Configuring Switch Security Features

CIT 167

Chaz Davis

BCTC
Spring 2020

February 26, 2020

Part 1: The Lab

i) Cable the Network I created and cabled the network according to the diagram.

ii) Initialize and reload the router and switch

I went into router configuration, and checked the flash.

iii) Configure an IP address on PC-A

I then went to PC-A and setup the IP configuration.

iv) Configure basic settings on R1

I went into R1 and entered the commands and then copied the running and startup configs.

v) Configure basic settings on S1

I ran the commands from the diagram, setting up basic settings and then creatings and configuring vlan 99.

When I issued the `show vlan` command it shows vlan 99 as active.

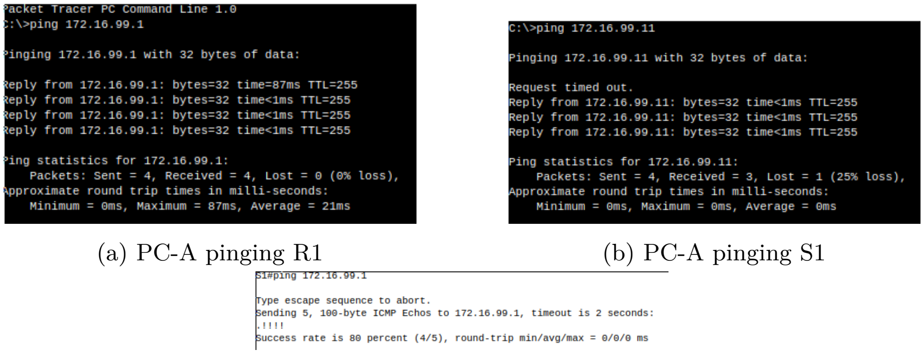
When I ran the command `show ip interface brief` the status was ok and protocol was down.

It shows as down becuase its not connected to a network.

After assigning f0/5 and f0/6 to vlan 99 no when running the `show ip int brief` command we can see vlan 99 as up.

vi) Verify Connectivity between Devices

As you can see in Fig. 1 All of the pings were successful.



```
acket Tracer PC Command Line 1.0
:\>ping 172.16.99.1

inging 172.16.99.1 with 32 bytes of data:

eply from 172.16.99.1: bytes=32 time=87ms TTL=255
eply from 172.16.99.1: bytes=32 time<1ms TTL=255
eply from 172.16.99.1: bytes=32 time<1ms TTL=255
eply from 172.16.99.1: bytes=32 time<1ms TTL=255

ing statistics for 172.16.99.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 87ms, Average = 21ms
```

(a) PC-A pinging R1

```
C:\>ping 172.16.99.11

Pinging 172.16.99.11 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

(b) PC-A pinging S1

```
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
```

(c) S1 pinging R1

Figure 1: Successful pings on the network

vii) Configure SSH access on S1

The ssh-version is 1.99
SSH will allow 3 retries
the default timeout is 120 secs

viii) Modify the SSH configuration on S1

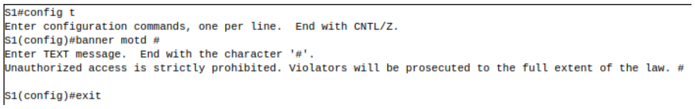
It will now allow 2 retries, so a total of 3 attempts.
The timeout would be 75 seconds. So, 1 minute and 15 seconds.

a)

It was successful, and the prompt said unauthorized access is strictly prohibited, and the gave the S1 prompt with the octothorpe signifying the admin account.

ix) Configure general security features on S1

a)



```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Unauthorized access is strictly prohibited. Violators will be prosecuted to the full extent of the law. #

S1(config)#exit
```

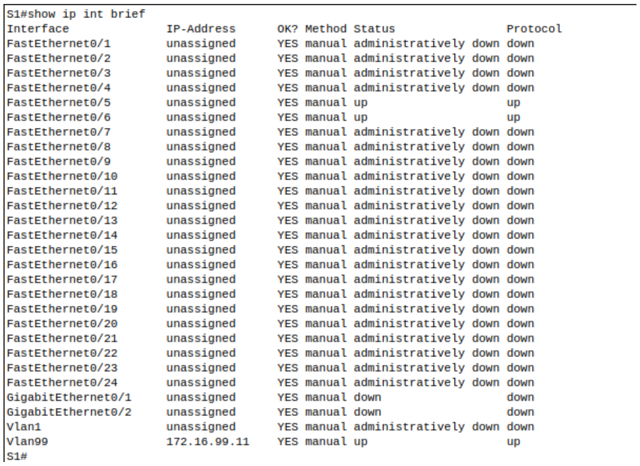
Figure 2: Banner MOTD update

b

The physical ports that are open are Fa0/5 and Fa0/6

c & d)

I ran the commands the output of `show ip int brief` gives us:



```
S1#show ip int 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
FastEthernet0/5        unassigned      YES manual up                    up
FastEthernet0/6        unassigned      YES manual up                    up
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
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual administratively down down
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively 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#
```

Figure 3: Output of show ip int brief

x) Configure and verify port security on S1

a)

The macaddress is 0004.9a08.6602

b)

fa0/5 has a mac address of 0004.9a08.6602 and fa0/6 doesnt show on the table.

c & d)

The port status is `Secure-Up`.

e)

From R1 I pinged PC-A as seen in Fig. 4a.

l)

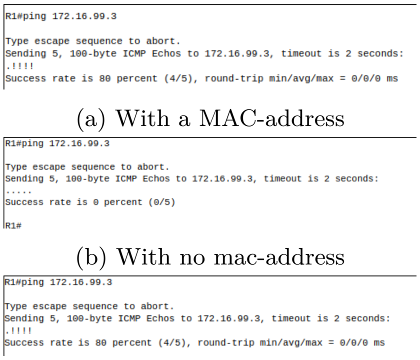
The ping from R1 to PC-A was not successful.

m)

See Fig. 4b for the output of `show int f0/5`.

p)

This time the ping was successful again. See Fig. 4c



```
R1#ping 172.16.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

(a) With a MAC-address

```
R1#ping 172.16.99.3

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

R1#
```

(b) With no mac-address

```
R1#ping 172.16.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

(c) With S1 back on

Figure 4: Ping from R1 to PC-A

Reflection

i) Why would you enable port security on a switch? To prevent unauthorized users to gain access to the LAN.

ii) Why should unused ports on a switch be disabled?

Any enabled port not in use could allow someone to come in and plug into your network and gain access. So, it's best practice to disable any unused ports.