

ASSIGNMENT 1: VLANS AND SECURE SWITCH CONFIGURATION WRITEUP

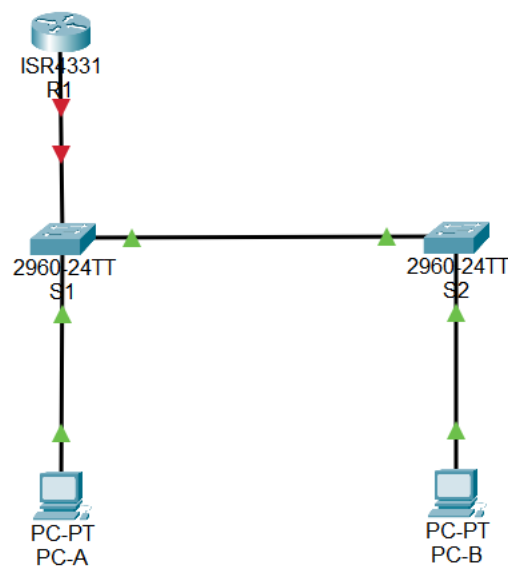
Introduction

In the rapidly evolving world of networking, efficient and secure configuration of network devices is of paramount importance. This assignment aims to provide the learner with skills in network device configuration and various aspects of network security. This assignment is divided into three main parts: Part 1 focuses on configuring the network devices and establishing a solid foundation for the network. Part 2 focuses on the configuration of Virtual LANs (VLANs) on the switches and Part 3 revolves around implementing switch security measures to safeguard the network against potential threats. This involves implementing 802.1Q trunking for efficient VLAN communication.

Part 1: Configure the Network Devices.

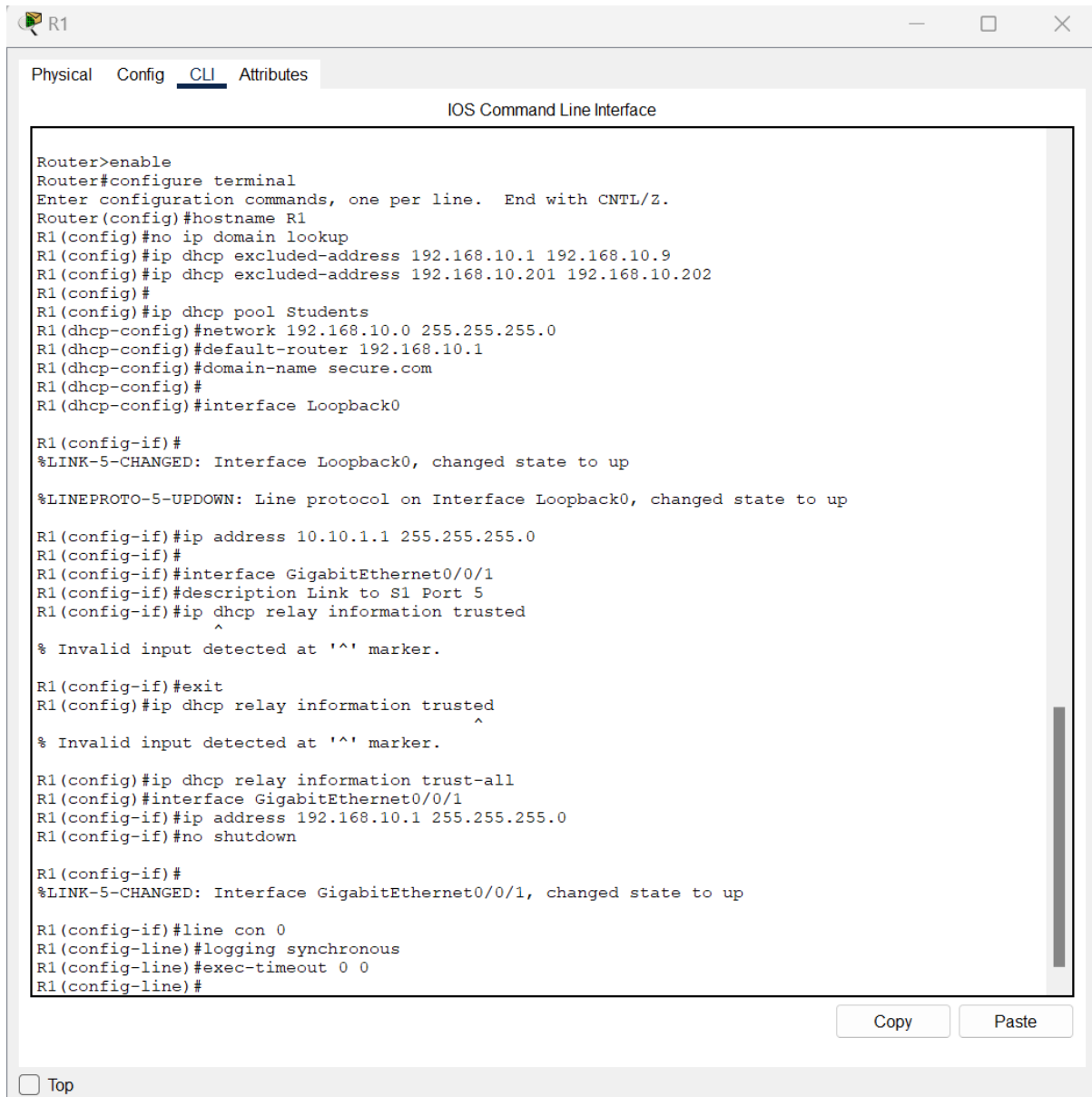
Step 1: Cable the network.

In this step cabling of the network with respect to the topology was done as shown below.



Step 2: Configure R1.

In this step, loaded the following configuration script on R1.



The screenshot shows a window titled 'R1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal shows the following commands and output:

```
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)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#ip dhcp excluded-address 192.168.10.201 192.168.10.202
R1(config)#
R1(config)#ip dhcp pool Students
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#domain-name secure.com
R1(dhcp-config)#
R1(dhcp-config)#interface Loopback0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ip address 10.10.1.1 255.255.255.0
R1(config-if)#
R1(config-if)#interface GigabitEthernet0/0/1
R1(config-if)#description Link to S1 Port 5
R1(config-if)#ip dhcp relay information trusted
R1(config-if)#^
% Invalid input detected at '^' marker.

R1(config-if)#exit
R1(config)#ip dhcp relay information trusted
R1(config)#^
% Invalid input detected at '^' marker.

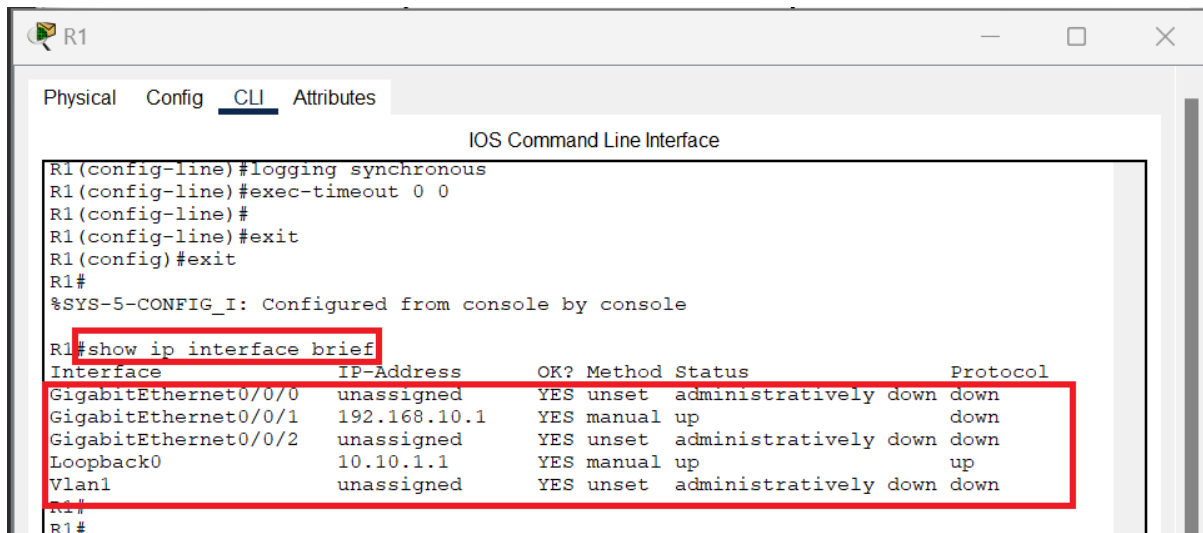
R1(config)#ip dhcp relay information trust-all
R1(config)#interface GigabitEthernet0/0/1
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#
```

At the bottom of the window, there is a 'Top' button and a status bar.

To verify the running-configuration on R1 show ip interface brief command and confirmed the configuration.



The screenshot shows the CLI of router R1. The 'CLI' tab is selected. The command history shows the following sequence of commands and their outputs:

```
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface brief
Interface                IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0/0    unassigned      YES unset    administratively down down
GigabitEthernet0/0/1    192.168.10.1    YES manual   up            down
GigabitEthernet0/0/2    unassigned      YES unset    administratively down down
Loopback0               10.10.1.1       YES manual   up            up
Vlan1                   unassigned      YES unset    administratively down down
```

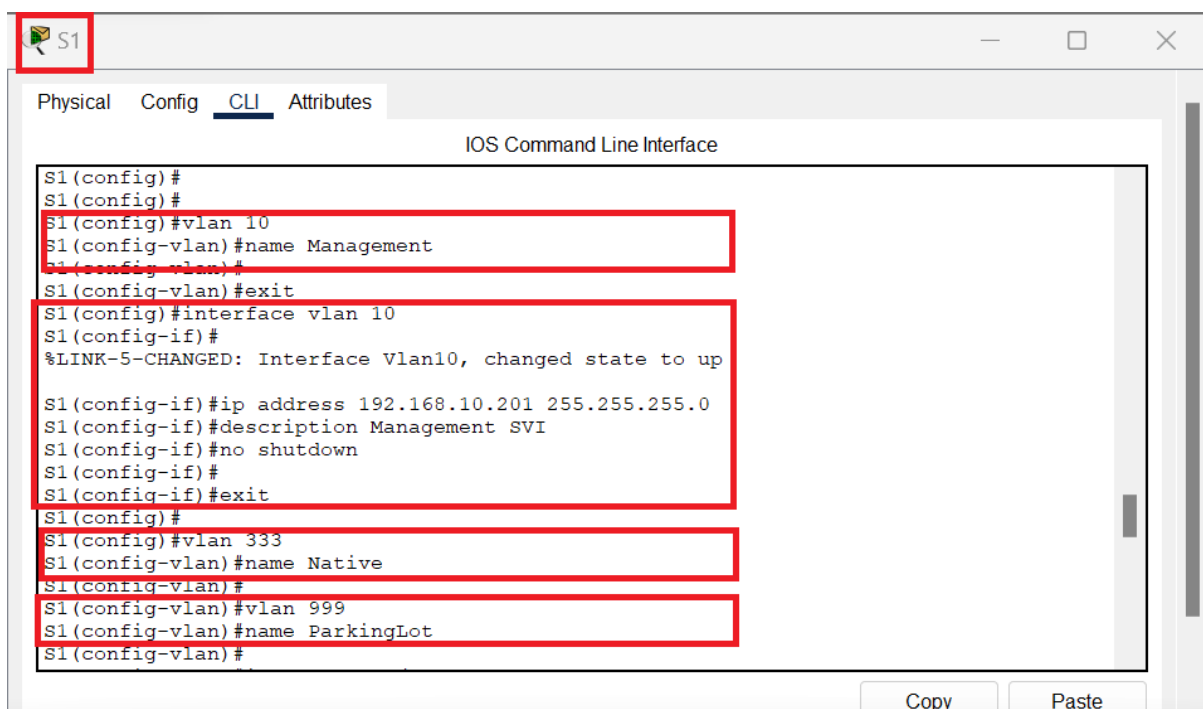
The output of the `show ip interface brief` command is highlighted with a red box.

Step 3: Configure and verify basic switch settings.

In this step, configuration of the hostname for switches S1(hostname S1) and S2 (hostname S2) was done, preventing unwanted DNS lookups on both switches, configuring descriptions for the ports that are in use in S1 and S2 and setting of the default-gateway for the Management VLAN to 192.168.10.1 on both switches was done.

Part 2: Configure VLANs on Switches.

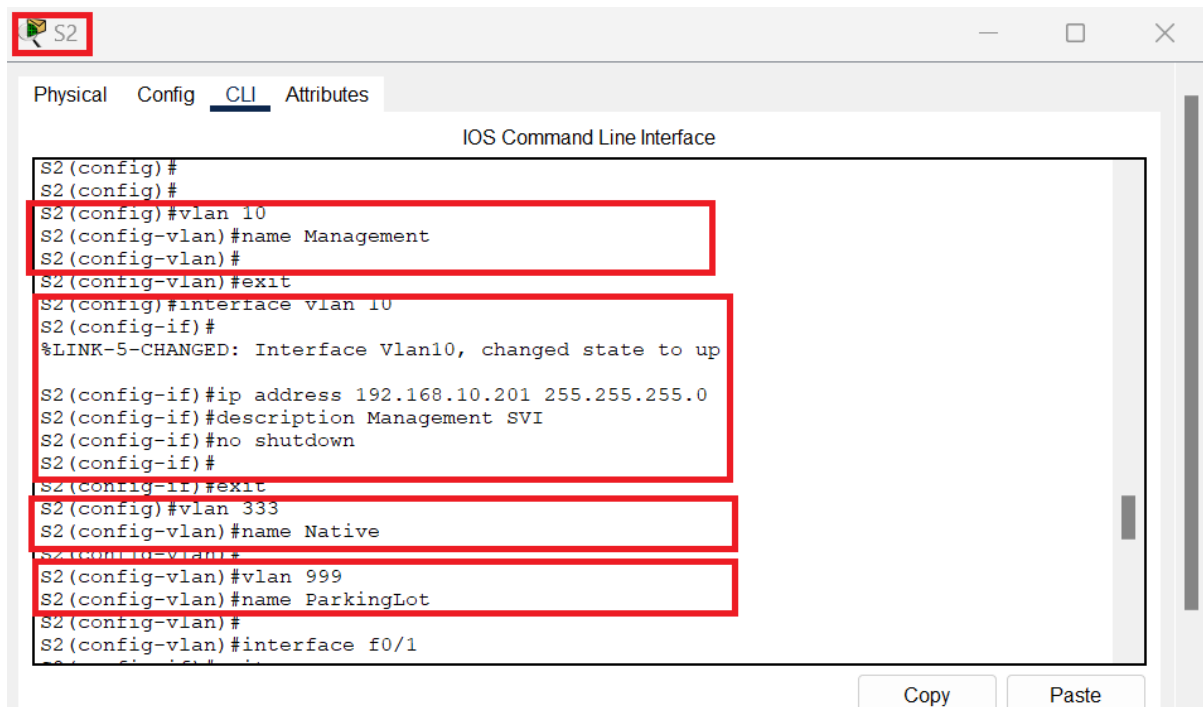
In this section details the process of configuring VLANs on Switches. Firstly, we configured VLAN 10 and named it VLAN Management, we then configured the SVI for VLAN 10, then configured VLAN 333 with its name Native and VLAN 999 with packing Lot for both S1 and S2, which can be shown the below pictures:



The screenshot shows the CLI of switch S1. The 'CLI' tab is selected. The command history shows the following sequence of commands and their outputs:

```
S1(config)#
S1(config)#
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#
S1(config-vlan)#exit
S1(config)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#
S1(config-if)#exit
S1(config)#
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#
```

The commands for configuring VLAN 10, the SVI for VLAN 10, and VLANs 333 and 999 are highlighted with red boxes.

A screenshot of a network switch configuration window titled 'S2'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The main area is labeled 'IOS Command Line Interface' and contains a list of configuration commands. Several lines of commands are highlighted with red rectangular boxes. The commands are: 'S2(config)#', 'S2(config)#', 'S2(config)#vlan 10', 'S2(config-vlan)#name Management', 'S2(config-vlan)#', 'S2(config-vlan)#exit', 'S2(config)#interface vlan 10', 'S2(config-if)#', '%LINK-5-CHANGED: Interface Vlan10, changed state to up', 'S2(config-if)#ip address 192.168.10.201 255.255.255.0', 'S2(config-if)#description Management SVI', 'S2(config-if)#no shutdown', 'S2(config-if)#', 'S2(config-if)#exit', 'S2(config)#vlan 333', 'S2(config-vlan)#name Native', 'S2(config-vlan)#', 'S2(config-vlan)#vlan 999', 'S2(config-vlan)#name ParkingLot', 'S2(config-vlan)#', and 'S2(config-vlan)#interface f0/1'. At the bottom right, there are 'Copy' and 'Paste' buttons.

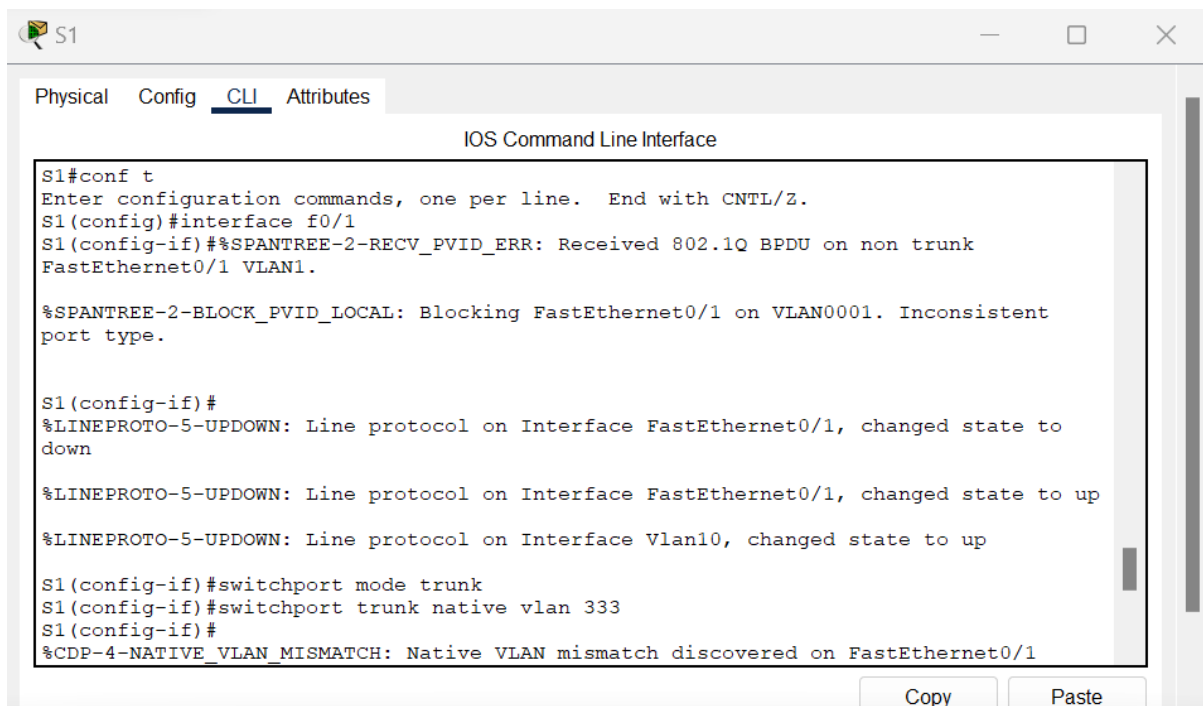
```
S2(config)#
S2(config)#
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#
S2(config-vlan)#exit
S2(config)#interface vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
S2(config-if)#ip address 192.168.10.201 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown
S2(config-if)#
S2(config-if)#exit
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#
S2(config-vlan)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#
S2(config-vlan)#interface f0/1
```

Part 3: Configure Switch Security.

This section presents a step a step process of configuring switch security.

Step 1: Implement 802.1Q trunking.

In this step, configuring trunking on F0/1 to use VLAN 333 as the native VLAN on both switches was done as shown below:

A screenshot of a network switch configuration window titled 'S1'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The main area is labeled 'IOS Command Line Interface' and contains a list of configuration commands. The commands are: 'S1#conf t', 'Enter configuration commands, one per line. End with CNTL/Z.', 'S1(config)#interface f0/1', 'S1(config-if)%%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/1 VLAN1.', '%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent port type.', 'S1(config-if)#', '%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down', '%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up', '%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up', 'S1(config-if)#switchport mode trunk', 'S1(config-if)#switchport trunk native vlan 333', 'S1(config-if)#', and '%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1'. At the bottom right, there are 'Copy' and 'Paste' buttons.

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)%%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk
FastEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent
port type.

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 333
S1(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
```

To verify that trunking is configured on both switches the show interface trunk is used.

The screenshot shows the CLI of switch S1. The output of the `show interface trunk` command is highlighted with a red box. It shows that Fa0/1 is configured as a trunk port with encapsulation 802.1q, status 'trunking', and native VLAN 333. It also lists the allowed VLANs (1-1005) and the active VLANs in the management domain (1, 10, 333, 999).

```
S1#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    333

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,333,999

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,333,999

S1#
```

Then disable DTP negotiation on F0/1 on S1 and S2 and verification using show interface command.

Step 2: Configure access ports.

In this step, On S1, configured F0/5 and F0/6 as access ports that are associated with VLAN 10. And On S2, configure F0/18 as an access port that is associated with VLAN 10 and then we secure and disable unused switchports.

The first screenshot shows the CLI of switch S1. The configuration commands for interfaces f0/5-6 and f0/2-4, f0/7-24, g0/1-2 are highlighted with red boxes. The second screenshot shows the CLI of switch S2. The configuration commands for interface f0/18 and f0/2-17, f0/19-24, g0/1-2 are highlighted with red boxes.

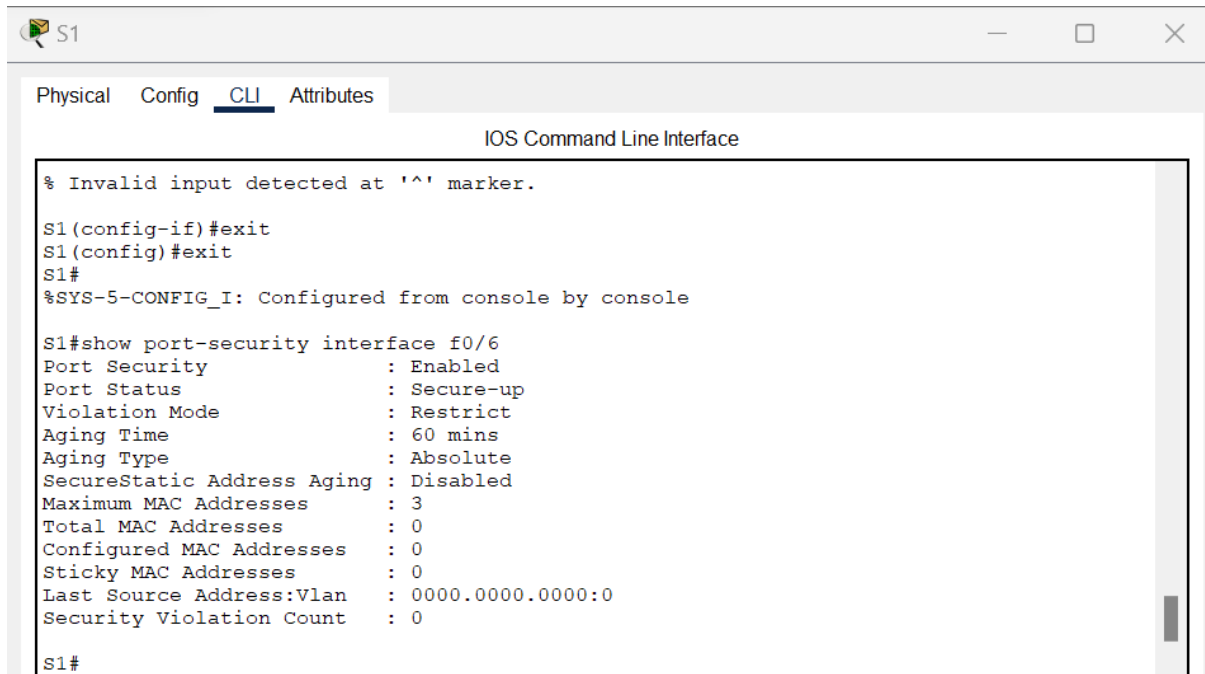
```
S1(config)#interface range f0/5 - 6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#exit
S1(config)#interface range f0/2-4 , f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
```

```
S2(config)#
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#
S2(config-if)#interface range f0/2-17 , f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
```

Step 4: Document and implement port security features.

In this step, one will also configure port security on the two access ports.

On S1, enable port security on F0/6 then issue the show port-security interface f0/6 command to display the default port security settings for interface F0/6.



```
S1
Physical Config CLI Attributes
IOS Command Line Interface

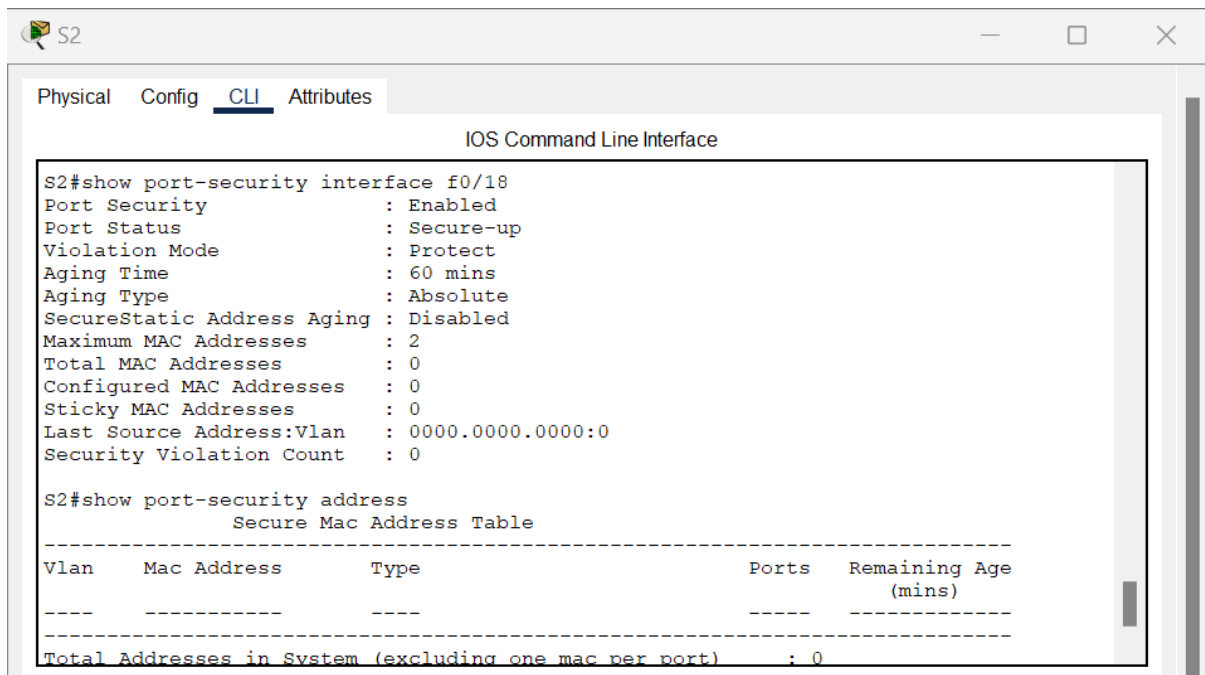
% Invalid input detected at '^' marker.

S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show port-security interface f0/6
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Restrict
Aging Time             : 60 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 3
Total MAC Addresses    : 0
Configured MAC Addresses : 0
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

S1#
```

On S2, enable port security for F0/18., then verify with show port-security interface f0/18 command.



```
S2
Physical Config CLI Attributes
IOS Command Line Interface

S2#show port-security interface f0/18
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Protect
Aging Time             : 60 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 2
Total MAC Addresses    : 0
Configured MAC Addresses : 0
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

S2#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
Total Addresses in System (excluding one mac per port)  : 0
```

Finally, to verify end to end connectivity one should ping from PC-B from PC-A or even the default gateway just as shown below:

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time=1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Questions to answer

1. In reference to Port Security on S2, why is there no timer value for the remaining age in minutes when sticky learning was configured?



This switch does not support the port security aging of sticky secure addresses.

2. In reference to Port Security on S2, if you load the running-config script on S2, why will PC-B on port 18 never get an IP address via DHCP?

Using the show running config. The Port security is set for only two MAC addresses and port 18 has two “sticky” MAC addresses bound to the port. Additionally, the violation is protected, which will never send a console/syslog message or increment the violation counter.

3. In reference to Port Security, what is the difference between the absolute aging type and inactivity aging type?

If the inactivity type is set, then the secure addresses on the port will be removed only if there is no data traffic from the secure source addresses for the specified time period. If the absolute type is set, then all secure addresses on this port age out exactly after the time specified ends.

Conclusion

In conclusion, this assignment has provided a comprehensive exploration of network configuration and security. By accomplishing the outlined objectives, I have gained experience in configuring network devices. The highlight of this assignment lies in Part 3, where I implemented a range of security measures to protect the network from potential threats. By configuring 802.1Q trunking, access ports, and implementing port security features, you have fortified the network's defenses against unauthorized access and devices. Additionally, the implementation of DHCP snooping security, PortFast, and BPDU guard further enhances network stability and mitigates potential vulnerabilities.