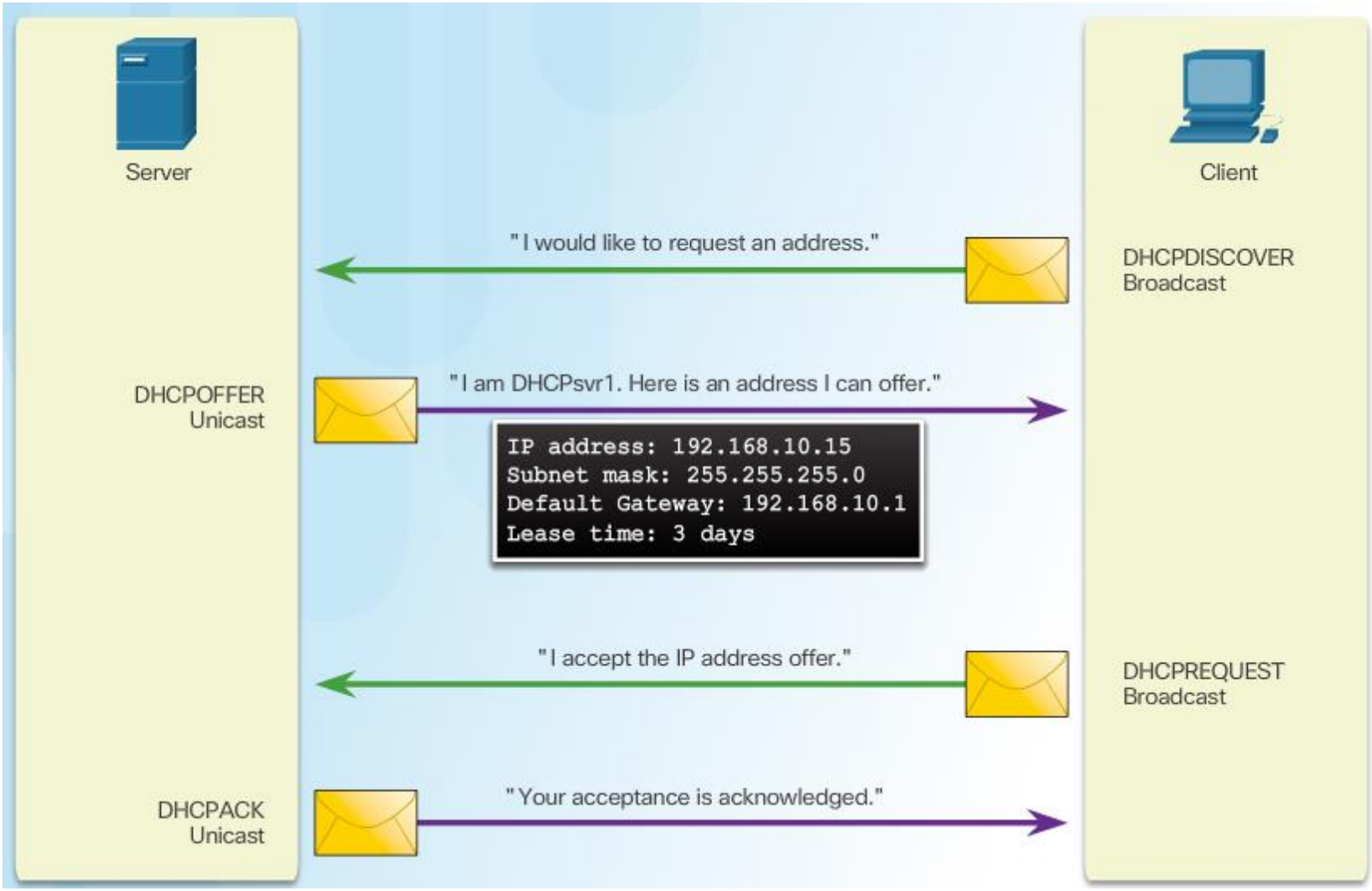
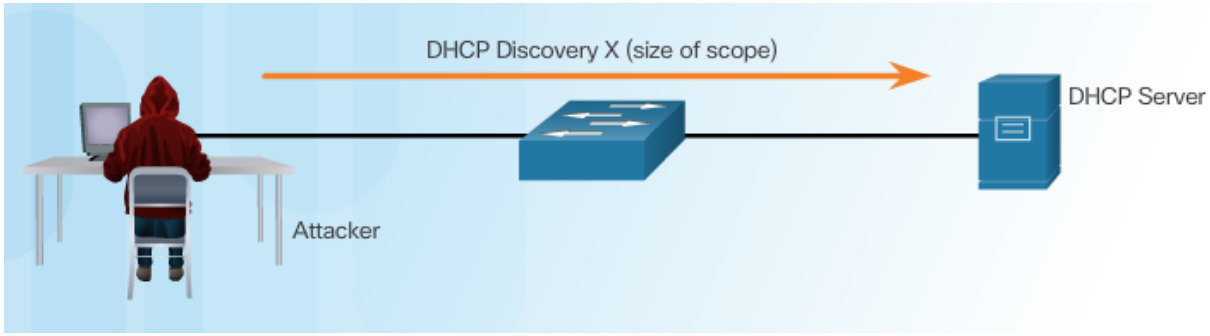
DHCP Attacks

DHCP Spoofing Attack

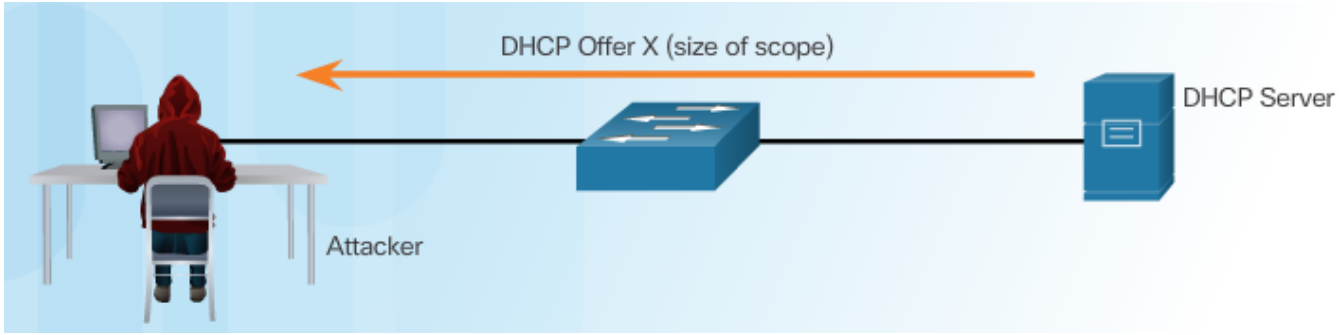


DHCP Starvation Attack

Attacker Initiates a Starvation Attack

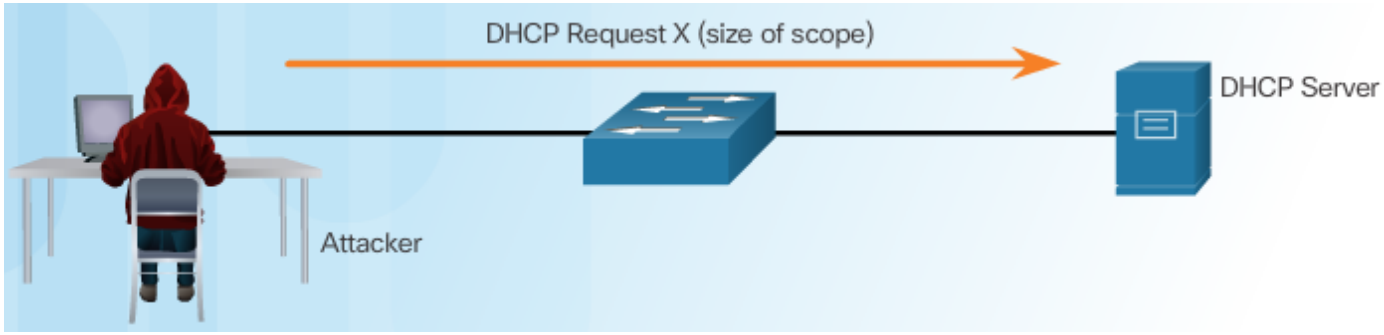


DHCP Server Offers Parameters

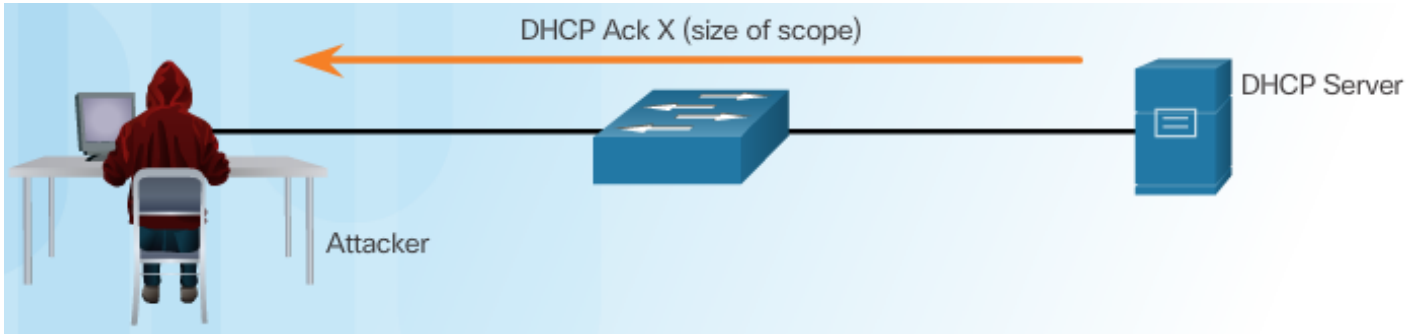


DHCP Starvation Attack

Client Requests all Offers



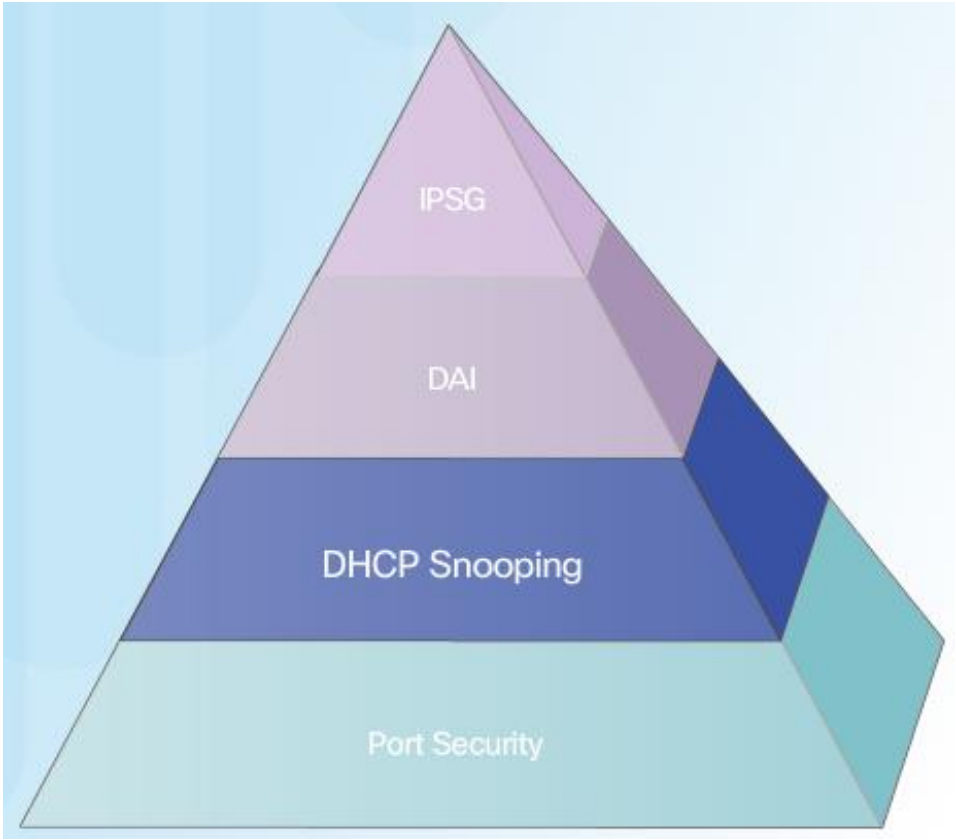
DHCP Server Acknowledges All Requests



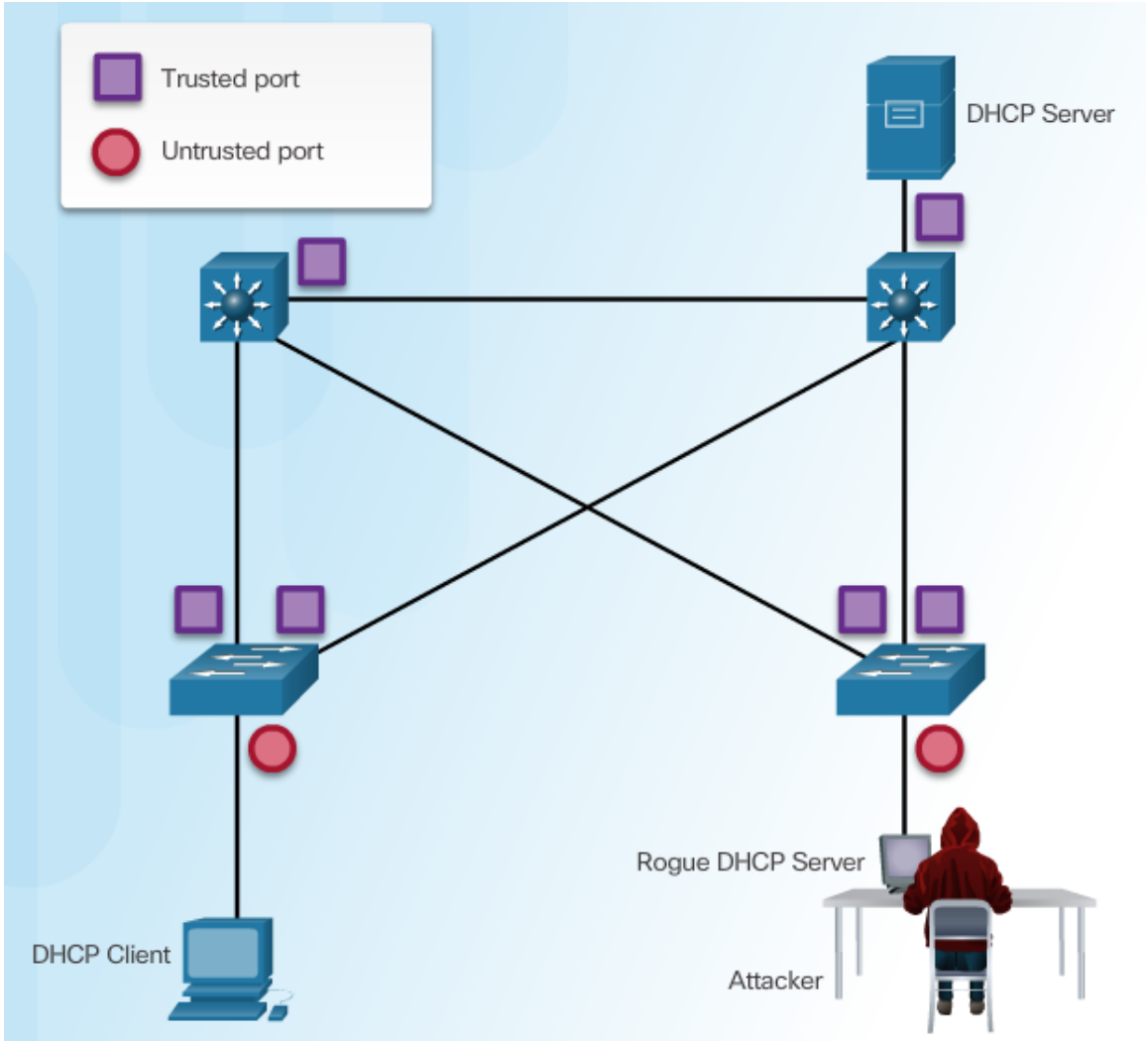
Mitigating VLAN Attacks

The switch will deny packets containing specific information:

- Unauthorized DHCP server messages from an untrusted port
- Unauthorized DHCP client messages not adhering to the snooping binding table or rate limits
- DHCP relay-agent packets that include option-82 information on an untrusted port



Configuring DHCP Snooping



Configuring DHCP Snooping Example

DHCP Snooping Reference Topology

Configuring a Maximum Number of MAC Addresses

```
S1(config)# ip dhcp snooping
S1(config)#
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)#
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)#
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)#
```

Configuring DHCP Snooping Example

Verifying DHCP Snooping

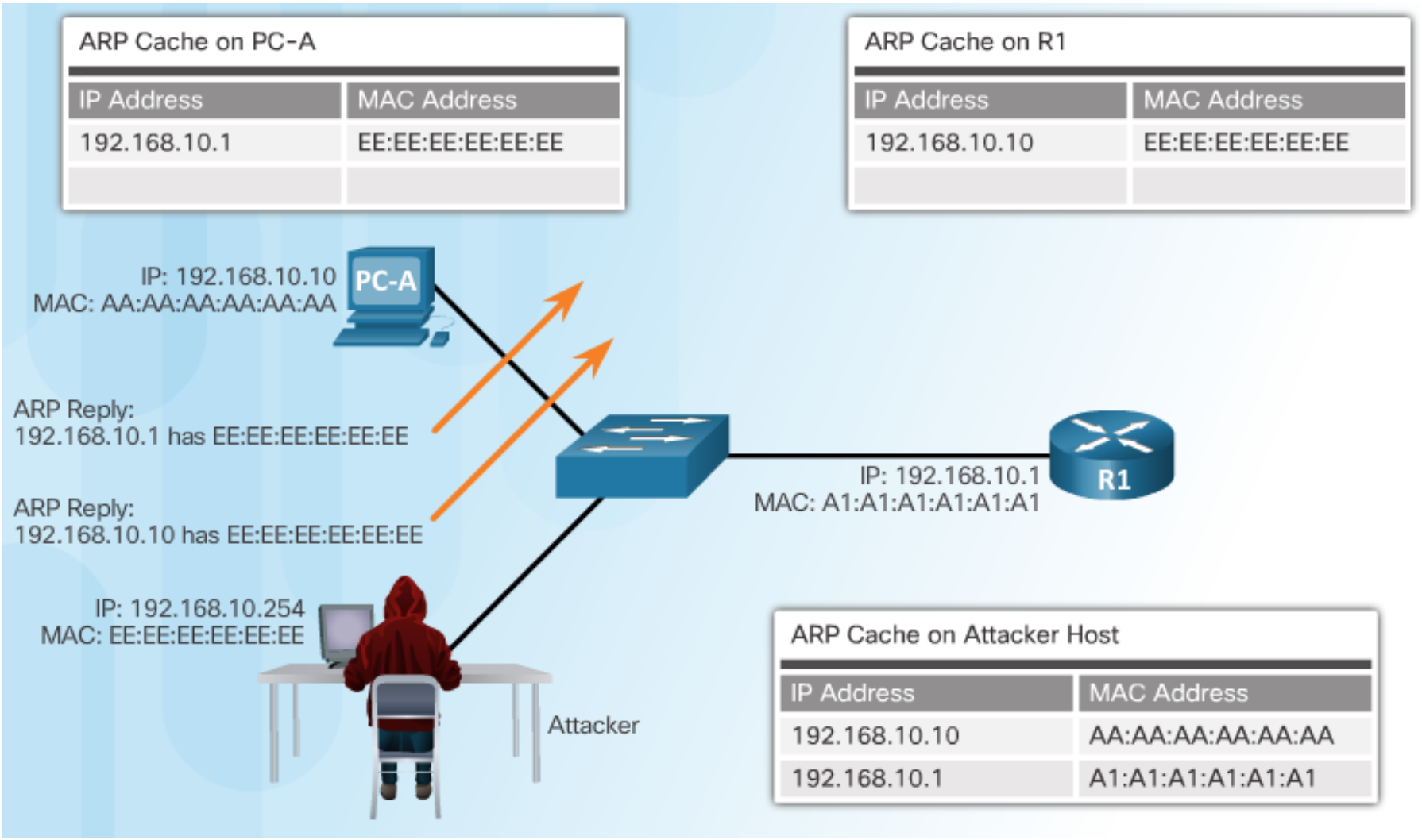
```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

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:

<output omitted>
```

Configuring a Maximum Number of MAC Addresses

```
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
```

Mitigating ARP Spoofing and ARP Poisoning Attack

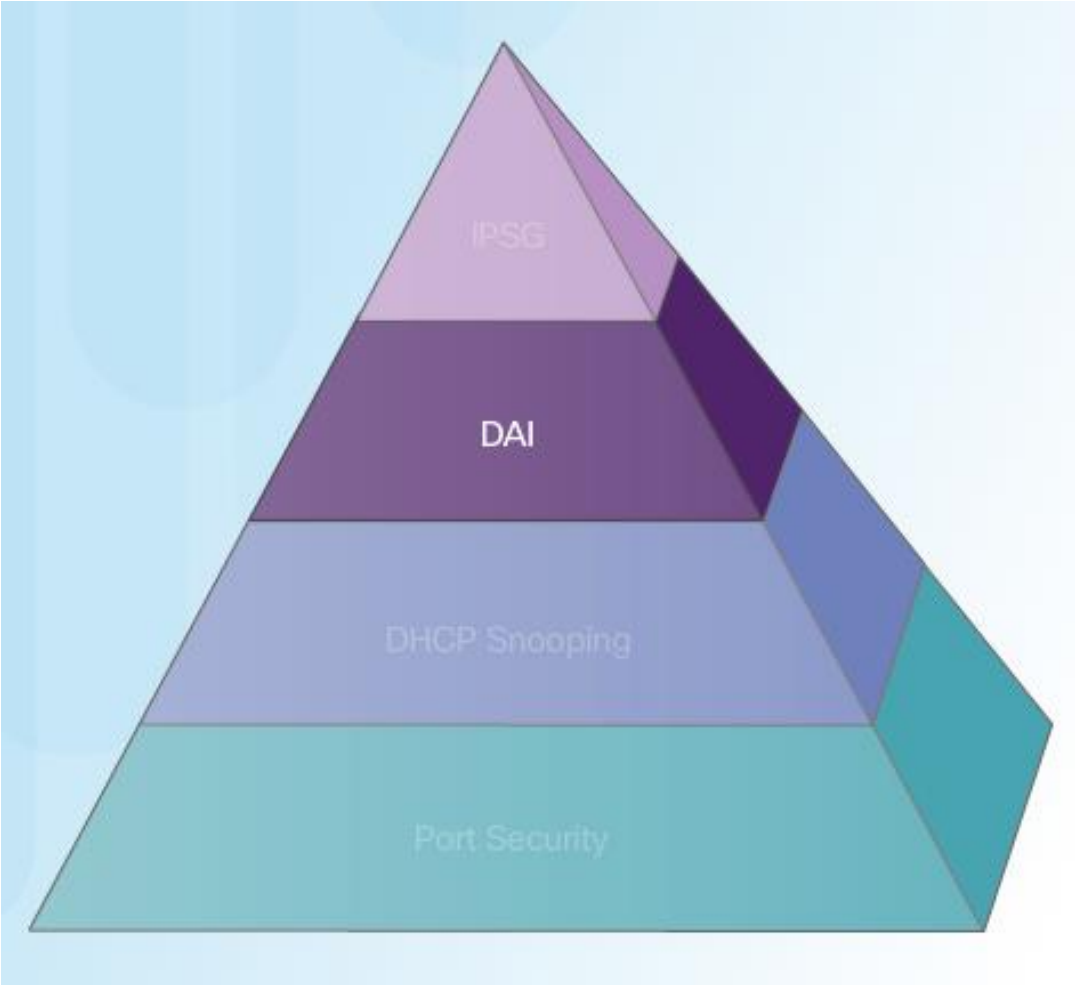
ARP Spoofing and ARP Poisoning Attack



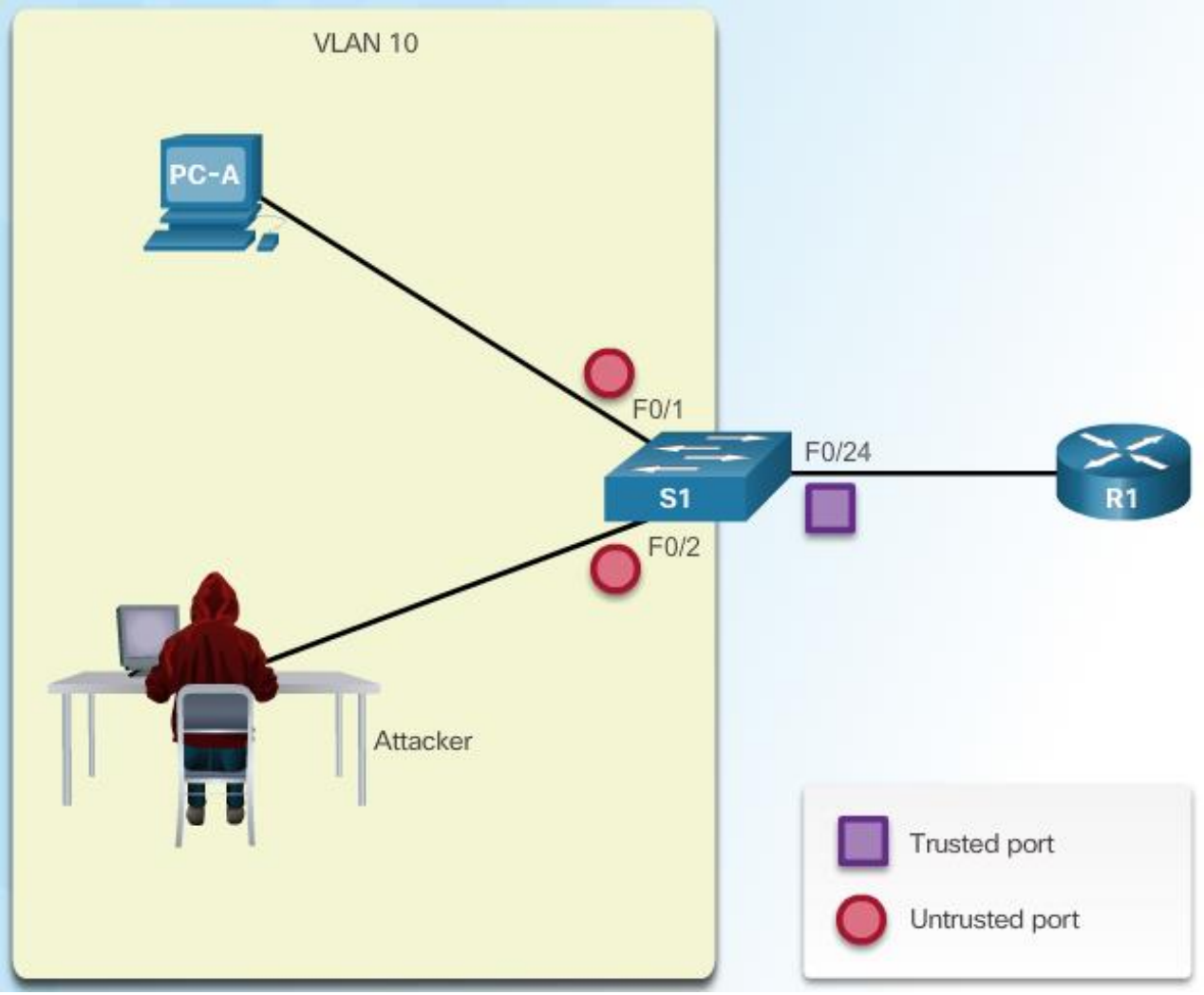
Mitigating ARP Attacks

Dynamic ARP Inspection:

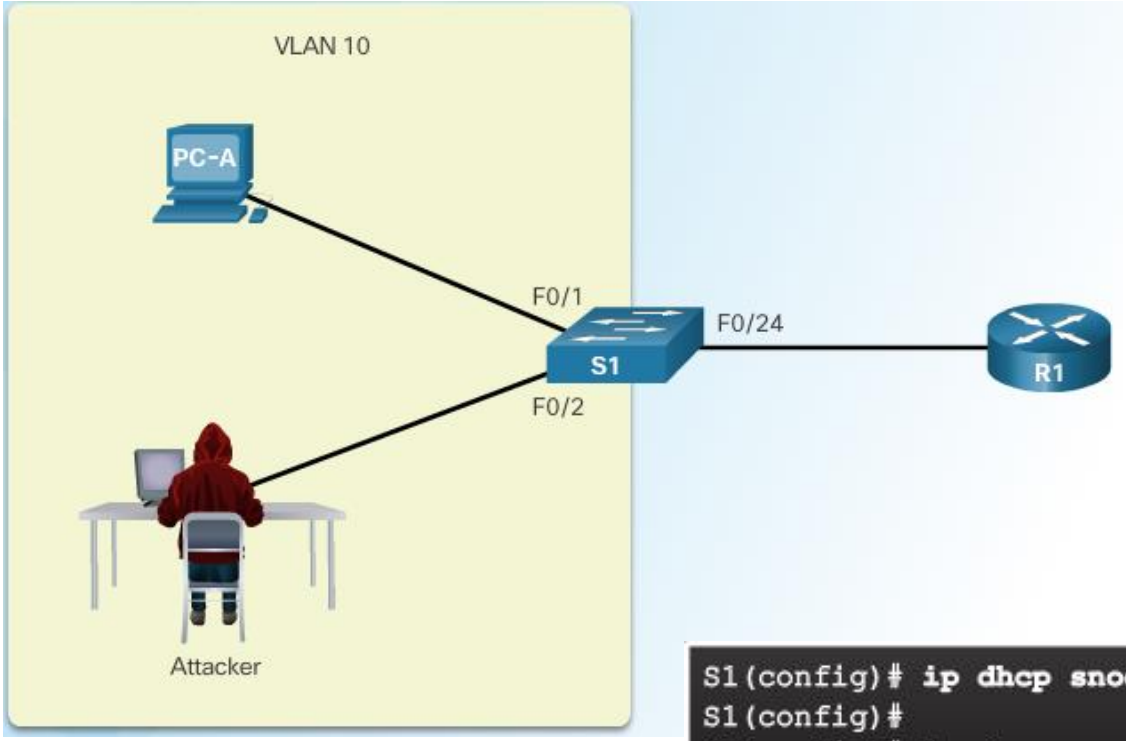
- DAI associates each interface with a trusted state or an untrusted state.
- Trusted interfaces bypass all DAI.
- Untrusted interfaces undergo DAI validation.



Configuring Dynamic ARP Inspection



Configuring DHCP Snooping Example



ARP Reference Topology

Configuring Dynamic ARP Inspection

```
S1(config)# ip dhcp snooping
S1(config)#
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)#
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection  trust
S1(config-if)#
```

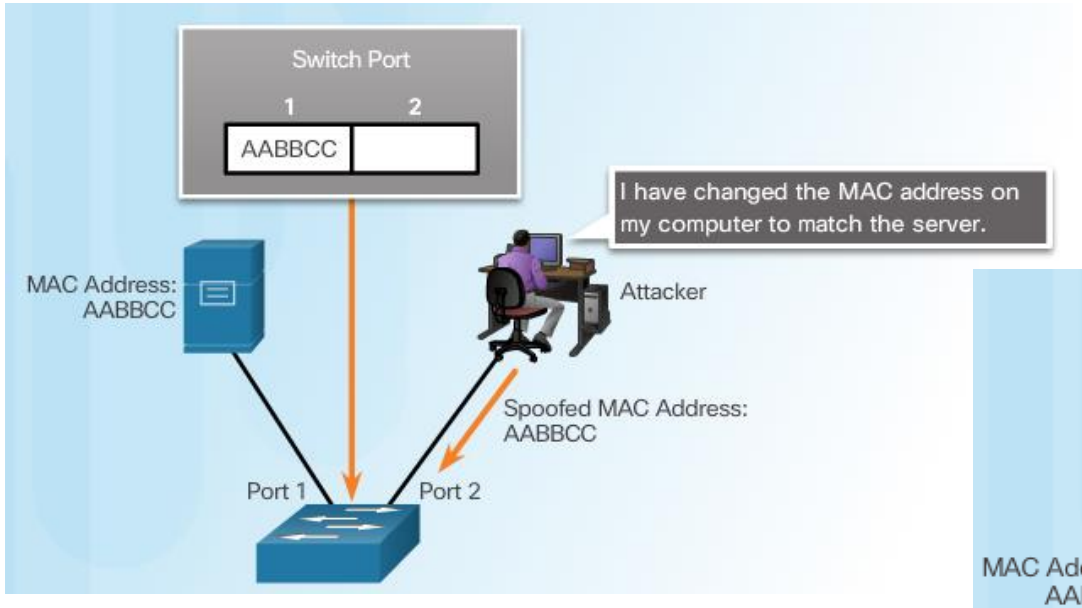
Configuring DHCP Snooping Example

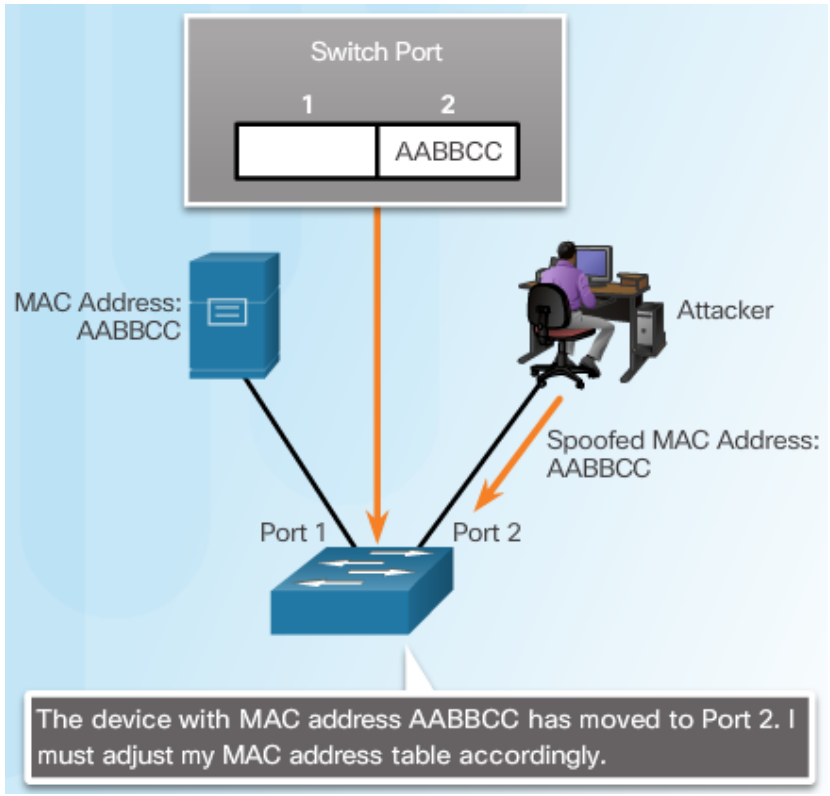
Checking Source, Destination, and IP

```
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)#
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)#
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)#
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

Mitigating Address Spoofing Attacks

Address Spoofing Attack

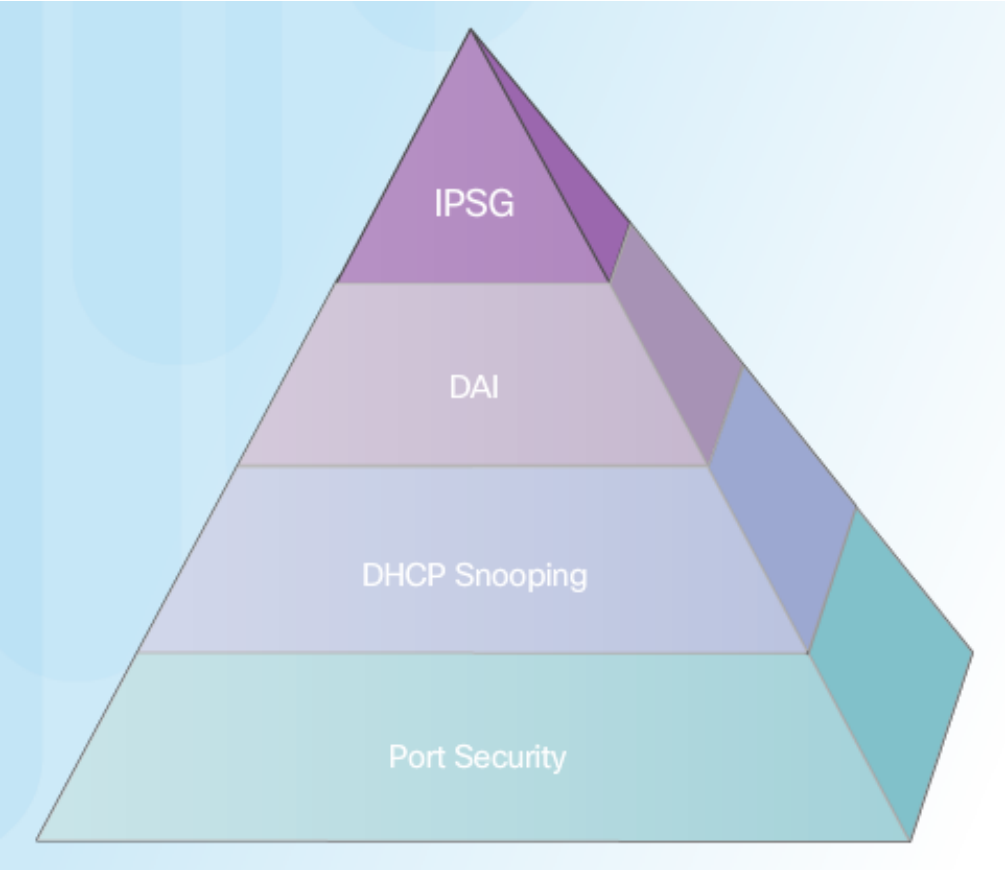




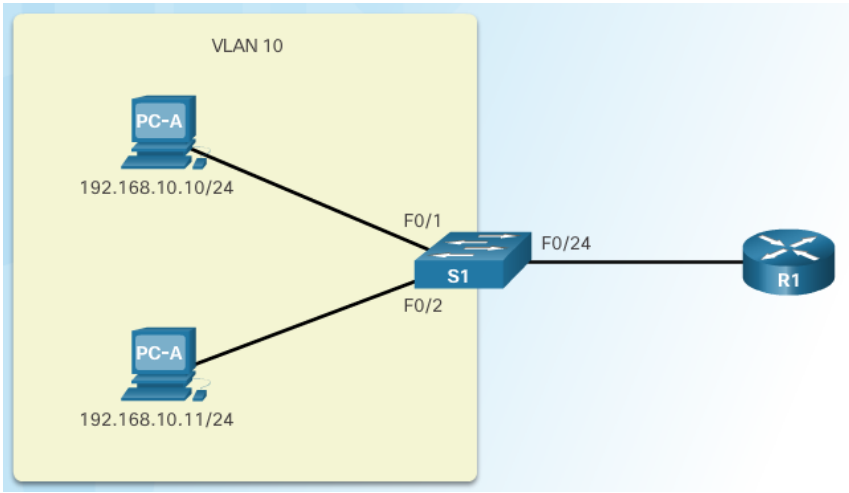
Mitigating Address Spoofing Attacks

For each untrusted port, there are two possible levels of IP traffic security filtering:

- Source IP address filter
- Source IP and MAC address filter



Configuring IP Source Guard



IP Source Guard Reference Topology

Configuring IP Source Guard

```
S1(config)# interface range fastethernet 0/1 - 2
S1(config-if-range)# ip verify source
S1(config-if-range)# end
S1#
```

Checking IP Source Guard

```
S1# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
F0/1       ip           active       192.168.10.10                       10
F0/2       ip           active       192.168.10.11                       10
S1#
```

Introduction to the Spanning Tree Protocol