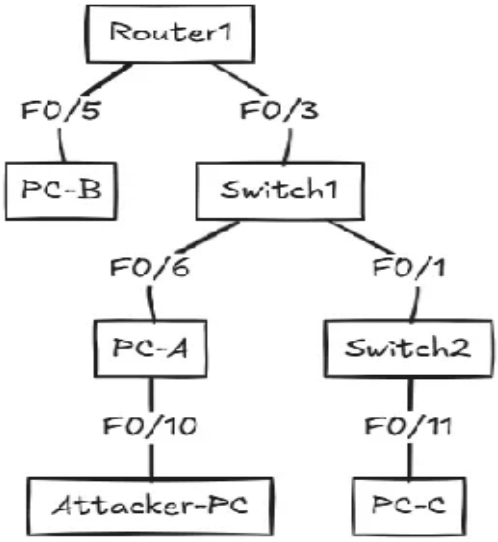
Lab - Comprehensive Layer 2 Security Configuration

Port Security, VLAN Security, DHCP Snooping, DAI, IP Source Guard, and STP Protection

Topology

Network Diagram:



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Port
R1	G0/0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/5
PC-A	NIC	DHCP	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	DHCP	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	DHCP	255.255.255.0	192.168.1.1	S2 F0/11
Attacker-PC	NIC	DHCP/Static	255.255.255.0	192.168.1.1	S1 F0/10

VLAN Configuration

VLAN ID	VLAN Name	Ports
1	default	Management (no access ports)
10	STUDENT	S1: F0/3, F0/6, F0/10; S2: F0/11
99	MANAGEMENT	S1: VLAN 99; S2: VLAN 99
999	PARKING_LOT	All unused ports

Objectives

- Part 1: Configure Basic Device Settings and Connectivity
- Part 2: Configure Port Security
- Part 3: Configure VLAN Security (VLAN Hopping Mitigation)
- Part 4: Configure DHCP Snooping
- Part 5: Configure Dynamic ARP Inspection (DAI)
- Part 6: Configure IP Source Guard
- Part 7: Configure Spanning Tree Protocol Security

Background / Scenario

Layer 2 attacks are often the first step in network compromise. Attackers can exploit vulnerabilities in MAC address handling, VLAN configurations, DHCP services, ARP protocols, and spanning tree to gain unauthorized access or disrupt network operations. This lab demonstrates how to configure multiple Cisco IOS security features to protect against common Layer 2 attacks.

Required Resources

- 2 Cisco Switches (2960 or comparable with IOS 15.x or later)
- 1 Cisco Router (with IOS 15.x or later)
- 4 PCs (Windows OS)
- Console cables to configure Cisco networking devices
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Basic Device Settings and Connectivity

Step 1: Cable the network

Cable the network as shown in the topology diagram.

Step 2: Configure basic settings for S1 and S2

a. Console into S1 and enable privileged EXEC mode.

b. Enter global configuration mode and configure the hostname.

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

c. Disable DNS lookup.

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

d. Configure the enable secret password.

```
S1(config)# enable secret class12345
```

e. Configure console password and enable login.

```
S1(config)# line console 0
S1(config-line)# password cisco12345
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit
```

f. Configure VTY lines for remote access.

```
S1(config)# line vty 0 15
S1(config-line)# password cisco12345
S1(config-line)# login
S1(config-line)# transport input telnet ssh
S1(config-line)# exit
```

g. Configure a message of the day banner.

```
S1(config)# banner motd #Unauthorized Access is Prohibited!#
```

h. Repeat Steps 2a-2g for S2.

Step 3: Configure VLANs on S1 and S2

a. Create VLANs on S1.

```
S1(config)# vlan 10
S1(config-vlan)# name STUDENT
S1(config-vlan)# exit
S1(config)# vlan 99
S1(config-vlan)# name MANAGEMENT
S1(config-vlan)# exit
S1(config)# vlan 999
S1(config-vlan)# name PARKING_LOT
S1(config-vlan)# exit
```

b. Assign access ports to VLANs on S1.

```
S1(config)# interface f0/3
S1(config-if)# description PC-B Access Port
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
S1(config)# interface f0/6
S1(config-if)# description PC-A Access Port
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
S1(config)# interface f0/10
S1(config-if)# description Attacker-PC Access Port
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
```

c. Configure management VLAN interface on S1.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 192.168.99.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.99.1
```

d. Repeat Steps 3a-3c for S2.

Step 4: Configure trunk links between S1 and S2

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

```
S1(config)# interface f0/1
S1(config-if)# description Trunk Link to S2
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 10,99
S1(config-if)# exit
```

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

```
S2(config)# interface f0/1
S2(config-if)# description Trunk Link to S1
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk allowed vlan 10,99
S2(config-if)# exit
```

Note: We will secure these trunk links further in Part 3.

Step 5: Configure R1 router interface and DHCP service

a. Console into R1 and configure the hostname.

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config)#
```

b. Disable DNS lookup.

```
R1(config)# no ip domain-lookup
```

c. Configure the GigabitEthernet 0/0/0 interface.

```
R1(config)# interface g0/0/0
R1(config-if)# description Gateway for VLAN 10
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

d. Configure DHCP pool for VLAN 10 (STUDENT network).

```
R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
R1(config)# ip dhcp pool STUDENT_POOL
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.1.1
R1(dhcp-config)# dns-server 8.8.8.8
R1(dhcp-config)# lease 0 8
```

```
R1(dhcp-config)# exit
```

Note: The excluded address range reserves 192.168.1.1 through 192.168.1.10 for static assignment. The lease time is set to 8 hours.

Step 6: Configure PC hosts to use DHCP

Configure PC-A, PC-B, PC-C, and Attacker-PC to obtain IP addresses automatically via DHCP.

Windows: Control Panel → Network and Sharing → Adapter Settings → Properties → IPv4 → Obtain an IP address automatically

Step 7: Verify connectivity

a. Verify that all PCs have obtained IP addresses from R1's DHCP server.

From PC-A command prompt:

```
C:\> ipconfig /all
```

Look for IP address in the 192.168.1.11-192.168.1.254 range.

b. Verify DHCP leases on R1.

```
R1# show ip dhcp binding

IP address Client-ID/ Lease expiration Type
Hardware address
192.168.1.11 0100.5056.be6c.89 Oct 27 2025 07:30 AM Automatic
192.168.1.12 0100.5056.be7d.2a Oct 27 2025 07:31 AM Automatic
```

c. Ping from PC-A to the gateway (R1).

```
C:\> ping 192.168.1.1
```

d. Ping from PC-A to PC-C.

If pings are not successful, troubleshoot basic connectivity before continuing.

Part 2: Configure Port Security

Port security helps prevent MAC address table overflow attacks and restricts which devices can connect to switch ports.

Step 1: Enable port security on PC-A's access port (S1 F0/6)

a. Verify the interface is in access mode.

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

b. Enable port security on the interface.

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

c. Set the maximum number of allowed MAC addresses to 1.

```
S1(config-if)# switchport port-security maximum 1
```

d. Configure the violation mode to shutdown.

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

e. Configure sticky MAC address learning.

```
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# exit
```

Step 2: Verify port security configuration on F0/6

a. Use the show port-security interface command.

```
S1# show port-security interface f0/6

Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Sticky MAC Addresses : 1
```

b. Verify that the sticky MAC address has been added to the running configuration.

```
S1# show run interface f0/6
```

Look for the line:

```
switchport port-security mac-address sticky xxxx.xxxx.xxxx
```

Step 3: Configure port security with a static MAC address on F0/3 (PC-B)

a. First, determine PC-B's MAC address.

From PC-B:

```
C:\> ipconfig /all
```

Note the Physical Address.

b. Configure port security with a static MAC address.

```
S1(config)# interface f0/3
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 1
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# exit
```

Note: Replace xxxx.xxxx.xxxx with PC-B's actual MAC address in format 0050.56be.6c89

Step 4: Configure port security with restrict violation mode on F0/10

a. Configure port security with violation mode set to restrict.

```
S1(config)# interface f0/10
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 2
S1(config-if)# switchport port-security violation restrict
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# exit
```

Note: The restrict mode will drop packets from violating MAC addresses but will not shut down the port. Instead, it generates a syslog message and increments the violation counter.

Step 5: Configure port security aging on F0/11 (PC-C on S2)

Port security aging allows secure MAC addresses to age out after a specified time period.

```
S2(config)# interface f0/11
S2(config-if)# switchport mode access
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security maximum 1
S2(config-if)# switchport port-security violation shutdown
S2(config-if)# switchport port-security mac-address sticky
S2(config-if)# switchport port-security aging time 10
S2(config-if)# switchport port-security aging type inactivity
```

```
S2(config-if)# exit
```

Note: This configures the secure MAC address to age out after 10 minutes of inactivity.

Step 6: View all port security configurations

a. View port security settings for all interfaces.

```
S1# show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
---------------------------------------------------------------------
Fa0/3 1 1 0 Shutdown
Fa0/6 1 1 0 Shutdown
Fa0/10 2 1 0 Restrict
```

b. View detailed port security address table.

```
S1# show port-security address
```

Step 7: Test port security - Trigger a violation

a. On Attacker-PC, change the MAC address or connect a second device.

b. Try to obtain a new IP address or ping the gateway.

```
C:\> ipconfig /release
C:\> ipconfig /renew
```

c. Check the port status on S1.

```
S1# show port-security interface f0/10
```

For 'restrict' mode, the violation counter will increment but the port stays up.

Step 8: Recover from error-disabled state

a. If a port is in error-disabled state due to port security violation, check the status.

```
S1# show interface f0/6 status
```

b. To recover the port, manually shut down and re-enable the interface.

```
S1(config)# interface f0/6
S1(config-if)# shutdown
S1(config-if)# no shutdown
S1(config-if)# exit
```

c. Verify the port has recovered.

```
S1# show interface f0/6 status
```

Part 3: Configure VLAN Security (VLAN Hopping Mitigation)

VLAN hopping attacks exploit Dynamic Trunking Protocol (DTP) and the native VLAN to gain unauthorized access to other VLANs. Securing trunk ports and disabling DTP prevents these attacks.

Step 1: Disable DTP and secure the trunk link between S1 and S2

a. On S1, reconfigure the trunk link on F0/1 with DTP disabled.

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

Note: The switchport nonegotiate command disables DTP, preventing the switch from automatically negotiating trunk status.

b. Repeat on S2.

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

c. Verify the trunk configuration.

```
S1# show interfaces f0/1 switchport
```

Look for:

```
Administrative Mode: trunk
Operational Mode: trunk
Negotiation of Trunking: Off
```

Step 2: Change the native VLAN on trunk ports

The native VLAN carries untagged traffic on trunk links. Using the default native VLAN (VLAN 1) is a security risk. Change it to an unused VLAN.

a. Change the native VLAN to VLAN 999 on S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 999
S1(config-if)# exit
```

b. Change the native VLAN to VLAN 999 on S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 999
S2(config-if)# exit
```

Note: You may see a message about native VLAN mismatch if you configure only one side. Both trunk ends must use the same native VLAN.

c. Verify the native VLAN change.

```
S1# show interfaces f0/1 switchport
```

Look for:

```
Trunking Native Mode VLAN: 999 (PARKING_LOT)
```

Step 3: Disable and secure unused ports

Unused switch ports should be disabled and placed in an unused VLAN to prevent unauthorized access.

a. On S1, disable unused ports (for this lab, assume F0/2, F0/4, F0/7-F0/24 and G0/1-G0/2 are unused).

```
S1(config)# interface range f0/2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)# description Unused Ports - Security Disabled
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown
S1(config-if-range)# exit
```

b. Repeat for unused ports on S2 (adjust port ranges as needed).

```
S2(config)# interface range f0/2-10, f0/12-24, g0/1-2
S2(config-if-range)# description Unused Ports - Security Disabled
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown
S2(config-if-range)# exit
```

c. Verify unused ports are disabled.

```
S1# show ip interface brief
```

Step 4: Configure Protected Ports (PVLAN Edge)

Protected ports (also called Private VLAN Edge) prevent traffic from being forwarded between protected ports on the same switch. This isolates devices on access ports from each other while still allowing them to communicate with the gateway.

a. Configure PC-A and PC-B ports as protected ports on S1.

```
S1(config)# interface f0/6
S1(config-if)# switchport protected
S1(config-if)# exit
S1(config)# interface f0/3
S1(config-if)# switchport protected
S1(config-if)# exit
```

b. Verify protected port configuration.

```
S1# show interfaces f0/6 switchport
```

Look for:

```
Protected: true
```

c. Test protected port functionality by pinging from PC-A to PC-B.

From PC-A:

```
C:\> ping [PC-B IP address]
```

The ping should fail because both ports are protected.

d. Verify that PC-A can still reach the gateway and devices on other switches.

From PC-A:

```
C:\> ping 192.168.1.1
C:\> ping [PC-C IP address]
```

These pings should succeed.

Part 4: Configure DHCP Snooping

DHCP snooping protects against DHCP starvation and rogue DHCP server attacks by validating DHCP messages and building a binding table of legitimate IP-to-MAC mappings.

Step 1: Enable DHCP snooping globally on S1 and S2

a. Enable DHCP snooping on S1.

```
S1(config)# ip dhcp snooping
```

b. Enable DHCP snooping for specific VLANs.

```
S1(config)# ip dhcp snooping vlan 10
```

c. Repeat on S2.

```
S2(config)# ip dhcp snooping
S2(config)# ip dhcp snooping vlan 10
```

Step 2: Configure trusted ports

Only ports connected to legitimate DHCP servers or upstream switches should be trusted.

a. On S1, trust the port connected to the router (F0/5) and the trunk port (F0/1).

```
S1(config)# interface f0/5
S1(config-if)# description Router Connection - DHCP Server
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface f0/1
S1(config-if)# description Trunk to S2
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
```

b. On S2, trust the trunk port connected to S1.

```
S2(config)# interface f0/1
S2(config-if)# description Trunk to S1
S2(config-if)# ip dhcp snooping trust
S2(config-if)# exit
```

Note: Access ports connected to end devices should NOT be trusted.

Step 3: Configure DHCP snooping rate limiting

Rate limiting prevents DHCP starvation attacks by limiting the number of DHCP discovery messages per second on untrusted ports.

a. Configure rate limiting on untrusted access ports on S1.

```
S1(config)# interface f0/3
S1(config-if)# ip dhcp snooping limit rate 10
S1(config-if)# exit
S1(config)# interface f0/6
S1(config-if)# ip dhcp snooping limit rate 10
S1(config-if)# exit
S1(config)# interface f0/10
S1(config-if)# ip dhcp snooping limit rate 10
S1(config-if)# exit
```

Note: The rate limit of 10 allows up to 10 DHCP packets per second on each interface.

b. Configure rate limiting on S2 access ports.

```
S2(config)# interface f0/11
S2(config-if)# ip dhcp snooping limit rate 10
S2(config-if)# exit
```

Step 4: Verify DHCP snooping configuration

a. Verify DHCP snooping is enabled.

```
S1# show ip dhcp snooping

Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
```

b. Check which interfaces are trusted.

```
S1# show ip dhcp snooping

Interface Trusted Rate limit (pps)
----------------------- ------- ----------------
FastEthernet0/1 yes unlimited
FastEthernet0/3 no 10
FastEthernet0/5 yes unlimited
FastEthernet0/6 no 10
FastEthernet0/10 no 10
```

Step 5: View the DHCP snooping binding table

a. Release and renew IP addresses on PC-A.

From PC-A:

```
C:\> ipconfig /release
C:\> ipconfig /renew
```

b. View the DHCP snooping binding database on S1.

```
S1# show ip dhcp snooping binding

MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------- ---- -----------------
00:50:56:BE:6C:89 192.168.1.11 28656 dhcp-snooping 10 FastEthernet0/3
00:50:56:BE:7D:2A 192.168.1.12 28689 dhcp-snooping 10 FastEthernet0/6
```

Note: This binding table will be used by DAI and IP Source Guard in the following parts.

Step 6: Test DHCP snooping against a rogue DHCP server

a. On Attacker-PC, attempt to run a rogue DHCP server (requires admin privileges and DHCP server software).

b. Try to configure the rogue DHCP server to offer IP addresses.

c. From PC-B, attempt to obtain an IP address.

```
C:\> ipconfig /release
```

```
C:\> ipconfig /renew
```

d. Check for DHCP snooping violations on S1.

```
S1# show ip dhcp snooping
```

The attack should be blocked because F0/10 is not a trusted interface, and DHCP offer/ack messages from untrusted ports are dropped.

Part 5: Configure Dynamic ARP Inspection (DAI)

DAI protects against ARP spoofing attacks by validating ARP packets against the DHCP snooping binding table.

Step 1: Enable DAI on VLANs

a. Enable DAI for VLAN 10 on S1.

```
S1(config)# ip arp inspection vlan 10
```

b. Enable DAI for VLAN 10 on S2.

```
S2(config)# ip arp inspection vlan 10
```

Note: You will see log messages as DAI begins inspecting ARP packets.

Step 2: Configure DAI trusted interfaces

Interfaces connected to other switches or routers should be trusted to prevent legitimate ARP traffic from being dropped.

a. On S1, trust the uplink to S2 and the router.

```
S1(config)# interface f0/1
S1(config-if)# ip arp inspection trust
S1(config-if)# exit
S1(config)# interface f0/5
S1(config-if)# description Router Connection
S1(config-if)# ip arp inspection trust
S1(config-if)# exit
```

b. On S2, trust the trunk port to S1.

```
S2(config)# interface f0/1
S2(config-if)# ip arp inspection trust
S2(config-if)# exit
```

Note: Access ports connected to end devices should remain untrusted.

Step 3: Configure DAI validation checks

DAI can validate source MAC, destination MAC, and IP addresses in ARP packets.

a. Configure all three validation checks on S1.

```
S1(config)# ip arp inspection validate src-mac dst-mac ip
```

Note: This command enables validation of:

• src-mac: source MAC in Ethernet header matches sender MAC in ARP body

• dst-mac: destination MAC in Ethernet header matches target MAC in ARP body

• ip: sender and target IP addresses are valid

b. Repeat on S2.

```
S2(config)# ip arp inspection validate src-mac dst-mac ip
```

Step 4: Verify DAI configuration

a. Check DAI status on S1.

```
S1# show ip arp inspection

Source Mac Validation : Enabled
Destination Mac Validation : Enabled
IP Address Validation : Enabled
```

b. View DAI statistics.

```
S1# show ip arp inspection statistics
```

c. View DAI trust configuration on interfaces.

```
S1# show ip arp inspection interfaces
```

Step 5: Test DAI against ARP spoofing

a. On Attacker-PC, attempt to perform an ARP spoofing attack using tools like arpspoof, Cain & Abel, or Ettercap.

b. Monitor DAI on S1 for dropped packets.

```
S1# show ip arp inspection statistics vlan 10
```

The Dropped and DHCP Drops counters should increment as malicious ARP packets are blocked.

c. Verify that legitimate ARP traffic still functions by pinging from PC-A to the gateway.

From PC-A:

```
C:\> ping 192.168.1.1
```

The ping should succeed, showing that DAI allows valid ARP traffic.

Part 6: Configure IP Source Guard

IP Source Guard prevents IP spoofing attacks by filtering traffic based on the DHCP snooping binding table and manually configured IP source bindings.

Step 1: Enable IP Source Guard on access ports

a. Enable IP source verification on S1 access ports.

```
S1(config)# interface f0/6
S1(config-if)# ip verify source
S1(config-if)# exit
S1(config)# interface f0/3
S1(config-if)# ip verify source
S1(config-if)# exit
```

Note: This enables IP-based filtering only. Traffic will be permitted only if the source IP matches the DHCP snooping binding table.

Step 2: Enable IP Source Guard with MAC address filtering

For stronger security, enable both IP and MAC filtering.

a. Enable IP and MAC verification on F0/10.

```
S1(config)# interface f0/10
S1(config-if)# ip verify source port-security
S1(config-if)# exit
```

Note: This requires port security to be configured on the interface (which we did in Part 2).

b. Repeat IP and MAC filtering on S2 for PC-C.

```
S2(config)# interface f0/11
S2(config-if)# ip verify source port-security
S2(config-if)# exit
```

Step 3: Verify IP Source Guard configuration

a. Check IP Source Guard bindings on S1.

```
S1# show ip verify source
Interface Filter-type Filter-mode IP-address Mac-address Vlan
--------- ----------- ----------- --------------- ----------------- ----
Fa0/3 ip active 192.168.1.11 10
Fa0/6 ip active 192.168.1.12 10
Fa0/10 ip-mac active 192.168.1.15 0050.56be.8e3b 10
```

b. Verify entries match the DHCP snooping binding table.

```
S1# show ip dhcp snooping binding
```

Step 4: Test IP Source Guard against IP spoofing

a. On Attacker-PC, change the static IP address to an unauthorized address.

Windows: Control Panel → Network Adapter → IPv4 Properties
Set IP address to: 192.168.1.200

b. Attempt to ping the gateway from Attacker-PC.

```
C:\> ping 192.168.1.1
```

The ping should fail because the source IP (192.168.1.200) does not match the DHCP binding entry.

c. Verify that IP Source Guard is blocking traffic on S1.

```
S1# show ip verify source
```

The filter will show the original permitted IP, and traffic from 192.168.1.200 will be silently dropped.

d. Change Attacker-PC back to DHCP to restore connectivity.

```
C:\> ipconfig /release
C:\> ipconfig /renew
```

Part 7: Configure Spanning Tree Protocol Security

STP attacks can manipulate the spanning tree topology to redirect traffic through an attacker's system. STP security features prevent these attacks.

Step 1: Determine the current root bridge

a. Check STP status on S1.

```
S1# show spanning-tree
```

Note: The Root ID shows which switch is the root bridge.

Step 2: Configure S1 as the root bridge

For this lab, we want S1 to be the root bridge for all VLANs.

a. Set S1 as the primary root bridge.

```
S1(config)# spanning-tree vlan 10,99 root primary
```

Note: This sets the bridge priority to 24576 (or 4096 lower than the current root).

b. Verify S1 is now the root bridge.

```
S1# show spanning-tree
```

c. Alternatively, manually set the bridge priority.

```
S1(config)# spanning-tree vlan 10 priority 4096
```

Note: Priority must be a multiple of 4096 (0, 4096, 8192, 16384, 24576, 28672, 32768).

Step 3: Configure S2 as the secondary root bridge

The secondary root bridge will take over if the primary root fails.

```
S2(config)# spanning-tree vlan 10,99 root secondary
```

Note: This sets the bridge priority to 28672.

Step 4: Enable PortFast on access ports

PortFast allows access ports to transition immediately to forwarding state, bypassing the listening and learning states. This should ONLY be enabled on access ports connected to end devices.

a. Enable PortFast on individual access ports on S1.

```
S1(config)# interface f0/3
S1(config-if)# spanning-tree portfast
S1(config-if)# exit
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
S1(config-if)# exit
S1(config)# interface f0/10
S1(config-if)# spanning-tree portfast
S1(config-if)# exit
```

Note: You will see a warning message. PortFast should only be used on ports connected to end devices.

b. Alternatively, enable PortFast globally for all access ports.

```
S1(config)# spanning-tree portfast default
```

Note: This enables PortFast on all non-trunk ports by default.

c. Repeat PortFast configuration on S2 access ports.

```
S2(config)# interface f0/11
S2(config-if)# spanning-tree portfast
S2(config-if)# exit
```

Step 5: Enable BPDU Guard on access ports

BPDU Guard protects against STP manipulation attacks by shutting down any PortFast-enabled port that receives a BPDU.

a. Enable BPDU Guard on individual access ports.

```
S1(config)# interface f0/3
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# interface f0/6
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# interface f0/10
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
```

b. Alternatively, enable BPDU Guard globally for all PortFast ports.

```
S1(config)# spanning-tree portfast bpduguard default
```

Note: This automatically enables BPDU Guard on all PortFast-enabled ports.

c. Repeat on S2.

```
S2(config)# spanning-tree portfast bpduguard default
```

Step 6: Enable Root Guard on boundary ports

Root Guard prevents unauthorized switches from becoming the root bridge by disabling ports that receive superior BPDUs.

a. Enable Root Guard on S2's trunk port to S1.

```
S2(config)# interface f0/1
S2(config-if)# spanning-tree guard root
S2(config-if)# exit
```

Note: Root Guard should be enabled on all ports where the root bridge should never appear.

Step 7: Enable Loop Guard (optional)

Loop Guard prevents alternate or root ports from becoming designated ports due to loss of BPDUs, which could create a bridging loop.

a. Enable Loop Guard globally.

```
S1(config)# spanning-tree loopguard default
S2(config)# spanning-tree loopguard default
```

b. Alternatively, enable Loop Guard on specific interfaces.

```
S1(config)# interface f0/1
S1(config-if)# spanning-tree guard loop
S1(config-if)# exit
```

Step 8: Verify STP security features

a. View the overall STP summary.

```
S1# show spanning-tree summary

Switch is in pvst mode
Root bridge for: VLAN0010, VLAN0099
Portfast Default is enabled
PortFast BPDU Guard Default is enabled
Loopguard Default is enabled
```

b. Verify PortFast and BPDU Guard status on access ports.

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

Look for:

```
The port is in the portfast mode
Bpdu guard is enabled
```

c. Check for any STP inconsistencies.

```
S1# show spanning-tree inconsistentports
```

No inconsistencies found (this is good).

d. Test BPDU Guard by connecting a switch to an access port (F0/10).
Connect a switch and verify that the port is error-disabled.

e. Recover the error-disabled port.

```
S1(config)# interface f0/10
S1(config-if)# shutdown
S1(config-if)# no shutdown
S1(config-if)# exit
```

Part 8: Final Verification

Verification Checklist

Verify all security features are operational using the following commands:

Port Security:

- `show port-security`
- `show port-security interface [interface]`
- `show port-security address`

VLAN Security:

- `show interfaces trunk`
- `show interfaces switchport`
- `Verify DTP is disabled`
- `Verify native VLAN is changed`
- `Verify unused ports are shutdown`

DHCP Snooping:

- `show ip dhcp snooping`
- `show ip dhcp snooping binding`

Dynamic ARP Inspection:

- `show ip arp inspection`
- `show ip arp inspection interfaces`
- `show ip arp inspection statistics`

IP Source Guard:

- `show ip verify source`

STP Security:

- `show spanning-tree summary`
- `show spanning-tree interface [interface] detail`
- `show spanning-tree inconsistentports`

End of Lab

Appendix A: Quick Reference Command Summary

Port Security:

```
switchport mode access
switchport port-security
switchport port-security maximum [number]
switchport port-security mac-address [mac-address | sticky]
switchport port-security violation {protect | restrict | shutdown}
switchport port-security aging time [minutes]
switchport port-security aging type {absolute | inactivity}
```

VLAN Security:

```
switchport mode {access | trunk}
switchport nonegotiate
switchport trunk native vlan [vlan-id]
switchport access vlan [vlan-id]
switchport protected
shutdown
```

DHCP Snooping:

```
ip dhcp snooping
ip dhcp snooping vlan [vlan-list]
ip dhcp snooping trust
ip dhcp snooping limit rate [rate]
```

Dynamic ARP Inspection:

```
ip arp inspection vlan [vlan-list]
ip arp inspection trust
ip arp inspection validate {src-mac | dst-mac | ip}
```

IP Source Guard:

```
ip verify source
ip verify source port-security
```

Spanning Tree Security:

```
spanning-tree vlan [vlan-list] root {primary | secondary}
spanning-tree vlan [vlan-list] priority [priority]
spanning-tree portfast
spanning-tree portfast default
spanning-tree bpduguard enable
spanning-tree portfast bpduguard default
spanning-tree guard root
spanning-tree guard loop
```

```
spanning-tree loopguard default
```

Verification Commands:

```
show port-security
show port-security interface [interface]
show port-security address
show interfaces [interface] switchport
show interfaces trunk
show ip dhcp snooping
show ip dhcp snooping binding
show ip arp inspection
show ip arp inspection interfaces
show ip arp inspection statistics
show ip verify source
show spanning-tree
show spanning-tree summary
show spanning-tree interface [interface] detail
show spanning-tree inconsistentports
show interface status
show run
show ip dhcp binding
```