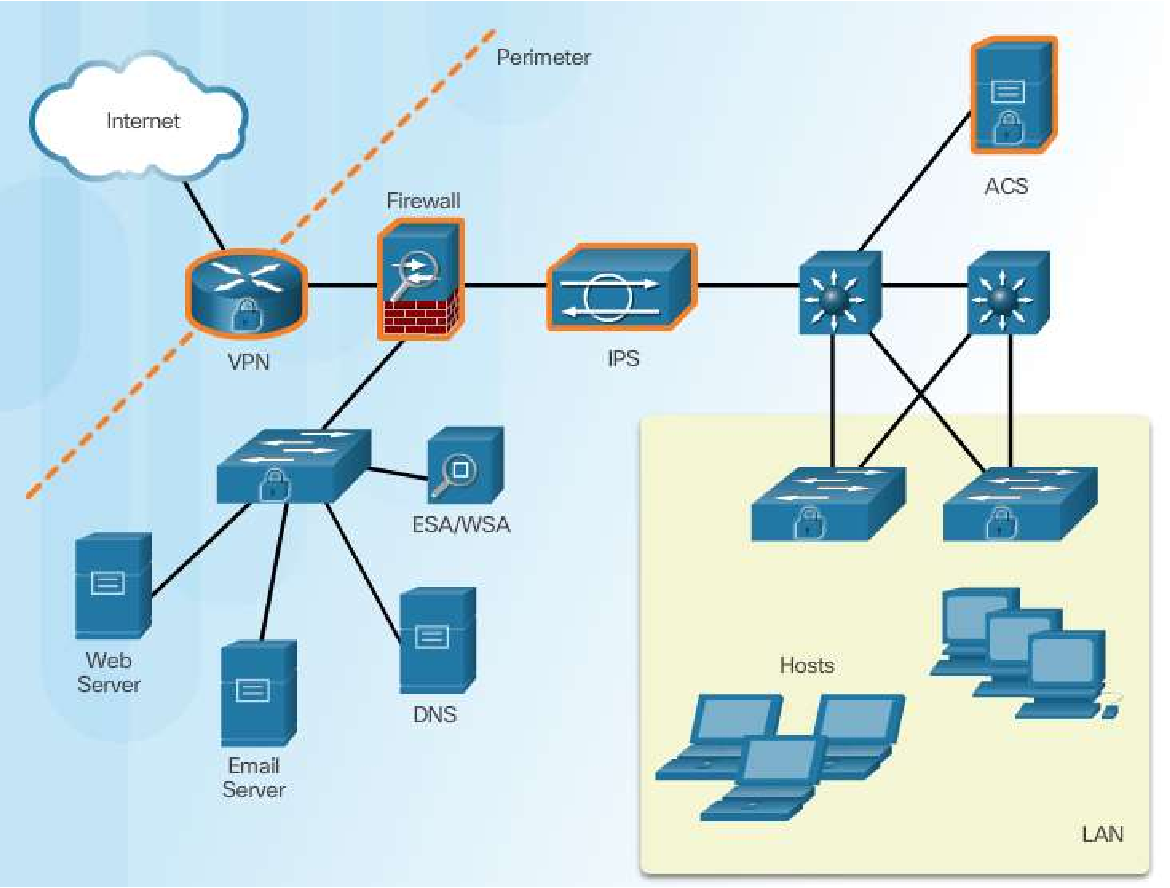
CCS6224
Network Security

Lecture 4
Securing the Local Area Network

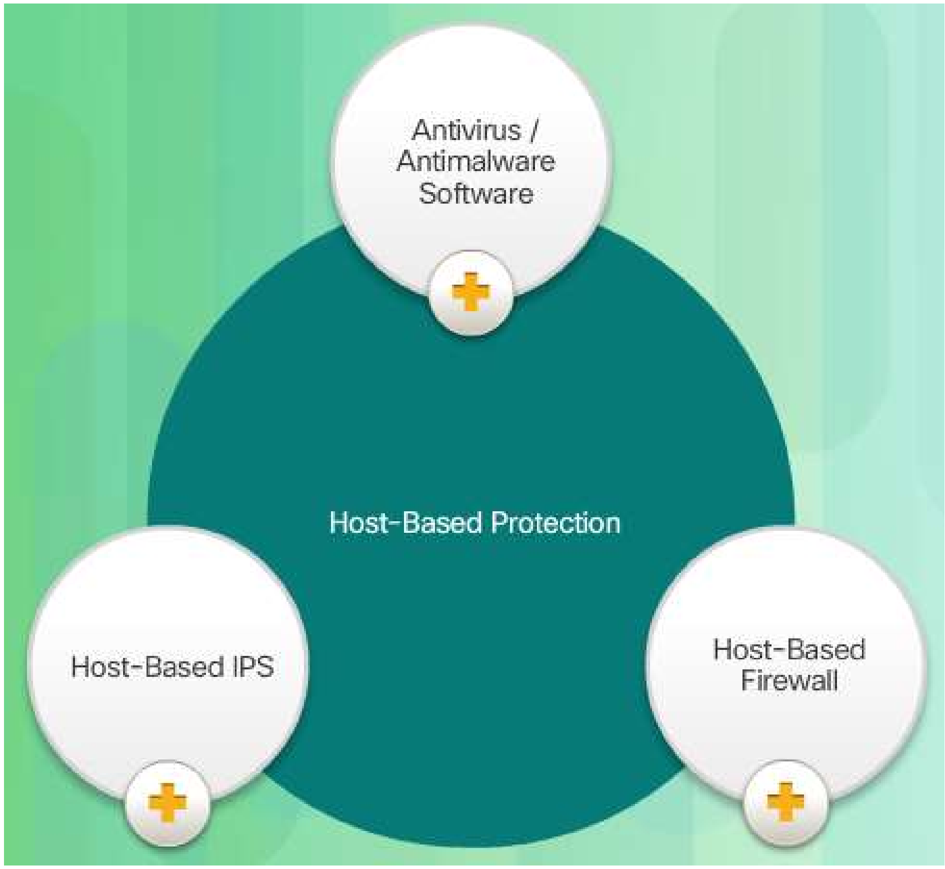
Outline

- Introduction to Endpoint Security
  - Host-Based protection
- Layer 2 Security Threats
  - CAM Table Attack & Mitigation
  - VLAN Attack & Mitigation
  - DHCP Attack & Mitigation
  - ARP Attack & Mitigation
  - Address Spoofing Attack & Mitigation
  - STP Attack & Mitigation

Securing LAN Elements



Endpoint Security



Securing Endpoints in the Borderless Network

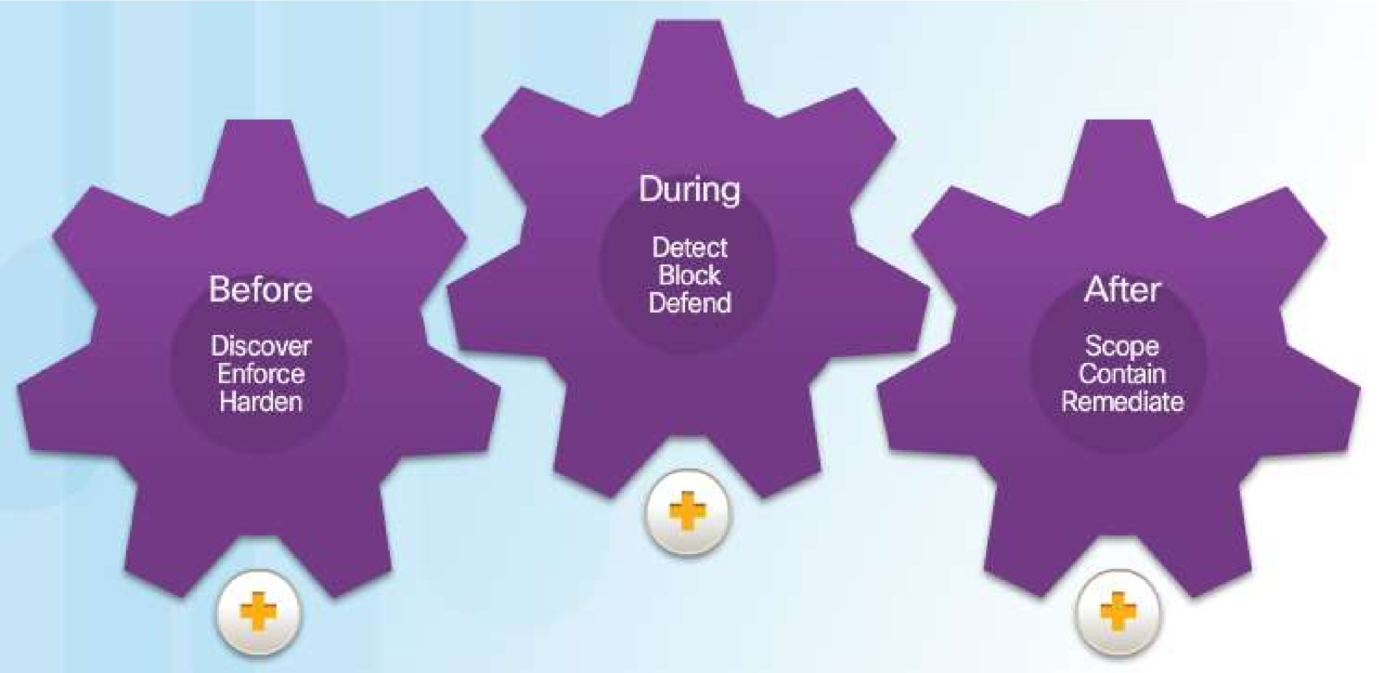
Post malware attack questions:

- Where did it come from?
- What was the threat method and point of entry?
- What systems were affected?
- What did the threat do?
- Can I stop the threat and root cause?
- How do we recover from it?
- How do we prevent it from happening again?

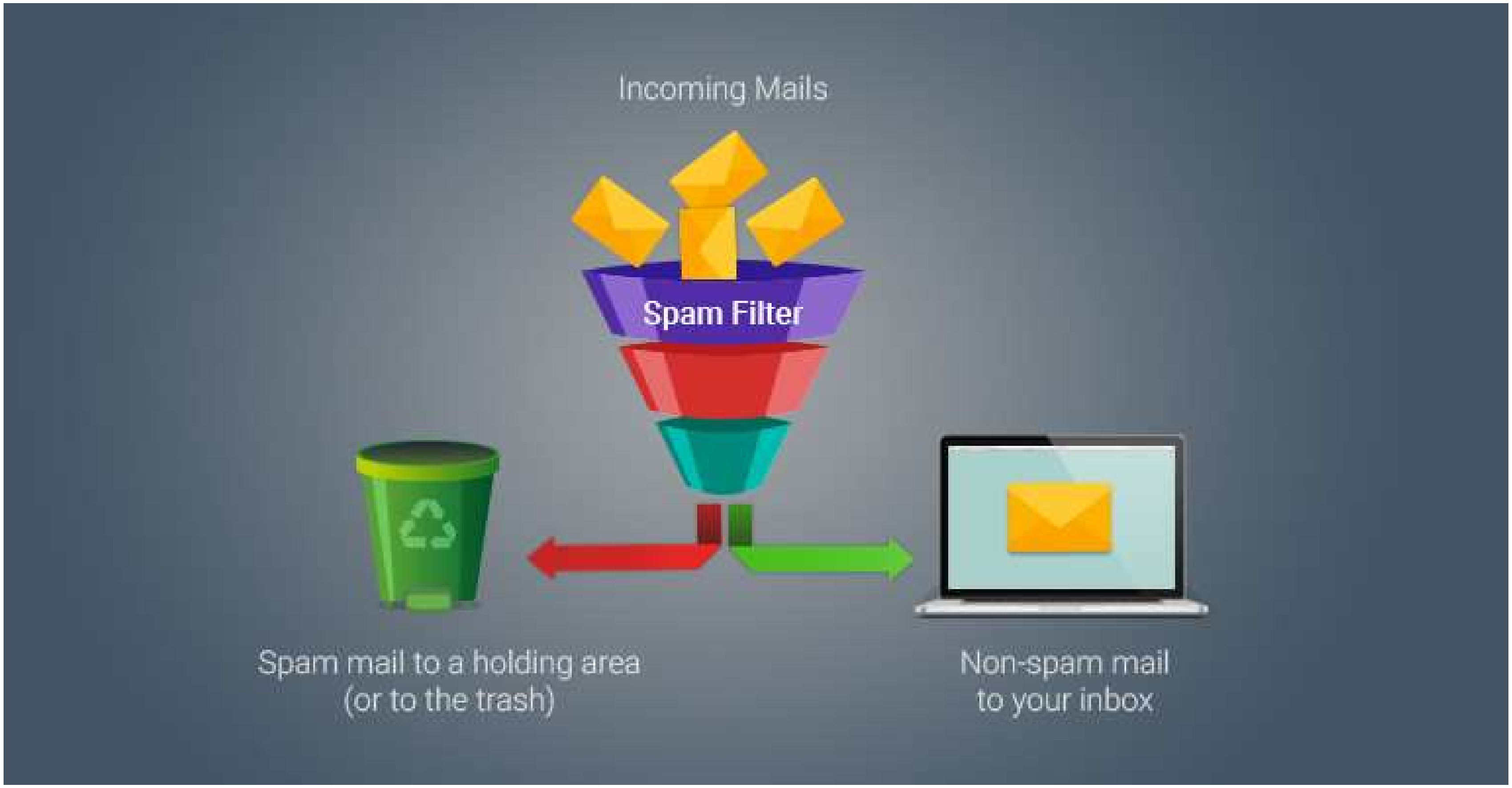
Host-Based Protection:

- Antivirus/Antimalware
- SPAM Filtering
- URL Filtering
- Blacklisting
- Data Loss Prevention (DLP)

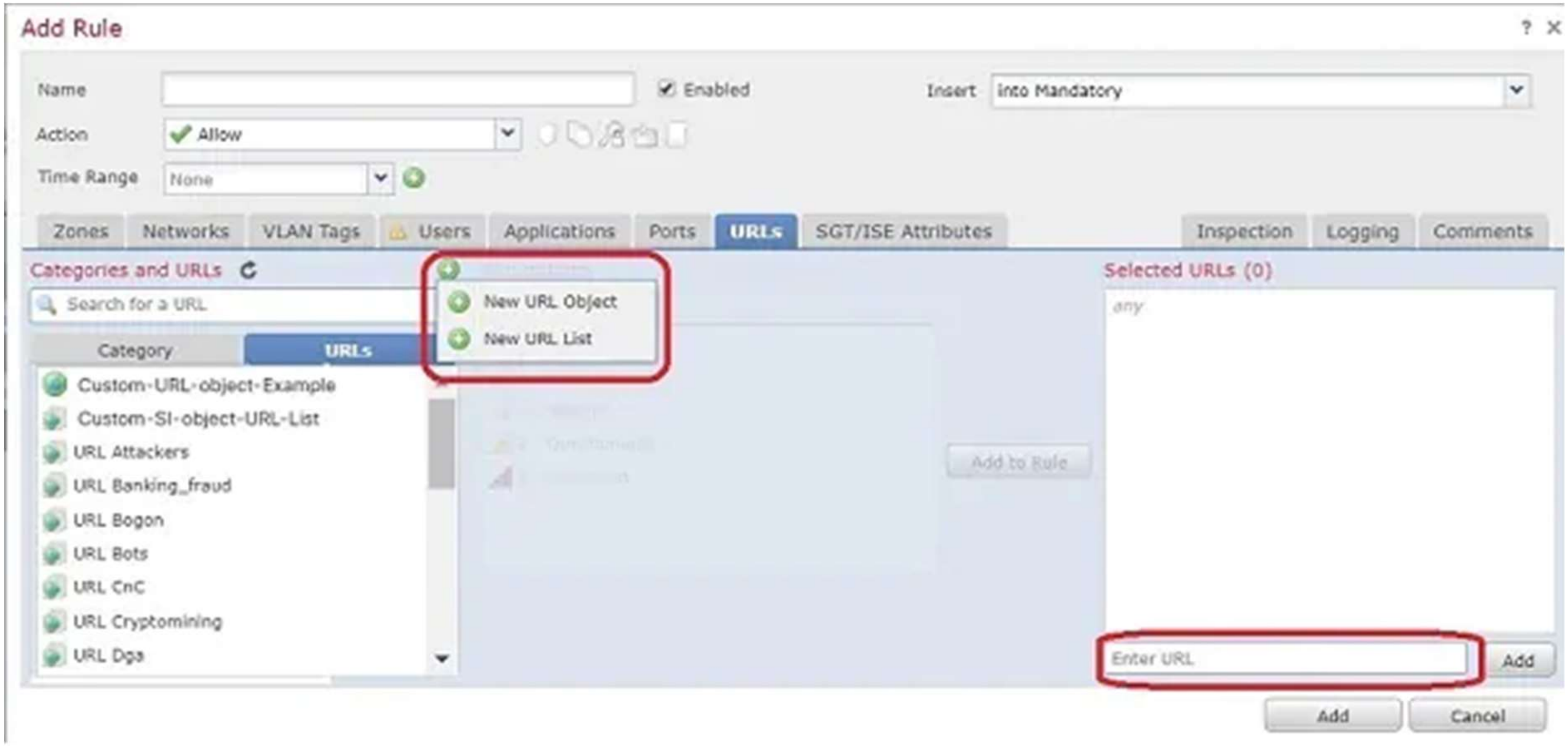
Antimalware Protection



Spam Filtering



URL Filtering



Add Rule

Name:

☑ Enabled

Insert: into Mandatory

Action: ✓ Allow

Time Range: None

Categories and URLs

Search for a URL

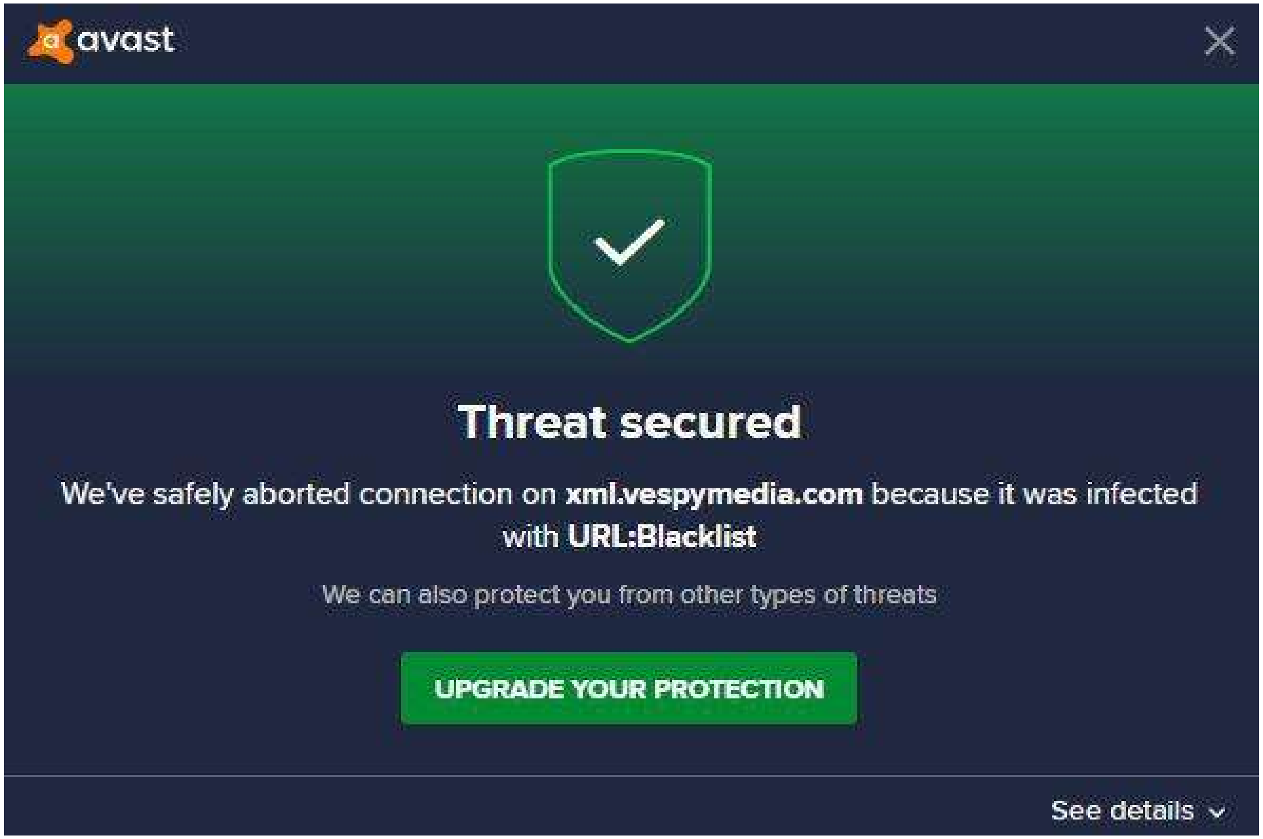
Category | URLs

- Custom-URL-object-Example
- Custom-SI-object-URL-List
- URL Attackers
- URL Banking_fraud
- URL Bogon
- URL Bots
- URL CnC
- URL Cryptomining
- URL Dga

Selected URLs (0)

any

Blacklisting

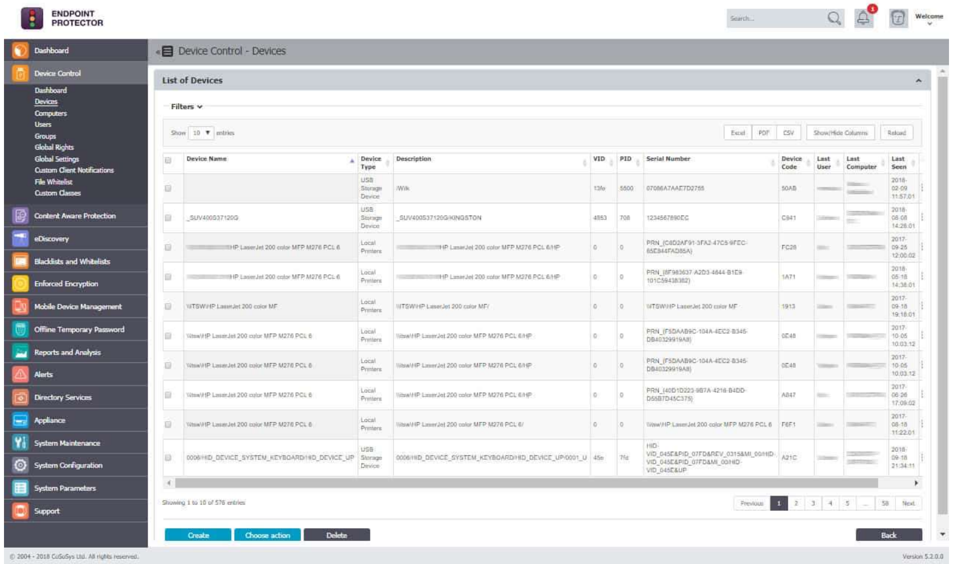


Threat secured

We've safely aborted connection on **xml.vespymedia.com** because it was infected with **URL:Blacklist**

We can also protect you from other types of threats

Data Loss Prevention (DLP)



Device Control - Devices

List of Devices

□	Device Name	Device Type	Description	VID	PID	Serial Number	Device Code	Last User	Last Computer	Last Seen
□		USB Storage Device	/Wik	13fe	5500	07086A7AAE7D2755	50AB	[redacted]	[redacted]	2018-02-09 11:57:01
□	_SUV400S37120G	USB Storage Device	_SUV400S37120G/KINGSTON	4853	708	1234567890EC	C941	[redacted]	[redacted]	2018-08-08 14:26:01
□	[redacted]HP LaserJet 200 color MFP M276 PCL 6	Local Printers	[redacted]HP LaserJet 200 color MFP M276 PCL 6/HP	0	0	PRN_{C8D2AF91-3FA2-47C5-9FEC-65E844FAD85A}	FC28	[redacted]	[redacted]	2017-09-25 12:00:02
□	[redacted]HP LaserJet 200 color MFP M276 PCL 6	Local Printers	[redacted]HP LaserJet 200 color MFP M276 PCL 6/HP	0	0	PRN_{8F983637-A2D3-4844-B1E9-101C59438382}	1A71	[redacted]	[redacted]	2018-05-18 14:38:01
□	\\TSW\HP LaserJet 200 color MF	Local Printers	\\TSW\HP LaserJet 200 color MF/	0	0	\\TSW\HP LaserJet 200 color MF	1913	[redacted]	[redacted]	2017-09-18 19:18:01
□	\\tsw\HP LaserJet 200 color MFP M276 PCL 6	Local Printers	\\tsw\HP LaserJet 200 color MFP M276 PCL 6/HP	0	0	PRN_{F5DAAB9C-104A-4EC2-B345-DB40329919A8}	0E48	[redacted]	[redacted]	2017-10-05 10:03:12
□	\\tsw\HP LaserJet 200 color MFP M276 PCL 6	Local Printers	\\tsw\HP LaserJet 200 color MFP M276 PCL 6/HP	0	0	PRN_{F5DAAB9C-104A-4EC2-B345-DB40329919A8}	0E48	[redacted]	[redacted]	2017-10-05 10:03:12
□	\\tsw\HP LaserJet 200 color MFP M276 PCL 6	Local Printers	\\tsw\HP LaserJet 200 color MFP M276 PCL 6/HP	0	0	PRN_{40D1D223-9B7A-4216-B4DD-D55B7D45C375}	A847	[redacted]	[redacted]	2017-06-26 17:09:02
□	\\tsw\HP LaserJet 200 color MFP M276 PCL 6	Local Printers	\\tsw\HP LaserJet 200 color MFP M276 PCL 6/	0	0	\\tsw\HP LaserJet 200 color MFP M276 PCL 6	F6F1	[redacted]	[redacted]	2017-08-18 11:22:01
□	0006/HID_DEVICE_SYSTEM_KEYBOARD/HID_DEVICE_UP	USB Storage Device	0006/HID_DEVICE_SYSTEM_KEYBOARD/HID_DEVICE_UP/0001_U	45e	7fd	HID-VID_045E&PID_07FD&REV_0315&MI_00/HID-VID_045E&PID_07FD&MI_00/HID-VID_045E&UP	A21C	[redacted]	[redacted]	2018-09-18 21:34:11

Showing 1 to 10 of 576 entries

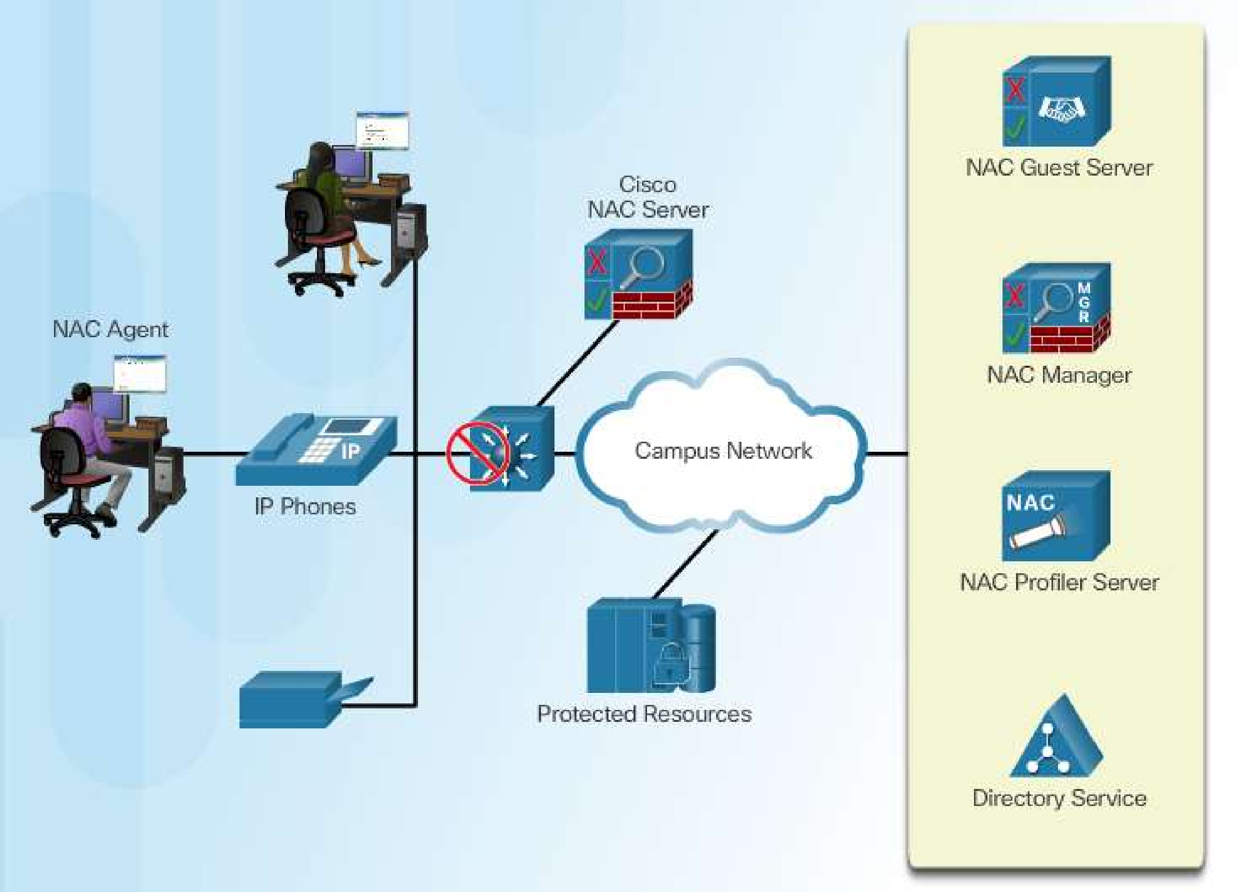
© 2004 - 2018 CoSoSys Ltd. All rights reserved.

Version 5.2.0.0

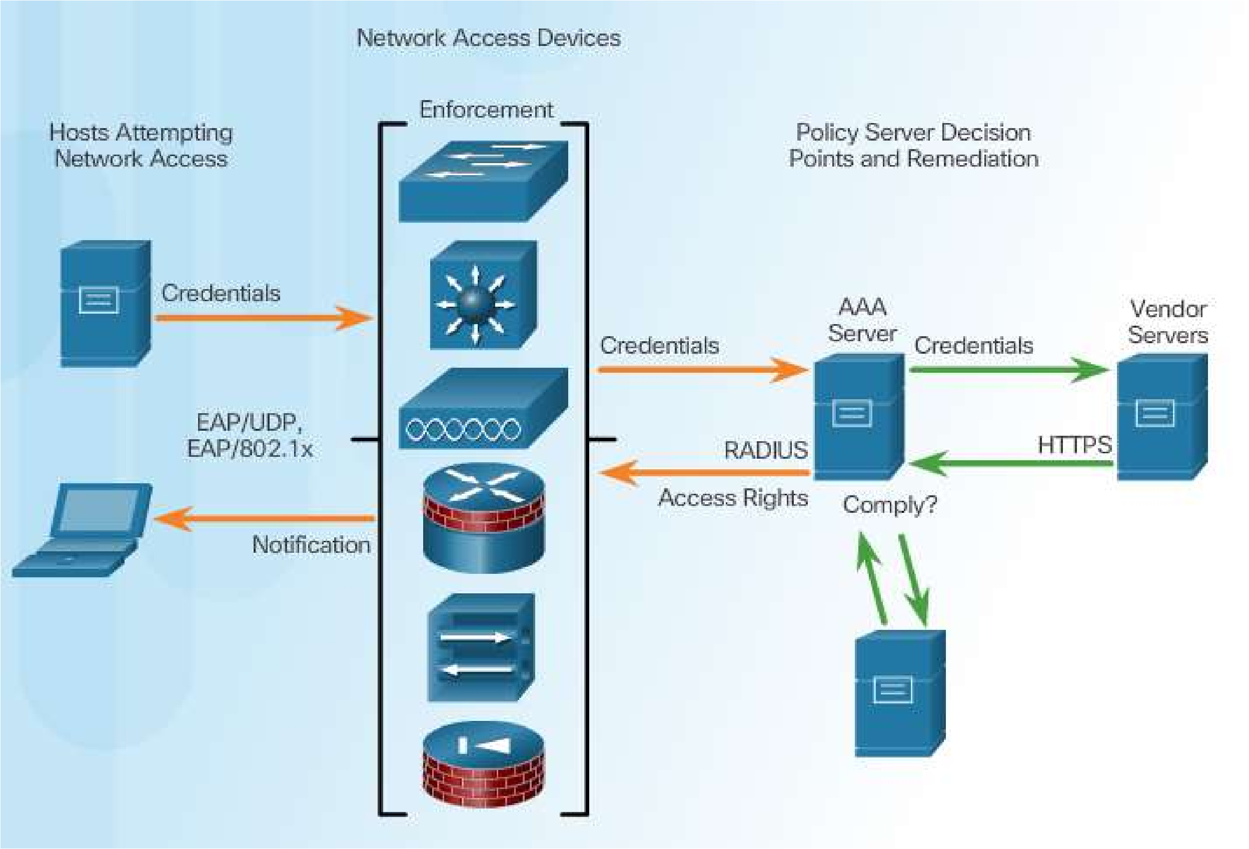
DLP provides services and protections:

- Detailed logging and forensic evidence gathering
- User/Administrator notification
- Real time prevention and blocking
- Quarantine of confidential data

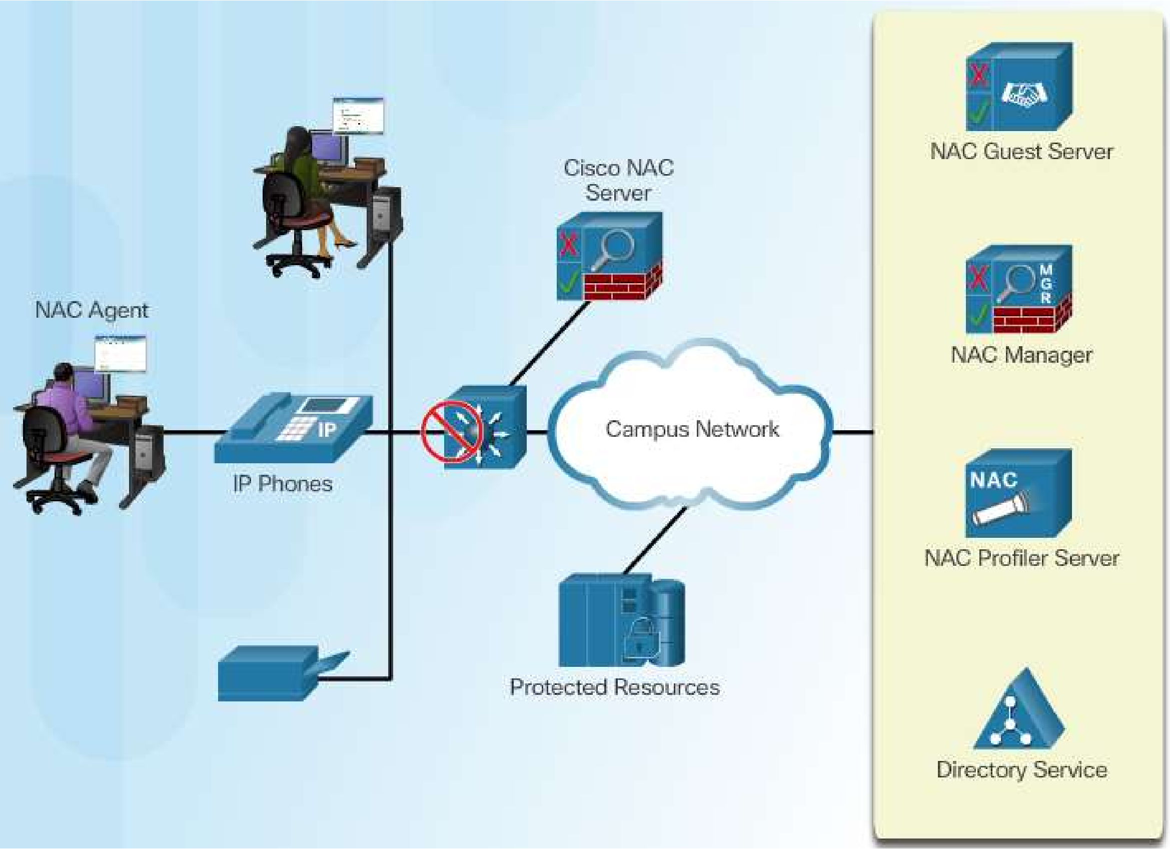
Cisco Network Access Control



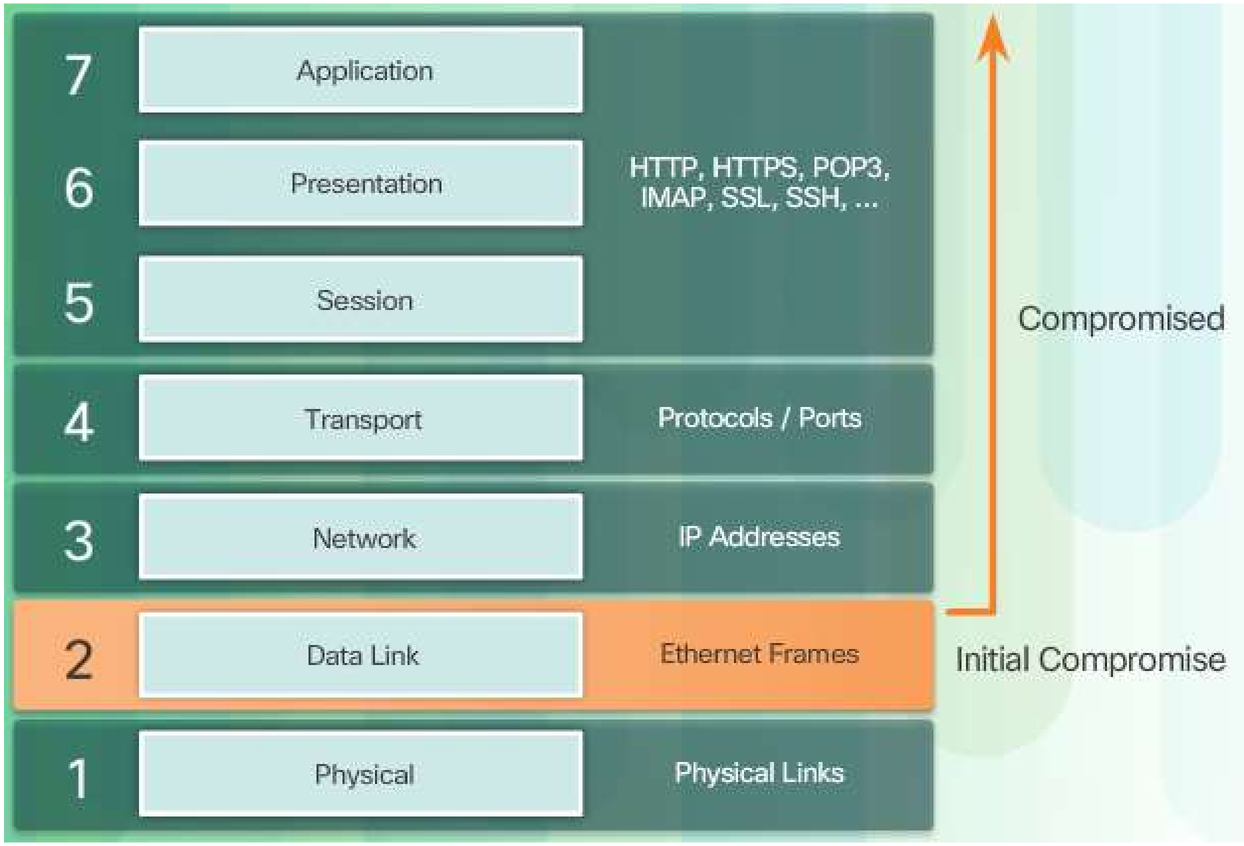
Cisco NAC Functions



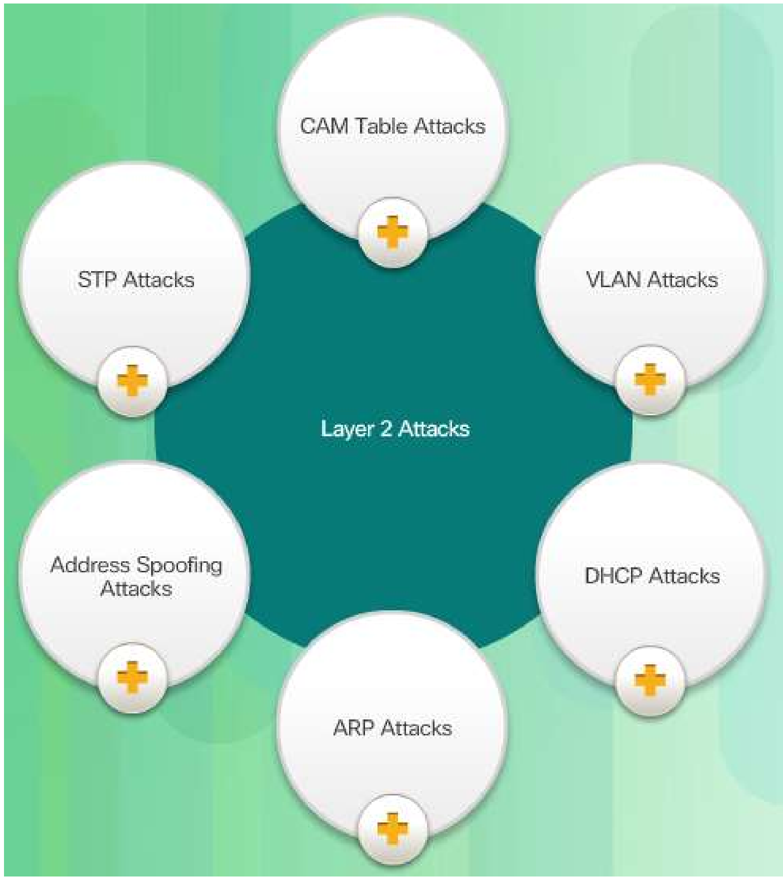
Cisco NAC Components



Layer 2 Security Threats

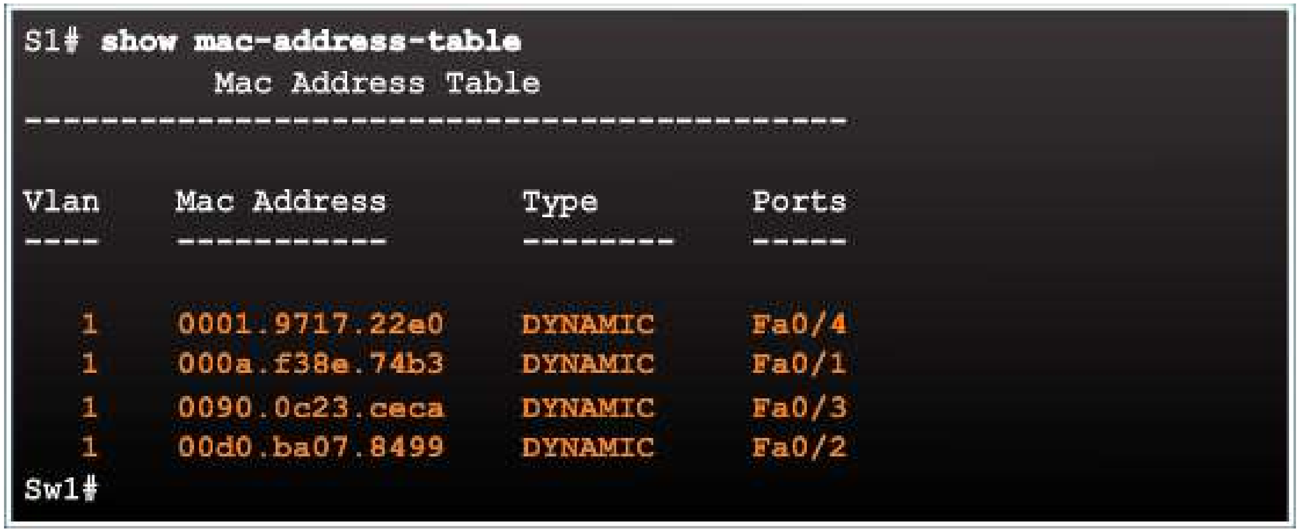


Switch Attack Categories



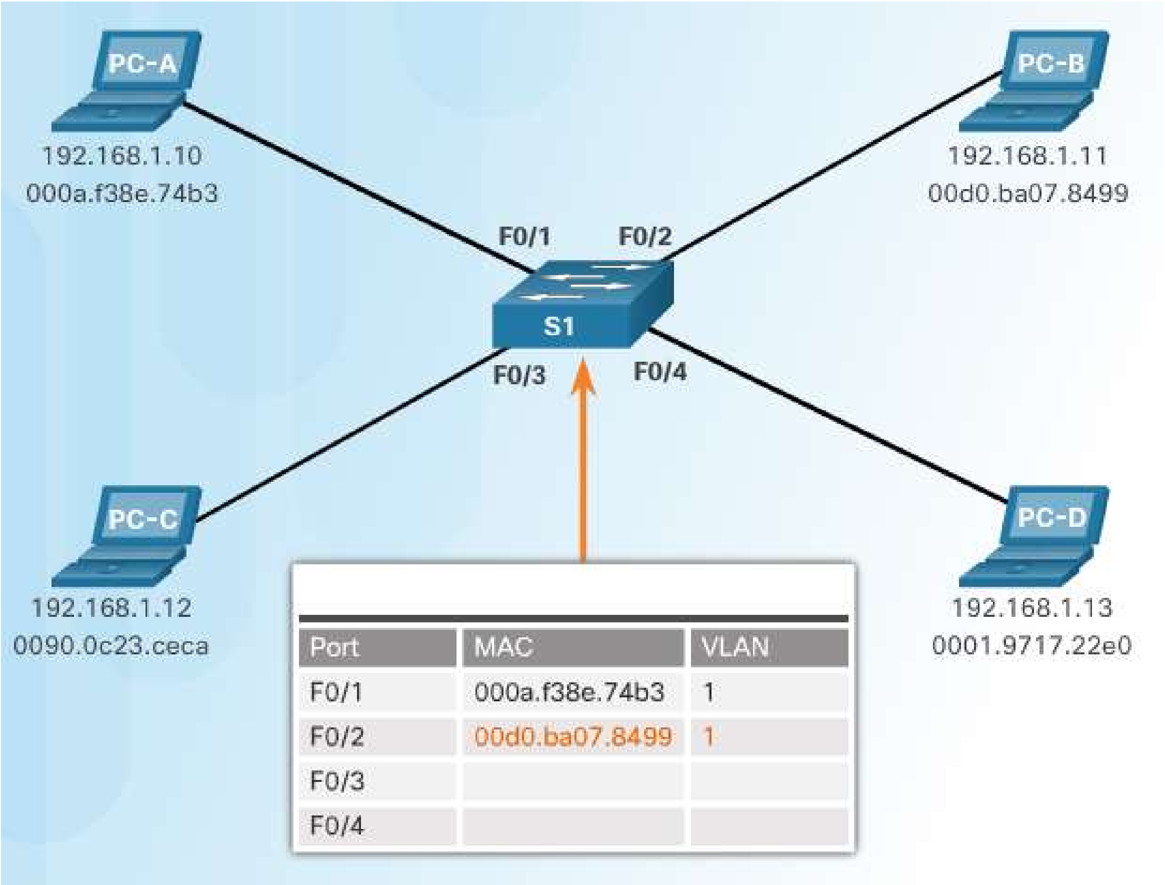
CAM Table Attack

Basic Switch Operation



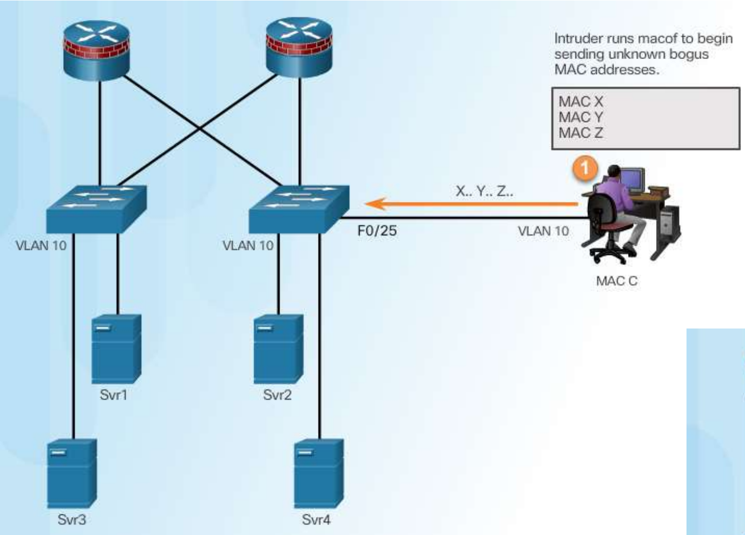
```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

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



Port	MAC	VLAN
F0/1	000a.f38e.74b3	1
F0/2	00d0.ba07.8499	1
F0/3		
F0/4		

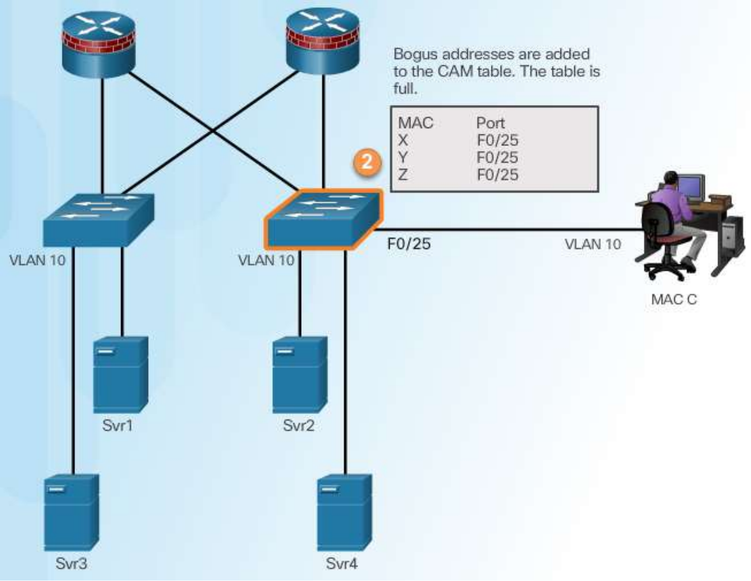
CAM Table Attack


Intruder runs macof to begin sending unknown bogus MAC addresses.

MAC X
MAC Y
MAC Z

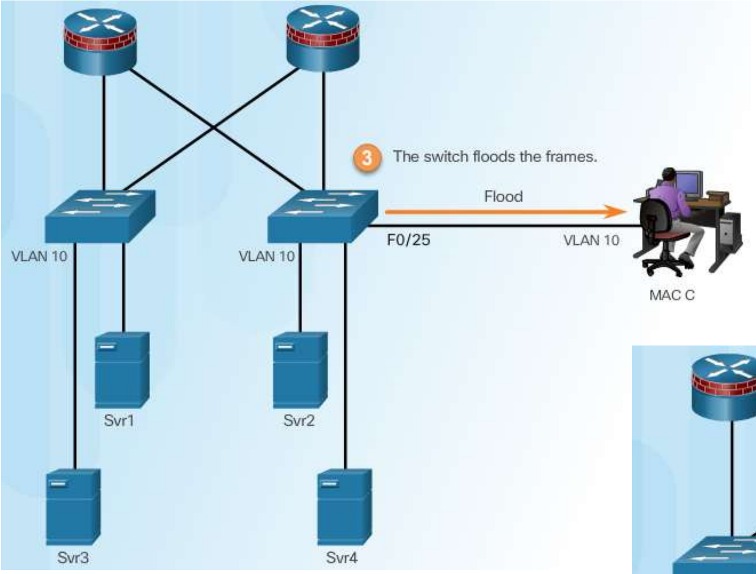
Intruder Runs Attack Tool

Fill CAM Table

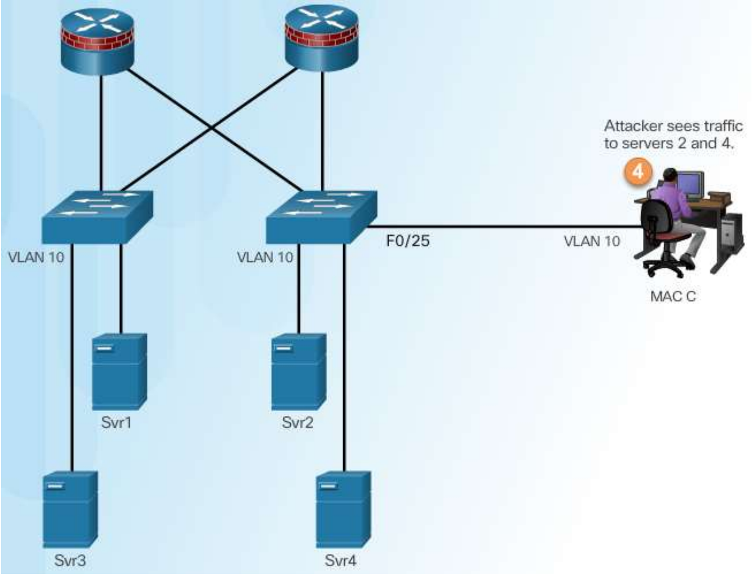

Bogus addresses are added to the CAM table. The table is full.

MAC	Port
X	F0/25
Y	F0/25
Z	F0/25

CAM Table Attack

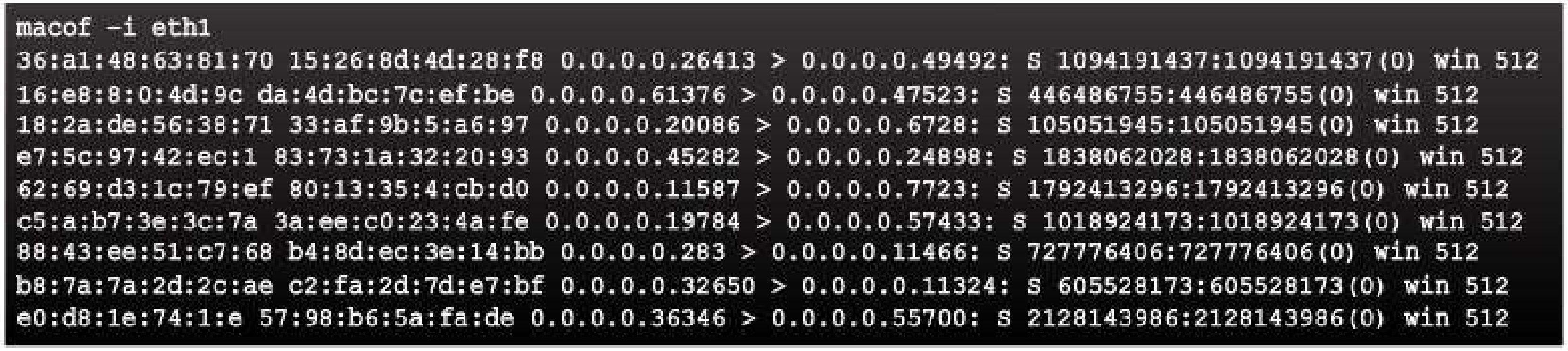


Switch Floods All Traffic



Attacker Captures Traffic

CAM Table Attack Tools

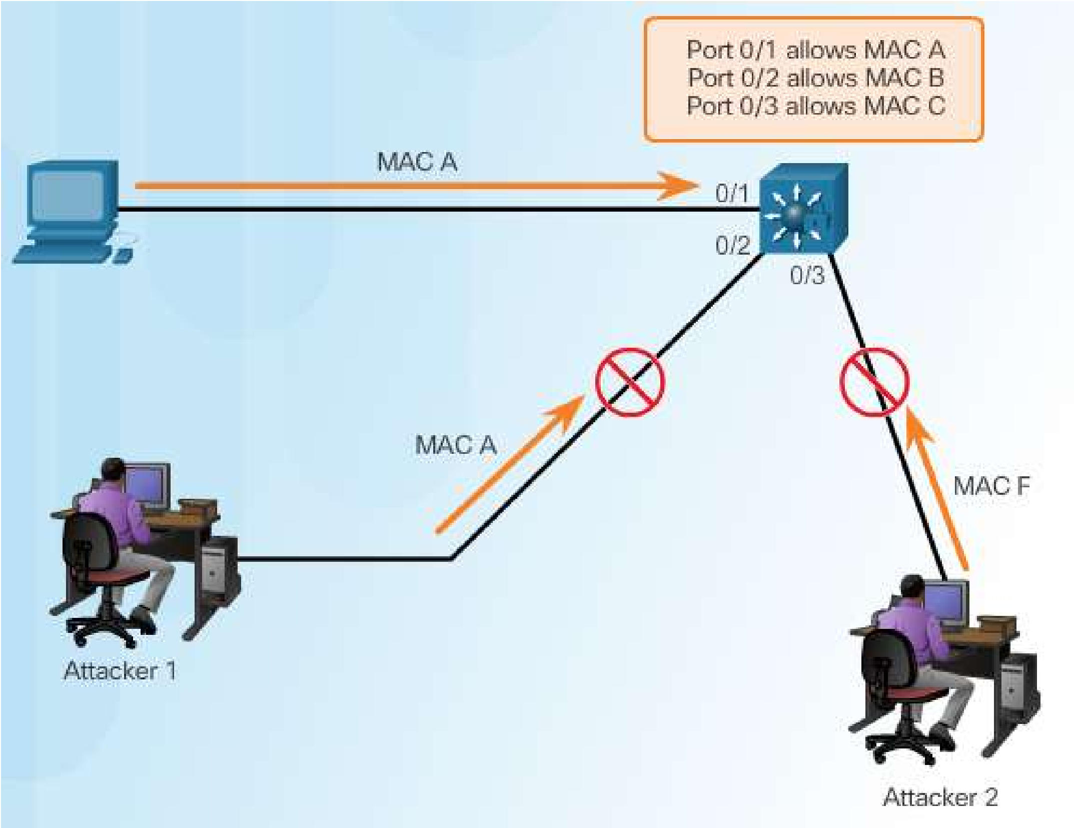


```
macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) 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
```

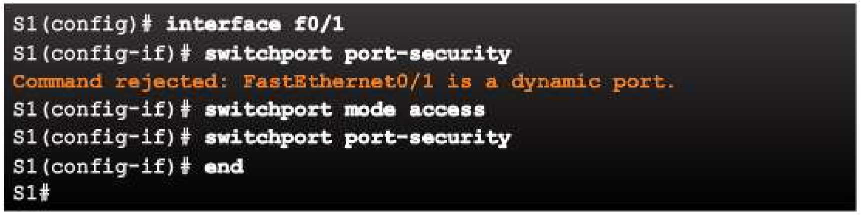
Topic 6.2.3:
Mitigating CAM Table Attacks

Mitigating CAM Table Attacks

Countermeasure for CAM Table Attacks



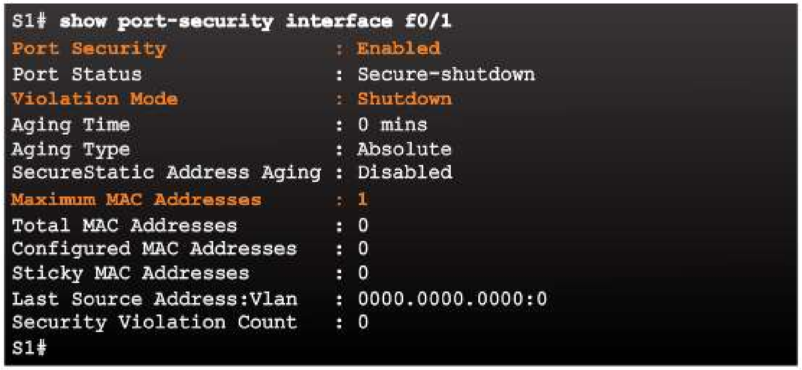
Port Security



```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

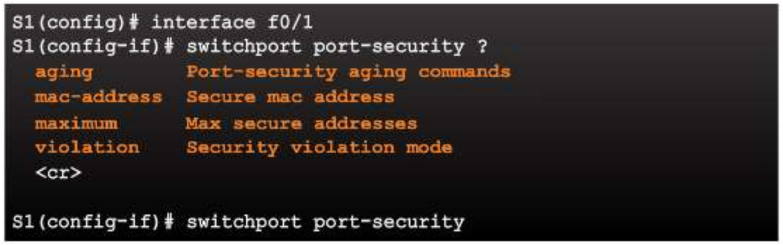
Enabling Port Security

Verifying Port Security



```
S1# show port-security interface f0/1
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   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

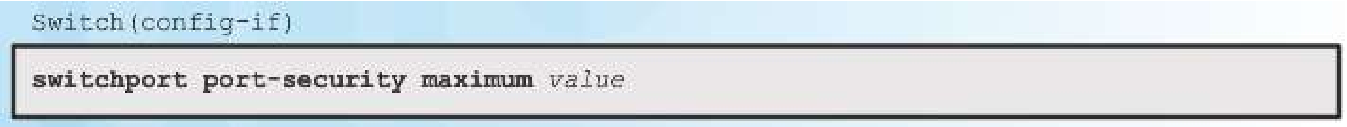
Port Security Options



```
S1(config)# interface f0/1
S1(config-if)# switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
  <cr>

S1(config-if)# switchport port-security
```

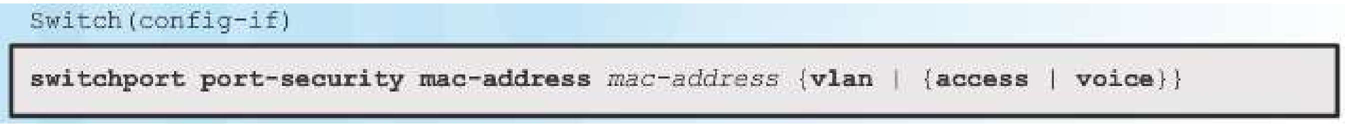
Enabling Port Security Options

Setting the Maximum Number of Mac Addresses



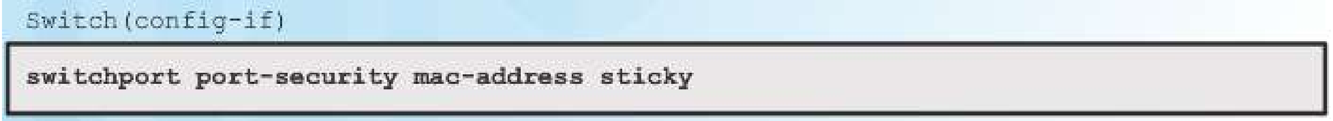
```
Switch(config-if)
switchport port-security maximum value
```

Manually Configuring Mac Addresses



```
Switch(config-if)
switchport port-security mac-address mac-address {vlan | {access | voice}}
```

Learning Connected Mac Addresses Dynamically

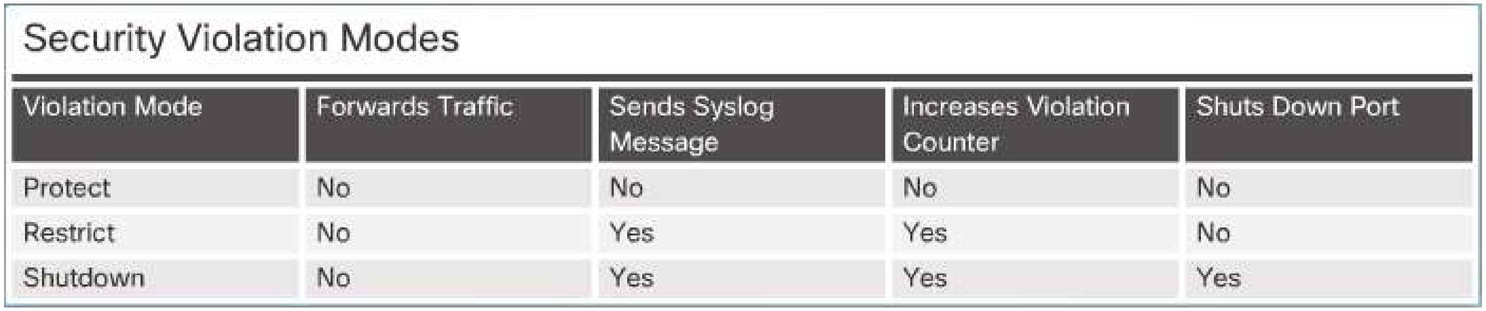


```
Switch(config-if)
switchport port-security mac-address sticky
```

Port Security Violations

Security Violation Modes:

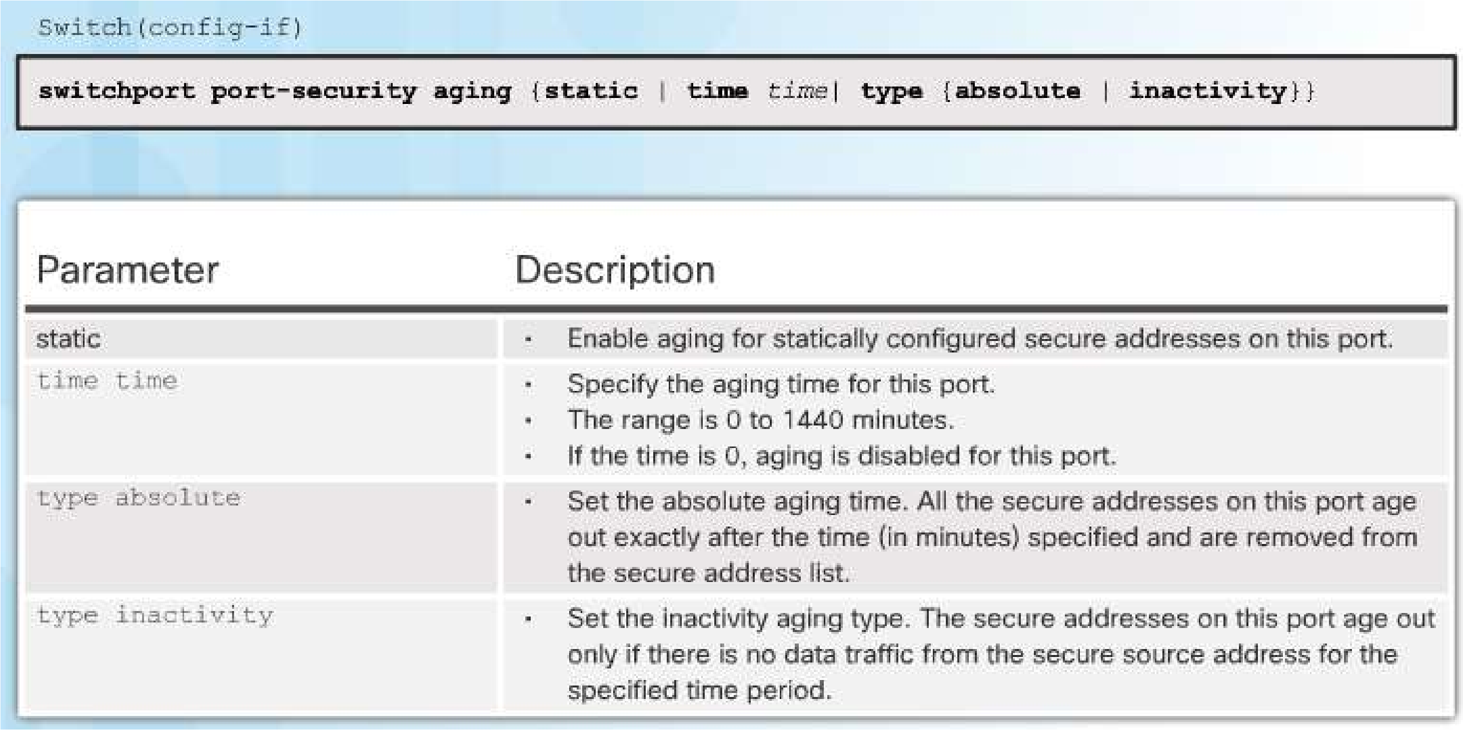
- Protect
- Restrict
- Shutdown



Security Violation Modes

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

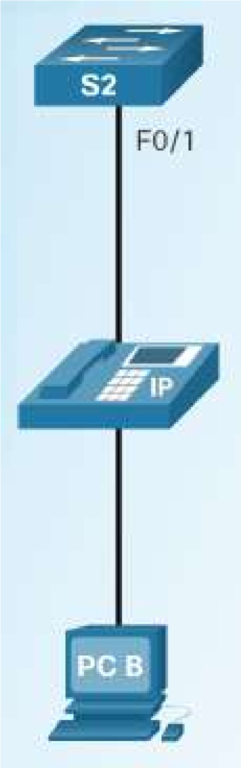
Port Security Aging

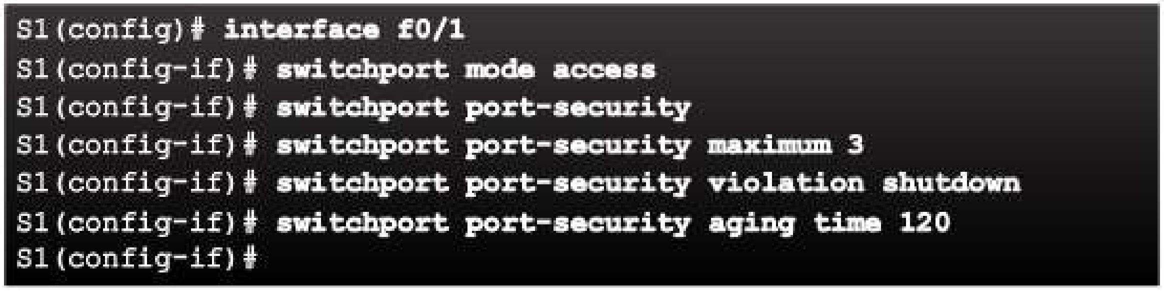


```
Switch(config-if)
switchport port-security aging {static | time time| type {absolute | inactivity}}
```

Parameter	Description
static	• Enable aging for statically configured secure addresses on this port.
`time time`	• Specify the aging time for this port. • The range is 0 to 1440 minutes. • If the time is 0, aging is disabled for this port.
`type absolute`	• Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.
`type inactivity`	• Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

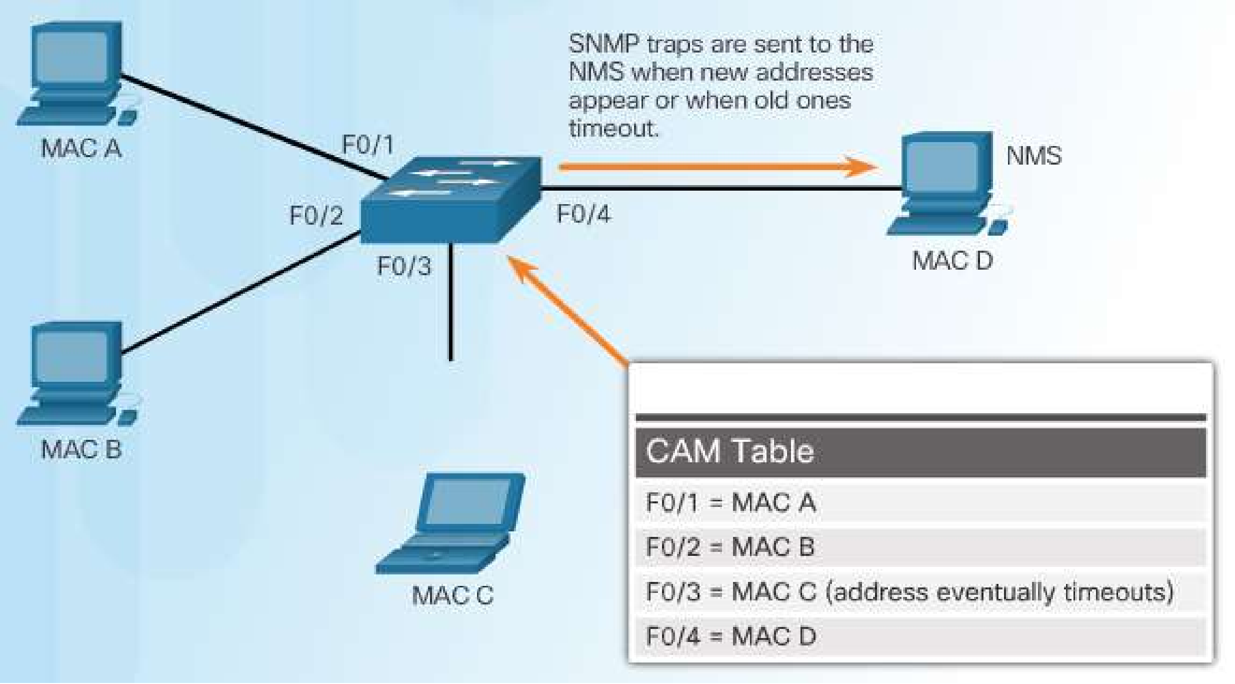
Port Security with IP Phones





```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# switchport port-security aging time 120
S1(config-if)#
```

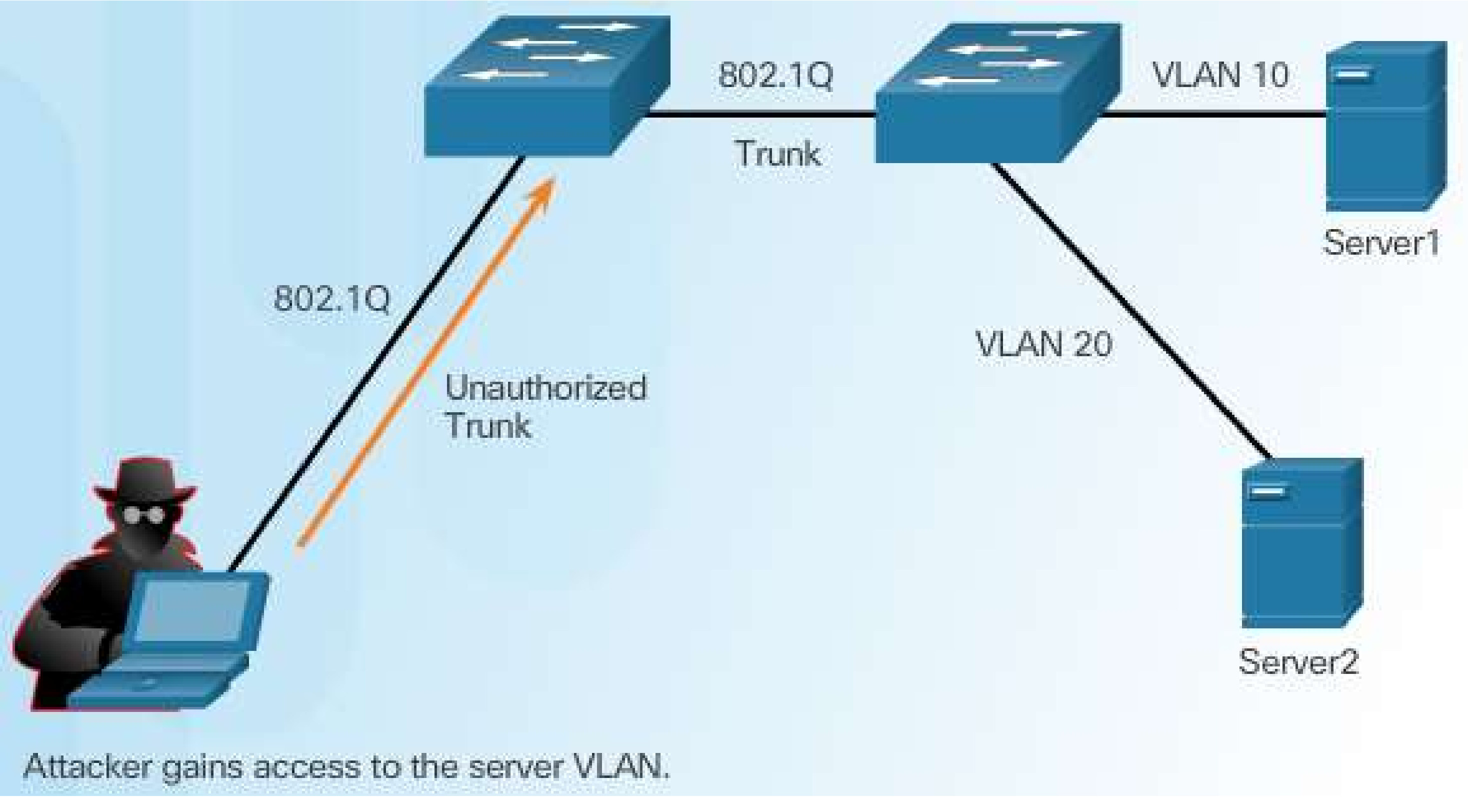
SNMP MAC Address Notification



SNMP traps are sent to the NMS when new addresses appear or when old ones timeout.

CAM Table
F0/1 = MAC A
F0/2 = MAC B
F0/3 = MAC C (address eventually timeouts)
F0/4 = MAC D

VLAN Hopping Attacks

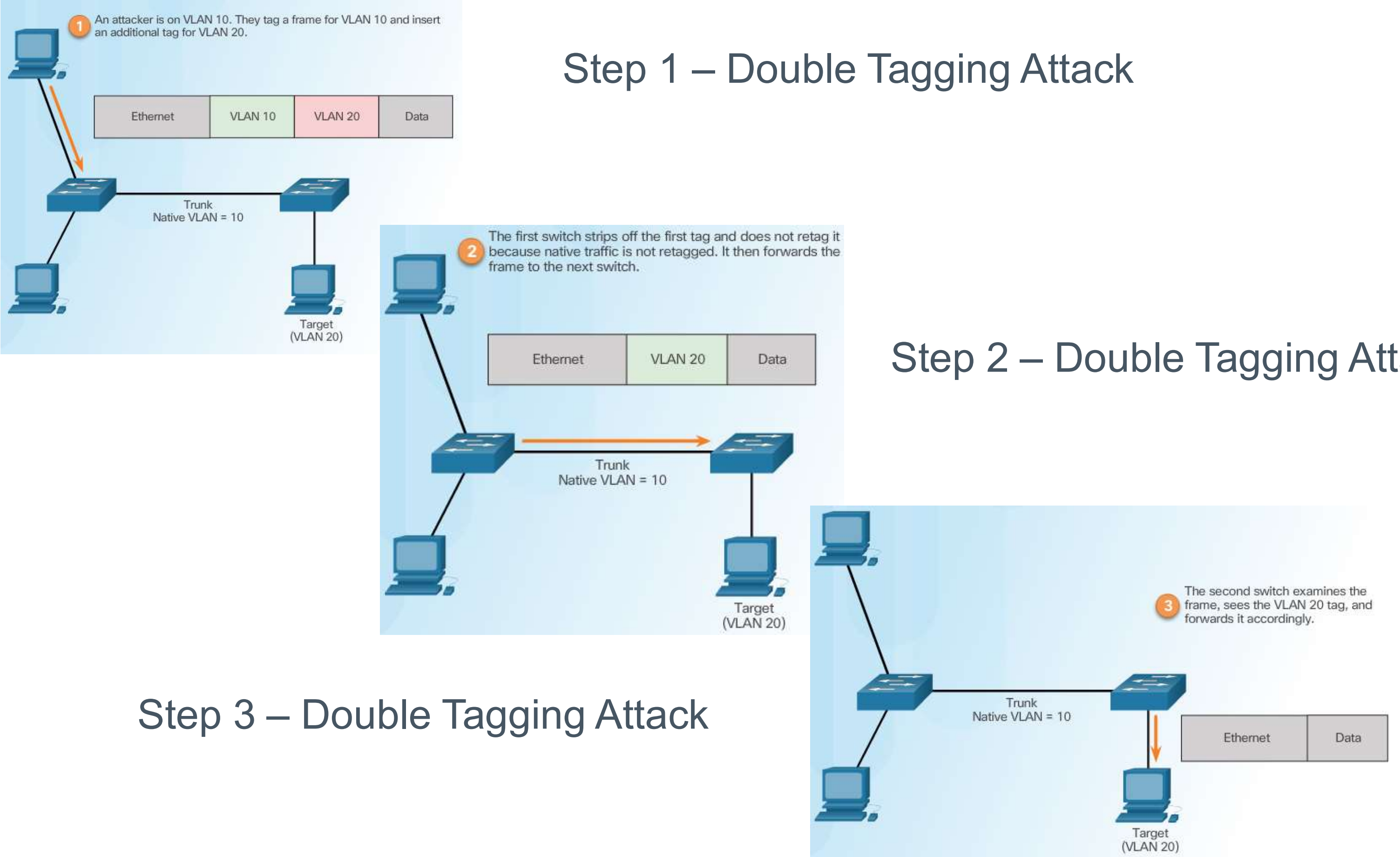


Attacker gains access to the server VLAN.

VLAN Hopping Attacks

- Trunk ports have access to all VLANs by default
- Used to route traffic for multiple VLANs across the same physical link (generally between switches)
- Encapsulation can be 802.1q or ISL
- An end station can spoof as a switch with ISL or 802.1q
- The station is then a member of all VLANs

VLAN Double-Tagging Attack



1 An attacker is on VLAN 10. They tag a frame for VLAN 10 and insert an additional tag for VLAN 20.

Step 1 – Double Tagging Attack

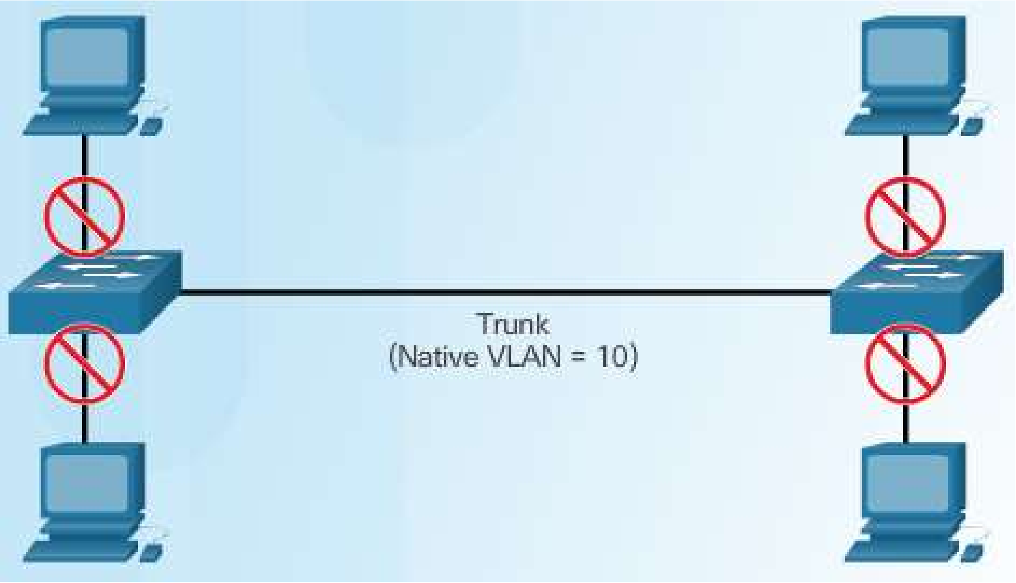
2 The first switch strips off the first tag and does not retag it because native traffic is not retagged. It then forwards the frame to the next switch.

Step 2 – Double Tagging Attack

3 The second switch examines the frame, sees the VLAN 20 tag, and forwards it accordingly.

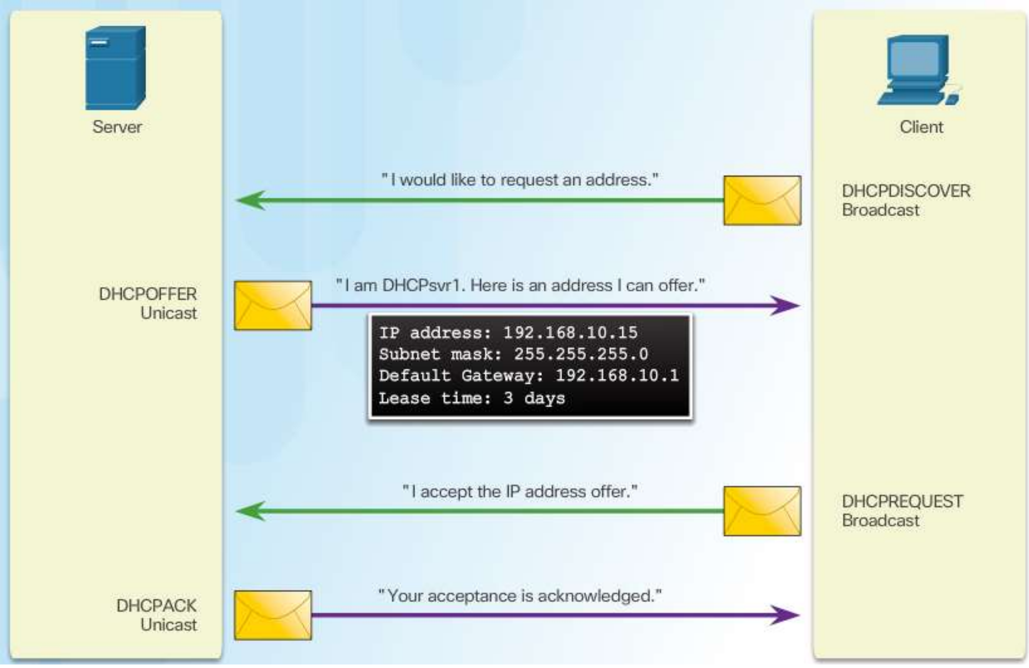
Step 3 – Double Tagging Attack

Mitigating VLAN Hopping Attacks



- A double-tagging VLAN hopping attack is unidirectional, works only if the attacker and the trunk port are in the same native VLAN
- To mitigate the hopping attack, the best way is to make sure the native VLAN of the trunk port(s) is different than any users’ ports
- Do not use VLAN1 for anything

DHCP Function



"I would like to request an address."

DHCPDISCOVER
Broadcast

DHCPOFFER
Unicast

"I am DHCPsvr1. Here is an address I can offer."

```
IP address: 192.168.10.15
Subnet mask: 255.255.255.0
Default Gateway: 192.168.10.1
Lease time: 3 days
```

"I accept the IP address offer."

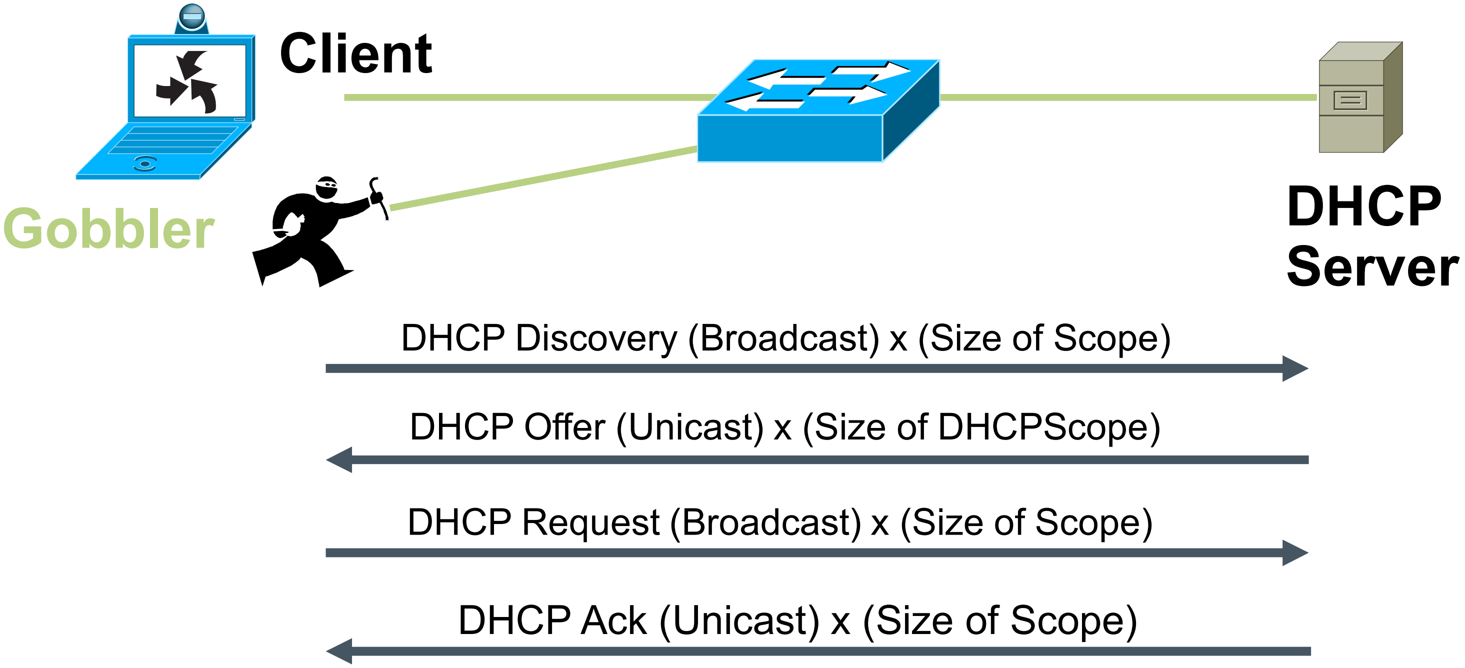
DHCPREQUEST
Broadcast

DHCPACK
Unicast

"Your acceptance is acknowledged."

- Server dynamically assigns IP address on demand
- Administrator creates pools of addresses available for assignment
- Address is assigned with lease time
- DHCP delivers other configuration information in options

DHCP Starvation Attack



Client

Gobbler

DHCP Server

DHCP Discovery (Broadcast) x (Size of Scope)

DHCP Offer (Unicast) x (Size of DHCPScope)

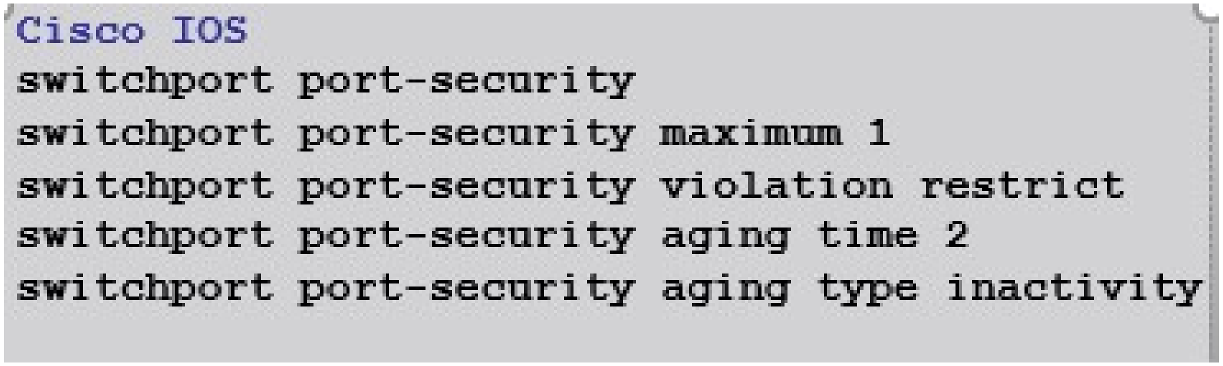
DHCP Request (Broadcast) x (Size of Scope)

DHCP Ack (Unicast) x (Size of Scope)

- Gobbler/DHCPx looks at the entire DHCP scope and tries to lease all of the DHCP addresses available in the DHCP scope
- This is a Denial of Service (DoS) attack using DHCP leases

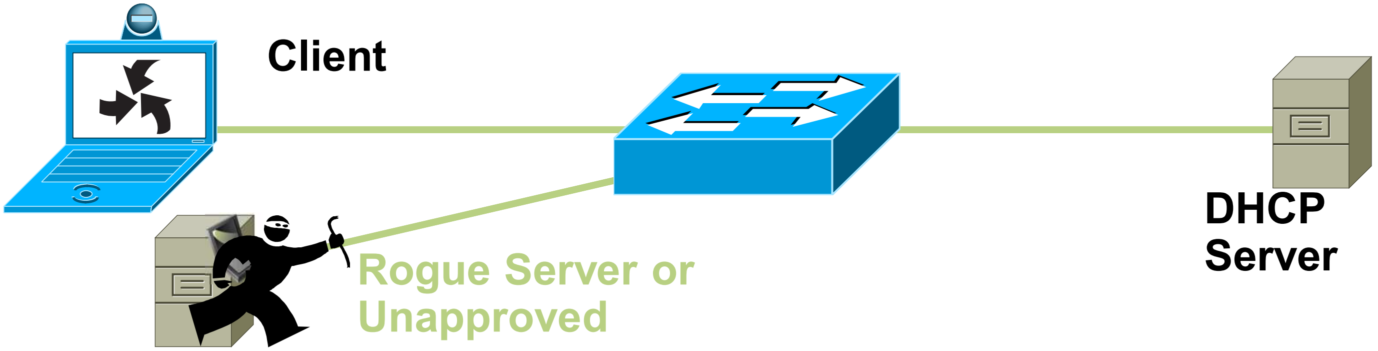
Mitigating DHCP Starvation Attack

- Gobbler uses a new MAC address to request a new DHCP lease
- Restrict the number of MAC addresses on a port
- Will not be able to lease more IP address then MAC addresses allowed on the port
- In the example the attacker would get one IP address from the DHCP server



```
Cisco IOS
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

Rogue DHCP Server Attack



› What can the attacker do if he is the DHCP server?

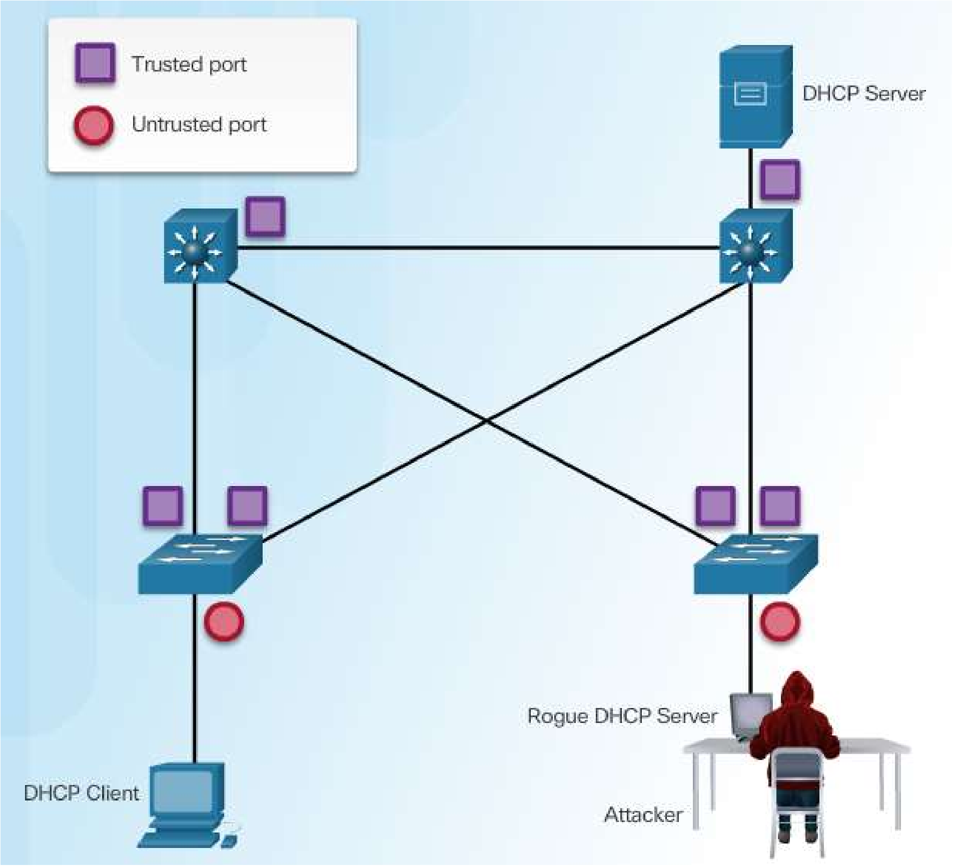
IP Address: 10.10.10.101
Subnet Mask: 255.255.255.0
Default Routers: 10.10.10.1
DNS Servers: 192.168.10.4, 192.168.10.5
Lease Time: 10 days

Here Is Your Configuration

- What do you see as a potential problem with incorrect information?
  - Wrong default gateway—Attacker is the gateway
  - Wrong DNS server—Attacker is DNS server
  - Wrong IP address—Attacker does DOS with incorrect IP

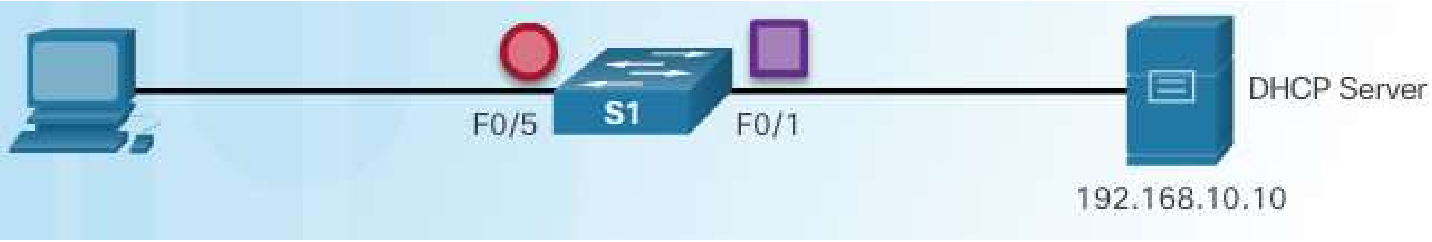
Mitigating Rogue DHCP Server Attack

Configuring DHCP Snooping

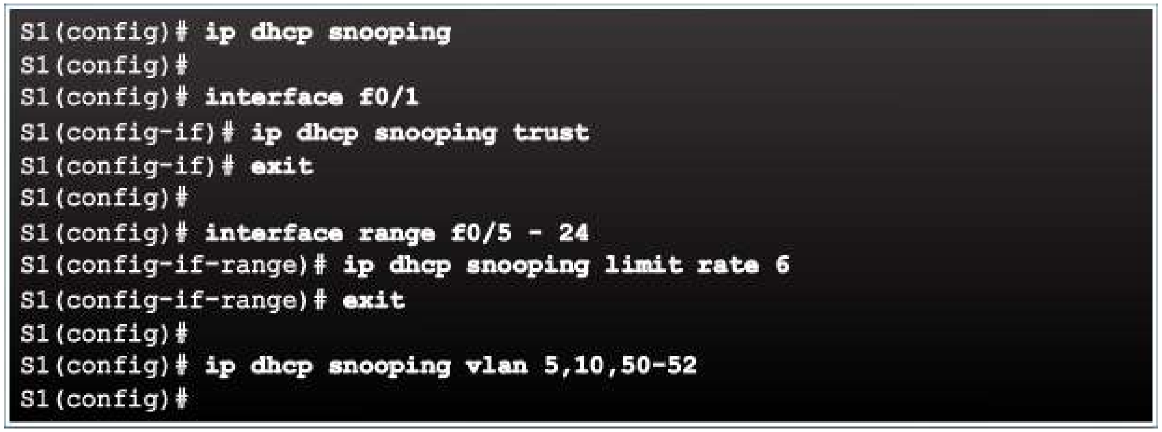


Configuring DHCP Snooping Example

DHCP Snooping Reference Topology



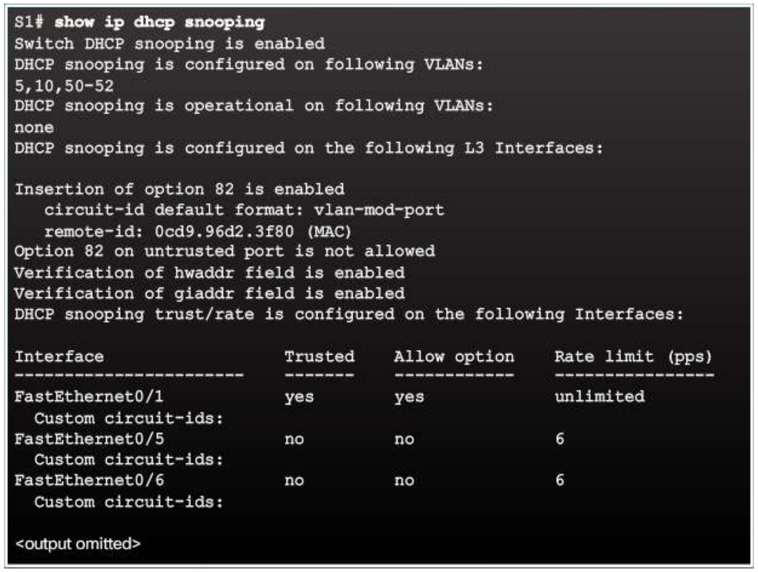
Configuring a Maximum Number of MAC Addresses



```
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)#
```

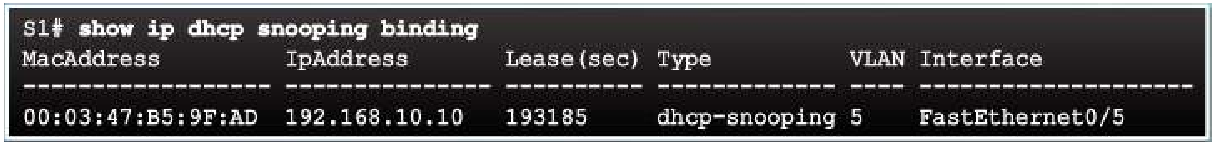
Configuring DHCP Snooping Example

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>
```

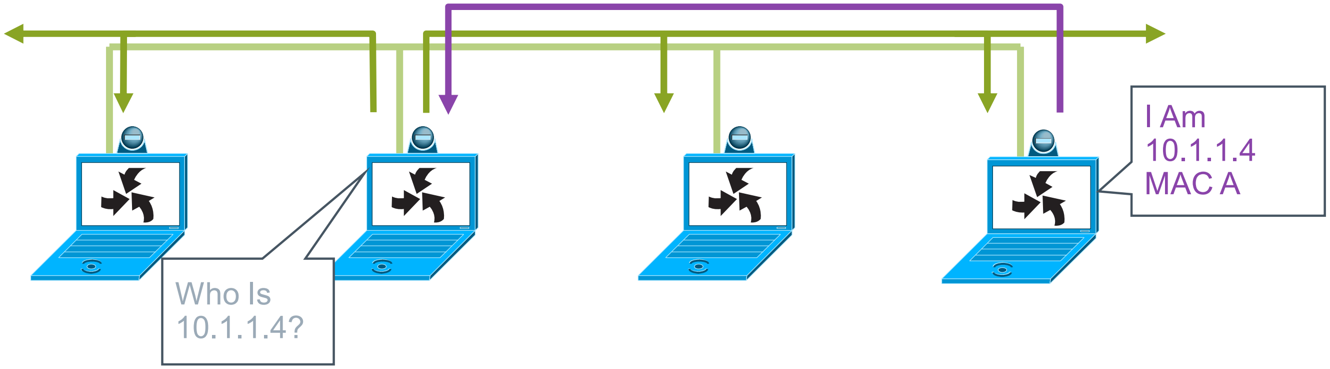
View the DHCP snooping database



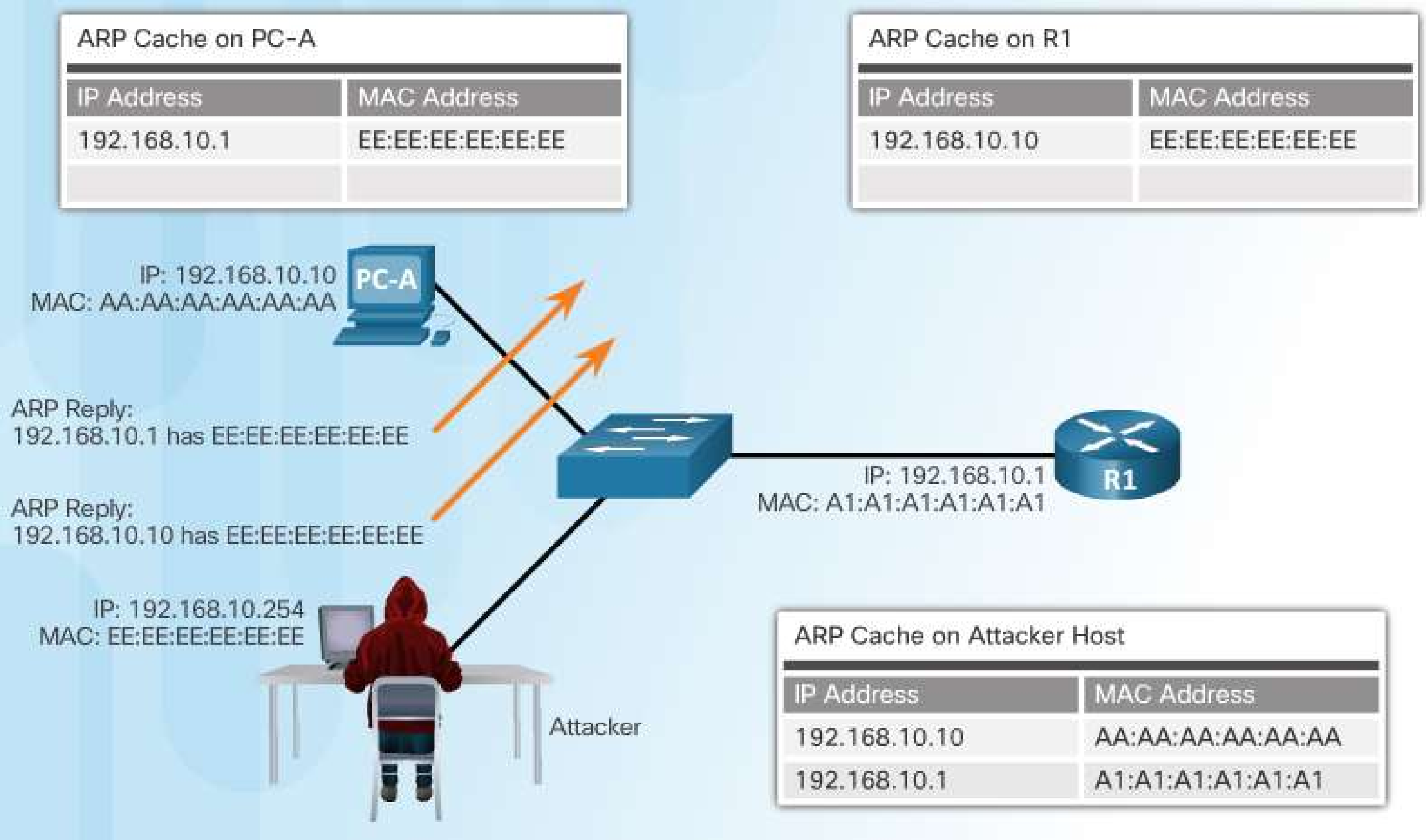
```
S1# show ip dhcp snooping binding
MacAddress         IpAddress        Lease(sec)  Type           VLAN  Interface
------------------ ---------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD  192.168.10.10    193185      dhcp-snooping  5     FastEthernet0/5
```

ARP Function

- Before a station can talk to another one
  - it must do an ARP request to map the IP address to the MAC address
  - This ARP request is broadcast
  - All computers on the subnet will receive and process the ARP request
  - the station that matches the IP address in the request will send an ARP reply



ARP Spoofing and ARP Poisoning Attack



ARP Cache on PC-A

IP Address	MAC Address
192.168.10.1	EE:EE:EE:EE:EE:EE

ARP Cache on R1

IP Address	MAC Address
192.168.10.10	EE:EE:EE:EE:EE:EE

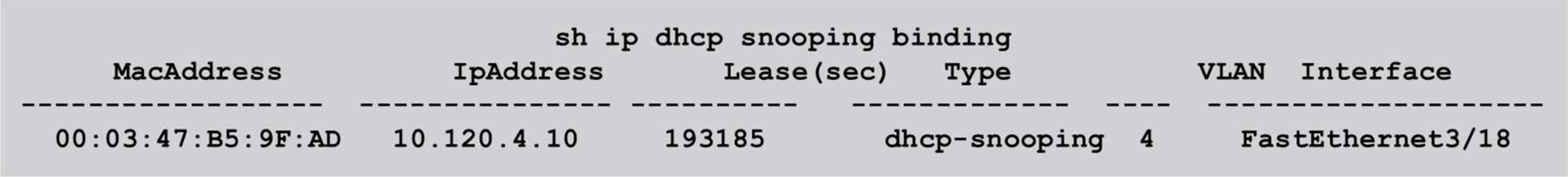
ARP Cache on Attacker Host

IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA
192.168.10.1	A1:A1:A1:A1:A1:A1

Mitigating ARP Attacks

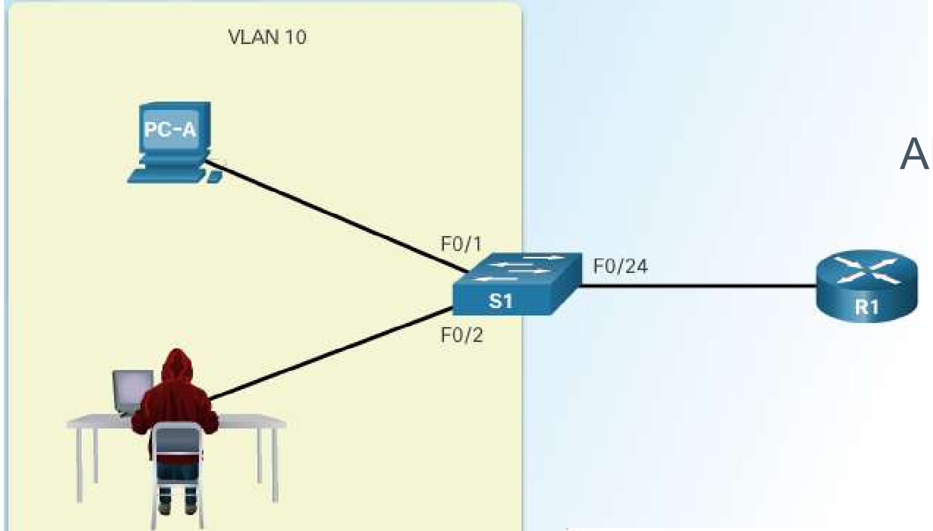
Configuring Dynamic ARP Inspection

- Uses the DHCP snooping binding table information
- Check the mac address and IP address fields to see
  - if the ARP from the interface is in the binding
  - if not, traffic is blocked



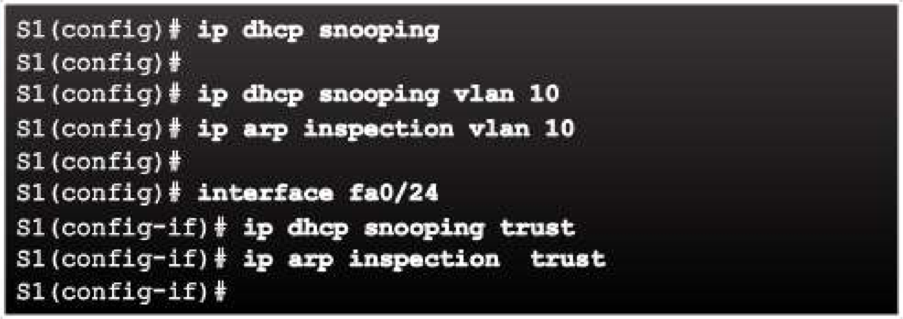
```
                        sh ip dhcp snooping binding
     MacAddress           IpAddress        Lease(sec)    Type          VLAN  Interface
------------------  ---------------- ----------   -------------  ----  --------------------
  00:03:47:B5:9F:AD   10.120.4.10      193185       dhcp-snooping  4     FastEthernet3/18
```

Configuring DHCP Snooping Example



ARP Reference Topology

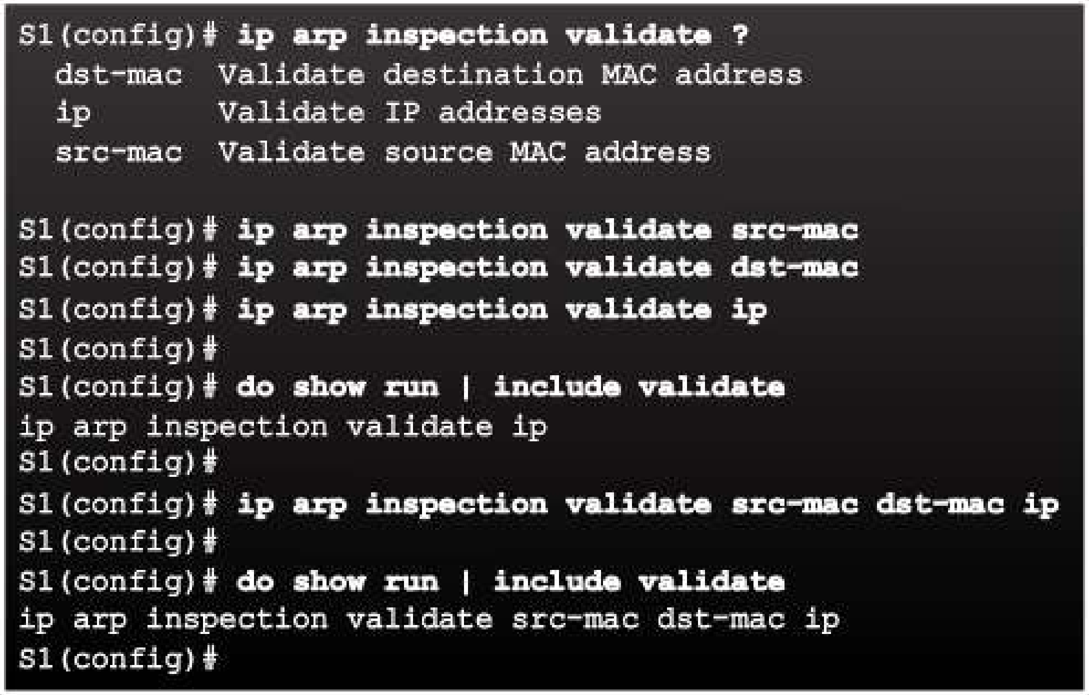
Configuring Dynamic ARP Inspection



```
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)#
```

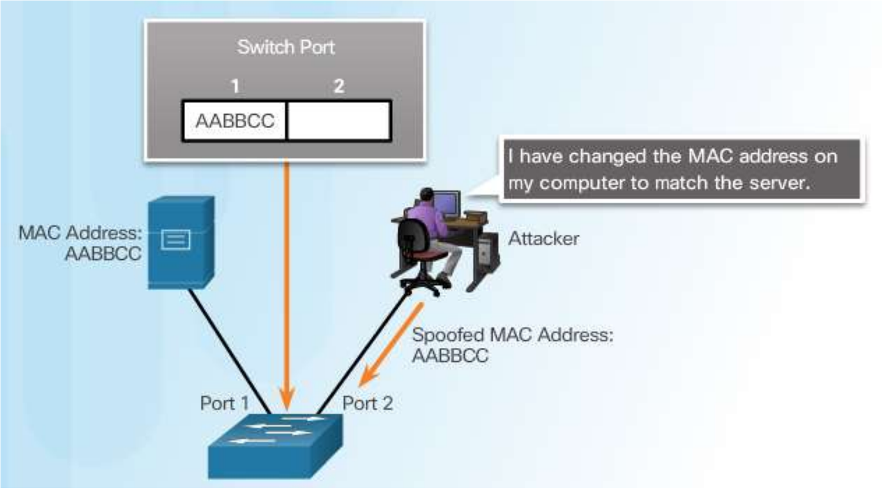
Configuring DHCP Snooping Example

Checking Source, Destination, and IP

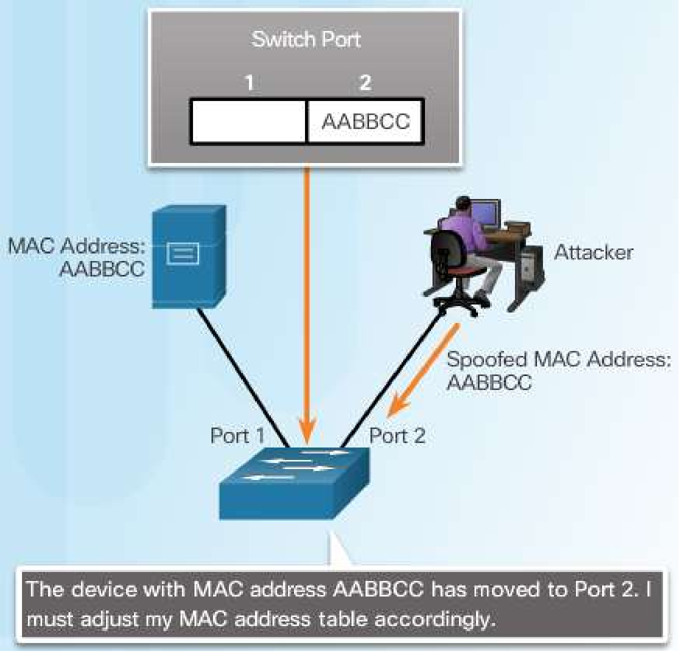


```
S1(config)# ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address

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)#
```

Address Spoofing Attack



I have changed the MAC address on my computer to match the server.

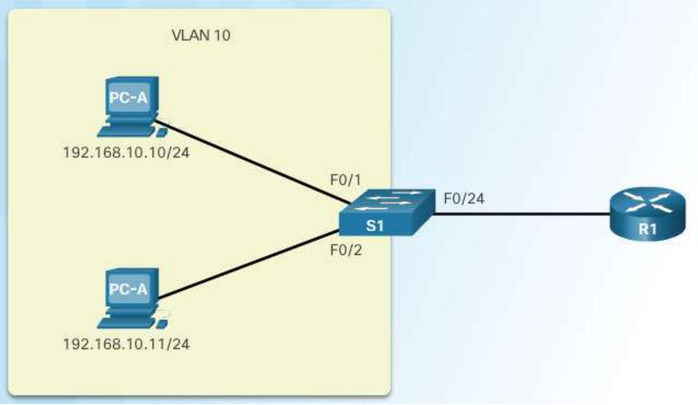


The device with MAC address AABBCC has moved to Port 2. I must adjust my MAC address table accordingly.

- Attacker sends packets with the incorrect source MAC address
- If network control is by MAC address, the attacker now looks like the Server

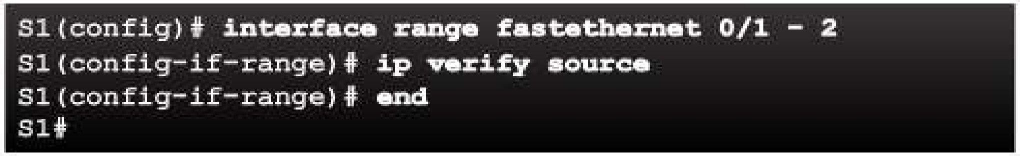
Mitigating Address Spoofing Attack

Configuring IP Source Guard



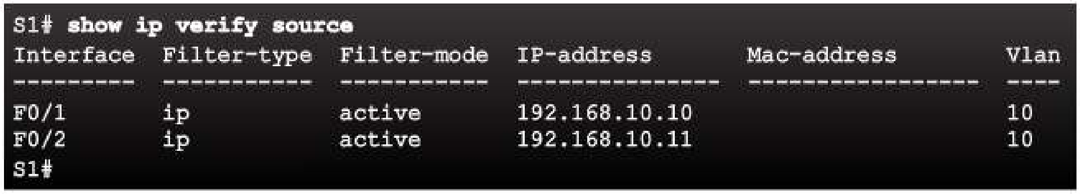
IP Source Guard Reference Topology

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



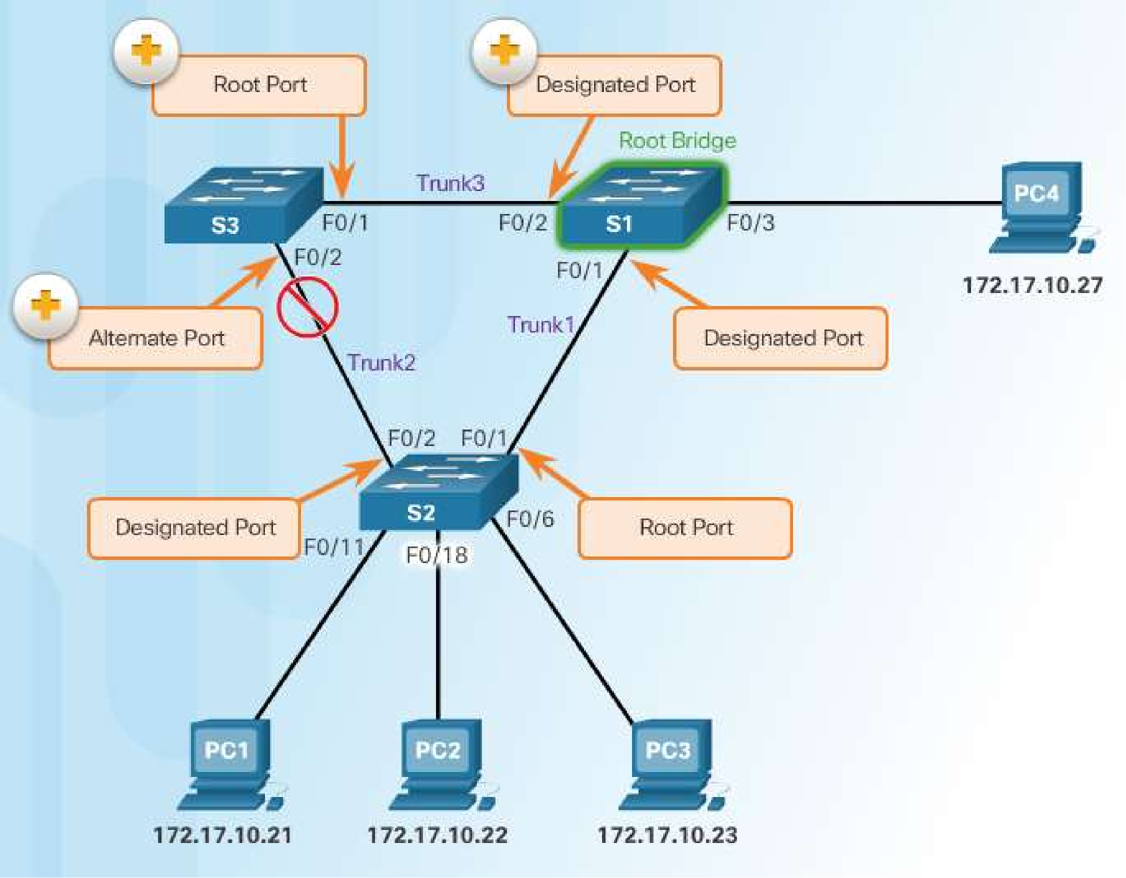
```
S1# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
F0/1       ip           active       192.168.10.10                       10
F0/2       ip           active       192.168.10.11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

- We can use the DHCP snooping binding table information

```
ip verify source dhcp-snooping-vlan
```

- Operates just like dynamic ARP inspection, but it looks at every packet, not just ARP packet

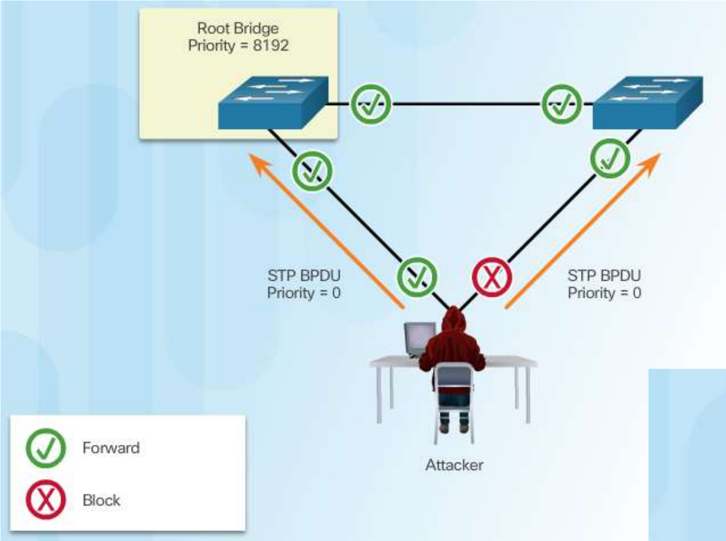
STP Basics



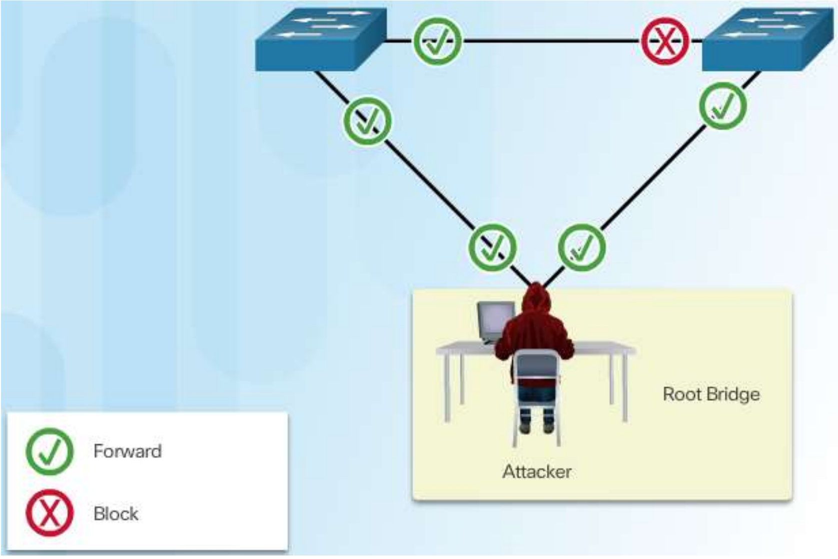
- STP is used to maintain loop-free topologies in a redundant layer 2 architecture
- 4-key steps involved

1. Elect root bridge
2. Elect root port
3. Elect designated port
4. Block all remaining ports

STP Manipulation Attacks

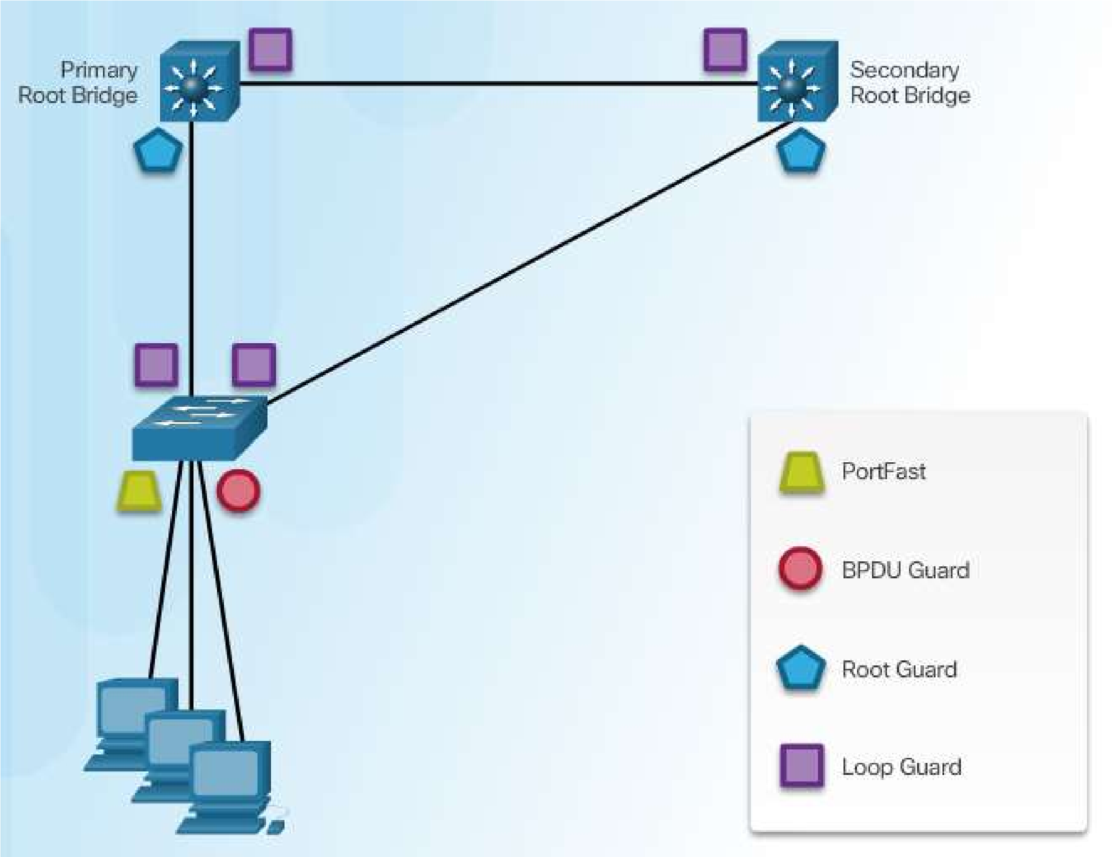


Spoofing the Root Bridge

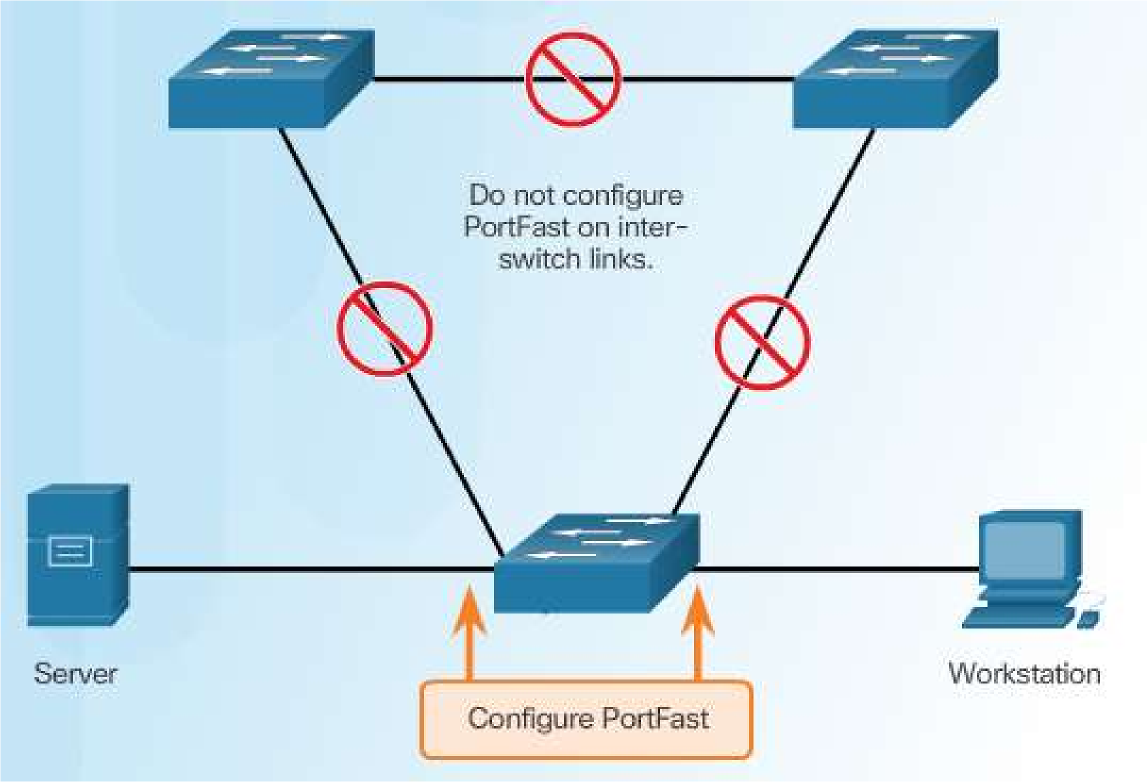


Successful STP Manipulation Attack

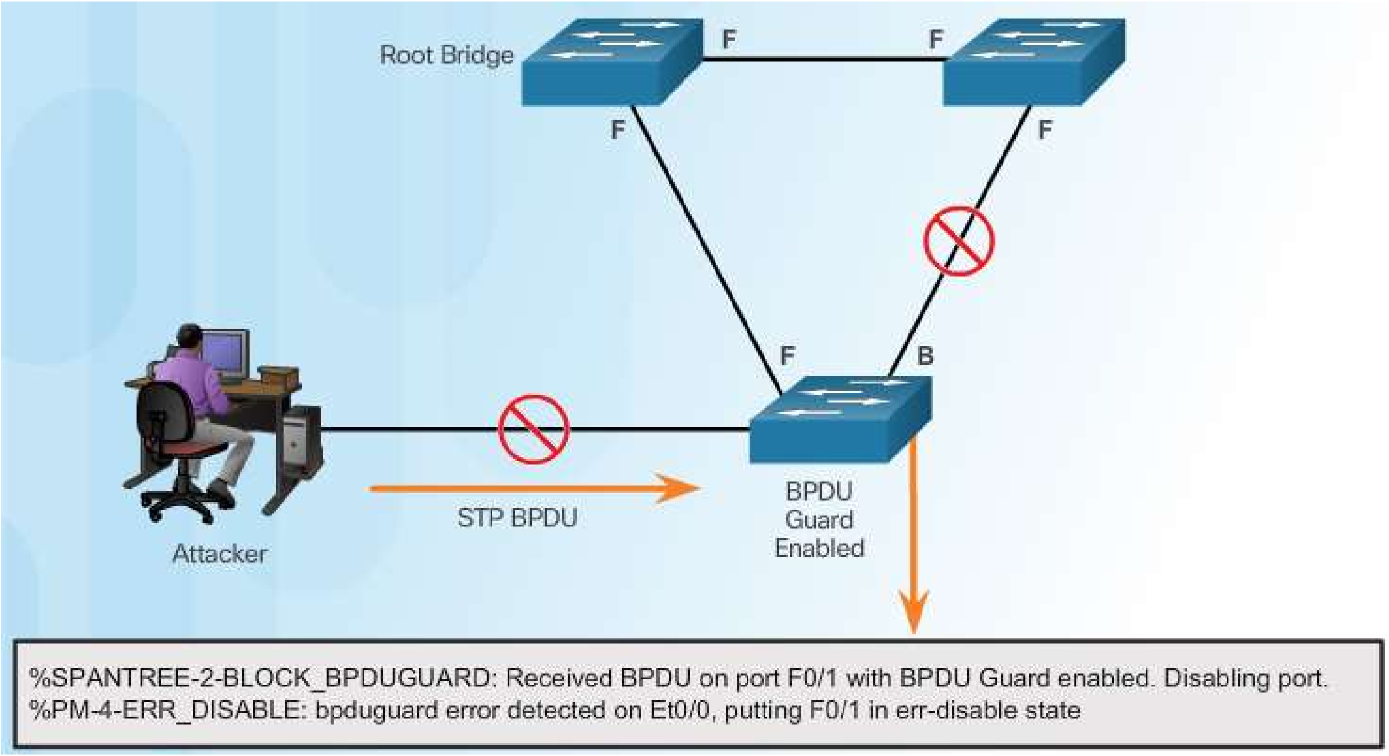
Mitigating STP Attacks



Configuring PortFast

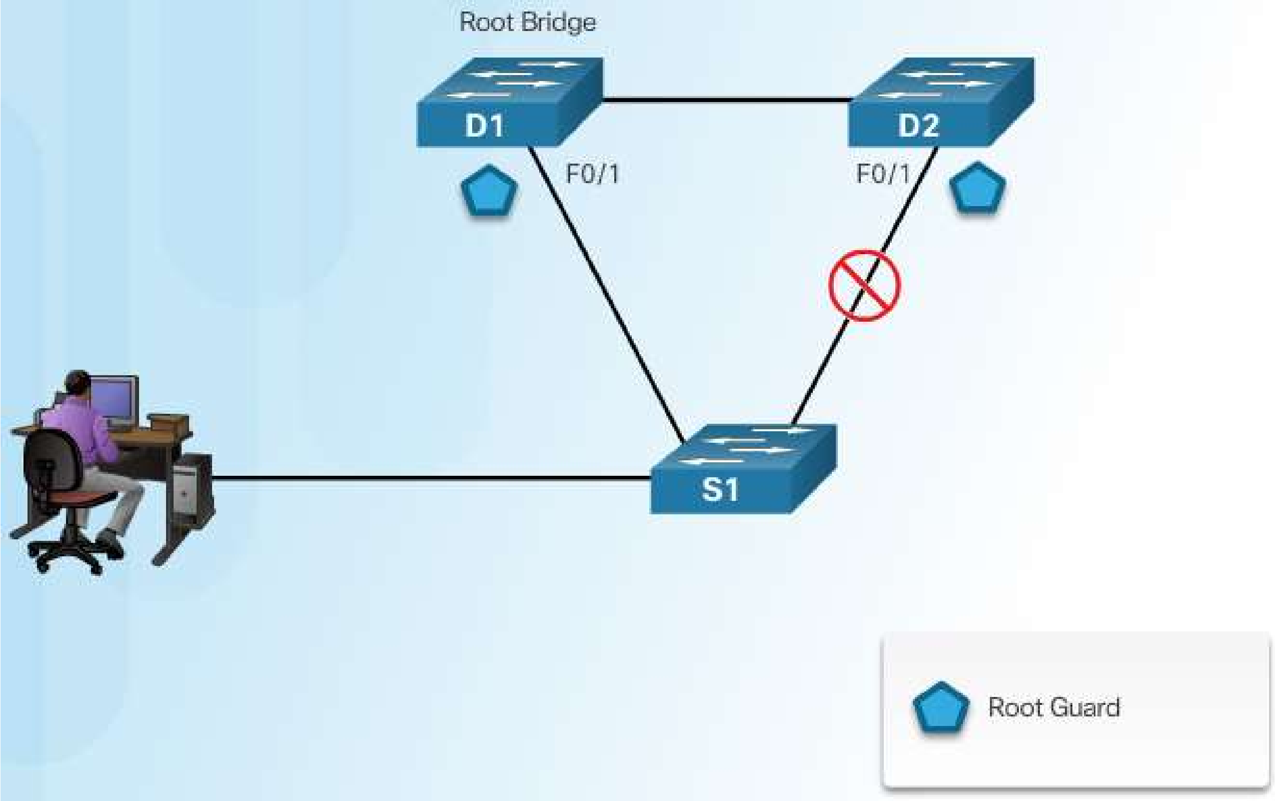


Configuring BDPU Guard

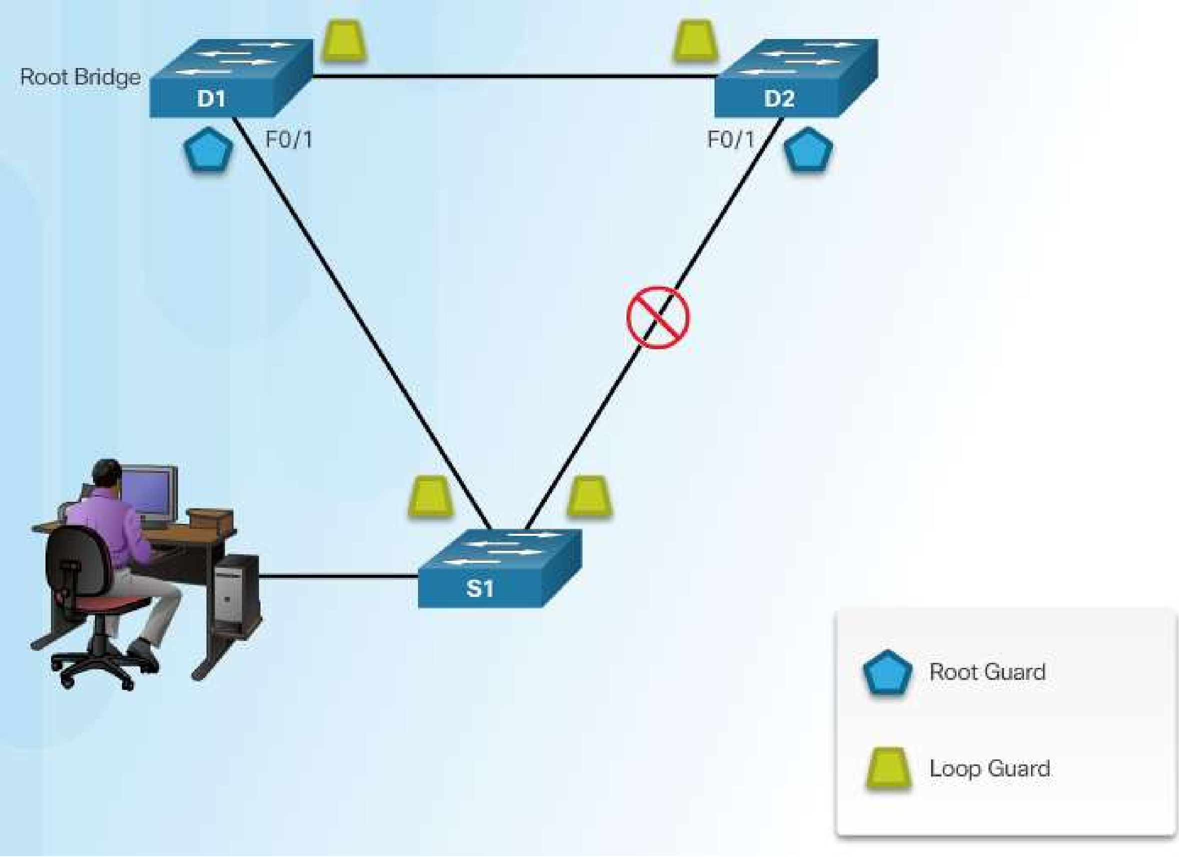


```
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port F0/1 with BPDU Guard enabled. Disabling port.
%PM-4-ERR_DISABLE: bpduguard error detected on Et0/0, putting F0/1 in err-disable state
```

Configuring Root Guard



Configuring Loop Guard


Root Bridge
D1
D2
F0/1
F0/1
S1
Root Guard
Loop Guard