# Access Layer Switch Security Mechanisms

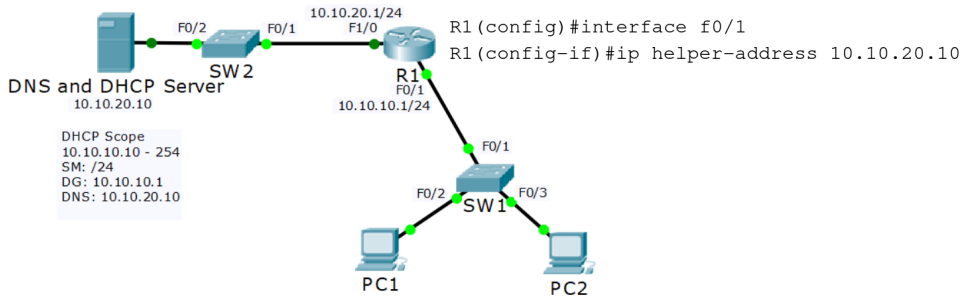
- **DHCP Snooping**
- **DAI Dynamic ARP Inspection**
- **802.1X Identity Based Networking**
- **Port Security**

# DHCP Snooping

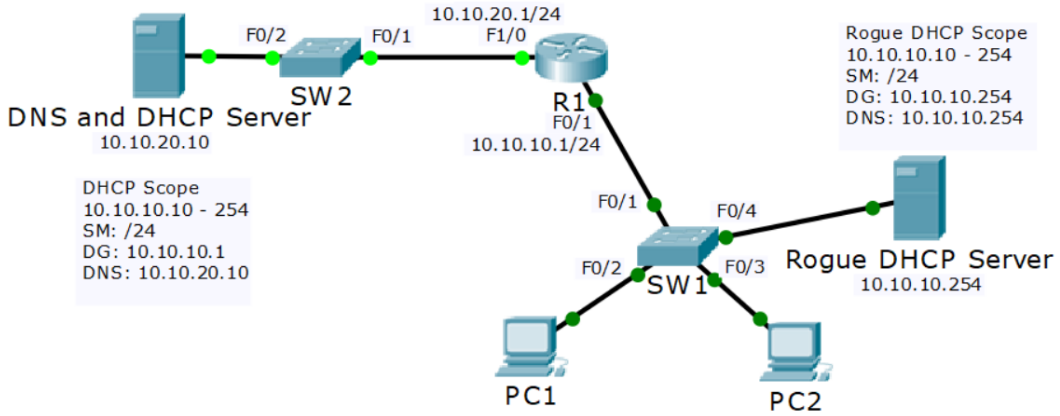
External DHCP Server Configuration

*R1(config)#interface f0/1*

*R1(config-if)#ip helper-address 10.10.20.10*




**Rogue DHCP Server**




*SW1(config)#ip dhcp snooping*

*SW1(config)#ip dhcp snooping vlan 10*

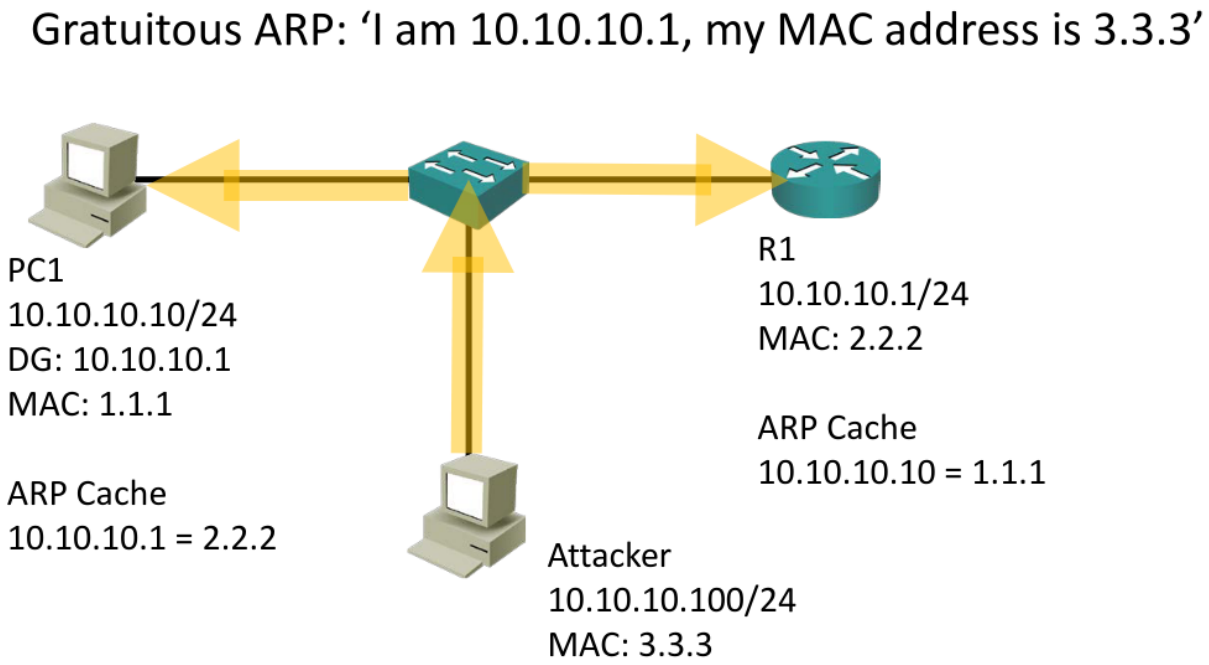
*SW1(config)#int f0/1*

*SW1(config-if)#ip dhcp snooping trust*

When DHCP Snooping is enabled, DHCP Server responses are dropped if they don't arrive on a trusted port.

# DAI Dynamic ARP Inspection

**Man in the Middle ARP Spoofing**

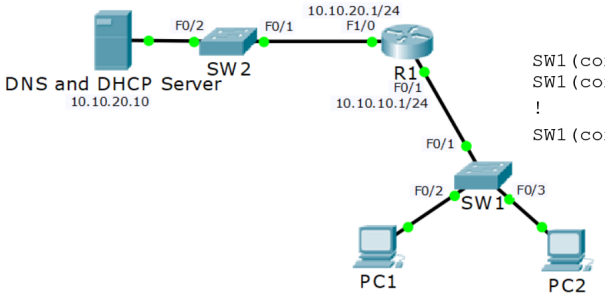



- When you enable DHCP snooping, the switch inspects the DHCP traffic and keeps track of which IP addresses were assigned to which MAC addresses
- For example, PC1 with MAC address 1.1.1 was assigned IP address 10.10.10.10
- If invalid ARP traffic tries to pass through the switch, for example 3.3.3 saying it is 10.10.10, the switch drops the traffic

**DAI Configuration**

*SW1(config)#int f0/1*
*SW1(config-if)#ip arp inspection trust*
!
*SW1(config)#ip arp inspection vlan 10*

DAI is not performed on trusted ports.
Enable this for non DHCP clients.

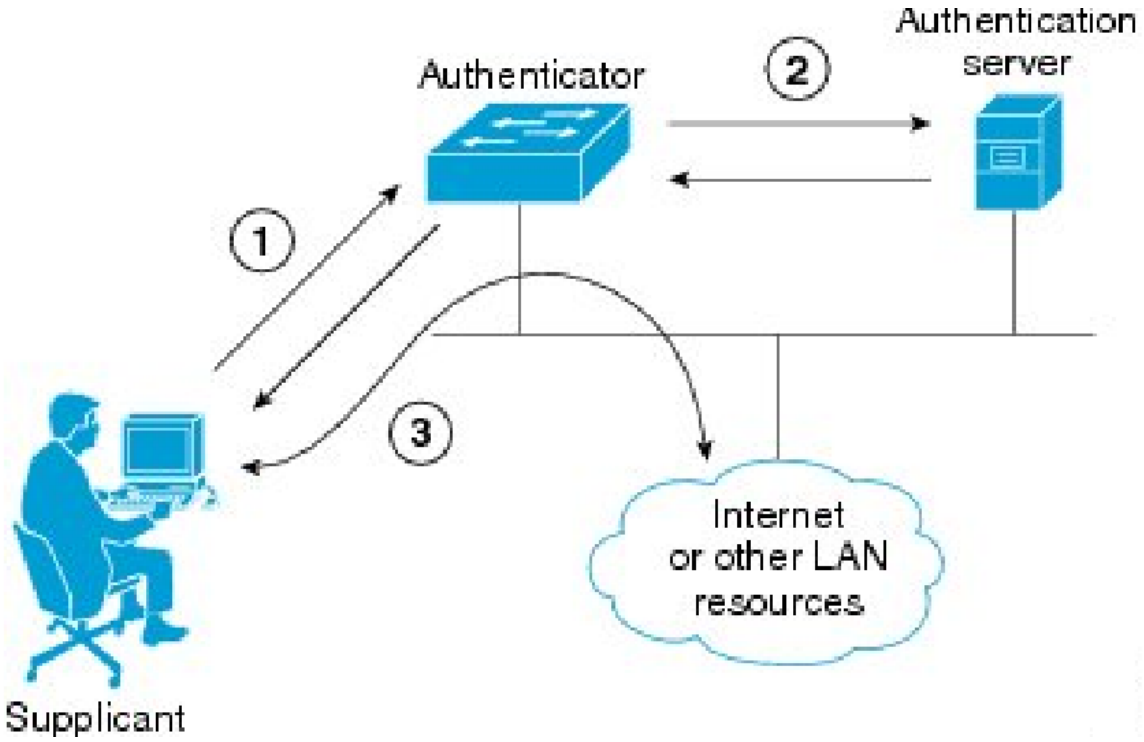



```
SW1(config)#int f0/1
SW1(config-if)#ip arp inspection trust
!
SW1(config)#ip arp inspection vlan 10
```

DAI is not performed on trusted ports.
Enable this for non DHCP clients.

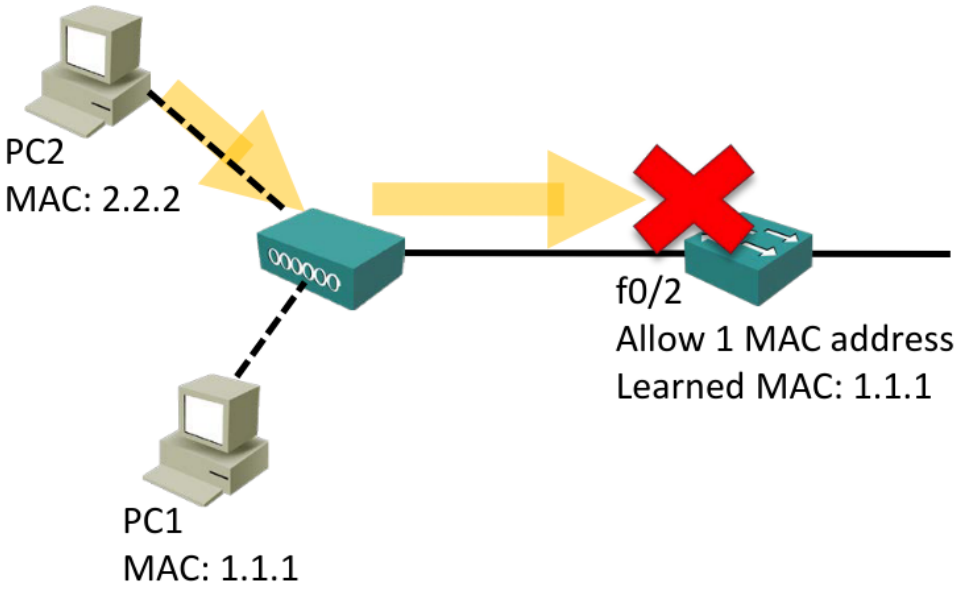
# 802.1X Identity Based Networking

- When 802.1X is enabled, only authentication traffic is allowed on switch ports until the host and user are authenticated
- When the user has entered a valid username and password, the switch port transitions to a normal access port in the relevant VLAN



# Port Security

- Port Security enables an administrator to specify which MAC address or addresses can send traffic into an individual switch port.
- This can be used to lock a port down to a particular host or hosts
- It is easy to spoof a MAC address, so locking ports down to a specific host is not usually Port Security's main role in production networks
- Port Security can also configure individual switch ports to allow only a specified number of source MAC addresses to send traffic in to the port
- It can learn connected MAC addresses
- This is useful to prevent users from adding Wireless Access Points or other shared devices




*SW1(config)#int f0/2*
*SW1(config-if)#switchport port-security*

- If you configure Port Security with no additional parameters then only one MAC address is allowed to transmit on the port
- The current MAC address can be disconnected and replaced. The port is not locked down to a particular MAC address
- If a shared device is connected and multiple hosts try to transmit the port will be shut down

*SW1#show port-security interface f0/2*

You have three options when an unauthorised MAC address sends traffic in to the port:

- **Shutdown** (Default): The interface is placed into the error-disabled state, blocking all traffic
- **Protect**: Traffic from unauthorised addresses is dropped. Traffic from allowed addresses is forwarded
- **Restrict**: Traffic from unauthorised addresses is dropped, logged and the violation counter incremented. Traffic from allowed addresses is forwarded

*SW1(config)#int f0/2*
*SW1(config-if)# switchport port-security violation protect*
*SW1(config-if)# switchport port-security violation restrict*

- If the Violation Action is set to Shutdown and a violation occurs, the port will move to an error-disabled state
- To bring an error-disabled interface back into service:
    - Physically remove the host with the offending MAC address
    - Manually shutdown then no shutdown the interface

Auto-Recovery
You can bring error disabled ports back into service automatically after they have been disabled for a configurable period of time (in seconds)
*SW1(config)# errdisable recovery cause psecure-violation*
*SW1(config)# errdisable recovery interval 600*

Maximum MAC Addresses

- When Port Security is enabled the maximum number of MAC addresses allowed to send traffic into the interface is one by default
- This can be increased if multiple hosts share the port, for example an IP phone with a PC plugged into the back of it

*SW1(config)# interface f0/2*
*SW1(config-if)# switchport port-security maximum 2*

Manually Adding MAC Addresses

- You can statically configure allowed MAC addresses if you want to lock the port down to a particular host:

*SW1(config)# interface f0/10*
*SW1(config-if)# switchport port-security*
*SW1(config-if)#switchport port-security mac-address 1111.2222.3333*
*SW1(config-if)# switchport port-security maximum 1*

MAC Address Learning

- Scenario: You have 1000 authorised hosts connected to the network. You want to lock the ports down to these particular hosts
- Manually adding the MAC addresses is not a scalable solution
- Sticky MAC addresses add the learned MAC address to the running configuration. Save to the startup config to make them permanent

*SW1(config)# interface f0/2*
*SW1(config-if)# switchport port-security*
*SW1(config-if)# switchport port-security mac-address sticky*

View
*show port-security address*
*show port-security*