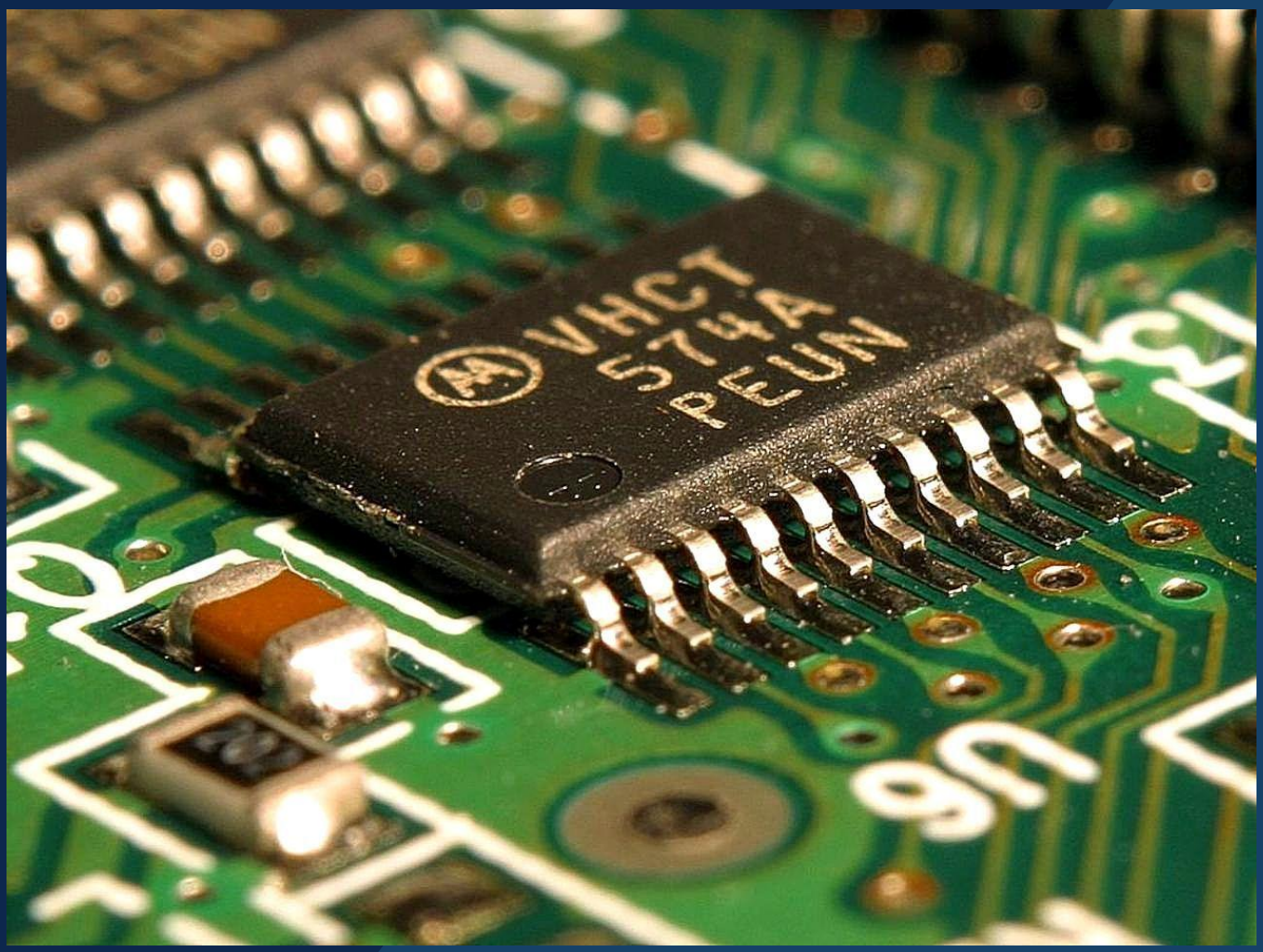


Networking Academy:
Layer 2 Attacks: Prevention & Execution

Hunter Zhuang

Contents

Purpose

The purpose of this lab is to perform three layer 2 attacks to understand them. Then to discover how to prevent and mitigate these attacks. This lab's purpose is to demonstrate practices that can prevent a network from being attacked from layer 2. The following attacks have been performed CAM table overflow, DHCP starvation, VLAN hopping, ARP spoofing.
Configurations of devices are available at the end of this document.

Background

Layer 2 attacks are attacks that are performed on the data link layer of the OSI model. This generally means that attacks are performed on Ethernet. These attacks are often done to disable the network, deny users access to the network, or obtain passwords and usernames. Another characteristic of these attacks is that they often manipulate frame data to take advantage of the common behaviors of layer 2 networks.

One layer 2 attack is MAC Flooding. This attack is performed on a switch, which takes advantage of the switch's switching behavior. When a switch receives a frame with a MAC address that it doesn't recognize, it will send that frame out all its ports. Because of this behavior when the switch's CAM table is full, it will flood out most frames that are sent through it because there will be no space for any MAC addresses to be learned in the CAM table. So, by filling the CAM table, the switch floods traffic out its ports, allowing anyone connected to the switch to read the data sent through the switch. The best way to prevent an attack like this is to limit the number of MAC addresses a port can learn with port-security. This way the CAM table can't be flooded.

Another layer 2 attack is VLAN hopping. This works by taking advantage of DTP, which is often on by default on many switches. A host can perform an attack like this by negotiating to trunk the switch port that it is connected to. By trunking the port it's connected to, the host can send frames that are tagged with a specific VLAN, allowing it to reach VLANs that it shouldn't be able to reach. This attack can be prevented by configuring all host ports to statically be access ports.

DHCP starvation is an attack performed to starve IP addresses from the DHCP server on the network. The host does this by sending many DHCP discover packets with random MAC addresses to the DHCP server. This causes the DHCP server to try to lease out all its addresses, which leaves none for any real users. This attack can be prevented by setting the maximum number of MAC addresses a port can learn to port security and by DHCP Snooping. DHCP snooping is used to prevent rogue DHCP servers by configuring a trusted port where the real DHCP server is, but that isn't the feature that prevents DHCP starvation. The feature that can be configured is to have DHCP snooping verify that the mac address in the DHCP packets match the DHCP address learned on the port. This prevents false DHCP discover packets from reaching the DHCP server, starving it of its addresses.

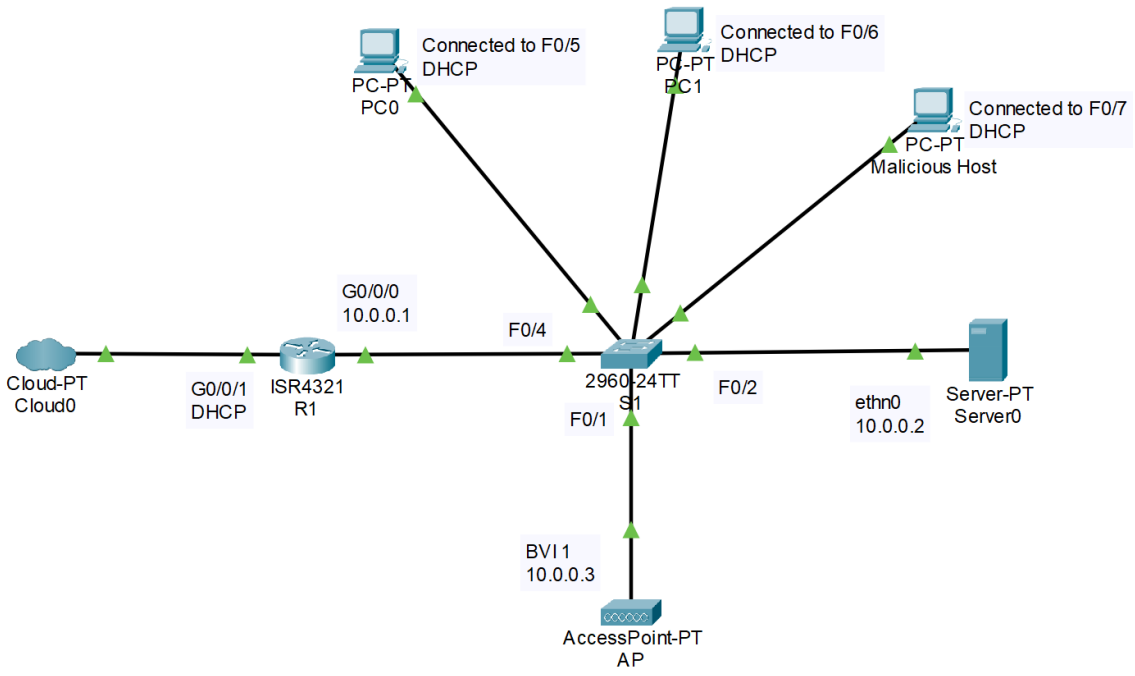
ARP spoofing is a layer two attack that uses ARP frames to just lie to hosts. A host can tell other hosts that it has an IP that it doesn't have using gratuitous ARPs (GARPs), ARPs messages that are broadcast to every host on a local network. This way hosts on the switch when sending a packet to an IP will use the spoofed MAC address. Malicious hosts can send attacks to intercept traffic between two hosts. This attack can be prevented using dynamic ARP inspection (DAI). DAI can disable gratuitous ARPs and prevent false ARP packets from being sent out on the switch. This way DAI can stop ARP spoofing attacks.

Lab Summary

In this lab, three layer 2 attacks were performed: MAC flooding, DHCP starvation & VLAN hopping, and ARP spoofing. These attacks were performed on a common office network with an access point, a switch, and a router. This report details how to perform these attacks as well as mitigate each of these attacks in their respective sections. Further information on setup for this lab is available here: https://github.com/101zh/Layer2AttacksLab.

Note: a VLAN other than VLAN 1 should be used as the native VLAN to further mitigate VLAN hopping attacks, but it is not configured here.

Network Diagram with IPs



Lab Commands

- **`interface`** {*`type slot/port`*}
  - **`switchport port-security maximum`** [`number-of-addresses`]
    - Sets the maximum number of mac-addresses a port can learn
  - **`switchport mode access`**
    - Sets the interface to a non-trunking VLAN layer 2 interface
  - **`switchport access vlan`** [*`vlan-number`*]
    - Sets the VLAN the interface operates in for access mode
  - **`ip dhcp snooping trust`**

        - Configures the specified interface to be a trusted interface. By default, interfaces are not trusted. Usually, interfaces that are configured as trusted are the interface closest to the DHCP server.
    - **`switchport port-security`**
        - Enables port security on the specified interface
    - **`switchport port-security aging time`** [*`time`*]
        - Sets the time for which a mac-address is remembered as a secure address.
    - **`switchport port-security aging type {absolute | inactivity}`**
        - Sets the type of aging the port will use. The type of inactivity sets it so that the mac-addresses are forgotten after a period of inactivity specified by the aging time. The type of absolute, which is default, will forget a mac-address in the specified aging time after it was learned.
    - **`switchport port-security mac-address`** {*`mac-addr`* | **`sticky`**}
        - Specifies the secure mac-addresses. Addresses can be statically set or by using the keyword "sticky," mac-addresses can be dynamically learned.
    - **`switchport nonegotiate`**
        - Statically sets the specified interface to not use Dynamic Trunking Protocol (DTP)
- **`ip dhcp snooping`**
    - Enables DHCP snooping globally in the switch
- **`ip dhcp snooping verify mac-address`**
    - Configures the switch to verify that the mac-address learned on the port matches the mac-address field in DHCP packets
- **`ip arp inspection vlan`** [*`vlan-number1 … vlan-number8`*]
    - Enables dynamic ARP inspection (DAI) on the specified VLANs
- **`ip arp inspection validate`** {`dst-mac | src-mac`}
    - Validates the ARP frames that go through the switch. The two options configure DAI to compare the ethernet mac-addresses of the destination and source to the ARP body, respectively.
- **`ip arp gratuitous none`**
    - Rejects gratuitous ARPs.

Prevention and Execution of MAC Flooding

Prevention

Useful interface configuration commands:

- **`switchport port-security maximum`** [*`number-of-addresses`*]
- **`switchport port-security`**
- **`switchport port-security aging time`** [*`time`*]
- **`switchport port-security aging type`** {**`absolute | inactivity`**}
- **`switchport port-security mac-address`** {*`mac-addr`* | **`sticky`**}

Execution

Setup

1. Setup your local topology
2. Install the required software for this attack
    - Have a Linux machine or a linux virtual machine (VM).
    - install the software on the machine
      ```
      ~$ sudo apt install dsniff
      ```

Flood MAC Addresses

1. Run attack in the terminal
   ```
   ~$ sudo macof -i <interface-name>
   # For example: sudo macof -i eth0
   ```
2. Use "Control-C" to exit the program
3. All traffic is now flooded out the switch, so you can now view all traffic that goes through the switch in Wireshark.

Prevention and Execution of DHCP Starvation & VLAN Hopping

Prevention

Useful global configuration commands:

- **`ip dhcp snooping`**
- **`ip dhcp snooping verify mac-address`**

Useful interface configuration commands:

- **`switchport port-security maximum`** [*`number-of-addresses`*]
- **`switchport port-security`**
- **`switchport mode access`**
- **`switchport access vlan`** [*`vlan-number`*]
- **`ip dhcp snooping trust`**
- (Note: by default, all interfaces are untrusted in DHCP snooping)

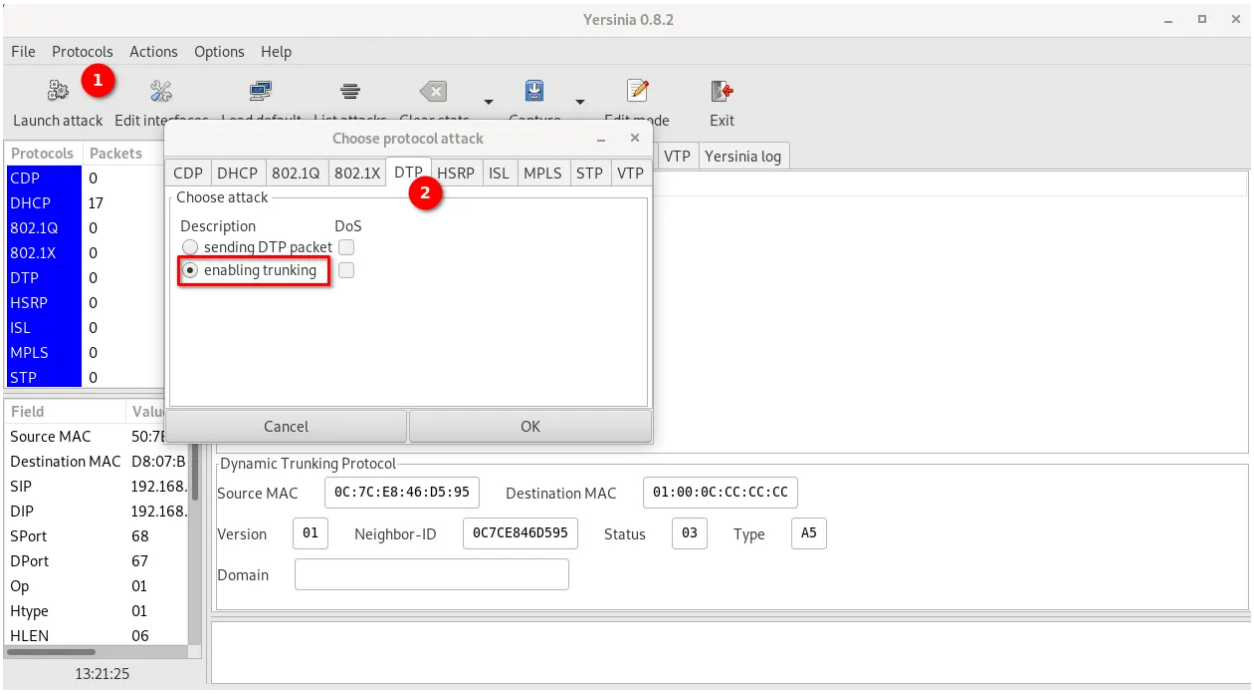
Execution

Setup

1. Setup your local topology
2. Install the required software for this attack
    - Have a Linux machine or a linux virtual machine (VM).
    - install the software on the machine
      ```
      ~$ sudo apt install yersinia
      ~$ sudo apt install dsniff
      ```

Setting up Vlan Hopping

1. Start Yersinia in GUI mode
   ```
   ~$ sudo yersinia -G
   ```
2. Connect to the switch
3. Ensure that the outgoing interface used is correct.
4. With Yersinia enable trunking with dynamic trunking protcol (DTP).



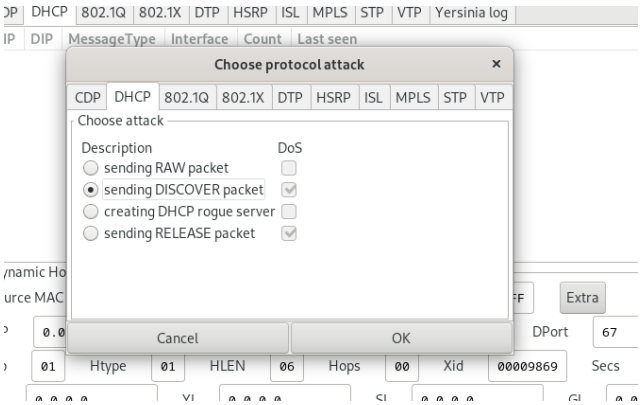
5. Create and enable a VLAN interface with the desired Vlan.

```
~$ ip link add link [interface-name] name [subinterface-name]
type vlan id [vlan-id]
# For example: ~$ ip link add link eth0 name eth0.5 type vlan id
5

~$ ip link set [interface-name] up
~$ ip link set [subinterface-name] up
# For example:
# ~$ ip link set eth0 up
# ~$ ip link set eth0.5 up
```

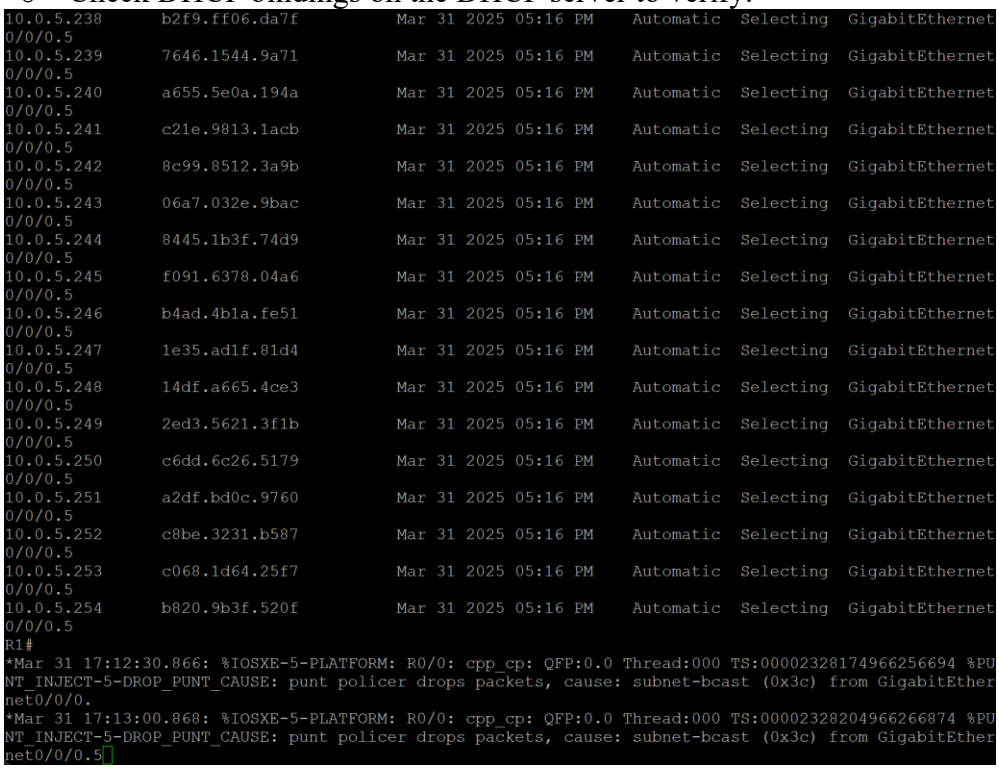
Starve DHCP Addresses

1. Launch a DHCP discover packet denial of service (DoS) attack with Yersinia's GUI



2. Verify that the attack is successful

- Try connecting obtaining a DHCP address from the DHCP server. (it shouldn't be sucessful)
- Check DHCP bindings on the DHCP server to verify.



Prevention and Execution of ARP Spoofing

Prevention

Useful global configuration commands:

- **`ip arp inspection vlan`** [*`vlan-number1 … vlan-number8`*]
- **`ip arp inspection validate`** {`dst-mac | src-mac`}
- **`ip arp gratuitous none`**
- **`ip dhcp snooping`**

Execution

Setup

1. Setup your topology
2. Install the required software for this attack
    - Have a Linux machine or a linux virtual machine (VM).
    - install the software on the machine
      `~$ sudo apt install dsniff`

ARP Spoof

1. Configure port forwarding
   `~$ sudo sysctl -w net.ipv4.ip_forward=1`
2. Run attack in the terminal

```
~$ sudo arpspoof -i INTERFACE -t VICTIM_IP GATEWAY_IP
# For example: sudo arpspoof -i eth0 -t 10.0.0.10 10.0.0.1

~$ sudo arpspoof -i INTERFACE -t GATEWAY_IP VICTIM_IP
# For example: sudo arpspoof -i eth0 -t 10.0.0.1 10.0.0.10

# Note: Use "Control-C" to exit the program
```

3. Observe traffic between the gateway and the victim in Wireshark

Problems

One problem that was encountered was during the MAC Flooding attack. The attack was being executed, but traffic that was going through the switch wasn't being flooded out all ports. At least that's what it looked like; it turns out that the switch had the host's MAC address learned in CAM table. So, the switch was forwarding the traffic to only one port and not flooding the frame received. All that had to be done was to wait a longer period of time, since that MAC address would eventually age out and be filled with a fake MAC address. Then the attack started working.

Conclusion

In conclusion, this lab was completed and taught us how to prevent common layer 2 attacks. (I also learned how to execute them, but only for testing and educational purposes). This lab was difficult to complete because the documentation on how to execute these attacks was scarce, even though the documentation on how to prevent them was prevalent.

Configurations

Important Note About Configuration of Other Devices

Configurations for devices such as the AP, RADIUS server, and router can be found in the link below. Since this network is based off a network I have previously configured.
https://github.com/101zh/StandAloneAccessPoint

S1 Secure Configuration

```
hostname S1
ip arp gratuitous none
ip dhcp snooping
ip arp inspection vlan 1,5,24,50,99
ip arp inspection validate ip
interface FastEthernet0/1
 description Connection to AP
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security maximum 55
 switchport port-security
 switchport port-security aging time 1
 switchport port-security aging type inactivity
```

```
 switchport port-security mac-address sticky
interface FastEthernet0/2
 description Connection to RADIUS server
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/3
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/4
 description Connection to router
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security maximum 5
 switchport port-security
 switchport port-security mac-address sticky
 ip dhcp snooping trust
interface FastEthernet0/5
 description User connection to internet
 switchport access vlan 24
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/6
 description User connection to internet
 switchport access vlan 24
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/7
 description User connection to internet
 switchport access vlan 24
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/8
 switchport access vlan 99
 switchport mode access
```

```
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/9
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/10
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/11
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/12
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/13
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/14
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/15
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/16
```

```
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/17
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/19
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/20
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/21
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/22
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/23
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
```

```
 switchport port-security mac-address sticky
interface FastEthernet0/24
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/25
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/26
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/27
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/28
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/29
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/30
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/31
 switchport access vlan 99
 switchport mode access
```

```
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/32
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/33
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/34
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/35
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/36
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/37
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/38
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/39
```

```
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/40
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/41
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/42
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/43
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/44
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/45
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/46
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
```

```
 switchport port-security mac-address sticky
interface FastEthernet0/47
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface FastEthernet0/48
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface GigabitEthernet0/1
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface GigabitEthernet0/2
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface GigabitEthernet0/3
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface GigabitEthernet0/4
 switchport access vlan 99
 switchport mode access
 switchport port-security maximum 2
 switchport port-security
 switchport port-security mac-address sticky
interface Vlan1
 ip address 10.0.0.4 255.255.255.0
interface Vlan5
 ip address 10.0.5.4 255.255.255.0
interface Vlan24
 ip address 10.0.24.4 255.255.255.0
interface Vlan50
 ip address 10.0.50.4 255.255.255.0
end
```

S1 Insecure Configuration

```
hostname S1
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface FastEthernet0/3
 spanning-tree portfast
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
interface Vlan1
 ip address 10.0.0.4 255.255.255.0
interface Vlan5
 ip address 10.0.5.4 255.255.255.0
interface Vlan24
 ip address 10.0.24.4 255.255.255.0
interface Vlan50
 ip address 10.0.50.4 255.255.255.0
end
```