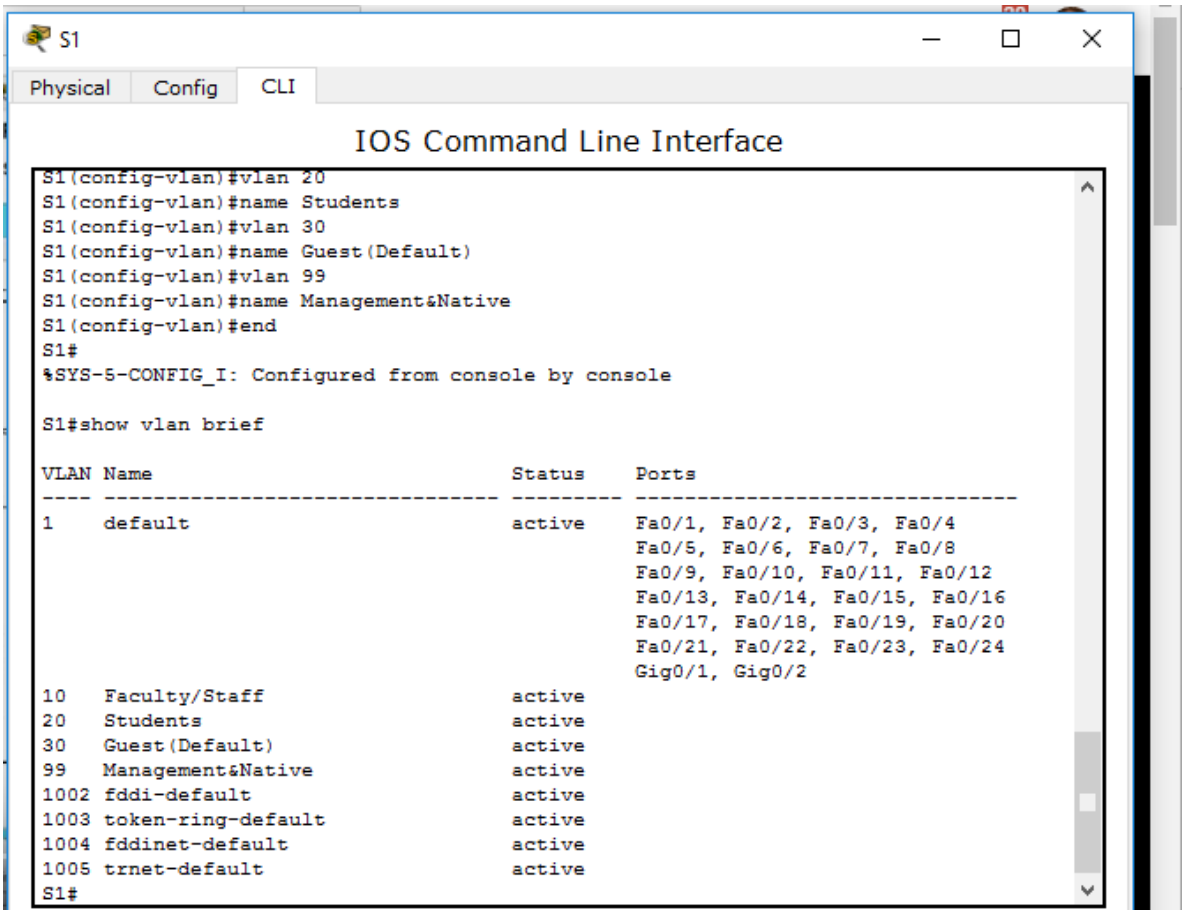


Step 2: Verify the VLAN configuration.

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

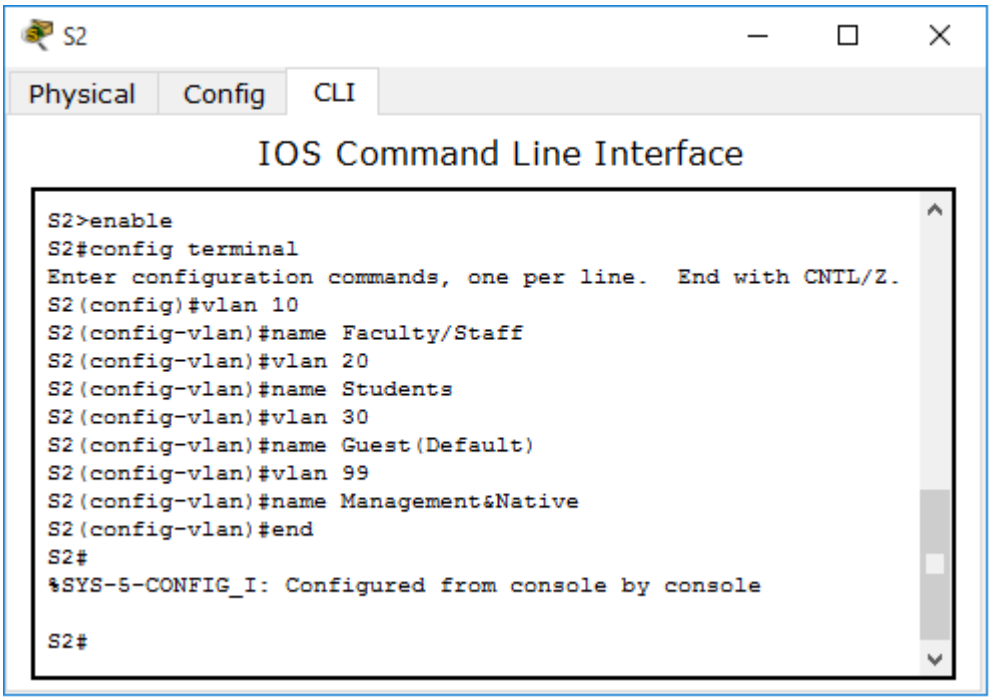
S1# show vlan brief

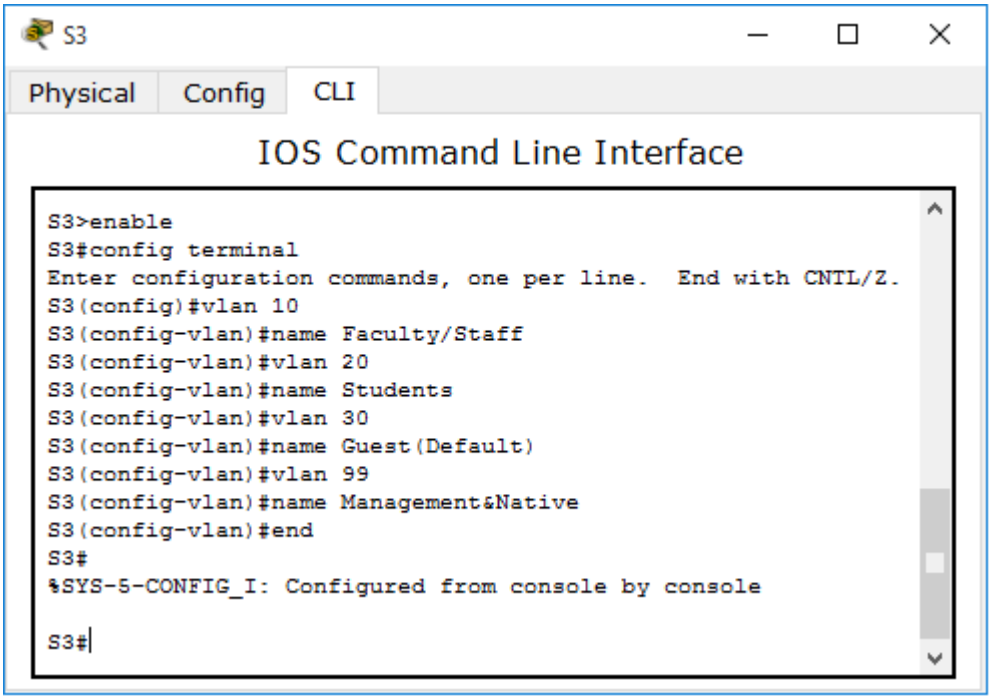

S1
Physical
Config
CLI
IOS Command Line Interface
S1#show vlan brief
VLAN Name Status Ports
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
10 Faculty/Staff active
20 Students active
30 Guest(Default) active
99 Management&Native active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
S1#
Interfaces creadas


S1
Physical
Config
CLI
IOS Command Line Interface
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
S1(config-vlan)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#show vlan brief
VLAN Name Status Ports
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/1, Gig0/2
10 Faculty/Staff active
20 Students active
30 Guest(Default) active
99 Management&Native active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
S1#

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.





Step 4: Verify the VLAN configuration.
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

```
S2#confi t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int fa0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#int fa0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#int fa0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#
```

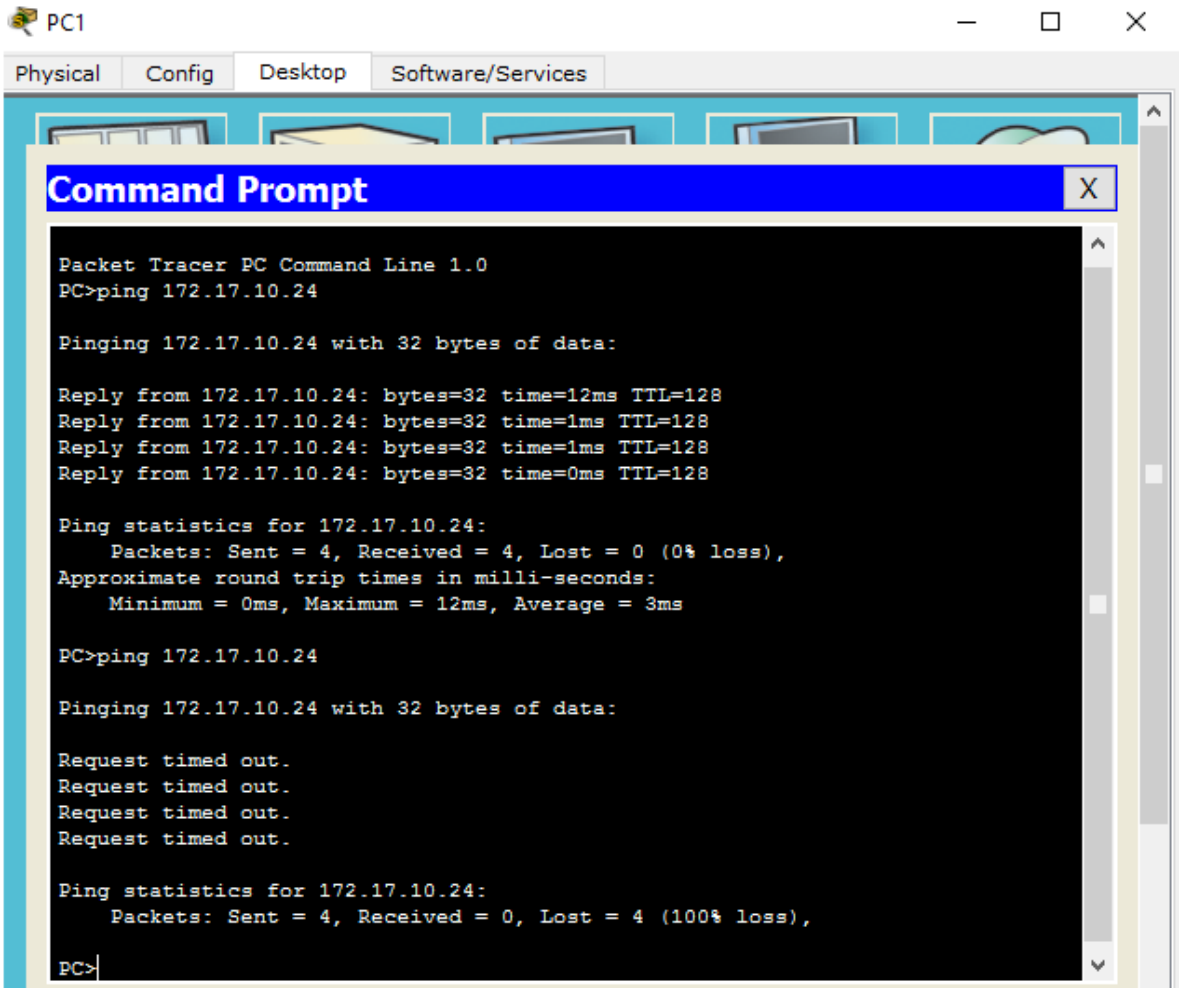
Step 2: Assign VLANs to the active ports on S3.

S3 uses the same VLAN access port assignments as S2.

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

Step 3: Verify loss of connectivity.

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

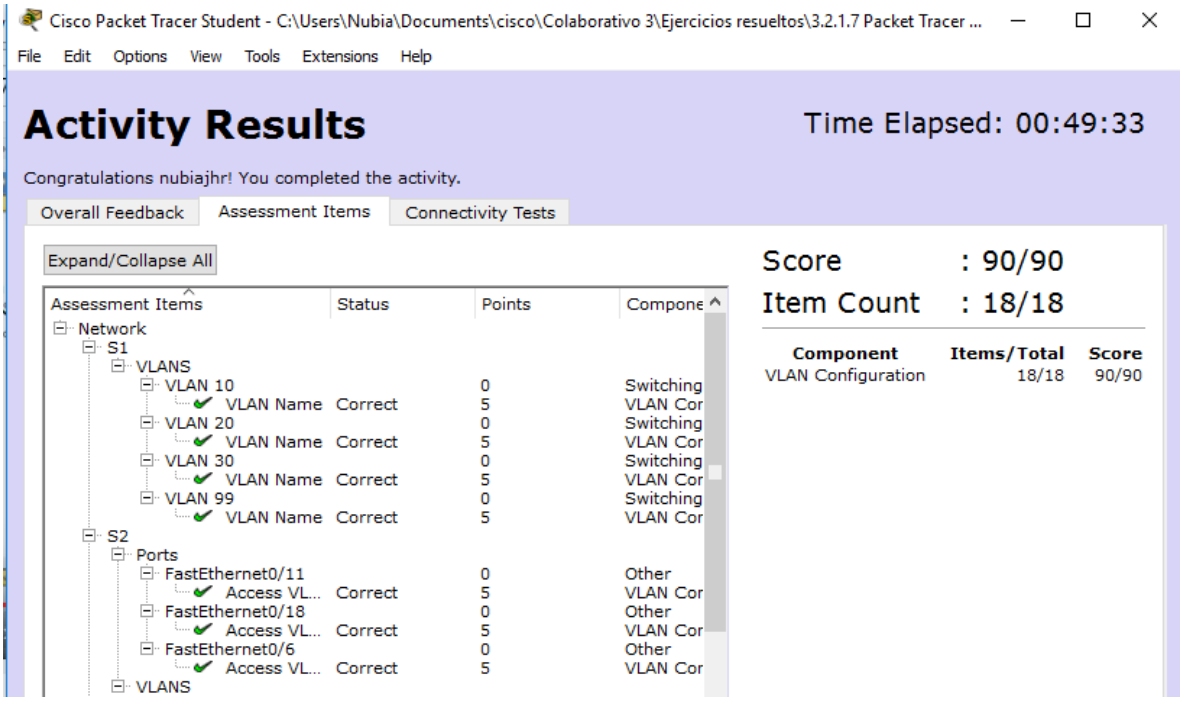


Ping fallido

Se debe configurar los puertos entre los swiches como puertos troncales

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

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Verify the Default VLAN Configuration	Step 2	**4**	
Part 2: Configure VLANs	Step 2	**2**	
Part 3: Assign VLANs to Ports	Step 3	**4**	
	Packet Tracer Score	**90**	
	Total Score	**100**	


Cisco Packet Tracer Student - C:\Users\Nubia\Documents\cisco\Colaborativo 3\Ejercicios resueltos\3.2.1.7 Packet Tracer ...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 00:49:33
Congratulations nubiajhr! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Compone
Network
S1
VLANS
VLAN 10 0 Switching
VLAN Name Correct 5 VLAN Cor
VLAN 20 0 Switching
VLAN Name Correct 5 VLAN Cor
VLAN 30 0 Switching
VLAN Name Correct 5 VLAN Cor
VLAN 99 0 Switching
VLAN Name Correct 5 VLAN Cor
S2
Ports
FastEthernet0/11 0 Other
Access VL... Correct 5 VLAN Cor
FastEthernet0/18 0 Other
Access VL... Correct 5 VLAN Cor
FastEthernet0/6 0 Other
Access VL... Correct 5 VLAN Cor
VLANS
Score : 90/90
Item Count : 18/18
Component Items/Total Score
VLAN Configuration 18/18 90/90

Informe No. 3

3.2.2.4: Packet Tracer – Configuring Trunks

Addressing Table

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

Objectives

Part 1: Verify VLANs

Part 2: Configure Trunks

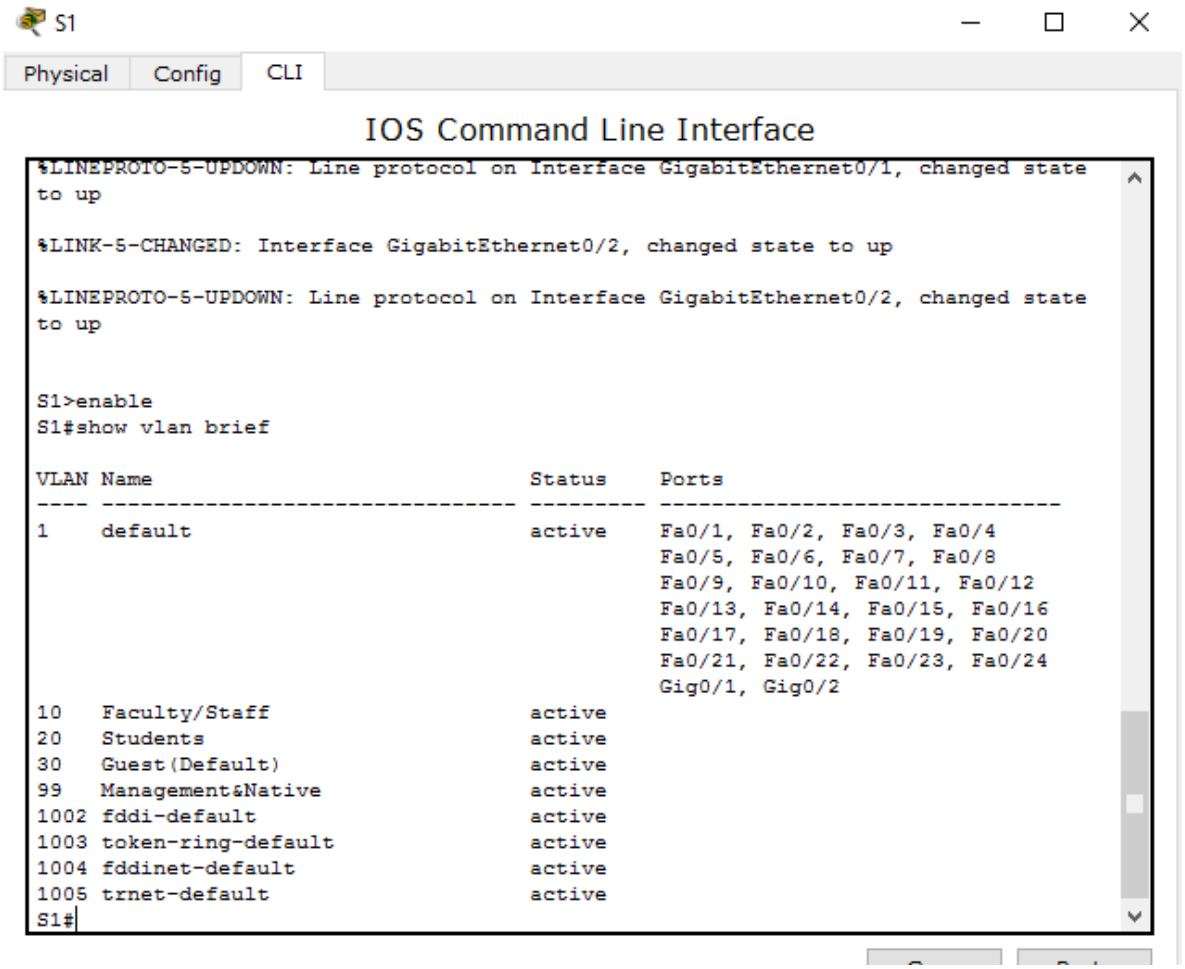
Background

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

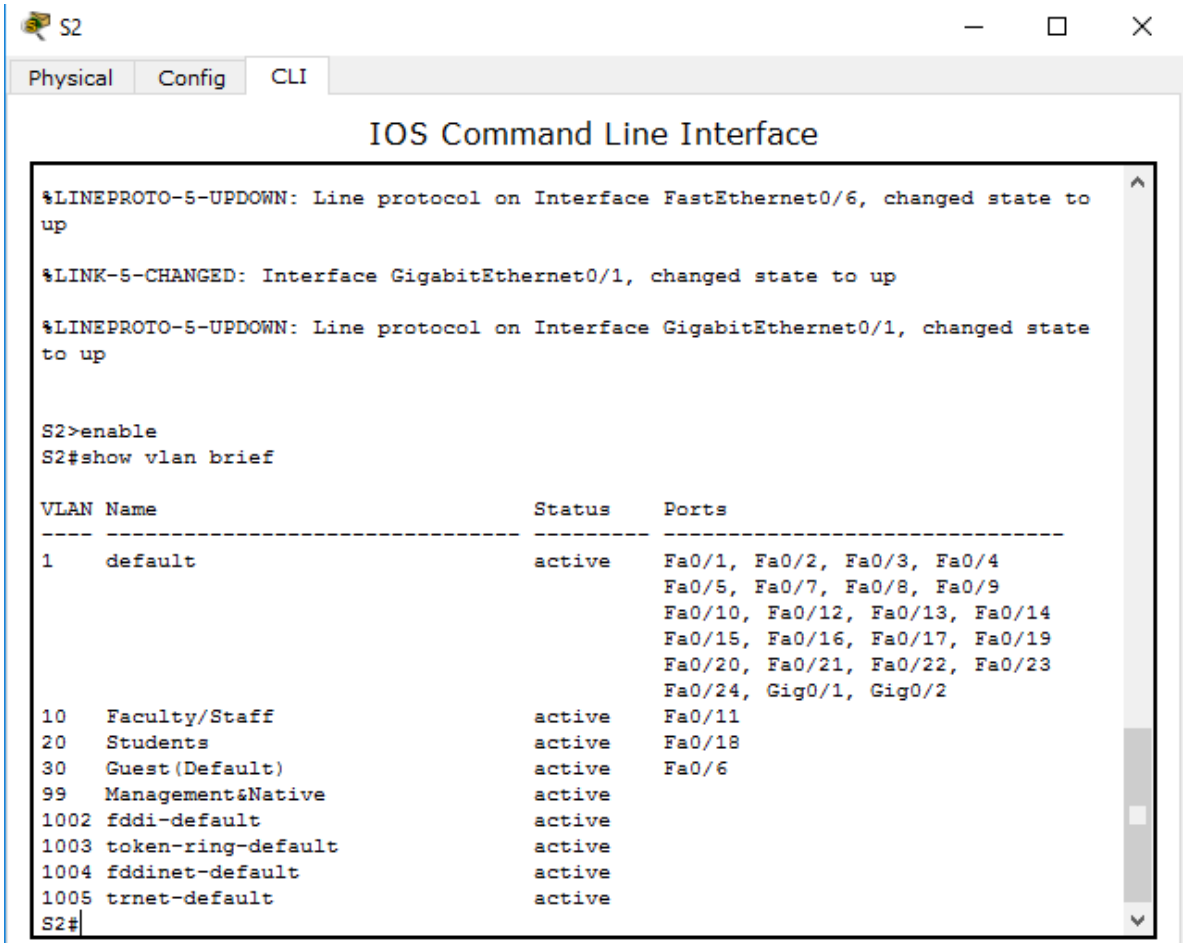
Part 1: Verify VLANs

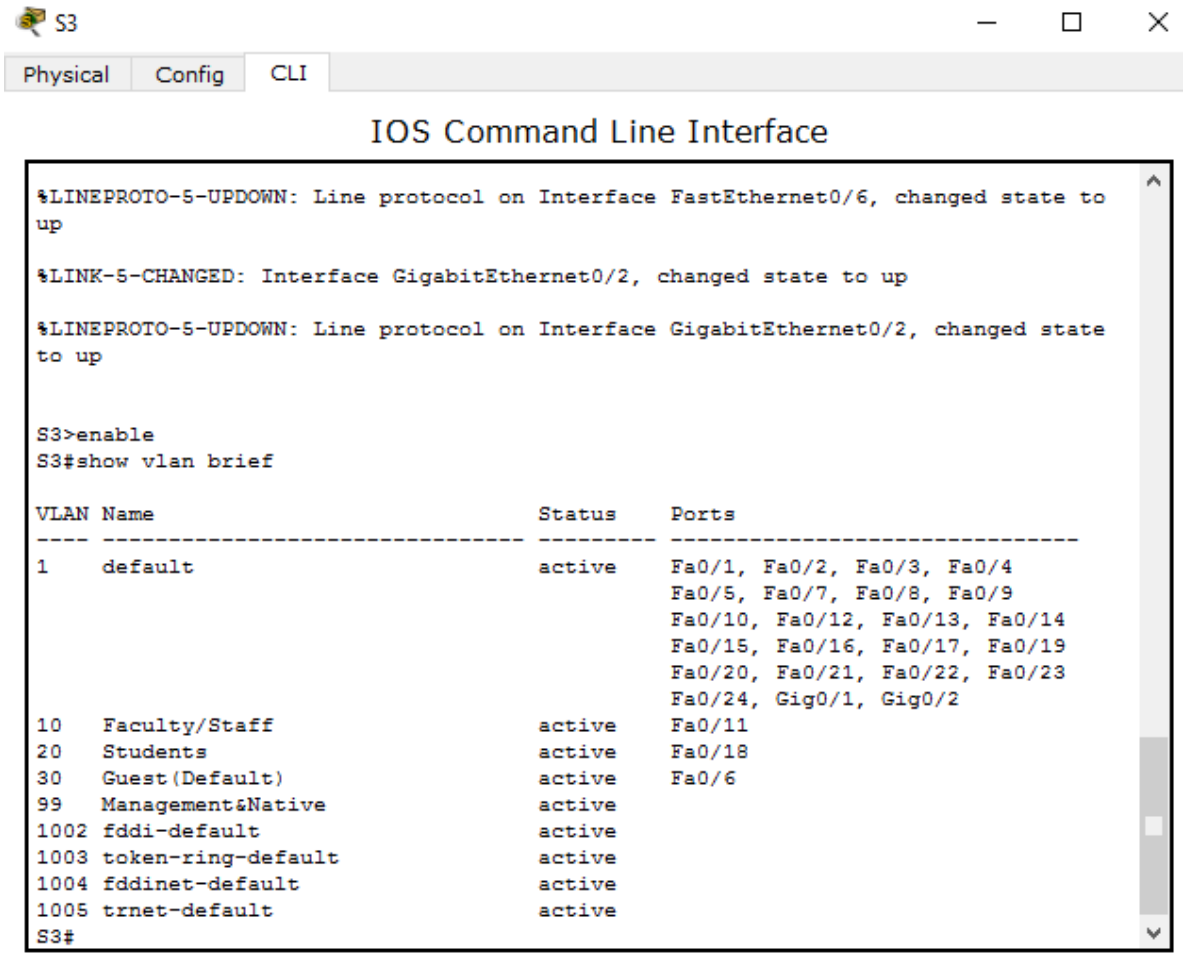
Step 1: Display the current VLANs.

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



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

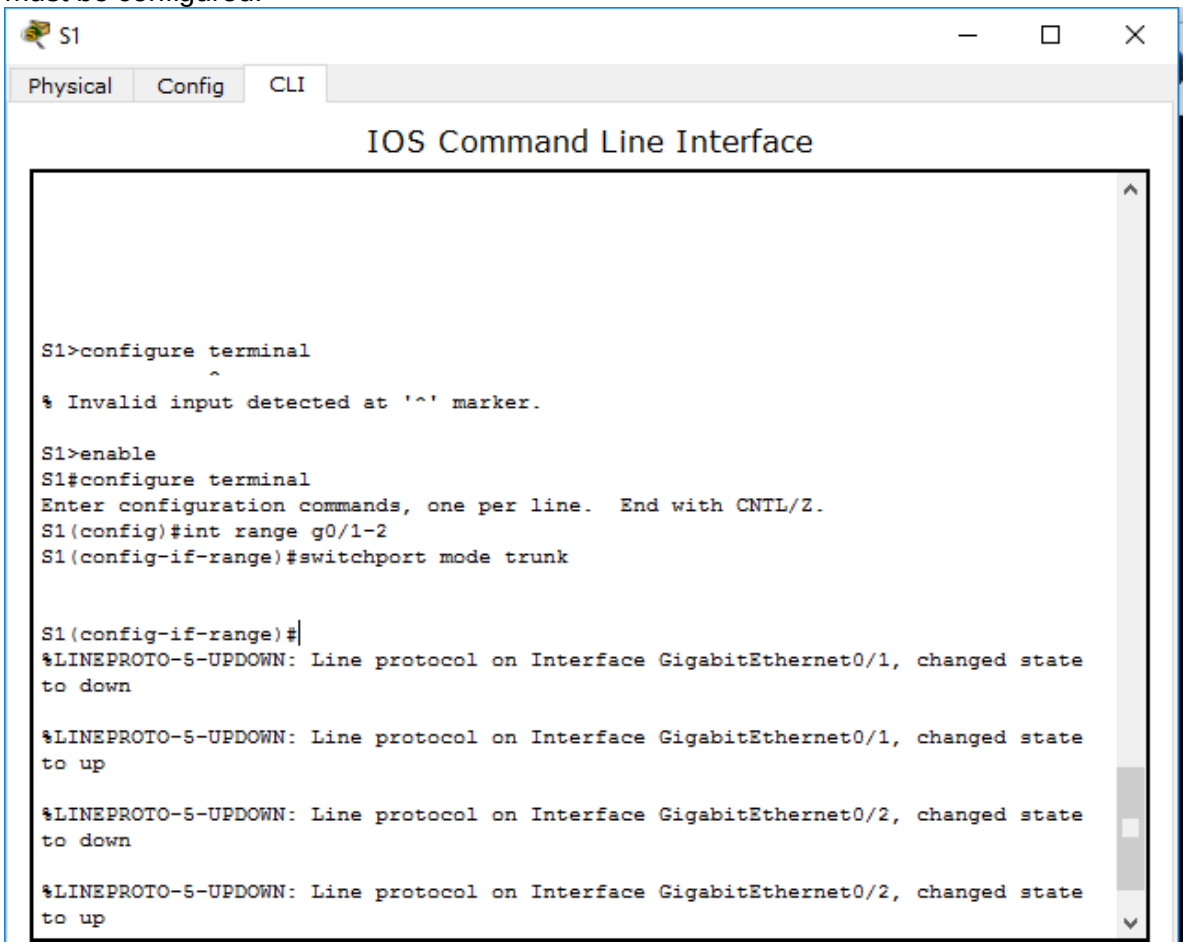

S2
Physical
Config
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
S2>enable
S2#show 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, Fa0/19
Fa0/20, Fa0/21, Fa0/22, Fa0/23
Fa0/24, Gig0/1, Gig0/2
10 Faculty/Staff active Fa0/11
20 Students active Fa0/18
30 Guest(Default) active Fa0/6
99 Management&Native active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
S2#



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

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

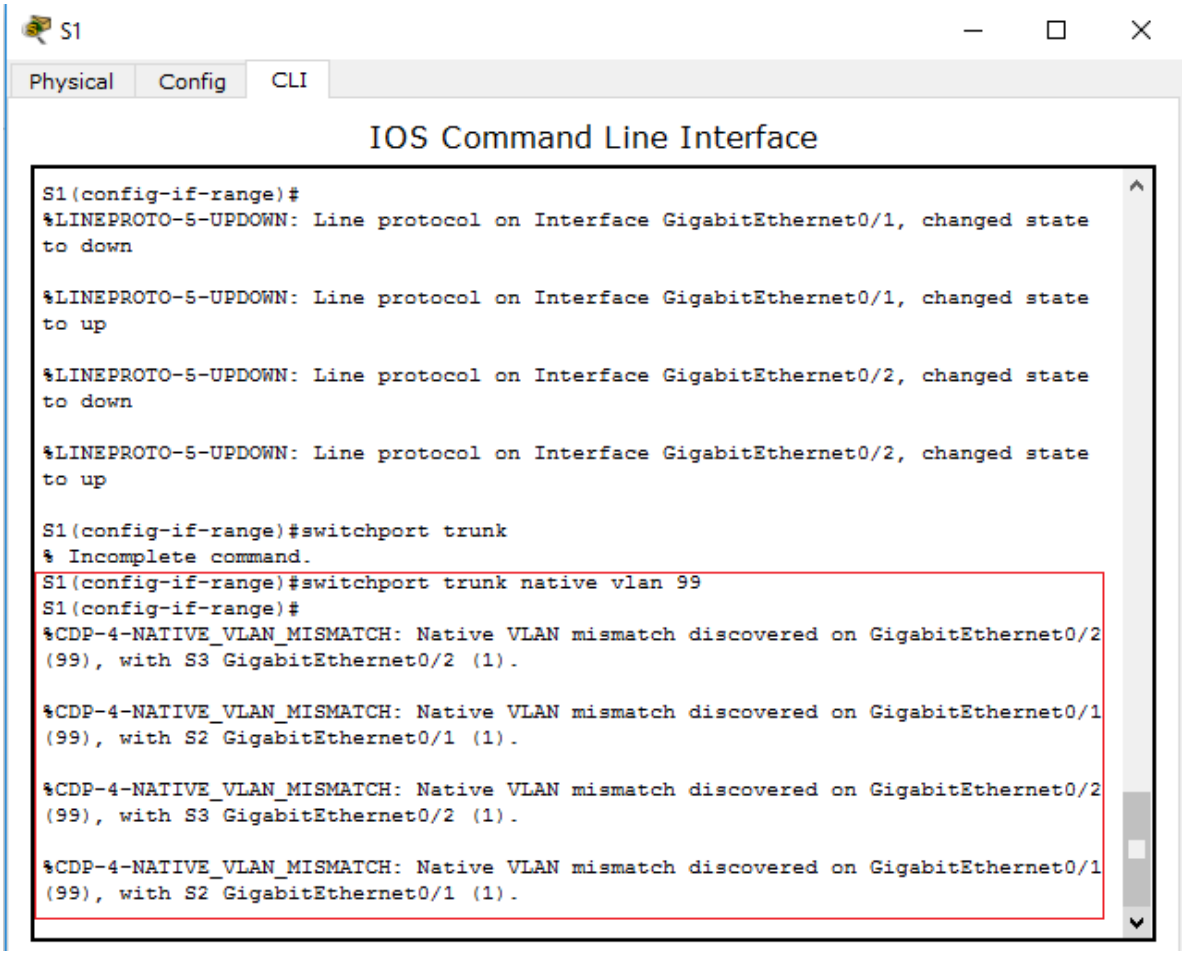
must be configured.



Part 2: Configure Trunks

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

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



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

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).

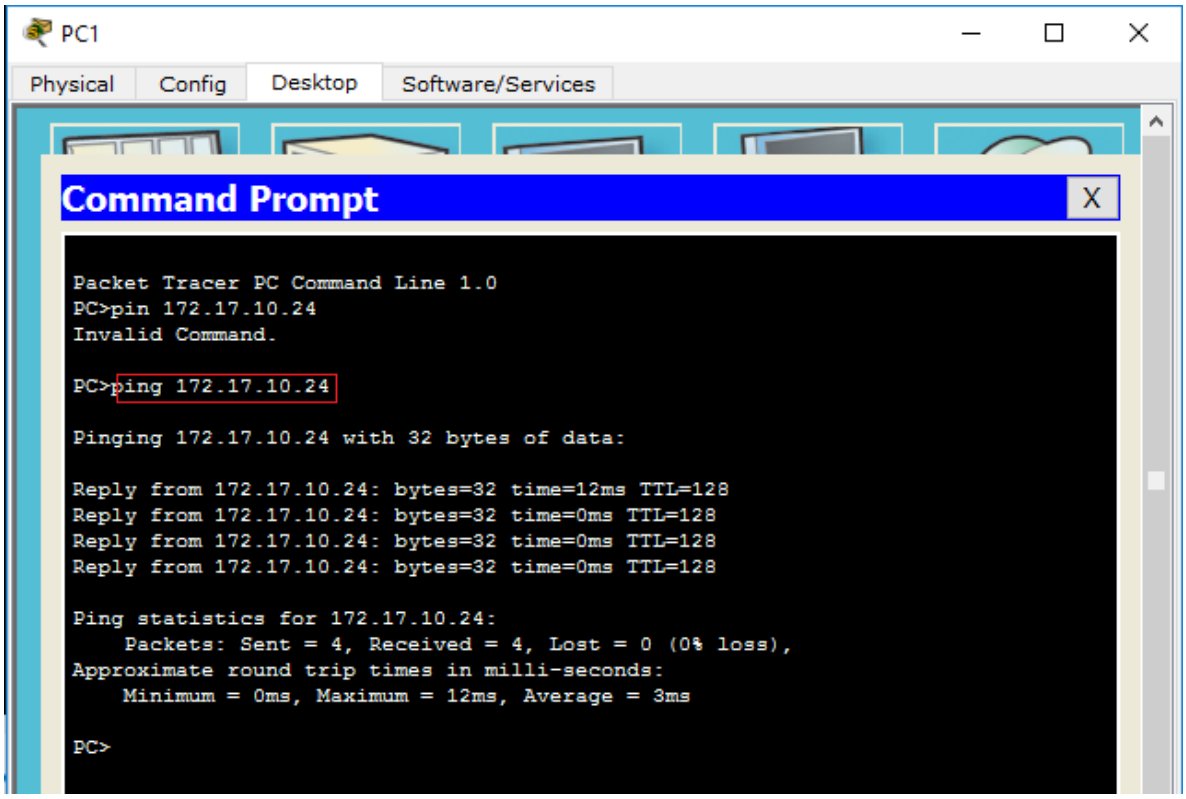
You configured VLAN 99 as the native VLAN on S1. However, the S2 and S3 are using VLAN 1 as the default native VLAN as indicated by the syslog message.

Although you have a native VLAN mismatch, pings between PCs on the same VLAN are now successful. Why?

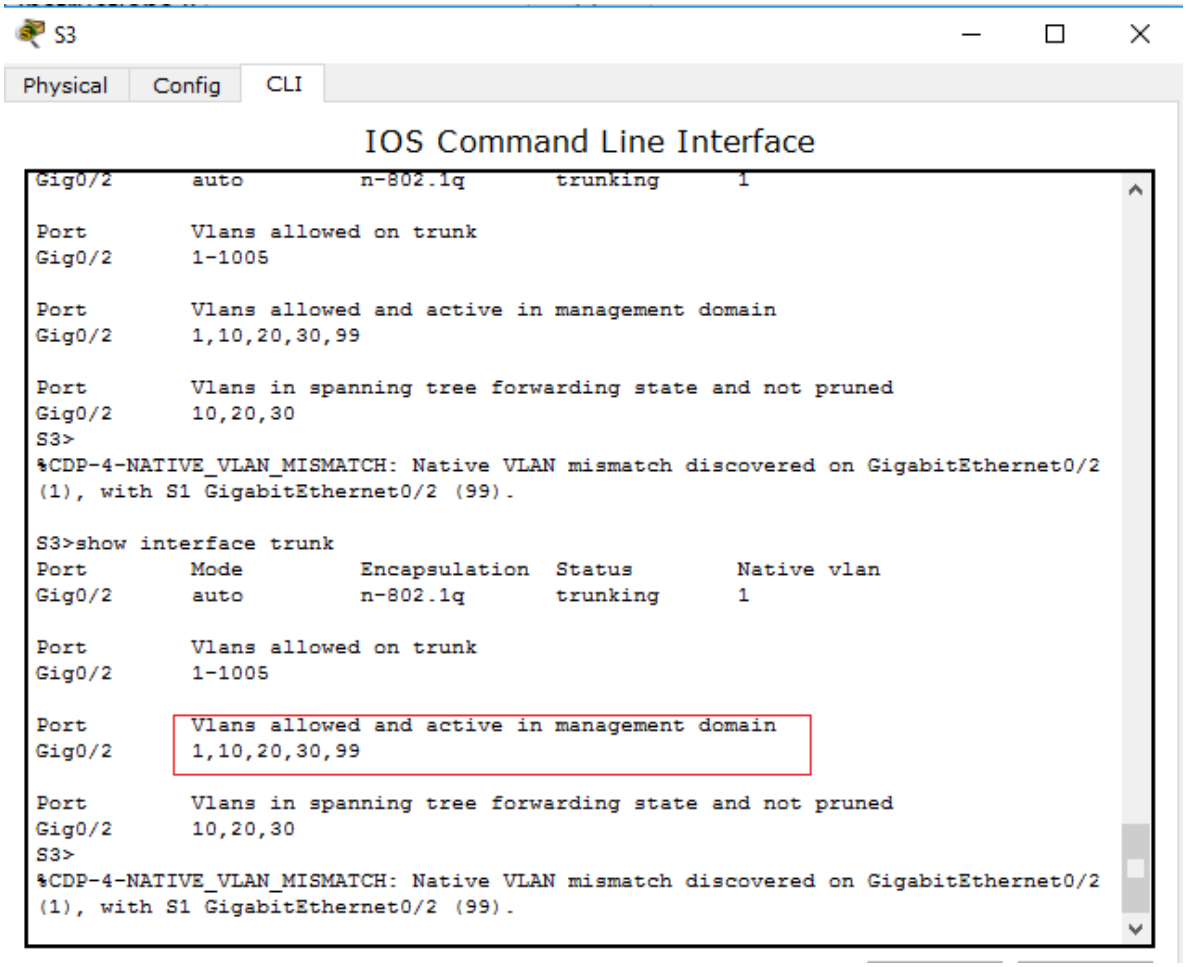
Verify trunking is enabled on S2 and S3.

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?




```
S2#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Gig0/1      1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10,20,30
S2#
```

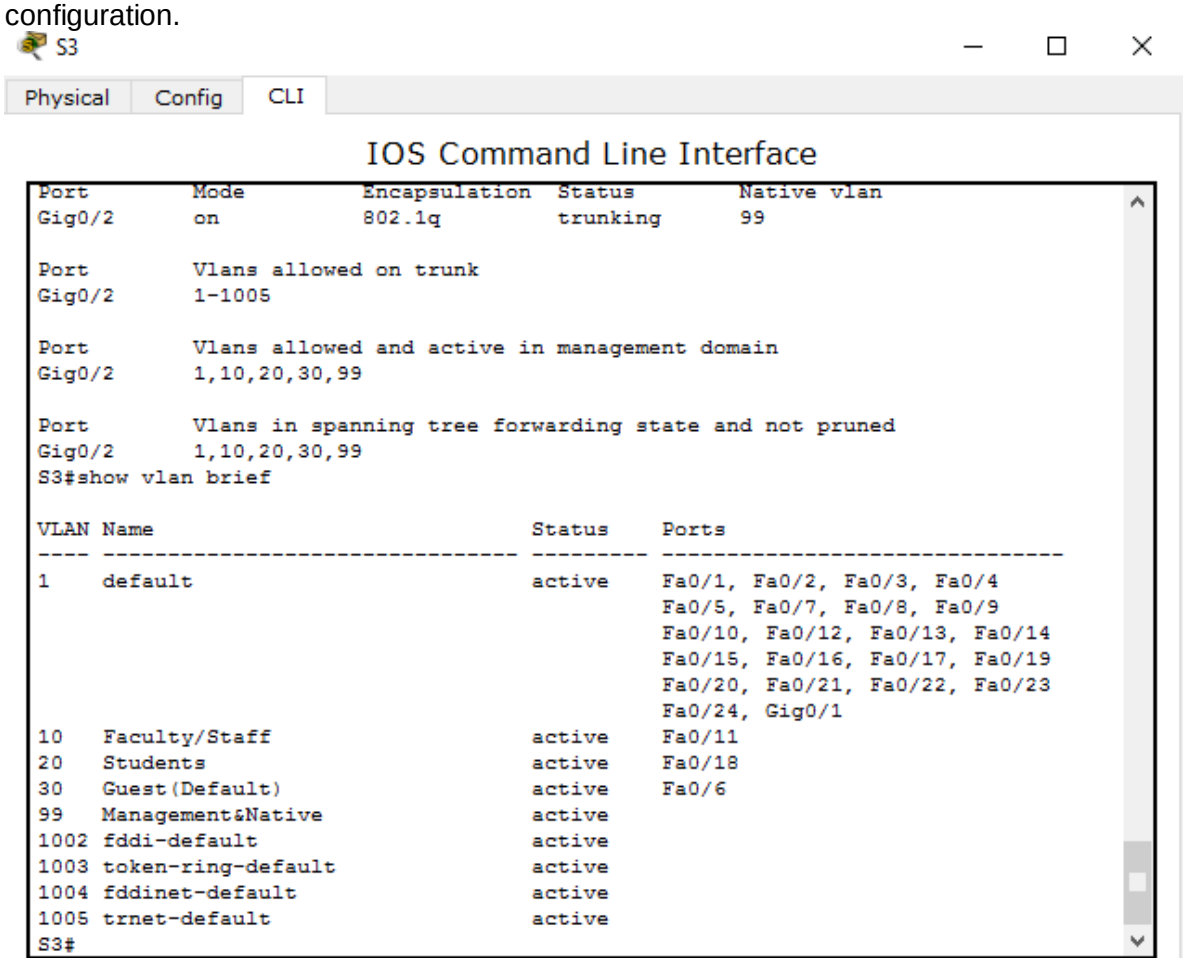


Step 2: Correct the native VLAN mismatch on S2 and S3.

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

```
S3#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/2      on           802.1q         trunking      99

Port        Vlans allowed on trunk
Gig0/2      1-1005

Port        Vlans allowed and active in management domain
Gig0/2      1,10,20,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/2      1,10,20,30,99
S3#
```

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



Step 3: Verify configurations on S2 and S3.

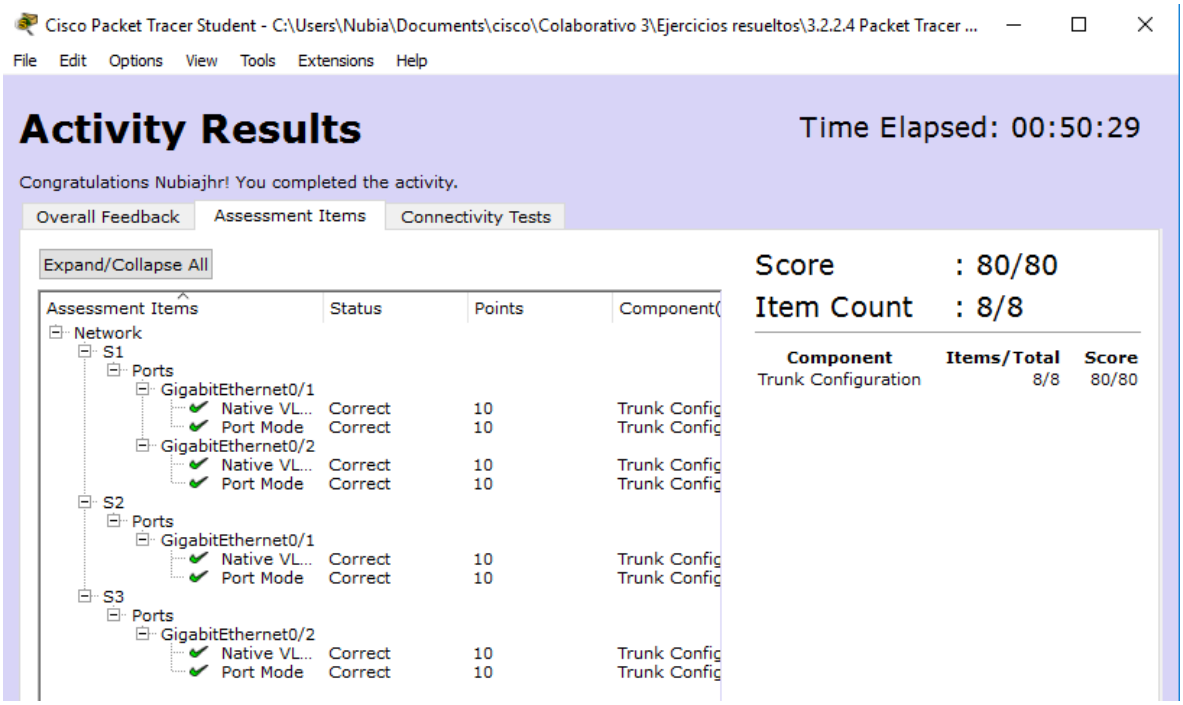
a. Issue the **show interface** *interface* **switchport** command to verify that the native VLAN is now 99.

```
S2>enable
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, 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, Gig0/2
10   Faculty/Staff                     active    Fa0/11
20   Students                          active    Fa0/18
30   Guest(Default)                    active    Fa0/6
99   Management&Native                 active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S2#
```

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?

Suggested Scoring Rubric

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



Informe No. 4

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

Addressing Table

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

Objectives

Part 1: Test Connectivity without Inter-VLAN Routing

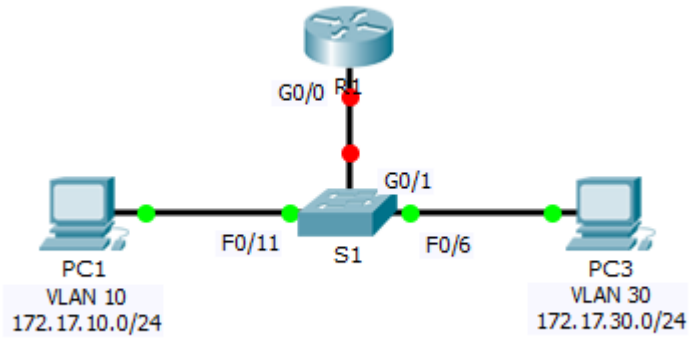
Part 2: Add VLANs to a Switch

Part 3: Configure Subinterfaces

Part 4: Test Connectivity with Inter-VLAN Routing

Scenario

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

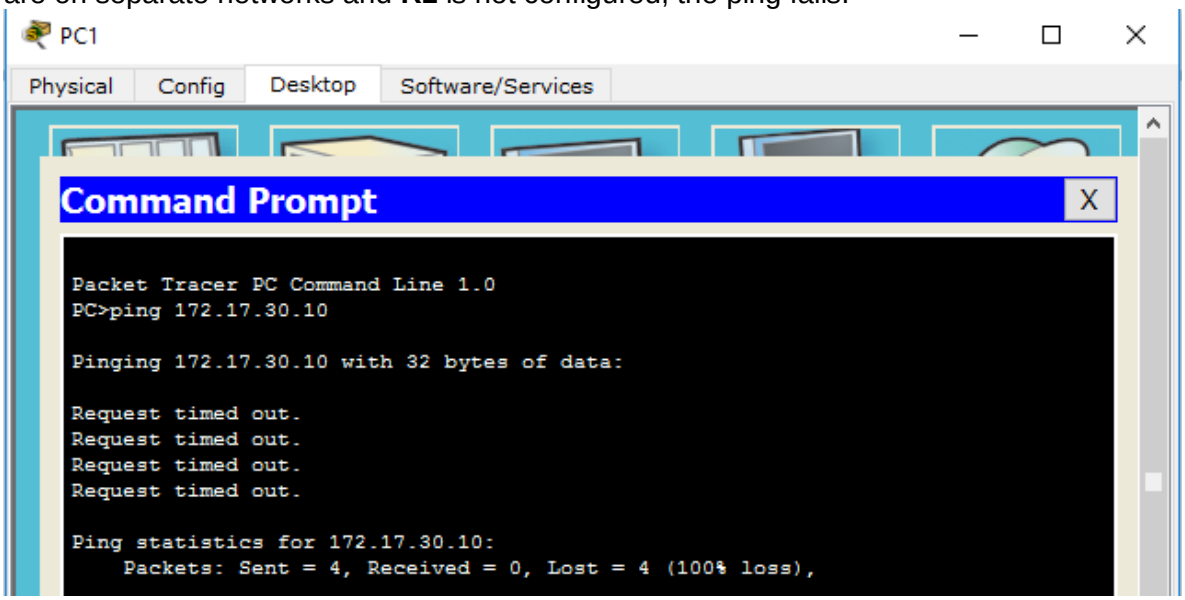


Part 1: Test Connectivity Without Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

Wait for switch convergence or click **Fast Forward Time** a few times. When the link lights are green for **PC1** and **PC3**, ping between **PC1** and **PC3**. Because the two PCs

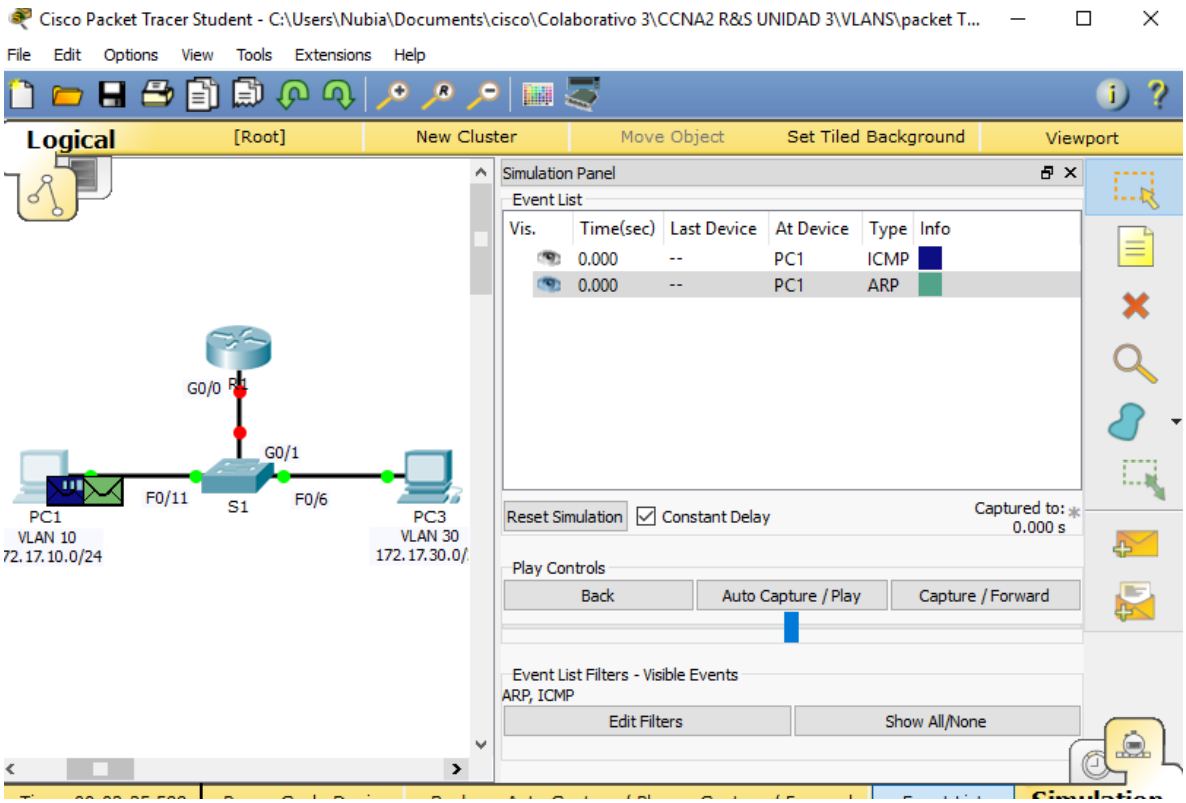
are on separate networks and **R1** is not configured, the ping fails.



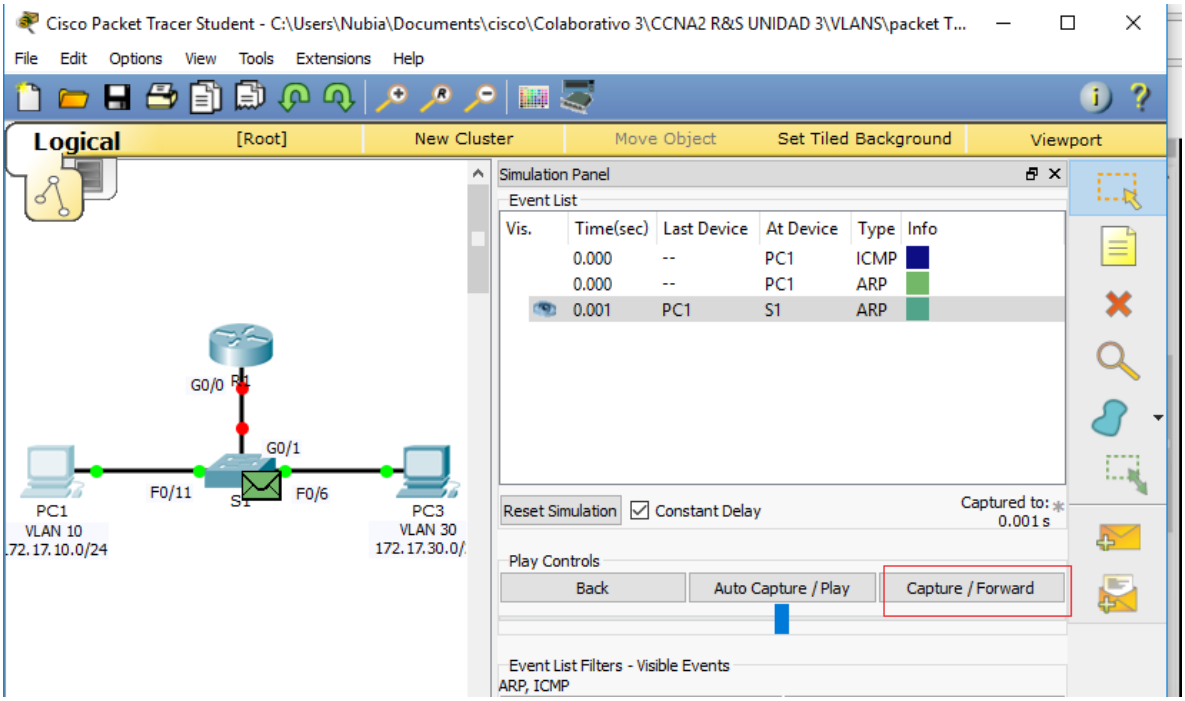
Ping fallido

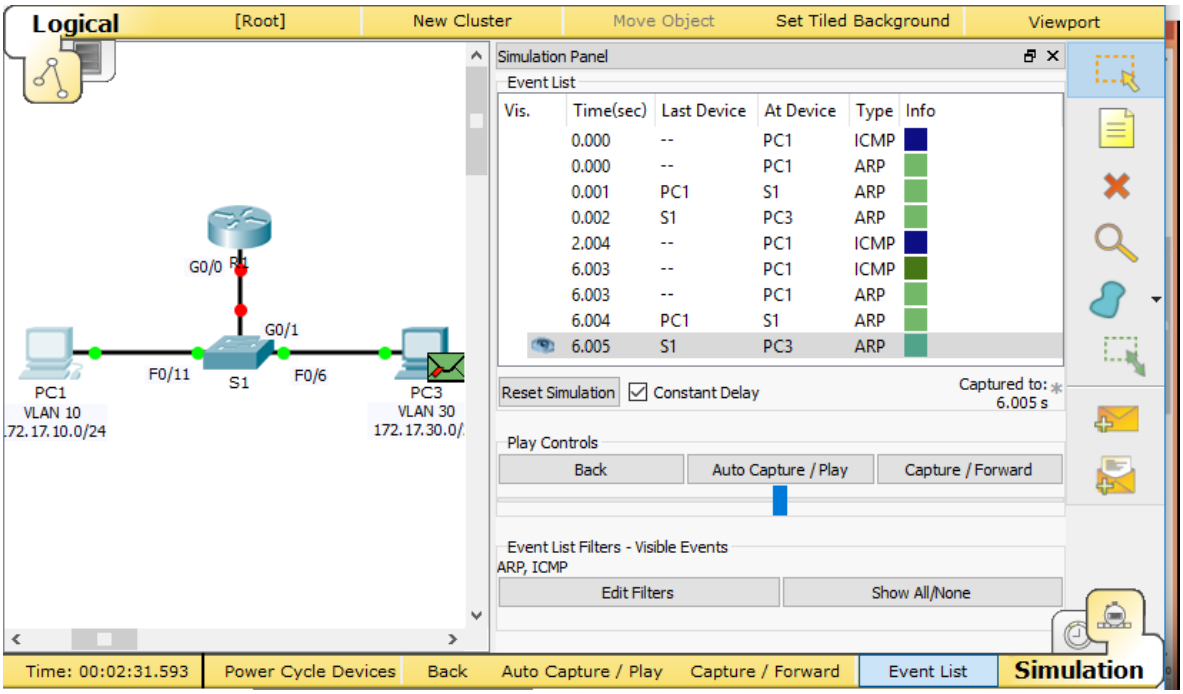
Step 2: Switch to Simulation mode to monitor pings.

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



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





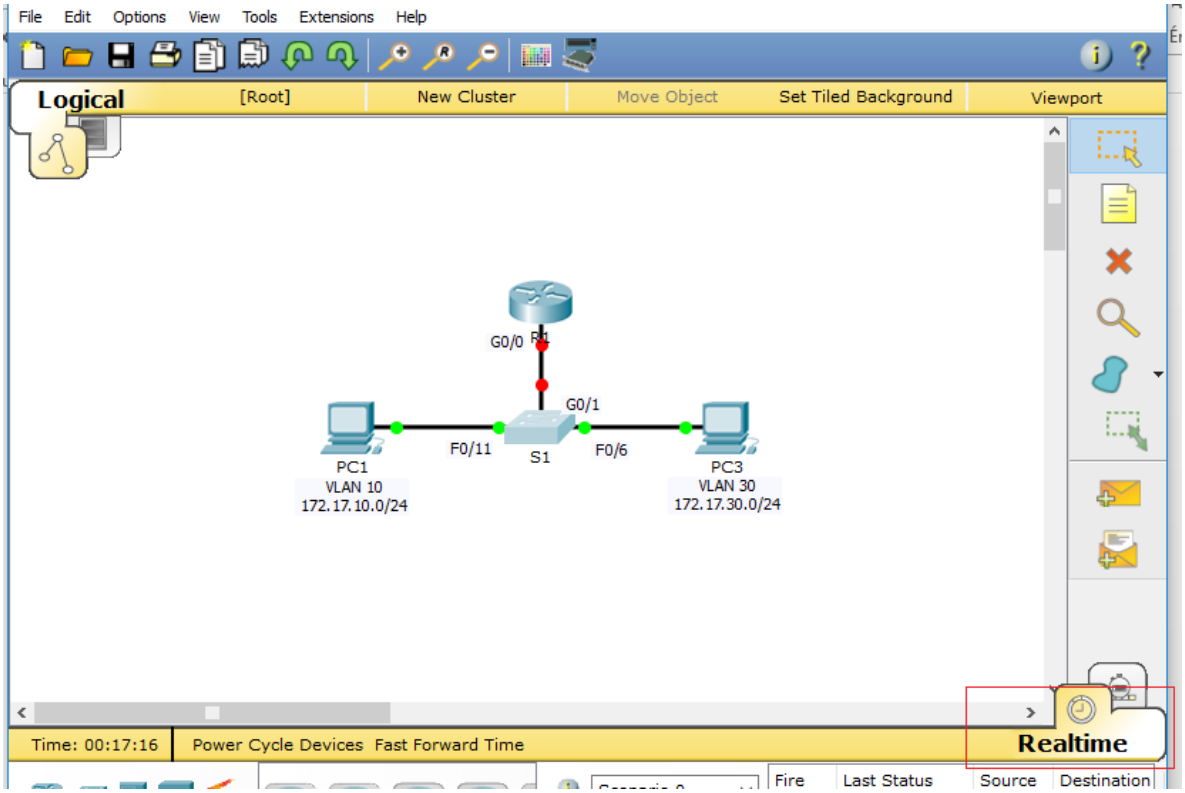
El ping nunca llega a PC1

Falla por que la PC1 está en otra red diferente que en la PC3, al estar en otra red en la capa 3 no pueden hacer ping

Part 2: Add VLANs to a Switch

Step 1: Create VLANs on S1.

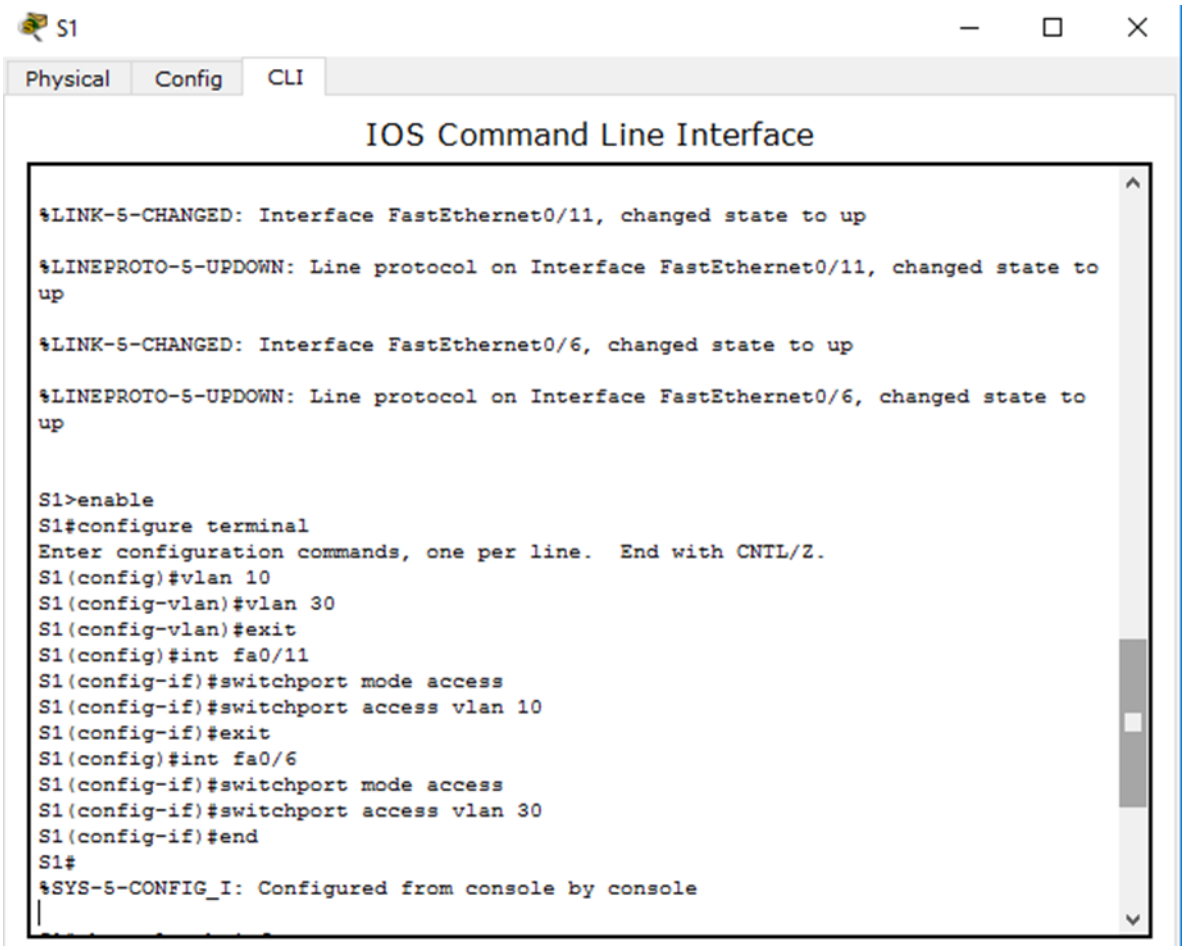
Return to **Realtime** mode and create VLAN 10 and VLAN 30 on**S1**.



Step 2: Assign VLANs to ports.

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

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



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

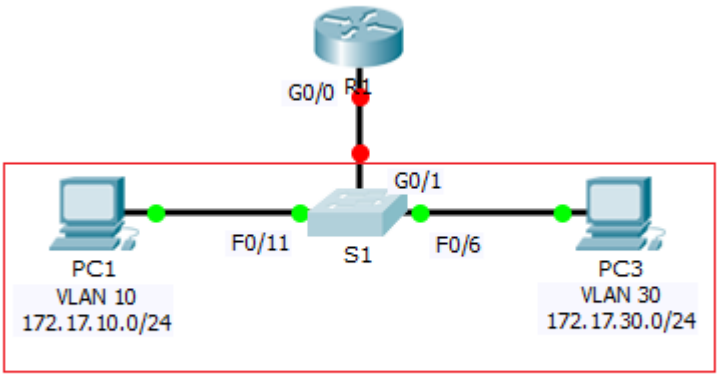
S1# **show vlan brief**

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/11
30   VLAN0030                          active    Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/11
30   VLAN0030                          active    Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S1#
```

Step 3: Test connectivity between PC1 and PC3.

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



Los led están en verde

```
PC>ping 172.17.30.10

Pinging 172.17.30.10 with 32 bytes of data:

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

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

PC>
```

Ping fallido no son satisfactorios

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.

```
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
```

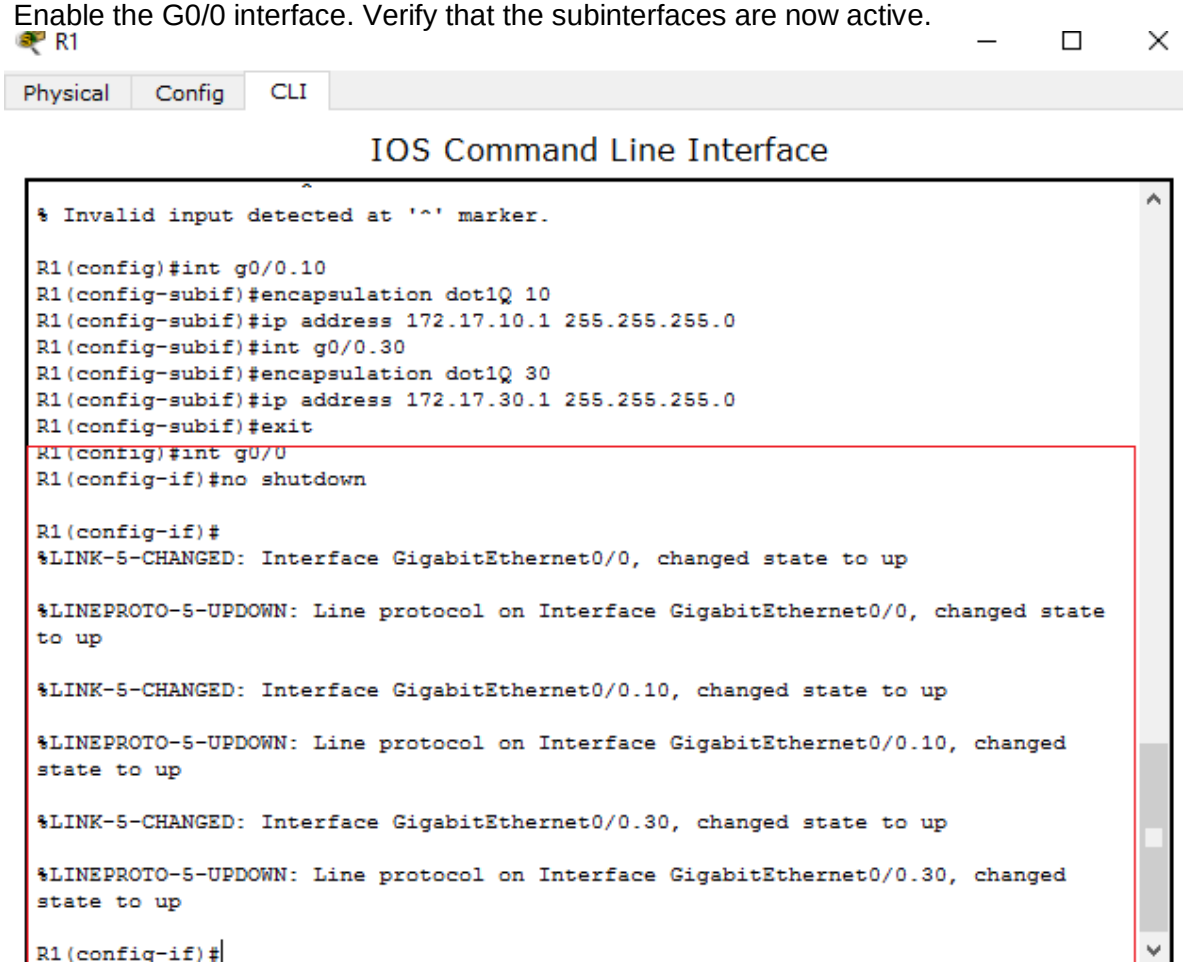
c. Repeat for the G0/0.30 subinterface.

```
R1(config-subif)#int g0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#
```

Step 2: Verify Configuration.

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

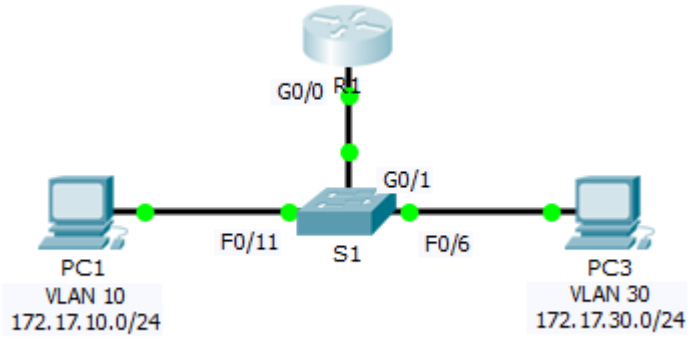
b. Enable the G0/0 interface. Verify that the subinterfaces are now active.



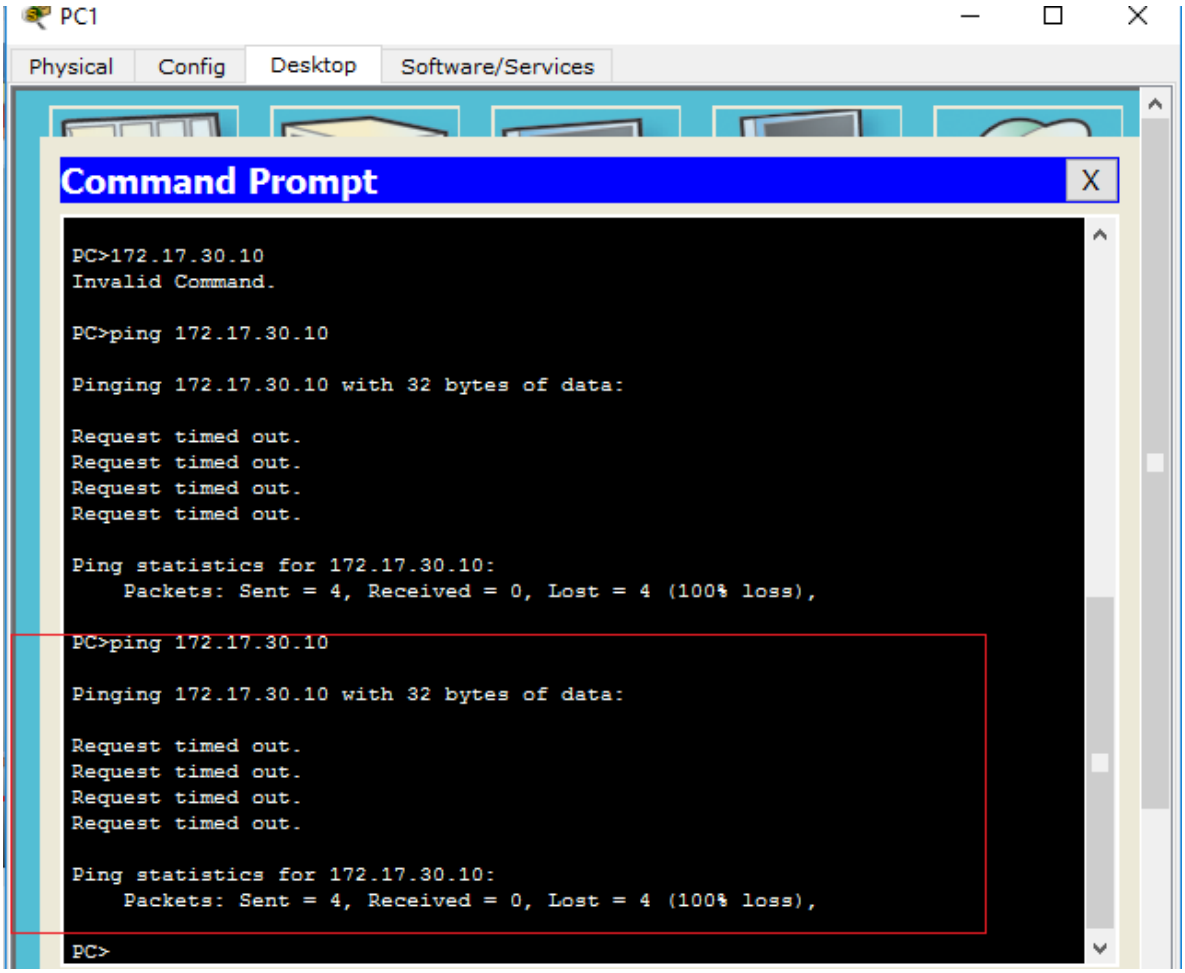
Part 4: Test Connectivity with Inter-VLAN Routing

Step 1: Ping between PC1 and PC3.

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



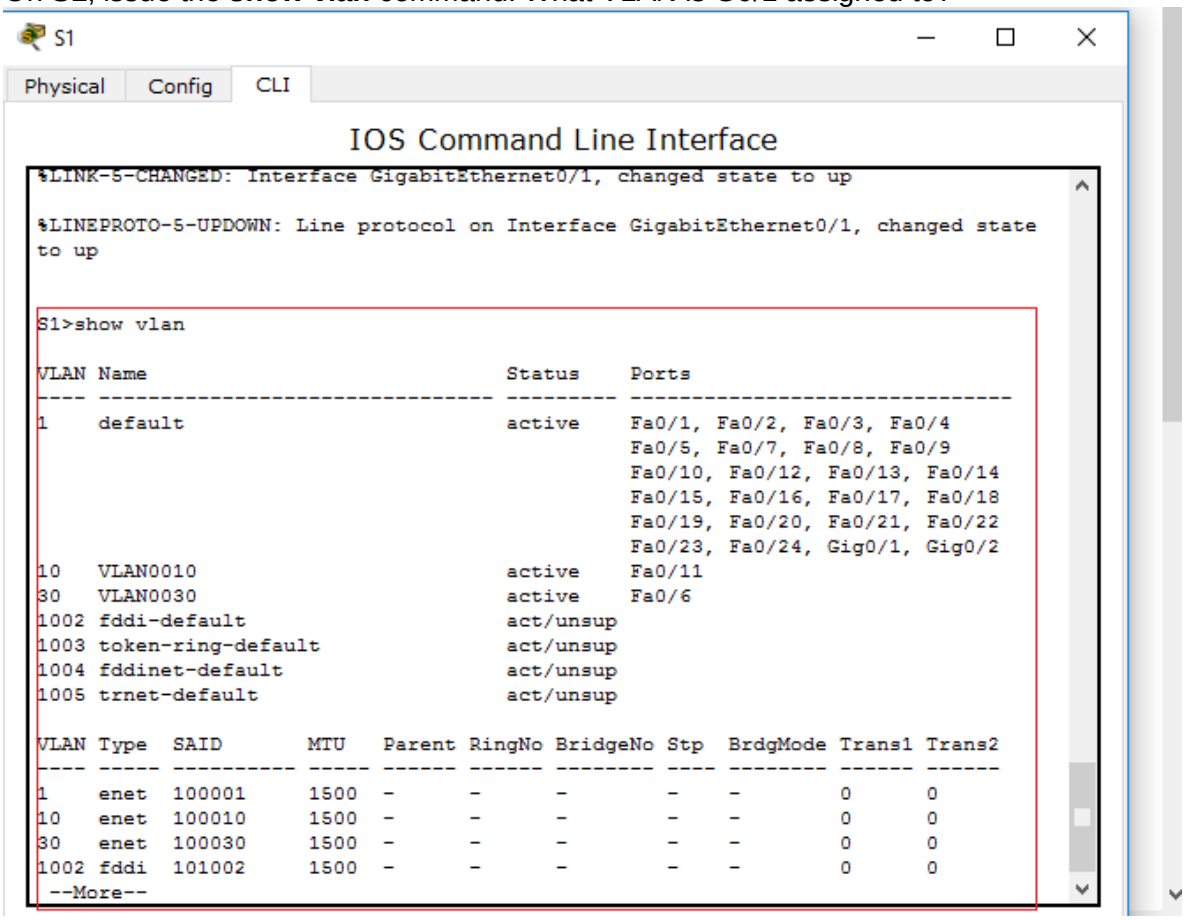
Los led están verdes



Ping fallido

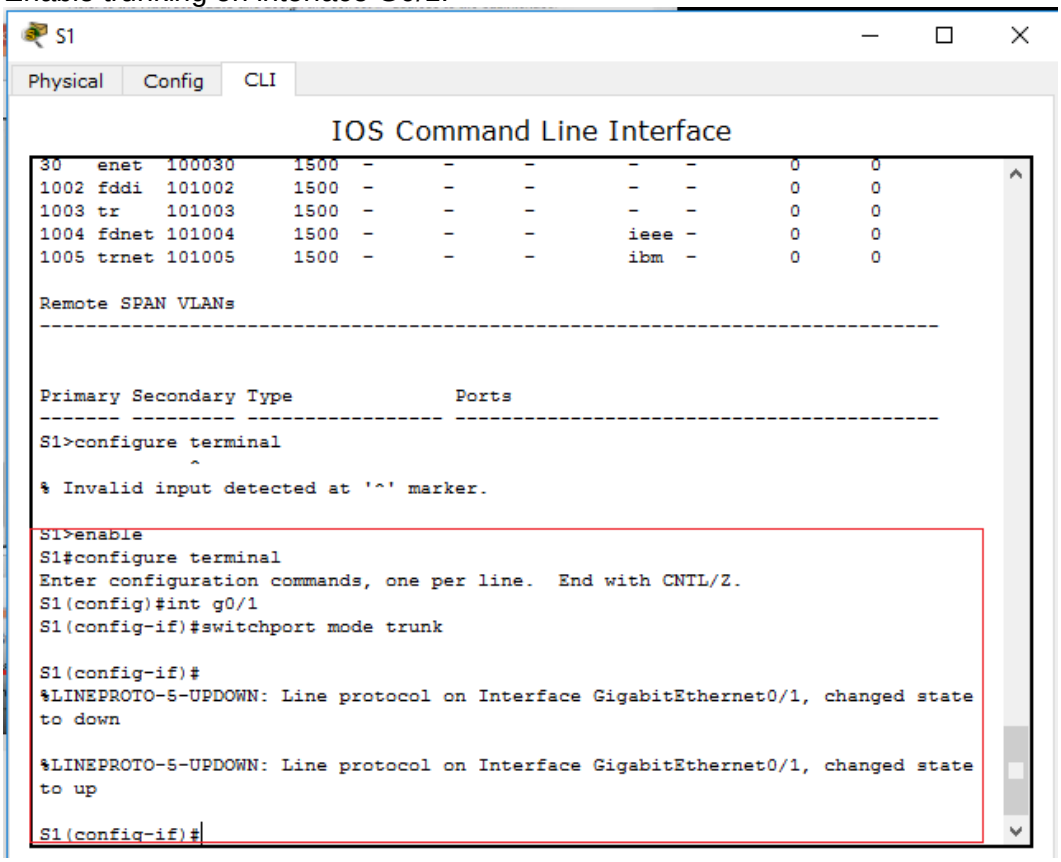
Step 2: Enable trunking.

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

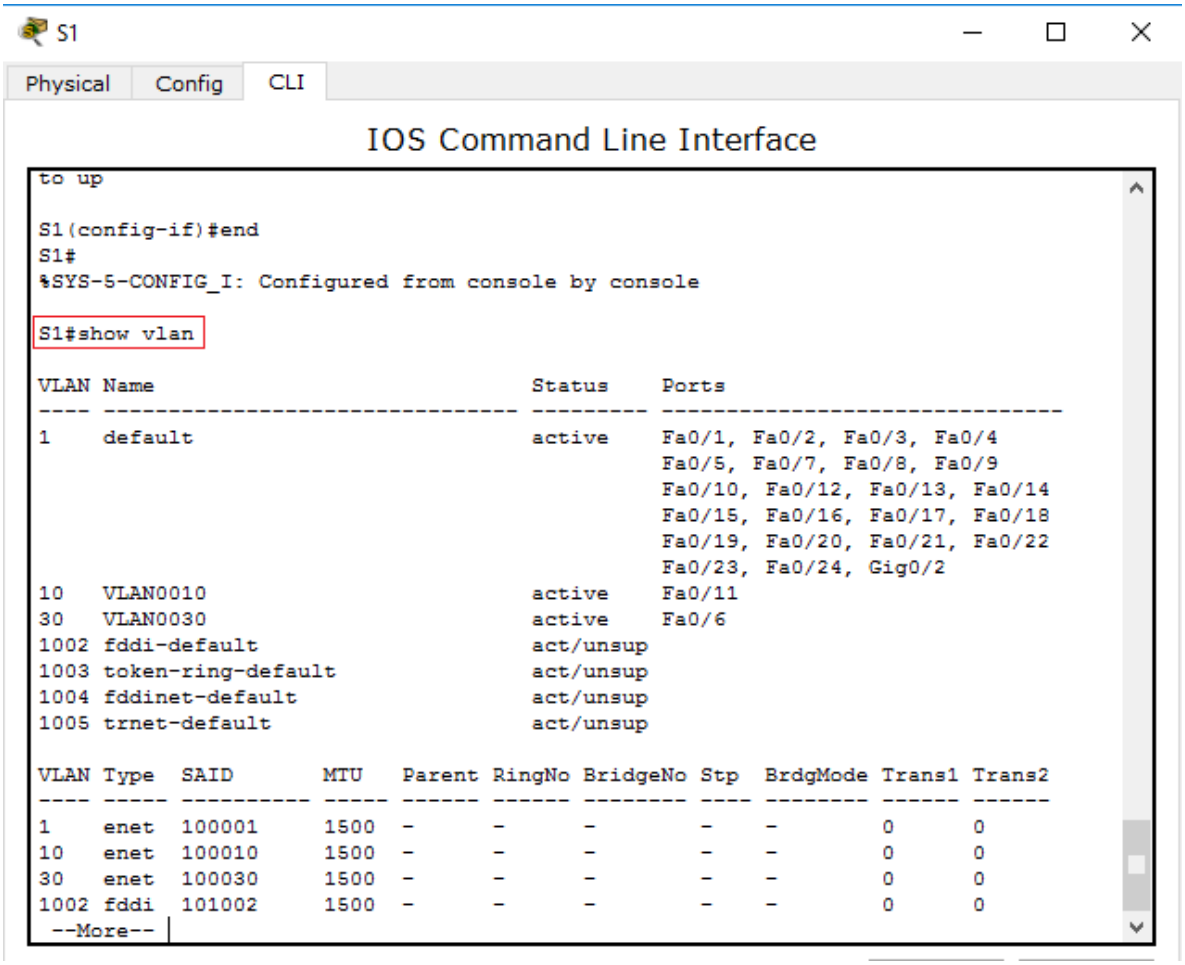


b. Because the router was configured with multiple subinterfaces assigned to different VLANs, the switch port connecting to the router must be configured as a trunk.

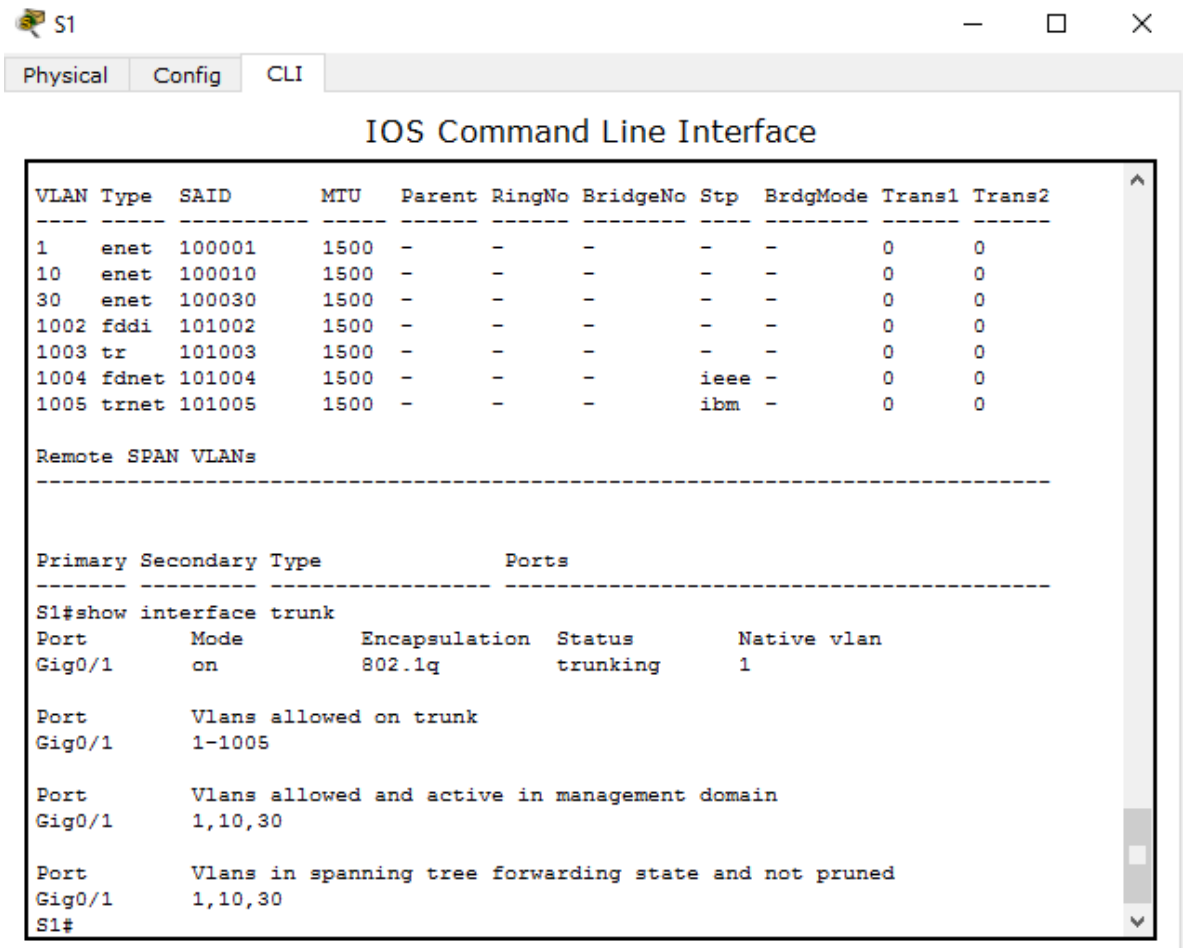
Enable trunking on interface G0/1.

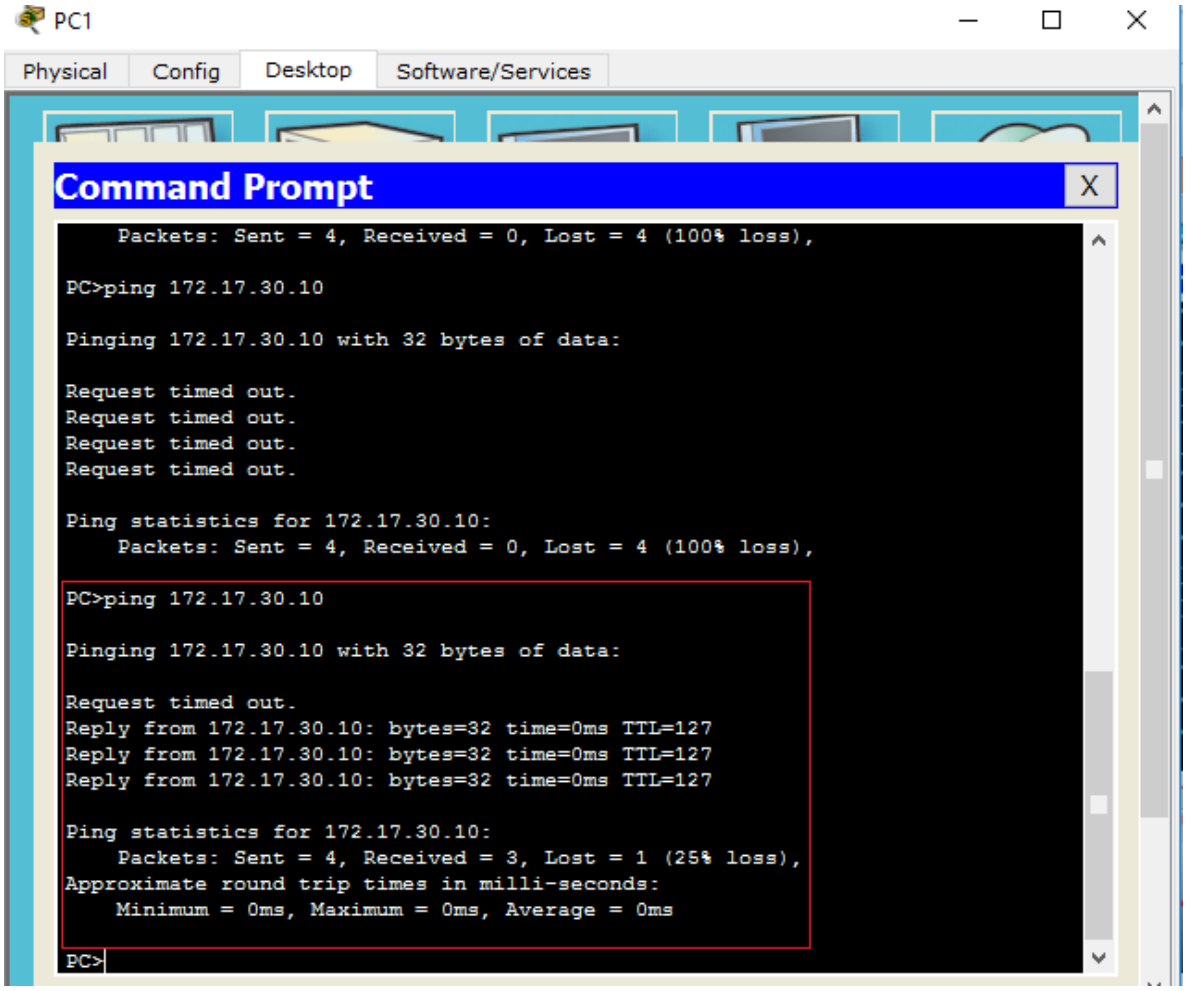


c. How can you determine that the interface is a trunk port using the **show vlan** command?



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

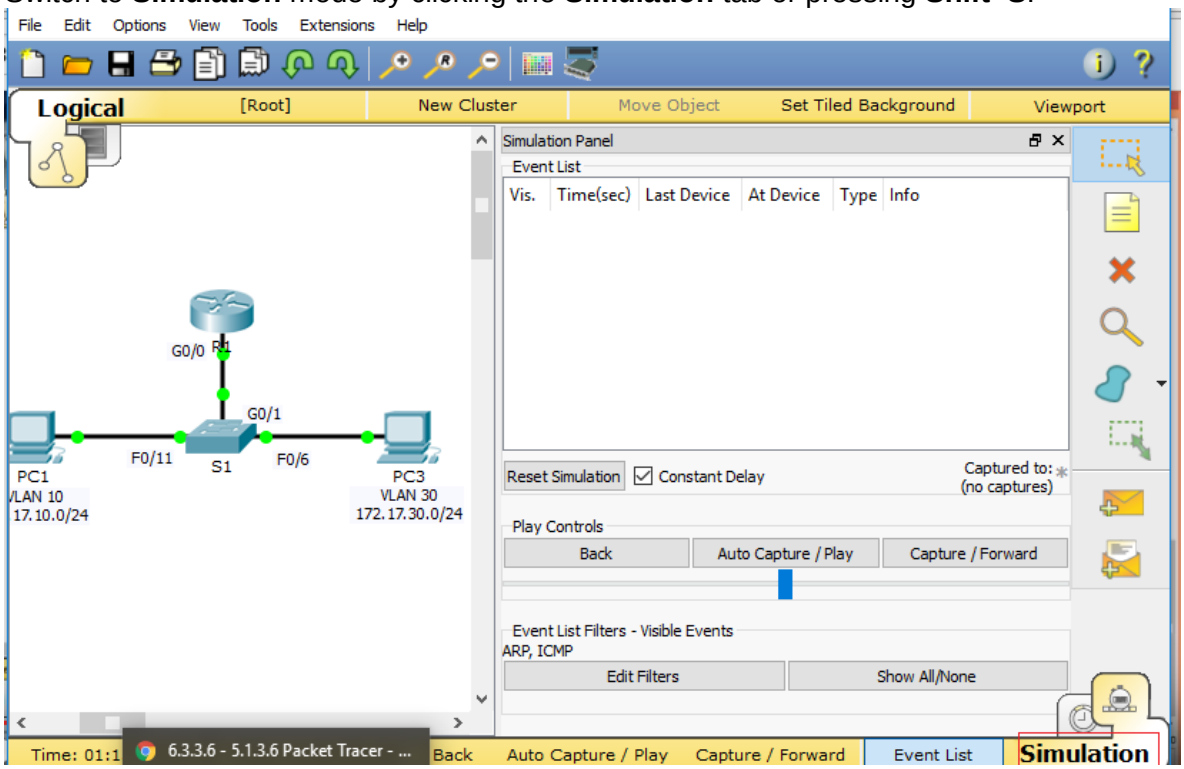

S1
Physical
Config
CLI
IOS Command Line Interface
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
30 enet 100030 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
Remote SPAN VLANs
Primary Secondary Type Ports
S1#show interface trunk
Port Mode Encapsulation Status Native vlan
Gig0/1 on 802.1q trunking 1
Port Vlans allowed on trunk
Gig0/1 1-1005
Port Vlans allowed and active in management domain
Gig0/1 1,10,30
Port Vlans in spanning tree forwarding state and not pruned
Gig0/1 1,10,30
S1#



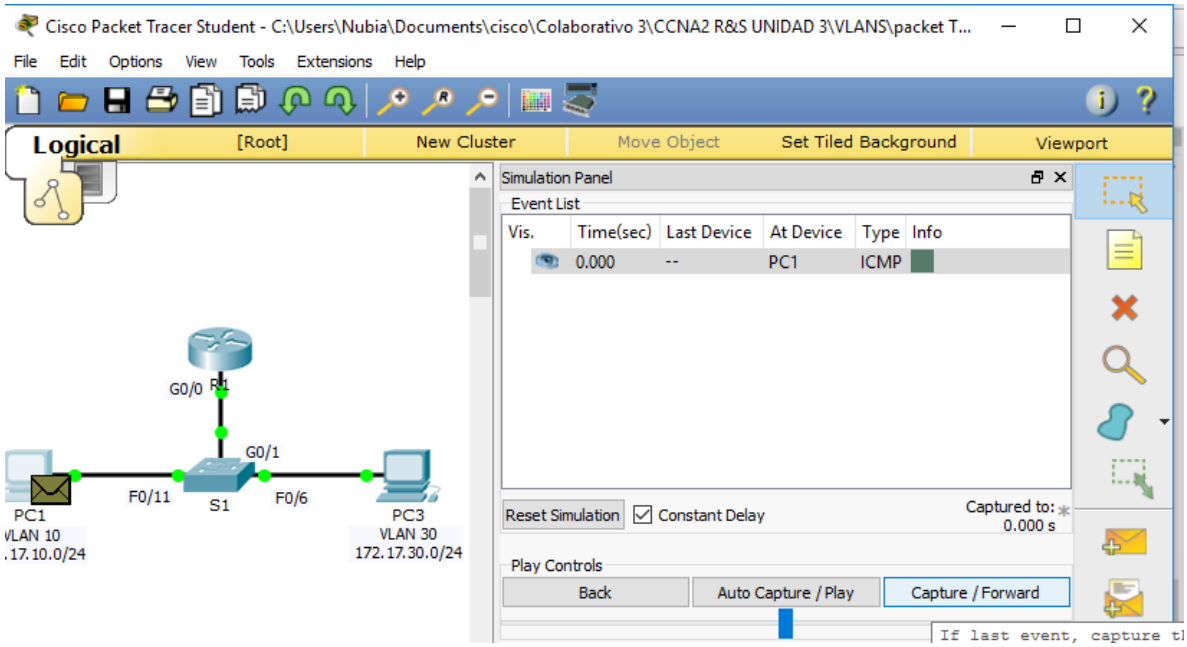
Ping satisfactorio

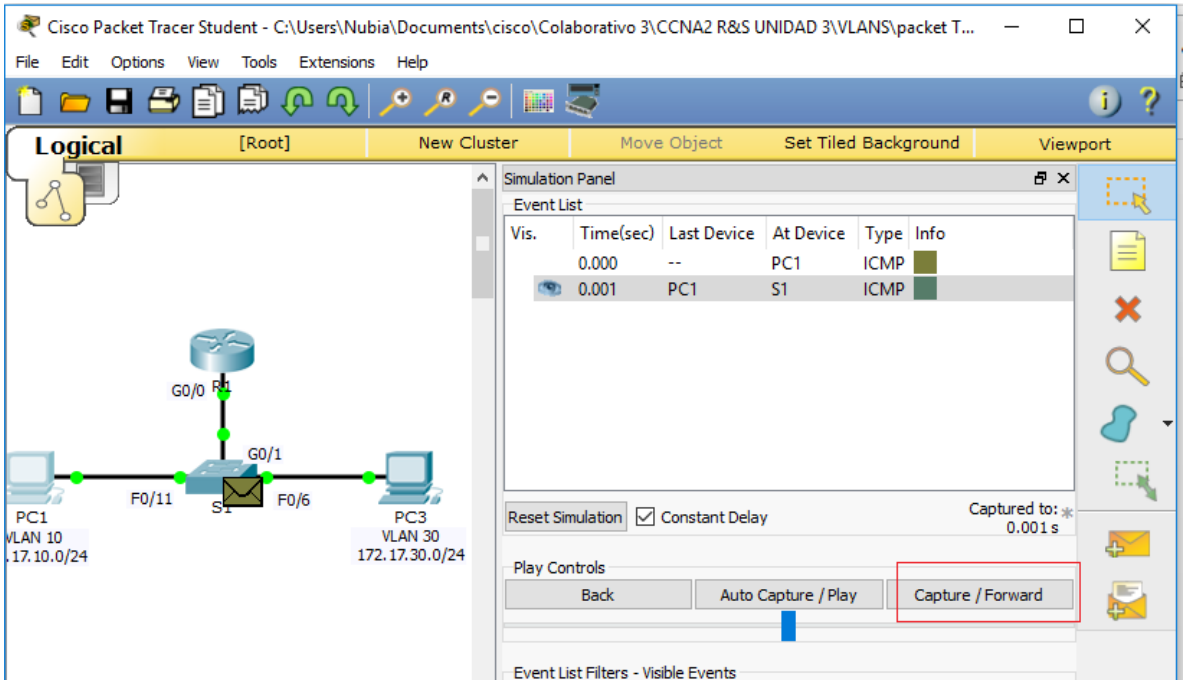
Step 3: Switch to Simulation mode to monitor pings.

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

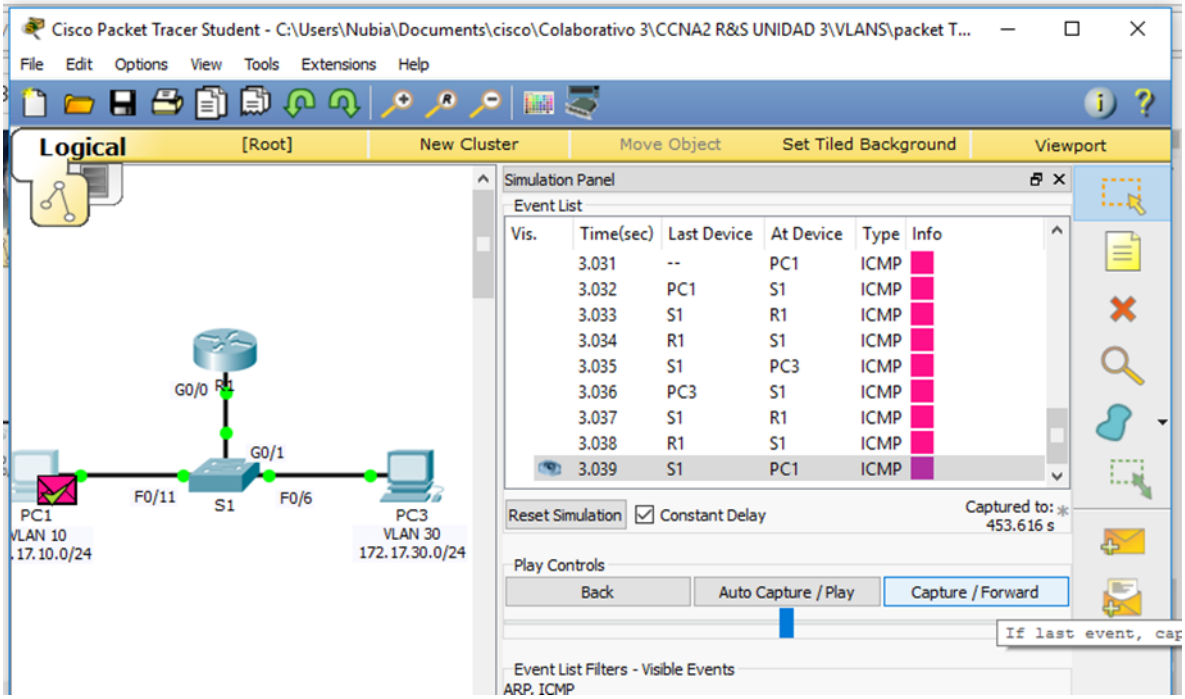


b. Click **Capture/Forward** to see the steps the ping takes between **PC1** and **PC3**.





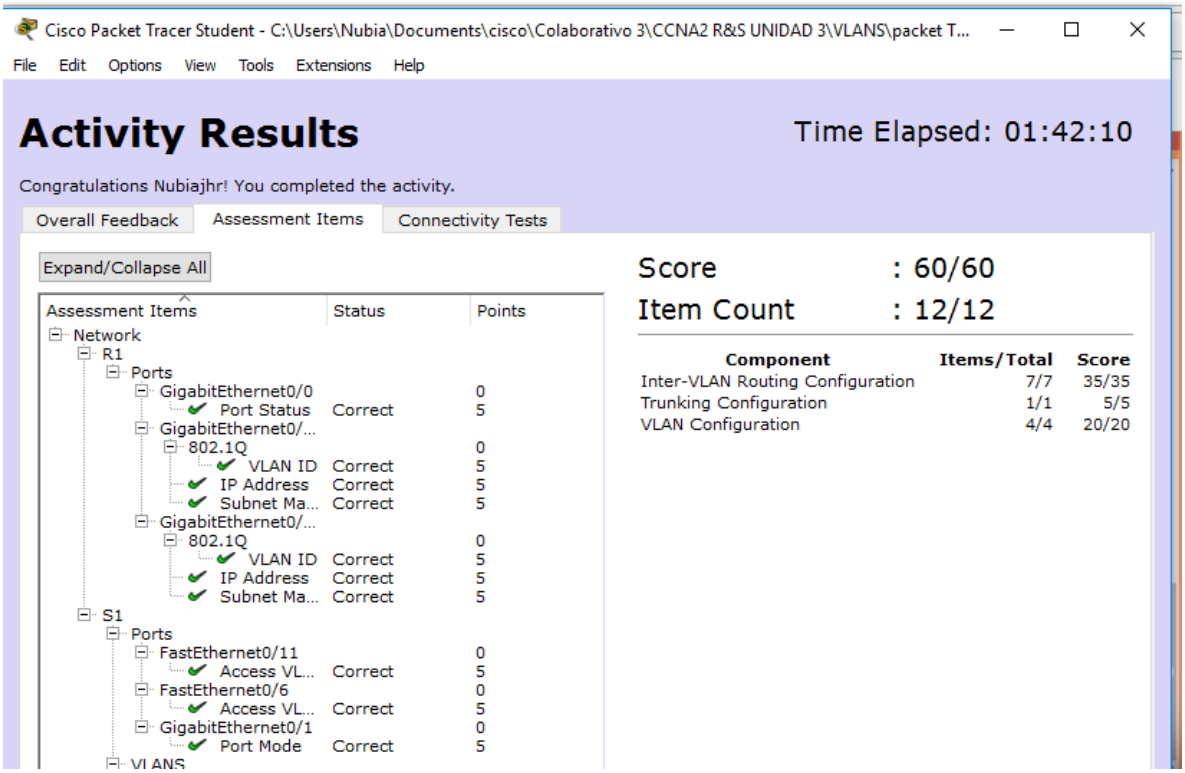
b. You should see ARP requests and replies between **S1** and**R1**. Then ARP requests and replies between **R1** and **S3**. Then **PC1** can encapsulate an ICMP echo request with the proper data-link layer information and R1 will route the request to **PC3**.



Note: After the ARP process finishes, you may need to click Reset Simulation to see the ICMP process complete.

Suggested Scoring Rubric

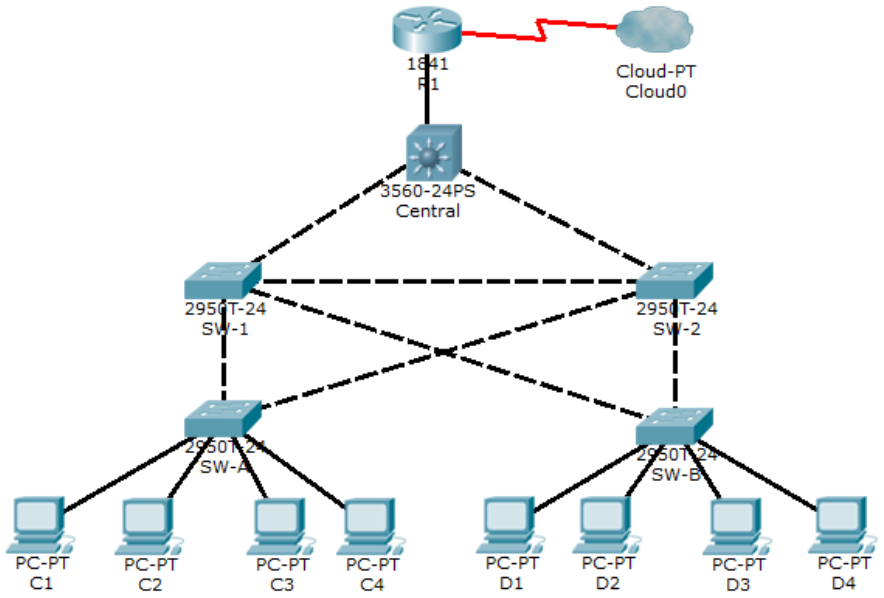
Packet Tracer scores 60 points. The four questions are worth 10 points each.



Informe No. 5

6.5.1.2: Packet Tracer - Layer 2 Security

Topology



Objectives

- Assign the Central switch as the root bridge.
- Secure spanning-tree parameters to prevent STP manipulation attacks.
- Enable storm control to prevent broadcast storms.
- Enable port security to prevent MAC address table overflow attacks.

Background / Scenario

There have been a number of attacks on the network recently. For this reason, the network administrator has assigned you the task of configuring Layer 2 security.

For optimum performance and security, the administrator would like to ensure that the root bridge is the 3560 Central switch. To prevent against spanning-tree manipulation attacks, the administrator wants to ensure that the STP parameters are secure. In addition, the network administrator would like to enable storm control to prevent broadcast storms. Finally, to prevent against MAC address table overflow attacks, the network administrator has decided to configure port security to limit the number of MAC addresses that can be learned per switch port. If the number of MAC addresses exceeds the set limit, the administrator would like the port to be shutdown.

All switch devices have been preconfigured with the following:

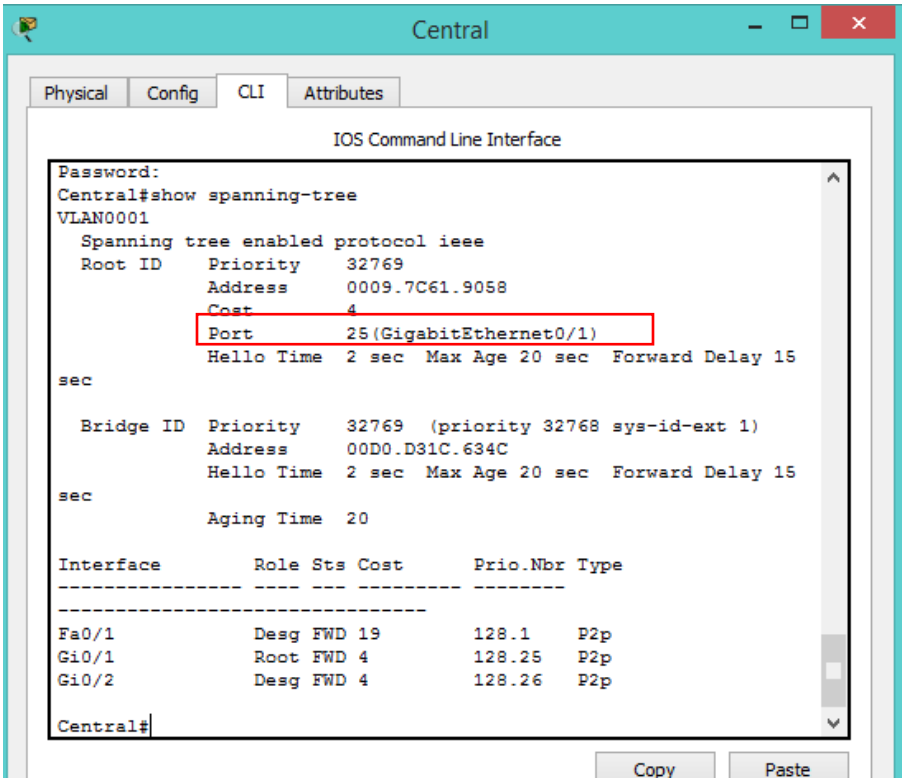
- Enable password: **ciscoenpa55**
- Console password: **ciscoconpa55**

- VTY line password: **ciscovtypa55**

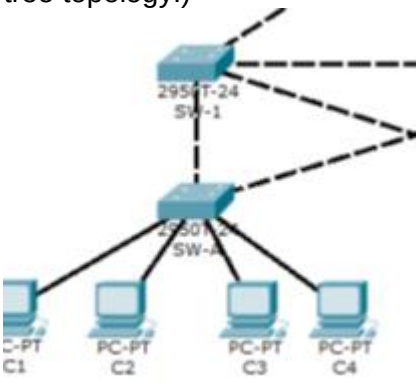
Part 1: Configure Root Bridge

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?
Current root is SW-1

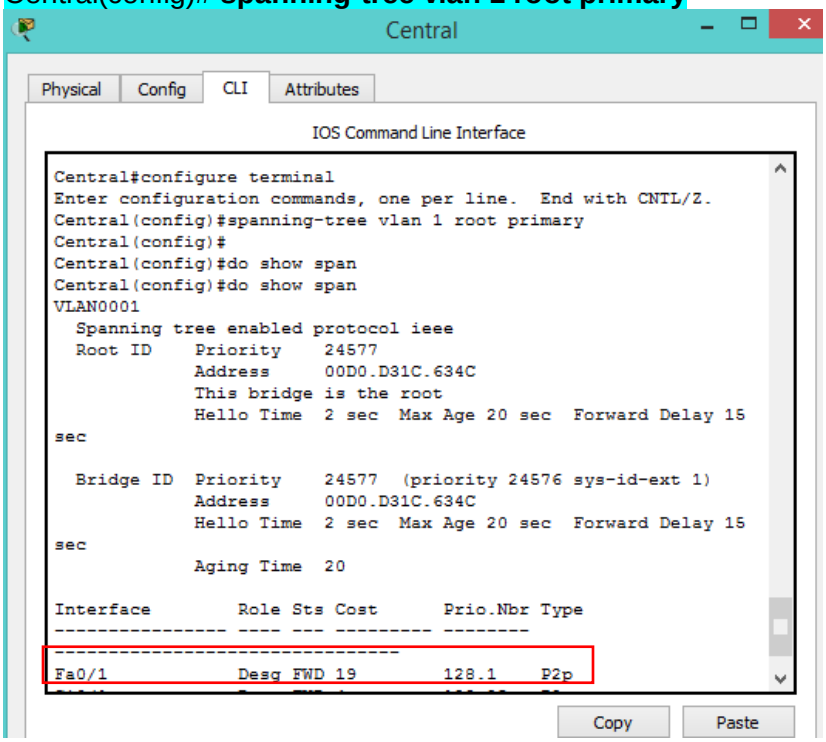


Based on the current root bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)



Step 2: Assign Central as the primary root bridge.
Using the **spanning-tree vlan 1 root primary** command, assign **Central** as the root bridge.

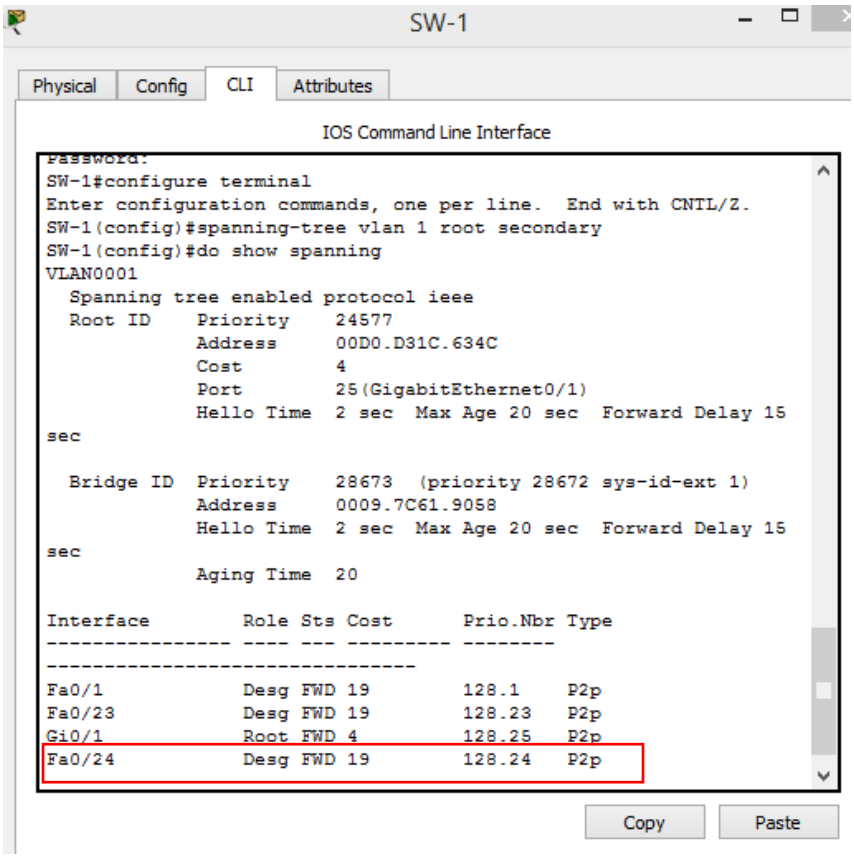
Central(config)# **spanning-tree vlan 1 root primary**



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?
Current root is Central

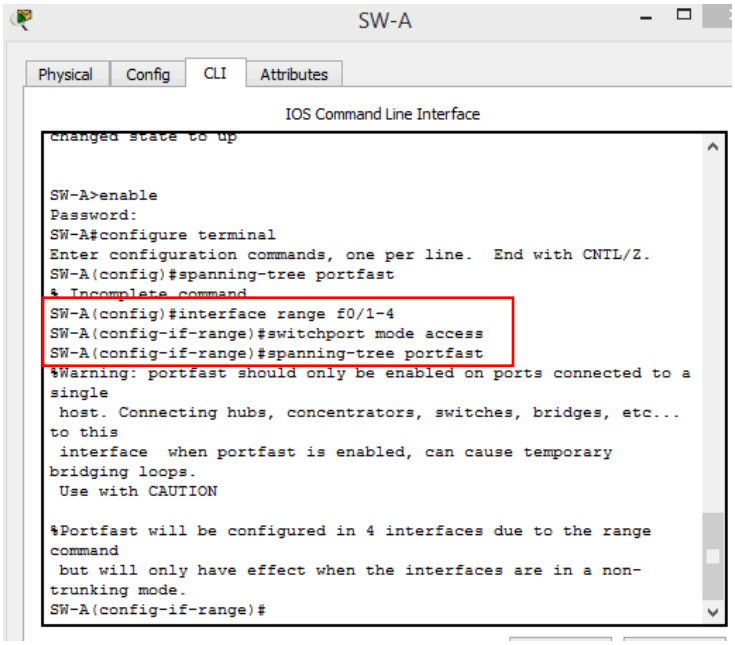
```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     00D0.D31C.634C
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
---
```

Based on the new root-bridge, what is the resulting spanning tree? (Draw the spanning-tree topology.)

Part 2: Protect Against STP Attacks
Secure the STP parameters to prevent STP manipulation attacks.

Step 1: Enable PortFast on all access ports.
PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly. On the connected access ports of the **SW-A** and **SW-B**, use the **spanning-tree portfast** command.
SW-A(config)# **interface range fastethernet 0/1 - 4**
SW-A(config-if-range)# **spanning-tree portfast**
SW-B(config)# **interface range fastethernet 0/1 - 4**

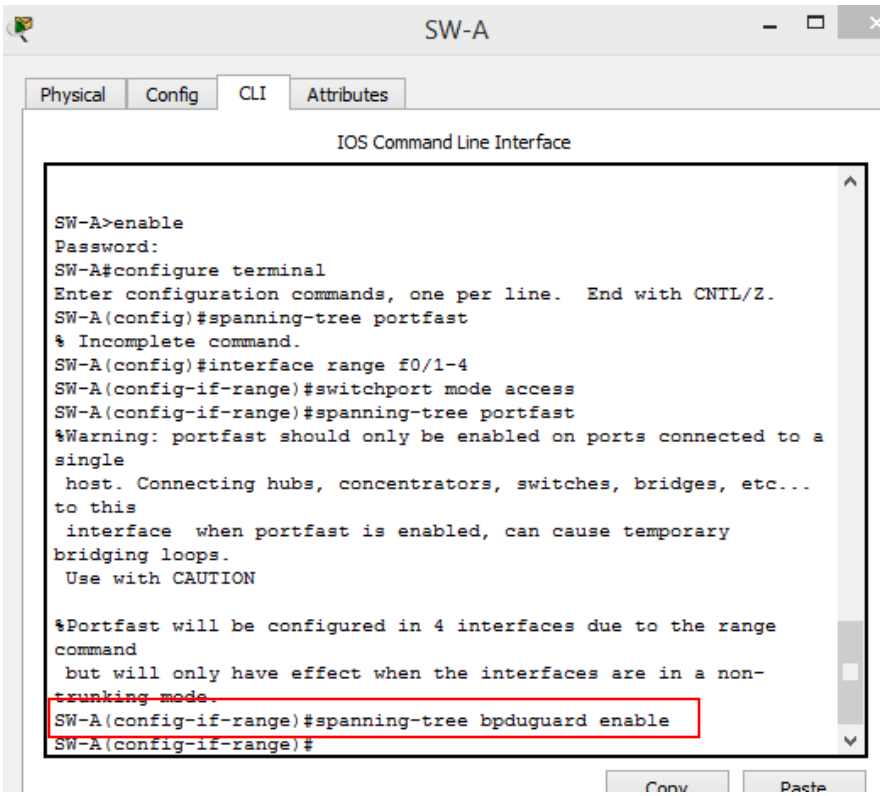
SW-B(config-if-range)# **spanning-tree portfast**

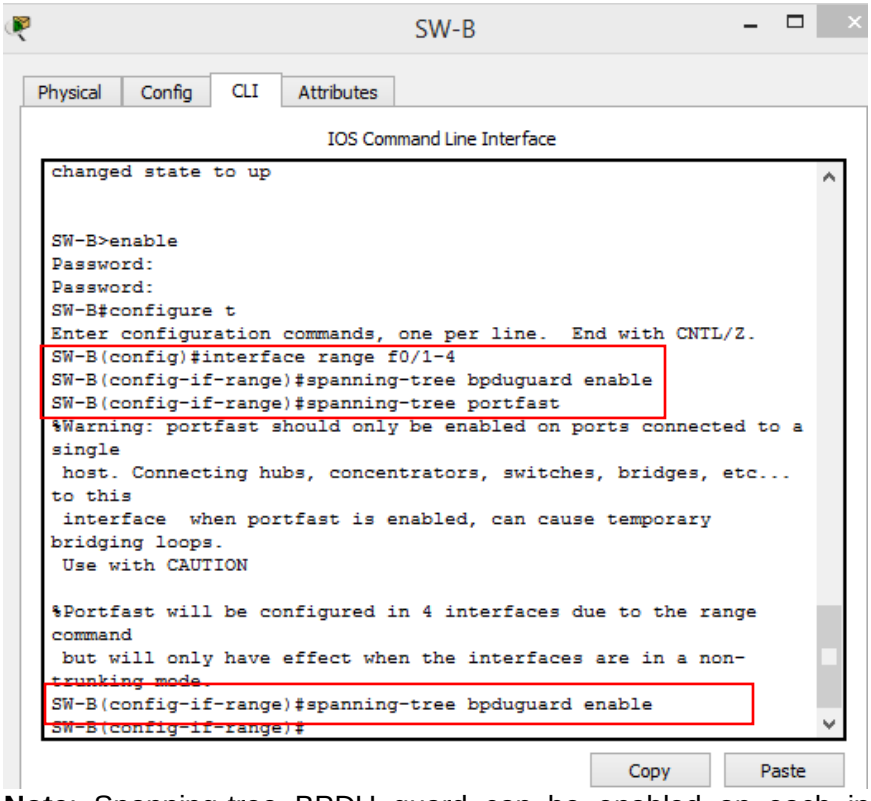


Step 2: Enable BPDU guard on all access ports.

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**
SW-B(config)# **interface range fastethernet 0/1 - 4**
SW-B(config-if-range)# **spanning-tree bpduguard enable**





Note: Spanning-tree BPDU guard can be enabled on each individual port using the **spanning-tree bpduguard enable** command in the interface configuration mode or the **spanning-tree portfast bpduguard default** command in the global configuration mode.

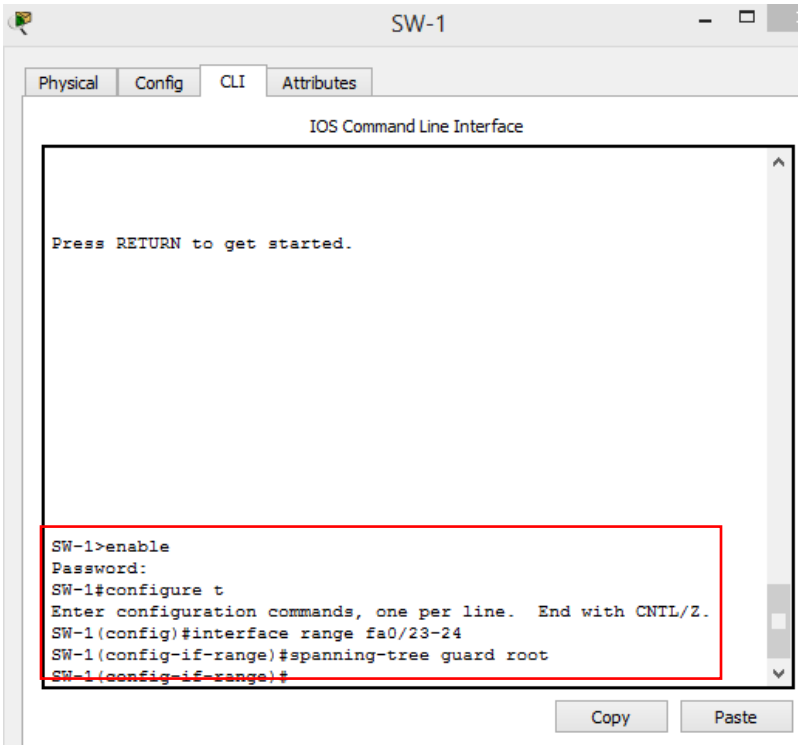
For grading purposes in this activity, please use the **spanning-tree bpduguard enable** command.

Step 3: Enable root guard.

Root guard can be enabled on all ports on a switch that are not root ports. It is best deployed on ports that connect to other non-root switches. Use the **show spanning-tree** command to determine the location of the root port on each switch.

On **SW-1**, enable root guard on ports Fa0/23 and Fa0/24. On **SW-2**, enable root guard on ports Fa0/23 and Fa0/24.

SW-1(config)# **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**



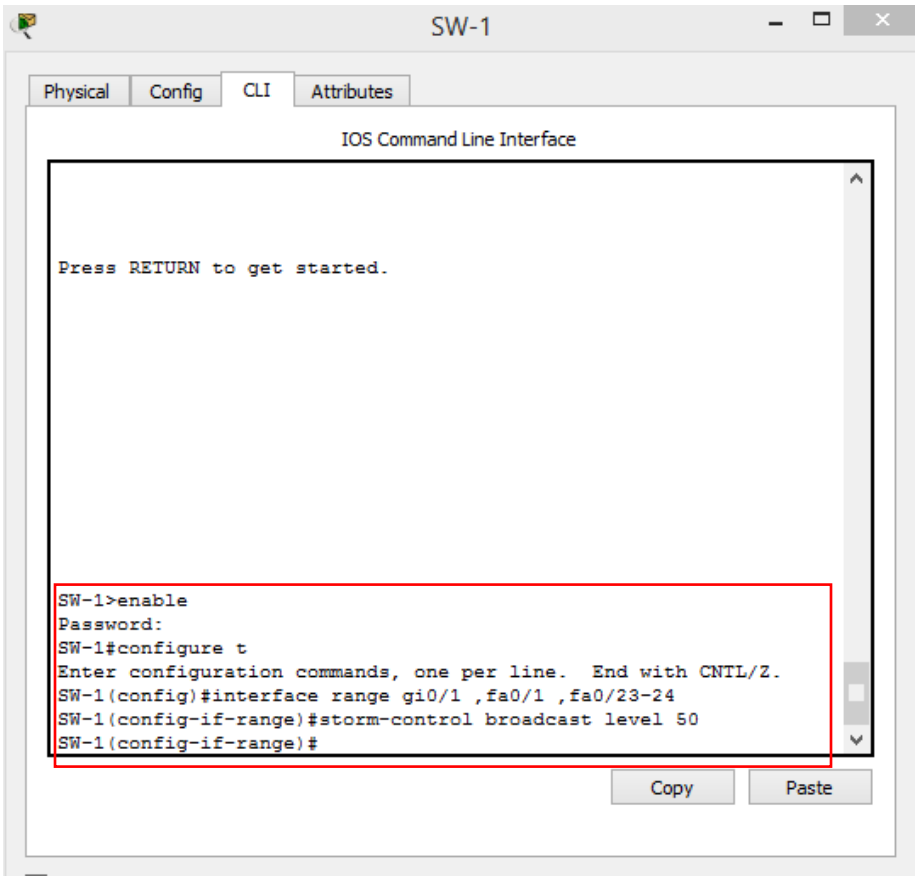
Part 3: Enable Storm Control

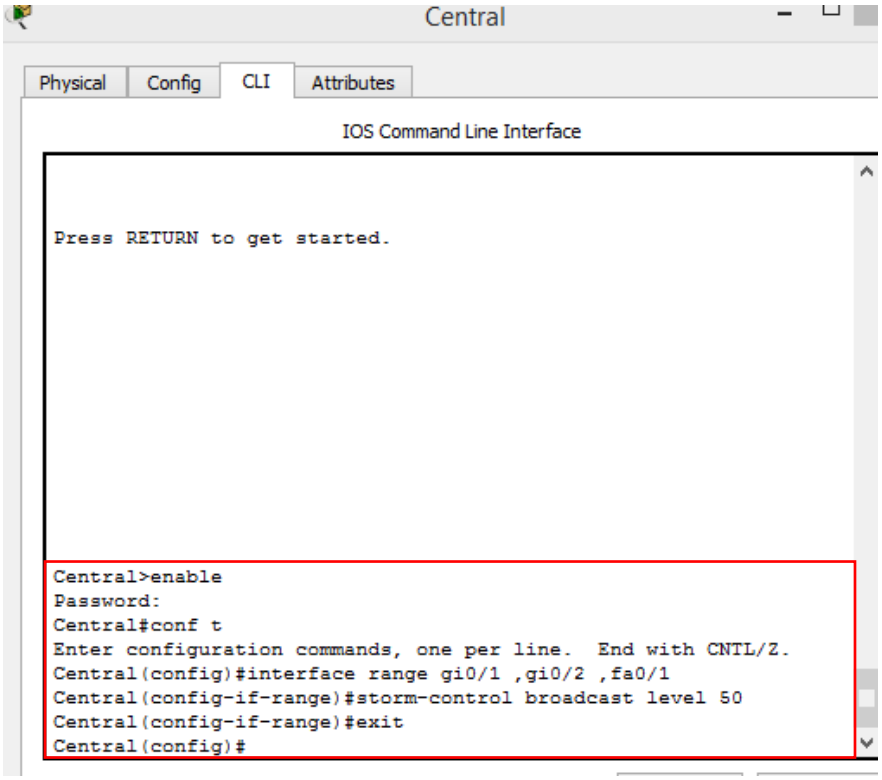
Step 1: Enable storm control for broadcasts.

a. Enable storm control for broadcasts on all ports connecting switches (trunk ports).

b. Enable storm control on interfaces connecting **Central**, **SW-1**, and **SW-2**. Set a **50** percent rising suppression level using the **storm-control broadcast** command.

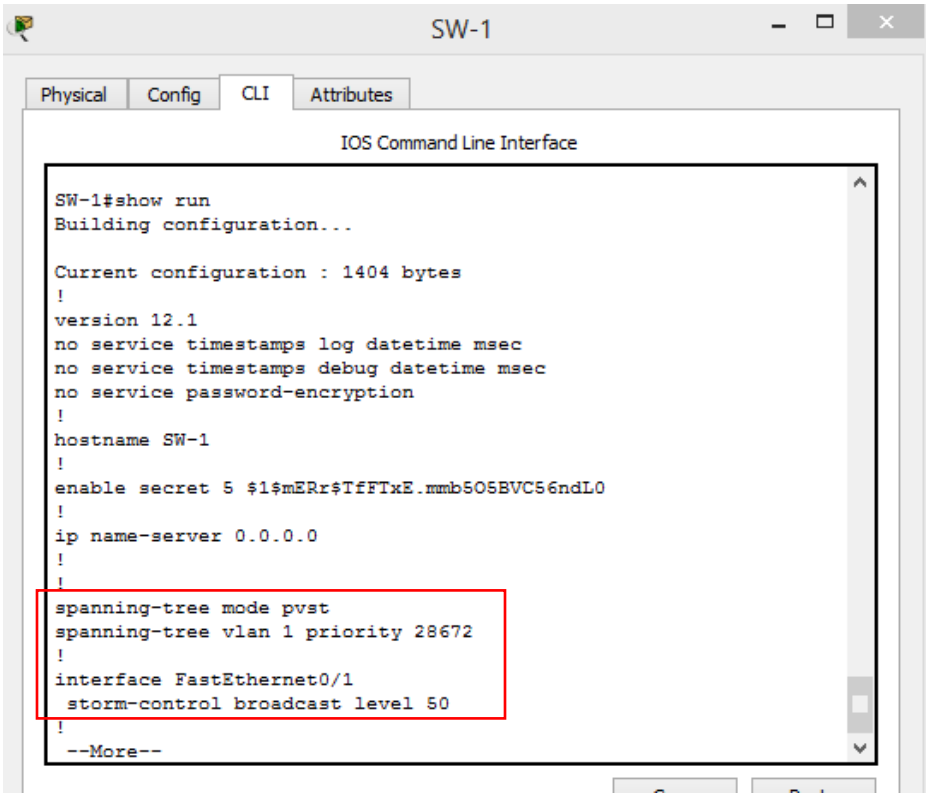
SW-1(config)# **interface range gi0/1 , fa0/1 , fa0/23 - 24**
SW-1(config-if)# **storm-control broadcast level 50**
SW-2(config)# **interface range gi0/1 , fa0/1 , fa0/23 - 24**
SW-2(config-if)# **storm-control broadcast level 50**
Central(config-if)# **interface range gi0/1 , gi0/2 , fa0/1**
Central(config-if)# **storm-control broadcast level 50**

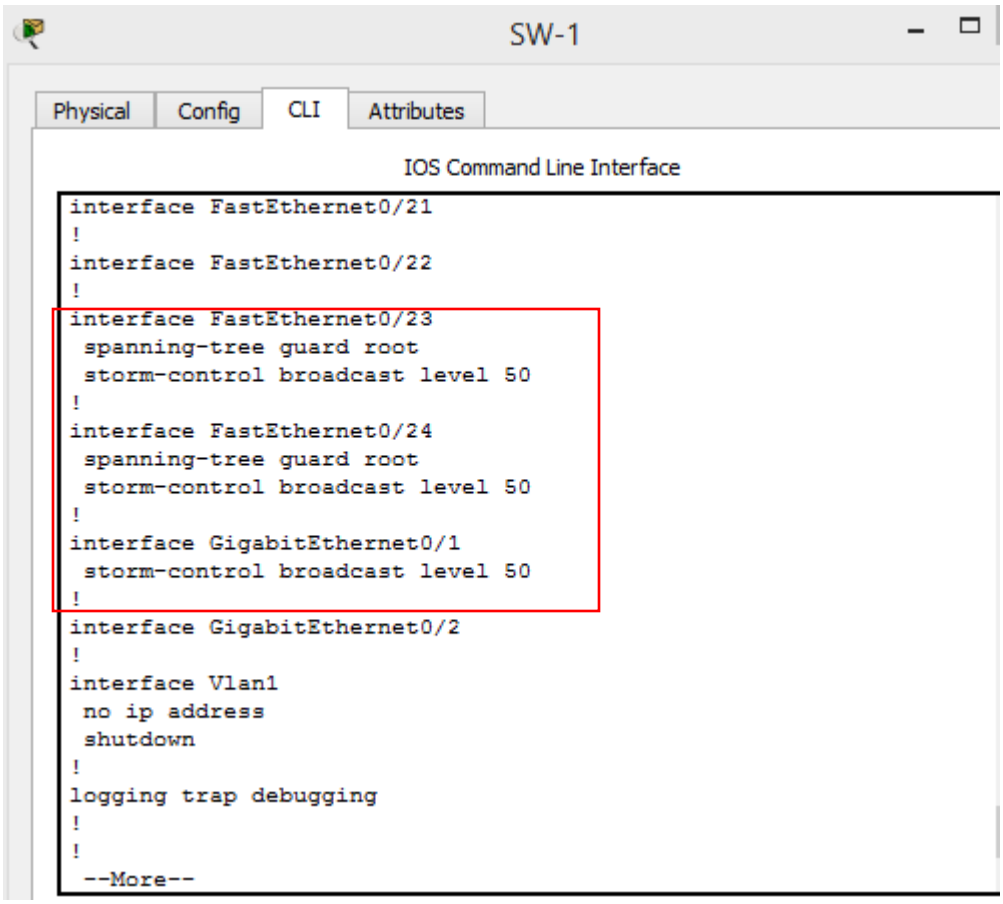

SW-1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
SW-1>enable
Password:
SW-1#configure t
Enter configuration commands, one per line. End with CNTL/Z.
SW-1(config)#interface range gi0/1 ,fa0/1 ,fa0/23-24
SW-1(config-if-range)#storm-control broadcast level 50
SW-1(config-if-range)#
Copy
Paste


Central
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
Central>enable
Password:
Central#conf 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)#exit
Central(config)#

Step 2: Verify storm control configuration.

Verify your configuration with the **show storm-control broadcast** and the **show run** commands.

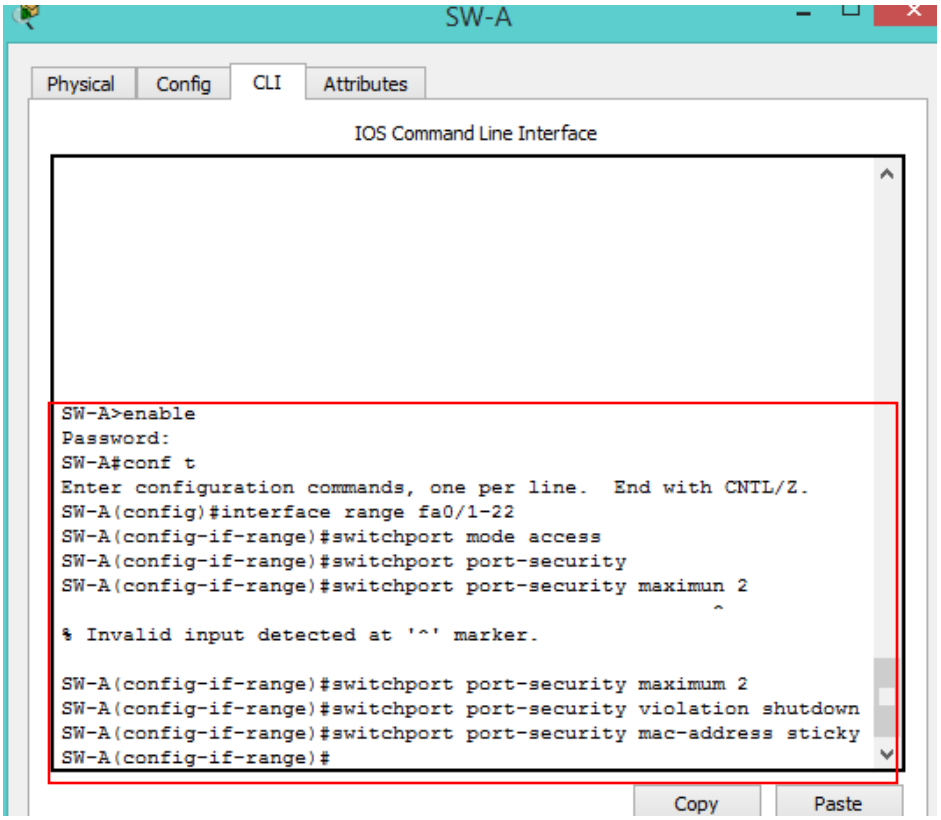




Part 4: Configure Port Security and Disable Unused Ports

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-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.

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 pueden aprenderse en estos puertos puede afectar significativamente la funcionalidad de la red.

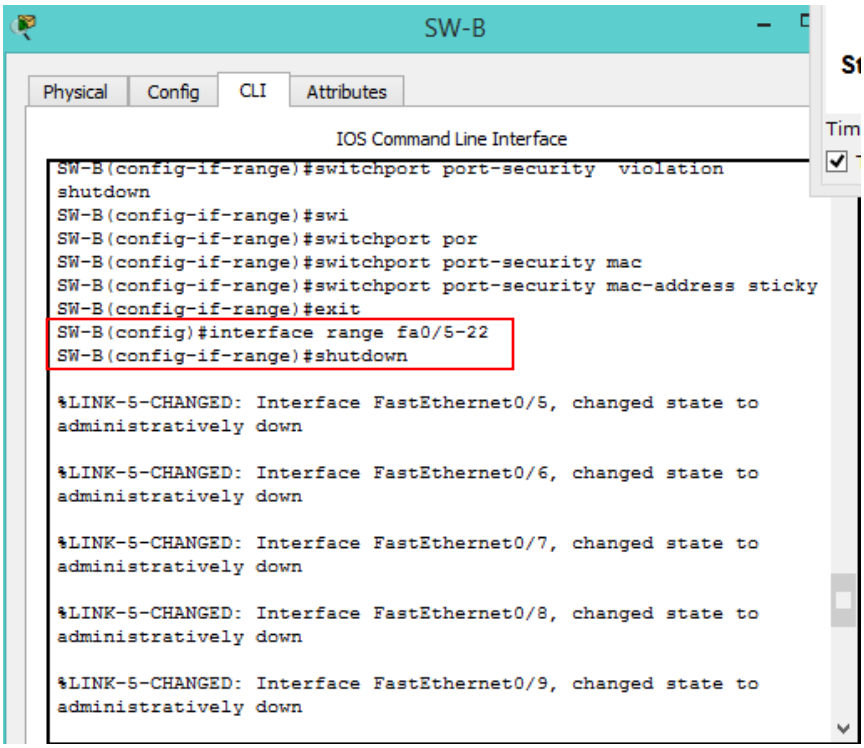
Step 2: Verify port security.

On **SW-A**, issue the **show port-security interface fa0/1** command to verify that port security has been configured.

Step 3: Disable unused ports.

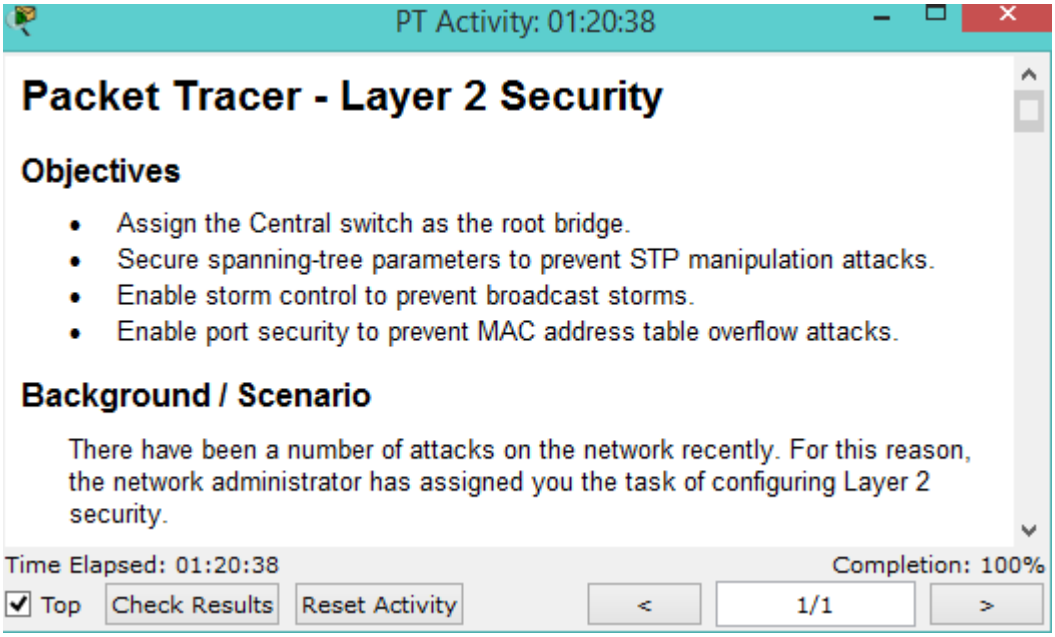
Disable all ports that are currently unused.

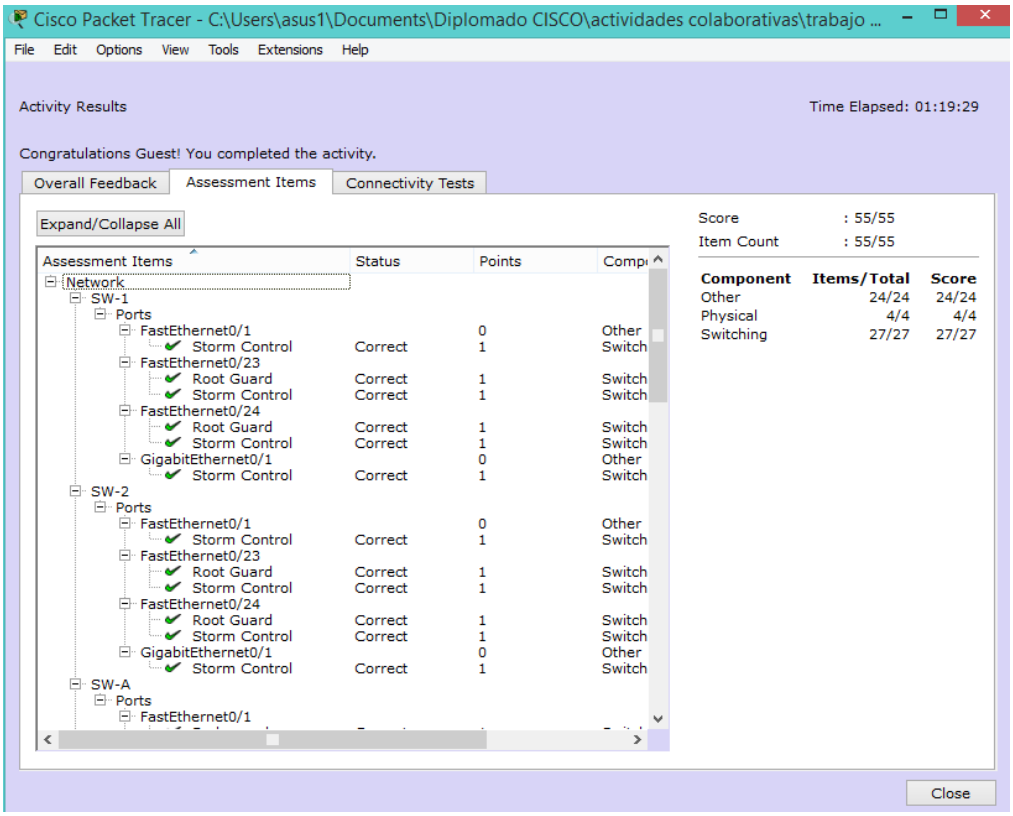
SW-A(config)# **interface range fa0/5 - 22**
SW-A(config-if-range)# **shutdown**
SW-B(config)# **interface range fa0/5 - 22**
SW-B(config-if-range)# **shutdown**



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.

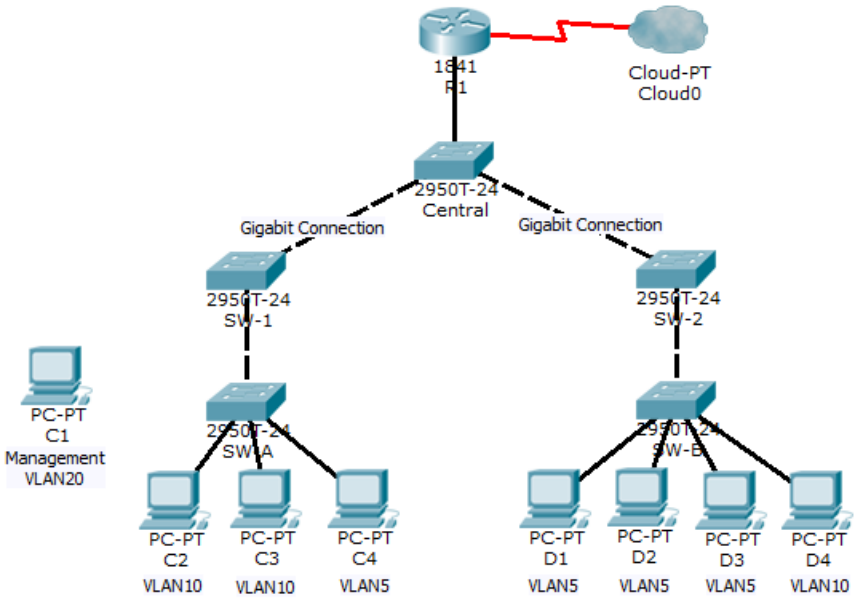



Cisco Packet Tracer - C:\Users\asus1\Documents\Diplomado CISCO\actividades colaborativas\trabajo ...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 01:19:29
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items Status Points Compl
Network
SW-1
Ports
FastEthernet0/1 0 Other
Storm Control Correct 1 Switch
FastEthernet0/23
Root Guard Correct 1 Switch
Storm Control Correct 1 Switch
FastEthernet0/24
Root Guard Correct 1 Switch
Storm Control Correct 1 Switch
GigabitEthernet0/1 0 Other
Storm Control Correct 1 Switch
SW-2
Ports
FastEthernet0/1 0 Other
Storm Control Correct 1 Switch
FastEthernet0/23
Root Guard Correct 1 Switch
Storm Control Correct 1 Switch
FastEthernet0/24
Root Guard Correct 1 Switch
Storm Control Correct 1 Switch
GigabitEthernet0/1 0 Other
Storm Control Correct 1 Switch
SW-A
Ports
FastEthernet0/1
Score : 55/55
Item Count : 55/55
Component Items/Total Score
Other 24/24 24/24
Physical 4/4 4/4
Switching 27/27 27/27
Close

Informe No. 6

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.

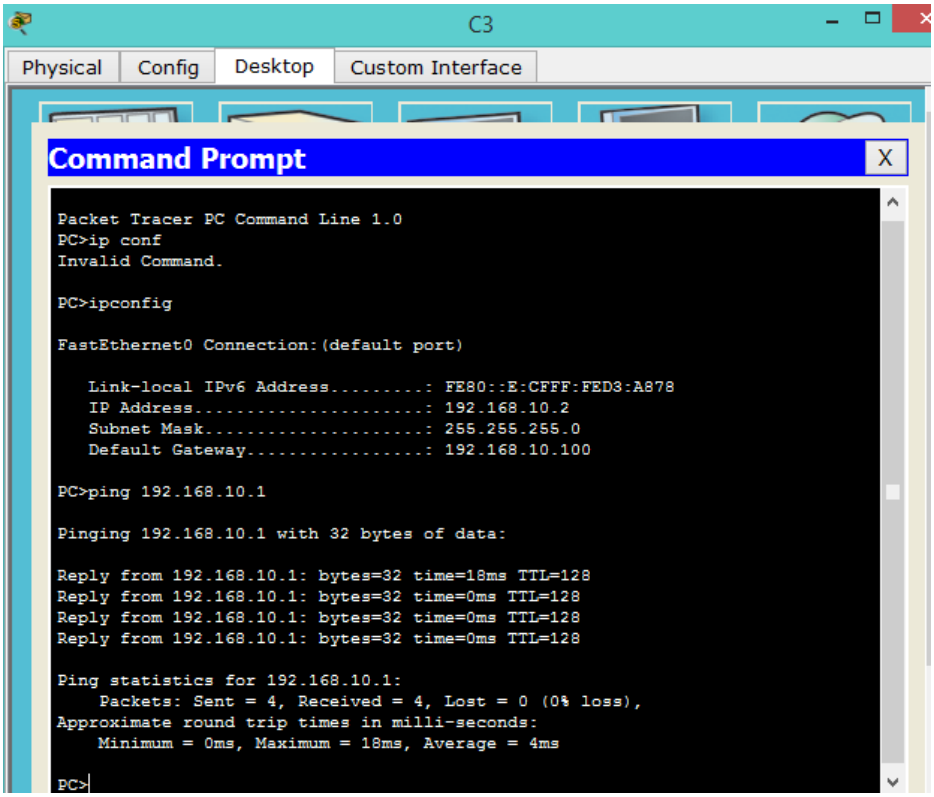
All devices have been preconfigured with:

- Enable secret password: **ciscoenpa55**

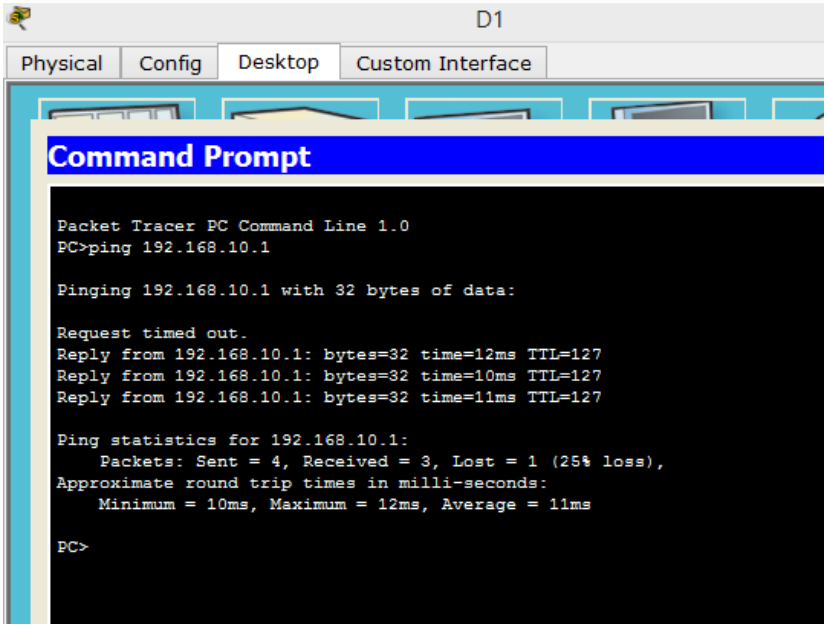
- Console password: **ciscoconpa55**
- VTY line password: **ciscovtypa55**

Part 1: Verify Connectivity

Step 1: Verify connectivity between C2 (VLAN 10) and C3 (VLAN 10).



Step 2: Verify connectivity between C2 (VLAN 10) and D1 (VLAN 5).

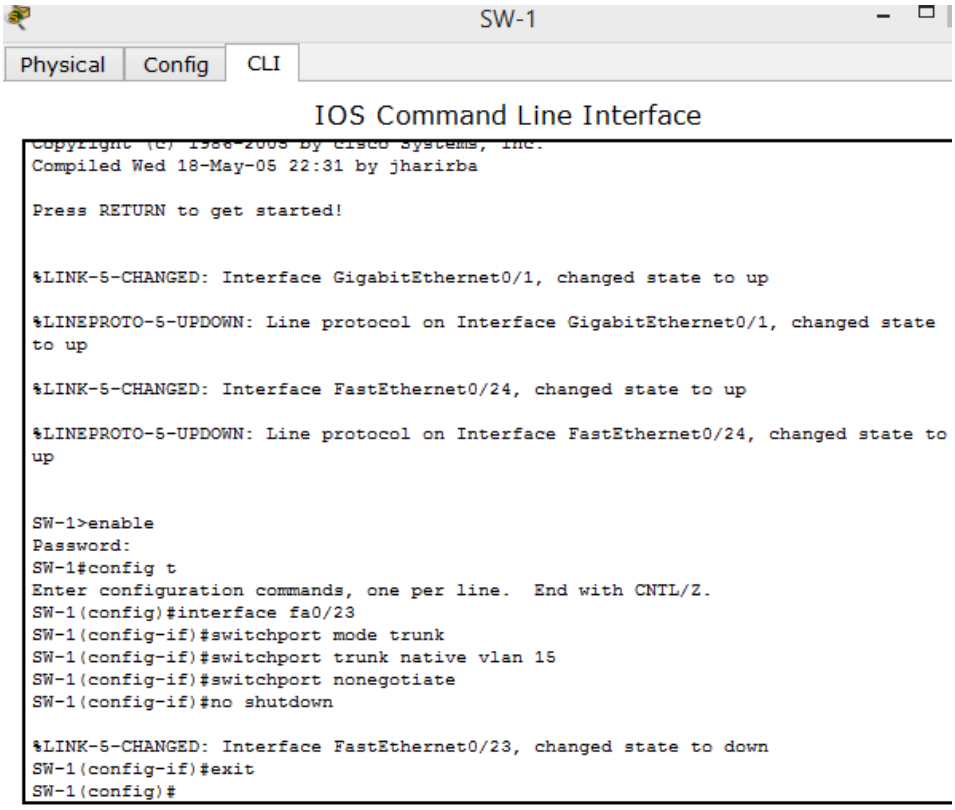


Note: If using the simple PDU GUI packet, be sure to ping twice to allow for ARP.

Part 2: Create a Redundant Link Between SW-1 and SW-2

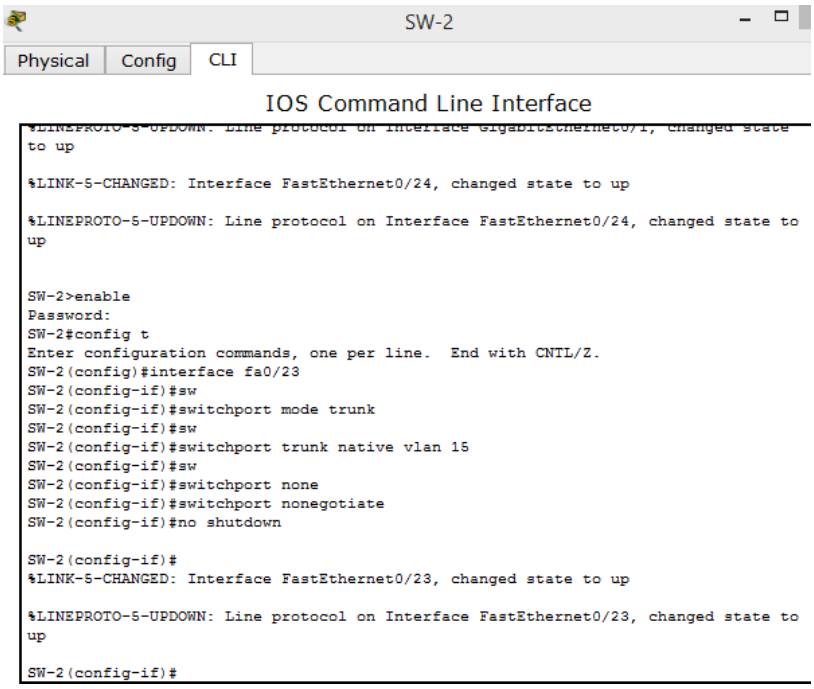
Step 1: Connect SW-1 and SW-2.
Using a crossover cable, connect port Fa0/23 on **SW-1** to port Fa0/23 on **SW-2**.

Step 2: Enable trunking, including all trunk security mechanisms on the link between SW-1 and SW-2.
Trunking has already been configured on all pre-existing trunk interfaces. The new link must be configured for trunking, including all trunk security mechanisms. On both **SW-1** and **SW-2**, set the port to trunk, assign native VLAN 15 to the trunk port, and disable auto-negotiation.



SW-1(config)# **interface fa0/23**
SW-1(config-if)# **switchport mode trunk**
SW-1(config-if)# **switchport trunk native vlan 15**
SW-1(config-if)# **switchport nonegotiate**
SW-1(config-if)# **no shutdown**

SW-2(config)# **interface fa0/23**
SW-2(config-if)# **switchport mode trunk**
SW-2(config-if)# **switchport trunk native vlan 15**
SW-2(config-if)# **switchport nonegotiate**
SW-2(config-if)# **no shutdown**



Part 3: Enable VLAN 20 as a Management VLAN

The network administrator wants to access all switch and routing devices using a management PC. For security, the administrator wants to ensure that all managed devices are on a separate VLAN.

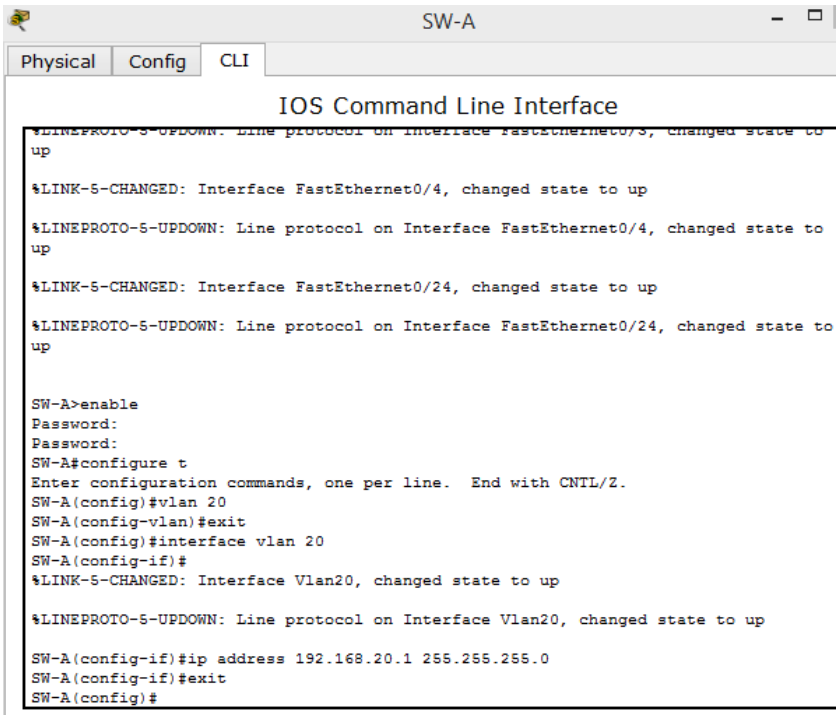
Step 1: Enable a management VLAN (VLAN 20) on SW-A.

a. Enable VLAN 20 on **SW-A**.

SW-A(config)# **vlan 20**
SW-A(config-vlan)# **exit**

b. Create an interface VLAN 20 and assign an IP address within the 192.168.20.0/24 network.

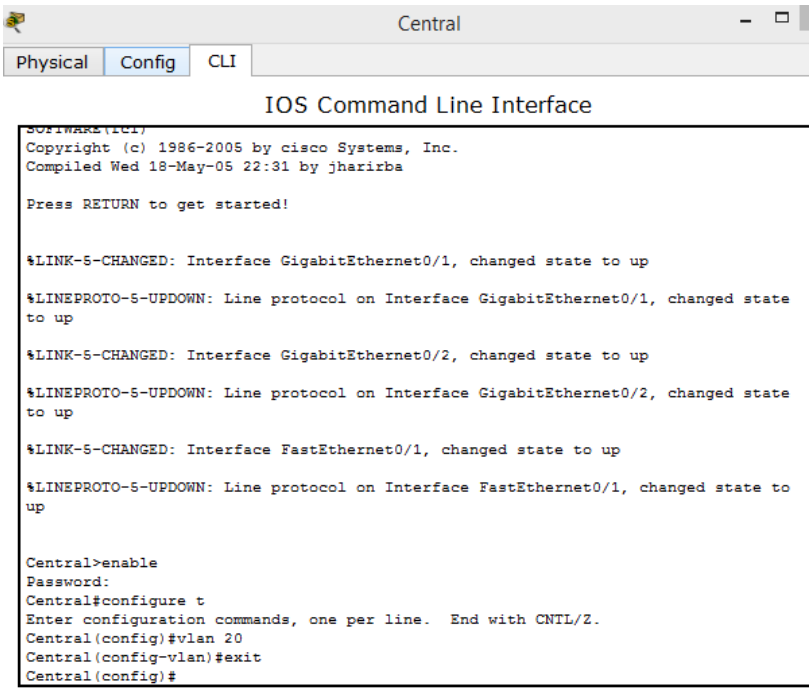
SW-A(config)# **interface vlan 20**
SW-A(config-if)# **ip address 192.168.20.1 255.255.255.0**



Step 2: Enable the same management VLAN on all other switches.

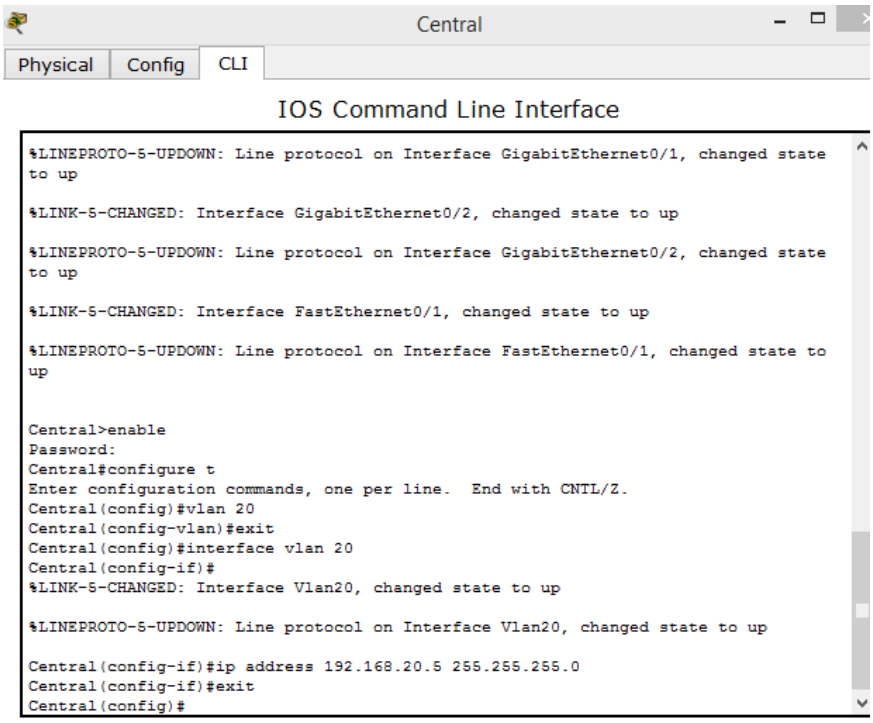
a. Create the management VLAN on all switches: **SW-B**, **SW-1**, **SW-2**, and **Central**.

SW-B(config)# **vlan 20**
SW-B(config-vlan)# **exit**
SW-1(config)# **vlan 20**
SW-1(config-vlan)# **exit**
SW-2(config)# **vlan 20**
SW-2(config-vlan)# **exit**
Central(config)# **vlan 20**
Central(config-vlan)# **exit**

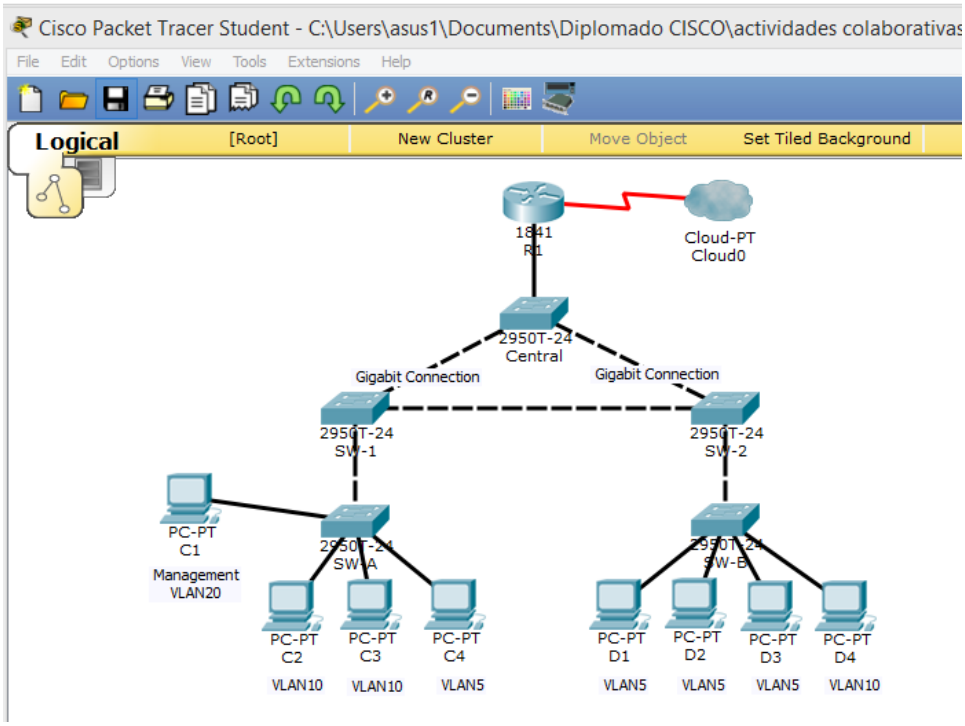


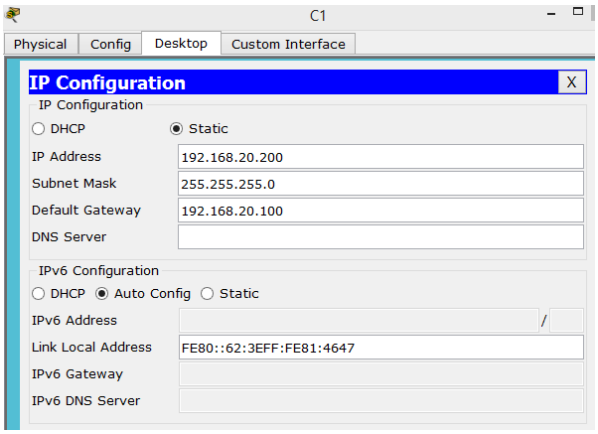
b. Create an interface VLAN 20 on all switches and assign an IP address within the 192.168.20.0/24 network.

SW-B(config)# **interface vlan 20**
SW-B(config-if)# **ip address 192.168.20.2 255.255.255.0**
SW-1(config)# **interface vlan 20**
SW-1(config-if)# **ip address 192.168.20.3 255.255.255.0**
SW-2(config)# **interface vlan 20**
SW-2(config-if)# **ip address 192.168.20.4 255.255.255.0**
Central(config)# **interface vlan 20**
Central(config-if)# **ip address 192.168.20.5 255.255.255.0**

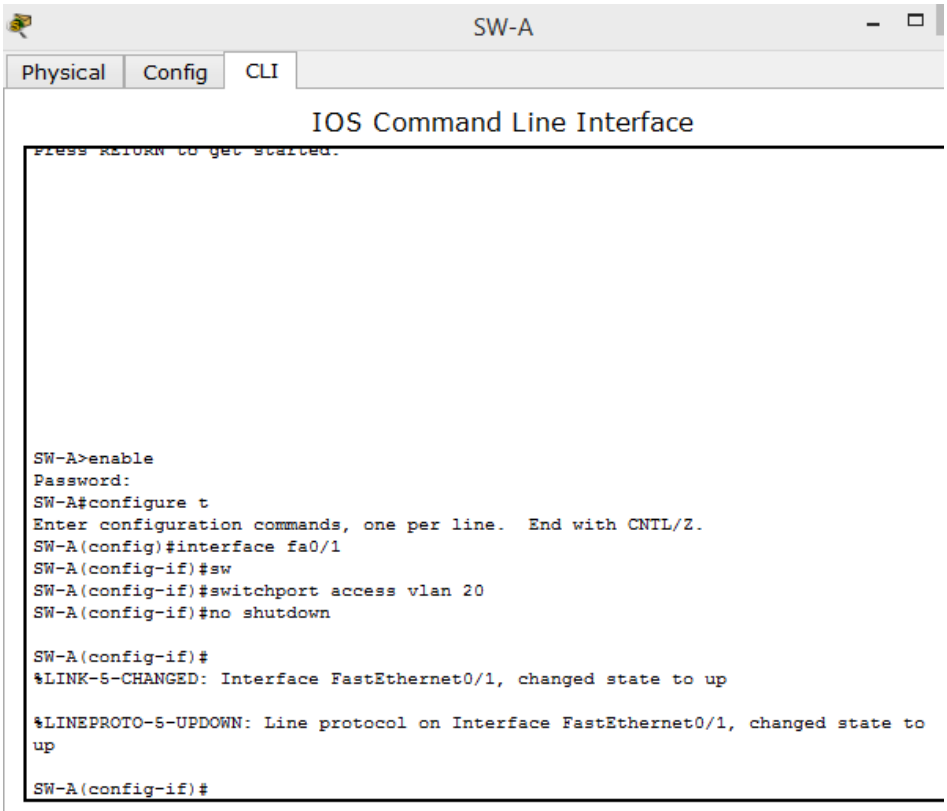


Step 3: Configure the management PC and connect it to SW-A port Fa0/1.
Ensure that the management PC is assigned an IP address within the 192.168.20.0/24 network. Connect the management PC to **SW-A** port Fa0/1.



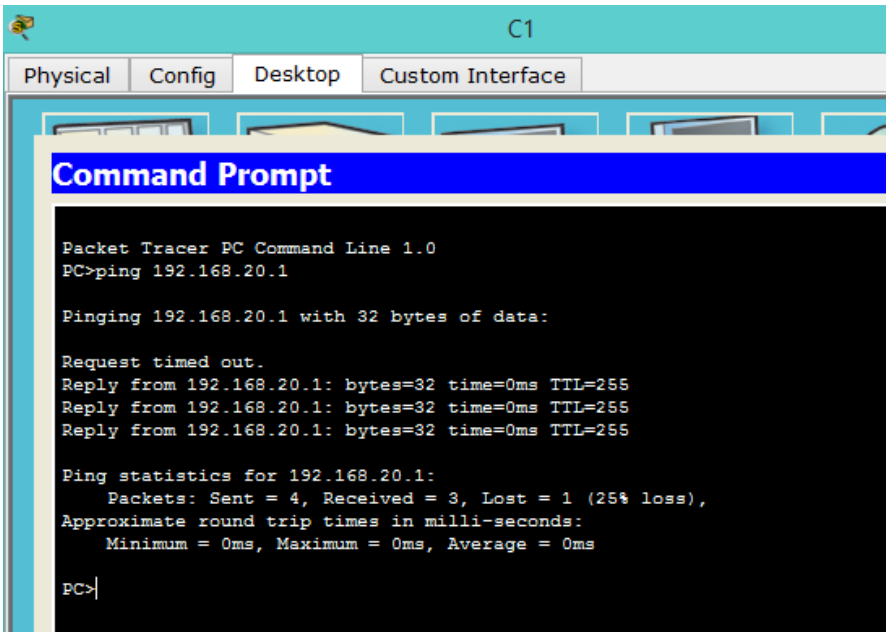


Step 4: On SW-A, ensure the management PC is part of VLAN 20.
Interface Fa0/1 must be part of VLAN 20.



SW-A(config)# **interface fa0/1**
SW-A(config-if)# **switchport access vlan 20**
SW-A(config-if)# **no shutdown**

Step 5: Verify connectivity of the management PC to all switches.
The management PC should be able to ping **SW-A**, **SW-B**, **SW-1**, **SW-2**, and **Central**.

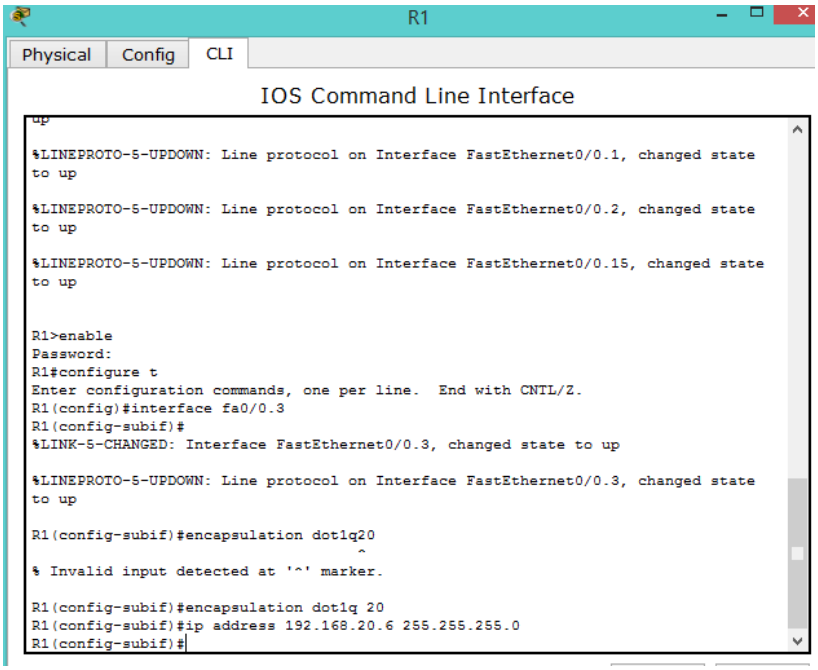


Part 4: Enable the Management PC to Access Router R1

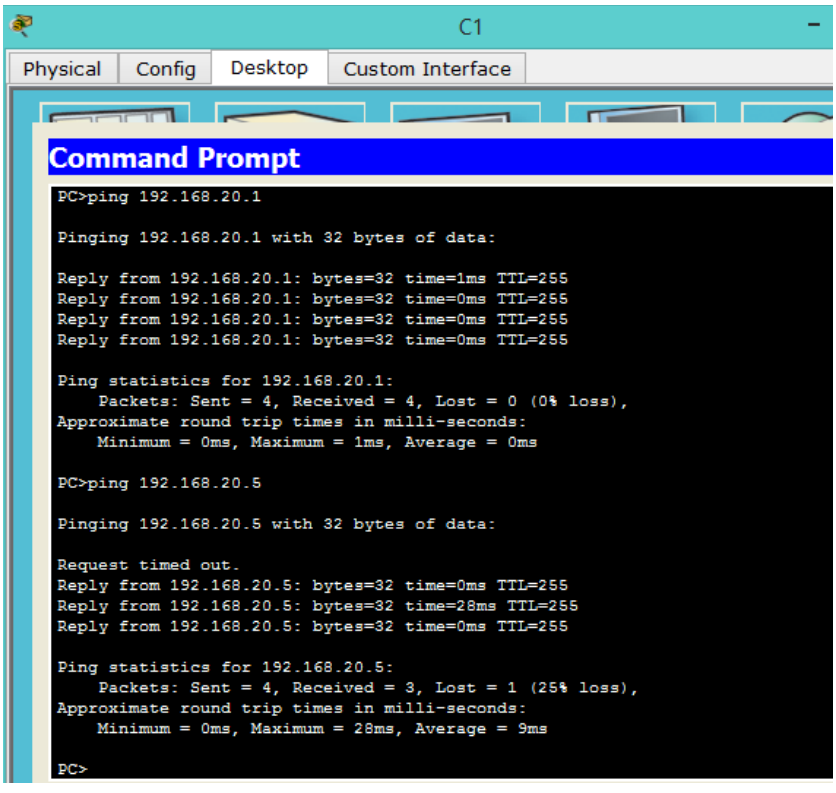
Step 1: Enable a new subinterface on router R1.
a. Create subinterface Fa0/0.3 and set encapsulation to dot1q 20 to account for VLAN 20.

R1(config)# **interface fa0/0.3**
R1(config-subif)# **encapsulation dot1q 20**

b. Assign an IP address within the 192.168.20.0/24 network.
R1(config)# **interface fa0/0.3**
R1(config-subif)# **ip address 192.168.20.100 255.255.255.0**



Step 2: Verify connectivity between the management PC and R1.
Be sure to configure the default gateway on the management PC to allow for connectivity.

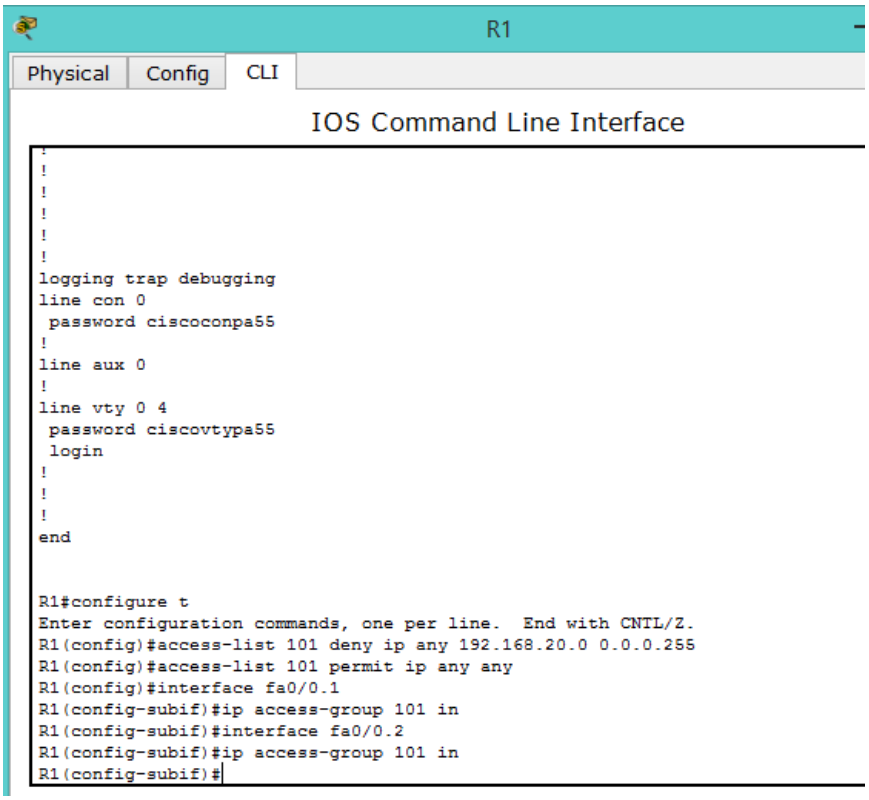


Step 3: Enable security.
While the management PC must be able to access the router, no other PC should be able to access the management VLAN.

a. Create an ACL that denies any network from accessing the 192.168.20.0/24 network, but permits all other networks to access one another.

Example: (may vary from student configuration)
R1(config)# **access-list 101 deny ip any 192.168.20.0 0.0.0.255**
R1(config)# **access-list 101 permit ip any any**
b. Apply the ACL to the proper interface(s).

Example: (may vary from student configuration)
R1(config)# **interface fa0/0.1**
R1(config-subif)# **ip access-group 101 in**
R1(config-subif)# **interface fa0/0.2**
R1(config-subif)# **ip access-group 101 in**

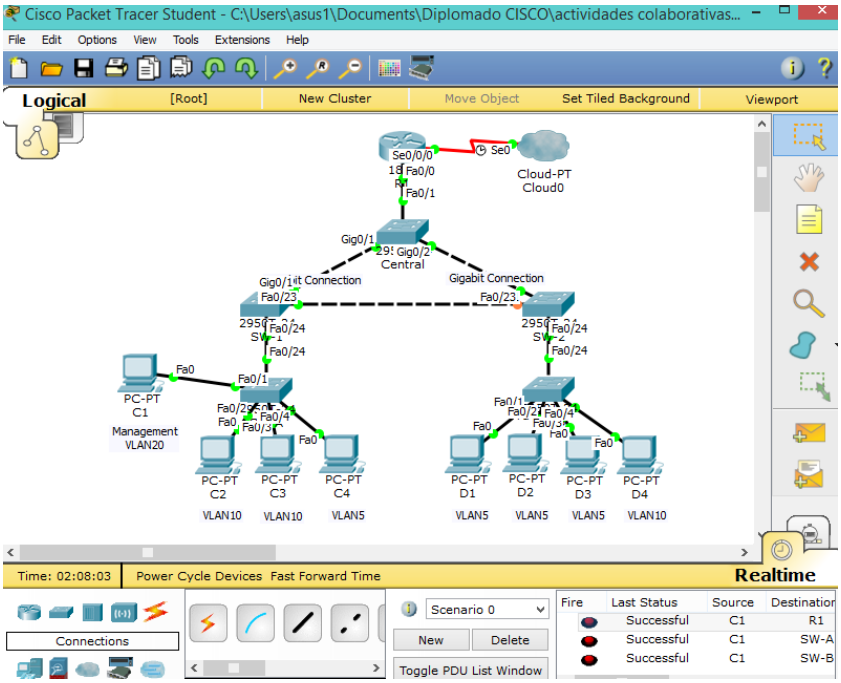


Note: There are multiple ways in which an ACL can be created to accomplish the necessary security. For this reason, grading on this portion of the activity is based on the correct connectivity requirements. The management PC must be able to connect to all switches and the router. All other PCs should not be able to connect to any devices within the management VLAN.

Step 4: Verify security.
a. From the management PC, ping **SW-A**, **SW-B**, and **R1**. Were the pings successful? Explain.

The pings should have been successful because all devices within the 192.168.20.0 network should be able to ping one another. Devices within VLAN20 are not required to route through the router.

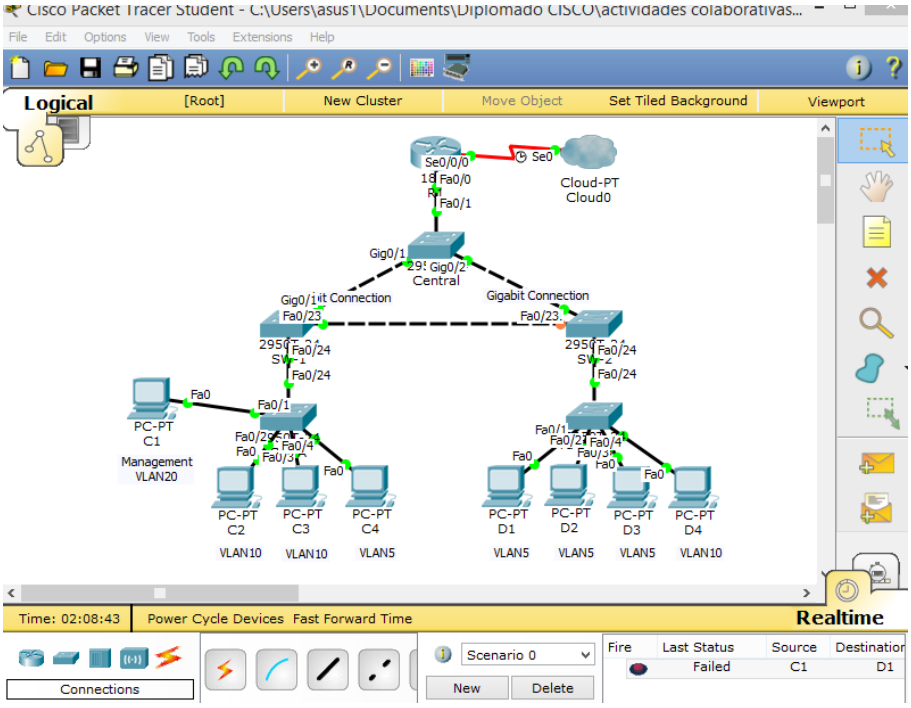
Los pings deberían haber tenido éxito porque todos los dispositivos dentro de la red 192.168.20.0 deberían ser capaces de hacer ping uno al otro. Los dispositivos dentro de VLAN20 no son necesarios para la ruta a través del enrutador.



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.

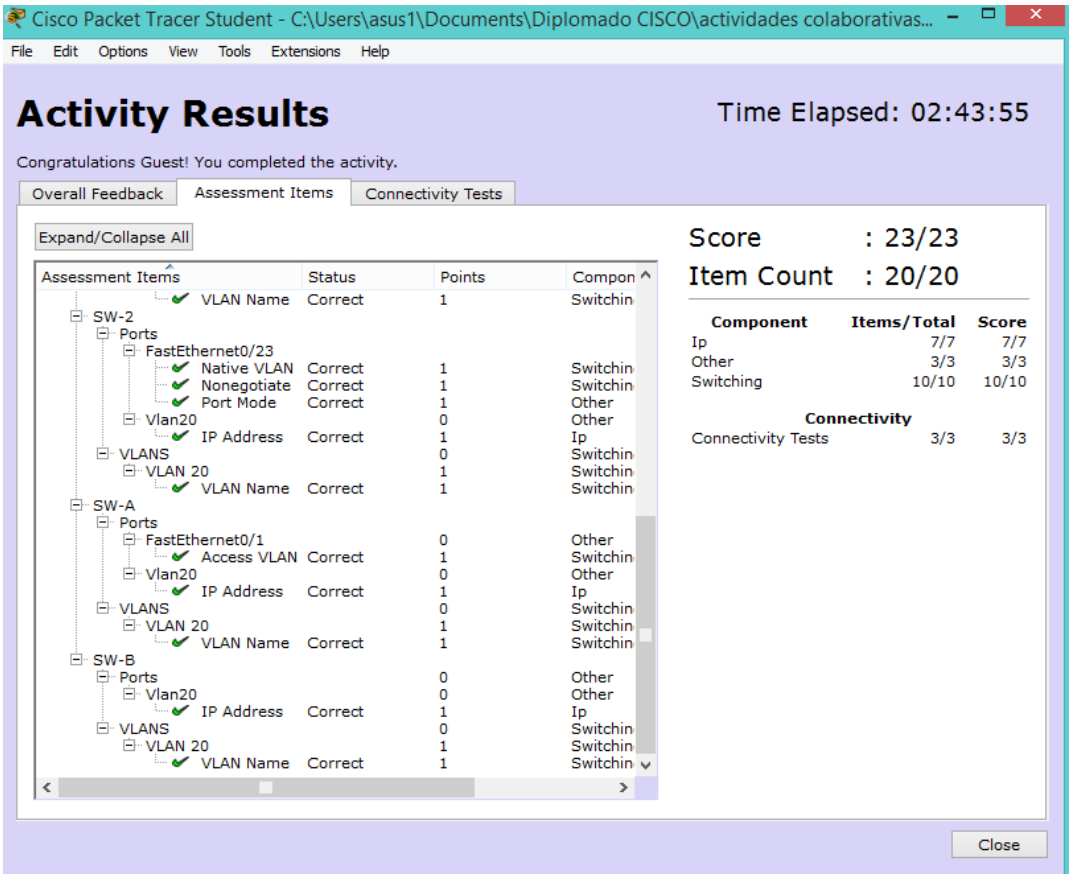
El ping debería haber fallado. Esto se debe a que para que un dispositivo dentro de una VLAN diferente pueda hacer ping exitosamente a un dispositivo dentro de VLAN20, debe ser enrutado. El enrutador tiene una ACL que impide que todos los paquetes accedan a la red 192.168.20.0.

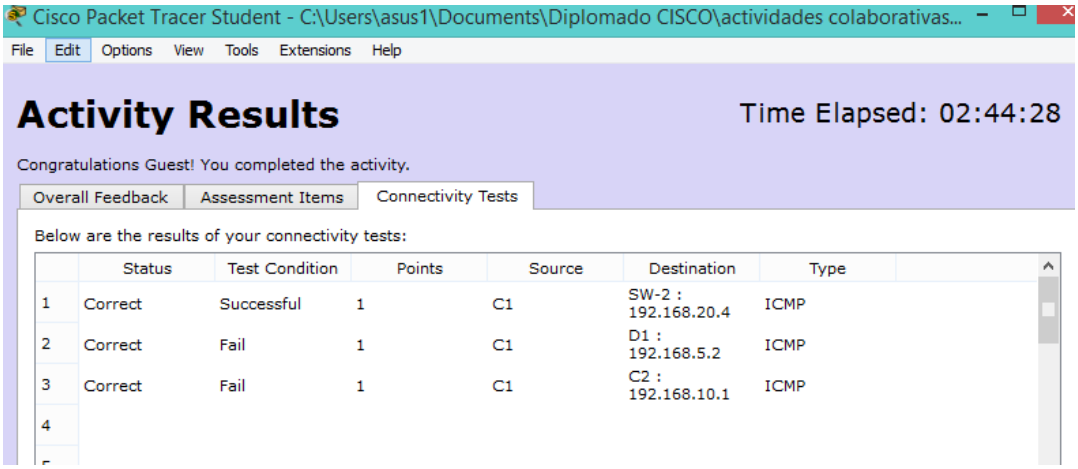


Step 5: Check results.

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.


Cisco Packet Tracer Student - C:\Users\asus1\Documents\Diplomado CISCO\actividades colaborativas...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 02:43:55
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Assessment Items
Status
Points
Compon
VLAN Name Correct 1 Switchin
SW-2
Ports
FastEthernet0/23
Native VLAN Correct 1 Switchin
Nonegotiate Correct 1 Switchin
Port Mode Correct 1 Other
Vlan20 0 Other
IP Address Correct 1 Ip
VLANS 0 Switchin
VLAN 20 1 Switchin
VLAN Name Correct 1 Switchin
SW-A
Ports
FastEthernet0/1 0 Other
Access VLAN Correct 1 Switchin
Vlan20 0 Other
IP Address Correct 1 Ip
VLANS 0 Switchin
VLAN 20 1 Switchin
VLAN Name Correct 1 Switchin
SW-B
Ports 0 Other
Vlan20 0 Other
IP Address Correct 1 Ip
VLANS 0 Switchin
VLAN 20 1 Switchin
VLAN Name Correct 1 Switchin
Score : 23/23
Item Count : 20/20
Component Items/Total Score
Ip 7/7 7/7
Other 3/3 3/3
Switching 10/10 10/10
Connectivity
Connectivity Tests 3/3 3/3
Close


Cisco Packet Tracer Student - C:\Users\asus1\Documents\Diplomado CISCO\actividades colaborativas...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 02:44:28
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Below are the results of your connectivity tests:
Status Test Condition Points Source Destination Type
1 Correct Successful 1 C1 SW-2 : 192.168.20.4 ICMP
2 Correct Fail 1 C1 D1 : 192.168.5.2 ICMP
3 Correct Fail 1 C1 C2 : 192.168.10.1 ICMP
4

Informe No. 7

3.2.2.5: Laboratorio: configuración de redes VLAN y enlaces troncales

Topología

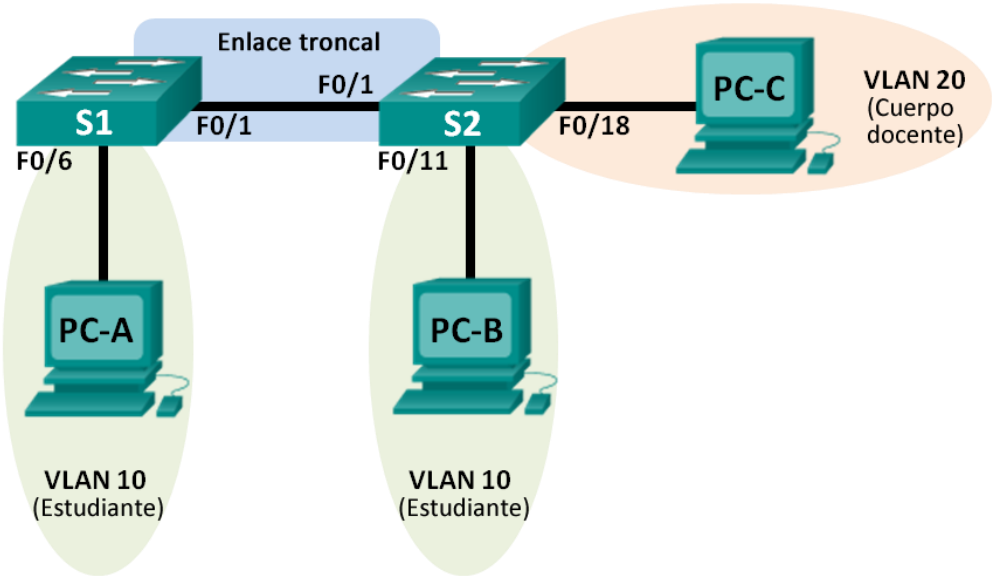


Tabla de direccionamiento

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

Objetivos

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

Parte 2: crear redes VLAN y asignar puertos de switch

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

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

Parte 5: eliminar la base de datos de VLAN

Información básica/situación

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

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

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

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

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

Recursos necesarios

2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

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

Cables Ethernet, como se muestra en la topología

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.

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

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

Inicializar y volver a cargar los switches según sea necesario.

Configurar los parámetros básicos para cada switch.

Desactive la búsqueda del DNS.

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

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

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.

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

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

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

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

Copie la configuración en ejecución en la configuración de inicio

Configurar los equipos host.

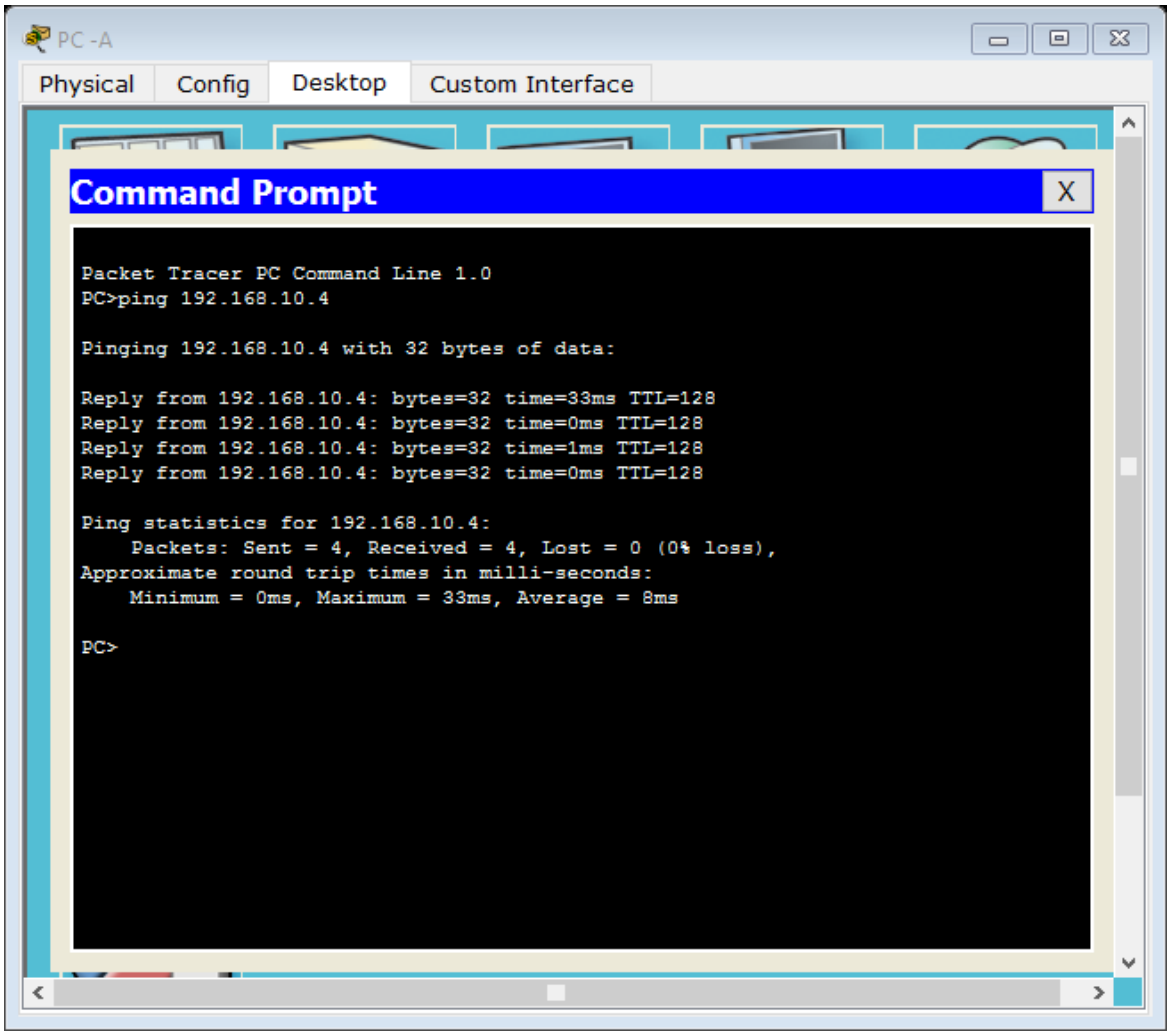
Consulte la tabla de direccionamiento para obtener información de direcciones de los equipos host.

Probar la conectividad.

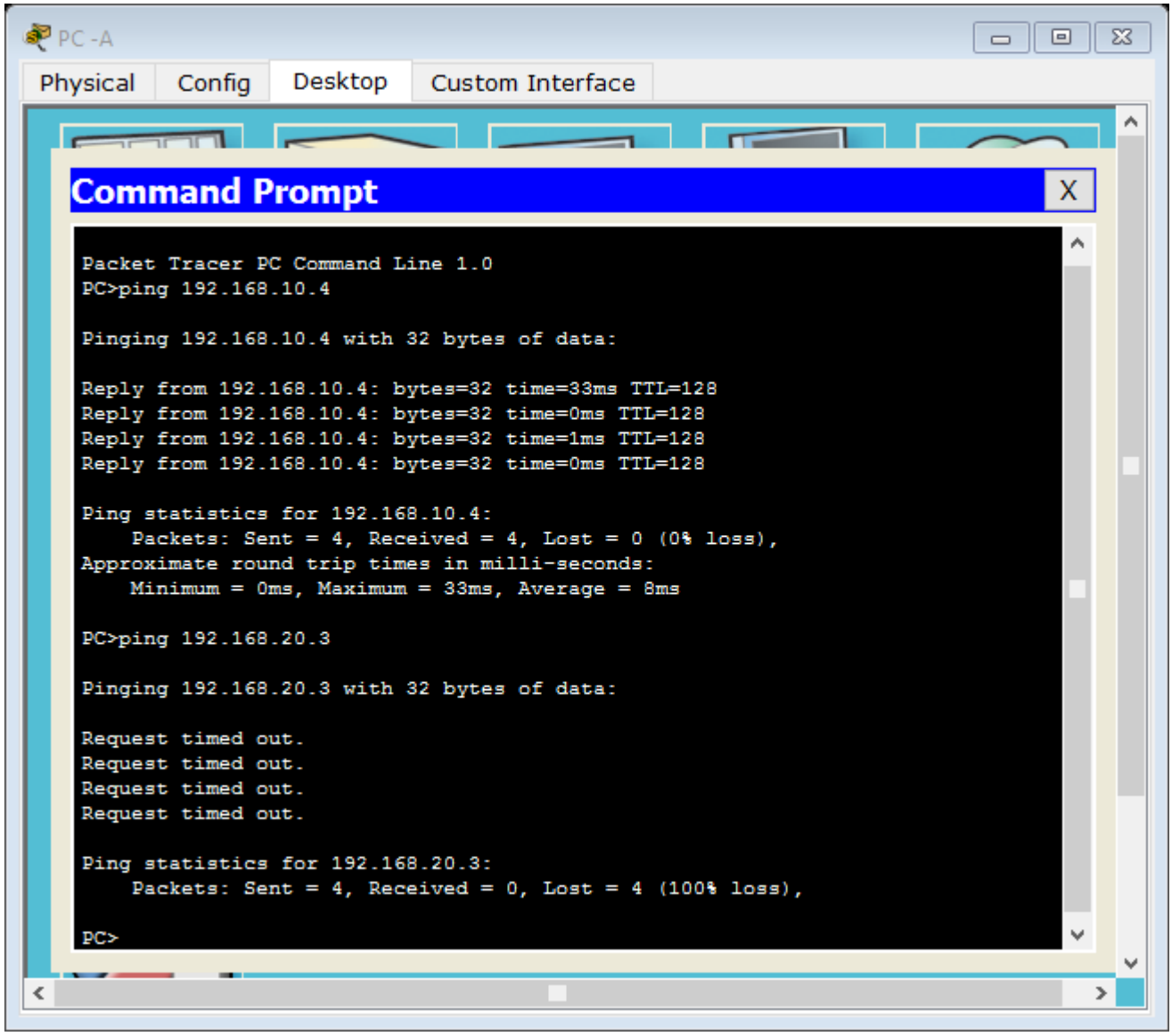
Verifique que los equipos host puedan hacer ping entre sí.

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

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



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



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

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

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

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

¿Se puede hacer ping del S1 al S2? ___SI_____

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

____**La red de los dispositivos que fallaron los ping se encuentran con diferentes subneting sería necesario un router**_____

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.

Crear las VLAN en los switches.

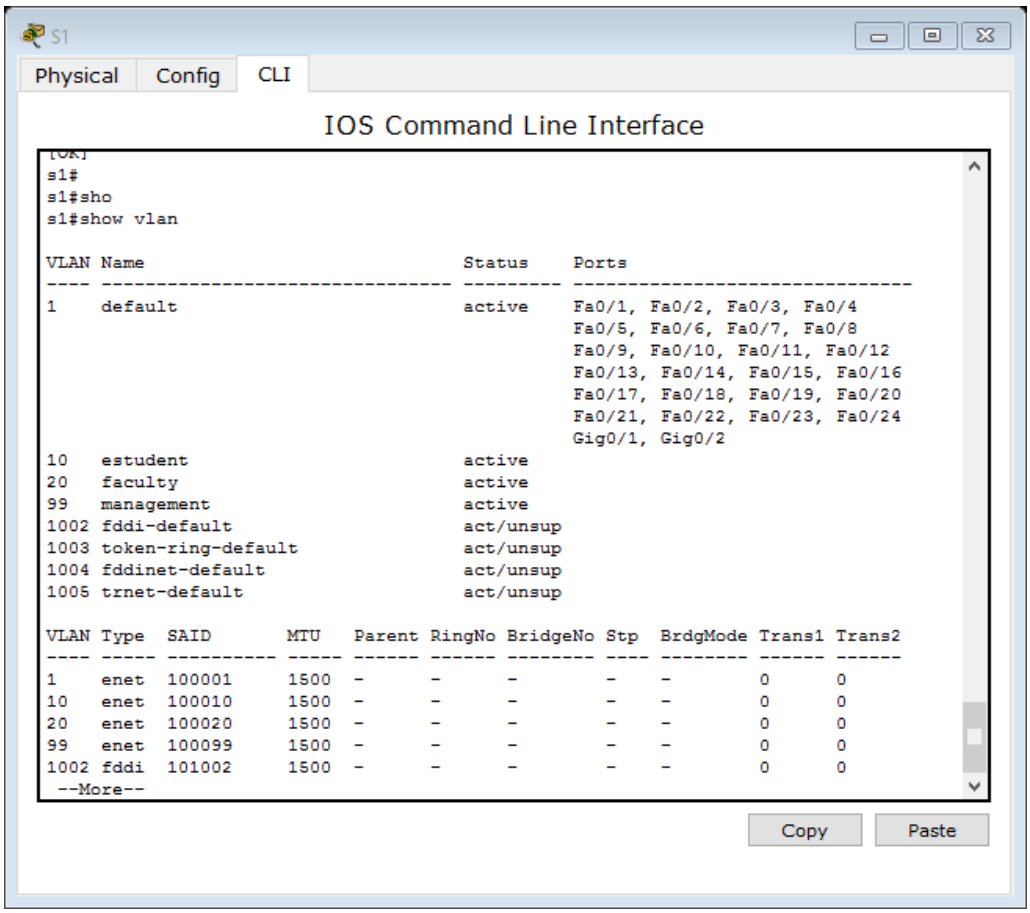
Cree las VLAN en S1. Dispositivos

```
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
```

Cree las mismas VLAN en el S2.

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

```
S1# show vlan
```



VLAN Name Status Ports

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

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gi0/1, Gi0/2

10 Student active

20 Faculty active

99 Management active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

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

1 enet 100001 1500 - - - - - 0 0

10 enet 100010 1500 - - - - - 0 0

20 enet 100020 1500 - - - - - 0 0

99 enet 100099 1500 - - - - - 0 0

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

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

1002 fddi 101002 1500 - - - - - 0 0

1003 tr 101003 1500 - - - - - 0 0

1004 fdnet 101004 1500 - - - ieee - 0 0

1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs

Primary Secondary Type Ports

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

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

¿Qué puertos se asignan a la VLAN predeterminada?

___**TODOS LOS PUERTOS**____

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7,

Fa0/8

Fa0/9, Fa0/10, Fa0/11,

Fa0/12

Fa0/13, Fa0/14, Fa0/15,

Fa0/16

Fa0/17, Fa0/18, Fa0/19,

Fa0/20

Fa0/21, Fa0/22, Fa0/23,

Fa0/24

Gig0/1, Gig0/2

Asignar las VLAN a las interfaces del switch correctas.

Asigne las VLAN a las interfaces en el S1.

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
```

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
```

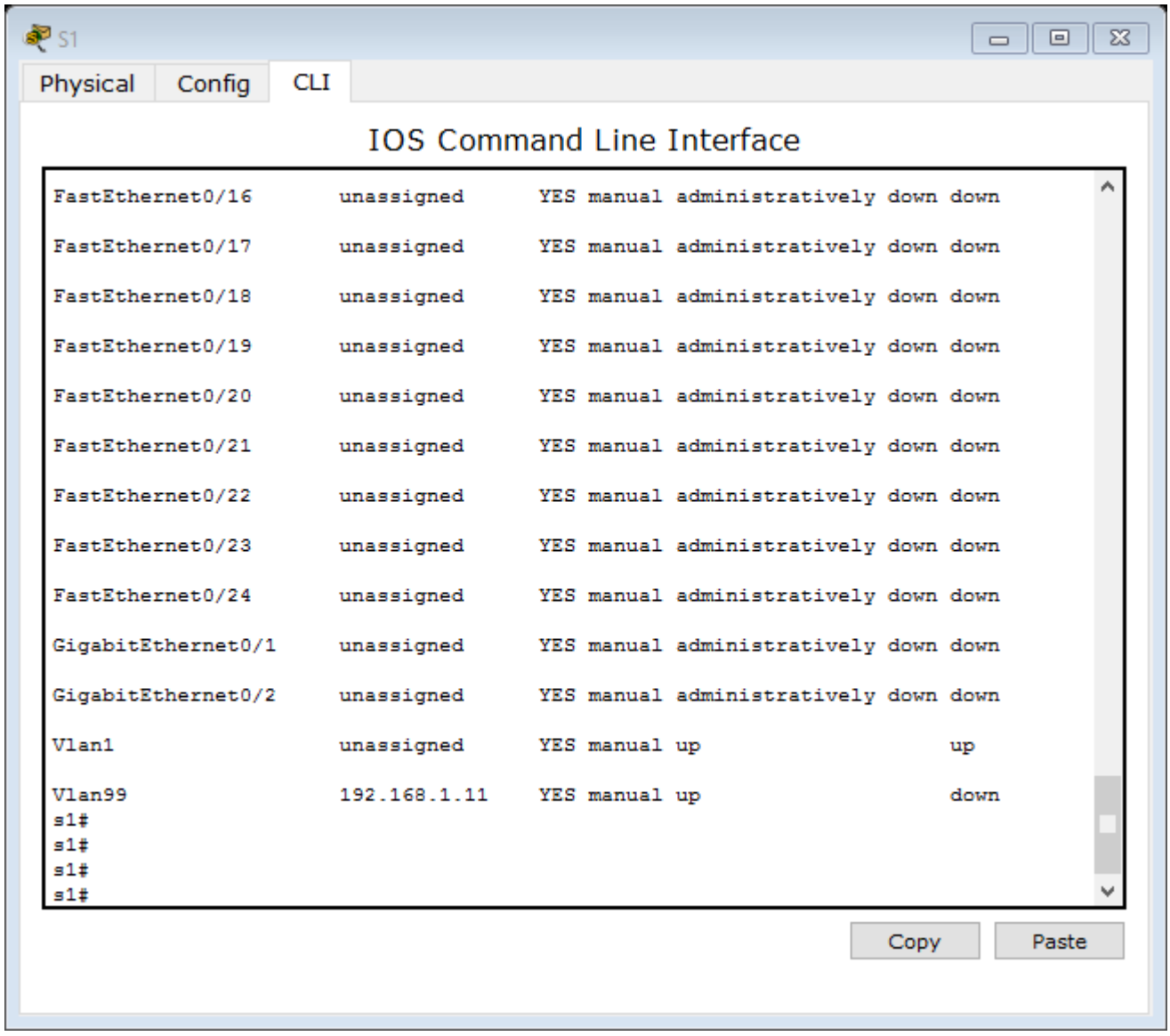
Emita el comando **show vlan brief** y verifique que las VLAN se hayan asignado a las interfaces correctas.

```
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
```

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

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

__**VLAN 99 ESTA down porque todavía no ha sido activada a un puerto activo**___



Use la topología para asignar las VLAN a los puertos correspondientes en el S2. Elimine la dirección IP para la VLAN 1 en el S2.

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

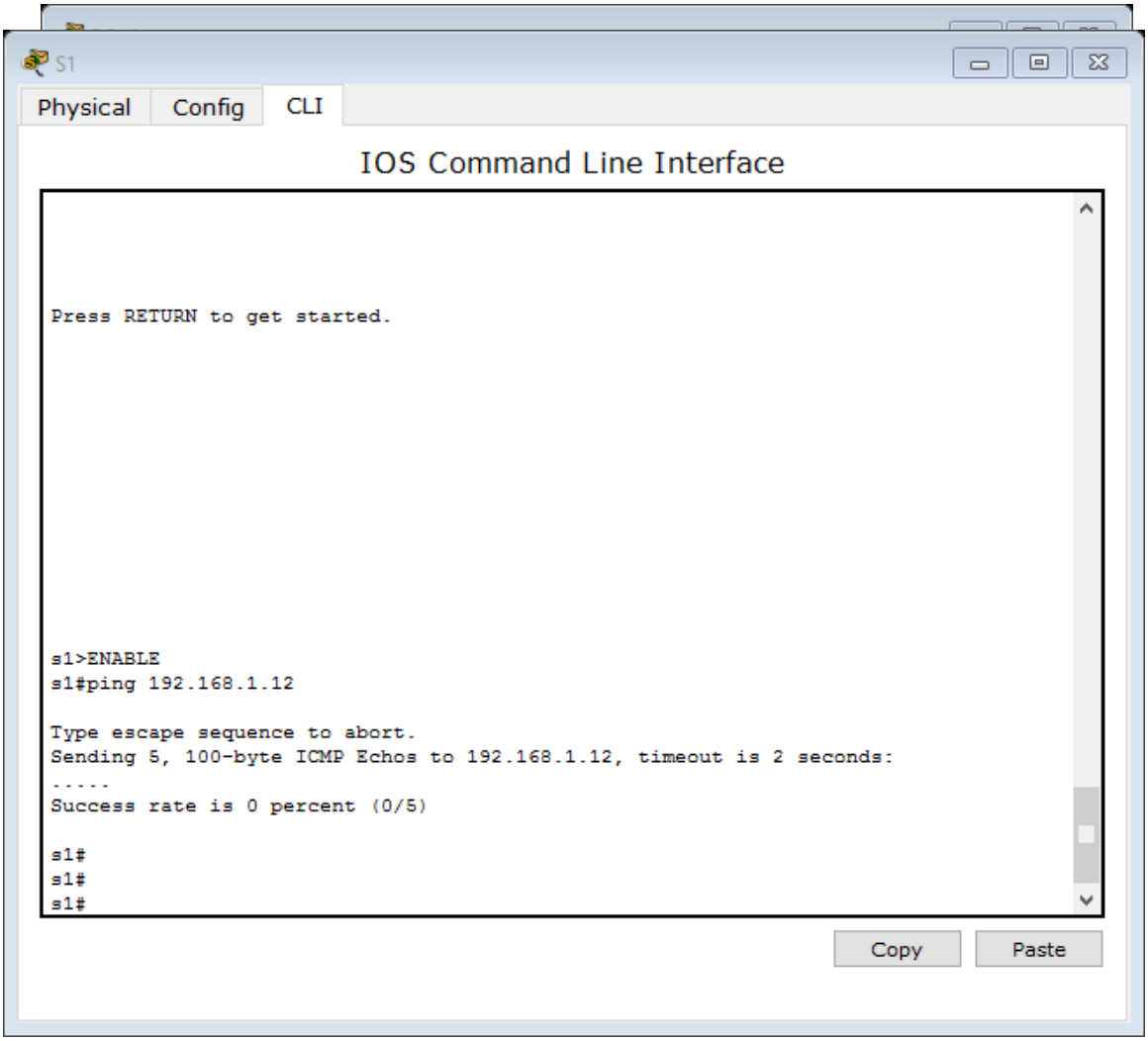
Use el comando **show vlan brief** para verificar que las VLAN se hayan asignado a las interfaces correctas.

S2# **show vlan brief**

```
VLAN Name                         Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                            Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                            Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                            Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                            Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                            Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Student                      active    Fa0/11
20   Faculty                      active    Fa0/18
99   Management                   active
1002 fddi-default                 act/unsup
1003 token-ring-default           act/unsup
1004 fddinet-default              act/unsup
1005 trnet-default                act/unsup
```

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

_____ **NO ASIGNADA A VLAN 10, POR QUE LA INTERFACE F 0/1 NO ESTA, NO PUEDE PASAR POR ESTA INTERFACE** _____



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

_____**NO, POR QUE LAS DIRECCIONES IP PARA LOS SWITCHES AHORA RESIDEN EN LA VLAN 99** _____

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.

Asignar una VLAN a varias interfaces.

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
```

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

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

Verifique que las asignaciones de VLAN sean las correctas.

Eliminar una asignación de VLAN de una interfaz.

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
```

Verifique que se haya realizado el cambio de VLAN.

¿A qué VLAN está asociada ahora F0/24?

____**ESTA ASOCIADA A VLAN 1**_____

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

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

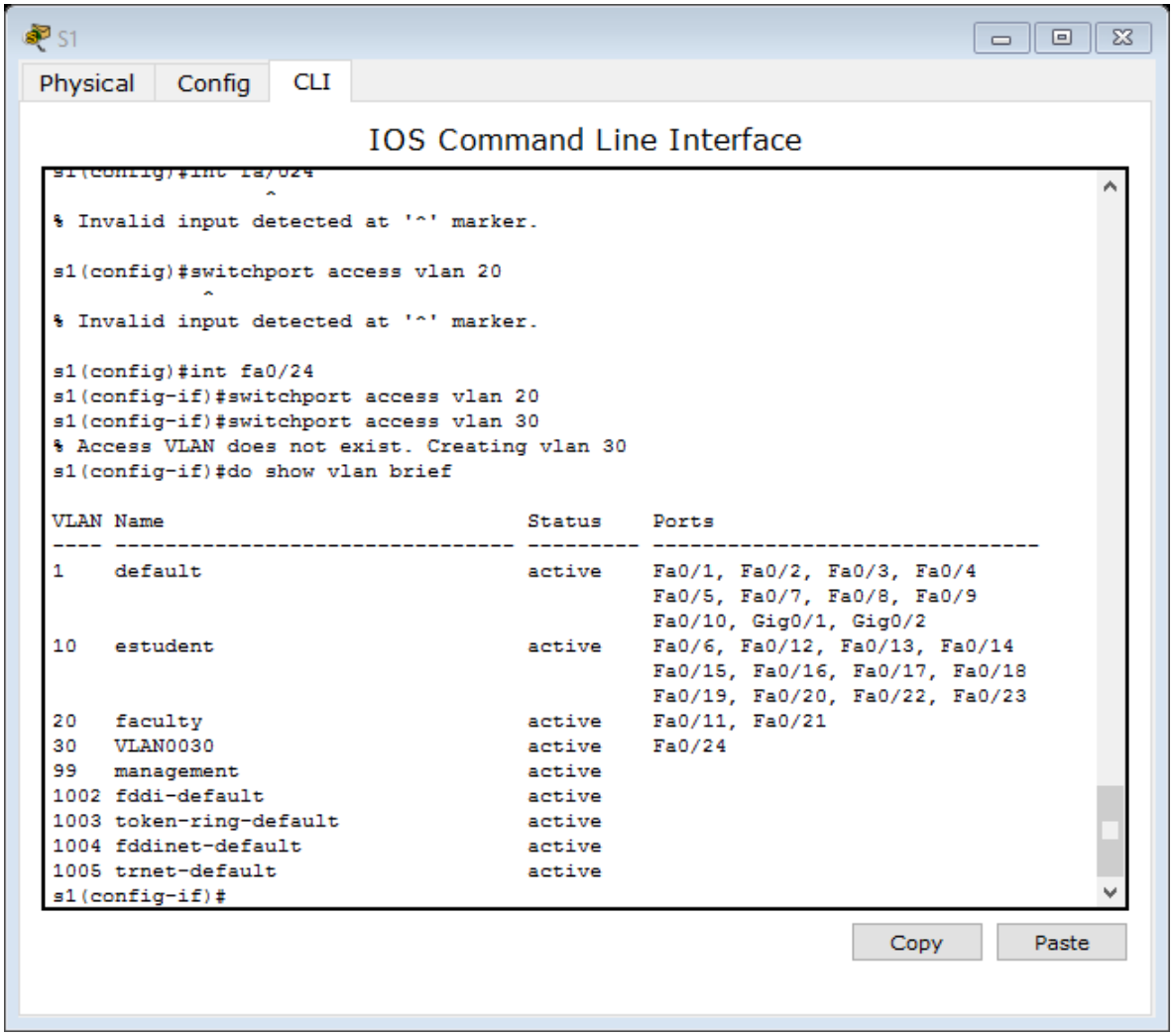
```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

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.

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

```
S1# show vlan brief

VLAN Name                         Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                      active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                            Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                            Fa0/9, Fa0/10, Gi0/1, Gi0/2
```

10 Student active Fa0/12, Fa0/13, Fa0/14, Fa0/15
Fa0/16, Fa0/17, Fa0/18, Fa0/19
Fa0/20, Fa0/22, Fa0/23



20 Faculty active Fa0/11, Fa0/21
30 VLAN0030 active Fa0/24
99 Management active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

¿Cuál es el nombre predeterminado de la VLAN 30?

___**S1 (config) # VLAN 30** __

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**

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?

__**NO PUEDE TRANSFERIR TRAFICO** ___

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
```

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

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

_____**VLAN 1** ___

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

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

____**UNA RECOMENDACIÓN IMPORTANTE DESDE UNA BASE DE DATOS ES REASIGNAR TODOS LOS PUERTOS ASIGNADOS A LA VLAN ANTES DE EXTRAER UNA VLAN.** _____

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.

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.

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

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
```

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

S1# **show interfaces trunk**

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

Port        Vlans allowed on trunk
Fa0/1       1-4094

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

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

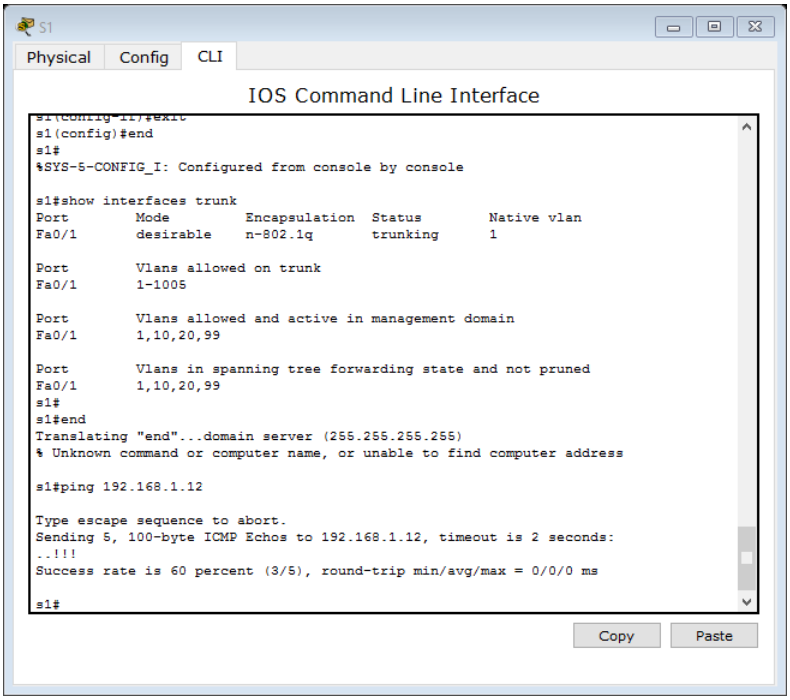
S2# **show interfaces trunk**

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

Port        Vlans allowed on trunk
Fa0/1       1-4094

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

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

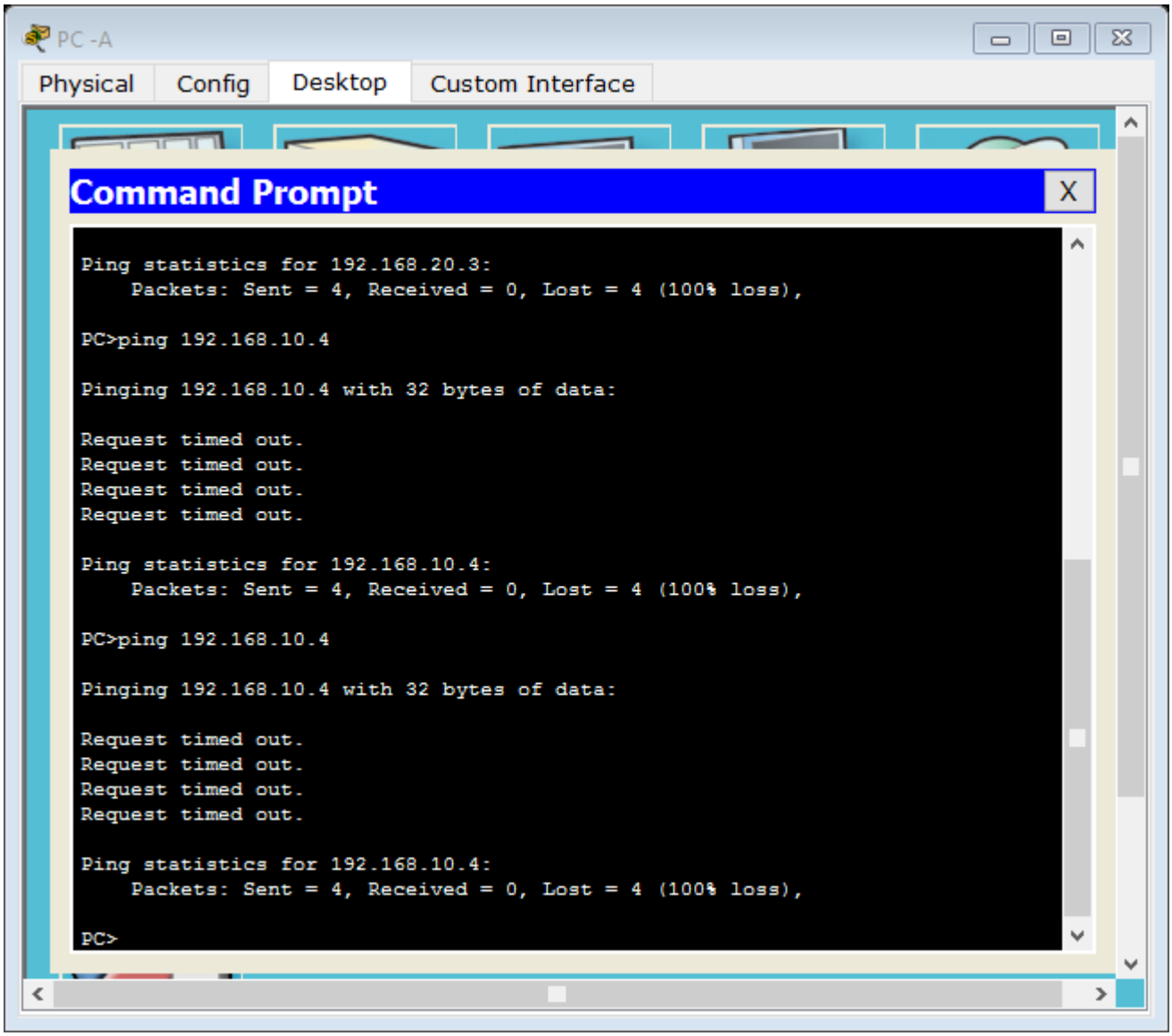
Nota: de manera predeterminada, todas las VLAN se permiten en un enlace troncal. El comando **switchport trunk** le permite controlar qué VLAN tienen acceso al enlace troncal. Para esta práctica de laboratorio, mantenga la configuración predeterminada que permite que todas las VLAN atraviesen F0/1.

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? ___NO_____



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

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

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

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

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

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

____LA COMPUTADORA PC-C NO PUEDE ENVIAR PING A PC-B POR QUE PC-C ESTA EN UNA VLAN DIFERENTE. LOS SWITCHES ESTA EN UNA VLAN

DIFERENTES QUE LAS DEMAS PC, POR TAL MOTIVO LOS PING NO SERAN SATISFACTORIOS.

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.

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**

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

S2# **show interfaces trunk**

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

Port	Vlans allowed on trunk
Fa0/1	1-4094

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

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

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

_____**NO TODOS ESTOS EQUIPOS UTILIZAN DTP** _____

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.

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.

Eliminar la base de datos de VLAN.

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#

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?

Borrar startup-config y reemplazar diferentes comandos deben ser emitidos después de la eliminación vlan.dat Comand

Reflexión

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

Se necesita un ROUTER

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

Mejores costos, mejor seguridad

Informe No. 8

3.3.2.2: Práctica de laboratorio: implementación de seguridad de VLAN

Topología

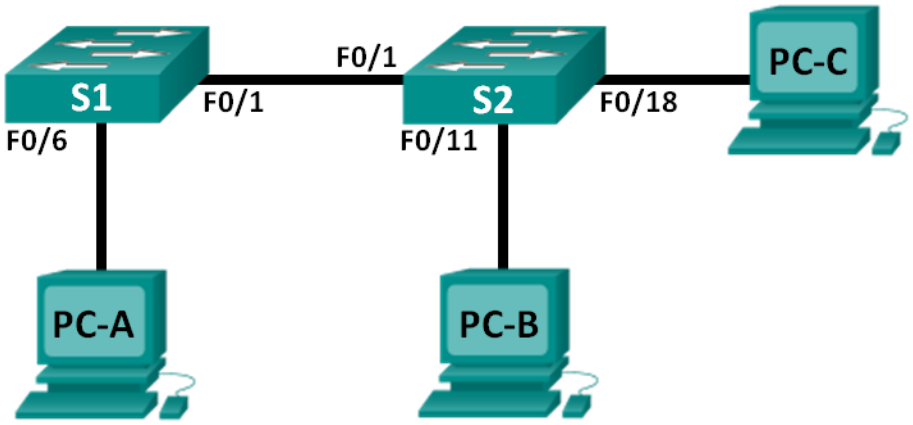


Tabla de direccionamiento

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

Asignaciones de VLAN

VLAN	Nombre
10	Datos
99	Management&Native
999	BlackHole

Objetivos

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

Parte 2: implementar seguridad de VLAN en los switches

Información básica/situación

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

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

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

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

Recursos necesarios

2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)

3 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

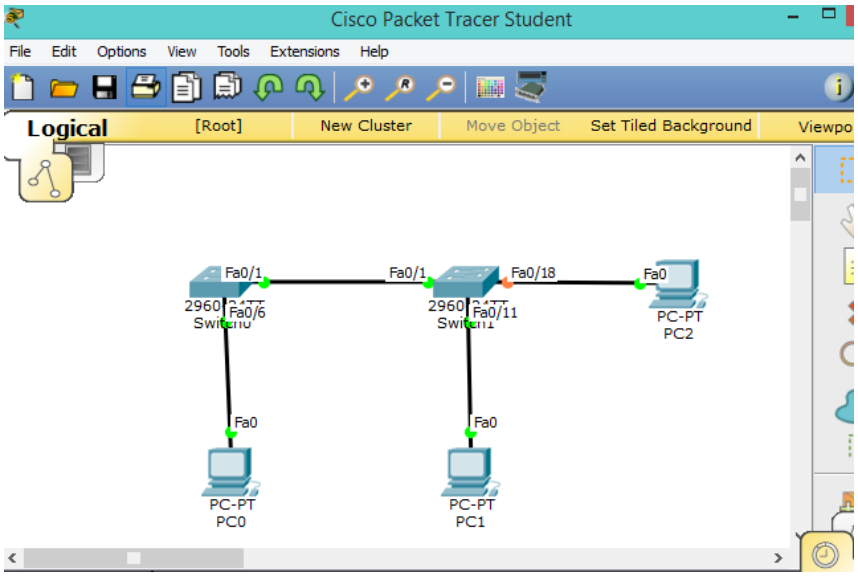
Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

Cables Ethernet, como se muestra en la topología

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.

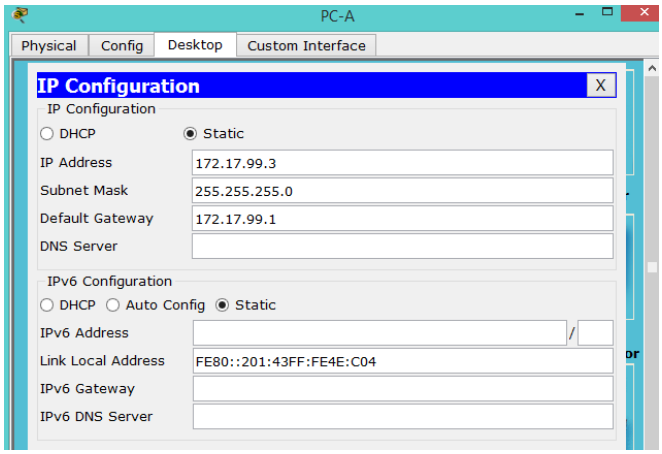
realizar el cableado de red tal como se muestra en la topología.



inicializar y volver a cargar los switches.

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.



configurar los parámetros básicos para cada switch.

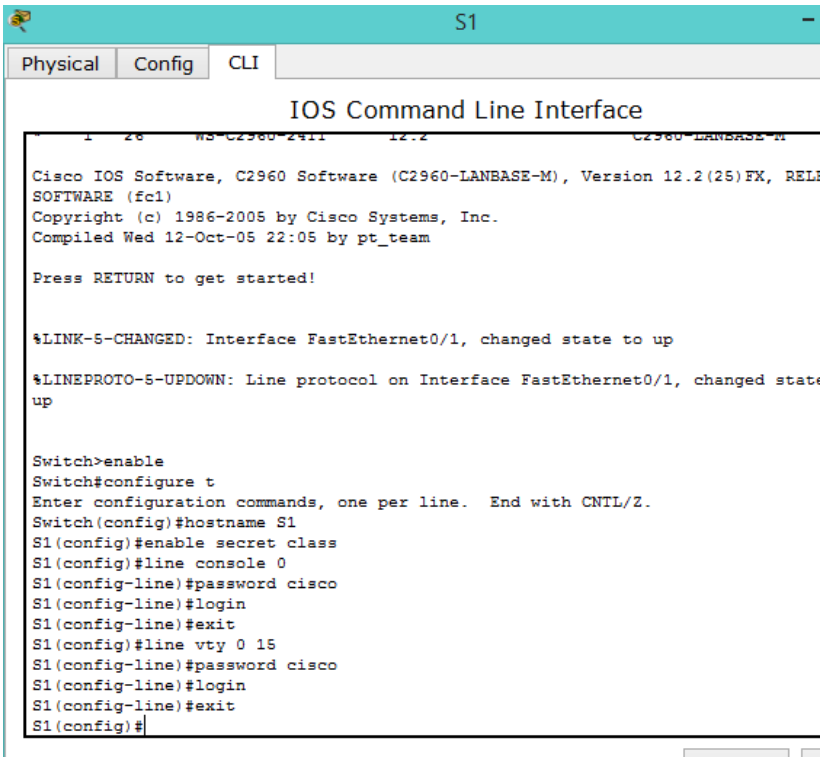
a. Desactive la búsqueda del DNS.

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.



configurar las VLAN en cada switch.

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

```
S1(config)#vlan 10
S1(config-vlan)#name Date
S1(config-vlan)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#vlan 999
S1(config-vlan)#BlackHole
                 ^
% Invalid input detected at '^' marker.

S1(config-vlan)#name BlackHole
S1(config-vlan)#
```

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

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

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

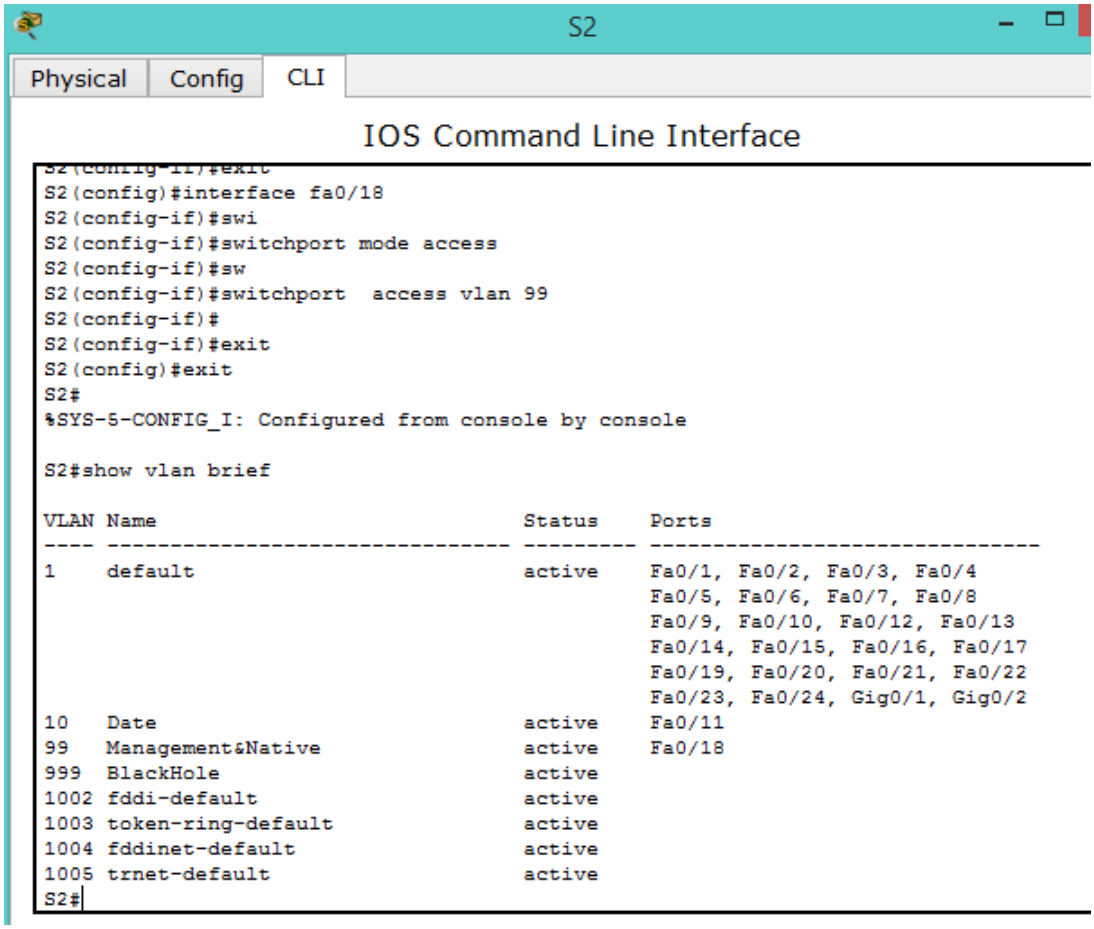
Configure F0/6 en el S1 como puerto de acceso y asígnelo a la VLAN 99.

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

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

```
S2(config)#interface fa0/11
S2(config-if)#sw
S2(config-if)#switchport mode access
S2(config-if)#sw
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#interface fa0/18
S2(config-if)#swi
S2(config-if)#switchport mode access
S2(config-if)#sw
S2(config-if)#switchport  access vlan 99
S2(config-if)#
```

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



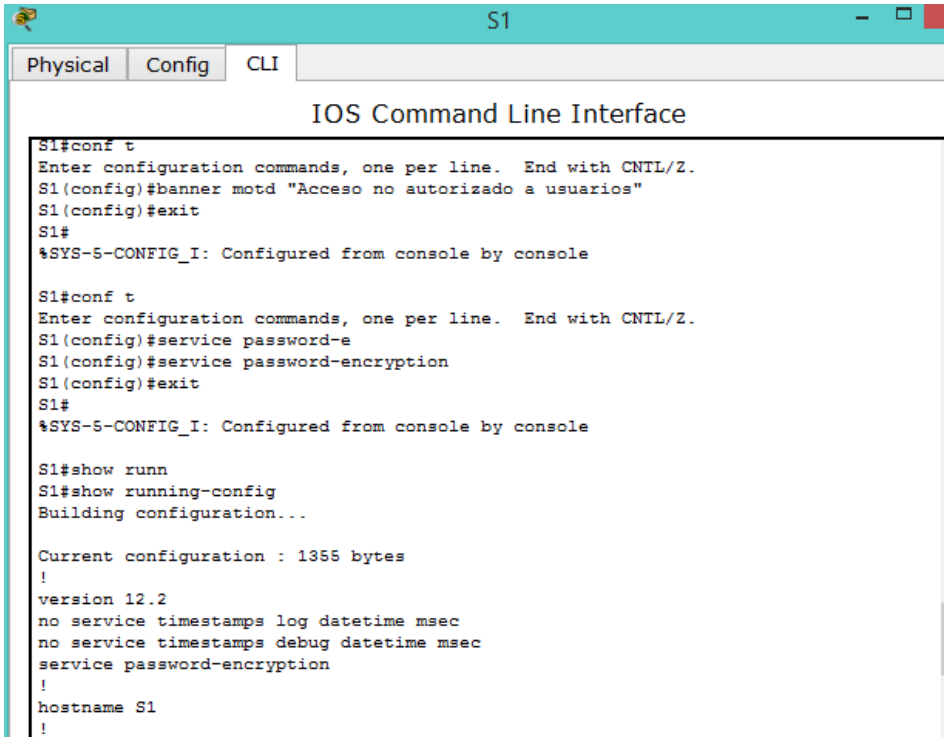
¿A qué VLAN pertenecería un puerto sin asignar, como F0/8 en el S2?

Pertenecería a la Vlan 1,que es la nativa y que está por defecto.

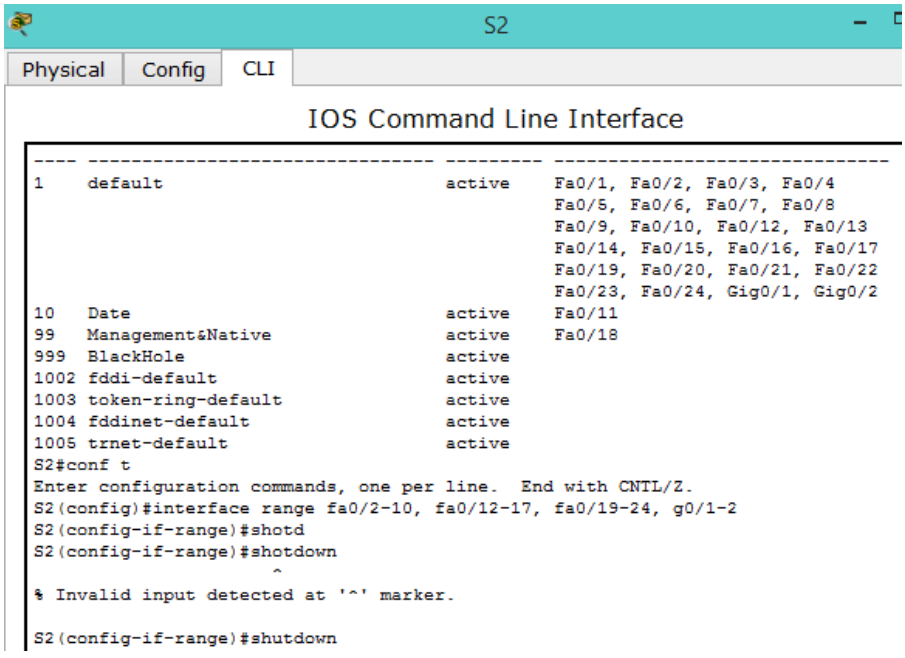
configurar la seguridad básica del switch.

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.



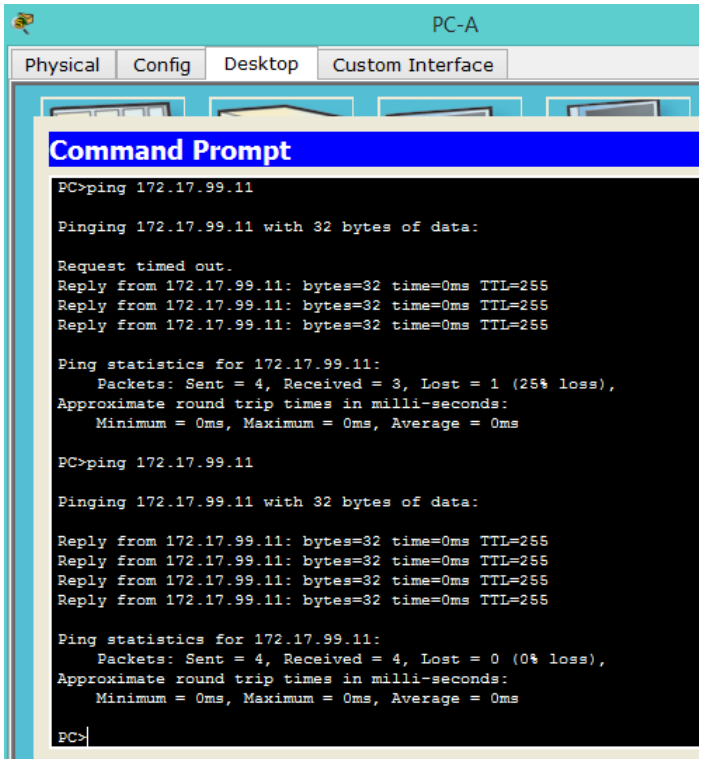
d. Deshabilite el servicio web básico en ejecución.

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

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

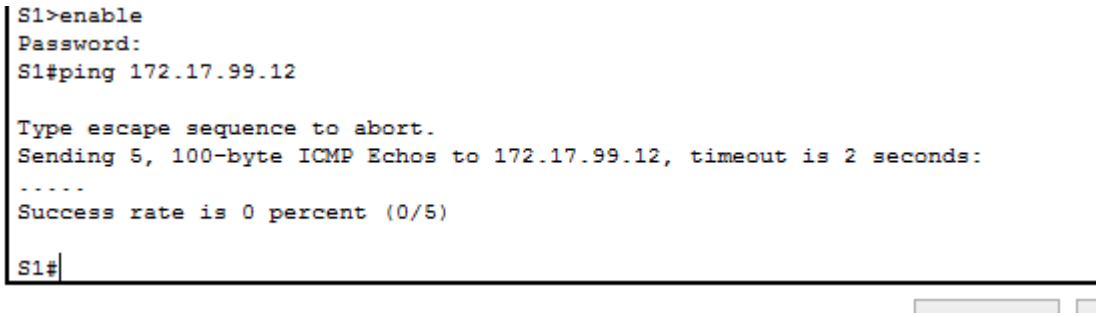
verificar la conectividad entre la información de VLAN y los dispositivos.

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



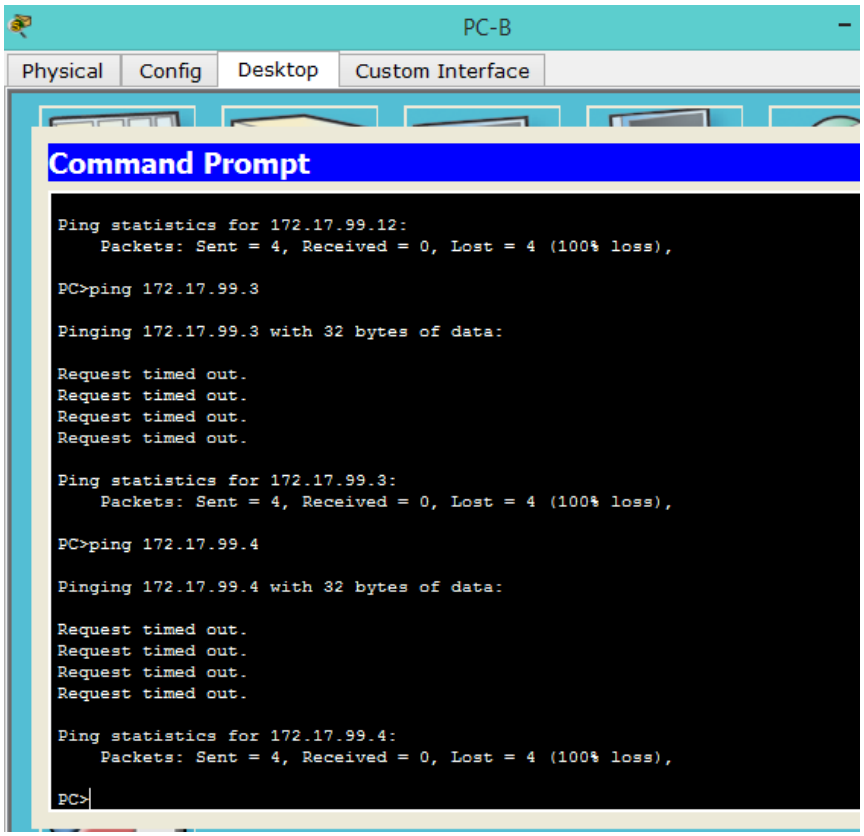
El ping es exitoso, porque PC-A esta en la misma Vlan que la dirección de administrativa del switch.

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



no hay ping entre los switch y no exitoso. Porque la dirección administrativa del S1 y S2 están e la misma Vlan, pero la interface f0/1 en ambos switches no están configurados como un puerto troncal. El puerto f0/1 aun pertenece a la vlan 1 y no a la vlan 99.

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

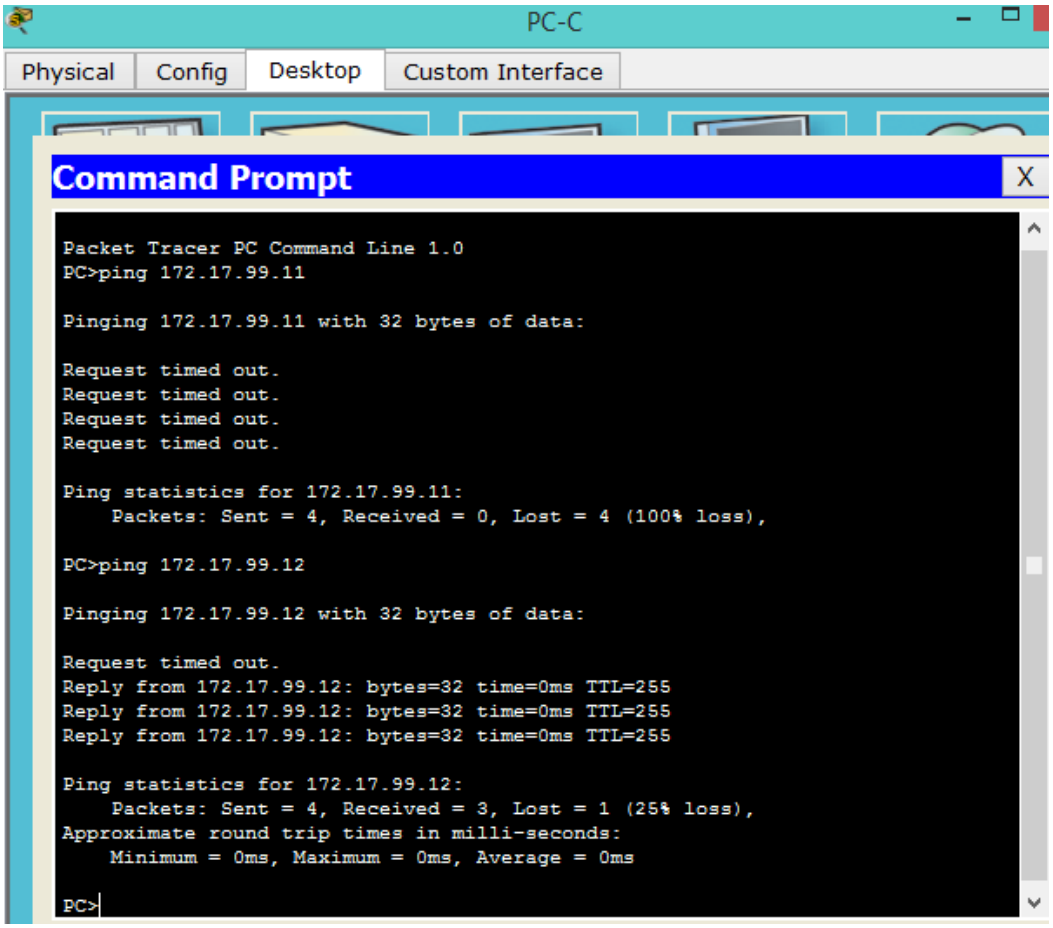


Los ping al S1 y al S2, como al PC-A y al PC-C todos fueron fallidos.

Porque PC-B está en la vlan 10 y los otros están en la vlan 99. No hay dispositivos de capa 3 que puedan rutear los paquetes entre las redes.

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

   Parcialmente es satisfatorio. La PC-C esta en la misma vlan que S1 y S2. Pero la PC-C es capaz de hacer ping en la direccion administrativa S2 pero no a la dirección de S1, porque el enlace troncal no ha sido establecido aun entre S1 y S2.



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

implementar seguridad de VLAN en los switches

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

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

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

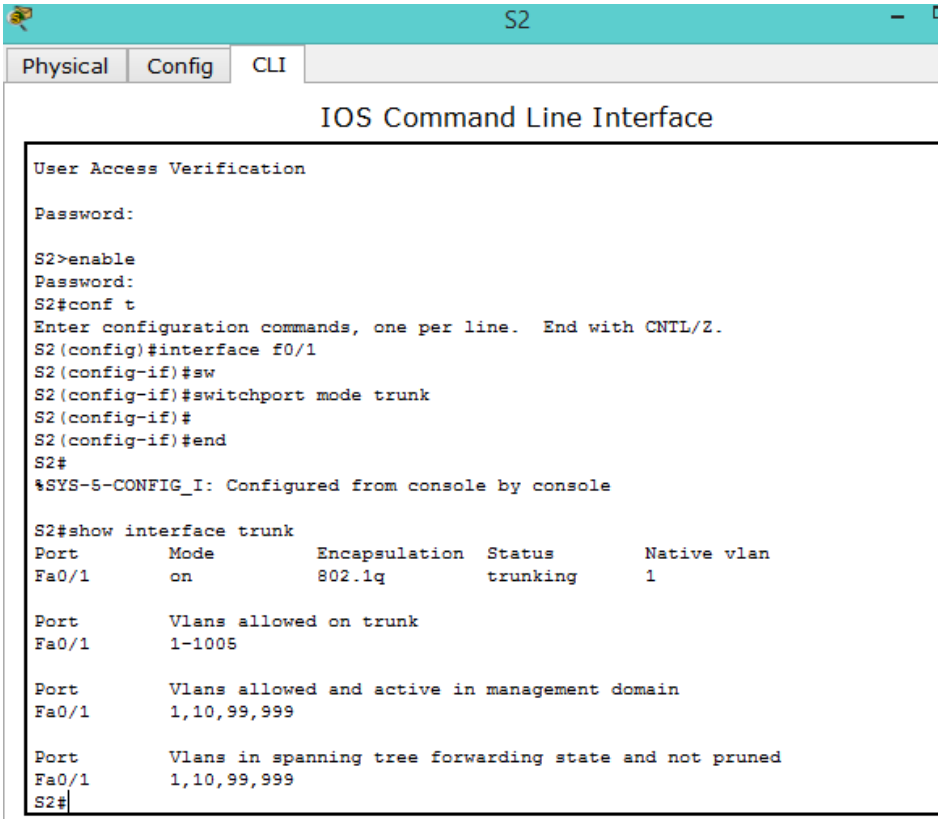
f. Configure el puerto F0/1 en el S2 como puerto de enlace troncal.

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

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

S1# **show interface trunk**

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

Port        Vlans allowed on trunk
Fa0/1       1-1005

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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
S1#
```



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 en el S1 y S2 es la Vlan 1.

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

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

```
S1#confi t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#sw
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

S1#
```

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:?

   Es un mensaje CDP (cisco discovery protocol) indica que entre la S1 y S2 tiene sus vlan que no coinciden. S2 tiene la vlan native a la vlan1 y S1 tiene la vlan native a la vlan 99.

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

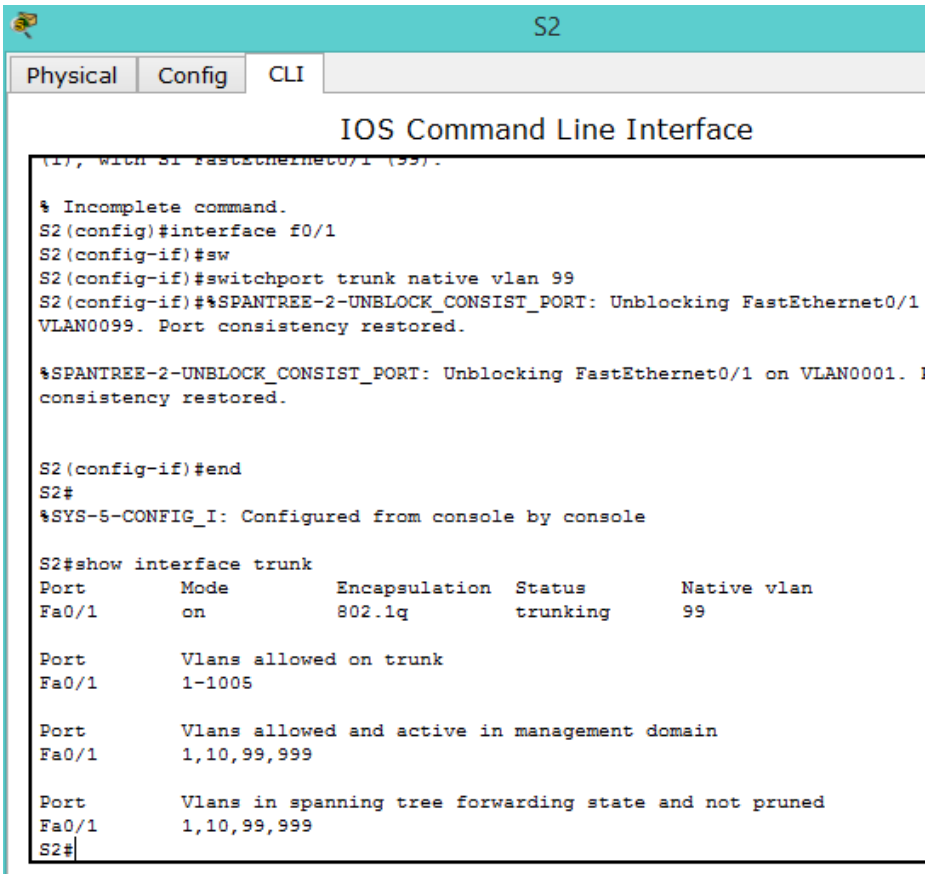
   S2(config)# **interface f0/1**

   S2(config-if)# **switchport trunk native vlan 99**

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

   S1# **show interface trunk**

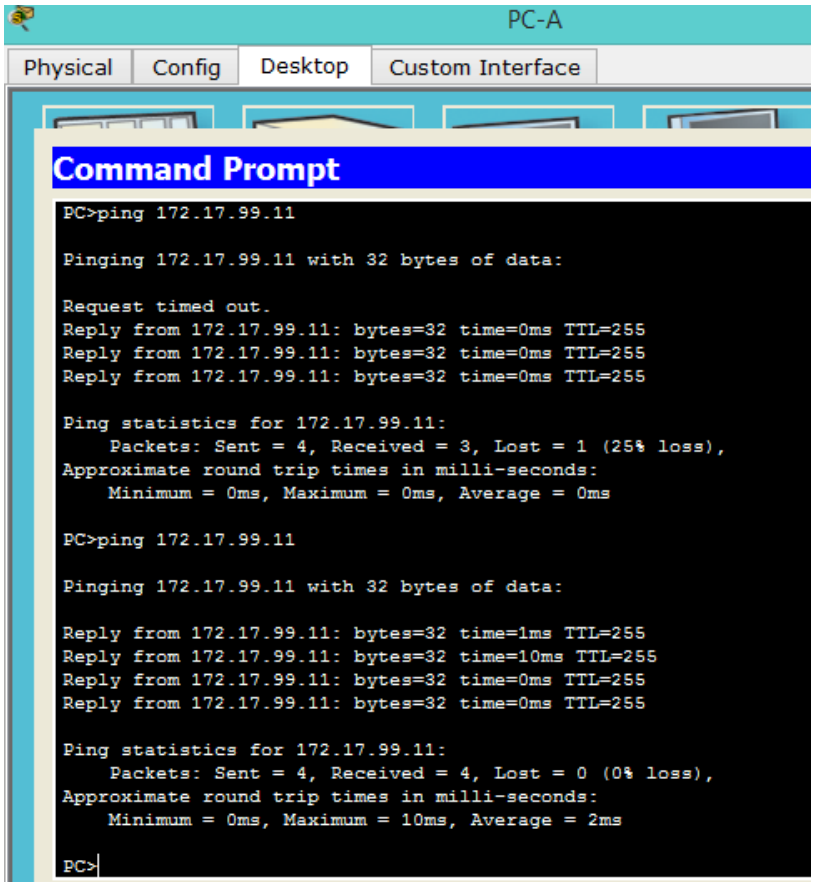
```
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-1005

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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
S1#
```



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?

   El ping es exitoso, Porque la PC-A esta en la misma vlan de la interface administrativa del switch.



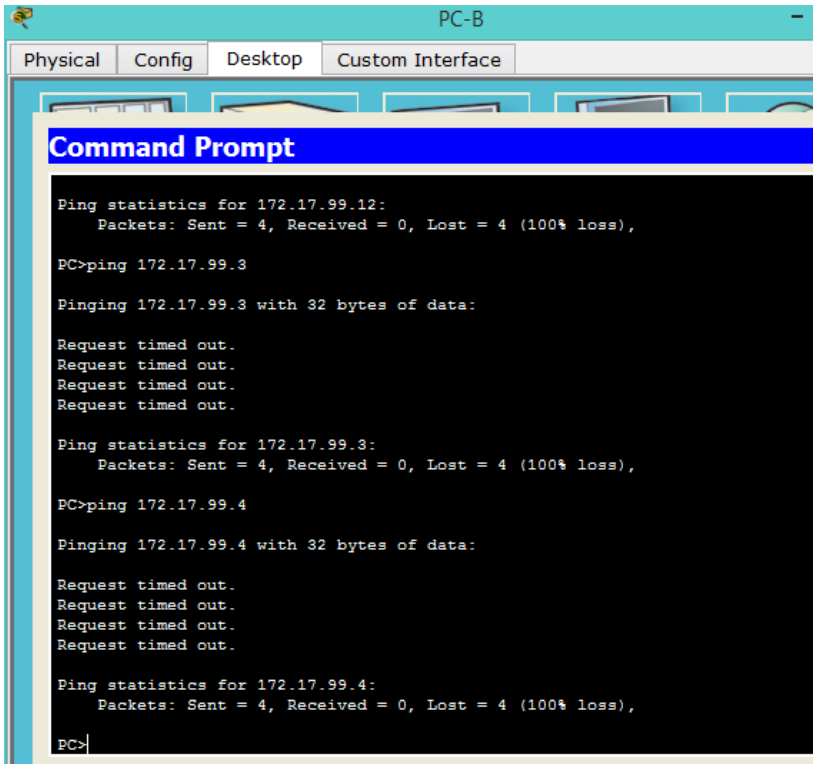
b. En la sesión de consola del S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?

   El ping es exitoso. Porque las troncales han sido satisfatoriamente establecidas y ambos switches estan en la misma vlan 99

```
S1#ping 172.17.99.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/3/11 ms

S1#
```

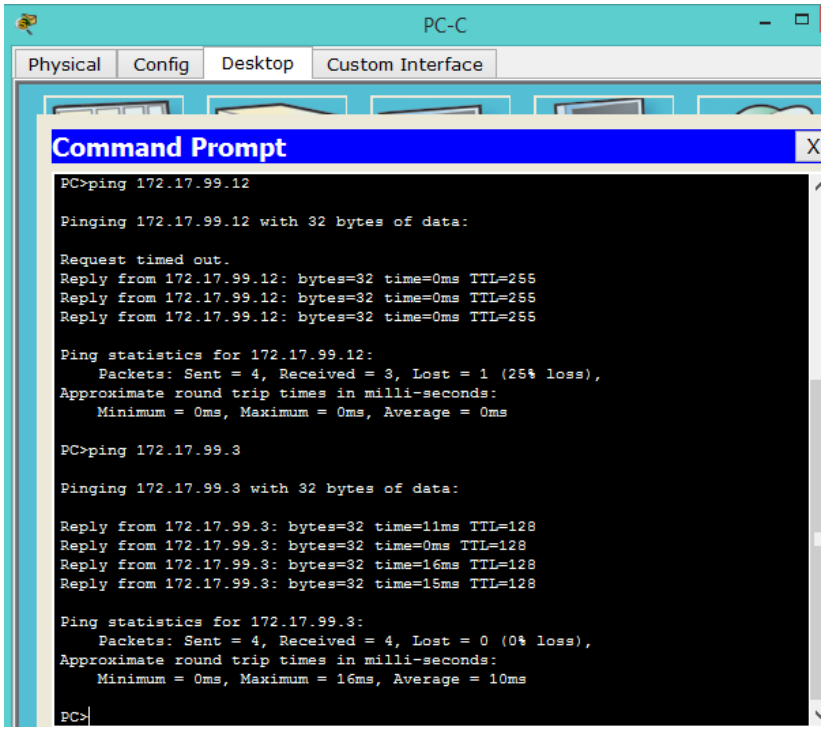
c. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué?

   Los ping desde la PC-B a la S1, S2, PC-A y PC-C no son satisfactorios. Porque la PC-B esta en la vlan 10 y los otros están en la vlan 99. No hay dispositivo de capa 3 que pueda rutear entre las redes.



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

Todos los ping fueron exitosos. Porque la PC-C está en la misma vlan que S1 ,S2 y PC-A.



impedir el uso de DTP en el S1 y el S2.

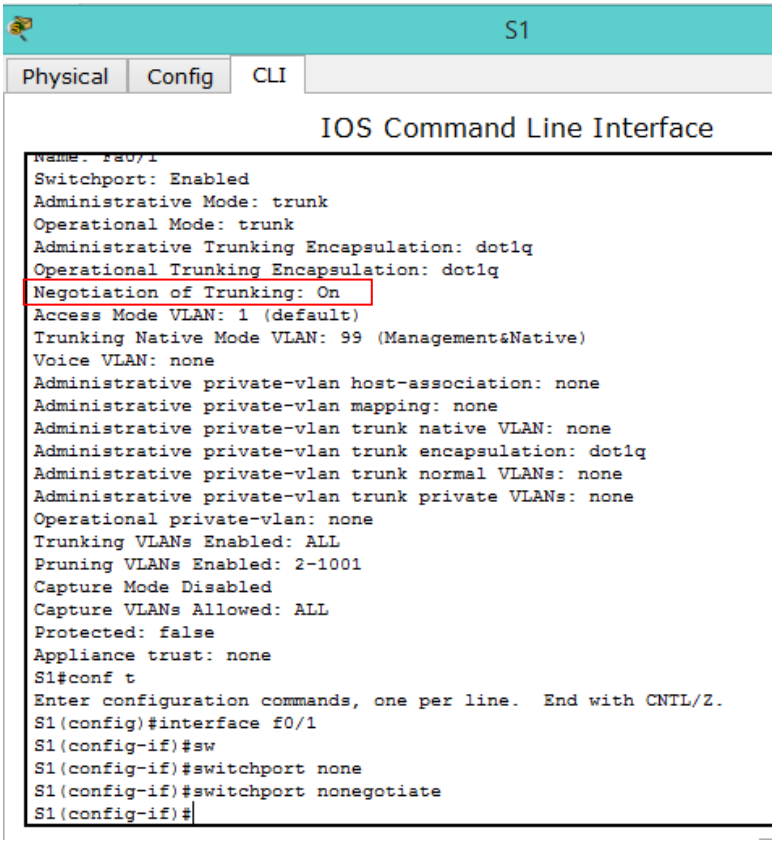
Cisco utiliza un protocolo exclusivo conocido como “protocolo de enlace troncal dinámico” (DTP) en los switches. Algunos puertos negocian el enlace troncal de manera automática. Se recomienda desactivar la negociación. Puede ver este comportamiento predeterminado mediante la emisión del siguiente comando:

S1# **show interface f0/1 switchport**

a. Desactive la negociación en el S1.

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

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



b. Desactive la negociación en el S2.

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

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

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**

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#sw
S2(config-if)#switchport none
S2(config-if)#switchport nonegotiate
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show interface f0/1 sw
S2#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
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Management&Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
```

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**

```
S1>enable
Password:
Password:
S1#show interface f0/2sw
S1#show interface f0/2 sw
S1#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

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.

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

S1# **show interface f0/2 switchport**

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

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

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**

```
S1#show vlan brief

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

De manera predeterminada, se permite transportar todas las VLAN en los puertos de enlace troncal. Por motivos de seguridad, se recomienda permitir que solo se transmitan las VLAN deseadas y específicas a través de los enlaces troncales en la red.

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

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

S1(config-if)# **switchport trunk allowed vlan 10,99**

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

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#sw
S2(config-if)#switchport  trunk allowed vlan 10,99
S2(config-if)#
```

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

S1# **show interface trunk**

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

Port        Vlans allowed on trunk
Fa0/1       10,99

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

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

¿Cuál es el resultado?

Que solo la vlan 10 y la vlan 99 están permitidas en el enlace troncal entre S1 y S2.

Reflexión

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

Que desde un principio todas la vlan están por defecto asignadas a la vlan 1, esto causa un problema de seguridad. Otro problema es que muchos switches troncales están en la auto negociación, de tal forma los enlaces troncales pueden ser manipulados sin nuestro consentimiento.

Informe No. 9

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

Topología

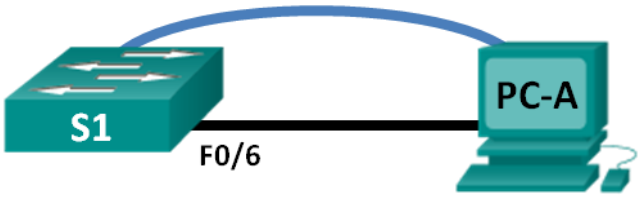


Tabla de direccionamiento

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

Objetivos

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

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

Configurar los parámetros básicos del switch.

Configurar la dirección IP de la computadora.

Parte 3: verificar y probar la conectividad de red

Mostrar la configuración del dispositivo.

Probar la conectividad de extremo a extremo con ping.

Probar las capacidades de administración remota con Telnet.

Guardar el archivo de configuración en ejecución del switch.

Parte 4: administrar la tabla de direcciones MAC

Registrar la dirección MAC del host.

Determine las direcciones MAC que el switch ha aprendido.

Enumere las opciones del comando **show mac address-table**.

Configure una dirección MAC estática.

Información básica/situación

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

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

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

Nota: asegúrese de que el switch se haya borrado y no tenga una configuración de inicio. Consulte el apéndice A para conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)

1 computadora (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term, y capacidad para Telnet)

Cable de consola para configurar el dispositivo con IOS de Cisco mediante el puerto de consola

Cable Ethernet, como se muestra en la topología

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.

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

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.

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?

R: Porque es Swich en este momento carece de configuración IP y por tanto es imposible el acceso remoto.

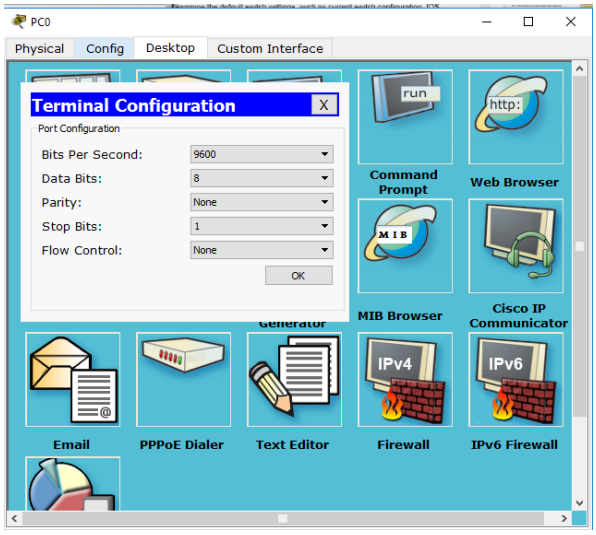
_____

_____

_____

_____

Verificar la configuración predeterminada del switch.



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

Puede acceder a todos los comandos IOS del switch en el modo EXEC privilegiado. Se debe restringir el acceso al modo EXEC privilegiado con protección con contraseña

para evitar el uso no autorizado, dado que proporciona acceso directo al modo de configuración global y a los comandos que se usan para configurar los parámetros de funcionamiento. Establecerá las contraseñas más adelante en esta práctica de laboratorio.

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

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.

Examine el archivo de configuración activa actual.

Switch# **show running-config**

```
Switch>enable
Switch#show running-config
Building configuration...

Current configuration : 1043 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

- ¿Cuántas interfaces FastEthernet tiene un switch 2960? R: 24

- ¿Cuántas interfaces Gigabit Ethernet tiene un switch 2960? R: 2
- ¿Cuál es el rango de valores que se muestra para las líneas vty? R: 16

Examine el archivo de configuración de inicio en la NVRAM.

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

¿Por qué aparece este mensaje? R: Por qué no hemos guardado nada en NVRAM

Examine las características de la SVI para la VLAN 1.

Switch# **show interface vlan1**

```
Switch#show interface vlan1
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 000a.f3a3.e05d (bia 000a.f3a3.e05d)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
Switch#
```

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

```
interface Vlan1
 no ip address
 shutdown
```

- ¿Cuál es la dirección MAC de esta SVI? R: 000a.f3a3.e05d
- ¿Está activa esta interfaz? R: Esta Administrativamente apagada

```
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 000a.f3a3.e05d (bia 000a.f3a3.e05d)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Examine las propiedades IP de la VLAN 1 SVI.

Switch# **show ip interface vlan1**

- ¿Qué resultado ve? R: La IP aún no está configurada, por tanto esta administrativamente apagada

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

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.

Switch# **show ip interface vlan1**

¿Qué resultado ve?

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

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

Switch# **show versión**

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

- ¿Cuál es la versión del IOS de Cisco que está ejecutando el switch? R: Version 12.2 (25)FX
- ¿Cuál es el nombre del archivo de imagen del sistema? R: C2960-LANBASE-M
- ¿Cuál es la dirección MAC base de este switch? R: 000A.F3A3.E05D

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

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 000A.F3A3.E05D
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01
```

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

Switch# **show interface f0/6**

- ¿La interfaz está activa o desactivada? R: FastEthernet0/6 is up, line protocol is up (connected)
- ¿Qué haría que una interfaz se active? R: La conexión Física del cable Ethernet de la PC-A al puerto 6 en el switch
- ¿Cuál es la dirección MAC de la interfaz? R: 000a.f3d3.6506
- ¿Cuál es la configuración de velocidad y de dúplex de la interfaz? R: Full-duplex, 100Mb/s

```
Switch#show interface f0/6
FastEthernet0/6 is up, line protocol is up (connected)
  Hardware is Lance, address is 000a.f3d3.6506 (bia 000a.f3d3.6506)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
```

Examine la configuración VLAN predeterminada del switch.

Switch# **show vlan**

```
Switch#show vlan

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

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

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


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

¿Cuál es el nombre predeterminado de la VLAN 1? R: default

¿Qué puertos hay en esta VLAN? R: 24

¿La VLAN 1 está activa? R: Active

¿Qué tipo de VLAN es la VLAN predeterminada? R: VLAN 1_ type. enet

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.

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

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

64016384 bytes total (59601463 bytes free)
```

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

Configurar los parámetros básicos de los dispositivos de red

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

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.

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#
```

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.

Asigne el nombre de host del switch.

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

Configurar la encriptación de contraseñas.

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

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

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

Evite las búsquedas de DNS no deseadas.

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

Configure un mensaje MOTD.

```
S1(config)# banner motd #
Enter Text message.  End with the character '#'.
```

Unauthorized access is strictly prohibited. #

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

S1(config)# **exit**

S1#

*Mar 1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console

S1# **exit**

S1 con0 is now available

Press RETURN to get started.

Unauthorized access is strictly prohibited.

S1>

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

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.

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.

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).

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
```

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)#

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)#

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**?

_____

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.

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.

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.

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

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

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

```
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password 7 104D000A0618
 logging synchronous
 login
line vty 0 4
 password 7 14141B180F0B
 login
line vty 5 15
 password 7 14141B180F0B
 login
!
end

S1#
```

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? _____

¿Cuál es el estado de la VLAN 99? _____

¿Cuál es el estado del protocolo de línea? _____

Probar la conectividad de extremo a extremo con ping.

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**

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.

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"**

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**

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

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

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#

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.

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.

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? _____

¿Cuántas direcciones MAC hay en total? _____

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

_____

Enumerar las opciones del comando show mac address-table.

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**?

_____

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? _____

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

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

Configure una dirección MAC estática.

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**

Verifique que la tabla de direcciones MAC se haya eliminado.

S1# **show mac address-table**

¿Cuántas direcciones MAC estáticas hay?

_____
_____

¿Cuántas direcciones dinámicas hay?

_____
_____

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? _____

¿Por qué cambió esto desde la última visualización?

_____
_____

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

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**

Verifique las entradas de la tabla de direcciones MAC.

S1# **show mac address-table**

¿Cuántas direcciones MAC hay en total? _____

¿Cuántas direcciones estáticas hay?

_____
_____

_____
_____

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**

Verifique que la dirección MAC estática se haya borrado.

S1# **show mac address-table**

¿Cuántas direcciones MAC estáticas hay en total? _____

Reflexión

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

_____
_____

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

_____
_____

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

_____
_____

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

_____
_____

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

Step 1: inicializar y volver a cargar el router.

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

Router> **enable**

Router#

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

Router# **erase startup-config**

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

[OK]

Erase of nvram: complete

Router#

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

Router# **reload**

Proceed with reload? [confirm]

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

Nota: es posible que reciba una petición de entrada para guardar la configuración en ejecución antes de volver a cargar el router. Responda escribiendo **no** y presione Enter.

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

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

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

e. Aparece otra petición de entrada para finalizar la instalación automática. Responda escribiendo **yes** (sí) y presione Enter.

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

Inicializar y volver a cargar el switch.

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

Switch> **enable**

Switch#

g. 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#

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

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

i. 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.

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

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

k. 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#

l. 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**

m. 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>

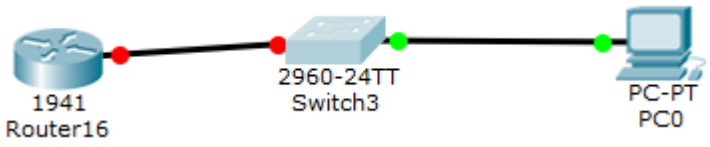
Informe No. 10

2.2.4.11: Lab: Configuring Switch Security Features

Establecer la topología e inicializar los dispositivos

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

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



Inicializar y volver a cargar el router y el switch.

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

Switch> enable

Switch#

```
Switch>enable
Switch#
```

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

Switch# show flash

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

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

64016384 bytes total (59601463 bytes free)
```

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

Switch# delete vlan.dat

Delete filename [vlan.dat]?

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

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

Delete flash:/vlan.dat?

[confirm] Switch#

f. Utilice el comando erase startup-config para eliminar el archivo de configuración de inicio de la NVRAM.

Se le solicitará que confirme la eliminación del archivo de configuración. Presione Enter para confirmar que desea borrar este archivo. (Al pulsar cualquier otra tecla, se cancela la operación).

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

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

```
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0003.E4E1.169A
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

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


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
####
```

Paso 1. inicializar y volver a cargar el router.

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

Router> enable

```
Router>enable
Router#
```

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

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

Readonly ROMMON initialized

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

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
####
```

Configurar los parámetros básicos de los dispositivos y verificar la conectividad

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

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

Configurar los parámetros básicos en el R1.

Configure el nombre del dispositivo.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

Desactive la búsqueda del DNS.

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

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

```
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 172.16.99.1 255.255.255.0
R1(config-if)#no shutdown
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
```

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

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

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

```
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

Cifre las contraseñas de texto no cifrado.

```
R1#show running-configuration
                             ^
% Invalid input detected at '^' marker.

R1#show running-config
Building configuration...

Current configuration : 749 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password class
!
```

Despues de encriptar la contraseña

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

R1#show running-config
Building configuration...

Current configuration : 773 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password 7 0822404F1A0A
!
```

Guarde la configuración en ejecución en la configuración de inicio.

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

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.

n. Configure el nombre del dispositivo.

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

Desactive la búsqueda del DNS.

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

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

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

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

```
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

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

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

Cifre las contraseñas de texto no cifrado.

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

Guarde la configuración en ejecución en la configuración de inicio.

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

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)#

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

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#

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

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

```
S1#show vlan

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
 --More--
```

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

```
Vlan1                  unassigned      YES manual administratively down down

Vlan99                 172.16.99.11    YES manual up                    down
S1#
```

Paso 2.

Paso 3. ¿Por qué el protocolo figura como down, a pesar de que usted emitió el comando **no shutdown** para la interfaz VLAN 99?

Paso 4. **PORQUE NO SE HA CONFIGURADO EL PROTOCOLO, TAN SOLO SE HABILITO LA VLAN**

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

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

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? **STATUS=UP Y PROTOCOLO=UP**

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

Paso 5.

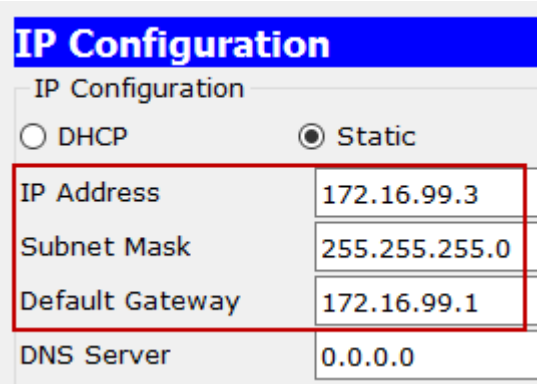
verificar la conectividad entre los dispositivos.

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

INICIALMENTE ERA PING NO EXITOSOS, PERO LUEGO DE CONFIGURAR EL PC CON LA IP, MASK Y GATEWAY DEL CUADRO LOS PING SON EXITOSOS.

```
PC>ping 172.16.99.1

Pinging 172.16.99.1 with 32 bytes of data:

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

```
Pinging 172.16.99.1 with 32 bytes of data:

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

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



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

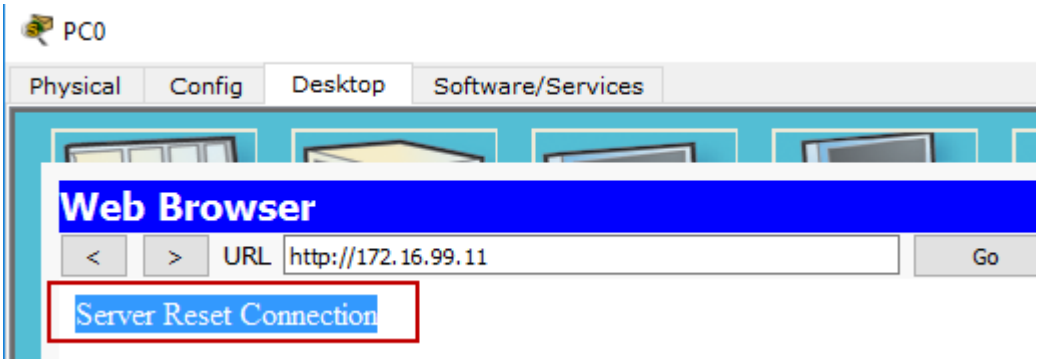
```
PC>ping 172.16.99.11

Pinging 172.16.99.11 with 32 bytes of data:

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

```
Pinging 172.16.99.11 with 32 bytes of data:

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

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

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

```
S1#ping 172.16.99.1

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

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



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

```
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

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

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

S1(config)# line vty 0 15

S1(config-line)# transport input ssh

S1(config-line)# login local

S1(config-line)# exit

```
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

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

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

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

S1# show ip ssh

```
S1#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

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

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

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

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

a. Modifique la configuración predeterminada de SSH.

b. S1# config t

S1(config)# ip ssh time-out 75

S1(config)# ip ssh authentication-retries 2

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

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

```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip ssh time-out 75
S1(config)#ip ssh authentication-retries 2
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 75 secs; Authentication retries: 2
S1#
```

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

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? _____

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

_____

_____

_____

_____

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

ESTA PRUEBA DEBE HACERCE EN UN ENTORNO REAL, PACKET TRACER NO FUNCIONA

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.

```
S1(config)#banner motd #ACCESO RESTRINGUIDO#
S1(config)#exit
```

```
Press RETURN to get started!

ACCESO RESTRINGUIDO
```

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

Puertos activos Fastethernet 5, 6 y VLAN99

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

FastEthernet0/1        unassigned      YES manual down                  down

FastEthernet0/2        unassigned      YES manual down                  down

FastEthernet0/3        unassigned      YES manual down                  down

FastEthernet0/4        unassigned      YES manual down                  down

FastEthernet0/5        unassigned      YES manual up                    up

FastEthernet0/6        unassigned      YES manual up                    up

FastEthernet0/7        unassigned      YES manual down                  down

FastEthernet0/8        unassigned      YES manual down                  down

FastEthernet0/9        unassigned      YES manual down                  down

FastEthernet0/10       unassigned      YES manual down                  down

 --More-- |

Vlan99                 172.16.99.11    YES manual up                      up
```

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#

```
S1(config)#interface range f0/1-4
S1(config-if-range)#shutdown

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

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

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

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
S1(config-if-range)#interface range f0/7-24
S1(config-if-range)#shutdown

%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 FastEthernet0/18, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively
down

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

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively
down
S1(config-if-range)#interface range g0/1-2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively
down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively
down
S1(config-if-range)#
```

d.Emita el comando show ip interface brief en el S1. ¿Cuál es el estado de los puertos 0/1 a F0/4? **El estado es ADMINISTRATIVEVELY**

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

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

Paso 6. ¿Cuál es el estado del servidor HTTP? _____

Paso 7. ¿Qué puerto del servidor utiliza? _____

Paso 8. ¿Cuál es el estado del servidor seguro de HTTP?

_____

Paso 9. ¿Qué puerto del servidor seguro utiliza? _____

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**

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

Paso 10. _____

_____

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?

Paso 11. _____

_____

Cierre la sesión web en la PC-A.

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

S1#show ip ?
  access-lists  List access lists
  arp           IP ARP table
  dhcp          Show items in the DHCP database
  interface     IP interface status and configuration
  ssh           Information on SSH
S1#show ip
```

configurar y verificar la seguridad de puertos en el S1.

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

R1# **show interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

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

Paso 12. ¿Cuál es la dirección MAC de la interfaz G0/1 del R1?

```
R1#show interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is CN Gigabit Ethernet, address is 00d0.bac1.1002 (bia 00d0.bac1.1002)
  Internet address is 172.16.99.1/24
```

Paso 13. 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.

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

  99    0030.a39d.da78    DYNAMIC     Fa0/6
  99    00d0.bac1.1002    STATIC      Fa0/5
```

Configure la seguridad básica de los puertos.

Paso 14. **Nota:** normalmente, este procedimiento se realizaría en todos los puertos de acceso en el switch. Aquí se muestra F0/5 como ejemplo.

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**

Desactive el puerto.

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

Habilite la seguridad de puertos en F0/5.

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

Parte 2. **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.

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

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

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

S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address 00d0.bac1.1002
S1(config-if)#no shutdown

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

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

a. 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   : 00D0.BAC1.1002:99
Security Violation Count   : 0
```

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

ENABLE

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

```
R1#ping 172.16.99.3

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

fAhora 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

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

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

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

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

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

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

R1(config-if)#mac address aaaa.bbbb.cccc
                  ^
% Invalid input detected at '^' marker.

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

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

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

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

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

```
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)
```

EL PING ES NO EXITOSO PORQUE LA MAC CONFIGURADA NO ES LA CORRECTA

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

S1# **show port-security**

```
S1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)         (Count)
-----------------------------------------------------------------------
        Fa0/5        1            1                  1          Shutdown
-----------------------------------------------------------------------
```

```
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 interfaces f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 00e0.f787.3d05 (bia 00e0.f787.3d05)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

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

(mins)
----       -----------  ----                                 -----
-------------
99         00D0.BAC1.1002         SecureConfigured       FastEthernet0/5
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

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**

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

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

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

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

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

```
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)
```

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

```
R1#show interface f0/5
%Invalid interface type and number
R1#
```

Paso 15.

```
S1#show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 00e0.f787.3d05 (bia 00e0.f787.3d05)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Paso 16.

Paso 17. **EL PUERTO APARECE COMO DOWN**

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**

Paso 18. **Nota:** puede haber una demora mientras convergen los estados de los puertos.

```
S1#show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Lance, address is 00e0.f787.3d05 (bia 00e0.f787.3d05)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

Paso 19.

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

```
S1#show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Lance, address is 00e0.f787.3d05 (bia 00e0.f787.3d05)
 BW 100000 Kbit, DLY 1000 usec,
```

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

```
R1#ping 172.16.99.3

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

Reflexión

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

Se habilita la seguridad para proteger al switch de ataques, desbordamientos y falsas ip que intentaran conexiones a nuestra red

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

Para evitar que estos puertos sean utilizados como entrada de ataques informáticos, además podemos tener una mejor gestión de la red IP, sabiendo que elementos, puertos, interfaces están operativas y cuales no.

Informe No. 11

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

Topología

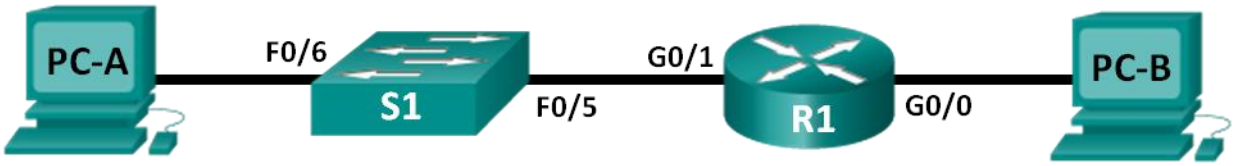


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

Realizar el cableado de los equipos para que coincidan con la topología de la red.

Inicializar y reiniciar el router y el switch.

Parte 2: configurar los dispositivos y verificar la conectividad

Asignar información de IPv4 estática a las interfaces de la computadora.

Configurar los parámetros básicos del router.

Verificar la conectividad de la red

Configurar el router para el acceso por SSH.

Parte 3: mostrar la información del router

Recuperar información del hardware y del software del router.

Interpretar el resultado de la configuración de inicio.

Interpretar el resultado de la tabla de routing.

Verificar el estado de las interfaces.

Parte 4: configurar IPv6 y verificar la conectividad

Información básica/situación

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

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

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

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960 con IOS de Cisco, versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que el router y el switch se hayan borrado y no tengan configuraciones de inicio. Consulte el apéndice A para conocer los procedimientos para inicializar y volver a cargar los dispositivos.

Recursos necesarios

1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)

2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

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

Cables Ethernet, como se muestra en la topología

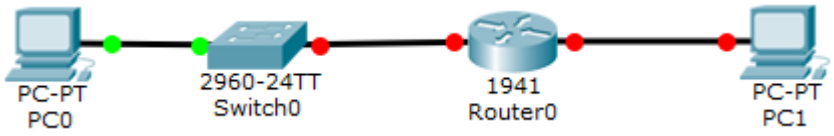
Nota: las interfaces Gigabit Ethernet en los ISR Cisco 1941 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre el router y la PC-B. Si utiliza otro modelo de router Cisco, puede ser necesario usar un cable cruzado Ethernet.

Parte 1: establecer la topología e inicializar los dispositivos

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.

Encienda todos los dispositivos de la topología.



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.

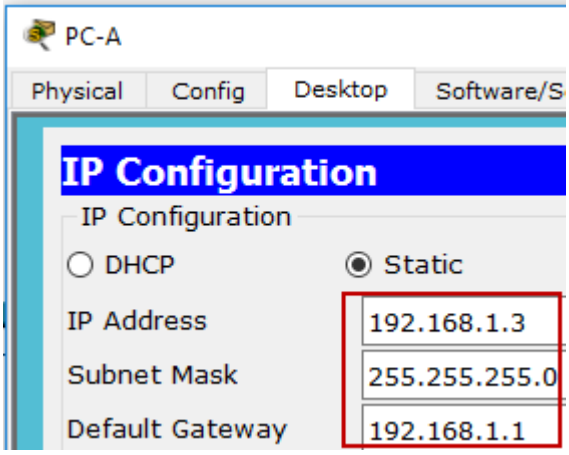
```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0090.2B25.815D
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

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


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
###################################
```

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

Readonly ROMMON initialized

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

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
#############
```

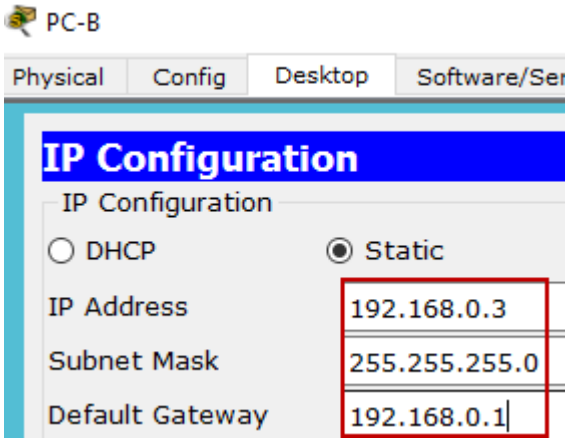
Parte 2: Configurar dispositivos y verificar la conectividad

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.



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



Configurar el router.

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

```
Router> enable
Router#
```

Ingrese al modo de configuración global.

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

Asigne un nombre de dispositivo al router.

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

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
```

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

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

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

_____
_____

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

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

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

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

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

_____
_____

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)#
```

Cifre las contraseñas de texto no cifrado.

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

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!#
```

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#
```

Configure el reloj en el router, por ejemplo:

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

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**?

EJECUCION COMANDOS

```
Router(config)#hostname R1
R1(config)#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 10
R1(config)#enable secret cisco12345
```

```
R1(config)#line console 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)#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)#service password-encryption
R1(config)#banner motd #Unauthorized access prohibited!#
R1(config)#int g0/0
R1(config-if)#description Connection to PC-B
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no 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

R1#clock
R1#clock set 21:06:00 30 April 2017
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

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?

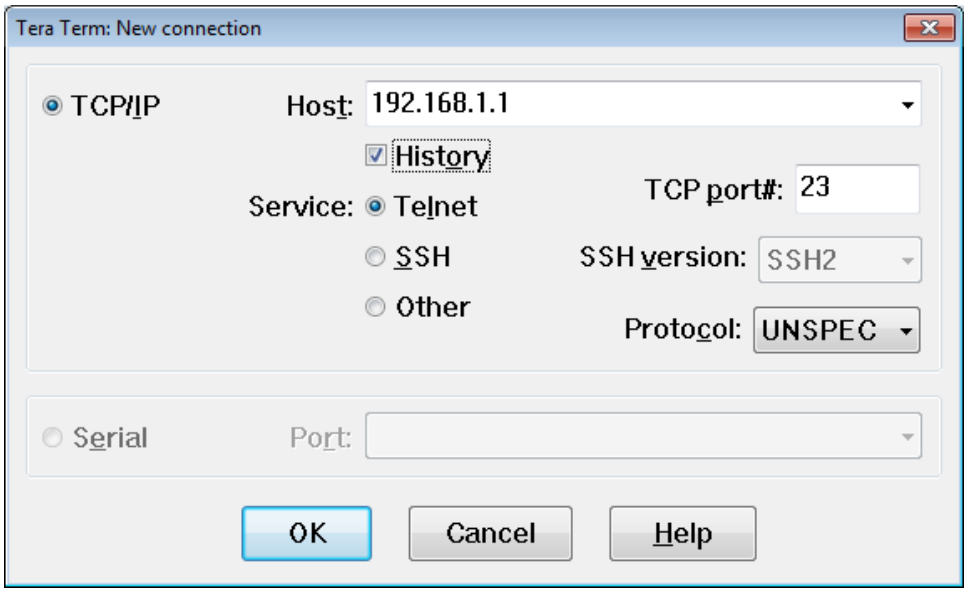
```
Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=1ms TTL=127
Reply from 192.168.0.3: bytes=32 time=11ms TTL=127
Reply from 192.168.0.3: bytes=32 time=0ms TTL=127
Reply from 192.168.0.3: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 5ms
```

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

_____
_____

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

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



¿Pudo conectarse remotamente? ____

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

_____
_____

_____
_____

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
```

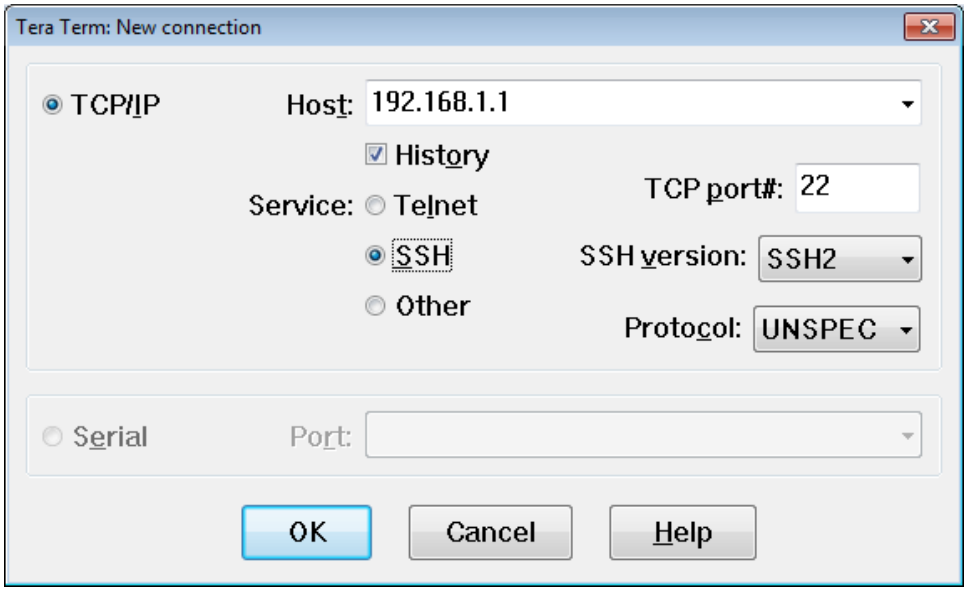
```
R1(config)# ip domain-name CCNA-lab.com
R1(config)# username admin privilege 15 secret adminpass1
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
R1(config)# crypto key generate rsa modulus 1024
R1(config)# exit
```

COMANDOS

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name CCNA-lab.com
R1(config)#username admin privilege 15 secret adminpass1
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#crypto key generate rsa modulus 1024
                                           ^
% Invalid input detected at '^' marker.

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

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

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



¿Pudo conectarse remotamente? ____

Parte 3: mostrar la información del router

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

Paso 1. establecer una sesión SSH para el R1.

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

recuperar información importante del hardware y el software.

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

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

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 21 hours, 17 minutes, 41 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

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

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

b. --More--

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

```
R1#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M) Version 15.1(4)M4,
```

¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) tiene el router? **255K**

```
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
```

¿Cuánta memoria flash tiene el router? **249856K**

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

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?

_____
_____

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?

```
hostname R1
!
!
!
enable secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUUl.
!
```

LA CLAVE ESTA ENCRIPTADA

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

¿Qué resultado se obtiene al usar este comando?

_____
_____

_____
_____

mostrar la tabla de routing en el router.

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

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

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

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```

¿Cuántas entradas de ruta están cifradas con un código C en la tabla de routing? **1**

```
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```

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.

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

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

NO SHUTDOWN

Parte 4: configurar IPv6 y verificar la conectividad

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

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

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

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

COMANDOS

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

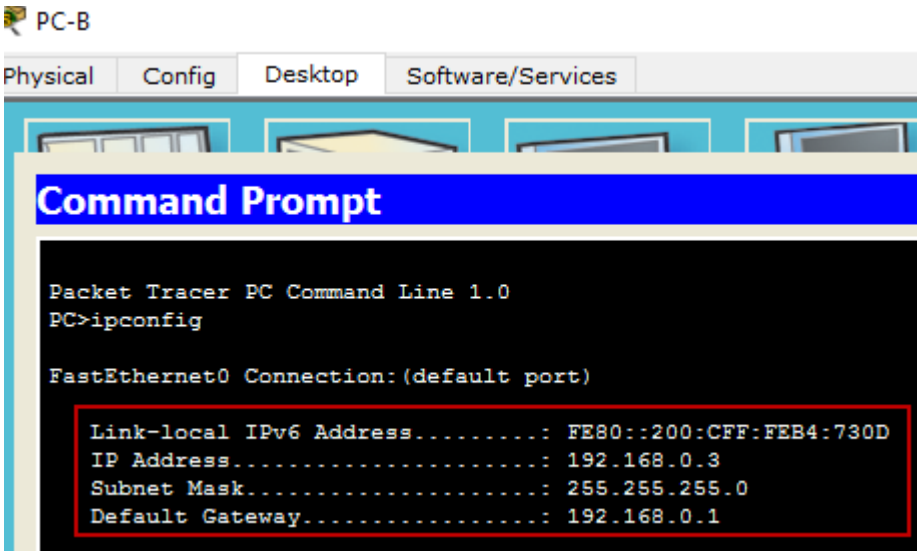
b. Use el comando **show ipv6 int brief** para verificar la configuración de IPv6 en el R1.

Si no se asignó una dirección IPv6 a la G0/1, ¿por qué se indica como [up/up]? **Porque no se ha habilitado el puerto**

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

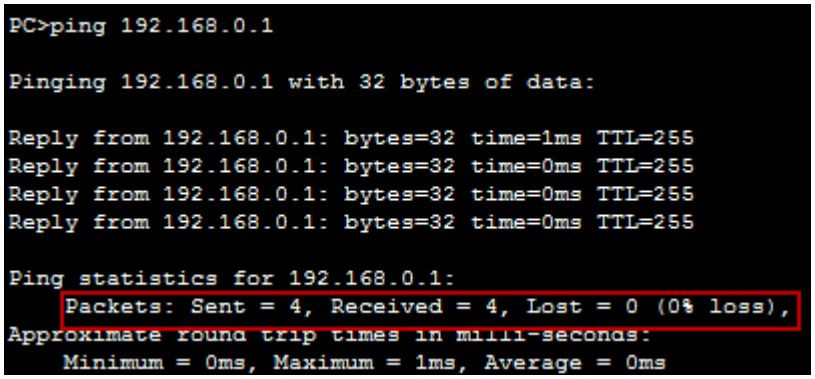
c. Emita el comando **ipconfig** en la PC-B para examinar la configuración de IPv6.

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

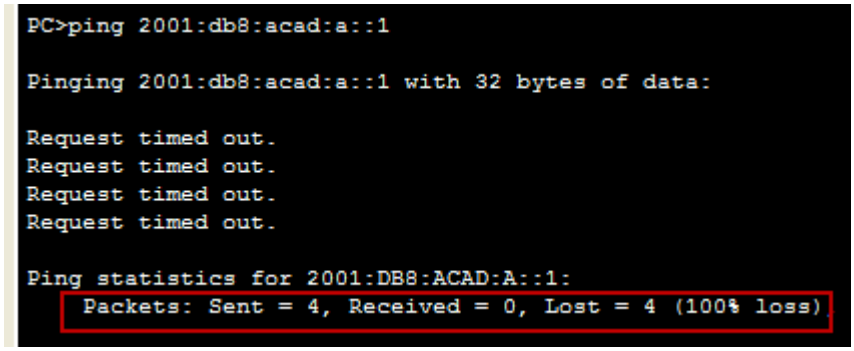


¿Cuál es el gateway predeterminado asignado a la PC-B? **192.168.0.1**

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



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



Reflexión

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

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

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? **si seria correcto el ping, porque estaría configurado la interface con IPV6**

Tabla de resumen de interfaces del router

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

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

Paso 1. inicializar y volver a cargar el router.

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

```
Router> enable
Router#
```

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#
```

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
```

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

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

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

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

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#
```

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#
```

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

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

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

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

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

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#
```

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
```

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

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

Informe No.12

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

Topología

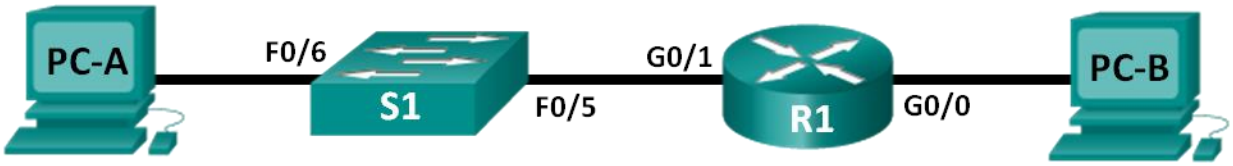


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	N/A	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

Parte 2: configurar los dispositivos y verificar la conectividad

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

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

Parte 5: configurar los parámetros del R1 con CCP

Parte 6: usar las utilidades de CCP

Información básica/situación

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

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

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

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

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

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)

2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

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

Cables Ethernet, como se muestra en la topología

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

Procesador de 2 GHz o más rápido

1 GB de DRAM como mínimo; se recomienda contar con 2 GB

400 MB de espacio en disco duro disponible

Internet Explorer 6.0 o más reciente

Resolución de pantalla de 1024x768 o superior

Java Runtime Environment (JRE), versión 1.6.0_11 o más reciente

Adobe Flash Player, versión 10.0 o más reciente, con la depuración configurada en No

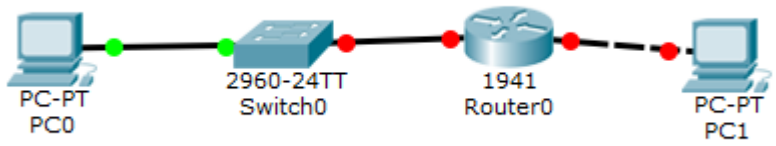
Nota: las interfaces Gigabit Ethernet en los ISR Cisco 1941 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre el router y la PC-B. Si utiliza otro modelo de router Cisco, puede ser necesario usar un cable cruzado Ethernet.

establecer la topología e inicializar los dispositivos

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

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

Encienda todos los dispositivos de la topología.



inicializar y volver a cargar el router y el switch.

```
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 00D0.BCA8.AECD
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

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


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
##########
```

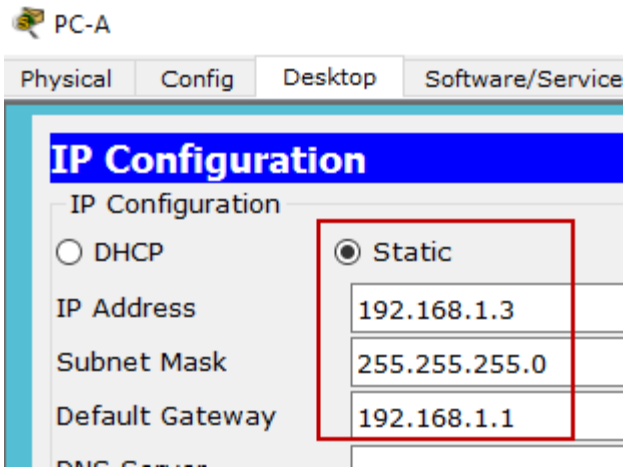
```
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE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

Readonly ROMMON initialized

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

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
#########
```

Configurar dispositivos y verificar la conectividad

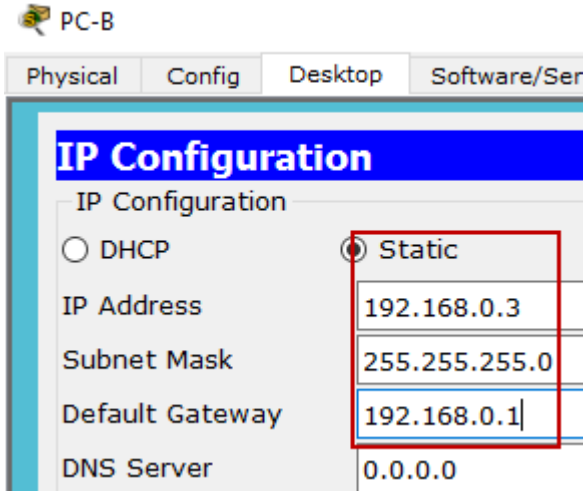
En la parte 2, configurará los parámetros básicos, como las direcciones IP de interfaz (solo G0/1), el acceso seguro a dispositivos y las contraseñas. Consulte la topología y la tabla de direccionamiento para conocer los nombres de los dispositivos y obtener información de direcciones.

Paso 1. Configure las interfaces de la PC.

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



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



Configurar el router.

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

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

Ingrese al modo de configuración global.

Desactive la búsqueda del DNS.

Asigne un nombre de dispositivo al router.

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

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

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

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

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

Cifre las contraseñas de texto no cifrado.

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

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

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

```
Router>enable
Router#configure terminal
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
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
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)#service password-encryption
R1(config)#banner motd #Unauthorized access prohibited!#
R1(config)#int g0/0
R1(config-if)#description Connection to PC-B
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown

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

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

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)#
```

Verificar la conectividad de la red

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

configurar el router para permitir el acceso de CCP

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

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

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

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

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

configurar el router para el acceso de CCP.

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

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

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

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

Paso 1. instalar CCP.

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

Descargue CCP 2.6 del sitio web de Cisco:

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

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

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

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

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

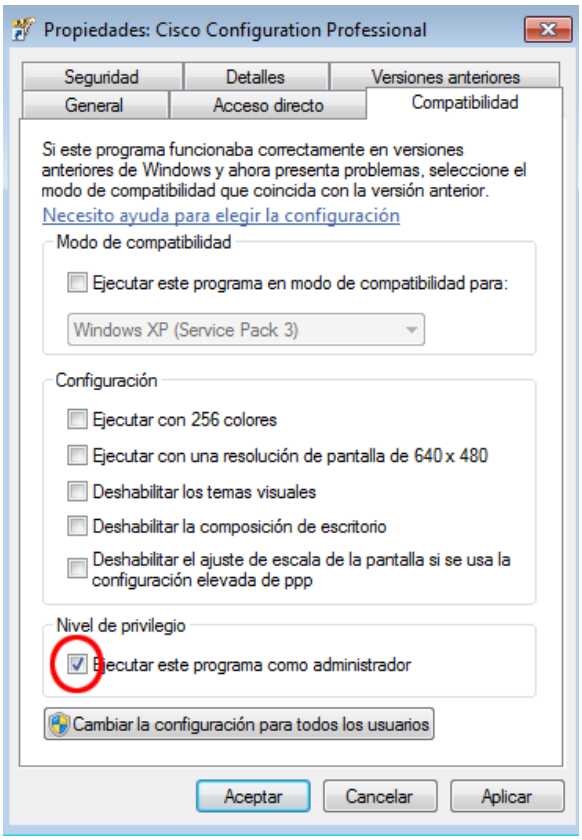
Siga las instrucciones en pantalla para instalar CCP 2.6 en la computadora.

cambiar la configuración para ejecutar como administrador.

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

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

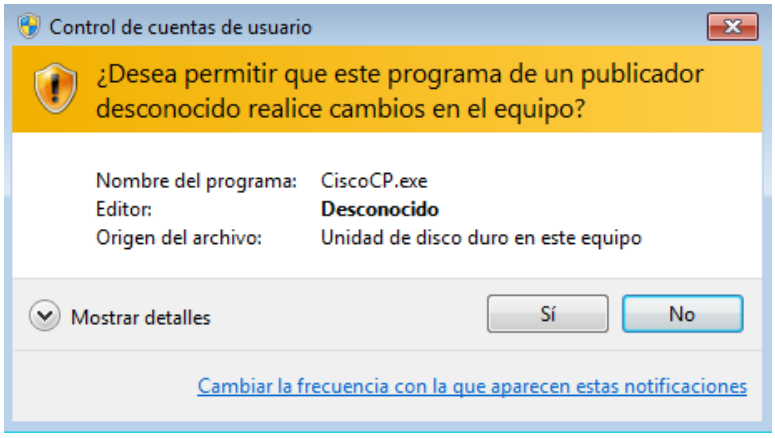
En el cuadro de diálogo Properties, seleccione la ficha **Compatibilidad**. En la sección Nivel de privilegio, haga clic en la casilla de verificación **Ejecutar este programa como administrador** y luego haga clic en **Aceptar**.



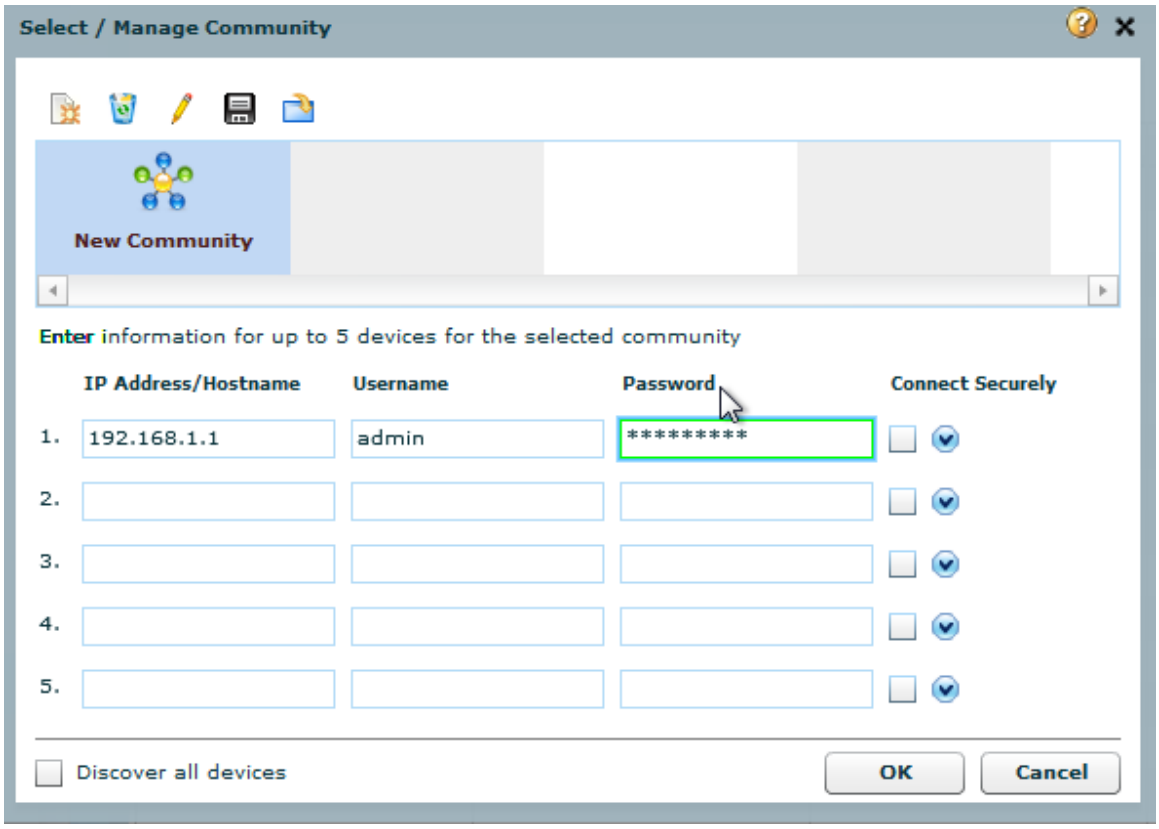
crear o administrar comunidades.

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

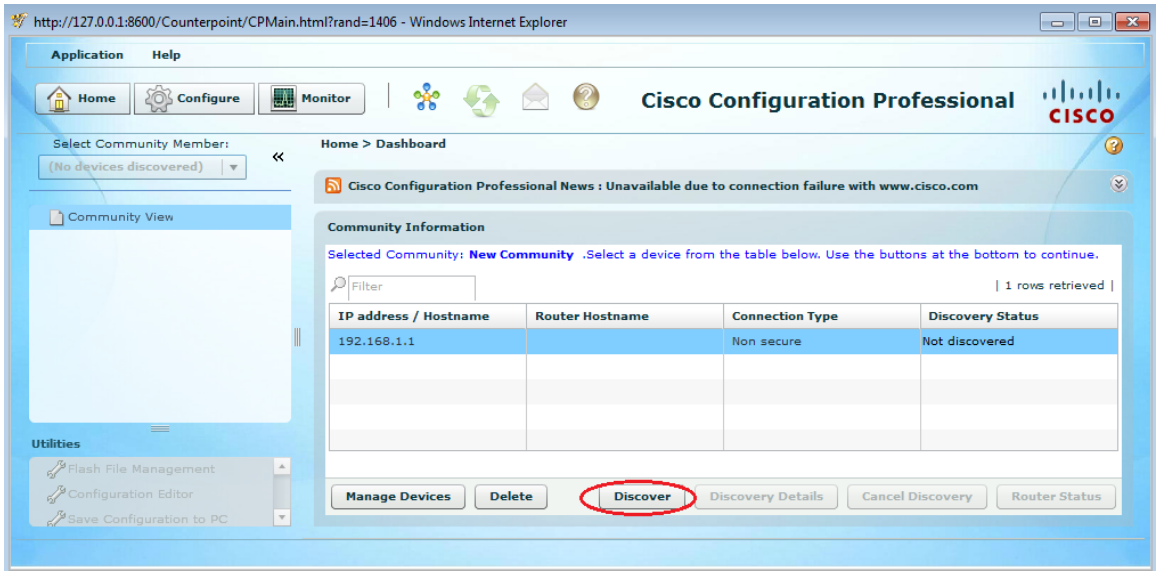
Si recibe un mensaje de advertencia de seguridad que le solicita que permita que el programa CiscoCP.exe realice cambios en la computadora, haga clic en **Sí**.



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



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



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

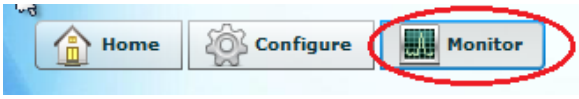
Nota: si hay un problema de configuración, verá el estado Discovery failed (Error de detección). Haga clic en **Discovery Details** (Detalles de detección) para determinar el motivo de la falla en el proceso de detección y luego resuelva el problema.

configurar los parámetros del R1 con CCP

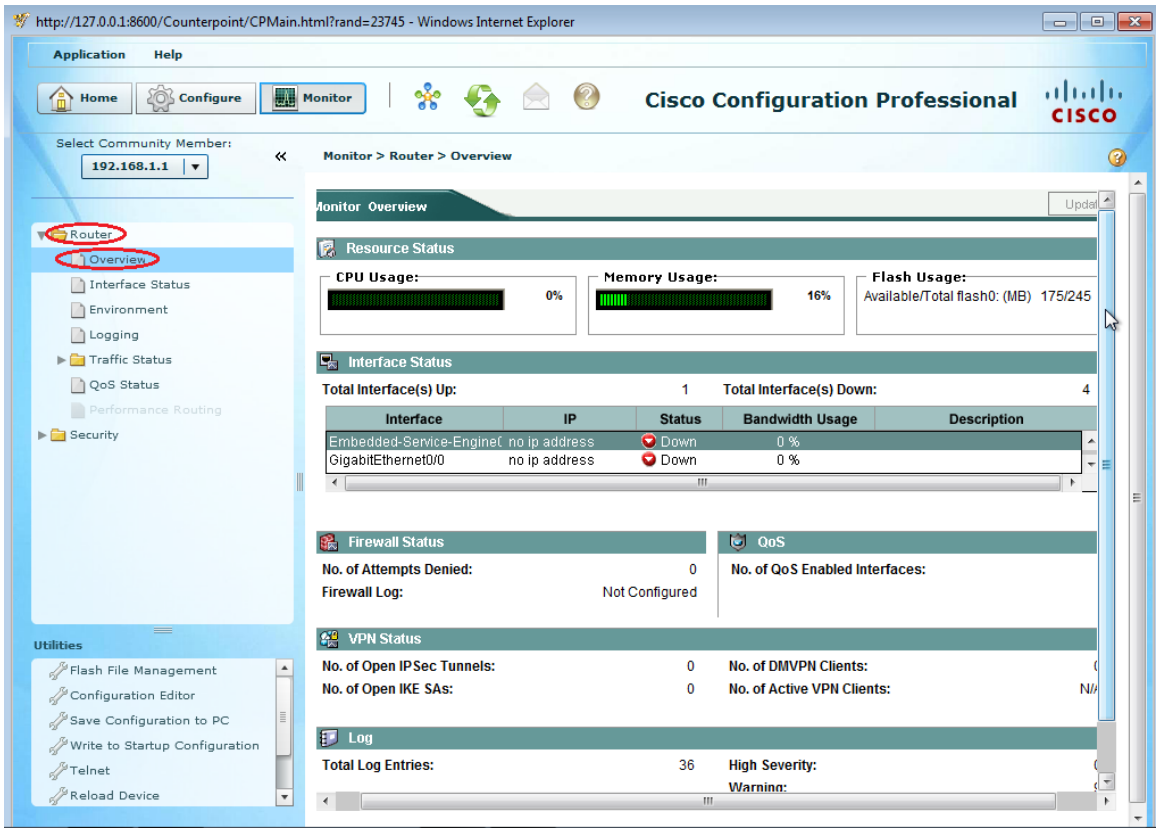
En la parte 5, utilizará CCP para mostrar información sobre el R1, configurará la interfaz G0/0, establecerá la fecha y hora, agregará un usuario a la base de datos local y cambiará la configuración de vty.

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

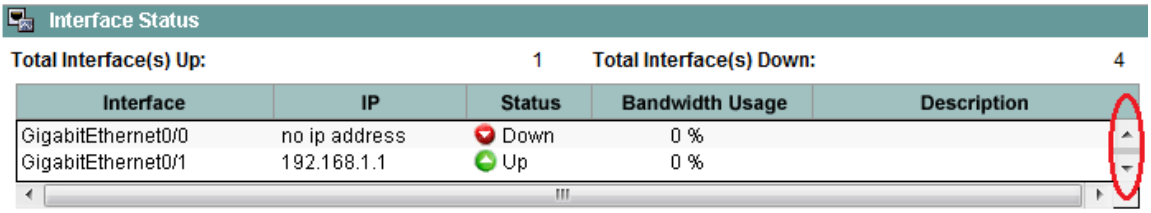
En la barra de herramientas de CCP, haga clic en **Monitor**.



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



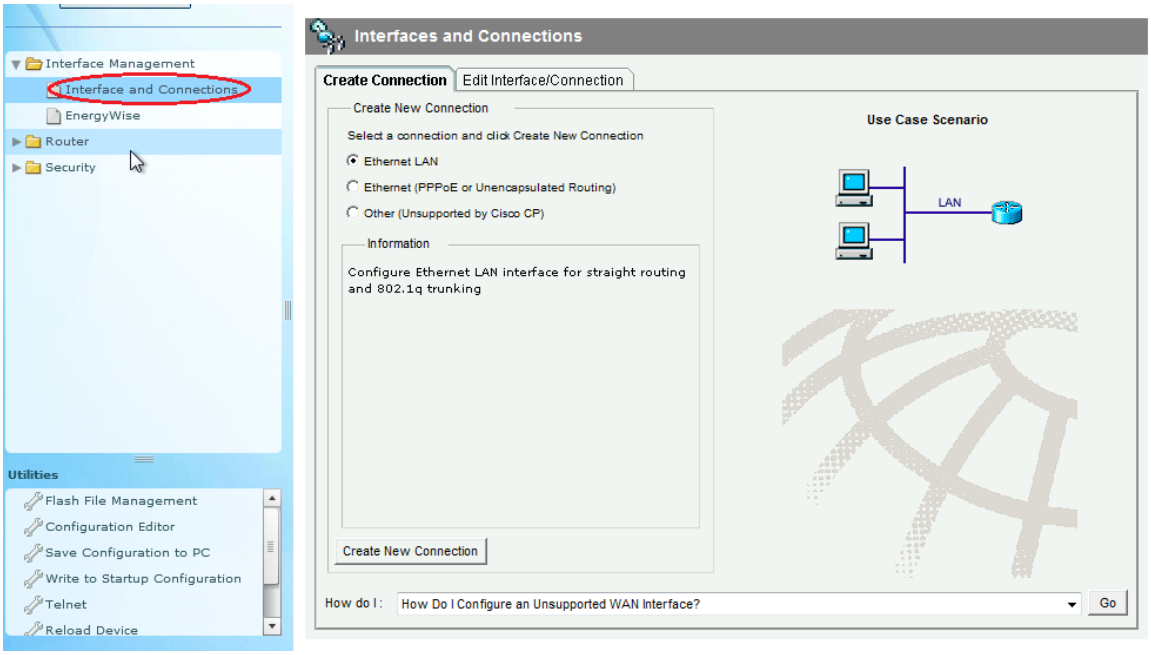
Utilice las flechas arriba y abajo en el lado derecho de la lista de interfaces para desplazarse por la lista de interfaces del router.



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

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

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



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

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

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

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

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

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

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

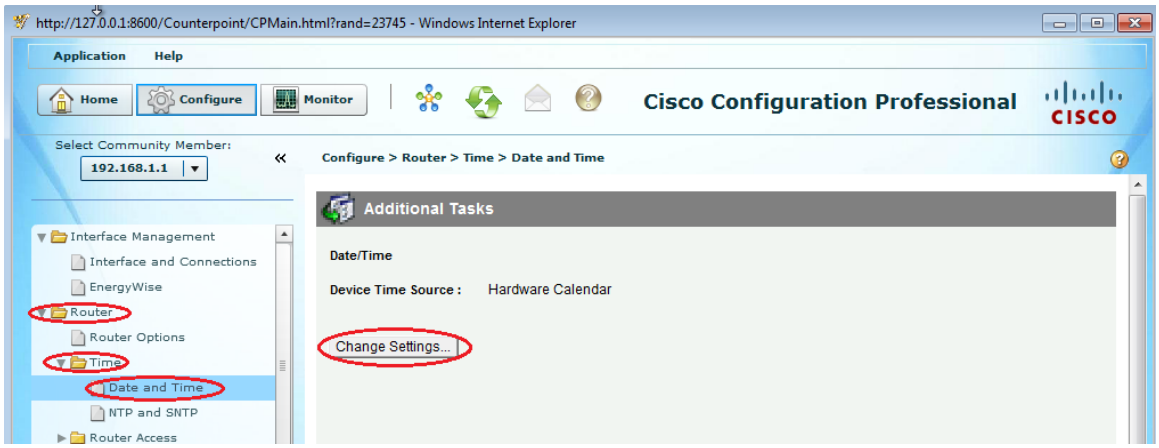
Haga clic en la casilla de verificación **Save running config to device's startup config** (Guardar configuración en ejecución en la configuración de inicio del dispositivo) y luego haga clic en **Deliver** (Entregar). Esta acción agrega los comandos que aparecen en la ventana de vista previa a la configuración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

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

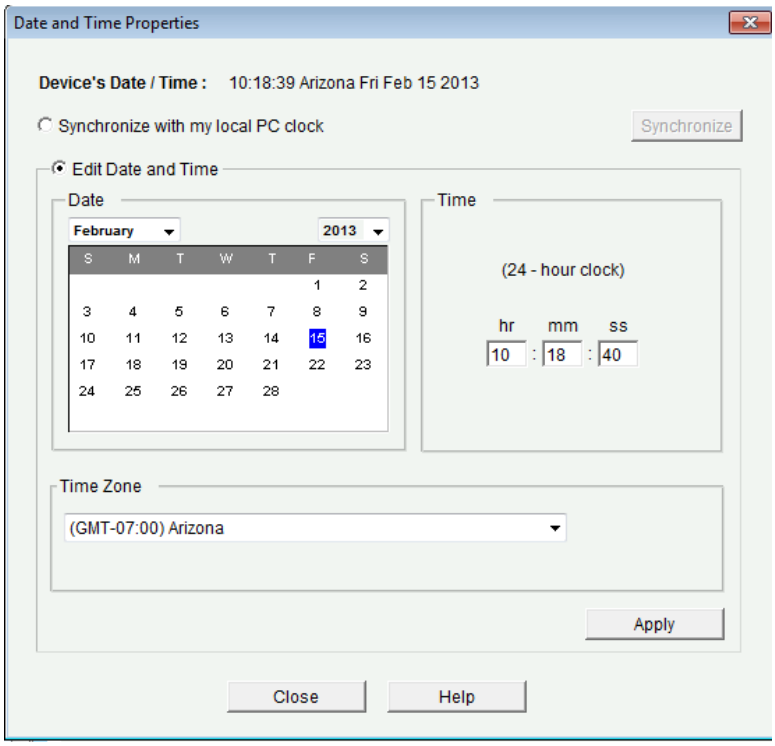
Interface	IP	Type	Slot	Status	Description
Embedded-Service-Engi	no IP address	Embedded-Service-Engin	0	Dow	
GigabitEthernet0/0	192.168.0.1	GigabitEthernet	0	Up	
GigabitEthernet0/1	192.168.1.1	GigabitEthernet	0	Up	Connection to S1 F0/5
Serial0/0/0	no IP address	Serial	0	Dow	
Serial0/0/1	no IP address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

establecer fecha y hora en el router.

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



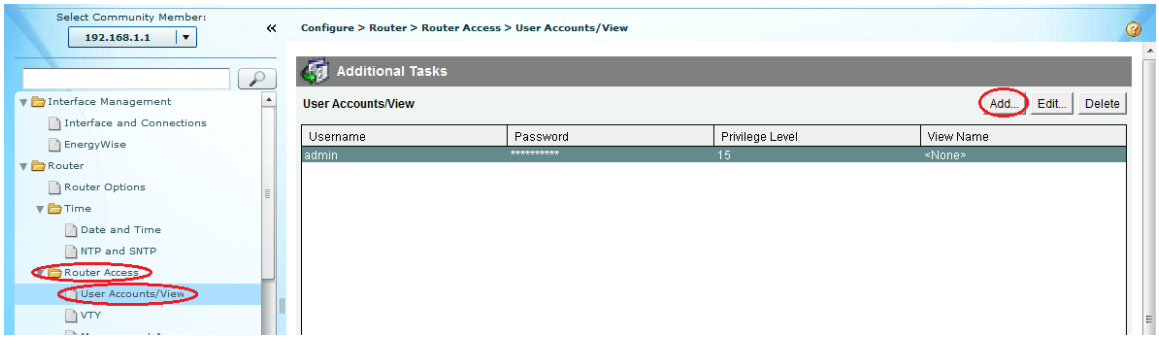
En la ventana Date and Time Properties (Propiedades de fecha y hora), edite Date (Fecha), Time (Hora) y Time Zone (Zona horaria). Haga clic en **Apply (Aplicar).**



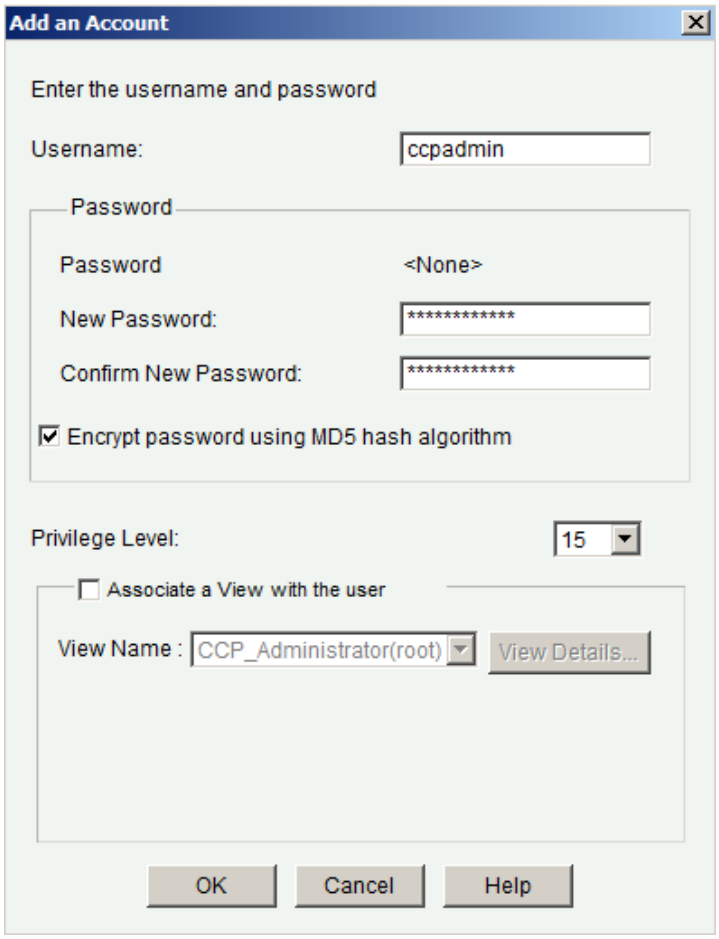
En la ventana de configuración del reloj de Router, haga clic en **OK**. En la ventana Date and Time Properties, haga clic en **Close** (Cerrar).

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

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

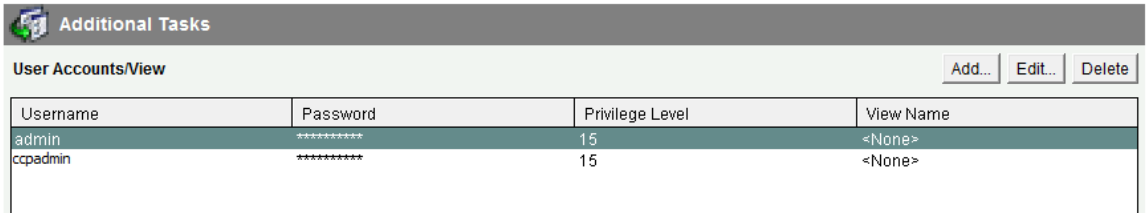


Introduzca **ccpadmin** en el campo Username: (Nombre de usuario:). Introduzca **ciscoccppass** en los campos New Password: (Contraseña nueva:) y Confirm New Password: (Confirmar contraseña nueva:). Seleccione **15** en la lista desplegable Privilege Level: (Nivel de privilegio). Haga clic en **OK**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



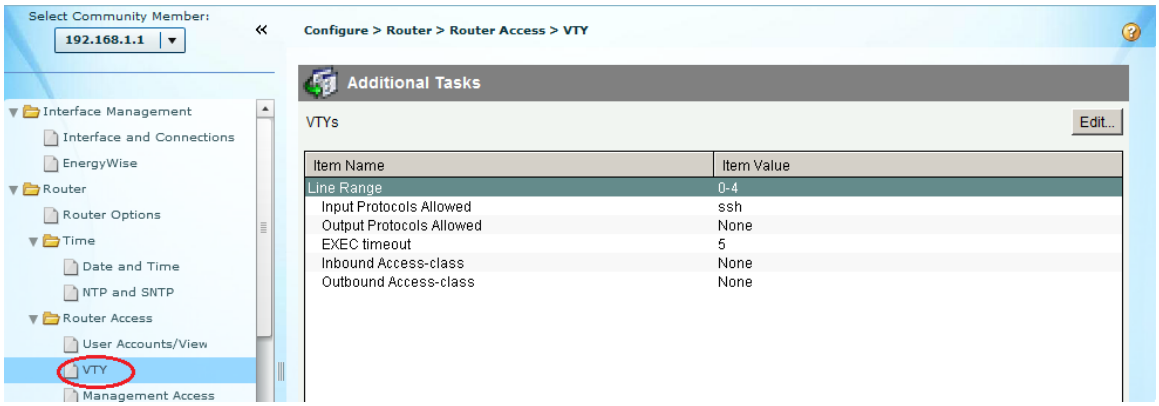
En la ventana Deliver Configuration to Device (Entregar configuración al dispositivo), haga clic en la casilla de verificación **Save running config to device's startup config** y luego haga clic en **Deliver**.

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

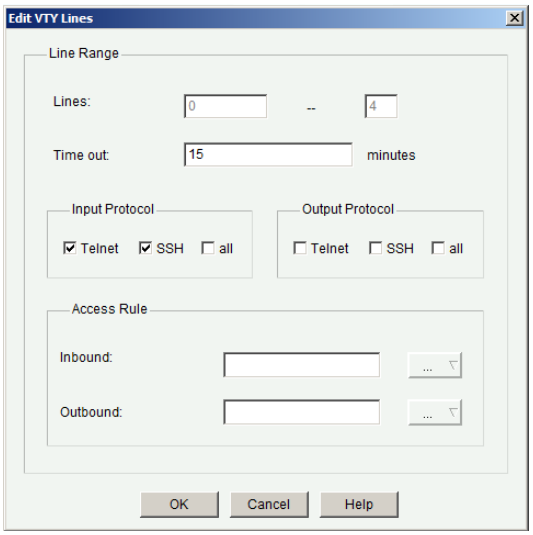


editar la configuración de las líneas vty.

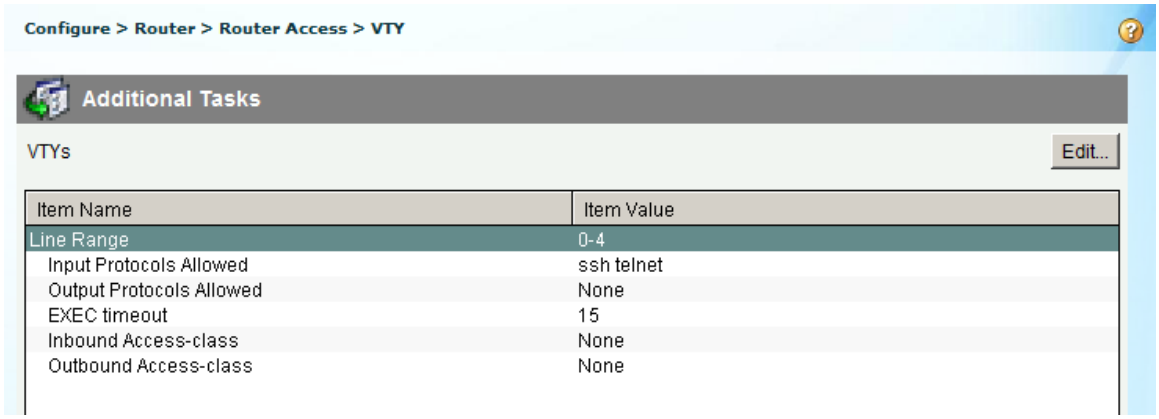
h. En el panel de navegación izquierdo, seleccione **Router Access** > **VTY** (Acceso al router > VTY) para visualizar la ventana Additional Tasks > VTYs (Tareas adicionales > VTY) en el panel de contenido derecho. Haga clic en **Edit…** (Editar).



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



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

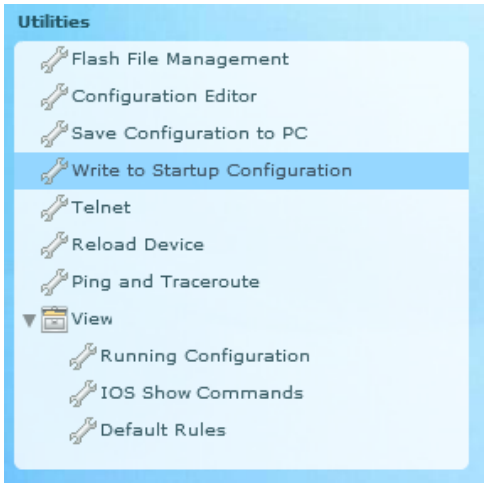


usar utilidades de CCP

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

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

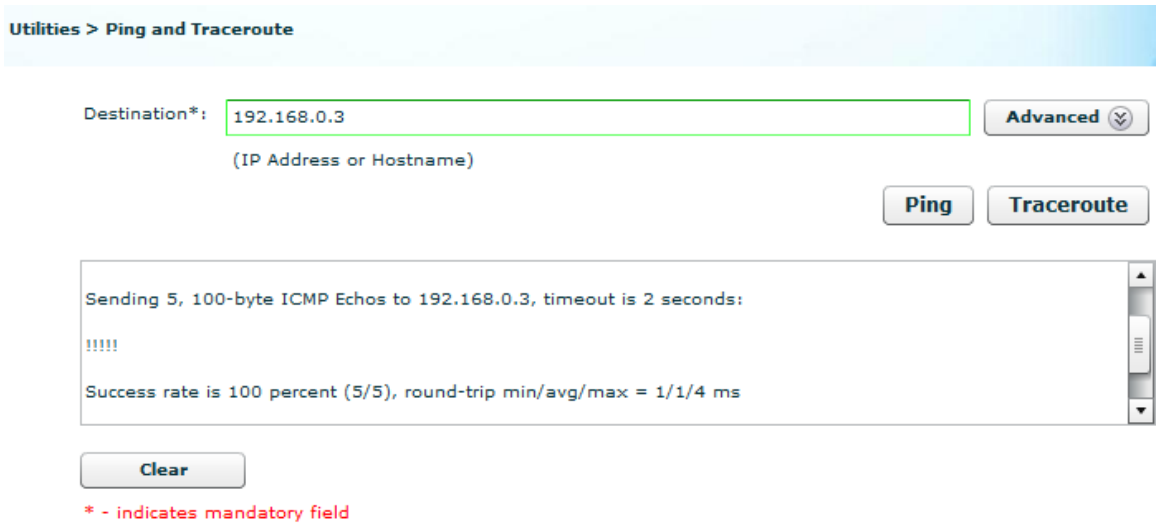
En la parte inferior del panel de navegación izquierdo, busque el panel Utilities (Utilidades). Haga clic en **Write to Startup Configuration** (Escribir en la configuración de inicio).



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

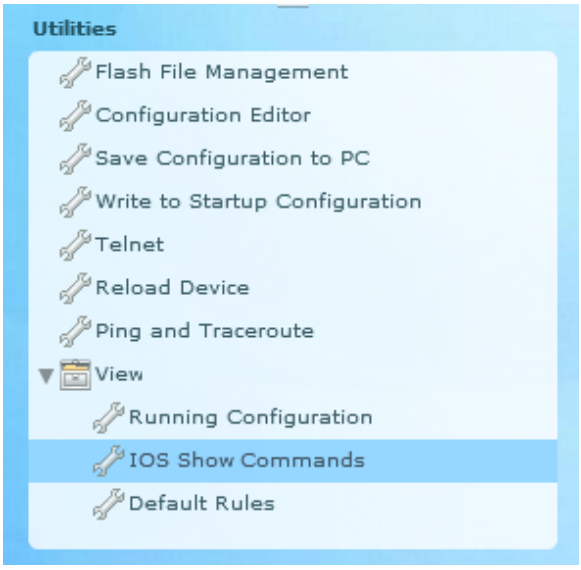
usar la utilidad Ping para probar la conectividad a la PC-B.

i. En el panel Utilities (Utilidades), haga clic en **Ping and Traceroute** (Ping y traceroute) para mostrar la pantalla Ping and Traceroute en el panel de contenido. Introduzca **192.168.0.3** en el campo Destination*: (Destino*:) y luego haga clic en **Ping**. Use la barra de desplazamiento ubicada a la derecha del cuadro de resultados para ver los resultados del ping.

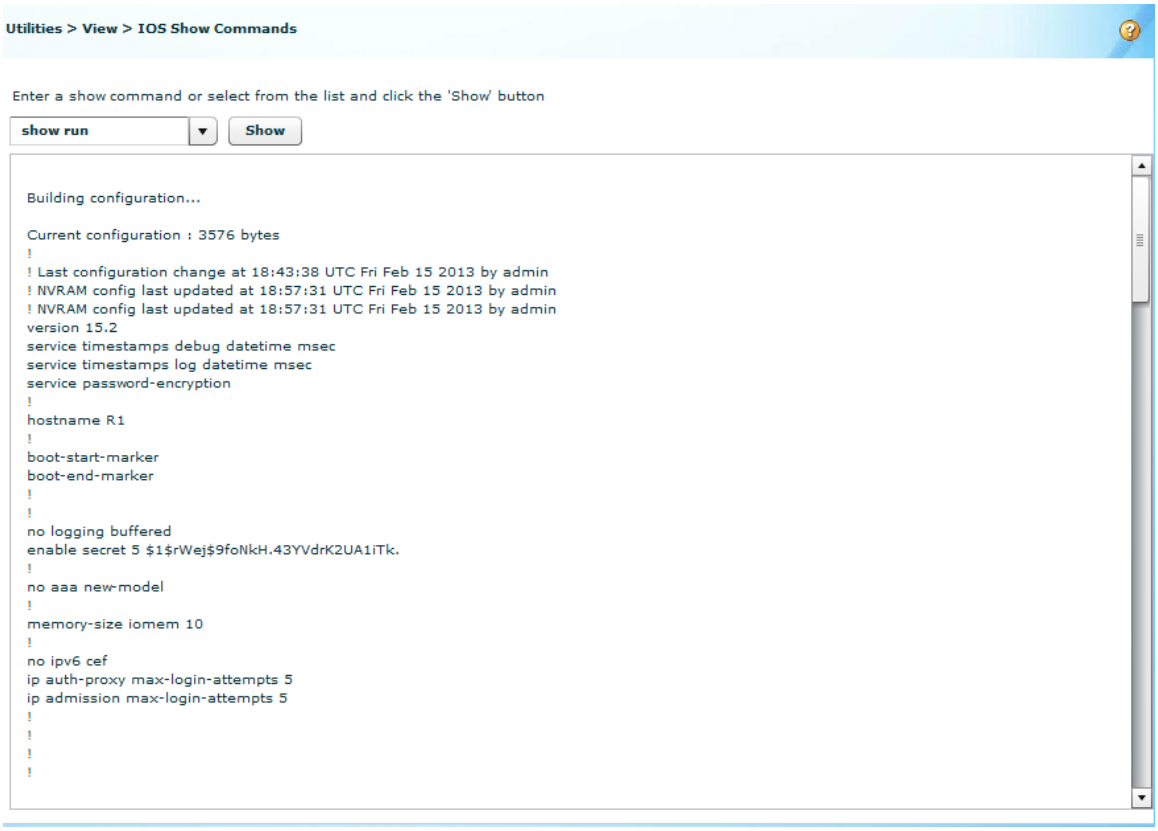


Use la utilidad View para visualizar la configuración en ejecución del router.

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

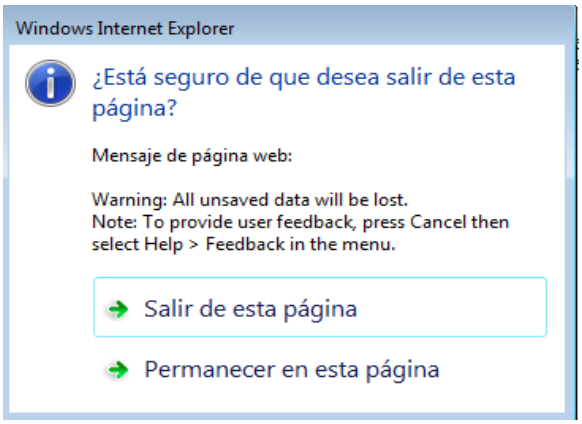


Seleccione **show run** en la lista desplegable y haga clic en **Show** (Mostrar). La configuración en ejecución del router se muestra en el panel de contenido.



cerrar CCP.

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



Reflexión

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

_____
_____

_____
_____

_____
_____

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

_____
_____

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

_____
_____

_____
_____

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

_____
_____

_____
_____

_____
_____

Tabla de resumen de interfaces del router

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

Informe No. 13

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

Topología

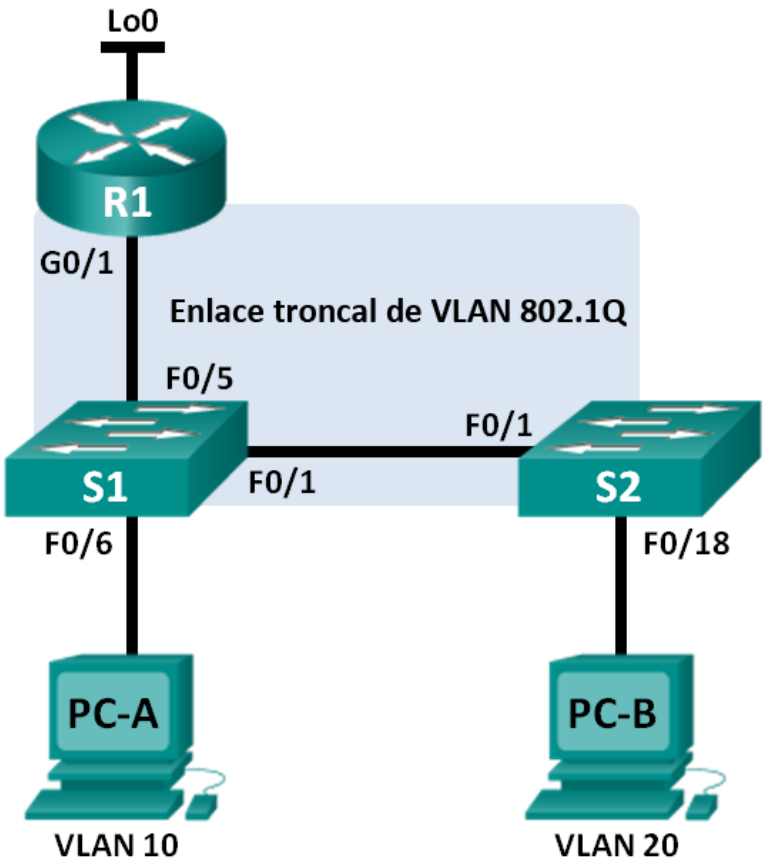


Tabla de direccionamiento

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

Especificaciones de la asignación de puertos de switch

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

Objetivos

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

Parte 2: configurar switches con VLAN y enlaces troncales

Parte 3: configurar routing entre VLAN basado en enlaces troncales

Información básica/situación

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

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

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing entre VLAN basado en enlaces troncales. Sin embargo, los comandos requeridos para la configuración se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de la práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

1 router (Cisco 1941 con IOS de Cisco, versión 15.2(4)M3, imagen universal o similar)

2 switches (Cisco 2960 con IOS de Cisco, versión 15.0(2), imagen lanbasek9 o similar)

2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

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

Cables Ethernet, como se muestra en la topología

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

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

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

Configurar los equipos host.

Inicializar y volver a cargar los routers y switches, según sea necesario.

Configurar los parámetros básicos para cada switch.

Desactive la búsqueda del DNS.

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

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

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

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

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

```
S1# configure terminal
S1(config)# vlan 1
S1(config-vlan)# exit
S1(config)# interface vlan1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
```

Configure el gateway predeterminado en los dos switches.

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

Copie la configuración en ejecución en la configuración de inicio

```
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#exit
S1(config)#exit
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configurar los parámetros básicos para el router.

a. Desactive la búsqueda del DNS.

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

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.

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

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

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

Copie la configuración en ejecución en la configuración de inicio.

```
R1>enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#host
R1(config)#hostname R1
R1(config)#no ip doma
R1(config)#no ip domain-lookup
R1(config)#interface Lo0
R1(config-if)#
R1(config-if)#ip add
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#exit
R1(config)#enab
R1(config)#enable pass
R1(config)#enable password class
R1(config)#line console 0
R1(config)#line console 0
R1(config-line)#pass
R1(config-line)#password cisco
R1(config-line)#log
R1(config-line)#login
R1(config-line)#logg
R1(config-line)#logging syn
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#passw
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1#copy run star
Destination filename [startup-config]?
Building configuration...
[OK]
```

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 Estudiantes

S1(config-vlan)#vlan 20

S1(config-vlan)#vlan 20

S1(config-vlan)#name CuerpoDocente

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 f0/1

S1(config-if)#switchport mode trunk

S1(config-if)#exit

S1(config)#interface f0/5

S1(config-if)#switchport mode trunk

S1(config-if)#exit

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

S1(config-if)#exit

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.}

S2(config)#interface f0/1
S2(config-if)#swi
S2(config-if)#switchport mode trunk
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
S2(config-if)#exit
S2(config)#vlan 10
S2(config-vlan)#name Estudiantes
S2(config-vlan)#vlan 20
S2(config-vlan)#name CuerpoDocente
S2(config-vlan)#exit

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

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, Fa0/11, 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 Estudiantes active
20 CuerpoDocente active Fa0/18
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

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

S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#exit

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

Parte 3: configurar routing entre VLAN basado en enlaces troncales

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

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

Paso 1. configurar una subinterfaz para la VLAN 1.

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

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

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

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.

- R1(config-subif)#interface g0/1.10

Configure la subinterfaz para que opere en la VLAN 10.

- R1(config-subif)#encapsulation dot1Q 10

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

- R1(config-subif)#ip address 192.168.10.1 255.255.255.0

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.

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

Configure la subinterfaz para que opere en la VLAN 20.

- R1(config-subif)#encapsulation dot1Q 20

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

- R1(config-subif)#encapsulation dot1Q 20

Habilitar la interfaz G0/1.

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

- R1(config-subif)#int g0/1
- R1(config-if)#no shutdown

Verifique la conectividad.

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

- R1#show run

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

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

```
Pinging 192.168.10.1 with 32 bytes of data:

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

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

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

```
PC>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Reply from 192.168.20.3: bytes=32 time=1ms TTL=127
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127

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

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

```
PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

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

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

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

```
PC>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time=0ms TTL=254
Reply from 192.168.1.12: bytes=32 time=0ms TTL=254
Reply from 192.168.1.12: bytes=32 time=1ms TTL=254
Reply from 192.168.1.12: bytes=32 time=0ms TTL=254

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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

Reflexión

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

Al trabajar con subredes se pueden identificar de manera más específica cualquier posible falla en la red, si afectar así la Tronca y las demás subredes del sistema.

Tabla de resumen de interfaces del router

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

1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

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

Apéndice A: comandos de configuración

Switch S1

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

Switch S2

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

Router R1

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

Informe No. 14

6.2.2.5: Práctica de laboratorio: configuración de rutas estáticas y predeterminadas IPv4

Topología

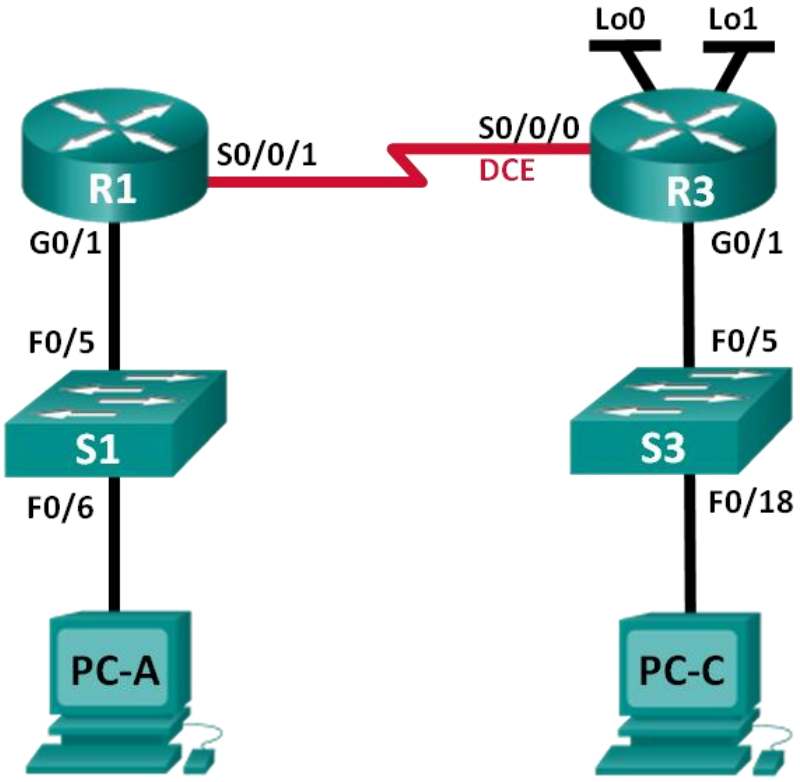


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A

	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objetivos

Parte 1: establecer la topología e inicializar los dispositivos

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

Parte 3: configurar rutas estáticas

Configurar una ruta estática recursiva.

Configurar una ruta estática conectada directamente.

Configurar y eliminar rutas estáticas.

Parte 4: configurar y verificar una ruta predeterminada

Información básica/situación

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

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

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing estático. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

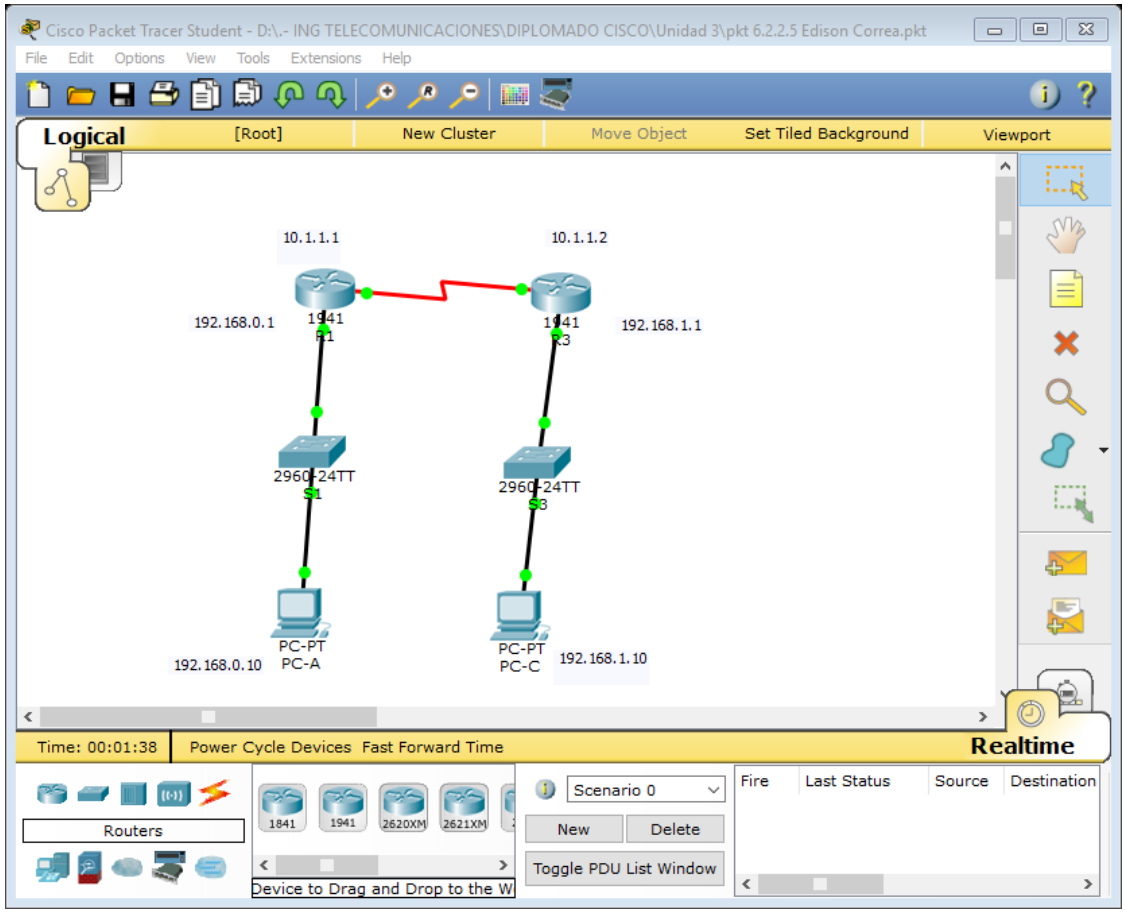
Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

2 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

2 switches (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o similar)



2 computadoras (Windows 7, Vista o XP con un programa de emulación de terminal, como Tera Term)

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

Cables Ethernet y seriales, como se muestra en la topología

Establecer la topología e inicializar los dispositivos

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

Inicializar y volver a cargar el router y el switch.

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.

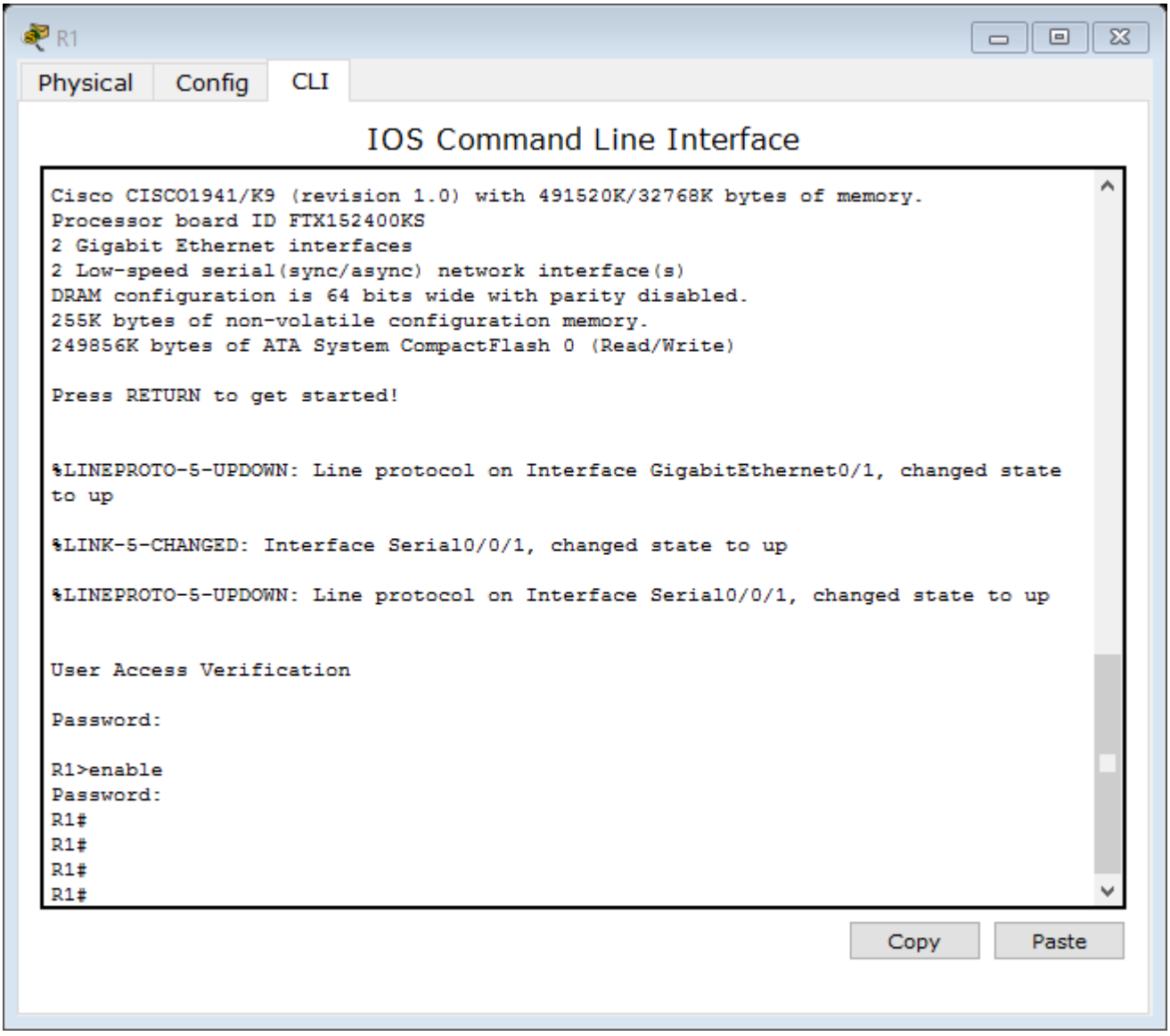
Configurar los parámetros básicos en los routers.

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

Desactive la búsqueda del DNS.

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

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



Configurar los parámetros IP en los routers.

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

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**

Verificar la conectividad de las LAN.

c. 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_____

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.

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

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

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

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

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

_Para R1, R3 con este ping no hay ningún protocolo en uso y R3 aún no está especificado. Por lo que, R3 no puede ser visto en la tabla de enrutamiento y no hay conexión entre los dos.

_____
_____

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

Reunir información.

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

¿Cuántas interfaces están activadas en el R1? ___2_____

Revise el estado de las interfaces en el R3.

¿Cuántas interfaces están activadas en el R3? ____4_____

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

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

__ red 192.168.0.0 y las dos interfaces de bucle invertido en R3 no están incluidos en la tabla de enrutamiento

_____
_____

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?

__ red 192.168.0.0 no está incluido en la tabla de enrutamiento.

_____
_____

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

___ **Debe saber que redes están al lado, Esto evita que el router sea atacado con bastante información, que a su vez, se pone lenta la CPU cuando se hace búsqueda recurrente**

_____
_____

_____
_____

Configure las rutas estáticas.

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

Nota: en esta práctica de laboratorio, se proporciona la ayuda mínima relativa a los comandos que efectivamente se necesitan para configurar el routing estático. Sin embargo, los comandos requeridos se proporcionan en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Paso 1. Configure una ruta estática recursiva.

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

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

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.

_____
_____

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 192.168.1.0/24 [1/0] via 10.1.1** _____

¿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.

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*

e. 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.

___ **i**p route 192.168.0.0 255.255.255.0 s0/0/0 _____

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 192.168.0.0/24 is directly connected, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

___

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

Este ping debe tener éxito.

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

Configurar una ruta estática.

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

____ Ip route 198.133.219.0 255.255.2550 s/0/0/1 _____

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

___ Ip route 209.165.200.224 255.255.255.224 s/0/0/1_____

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

209.165.200.0/27 is subnetted, 1 subnets_____

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

Este ping debe tener éxito.

Elimine las rutas estáticas de las direcciones de loopback.

g. 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.

__ No ip route 198.133.219.0 255.255.255.0

No ip route 209.165.200.224 255.255.255.224 ____

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

¿Cuántas rutas de red se indican en la tabla de routing del R1? ____3_____

¿El gateway de último recurso está establecido? _____SI_____

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*}

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.

___ ip route 0.0.0.0 0.0.0.0 s0/0/1 ____

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?

_____Gateway of last resort is 0.0.0.0 to network 0.0.0.0 _____

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

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

Estos pings deben tener éxito.

Reflexión

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?

___ La ruta del IP 192.168.3.0 255.255.255.0 g0 / 0 podría ser_____

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

_____Si Al No Tener Que Hacer La Busqueda Recurrente._____
_____

_____
_____

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

___si por que por medio de la ruta por defecto podría salir_____
_____

Tabla de resumen de interfaces del router

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

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

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

Configuración básica de los dispositivos

Configure los parámetros IP en el router.

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

Configuraciones de rutas estáticas

Configure una ruta estática recursiva.

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

Configure una ruta estática conectada directamente.

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

Elimine las rutas estáticas.

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

o

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

o

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

Configuración de rutas predeterminadas

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

INFORME No. 15

6.2.4.5: Práctica de laboratorio: configuración de rutas estáticas y predeterminadas IPv6

Topología

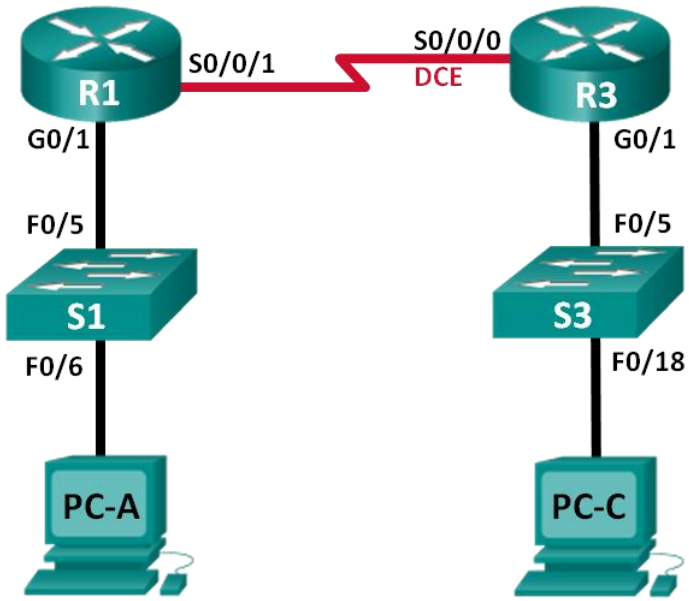


Tabla de direccionamiento

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.

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

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.

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

Inicializar y volver a cargar los routers y los switches.

Habilitar el routing de unidifusión IPv6 y configurar el direccionamiento IPv6 en los routers.

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

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

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

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

Asigne un nombre de dispositivo al router R3.

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

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

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**

Deshabilitar el direccionamiento IPv4 y habilitar SLAAC de IPv6 para las interfaces de red de las computadoras.

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

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

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

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

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

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.

Usar ipconfig y ping para verificar la conectividad LAN.

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

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

<Output Omitted>

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :

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

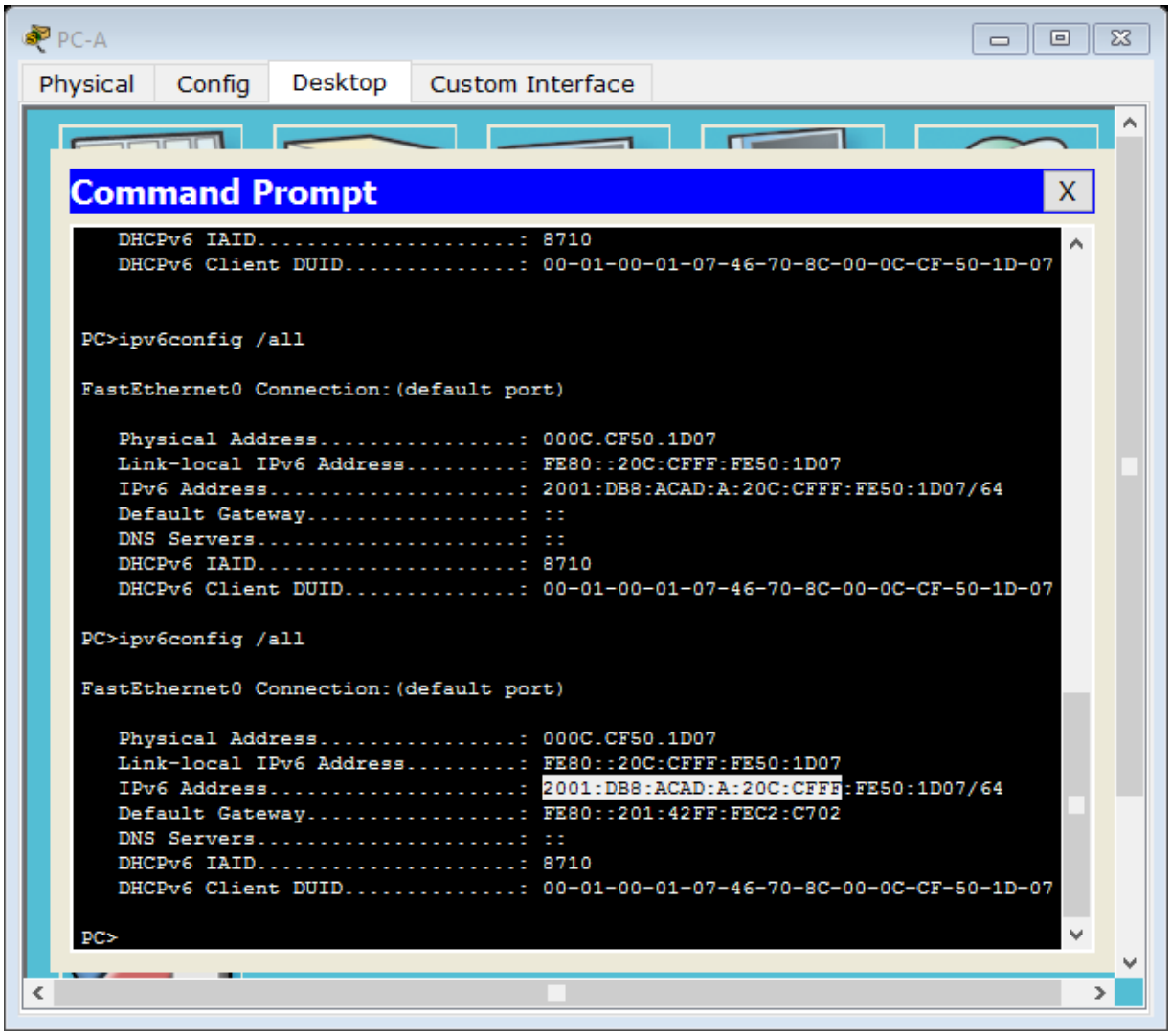
Sobre la base de la implementación de la red y el resultado del comando **ipconfig /all**, ¿la PC-A recibió información de direccionamiento IPv6 del R1?___SI____

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

2001:DB8:ACAD:A:20C:CFFF: FEC2:C702

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

R: FE80::20C:CFFF:FE50:1D07



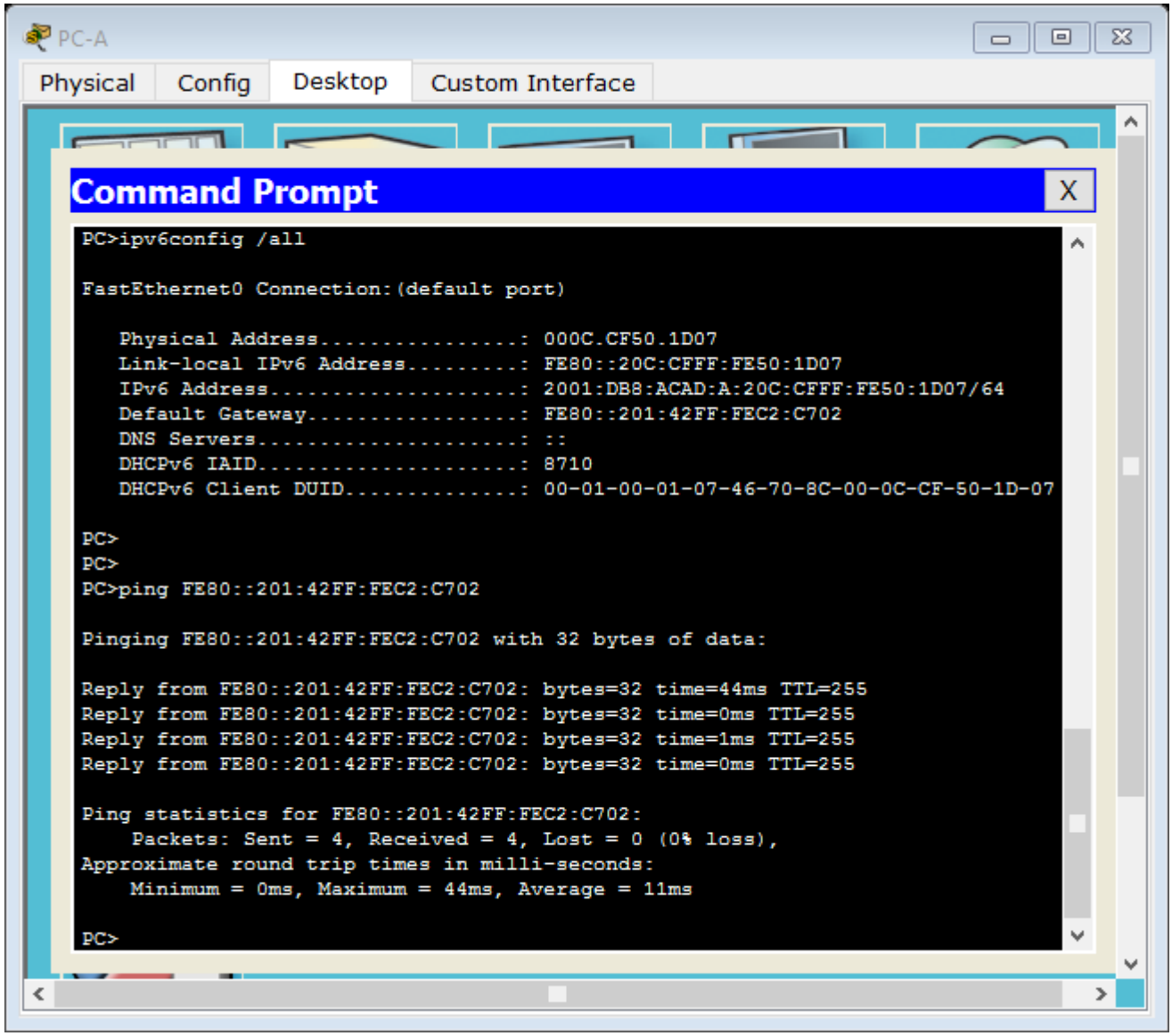
¿Cuál es la dirección IPv6 de gateway predeterminado de la PC-A?

R: FE80::201:42FF:FEC2:C702

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>**

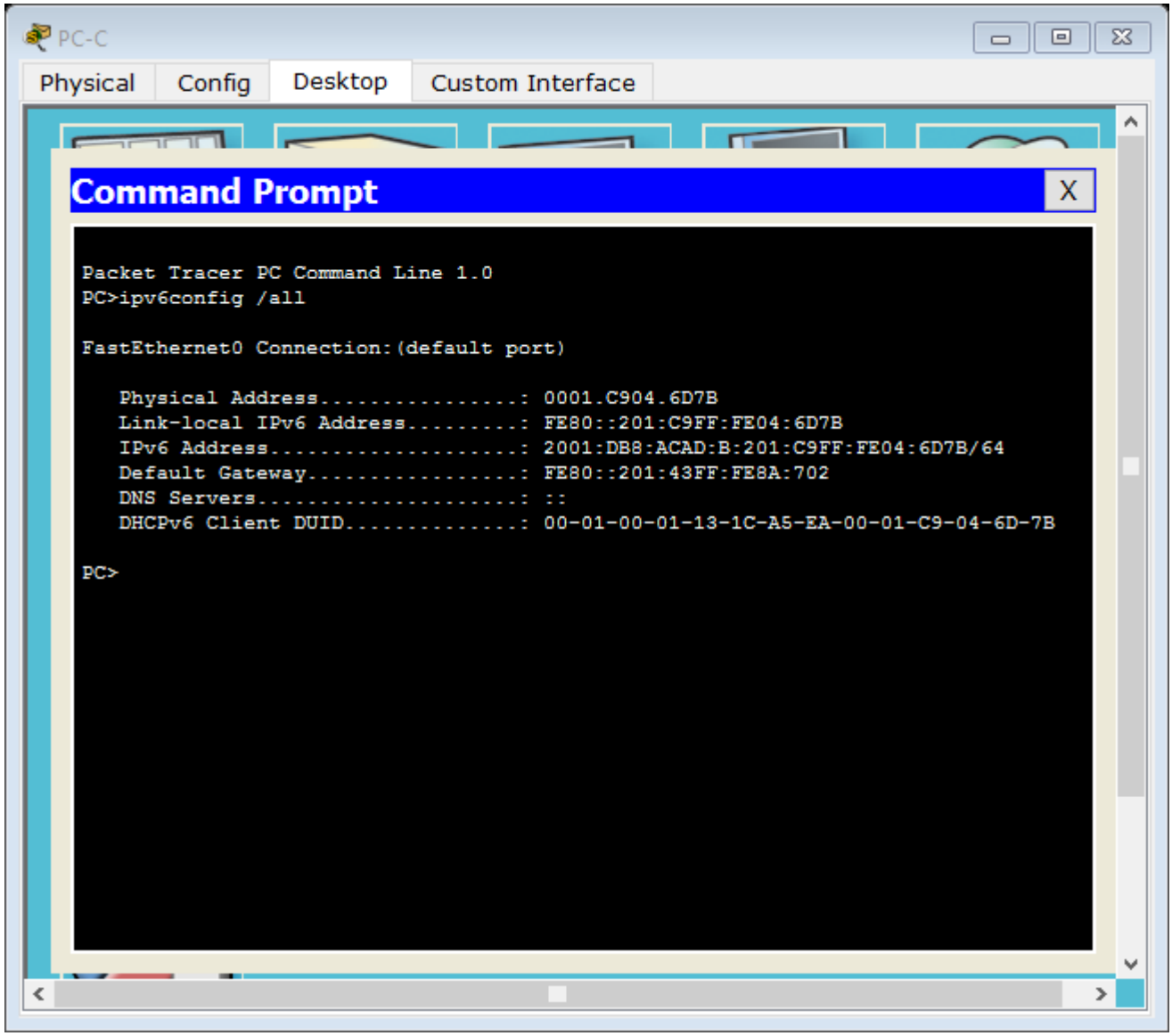
¿La PC-A recibió respuestas al ping hizo que al R1?



Repita el paso 5a en la PC-C.

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

SI



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

2001:DB8:ACAD:B:201:C9FF: FE8A:702

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

FE80::201:C9FF:FE04:6D7B

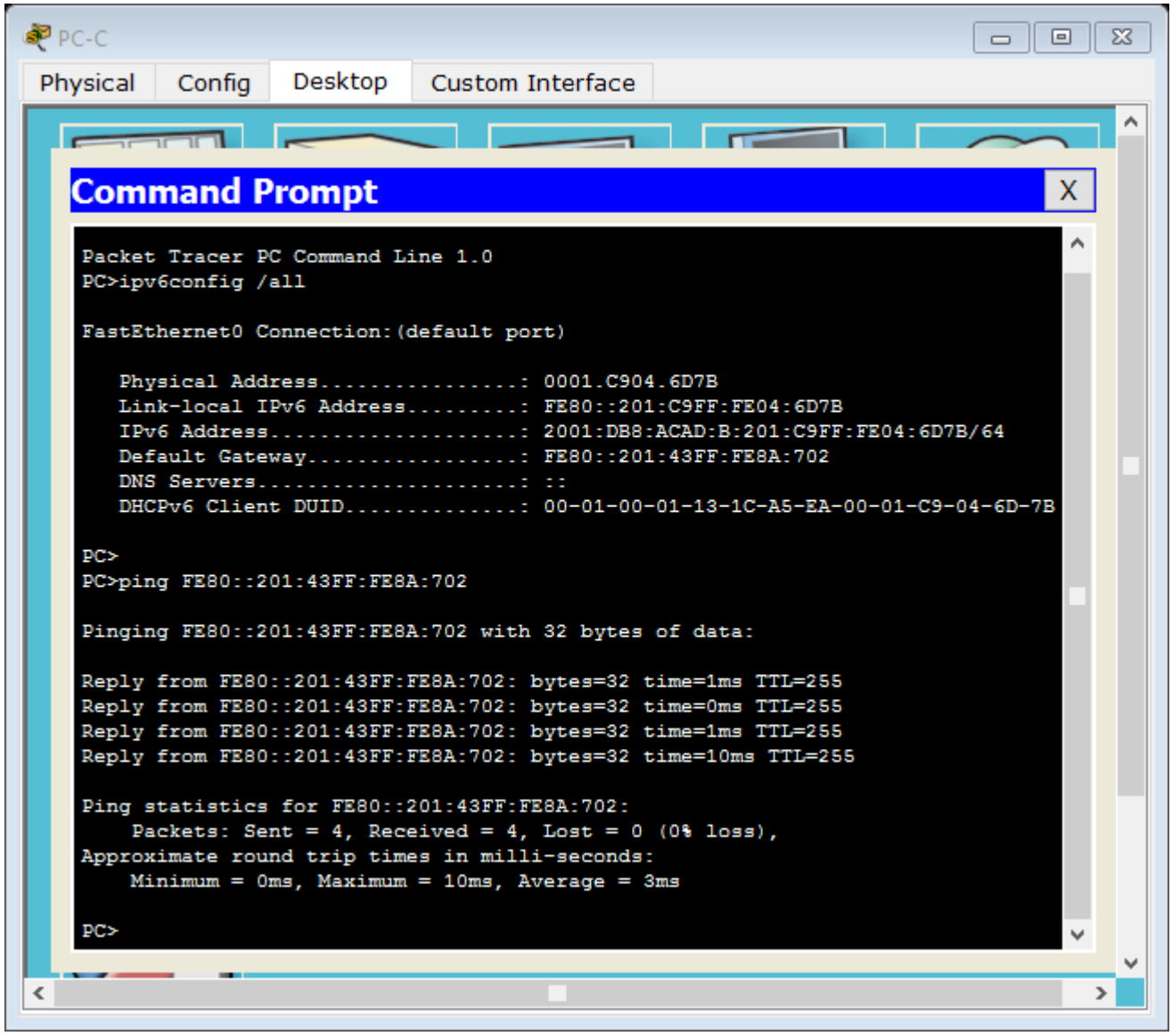
¿Cuál es la dirección IPv6 de gateway predeterminado de la PC-C?

FE80::201:43FF:FE8A:702

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

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

SI

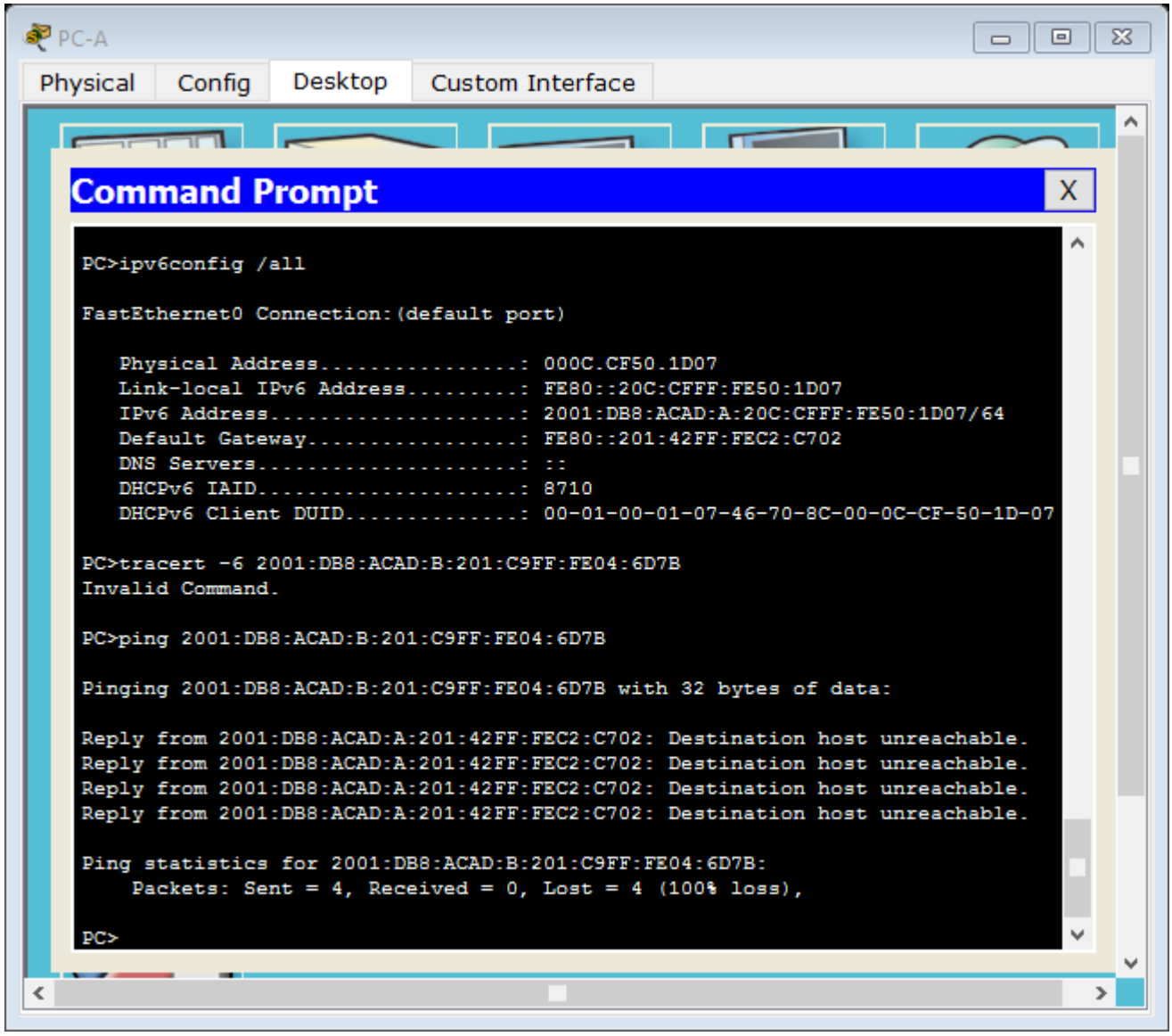


Intente hacer **ping -6** IPv6 de la PC-A a la dirección IPv6 de la PC-C.

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

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

No, por que los roters no tienen rutas que permitan direccionar el trafico entre redes que no estén conectadas directamente a cada uno de ellos



Use los comandos show para verificar la configuración de IPv6.

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

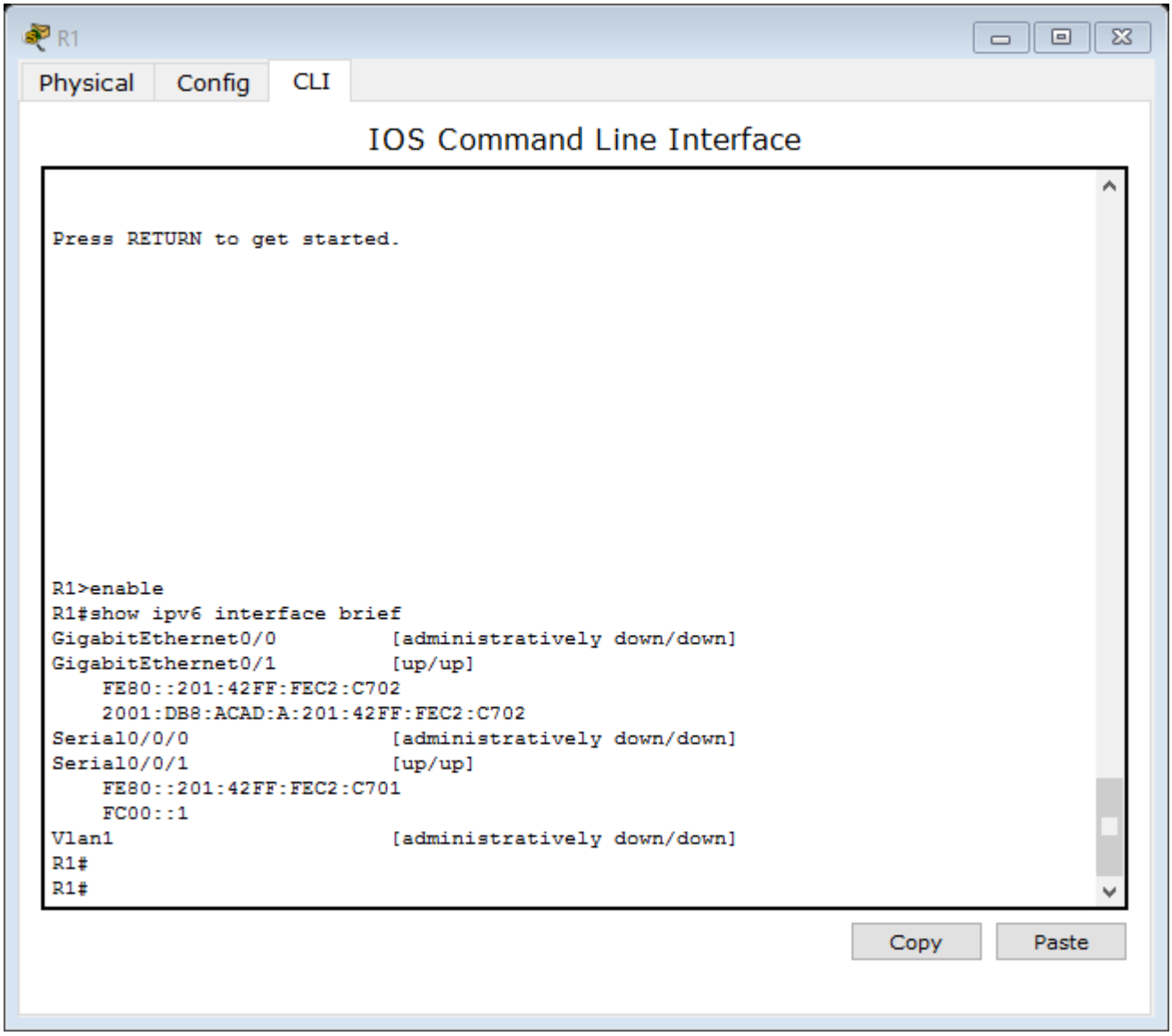
¿Cuáles son las dos direcciones IPv6 de la interfaz G0/1 y qué tipo de direcciones IPv6 son?

Link local

FE80::201:42FF:FEC2:C702

Unicast addres

2001:DB8:ACAD:A:201:42FF:FEC2:C702

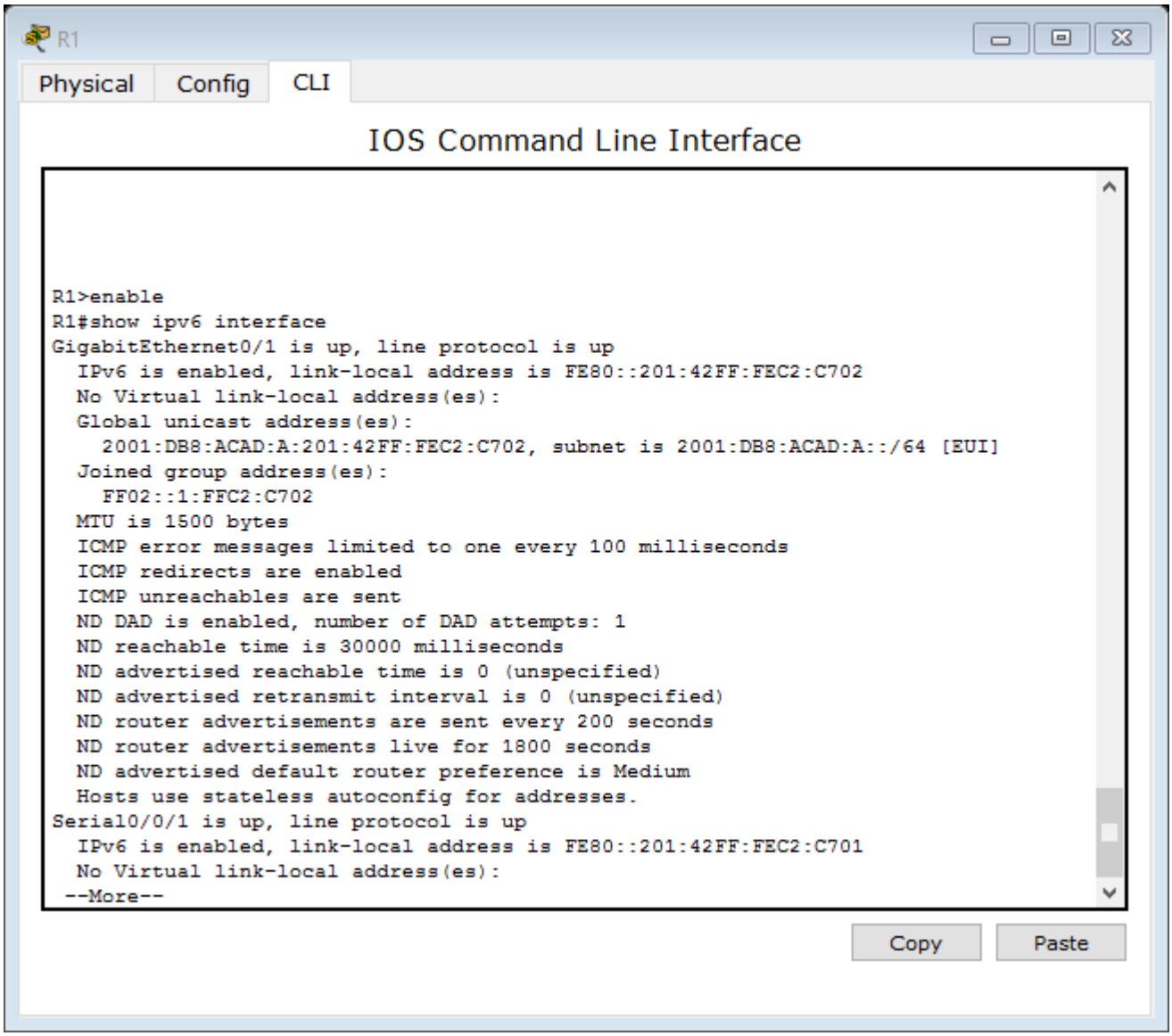


¿Cuáles son las dos direcciones IPv6 de la interfaz S0/0/1 y qué tipo de direcciones IPv6 son?

Link local FE80::201:42FF:FEC2:C701

Unicast Addres FC00::1

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:FFC2:C702

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

FF02::1

FF02::2

FF02::1:FF00:1

FF02::1:FFC2:C701

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

Para hacer una multidifusión hacia todos los nodos en el segmento de red local

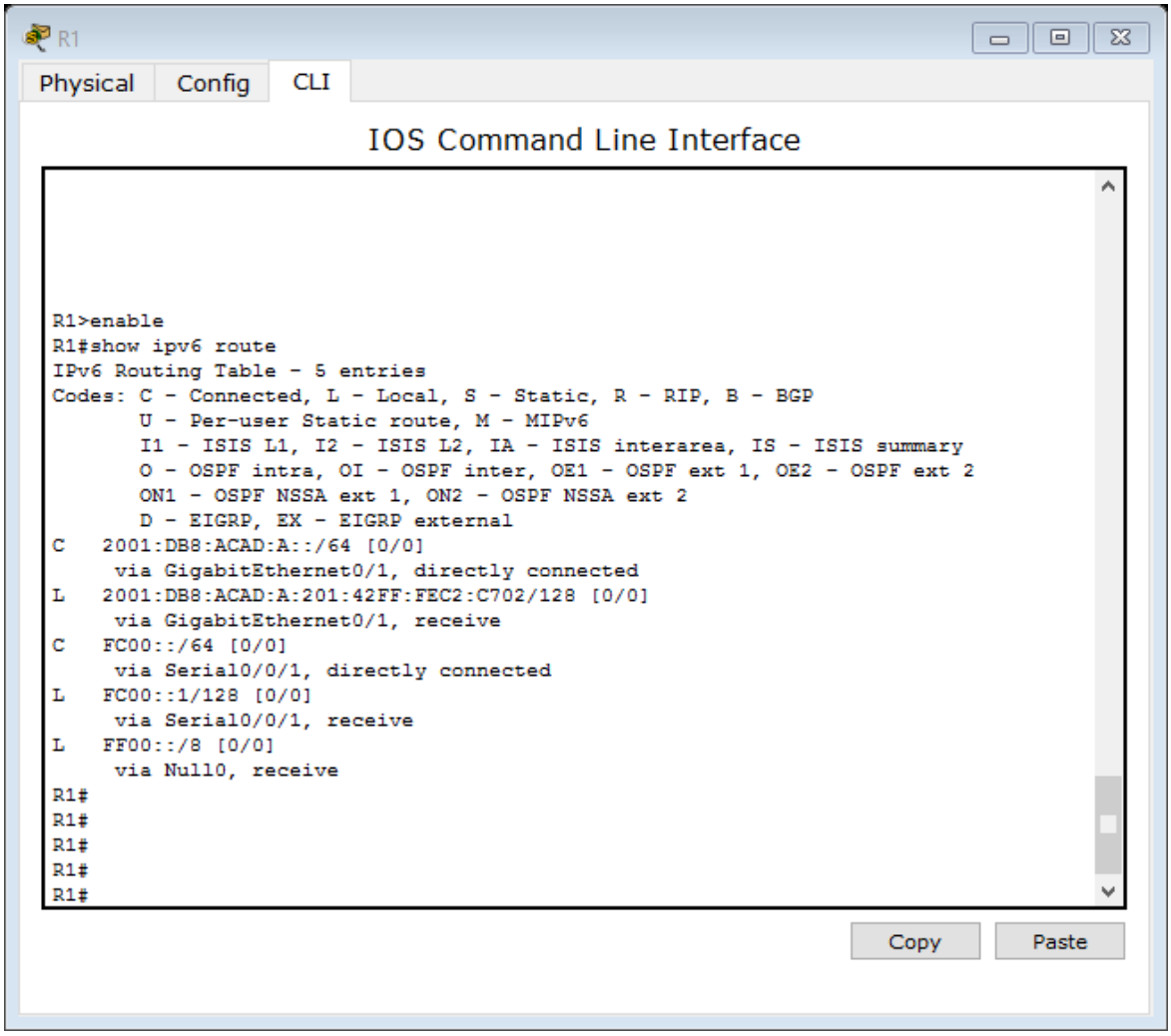
¿Para qué se usa la dirección de multidifusión FF02::2?

Para hacer una multidifusión hacia todos los enrutadores en el segmento de red local

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

Son las multidifusión de nodos solicitados y se usan para resolver las direcciones de los otros equipos en red local

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?

El ping desde la pc-c no es satisfactorio porque no hay una ruta lan a R3

Configurar rutas estáticas y predeterminadas IPv6

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

Configurará tres tipos de rutas estáticas IPv6:

Ruta estática IPv6 conectada directamente: una ruta estática conectada directamente se crea al especificar la interfaz de salida.

Ruta estática IPv6 recursiva: una ruta estática recursiva se crea al especificar la dirección IP del siguiente salto. Este método requiere que el router ejecute una búsqueda recursiva en la tabla de routing para identificar la interfaz de salida.

Ruta estática predeterminada IPv6: similar a una ruta IPv4 de cuádruple cero, una ruta estática predeterminada IPv6 se crea al hacer que el prefijo IPv6 de destino y la longitud de prefijo sean todos ceros, :: /0.

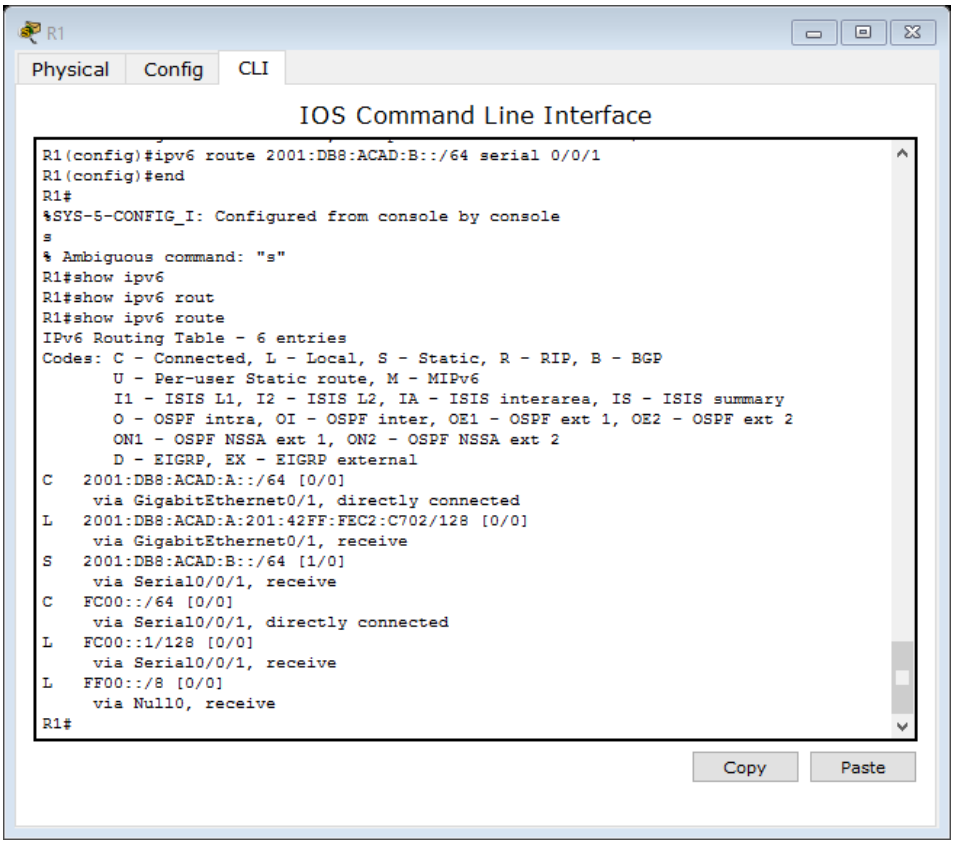
Paso 1. configurar una ruta estática IPv6 conectada directamente.

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

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

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)#



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

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

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

via Serial0/0/1, receive

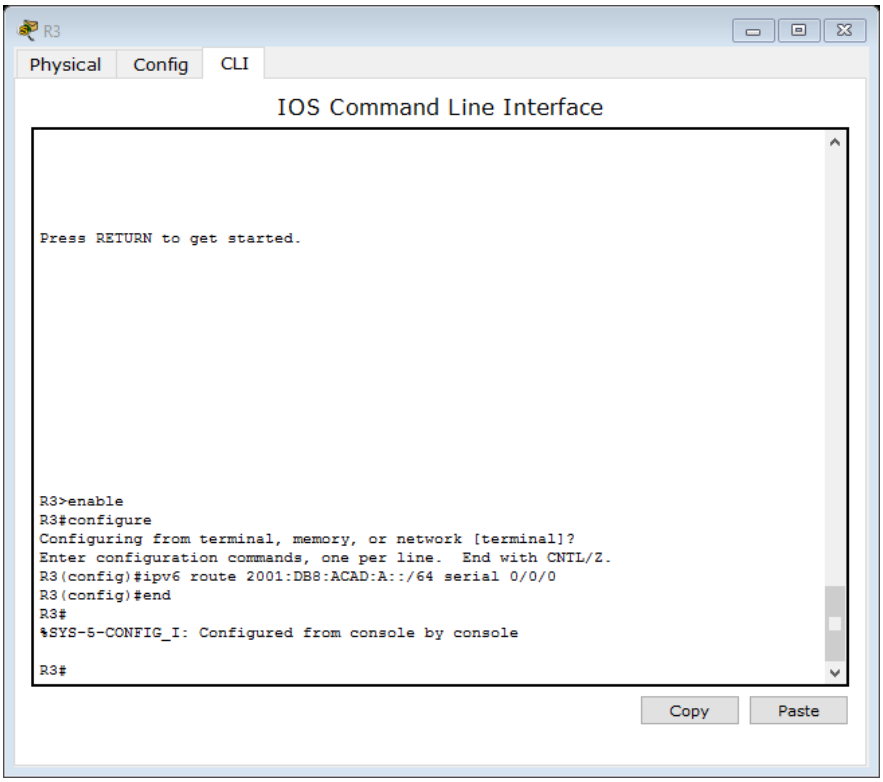
Ahora que la ruta estática se configuró en el R1, ¿es posible hacer ping de la PC-A al host PC-C? _____No

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, 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.

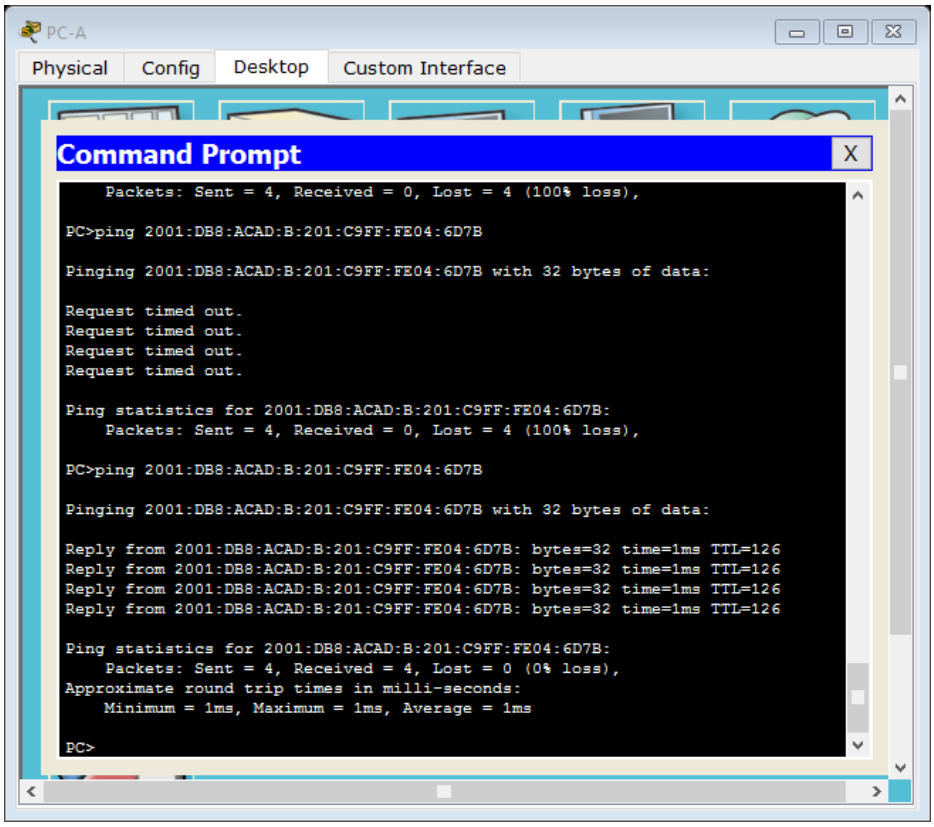
En el router R3, configure una ruta estática IPv6 a la red 2001:DB8:ACAD:A::/64, mediante la interfaz de salida S0/0/0 del R3.

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

R3(config)#



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 los enrutadores tienen una ruta para llegar desde la red del pc-a hasta la red de pc-c y retornar

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>*

k. 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**

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**

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

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

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

via FC00::2, receive

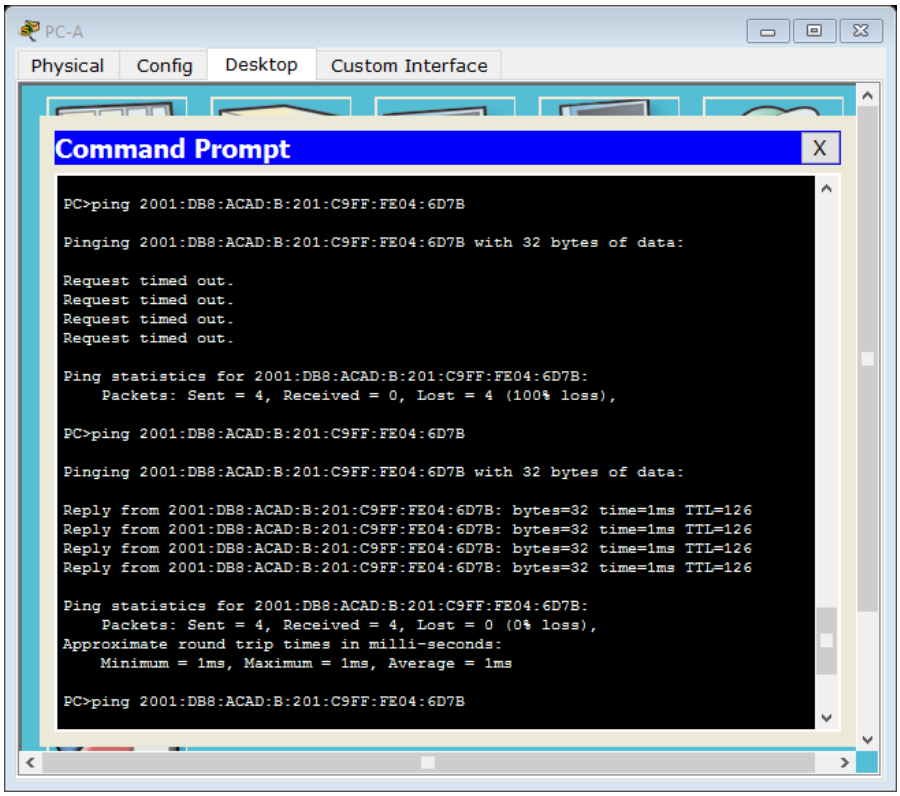
_____

_____

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.



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>*

I. 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)#

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

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

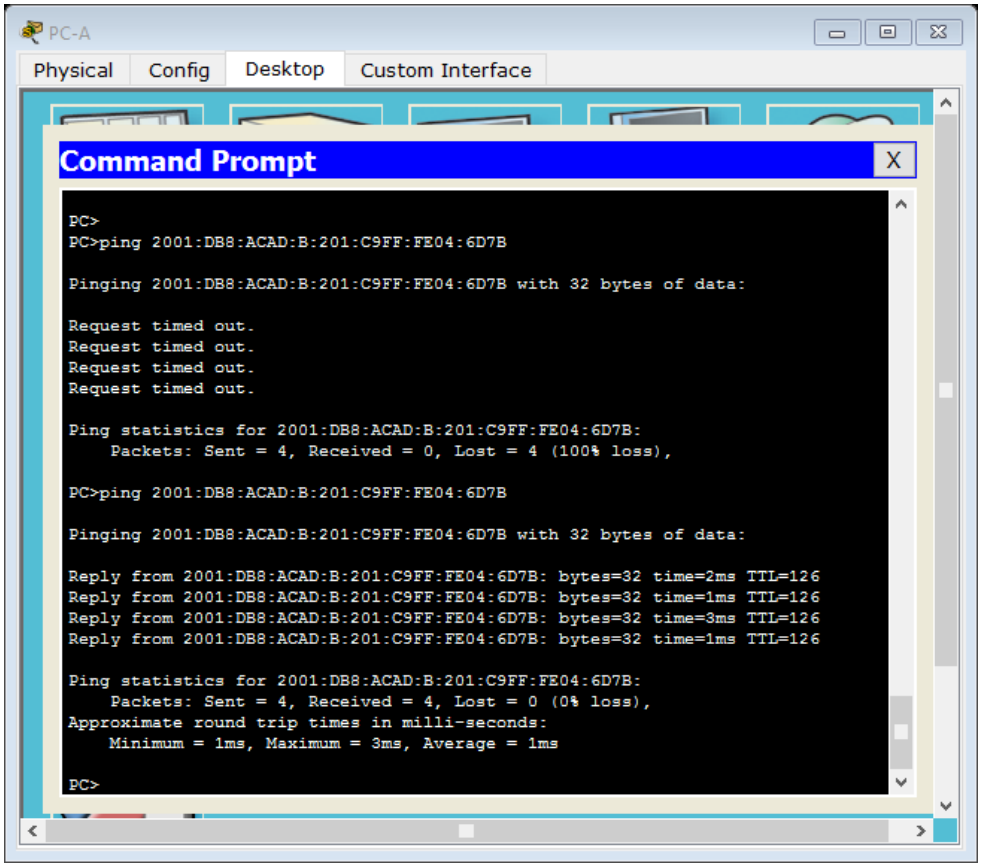
¿Cuál es la letra de código y la entrada de la tabla de routing de la ruta predeterminada que se agregó recientemente a la tabla de routing?

S ::/0 [1/0]

via Serial0/0/1, receive

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

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

Cuando se tiene una red en la cual conviven diferentes segmentos tanto con IPv4 como IPv6, y la misma requiere comunicaciones, debemos utilizar el enrutamiento ya sea dinámico o estático, por ejemplo una compañía que es absorbida por otra, y cada una tiene un esquema de direccionamiento o enrutamiento.

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?

Cuando se configura una ruta estática con ipv6 se configura con el comando ipv6 route en vez de ipv route, también al ingresar show ipv route

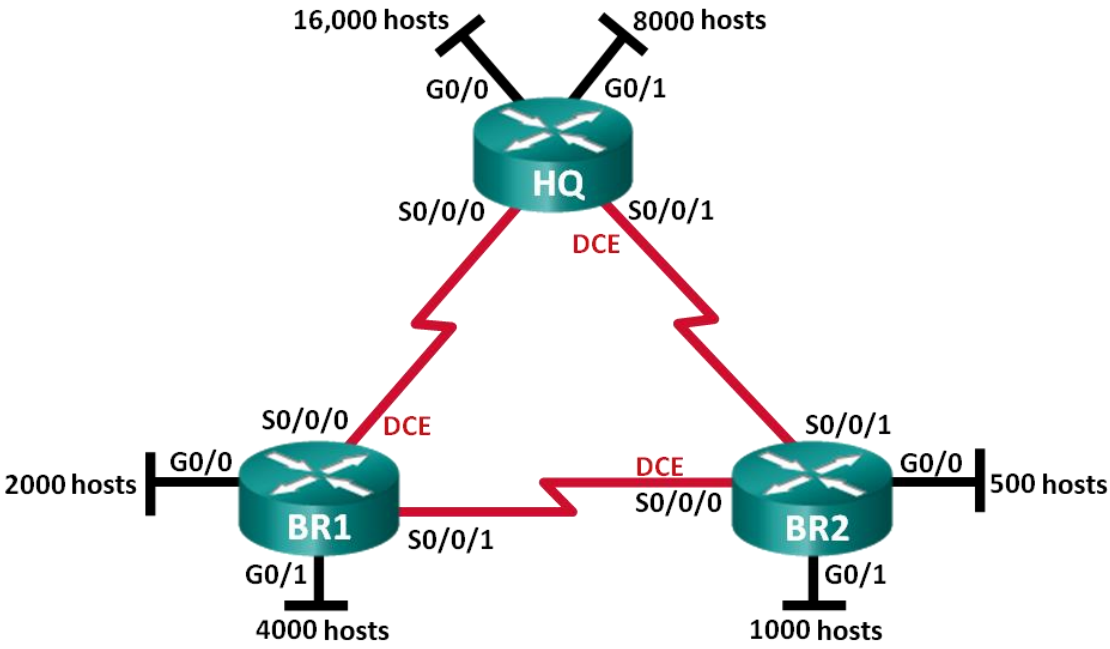
Tabla de resumen de interfaces del router

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

Informe No. 16

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

Topología



Objetivos

Parte 1: examinar los requisitos de la red

Parte 2: diseñar el esquema de direcciones VLSM

Parte 3: realizar el cableado y configurar la red IPv4

Información básica/situación

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

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

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen

universalk9). Pueden utilizarse otros routers y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

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

Recursos necesarios

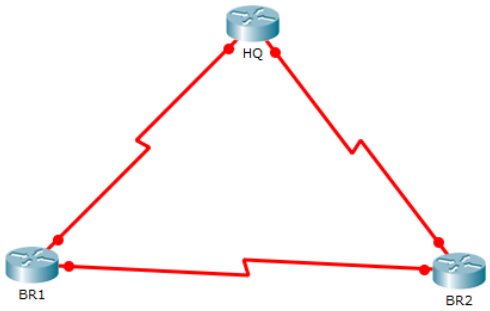
3 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)

1 computadora (con un programa de emulación de terminal, como Tera Term, para configurar los routers)

Cable de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola

Cables Ethernet (optativo) y seriales, como se muestra en la topología

Calculadora de Windows (optativo)



Parte 1: examinar los requisitos de la red

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

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

# hosts		32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	2^(N-1)
∑ bits	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	
# hosts REAL		32766	16382	8190	4094	2046	1022	510	254	126	62	30	14	6	2	0	(2^N)-2
N (# bi0t)	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	N bit
172	16	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
172	16	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	
172	16	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	
172	16	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	
172	16	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	
172	16	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	
172	16	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	
172	16	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	
172	16	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	
172	16	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	
172	16	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	
172	16	1	1	1	1	1	1	0	0	0	0	0	0	0	1	1	
172	16	1	1	1	1	1	1	0	0	0	0	0	0	1	0	0	
172	16	1	1	1	1	1	1	0	0	0	0	0	1	0	1	1	
172	16	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	
172	16	1	1	1	1	1	1	0	0	0	0	0	1	0	1	1	

	Network	First	Last	Broadcast
HQ g0/0 16000 hosts	172.16.128.0/18	172.16.128.1/18	172.16.191.254/18	172.16.191.255/18
HQ g0/1 8000 hosts	172.16.192.0/19	172.16.192.1/19	172.16.223.254/19	172.16.223.255/19
BR1 g0/1 4000 hosts	172.16.224.0/20	172.16.224.1/20	172.16.239.254/20	172.16.239.255/20
BR1 g0/0 2000 hosts	172.16.240.0/21	172.16.240.1/21	172.16.247.254/21	172.16.247.255/21
BR2 g0/1 1000 hosts	172.16.248.0/22	172.16.248.1/22	172.16.251.254/22	172.16.251.255/22
BR2 g0/0 500 hosts	172.16.252.0/23	172.16.252.1/23	172.16.253.254/23	172.16.253.255/23
HQ-BR1 2 hosts	172.16.254.0/30	172.16.254.1/30	172.16.254.2/30	172.16.254.3/30
HQ-BR2 2 hosts	172.16.254.4/30	172.16.254.5/30	172.16.254.6/30	172.16.254.7/30
BR1-BR2 2 hosts	172.16.254.8/30	172.16.254.9/30	172.16.254.10/30	172.16.254.11/30

Determinar la cantidad de direcciones host disponibles y la cantidad de subredes que se necesitan.

# hosts		32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2
∑ bits	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
# hosts REAL		32766	16382	8190	4094	2046	1022	510	254	126	62	30	14	6	2	0
N (# bi0t)	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

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

R: Si N= (32-17=15) → (2^N-1)-2 = 32766 Host

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

R: 31506 Host

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

R: 9 Subred

Determinar la subred más grande que se necesita.

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

R: HQ G0/0 LAN

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

R: 16000

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

R: /18

¿Cuántas direcciones host admite esa subred?

R: 16382

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

HQ g0/0 16000 hosts

HQ g0/1 8000 hosts

BR1 g0/1 4000 hosts

BR1 g0/0 2000 hosts

BR2 g0/1 1000 hosts

BR2 g0/0 500 hosts

HQ-BR1 2 hosts

HQ-BR2 2 hosts

BR1-BR2 2 hosts

R: si, POR QUE SOLO SE NECESITA 16000

¿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.

Determinar la segunda subred más grande que se necesita.

Descripción de la subred

R: HQ G0/1 LAN

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

R: 8000

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

R: /19

¿Cuántas direcciones host admite esa subred?

R: 8190

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

R: 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.

Determinar la siguiente subred más grande que se necesita.

Descripción de la subred R: BR1 G0/1 LAN

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

R: 4000

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

R: /20

¿Cuántas direcciones host admite esa subred?

R: 4094

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

R: 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.

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?

R: 2000

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

R: /21

¿Cuántas direcciones host admite esa subred?

R: 2046

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

R.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.

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?

R: 1000

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

R: /22

¿Cuántas direcciones host admite esa subred?

R: 1022

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

R: 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.

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?

R: 500

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

R: /23

¿Cuántas direcciones host admite esa subred?

R: 510

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

R: 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.

Determinar las subredes que se necesitan para admitir los enlaces seriales.

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

R: 2

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

R: /30

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

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

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

Enlace serial HQ - BR1

Enlace serial HQ - BR2

Enlace serial BR1 - BR2

Parte 2: diseñar el esquema de direcciones VLSM

Paso 1. calcular la información de subred.

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

Completar la tabla de direcciones de interfaces de dispositivos.

Descripción de la subred	Network	First	Last	Broadcast
HQ g0/0 16000 hosts	172.16.128.0/18	172.16.128.1/18	172.16.191.254/18	172.16.191.255/18
HQ g0/1 8000 hosts	172.16.192.0/19	172.16.192.1/19	172.16.223.254/19	172.16.223.255/19
BR1 g0/1 4000 hosts	172.16.224.0/20	172.16.224.1/20	172.16.239.254/20	172.16.239.255/20
BR1 g0/0 2000 hosts	172.16.240.0/21	172.16.240.1/21	172.16.247.254/21	172.16.247.255/21
BR2 g0/1 1000 hosts	172.16.248.0/22	172.16.248.1/22	172.16.251.254/22	172.16.251.255/22
BR2 g0/0 500 hosts	172.16.252.0/23	172.16.252.1/23	172.16.253.254/23	172.16.253.255/23
HQ-BR1 2 hosts	172.16.254.0/30	172.16.254.1/30	172.16.254.2/30	172.16.254.3/30
HQ-BR2 2 hosts	172.16.254.4/30	172.16.254.5/30	172.16.254.6/30	172.16.254.7/30
BR1-BR2 2 hosts	172.16.254.8/30	172.16.254.9/30	172.16.254.10/30	172.16.254.11/30

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

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

	G0/1	172.16.224.1	255.255.240.0	LAN de 4000 hosts
	S0/0/0	172.16.254.2	255.255.255.252	HQ S0/0/0
	S0/0/1	172.16.254.9	255.255.255.252	BR2 S0/0/0
BR2	G0/0	172.16.252.1	255.255.254.0	LAN de 500 hosts
	G0/1	172.16.248.1	255.255.252.0	LAN de 1000 hosts
	S0/0/0	172.16.254.10	255.255.255.252	BR1 S0/0/1
	S0/0/1	172.16.254.6	255.255.255.252	HQ S0/0/1

Parte 3: realizar el cableado y configurar la red IPv4

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

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

configurar los parámetros básicos en cada router.

m. Asigne el nombre de dispositivo al router.

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

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

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

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

Cifre las contraseñas de texto no cifrado.

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

configurar las interfaces en cada router.

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

Configure una descripción de interfaz para cada interfaz.

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

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

Active las interfaces.

Guardar la configuración en todos los dispositivos.

Probar la conectividad

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

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

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

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?

Para obtener la próxima dirección de red 172.16.254.0/30 sería tomando la dirección de red y sumarle 4 al último octeto.

Tabla de resumen de interfaces del router

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

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

Informe No. 17

6.4.2.5: Práctica de laboratorio: cálculo de rutas resumidas IPv4 e IPv6

Topología

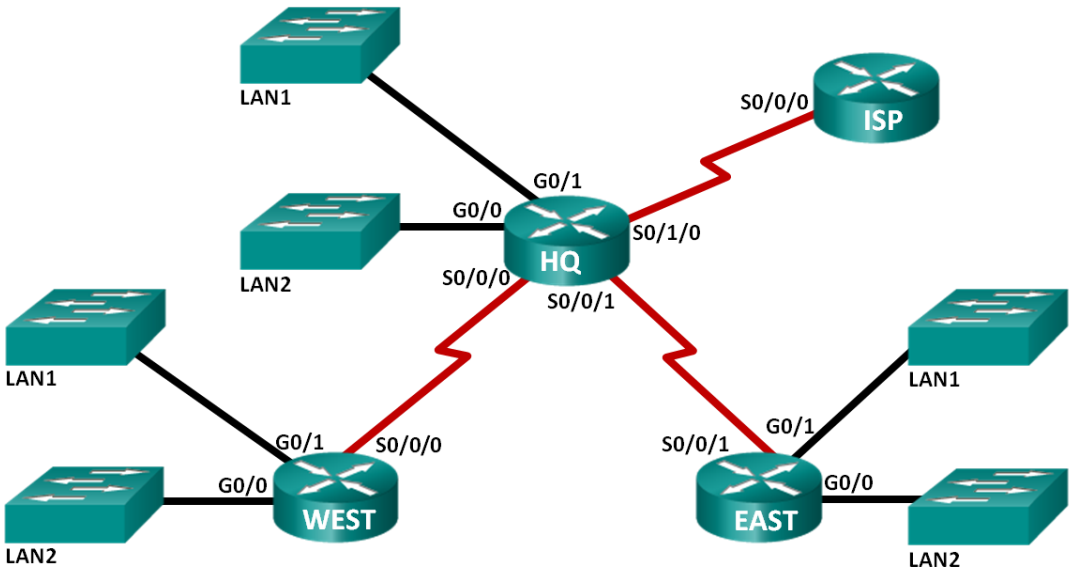


Tabla de direccionamiento

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

Objetivos

Parte 1: calcular rutas resumidas IPv4

Determinar la ruta resumida para las LAN de HQ.

Determinar la ruta resumida para las LAN ESTE.

Determinar la ruta resumida para las LAN OESTE.

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

Parte 2: calcular rutas resumidas IPv6

Determinar la ruta resumida para las LAN de HQ.

Determinar la ruta resumida para las LAN ESTE.

Determinar la ruta resumida para las LAN OESTE.

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

Información básica/situación

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

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

Recursos necesarios

1 computadora (Windows 7, Vista o XP, con acceso a Internet)

Optativo: calculadora para convertir los valores hexadecimales y decimales en valores binarios

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.

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

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

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

¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes?
__22_____

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

192.168.64.0/22

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

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

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

Indique las direcciones de red resumidas en formato decimal.

192	168	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	192.168.64.0/23
192	168	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	192.168.66.0/23
192	168	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	192.168.64.0/22

Subred	Dirección IPv4	Máscara de subred	Dirección IP de la subred en formato binario
LAN1 de HQ	192.168.64.0	255.255.254.0	11000000.10101000.01000000.00000000
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

Indicar la máscara de subred de la dirección IP de la LAN1 ESTE y la LAN2 ESTE en formato decimal.

Indicar la dirección IP de la LAN1 ESTE y la LAN2 ESTE en formato binario.

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

c. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes? ____23_____

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

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

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

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

Indique las direcciones de red resumidas en formato decimal.

192	168	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	192.168.68.0/24
192	168	0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	192.168.69.0/24
192	168	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	192.168.68.0/23

Subred	Dirección IPv4	Máscara de subred	Dirección de subred en formato binario
LAN1 de EAST	192.168.68.0	255.255.255.0	11000000.10101000.01000100.00000000
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

Indicar la máscara de subred de la dirección IP de la LAN1 OESTE y la LAN2 OESTE en formato decimal.

Indicar la dirección IP de la LAN1 OESTE y la LAN2 OESTE en formato binario.

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

e. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos redes? ___24_____

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

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

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

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

Indique las direcciones de red resumidas en formato decimal.

192	168	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	192.168.70.0/25
192	168	0	1	0	0	0	1	1	0	1	0	0	0	0	0	0	192.168.70.128/25
192	168	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	192.168.70.0/24

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

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

Indicar la dirección IP de la ruta resumida de HQ, ESTE y OESTE en formato binario.

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

g. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las tres redes? _____21_____

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

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

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

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

Indique las direcciones de red resumidas en formato decimal.

192	168	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	192.168.64.0/22
192	168	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	192.168.68.0/23
192	168	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	192.168.70.0/24
192	168	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	192.168.64.0/21

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

Ruta resumida de la dirección de red	192.168.64.0	255.255.248.0	11000000.10101000.01000000.00000000

Calcular rutas resumidas IPv6

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

Topología

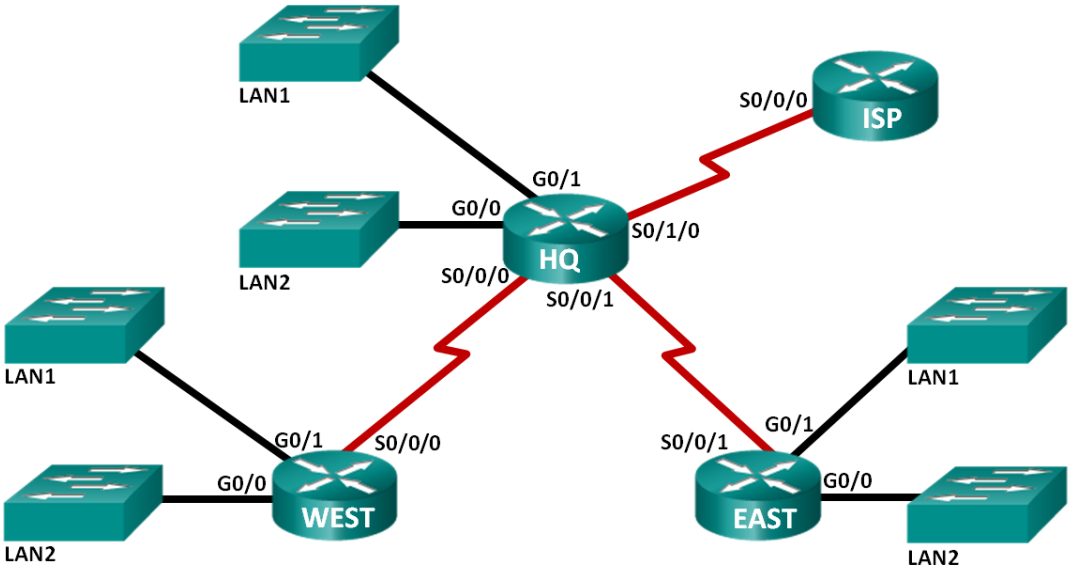


Tabla de direccionamiento

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

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

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

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

¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred? ____63__

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

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

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

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

Indique las direcciones de red resumidas en formato decimal.

2001:DB8:ACAD:E::/64	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0
2001:DB8:ACAD:F::/64	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
2001:DB8:ACAD:E::/63	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0

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

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.

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

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

j. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred? ___62___

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

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

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

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

Indique las direcciones de red resumidas en formato decimal.

2001:DB8:ACAD:1::/64	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
2001:DB8:ACAD:2::/64	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
2001:DB8:ACAD:0::/64	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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:0::/62	FFFF:FFFF:FFFF:FFFC	0000000000000000

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.

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

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

l. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las dos ID de subred? _62____

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

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

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

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

Indique las direcciones de red resumidas en formato decimal.

2001:DB8:ACAD:9::/64	2001 DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
2001:DB8:ACAD:A::/64	2001 DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
2001:DB8:ACAD:8::/62	2001 DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0

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:FFFF:FFFF	0000000000001001

LAN2 de WEST	2001:DB8:ACAD:A::/64	FFFF:FFFF:FFFF:FFFF	0000000000001010
Dirección de resumen de las LAN OESTE	2001:DB8:ACAD:8::/62	FFFF:FFFF:FFFF:FFFC	0000000000001000

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.

Indicar la ID de subred de la ruta resumida de HQ, ESTE y OESTE en formato binario.

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

n. ¿Cuántos bits coincidentes en el extremo izquierdo están presentes en las tres ID de subred? ___60___

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

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

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

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

Indique las direcciones de red resumidas en formato decimal.

2001:DB8:ACAD:E::/63	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0
2001:DB8:ACAD:0::/64	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2001:DB8:ACAD:8::/62	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
2001:DB8:ACAD:0::/60	2001	DB8	ACAD	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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:0::/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:0::/60	FFFF:FFFF:FFFF:FFF0	0000000000000000

Reflexión

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

No hay mucha diferencia excepto que en el IPv4 tiene 32 bits y IPv6 tiene 128 bits. La otra diferencia es que la dirección IPv4 es convertida de decimal a binario y el IPv6 es convertido de hexadecimal a binario.

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

Hace que las tablas de ruteo se vea un proceso más eficiente y reduce los requerimientos de memoria para el router.

CONCLUSIONES

- A la hora de realizar el direccionamiento debemos tener en cuenta datos básicos como lo es la división de las redes con base en la máscara de red, la cual permite expandir la cantidad de host o de redes de un segmento determinado.
- En cuanto a los ejercicios pudimos apreciar que realizando subneting logramos segmentar una red en diferentes subredes para posteriormente comprobar el tráfico entre ellas a través de los enrutadores.
- En estos laboratorios nos sirve para examinar un sistema de Swich básico virgen y validar los datos naturales del equipo, antes de la configuración del sistema como tal.

BIBLIOGRAFIA

- Buriticá Rodríguez, O. (2014). *Diseño e implementación de soluciones Integradas Lan-Wan-Cisco.*
- Corredor, T. M. (2013). *Diseño e implementación de soluciones integradas LAN-WAN.*
- Parra, J., & Ludy, R. (2013). *Diseño e implementación de redes Lan-Wan ccna1-ccna2.*
- Plataforma CISCO, CCNA1 – CCNA2 https://www.netacad.com/es/