

5.2.2.9 - Configuración de seguridad de un switch



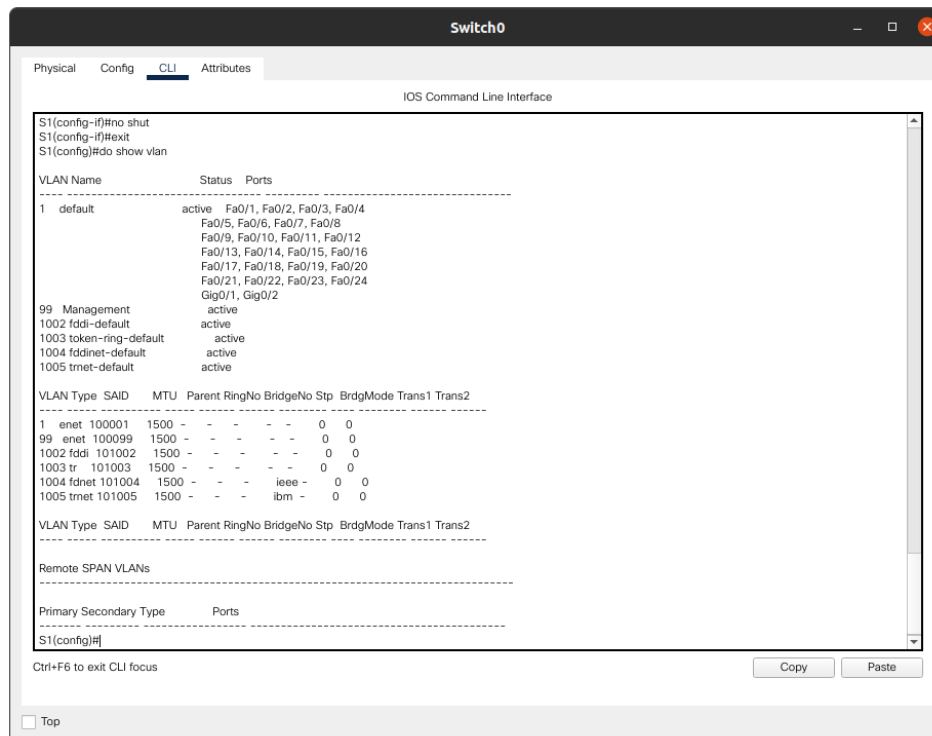
Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|--------|-----------|--------------|---------------|-----------------|
| R1 | G0/0/1 | 172.16.99.1 | 255.255.255.0 | N/A |
| S1 | VLAN 99 | 172.16.99.11 | 255.255.255.0 | 172.16.99.1 |
| PC-A | NIC | 172.16.99.3 | 255.255.255.0 | 172.16.99.1 |

Preguntas

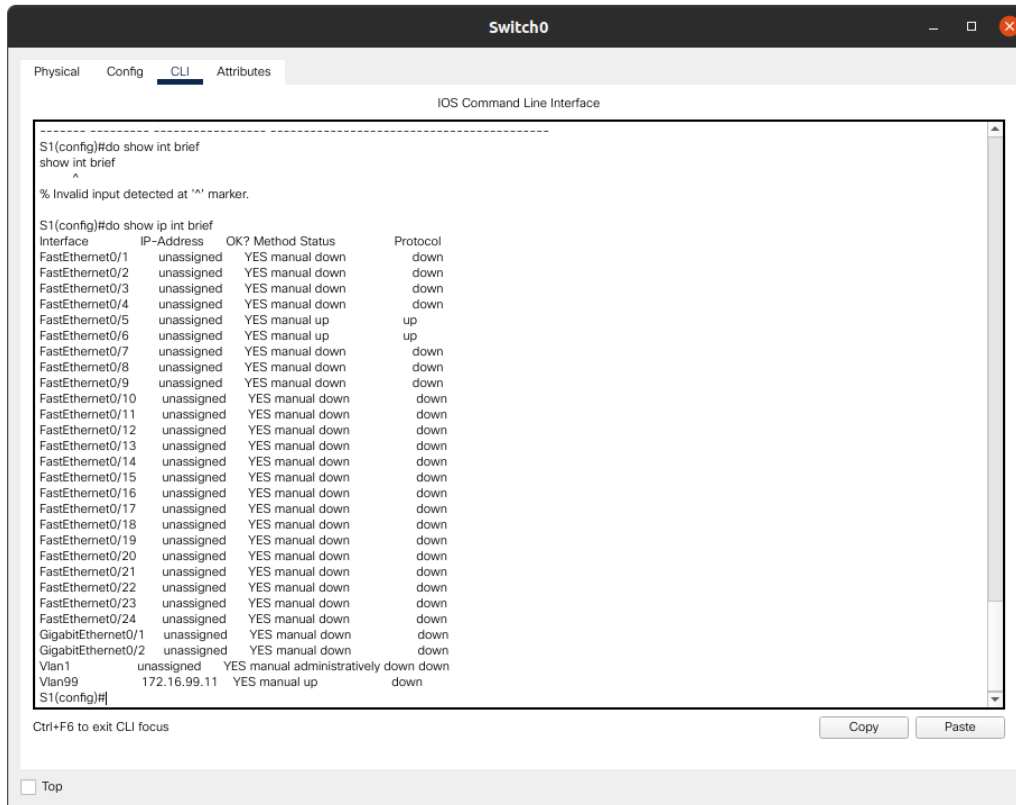
Parte 2, Paso 3, pregunta e:

Usa el comando *show vlan*, ¿Cuál es el estatus de la VLAN99? Aparece activa.



Parte 2, Paso 3, pregunta f:

Usa el comando *show ip interface brief*, ¿Cuál es el estatus y el protocolo para *management interface VLAN99*? El estatus está manualmente activa, y el protocolo no se encuentra activo



The screenshot shows a network switch CLI window titled "Switch0". The window has tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, showing the "IOS Command Line Interface". The user has entered the command "show ip interface brief" and the output is displayed as follows:

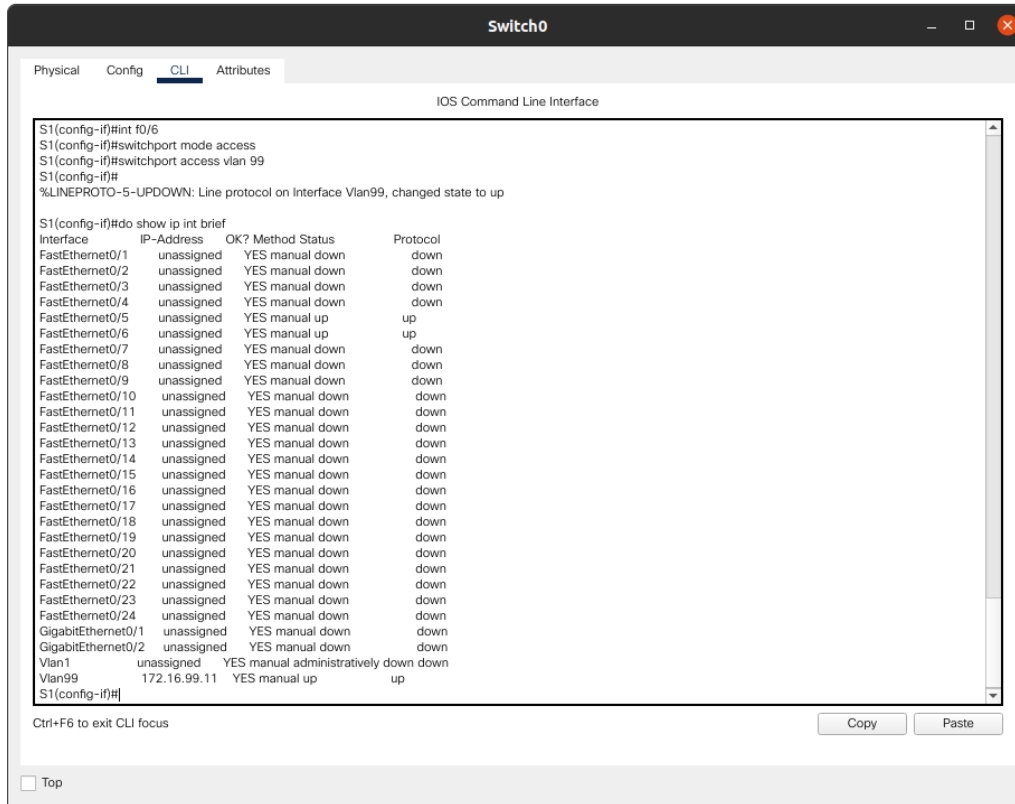
```
S1(config)#do show ip int brief
show ip int brief
^
% Invalid input detected at '^' marker.

S1(config)#do show ip int 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
FastEthernet0/11 unassigned      YES manual down        down
FastEthernet0/12 unassigned      YES manual down        down
FastEthernet0/13 unassigned      YES manual down        down
FastEthernet0/14 unassigned      YES manual down        down
FastEthernet0/15 unassigned      YES manual down        down
FastEthernet0/16 unassigned      YES manual down        down
FastEthernet0/17 unassigned      YES manual down        down
FastEthernet0/18 unassigned      YES manual down        down
FastEthernet0/19 unassigned      YES manual down        down
FastEthernet0/20 unassigned      YES manual down        down
FastEthernet0/21 unassigned      YES manual down        down
FastEthernet0/22 unassigned      YES manual down        down
FastEthernet0/23 unassigned      YES manual down        down
FastEthernet0/24 unassigned      YES manual down        down
GigabitEthernet0/1 unassigned      YES manual down        down
GigabitEthernet0/2 unassigned      YES manual down        down
Vlan1          unassigned      YES manual administratively down down
Vlan99          172.16.99.11    YES manual up          down
S1(config)#
```

At the bottom of the window, there is a "Ctrl+F6 to exit CLI focus" message and "Copy" and "Paste" buttons. A "Top" button is also visible at the bottom left.

Parte 2, Paso 3, pregunta h:

Usa el comando **show ip interface brief**. ¿Cuál es el estatus y el protocolo para VLAN 99?
Ambos se encuentran activos.



The screenshot shows a network switch CLI window titled "Switch0". The "CLI" tab is selected. The command prompt is "S1(config-if)#". The user has entered the command "show ip int brief". The output is as follows:

```
S1(config-if)#show ip int 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
FastEthernet0/11 unassigned     YES manual down    down
FastEthernet0/12 unassigned     YES manual down    down
FastEthernet0/13 unassigned     YES manual down    down
FastEthernet0/14 unassigned     YES manual down    down
FastEthernet0/15 unassigned     YES manual down    down
FastEthernet0/16 unassigned     YES manual down    down
FastEthernet0/17 unassigned     YES manual down    down
FastEthernet0/18 unassigned     YES manual down    down
FastEthernet0/19 unassigned     YES manual down    down
FastEthernet0/20 unassigned     YES manual down    down
FastEthernet0/21 unassigned     YES manual down    down
FastEthernet0/22 unassigned     YES manual down    down
FastEthernet0/23 unassigned     YES manual down    down
FastEthernet0/24 unassigned     YES manual down    down
GigabitEthernet0/1 unassigned     YES manual down    down
GigabitEthernet0/2 unassigned     YES manual down    down
Vlan1          unassigned      YES manual administratively down down
Vlan99          172.16.99.11   YES manual up      up
S1(config-if)#
```

At the bottom of the window, there is a "Copy" button and a "Paste" button. A "Top" button is also visible at the bottom left.

Parte 2, Paso 4

PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 172.16.99.11

Pinging 172.16.99.11 with 32 bytes of data:

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

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

C:\>ping 172.16.99.1

Pinging 172.16.99.1 with 32 bytes of data:

Reply from 172.16.99.1: bytes=32 time=62ms TTL=255
Reply from 172.16.99.1: bytes=32 time<1ms TTL=255
Reply from 172.16.99.1: bytes=32 time<1ms TTL=255
Reply from 172.16.99.1: bytes=32 time<1ms 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 = 62ms, Average = 15ms

C:\>|
```

☐ Top

Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
S1 con0 is now available

Press RETURN to get started.

User Access Verification

Password:
S1>enable
Password:
S1#ping 172.16.99.1

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

S1#|
```

Ctrl+F6 to exit CLI focus

☐ Top

Copy Paste

Parte 3, paso1, pregunta e:

Verifica la configuración de ssh con: *show ip ssh*

¿Qué versión the ssh se utiliza? Versión 1.99

¿Cuántos intentos de autenticación se permiten con ssh? 3 intentos.

¿Cuál es el timeout determinado? 120 segundos.

Parte 3, paso2, pregunta a:

Verifica la configuración de ssh con: *show ip ssh*

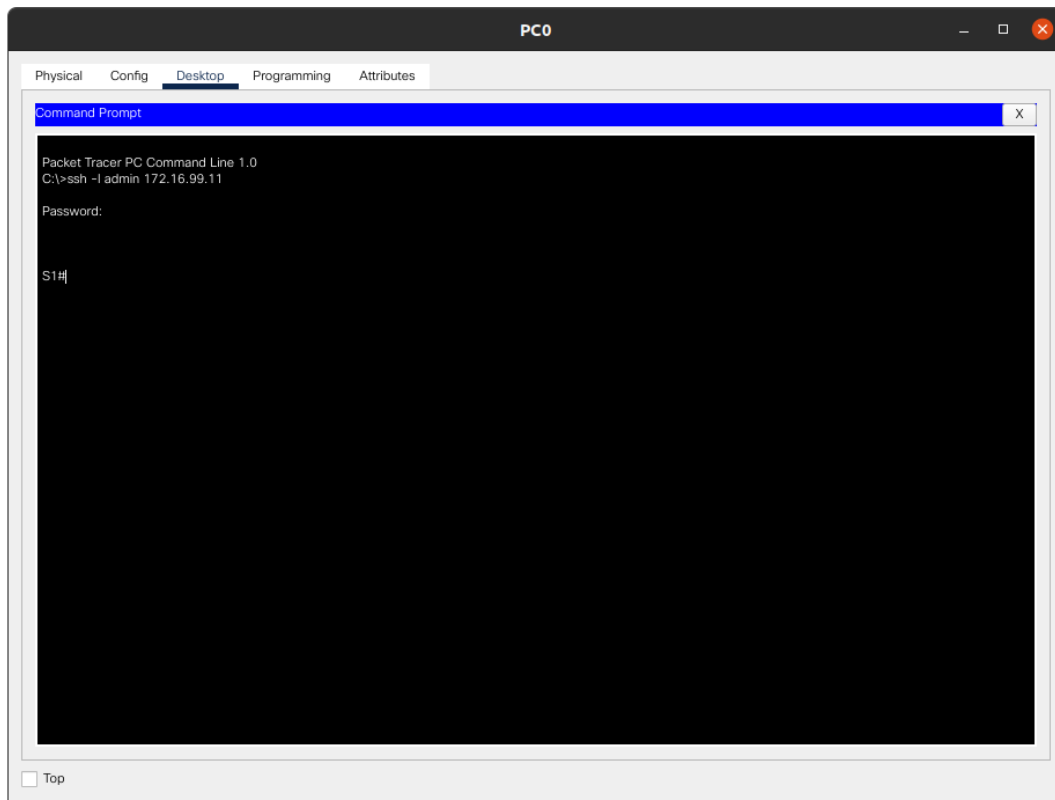
¿Cuántos intentos de autenticación se permiten con ssh? 2 intentos.

¿Cuál es el timeout determinado? 75 segundos.

On PC-A, execute de following command in the CLI: `ssh -l admin 172.16.99.11`

¿Was the connection succesful? Sí

¿Cuál fue el prompt? S# ¿Por qué? Porque es el prompt del switch



¿Por qué activaste el puerto de seguridad en el switch? Por seguridad.

¿Por qué los puertos no utilizados son desactivados? Para que haya un menor riesgo de ser atacado con éxito ya que se tiene menos vulnerabilidades.

Configuración Router

```
enable  
config t
```

```
hostname R1
```

```
service password  
no ip domain-lookup
```

```
line con 0  
password cisco  
login  
loggin sync
```

```
line vty 0 15
```

```
password cisco  
login  
loggin sync
```

```
enable password class
```

```
int g0/0/1  
desc Interfaz con el switch  
ip add 172.16.99.1 255.255.255.0  
no shut
```

Configuración Switch

```
enable  
config t
```

```
hostname S1
```

```
ip domain-name CCNA-Lab.com  
enable secret class  
username admin privilege 15 secret sshadmin  
crypto key generate rsa  
1024
```

```
banner motd #  
Personal no autorizado sera perseguido por la ley!#
```

```
ip ssh time-out 75  
ip ssh authentication-retries 2
```

```
line con 0  
password cisco  
login  
loggin sync
```

```
line vty 0 15  
password cisco  
transport input ssh  
login local  
loggin syn
```

```
vlan 99  
name Management
```

```
int vlan 99  
ip add 172.16.99.11 255.255.255.0  
no shut
```

```
int f0/5  
switchport mode access  
switchport access vlan 99
```

```
int f0/6
```

```
switchport mode access  
switchport access vlan 99
```

```
exit
```