CCNA 2 v7.0 Curriculum: Module 11 – Switch Security Configuration

itexamanswers.net/ccna-2-v7-0-curriculum-module-11-switch-security-configuration.html

June 6, 2020

11.0 Introduction

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.

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.

Topic Title	Topic Objective
Mitigate STP Attacks	Explain how to configure PortFast and BPDU Guard to mitigate STP attacks.

11.1 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.

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

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

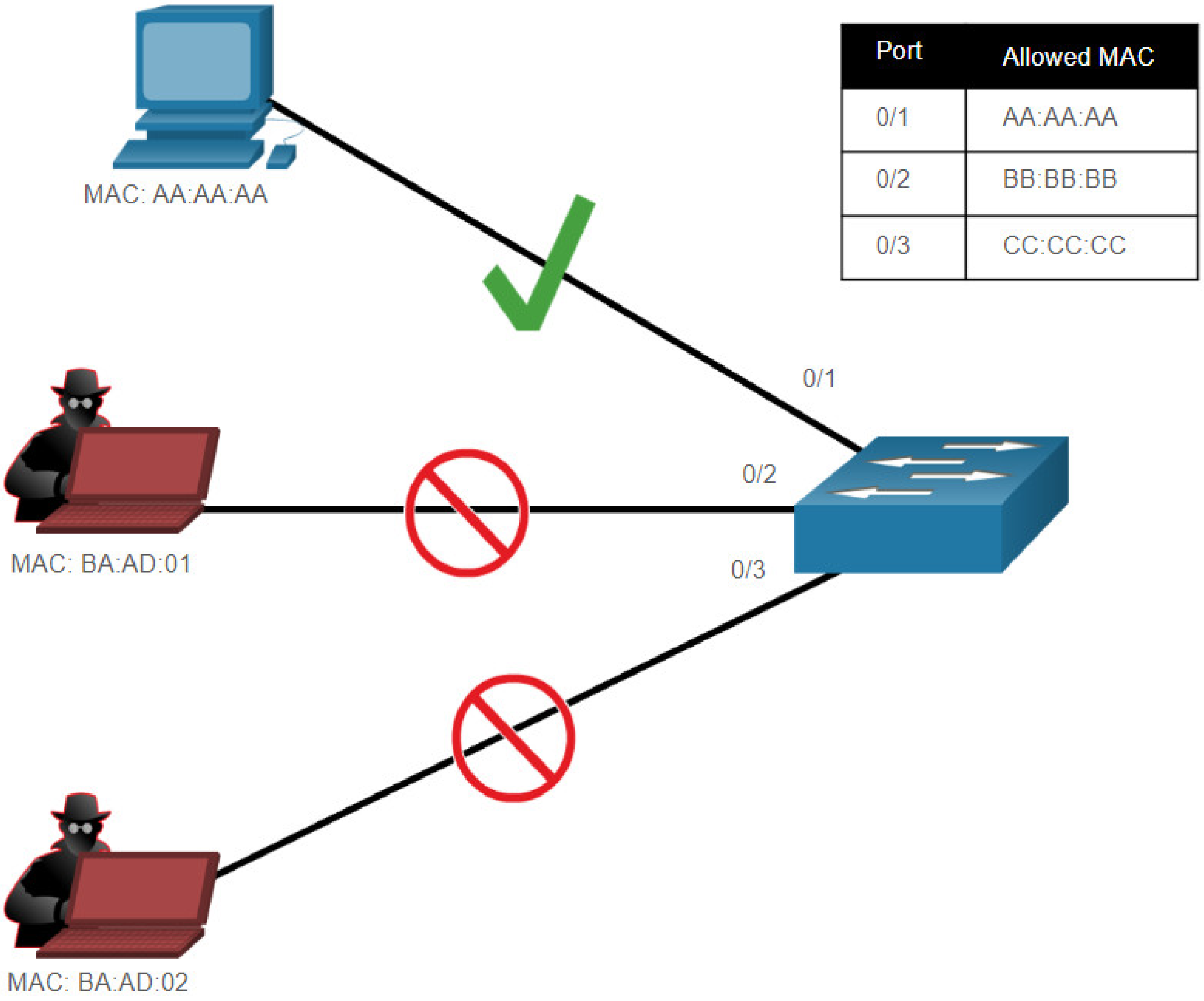
```
S1(config)# interface range fa0/8 - 24
S1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
(output omitted)
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#
```

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.



Port	Allowed MAC
0/1	AA:AA:AA
0/2	BB:BB:BB
0/3	CC:CC:CC

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.

```
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#
```

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, 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.

```
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#
```

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.

```
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
```

11.1.4 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
```

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 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:

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

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. 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#
```

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.

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

The parameters for the command are described in the table.

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.

```
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
```

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.

```
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#
```

11.1.7 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.

```
*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
```

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**. The Security Violation counter increments by 1.

```
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#
```

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 to make the port operational, as shown in the example.

```
S1(config)# interface fa0/18
S1(config-if)# shutdown
*Sep 20  07:11:18.845: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
S1(config-if)# no shutdown
*Sep 20  07:11:32.006: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to
up
*Sep 20  07:11:33.013: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/18, changed state to up
S1(config-if)#
```

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 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#
```

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.

```
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 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.

```
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 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.

```
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#
```

11.1.9 Syntax Checker – Implement Port Security

Implement port security for a switch interface based on the specified requirements

You are currently logged into S1. Configure FastEthernet 0/5 for port security by using the following requirements:

- Use the interface name fa0/5 to enter interface configuration mode.
- Enable the port for access mode.
- Enable port security.
- Set the maximum number of MAC address to 3.
- Statically configure the MAC address aaaa.bbbb.1234.
- Configure the port to dynamically learn additional MAC addresses and dynamically add them to the running configuration.
- Return to privileged EXEC mode.

```
S1(config)#interface fa0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#end
```

Enter the command to verify port security for all interfaces.

```
S1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/5              3            2                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

Enter the command to verify port security on FastEthernet 0/5. Use fa0/5 for the interface name.

```
S1#show port-security interface fa0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0090.2135.6B8C:1
Security Violation Count   : 0
```

Enter the command that will display all of the addresses to verify that the manually configured and dynamically learned MAC addresses are in the running configuration.

```
S1#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
   1    0090.2135.6b8c    SecureSticky                  Fa0/5        -
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/5        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

You have successfully configured and verified port security for the interface.
```

11.1.10 Packet Tracer – Implement Port Security

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

11.1.10 Packet Tracer – Implement Port Security

11.2 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 0/24 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.

```
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#
```

- 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.

11.2.3 Syntax Checker – Mitigate VLAN Hopping Attacks

Mitigate VLAN hopping attacks on the switch based on the specified requirements.

You are currently logged into S1. The ports status of the ports are as follows:

- FastEthernet ports 0/1 through 0/4 are used for trunking with other switches.
- FastEthernet ports 0/5 through 0/10 are unused.
- FastEthernet ports 0/11 through 0/24 are active ports currently in use.

Use range fa0/1 – 4 to enter interface configuration mode for the trunks.

```
S1(config)#interface range fa0/1 - 0/4
```

Configure the interfaces as nonnegotiating trunks assigned to default VLAN 99.

```
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport nonegotiate
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)# exit
```

Use range fa0/5 – 10 to enter interface configuration mode for the trunks.

```
S1(config)#interface range fa0/5 - 10
```

Configure the unused ports as access ports, assign them to VLAN 86, and shutdown the ports.

```
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 86
% Access VLAN does not exist. Creating vlan 86
S1(config-if-range)#shutdown
\*Mar  1 00:28:48.883: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down
\*Mar  1 00:28:48.900: %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down
\*Mar  1 00:28:48.908: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to
administratively down
\*Mar  1 00:28:48.917: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down
\*Mar  1 00:28:48.942: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to
administratively down
\*Mar  1 00:28:48.950: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down
\*Mar  1 00:28:49.890: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/5, changed state to down
\*Mar  1 00:28:49.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/6, changed state to down
S1(config-if-range)# exit
```

Use range fa0/11 – 24 to enter interface configuration mode for the active ports and then configure them to prevent trunking.

```
S1(config)#interface range fa0/11 - 24
S1(config-if-range)#switchport mode access
S1(config-if-range)# end
S1#

You have successfully mitigated VLAN hopping attacks on this switch.
```

11.3 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.

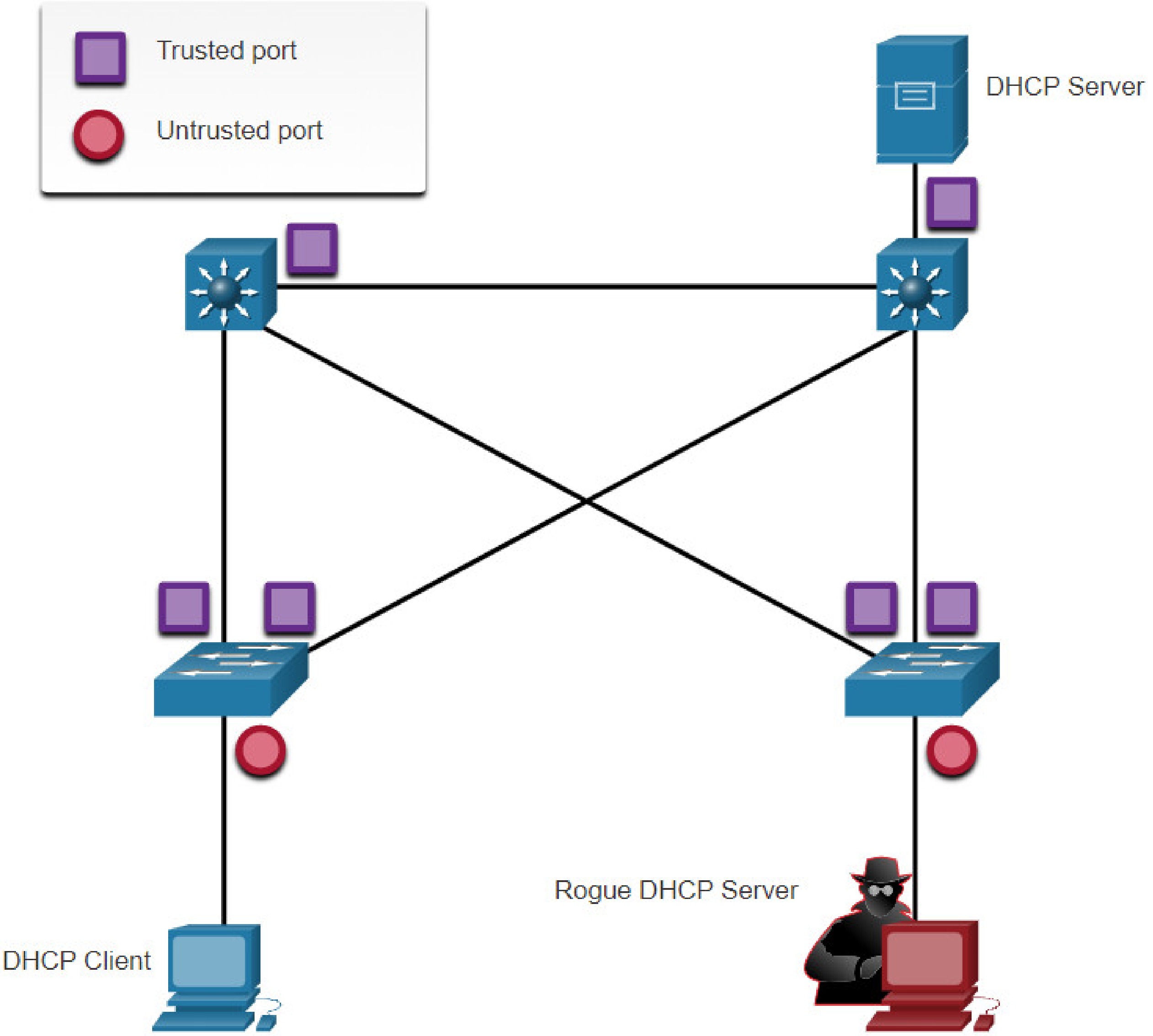
However, mitigating DHCP spoofing attacks requires more protection. Gobbler could be configured to use the actual interface MAC address as the source Ethernet address, but specify a different Ethernet address in the DHCP payload. This would render port security ineffective because the source MAC address 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 rouge 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.

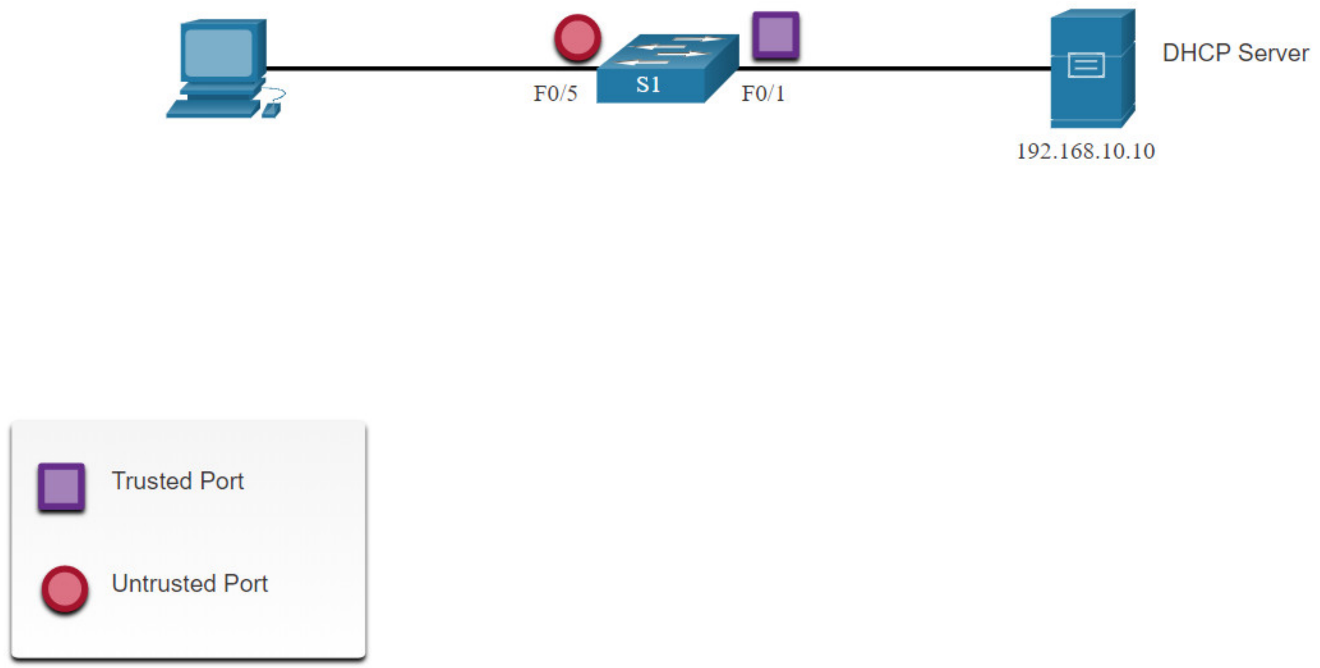
Step 2. On trusted ports, use the **ip dhcp snooping trust** interface configuration command.

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 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.

```
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#
```

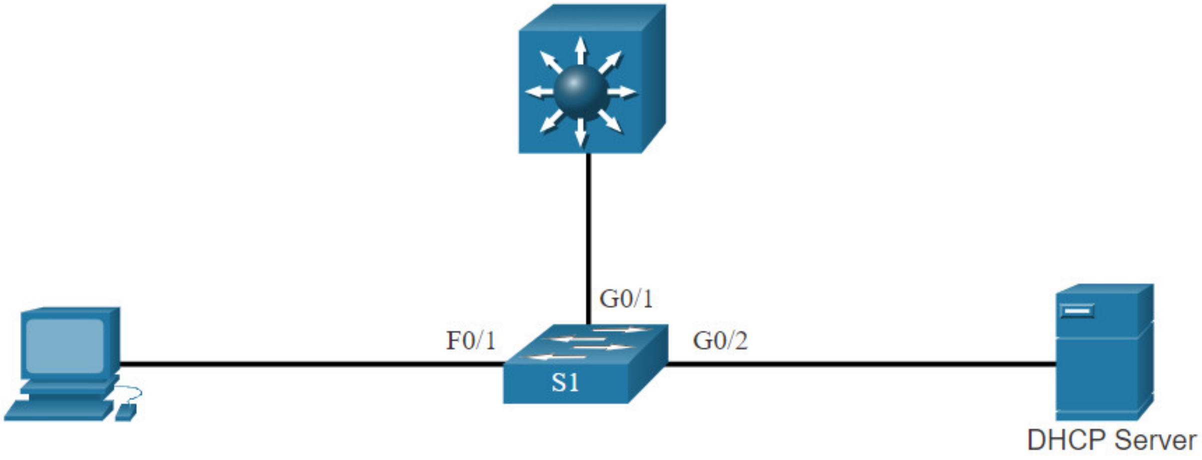
Use the **show ip dhcp snooping** privileged EXEC command to verify DHCP snooping and **show ip dhcp snooping binding** to view the clients that have received DHCP information, as shown in the example.

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

```
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
```

11.3.5 Syntax Checker – Mitigate DHCP Attacks

Implement DHCP snooping for a switch based on the following topology and specified requirements.



You are currently logged into S1. Enable DHCP snooping globally for the switch.

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

Enter interface configuration mode for g0/1 – 2, trust the interfaces, and return to global configuration mode.

```
S1(config)#interface range g0/1 - 2
S1(config-if-range)#ip dhcp snooping trust
S1(config-if-range)#exit
```

Enter interface configuration mode for f0/1 – 24, limit the DHCP messages to no more than 10 per second, and return to global configuration mode.

```
S1(config)#interface range f0/1 - 24
S1(config-if-range)#ip dhcp snooping limit rate 10
S1(config-if-range)#exit
```

Enable DHCP snooping for VLANs 10,20,30-49.

```
S1(config)#ip dhcp snooping vlan 10,20,30-49
S1(config)# exit
```

Enter the command to verify DHCP snooping.

```
S1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20,30-49
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)
-----------------------    -------    ------------    ----------------
GigabitEthernet0/1          yes        yes             unlimited
  Custom circuit-ids:
GigabitEthernet0/2          yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/1             no         no              10
  Custom circuit-ids:
```

Enter the command to verify the current DHCP bindings logged by DHCP snooping

```
S1#show ip dhcp snooping binding
MacAddress         IpAddress        Lease(sec) Type          VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:03:47:B5:9F:AD  10.0.0.10        193185     dhcp-snooping 5    FastEthernet0/1
S1#

You have successfully configured and verified DHCP snooping for the switch.
```

11.4 Mitigate ARP Attacks

11.4.1 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.

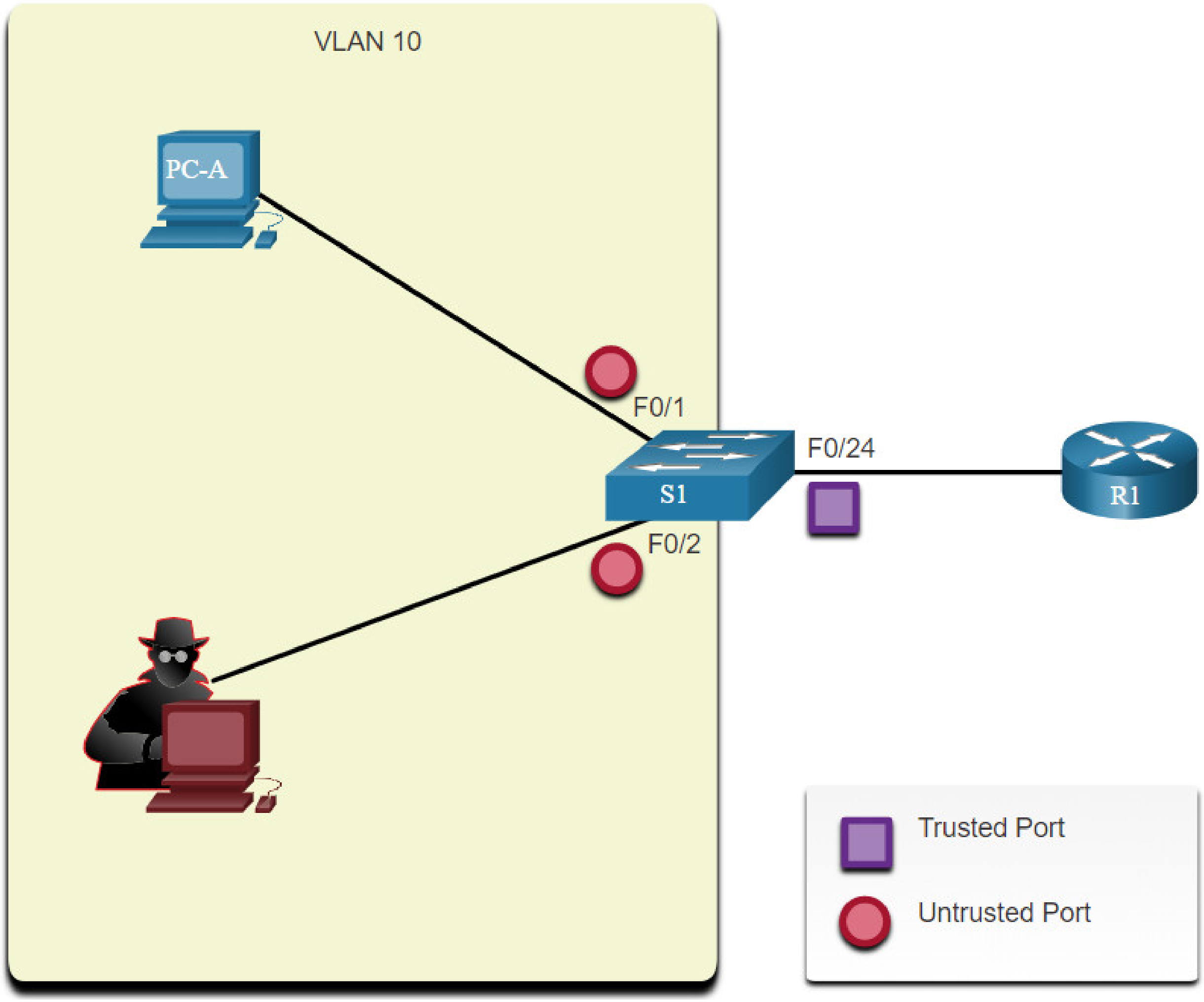
11.4.2 DAI Implementation Guidelines

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.



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.

```
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 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.

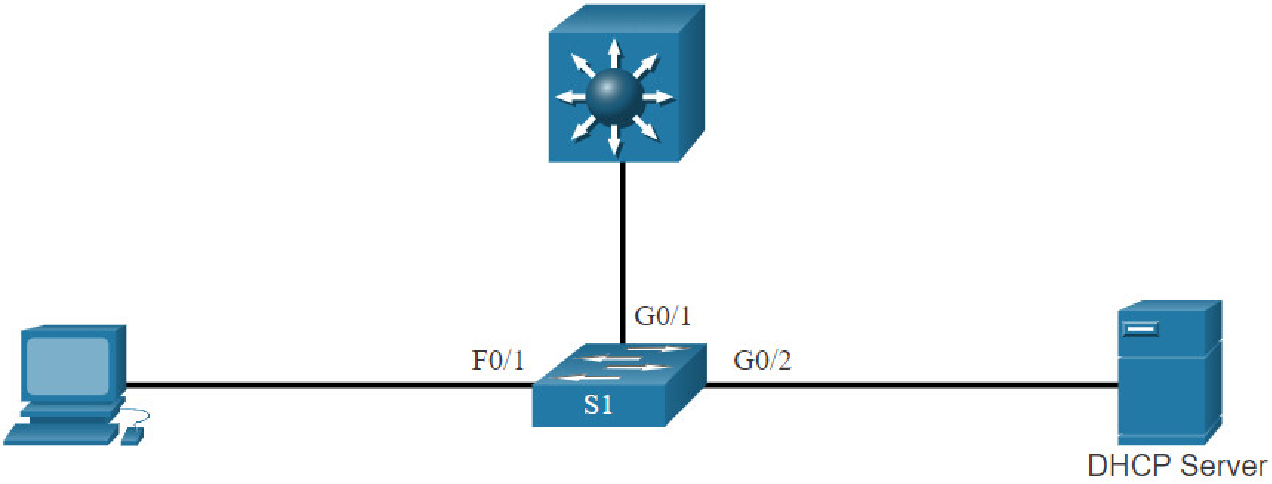
- **Source MAC** – Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.
- **IP address** – Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

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.

```
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)#
```

11.4.4 Syntax Checker – Mitigate ARP Attacks

Implement DAI for a switch based on the following topology and specified requirements.



You are currently logged into S1. Enable DHCP snooping globally for the switch.

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

Enter interface configuration mode for g0/1 – 2, trust the interfaces for both DHCP snooping and DAI, and then return to global configuration mode.

```
S1(config)#interface range g0/1 - 2
S1(config-if-range)#ip dhcp snooping trust
S1(config-if-range)#ip arp inspection trust
S1(config-if-range)#exit
```

Enable DHCP snooping and DAI for VLANs 10,20,30-49.

```
S1(config)#ip dhcp snooping vlan 10,20,30-49
S1(config)#ip arp inspection vlan 10,20,30-49
S1(config)#

You have successfully configured DAI for the switch.
```

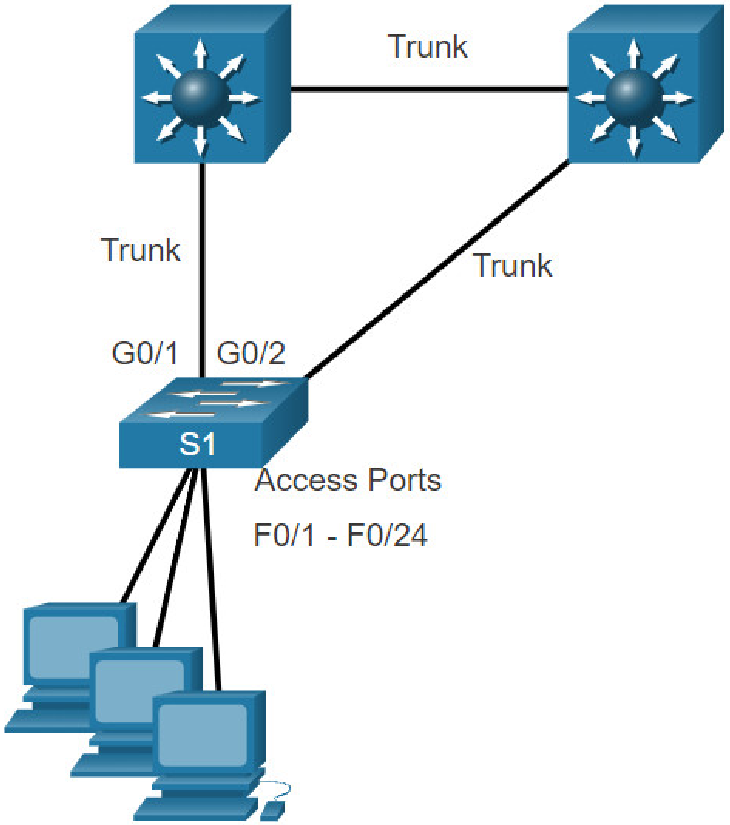
11.5 Mitigate STP Attacks

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 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.
- **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.



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.

```
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
S1# show running-config | begin span
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
(output omitted)
S1#
```

11.5.3 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 psecure_violation** 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.

```
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#
```

11.5.4 Syntax Checker – Mitigate STP Attacks

Implement PortFast and BPDU Guard for a switch based on the following topology and specified requirements

You are currently logged into S1. Complete the following steps to implement PortFast and BPDU Guard on all access ports:

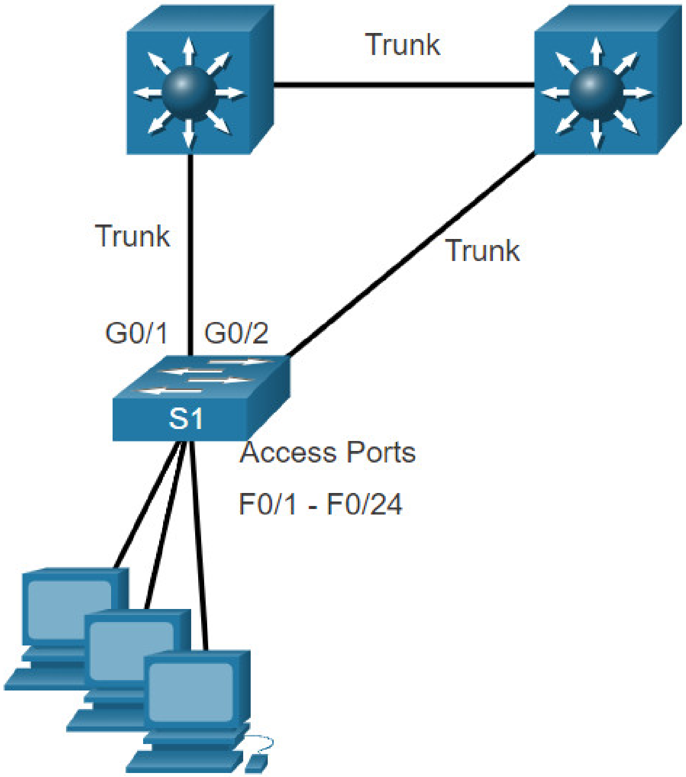
- Enter interface configuration mode for fa0/1 – 24.
- Configure the ports for access mode.
- Return to global configuration mode.
- Enable PortFast by default for all access ports.
- Enable BPDU Guard by default for all access ports.

```
S1(config)#interface range fa0/1 - 24
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
S1(config)#spanning-tree portfast default
S1(config)#spanning-tree portfast bpduguard default
S1(config)# exit
```

Verify that PortFast and BPDU Guard is enabled by default by viewing STP summary information.

```
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#

You have successfully configured and
verified PortFast and BPDU Guard for
the switch.
```



11.6 Module Practice and Quiz

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

11.6.1 Packet Tracer – 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

11.6.2 Lab – 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.

11.6.4 Module Quiz – Switch Security Configuration

Download Slide Powerpoint (PPT)

PPT

CCNA 2 v7.0 Curriculum: Module 11 - Switch Security Configuration.pptx

1 file(s) 1.50 MB

Download

Tags:ccna 2 v7 modules