LAN Security Concepts

IT54 – Routing and Switching

Things we'll cover today

- Examples of Layer 2 Attacks
- VLAN Security
- DHCP Security
- ARP Security
- STP Security

Attack Types

- Distributed Denial of Service (DDoS)
  - Denies a particular type of service from a server or domain by flooding the entire network with useless packets, halting public access to an organization’s website and resources.
- Data Breach
  - An attack which compromises an organization’s data servers or hosts to steal confidential information.
- Malware
  - An attack in which an organization’s hosts are infected with malicious software that causes a variety of problems, such as ransomware that is injected into the hosts, and are replicated through its connection within a particular local area network.

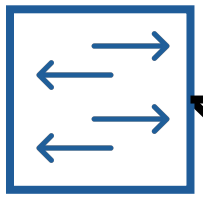
VLAN Hopping

- Attacker configures their computer's Network Interface Card (NIC) to mimic a switch by spoofing its configurations with 802.1Q trunking mode.
  - Spoofing is the act of "imitating" something as if it was real.
  - For example, a spoofed MAC Address is a fake MAC address sent by an attacker, but is somewhat considered ***legit*** by an unassuming network device.

VLAN Hopping

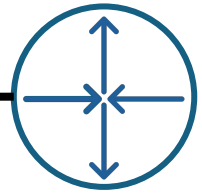
PC1
MAC:
A.A.A.A

F0/1



SW1

Running DTP by default

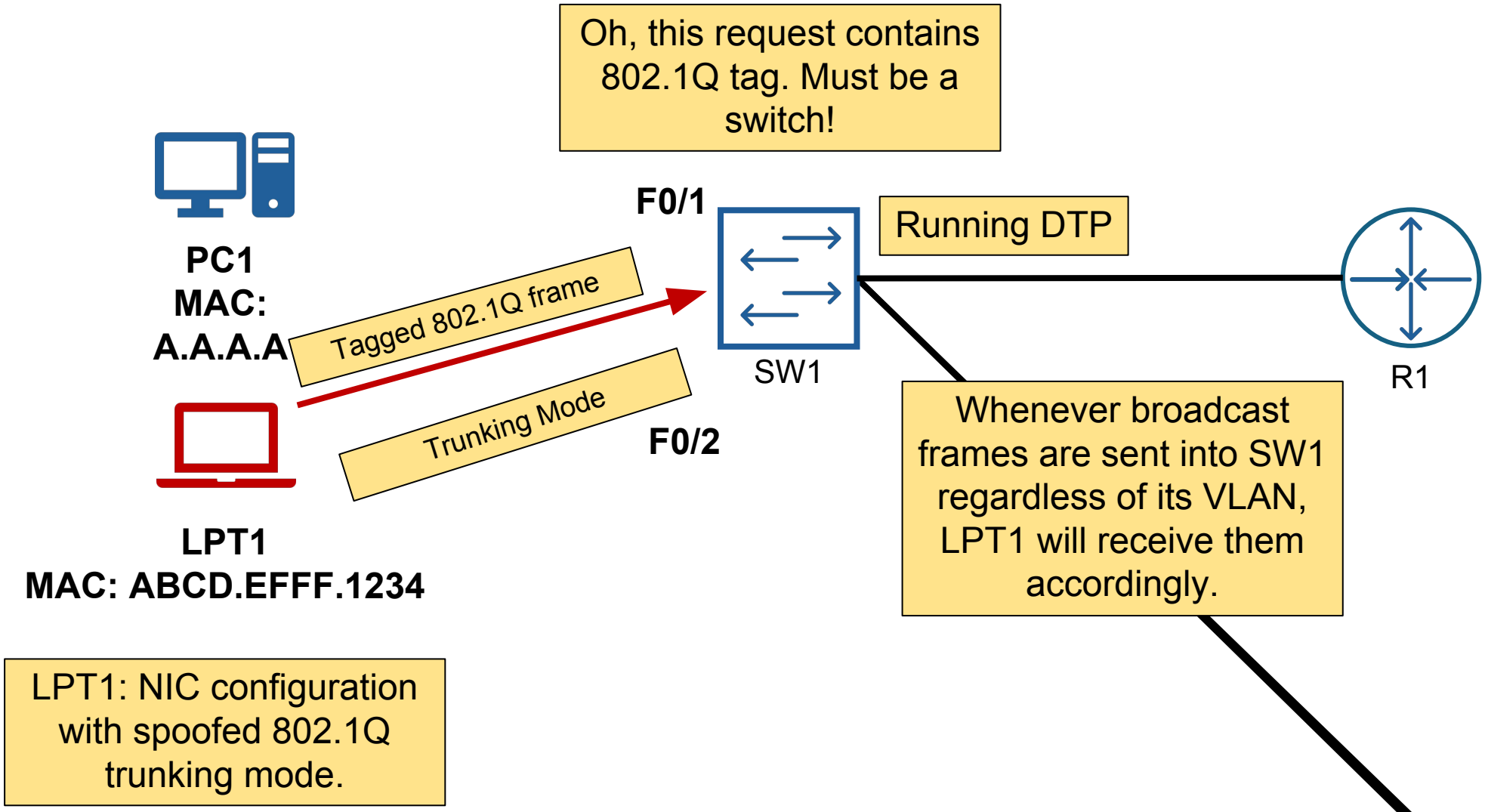


R1

When a switch is running DTP, all of its ports are at **dynamic auto** mode by default.

This means that if the other side is a switch that also sends DTP, it will form a **trunk** connection with it.

VLAN Hopping



Mitigating VLAN Hopping

Step 1: Disable DTP (auto trunking) negotiations on everything.

```
SW1(config)#interface range f0/1-24
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport nonegotiate
```

Step 2: Set the VLAN Explicitly

```
SW1(config-if-range)#switchport access vlan 1000
```

Mitigating VLAN Hopping

Step 3: Set a select range of interfaces to be on trunking mode

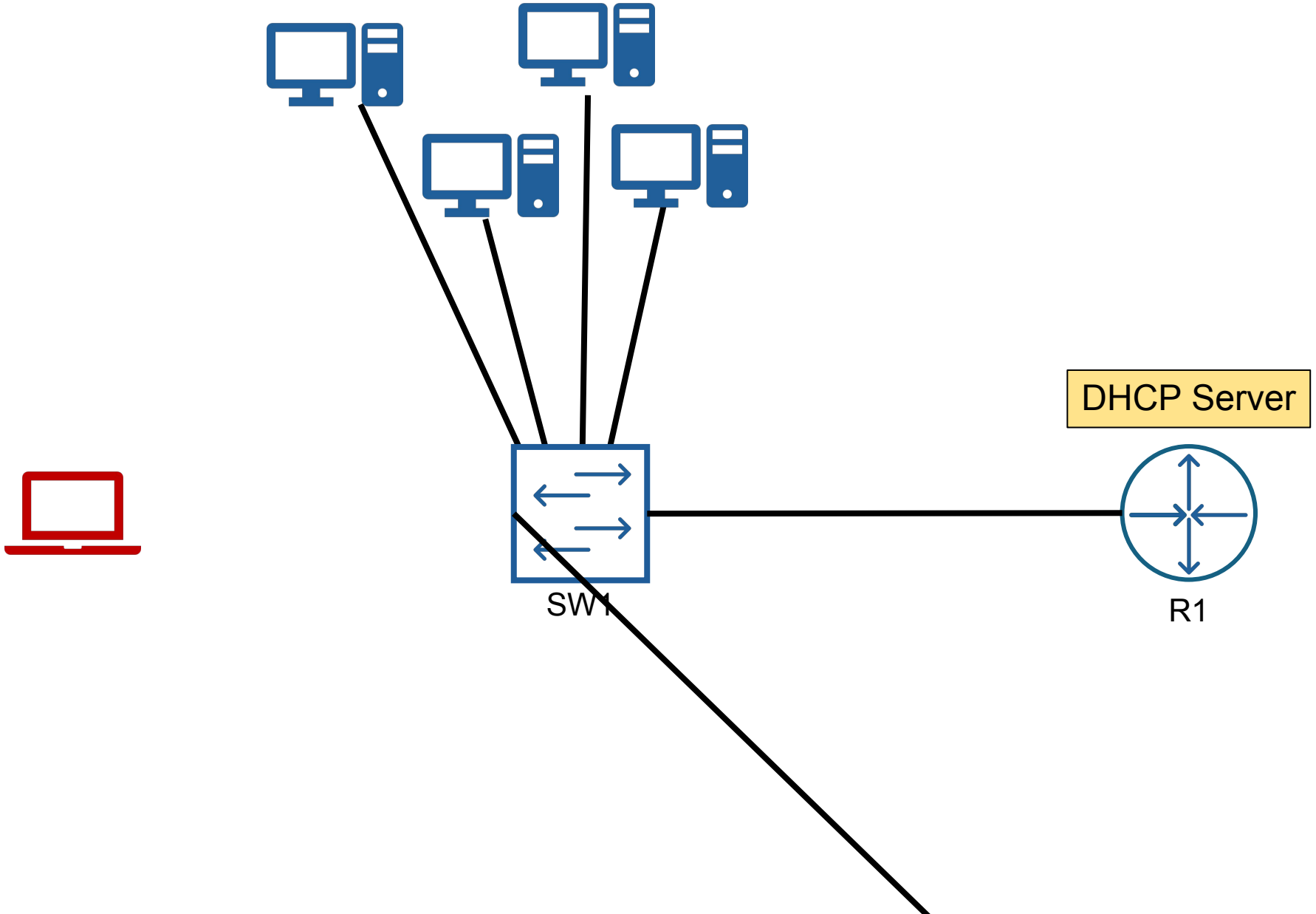
```
SW1(config)#interface range f0/20-24
SW1(config-if-range)#switchport mode trunk
SW1(config-if-range)#switchport nonegotiate
SW1(config-if-range)#switchport trunk native vlan 99
```

By changing the native VLAN to anything other than 1, attackers won't be able to easily identify your switch's Native VLAN.

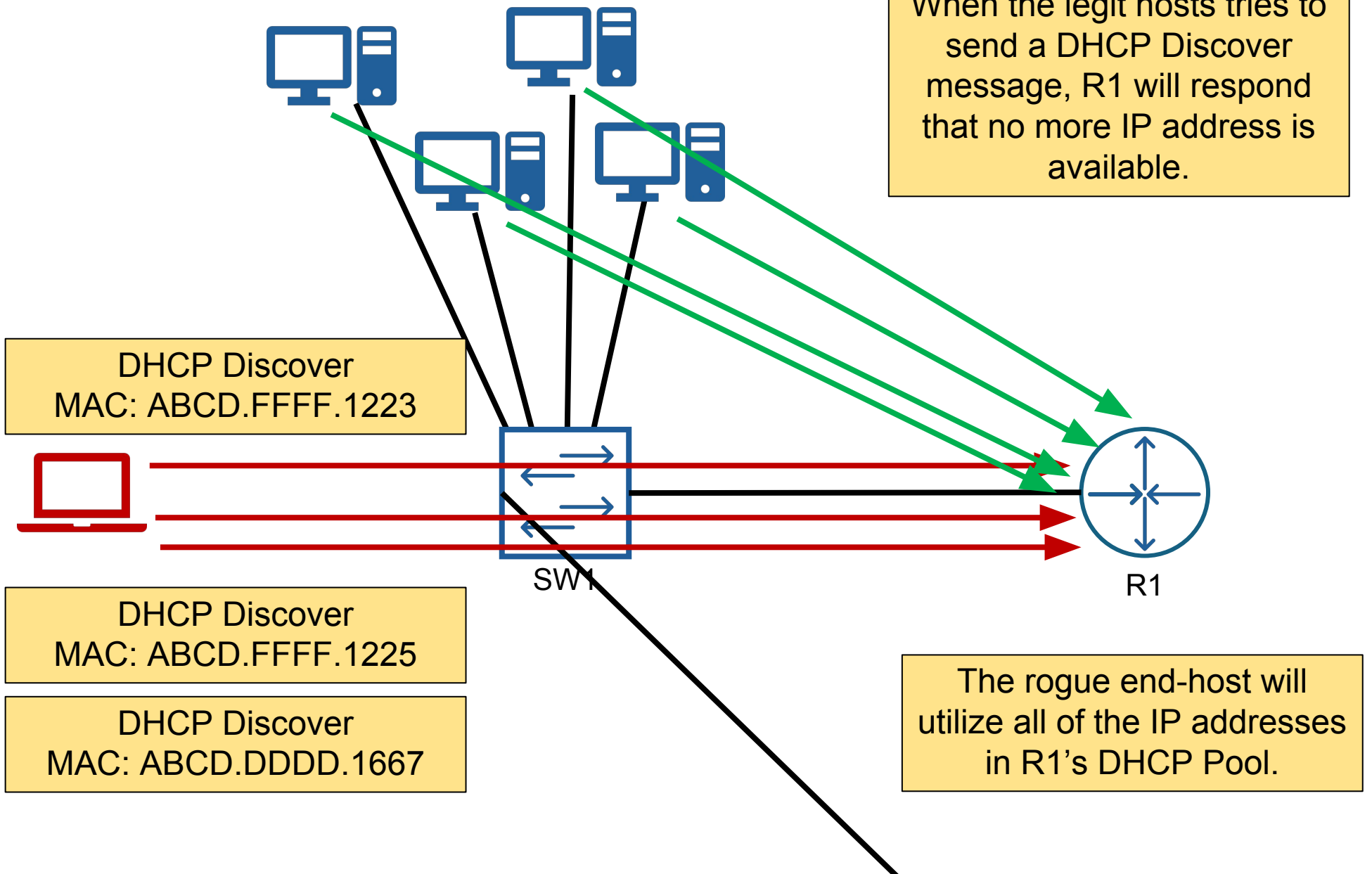
DHCP Starvation

- DHCP Starvation is a Denial of Service (DoS) attack in which an attacker spoofs multiple MAC addresses and DHCP messages which utilizes an entire DHCP pool and leaving none for an organization’s hosts to use.
- This is usually done by spoofing a set of MAC address as multiple DHCP Discover messages are sent from one rogue end host to the DHCP Server.

DHCP Starvation



DHCP Starvation



Mitigating DHCP Starvation Attacks

- DHCP Snooping
  - Filters DHCP messages and rate-limits DHCP traffic on untrusted ports.
    - Devices under administrative control such as switches, routers, and servers are trusted sources.
  - Trusted interfaces such as trunk links and server ports must be explicitly configured as trusted.
  - Devices outside the network and all access ports are generally treated as untrusted sources.

Implementing DHCP Snooping

Step 1: Disable DTP (auto trunking) negotiations on everything.

```
SW1(config)#ip dhcp snooping
SW1(config)#interface f0/1
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#interface range f0/5-24
SW1(config-if-range)#ip dhcp snooping limit rate 6
SW1(config-if-range)#end
```

Step 2: Set DHCP Snooping on VLANs

```
SW1(config)#ip dhcp snooping vlan 5, 10, 50-52
```

Verifying DHCP Snooping

Verify DHCP Snooping Settings

```
SW1#show ip dhcp snooping
```

View clients that has received DHCP information

```
SW1#show ip dhcp snooping binding
```