Module 11: Switch Security Configuration

Instructor Materials

Switching, Routing and Wireless
Essentials v7.0 (SRWE)

Module 11: Switch Security Configuration

Switching, Routing and Wireless
Essentials v7.0 (SRWE)

Module Objectives

Module Title: Switch Security Configuration

Module Objective: Configure switch security to mitigate LAN attacks

Topic Title	Topic Objective
Implement Port Security	Implement port security to mitigate MAC address table attacks.
Mitigate VLAN Attacks	Explain how to configure DTP and native VLAN to mitigate VLAN attacks.
Mitigate DHCP Attacks	Explain how to configure DHCP snooping to mitigate DHCP attacks.
Mitigate ARP Attacks	Explain how to configure ARP inspection to mitigate ARP attacks.
Mitigate STP Attacks	Explain how to configure PortFast and BPDU Guard to mitigate STP Attacks.

11.1 Implement Port Security

Secure Unused Ports

Layer 2 attacks are some of the easiest for hackers to deploy but these threats can also be mitigated with some common Layer 2 solutions.

- All switch ports (interfaces) should be secured before the switch is deployed for production use. How a port is secured depends on its function.

- A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch. Navigate to each unused port and issue the Cisco IOS **shutdown** command. If a port must be reactivated at a later time, it can be enabled with the **no shutdown** command.

- To configure a range of ports, use the **interface range** command.

```
Switch(config)# interface range type module/first-number - last-number
```

Mitigate MAC Address Table Attacks

The simplest and most effective method to prevent MAC address table overflow attacks is to enable port security.

- Port security limits the number of valid MAC addresses allowed on a port. It allows an administrator to manually configure MAC addresses for a port or to permit the switch to dynamically learn a limited number of MAC addresses. When a port configured with port security receives a frame, the source MAC address of the frame is compared to the list of secure source MAC addresses that were manually configured or dynamically learned on the port.

- By limiting the number of permitted MAC addresses on a port to one, port security can be used to control unauthorized access to the network.

Enable Port Security

Port security is enabled with the **switchport port-security** interface configuration command.

Notice in the example, the **switchport port-security** command was rejected. This is because port security can only be configured on manually configured access ports or manually configured trunk ports. By default, Layer 2 switch ports are set to dynamic auto (trunking on). Therefore, in the example, the port is configured with the **switchport mode access** interface configuration command.

Note: Trunk port security is beyond the scope of this course.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Enable Port Security (Cont.)

Use the **show port-security interface** command to display the current port security settings for FastEthernet 0/1.

- Notice how port security is enabled, the violation mode is shutdown, and how the maximum number of MAC addresses is 1.

- If a device is connected to the port, the switch will automatically add the device's MAC address as a secure MAC. In this example, no device is connected to the port.

Note: If an active port is configured with the **switchport port-security** command and more than one device is connected to that port, the port will transition to the error-disabled state.

```
S1# show port-security interface f0/1
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        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Enable Port Security (Cont.)

After port security is enabled, other port security specifics can be configured, as shown in the example.

```
S1(config-if)# switchport port-security ?
  aging           Port-security aging commands
  mac-address     Secure mac address
  maximum         Max secure addresses
  violation       Security violation mode
  <cr>
S1(config-if)# switchport port-security
```

Limit and Learn MAC Addresses

To set the maximum number of MAC addresses allowed on a port, use the following command:

```
Switch(config-if)# switchport port-security maximum value
```

- The default port security value is 1.
- The maximum number of secure MAC addresses that can be configured depends the switch and the IOS.
- In this example, the maximum is 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

Limit and Learn MAC Addresses (Cont.)

The switch can be configured to learn about MAC addresses on a secure port in one of three ways:

1. Manually Configured: The administrator manually configures a static MAC address(es) by using the following command for each secure MAC address on the port:

```
Switch(config-if)# switchport port-security mac-address mac-address
```

2. Dynamically Learned: When the **switchport port-security** command is entered, the current source MAC for the device connected to the port is automatically secured but is not added to the running configuration. If the switch is rebooted, the port will have to re-learn the device's MAC address.

3. Dynamically Learned – Sticky: The administrator can enable the switch to dynamically learn the MAC address and "stick" them to the running configuration by using the following command:

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

Saving the running configuration will commit the dynamically learned MAC address to NVRAM.

Limit and Learn MAC Addresses (Cont.)

The example demonstrates a complete port security configuration for FastEthernet 0/1.

- The administrator specifies a maximum of 4 MAC addresses, manually configures one secure MAC address, and then configures the port to dynamically learn additional secure MAC addresses up to the 4 secure MAC address maximum.

- Use the **show port-security interface** and the **show port-security address** command to verify the configuration.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 4
Total MAC Addresses         : 1
Configured MAC Addresses    : 1
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 0000.0000.0000:0
Security Violation Count    : 0
S1# show port-security address
            Secure Mac Address Table
---------------------------------------------------------------------
Vlan    Mac Address      Type            Ports     Remaining Age
                                                      (mins)
----    -----------      ----            -----     -------------
   1    aaaa.bbbb.1234   SecureConfigured   Fa0/1       -

---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

S1#
```

Port Security Aging

Port security aging can be used to set the aging time for static and dynamic secure addresses on a port and two types of aging are supported per port:

- **Absolute** - The secure addresses on the port are deleted after the specified aging time.
- **Inactivity** - The secure addresses on the port are deleted if they are inactive for a specified time.

Use aging to remove secure MAC addresses on a secure port without manually deleting the existing secure MAC addresses.

- Aging of statically configured secure addresses can be enabled or disabled on a per-port basis.

Use the **switchport port-security aging** command to enable or disable static aging for the secure port, or to set the aging time or type.

```
Switch(config-if)# switchport port-security aging {static | time time | type {absolute | inactivity}}
```

Port Security Aging (Cont.)

The example shows an administrator configuring the aging type to 10 minutes of inactivity.

The **show port-security** command confirms the changes.

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
```

CISCO

Port Security Violation Modes

If the MAC address of a device attached to a port differs from the list of secure addresses, then a port violation occurs and the port enters the error-disabled state.

- To set the port security violation mode, use the following command:

```
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}
```

The following table shows how a switch reacts based on the configured violation mode.

Mode	Description
shutdown (default)	The port transitions to the error-disabled state immediately, turns off the port LED, and sends a syslog message. It increments the violation counter. When a secure port is in the error-disabled state, an administrator must re-enable it by entering the **shutdown** and **no shutdown** commands.
restrict	The port drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value. This mode causes the Security Violation counter to increment and generates a syslog message.
protect	This is the least secure of the security violation modes. The port drops packets with unknown MAC source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value. No syslog message is sent.

Port Security Violation Modes (Cont.)

The example shows an administrator changing the security violation to "Restrict".

The output of the **show port-security interface** command confirms that the change has been made.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
S1#
```

Ports in error-disabled State

When a port is shutdown and placed in the error-disabled state, no traffic is sent or received on that port.

A series of port security related messages display on the console, as shown in the following example.

Note: The port protocol and link status are changed to down and the port LED is turned off.

```
*Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting Fa0/18 in
err-disable state
*Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address 000c.292b.4c75 on port FastEthernet0/18.
*Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface FastEthernet0/18, changed state
to down
*Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

Ports in error-disabled State (Cont.)

- In the example, the **show interface** command identifies the port status as **err-disabled**. The output of the **show port-security interface** command now shows the port status as **secure-shutdown**. The Security Violation counter increments by 1.

- The administrator should determine what caused the security violation If an unauthorized device is connected to a secure port, the security threat is eliminated before re-enabling the port.

- To re-enable the port, first use the **shutdown** command, then, use the **no shutdown** command.

```
S1# show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/18
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   : c025.5cd7.ef01:1
Security Violation Count   : 1
S1#
```

Verify Port Security

After configuring port security on a switch, check each interface to verify that the port security is set correctly, and check to ensure that the static MAC addresses have been configured correctly.

To display port security settings for the switch, use the **show port-security** command.

- The example indicates that all 24 interfaces are configured with the **switchport port-security** command because the maximum allowed is 1 and the violation mode is shutdown.
- No devices are connected, therefore, the CurrentAddr (Count) is 0 for each interface.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)        (Count)        (Count)
---------------------------------------------------------------------------
    Fa0/1          1              0              0              Shutdown
    Fa0/2          1              0              0              Shutdown
    Fa0/3          1              0              0              Shutdown
(output omitted)
    Fa0/24         1              0              0              Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)       : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

CISCO

Verify Port Security (Cont.)

Use the **show port-security interface** command to view details for a specific interface, as shown previously and in this example.

```
S1# show port-security interface fastethernet 0/18
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    : 0
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 0025.83e6.4b01:1
Security Violation Count    : 0
S1#
```

Verify Port Security (Cont.)

To verify that MAC addresses are "sticking" to the configuration, use the **show run** command as shown in the example for FastEthernet 0/19.

```
S1# show run | begin interface FastEthernet0/19
interface FastEthernet0/19
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0025.83e6.4b02
(output omitted)
S1#
```

Verify Port Security (Cont.)

To display all secure MAC addresses that are manually configured or dynamically learned on all switch interfaces, use the **show port-security address** command as shown in the example.

```
S1# show port-security address
Secure Mac Address Table
----------------------------------------------------------------------
Vlan    Mac Address      Type            Ports       Remaining Age
                                                       (mins)
----    -----------      ----            -----       ------------
1       0025.83e6.4b01   SecureDynamic   Fa0/18          -
1       0025.83e6.4b02   SecureSticky    Fa0/19          -
----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Packet Tracer – Implement Port Security

In this Packet Tracer, you will complete the following objectives:

- Part 1: Configure Port Security
- Part 2: Verify Port Security

11.2 Mitigate VLAN Attacks

VLAN Attacks Review

A VLAN hopping attack can be launched in one of three ways:

- Spoofing DTP messages from the attacking host to cause the switch to enter trunking mode. From here, the attacker can send traffic tagged with the target VLAN, and the switch then delivers the packets to the destination.

- Introducing a rogue switch and enabling trunking. The attacker can then access all the VLANs on the victim switch from the rogue switch.

- Another type of VLAN hopping attack is a double-tagging (or double-encapsulated) attack. This attack takes advantage of the way hardware on most switches operate.

Steps to Mitigate VLAN Hopping Attacks

Use the following steps to mitigate VLAN hopping attacks:

Step 1: Disable DTP (auto trunking) negotiations on non-trunking ports by using the **switchport mode access** interface configuration command.

Step 2: Disable unused ports and put them in an unused VLAN.

Step 3: Manually enable the trunk link on a trunking port by using the **switchport mode trunk** command.

Step 4: Disable DTP (auto trunking) negotiations on trunking ports by using the **switchport nonegotiate** command.

Step 5: Set the native VLAN to a VLAN other than VLAN 1 by using the **switchport trunk native vlan** *vlan_number* command.

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

11.3 Mitigate DHCP Attacks

DHCP Attack Review

The goal of a DHCP starvation attack is to an attack tool such as Gobbler to create a Denial of Service (DoS) for connecting clients.

Recall that DHCP starvation attacks can be effectively mitigated by using port security because Gobbler uses a unique source MAC address for each DHCP request sent. However, mitigating DHCP spoofing attacks requires more protection.

Gobbler could be configured to use the actual interface MAC address as the source Ethernet address, but specify a different Ethernet address in the DHCP payload. This would render port security ineffective because the source MAC address would be legitimate.

DHCP spoofing attacks can be mitigated by using DHCP snooping on trusted ports.

DHCP Snooping

DHCP snooping filters DHCP messages and rate-limits DHCP traffic on untrusted ports.

- Devices under administrative control (e.g., switches, routers, and servers) are trusted sources.
- Trusted interfaces (e.g., trunk links, server ports) must be explicitly configured as trusted.
- Devices outside the network and all access ports are generally treated as untrusted sources.

A DHCP table is built that includes the source MAC address of a device on an untrusted port and the IP address assigned by the DHCP server to that device.

- The MAC address and IP address are bound together.
- Therefore, this table is called the DHCP snooping binding table.

Steps to Implement DHCP Snooping

Use the following steps to enable DHCP snooping:

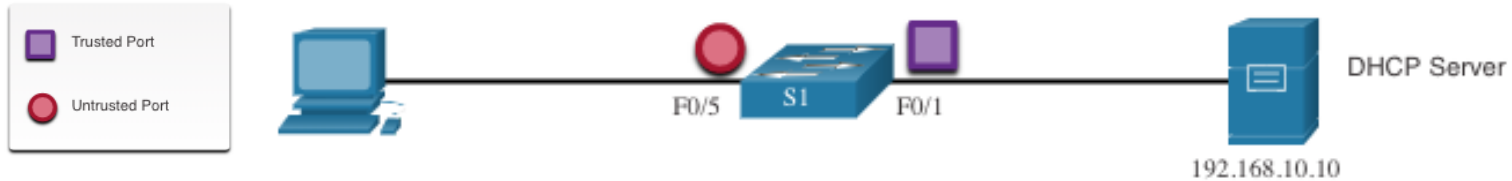**Step 1**. Enable DHCP snooping by using the **ip dhcp snooping** global configuration command.

Step 2. On trusted ports, use the **ip dhcp snooping trust** interface configuration command.

Step 3: On untrusted interfaces, limit the number of DHCP discovery messages that can be received using the **ip dhcp snooping limit rate** *packets-per-second* interface configuration command.

Step 4. Enable DHCP snooping by VLAN, or by a range of VLANs, by using the **ip dhcp snooping** *vlan* global configuration command.

DHCP Snooping Configuration Example

Refer to the DHCP snooping sample topology with trusted and untrusted ports.

- DHCP snooping is first enabled on S1.
- The upstream interface to the DHCP server is explicitly trusted.
- F0/5 to F0/24 are untrusted and are, therefore, rate limited to six packets per second.
- Finally, DHCP snooping is enabled on VLANS 5, 10, 50, 51, and 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

DHCP Snooping Configuration Example (Cont.)

Use the **show ip dhcp snooping** privileged EXEC command to verify DHCP snooping settings.

Use the **show ip dhcp snooping binding** command to view the clients that have received DHCP information.

Note: DHCP snooping is also required by Dynamic ARP Inspection (DAI).

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
    circuit-id default format: vlan-mod-port
    remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface              Trusted      Allow option    Rate limit (pps)
------------------     -------      ------------    ----------------
FastEthernet0/1        yes          yes             unlimited
  Custom circuit-ids:
FastEthernet0/5        no           no              6
  Custom circuit-ids:
FastEthernet0/6        no           no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress         IpAddress        Lease(sec) Type           VLAN Interface
------------------ ---------------- ---------- -------------- ---- --------------------
00:03:47:B5:9F:AD  192.168.10.10    193185     dhcp-snooping  5    FastEthernet0/5
```

11.4 Mitigate ARP Attacks

Dynamic ARP Inspection

In a typical ARP attack, a threat actor can send unsolicited ARP replies to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway. To prevent ARP spoofing and the resulting ARP poisoning, a switch must ensure that only valid ARP Requests and Replies are relayed.

Dynamic ARP inspection (DAI) requires DHCP snooping and helps prevent ARP attacks by:

- Not relaying invalid or gratuitous ARP Replies out to other ports in the same VLAN.
- Intercepting all ARP Requests and Replies on untrusted ports.
- Verifying each intercepted packet for a valid IP-to-MAC binding.
- Dropping and logging ARP Replies coming from invalid to prevent ARP poisoning.
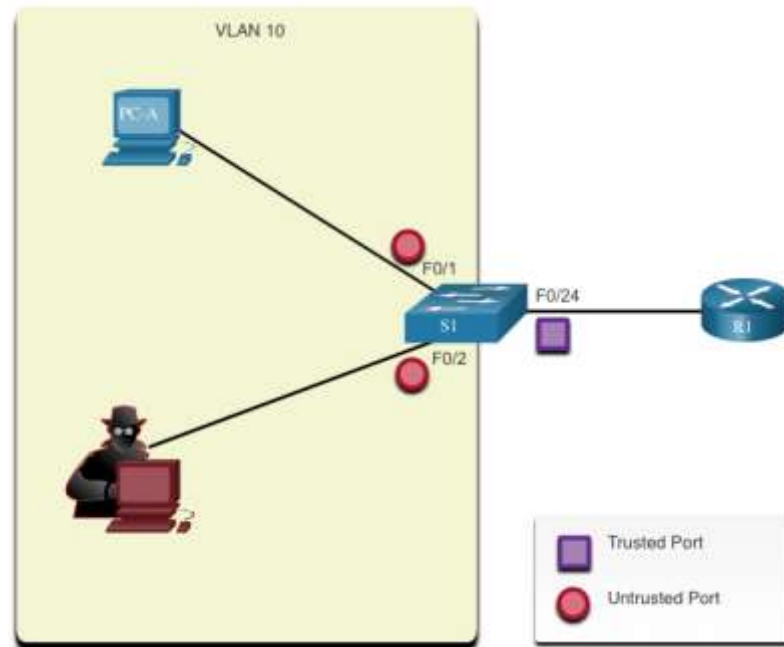- Error-disabling the interface if the configured DAI number of ARP packets is exceeded.

DAI Implementation Guidelines

To mitigate the chances of ARP spoofing and ARP poisoning, follow these DAI implementation guidelines:

- Enable DHCP snooping globally.
- Enable DHCP snooping on selected VLANs.
- Enable DAI on selected VLANs.
- Configure trusted interfaces for DHCP snooping and ARP inspection.

It is generally advisable to configure all access switch ports as untrusted and to configure all uplink ports that are connected to other switches as trusted.

DAI Configuration Example

In the previous topology, S1 is connecting two users on VLAN 10.

- DAI will be configured to mitigate against ARP spoofing and ARP poisoning attacks.

- DHCP snooping is enabled because DAI requires the DHCP snooping binding table to operate.

- Next, DHCP snooping and ARP inspection are enabled for the PCs on VLAN10.

- The uplink port to the router is trusted, and therefore, is configured as trusted for DHCP snooping and ARP inspection.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

DAI Configuration Example (Cont.)

DAI can also be configured to check for both destination or source MAC and IP addresses:

- **Destination MAC** - Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body.

- **Source MAC** - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.

- **IP address** - Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

DAI Configuration Example (Cont.)

The **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} global configuration command is used to configure DAI to drop ARP packets when the IP addresses are invalid.

- It can be used when the MAC addresses in the body of the ARP packets do not match the addresses that are specified in the Ethernet header.

- Notice in the following example how only one command can be configured.

- Therefore, entering multiple **ip arp inspection validate** commands overwrites the previous command.

- To include more than one validation method, enter them on the same command line as shown in the output.

```
S1(config)# ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

11.5 Mitigate STP Attacks

PortFast and BPDU Guard

Recall that network attackers can manipulate the Spanning Tree Protocol (STP) to conduct an attack by spoofing the root bridge and changing the topology of a network.

To mitigate STP attacks, use PortFast and Bridge Protocol Data Unit (BPDU) Guard:

PortFast

- PortFast immediately brings a port to the forwarding state from a blocking state, bypassing the listening and learning states.
- Apply to all end-user access ports.

BPDU Guard

- BPDU guard immediately error disables a port that receives a BPDU.
- Like PortFast, BPDU guard should only be configured on interfaces attached to end devices.

Configure PortFast

PortFast bypasses the STP listening and learning states to minimize the time that access ports must wait for STP to converge.

- Only enable PortFast on access ports.
- PortFast on inter switch links can create a spanning-tree loop.

PortFast can be enabled:

- **On an interface** – Use the **spanning-tree portfast** interface configuration command.
- **Globally** – Use the **spanning-tree portfast default** global configuration command to enable PortFast on all access ports.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
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 FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
```

Configure PortFast (Cont.)

To verify whether PortFast is enabled globally you can use either the:

- **show running-config | begin span** command
- **show spanning-tree summary** command

To verify if PortFast is enabled an interface, use the **show running-config interface** *type/number* command.

The show **spanning-tree interface** *type/number* **detail** command can also be used for verification.

Configure BPDU Guard

An access port could receive an unexpected BPDUs accidentally or because a user connected an unauthorized switch to the access port.

- If a BPDU is received on a BPDU Guard enabled access port, the port is put into error-disabled state.
- This means the port is shut down and must be manually re-enabled or automatically recovered through the **errdisable recovery cause psecure_violation** global command.

BPDU Guard can be enabled:

- **On an interface** – Use the **spanning-tree bpduguard enable** interface configuration command.
- **Globally** – Use the **spanning-tree portfast bpduguard default** global configuration command to enable BPDU Guard on all access ports.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID          is enabled
Portfast Default            is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default           is disabled
EtherChannel misconfig guard is enabled
UplinkFast                  is disabled
BackboneFast                is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```

11.6 Module Practice and Quiz

Packet Tracer – Switch Security Configuration

In this Packet Tracer activity, you will:

- Secure unused ports

- Implement port security

- Mitigate VLAN hopping attacks

- Mitigate DHCP attacks

- Mitigate ARP attacks

- Mitigate STP attacks

- Verify the switch security configuration

Lab – Switch Security Configuration

In this lab, you will:

- Secure unused ports

- Implement port security

- Mitigate VLAN hopping attacks

- Mitigate DHCP attacks

- Mitigate ARP attacks

- Mitigate STP attacks

- Verify the switch security configuration

What Did I Learn In This Module?

- All switch ports (interfaces) should be secured before the switch is deployed for production use.

- By default, Layer 2 switch ports are set to dynamic auto (trunking on).

- The simplest and most effective method to prevent MAC address table overflow attacks is to enable port security.

- The switch can be configured to learn about MAC addresses on a secure port in one of three ways: manually configured, dynamically learned, and dynamically learned – sticky.

- If the MAC address of a device attached to the port differs from the list of secure addresses, then a port violation occurs. By default, the port enters the error-disabled state. When a port is placed in the error-disabled state, no traffic is sent or received on that port.

- Mitigate VLAN Hopping attacks by disabling DTP negotiations, disabling unused ports, manually setting trunking where required, and using a native VLAN other than VLAN 1.

What Did I Learn In This Module? (Cont.)

- The goal of a DHCP starvation attack is to create a Denial of Service (DoS) for connecting clients. DHCP spoofing attacks can be mitigated by using DHCP snooping on trusted ports.

- DHCP snooping determines whether DHCP messages are from an administratively-configured trusted or untrusted source. It then filters DHCP messages and rate-limits DHCP traffic from untrusted sources.

- Dynamic ARP inspection (DAI) requires DHCP snooping and helps prevent ARP attacks by verifying ARP traffic.

- Implement Dynamic ARP Inspection to mitigate ARP spoofing and ARP poisoning.

- To mitigate Spanning Tree Protocol (STP) manipulation attacks, use PortFast and Bridge Protocol Data Unit (BPDU) Guard.