CCNA Security 2.0 Study Material – Chapter 6: Securing the Local Area Network

itexamanswers.net/ccna-security-2-0-study-material-chapter-6-securing-local-area-network.html

October 7, 2017

Chapter Outline:

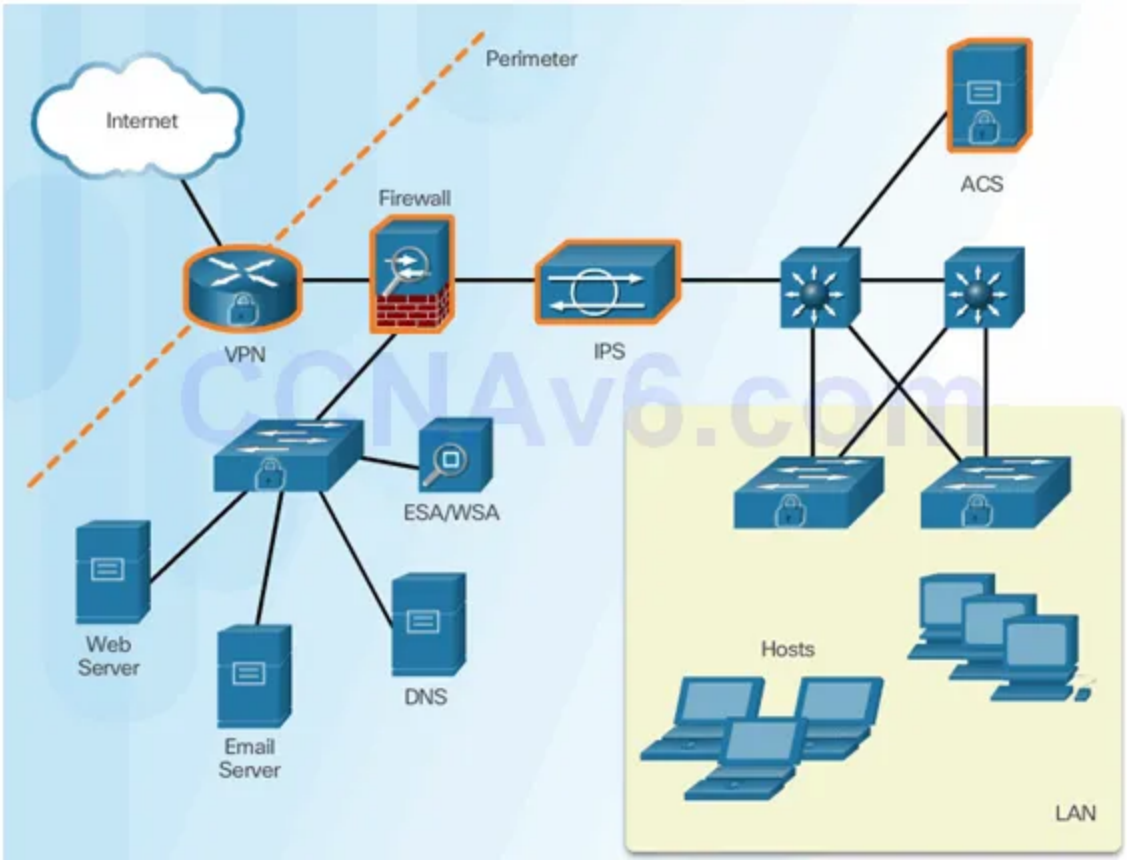
Section 6.1: Endpoint Security

Upon completion of this section, you should be able to:

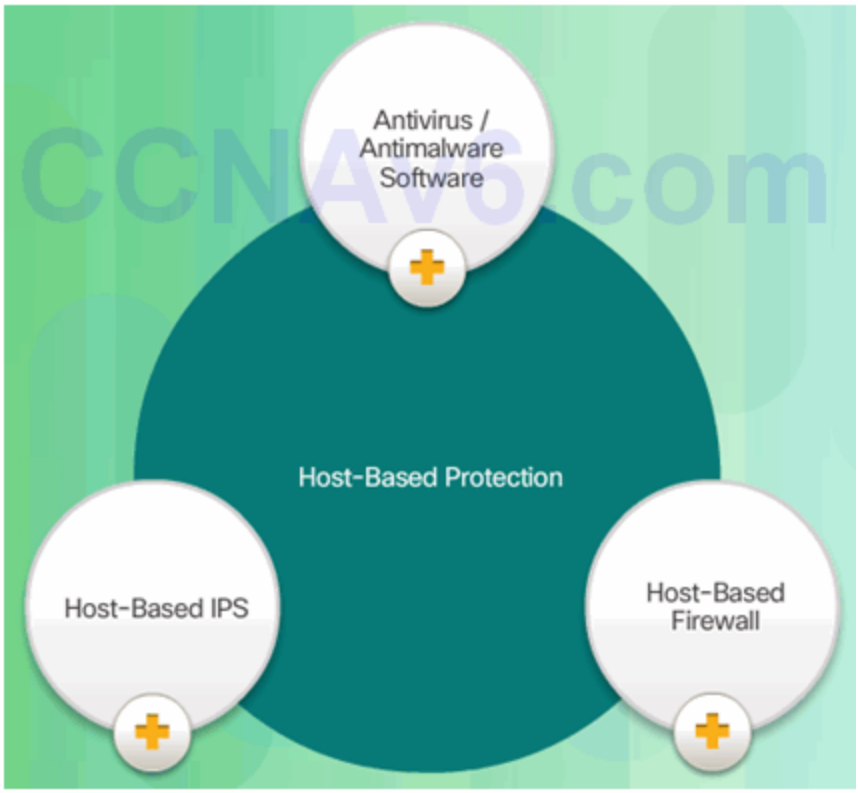
- Describe endpoint security and the enabling technologies.
- Explain how Cisco AMP is used to ensure endpoint security.
- Explain how Cisco NAC authenticates and enforces the network security policy.

Topic 6.1.1: Introducing Endpoint Security

Securing LAN Elements



Traditional Endpoint Security



The Borderless Network

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:

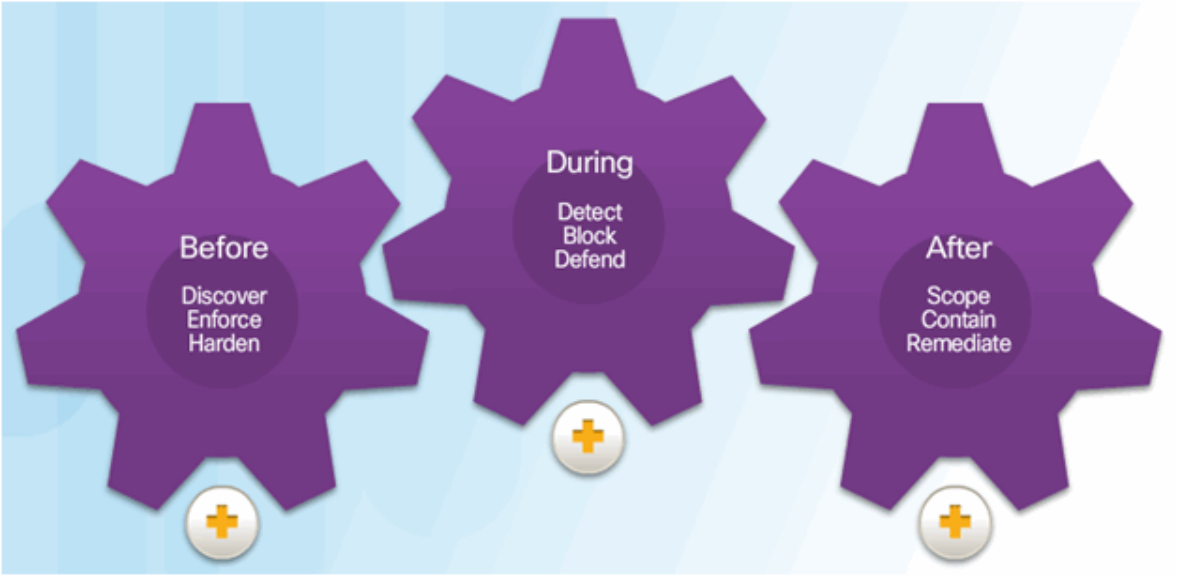
- Antivirus/Antimalware
- SPAM Filtering
- URL Filtering
- Blacklisting
- Data Loss Prevention (DLP)

Modern Endpoint Security Solutions

Hardware and Software Encryption of Local Data

Topic 6.1.2: Antimalware Protection

Advanced Malware Protection



AMP and Managed Threat Defense

Talos teams gather real-time threat intelligence from a variety of sources:

- 1.6 million deployed security devices, including firewall, IPS, web, and email appliances
- 150 million endpoints

They then analyze this data:

- 100 TB of security intelligence daily
- 13 billion web requests per day
- 35% of the world's enterprise email traffic

AMP for Endpoints

- **AMP for Endpoints**– AMP for Endpoints integrates with Cisco AMP for Networks to deliver comprehensive protection across extended networks and endpoints.
- **AMP for Networks**– Provides a network-based solution and is integrated into dedicated Cisco ASA Firewall and Cisco FirePOWER network security appliances.
- **AMP for Content Security**– This is an integrated feature in Cisco Cloud Web Security or Cisco Web and Email Security Appliances to protect against email and web-based advanced malware attacks.

Topic 6.1.3: Email and Web Security

Securing Email and Web

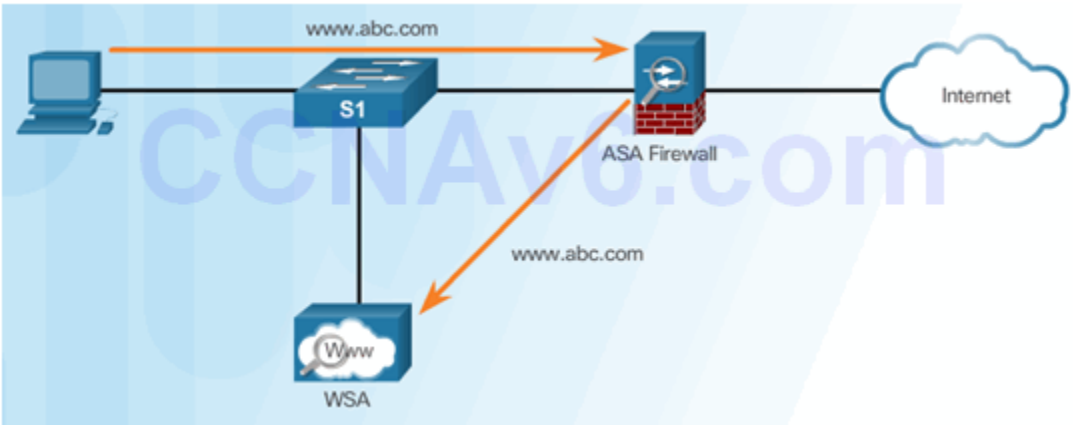
Cisco Email Security Appliance

Features and benefits of Cisco Email Security solutions:

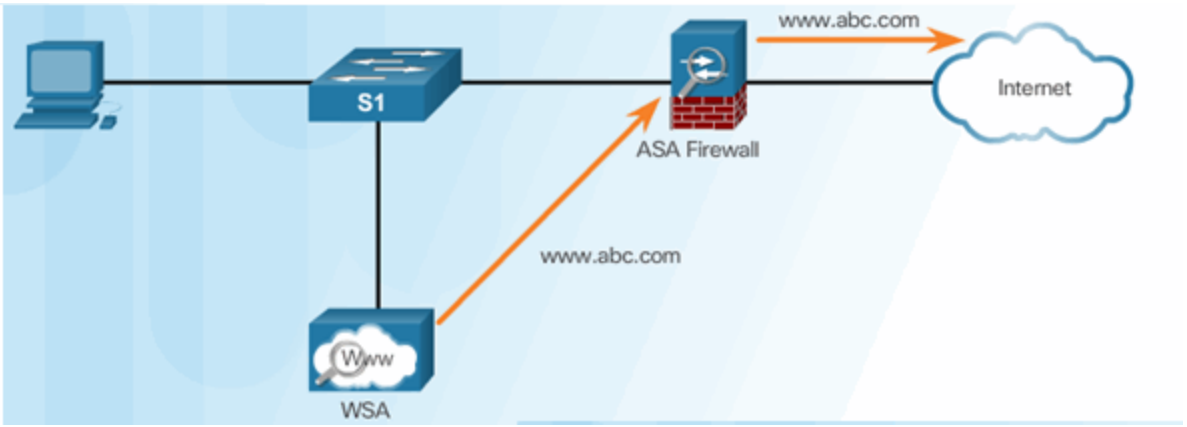
- Global threat intelligence
- Spam blocking
- Advanced malware protection
- Outbound message control

Cisco Web Security Appliance

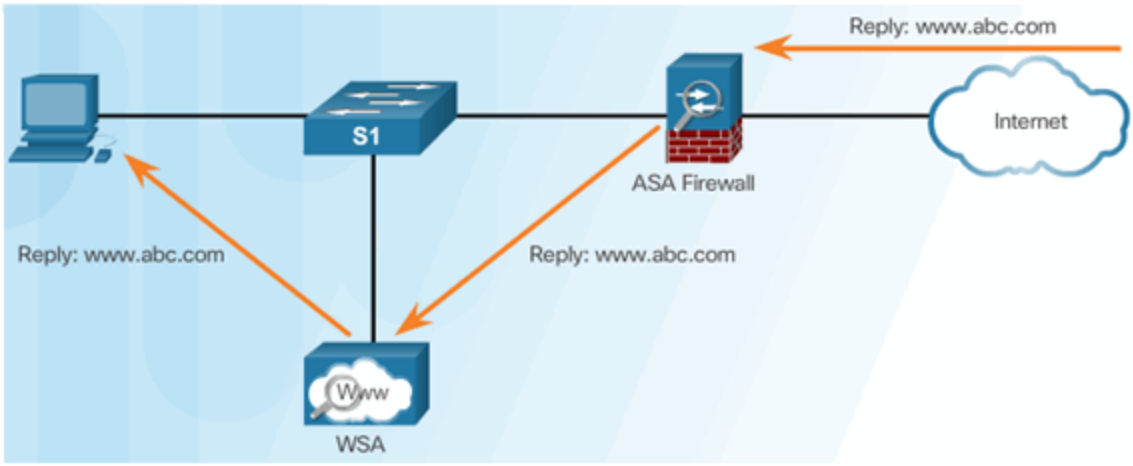
Client Initiates Web Request



WSA Forwards Request

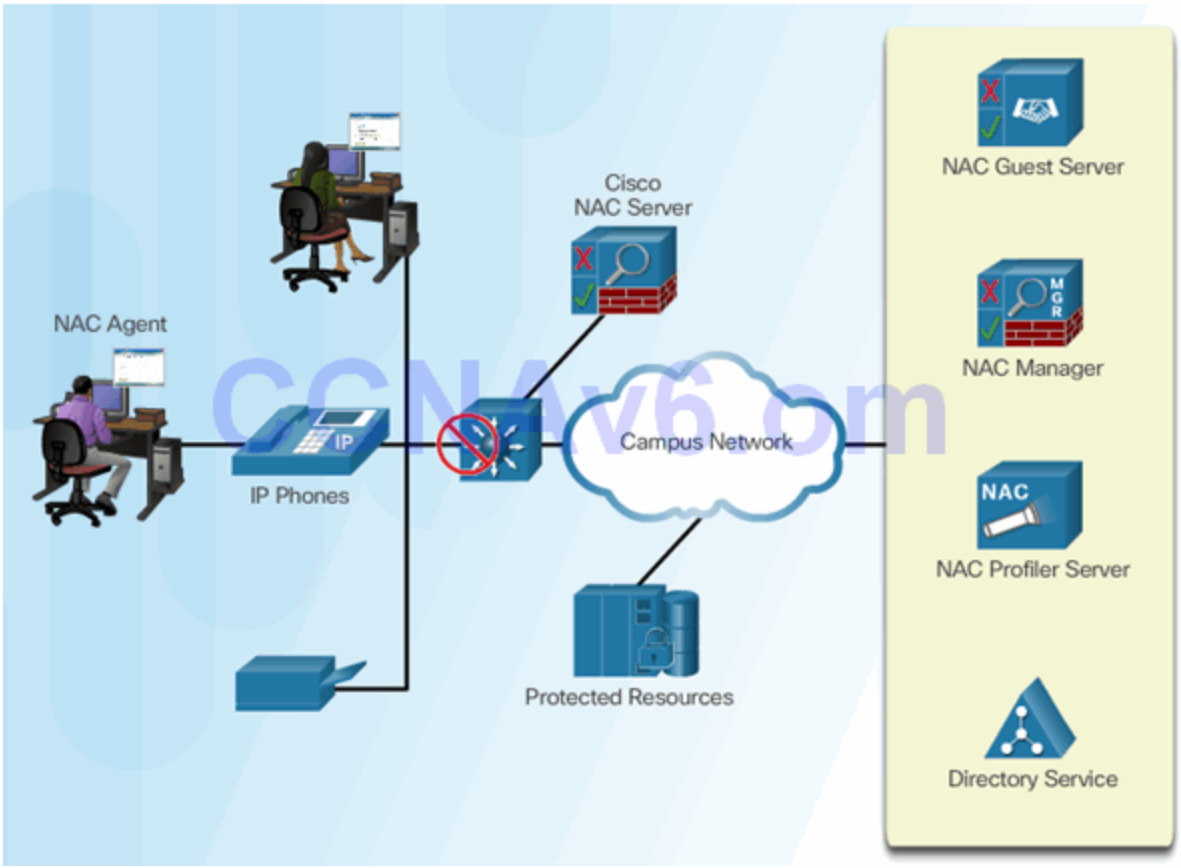


Reply Sent to WSA and Then To Client

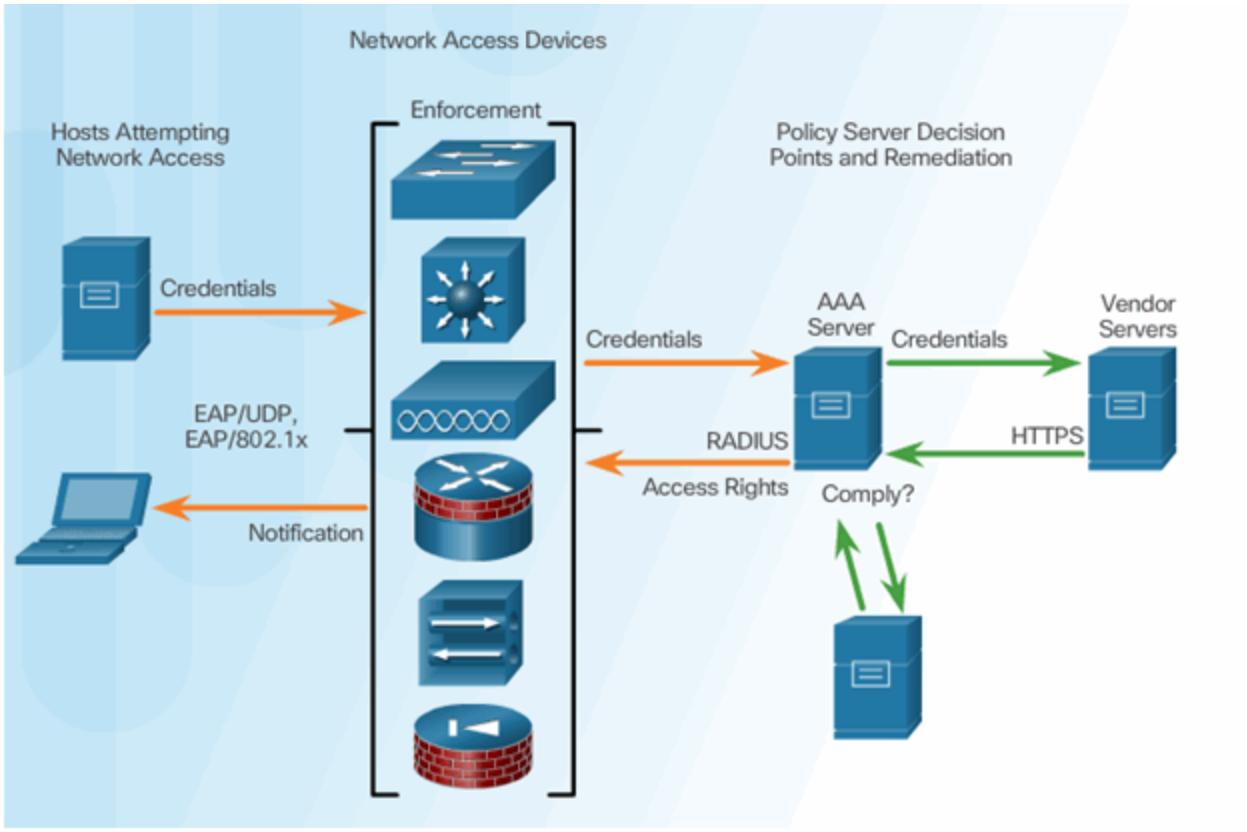


Topic 6.1.4: Controlling Network Access

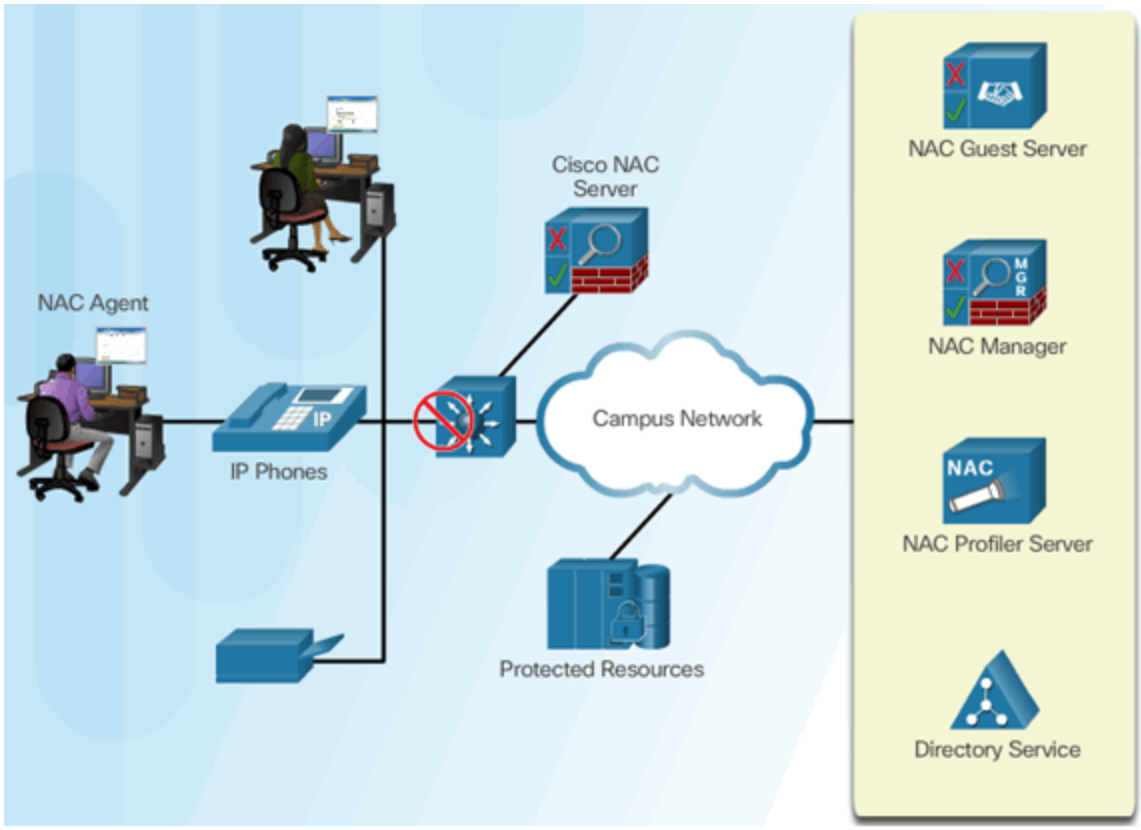
Cisco Network Admission Control



Cisco NAC Functions



Cisco NAC Components

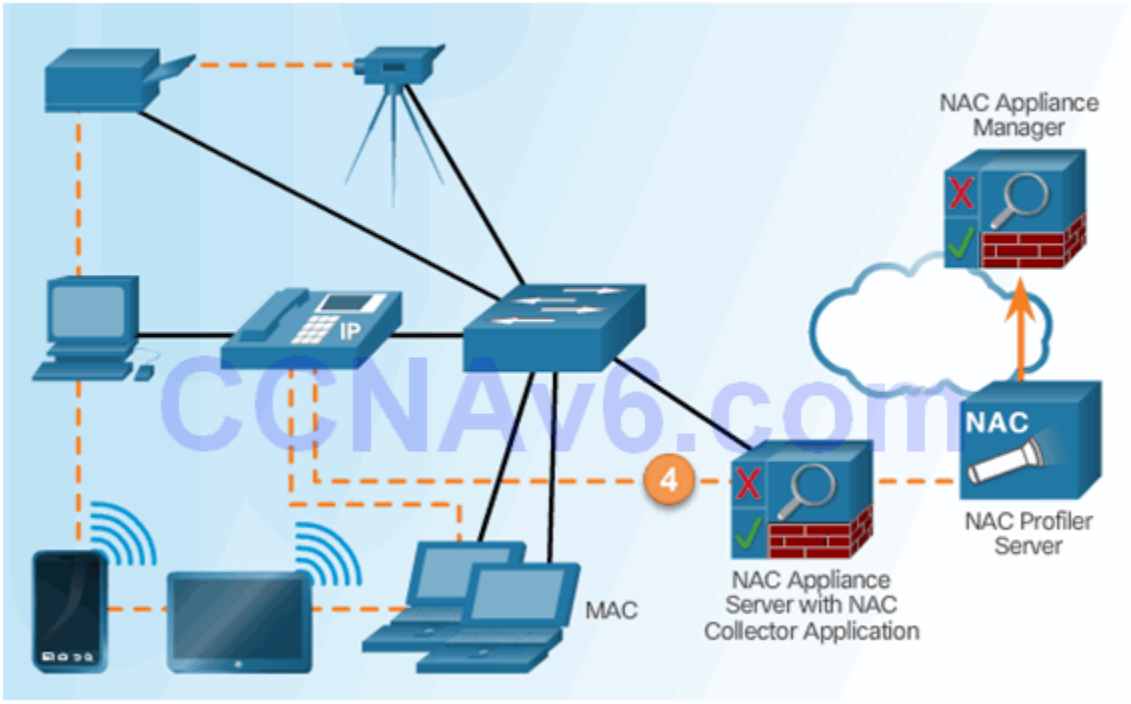


Network Access for Guests

Three ways to grant sponsor permissions:

- to only those accounts created by the sponsor
- to all accounts
- to no accounts (i.e., they cannot change any permissions)

Cisco NAC Profiler



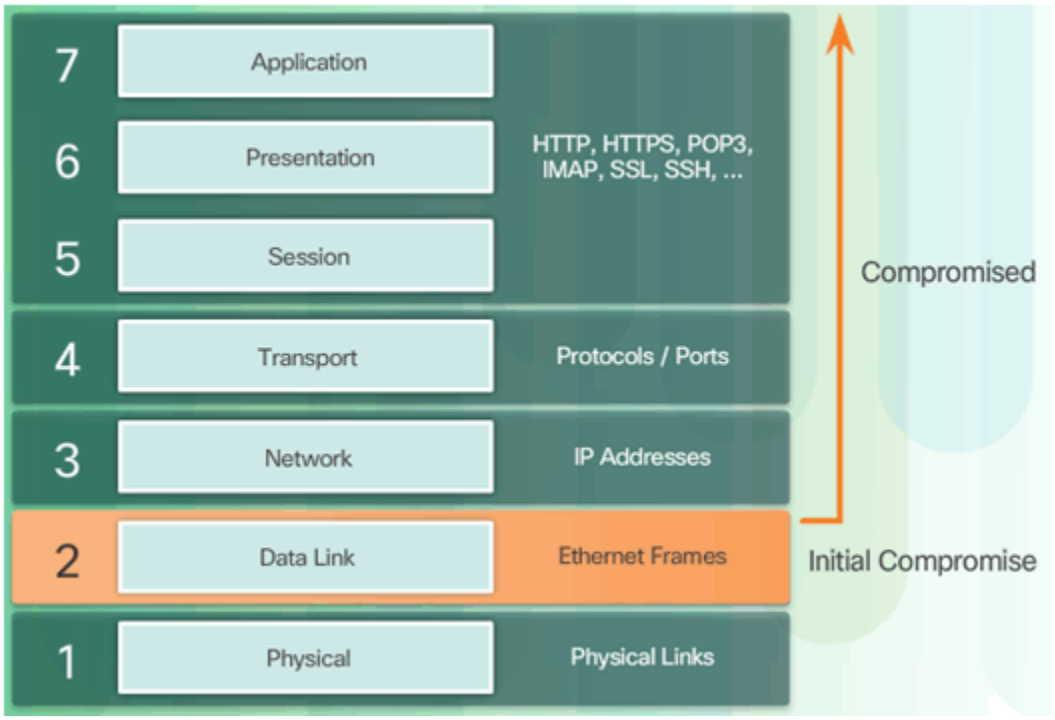
Section 6.2: Layer 2 Security Considerations

Upon completion of the section, you should be able to:

- Describe Layer 2 vulnerabilities.
- Describe 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.
- Implement IP Source Guard to mitigate address spoofing attacks.

Topic 6.2.1: Layer 2 Security Threats

Describe Layer 2 Vulnerabilities



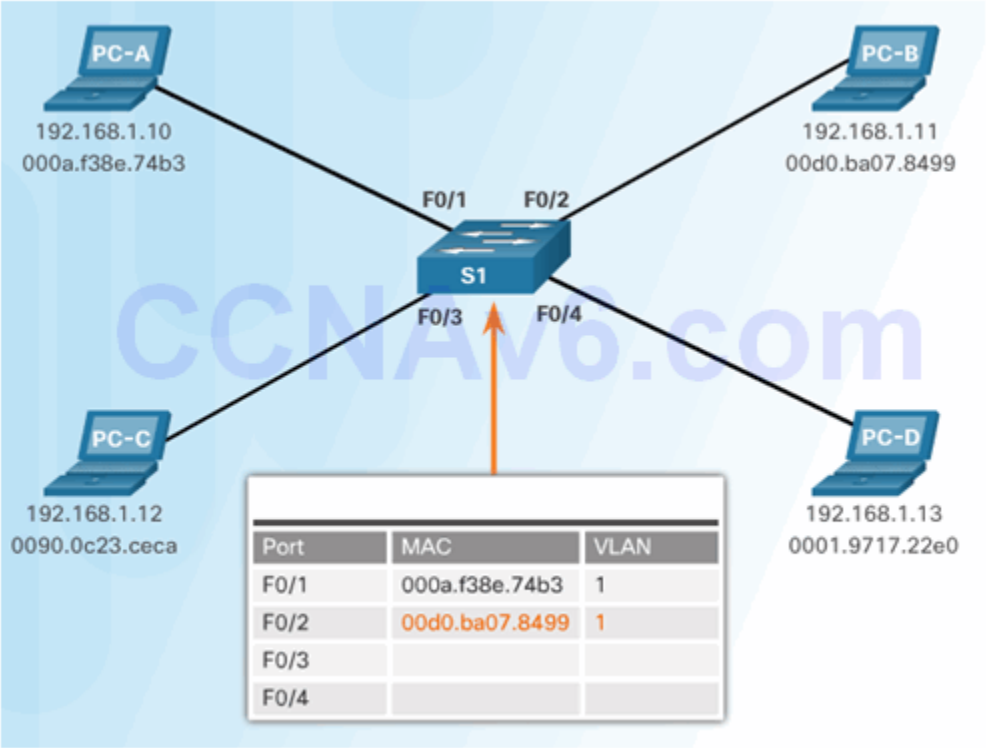
Switch Attack Categories

Topic 6.2.2: CAM Table Attacks

Basic Switch Operation

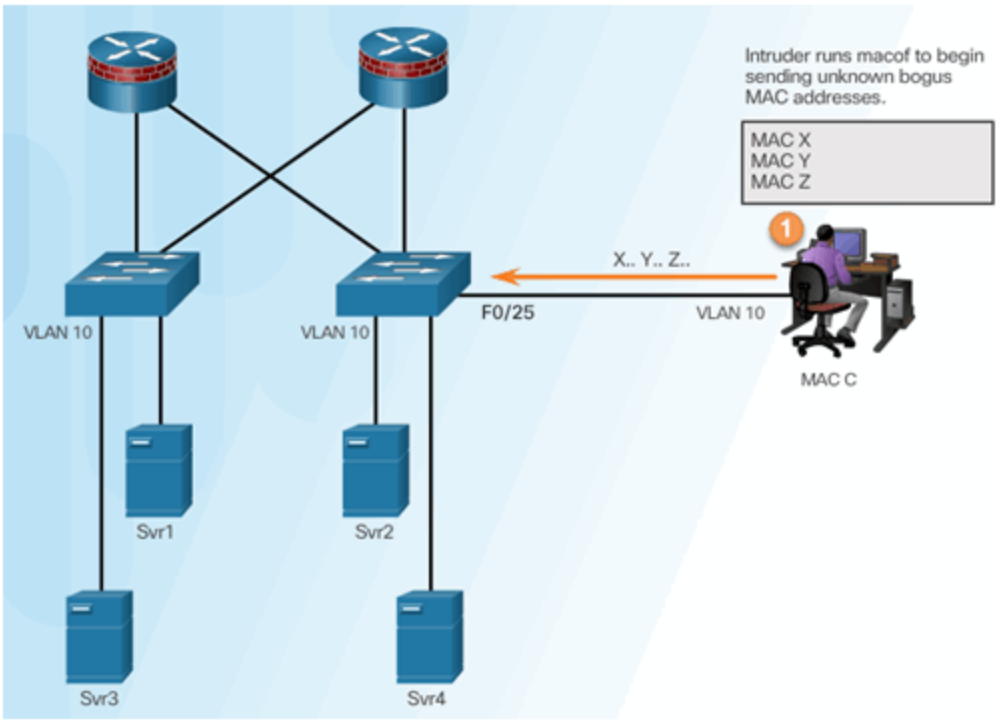
```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

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

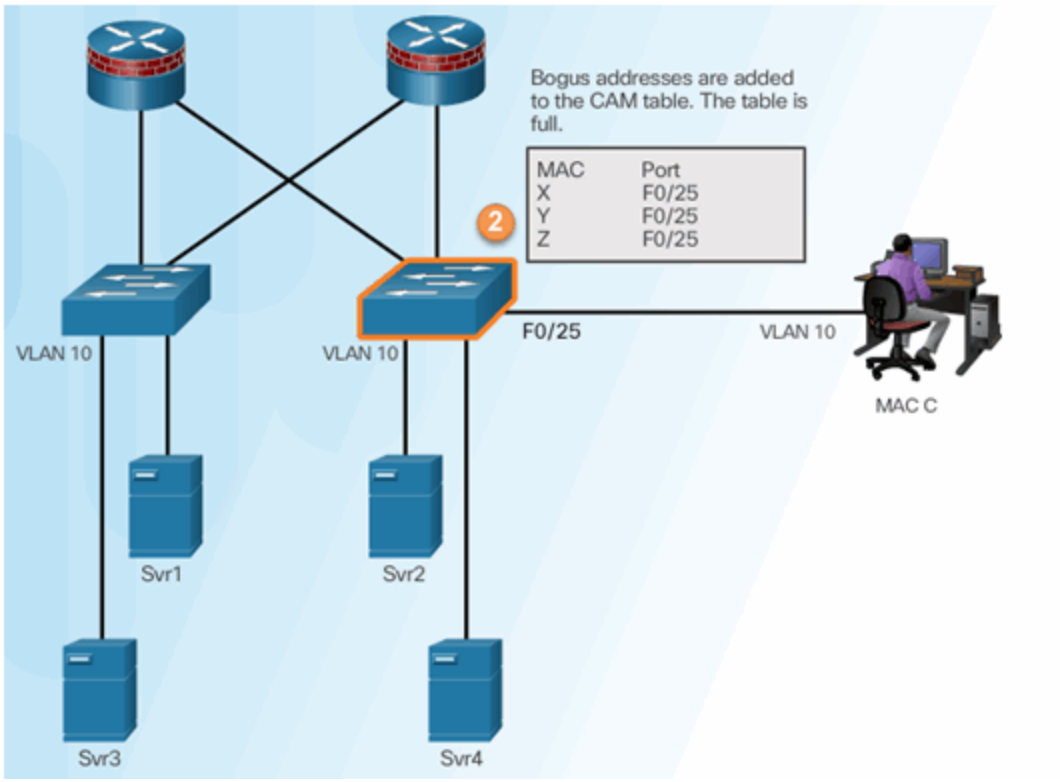


CAM Table Attack

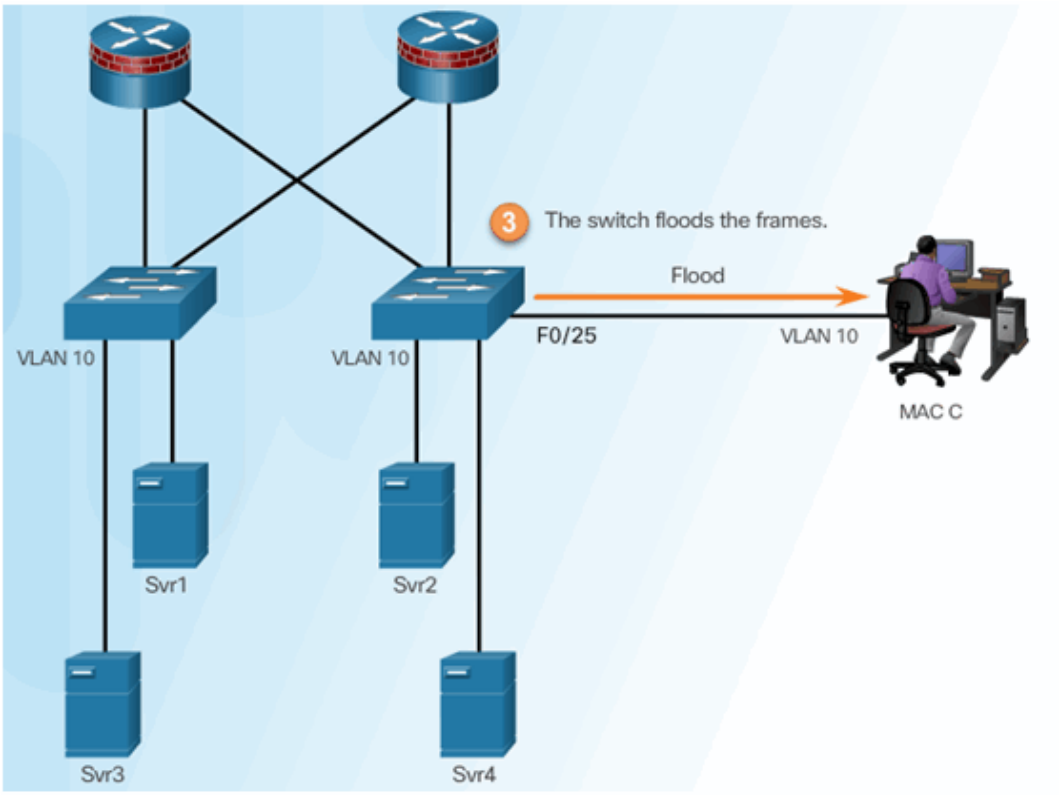
Intruder Runs Attack Tool



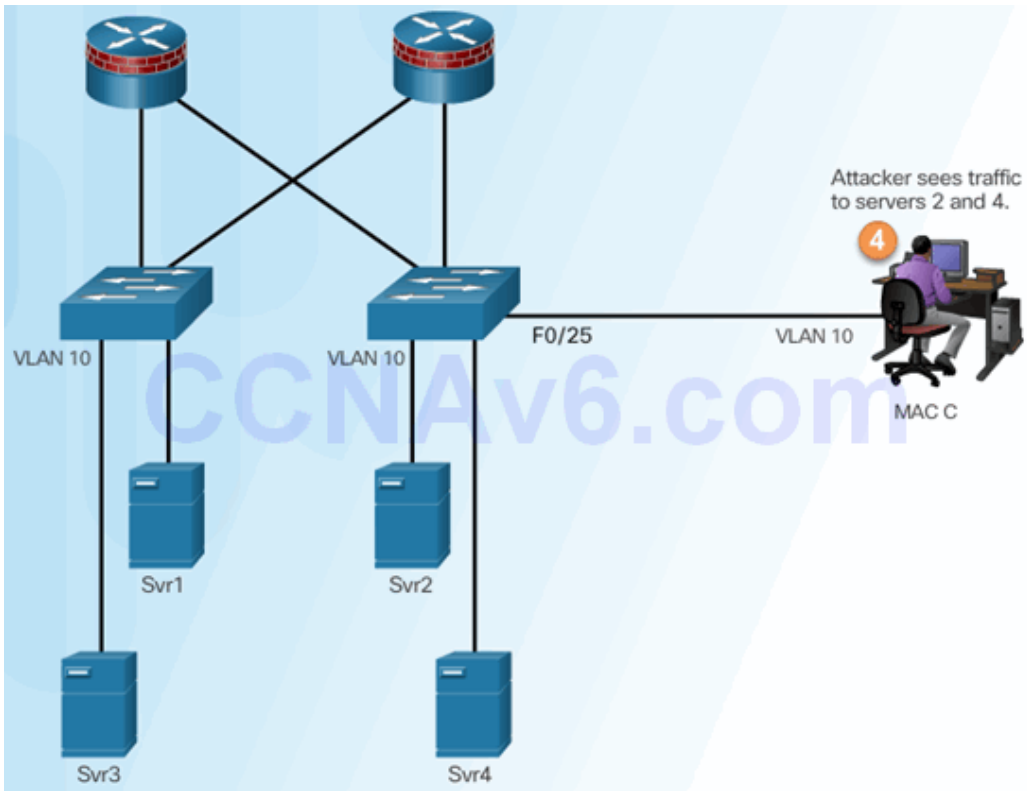
Fill CAM Table



Switch Floods All Traffic



Attacker Captures Traffic

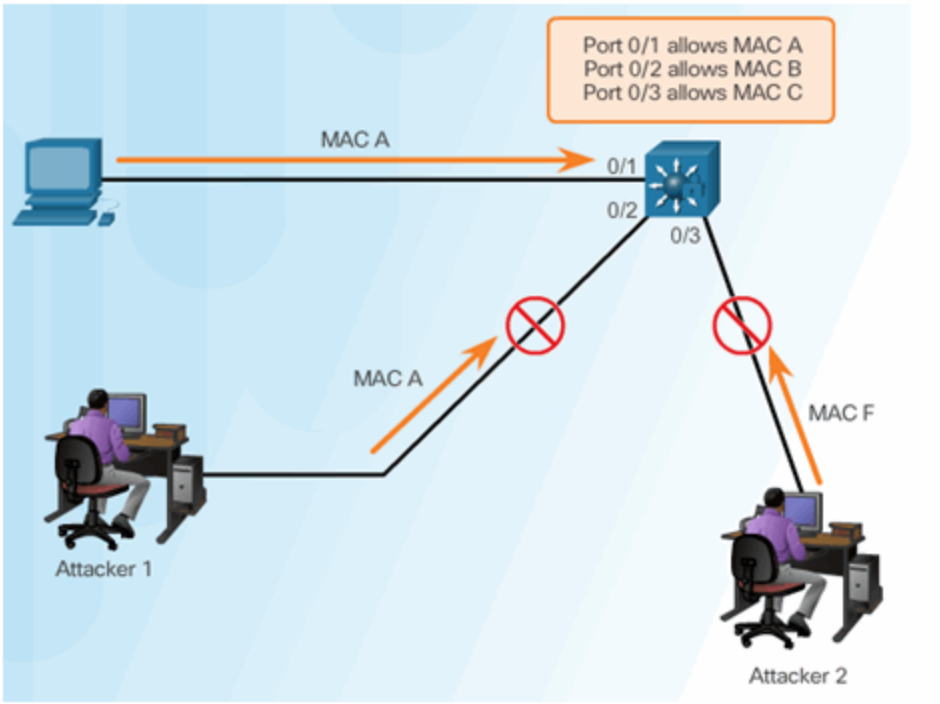


CAM Table Attack Tools

```
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

Countermeasure for CAM Table Attacks



Port Security

Enabling 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#
```

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

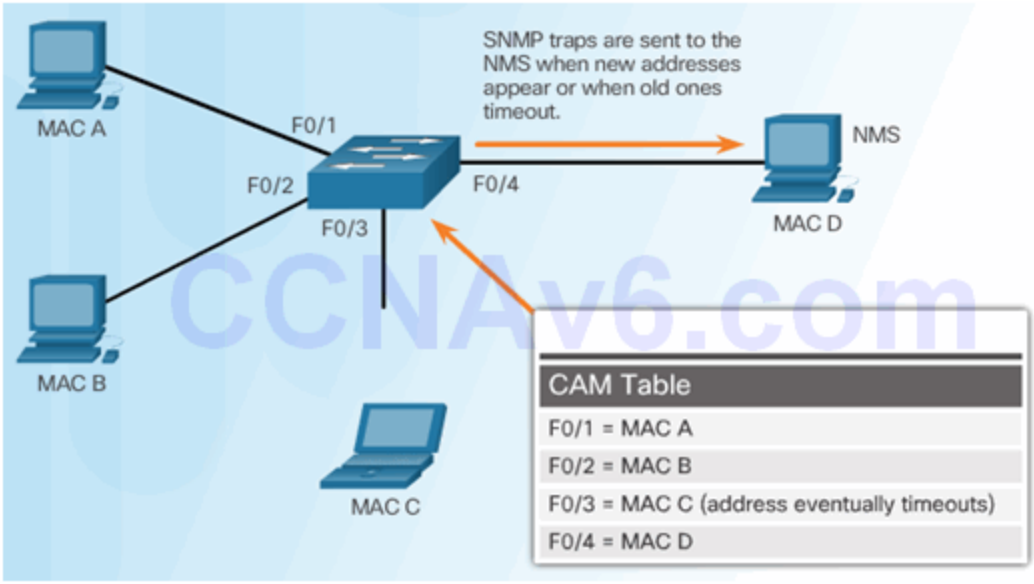
```
Switch(config-if)
switchport port-security aging {static | time time| type {absolute | inactivity}}
```

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

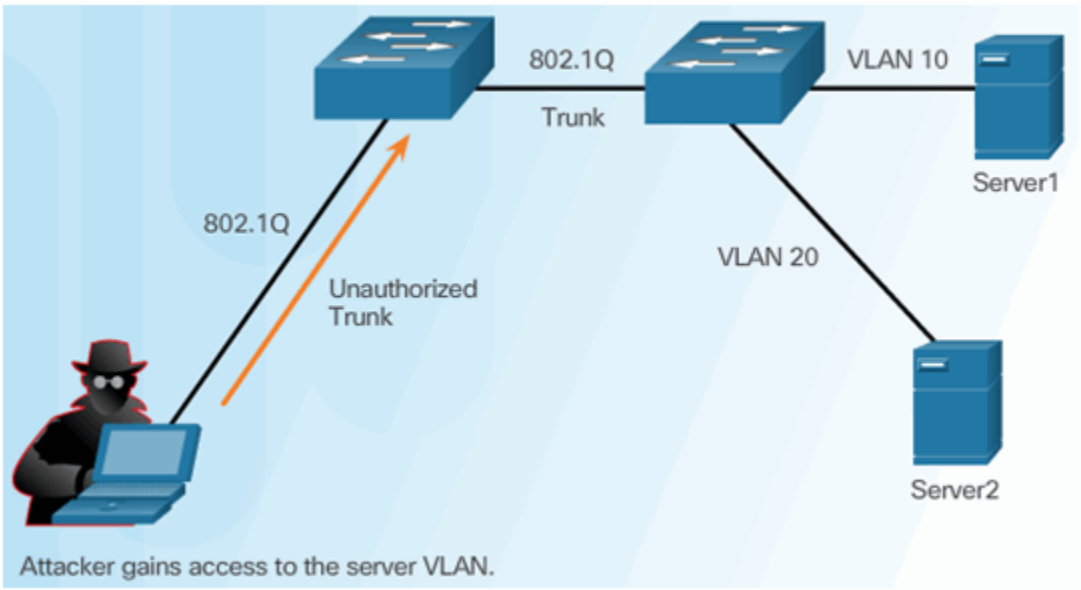

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# switchport port-security aging time 120
S1(config-if)#
```

SNMP MAC Address Notification



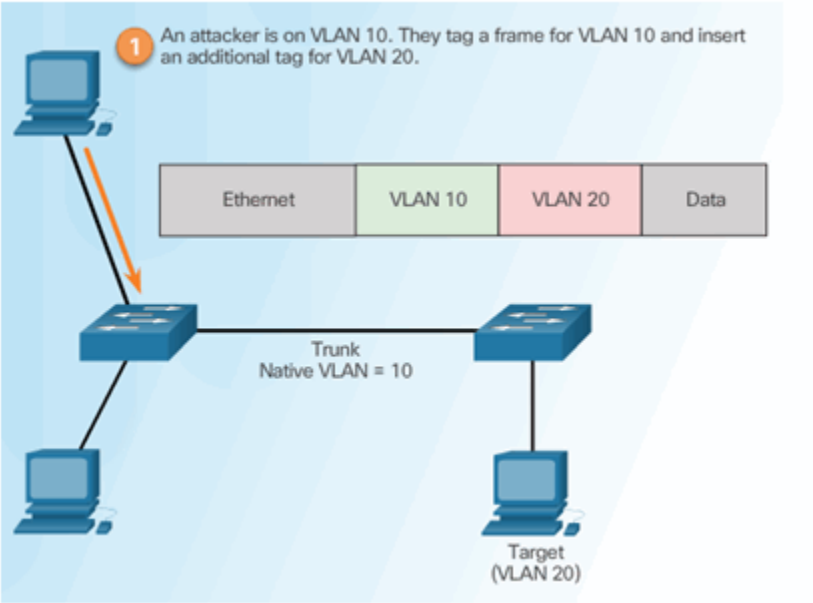
Topic 6.2.4: Mitigating VLAN Attacks

VLAN Hopping Attacks

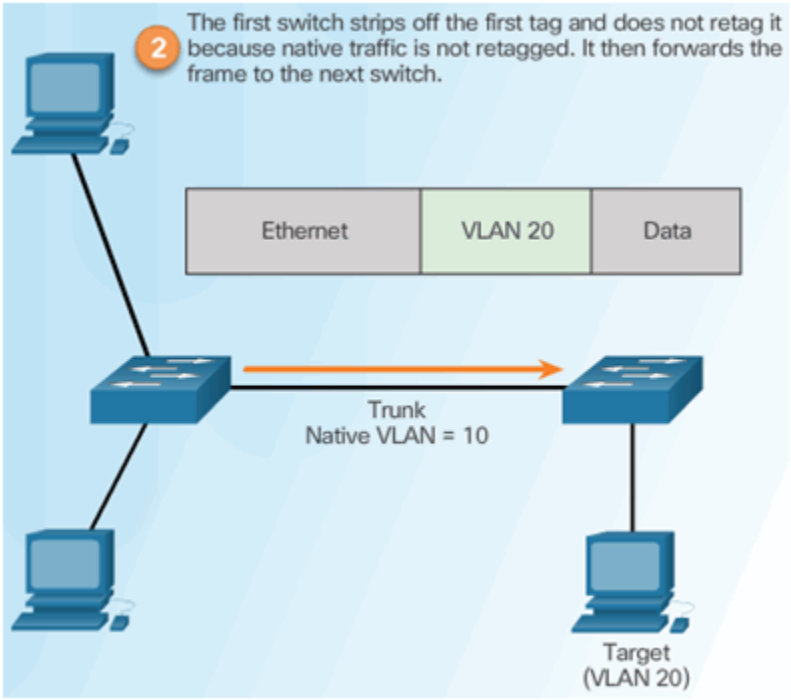


VLAN Double-Tagging Attack

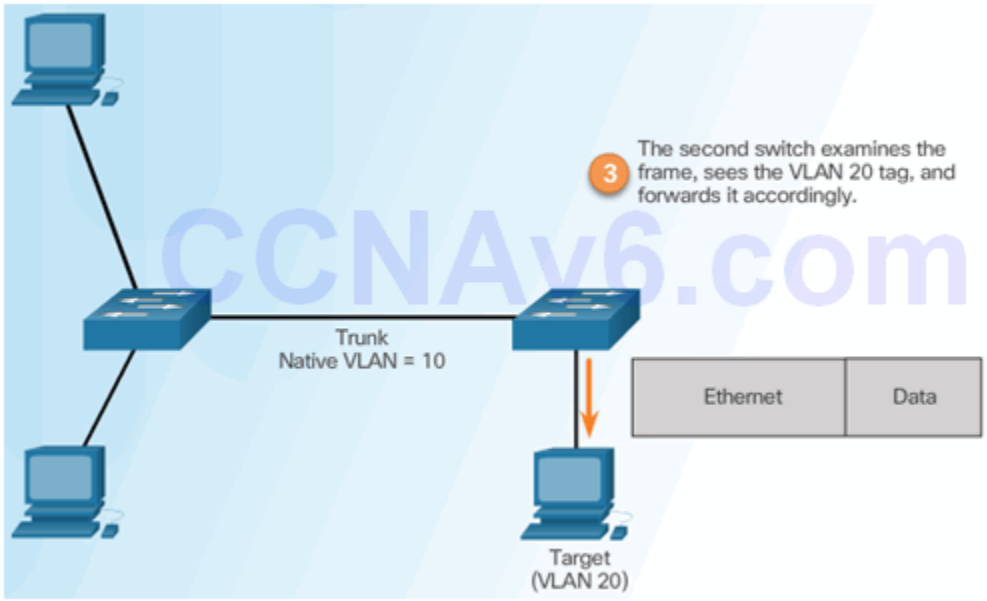
Step 1 – Double Tagging Attack



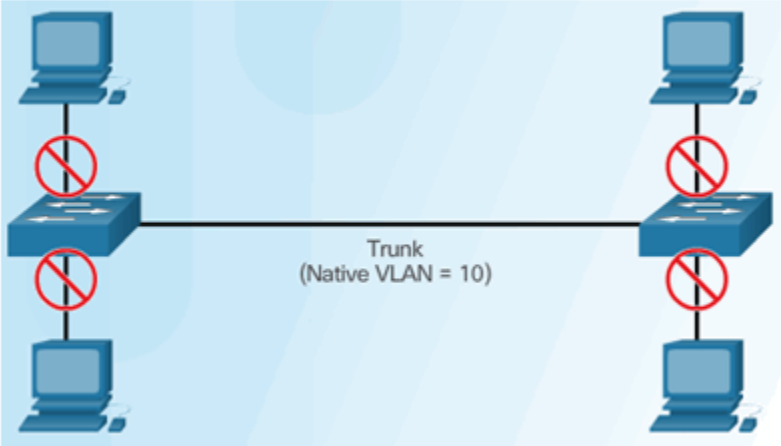
Step 2 – Double Tagging Attack



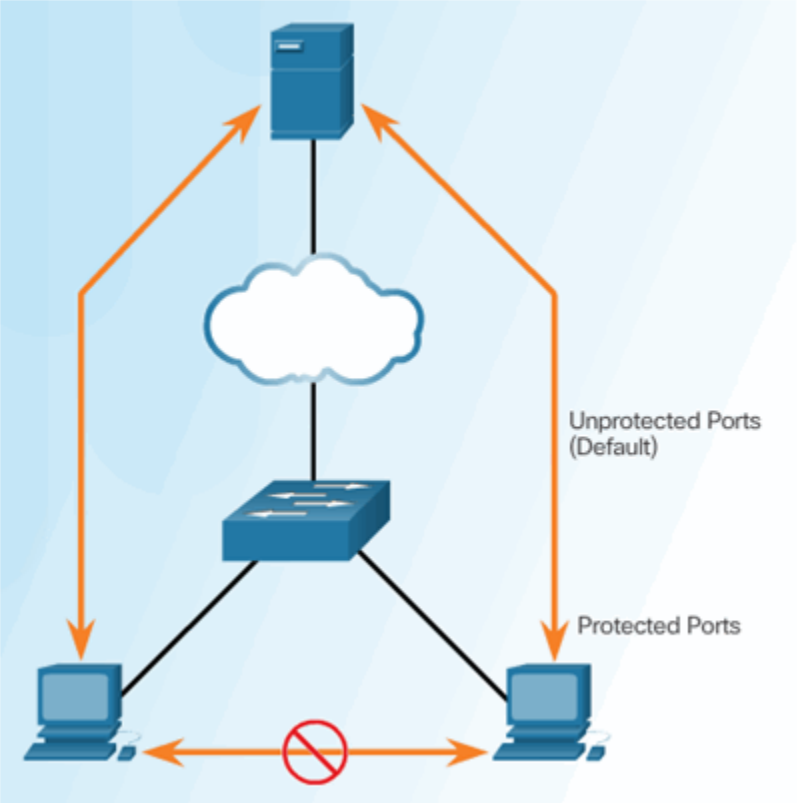
Step 3 – Double Tagging Attack



Mitigating VLAN Hopping Attacks



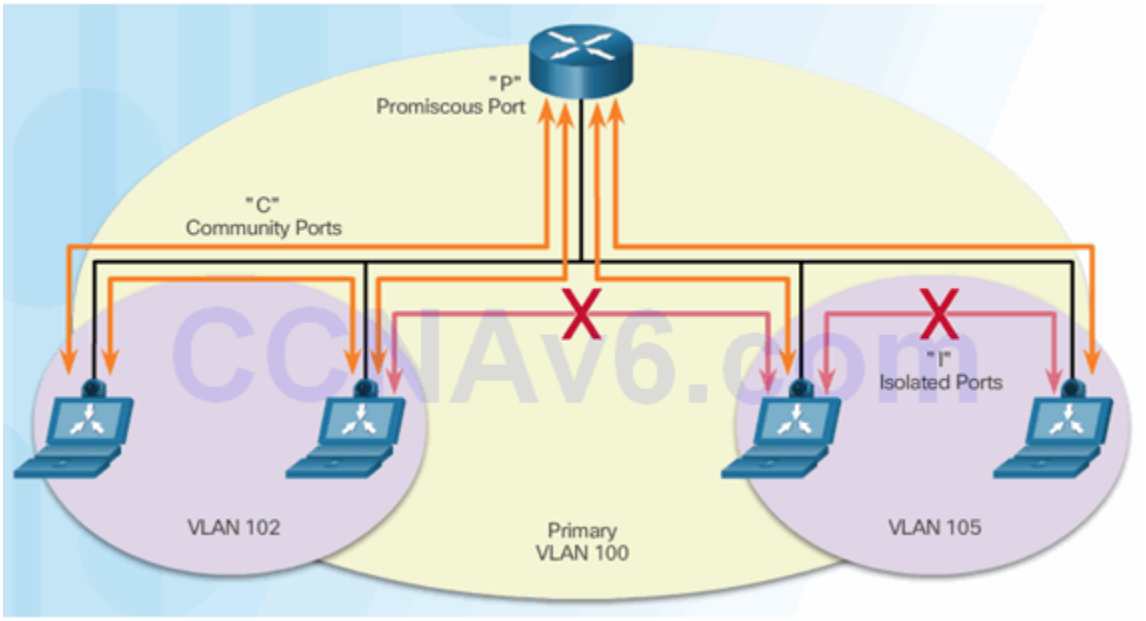
PVLAN Edge Feature



Verifying Protected Ports

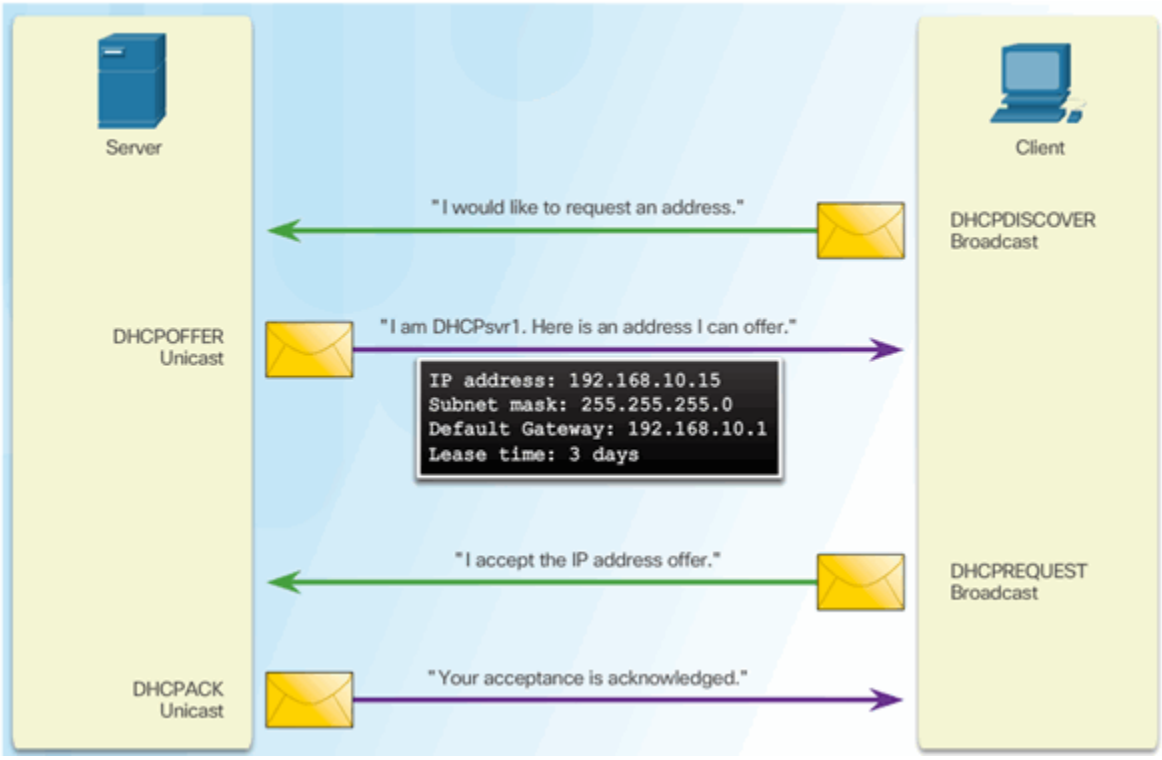
```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: G1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
<output omitted >
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

Private VLANs



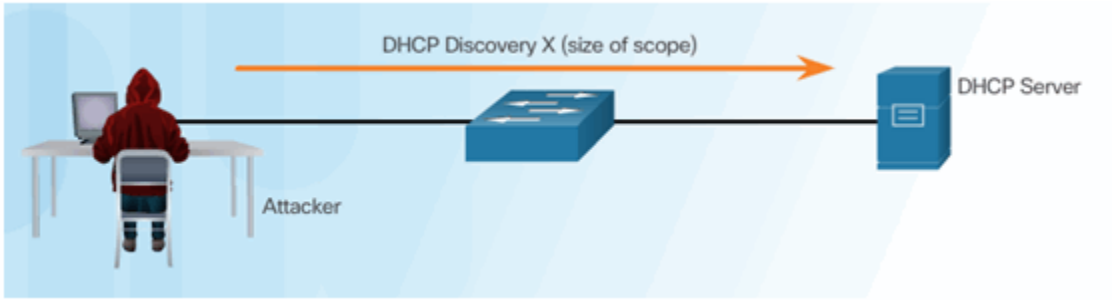
Topic 6.2.5: Mitigating DHCP Attacks

DHCP Spoofing Attack

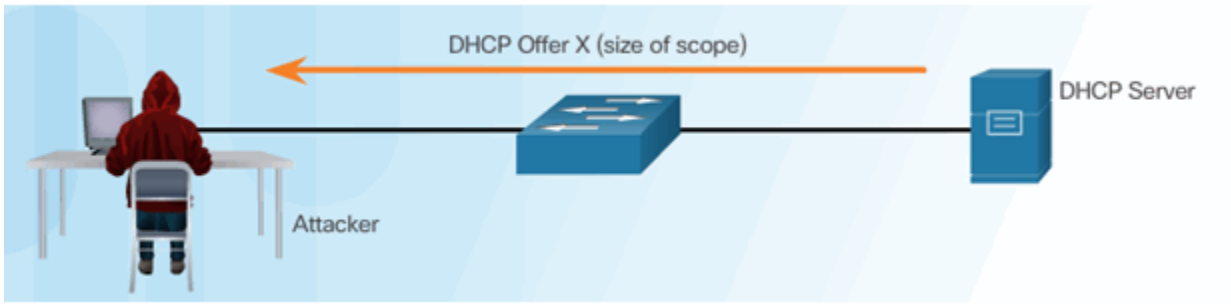


DHCP Starvation Attack

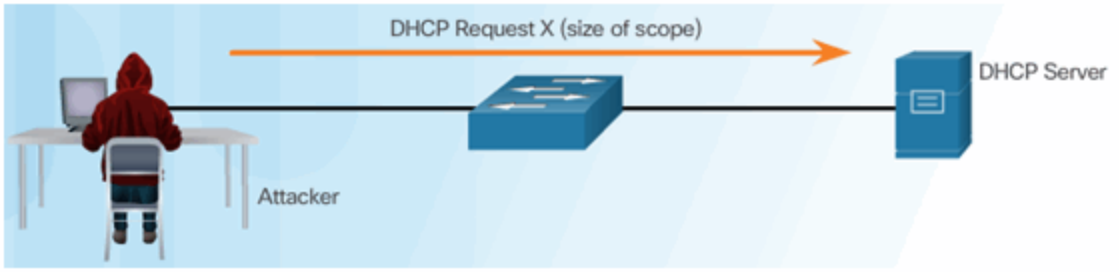
Attacker Initiates a Starvation Attack



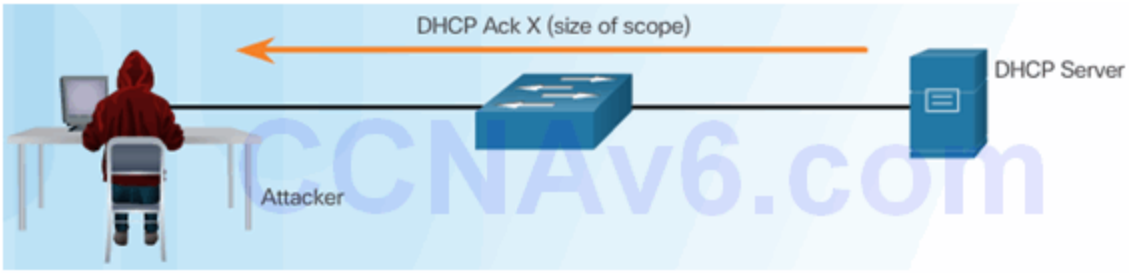
DHCP Server Offers Parameters



Client Requests all Offers



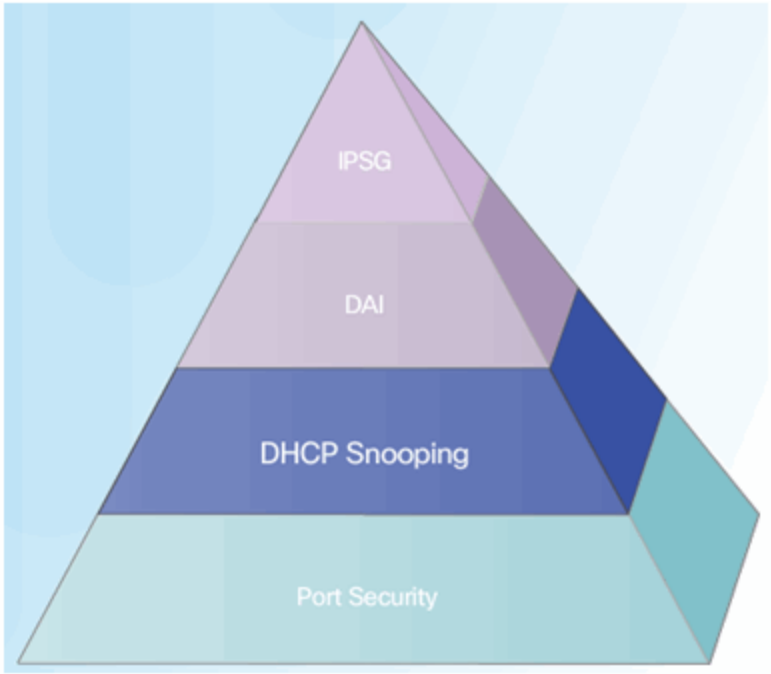
DHCP Server Acknowledges All Requests



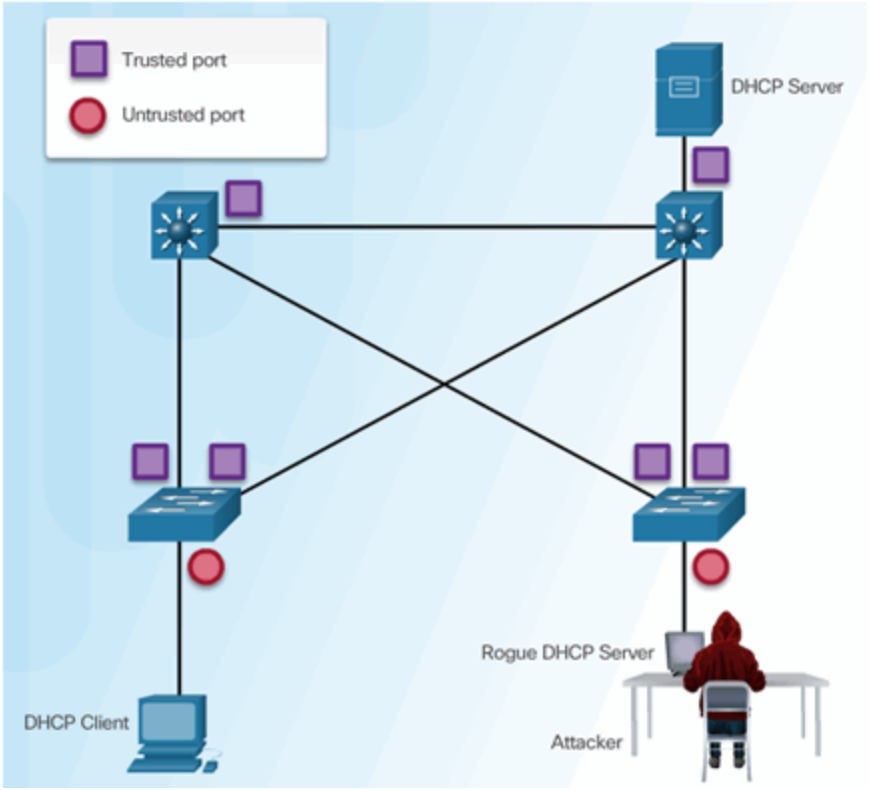
Mitigating VLAN Attacks

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

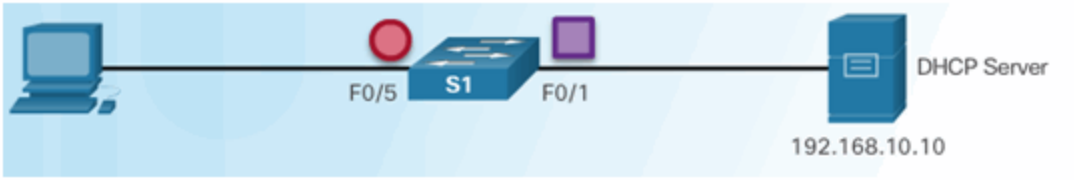


Configuring DHCP Snooping



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)#
```

Verifying DHCP Snooping

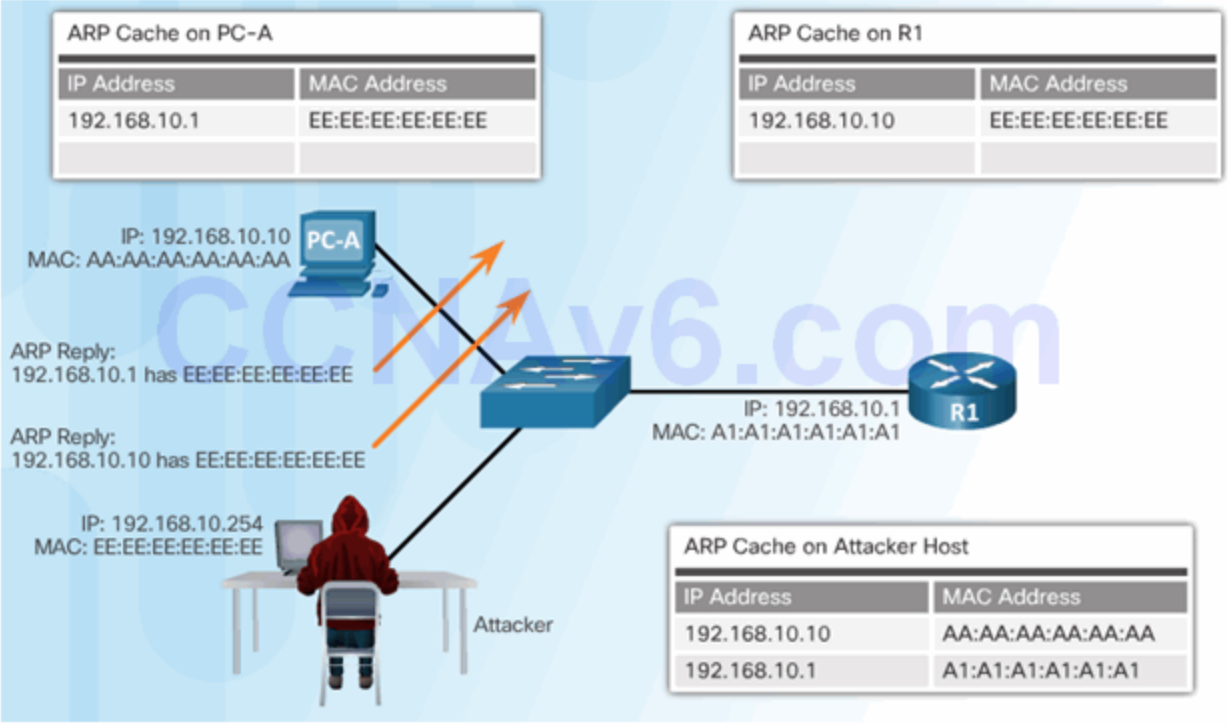
```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

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
```

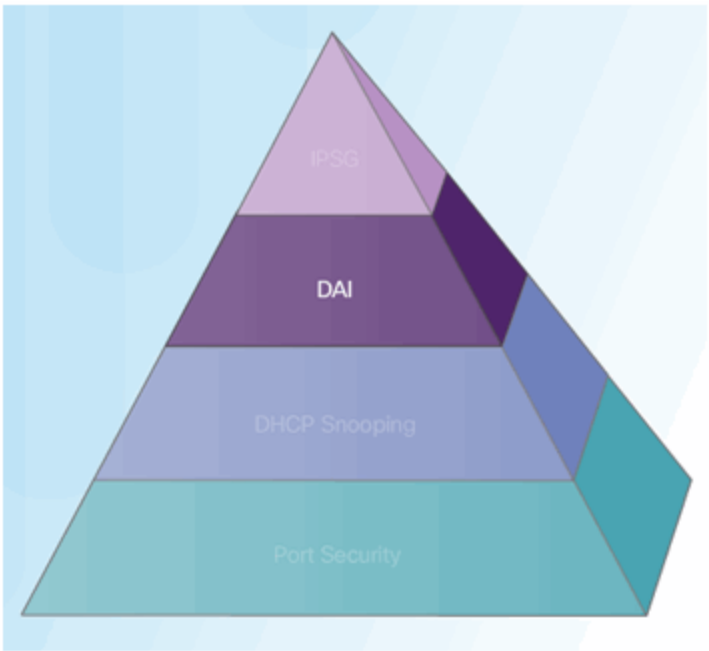
Topic 6.2.6: Mitigating ARP Attacks

ARP Spoofing and ARP Poisoning Attack

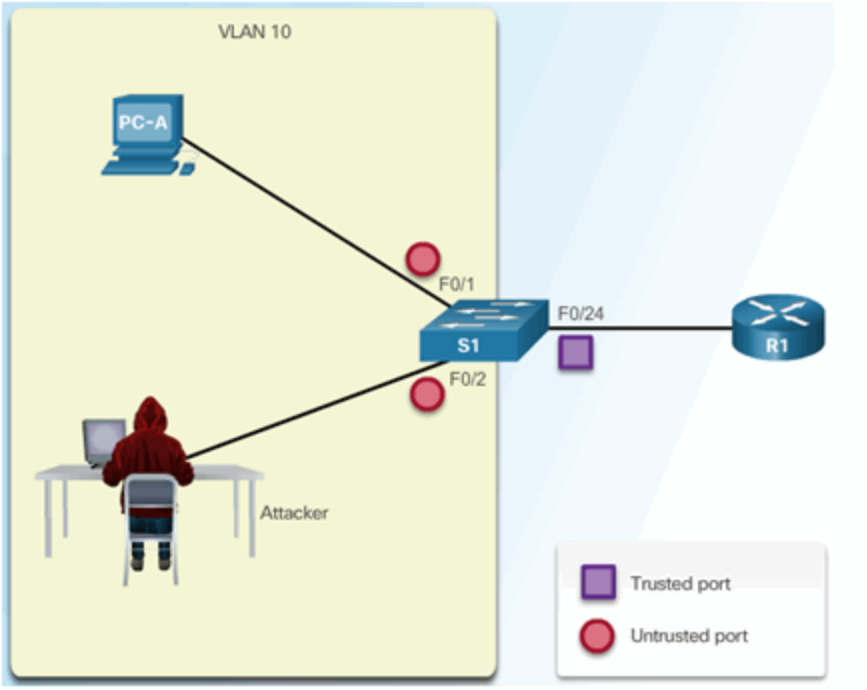


Mitigating ARP Attacks

Dynamic ARP Inspection:

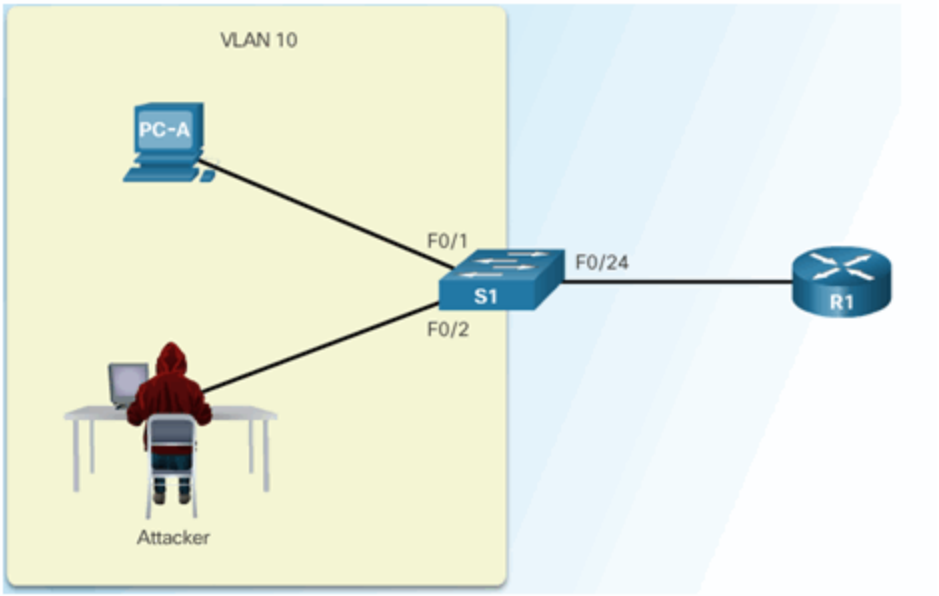


Configuring Dynamic ARP Inspection



Configuring DHCP Snooping Example

ARP Reference Topology



Configuring Dynamic ARP Inspection

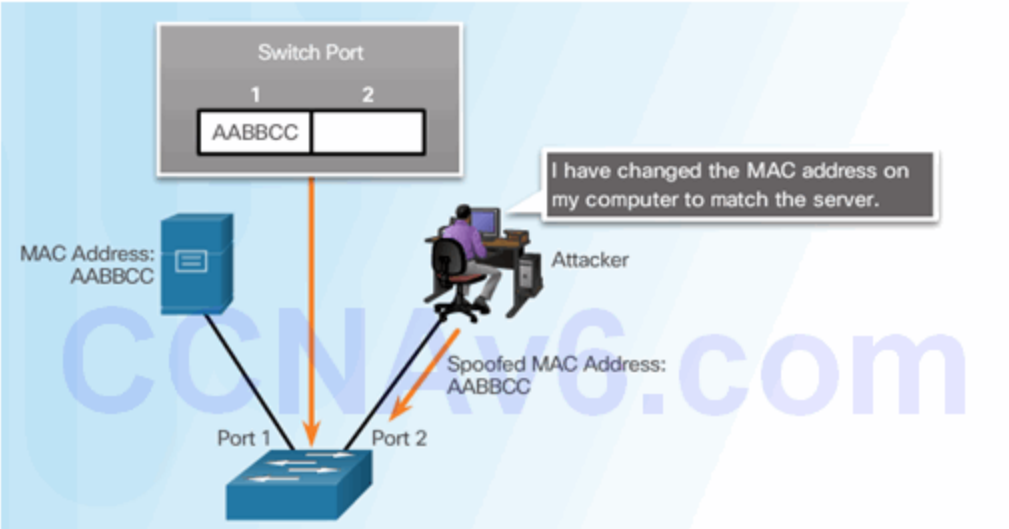
```
S1(config)# ip dhcp snooping
S1(config)#
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)#
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection  trust
S1(config-if)#
```

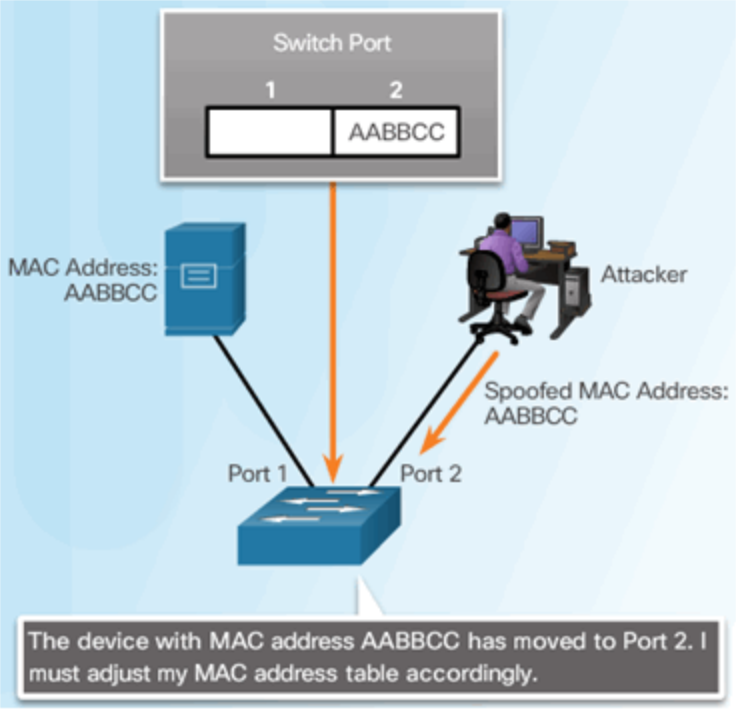
Checking Source, Destination, and IP

```
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)#
```

Topic 6.2.7: Mitigating Address Spoofing Attacks

Address Spoofing Attack

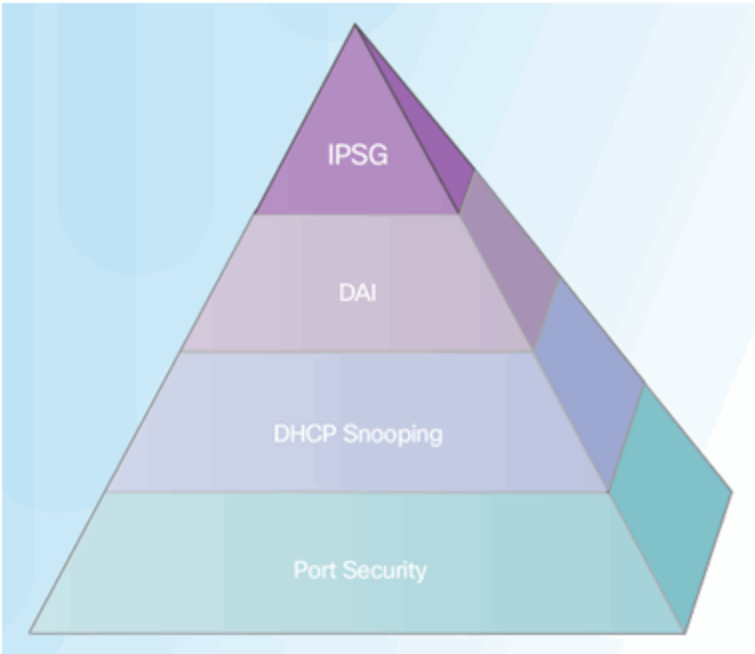




Mitigating Address Spoofing Attacks

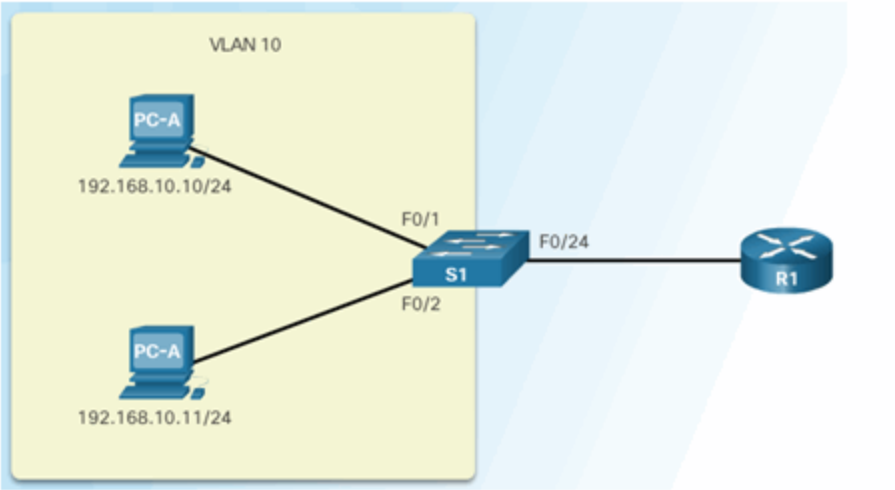
For each untrusted port, there are two possible levels of IP traffic security filtering:

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



Configuring IP Source Guard

IP Source Guard Reference Topology



Configuring IP Source Guard

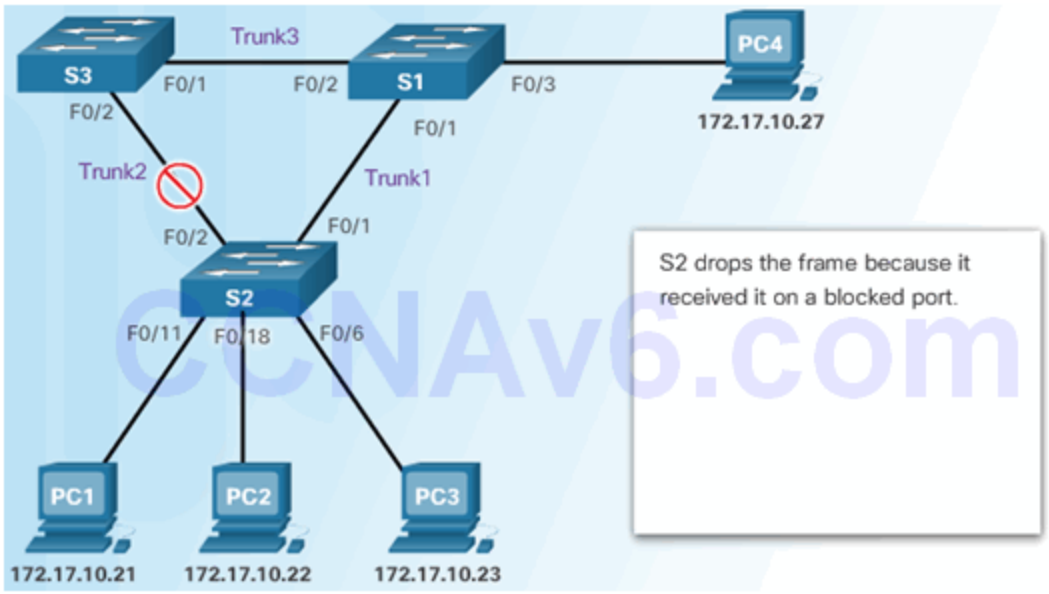
```
S1(config)# interface range fastethernet 0/1 - 2
S1(config-if-range)# ip verify source
S1(config-if-range)# end
S1#
```

Checking IP Source Guard

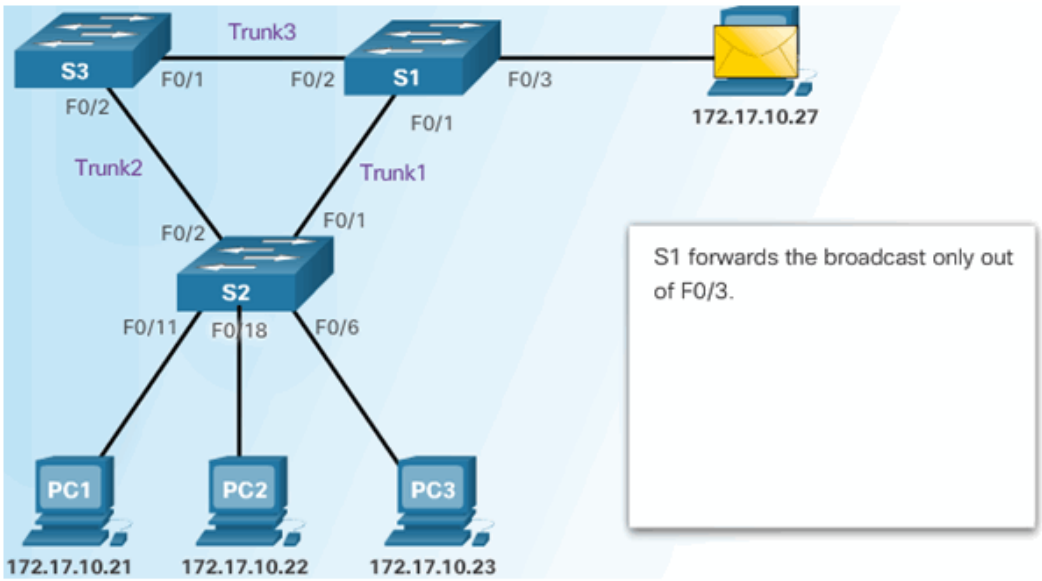
```
S1# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
F0/1       ip           active       192.168.10.10                       10
F0/2       ip           active       192.168.10.11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

Topic 6.2.8: Spanning Tree Protocol

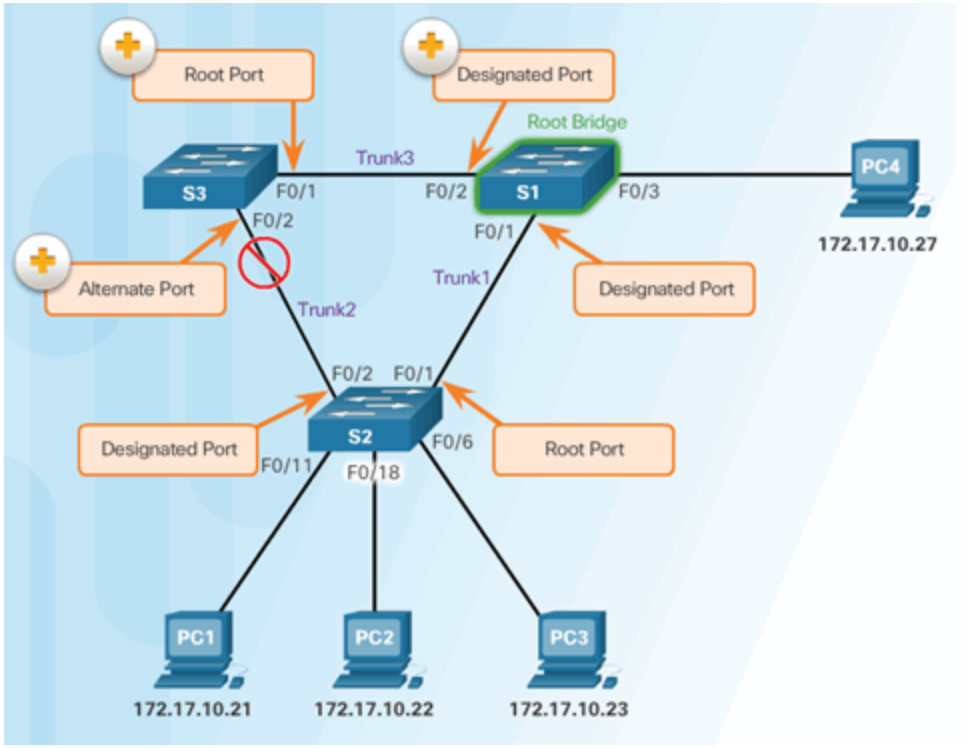
Introduction to the Spanning Tree Protocol



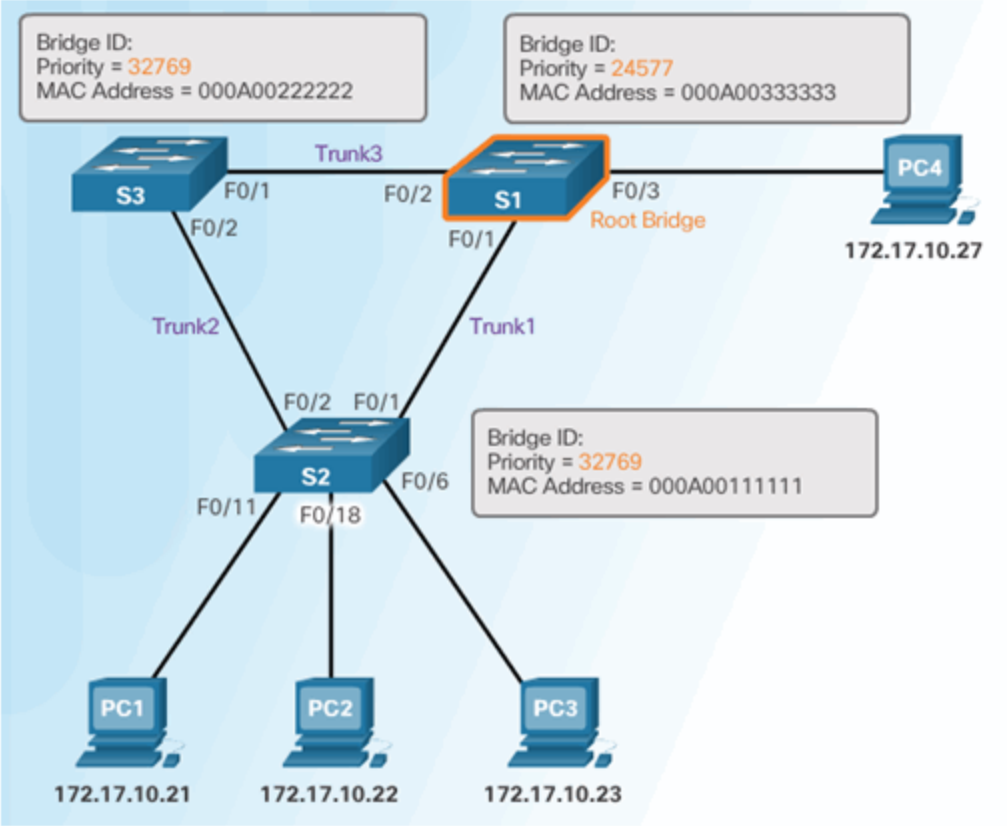
Various Implementations of STP



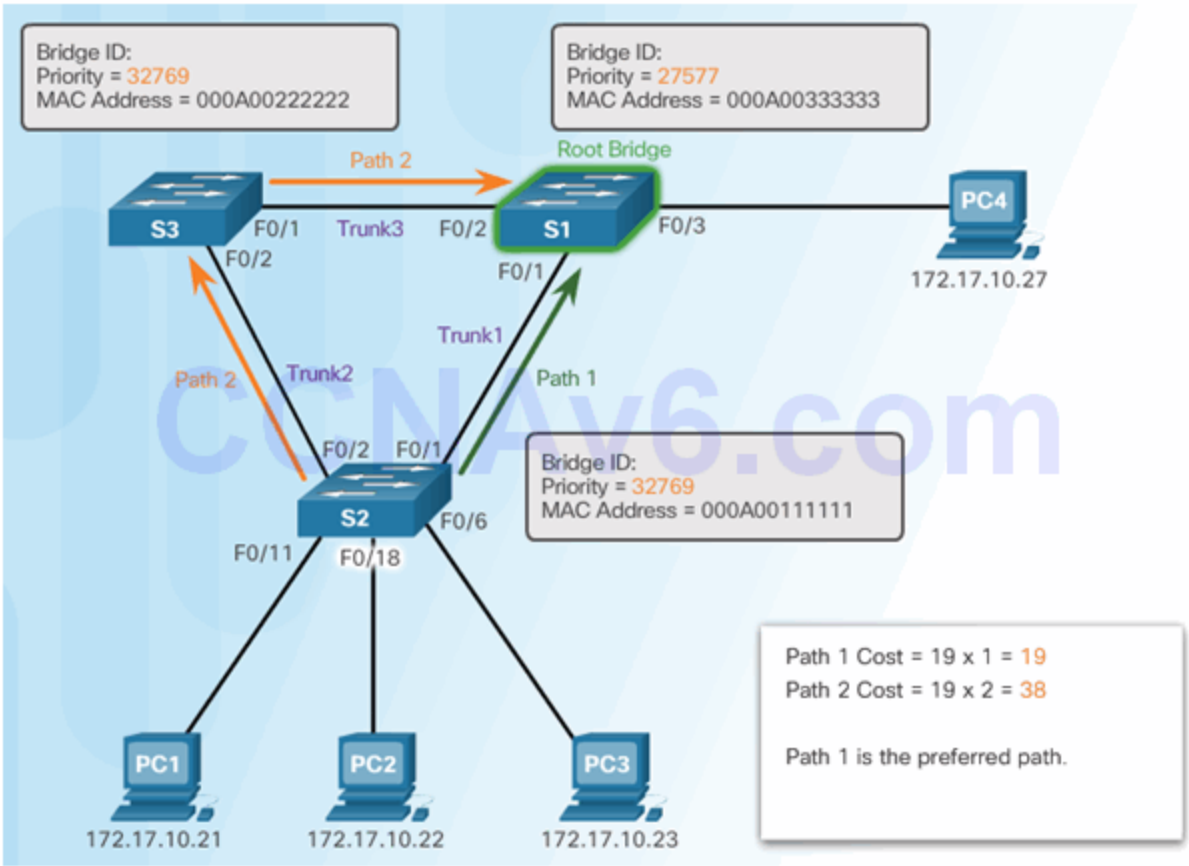
STP Port Roles



STP Root Bridge



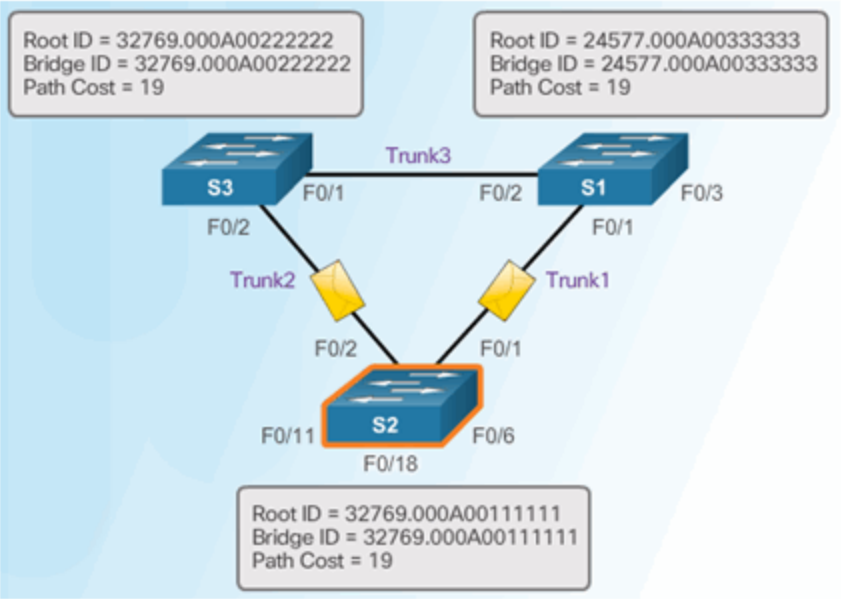
STP Path Cost



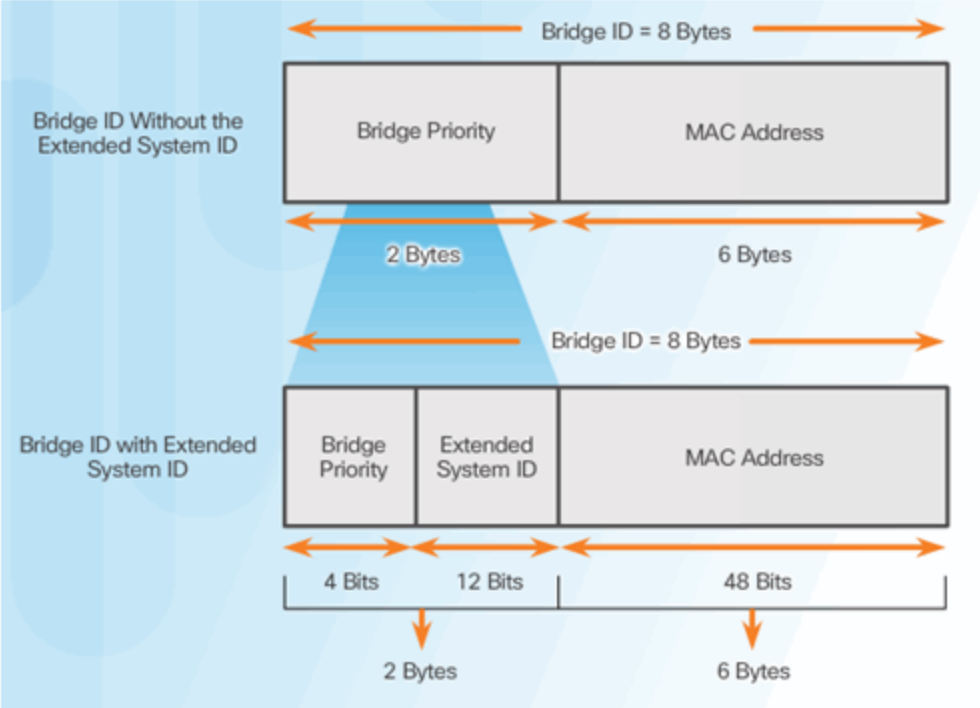
802.1D BPDU Frame Format

Field Number	Bytes	Field
1-4	2	Protocol ID
	1	Version
	1	Message type
	1	Flags
5-8	8	Root ID
	4	Cost of path
	8	Bridge ID
	2	Port ID
9-12	2	Message age
	2	Max age
	2	Hello time
	2	Forward delay

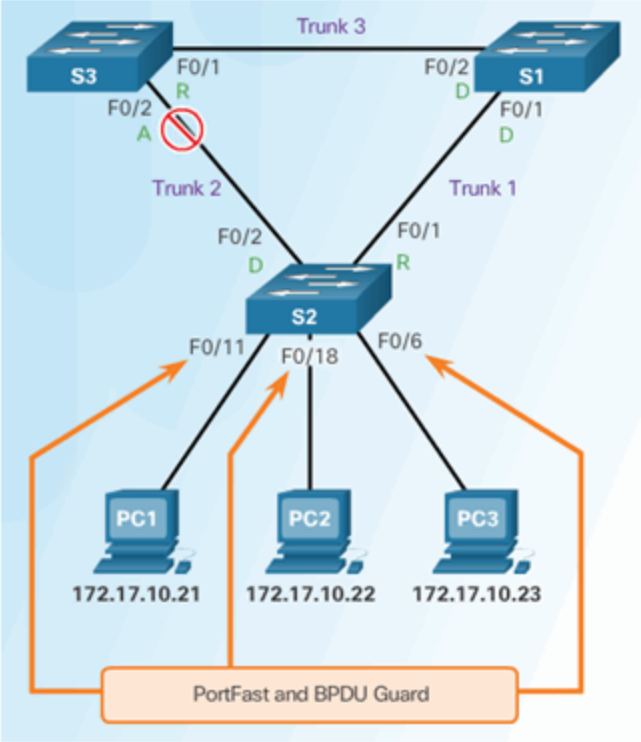
BPDU Propagation and Process



Extended System ID



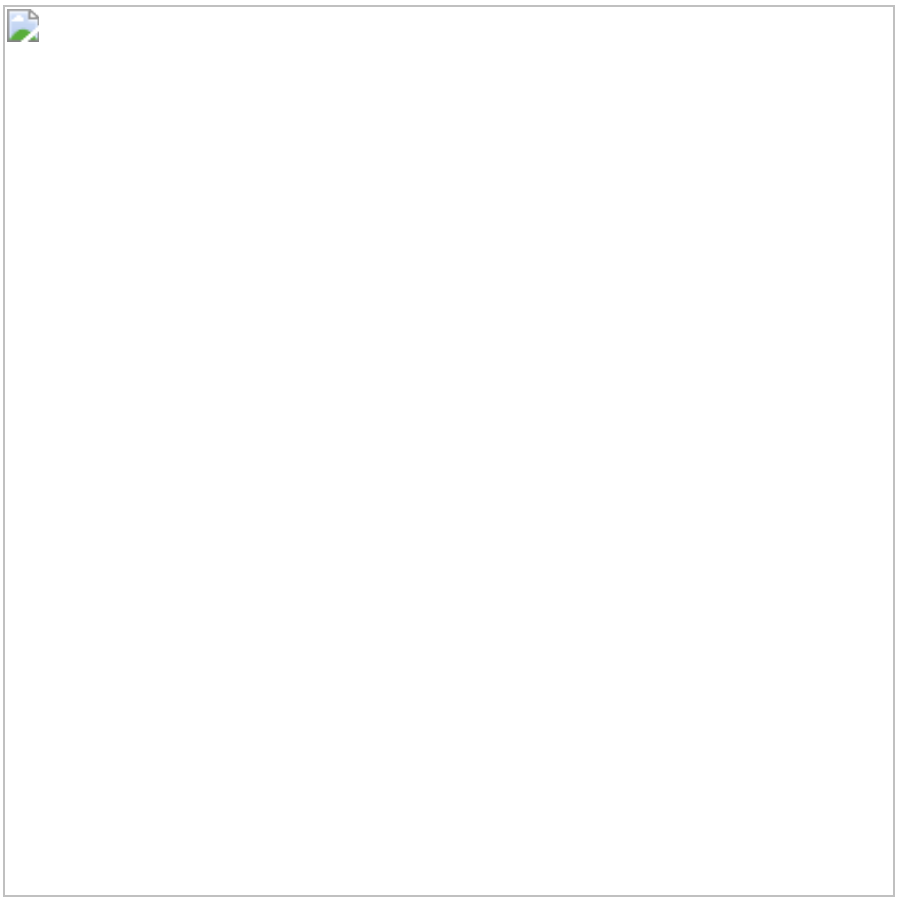
Select the Root Bridge

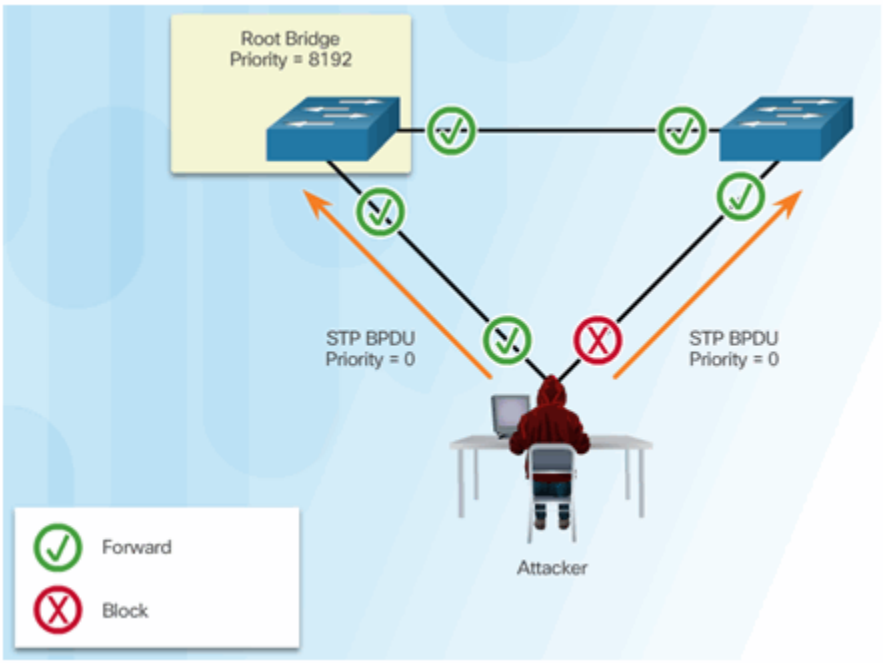


Topic 6.2.9: Mitigating STP Attacks

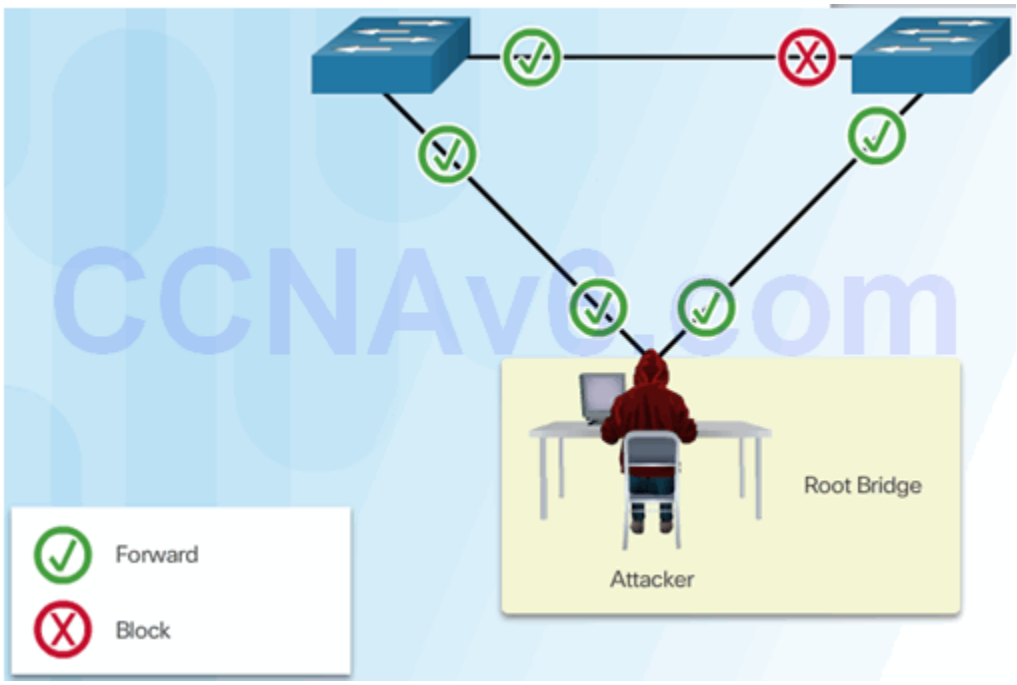
STP Manipulation Attacks

Spoofing the Root Bridge

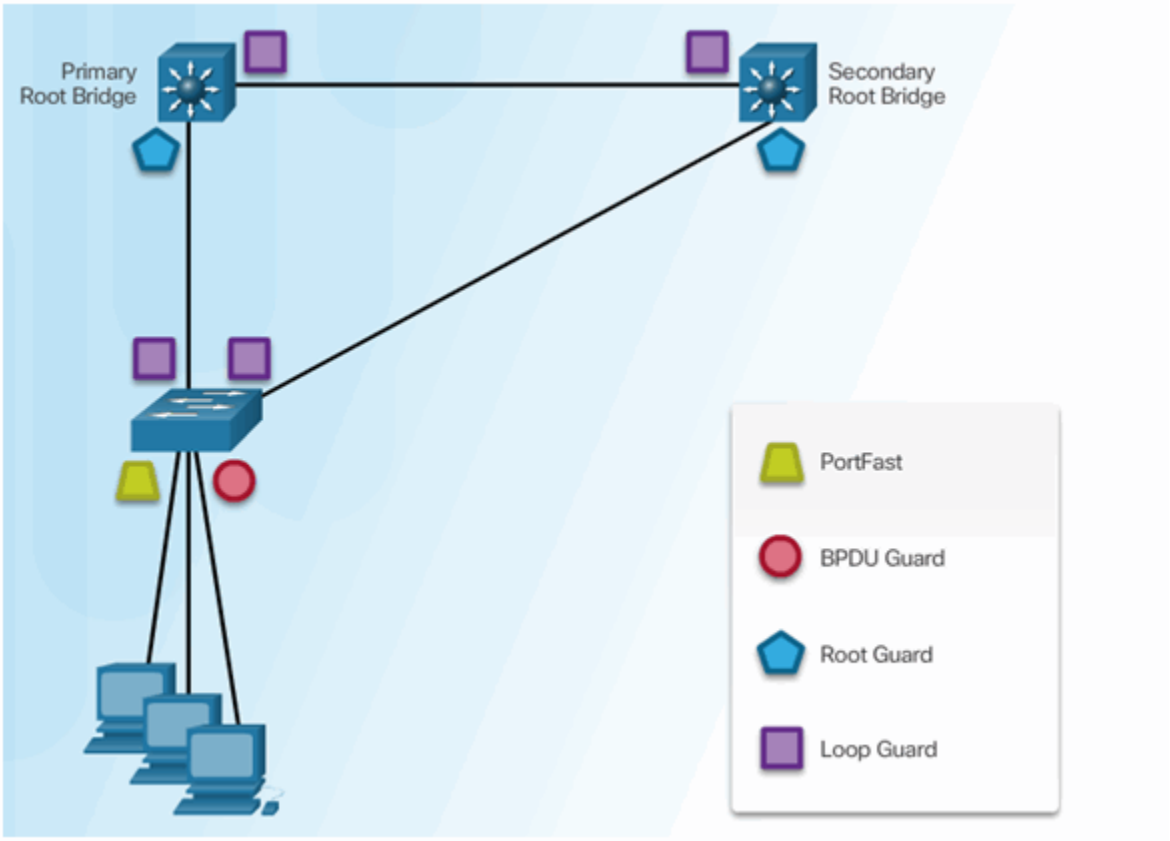




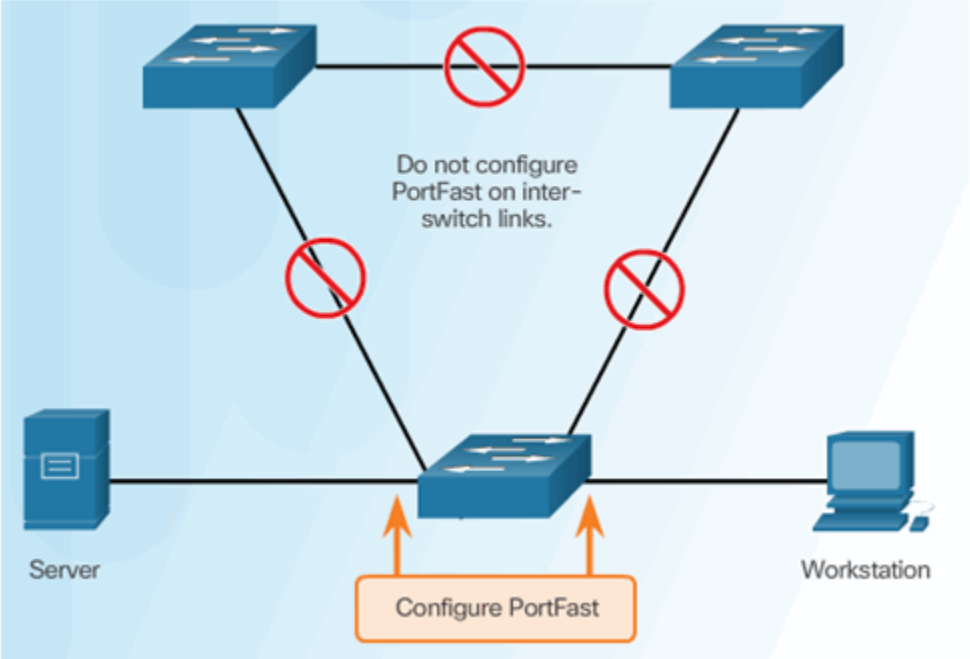
Successful STP Manipulation Attack



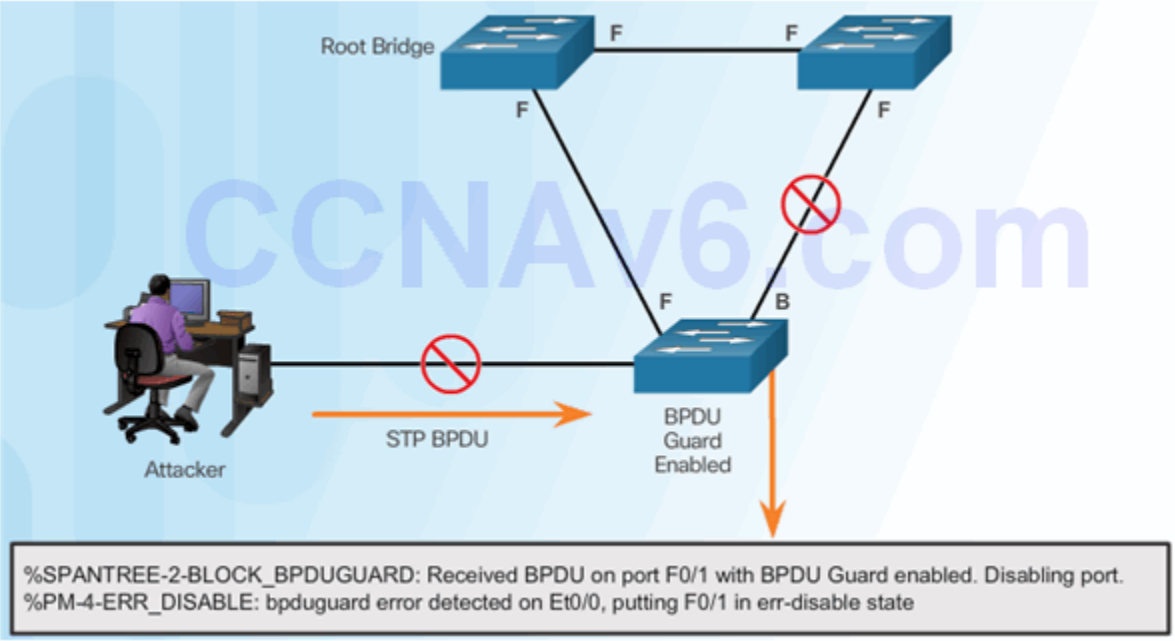
Mitigating STP Attacks



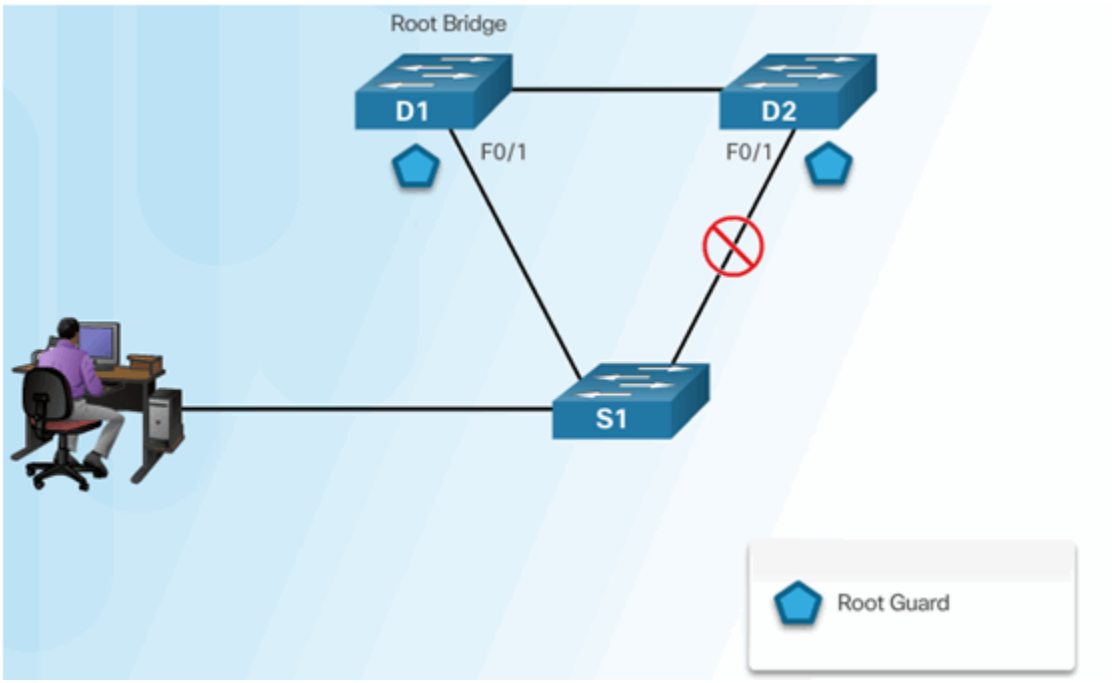
Configuring PortFast



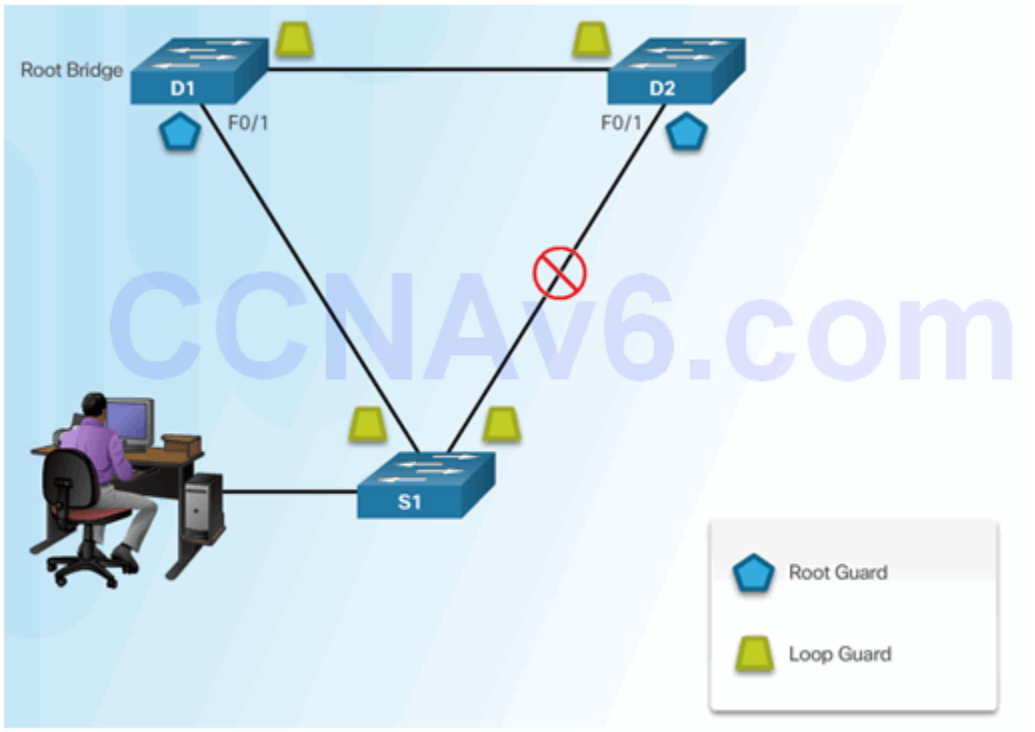
Configuring BDPU Guard



Configuring Root Guard



Configuring Loop Guard



Section 6.3: Summary

Chapter Objectives:

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

Download Slide PowerPoint (pptx):

[sociallocker id=”54558″]

CCNASv2_InstructorPPT_CH6 5.70 MB 2085 downloads

...

Download

[/sociallocker]