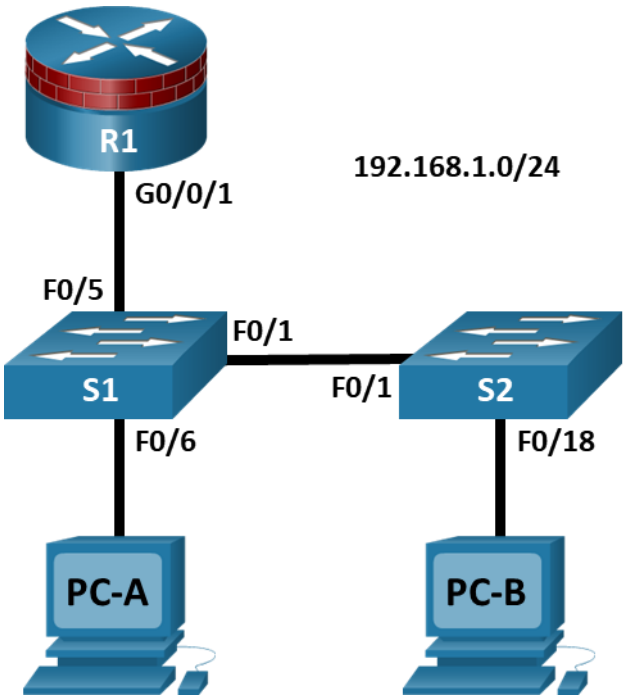
Answers: 14.9.9 Lab - Configure STP Security

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A	N/A
S2	VLAN 1	192.168.1.3	255.255.255.0	N/A	N/A
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.1.11	255.255.255.0	192.168.1.1	S2 F0/18

Objectives

Part 1: Configure Basic Switch Settings

- Build the topology.
- Configure the hostname, IP address, and access passwords.

Part 2: Configure Secure Trunks Ports

- Configure trunk port mode.
- Change the native VLAN for trunk ports.

- Verify trunk configuration.
- Disable trunking.

Part 3: Protect Against STP Attacks

- Enable PortFast and BPDU guard.
- Verify BPDU guard.
- Enable root guard.
- Enable loop guard.

Part 4: Configure Port Security and Disable Unused Ports

- Configure and verify port security.
- Disable unused ports.
- Move ports from default VLAN 1 to alternate VLAN.
- Configure the PVLAN Edge feature on a port.

Background / Scenario

The Layer 2 infrastructure consists mainly of interconnected Ethernet switches. Most end-user devices, such as computers, printers, IP phones, and other hosts, connect to the network via Layer 2 access switches. As a result, switches can present a network security risk. Similar to routers, switches are subject to attack from malicious internal users. The switch Cisco IOS software provides many security features that are specific to switch functions and protocols.

In this lab, you will configure various switch protection measures, including access port security and Spanning Tree Protocol (STP) features, such as BPDU guard and root guard.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.6 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960+ with Cisco IOS Release 15.2(7) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Before you begin, ensure that the routers and the switches have been erased and have no startup configurations.

Required Resources

- 1 Router (Cisco 4221 with Cisco XE Release 16.9.6 universal image or comparable with a Security Technology Package license)
- 2 Switches (Cisco 2960+ with Cisco IOS Release 15.2(7) lanbasek9 image or comparable)
- 2 PCs (Windows OS with a terminal emulation program, such as PuTTY or Tera Term installed)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Switch Settings

In Part 1, you will set up the network topology and configure basic settings, such as the hostnames, IP addresses, and device access passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices, as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for the router and each switch.

Perform all tasks on R1, S1, and S2. The procedure for S1 is shown here as an example.

Configure hostnames, as shown in the topology.

Configure interface IP addresses, as shown in the IP Addressing Table. The following configuration displays the VLAN 1 management interface on S1:

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
```

Prevent the router or switch from attempting to translate incorrectly entered commands by disabling DNS lookup. S1 is shown here as an example.

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

HTTP access to the switch is enabled by default. Prevent HTTP access by disabling the HTTP server and HTTP secure server.

```
S1(config)# no ip http server
S1(config)# no ip http secure-server
```

Note: The switch must have a cryptography IOS image to support the **ip http secure-server** command. HTTP access to the router is disabled by default.

Configure the enable secret password.

```
S1(config)# enable algorithm-type scrypt secret cisco12345
```

Configure console password.

```
S1(config)# line console 0
S1(config-line)# password ciscoconpass
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
S1(config-line)# logging synchronous
```

Step 3: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-B, as shown in the Addressing Table.

Step 4: Verify basic network connectivity.

a. Ping from PC-A and PC-B to the R1 G0/0/1 interface at IP address **192.168.1.1**.

   If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A to PC-B.

   If the pings are unsuccessful, troubleshoot the basic device configurations before continuing.

Step 5: Save the basic configurations for the router and both switches.

Save the running configuration to the startup configuration from the privileged EXEC mode prompt.

```
S1# copy running-config startup-config
```

Part 2: Configure Secure Trunk Ports

In this part, you will configure trunk ports, change the native VLAN for trunk ports, and verify trunk configuration.

Securing trunk ports can help stop VLAN hopping attacks. The best way to prevent a basic VLAN hopping attack is to explicitly disable trunking on all ports except the ports that specifically require trunking. On the required trunking ports, disable DTP (auto trunking) negotiations and manually enable trunking. If no trunking is required on an interface, configure the port as an access port. This disables trunking on the interface.

Note: Tasks should be performed on S1 or S2, as indicated.

Step 1: Configure S1 as the root switch.

For the purposes of this lab, S2 is currently the root bridge. You will configure S1 as the root bridge by changing the bridge ID priority level.

a. From the console on S1, enter global configuration mode.

b. The default priority for S1 and S2 is 32769 (32768 + 1 with System ID Extension). Set S1 priority to **0** so that it becomes the root switch.

```
S1(config)# spanning-tree vlan 1 priority 0
S1(config)# exit
```

Note: You can also use the **spanning-tree vlan 1 root primary** command to make S1 the root switch for VLAN 1.

c. Issue the **show spanning-tree** command to verify that S1 is the root bridge, to see the ports in use, and to see their status.

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001d.4635.0c80
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1      (priority 0 sys-id-ext 1)
              Address     001d.4635.0c80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
```

What is the S1 priority?

Which ports are in use and what is their status?

Step 2: Configure trunk ports on S1 and S2.

a. Configure port F0/1 on S1 as a trunk port.

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

Note: If performing this lab with a 3560 switch, the user must first enter the **switchport trunk encapsulation dot1q** command.

b. Configure port F0/1 on S2 as a trunk port.

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

c. Verify that S1 port F0/1 is in trunking mode with the **show interfaces trunk** command.

```
S1# show interfaces 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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

Step 3: Change the native VLAN for the trunk ports on S1 and S2.

a. Changing the native VLAN for trunk ports to an unused VLAN helps prevent VLAN hopping attacks.

From the output of the **show interfaces trunk** command in the previous step, what is the current native VLAN for the S1 F0/1 trunk interface?

b. Set the native VLAN on the S1 F0/1 trunk interface to an unused VLAN 99.

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

c. The following message should display after a brief period of time:

```
02:16:28: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (99), with S2 FastEthernet0/1 (1).
```

What does the message mean?

d. Set the native VLAN on the S2 F0/1 trunk interface to VLAN 99.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# end
```

Step 4: Prevent the use of DTP on S1 and S2.

Setting the trunk port to **nonegotiate** also helps to mitigate VLAN hopping by turning off the generation of DTP frames.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate

S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

Step 5: Verify the trunking configuration on port F0/1.

```
S1# show interfaces f0/1 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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1

S1# show interfaces 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 (Inactive)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

```
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Step 6: Verify the configuration with the show run command.

Use the **show run** command to display the running configuration, beginning with the first line that has the text string “0/1” in it.

```
S1# show run | begin 0/1
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate

<output omitted>
```

Step 7: Disable trunking on S1 access ports.

a. On S1, configure F0/5, the port to which R1 is connected, as access mode only.

```
S1(config)# interface f0/5
S1(config-if)# switchport mode access
```

b. On S1, configure F0/6, the port to which PC-A is connected, as access mode only.

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

Step 8: Disable trunking on S2 access ports.

On S2, configure F0/18, the port to which PC-B is connected, as access mode only.

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
```

Part 3: Protect Against STP Attacks

Network attackers hope to spoof their system, or a rogue switch that they add to the network, as the root bridge in the topology by manipulating the STP root bridge parameters. If a port that is configured with PortFast receives a BPDU, STP can put the port into the blocking state by using a feature called BPDU guard.

The topology has only two switches and no redundant paths, but STP is still active. In this part, you will enable switch security features that can help reduce the possibility of an attacker manipulating switches via STP-related methods.

Step 1: Enable portfast.

PortFast is configured on access ports that connect to a single workstation or server, which enables them to become active more quickly.

a. Enable PortFast on the S1 F0/5 access port.

```
S1(config)# interface f0/5
S1(config-if)# spanning-tree portfast
```

```
%Warning: portfast should only be enabled on ports connected to a single host.
Connecting hubs, concentrators, switches, bridges, etc... to this interface when
portfast is enabled, can cause temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
 have effect when the interface is in a non-trunking mode.
```

b. Enable PortFast on the S1 F0/6 access port.

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
```

c. Enable PortFast on the S2 F0/18 access ports.

```
S2(config)# interface f0/18
S2(config-if)# spanning-tree portfast
```

Step 2: Enable BPDU guard.

BPDU guard is a feature that can help prevent rogue switches and spoofing on access ports.

a. Enable BPDU guard on the switch port F0/6.

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18
S2(config-if)# spanning-tree bpduguard enable
```

Note: PortFast and BPDU guard can also be enabled globally with the **spanning-tree portfast default** and **spanning-tree portfast bpduguard** commands in global configuration mode.

Note: BPDU guard can be enabled on all access ports that have PortFast enabled. These ports should never receive a BPDU. BPDU guard is best deployed on user-facing ports to prevent rogue switch network extensions by an attacker. If a port is enabled with BPDU guard and receives a BPDU, it is disabled and must be manually re-enabled. An **err-disable timeout** can be configured on the port so that it can recover automatically after a specified time period.

b. Verify that BPDU guard is configured by using the **show spanning-tree interface f0/6 detail** command on S1.

```
S1# show spanning-tree interface f0/6 detail

Port 6 (FastEthernet0/6) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.6.
   Designated root has priority 1, address 001d.4635.0c80
   Designated bridge has priority 1, address 001d.4635.0c80
   Designated port id is 128.6, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 3349, received 0
```

Step 3: Enable root guard.

Root guard is another option to help prevent rogue switches and spoofing. Root guard can be enabled on all ports on a switch that are not root ports. It is normally enabled only on ports connecting to edge switches where a superior BPDU should never be received. Each switch should have only one root port, which is the best path to the root switch.

a. The following command configures root guard on S2 interface G0/1. Normally, this is done if another switch is attached to this port. Root guard is best deployed on ports that connect to switches that should not be the root bridge. In the lab topology, S1 F0/1 would be the most logical candidate for root guard. However, S2 G0/1 is shown here as an example, as Gigabit ports are more commonly used for inter-switch connections.

```
S2(config)# interface g0/1
S2(config-if)# spanning-tree guard root
```

b. Issue the **show run | begin Gig** command to verify that root guard is configured.

```
S2# show run | begin Gig
interface GigabitEthernet0/1
 spanning-tree guard root
```

Note: The S2 Gi0/1 port is not currently up, so it is not participating in STP. Otherwise, you could use the **show spanning-tree interface Gi0/1 detail** command.

Note: The expression in the command **show run | begin** is case-sensitive.

c. If a port that is enabled with BPDU guard receives a superior BPDU, it enters a root-inconsistent state. Use the **show spanning-tree inconsistentports** command to determine if there are any ports currently receiving superior BPDUs that should not be.

```
S2# show spanning-tree inconsistentports

Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
Number of inconsistent ports (segments) in the system : 0
```

Note: Root guard allows a connected switch to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. The port returns to the forwarding state if the superior BPDUs stop.

Step 4: Enable loop guard.

The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. Having all ports in forwarding state will result in forwarding loops. If a port enabled with loopguard stops hearing BPDUs from the designated port on the segment, it goes into the loop inconsistent state instead of transitioning into forwarding state. Loop inconsistent is basically blocking, and no traffic is forwarded. When the port detects BPDUs again it automatically recovers by moving back into blocking state.

a. Loop guard should be applied to non-designated ports. Therefore, the global command can be configured on non-root switches.

```
S2(config)# spanning-tree loopguard default
```

b. Verify Loopguard configuration.

```
S2# show spanning-tree summary
Switch is in pvst mode
```

```
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        0          3          3
---------------------- -------- --------- -------- ---------- ---------
```

Part 4: Configure Port Security and Disable Unused Ports

Switches can be subject to a CAM table, also known as a MAC address table, overflow, MAC spoofing attacks, and unauthorized connections to switch ports. In this task, you will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

Step 1: Record the R1 G0/0/1 MAC address.

From the R1 CLI, use the **show interface** command and record the MAC address of the interface.

```
R1# show interfaces g0/0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e1 (bia fc99.4775.c3e1)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
<Output Omitted>
```

What is the MAC address of the R1 G0/0/1 interface?

Step 2: Configure basic port security.

This procedure should be performed on all access ports that are in use. S1 port F0/5 is shown here as an example.

a. From the S1 CLI, enter interface configuration mode for the port that connects to the router (Fast Ethernet 0/5).

```
S1(config)# interface f0/5
```

b. Shut down the switch port.

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

c. Enable port security on the port.

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

Note: A switch port must be configured as an access port to enable port security.

Note: Entering just the **switchport port-security** command sets the maximum MAC addresses to **1** and the violation action to **shutdown**. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

d. Configure a static entry for the MAC address of R1 G0/0/1 interface recorded in Step 1.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

Note: *xxxx.xxxx.xxxx* is the actual MAC address of the router G0/0/1 interface.

Note: You can also use the **switchport port-security mac-address sticky** command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

e. Enable the switch port.

```
S1(config-if)# no shutdown
```

Step 3: Verify port security on S1 F0/5.

a. On S1, issue the **show port-security** command to verify that port security has been configured on S1 F0/5.

```
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   : 0000.0000.0000:0
Security Violation Count   : 0
```

What is the Security Violation Count?

What is the status of the F0/5 port?

What is the Last Source Address and VLAN?

b. From the R1 CLI, ping PC-A to verify connectivity. This also ensures that the R1 G0/0/1 MAC address is learned by the switch.

```
R1# ping 192.168.1.10
```

c. Now, violate security by changing the MAC address on the router interface. Enter interface configuration mode for the Fast Ethernet 0/1. Configure a MAC address for the interface on the interface, using **aaaa.bbbb.cccc** as the address.

```
R1(config)# interface g0/0/1
R1(config-if)# mac-address aaaa.bbbb.cccc
R1(config-if)# end
```

Note: You can also change the PC MAC address attached to S1 F0/6 and achieve similar results to those shown here.

From the R1 CLI, ping PC-A. Was the ping successful? Explain.

d. On S1 console, observe the messages when port F0/5 detects the violating MAC address.

```
*Jan 14 01:34:39.750: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/5,
putting Fa0/5 in err-disable state
*Jan 14 01:34:39.750: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address aaaa.bbbb.cccc on port FastEthernet0/5.
*Jan 14 01:34:40.756: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5,
changed state to down
*Jan 14 01:34:41.755: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to down
```

e. On the switch, use the **show port-security** commands to verify that port security has been violated.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
      Fa0/5            1           1                1         Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

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:1
Security Violation Count   : 1

S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    fc99.4775.c3e1    SecureConfigured              Fa0/5        -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

f. Remove the hard-coded MAC address from the router and re-enable the G0/0/1 interface.

```
R1(config)# interface g0/0/1
R1(config-if)# no mac-address aaaa.bbbb.cccc
```

Note: This will restore the original GigabitEthernet interface MAC address.

From R1, try to ping the PC-A again at 192.168.1.10. Was the ping successful? Explain.

Step 4: Clear the S1 F0/5 error disabled status.

a. From the S1 console, clear the error and re-enable the port using the commands shown in the example. This will change the port status from Secure-shutdown to Secure-up.

```
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Note: This assumes the device/interface with the violating MAC address has been removed and replaced with the original device/interface configuration.

b. From R1, ping PC-A again. You should be successful this time.

```
R1# ping 192.168.1.10
```

Step 5: Remove basic port security on S1 F0/5.

From the S1 console, remove port security on F0/5. This procedure can also be used to re-enable the port, but **port security** commands must be reconfigured.

```
S1(config)# interface f0/5
S1(config-if)# no switchport port-security
S1(config-if)# no switchport port-security mac-address fc99.4775.c3e1
```

You can also use the following commands to reset the interface to its default settings:

```
S1(config)# default interface f0/5
S1(config)# interface f0/5
```

Note: This **default interface** command also requires that you reconfigure the port as an access port to re-enable the security commands.

Step 6: (Optional) Configure port security for VoIP.

This example shows a typical port security configuration for a voice port. Three MAC addresses are allowed and should be learned dynamically. One MAC address is for the IP phone, one is for the switch, and one is for the PC connected to the IP phone. Violations of this policy result in the port being shut down. The aging timeout for the learned MAC addresses is set to two hours.

The following example displays S2 port F0/18:

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security maximum 3
S2(config-if)# switchport port-security violation shutdown
S2(config-if)# switchport port-security aging time 120
```

Step 7: Disable unused ports on S1 and S2.

As a further security measure, disable ports that are not being used on the switch.

a. Ports F0/1, F0/5, and F0/6 are used on S1. The remaining Fast Ethernet ports and the two Gigabit Ethernet ports will be shut down.

```
S1(config)# interface range f0/2 - 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
```

b. Ports F0/1 and F0/18 are used on S2. The remaining Fast Ethernet ports and the Gigabit Ethernet ports will be shut down.

```
S2(config)# interface range f0/2 – 17, f0/19 – 24, g0/1 - 2
S2(config-if-range)# shutdown
```

Step 8: Move active ports to a VLAN other than the default VLAN 1.

As a further security measure, you can move all active end-user ports and router ports to a VLAN other than the default VLAN 1 on both switches.

a. Configure a new VLAN for users on each switch using the following commands:

```
S1(config)# vlan 20
S1(config-vlan)# name Users

S2(config)# vlan 20
S2(config-vlan)# name Users
```

b. Add the current active access (non-trunk) ports to the new VLAN.

```
S1(config)# interface f0/6
S1(config-if-range)# switchport access vlan 20

S2(config)# interface f0/18
S2(config-if)# switchport access vlan 20
```

Note: This will prevent communication between end-user hosts and the management VLAN IP address of the switch, which is currently VLAN 1. The switch can still be accessed and configured using the console connection.

Note: To provide SSH access to the switch, a specific port can be designated as the management port and added to VLAN 1 with a specific management workstation attached. A more elaborate solution is to create a new VLAN for switch management (or use the existing native trunk VLAN 99), and configure a separate subnet for the management and user VLANs.

Step 9: Configure a port with the PVLAN Edge feature.

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of the Private VLAN (PVLAN) Edge feature, also known as protected ports, ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch. The PVLAN Edge feature can only be implemented for ports on the same switch and is locally significant.

For example, to prevent traffic between host PC-A on S1 (port F0/6) and a host on another S1 port (e.g. port F0/7, which was previously shut down), you could use the **switchport protected** command to activate the PVLAN Edge feature on these two ports. Use the **no switchport protected** interface configuration command to disable protected port.

a. Configure the PVLAN Edge feature in interface configuration mode using the following commands:

```
S1(config)# interface f0/6
S1(config-if)# switchport protected
S1(config-if)# interface f0/7
S1(config-if)# switchport protected
S1(config-if)# no shut
S1(config-if)# end
```

b. Verify that the PVLAN Edge Feature (protected port) is enabled on F0/6.

```
S1# show interfaces f0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 20 (Users)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
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 Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

c. Deactivate protected port on interfaces F0/6 and F0/7 using the following commands:

```
S1(config)# interface range f0/6 - 7
S1(config-if-range)# no switchport protected
```

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
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)

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
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)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.