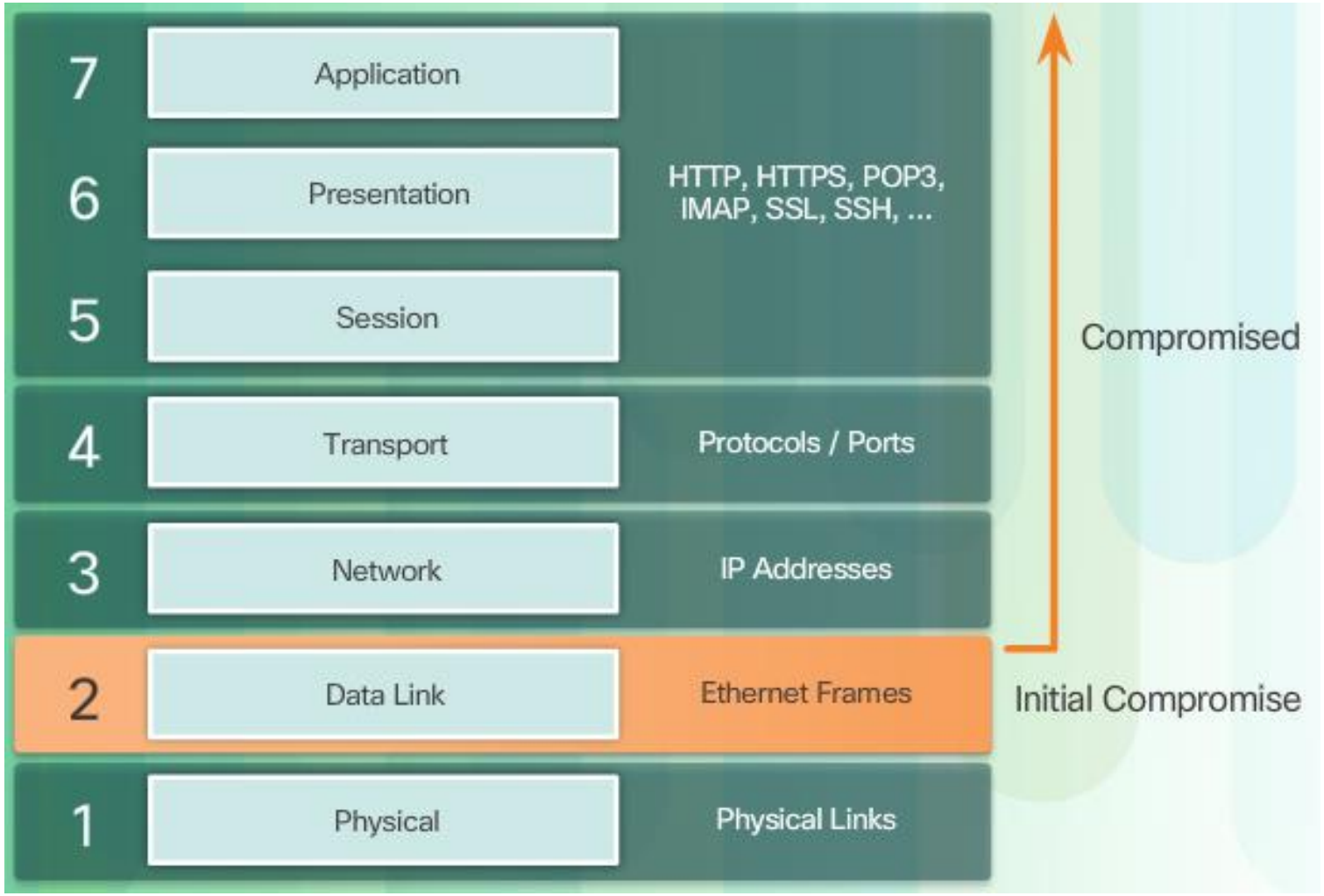
Computer Networks
Day 2
Layer 2 Security

Outline

- ✓ Layer 2 vulnerabilities.
- ✓ CAM table overflow attacks.
- ✓ Configure port security to mitigate CAM table overflow attacks.
- ✓ Configure VLAN Truck security to mitigate VLAN hopping attacks.
- ✓ Implement DHCP Snooping to mitigate DHCP attacks.
- ✓ Implement Dynamic ARP Inspection to mitigate ARP attacks.

Layer 2 Vulnerabilities

Layer 2 Vulnerabilities



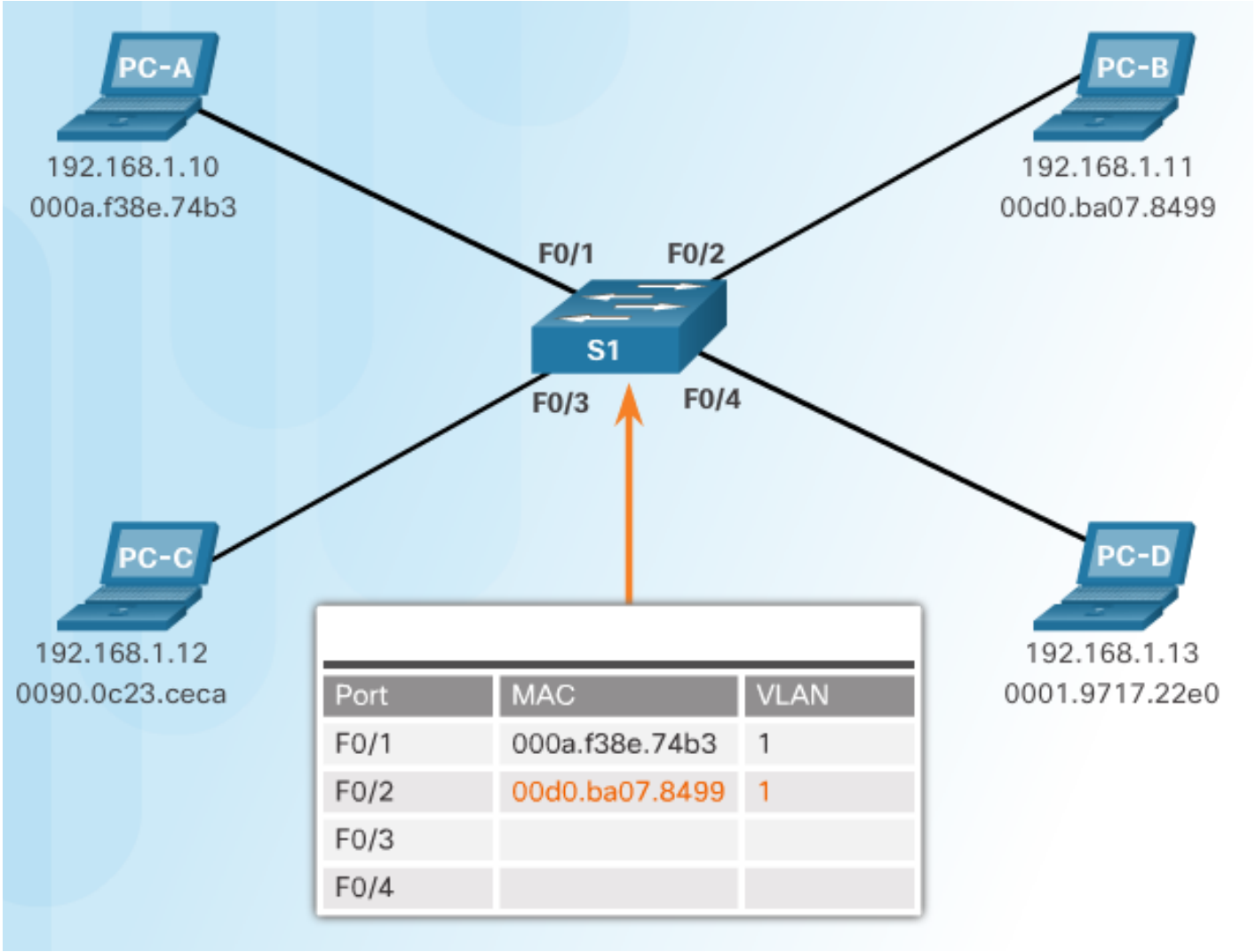
Switch Attack Categories

CAM Table Attacks

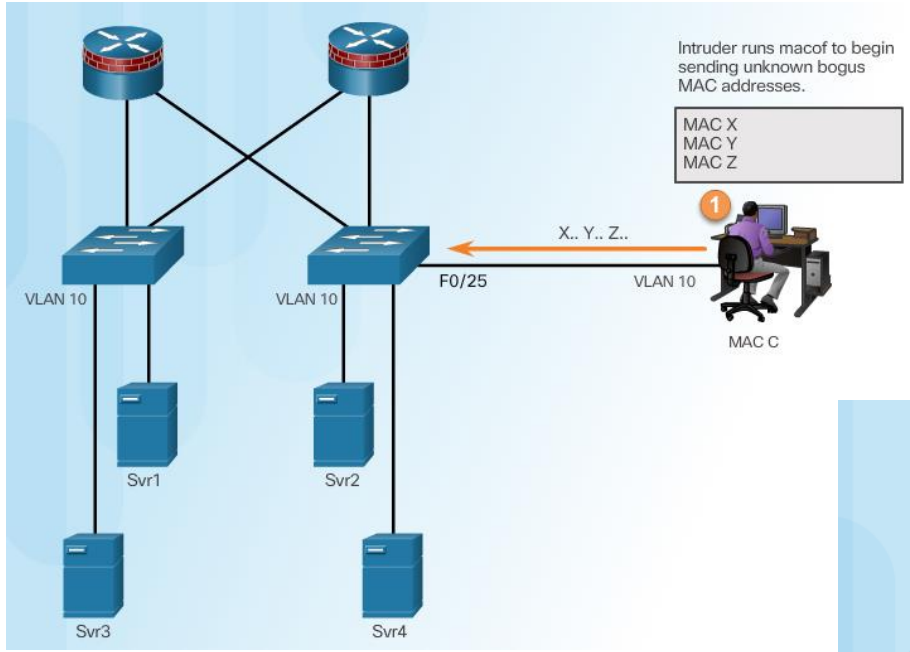
Basic Switch Operation

```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
Sw1#
```

CAM Table Operation Example

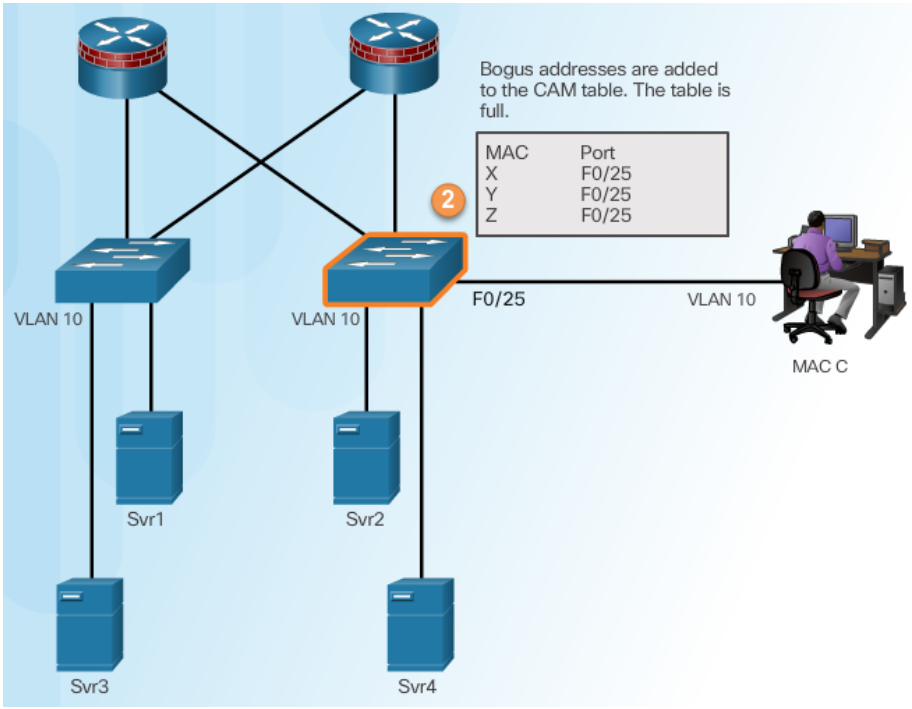


CAM Table Attack

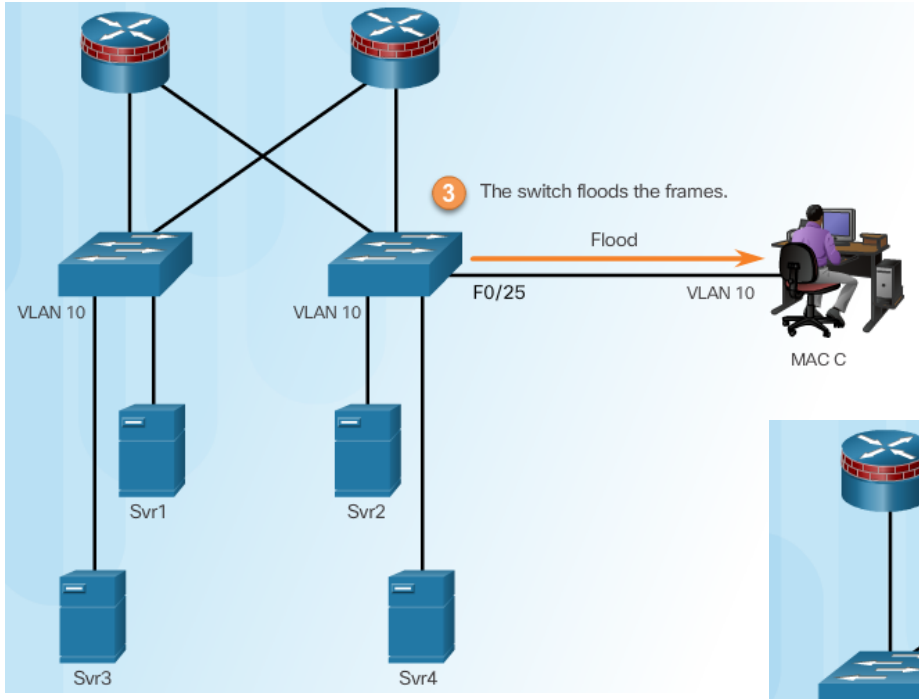


Intruder Runs Attack Tool

Fill CAM Table

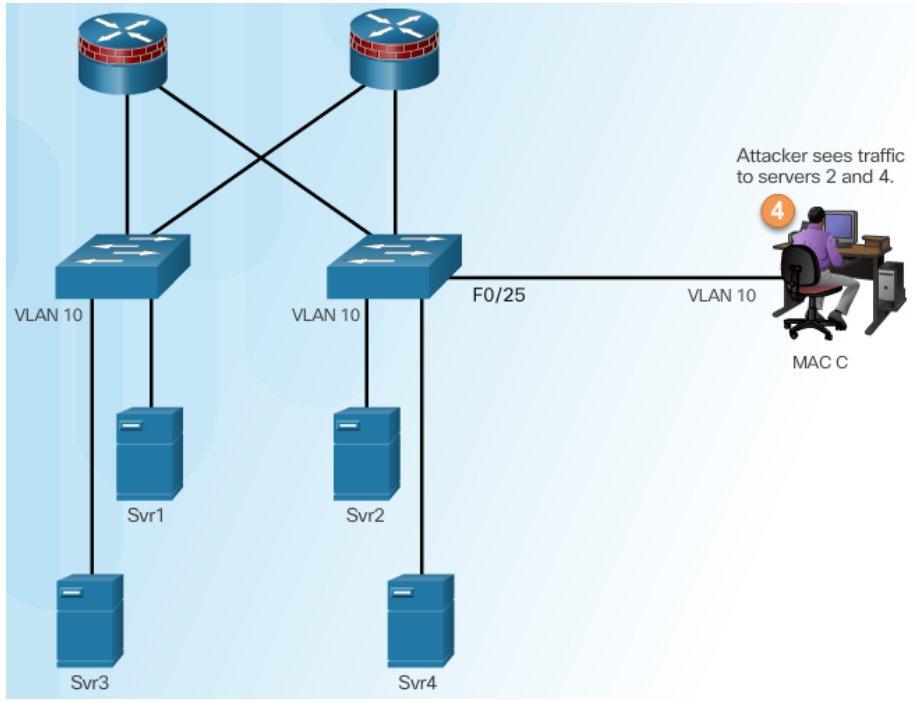


CAM Table Attack



Switch Floods All Traffic

Attacker Captures Traffic



CAM Table Attack Tools

```
macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

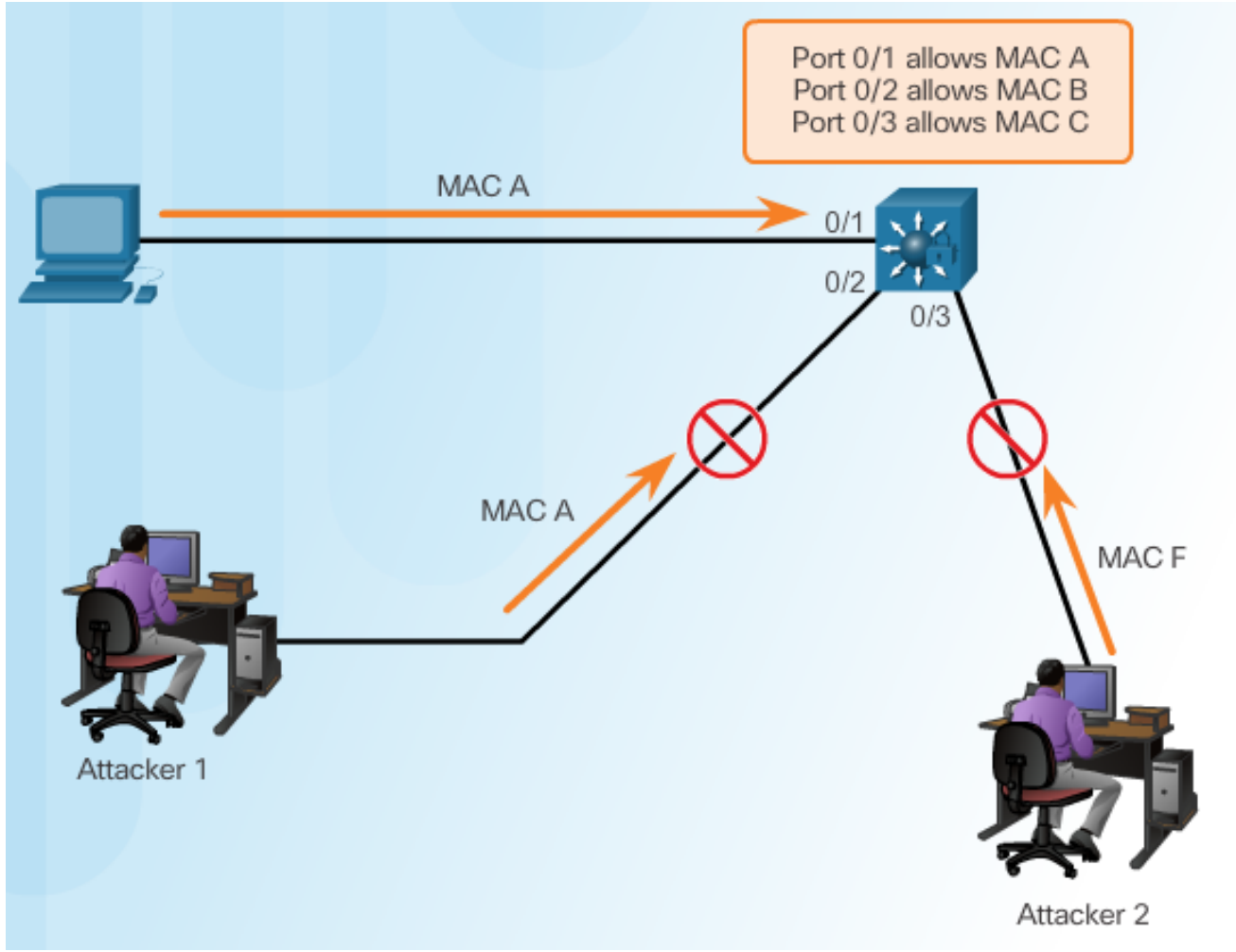
Mitigating CAM Table Attacks

Switch Port Security

Secure Unused Ports

The **`interface range`** command can be used to apply a configuration to several switch ports at one time.

Countermeasure for CAM Table Attacks



Switch Port Security

Port Security: Operation

- Port security limits the number of valid MAC addresses allowed to transmit data through a switch port.
  - If a port has port security enabled and an unknown MAC address sends data, the switch presents a security violation.
  - Default number of secure MAC addresses allowed is 1.
- Methods use to configure MAC addresses within port security:
  - Static secure MAC addresses – manually configure

    switchport port-security mac-address *mac-address*
  - Dynamic secure MAC addresses – dynamically learned and removed if the switch restarts
  - Sticky secure MAC addresses – dynamically learned and added to the running configuration (which can later be saved to the startup-config to permanently retain the MAC addresses)

    switchport port-security mac-address sticky mac-address

Note: Disabling sticky learning converts sticky MAC addresses to dynamic secure addresses and removes them from the running-config.

Switch Port Security

Port Security: Violation Modes

- Protect – data from unknown source MAC addresses are dropped; a security notification IS NOT presented by the switch
- Restrict - data from unknown source MAC addresses are dropped; a security notification IS presented by the switch and the violation counter increments.
- Shutdown – (default mode) interface becomes error-disabled and port LED turns off. The violation counter increments. Issues the shutdown and then the no shutdown command on the interface to bring it out of the error-disabled state.

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

Security Violations Occur In These Situations

- A station with MAC address that is not in the address table attempts to access the interface when the table is full.
- An address is being used on two secure interfaces in the same VLAN.

Switch Port Security

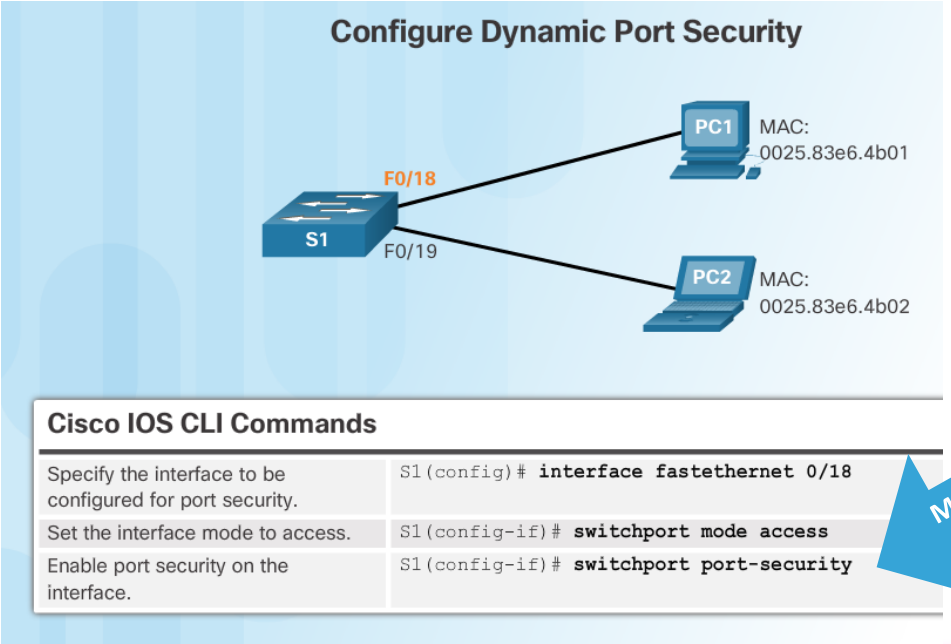
Port Security: Configuring

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Sticky address learning	Disabled

Switch Port Security

Port Security: Configuring (Cont.)

- Before configuring port-security features, place the port in access mode and use the **switchport port-security** interface configuration command to enable port security on an interface.



Switch Port Security

Port Security: Configuring (Cont.)

Configure Sticky Port Security

Cisco IOS CLI Commands

Specify the interface to be configured for port security.	`S1(config)# interface fastethernet 0/19`
Set the interface mode to access.	`S1(config-if)# switchport mode access`
Enable port security on the interface.	`S1(config-if)# switchport port-security`
Set the maximum number of secure addresses allowed on the port.	`S1(config-if)# switchport port-security maximum 10`
Enable sticky learning.	`S1(config-if)# switchport port-security mac-address sticky`

Most common configuration error is to forget this command!

Switch Port Security

Port Security: Verifying

- Use the **show port-security interface** command to verify the maximum number of MAC addresses allowed on a particular port and how many of those addresses were learned dynamically using sticky.

Dynamic

```
S1# show port-security interface fastethernet 0/18
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   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
```

Sticky

```
S1# show port-security interface fastethernet 0/19
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 10
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0025.83e6.4b02:1
Security Violation Count   : 0
```

Switch Port Security

Port Security: Verifying (Cont.)

- Use the **show running-config** command to see learned MAC addresses added to the configuration.

```
S1# show run | begin FastEthernet 0/19
interface FastEthernet0/19
 switchport mode access
 switchport port-security maximum 10
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0025.83e6.4b02
```

- The **show port-security address** command shows how MAC addresses were learned on a particular port.

```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------
Vlan    Mac Address       Type             Ports   Remaining Age
                                                     (mins)
----    -----------       ----             -----   -------------
1       0025.83e6.4b01    SecureDynamic    Fa0/18       -
1       0025.83e6.4b02    SecureSticky     Fa0/19       -
------------------------------------------------------------
```

Switch Port Security

Ports in Error Disabled State

- Switch console messages display when a port security violation occurs. Notice the port link status changes to down.

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18,
putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

Switch Port Security

Ports in Error Disabled State (Cont.)

- Check the port status and the port security settings.

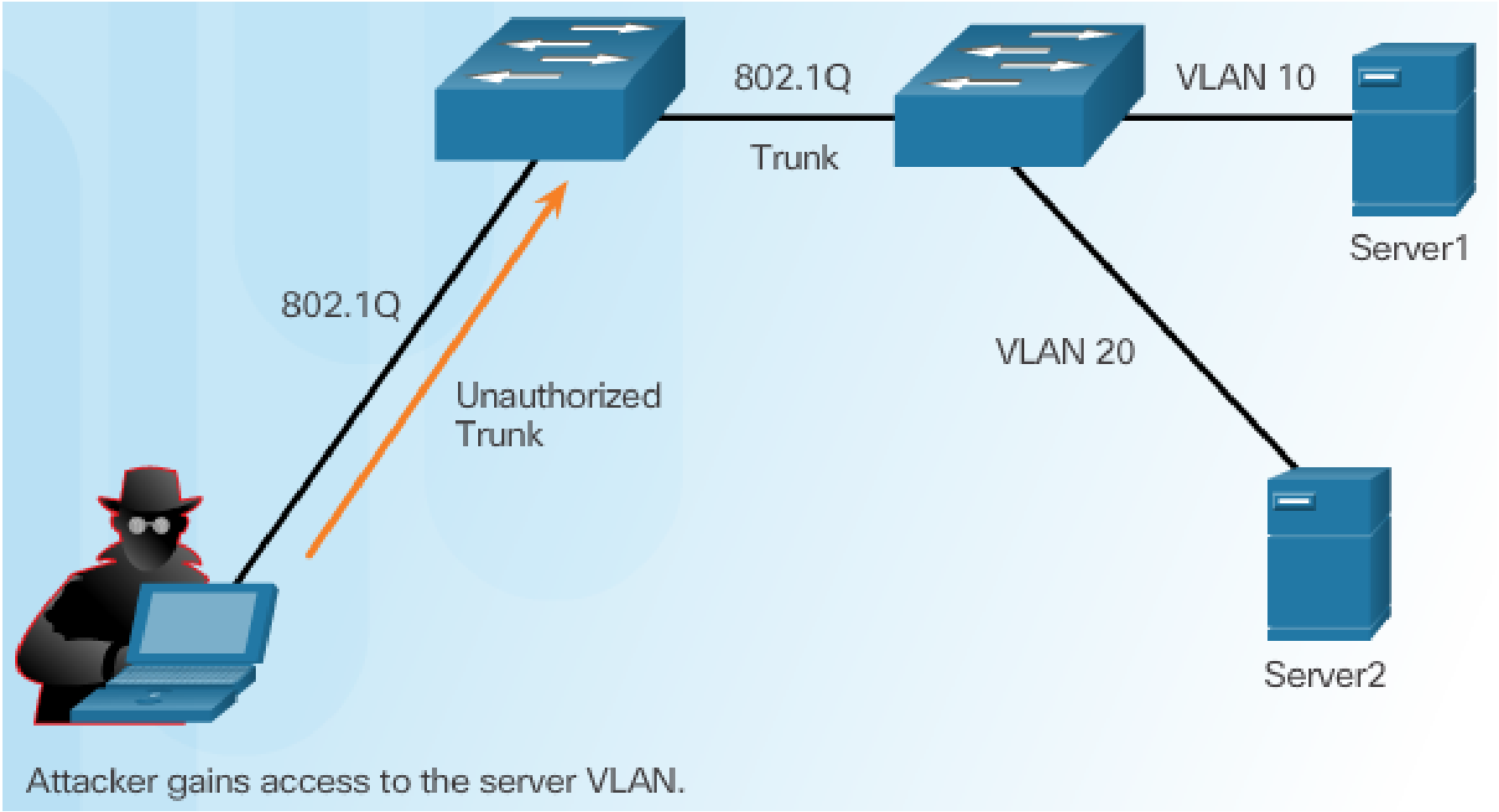
```
S1# show interface fa0/18 status
Port Name   Status        Vlan  Duplex  Speed   Type
Fa0/18      err-disabled  1     auto    auto    10/100BaseTX

S1# show port-security interface fastethernet 0/18
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        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.292b.4c75:1
Security Violation Count   : 1
```

- Do not re-enable a port until the security threat is investigated and eliminated.
- Notice that you must first shut the port down and then issue the **no shutdown** command in order to use the particular port again after a security violation has occurred.

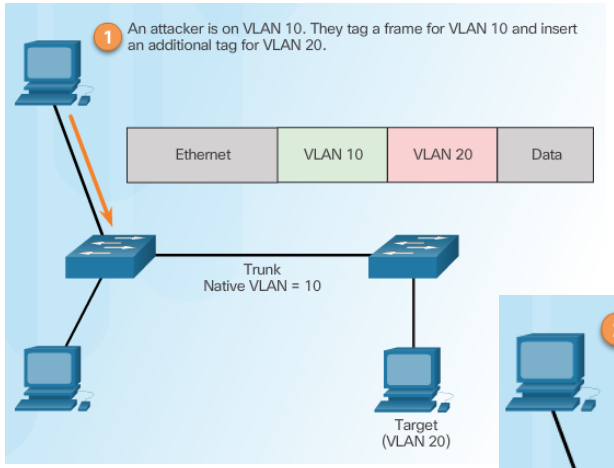
```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
 administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on Interface
 FastEthernet0/18, changed state to up
```

Mitigating VLAN Attacks

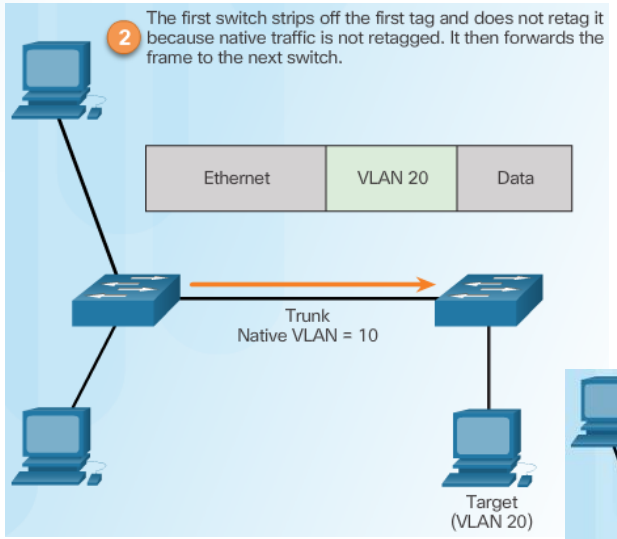
VLAN Hopping Attacks



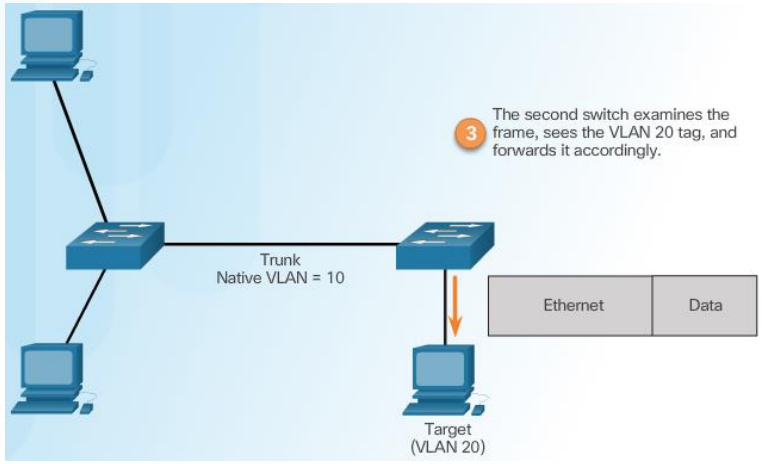
VLAN Double-Tagging Attack



Step 1 – Double Tagging Attack

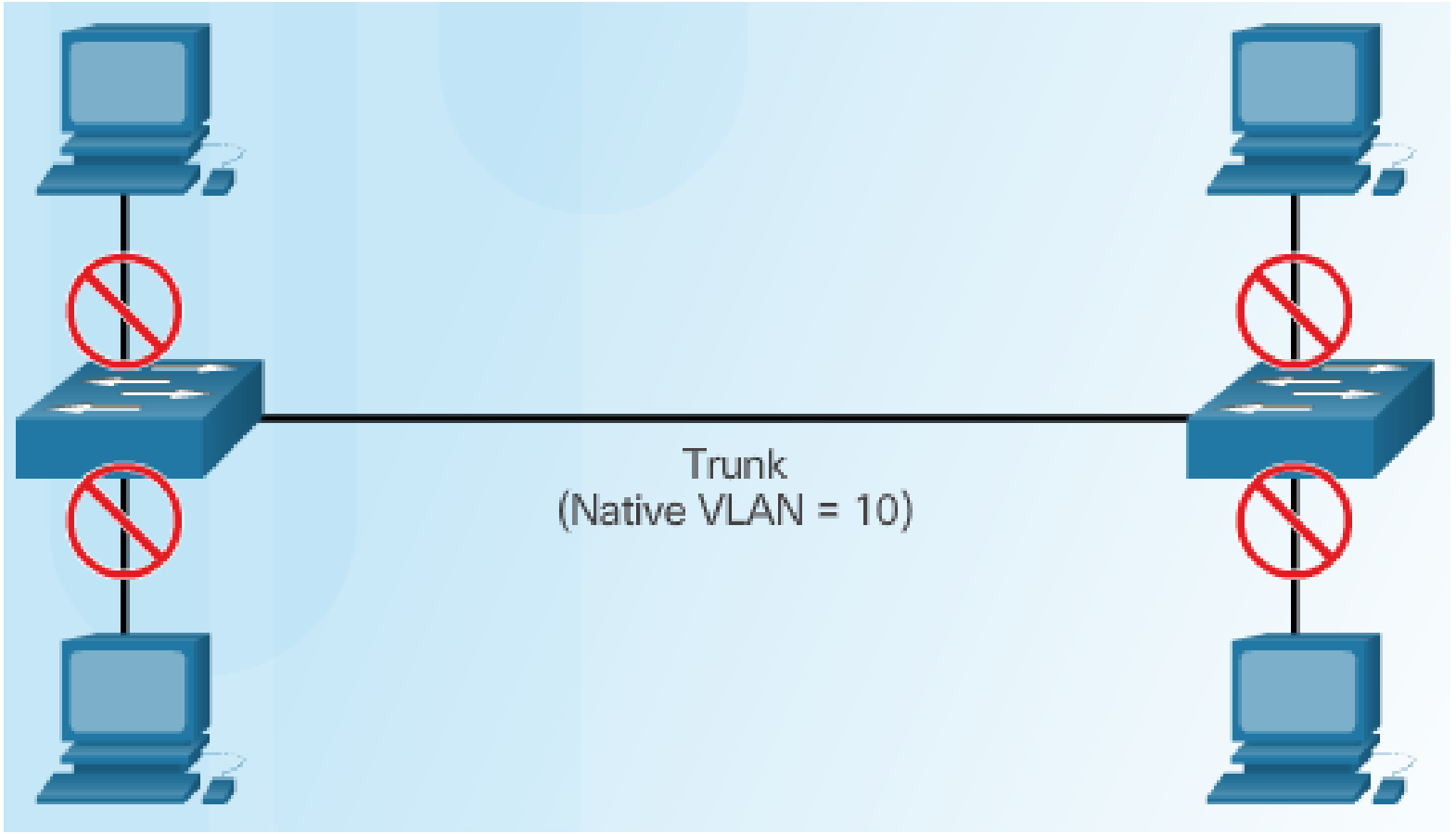


Step 2 – Double Tagging Attack



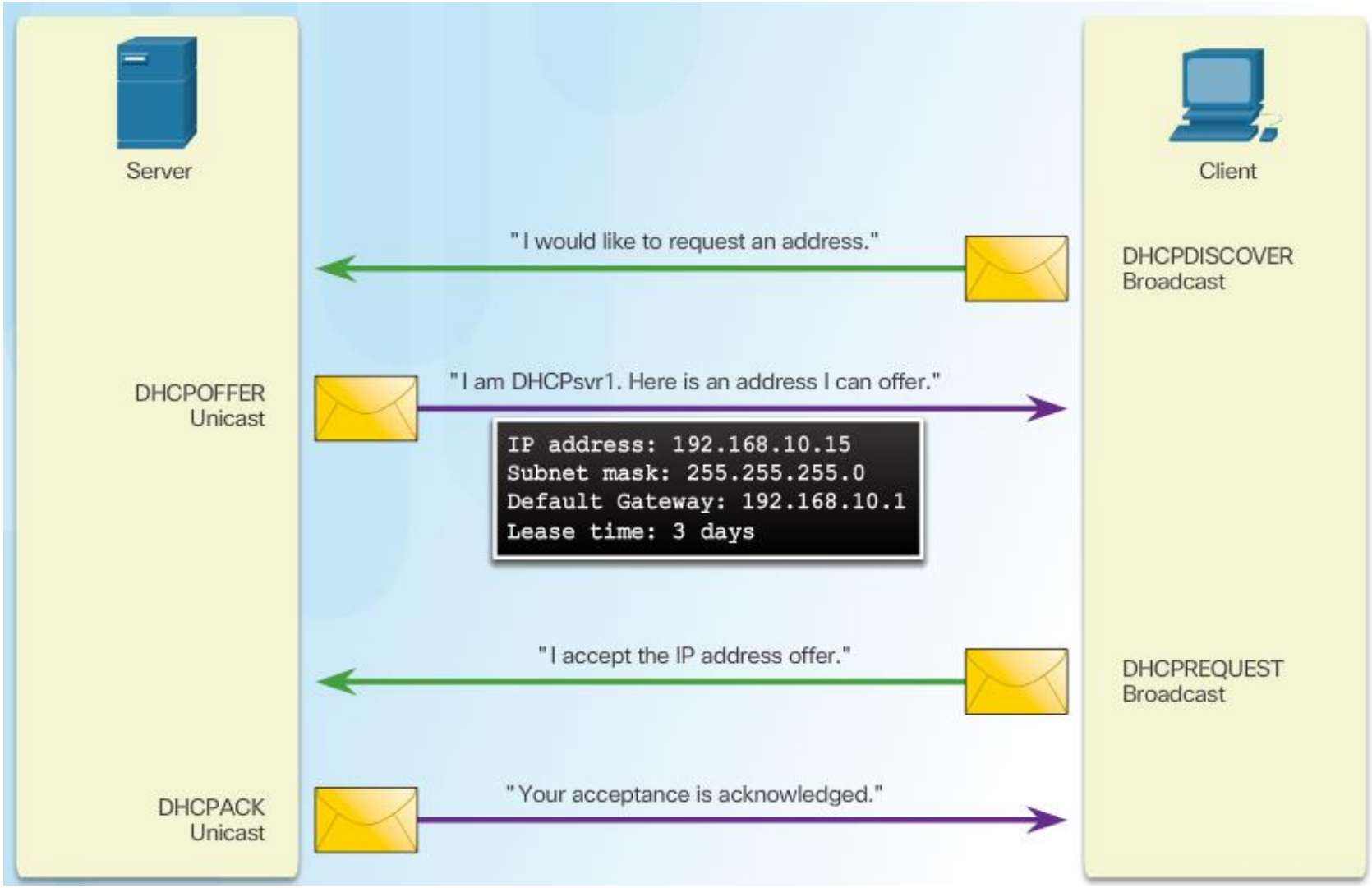
Step 3 – Double Tagging Attack

Mitigating VLAN Hopping Attacks



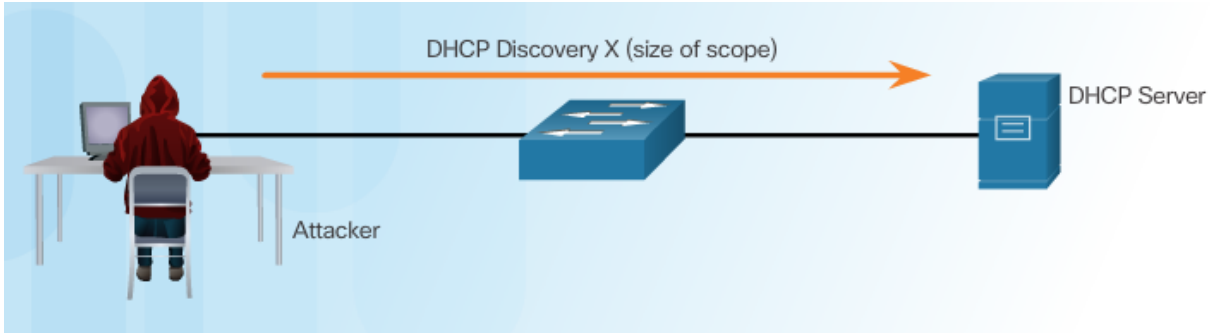
Mitigating DHCP Attacks

DHCP Spoofing Attack

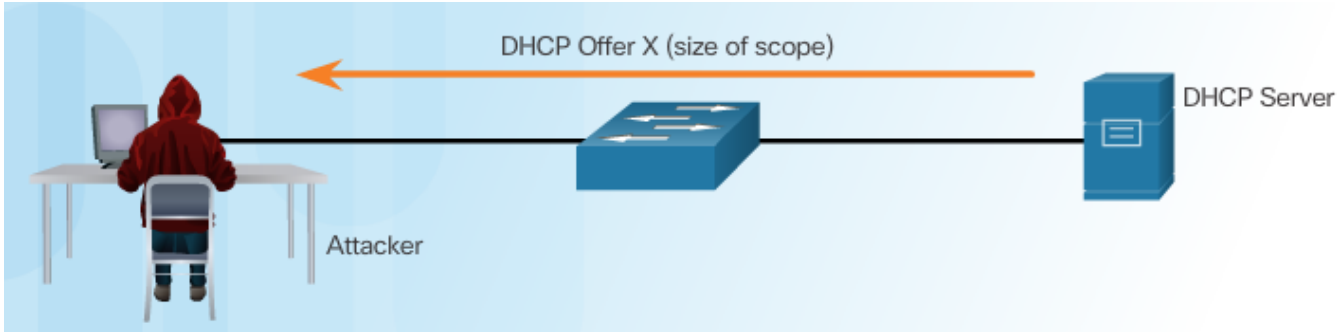


DHCP Starvation Attack

Attacker Initiates a Starvation Attack

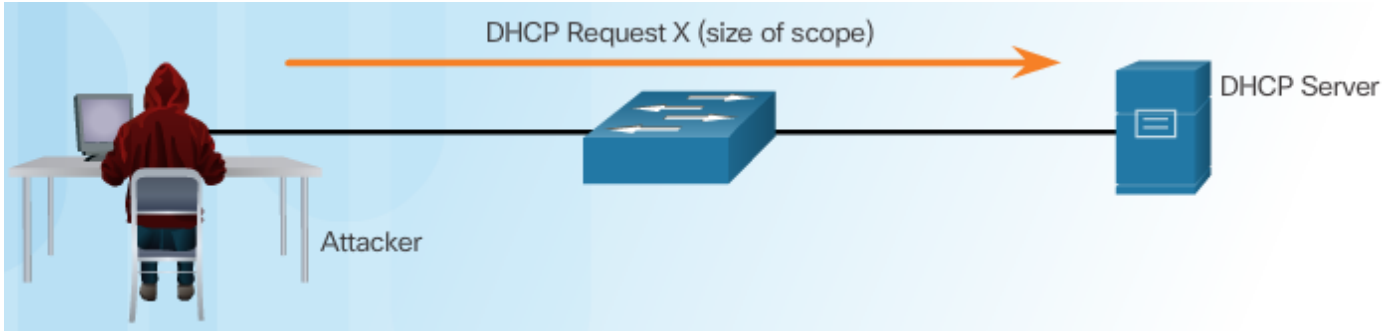


DHCP Server Offers Parameters

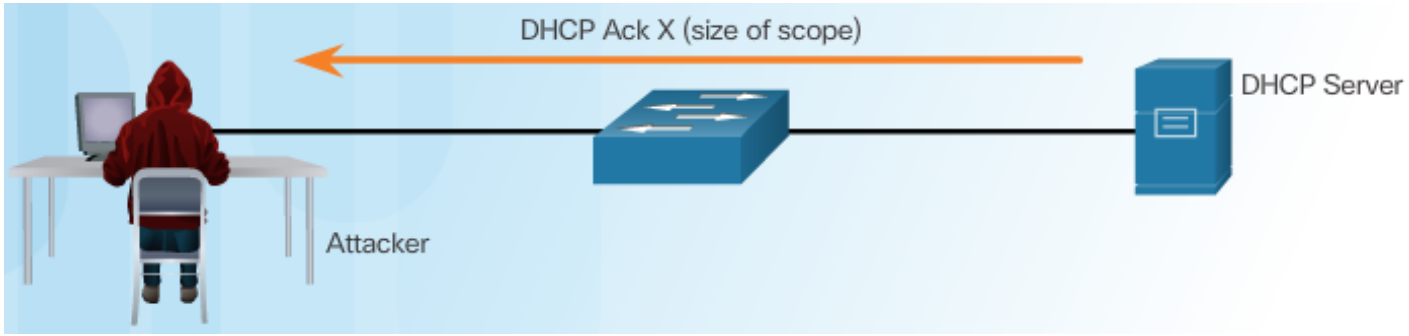


DHCP Starvation Attack

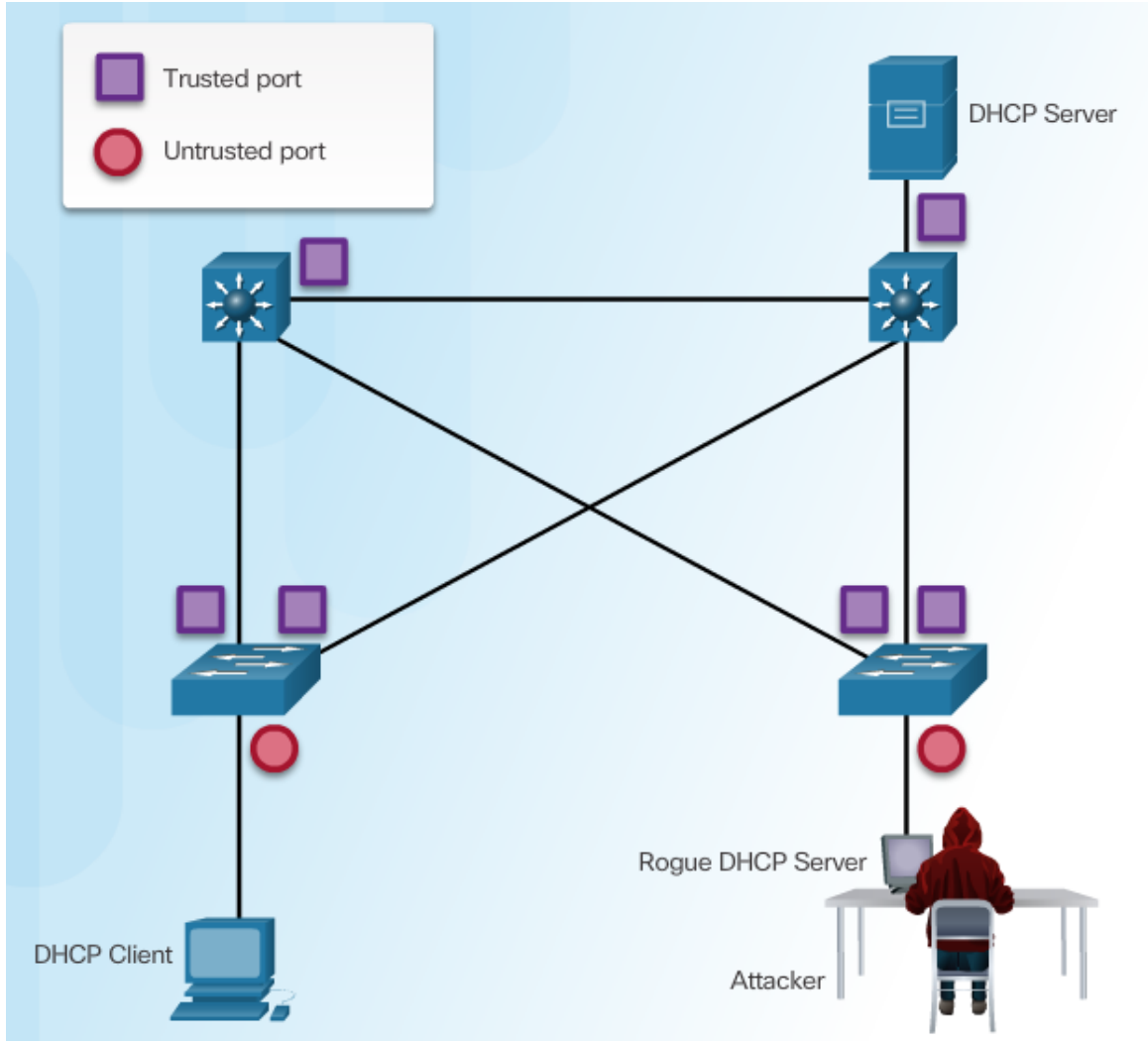
Client Requests all Offers



DHCP Server Acknowledges All Requests



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

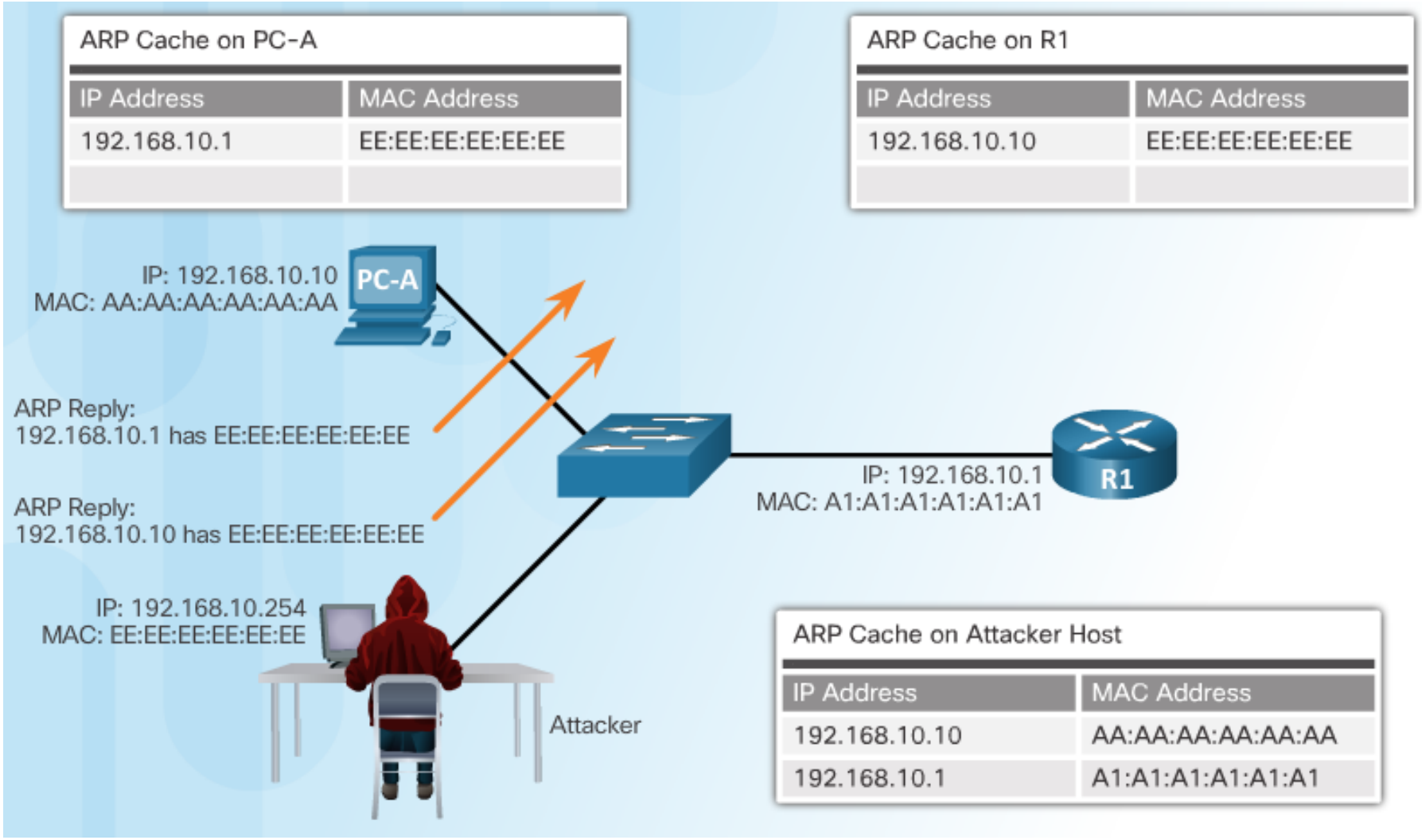
```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

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

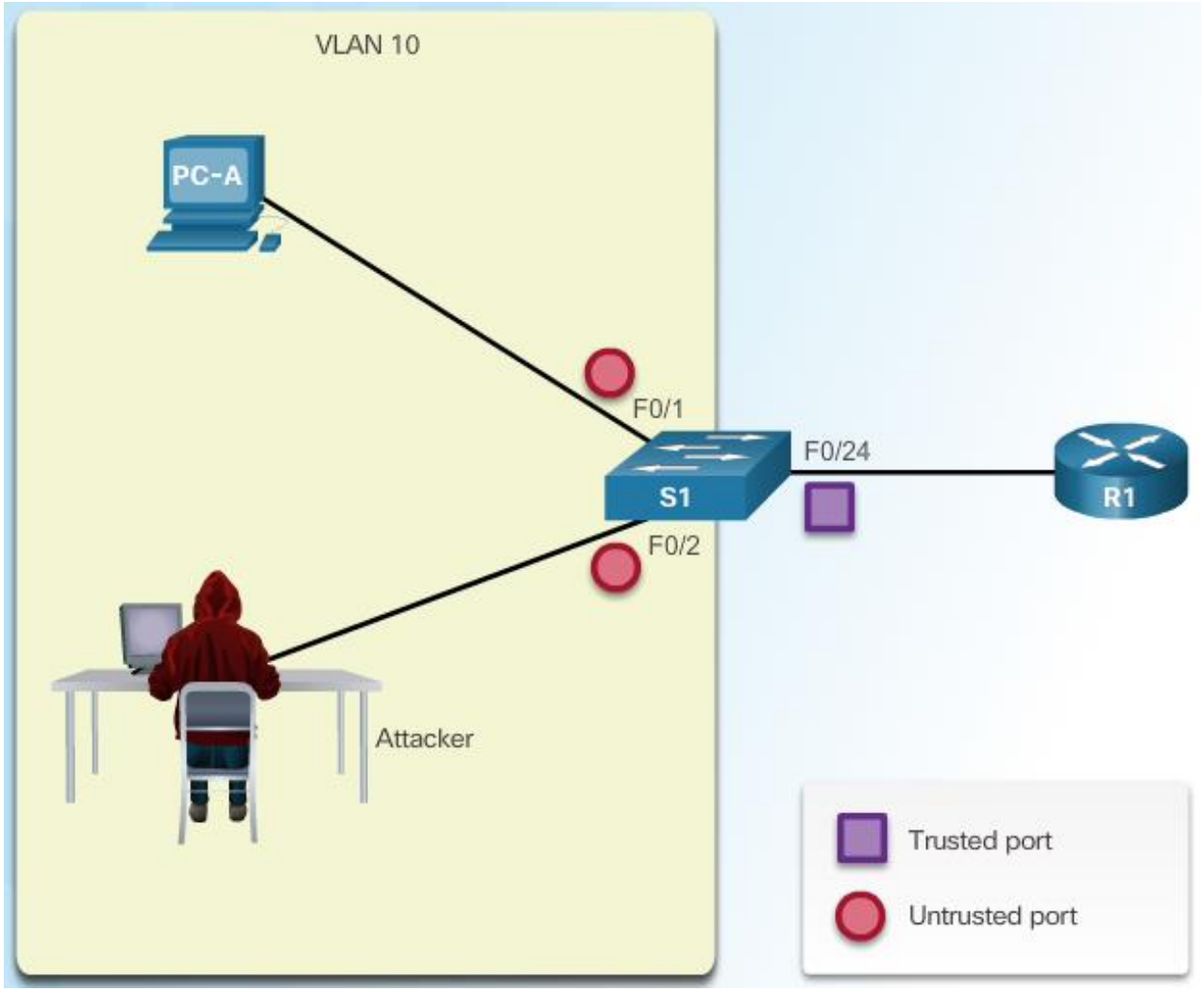
```
S1# show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN Interface
------------------- --------------- ---------- -------------- ---- --------------------
00:03:47:B5:9F:AD   192.168.10.10   193185     dhcp-snooping  5    FastEthernet0/5
```

Mitigating ARP Attacks

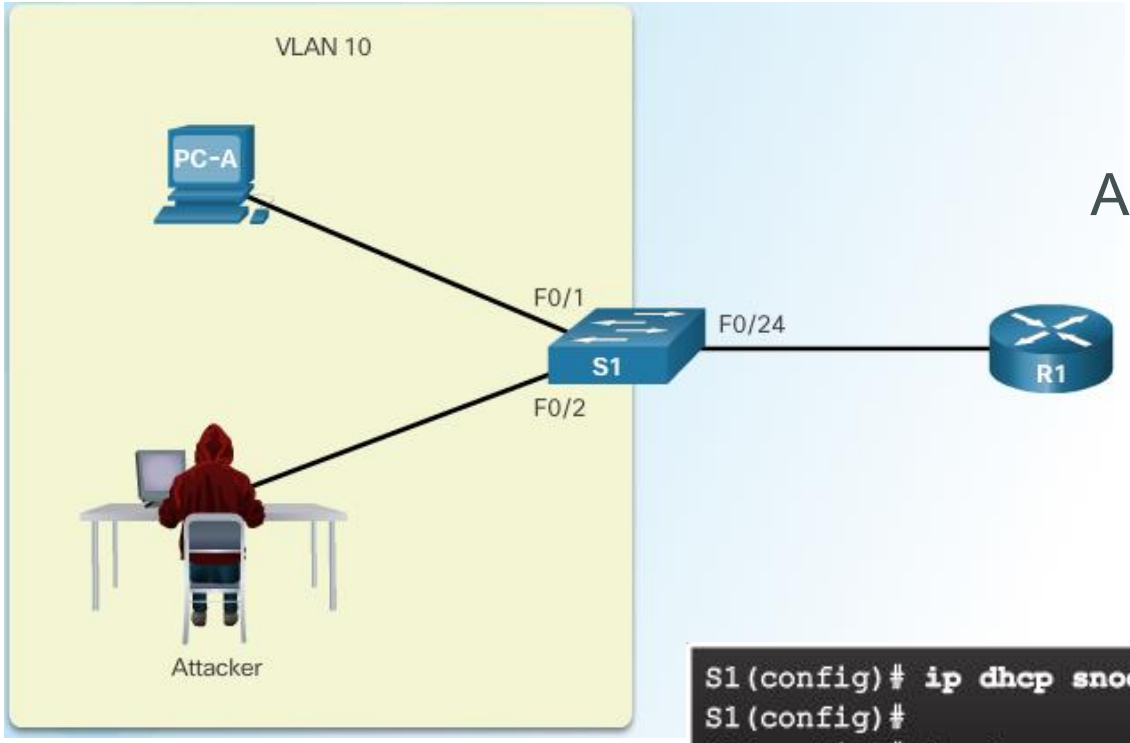
ARP Spoofing and ARP Poisoning Attack



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)#
```

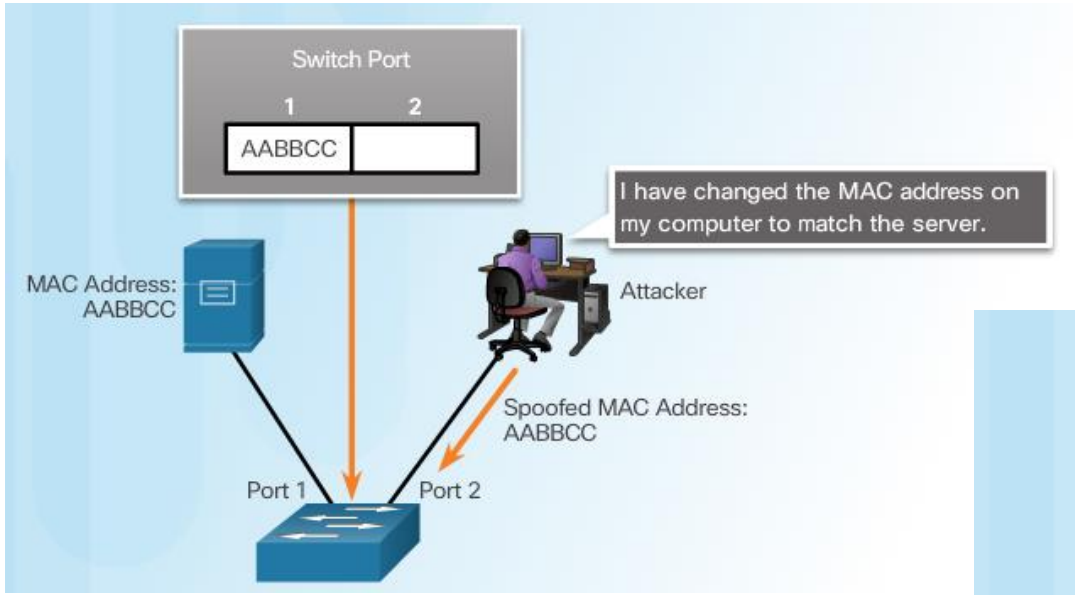
Configuring DHCP Snooping Example

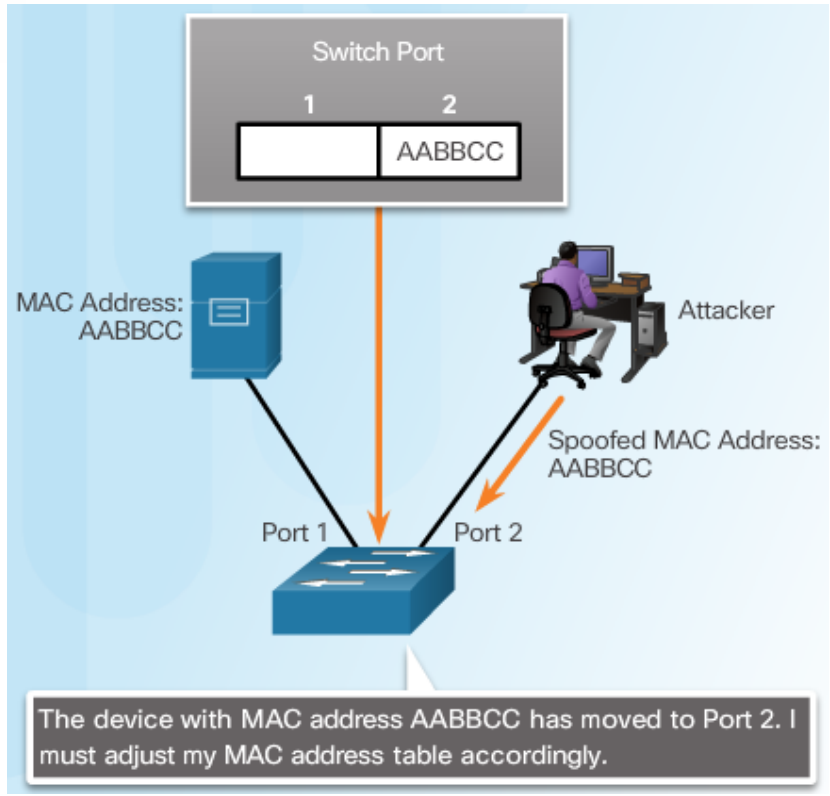
Checking Source, Destination, and IP

```
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

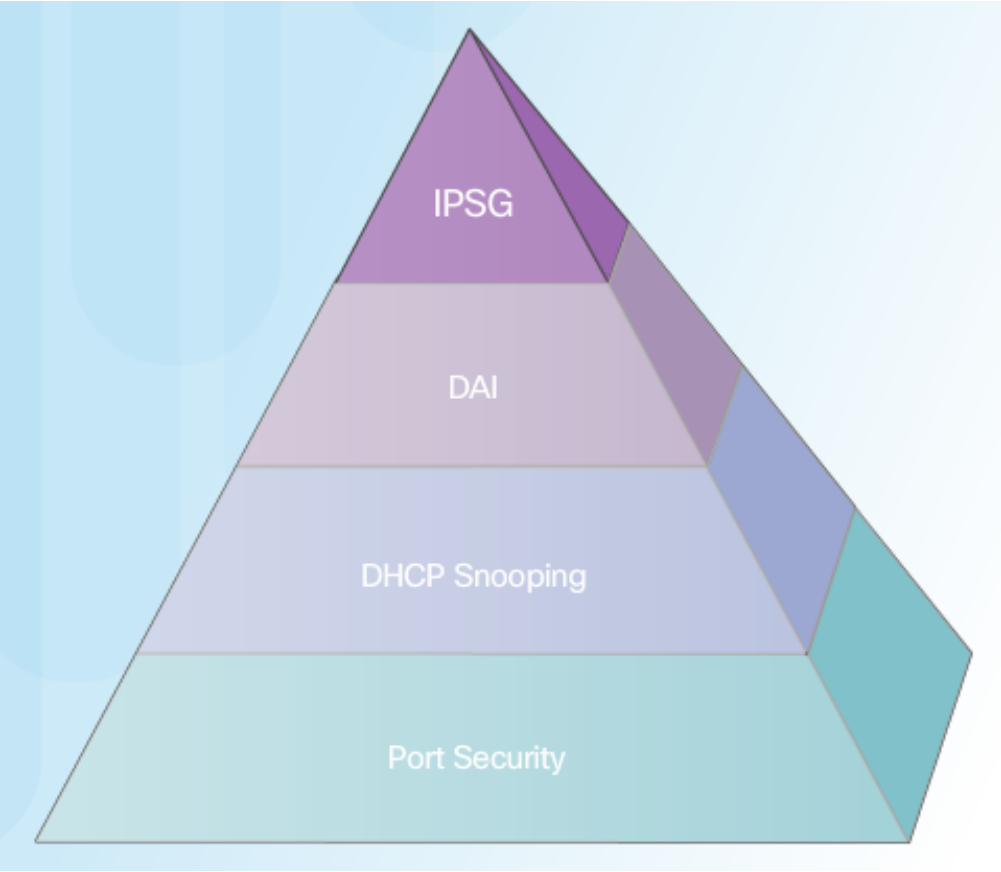




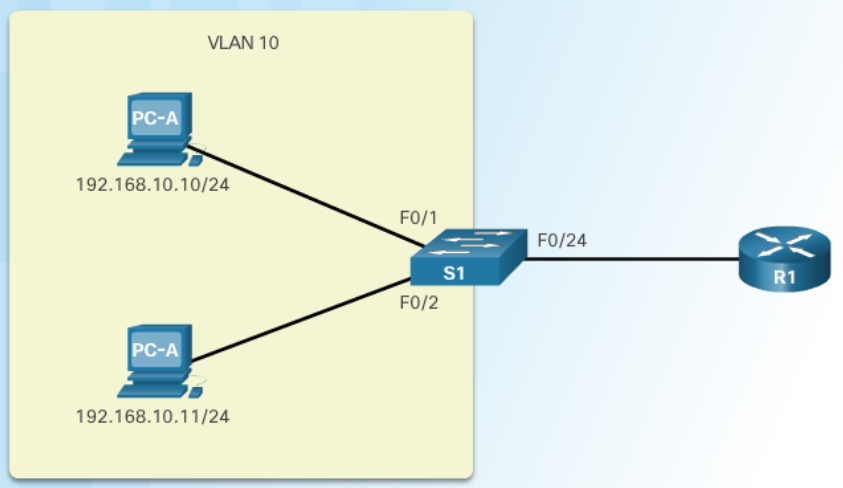
Mitigating Address Spoofing Attacks

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

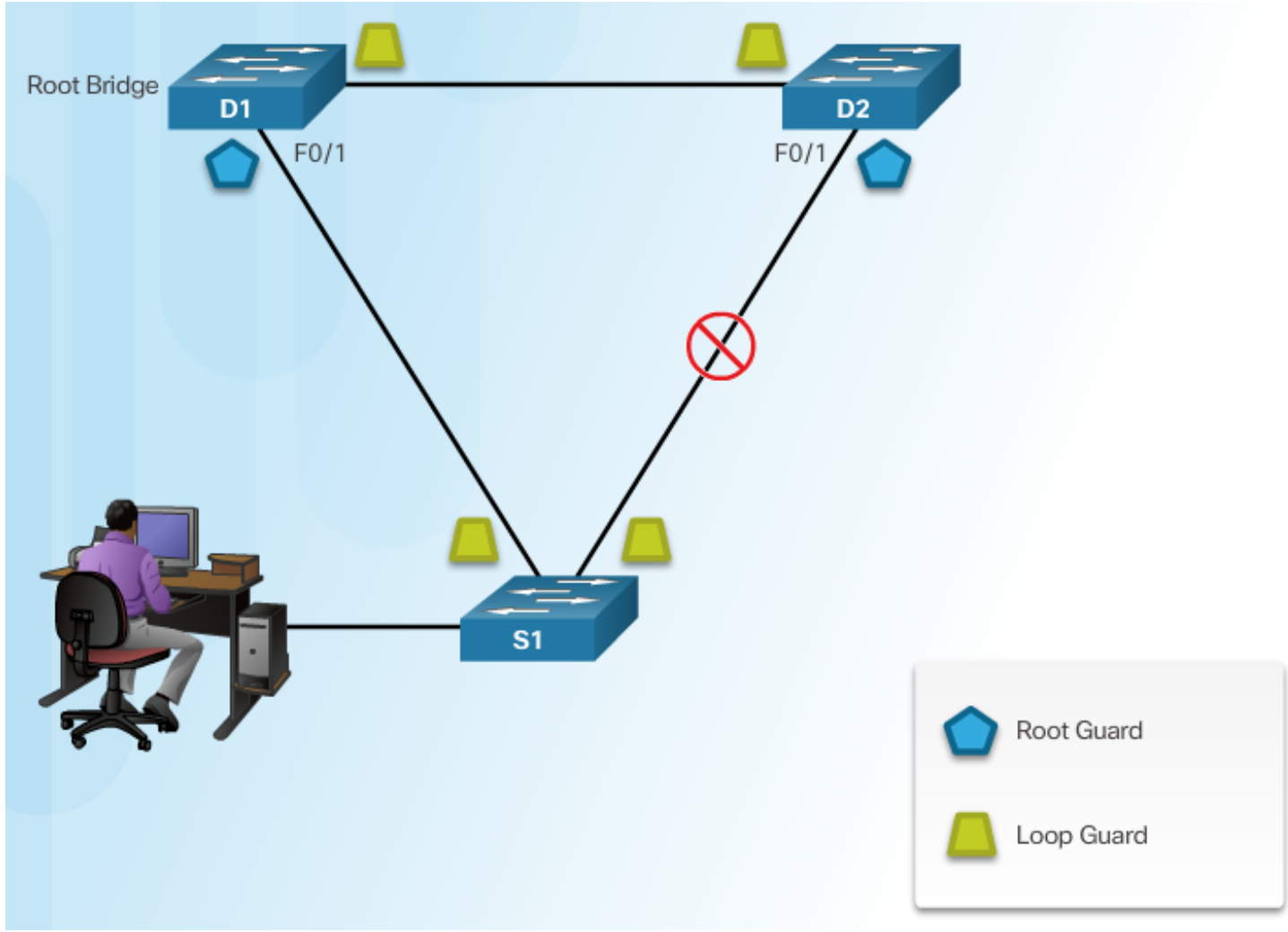
Configuring IP Source Guard

```
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#
```

Configuring Loop Guard



Summary

- Explain endpoint security.
- Describe various types of endpoint security applications.
- Describe Layer 2 vulnerabilities.

Q&A