

## Lab 10.2.4 Mitigate Layer 2 Attacks

### Objective

In this lab, the students will complete the following tasks:

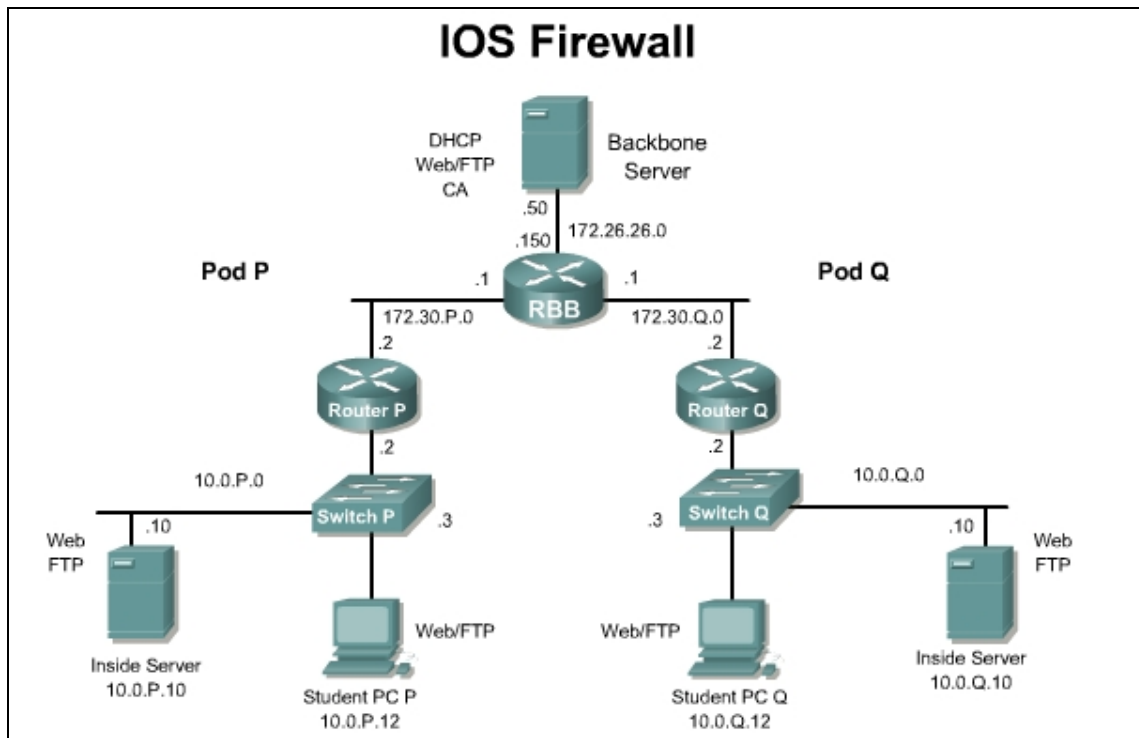
- Mitigate against CAM table overflow attack with appropriate Cisco IOS commands.
- Mitigate against MAC spoofing attacks with appropriate Cisco IOS commands.
- Mitigate against DHCP starvation attacks with appropriate Cisco IOS commands.

### Scenario

The XYZ Company has a number of 2950 switches that are deployed throughout the building in order to provide network access for the employees. Attacks that use Layer 2 of the OSI model are quickly gaining sophistication and popularity. The network administrator must mitigate the effects of these attacks as much as possible.

### Topology

This figure illustrates the lab network environment.



### Preparation

Begin with the standard lab topology and verify the starting configuration on the pod switch. Access the pod switch console port using the terminal emulator on the Windows 2000 server. If desired, save the switch configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

## Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- A second PC to be used to test the configuration

## Command List

In this lab exercise, the following switch commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

### Switch Commands

Command	Description
<code>arp timeout <i>seconds</i></code>	To configure how long an entry remains in the Address Resolution Protocol (ARP) cache, use the <b>arp timeout</b> command in interface configuration mode. To restore the default value, use the <b>no</b> form of this command.
<code>show port-security [<i>address</i>] [<i>interface interface-id</i>]</code>	To display the port security settings for an interface or for the switch, use the <b>show port-security</b> command.
<code>switchport port-security</code>	Enables port security on the interface.
<code>switchport port-security mac-address <i>mac-addr</i></code>	To set the maximum number of secure MAC addresses on an interface, use the <b>switchport-port-security mac-address</b> command. Use the <b>no</b> form of this command to remove a MAC address from the list of secure MAC addresses.
<code>switchport port-security maximum <i>max-addr</i></code>	Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 128; the default is 128.
<code>switchport port-security violation {<i>shutdown</i>   <i>restrict</i>   <i>protect</i>}</code>	Set the security violation mode for the interface.
<code>ip dhcp snooping</code>	Enables DHCP snooping globally.
<code>ip dhcp snooping vlan <i>vlan_id</i> {<i>,vlan_id</i>}</code>	Enable DHCP snooping on a VLAN or range of VLANs. A single VLAN can be identified by VLAN ID number, or start and end VLAN IDs can be used to specify a range of VLANs. The range is 1 to 4094.
<code>ip dhcp snooping trust</code>	Configure the interface as trusted or untrusted. The default is untrusted.
<code>ip dhcp snooping limit rate <i>rate</i></code>	Configure the number of DHCP packets per second than an interface can receive. The range is 1 to 4294967294. The default is no rate limit configured.

## Step 1 Mitigate the CAM Table Overflow Attack

Complete the following steps to mitigate against CAM table overflow attack with appropriate Cisco IOS commands:

---

<b>Note</b>	The enable secret password for the pod switch is <b>cisco</b> .
-------------	---

---

- a. Enter the interface configuration mode for port FastEthernet 0/12

```
SwitchP(config)#interface fastEthernet 0/12  
SwitchP(config-if)#
```

(Where P = pod number)

- b. Set the port mode to access.

```
SwitchP(config-if)# switchport mode access
```

- c. Enable port security on the selected interface.

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

- d. Configure the maximum number of MAC addresses that can be configured or learned on this port. The default is 1.

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

- e. Configure an action to be taken when a violation occurs. The default is shutdown.

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

1. What other options are available for actions to be taken when a violation to occur?
- 

- f. Record the MAC address of the student PC for use in the next step. For example, **0000.ffff.1111**

- g. Configure a static MAC address entry for the device that will be attached to the port.

```
SwitchP(config-if)# switchport port-security mac-address  
0000.ffff.1111
```

- h. Plug the student PC into the port Fa0/12 and try to ping the gateway.

```
C:\WINNT\system32>ping 10.0.P.2
```

1. Was the ping successful?
- 

- i. Return to privileged EXEC mode.

```
SwitchP(config-if)# end  
SwitchP#
```

- j. Verify the port security settings for port Fa0/12.

```
SwitchP# show port-security interface fastEthernet 0/12  
  
Port Security                : Enabled  
Port Status                   : Secure-up  
Violation Mode                : Shutdown  
Aging Time                    : 0 mins  
Aging Type                    : Absolute  
SecureStatic Address Aging    : Disabled  
Maximum MAC Addresses         : 1  
Total MAC Addresses           : 1  
Configured MAC Addresses      : 1  
Sticky MAC Addresses          : 0
```

```
Last Source Address      : 0000.0000.0000
Security Violation Count : 0
```

- k. Verify that the MAC address of the student PC is configured as a secure address.

```
SwitchP# show port-security address
```

```
Secure Mac Address Table
```

```
-----
Vlan    Mac Address      Type                Ports    Remaining Age
        (mins)
-----
30P     0000.ffff.1111   SecureConfigured   Fa0/12   -
-----

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

1. What address type is shown for the MAC address of the student PC?
- 

## Step 2 Mitigate MAC Spoofing Attacks

Complete the following steps to mitigate against CAM table overflow attack with appropriate Cisco IOS commands.

- a. Enter the interface configuration mode for port FastEthernet 0/12

```
SwitchP(config)# interface fastEthernet 0/12
SwitchP(config-if)#
```

(Where P = pod number)

- b. Configure the maximum number of MAC addresses that can be configured or learned on this port.

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

- c. Configure an action to be taken when a violation occurs.

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

- d. Specify an ARP timeout of ten seconds. The default is four minutes.

```
SwitchP(config-if)# arp timeout 10
```

- e. Unplug the student PC from port Fa 0/12. Plug another PC that does not have the correct MAC address into port Fa 0/12.

- f. Return to privileged EXEC mode.

```
SwitchP(config-if)# end
SwitchP#
```

- g. Use the following commands to verify that the interface Fa 0/12 is shut down due to a security violation.

```
SwitchP# show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/12	1	1	1	Shutdown

```
-----  
Total Addresses in System (excluding one mac per port)      : 0  
Max Addresses limit in System (excluding one mac per port) : 1024  
SwitchP# show port-security interface fastEthernet 0/12
```

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	: 0000.ffff.2222
Security Violation Count	: 1

2. What state is the port in after the security violation occurs?

```
SwitchP# show interfaces status err-disabled
```

Port	Name	Status	Reason
Fa0/12		err-disabled	psecure-violation

### Step 3 Mitigate DHCP Starvation Attacks

Complete the following steps to mitigate against DHCP starvation attacks with appropriate Cisco IOS commands.

- a. Enable DHCP snooping globally.

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

- b. Enable DHCP snooping on VLAN 301.

```
SwitchP(config)# ip dhcp snooping vlan 301
```

- c. Switch to interface configuration mode for interface Fa 0/12.

```
SwitchP(config)# interface fastEthernet 0/12
```

- d. Configure the interface as trusted. The **no** keyword can be used to configure an interface to receive messages from an untrusted client. The default is untrusted.

```
SwitchP(config-if)# ip dhcp snooping trust
```

- e. Configure the number of DHCP packets per second than an interface can receive to be 100. The default is no rate limit configured.

```
SwitchP(config-if)# ip dhcp snooping limit rate 100
```

1. What is the range of DHCP packets per second that can be configured on the interface?
- 

- h. Return to privileged EXEC mode.

```
SwitchP(config-if)# end  
SwitchP#
```

- f. Verify the DHCP snooping configuration.

```
SwitchP# show ip dhcp snooping
```

```
Switch DHCP snooping is enabled
```

```
DHCP snooping is configured on following VLANs:
```

```
301
```

```
Insertion of option 82 is enabled
```

Interface	Trusted	Rate limit (pps)
-----	-----	-----
FastEthernet0/12	yes	100