**SWITCH SECURITY CONFIGURATIONS**

11.0.1

Why should I take this module?

Welcome to Switch Security Configuration!

An important part of your responsibility as a network professional is to keep the network secure. Most of the time we only think about security attacks coming from outside the network, but threats can come from within the network as well. These threats can range anywhere from an employee innocently adding an Ethernet switch to the corporate network so they can have more ports, to malicious attacks caused by a disgruntled employee. It is your job to keep the network safe and ensuring that business operations continue uncompromised.

How do we keep the network safe and stable? How do we protect it from malicious attacks from within the network? How do we make sure employees are not adding switches, servers and other devices to the network that might compromise network operations?

This module is your introduction to keeping your network secure from within!

11.0.2

What will I learn in this module?

**Module Title**: Switch Security Configuration

**Module Objective**: Configure switch security to mitigate LAN attacks.

| Table caption | |
| --- | --- |
| **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. |

**IMPLEMENT PORT SECURITY**

11.1.1

Secure Unused Ports

Layer 2 devices are considered to be the weakest link in a company’s security infrastructure. 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.

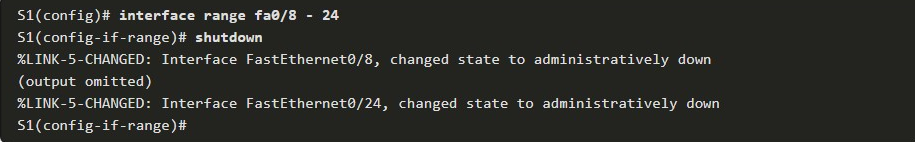
All switch ports (interfaces) should be secured before the switch is deployed for production use. How a port is secured depends on its function.

A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch. For example, if a Catalyst 2960 switch has 24 ports and there are three Fast Ethernet connections in use, it is good practice to disable the 21 unused ports. 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.



For example, to shutdown ports for Fa0/8 through Fa0/24 on S1, you would enter the following command.

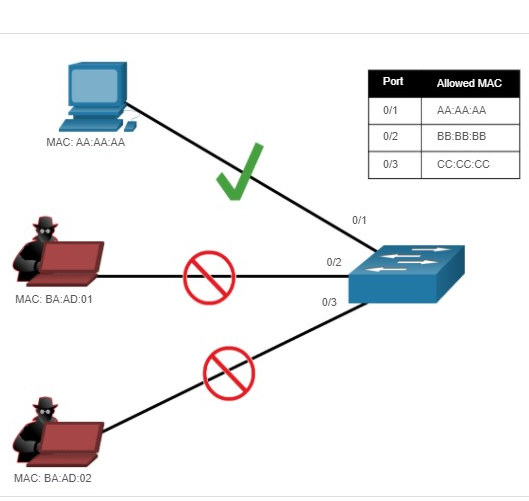
11.1.2

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, as shown in the figure.

****

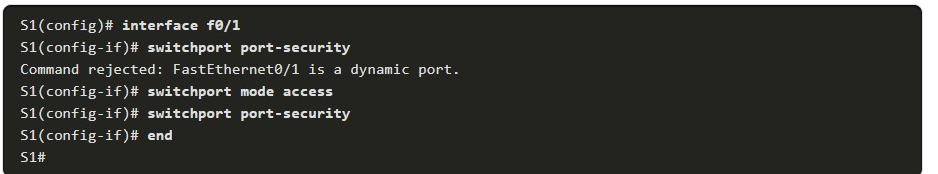
**Note**: MAC addresses are shown as 24 bits for simplicity.

11.1.3

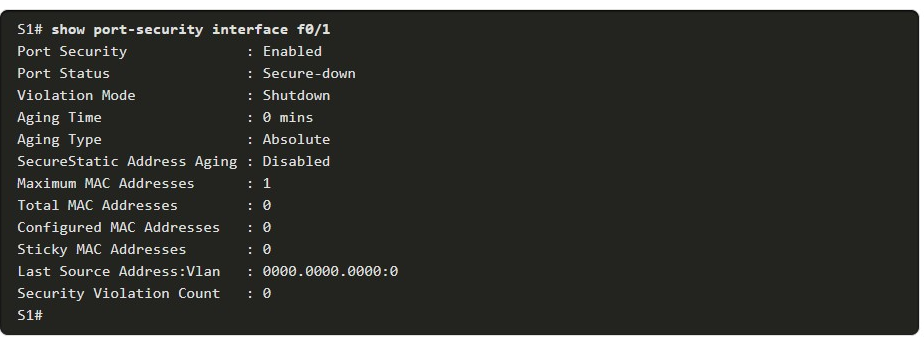
Enable Port Security

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.

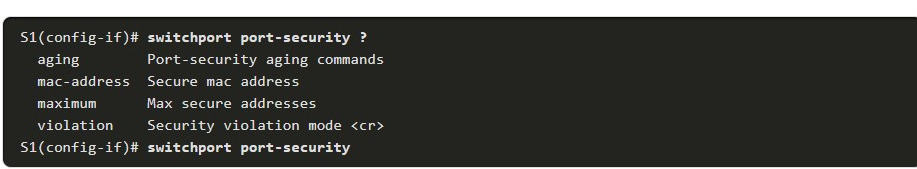
****

Use the **show port-security interface** command to display the current port security settings for FastEthernet 0/1, as shown in the example. Notice how port security is enabled, port status is Secure-down which means there are no devices attached and no violation has occurred, 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 port status would display Secure-up and 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. This condition is discussed later in this topic.

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

****

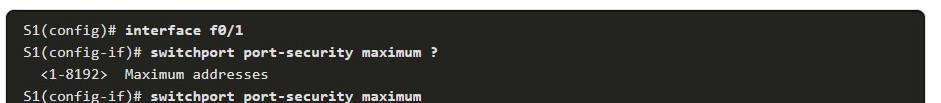
11.1.4

Limit and Learn MAC Addresses

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

****

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.

****

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:



**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 startup configuration. If the switch is rebooted, the port will have to re-learn the device’s MAC address.

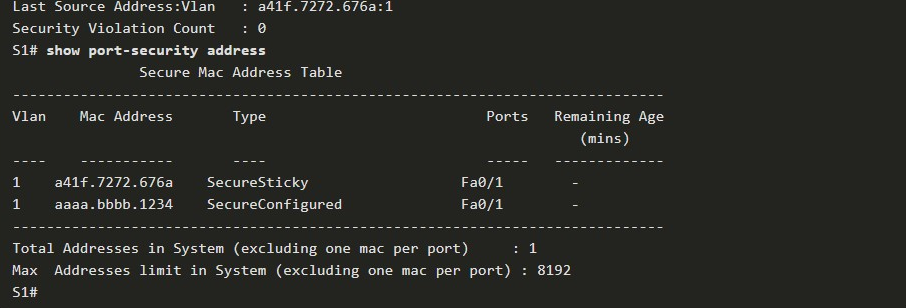
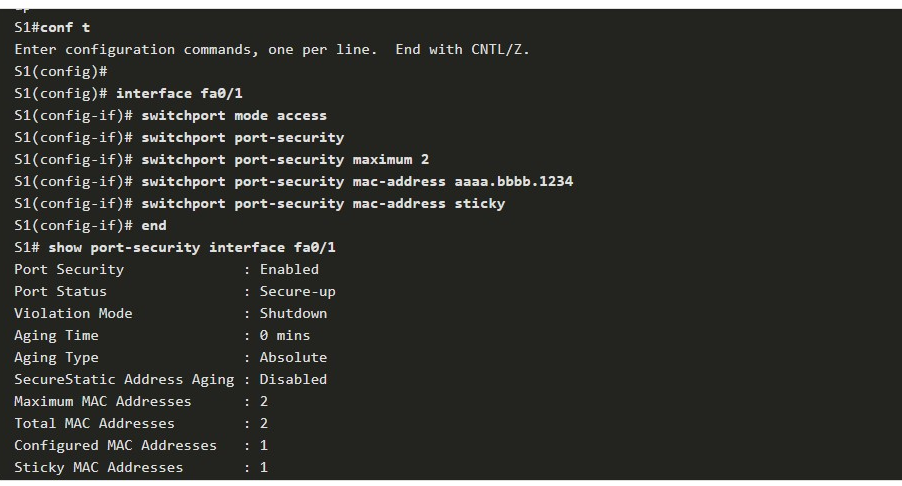
**3. Dynamically Learned – Sticky**

The administrator can enable the switch to dynamically learn the MAC address and “stick” them to the running configuration by using the following command:



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

The following example demonstrates a complete port security configuration for FastEthernet 0/1 with a host connected to port Fa0/1. The administrator specifies a maximum of 2 MAC addresses, manually configures one secure MAC address, and then configures the port to dynamically learn additional secure MAC addresses up to the 2 secure MAC address maximum. Use the **show port-security interface** and the **show port-security address** command to verify the configuration.



The output of the **show port-security interface** command verifies that port security is enabled, there is a host connected to the port (i.e., Secure-up), a total of 2 MAC addresses will be allowed, and S1 has learned one MAC address statically and one MAC address dynamically (i.e., sticky).

The output of the **show port-security address** command lists the two learned MAC addresses.

11.1.5

## Port Security Aging

Port security aging can be used to set the aging time for static and dynamic secure addresses on a port. 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 only if they are inactive for the specified aging time.

Use aging to remove secure MAC addresses on a secure port without manually deleting the existing secure MAC addresses. Aging time limits can also be increased to ensure past secure MAC addresses remain, even while new MAC addresses are added. 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.

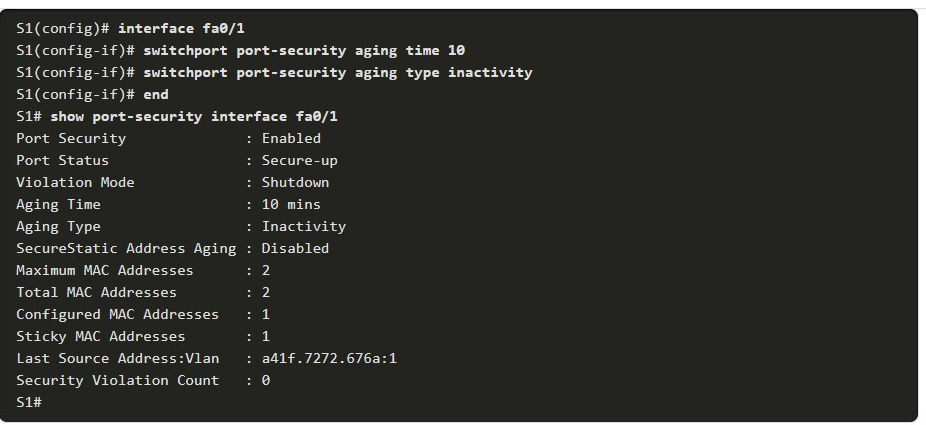
****

The parameters for the command are described in the table.

| Parameter Description staticEnable aging for statically configured secure addresses on this port.time time Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.type absoluteSet the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.type inactivitySet the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period. | |
| --- | --- |
| **Parameter** | **Description** |
| **static** | Enable aging for statically configured secure addresses on this port. |
| **time** *time* | Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port. |
| **type absolute** | Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list. |
| **type inactivity** | Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period. |

**Note**: MAC addresses are shown as 24 bits for simplicity.

The example shows an administrator configuring the aging type to 10 minutes of inactivity and by using the **show port-security interface** command to verify the configuration.

****

11.1.6

## Port Security Violation Modes

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.

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

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

The following tables show how a switch reacts based on the configured violation mode.

### **Security Violation Mode Descriptions**

| **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. |

### **Security Violation Mode Comparison**

| **Violation Mode** | **Discards Offending Traffic** | **Sends Syslog Message** | **Increase Violation Counter** | **Shuts Down Port** |
| --- | --- | --- | --- | --- |
| Protect | Yes | No | No | No |
| Restrict | Yes | Yes | Yes | No |
| Shutdown | Yes | Yes | Yes | Yes |

The following 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.

****

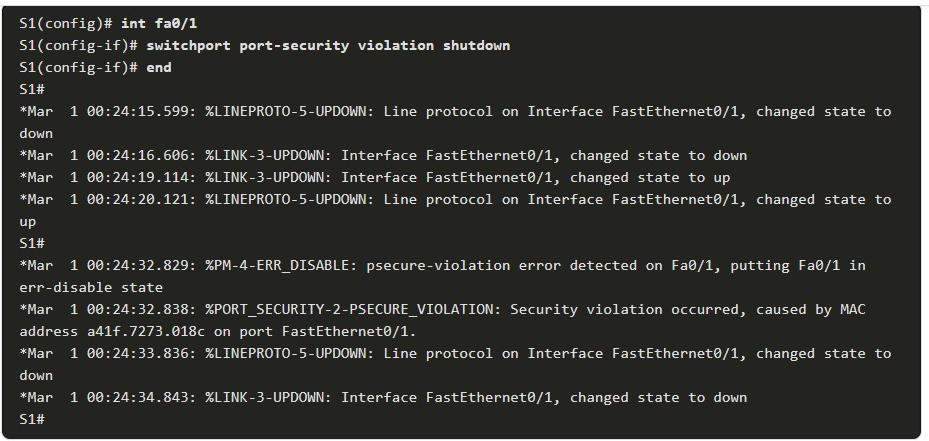
11.1.7

## Ports in error-disabled State

What happens when the port security violation is shutdown and a port violation occurs? The port is physically shutdown and placed in the error-disabled state, and no traffic is sent or received on that port.

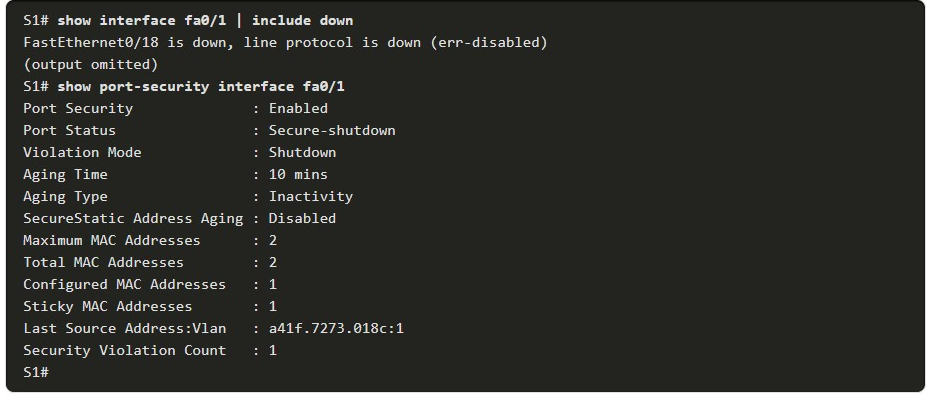
In the figure, the port security violation is changed back to the default shutdown setting. Then the host with MAC address a41f.7272.676a is disconnected and a new host is plugged into Fa0/1.

Notice how a series of port security related messages are generated on the console.

****

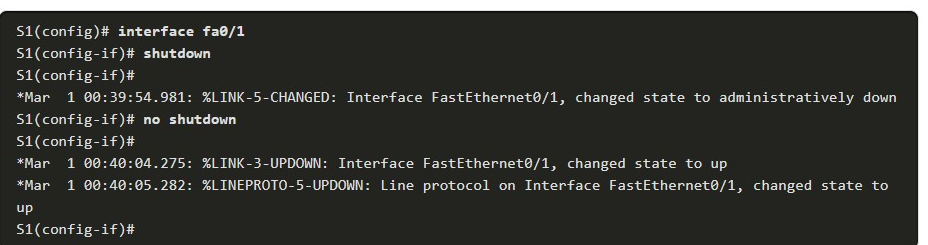
**Note**: The port protocol and link status are changed to down and the port LED is turned off.

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 instead of Secure-up. 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.

In the next example, the first host is reconnected to Fa0/1. To re-enable the port, first use the **shutdown** command, then, use the **no shutdown** command to make the port operational, as shown in the example.

****

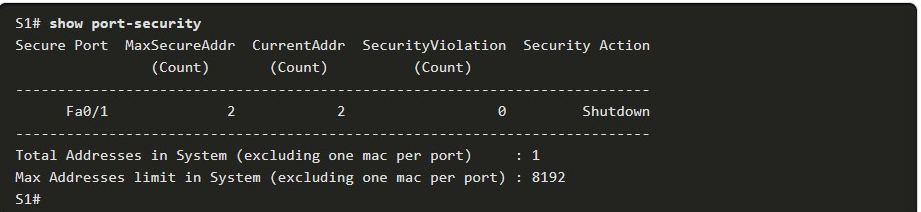
11.1.8

## 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.

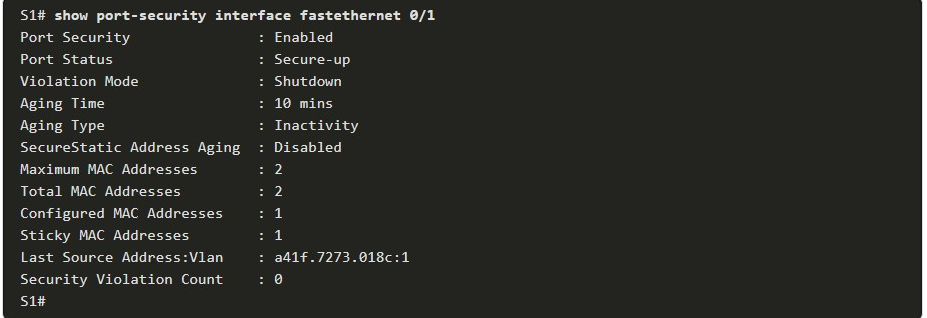
**Port Security for All Interfaces**

To display port security settings for the switch, use the **show port-security** command. The example indicates that only one port is configured with the switchport port-security command.

****

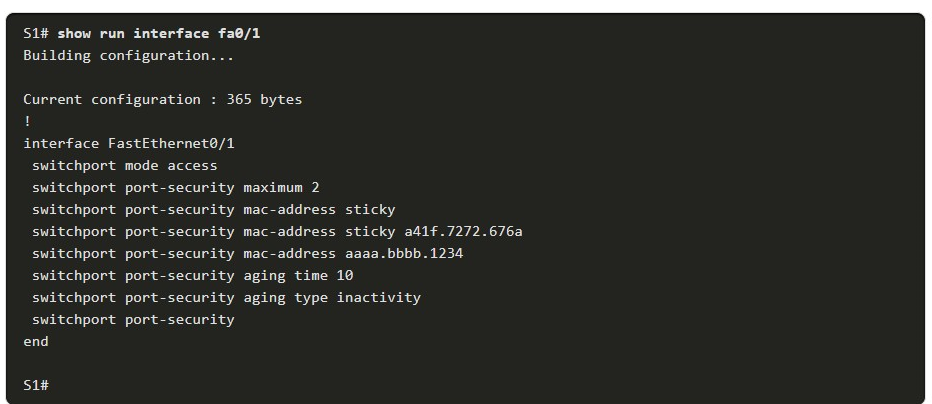
**Port Security for a Specific Interface**

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

****

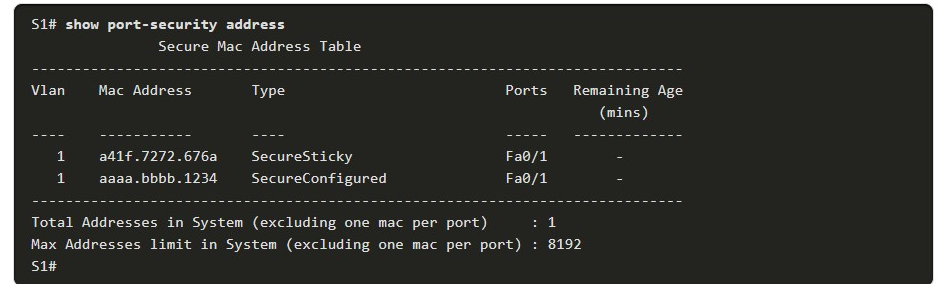
**Verify Learned MAC Addresses**

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

****

**Verify Secure MAC Addresses**

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.

****

**MITIGATE VLAN ATTACKS**

11.2.1

VLAN Attacks Review

As a quick 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.

11.2.2

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.

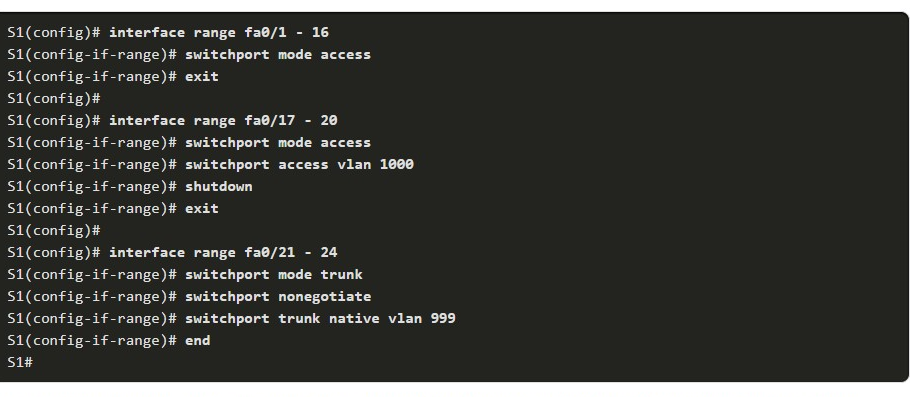
**Step 4**: Disable DTP (auto trunking) negotiations on trunking ports by using the **switchport nonegotiate** command.

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

For example, assume the following:

* FastEthernet ports 0/1 through fa0/16 are active access ports
* FastEthernet ports 0/17 through 0/20 are not currently in use
* FastEthernet ports 0/21 through 0/24 are trunk ports.

VLAN hopping can be mitigated by implementing the following configuration.

****

* FastEthernet ports 0/1 to 0/16 are access ports and therefore trunking is disabled by explicitly making them access ports.
* FastEthernet ports 0/17 to 0/20 are unused ports and are disabled and assigned to an unused VLAN.
* FastEthernet ports 0/21 to 0/24 are trunk links and are manually enabled as trunks with DTP disabled. The native VLAN is also changed from the default VLAN 1 to an unused VLAN 999.

**MITIGATE DHCP ATTACKS**

11.3.1

## DHCP Attack Review

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

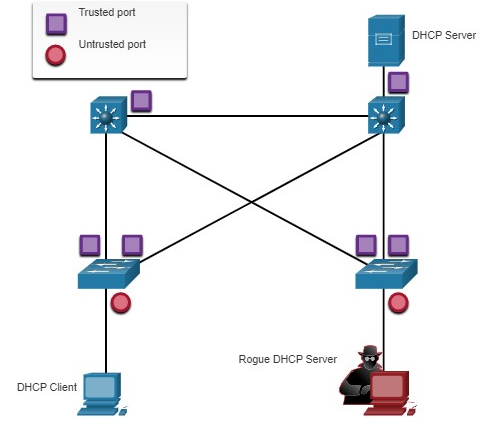
DHCP spoofing attacks can be mitigated by using DHCP snooping on trusted ports.

11.3.2

## DHCP Snooping

DHCP snooping does not rely on source MAC addresses. Instead, 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.

Devices under your administrative control, such as switches, routers, and servers, are trusted sources. Any device beyond the firewall or outside your network is an untrusted source. In addition, all access ports are generally treated as untrusted sources. The figure shows an example of trusted and untrusted ports.

****

Notice that the rogue DHCP server would be on an untrusted port after enabling DHCP snooping. All interfaces are treated as untrusted by default. Trusted interfaces are typically trunk links and ports directly connected to a legitimate DHCP server. These interfaces must be explicitly configured as trusted.

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.

11.3.3

## 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**. Limit the number of DHCP discovery messages that can be received per second on untrusted ports by using the **ip dhcp snooping limit rate** interface configuration command.

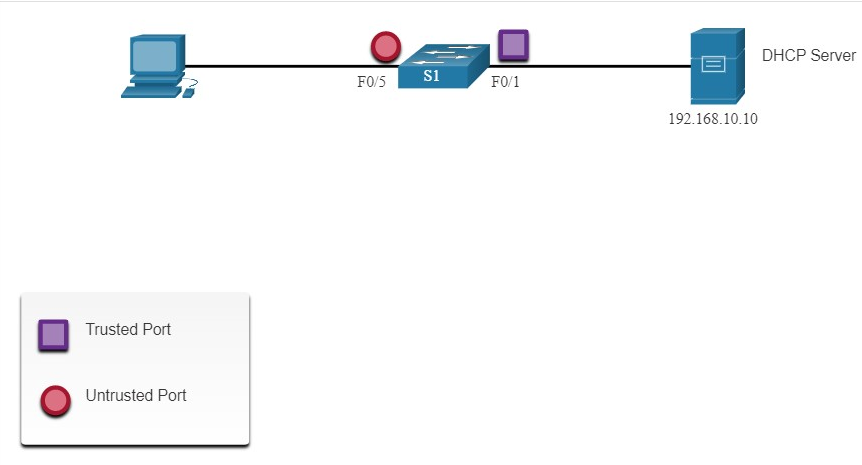
**Step 4**. Enable DHCP snooping by VLAN, or by a range of VLANs, by using the **ip dhcp snooping** vlan global configuration command.

11.3.4

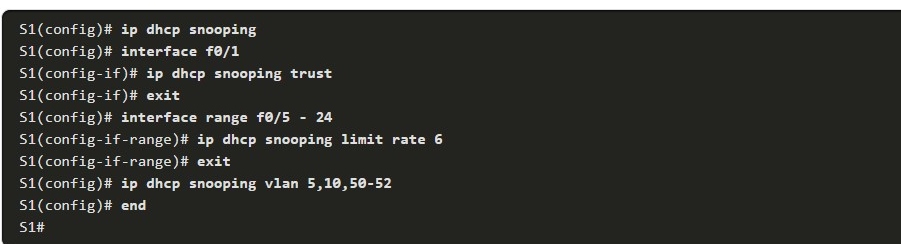
## DHCP Snooping Configuration Example

The reference topology for this DHCP snooping example is shown in the figure. Notice that F0/5 is an untrusted port because it connects to a PC. F0/1 is a trusted port because it connects to the DHCP server.

The graphic has a legend with a Purple square Trusted Port and a red circle Untrusted Port below the topology diagram. Then the graphic shows a LAN network with a switch with trusted and untrusted ports. The switch has a P C connected to the left and a D H C P connected to it on the right. On the interface connecting to the P C is a red circle for an untrusted interface and on the interface connected to the D H C P Server is the purple square for a trusted port.

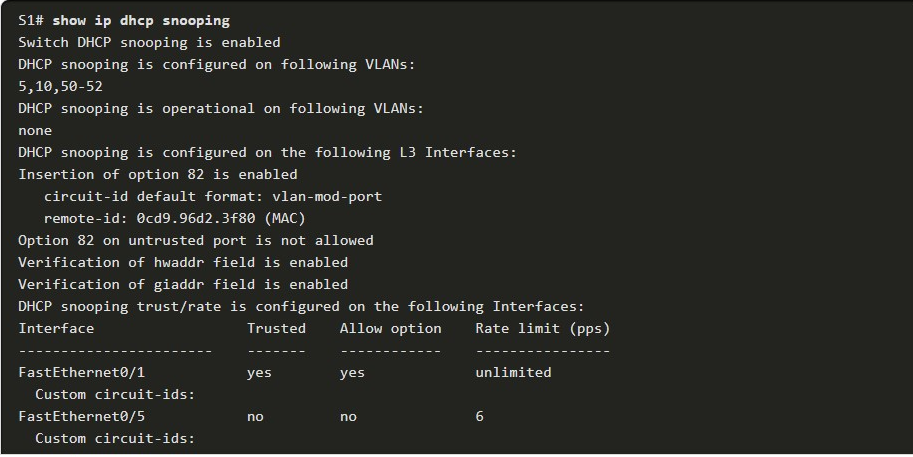
****

The following is an example of how to configure DHCP snooping on S1. Notice how DHCP snooping is first enabled. Then the upstream interface to the DHCP server is explicitly trusted. Next, the range of FastEthernet ports from F0/5 to F0/24 are untrusted by default, so a rate limit is set to six packets per second. Finally, DHCP snooping is enabled on VLANS 5, 10, 50, 51, and 52.

****

Use the **show ip dhcp snooping** privileged EXEC command to verify DHCP snooping and **show ip dhcp snooping binding** to view the clients that have received DHCP information, as shown in the example.

**Note**: DHCP snooping is also required by Dynamic ARP Inspection (DAI), which is the next topic

****

**MITIGATE ARP ATTACKS**

11.4.1

Dynamic ARP Inspection

In a typical ARP attack, a threat actor can send unsolicited ARP requests 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 Requests 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 Requests coming from invalid sources to prevent ARP poisoning.
* Error-disabling the interface if the configured DAI number of ARP packets is exceeded.

11.4.2

DAI Implementation Guidelines

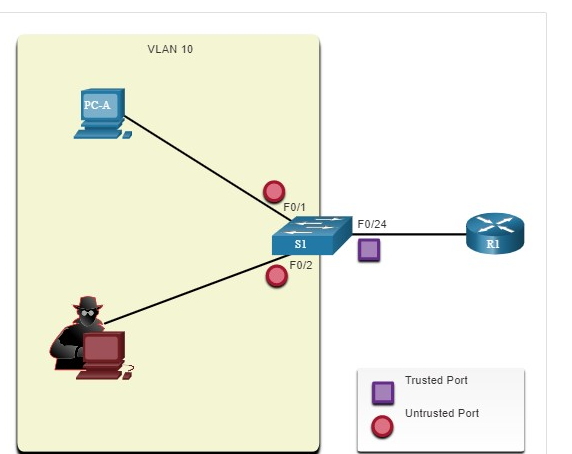
To mitigate the chances of ARP spoofing and ARP poisoning, follow these DAI implementation guidelines:

* 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.

The sample topology in the figure identifies trusted and untrusted ports.

The graphic shows a legend with a Purple square Trusted Port and a red circle Untrusted Port, above that is a LAN diagram showing Dynamic ARP Inspection Trust. The diagram illustrates a LAN network with trusted and untrusted ports. On one interface to the lower left is an attacker on one P C and to the upper left is a regular P C. Both devices are connected to the switch and both have a red circle on the switch port for an untrusted port. To the right of the switch is a router that is also connected to the switch. The router connection has a purple square on the switch that symbolizes a trusted connection for ARP.

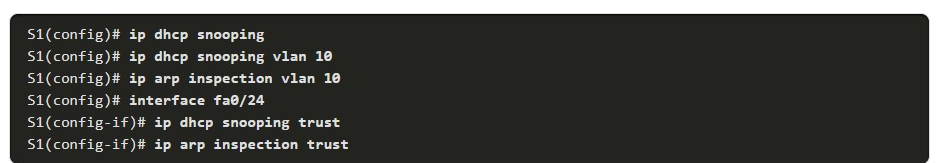
****

11.4.3

## 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.

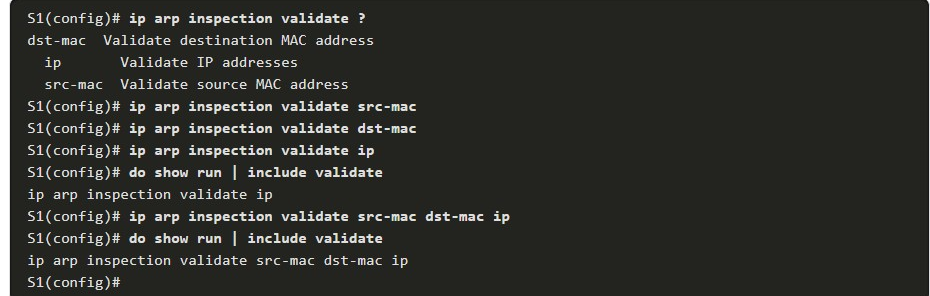
As shown in the example, DHCP snooping is enabled because DAI requires the DHCP snooping binding table to operate. Next, DHCP snooping and ARP inspection are enabled for the PCs on VLAN10. The uplink port to the router is trusted, and therefore, is configured as trusted for DHCP snooping and ARP inspection.

****

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.

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 and verified in the following output.

****

**MITIGATE STP ATTACKS**

11.5.1

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 Spanning Tree Protocol (STP) manipulation attacks, use PortFast and Bridge Protocol Data Unit (BPDU) Guard:

* **PortFast** - PortFast immediately brings an interface configured as an access port to the forwarding state from a blocking state, bypassing the listening and learning states. Apply to all end-user ports. PortFast should only be configured on ports attached to end devices.
* **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.

In the figure, the access ports for S1 should be configured with PortFast and BPDU Guard.

There are two distribution layer 3 switches at the top of the diagram that are connected by a trunk.  
Both layer 3 switches have a trunk link that are connected to the same access layer 2 switch below. This named S1 and is connected on int G0/1 and G0/2. Below S1 are several PCs and to the side of the switch it states Access Ports F0/1 - F0/24.

****

11.5.2

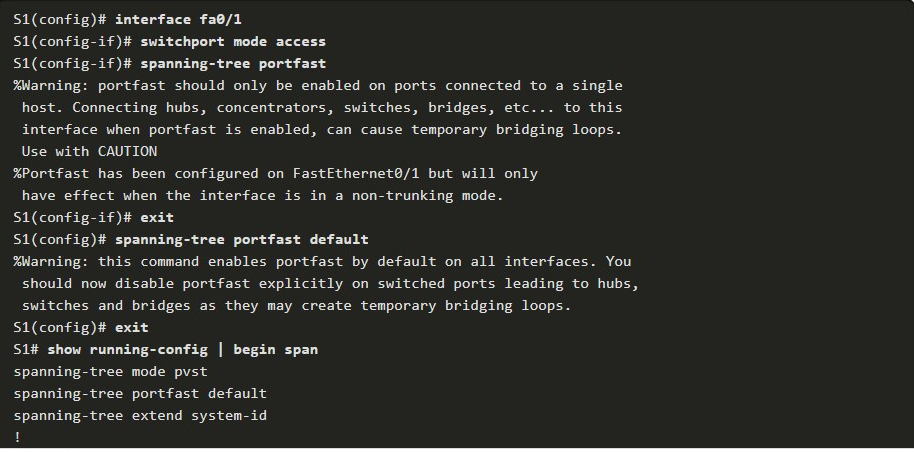
## Configure PortFast

PortFast bypasses the STP listening and learning states to minimize the time that access ports must wait for STP to converge. If PortFast is enabled on a port connecting to another switch, there is a risk of creating a spanning-tree loop.

PortFast can be enabled on an interface by using the **spanning-tree portfast** interface configuration command. Alternatively, Portfast can be configured globally on all access ports by using the **spanning-tree portfast default** global configuration command.

To verify whether PortFast is enabled globally you can use either the **show running-config | begin span** command or the **show spanning-tree summary** command. To verify if PortFast is enabled an interface, use the **show running-config interface** type/number command, as shown in the following example. The **show** **spanning-tree interface** type/number **detail** command can also be used for verification.

Notice that when PortFast is enabled, warning messages are displayed.

****

## Configure BPDU Guard

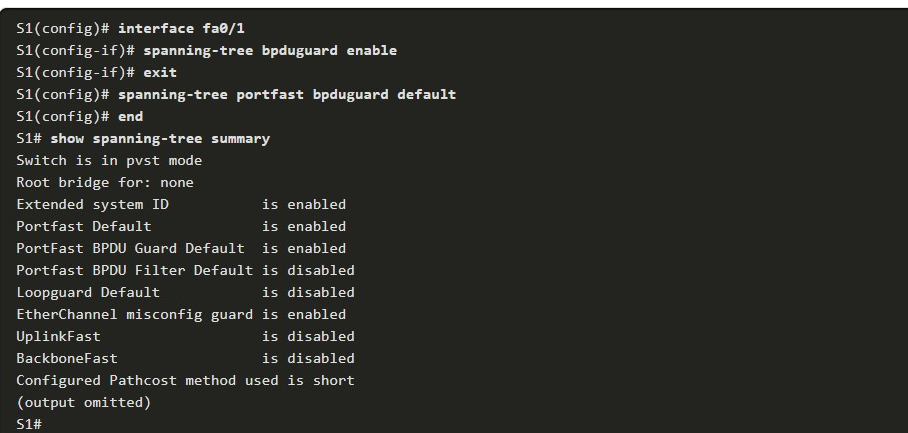
Even though PortFast is enabled, the interface will still listen for BPDUs. Unexpected BPDUs might be accidental, or part of an unauthorized attempt to add a switch to the network.

If any BPDUs are received on a BPDU Guard enabled port, that 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 bpduguard** global command.

BPDU Guard can be enabled on a port by using the **spanning-tree bpduguard enable** interface configuration command. Alternatively, Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on all PortFast-enabled ports.

To display information about the state of spanning tree, use the **show spanning-tree summary** command. In the example, PortFast default and BPDU Guard are both enabled as the default state for ports configured as access mode.

**Note**: Always enable BPDU Guard on all PortFast-enabled ports.

****

11.6.1

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

11.6.2

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

11.6.3

What did I learn in this module?

All switch ports (interfaces) should be secured before the switch is deployed for production use. The simplest and most effective method to prevent MAC address table overflow attacks is to enable port security. By default, Layer 2 switch ports are set to dynamic auto (trunking on). 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. Port security aging can be used to set the aging time for static and dynamic secure addresses on a port. Two types of aging are supported per port: absolute and inactivity. 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 shutdown and placed in the error-disabled state, no traffic is sent or received on that port. To display port security settings for the switch, use the **show port-security** command.

To mitigate VLAN hopping attacks:

**Step 1.** Disable DTP negotiations on non-trunking ports.  
**Step 2.** Disable unused ports.  
**Step 3.** Manually enable the trunk link on a trunking port.  
**Step 4.** Disable DTP negotiations on trunking ports.  
**Step 5.** Set the native VLAN to a VLAN other than VLAN 1.

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. Use the following steps to enable DHCP snooping:

**Step 1.** Enable DHCP snooping.  
**Step 2.** On trusted ports, use the **ip dhcp snooping trust** interface configuration command.  
**Step 3.** Limit the number of DHCP discovery messages that can be received per second on untrusted ports.  
**Step 4.** Enable DHCP snooping by VLAN, or by a range of VLANs.

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.

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.

As a general guideline, configure all access switch ports as untrusted and all uplink ports that are connected to other switches as trusted.

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.

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

* **PortFast** - PortFast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. Apply to all end-user ports. PortFast should only be configured on ports attached to end devices. PortFast bypasses the STP listening and learning states to minimize the time that access ports must wait for STP to converge. If PortFast is enabled on a port connecting to another switch, there is a risk of creating a spanning-tree loop.
* **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. BPDU Guard can be enabled on a port by using the **spanning-tree bpduguard enable** interface configuration command. Alternatively, Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on all PortFast-enabled ports.

1.What is a recommended best practice when dealing with the native VLAN?

Topic 11.2.0 - Port security cannot be enabled on a trunk and trunks are the only types of ports that have a native VLAN. Even though turning DTP off on a trunk is a best practice, it does not have anything to do with native VLAN risks. To prevent security breaches that take advantage of the native VLAN, place the native VLAN in an unused VLAN other than VLAN 1. The management VLAN should also be an unused VLAN that is different from the native VLAN and something other than VLAN 1.



Turn off DTP.



Assign it to an unused VLAN.



Use port security.



Assign the same VLAN number as the management VLAN.

* On what switch ports should PortFast be enabled to enhance STP stability?

Topic 11.5.0 - PortFast will immediately bring an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. If configured on a trunk link, immediately transitioning to the forwarding state could lead to the formation of Layer 2 loops.



only ports that are elected as designated ports



all trunk ports that are not root ports



only ports that attach to a neighboring switch



all end-user ports

* Which command would be best to use on an unused switch port if a company adheres to the best practices as recommended by Cisco?

Topic 11.1.0 - Unlike router Ethernet ports, switch ports are enabled by default. Cisco recommends disabling any port that is not used. The **ip dhcp snooping** command globally enables DHCP snooping on a switch. Further configuration allows defining ports that can respond to DHCP requests. The **switchport port-security** command is used to protect the network from unidentified or unauthorized attachment of network devices.



**shutdown**



**switchport port-security mac-address sticky** *mac-address*



**ip dhcp snooping**



**switchport port-security mac-address sticky**



**switchport port-security violation shutdown**

* Which two features on a Cisco Catalyst switch can be used to mitigate DHCP starvation and DHCP spoofing attacks? (Choose two.)

Topic 11.3.0 - In DHCP starvation attacks, an attacker floods the DHCP server with DHCP requests to use up all the available IP addresses that the DHCP server can issue. In DHCP spoofing attacks, an attacker configures a fake DHCP server on the network so that it provides clients with false DNS server addresses. The port security feature can limit the number of dynamically learned MAC addresses per port or allow only known valid NICs to be connected via their specific MAC addresses. The DHCP snooping feature can identify the legitimate DHCP servers and block fake DHCP servers from issuing IP address information. These two features can help fight against DHCP attacks.



strong password on DHCP servers



port security



DHCP snooping



DHCP server failover



extended ACL

* What is the best way to prevent a VLAN hopping attack?

Topic 11.2.0 - VLAN hopping attacks rely on the attacker being able to create a trunk link with a switch. Disabling DTP and configuring user-facing ports as static access ports can help prevent these types of attacks.  Disabling the Spanning Tree Protocol (STP) will not eliminate VLAN hopping attacks.



Use ISL encapsulation on all trunk links.



Use VLAN 1 as the native VLAN on trunk ports.



Disable STP on all nontrunk ports.



Disable trunk negotiation for trunk ports and statically set nontrunk ports as access ports.

* Which procedure is recommended to mitigate the chances of ARP spoofing?

Topic 11.4.0 - To mitigate the chances of ARP spoofing, these procedures are recommended:

* + Implement protection against DHCP spoofing by enabling DHCP snooping globally.
  + Enable DHCP snooping on selected VLANs.
  + Enable DAI on selected VLANs.
  + Configure trusted interfaces for DHCP snooping and ARP inspection. Untrusted ports are configured by default.​



Enable IP Source Guard on trusted ports.



Enable DHCP snooping on selected VLANs.



Enable port security globally.



Enable DAI on the management VLAN.

* What are two types of switch ports that are used on Cisco switches as part of the defense against DHCP spoofing attacks? (Choose two.)

Topic 11.3.0 - DHCP snooping recognizes two types of ports on Cisco switches:

* + Trusted DHCP ports – switch ports connecting to upstream DHCP servers
  + Untrusted ports – switch ports connecting to hosts that should not be providing DHCP server messages



trusted DHCP port



established DHCP port



authorized DHCP port



unknown port



unauthorized port



untrusted port

* Which two commands can be used to enable PortFast on a switch? (Choose two.)

Topic 11.5.0 - PortFast can be configured on all nontrunking ports using the **spanning-tree portfast default** global configuration command. Alternatively, PortFast can be enabled on an interface using the **spanning-tree portfast** interface configuration command.



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



S1(config-line)# **spanning-tree portfast**



S1(config-if)# **enable spanning-tree portfast**



S1(config-if)# **spanning-tree portfast**



S1(config)# **enable spanning-tree portfast default**

* An administrator who is troubleshooting connectivity issues on a switch notices that a switch port configured for port security is in the err-disabled state. After verifying the cause of the violation, how should the administrator re-enable the port without disrupting network operation?

Topic 11.1.0 - If an interface that has been protected with port security goes into the err-disabled state, then a violation has occurred and the administrator should investigate the cause of the violation. Once the cause is determined, the administrator can issue the **shutdown** command followed by the **no shutdown** command to enable the interface.



Issue the **no switchport port-security** command, then re-enable port security.



Reboot the switch.



Issue the **shutdown** command followed by the **no shutdown** command on the interface.



Issue the **no switchport port-security violation shutdown** command on the interface.

* A network administrator is configuring DHCP snooping on a switch. Which configuration command should be used first?

Topic 11.3.0 - The steps to enable DHCP snooping include these:

* + **Step 1**. Enable DHCP snooping using the **ip dhcp snooping** global configuration command.
  + **Step 2**. On trusted ports, use the **ip dhcp snooping trust** interface configuration command.
  + **Step 3**. Enable DHCP snooping by VLAN, or by a range of VLANs.



**ip dhcp snooping vlan**



**ip dhcp snooping trust**



**ip dhcp snooping**



**ip dhcp snooping limit rate**

* A network administrator is configuring DAI on a switch with the command **ip arp inspection validate dst-mac**. What is the purpose of this configuration command?

Topic 11.4.0 - DAI can 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 the 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.



to check the destination MAC address in the Ethernet header against the target MAC address in the ARP body



to check the destination MAC address in the Ethernet header against the user-configured ARP ACLs



to check the destination MAC address in the Ethernet header against the source MAC address in the ARP body



to check the destination MAC address in the Ethernet header against the MAC address table

* Which security feature should be enabled in order to prevent an attacker from overflowing the MAC address table of a switch?

Topic 11.1.0 - Port security limits the number of source MAC addresses allowed through a switch port. This feature can prevent an attacker from flooding a switch with many spoofed MAC addresses.



storm control



root guard



BPDU filter



port security

* What Layer 2 attack is mitigated by disabling Dynamic Trunking Protocol?

Topic 11.2.0 - Mitigating a VLAN hopping attack can be done by disabling Dynamic Trunking Protocol (DTP) and by setting the native VLAN of trunk links to VLANs not in use.



VLAN hopping



ARP poisoning



ARP spoofing



DHCP spoofing

* A network administrator is configuring DAI on a switch. Which command should be used on the uplink interface that connects to a router?

Topic 11.4.0 - In general, a router serves as the default gateway for the LAN or VLAN on the switch. Therefore, the uplink interface that connects to a router should be a trusted port for forwarding ARP requests.



**ip arp inspection trust**



**ip dhcp snooping**



**spanning-tree portfast**



**ip arp inspection vlan**

* Where are dynamically learned MAC addresses stored when sticky learning is enabled with the **switchport port-security mac-address sticky** command?

Topic 11.1.0 - When MAC addresses are automatically learned by using the **sticky** command option, the learned MAC addresses are added to the running configuration, which is stored in RAM.



ROM



NVRAM



flash



RAM