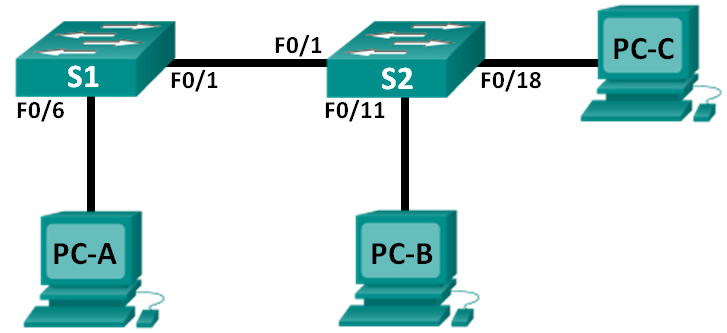
Práctica de laboratorio: implementación de seguridad de VLAN

1. Topología



1. 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 |

1. Asignaciones de VLAN

|  |  |
| --- | --- |
| VLAN | Nombre |
| 10 | Datos |
| 99 | Management&Native |
| 999 | BlackHole |

1. Objetivos

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

Parte 2: implementar seguridad de VLAN en los switches

1. 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.

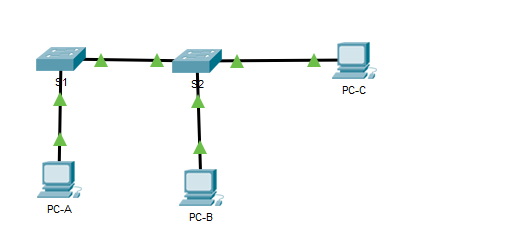
1. Recursos necesarios

* 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

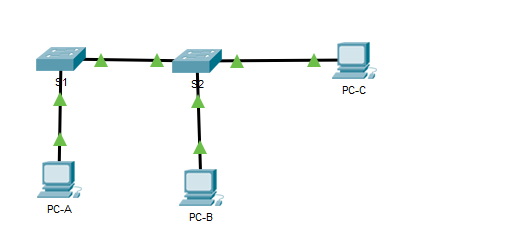
1. armar la red y configurar los parámetros básicos de los dispositivos

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

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

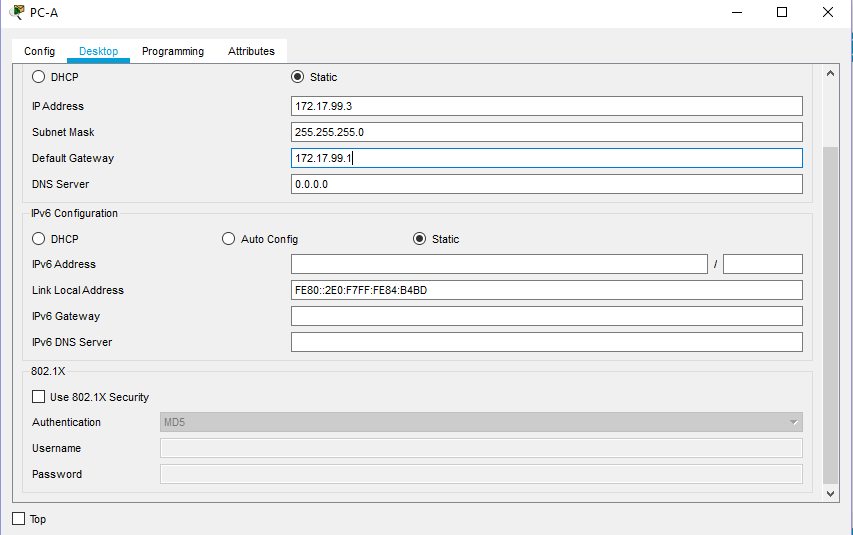


1. inicializar y volver a cargar los switches.

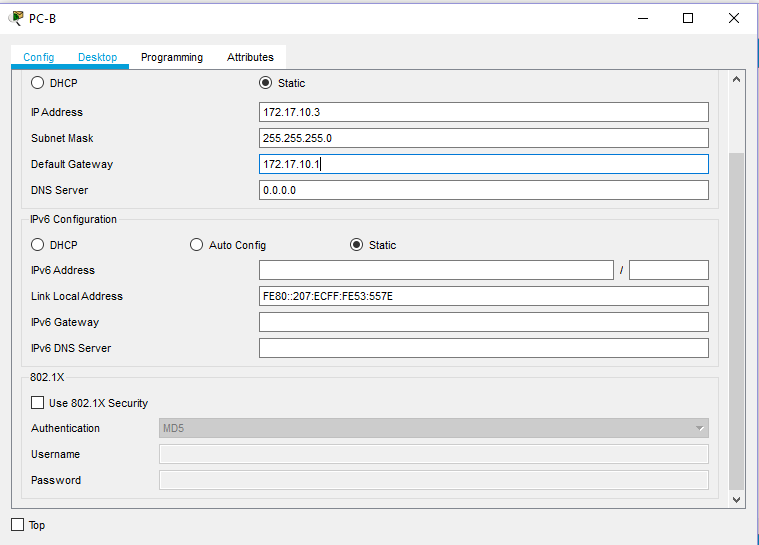


1. configurar las direcciones IP en la PC-A, la PC-B y la PC-C.

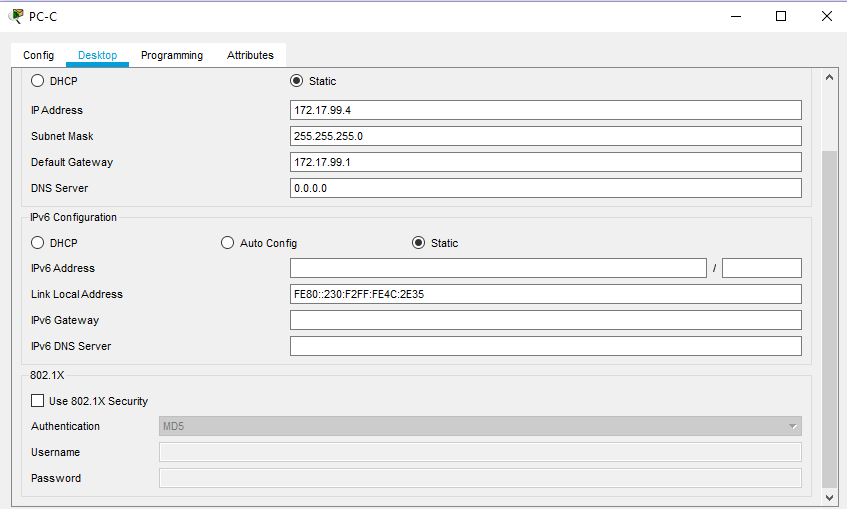
PC-A



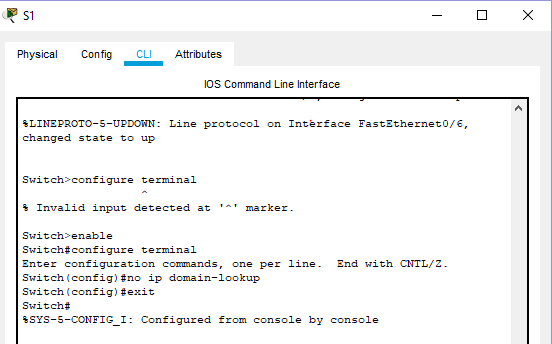
PC-B

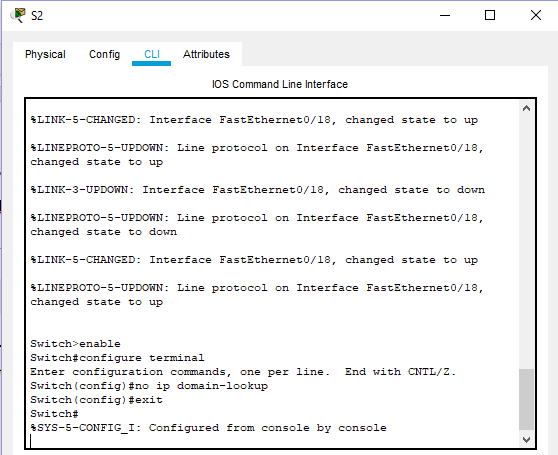


PC-C

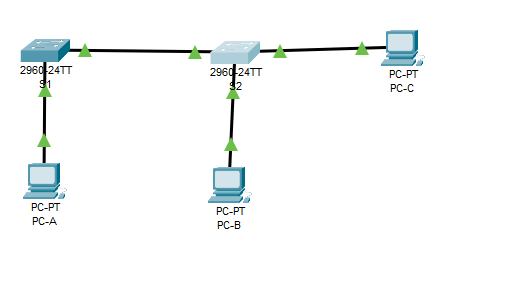


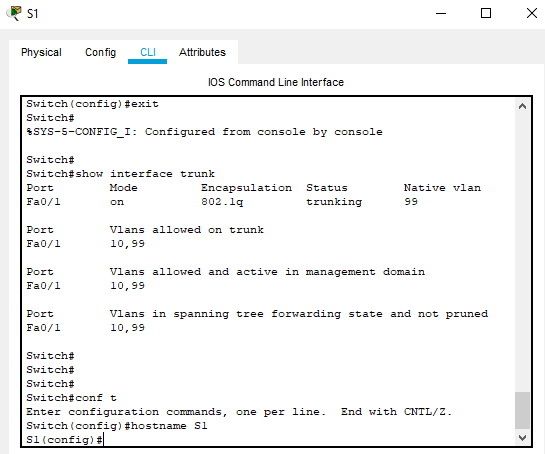
1. configurar los parámetros básicos para cada switch.
   * 1. Desactive la búsqueda del DNS.

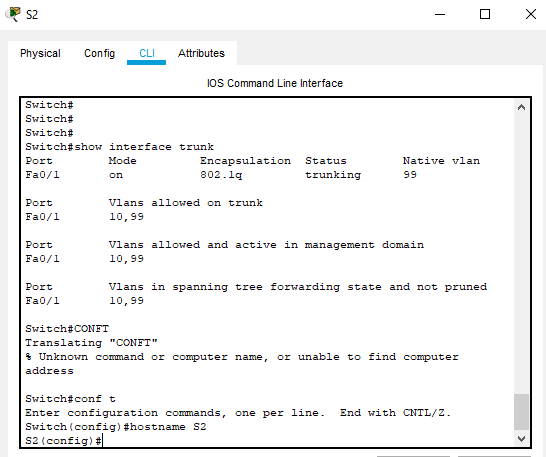




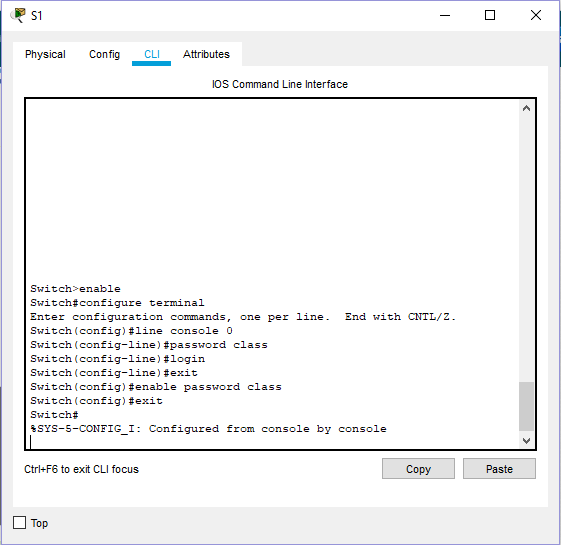
* + 1. Configure los nombres de los dispositivos como se muestra en la topología.

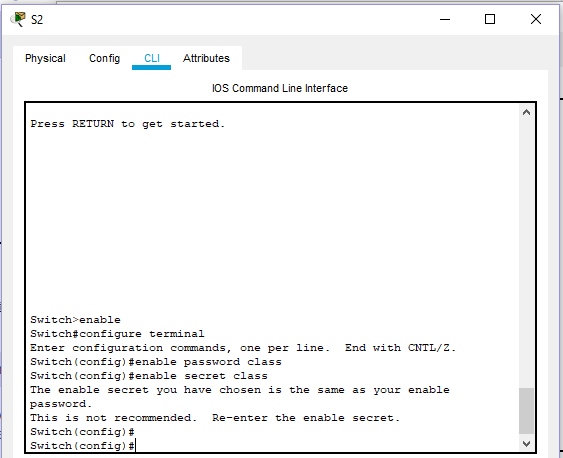




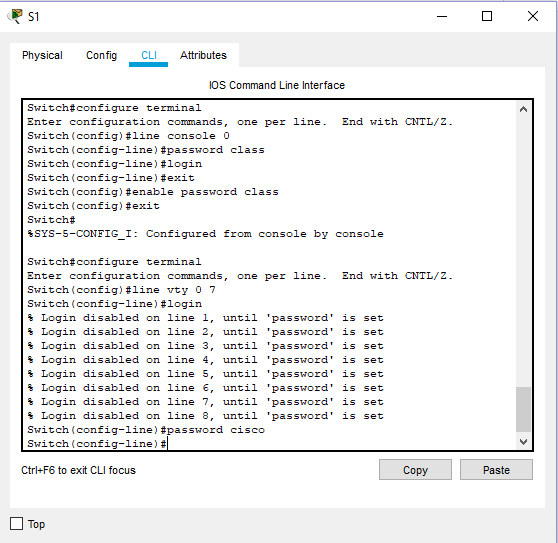


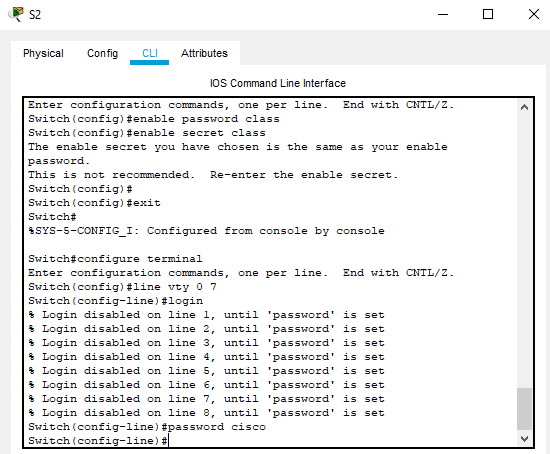
* + 1. Asigne **class** como la contraseña del modo EXEC privilegiado.

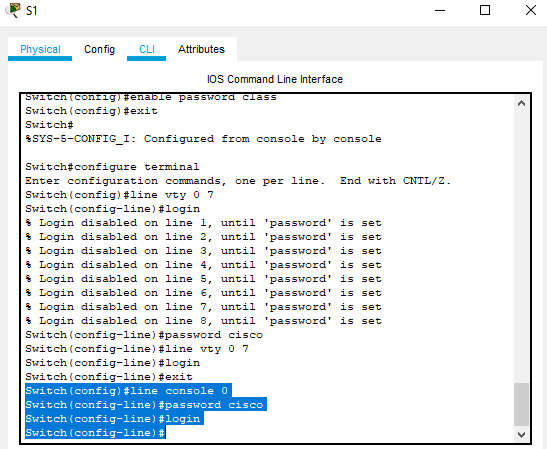


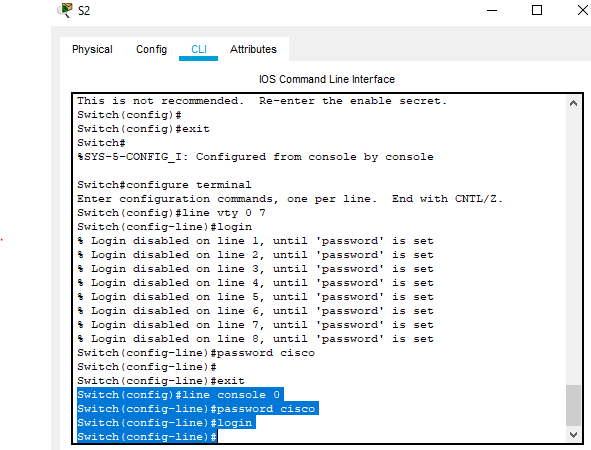


* + 1. Asigne **cisco** como la contraseña de VTY y la contraseña de consola, y habilite el inicio de sesión para las líneas de vty y de consola.

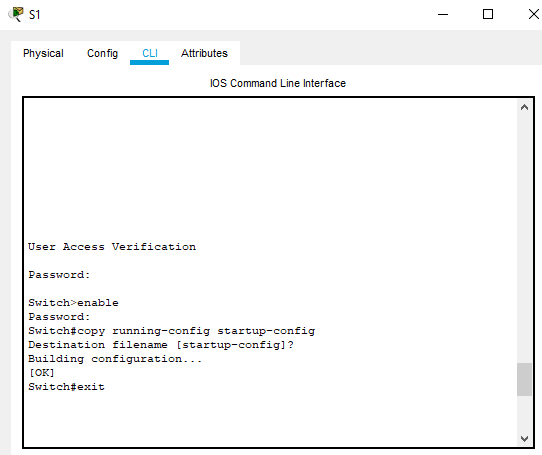


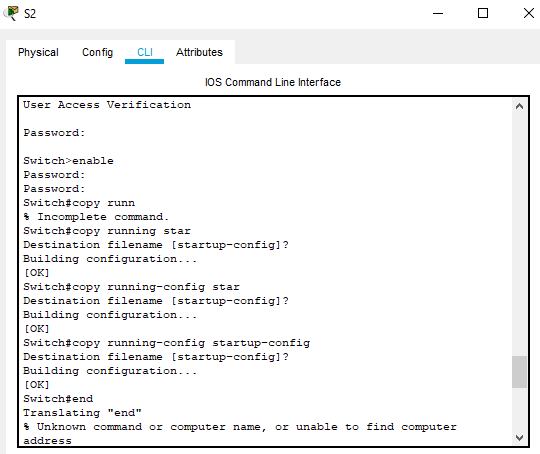




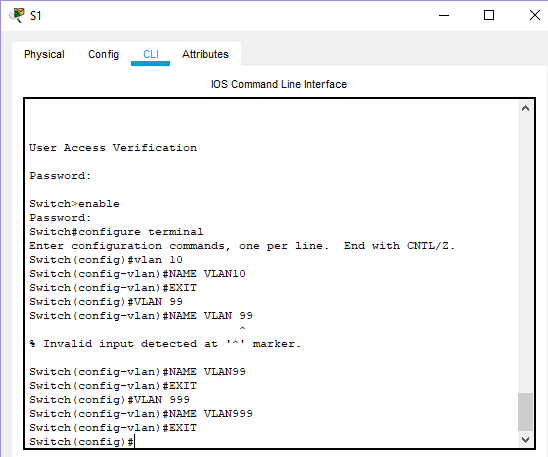


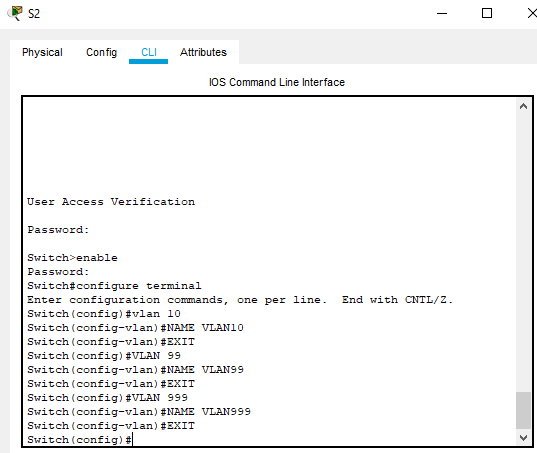
* + 1. Configure el inicio de sesión sincrónico para las líneas de vty y de consola.



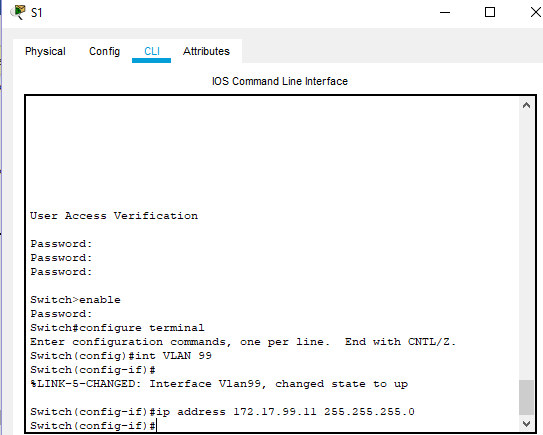


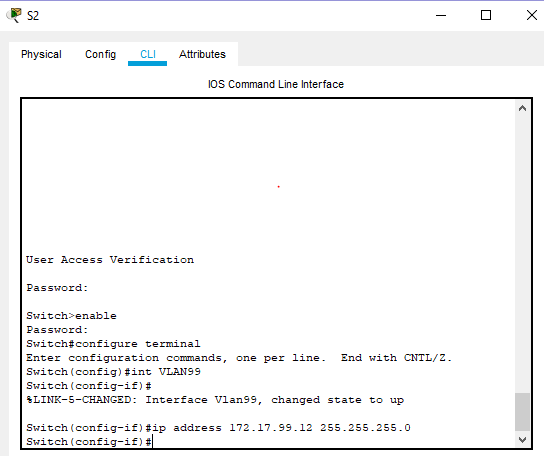
1. configurar las VLAN en cada switch.
   * 1. Cree las VLAN y asígneles nombres según la tabla de asignaciones de VLAN.



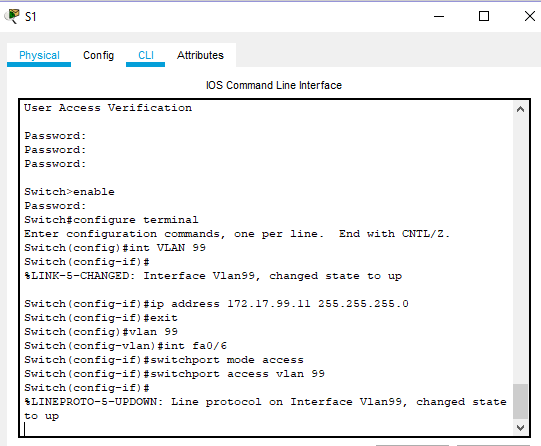


* + 1. Configure la dirección IP que se indica para la VLAN 99 en la tabla de direccionamiento en ambos switches.

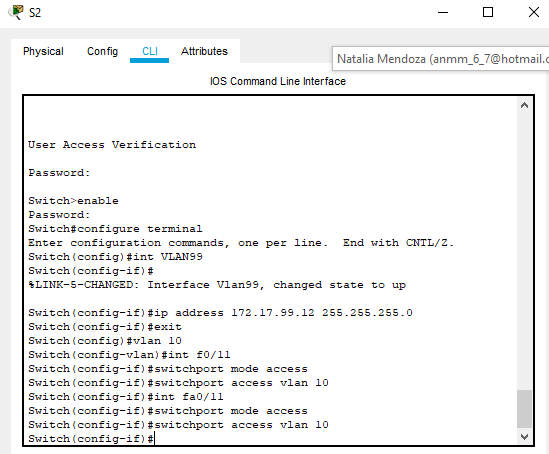




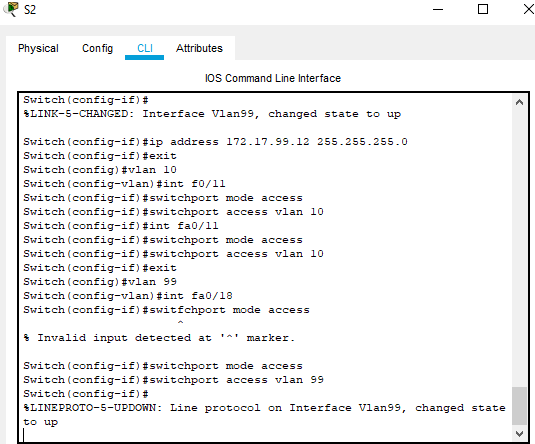
* + 1. Configure F0/6 en el S1 como puerto de acceso y asígnelo a la VLAN 99.



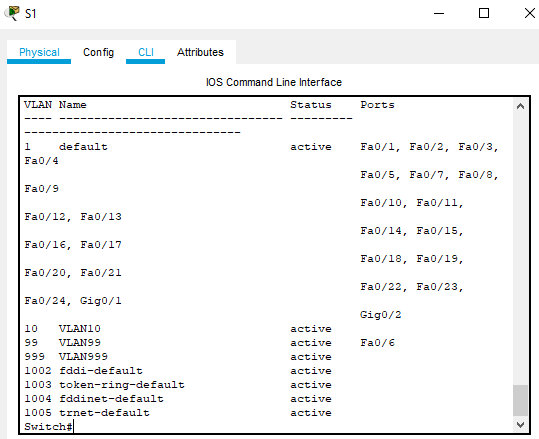
* + 1. Configure F0/11 en el S2 como puerto de acceso y asígnelo a la VLAN 10.

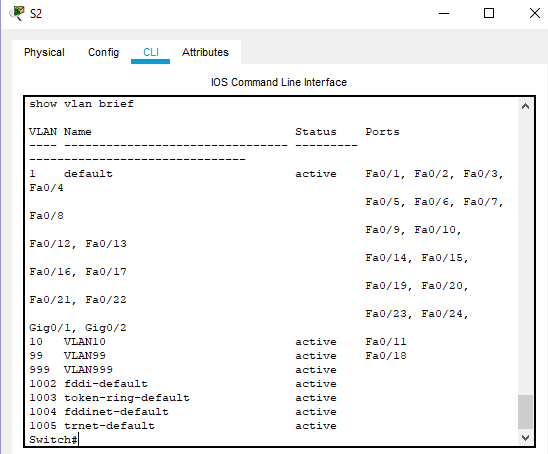


* + 1. Configure F0/18 en el S2 como puerto de acceso y asígnelo a la VLAN 99.



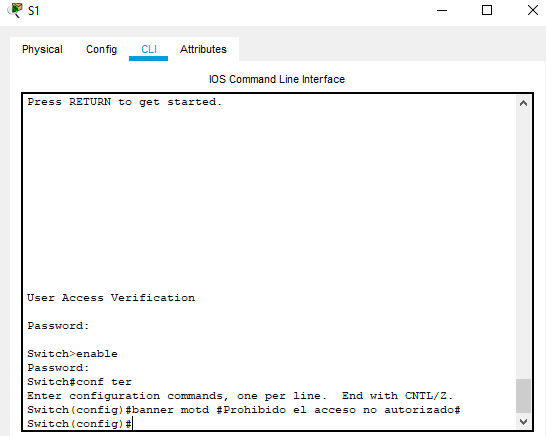
* + 1. Emita el comando **show vlan brief** para verificar las asignaciones de VLAN y de puertos.

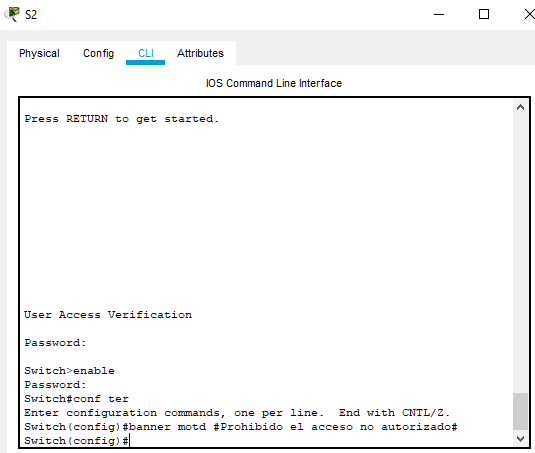




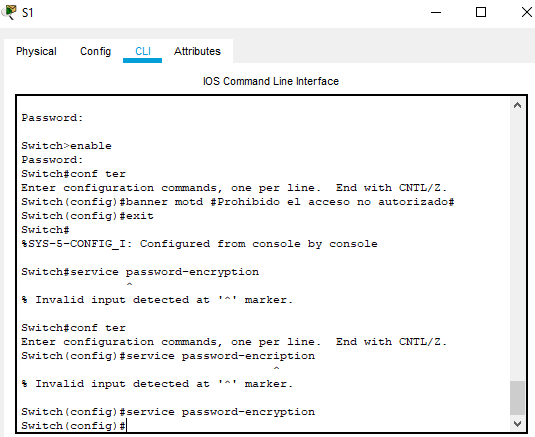
¿A qué VLAN pertenecería un puerto sin asignar, como F0/8 en el S2?

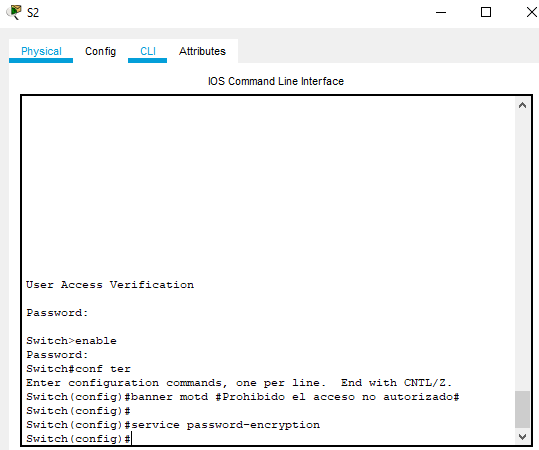
1. configurar la seguridad básica del switch.
   * 1. Configure un mensaje MOTD para advertir a los usuarios que se prohíbe el acceso no autorizado.



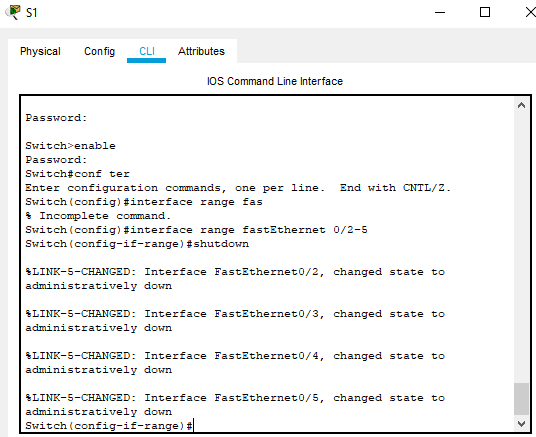


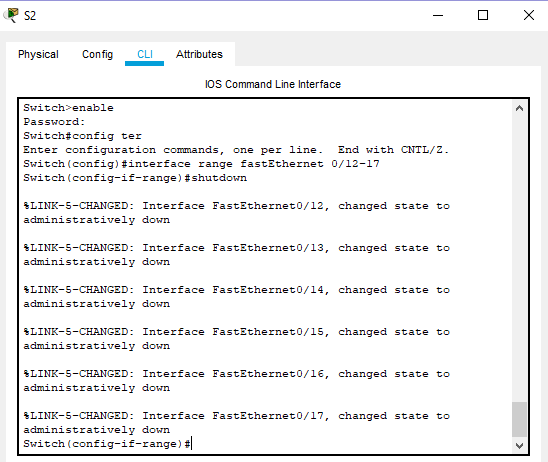
* + 1. Encripte todas las contraseñas.





* + 1. Desactive todos los puertos físicos sin utilizar.



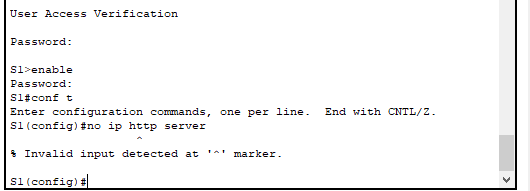


* + 1. Deshabilite el servicio web básico en ejecución.

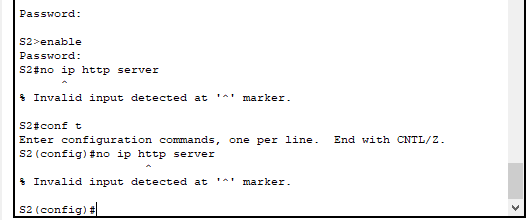
S1(config)# **no ip http server**

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

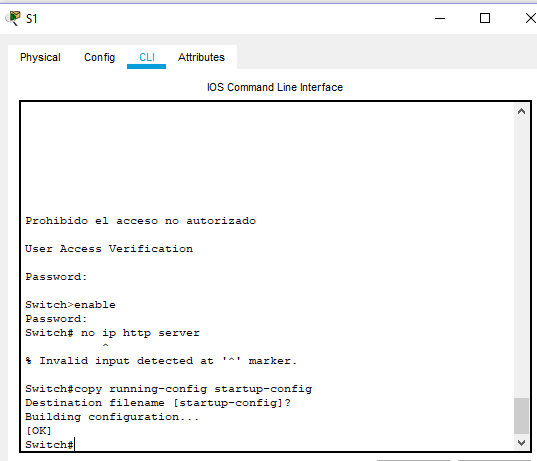
S1

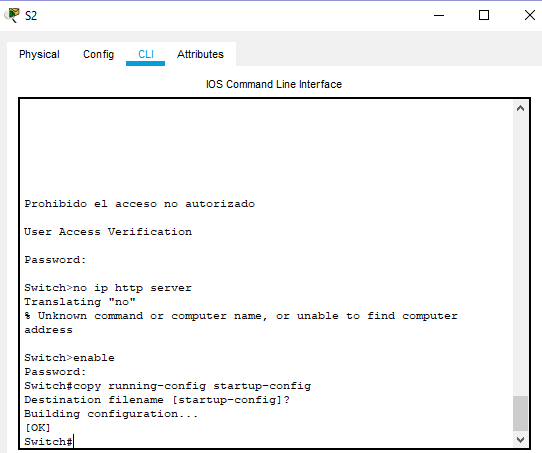


S2

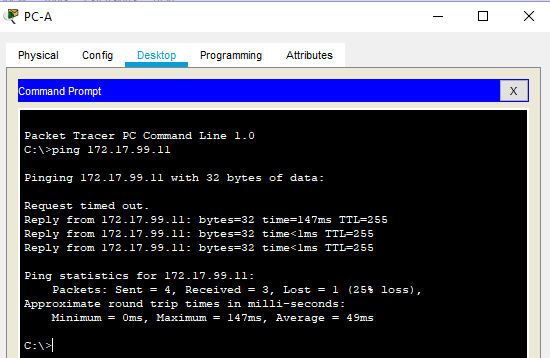


* + 1. Copie la configuración en ejecución en la configuración de inicio.

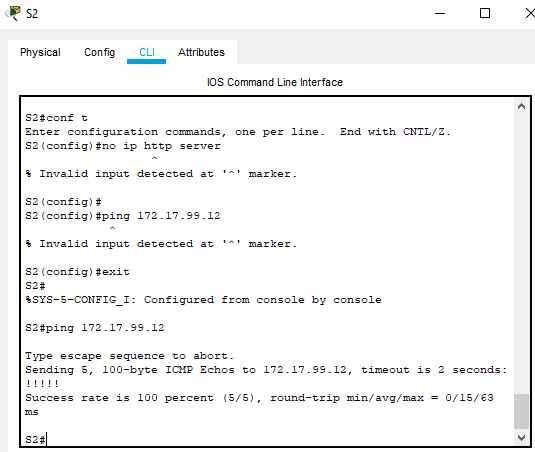




1. verificar la conectividad entre la información de VLAN y los dispositivos.
   * 1. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué? Si porque están configuradas las rutas.

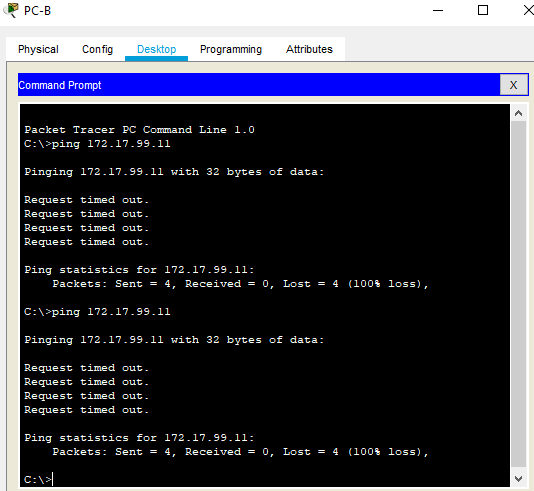


* + 1. Desde el S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?

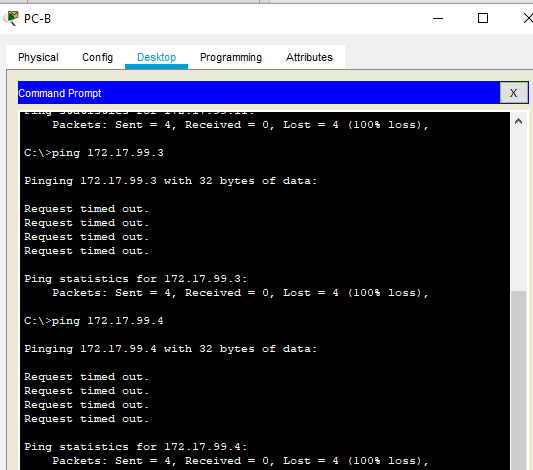


* + 1. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué? No, porque La red no cuenta con las subredes conectadas pero no se han configurado las rutas que permiten el intercambio entre las mismas

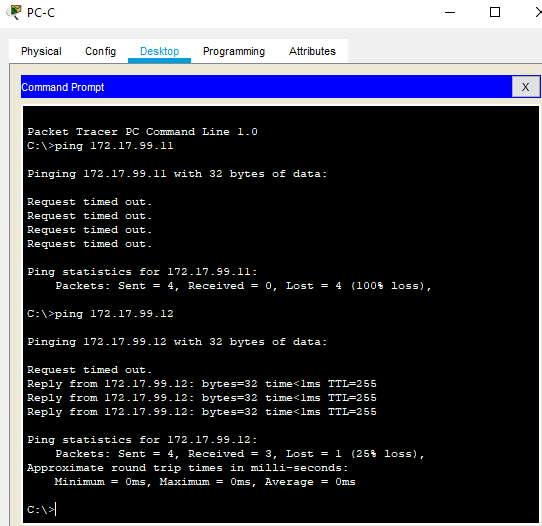
Ping de PC-B a S1 y S2



Ping de PC-B a PC-A y PC-C



* + 1. 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? No, porque la red no cuenta con una serie de subredes conectadas pero no se han configurado las rutas que permiten el intercambio entre las mismas

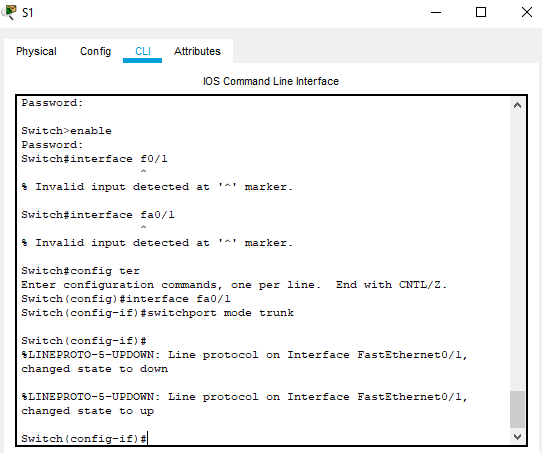


**Nota**: puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

1. implementar seguridad de VLAN en los switches
2. configurar puertos de enlace troncal en el S1 y el S2.
   * 1. Configure el puerto F0/1 en el S1 como puerto de enlace troncal.

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

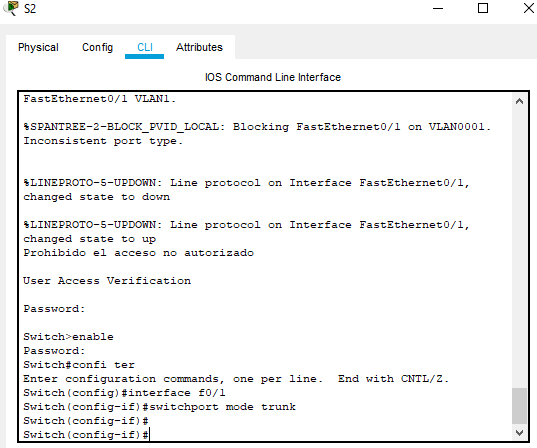
S1(config-if)# **switchport mode trunk**



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

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

S2(config-if)# **switchport mode trunk**



* + 1. Verifique los enlaces troncales en el S1 y el S2. Emita el comando **show interface trunk** en los dos switches.

S1# **show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1

Port Vlans allowed on trunk

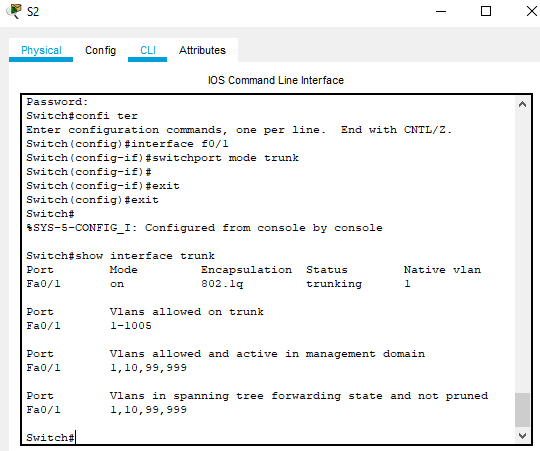
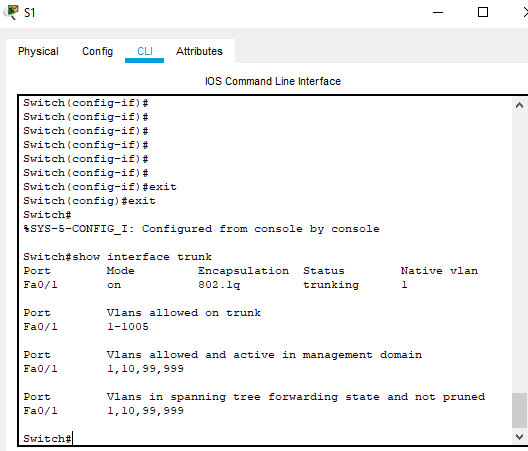
Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,99,999

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,99,999



1. 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.

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

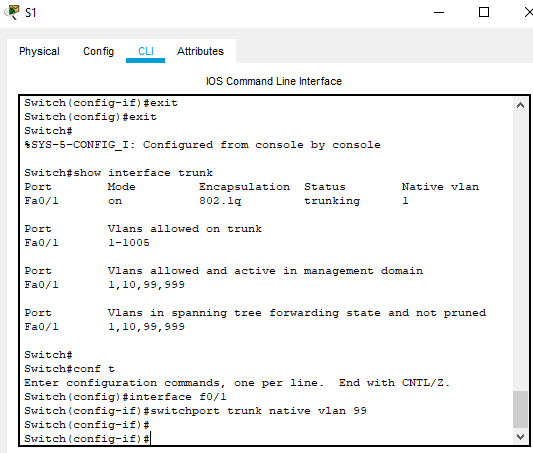
Respuesta: 1

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

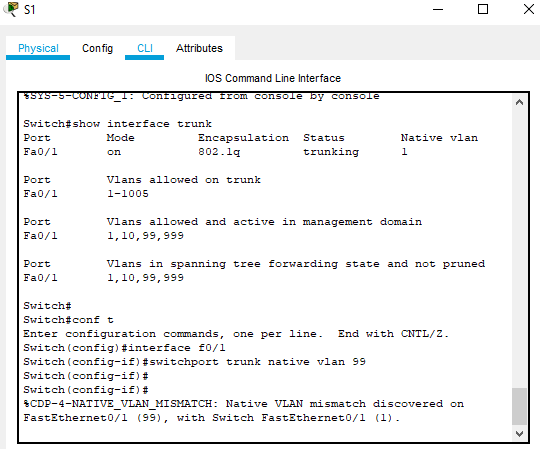
S1# **config t**

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

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



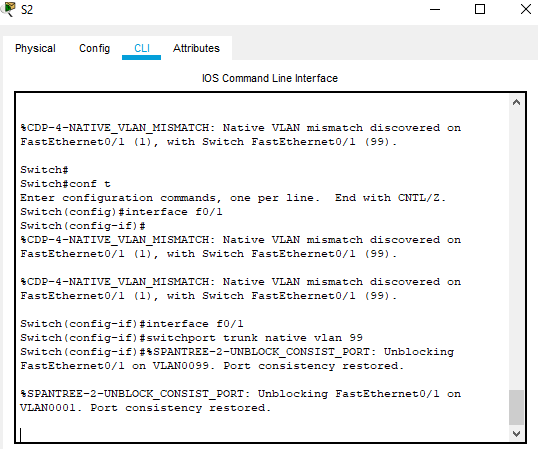
* + 1. Espere unos segundos. Debería comenzar a recibir mensajes de error en la sesión de consola del S1. ¿Qué significa el mensaje %CDP-4-NATIVE\_VLAN\_MISMATCH:?



* + 1. 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**



* + 1. Verifique que ahora la VLAN nativa sea la 99 en ambos switches. A continuación, se muestra el resultado del S1.

S1# **show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 99

Port Vlans allowed on trunk

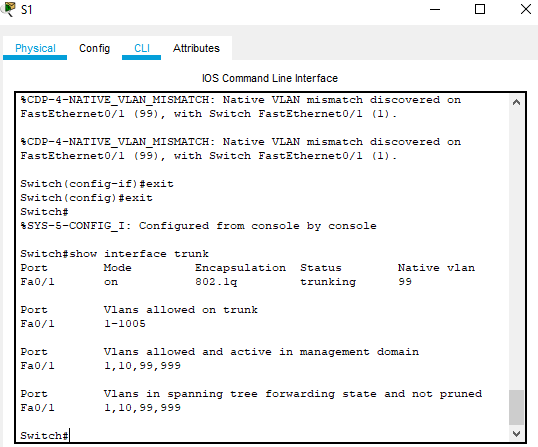
Fa0/1 1-4094

Port Vlans allowed and active in management domain

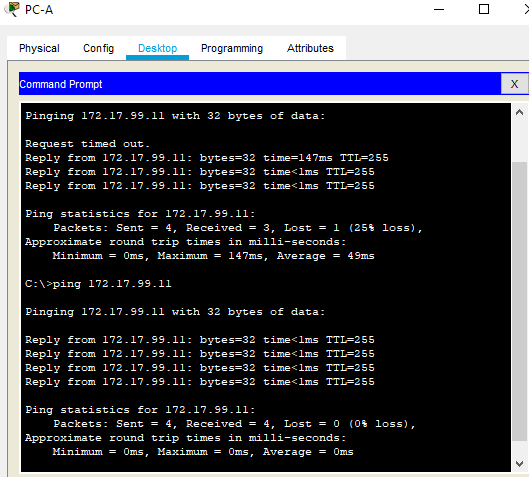
Fa0/1 1,10,99,999

Port Vlans in spanning tree forwarding state and not pruned

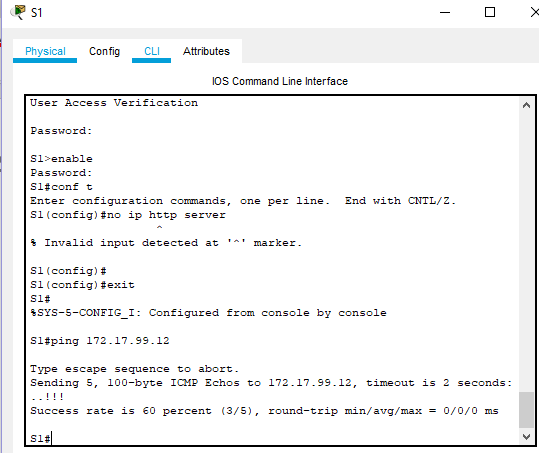
Fa0/1 10,999



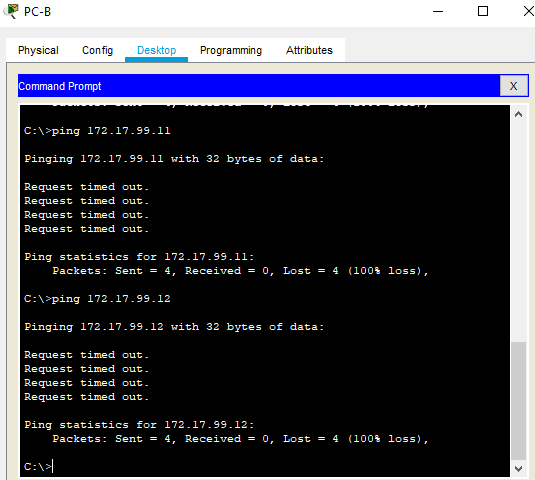
1. verificar que el tráfico se pueda transmitir correctamente a través del enlace troncal.
   * 1. En el símbolo del sistema de la PC-A, haga ping a la dirección de administración del S1. ¿Tuvieron éxito los pings? ¿Por qué? Si tuvieron éxito.

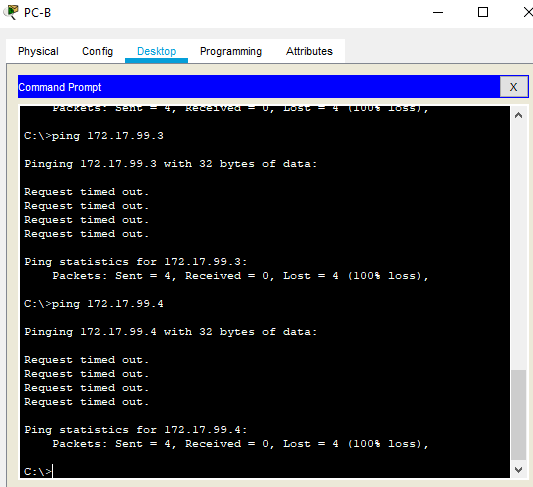


* + 1. En la sesión de consola del S1, haga ping a la dirección de administración del S2. ¿Tuvieron éxito los pings? ¿Por qué?

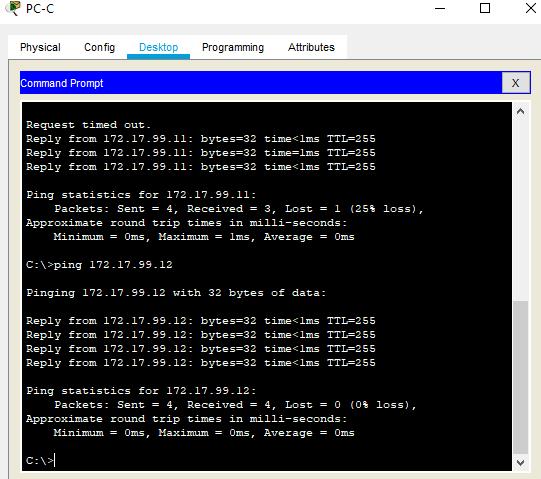


* + 1. En el símbolo del sistema de la PC-B, haga ping a las direcciones de administración del S1 y el S2, y a la dirección IP de la PC-A y la PC-C. ¿Los pings se realizaron correctamente? ¿Por qué? No.





* + 1. 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?. No.



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

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

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

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

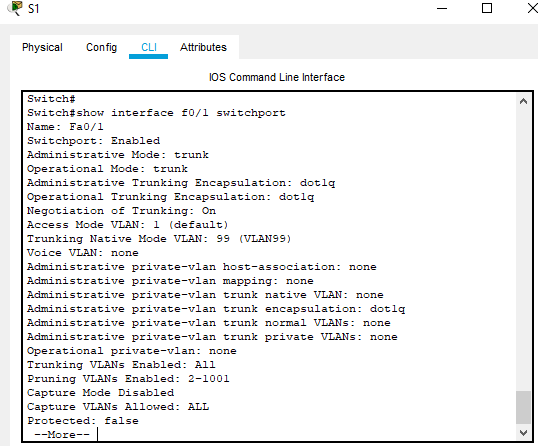
Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

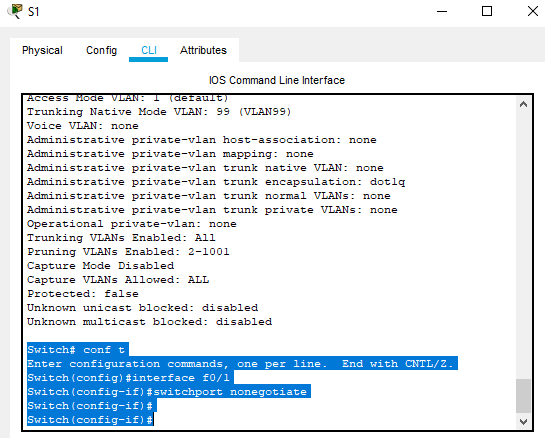
<Output Omitted>



* + 1. Desactive la negociación en el S1.

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

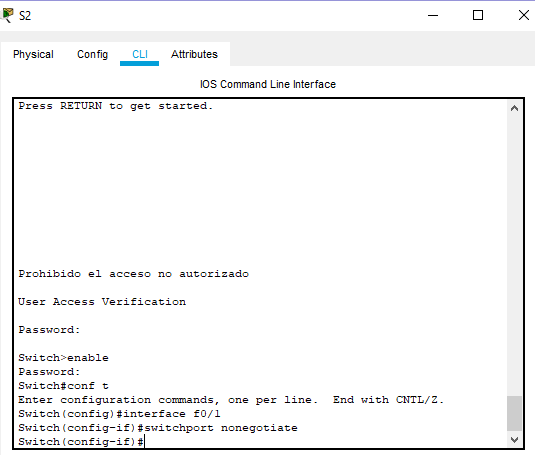
S1(config-if)# **switchport nonegotiate**



* + 1. Desactive la negociación en el S2.

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

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



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

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

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

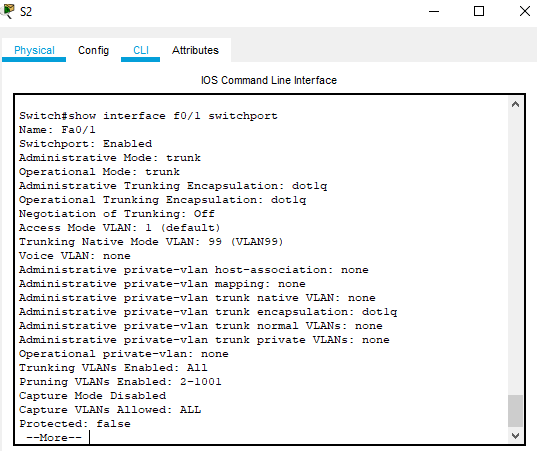
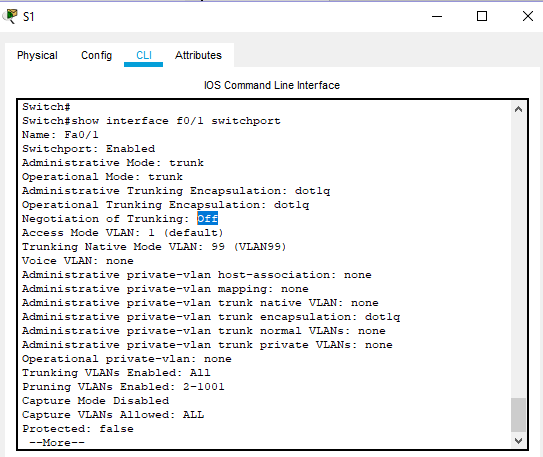
Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: Off

<Output Omitted>



1. 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.

* + 1. Emita el comando **show interface f0/2 switchport** en el S1. Observe el modo administrativo y el estado para la negociación de enlaces troncales.

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

Name: Fa0/2

Switchport: Enabled

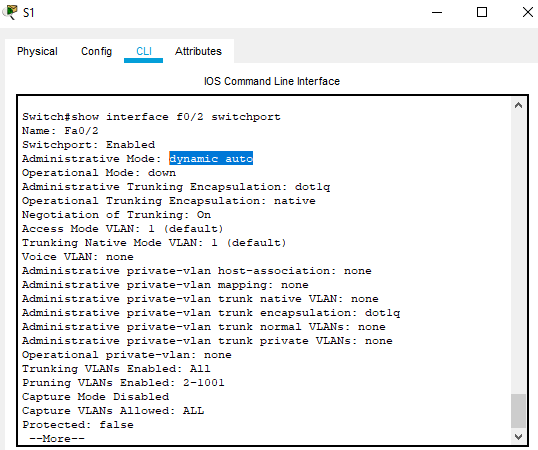
Administrative Mode: dynamic auto

Operational Mode: down

Administrative Trunking Encapsulation: dot1q

Negotiation of Trunking: On

<Output Omitted>

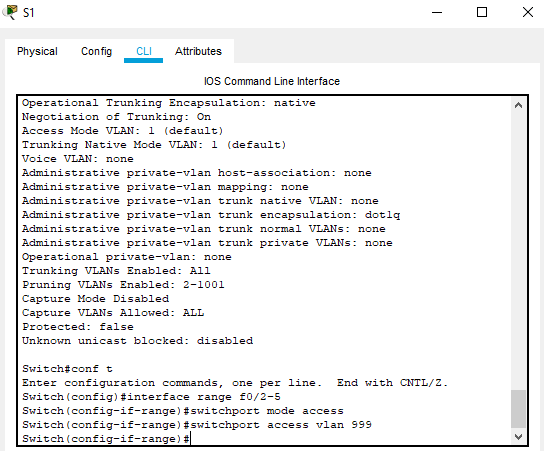


* + 1. Deshabilite los enlaces troncales en los puertos de acceso del S1.

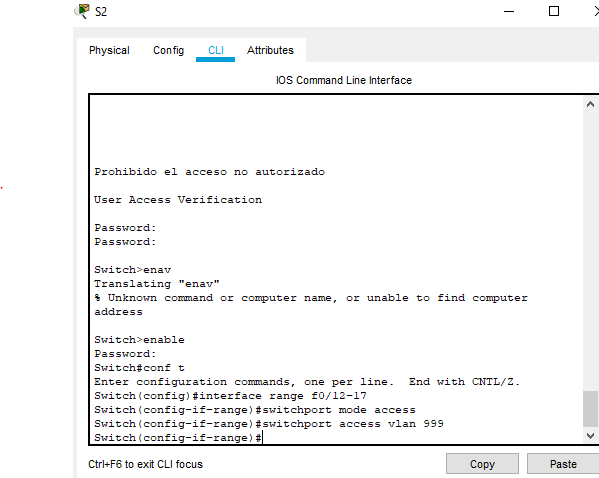
S1(config)# **interface range f0/2 – 5**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 999**



* + 1. Deshabilite los enlaces troncales en los puertos de acceso del S2.



* + 1. Verifique que el puerto F0/2 esté establecido en modo de acceso en el S1.

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

Name: Fa0/2

Switchport: Enabled

Administrative Mode: static access

Operational Mode: down

Administrative Trunking Encapsulation: dot1q

Negotiation of Trunking: Off

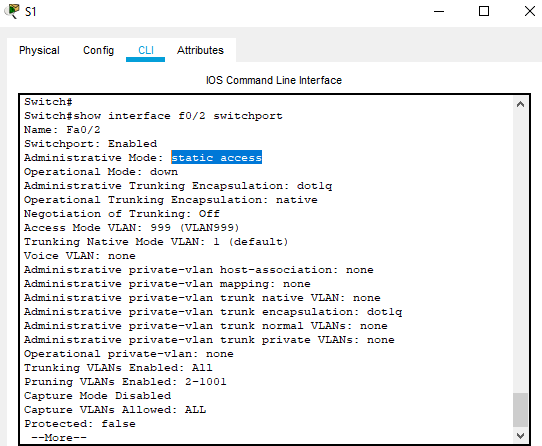
Access Mode VLAN: 999 (BlackHole)

Trunking Native Mode VLAN: 1 (default)

Administrative Native VLAN tagging: enabled

Voice VLAN: none

<Output Omitted>



* + 1. Verifique que las asignaciones de puertos de VLAN en ambos switches sean las correctas. A continuación, se muestra el S1 como ejemplo.

S1# **show vlan brief**

VLAN Name Status Ports

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

1 default active Fa0/7, Fa0/8, Fa0/9, Fa0/10

Fa0/11, Fa0/12, Fa0/13, Fa0/14

Fa0/15, Fa0/16, Fa0/17, Fa0/18

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24, Gi0/1, Gi0/2

10 Data active

99 Management&Native active Fa0/6

999 BlackHole active Fa0/2, Fa0/3, Fa0/4, Fa0/5

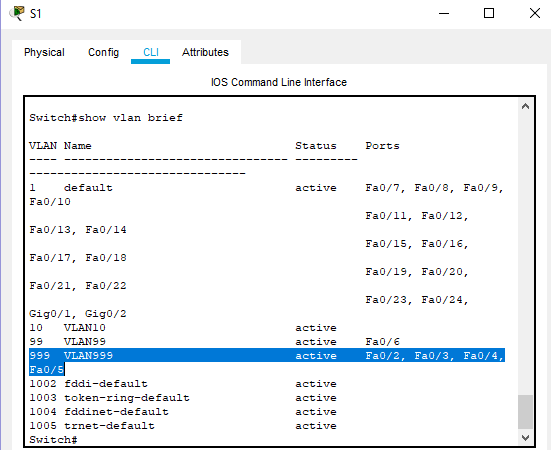
1002 fddi-default act/unsup

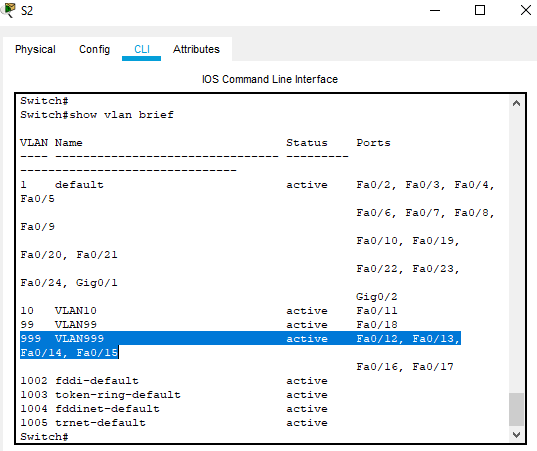
1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Restrict VLANs allowed on trunk ports.



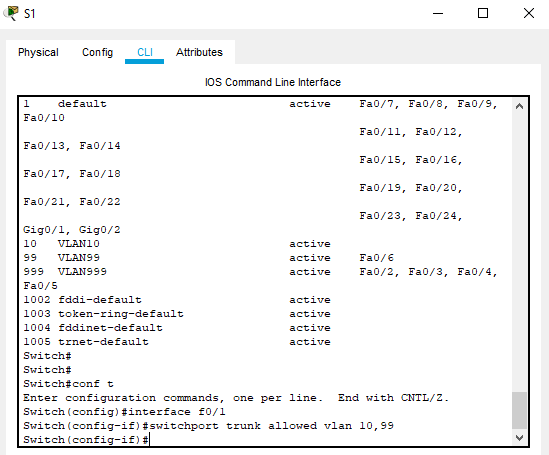


De manera predeterminada, se permite transportar todas las VLAN en los puertos de enlace troncal. Por motivos de seguridad, se recomienda permitir que solo se transmitan las VLAN deseadas y específicas a través de los enlaces troncales en la red.

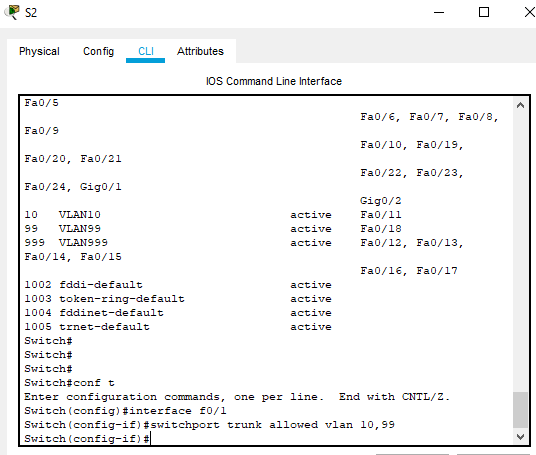
* + 1. Restrinja el puerto de enlace troncal F0/1 en el S1 para permitir solo las VLAN 10 y 99.

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

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



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



* + 1. Verifique las VLAN permitidas. Emita el comando **show interface trunk** en el modo EXEC privilegiado en el S1 y el S2

S1# **show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 99

Port Vlans allowed on trunk

Fa0/1 10,99

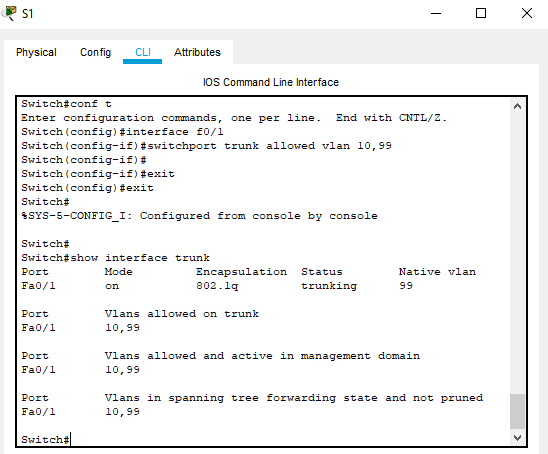
Port Vlans allowed and active in management domain

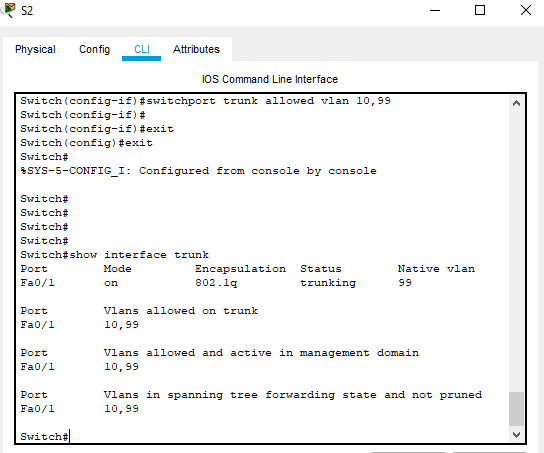
Fa0/1 10,99

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 10,99

¿Cuál es el resultado?

1. 



1. Reflexión

¿Qué problemas de seguridad, si los hubiera, tiene la configuración predeterminada de un switch Cisco? El servidor HTTP está habilitado de manera determinada y no admite el comando.