Chapter 5:

Securing the Campus Infrastructure

- CCNP-RS SWITCH

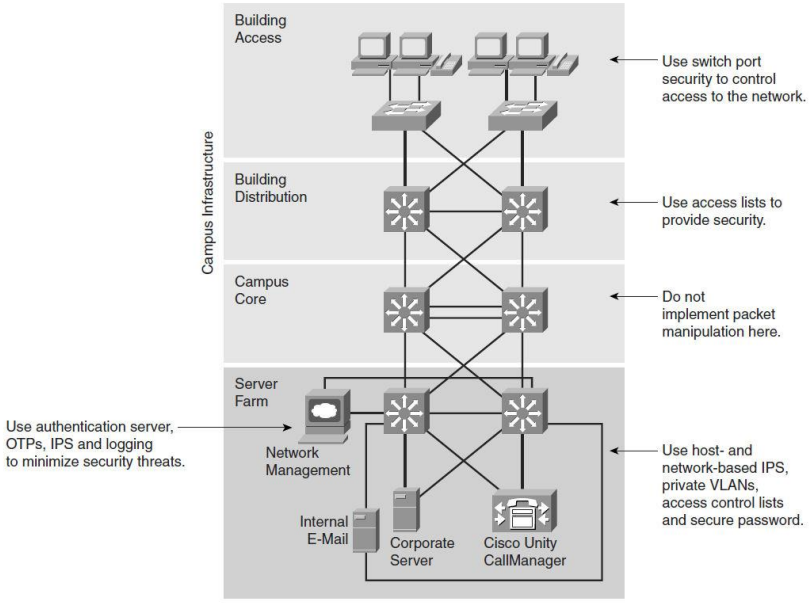
Chapter 5 Objectives

- Identify attacks and threats to switches and methods to mitigate attacks.
- Configure switches to guard against MAC-based attacks.
- Configure tight control of trunk links to mitigate VLAN hopping attacks.
- Configure switches to guard against DHCP, MAC, and address resolution protocol (ARP) threats.
- Secure Layer 2 devices and protocols.
- Develop and implement organizational security policies.
- Describe tools used to monitor and analyze network traffic.

Switch Security Fundamentals

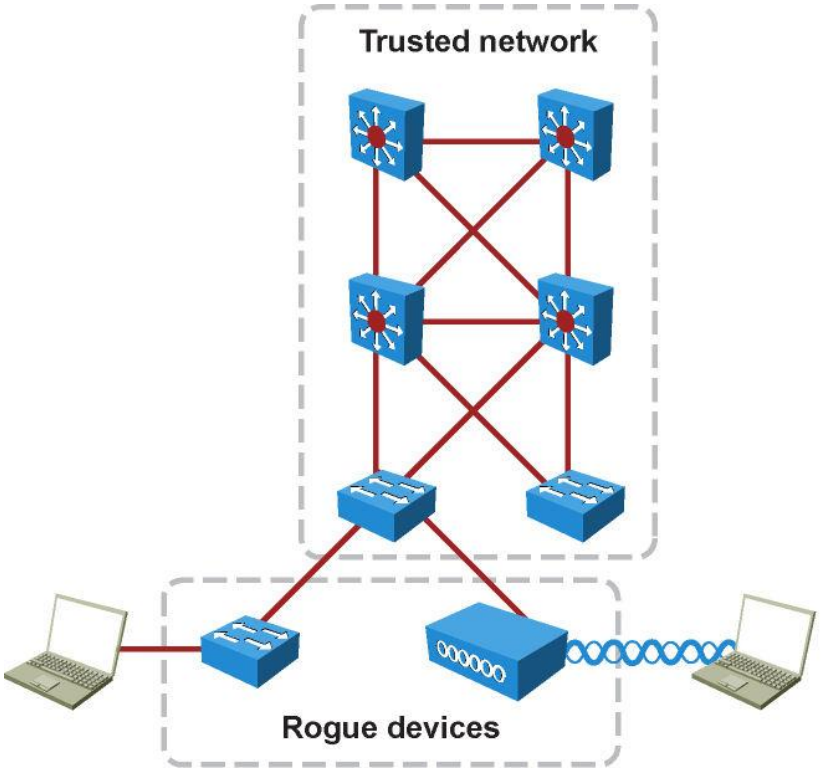
Security Infrastructure Services

- Core – switch packets quickly.
- Distribution – packet filtering.
- Access – Control at port level.
- Server farm – provide application services; include network management system.



Unauthorized Access by Rogue Devices

- Access Points
- Switches
- Servers



Layer 2 Attack Categories (1)

Attack Method	Description	Steps to Mitigation
MAC Layer Attacks		
MAC Address Flooding	Frames with unique, invalid source MAC addresses flood the switch, exhausting content addressable memory (CAM) table space, disallowing new entries from valid hosts. Traffic to valid hosts is subsequently flooded out all ports.	Port security. MAC address VLAN access maps.
VLAN Attacks		
VLAN Hopping	By altering the VLAN ID on packets encapsulated for trunking, an attacking device can send or receive packets on various VLANs, bypassing Layer 3 security measures.	Tighten up trunk configurations and the negotiation state of unused ports. Place unused ports in a common VLAN.
Attacks between Devices on a Common VLAN	Devices might need protection from one another, even though they are on a common VLAN. This is especially true on service-provider segments that support devices from multiple customers.	Implement private VLANs (PVLAN).

Layer 2 Attack Categories (2)

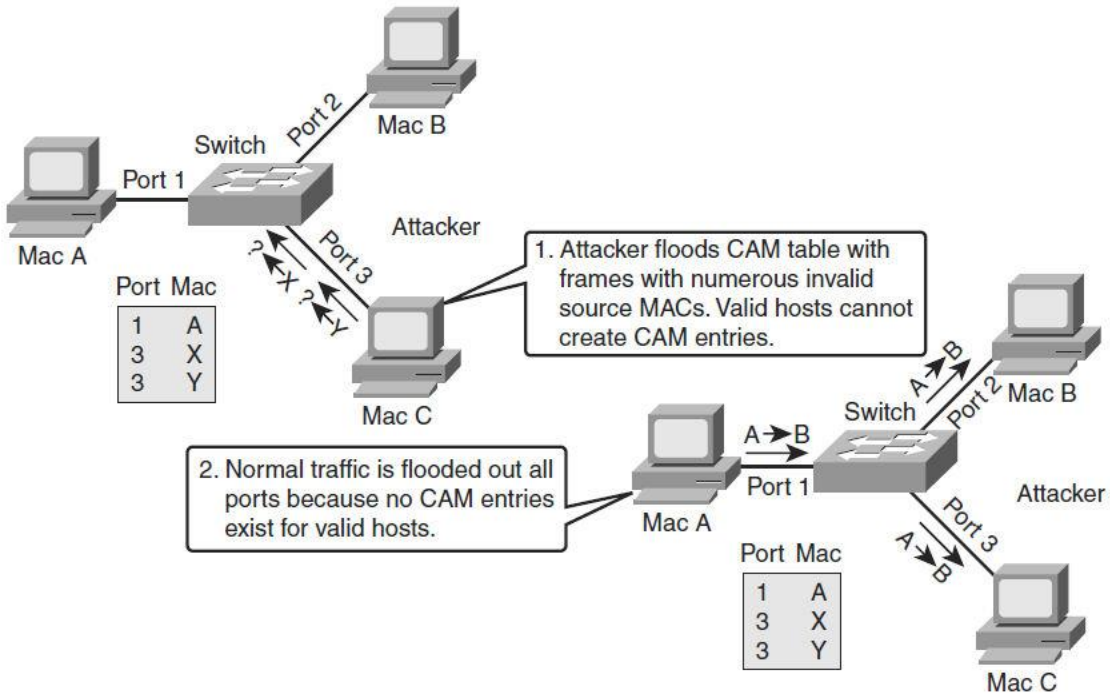
Attack Method	Description	Steps to Mitigation
Spoofing Attacks		
DHCP Starvation and DHCP Spoofing	An attacking device can exhaust the address space available to the DHCP servers for a period of time or establish itself as a DHCP server in man-in-the-middle attacks.	Use DHCP snooping.
Spanning-tree Compromises	Attacking device spoofs the root bridge in the STP topology. If successful, the network attacker can see a variety of frames.	Proactively configure the primary and backup root devices. Enable root guard.
MAC Spoofing	Attacking device spoofs the MAC address of a valid host currently in the CAM table. The switch then forwards frames destined for the valid host to the attacking device.	Use DHCP snooping, port security.
Address Resolution Protocol (ARP) Spoofing	Attacking device crafts ARP replies intended for valid hosts. The attacking device's MAC address then becomes the destination address found in the Layer 2 frames sent by the valid network device.	Use Dynamic ARP Inspection (DAI), DHCP snooping, port security.

Layer 2 Attack Categories (3)

Attack Method	Description	Steps to Mitigation
Switch Device Attacks		
Cisco Discovery Protocol (CDP) Manipulation	Information sent through CDP is transmitted in clear text and unauthenticated, allowing it to be captured and divulge network topology information.	Disable CDP on all ports where it is not intentionally used.
Secure Shell Protocol (SSH) and Telnet Attacks	Telnet packets can be read in clear text. SSH is an option but has security issues in version 1.	Use SSH version 2. Use Telnet with vty ACLs.

Understanding and Protecting against MAC Layer Attacks

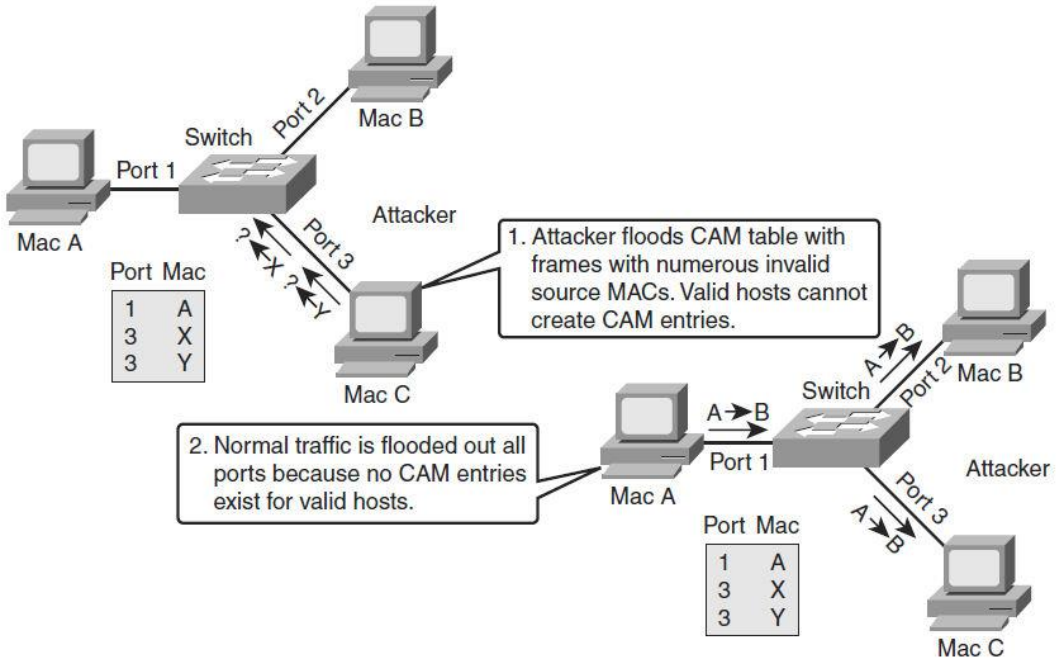
Understanding MAC Layer Attacks



Step 1. Switch forwards traffic based on valid MAC address table entries.

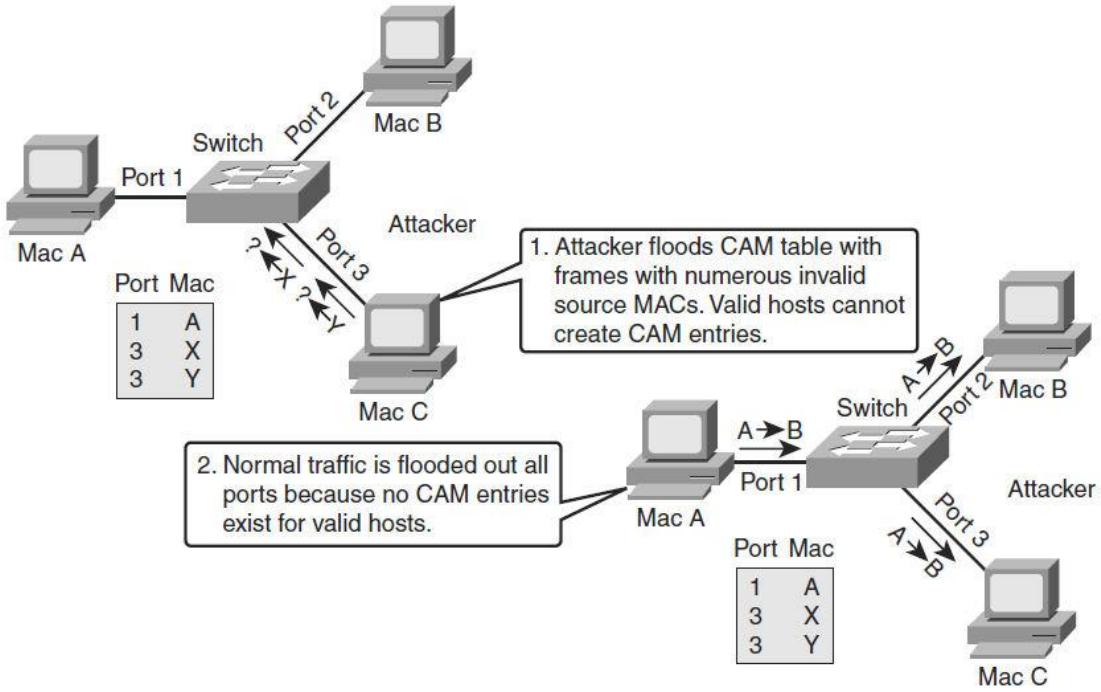
Step 2. Attacker (MAC address C) sends out multiple packets with various source MAC addresses.

Understanding MAC Layer Attacks



- **Step 3.** Over a short time period, the CAM table in the switch fills up until it cannot accept new entries. As long as the attack is running, the MAC address table on the switch remains full.
- **Step 4.** Switch begins to flood all packets that it receives out of every port so that frames sent from Host A to Host B are also flooded out of Port 3 on the switch.

Protecting against MAC Layer Attacks



- To prevent MAC Address flooding, port security can be used. Configure port security to define the number of MAC addresses allowed on a given port.
- Port security can also specify what MAC address is allowed on a given port.

Port Security

- Cisco-proprietary feature on Catalyst switches.
- Restricts switch port to specific set or number of MAC addresses, which can be learned dynamically or configured statically.
- “Sticky learning” combines dynamically learned and statically configured addresses.
- Dynamically learned addresses are converted to *sticky secure addresses*, as if they were configured using the **`switchport port-security mac-address sticky`** interface command.

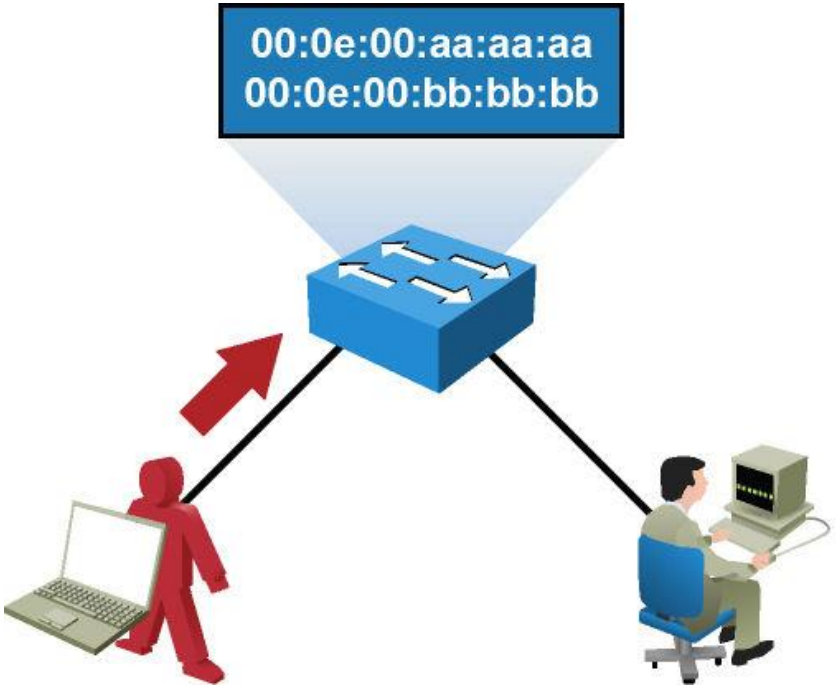
Port Security Scenario 1 (Slide 1)

- Imagine five individuals whose laptops are allowed to connect to a specific switch port when they visit an area of the building. You want to restrict switch port access to the MAC addresses of those five laptops and allow no addresses to be learned dynamically on that port.

Port Security Scenario 1 (Slide 2)

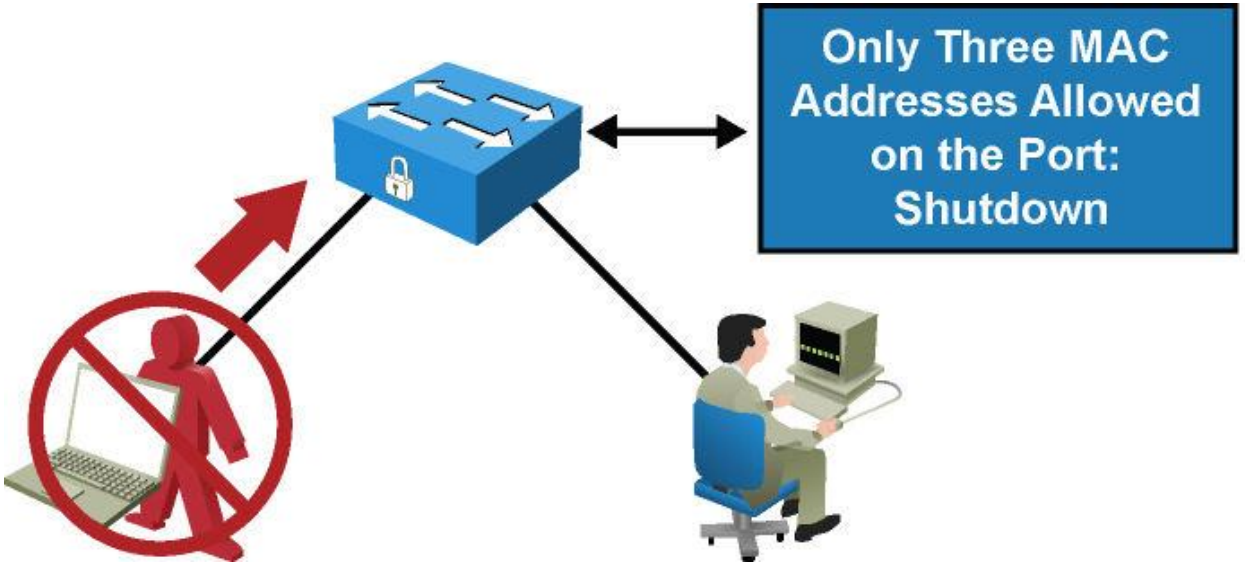
Step	Action	Notes
1	Configure port security.	Configure port security to allow only five connections on that port. Configure an entry for each of the five allowed MAC addresses. This, in effect, populates the MAC address table with five entries for that port and allows no additional entries to be learned dynamically.
2	Allowed frames are processed.	When frames arrive on the switch port, their source MAC address is checked against the MAC address table. If the frame source MAC address matches an entry in the table for that port, the frames are forwarded to the switch to be processed like any other frames on the switch.
3	New addresses are not allowed to create new MAC address table entries.	When frames with a non-allowed MAC address arrive on the port, the switch determines that the address is not in the current MAC address table and does not create a dynamic entry for that new MAC address because the number of allowed addresses has been limited.
4	Switch takes action in response to non-allowed frames.	The switch disallows access to the port and takes one of these configuration-dependent actions: (a) the entire switch port can be shut down; (b) access can be denied for that MAC address only and a log error can be generated; (c) access can be denied for that MAC address but without generating a log message.

Port Security Scenario 2 (Slide 1)



- An attacker enables a hacking tool on the attacker's rogue device to flood switch CAM tables with bogus MAC addresses, causing the MAC address table to fill up. When the MAC address table is full, it turns the switch into a hub and floods all unicast frames.

Port Security Scenario 2 (Slide 2)



- Port security is configured on untrusted user ports. Enabling port security limits MAC flooding attacks and locks down the port.
- Port security also sets an SNMP trap alerting of any violation. Port security allows the frames from already secured MAC address below the maximum number of MAC addresses enabled on that port, and any frame with a new MAC address over the limit is dropped.

Configuring Port Security

- Step 1. Enable port security:

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

- Step 2. Set a maximum number of MAC addresses that will be allowed on this port. The default is one:

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

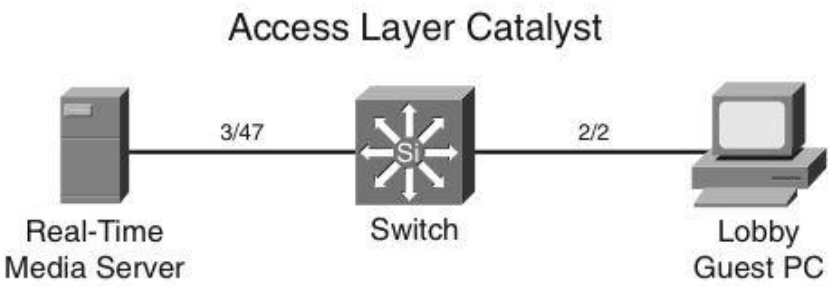
- Step 3. Specify which MAC addresses will be allowed on this port (optional):

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

- Step 4. Define what action an interface will take if a non-allowed MAC address attempts access:

```
Switch(config-if)#switchport port-security violation {shutdown | restrict | protect}
```

Port Security Example




```
4503(config)# interface FastEthernet 3/47
4503(config-if)# switchport
4503(config-if)# switchport mode access
4503(config-if)# switchport port-security
4503(config-if)# switchport port-security mac-address 0000.0000.0008
4503(config-if)# switchport port-security maximum 1
4503(config-if)# switchport port-security aging time 2
4503(config-if)# switchport port-security aging static
4503(config-if)# switchport port-security violation restrict
4503(config)# interface FastEthernet 2/2
4503(config-if)# switchport
4503(config-if)# switchport mode access
4503(config-if)# switchport port-security
4503(config-if)# switchport port-security mac-address 0000.0000.1118
4503(config-if)# switchport port-security maximum 1
4503(config-if)# switchport port-security aging time 2
4503(config-if)# switchport port-security aging static
4503(config-if)# switchport port-security violation shutdown
```

Verifying Port Security (1)

- The **`show port-security`** command can be used to verify the ports on which port security has been enabled. It also displays count information and security actions to be taken per interface.

```
switch# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)              (Count)     (Count)
-------------------------------------------------------------------------
  Fa0/1                   2           1           0            Restrict
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 6144
```

Verifying Port Security (2)

```
switch# show port-security interface fastethernet0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Restrict
Aging Time : 60 mins
Aging Type : Inactivity
SecureStatic Address Aging : Enabled
Maximum MAC Addresses : 2
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 001b.d513.2ad2:5
Security Violation Count : 0

switch# show port-security address
        Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address     Type            Ports   Remaining Age
                                                      (mins)
----    -----------     ----            -----   -------------
2       001b.d513.2ad2  SecureDynamic   Fa0/1   60 (I)
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 6144
```

Configuring Port Security with Sticky MAC Addresses

```
switch# show running-config fastethernet 0/1
interface FastEthernet0/1
switchport access vlan 2
switchport mode access
switchport port-security maximum 2
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky 001b.d513.2ad2

switch# show port-security address
Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address            Type            Ports   Remaining Age
                                                            (mins)
----    -----------             ----           -----   -------------
2       001b.d513.2ad2        SecureSticky     Fa0/1           -
```

Blocking Unicast Flooding

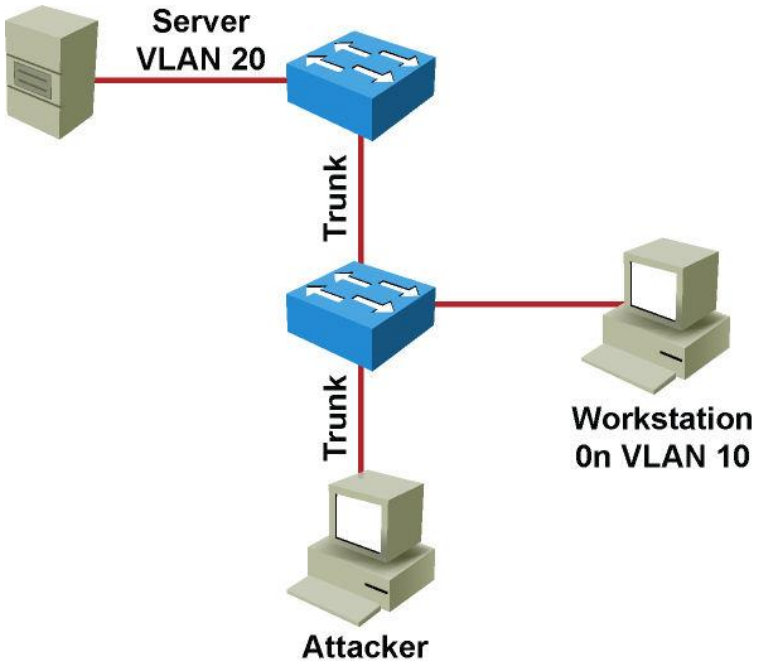
- Cisco Catalyst switches can restrict flooding of unknown multicast MAC-addressed traffic on a per-port basis, in addition to restricting flooding of unknown unicast destination MAC addresses.

```
4503# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
4503(config)# interface FastEthernet 3/22
4503(config-if)# switchport block unicast
4503(config-if)# switchport block multicast
```

Understanding and Protecting against VLAN Attacks

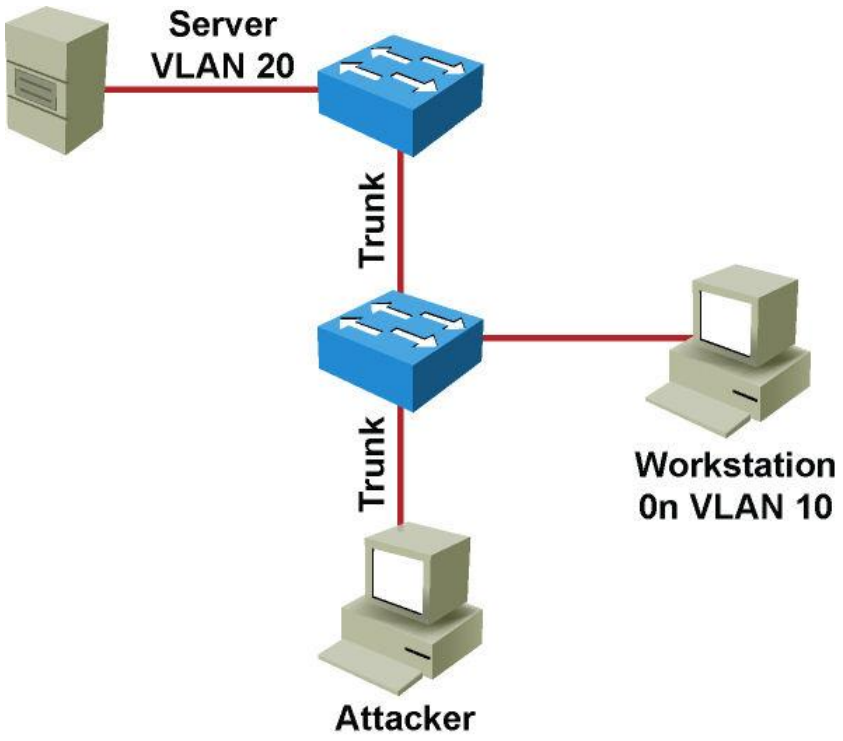
VLAN Hopping

- Switch Spoofing
- Double Tagging

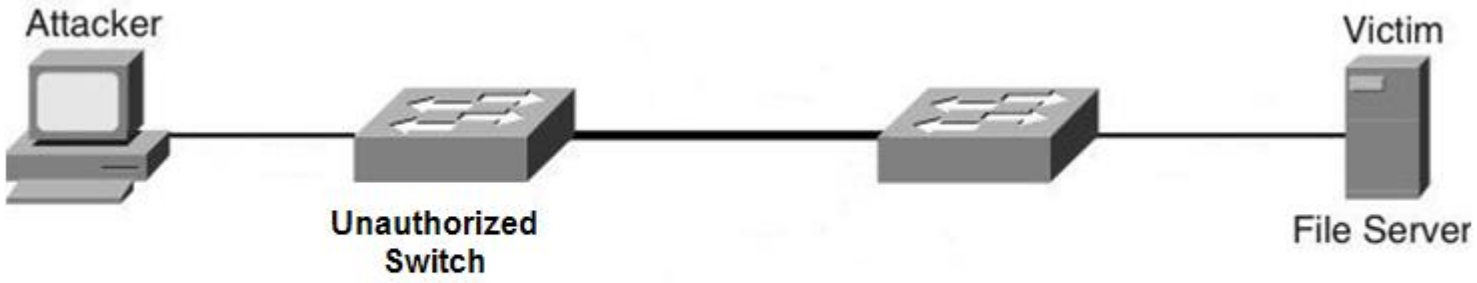


VLAN Hopping – Switch Spoofing (1)

- An attacker can send a malicious DTP frame. Upon receiving the frame, the switch would form a trunk port, which would then give the attacker access to all the VLANs on the trunk. The attacker port becomes a trunk port, and the attacker can attack a victim in any VLAN carried on the trunk.

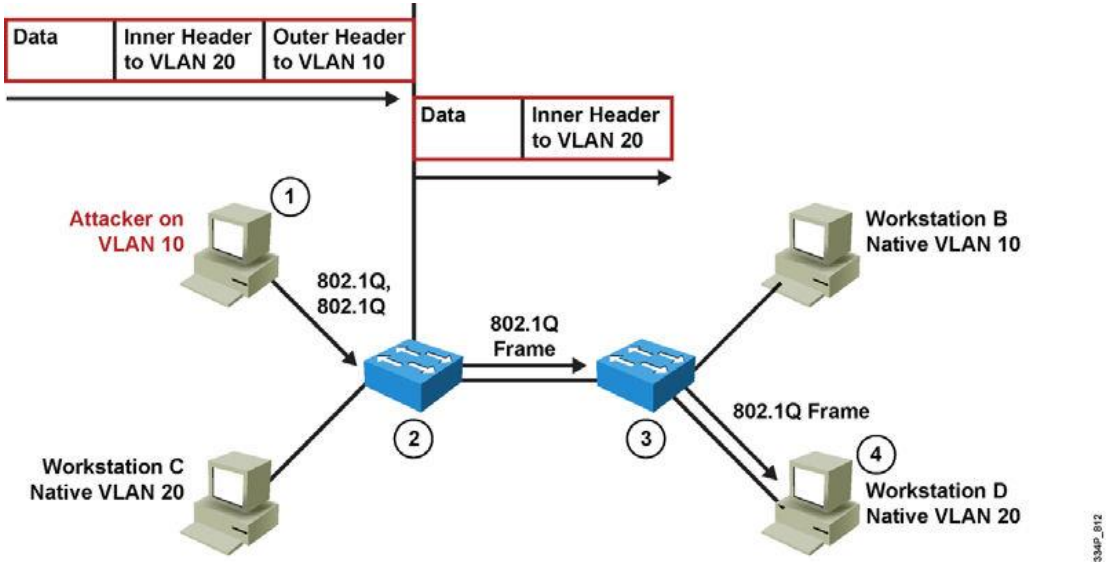


VLAN Hopping – Switch Spoofing (2)



- In another type of switch spoofing attack, the network attacker connects an unauthorized Cisco switch to the switch port. The unauthorized switch can send DTP frames and form a trunk. The attacker has access to all the VLANs through the trunk. The attacker can attack a victim in any VLAN.

VLAN Hopping – Double Tagging



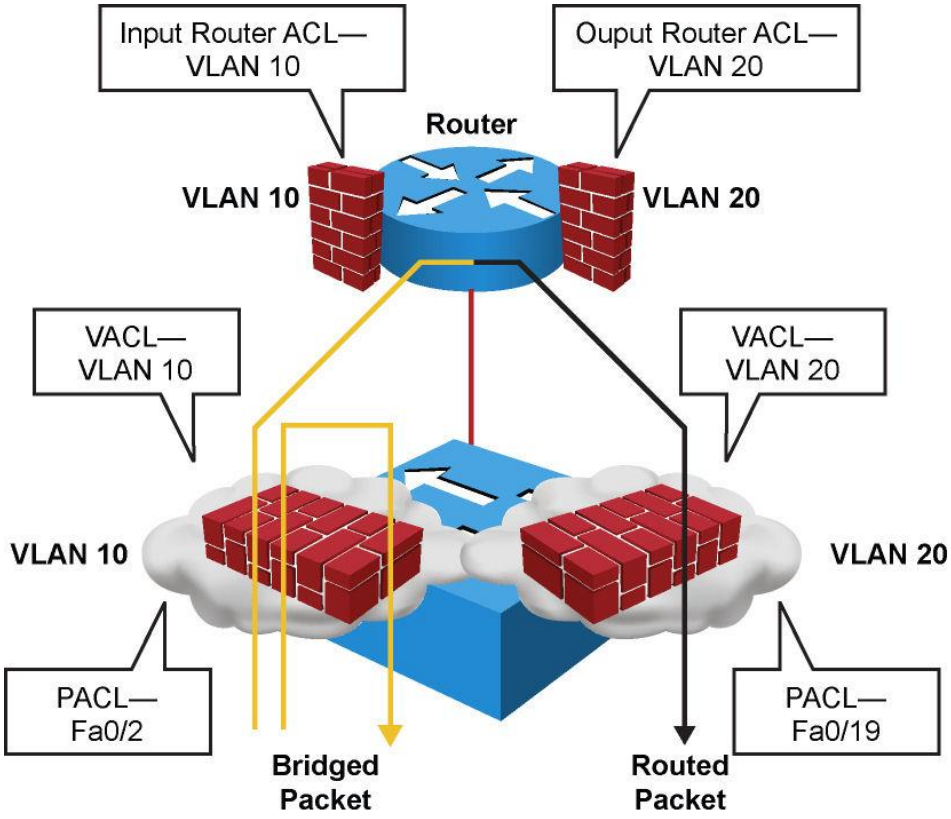
- **Step 1.** Attacker (native VLAN 10) sends a frame with two 802.1Q headers to Switch 1.
- **Step 2.** Switch 1 strips the outer tag and forwards the frame to all ports within same native VLAN.
- **Step 3.** Switch 2 interprets frame according to information in the inner tag marked with VLAN ID 20.
- **Step 4.** Switch 2 forwards the frame out all ports associated with VLAN 20, including trunk ports.

Mitigating VLAN Hopping Attacks

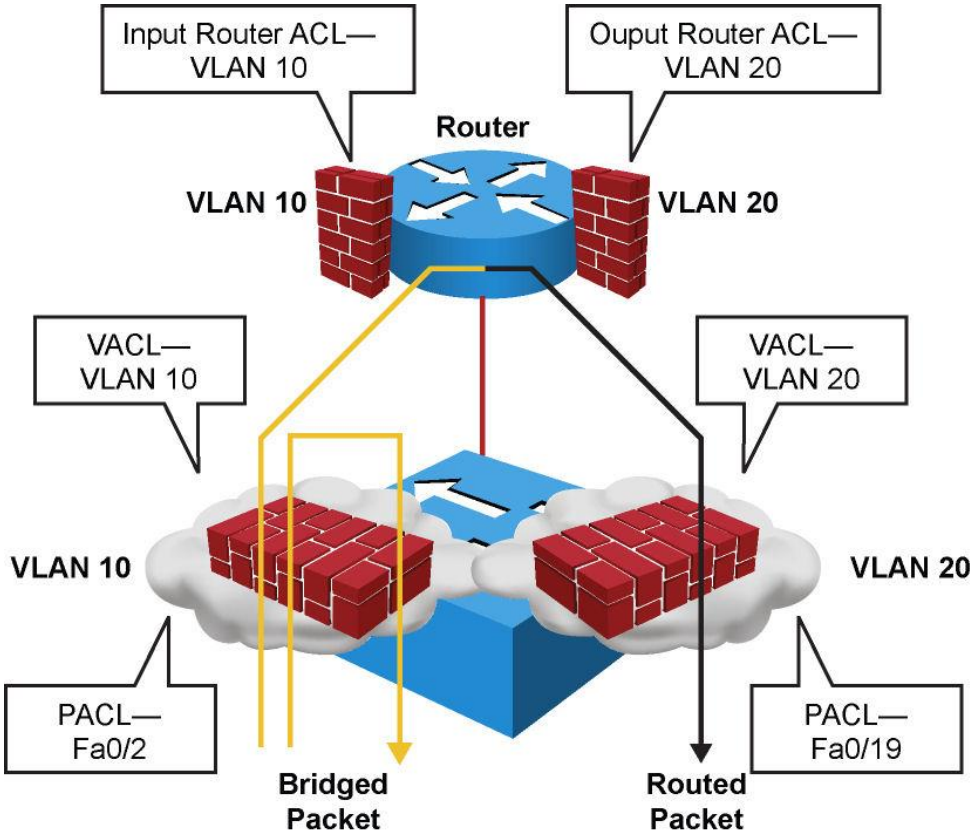
- Configure all unused ports as access ports so that trunking cannot be negotiated across those links.
- Place all unused ports in the shutdown state and associate them with a VLAN designed for only unused ports, carrying no user data traffic.
- When establishing a trunk link, purposefully configure arguments to achieve the following results:
  - The native VLAN is different from any data VLANs.
  - Trunking is set up as On or Nonegotiate rather than negotiated.
  - The specific VLAN range is carried on the trunk. This ensures that the native VLAN will be pruned along with any other VLANs not explicitly allowed on the trunk.

Catalyst Multilayer Switch ACL Types

- **Router access control lists (RACL):** Supported in the TCAM hardware on Cisco multilayer switches. In Catalyst switches, RACL can be applied to any routed interface, such as an SVI or routed port.
- **Port access control list (PACL):** Filters traffic at the port level. PACL's can be applied on a Layer 2 switch port, trunk port, or EtherChannel port. PACL's act at the Layer 2 port level but can filter based on Layer 3/Layer 4 information.



Catalyst Multilayer Switch ACL Types

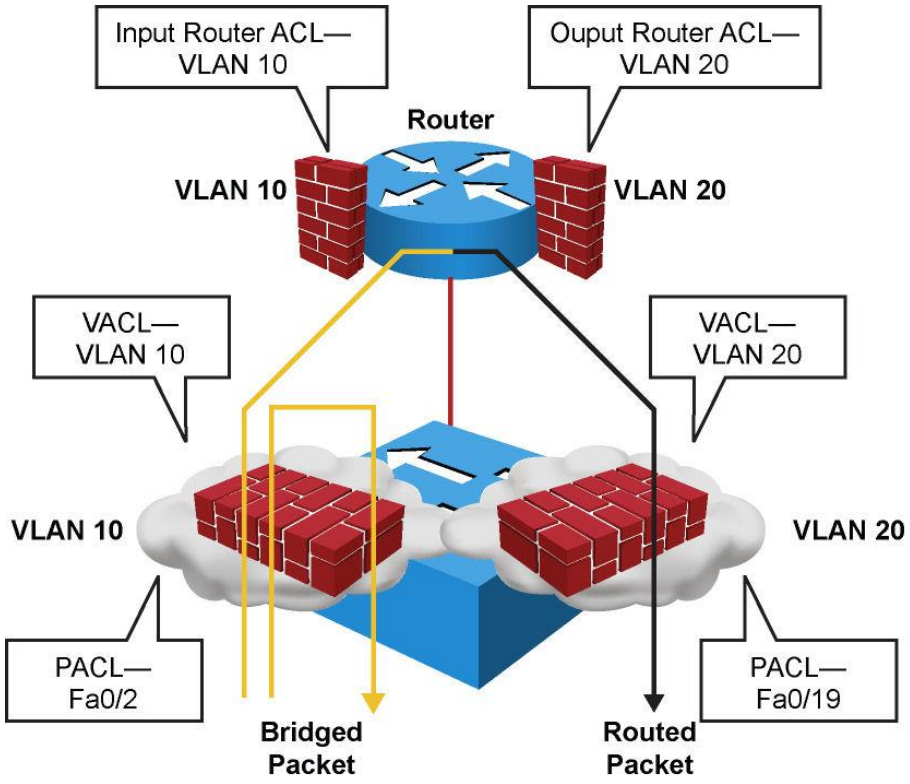


- **VACL's:** Also known as VLAN access-maps, apply to all traffic in a VLAN. VACL's support filtering based on Ethertype and MAC addresses. VACL's are order-sensitive, analogous to route maps. VACL's can control traffic flowing within the VLAN or control switched traffic, whereas RACL's control only routed traffic.

Configuring VACL's (1)

Three ACL actions are permitted with VACL's:

- **Permit** (with capture, Catalyst 6500 only)
- **Redirect** (Catalyst 6500 only)
- **Deny** (with logging, Catalyst 6500 only)



Configuring VACL's (2)

- Step 1. Define a VLAN access map:

```
Switch(config)# vlan access-map map_name [seq#]
```

- Step 2. Configure a match clause:

```
Switch(config-access-map)# match {drop [log]} | {forward
[capture]} | {redirect {{fastethernet | gigabitethernet |
tengigabitethernet} slot/port} | {port-channel channel_id}}
```

- Step 3. Configure an action clause:

```
Switch(config-access-map)# action {drop [log]} | {forward
[capture]} | {redirect {{fastethernet | gigabitethernet |
tengigabitethernet} slot/port} | {port-channel channel_id}}
```

- Step 4. Apply a map to VLANs:

```
Switch(config)# vlan filter map_name vlan_list list
```

- Step 5. Verify the VACL configuration:

```
Switch# show vlan access-map map_name
```

```
Switch# show vlan filter [ access-map map_name | vlan vlan_id
]
```

Configuring VACL's (3)

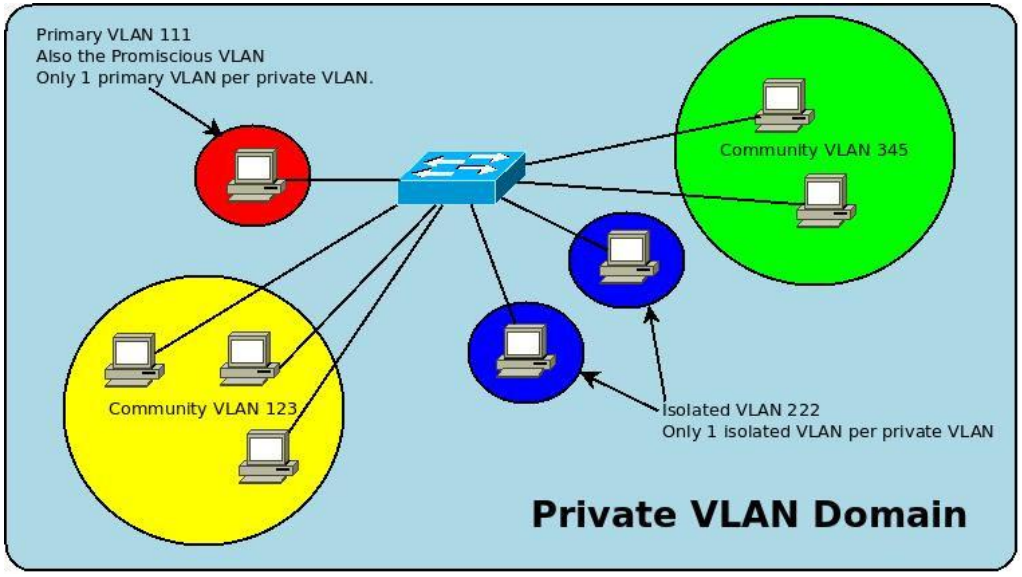
- Here a VACL is configured to drop all traffic from network 10.1.9.0/24 on VLAN 10 and 20 and drop all traffic to Backup Server 0000.1111.4444.

```
switch(config)# access-list 100 permit ip 10.1.9.0 0.0.0.255 any
switch(config)# mac access-list extended BACKUP_SERVER
switch(config-ext-mac)# permit any host 0000.1111.4444
switch(config)# vlan access-map XYZ 10
switch(config-map)# match ip address 100
switch(config-map)# action drop
switch(config-map)# vlan access-map XYZ 20
switch(config-map)# match mac address BACKUP_SERVER
switch(config-map)# action drop
switch(config-map)# vlan access-map XYZ 30
switch(config-map)# action forward
switch(config)# vlan filter XYZ vlan-list 10,20
```

Private VLANs

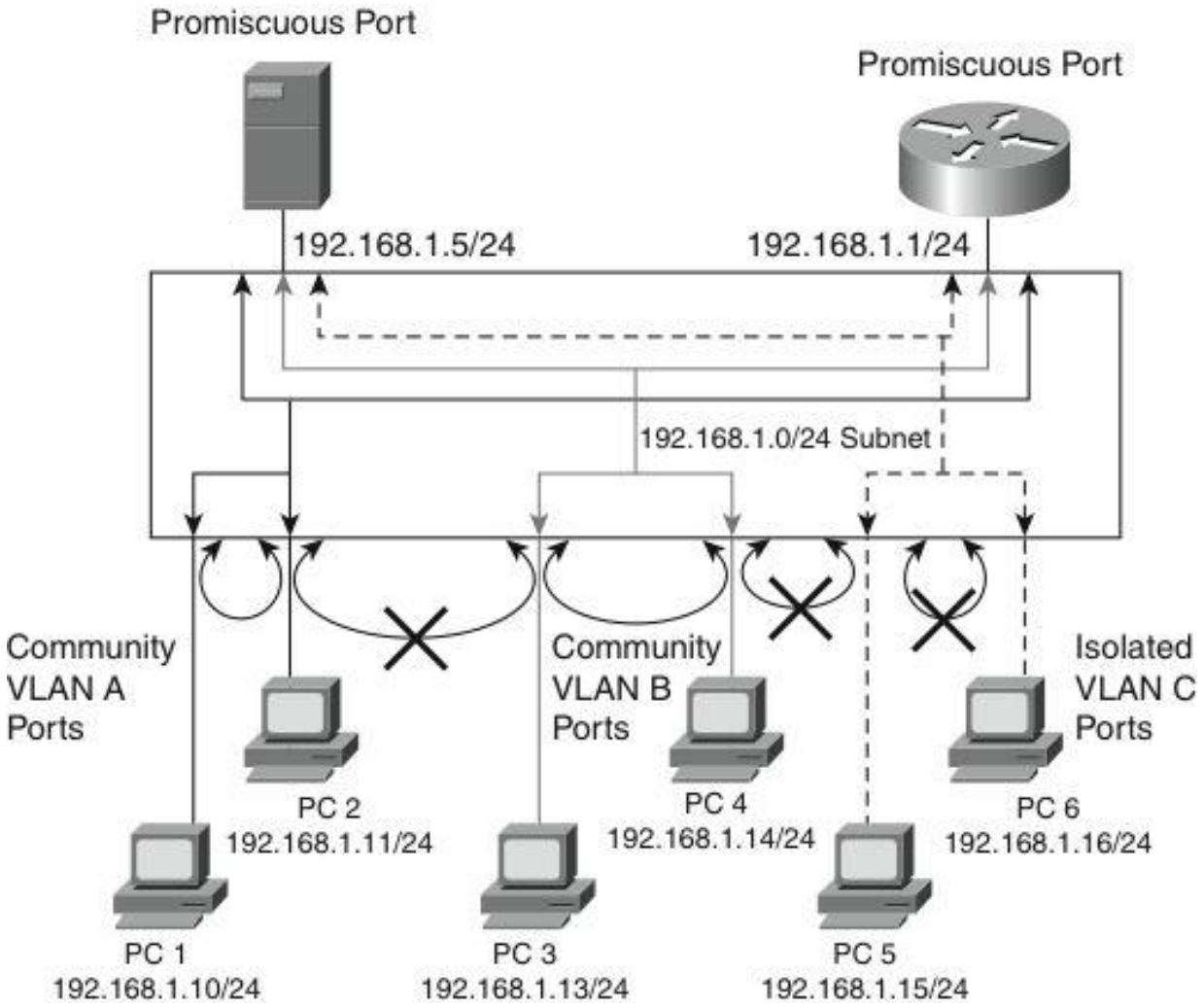
Motivation for Private VLANs

- Service providers often have devices from multiple clients, in addition to their own servers, in a single Demilitarized Zone (DMZ) segment or VLAN. As security issues abound, it becomes more important to provide traffic isolation between devices, even though they might exist on the same Layer 3 segment and VLAN.
- Most Cisco IOS-based switches implement private VLANs to keep some switch ports shared and some switch ports isolated, even though all ports remain in the same VLAN.



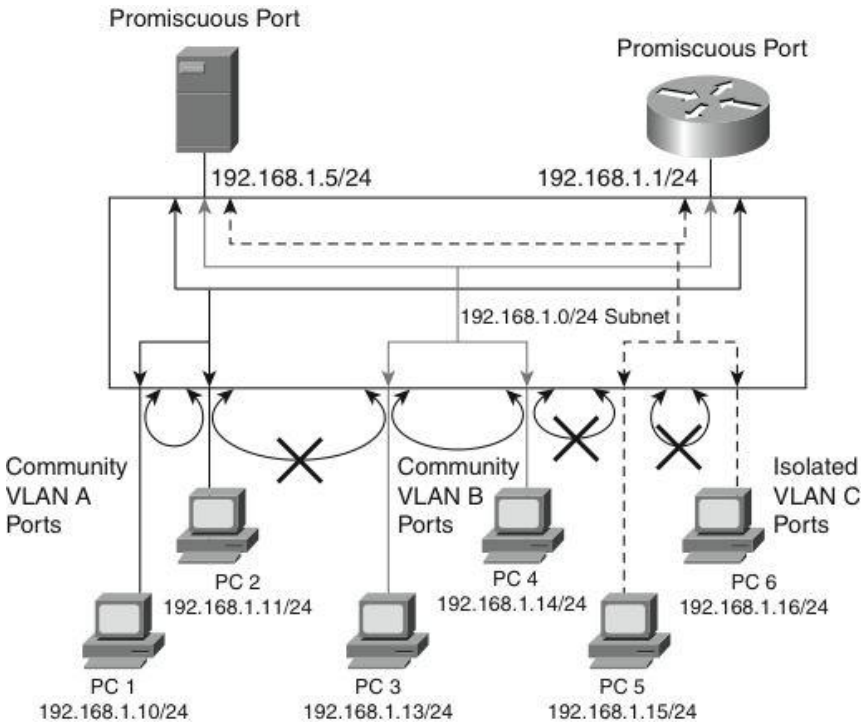
pVLAN Port Types

- Isolated
- Promiscuous
- Community



pVLAN Structure Supporting VLANs

- Primary Private VLAN
- Secondary Private VLAN
- Community Private VLAN
- Isolated Private VLAN



Configuring pVLANs - Steps

- **Step 1.** Set VTP mode to transparent.
- **Step 2.** Create the secondary pVLANs.
- **Step 3.** Create the primary pVLAN.
- **Step 4.** Associate the secondary pVLAN with the primary pVLAN.
  - Only one isolated pVLAN can be mapped to a primary pVLAN, but more than one community pVLAN can be mapped to a primary pVLAN.
- **Step 5.** Configure an interface as an isolated or community port.
- **Step 6.** Associate the isolated port or community port with the primary-secondary pVLAN pair.
- **Step 7.** Configure an interface as a promiscuous port.
- **Step 8.** Map the promiscuous port to the primary-secondary pVLAN pair.

Configuring pVLANs - Commands

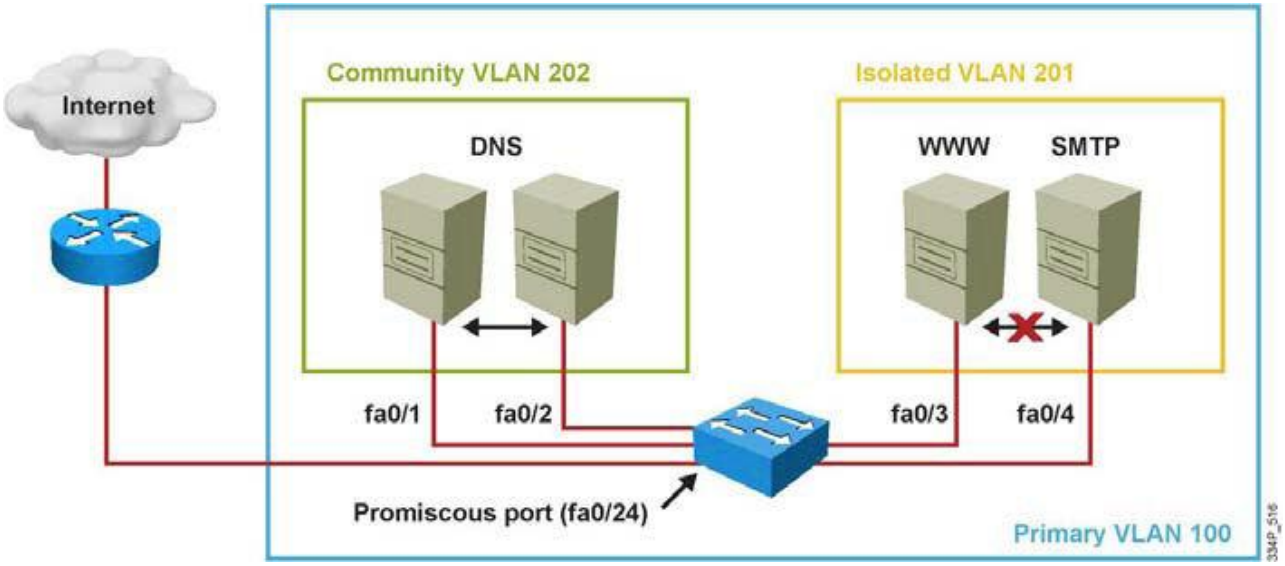
```
Switch(config)# vlan pvlan-id
Switch(config-vlan)# private-vlan {community | isolated | primary}
Switch(config-vlan)# exit
Switch(config)# vlan primary-vlan-id
Switch(config-vlan)# private-vlan association {secondary-vlan-list | add
secondary-vlan-list | remove secondary-vlan-list}
Switch(config-vlan)# interface vlan primary-vlan-id
Switch(config-if)# private-vlan mapping {secondary-vlan-list | add
secondary-vlan-list | remove secondary-vlan-list}
Switch(config-if)# interface type slot/port
Switch(config-if)# switchport
Switch(config-if)# switchport mode private-vlan {host | promiscuous}
Switch(config-if)# switchport private-vlan host-association primary-vlan-
id secondary-vlan-id
Switch(config-if)# switchport private-vlan mapping primary-vlan-id
{secondary-vlan-list | add secondary-vlan-list | remove secondary-vlan-
list}
```

Verifying pVLAN Configuration

- The two most useful commands for this purpose are **`show interface switchport`** and **`show vlan private-vlan`**.

```
Switch# show vlan private-vlan
Primary  Secondary         Type                  Interfaces
-------  ---------         --------------    -----------------
100      200       community
100      300       isolated

Switch# show interfaces FastEthernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: 100 (VLAN0200) 300 (VLAN0300)
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

pVLAN Scenario 1: Single Switch

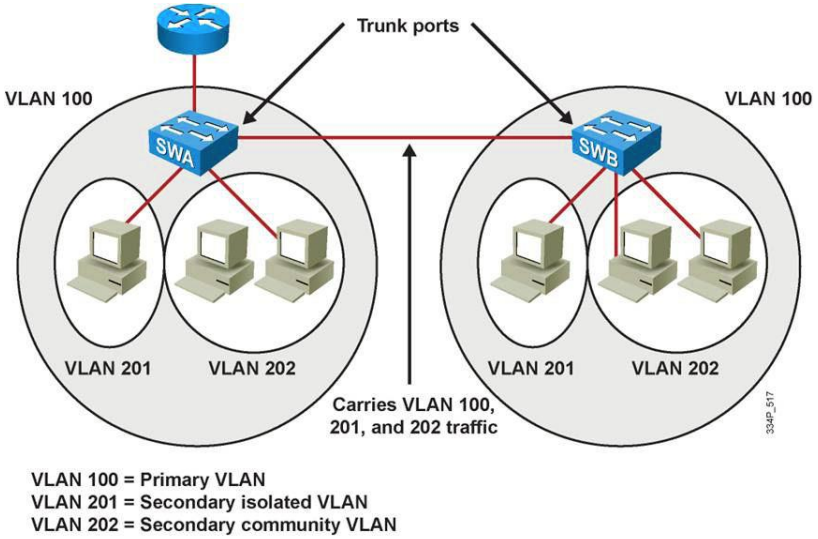


- A corporate DMZ contains two DNS servers, one web server and one SMTP server. All servers and their connecting router are in the same subnet.
- DNS servers are redundant copies, so they need to communicate with each other to update their entries and to the Internet. In addition to that, they also need to communicate with the Internet.
- The Web Server and the SMTP server need to communicate with the Internet, but for security purposes, the SMTP server should not be reachable from the Web or the DNS servers. The web server needs to be accessible from the Internet but not from the SMTP server.

pVLAN Configuration for Scenario 1

```
Switch(config)# vtp transparent
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# vlan 100
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 201,202
Switch(config-vlan)# interface fastethernet 0/24
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 100 201,202
Switch(config-if)# interface range fastethernet 0/1 - 2
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 202
Switch(config-if)# interface range fastethernet 0/3 - 4
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 201
```

pVLAN Scenario 2: Multiple Switches



- A trunk port carries the primary VLAN and secondary VLANs to a neighboring switch just like any other VLAN.
- A feature of pVLANs across multiple switches is that traffic from an isolated port in one switch does not reach an isolated port on another switch.
- Configure pVLANs on all switches on the path, which includes devices that have no pVLAN ports to maintain the security of your pVLAN configuration, and avoid using other VLANs configured as pVLANs.
- As shown in the figure, the switches SWA and SWB have the same pVLANs on two different switches and are connected through the trunk link.

pVLAN Configuration for Scenario 2

- To configure a Layer 2 interface as a Private VLAN trunk port, use the interface command:

  `Switch(config-if)# switchport private-vlan association trunk primary_vlan_ID secondary_vlan_ID`

- If the port is set to promiscuous, use the **mapping** command:

  `Switch(config-if)# switchport private-vlan mapping primary_vlan_ID secondary_vlan_list`

- Once the trunk is configured, allow VLANs with the command

  `Switch(config-if)# switchport private-vlan trunk allowed vlan vlan_list`

- Configure the native VLAN with following command

  `Switch(config-if)# switchport private-vlan trunk native vlan vlan_id`

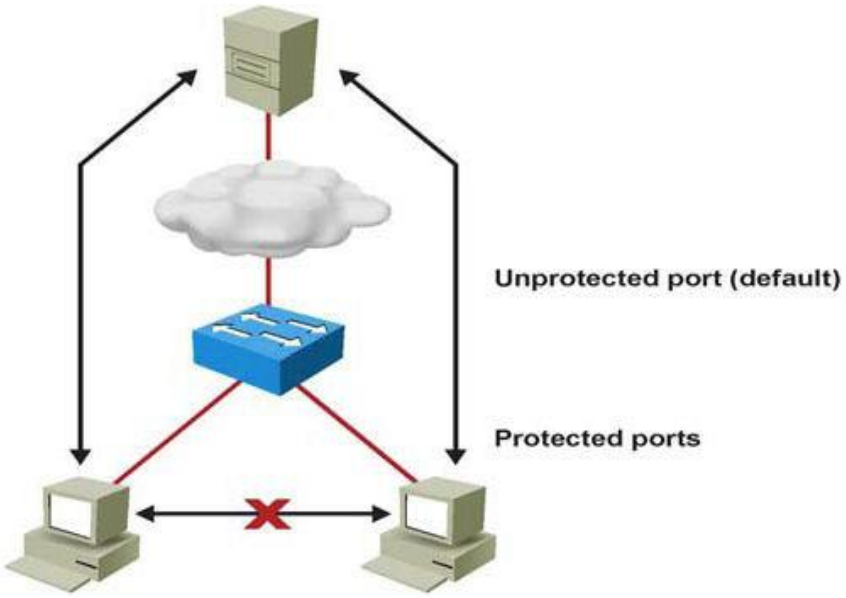
```
Switch(config)# interface fastethernet 5/2
Switch(config-if)# switchport mode private-vlan trunk secondary
Switch(config-if)# switchport private-vlan trunk native vlan 10
Switch(config-if)# switchport private-vlan trunk allowed vlan 10, 3,301-302
Switch(config-if)# switchport private-vlan association trunk 3 301
Switch(config-if)# switchport private-vlan association trunk 3 302
```

pVLAN Verification for Scenario 2

```
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk secondary
Operational Mode: private-vlan trunk secondary
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations:
3 (VLAN0003) 301 (VLAN0301)
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Operational Normal VLANs: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

pVLAN Edge (Protected Port) Feature

- The PVLAN edge (protected port) feature has only local significance to the switch (unlike pVLANs), and there is no isolation provided between two protected ports located on different switches.
- A protected port does not forward any traffic to any other port that is also a protected port on the same switch.
- Traffic cannot be forwarded between protected ports at L2, all traffic passing between protected ports must be forwarded through an L3 device.

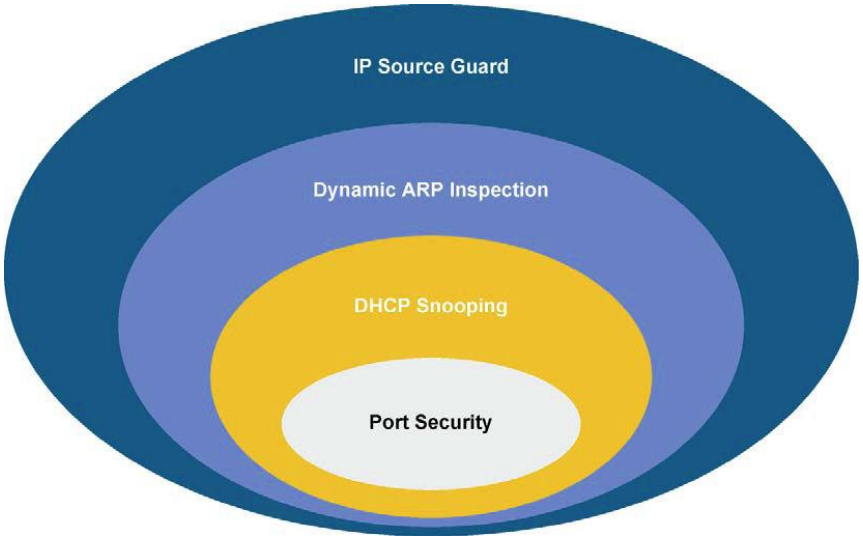



```
Switch(config-if)# switchport protected
```

Understanding and Protecting against Spoofing Attacks

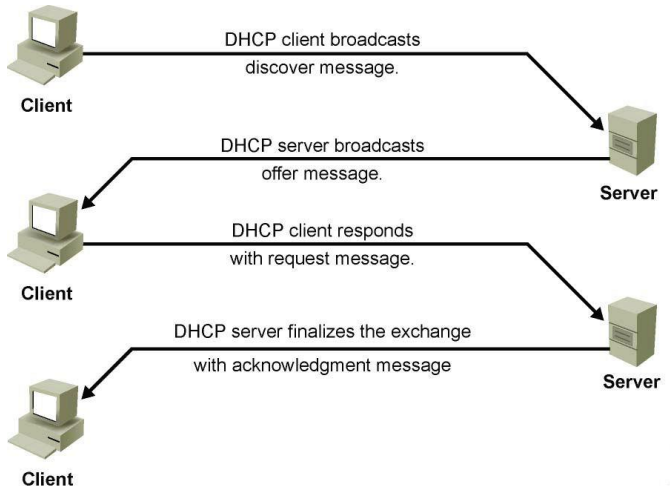
Catalyst Integrated Security Features

- Dynamic Address Resolution Protocol inspection (DAI) adds security to ARP using the DHCP snooping table to minimize the impact of ARP poisoning and spoofing attacks.
- IP Source Guard (IPSG) prevents IP spoofing addresses using the DHCP snooping table.
- Port security prevents MAC flooding attacks.
- DHCP snooping prevents client attacks on the DHCP server and switch.



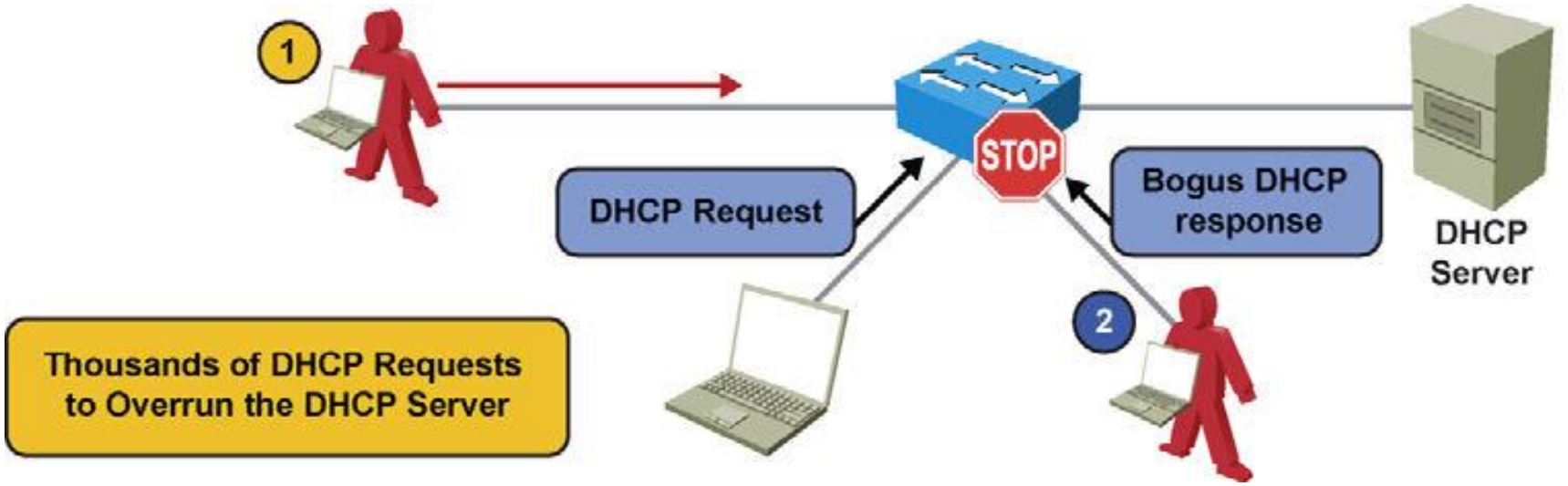
DHCP Spoofing Attack

- One of the ways that an attacker can gain access to network traffic is to spoof responses that would be sent by a valid DHCP server.
- The DHCP spoofing device replies to client DHCP requests. The legitimate server can reply also, but if the spoofing device is on the same segment as the client, its reply to the client might arrive first.
- The intruder's DHCP reply offers an IP address and supporting information that designates the intruder as the default gateway or DNS server.



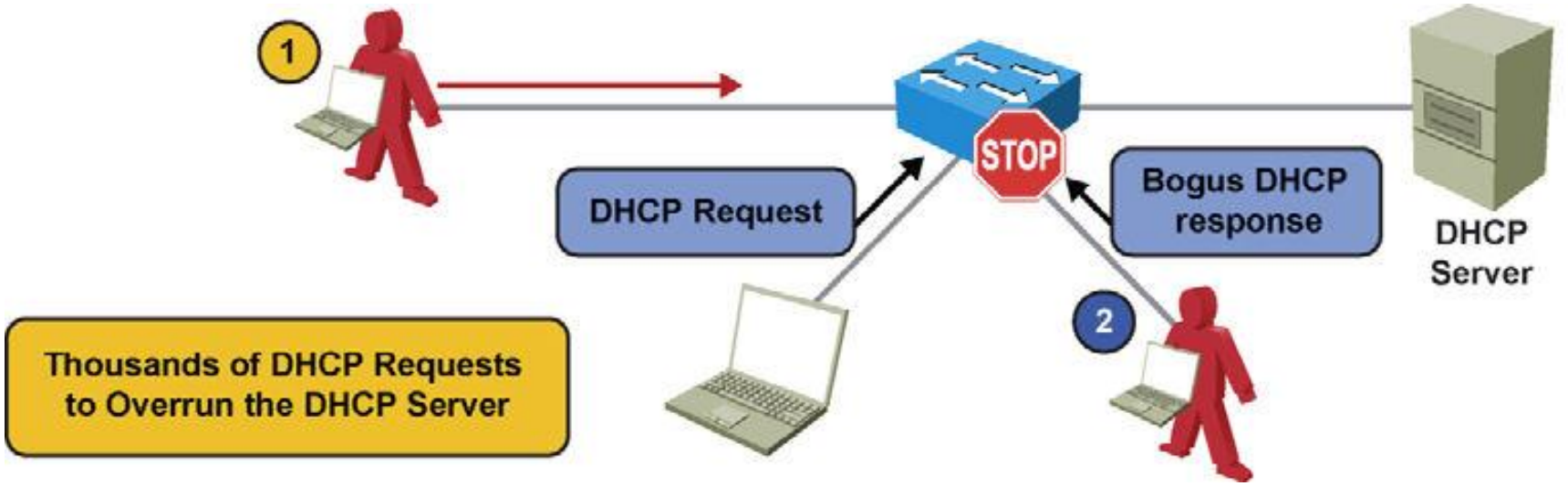
- For a gateway, the clients then forward packets to the attacking device, which in turn sends them to the desired destination. This is referred to as a man-in-the-middle attack and it can go entirely undetected as the intruder intercepts the data flow through the network.

DHCP Spoofing Attack – Scenario 1



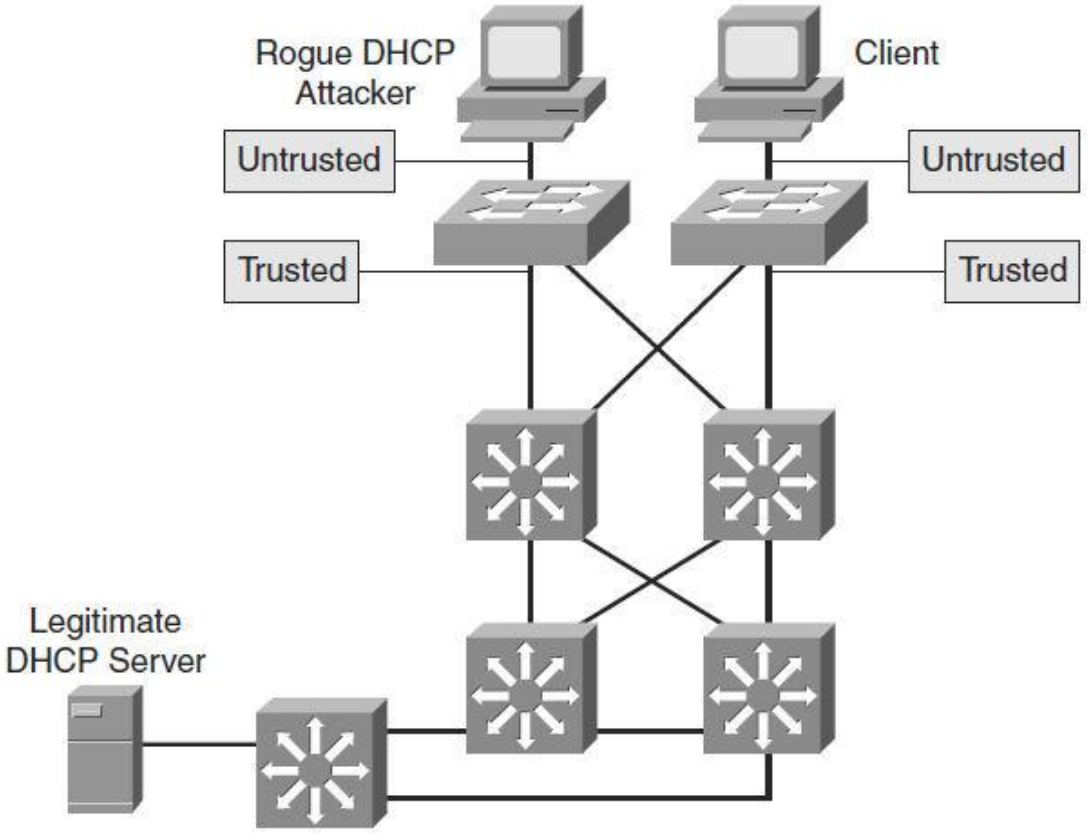
- In the first scenario, an attacker launches a DoS attack by sending thousands of DHCP requests. The DHCP server does not have the capability to determine whether the request is genuine and therefore might end up exhausting all the available IP addresses. This results in a legitimate client not getting a IP address via DHCP.

DHCP Spoofing Attack – Scenario 2



- A second scenario happens when the attacker attaches a DHCP server to the network and has it assume the role of the DHCP server for that segment. This enables the intruder to give out false DHCP information for the default gateway and domain name servers, which points clients to the hacker's machine. This misdirection enables the hacker to. become a man-in-the-middle and to gain access to confidential information, such as username and password pairs, while the end user is unaware of the attack.

DHCP Snooping

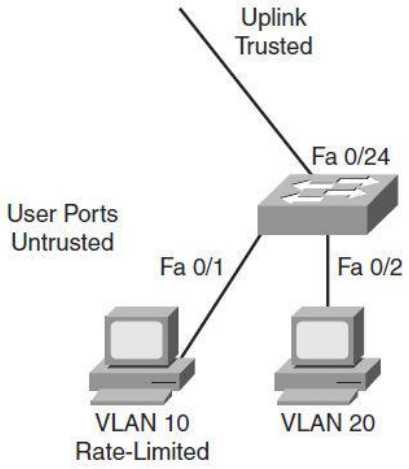


- DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests. Ports are identified as trusted and untrusted.

Configuring DHCP Snooping

Step	Commands
1.	Enable DHCP snooping globally: `Switch(config)# ip dhcp snooping`
2.	Enable DHCP Option 82: `Switch(config)# ip dhcp snooping information option`
3.	Configure DHCP server interfaces or uplink ports as trusted: `Switch(config-if)# ip dhcp snooping trust`
4.	Configure the number of DHCP packets per second (pps) that are acceptable on the port: `Switch(config-if)# ip dhcp snooping limit rate rate`
5.	Enable DHCP snooping on specific VLANs: `Switch(config)# ip dhcp snooping vlan number [number]`
6.	Verify the configuration: `Switch# show ip dhcp snooping`

DHCP Snooping Configuration Example

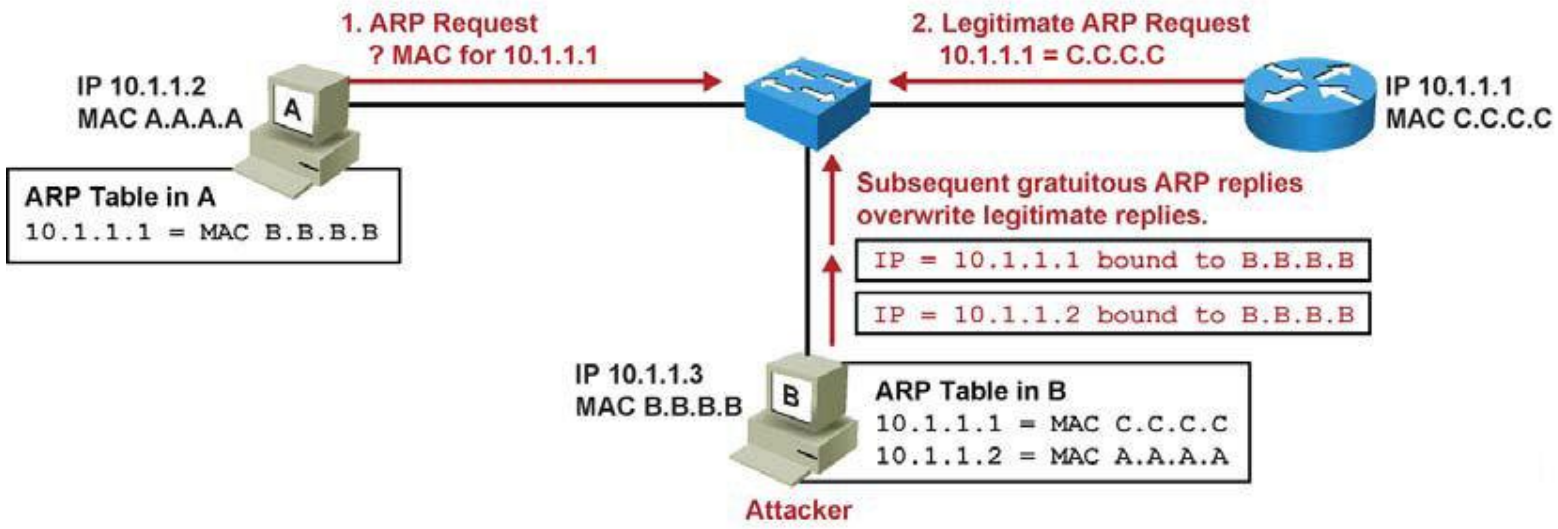



```
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping information option
switch(config)# ip dhcp snooping vlan 10,20
switch(config)# interface fastethernet 0/1
switch(config-if)# description Access Port
switch(config-if)# ip dhcp limit rate 5
switch(config)# interface fastethernet 0/24
switch(config-if)# description Uplink
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 10,20
switch(config-if)# ip dhcp snooping trust
```

Verifying the DHCP Snooping Configuration

```
switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20
DHCP snooping is operational on following VLANs:
10,20
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
circuit-id default format: vlan-mod-port
remote-id: 001a.e372.ab00 (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    no       no               5
FastEthernet0/24   yes      yes              unlimited
```

ARP Spoofing Attack



Step 1. Host A sends an ARP request for C's MAC address.

Step 2. Router C replies with its MAC and IP addresses. C also updates its ARP cache.

Step 3. Host A binds C's MAC address to its IP address in its ARP cache.

Step 4. Host B (attacker) sends ARP binding B's MAC address to C's IP address.

Step 5. Host A updates ARP cache with B's MAC address bound to C's IP address.

Step 6. Host B sends ARP binding B's MAC address to A's IP address.

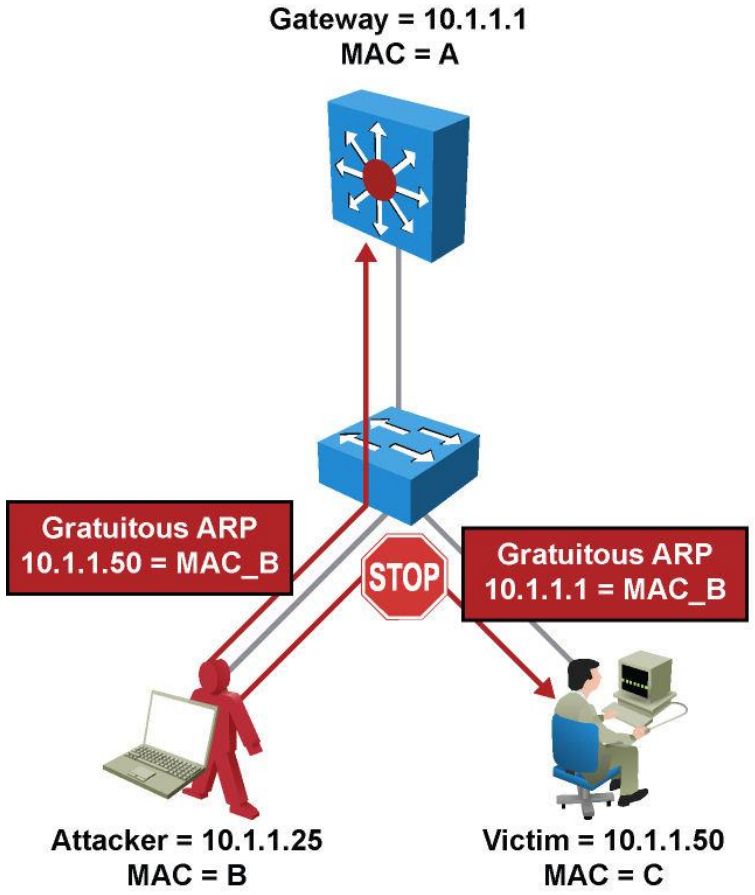
Step 7. Router C updates ARP cache with B's MAC address bound to A's IP address.

Step 8. Packets are diverted through attacker (B).

Preventing ARP Spoofing through Dynamic ARP Inspection (DAI)

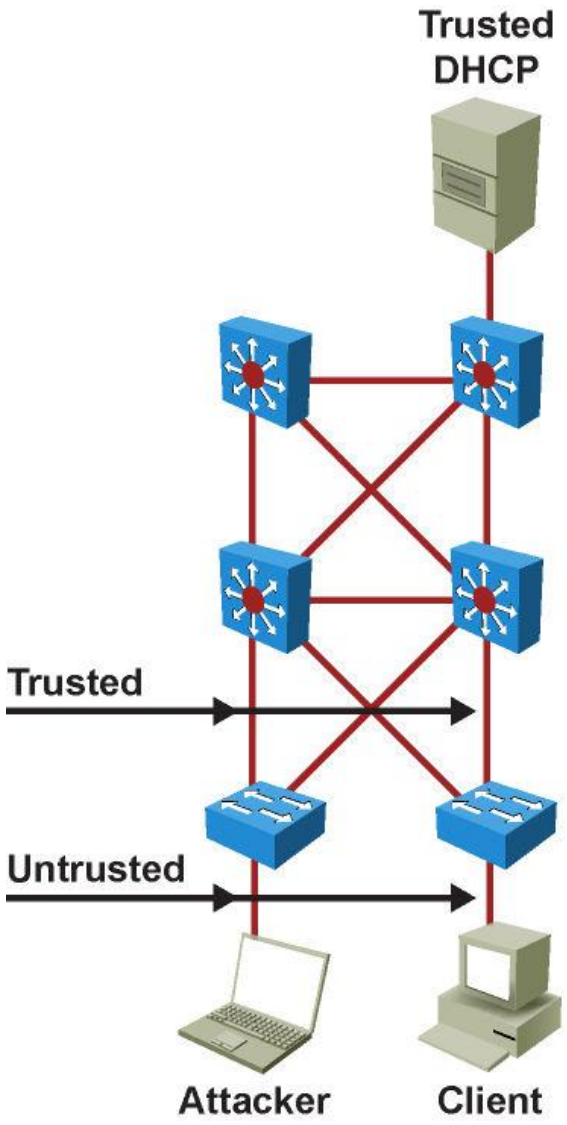
DAI takes these actions:

- Forwards ARP packets received on a trusted interface without any checks.
- Intercepts all ARP packets on untrusted ports.
- Verifies that each intercepted packet has a valid IP-to-MAC address binding before forwarding packets that can update the local ARP cache.
- Drops and logs ARP packets with invalid IP-to-MAC address bindings.



DAI Recommended Configuration

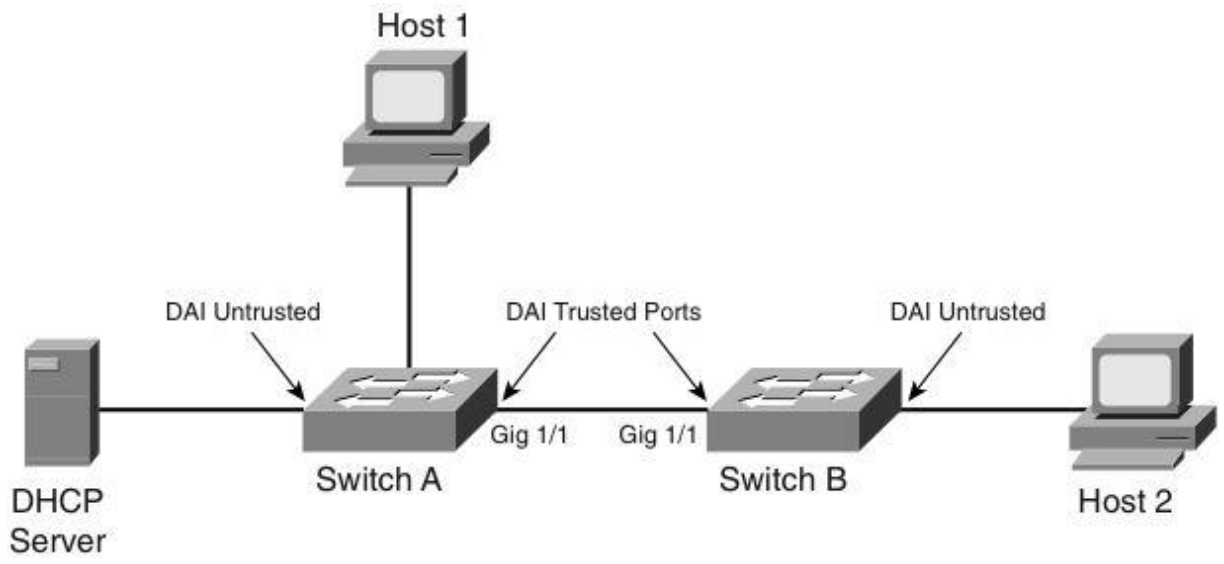
- DAI can also be used to rate limit the ARP packets and then errdisable the interface if the rate is exceeded.
- The figure here shows the recommended DAI configuration.



DAI Commands

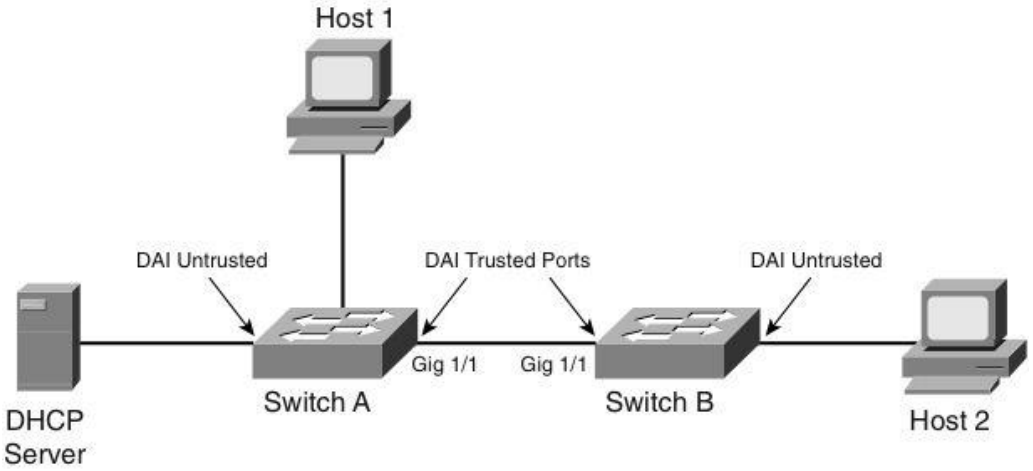
Command	Description
`Switch(config)# ip arp inspection vlan vlan_id [vlan_id]`	Enables DAI on a VLAN or range of VLAN's.
`Switch(config-if)# ip arp inspection trust`	Enables DAI on an interface and sets the interface as a trusted interface.
`Switch(config)# ip arp inspection validate {[src-mac] [dst-mac] [ip]}`	Configures DAI to drop ARP packets when the IP addresses are invalid, or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header.

DAI Scenario with Catalyst Switches (1)



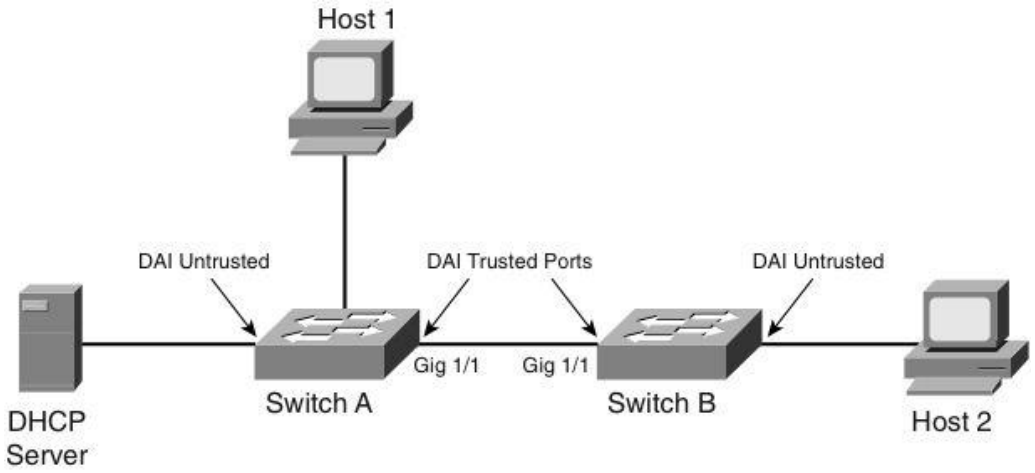
- Host 1 is connected to Switch A and Host 2 is connected to Switch B, both in VLAN 10.
- The DHCP server is connected to Switch A. DHCP snooping is enabled on both Switch A and Switch B as a prerequisite for DAI.
- The inter-switch links are configured as DAI trusted ports, and the user ports are left in the default untrusted state.

DAI Scenario with Catalyst Switches (2)



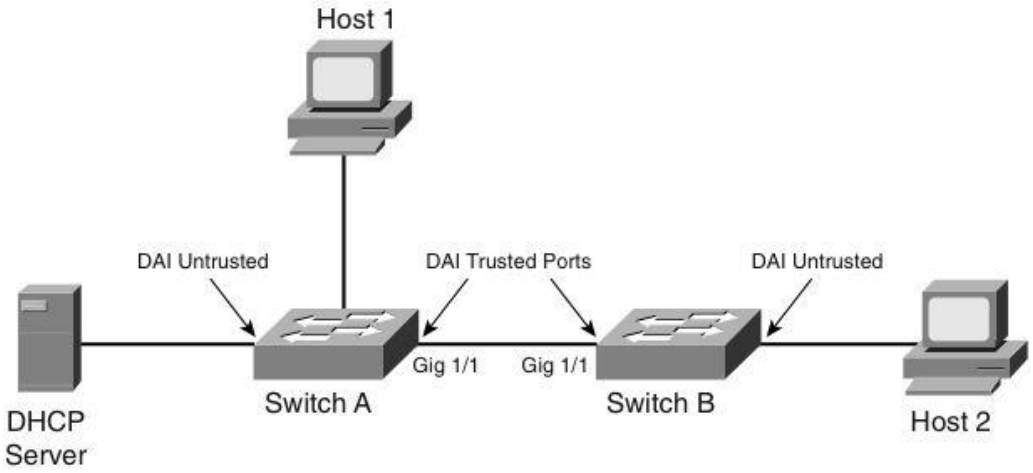

```
SwitchA# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)# ip arp inspection vlan 10
SwitchA(config)# interface gigabitEthernet 1/1
SwitchA(config-if)# ip arp inspection trust
SwitchA(config-if)# end

SwitchB# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchB(config)# ip arp inspection vlan 10
SwitchB(config)# interface gigabitEthernet 1/1
SwitchB(config-if)# ip arp inspection trust
SwitchB(config-if)# end
```

DAI Scenario with Catalyst Switches (3)



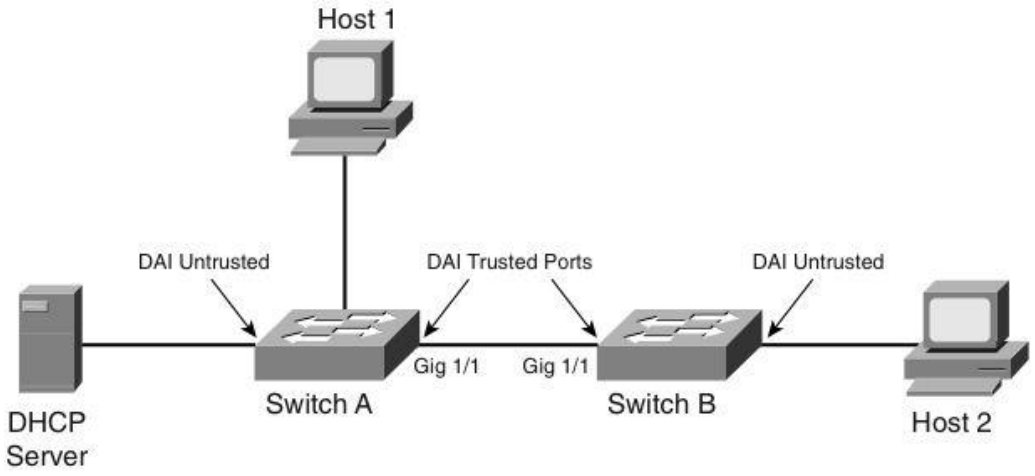

```
SwitchA# show ip arp inspection interfaces
Interface              Trust State  Rate (pps)    Burst Interval
---------------        -----------  ----------    --------------
Gi1/1                  Trusted      None          N/A
Gi1/2                  Untrusted    15            1
Fa2/1                  Untrusted    15            1
Fa2/2                  Untrusted    15            1
```

DAI Scenario with Catalyst Switches (4)



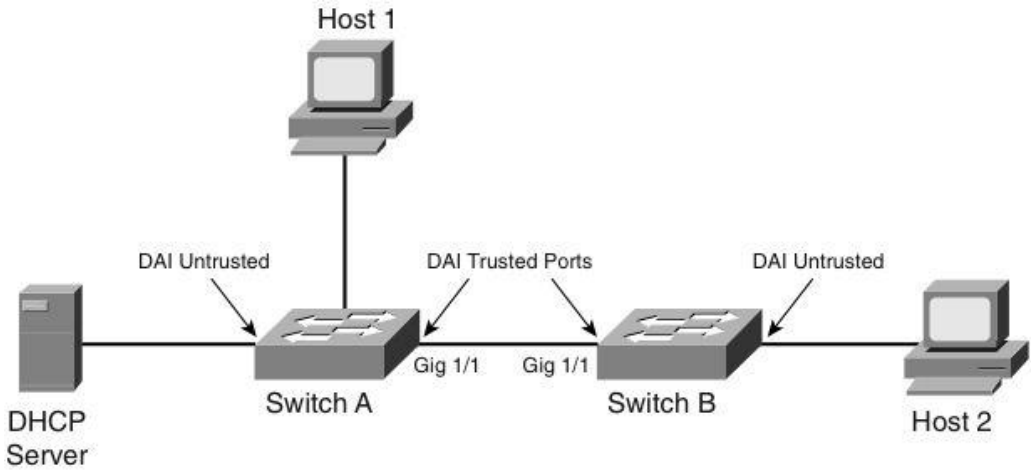

```
SwitchA# show ip arp inspection vlan 10
Source Mac Validation              : Disabled
Destination Mac Validation         : Disabled
IP Address Validation              : Disabled
Vlan   Configuration       Operation ACL Match        Static ACL
----   -------------       --------- ---------        ----------
10     Enabled       Active
Vlan   ACL Logging   DHCP Logging
----   -----------   ------------
10     Deny          Deny
```

DAI Scenario with Catalyst Switches (5)



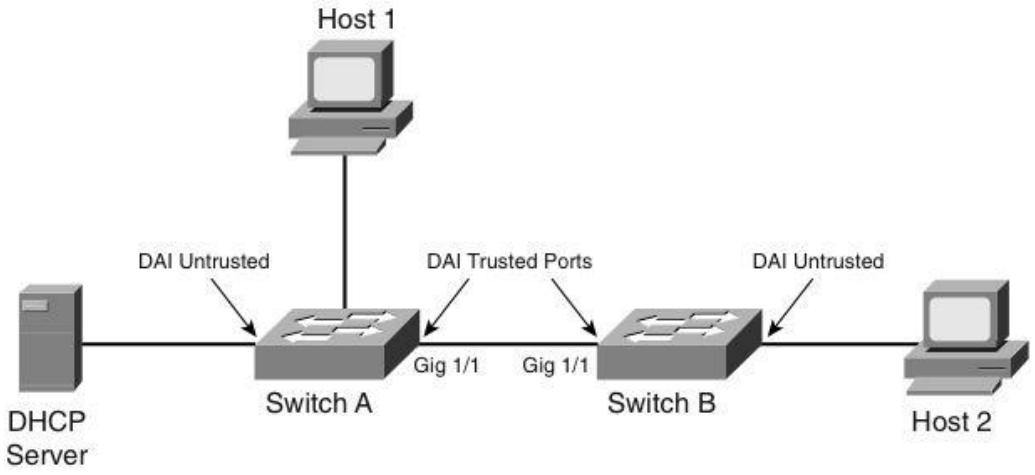

```
SwitchA# show ip dhcp snooping binding
MacAddress          IpAddress    Lease(sec)   Type            VLAN  Interface
------------------  ----------   ----------   -----------     ----  --------------
00:01:00:01:00:01   10.10.10.1   4995         dhcp-snooping   10    FastEthernet2/1
```

DAI Scenario with Catalyst Switches (6)



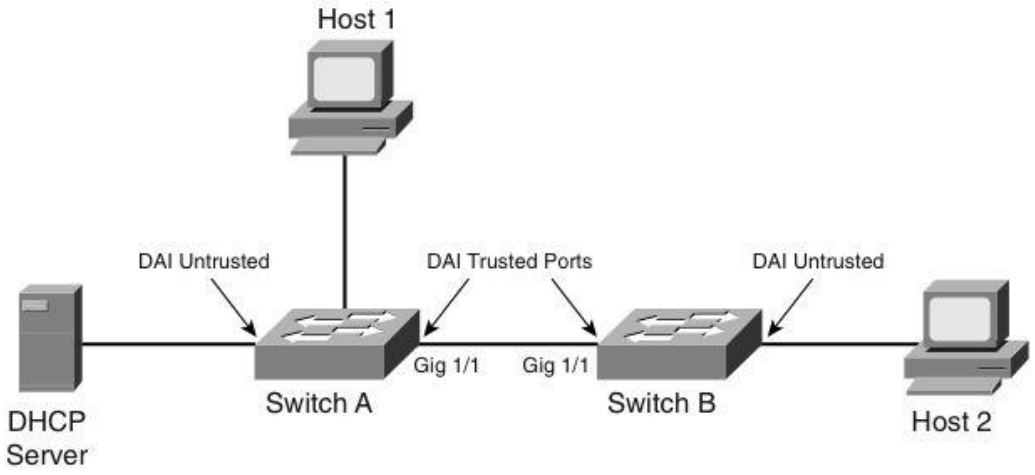

```
SwitchB# show ip arp inspection interfaces
Interface        Trust State      Rate (pps)    Burst Interval
---------------- -----------      ----------    --------------
Gi1/1            Trusted           None         N/A
Gi1/2            Untrusted         15           1
Fa2/1            Untrusted         15           1
Fa2/2            Untrusted         15           1
Fa2/3            Untrusted         15           1
Fa2/4            Untrusted        15            1
<output omitted>
```

DAI Scenario with Catalyst Switches (7)




```
SwitchB# show ip arp inspection vlan 10
Source Mac Validation              : Disabled
Destination Mac Validation         : Disabled
IP Address Validation              : Disabled
Vlan   Configuration   Operation  ACL Match     Static ACL
----   -------------   ---------  ---------     ----------
10     Enabled         Active

Vlan   ACL Logging     DHCP Logging
----   -----------     ------------
10     Deny            Deny
```

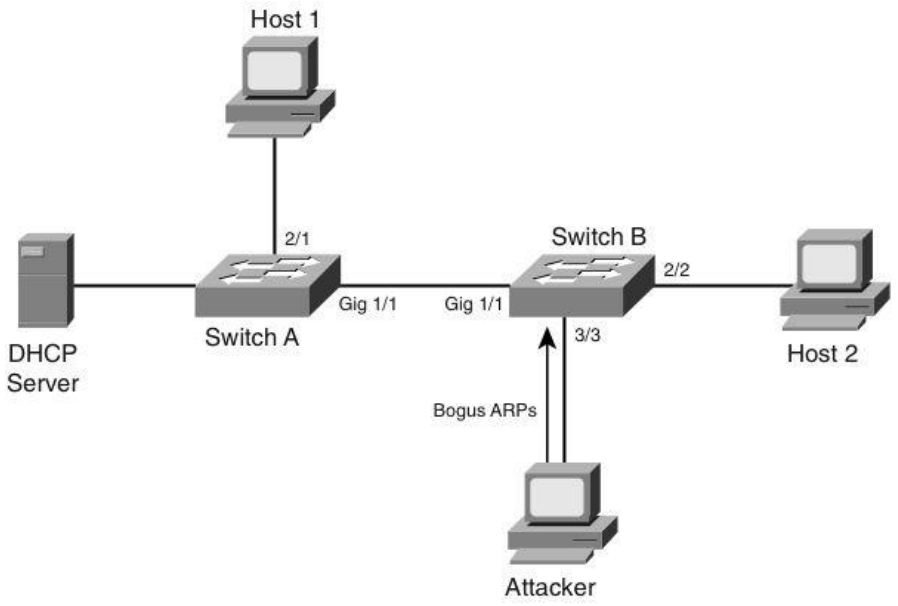
DAI Scenario with Catalyst Switches (8)




```
SwitchB# show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  ------------    ----------  -------------  ----  -----------
00:02:00:02:00:02   10.10.10.2      4995        dhcp-snooping  10    FastEthernet2/2
```

DAI Scenario with Catalyst Switches (9)

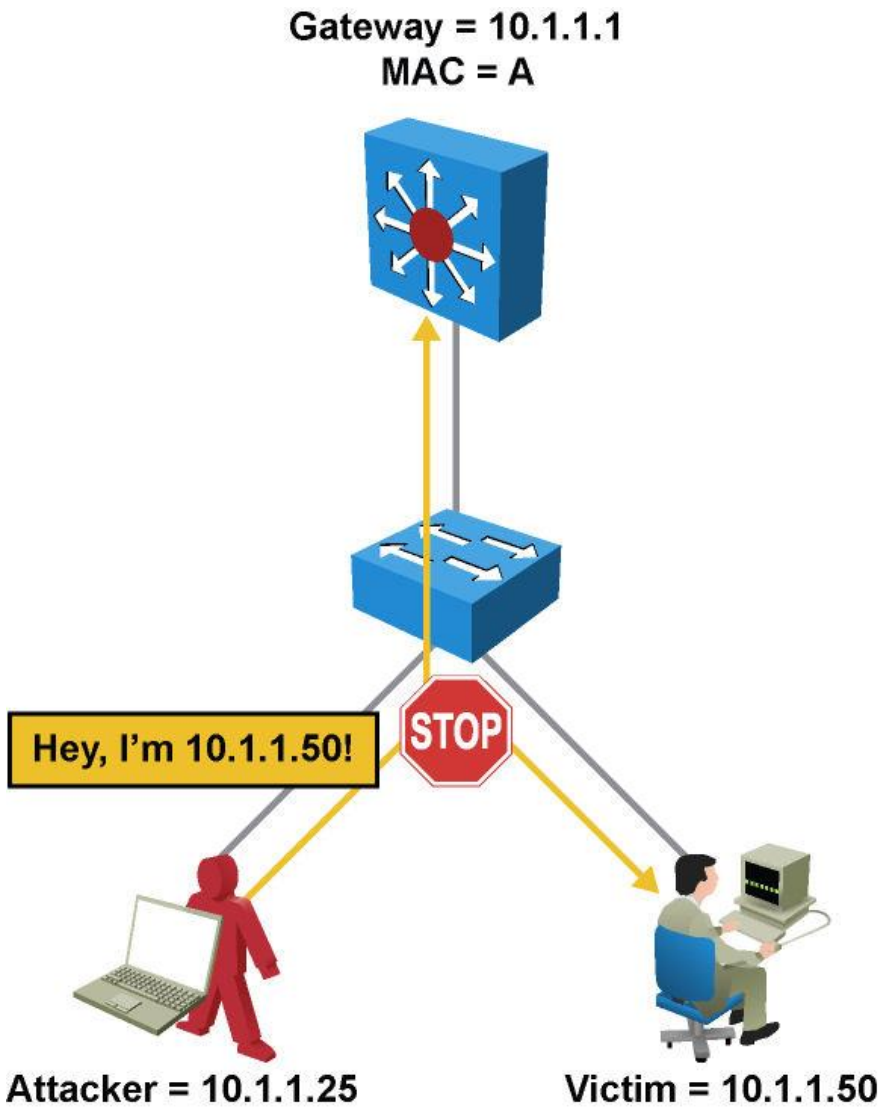
- If an attacker connects to Switch B and tries to send a bogus ARP request, Switch B will detect it and drop the ARP request packet. Switch B can also errdisable the port and send a log message to alert the administrator.
- DAI discards any ARP packets with invalid MAC-address-to-IP-address bindings. An error message is displayed on the switch when a security violation occurs:




```
02:46:49: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa3/3, vlan
10.([0001.0001.0001/10.10.10.1/0000.0000.0000/0.0.0.0/09:23:24 UTC Thu Nov 27
  2003])
```

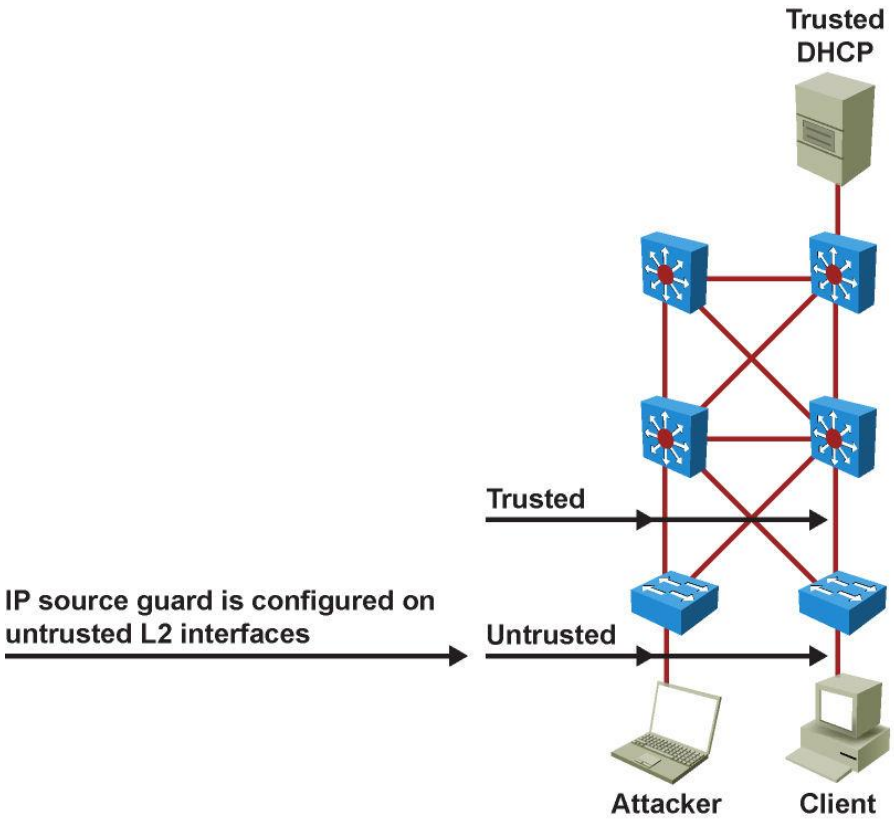
IP Spoofing and IP Source Guard

- Attacker impersonates a legitimate host on the network by spoofing the IP address of the victim.
- IP source guard (IPSG) prevents a malicious host from attacking the network with a hijacked IP address.
- IPSG provides per-port traffic filtering of assigned source IP.
- IPSG dynamically maintains per-port ACL's based on IP-to-MAC-to-switch port bindings.
- IPSG typically deployed for untrusted ports at access layer.
- IPSG works closely with DHCP snooping.



IP Source Guard Operations

- IPSG can be enabled on a DHCP snooping untrusted Layer 2 port to prevent IP spoofing.
- At first, all IP traffic on the port is blocked except for DHCP packets captured by the DHCP snooping process.
- This process restricts the client IP traffic to those source IP addresses configured in the binding; any IP traffic with a source IP address other than that in the IP source binding is filtered out. This filtering limits a host's capability to attack the network by claiming a neighbor host's IP address.



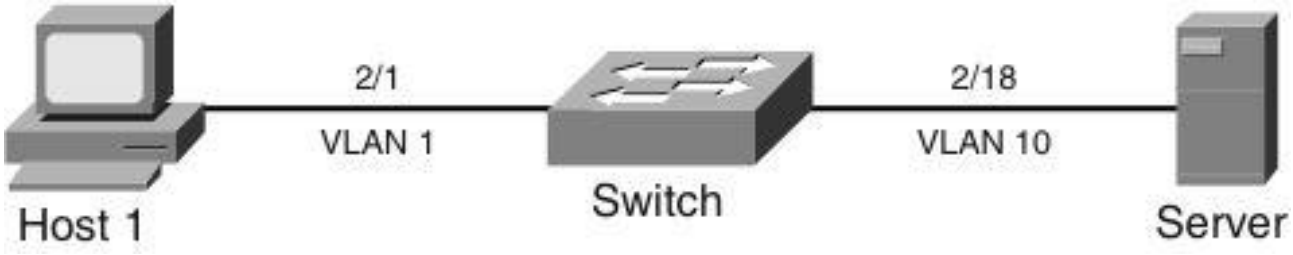
Configuring IP Source Guard

Step	Commands
1.	`Switch(config)# ip dhcp snooping`
2.	`Switch(config)# ip dhcp snooping vlan number [number]`

3.	`Switch(config-if)# ip verify source vlan dhcp-snooping`
	or
	`Switch(config-if)# ip verify source vlan dhcp-snooping port-security`

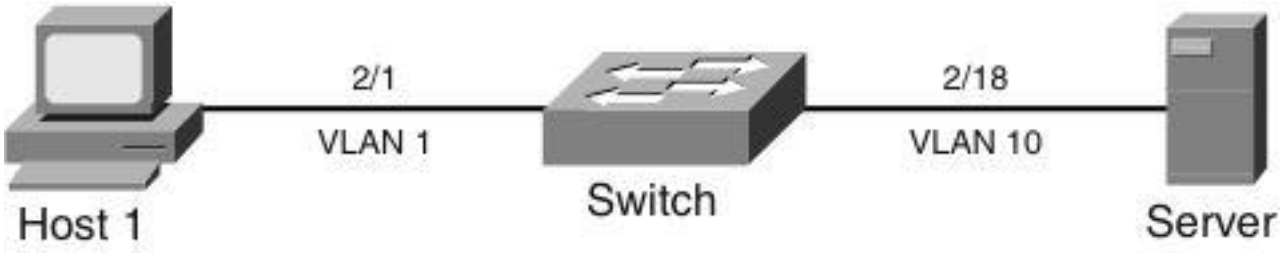
4.	`Switch(config-if)# switchport portsecurity limit rate invalid-source-mac N`
5.	`Switch(config)# ip source binding ipaddr ip vlan number interface interface-id`

IPSG Scenario (1)



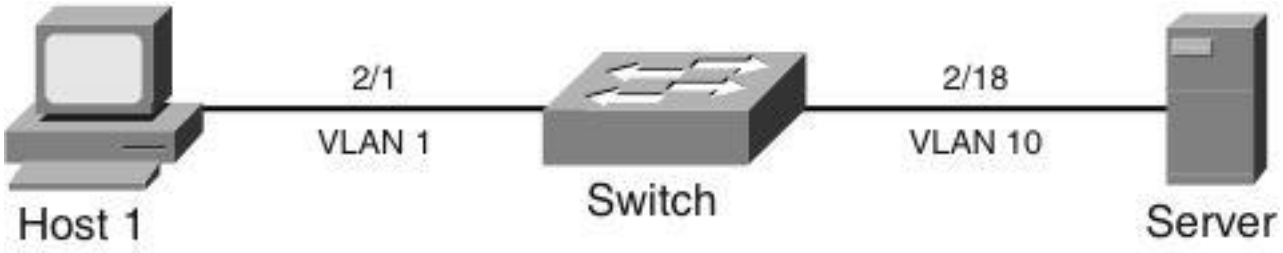
- A workstation using DHCP for acquiring IP addresses connects to the same Catalyst switch as a server with a static IP address.

IPSG Scenario (2)




```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 1,10
Switch(config)# ip dhcp snooping verify mac-address
Switch(config)# ip source binding 0000.000a.000b vlan 10 10.1.10.11 interface Fa2/18
Switch(config)# interface fastethernet 2/1
Switch(config-if)# switchport
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# ip verify source vlan dhcp-snooping port-security
Switch(config)# interface fastethernet 2/18
Switch(config-if)# switchport
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# ip verify source vlan dhcp-snooping port-security
```

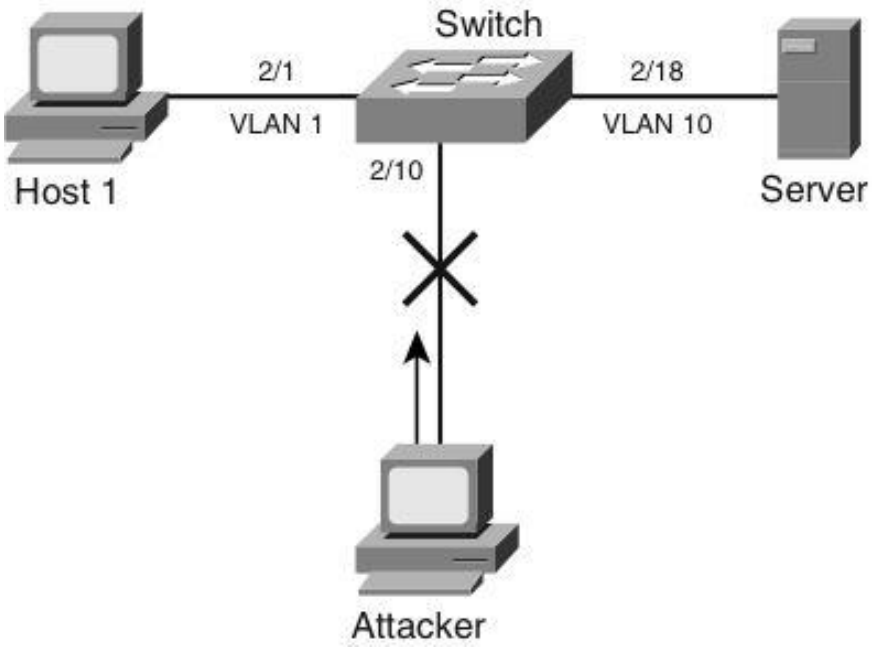
IPSG Scenario (3)




```
Switch# show ip source binding
MacAddress          IpAddress       Lease(sec)   Type            VLAN   Interface
------------------ ------------ ---------- -------------      ----   ----------
00:02:B3:3F:3B:99  10.1.1.11       6522          dhcp-snooping    1      FastEthernet2/1
00:00:00:0A:00:0B  10.1.10.11      infinite      static           10     FastEthernet2/18


Switch# show ip verify source
Interface Filter-type Filter-mode   IP-address        Mac-address        Vlan
--------- ----------- -----------   --------------- -----------------  ----------
Fa2/1      ip-mac      active       10.1.1.11         00:02:B3:3F:3B:99  1
Fa2/18     ip-mac      active       10.1.10.11        00:00:00:0a:00:0b  10
```

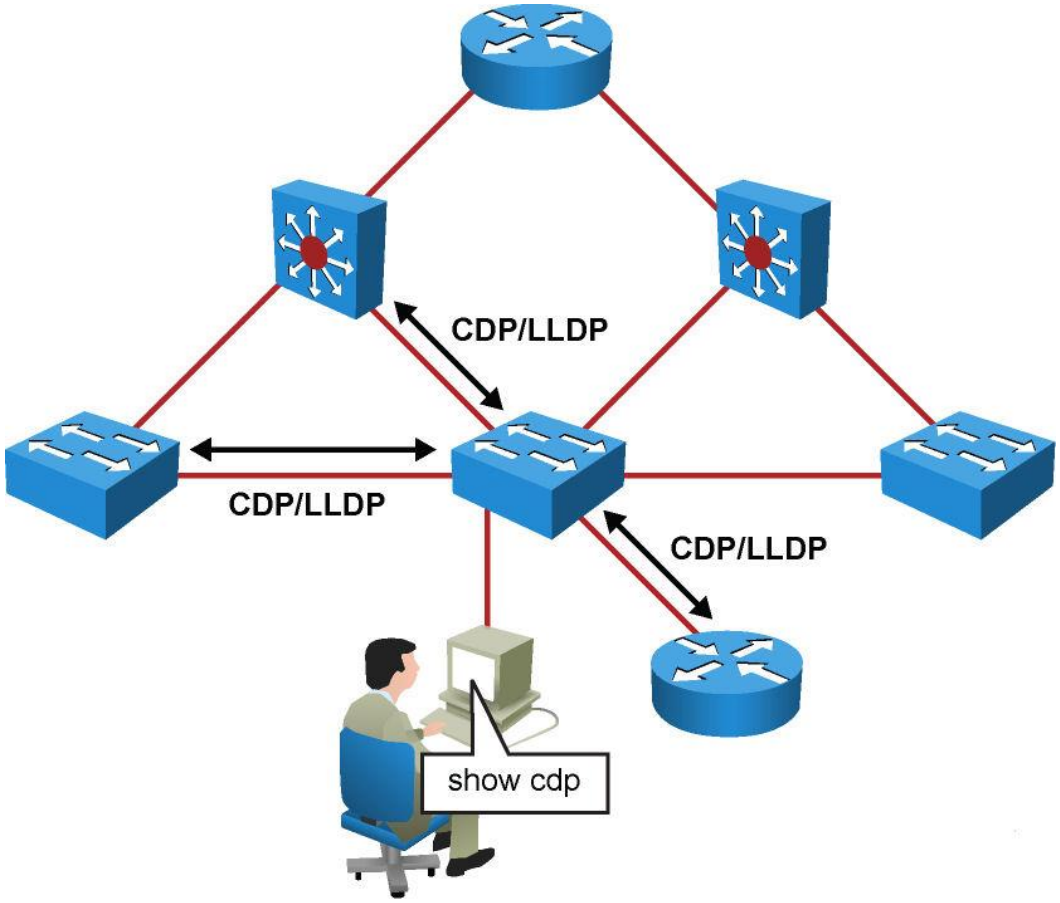
IPSG Scenario (4)

- An attacker is connected to interface 2/10 and is trying to spoof the IP address of the server.
- The Catalyst switch detects and drops the packets in the hardware path. The Catalyst switch also provides an error message to indicate the violation.



Securing Network Switches

Neighbor Discovery Protocols (NDP)



- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (LLDP)

Cisco Discovery Protocol

- Uses multicast hello messages
- Uses a TTL in seconds
- Cached CDP information available to network management system via SNMP – recommended to block SNMP access to CDP

Configuring CDP

- CDP is enabled by default.
- The **`no cdp run`** command disables CDP globally.
- The **`no cdp enable`** command disables CDP on an interface.

Displaying CDP Information (1)

- When CDP is enabled the command **show cdp neighbor** displays a summary of which devices are seen on which ports.

```
switch# show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce    Holdtme Capability  Platform Port ID
c2960-8          Fas 0/8          168     S I         WS-C2960-Fas 0/8
```

Displaying CDP Information (2)

```
4506# show cdp neighbor detail
-----------------------
Device ID: TBA03501074(SwitchA-6500)
Entry address(es):
IP address: 10.18.2.137
Platform: WS-C6506, Capabilities: Trans-Bridge Switch IGMP
Interface: FastEthernet3/21, Port ID (outgoing port): 3/36
Holdtime : 170 sec
Version :
WS-C6506 Software, Version McpSW: 7.6(1) NmpSW: 7.6(1)
Copyright © 1995-2003 by Cisco Systems
advertisement version: 2
VTP Management Domain: ‘0’
Native VLAN: 1
Duplex: full
-----------------------
Device ID: SwitchC-4503
Entry address(es):
IP address: 10.18.2.132
Platform: cisco WS-C4503, Capabilities: Router Switch IGMP
Interface: FastEthernet3/27, Port ID (outgoing port): FastEthernet3/14
Holdtime : 130 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I5S-M), Version 12.1(19)EW,
CISCO ENHANCED PRODUCTION VERSION
Copyright © 1986-2003 by cisco Systems, Inc.
Compiled Tue 27-May-03 04:31 by prothero
<output omitted>
```

Configuring LLDP

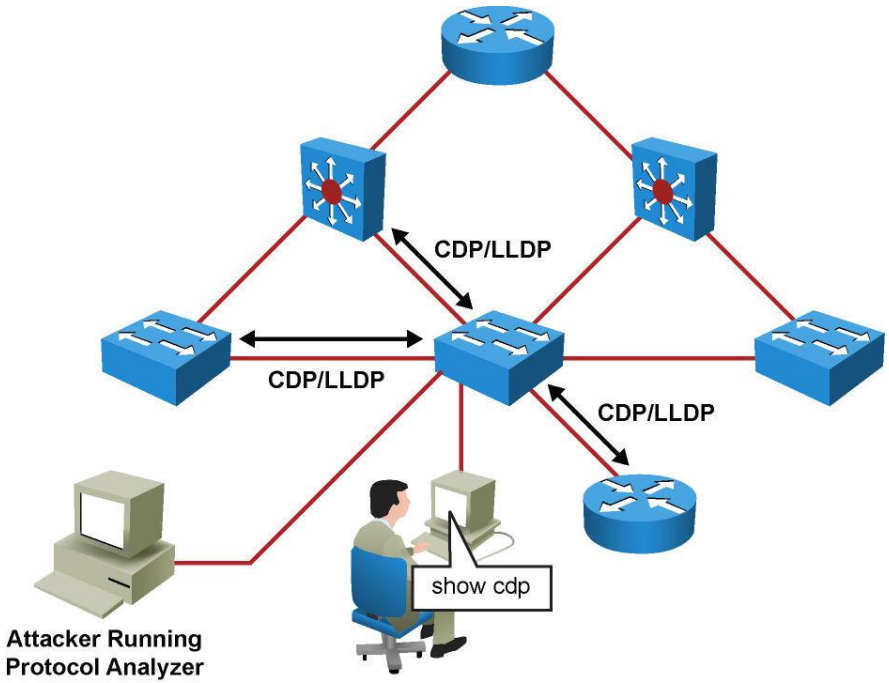
- LLDP is disabled by default.
- The command **`lldp run`** enables LLDP globally.
- The command **`lldp enable`** enables LLDP on an interface.

Displaying LLDP Information

- When LLDP is enabled the command **show lldp neighbor** displays a summary of which devices are seen on which ports.

```
switch(config)# lldp run
switch(config)# end
switch# show lldp neighbor
Capability codes:
        (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
        (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID       Local Intf     Hold-time      Capability     Port ID
c2960-8         Fa0/8          120            B              Fa0/8
Total entries displayed: 1
```

CDP Vulnerabilities



Sequence of Events	Description
1.	System administrator uses CDP to view neighbor information.
2.	Attacker uses a packet analyzer to intercept CDP traffic.
3.	Attacker analyzes information in CDP packets to gain knowledge of network address and device information.
4.	Attacker formulates attacks based on known vulnerabilities of network platforms.

Securing Switch Access

- Telnet Vulnerabilities
- Secure Shell (SSH) Vulnerabilities

Telnet Vulnerabilities

- All usernames, passwords, and data sent over the public network in clear text are vulnerable.
- A user with an account on the system could gain elevated privileges.
- A remote attacker could crash the Telnet service, preventing legitimate use of that service by performing a DoS attack such as opening too many bogus Telnet sessions.
- A remote attacker could find an enabled guest account that might be present anywhere within the trusted domains of the server.

Secure Shell (SSH)

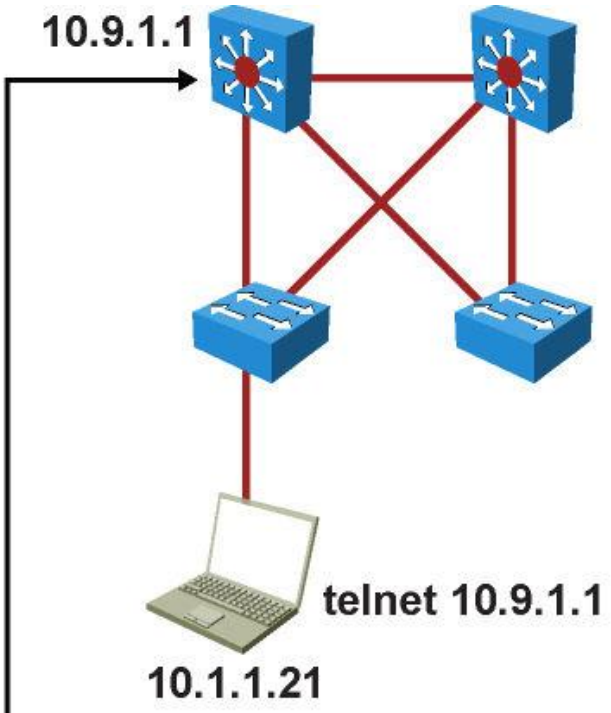
- All usernames, passwords, and data sent over the public network in clear text are vulnerable.
- A user with an account on the system could gain elevated privileges.
- A remote attacker could crash the Telnet service, preventing legitimate use of that service by performing a DoS attack such as opening too many bogus Telnet sessions.
- A remote attacker could find an enabled guest account that might be present anywhere within the trusted domains of the server.

Configuring SSH

- Step 1. Configure a user with a password.
- Step 2. Configure the hostname and domain name.
- Step 3. Generate RSA keys.
- Step 4. Allow SSH transport on the vty lines.

```
switch(config)# username xyz password abc123
switch(config)# ip domain-name xyz.com
switch(config)# crypto key generate rsa
switch(config)# ip ssh version 2
switch(config)# line vty 0 15
switch(config-line)# login local
switch(config-line)# transport input ssh
```

VTY Access Control Lists



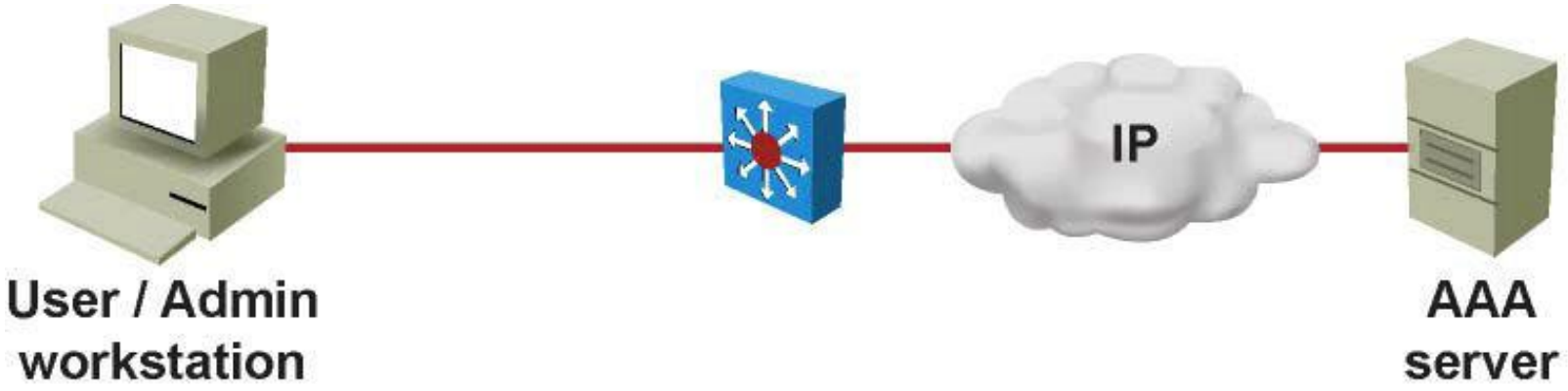

```
sw(config)# access-list 100 permit ip 10.1.1.0 0.0.0.255 any
sw(config)# line vty 0 15
sw(config-line)# access-class 100 in
```

HTTP Secure Server

- Step 1. Configure username and password.
- Step 2. Configure domain name.
- Step 3. Generate RSA keys.
- Step 4. Enable HTTPS (SSL) server.
- Step 5. Configure HTTP authentication.
- Step 6. Configure an access list to limit access.

```
sw(config)# access-list 100 permit ip 10.1.9.0 0.0.0.255 any
sw(config)# username xyz password abc123
sw(config)# ip domain-name xyz.com
sw(config)# crypto key generate rsa
sw(config)# no ip http server
sw(config)# ip http secure-server
sw(config)# ip http access-class 100 in
sw(config)# ip http authentication local
```

Authentication, Authorization, and Accounting (AAA)



- The AAA network-security services provide the primary framework through which you set up access control on a Cisco IOS switch. AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner.

Authentication

Authentication provides a method to handle:

- User identification
- Login and password dialog
- Challenge and response
- Messaging
- Encryption

Authorization

Authorization provides the method for remote access control.

- Remote access control includes:
  - One-time authorization or
  - Authorization for each service on a per-user account list or a user group basis.
- Uses RADIUS or TACACS+ security servers.

RADIUS Attribute-Value Pairs (AVP's)

Attribute	Type of Value
User-Name	String
Password	String
CHAP-Password	String
Client-Id	IP address
Login-Host	IP address
Login-Service	Integer
Login-TCP-Port	Integer

TACACS+ Attribute-Value Pairs (AVP's)

Attribute	Type of Value
Inacl	Integer
Addr-pool	String
Addr	IP address
Idletime	Integer
Protocol	Keyword
Timeout	Integer
Outacl	Integer

Accounting

- Authorization provides the method for collecting and sending security server information used for billing, auditing, and reporting. Includes:
  - User identities
  - Start and stop times
  - Executed commands
  - Number of packets
  - Number of bytes

Configuring Authentication

- Variety of login authentication methods.
- First use **aaa new-model** command to initialize AAA.
- Use **aaa authentication login** command to enable AAA login authentication.
- With **aaa authentication login** command, configure one or more lists of authentication methods.
- The **login authentication line {default |** *list-name*} *method1* **[***method2...***]** command defines the list name and the authentication methods in order, such as TACACS+ or RADIUS.
- The **login authentication {default |** *list-name*} command applies the authentication list to an input line.

AAA Authentication Example

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login TEST tacacs+
Switch(config)# tacacs-server host 192.168.100.100
Switch(config)# line vty 0 4
Switch(config-line)# login authentication TEST
```

AAA Authentication Configuration Detail

- Step 1. Configure the TACACS+ server for a test user:
  - When using Cisco Access Control Server (ACS) for Microsoft Windows, create a new test user without specific options.
- Step 2. Configure a new network device on the TACACS+ server:
  - When using Cisco ACS for Microsoft Windows, create a new network device by specifying the DNS name and IP address, and specify a key to be used for TACACS+.
- Step 3. Access the switch using the Console (out-of-band) connection.
- Step 4. Enable AAA globally:

```
svs-san-3550-1(config)# aaa new-model
```

- Step 5. Configure the TACACS+ server and key:

```
svs-san-3550-1(config)# tacacs-server host 172.18.114.33
svs-san-3550-1(config)# tacacs-server key SWITCH
```

- Step 6. Configure the default login access:

```
svs-san-3550-1(config)# aaa authentication login default group tacacs+
  enable
```

- Step 7. Test the login using a separate connection:
  - This enables you to troubleshoot and make changes in real time while testing the configuration.

AAA Authorization Configuration

- Use the command:

  aaa authorization {auth-proxy | network | exec | commands level | reverse-access | configuration | ipmobile} {default | *list-name*} [*method1* [*method2...*]]
  aaa *authorization* {arap | commands *level* | exec | reverse-access} {default | *list-name*}

- Use the **aaa authorization** command with the **group tacacs+** method keywords to request authorization via a TACACS+ server. The **group tacacs+** method instructs the switch to use a list of all TACACS+ servers for authentication.
- Use the **aaa authorization** command with the **local** method keyword to request authorization via the local user database.
- Use the **aaa authorization** command with the **group radius** method keywords to request authorization via a RADIUS server.

AAA Authorization Example

- This configuration example illustrates configuring AAA authorization for users via VTY access for shell commands.
- To allow users to access the functions they request as long as they have been authenticated, use the a**aa authorization** command with the **if-authenticated** method keyword, as shown.

```
Switch(config)# aaa new-model
Switch(config)# aaa authorization commands 0 default if-
authenticated group tacacs+
Switch(config)# line vty 0 4
Switch(config-line)# authorization commands 0 default
```

AAA Accounting Types Supported

- **Network accounting:** Provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.
- **Connection accounting:** Provides information about all outbound connections made from the network, such as Telnet and rlogin.
- **EXEC accounting:** Provides information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number from which the call originated.
- **System accounting:** Provides information about all system-level events (for example, when the system reboots and when accounting is turned on or off).
- **Command accounting:** Provides information about the EXEC shell commands for a specified privilege level executed on a network access server.
- **Resource accounting:** Provides start and stop record support for calls that have passed user authentication.

AAA Accounting Configuration

- Use the command:

  aaa accounting {system | network | exec | connection | commands *level*} **{default |** *list-name*} **{start-stop | stop-only | none}** [*method1* [*method2...*]]

- Apply the accounting method to an interface or lines using the command:

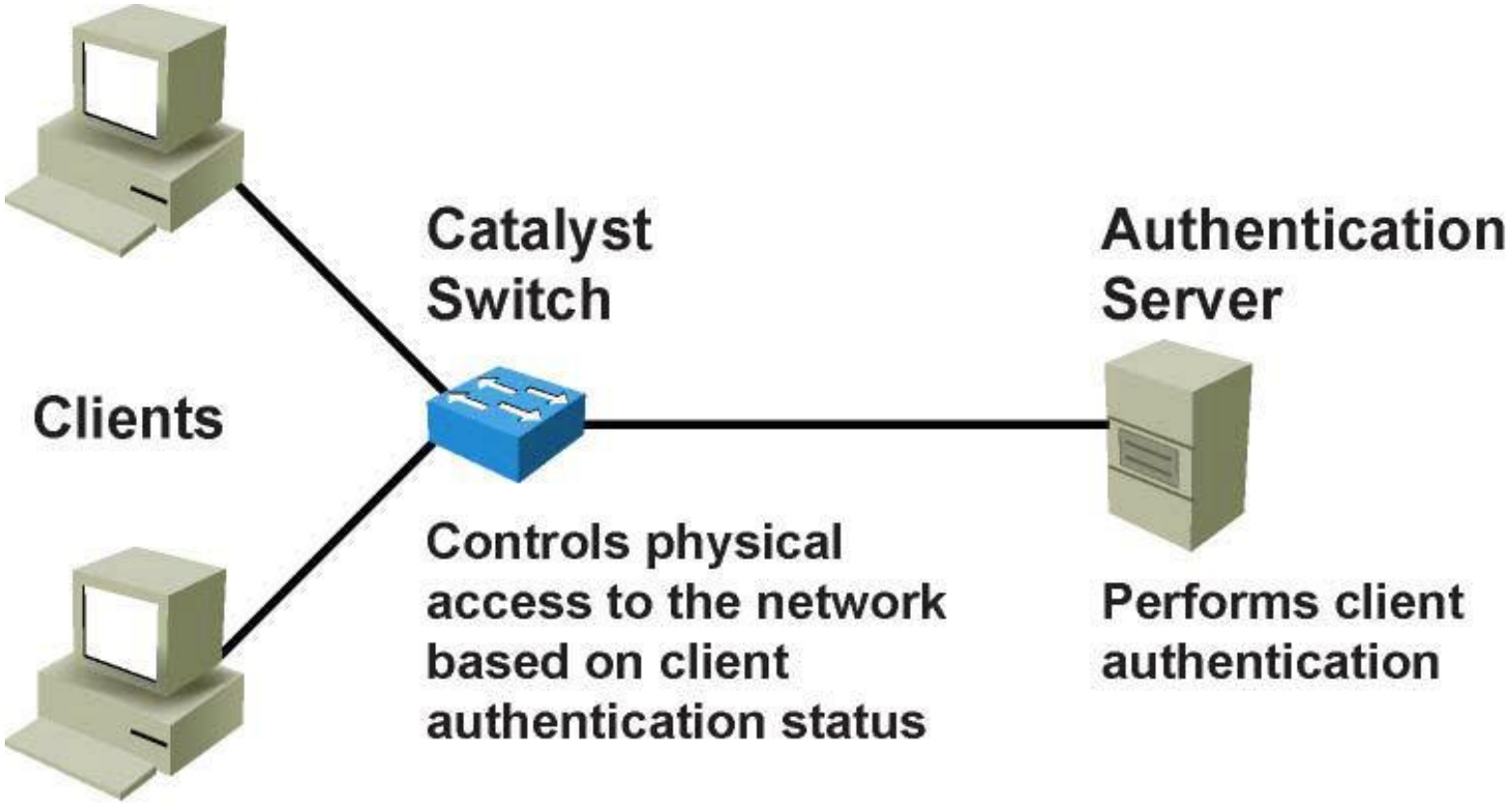
  accounting {arap | commands *level* **| connection | exec} {default |** *list-name*}

AAA Accounting Example

- This configuration example illustrates configuring AAA authorization for users via VTY access for shell commands.
- To allow users to access the functions they request as long as they have been authenticated, use the **aaa authorization** command with the **if-authenticated** method keyword, as shown.

```
Switch(config)# aaa new-model
Switch(config)# aaa accounting exec default start-stop group tacacs+
Switch(config)# line vty 0 4
Switch(config-line)# accounting exec default
```

Security Using IEEE 802.1X Port-Based Authentication



802.1X Roles

- **Client (or supplicant):** The device that requests access to LAN and switch services and then responds to requests from the switch. The workstation must be running 802.1X-compliant client software.
- **Authentication server:** Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether the client is authorized to access the LAN and switch services. The RADIUS security system with EAP extensions is the only supported authentication server.
- **Switch (or authenticator):** Controls physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identifying information from the client, verifying that information with the authentication server, and relaying a response to the client.

802.1X Port Authorization State (1)

- You control the port authorization state by using the interface configuration command :

  dot1x port-control {auto | force-authorized | force-unauthorized}

- The **force-authorized** keyword disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This is the default setting. This configuration mode supports any non-dot1x-enabled client.

802.1X Port Authorization State (2)

- You control the port authorization state by using the interface configuration command :

```
dot1x port-control {auto | force-authorized |
force-unauthorized}
```

- The **force-unauthorized** keyword causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface. This configuration mode can be enabled to prevent connections from any users from unauthorized ports.

802.1X Port Authorization State (3)

- You control the port authorization state by using the interface configuration command :

```
dot1x port-control {auto | force-authorized |   force-unauthorized}
```

- The **auto** keyword enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, enabling only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up (authenticator initiation) or when an EAPOL-start frame is received (supplicant initiation). The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The switch uniquely identifies each client attempting to access the network by using the client MAC address. This configuration mode can be used on ports that connect to a 802.1X client.

Configuring IEEE 802.1X

- Step 1. Enable AAA:

```
Switch(config)# aaa new-model
```

- Step 2. Create an 802.1X port-based authentication method list:

```
Switch(config)# aaa authentication dot1x {default}
method1 [method2...]
```

- Step 3. Globally enable 802.1X port-based authentication:

```
Switch(config)# dot1x system-auth-control
```

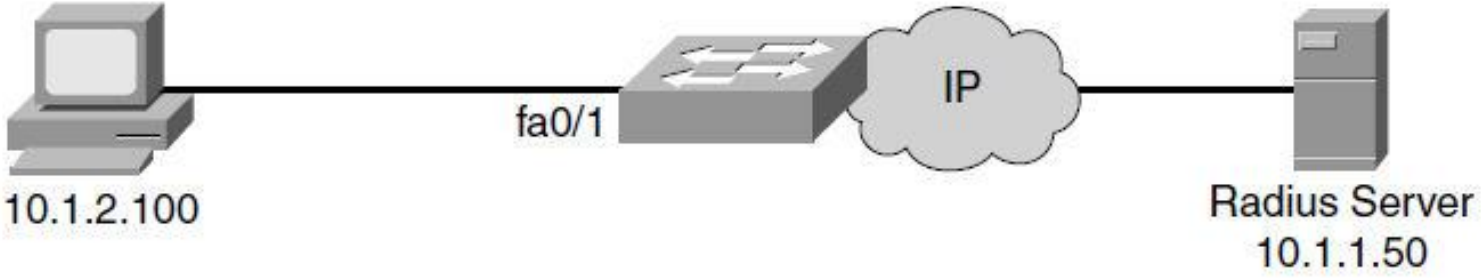
- Step 4. Enter interface configuration mode and specify the interface to be enabled for 802.1X port-based authentication:

```
Switch(config)# interface type slot/port
```

- Step 5. Enable 802.1X port-based authentication on the interface:

```
Switch(config-if)# dot1x port-control auto
```

IEEE 802.1X Configuration Example




```
sw(config)# aaa new-model
sw(config)# radius-server host 10.1.1.50 auth-port 1812 key xyz123
sw(config)# aaa authentication dot1x default group radius
sw(config)# dot1x system-auth-control
sw(config)# interface fa0/1
sw(config-if)# description Access Port
sw(config-if)# switchport mode access
sw(config-if)# dot1x port-control auto
```

Switch Security Considerations

Organizational Security Policies

- Provides a process for auditing existing network security.
- Provides a general security framework for implementing network security.
- Defines disallowed behaviors toward electronic data.
- Determines which tools and procedures are needed for the organization.
- Communicates consensus among a group of key decision makers and defines responsibilities of users and administrators.
- Defines a process for handling network security incidents.
- Enables an enterprise-wide, all-site security implementation and enforcement plan.

Securing Switch Devices and Protocols

- Configure strong system passwords.
- Restrict management access using ACLs.
- Secure physical access to the console.
- Secure access to vty lines.
- Configure system warning banners.
- Disable unneeded or unused services.
- Trim and minimize the use of CDP/LLDP.
- Disable the integrated HTTP daemon (where appropriate).
- Configure basic system logging (syslog).
- Secure SNMP.
- Limit trunking connections and propagated VLANs.
- Secure the spanning-tree topology.

Configuring Strong System Passwords

- Use the **`enable secret`** command instead of using the **`enable password`** command.
- Because the **`enable secret`** command simply implements an MD5 hash on the configured password, that password remains vulnerable to dictionary attacks. Therefore, standard practice in selecting a feasible password applies. Try to pick passwords that contain letters, numbers, and special characters.
- An example of a feasible password is “$pecia1$” – that is, the word “specials” where each “s” has been replaced by “$” and the letter “l” has been replaced with the numeral “1”.

Restricting Management Access Using ACL's

- Subnet 10.1.2.0/24 is used for accessing all network devices for management purposes. This subnet does not pass user data traffic. Access to this subnet is limited to system administrators in the 10.1.3.0/24 subnet.

```
<output omitted>
interface Vlan600
description User LAN
ip address 10.1.1.1 255.255.255.0
!
interface Vlan601
description Management VLAN
ip address 10.1.2.1 255.255.255.0
ip access-group 100 in
!
interface Vlan602
description IT LAN
ip address 10.1.3.1 255.255.255.0
!
access-list 100 permit ip 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 100 deny ip any any log
!
<output omitted>
```

Securing Physical Access to the Console

- Physical security of switches or routers is often overlooked but is a valuable security precaution.
- Console access requires a minimum level of security both physically and logically.
- An individual who gains console access to a system gains the ability to recover or reset the passwords or to reload the system, thereby enabling that individual to bypass all other security measures implemented on that system.
- It is imperative to physically secure access to the console by using security personnel, closed circuit television, card-key entry systems, locking cabinets, access logging, or other means to control physical access as standard practice.

Securing Access to vty Lines

- Apply ACLs on all vty lines to limit in-band access only to management stations from specific subnets.
- Configure strong passwords for all configured vty lines.
- Use Secure Shell (SSH) instead of Telnet to access the device remotely.

Configuring System Warning Banners

- For both legal and administrative purposes, configuring a system warning banner to display prior to login is a convenient and effective way of reinforcing security and general usage policies.
- Clearly stating the ownership, usage, access, and protection policies prior to a login aids in stronger prosecution if unauthorized access occurs. Use the global configuration banner command to configure system banner messages.

Disabling Unneeded or Unused Services

- TCP Small Servers (Echo, Chargen, Discard, Daytime)
- UDP Small Servers (Echo, Discard, Chargen)
- Finger
- Auto config
- Packet Assembler and Disassembler (PAD)
- BOOTP server
- Identification service
- NTP without authentication
- Source routing
- IP Proxy-ARP
- ICMP unreachables
- ICMP redirects
- Directed broadcast forwarding
- Maintenance Operation Protocol (MOP)

Trimming and Minimizing Use of CDP/LLDP

- Disable CDP/LLDP on a per-interface basis. Run CDP/LLDP only for administrative purposes, such as on inter-switch connections and interfaces where IP phones reside.
- Confine CDP/LLDP deployment to run between devices under your control. Because CDP/LLDP is a link-level (Layer 2) protocol, it does not propagate end-to-end over a MAN or WAN unless a Layer 2 tunneling mechanism is in place. As a result, for MAN and WAN connections, CDP tables might include the service provider's next-hop router or switch and not the far-end router under your control.
- Do not run CDP/LLDP to any unsecured connection, such as Internet connections.

Disabling Integrated HTTP Daemon

- Use the **`no ip http server`** command in Cisco IOS to disable HTTP server access on a switch.
- If HTTP access is needed, it is recommended to change the default TCP port number (80) using the **`ip http port port-no`** command. Secure HTTP is recommended over HTTP access.
- Secure HTTP can be enabled via the **`ip http secure-server`** command.

```
svs-san-msfc# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
svs-san-msfc(config)# no ip http server
svs-san-msfc(config)# end
```

Configuring Basic System Logging

- To assist and simplify both problem troubleshooting and security investigations, monitor switch subsystem information received from the logging facility.
- To render the on-system logging useful, increase the default buffer size; generally, the default buffer size is not adequate for logging most events.

Securing SNMP

- Whenever possible, avoid using SNMP read-write features. SNMPv2c authentication consists of simple text strings that are communicated between devices in clear, unencrypted text. In most cases, a read-only community string is sufficient.
- To use SNMP in a secure method, use SNMPv3 with an encrypted password and use ACL to limit SNMP from only trusted workstations and subnets.

Limiting Trunking Connections and Propagated VLAN's

- By default, specific models of Catalyst switches that are running Cisco IOS automatically negotiate trunking capabilities. This poses a security risk because the negotiation enables the introduction of an unauthorized trunk port into the network.
- If an unauthorized trunk port is used for traffic interception and to generate DoS attacks, the consequences can be far more serious than if only an access port is used. (A DoS attack on a trunk port might affect multiple VLANs, whereas a DoS attack on an access port affects only a single VLAN.)
- To prevent unauthorized trunks, disable automatic negotiation of trunking on host and access ports. In addition, remove unused VLANs from trunks manually or by using VTP.

Securing the Spanning-Tree Topology

- Inadvertent or malicious introduction of STP BPDUs potentially overwhelms a device or creates a DoS. The first step in stabilizing a spanning-tree installation is to positively identify the intended root and designated bridge in the design and to hard-code that bridge's STP bridge priority to an acceptable root value.
- Enable the root-guard feature to prevent authorized bridges with lower priorities from taking over the legitimate one.
- Use BPDU Guard feature to prevent host devices from maliciously sending BPDUs to a port. Upon receipt of an unauthorized STP BPDU, the feature automatically disables the port until user intervention occurs or a time-out value is reached.

Mitigating Issues Sourced from a Switch

- Enter the **shutdown** command on all unused ports and interfaces.
- Place all unused ports in a “parking-lot” VLAN used specifically to group unused ports until they are proactively placed into service.
- Configure all unused ports as access ports, disallowing automatic trunk negotiation.
  - **Physical device access:** Physical access to the switch should be closely monitored to avoid rogue device placement in wiring closets with direct access to switch ports.
  - **Access port–based security:** Specific measures should be taken on every access port of any switch placed into service. Ensure that a policy is in place outlining the configuration of unused switch ports in addition to those that are in use.

Troubleshooting Performance and Connectivity

Techniques to Enhance Performance (1)

Critical performance-management issues are:

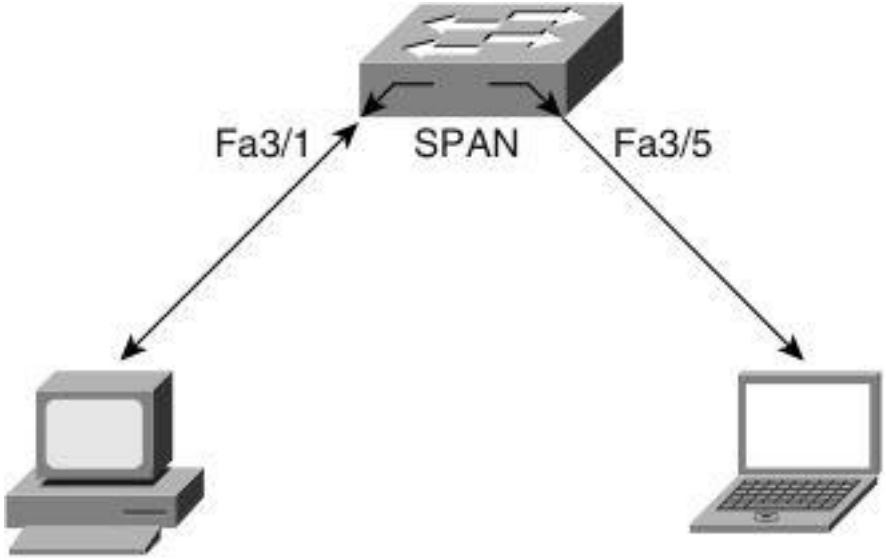
- **User/application performance**: For most users, response time is the critical performance success factor. This variable might shape the perception of network success by both your users and application administrators.
- **Capacity planning**: The process of determining future network resource requirements to prevent a performance or availability impact on business-critical applications.
- **Proactive fault management**: Involves both responding to faults as they occur and implementing solutions that prevent faults from affecting performance.

Techniques to Enhance Performance (2)

Critical success tasks for performance management are:

- Gather a baseline for both network and application data.
- Perform a what-if analysis on your network and applications.
- Perform exception reporting for capacity issues.
- Determine the network management overhead for all proposed or potential network management services.
- Analyze the capacity information.
- Periodically review capacity information, baseline, and exceptions for the network and applications.
- Maintain upgrade or tuning procedures set up to handle capacity issues on both a reactive and longer-term basis.

Monitoring Performance with SPAN and VSPAN



- The switch copies all traffic transmitted to and from Port 3/1 (the source port) to Port 3/5 (the destination port). A workstation running a packet-capturing application on Port 3/5 thus receives all network traffic received and transmitted on port 3/1.

Local SPAN Guidelines

- Both Layer 2 switched ports (LAN ports configured with the **`switchport`** command) and Layer 3 ports (LAN ports configured with the **`no switchport`** command) can be configured as source or destination ports in Cisco IOS–based switches.
- A port can act as the destination port for only one SPAN session.
- A port cannot be configured as a destination port if it is a source port of a span session.
- Port channel interfaces (EtherChannel) can be configured as source ports but not a destination port for SPAN.
- SPAN supports configuration of source ports belonging to different VLANs.
- Traffic direction is “both” by default for SPAN sources.
- Destination ports never participate in a spanning-tree instance. Local SPAN includes BPDUs in the monitored traffic, so any BPDUs seen on the destination port are from the source port. As a result, SPAN destination ports should not be connected to another switch because this might cause a network loop.
- Destination ports get a copy of all packets switched through the switch regardless of whether the packets actually leave the switch due to STP blocking state on an egress port.

VSPAN Guidelines

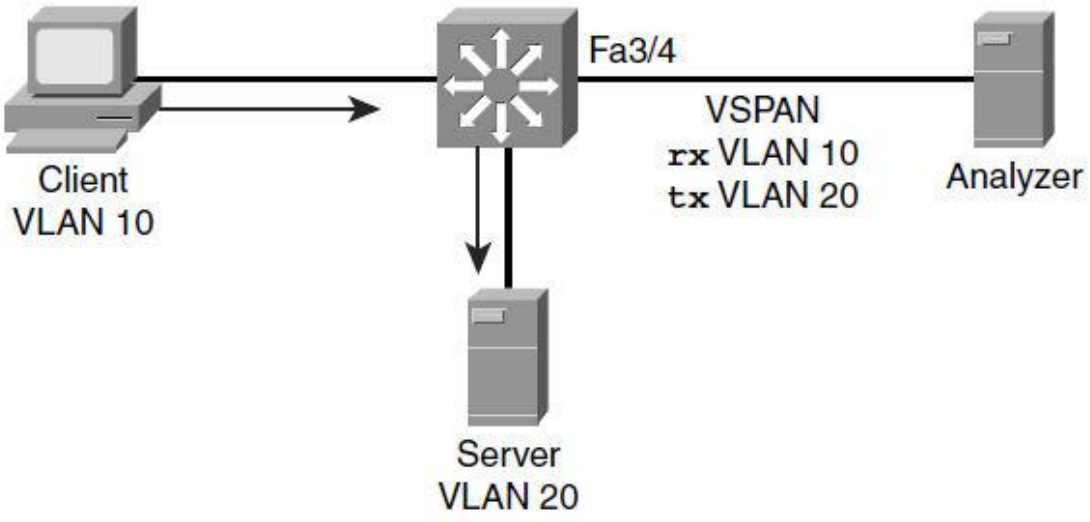
- VSPAN sessions, with both ingress and egress options configured, forward duplicate packets from the source port only if the packets get switched in the same VLAN.
- One copy of the packet is from the ingress traffic on the ingress port, and the other copy of the packet is from the egress traffic on the egress port.
- VSPAN monitors only traffic that leaves or enters Layer 2 ports in the VLAN:
  - Routed traffic that enters a monitored VLAN is not captured if the SPAN session is configured with that VLAN as an ingress source because traffic never appears as ingress traffic entering a Layer 2 port in the VLAN.
  - Traffic that is routed out of a monitored VLAN, which is configured as an egress source in a SPAN session, is not captured because the traffic never appears as egress traffic leaving a Layer 2 port in that VLAN.

Configuring Local SPAN

- The example shows the configuration and verification of a local SPAN session on a Cisco IOS–based switch for the topology in the figure. The source interface is FastEthernet 3/1, and the destination interface is FastEthernet 3/5.

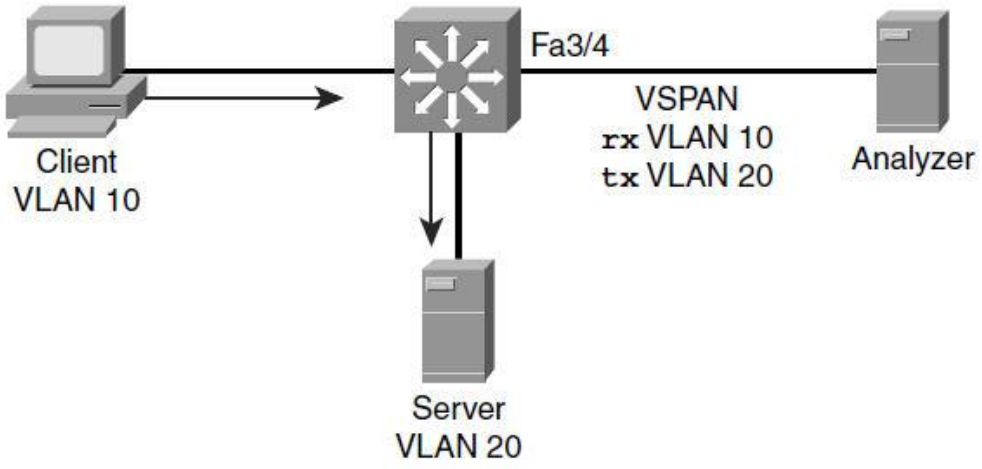
```
4506(config)# monitor session 1 source interface FastEthernet 3/1
4506(config)# monitor session 1 destination interface FastEthernet 3/5
4506(config)# end
4506# show monitor session 1
Session 1
---------
Type                   : Local Session
Source Ports           :
Both                   : Fa3/1
Destination Ports      : Fa3/5
Encapsulation          : Native
Ingress                : Disable
```

VSPAN Scenario (1)



- The administrator needs to troubleshoot the traffic flow between a client in VLAN 10 and server in VLAN 20.
- She configures a VSPAN session on a Cisco IOS–based Catalyst switch with rx-only traffic for VLAN 10 and tx-only traffic for VLAN 20 and destination port interface FastEthernet 3/4.

VSPAN Scenario (2)




```
cat4k(config)# monitor session 1 source vlan 10 rx
cat4k(config)# monitor session 1 source vlan 20 tx
cat4k(config)# monitor session 1 destination interface FastEthernet 3 /4
cat4k# show monitor session 1
Session 1
-----
Type                   : Local Session
Source VLANs    :
      RX Only   : 10
      TX Only   : 20
Destination Ports : Fa3/4
      Encapsulation : Native
                Ingress         : Disabled
```

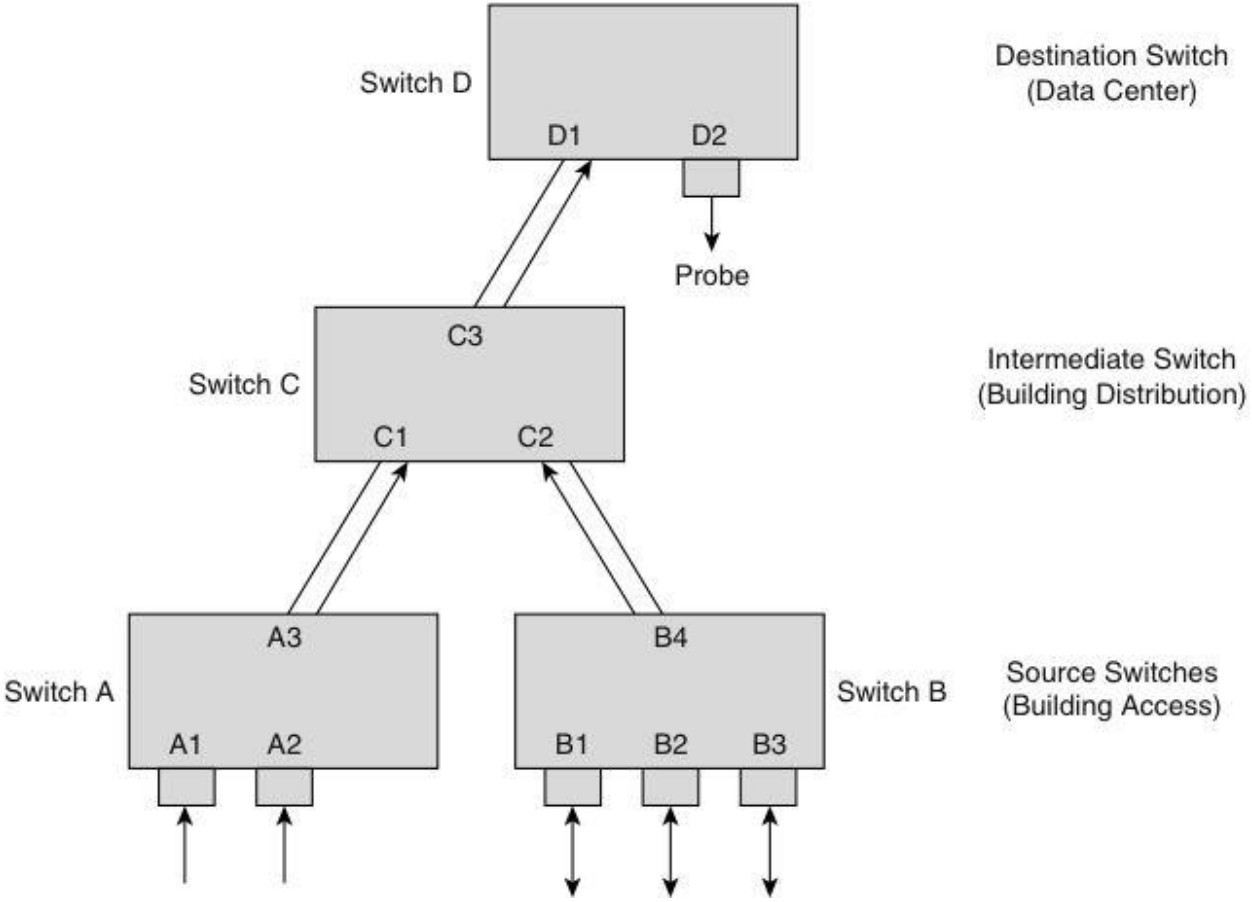
Using SPAN to Monitor the CPU Interface

- To configure a SPAN to monitor the CPU traffic on Catalyst 4500 switches, use the keyword **cpu** in the **monitor session** source configuration.

```
4506(config)# monitor session 1 source cpu ?
both Monitor received and transmitted traffic
queue SPAN source CPU queue
rx Monitor received traffic only
tx Monitor transmitted traffic only
<cr>
4506(config)# monitor session 1 destination interface fastEthernet
3/21
4506(config)# end
4506# show monitor session 1
Session 1
---------
Type                   : - Source Ports :
Both          : CPU Destination Ports : Fa3/21
Encapsulation          : Native
Ingress       : Disabled
```

Monitoring Performance with RSPAN

- Remote SPAN (RSPAN) is similar to SPAN, but it supports source ports, source VLANs, and destination ports on different switches.



RSPAN Guidelines

- Configure the RSPAN VLANs in all source, intermediate, and destination network devices. If enabled, VTP can propagate configurations of VLANs numbered 1 through 1024 as RSPAN VLANs. Manually configure VLANs numbered higher than 1024 as RSPAN VLANs on all source, intermediate, and destination network devices.
- Switches impose no limit on the number of RSPAN VLANs configured.
- Configure any VLAN as an RSPAN VLAN as long as all participating network devices support configuration of RSPAN VLANs, and use the same RSPAN VLAN for each RSPAN session.

Configuring RSPAN (1)

- **Step 1.** Configure the RSPAN VLAN in the VTP server. This VLAN is then dedicated for RSPAN. If VTP transparent mode is used, configure RSPAN in all the devices in the domain consistently.
- **Step 2.** Configure the RSPAN session in the source and destination switches and ensure that the intermediate switches carry the RSPAN VLAN across respective VLAN trunks.

Configuring RSPAN (2)

On the source switch:

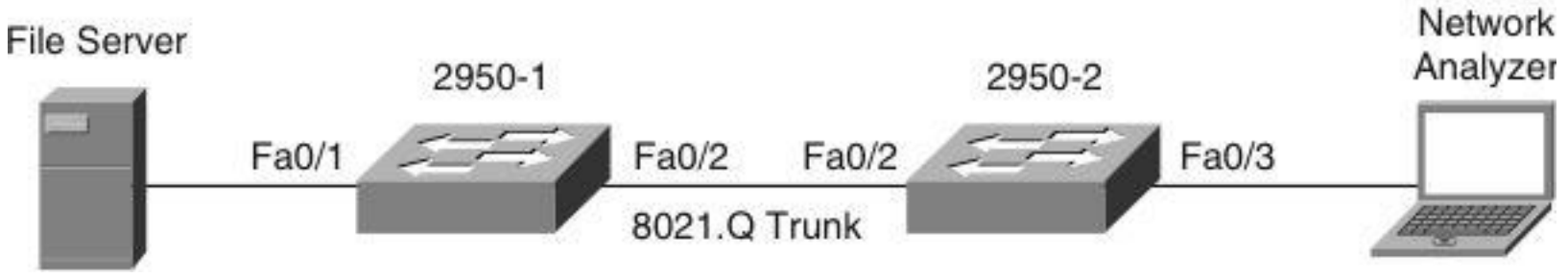
- **monitor session session source {interface** *interface-id* **| vlan** *vlan-id***}** ***[,][-] {rx*** **| tx | both}**
- **monitor session session destination remote vlan** *vlan-id*

On the destination switch:

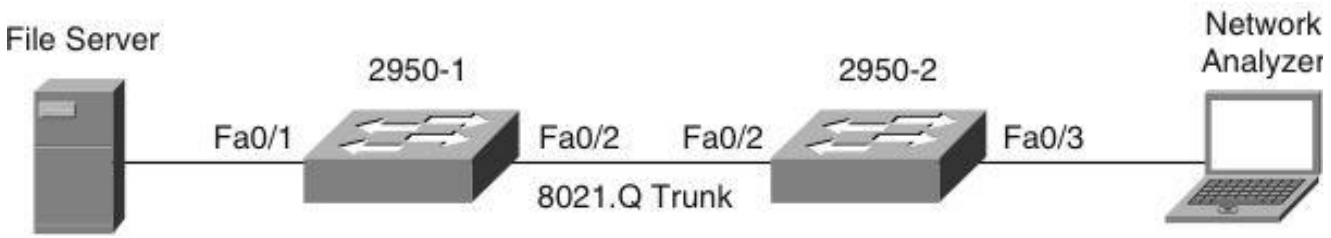
- **monitor session session source remote vlan** *vlan-id*
- **monitor session session destination interface** *interface-id* **[encapsulation {dot1q** | **isl}] [ingress vlan** *vlan-id***]**

RSPAN Configuration Example (1)

- Switch 2950-1 is the source switch for the RSPAN session and 2950-2 is the destination switch with the network analyzer.
- The Catalyst 2950 and Catalyst 2955 series switches require an additional port to be designated as the reflector port. The reflector port is used on the Catalyst 2950 switches as a way to overcome the limitation of that switch architecture for SPAN. The reflector should be left unconnected and is used internally by the Catalyst 2950 for implementing RSPAN.
- The reflector port in this example is interface FastEthernet 0/24.

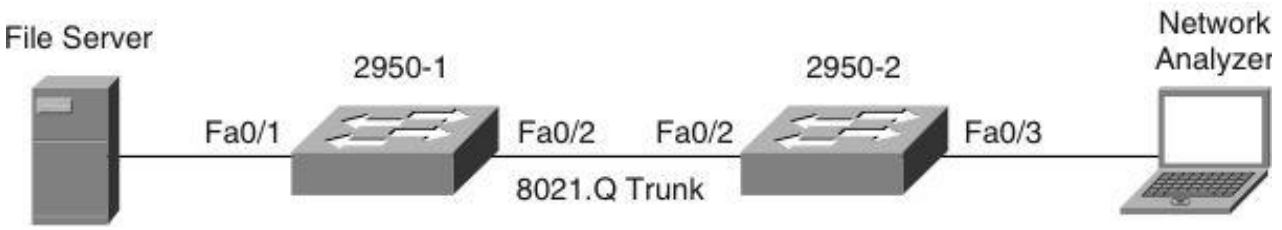


RSPAN Configuration Example (2)



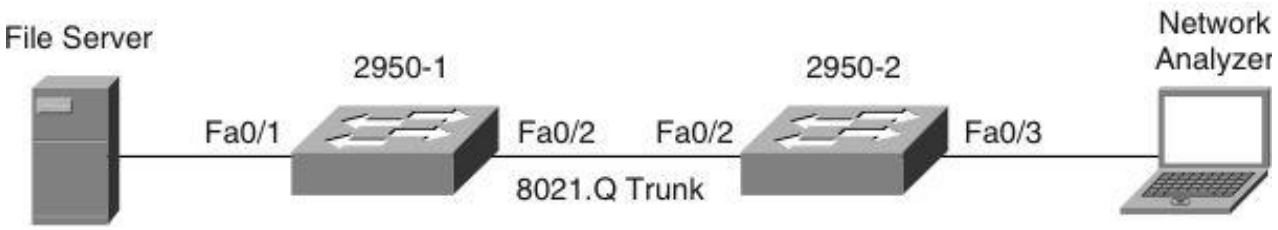

```
2950-1(config)# vlan 100
2950-1(config-vlan)# remote-span
2950-1(config-vlan)# exit
2950-1(config)# monitor session 1 source interface FastEthernet 0/1
2950-1(config)# monitor session 1 destination remote vlan 100
reflector-port FastEthernet 0/24
2950-1(config)# interface FastEthernet 0/2
2950-1(config-if)# switchport mode trunk
2950-1(config-vlan)# end


2950-2(config)# monitor session 2 source remote vlan 100
2950-2(config)# monitor session 2 destination interface FastEthernet
0/3
2950-2(config)# interface FastEthernet 0/2
2950-2(config-if)# switchport mode trunk
```

RSPAN Configuration Example (3)




```
2950-1# show monitor
Session 1
-----
Type                   : Remote Source Session
Source Ports           :
       Both            : Fa0/1
Reflector Port         : fa0/24
Dest RSPAN VLAN        : 100
2950-1# show interfaces trunk
Port   Mode   Encapsulation        Status        Native vlan
Fa0/2  on     802.1q               trunking      1
Port   Vlans allowed on trunk
Fa0/2  1-4094
Port   Vlans allowed and active in management domain
Fa0/2  1-30,100
Port   Vlans in spanning tree forwarding state and not pruned
Fa0/2  1-30,100
```

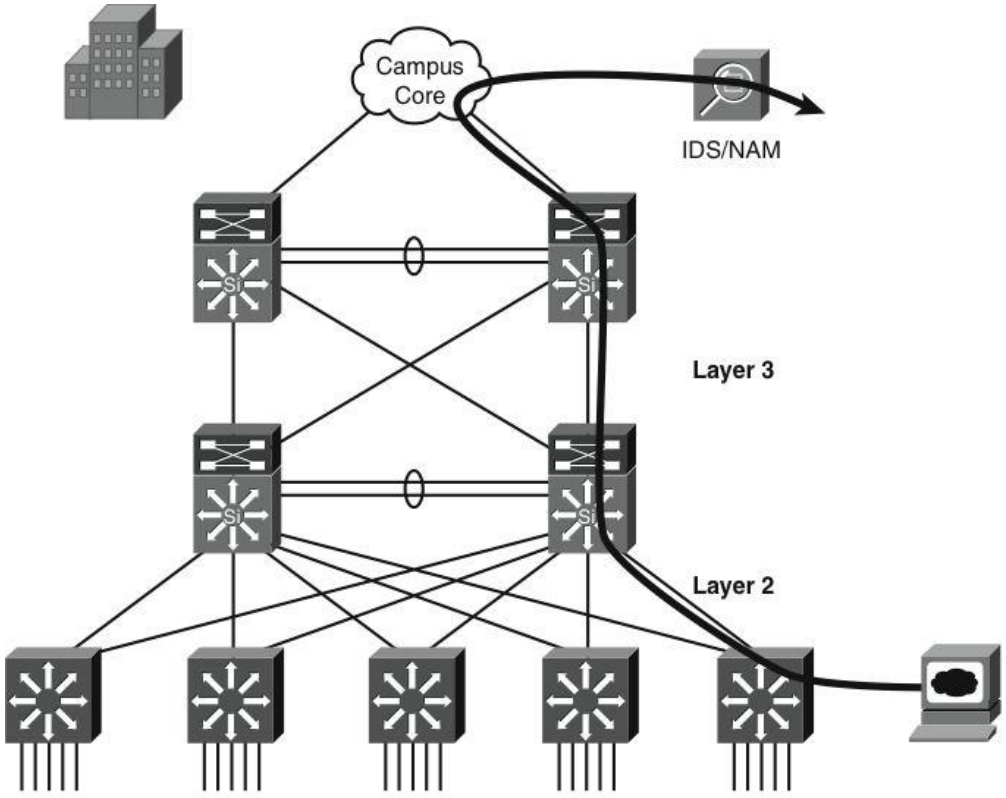
RSPAN Configuration Example (4)




```
2950-2# show interfaces trunk
Port   Mode   Encapsulation        Status        Native vlan
Fa0/2  on     802.1q               trunking      1
Port   Vlans allowed on trunk
Fa0/2  1-4094
Port   Vlans allowed and active in management domain
Fa0/2  1-30,100
Port   Vlans in spanning tree forwarding state and not pruned
Fa0/2  1-30,100
2950-2# show monitor session 2
Session 2
-----
Type                  : Remote Destination Session
Source RSPAN VLAN     : 100
Destination Ports     : Fa0/3
     Encapsulation    : Native
               Ingress : Disabled
```

Monitoring Performance with ERSPAN

- Enhanced Remote SPAN (ERSPAN) is similar to RSPAN, but it supports source ports, source VLANs, and destination ports on different switches, even across the Layer 3 boundary.



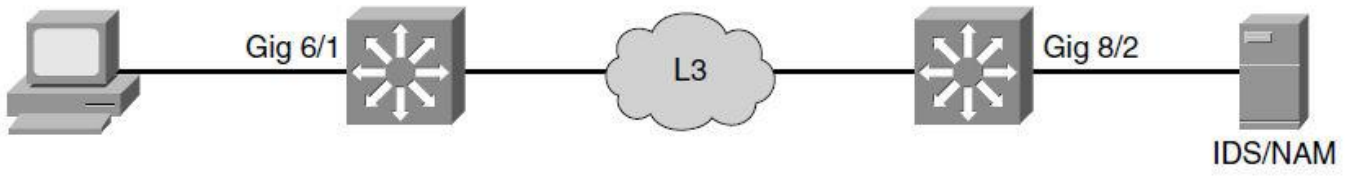
ERSPAN Guidelines

- The payload of a Layer 3 ERSPAN packet is a copied Layer 2 Ethernet frame, excluding any ISL or 802.1Q tags.
- ERSPAN adds a 50-byte header to each copied Layer 2 Ethernet frame and replaces the 4-byte cyclic redundancy check (CRC) trailer.
- ERSPAN supports jumbo frames that contain Layer 3 packets of up to 9202 bytes. If the length of the copied Layer 2 Ethernet frame is greater than 9170 bytes (9152-byte Layer 3 packet), ERSPAN truncates the copied Layer 2 Ethernet frame to create a 9202-byte ERSPAN Layer 3 packet.

Configuring ERSPAN

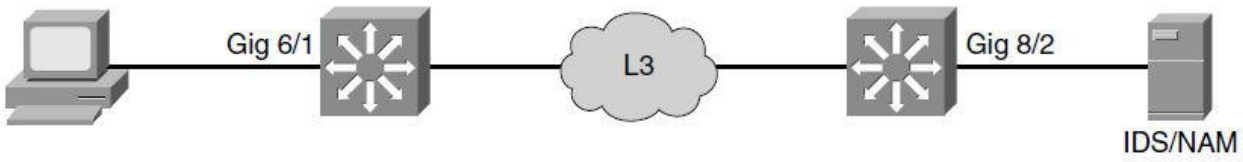
- **Step 1.** Configure the source ERSPAN session.
- **Step 2.** Configure the destination ERSPAN session on a different switch.

ERSPAN Configuration Example




```
Switch1(config)# monitor session 66 type erspan-source
Switch1(config-mon-erspan-src)# source interface gigabitethernet 6/1
Switch1(config-mon-erspan-src)# destination
Switch1(config-mon-erspan-src-dst)# ip address 10.10.10.10
Switch1(config-mon-erspan-src-dst)# origin ip address 20.20.20.200
Switch1(config-mon-erspan-src-dst)# erspan-id 111


Switch2(config)# monitor session 60 type erspan-destination
Switch2(config-erspan-dst)# destination interface gigabitethernet 8/2
Switch2(config-erspan-dst)# source
Switch2(config-erspan-dst-src)# ip address 10.10.10.10
Switch2(config-erspan-dst-src)# erspan-id 111
```

ERSPAN Verification Example (2)

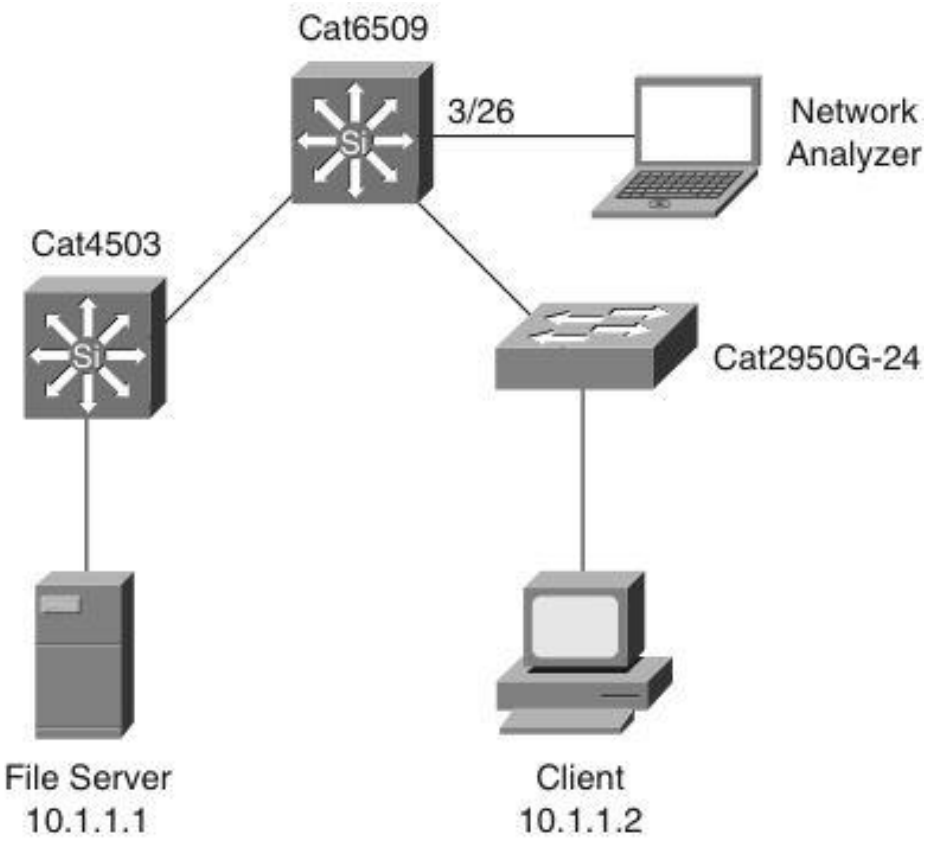



```
Switch1# show monitor session 66
Session 66
-----
Type                          : ERSPAN Source Session
Status                              : Admin Enabled
Source Ports                  :
    Both                      : Gi6/1
Destination IP Address        : 10.10.10.10
Destination ERSPAN ID               : 111
Origin IP Address             : 20.20.20.200

Switch2# show monitor session 60
Session 60
----------
Type                          : ERSPAN Destination Session
Status                              : Admin Enabled
Destination Ports             : Gi8/2
Source IP Address             : 10.10.10.10
Source ERSPAN ID              : 111
```

Monitoring Performance Using VACL's with the Capture Option

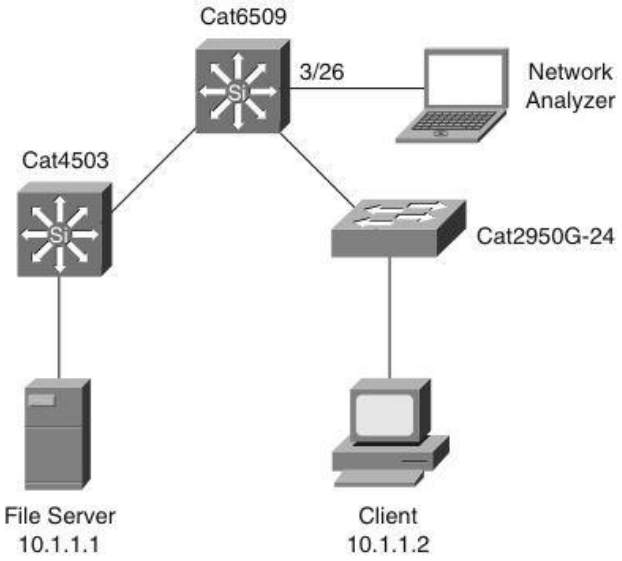
- Using VACLs with the **capture** option on a Catalyst 6500, the network analyzer receives only a copy of traffic matching the configured ACL.
- Guidelines for using the capture option in a VACL:
  - The capture port needs to be in the spanning-tree forwarding state for the VLAN.
  - The switch has no restriction on the number of capture ports.
  - The capture port captures only packets permitted by the configured ACL.
  - Capture ports transmit only traffic belonging to the capture port VLAN. To capture traffic going to many VLANs, configure the capture port as a trunk carrying the required VLANs.

Capture Option with VACL's Example (1)



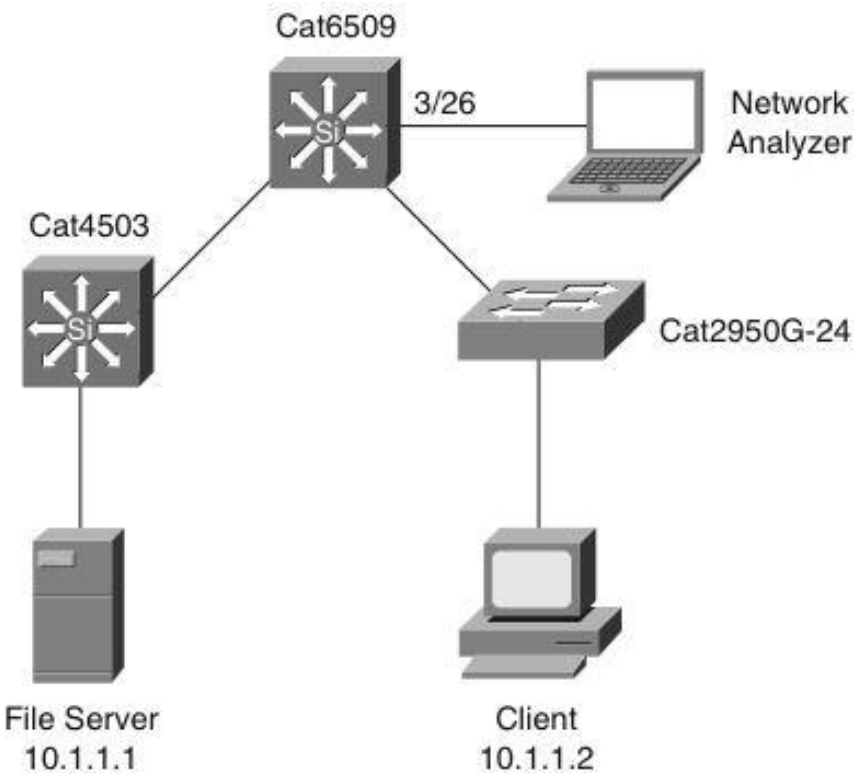
- A user is troubleshooting a session timeout between a server with IP address 10.1.1.1 and client with IP address 10.1.1.2.

Capture Option with VACL's Example (2)




```
cat6k(config)# access-list 101 permit ip host 10.1.1.1 host 10.1.1.2
cat6k(config)# access-list 101 permit ip host 10.1.1.2 host 10.1.1.1
cat6k(config)# vlan access-map SWITCHvacl
cat6k(config-access-map)# match ip address 101
cat6k(config-access-map)# action forward capture
cat6k(config-access-map)# exit
cat6k(config)# vlan filter SWITCHvacl vlan-list 1
cat6k(config)# in GigabitEthernet 3/26
cat6k(config-if)# switchport
cat6k(config-if)# switchport capture allowed vlan 1
cat6k(config-if)# switchport capture
```

Capture Option with VACL's Example (3)



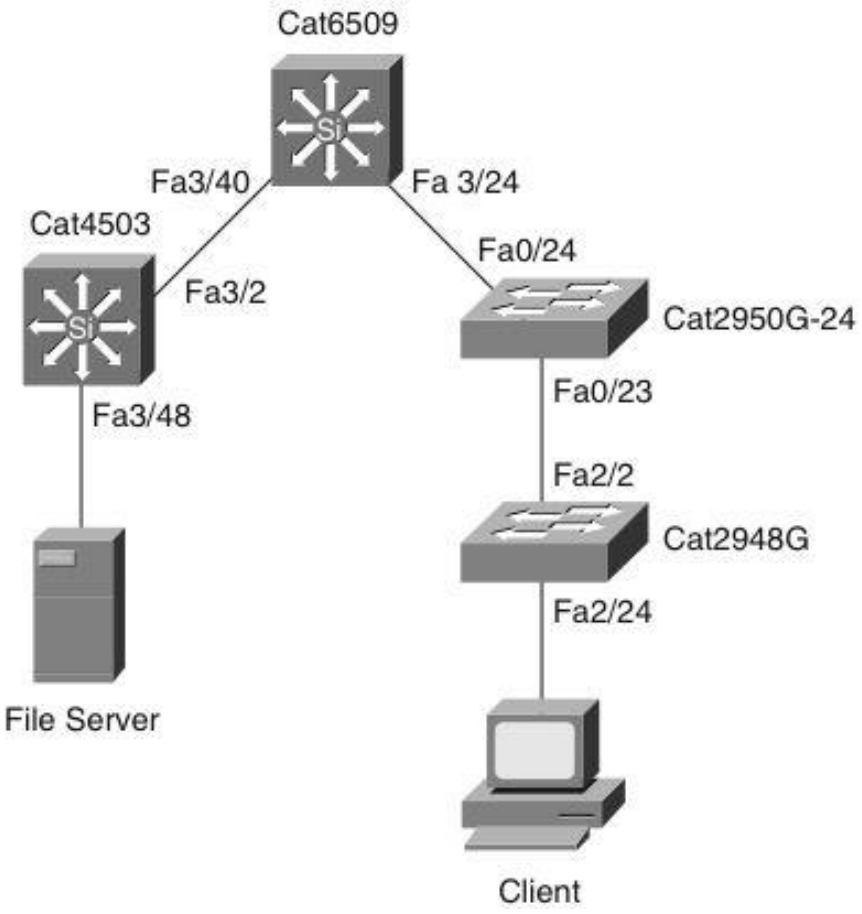

```
cat6k# show vlan access-map
Vlan access-map "SWITCHvacl" 10
        match: ip address 101
        action: forward capture
cat6k# show vlan filter
VLAN Map SWITCHvacl:
```

Troubleshooting Using L2 Traceroute

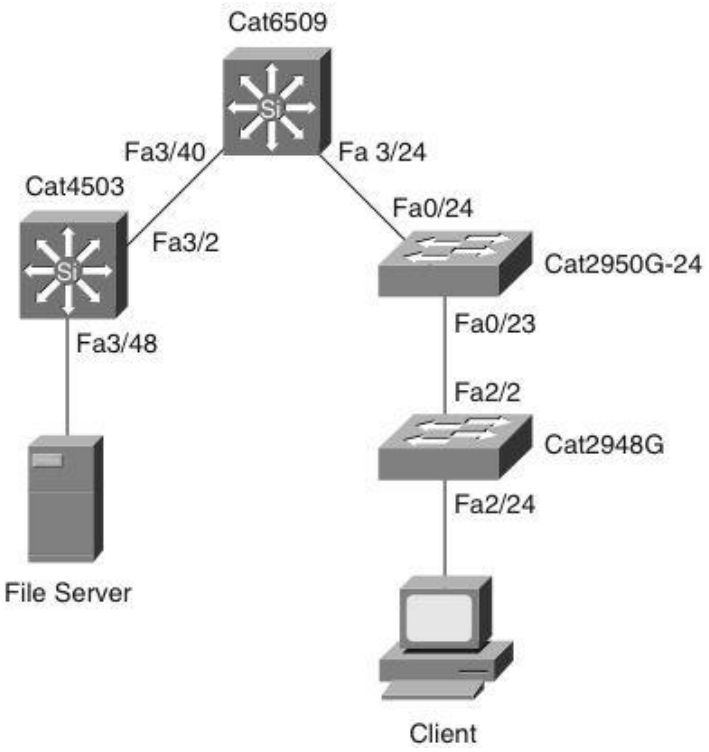
- All switches and interfaces in the network require CDP to be running and functioning properly.
- All intermediate switches between the source and device in question must support the L2 traceroute feature.

L2 Traceroute Example (1)

- A user needs to identify the performance and path on a hop-by-hop basis for a specific server and client exhibiting slow file-transfer performance, so she uses the L2 traceroute feature with the source MAC address of the server, 0000.0000.0007, to the destination MAC address of the client, 0000.0000.0011.
- To perform an L2 traceroute, she can choose any switch in the network as long as that switch has both the source and destination MAC addresses in the MAC address table. Here, she performed the L2 traceroute command on the Catalyst 2950 in the figure.



L2 Traceroute Example (2)




```
2950G# traceroute mac 0000.0000.0007 0000.0000.0011
Source 0000.0000.0007 found on 4503
4503 (14.18.2.132) : Fa3/48 => Fa3/2
6500 (14.18.2.145) : 3/40 => 3/24
2950G (14.18.2.176) : Fa0/24 => Fa0/23
2948G (14.18.2.91) : 2/2 => 2/24
Destination 0000.0000.0011 found on 2948G Layer 2 trace completed
```

Enhancing Troubleshooting and Recovery Using Cisco IOS Embedded Event Manager (EEM)

- Monitor events happening in a switch using embedded event collectors.
- Generic Online Diagnostic (GOLD) test can be tracked as an event.
- Enhances troubleshooting and recovery from network failures.

Sample Embedded Event Manager Scenarios

Event (User Configurable)	Action (User Defined)
A specific interface error crosses a user-defined threshold.	Disable the interface and bring up a backup interface.
Configuration changes are made during production hours.	Deny the configuration changes and send an email alert.
A GOLD diagnostic test fails.	Generate a custom syslog message indicating the action to take for Level 1 network operators.
A user logs into the system.	Generate a custom login message based on the user ID.
Unauthorized hardware is removed or added from the switch.	Send a page to the administrator.
It is necessary to collect data for capacity planning.	Run a user-defined set of commands to collect the capacity information at regular intervals.

Embedded Event Manager Configuration Options

- **EEM using applet** CLI: Cisco IOS CLI–based configuration that provides a limited set of actions and detection
- **EEM using Tool Command Language (TCL) script:** Provides full flexibility in defining the events and the subsequent actions

Performance Monitoring Using the Network Analysis Module (NAM) in the Catalyst 6500 Family of Switches

- Monitors and analyzes network traffic using remote network monitoring (RMON).
- Gives any web browser access to the RMON features of the NAM.
- Can monitor individual VLAN's.
- Can access link, host, protocol, and response-time statistics for capacity planning and real-time protocol monitoring.

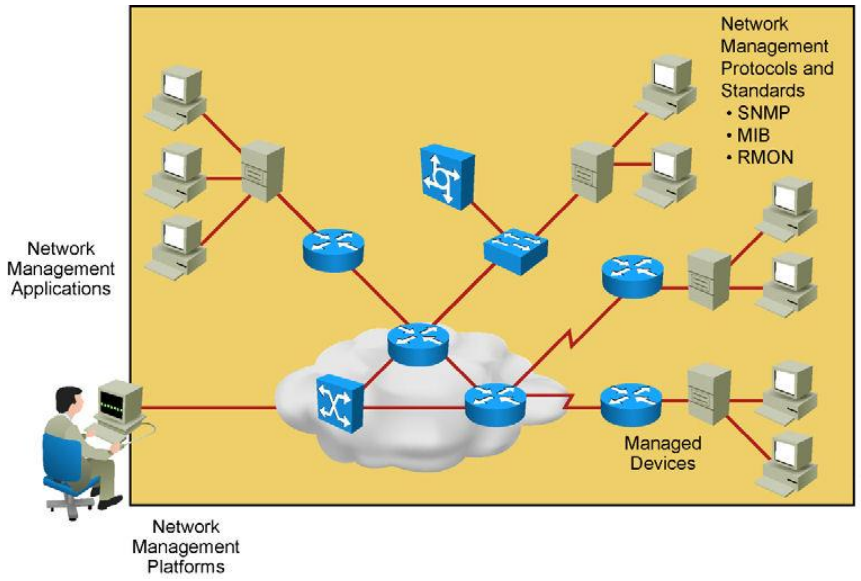
Network Analysis Module Source Support

Supports multiple simultaneous sources:

- Ethernet, Fast Ethernet, Gigabit Ethernet, trunk port, or Fast EtherChannel; SPAN or RSPAN source port; and VSPAN and VACL with the capture option.
- Locally generated NetFlow Data Export (NDE) records. The NDE feature collects individual flow statistics of the traffic switched through the switch. NDE can also export the collected information to external flow collectors such as the NetFlow FlowCollector application. The NAM is another example of such a flow collector.

Implementing Network Monitoring

Network Management Overview



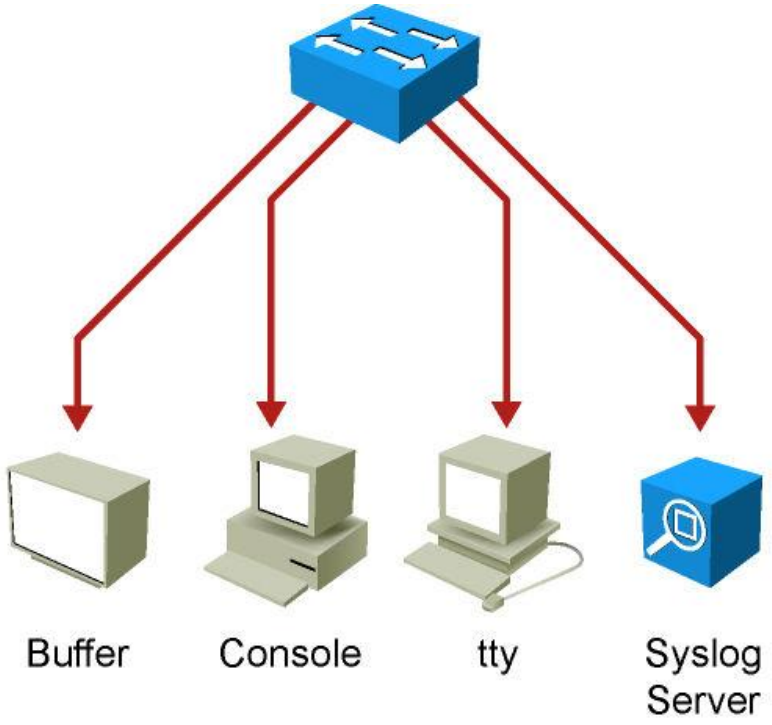
- Ability to verify the network is working well and behaving in the planned manner
- Ability to characterize the performance of the network
- Ability to understand how much traffic is flowing and where it is flowing in the network
- Ability to troubleshoot the network

Network Management Tools

- Syslog
- SNMP

Syslog

- System Message Logging
- Enables device to report error and notification messages.
- Uses UDP port 514.
- Every message contains a severity level and a facility.
- Routers, switches, application servers, firewalls, and other network appliances support syslog.



Syslog Severity Levels

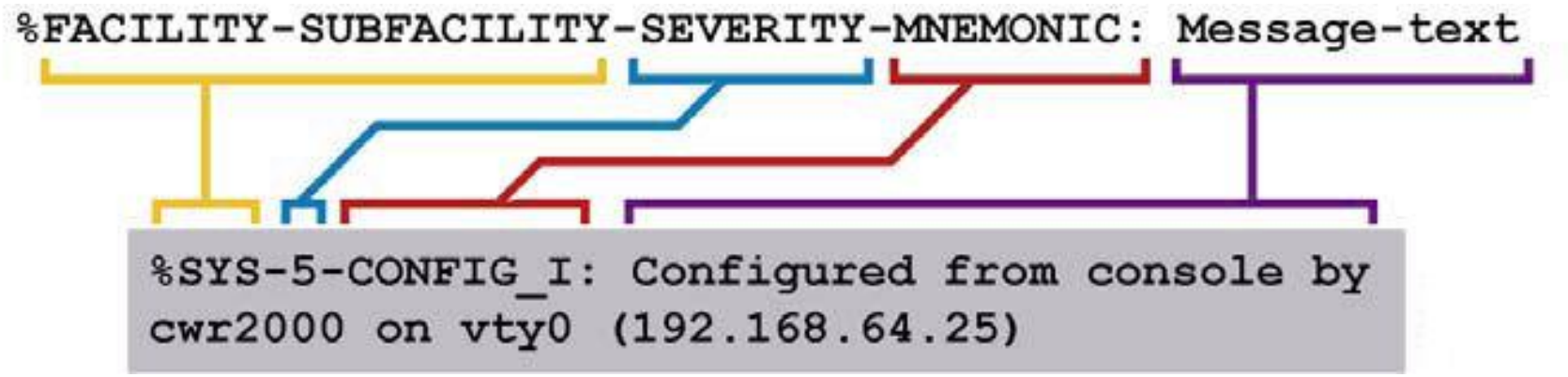
Smaller numerical levels are the more critical syslog alarms.

Syslog Severity	Severity Level
Emergency	Level 0, highest level
Alert	Level 1
Critical	Level 2
Error	Level 3
Warning	Level 4
Notice	Level 5
Informational	Level 6
Debugging	Level 7

Syslog Facilities

- Service identifiers.
- Identify and categorize system state data for error and event message reporting.
- Cisco IOS has more than 500 facilities.
- Most common syslog facilities:
  - IP
  - OSPF
  - SYS operating system
  - IP Security (IPsec)
  - Route Switch Processor (RSP)
  - Interface (IF)

Syslog Message Format



- System messages begin with a percent sign (%)
- **Facility:** A code consisting of two or more uppercase letters that indicates the hardware device, protocol, or a module of the system software.
- **Severity**: A single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation.
- **Mnemonic:** A code that uniquely identifies the error message.
- **Message-text:** A text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space.

Sample Syslog Messages

```
08:01:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/5, changed state to up
08:01:23: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(1) 1: Neighbor 10.1.1.1
(Vlan1) is up: new adjacency
08:02:31: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state
to up
08:18:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/5, changed state to down
08:18:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/5, changed state to up
08:18:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to down
08:18:24: %ILPOWER-5-IEEE_DISCONNECT: Interface Fa0/2: PD removed
08:18:26: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state
to down
08:19:49: %ILPOWER-7-DETECT: Interface Fa0/2: Power Device detected:
Cisco PD
08:19:53: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state
to up
08:19:53: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to up
```

Configuring Syslog (1)

- To configure a syslog server, use the **logging** *ip_addr* global configuration command.
- To which severity levels of messages are sent to the syslog server, use the global configuration command **logging trap** *level*.

```
Switch(config)# logging trap ?
<0-7>           Logging severity level
alerts          Immediate action needed                 (severity=1)
critical        Critical conditions                     (severity=2)
debugging       Debugging messages                      (severity=7)
emergencies     System is unusable                      (severity=0)
errors          Error conditions                        (severity=3)
informational   Informational messages                  (severity=6)
notifications   Normal but significant conditions      (severity=5)
warnings        Warning conditions                      (severity=4)
```

Configuring Syslog (2)

- To configure logging to the buffer of the local switch, use the command **logging buffered.**

```
Switch(config)# logging buffered ?
<0-7>                Logging severity level
<4096-2147483647>    Logging buffer size
alerts               Immediate action needed                 (severity=1)
critical             Critical conditions                     (severity=2)
debugging            Debugging messages                      (severity=7)
discriminator        Establish MD-Buffer association
emergencies          System is unusable                      (severity=0)
errors               Error conditions                        (severity=3)
informational        Informational messages                  (severity=6)
notifications        Normal but significant conditions       (severity=5)
warnings             Warning conditions                      (severity=4)
xml                  Enable logging in XML to XML logging buffer
```

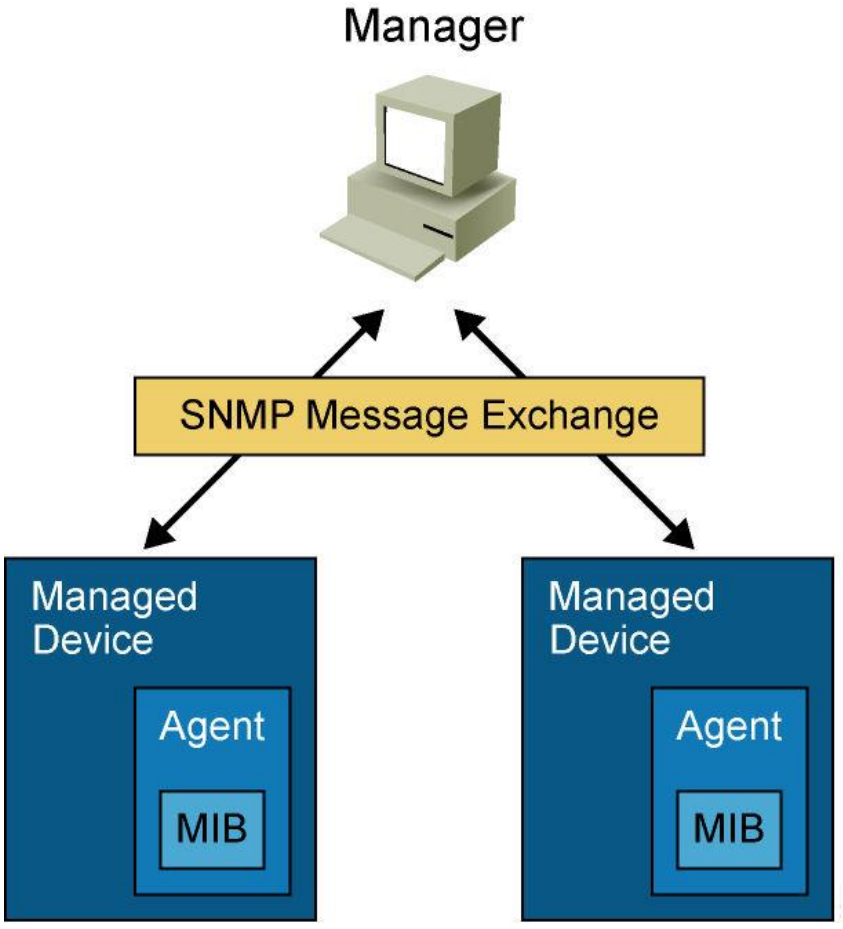
Verifying Syslog Configuration

- Use the **show logging** command to display the content of the local log files.
- Use the pipe argument (|) in combination with keywords such as **include** or **begin** to filter the output.

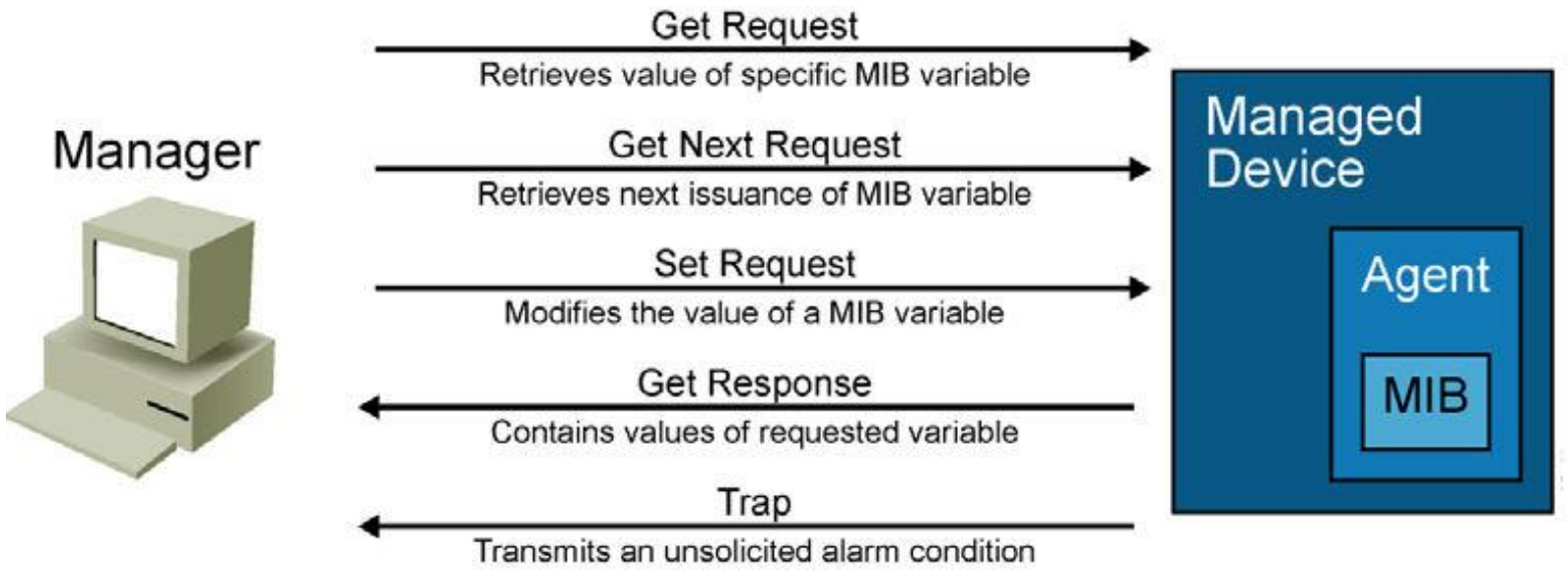
```
Switch# show logging | include LINK-3
2d20h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
2d20h: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
2d20h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Switch# show logging | begin %DUAL
2d22h: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(10) 10: Neighbor 10.1.253.13
(FastEthernet0/11) is down: interface down
2d22h: %LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to down
2d22h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11,
changed state to down
```

SNMP

- SNMP has three elements:
  - Network Management Application (SNMP Manager)
  - SNMP Agents (running inside a managed device)
  - MIB Database object that describes the information in a predetermined format that the agent can use to populate the data.
- SNMP defines how management information is exchanged between network management applications and management agents.



SNMP Version 1



- SNMP version 1 (SNMPv1), defined in RFC 1157. Five basic SNMP messages the network manager uses to transfer data from agents that reside on managed devices:
  - **Get Request:** Used to request the value of a specific MIB variable from the agent.
  - **Get Next Request**: Used after the initial Get Request to retrieve the next object instance from a table or a list.
  - **Set Request**: Used to set a MIB variable on an agent.
  - **Get Response**: Used by an agent to respond to a Get Request or Get Next Request from a manager.
  - **Trap**: Used by an agent to transmit an unsolicited alarm to the manager. An agent sends a Trap message when a certain condition occurs, such as a change in the state of a device, a device or component failure, or an agent initialization or restart.

SNMP Version 2

- SNMPv2 introduced with RFC 1441, but members of IETF subcommittee could not agree on the security and administrative sections of SNMPv2 specification. There were several attempts to achieve acceptance of SNMPv2 through release of experimental modified versions.
- Community-based SNMPv2 (SNMPv2C), defined in RFC 1901, is most common implementation. SNMPv2C deploys administrative framework defined in SNMPv1, which uses read/write community strings for administrative access.
- SNMPv2 introduces two new message types:
  - **Get Bulk Request**: Reduces repetitive requests and replies and improves performance when retrieving large amounts of data (e.g., tables).
  - **Inform Request**: Alert an SNMP manager of specific conditions. Unlike unconfirmed SNMP Trap messages, NMS acknowledges Inform Request by sending an Inform Response message back to requesting device.

SNMP Version 3

- SNMPv3 is described in RFCs 3410 through 3415. It adds methods to ensure the secure transmission of critical data between managed devices.
- SNMPv3 introduces three levels of security:
  - **noAuthNoPriv:** No authentication is required, and no privacy (encryption) is provided.
  - **authNoPriv:** Authentication is based on Hash-based Message Authentication Code with Message Digest 5 (HMAC-MD5) or Hash-based Message Authentication Code with Secure Hash Algorithm (HMAC-SHA). No encryption is provided.
  - **authPriv**: In addition to authentication, Cipher Block Chaining-Data Encryption Standard (CBC-DES) encryption is used as the privacy protocol.
- Security levels implemented for each security model determine which SNMP objects a user can access for reading, writing, or creating and list of notifications that its users can receive.

SNMP Recommendations

- SNMPv1 and SNMPv2 use community strings in clear text and so should be carefully chosen to ensure they are not trivial.
- Community strings should be changed at regular intervals and in accordance with network security policies. For example, the strings should be changed when a network administrator changes roles or leaves the company.
- If SNMP is used only to monitor devices, use read-only communities.
- Ensure that SNMP messages do not spread beyond the management consoles. Use access-lists to prevent SNMP messages from going beyond the required devices and on the monitored devices to limit access for management systems only.
- SNMPv3 is recommended because it provides authentication and encryption.

Configuring SNMP

- Step 1. Configure SNMP access lists.
- Step 2. Configure SNMP community strings.
- Step 3. Configure SNMP trap receiver.
- Step 4. Configure SNMPv3 user.

```
Switch(config)# access-list 100 permit ip 10.1.1.0 0.0.0.255 any
Switch(config)# snmp-server community cisco RO 100
Switch(config)# snmp-server community xyz123 RW 100
Switch(config)# snmp-server host 10.1.1.27 version 2c cisco
Switch(config)# snmp-server host 10.1.1.111 version 1 xyz123
Switch(config)# snmp-server host 10.1.1.33 cisco
```

Chapter 5 Summary (1)

- Security is a primary concern in maintaining a secure, stable, and uninterrupted network.
- Network security goes far beyond the information in this chapter and includes topics such as intrusion detection, firewalls, virus protection, and operating system patching.
- Unless you recognize and understand the importance of network security, your network is at risk.
- The following list summarizes the aspects and recommended practices for avoiding, limiting, and minimizing network vulnerabilities strictly related to Catalyst switches as a single network entity:

Chapter 5 Summary (2)

- Layer 2 attacks vary in nature and include spoofing attacks, VLAN attacks, MAC flood attacks, and switch device attacks, among others.
- Use strong passwords with SSH access instead of Telnet exclusively to Cisco network devices.
- Disable unused services such as TCP and UDP small services where appropriate.
- Use AAA for centralized authentication, authorization, and accounting of network devices and remote access.
- Use an access control feature such as 802.1X or port security to restrict workstation access to Catalyst switches.
- Use DHCP snooping to prevent rogue DHCP servers on the network.
- Use IPSG and DAI with DHCP snooping to prevent IP address and ARP spoofing attacks.
- Apply management ACLs to limit remote access to Cisco network devices.
- Apply data plane security ACLs to filter unwarranted traffic in the network.
- Use private VLANs where appropriate to limit communication in specific VLANs.
- Use troubleshooting and monitoring tools such as SPAN, VSPAN, RSPAN, ERSPAN,
- L2 Traceroute, EEM, and NAM to ensure proper network performance.

Chapter 5 Labs

- **SW-LAB-3.1**
  - **Securing Network Switches**
- **SW-LAB-3.2**
  - **Protecting Attacks**
- **SW-LAB-3.3**
  - **Securing VLANs with Private VLAN's, RACL's, and VACL's**
- **SW-LAB-3.4**
  - **SPAN, Remote SPAN**
- **SW-LAB-3.5**
  - **Syslog, SNMP**
- **SW-LAB-3.6**
  - **RADIUS**

Q&A