Campus Network Security

CCNP SWITCH: Implementing Cisco IP Switched Networks

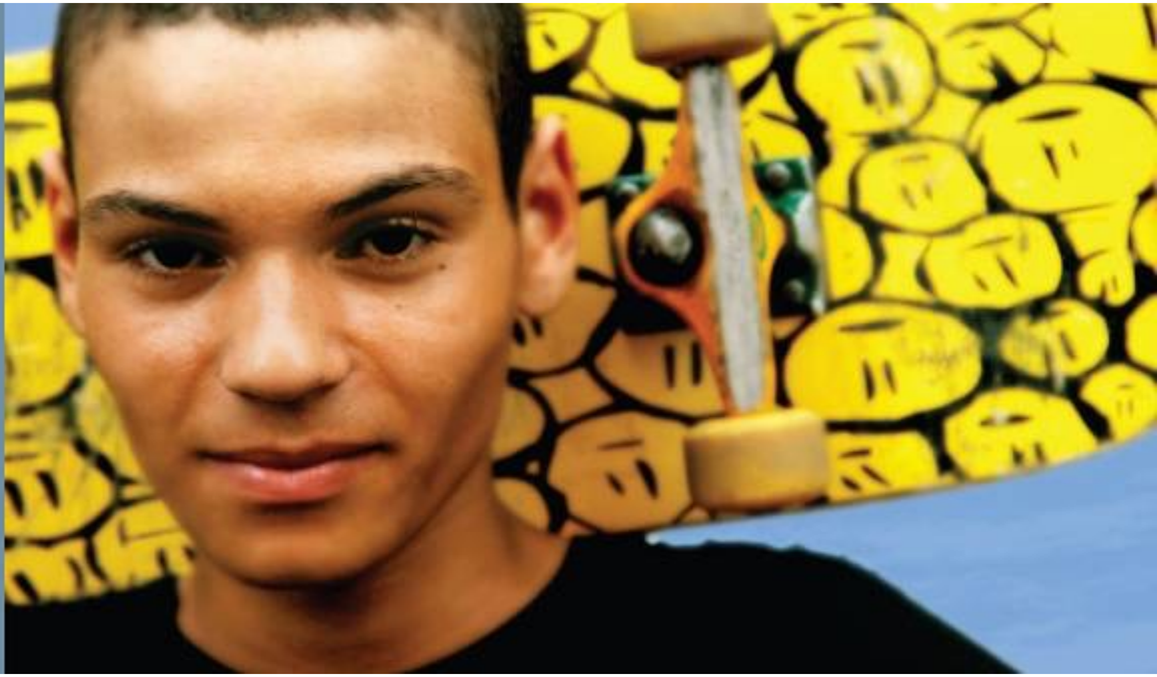
Cisco | Networking Academy®
Mind Wide Open™

Chapter 10 Objectives

This chapter covers the following topics:

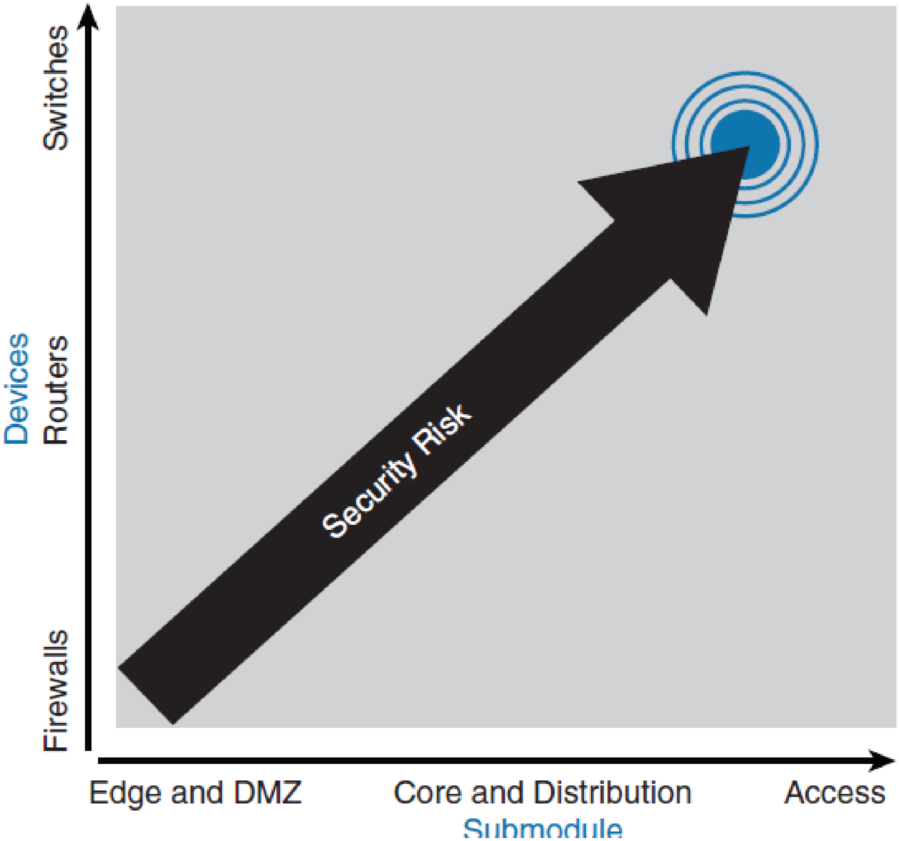
- Overview of switch security issues
- Required best practices for basic security protection on Catalyst switches
- Campus network vulnerabilities
- Port security
- Storm control
- Mitigating spoofing attacks
- DHCP snooping, IP Source Guard, and dynamic ARP inspection
- Securing VLAN trunks
- Private VLANs

Overview of Switch Security Issues



Overview of Switch Security Issues

- Most of the industry attention focuses on security attacks from outside the walls of an organization and at the upper OSI layers.
- The default state of networking equipment highlights this focus on external protection and internal open communication.
- Many security features are available for switches and routers, but they must be enabled to be effective



Overview of Switch Security Issues

Reasons exist for strong protection of the enterprise campus infrastructure

- Relying on the security that has been established at the enterprise edge fails as soon as security there is compromised. Having several layers of security increases the protection of the enterprise campus, where the most strategic assets usually reside.
- If the enterprise allows visitors into its buildings, an attacker can potentially gain physical access to devices in the enterprise campus. Relying on physical security is not enough.
- Very often, external access does not stop at the enterprise edge. Applications require at least an indirect access to the enterprise campus resources, which means that strong campus network security is also necessary.
- Public and hybrid cloud architectures pose new risks. Even if the cloud is secure, attacks from the inside can ultimately compromise the cloud.

Cisco Switch Security Configuration Best Practices

Cisco Switch Security Configuration Best Practices

- **Secure passwords**
  - The **`enable password`** command employs weak encryption.
  - Use **`enable secret`** whenever possible.
  - Use the **`service password-encryption`** global configuration command to encrypt all passwords that cannot be encrypted using strong authentication.
  - Having external AAA.
- **Leverage system banners**
  - The goal is to warn unauthorized users that their activities could be grounds for persecution.
  - Use the **`banner login`** command.
- **Secure console access**
  - Even though switches usually reside in locked cabinets and access-controlled data centers, it is a best practice to configure authentication on any console.

Cisco Switch Security Configuration Best Practices

- **Secure vty access**
  - Always secure all vty lines on a device.
  - Configure access lists to limit access from source IP addresses of potential administrative users who try to access the device remotely.
  - `access-list 1 permit 10.0.0.234`
  - `access-list 1 permit 10.0.0.235`
  - `line vty 0 15`
  - `access-class 1 in`
- **Secure the embedded web interface**
  - If you are not using web interface to manage a switch, disable its web interface using **`no ip http server`** command.
  - If you do decide to use the switch's web interface, use HTTPS. To enable HTTPS, use the **`ip http secure server`** global configuration command.
  - If you do decide to use the switch's web interface, use access lists to limit source addresses that can access the HTTPS interface.
  - `access-list 1 permit 10.100.50.0 0.0.0.255`
  - `ip http secure server`
  - `ip http access-class 1`

Cisco Switch Security Configuration Best Practices

- **Always leverage Secure Shell (SSH) and ensure that the Telnet server is disabled**
  - Telnet is easy to use but not secure. All text that is sent through a Telnet session is passed in clear text.
  - SSH uses strong encryption to secure session data. You should use the highest SSH version available on the device.
- **Secure SNMP access**
  - If you do not need the write access through SNMP, disable it.
  - It is always recommended to exclusively use SNMPv3, which leverages secure authentication.

Cisco Switch Security Configuration Best Practices

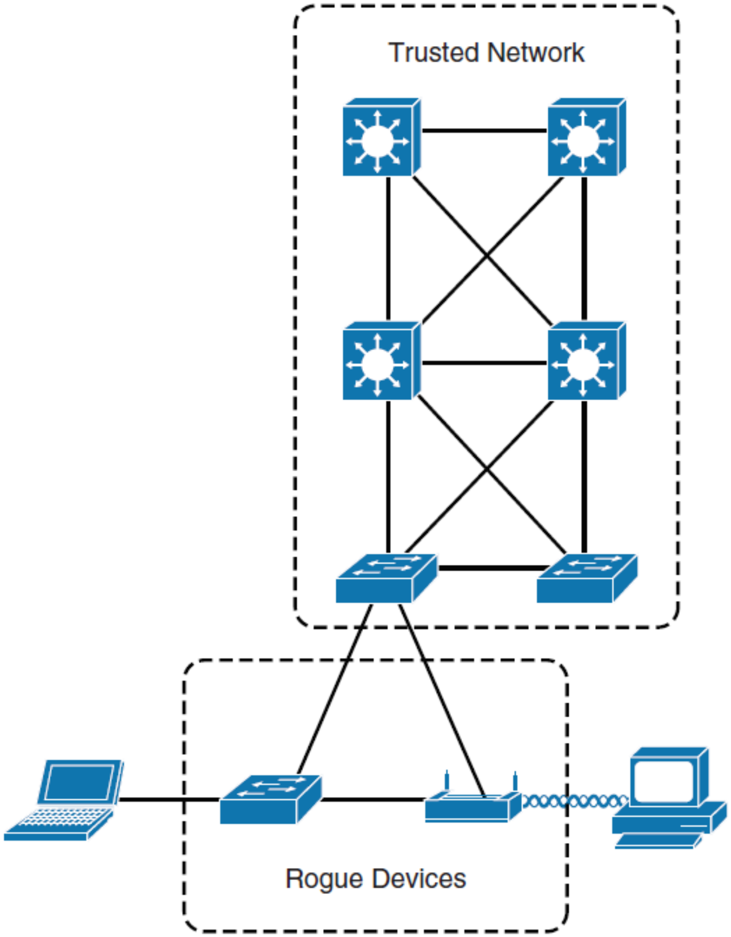
- **Secure STP operation**
  - You should always **enable the BPDU Guard** feature on any access switch ports.
  - Do not ever configure BPDU Guard and BPDU Filter on the same port. If you do, only BPDU Filter will take effect.
- **Secure Cisco Discovery Protocol (CDP)**
  - As a rule, all Cisco devices have CDP enabled on all ports by default. Disable CDP on ports that connect to outside networks.
  - In addition, always disable CDP on end-user access ports.
  - CDP advertisements are sent in clear text, and you cannot configure authentication.

Cisco Switch Security Configuration Best Practices

- **Secure unused switch ports**
  - All unused switch ports should be shut down to prevent unauthorized users from connecting to your network.
  - All user ports should be configured with **`switchport mode access`** command.
  - Place all unused ports into an isolated or bogus VLAN.

Campus Network Vulnerabilities

Rogue Access



- Rogue access comes in several forms.
- These rogue devices can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall.
- Because employees generally do not enable any security settings on the rogue AP, it is easy for unauthorized users to use the AP to intercept network traffic and hijack client sessions.

Switch Vulnerabilities

Attacks that are launched against switches and at Layer 2 can be grouped as follows:

- MAC layer attacks
- VLAN attacks
- Spoofing attacks
- Attacks on switch devices

MAC Layer Attacks

MAC Address Flooding

- Frames with unique, invalid source MAC addresses flood the switch, exhausting the content-addressable memory (CAM) table space, disallowing new entries from valid hosts.
- Traffic to valid hosts is then flooded out all ports.

- Mitigation
  - Port security.
  - MAC address VLAN access maps.

VLAN Attacks

VLAN Hopping

- VLAN Hopping is an attack where the attacker is able to send traffic from one VLAN into another. There are two different methods to accomplish this: **Double tags, Switch spoofing(DTP packets)**.

- Mitigation
  - Tighten up trunk configurations and the negotiation state of unused ports. Shut down unused ports. Place unused ports in a common VLAN.

Attacks Between Devices on a Common VLAN

- Devices may need protection from one another, even though they are on a common VLAN. This is especially true about service provider segments that support devices from multiple customers.

- Mitigation
  - Implement private VLANs (PVLANs).

Spoofing Attacks

DHCP Starvation and DHCP Spoofing

- An attacking device can exhaust the address space available to the DHCP servers for a time period or establish itself as a DHCP server in man-in-the-middle attacks.

- Mitigation
  - Use DHCP snooping.

Spanning-tree Compromises

- Attacking device spoofs the root bridge in the Spanning Tree Protocol (STP) topology. If successful, the network attacker can see various frames.

- Mitigation
  - Proactively configure the primary and backup root devices.
  - Enable Root Guard.

Spoofing Attacks

MAC Spoofing

- Attacking device spoofs the MAC address of a valid host currently in the CAM table. The switch then forwards to the attacking device any frames that are destined for the valid host.

- Mitigation
  - Use DHCP snooping, port security.

Address Resolution Protocol (ARP) spoofing

- Attacking device crafts Address Resolution Protocol (ARP) replies intended for valid hosts. The MAC address of the attacking device then becomes the destination address that is found in the Layer 2 frames that were sent by the valid network device.

- Mitigation
  - Use DAI.
  - Use DHCP snooping, port security.

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 to divulge network topology information.

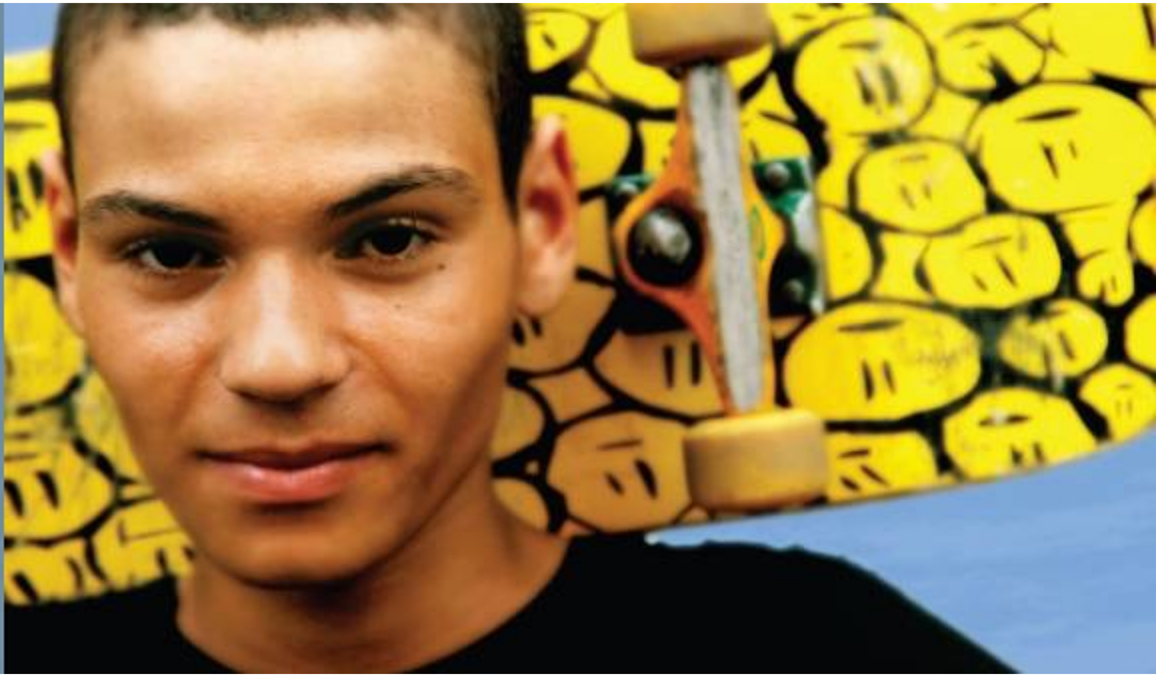
- Mitigation
  - Disable Cisco Discovery Protocol on all ports where it is not intentionally used.

SSH Protocol and Telnet Attacks

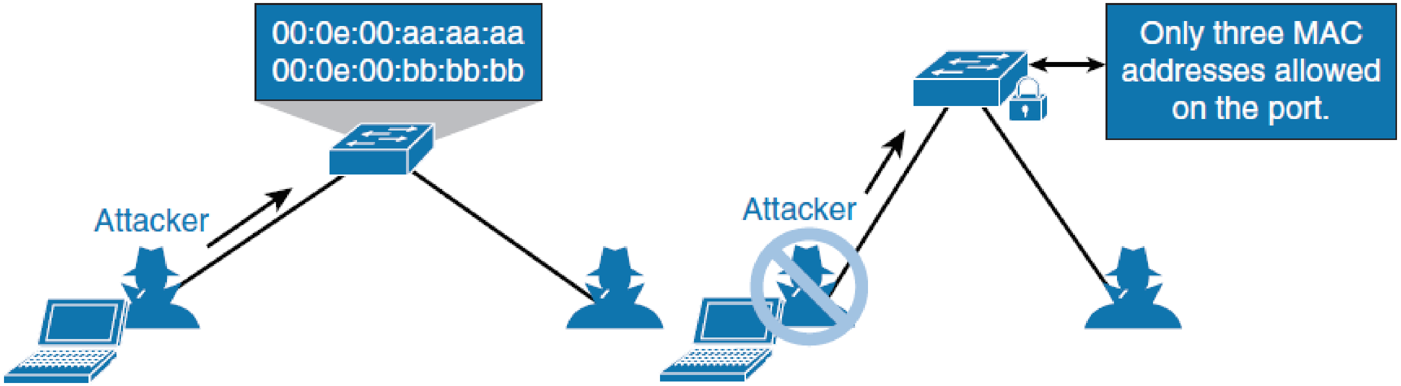
- Telnet packets can be read in clear text. SSH is an option, but it has security issues in Version 1.

- Mitigation
  - Use SSH Version 2.
  - Use Telnet with vty ACLs.

Introducing Port Security



Introducing Port Security



- Port security restricts a switch port to a specific set or number of MAC addresses.
- Those addresses can be learned dynamically or configured statically.
- The port will then provide access to frames from only those addresses.

Port Security Process

- **1. Configure port security.**
  - Configure port security to allow only the desired number of connections on the port.
  - Configure an entry for each of these allowed MAC addresses.
  - This configuration, in effect, populates the MAC address table with new 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.

Port Security Process (cont)

- 3. **New addresses are not allowed to create new MAC address table entries**.
  - When frames with a nonallowed 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 nonallowed frames.**
  - The switch will disallow access to the port and take one of these configuration-dependent actions: the entire switch port can be disabled, access can be denied for that MAC address only and a log error can be generated, or access can be denied for that MAC address but without generating a log message.

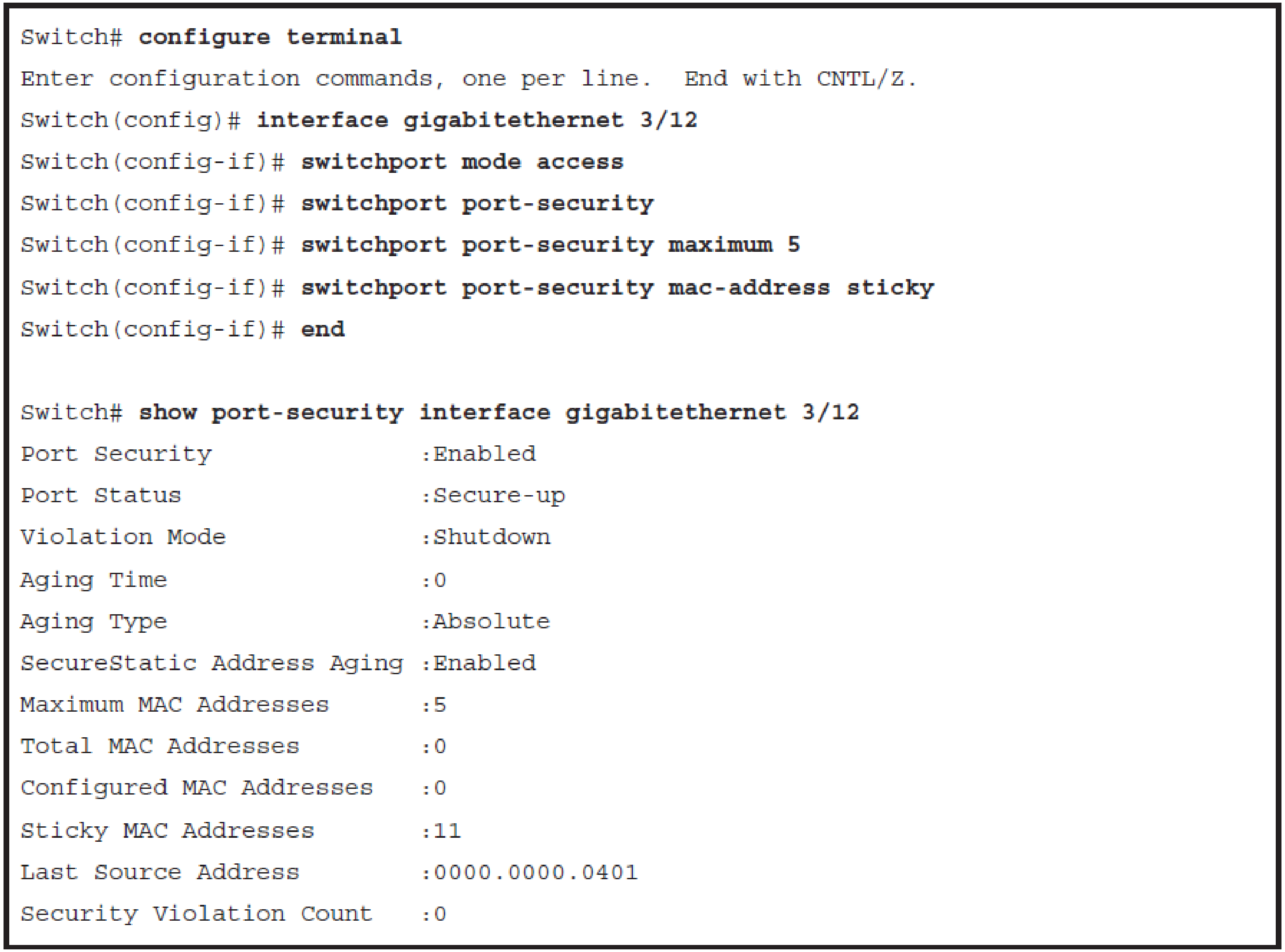
Port Security Configuration

- **`switchport port-security maximum`** ***`value`***
  - Optionally sets the maximum number of secure MAC addresses for the interface. The range is 1 to 3072; the default is 1.
- **`switchport port-security violation { restrict | shutdown }`**
  - Optionally sets the violation mode, the action to be taken when a security violation is detected, as one of these:
    - **restrict** A port security violation restricts data and causes the SecurityViolation counter to increment and send an SNMP trap notification.
    - **shutdown** The interface is err-disabled when a portsecurity violation occurs.
- **`switchport port-security limit rate invalid-source-mac`**
  - Sets the rate limit for bad packets.

Port Security Configuration (cont)

- **`switchport port-security mac-address`** ***`mac-address`***
  - Optionally enters a secure MAC address for the interface.
  - You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.
- **`switchport port-security mac-address sticky`**
  - Optionally enables sticky learning on the interface.

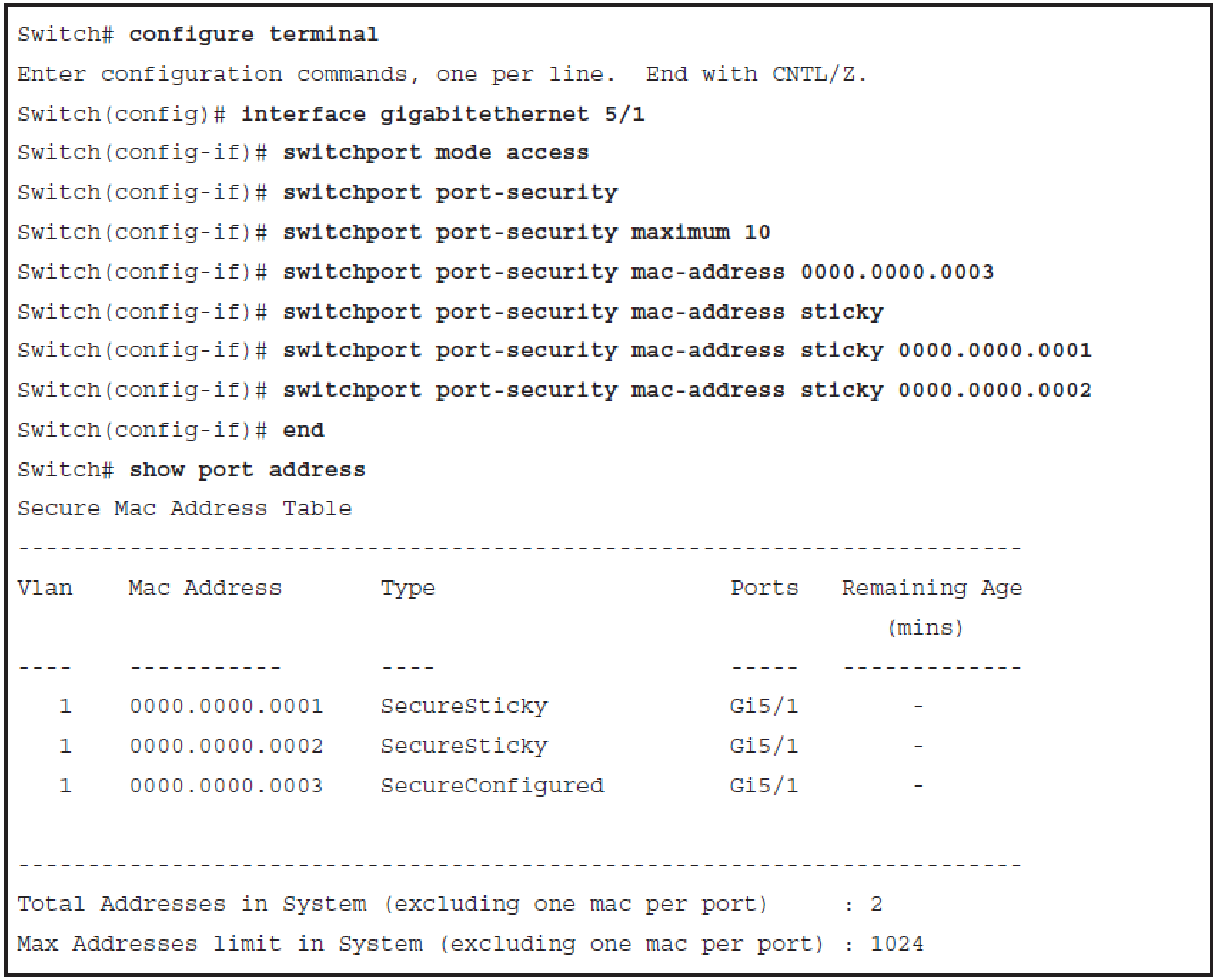
Port Security Example



```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet 3/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end

Switch# show port-security interface gigabitethernet 3/12
Port Security                :Enabled
Port Status                  :Secure-up
Violation Mode               :Shutdown
Aging Time                   :0
Aging Type                   :Absolute
SecureStatic Address Aging   :Enabled
Maximum MAC Addresses        :5
Total MAC Addresses          :0
Configured MAC Addresses     :0
Sticky MAC Addresses         :11
Last Source Address          :0000.0000.0401
Security Violation Count     :0
```

Port Security Example II



```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet 5/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 10
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# end
Switch# show port address
Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                     Ports    Remaining Age
                                                               (mins)
----    -----------       ----                     -----    -------------
   1    0000.0000.0001    SecureSticky             Gi5/1         -
   1    0000.0000.0002    SecureSticky             Gi5/1         -
   1    0000.0000.0003    SecureConfigured         Gi5/1         -


------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 2
Max Addresses limit in System (excluding one mac per port) : 1024
```

Port Error Conditions

The following list highlights the most common situations where a port will go into the err-disabled state:

- **Port security violation**
  - When an invalid MAC address is learned on a port or too many MAC addresses, the switch can optionally place the port into the err-disabled state.
- **Spanning-tree BPDU guard violation**
  - When you have PortFast configured in combination with BPDU Guard
- **EtherChannel misconfiguration**
  - All parameters have to be the same for all ports on both sides of the bundle
- **Duplex mismatch**
  - Duplex mode has to be the same on both sides of the link;

Port Error Conditions (cont)

- **UDLD condition**
  - Unidirectional Link Detection (UDLD) ensures that the link is bidirectional at all times; so when it detects a unidirectional link, it places the port into the err-disabled state.
- **Spanning-tree Root Guard**
  - If a Root Guard-enabled port receives a superior BPDU from those sent by the current root bridge
- **Link flapping**
  - When link state is flapping between the up and down states, the port is placed into the err-disabled state.
- **Other reasons**
  - Other reasons include late collision detection, Layer 2 Tunneling Protocol Guard, DHCP snooping rate-limit, incorrect gigabit interface convert (GBIC), and ARP inspection.

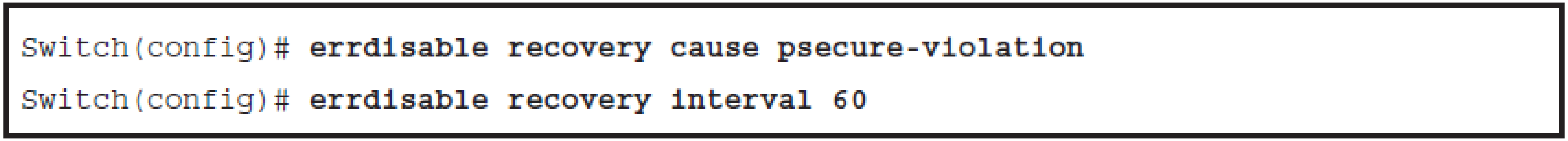
Err-Disable Ports

- Err-disabled detection is enabled for all of these causes by default.
- You can configure other reasons to trigger the port being disabled.
- Use the following command to specify the causes:

```
Switch(config)# errdisable detect cause [ all | cause-name ]
```

Err-Disabled Automatic Recovery

- Once the root cause of the err-disabled state is removed, an err-disabled port can become operational after a **`shut / no shut`**.
- Because the error condition is no longer present, the trigger for err-disable will not occur.
- Therefore, to reduce the administrative overhead, the switch port can be configured to be automatically reenabled after a specified time.
- Of course, if the error condition is still present, the port will immediately go back to the err-disabled state.



```
Switch(config)# errdisable recovery cause psecure-violation
Switch(config)# errdisable recovery interval 60
```

Port Access Lists

- Port access lists (PACLs) are yet another way to apply security in the campus network.
- Standard access control lists (ACLs) are applied to traffic passing through the Layer 3 interface.
- The PACL feature provides the ability to perform access control on a specific Layer 2 port.
- A Layer 2 port is a physical access or trunk port that belongs to a VLAN.
- The port ACL feature is supported only in hardware. (Port ACLs are not applied to any packets routed in software.)
- The PACL feature does not affect Layer 2 control packets, such as CDP, VTP, DTP, and STP, received on the port.

Port Access Lists

- There are two types of PACL:
- **IP access list**
  - Filters IPv4 and IPv6 packets on a Layer 2 port.
- **MAC access list**
  - Filters packets that are of an unsupported type (not IP, ARP, or MPLS) based on the fields of the Ethernet frame.
  - A MAC access list is *not applied* to IP, MPLS, or ARP messages.
  - You can define only named MAC access lists.

Port Access Lists

- PACLs interaction with other types of ACLs depends on the configured mode:
  - In **prefer port mode** , the PACL takes effect and overrides the effect of other ACLs. This mode is the only mode that is allowed when applying PACL on a trunk.
  - In **merge mode** , PACLs, VACLs, and standard ACLs are merged in the ingress direction. This is the default mode.
- IP and MAC ACLs can be applied to Layer 2 physical interfaces. Standard (numbered, named) and extended (numbered, named) IP ACLs and extended named MAC ACLs are supported.

Port Access Lists

Commands to configure a MAC ACL and apply it to a Layer 2 interface:

- SW(config)# **mac access-list extended** *acl-name*
- SW(config-ext-macl)# **permit host** [*source-mac* | **any**] [*destination-mac* | **any**]
- SW(config-ext-macl)# **interface** *interface-slot/number*
- SW(config-if)# **mac access-group** *acl-name* **in**

Commands to configure an IP ACL and apply it to a Layer 2 interface:

- SW(config)# **ip access-list** *acl-type acl-name*
- SW(config-ext-nacl)# **permit** *protocol* [*source-address* | **any**] [*destination-address* | **any**]
- SW(config-ext-nacl)# **interface** *interface-slot/number*
- SW(config-if)# **ip access-group** *acl-name* **in**

PACL’s Group Mode

Configure the access group mode on a Layer 2 interface:

```
SW(config)# interface interface-slot/number
SW(config-if)# access-group mode [ prefer port | merge ]
```

- Note:
  - Access mode command is not supported on all platforms.

Storm Control

Storm Control

- Describe what a traffic storm is and how to control it
- Configure and verify storm control

Introduction to Storm Control

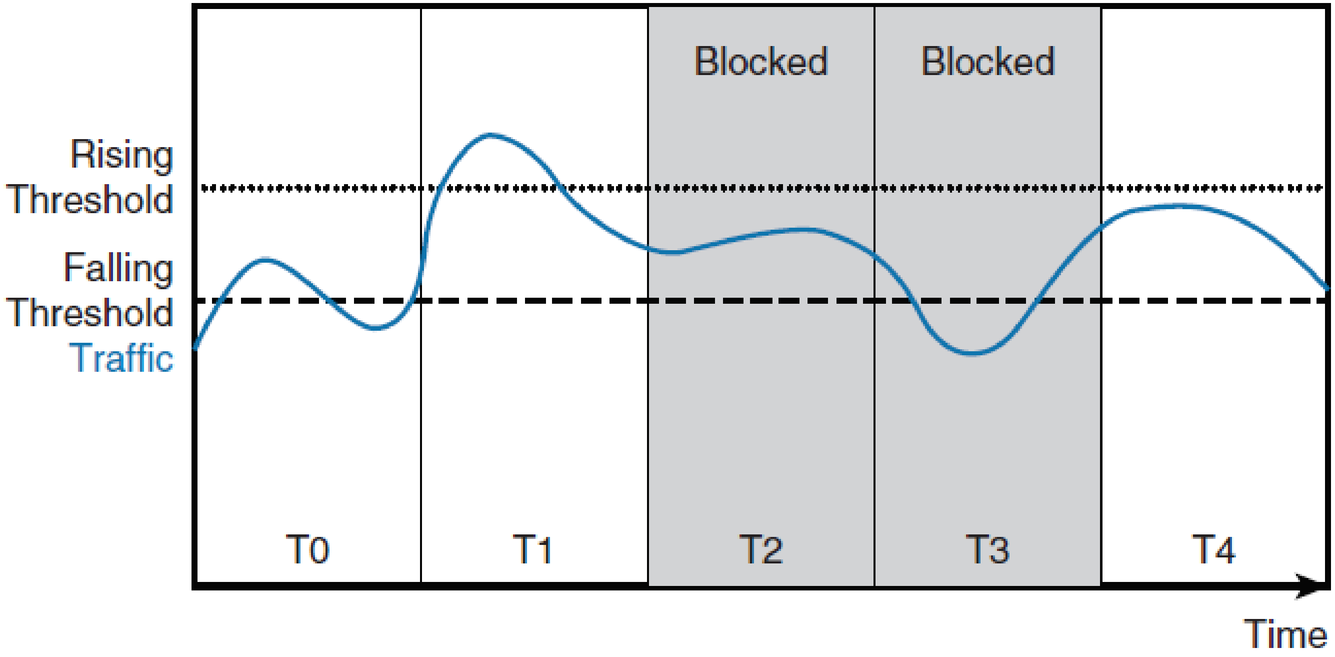
- A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance.
- The storm control feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.

Storm Control Behavior

- During the interval, it compares the traffic level with the traffic storm threshold level that you configure.
- The traffic storm control level is either an absolute number of bits or packets per second or a percentage of the total available bandwidth of the port.
- Two thresholds can be configured.
- When traffic exceeds the rising threshold level, storm control blocks the port.
- Once the traffic falls under the falling threshold, storm control removes the block.
- Configuration of a falling threshold is optional.

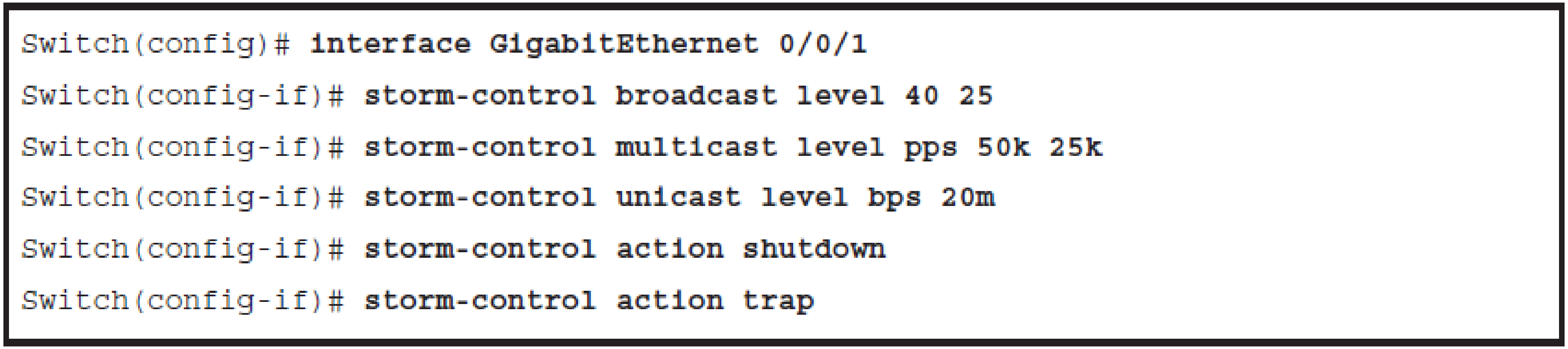
Storm Control Behavior

- Optionally, an interface can be shut down if a threshold level is breached or an SNMP trap is sent.
- In addition, storm control is configured per interface for each traffic type (unicast, multicast, broadcast) separately.



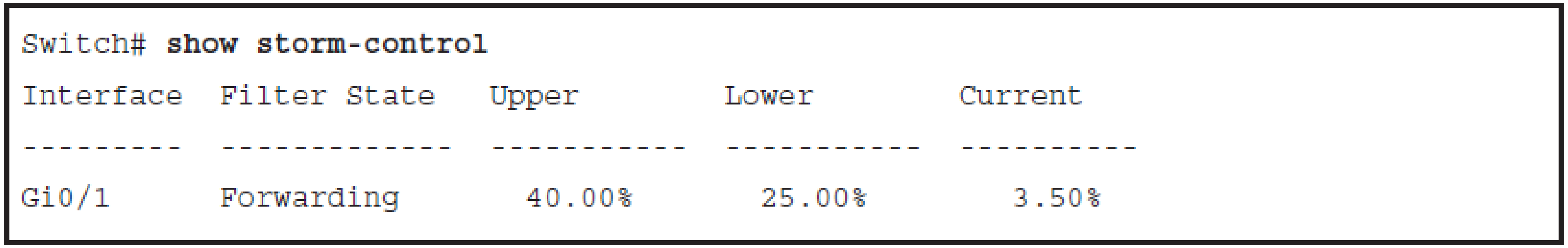
Configuring and Verifying Storm Control on an Interface

- Switch(config)# **interface** *interface-slot/int*
- Switch(config-if)# **storm-control** [**broadcast** | **multicast** | **unicast**] **level** { *risingpercent* | **bps** *rising-bps* | **pps** *rising-pps* } [*falling-percent*|*falling-bps*|*falling-pps*]
- Switch(config)# **interface** *interface-slot/int*
- Switch(config-if)# **storm-control action** { **shutdown**|**trap** }

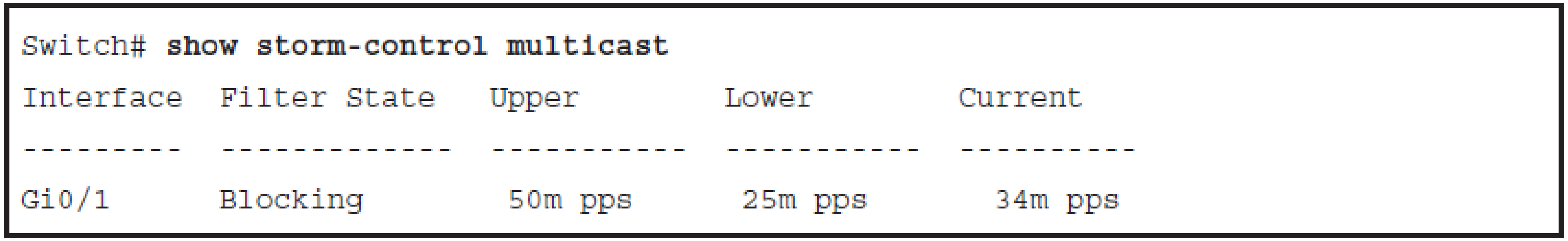


```
Switch(config)# interface GigabitEthernet 0/0/1
Switch(config-if)# storm-control broadcast level 40 25
Switch(config-if)# storm-control multicast level pps 50k 25k
Switch(config-if)# storm-control unicast level bps 20m
Switch(config-if)# storm-control action shutdown
Switch(config-if)# storm-control action trap
```

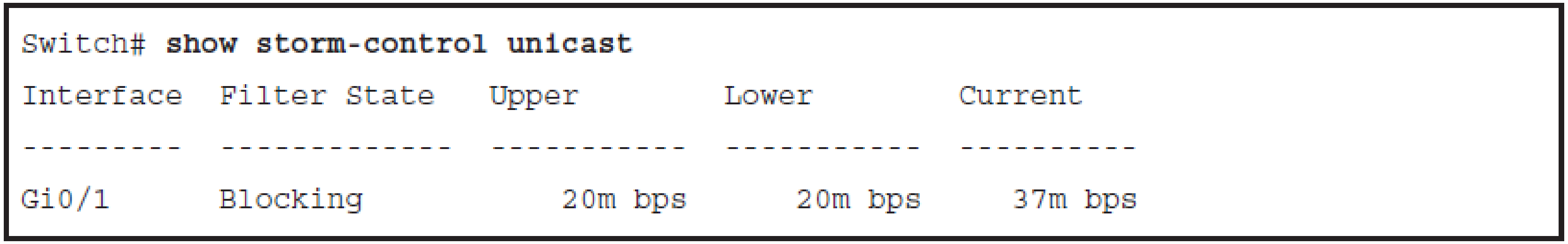
Verify Storm Control Configurations



```
Switch# show storm-control
Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Gi0/1      Forwarding       40.00%       25.00%        3.50%
```



```
Switch# show storm-control multicast
Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Gi0/1      Blocking         50m pps      25m pps       34m pps
```



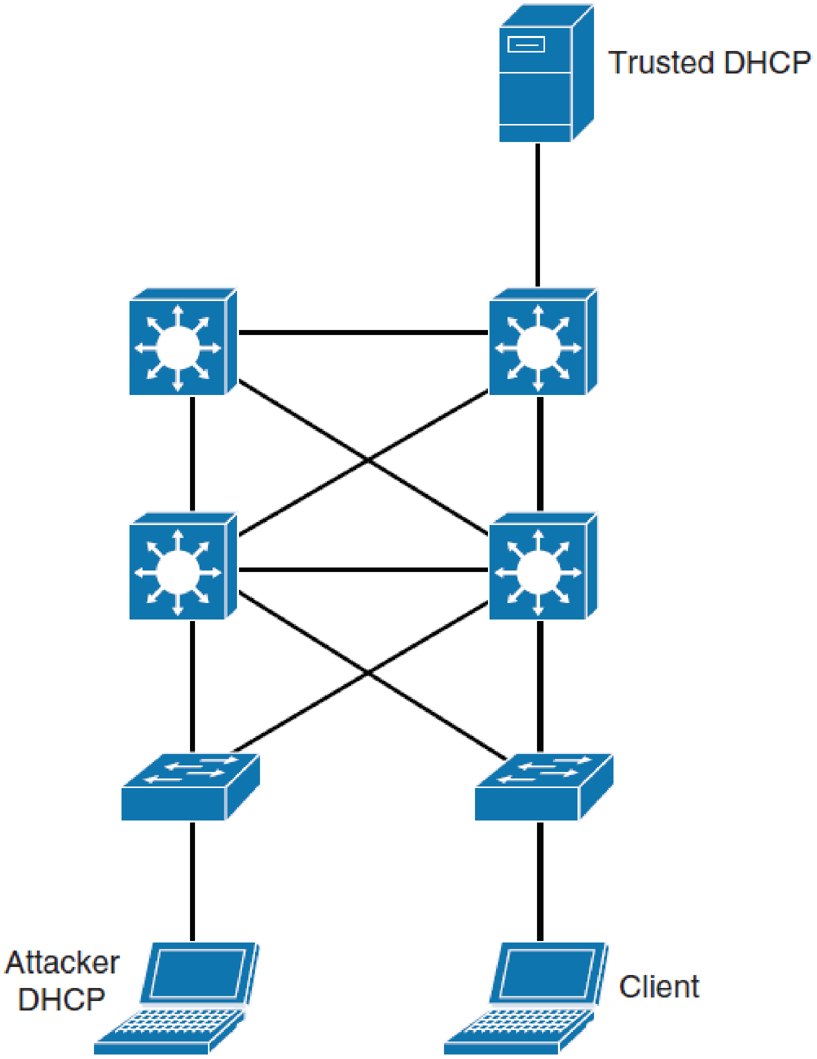
```
Switch# show storm-control unicast
Interface  Filter State   Upper        Lower        Current
---------  -------------  -----------  -----------  ----------
Gi0/1      Blocking            20m bps      20m bps     37m bps
```

Mitigating Spoofing Attacks

Mitigating Spoofing Attacks

- How can a rogue DHCP server harm your network
- DHCP spoofing
- Configuring and verifying DHCP snooping
- What IP Source Guard is and why you need it
- Configuring IP Source Guard
- ARP spoofing
- How DAI works
- Configure DAI

DHCP Spoofing Attacks



- The most common example of a rogue DHCP server is when a PC is configured as a DHCP server in the campus network.
- If the rogue DHCP server's reply arrives at the DHCP client first, the client will use this response.
- Because this first response from the rogue server is bogus, the client will not be able to gain the correct network connectivity and may have its traffic redirected to a bogus default gateway

Rogue DHCP Server Process

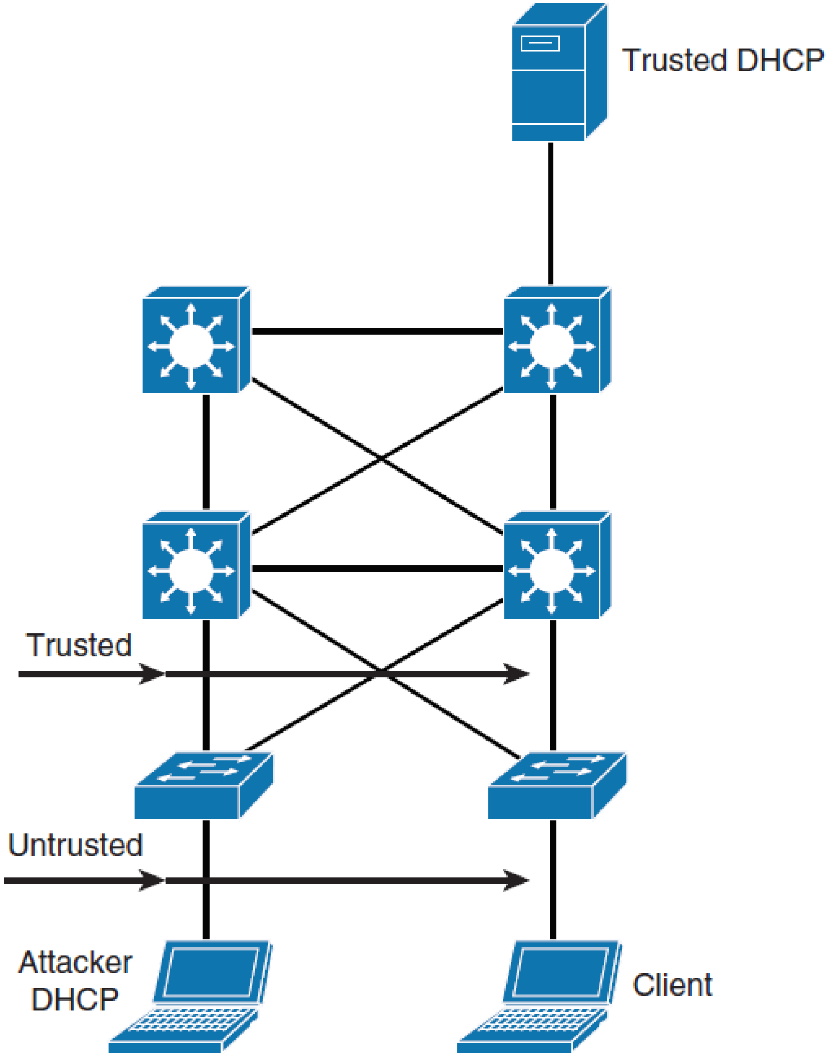
1. Attacker hosts a rogue DHCP server off a switch port to the same subnet as the clients.
2. Client broadcasts a request for DHCP configuration information.
3. The rogue DHCP server responds before the legitimate DHCP server, assigning attacker-defined IP configuration information.
4. Host packets are redirected to the attacker’s address because it emulates a default gateway for the erroneous IP address that is provided to the client via DHCP.

DHCP Snooping

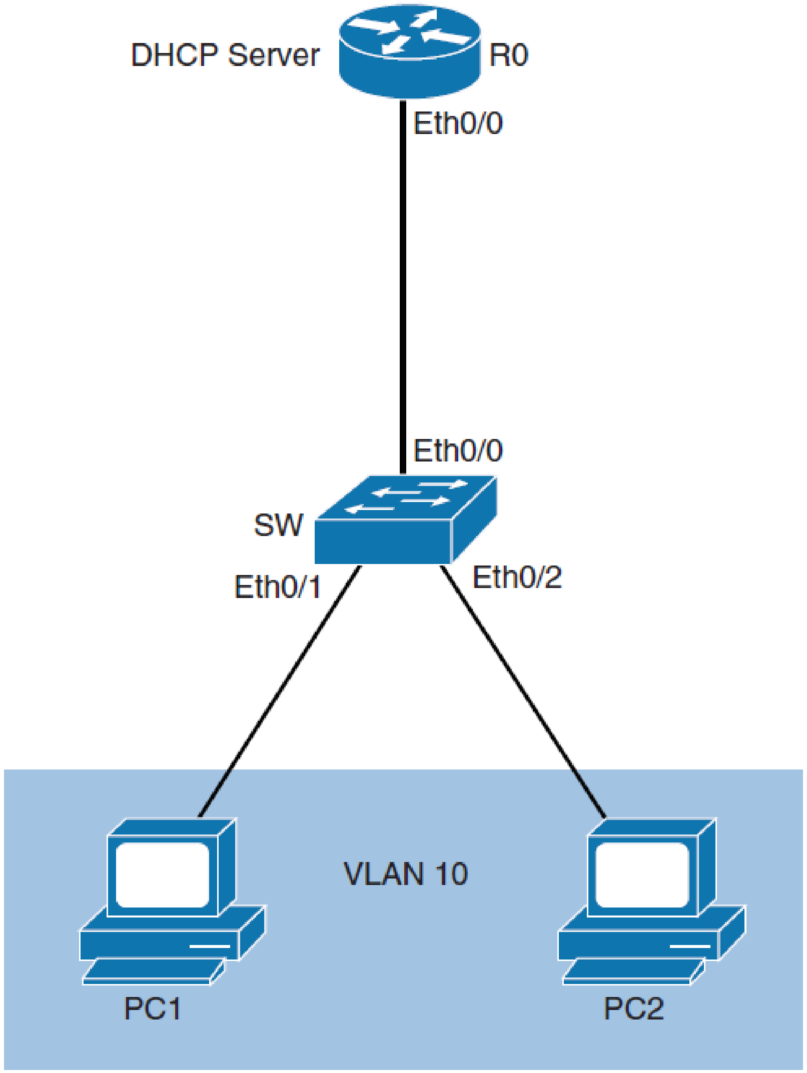
DHCP Snooping feature configures two types of port:

- **Trusted ports**
  - Host a DHCP server or can be an uplink toward the DHCP server.
- **Untrusted ports**
  - Are those that are not explicitly configured as trusted.
  - From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as DHCPOFFER, DHCPACK, or DHCPNAK.
  - If a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is shut down.
  - This feature can be coupled with DHCP option 82, in which switch information, such as the port ID of the DHCP request, can be inserted into the DHCP request packet.

DHCP Snooping



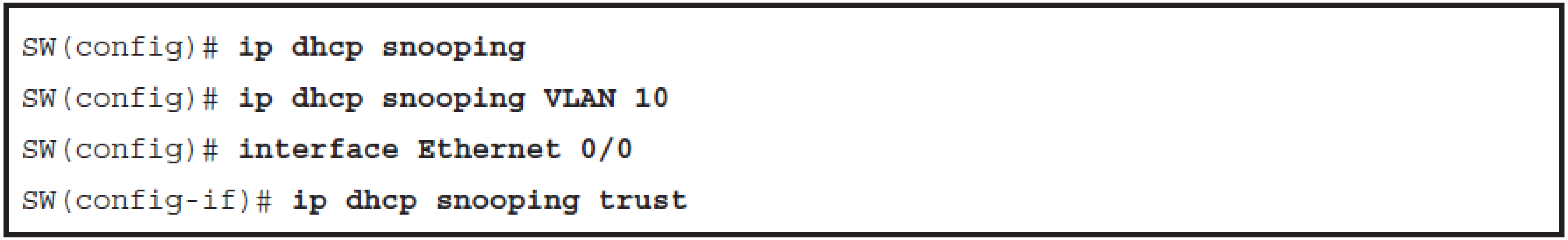
DHCP Snooping Example Configuration



DHCP Snooping Example Configuration

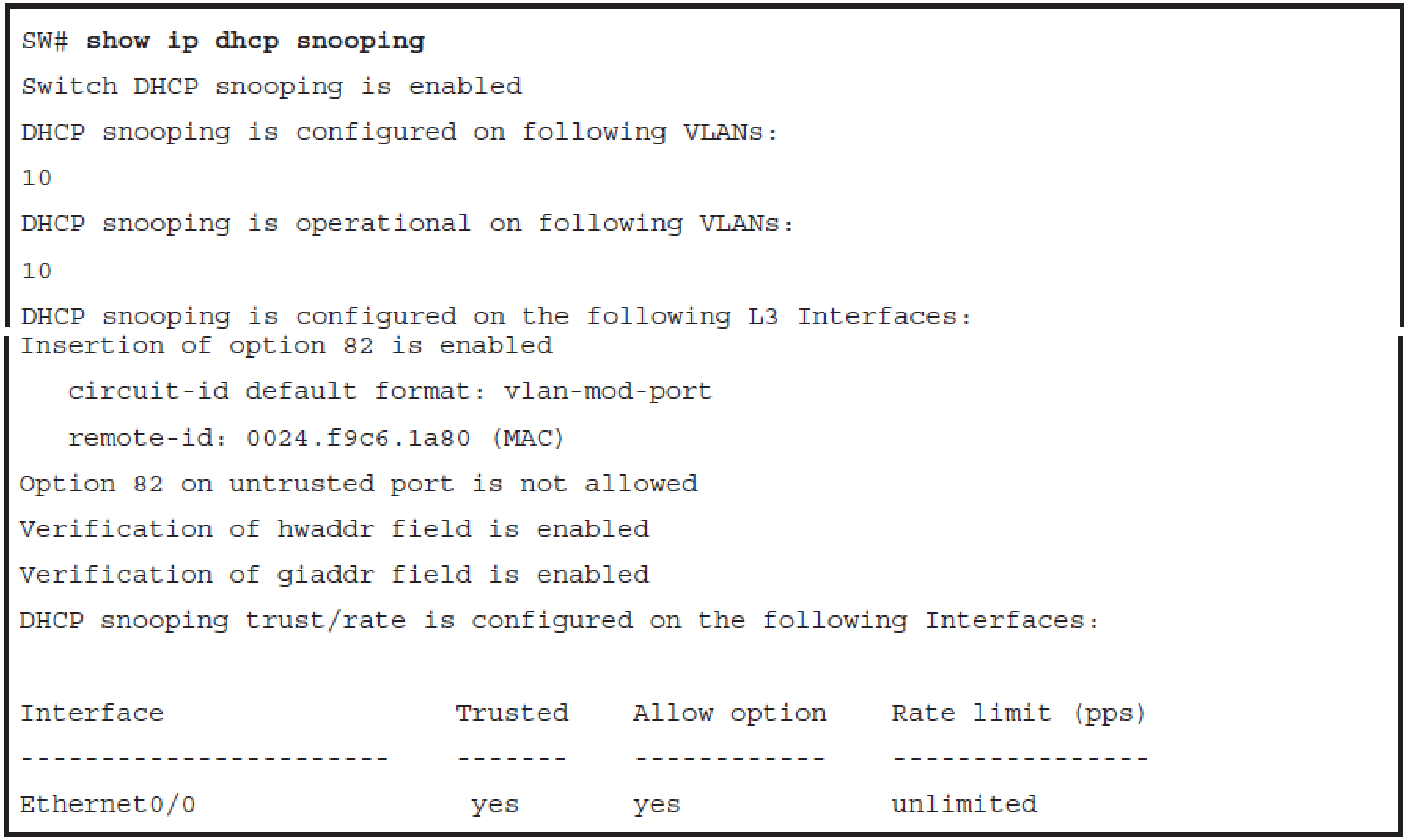
Steps to enable DHCP snooping for VLAN 10 with a DHCP server on Ethernet 0/0:

- **Step 1.** Enable DHCP snooping globally.
- **Step 2.** Enable DHCP snooping on selected VLANs.
- **Step 3.** Configure trusted interfaces, since untrusted is default.
- **Step 4.** Configure rate-limit of DHCP requests on untrusted ports.
- **Step 5.** Configure information option using DHCP option 82.



```
SW(config)# ip dhcp snooping
SW(config)# ip dhcp snooping VLAN 10
SW(config)# interface Ethernet 0/0
SW(config-if)# ip dhcp snooping trust
```

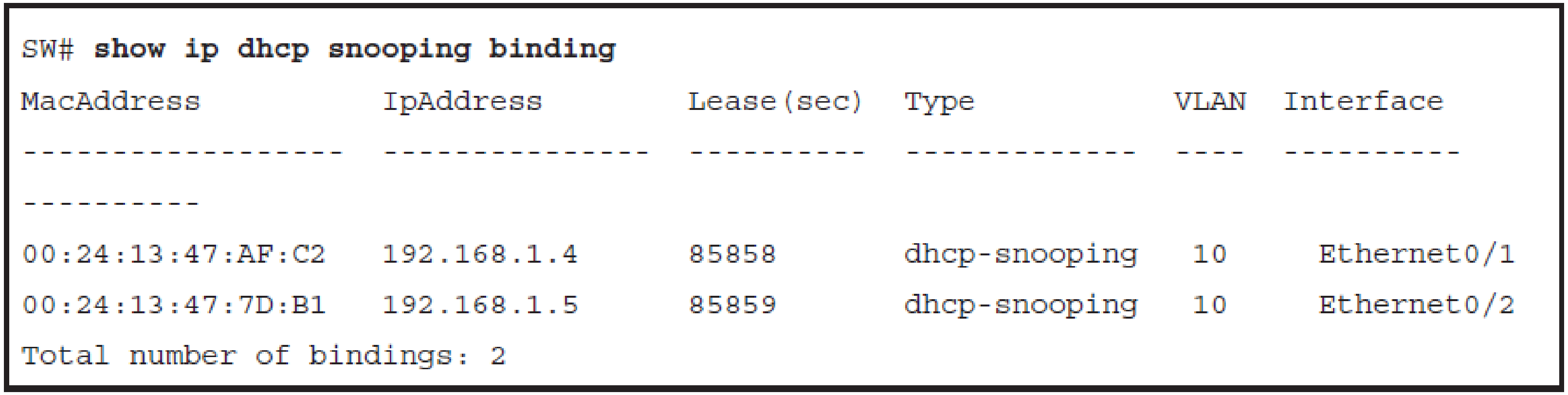
Verifying DHCP Snooping Configuration



```
SW# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0024.f9c6.1a80 (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)
-----------------------    -------    ------------    ----------------
Ethernet0/0                 yes       yes             unlimited
```

Verifying DHCP Snooping Configuration



```
SW# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ----------
----------
00:24:13:47:AF:C2   192.168.1.4      85858       dhcp-snooping   10     Ethernet0/1
00:24:13:47:7D:B1   192.168.1.5      85859       dhcp-snooping   10     Ethernet0/2
Total number of bindings: 2
```

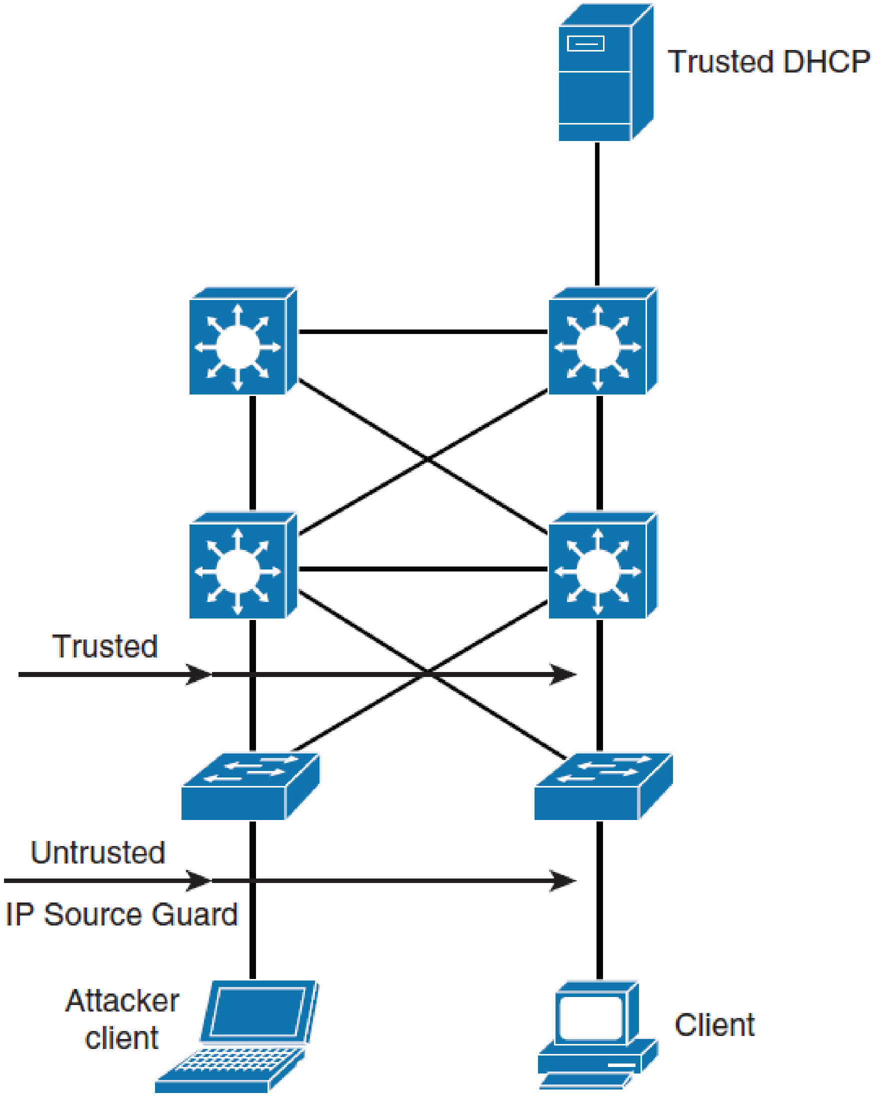
DHCP Snooping Command Review

- **ip dhcp snooping**
  - Enables DHCP snooping globally. By default, the feature is not enabled.
- **ip dhcp snooping information option**
  - Enables DHCP option 82. This is optional for the forwarded DHCP request packet to contain information on the switch port where it originated. The option is enabled by default.
- **ip dhcp snooping vlan** *vlan-id* [*vlan-id*]
  - Identifies VLANs that will be subject to DHCP snooping.
- **ip dhcp snooping trust**
  - Configures trusted port. Use the **no** keyword to revert to untrusted. Use this command in the interface configuration mode.
- **ip dhcp snooping limit rate** *rate*
  - Configures the number of DHCP packets per second that an interface can receive. This ensures that DHCP traffic will not overwhelm the DHCP servers. Normally, the rate limit applies to untrusted interfaces. Use this command in the interface configuration mode.
- **show ip dhcp snooping**
  - Verifies the configuration.

IP Source Guard

- IPSG operates by dynamically maintaining per-port VLAN ACLs based on learned IP-to-MAC-to-switch-port bindings.
- When IPSG is enabled, the switch blocks all IP traffic into the port except for DHCP packets captured by the DHCP snooping process.
- After the DHCP process is complete and the client receives a valid IP address from the DHCP server (or when a static IP source binding is configured by the user), a per-port and VLAN access control list (PVACL) is installed on the port dynamically.
- This process restricts the client IP traffic ingress on the respective port to the source IP address that is configured in the binding.
- Any IP traffic with a source IP address other than that in the IP source binding will be filtered out.

IPSG Topology Layout

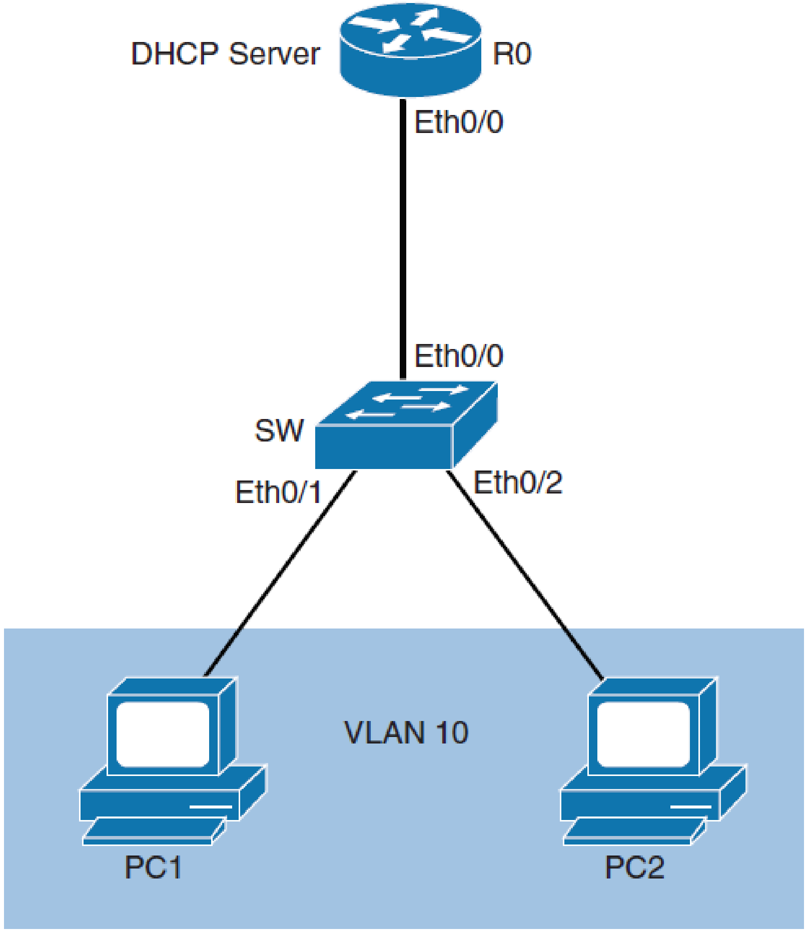


IPSG Filters

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

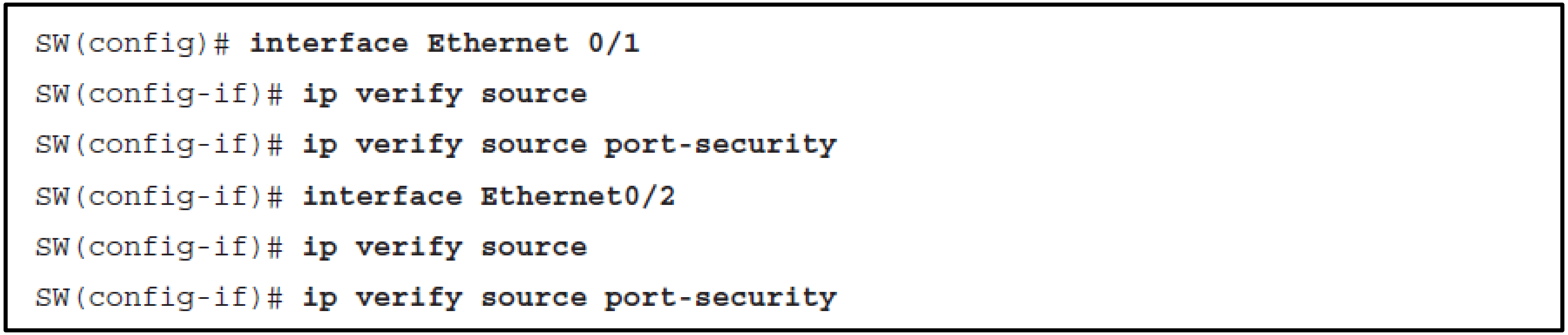
- **Source IP address filter**
  - IP traffic is filtered based on its source IP address. Only IP traffic with a source IP address that matches the IP source binding entry is permitted. An IP source address filter is changed when a new IP source entry binding is created or deleted on the port.
- **Source IP and MAC address filter**
  - IP traffic is filtered based on its source IP address in addition to its MAC address; only IP traffic with source IP and MAC addresses that match the IP source binding entry are permitted.

IPSG Configuration



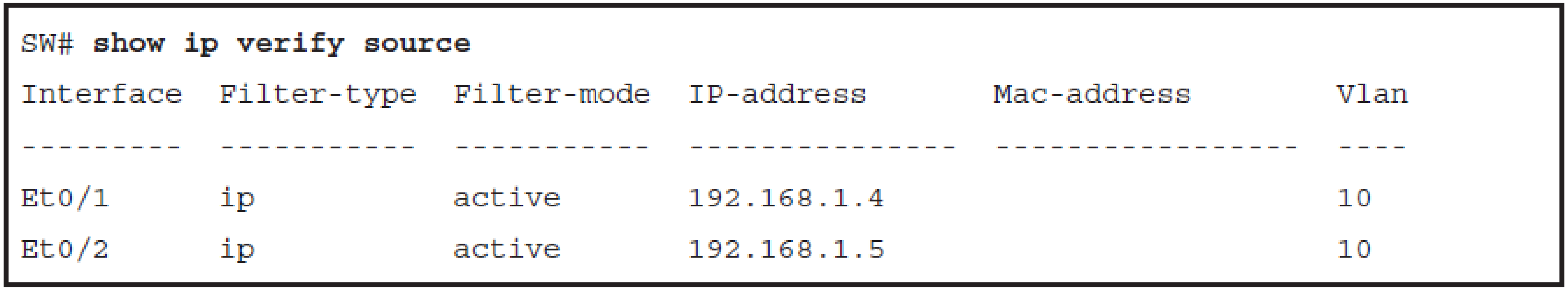
IPSG Configuration

- To enable IPSG on the port use the **ip verify source** interface command for enabling IP address filters.
- To enable MAC address filtering and IP filters, add the **ip verify source port-security** interface command.



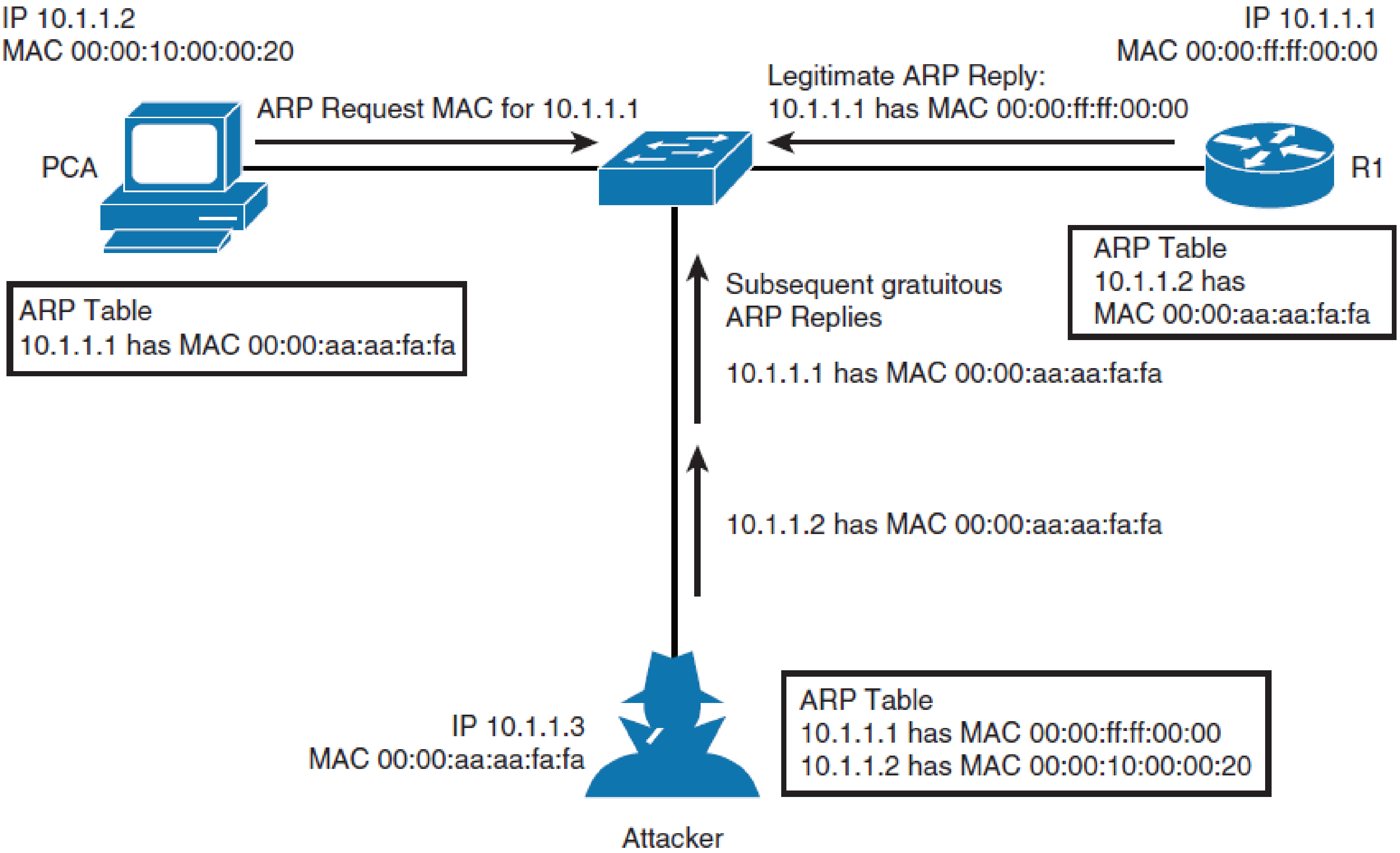
```
SW(config)# interface Ethernet 0/1
SW(config-if)# ip verify source
SW(config-if)# ip verify source port-security
SW(config-if)# interface Ethernet0/2
SW(config-if)# ip verify source
SW(config-if)# ip verify source port-security
```

IPSG Configuration and State Verification



```
SW# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Et0/1      ip           active       192.168.1.4                         10
Et0/2      ip           active       192.168.1.5                         10
```

ARP Spoofing


IP 10.1.1.2
MAC 00:00:10:00:00:20
ARP Request MAC for 10.1.1.1
PCA
Legitimate ARP Reply:
10.1.1.1 has MAC 00:00:ff:ff:00:00
IP 10.1.1.1
MAC 00:00:ff:ff:00:00
R1
ARP Table
10.1.1.1 has MAC 00:00:aa:aa:fa:fa
Subsequent gratuitous
ARP Replies
ARP Table
10.1.1.2 has
MAC 00:00:aa:aa:fa:fa
10.1.1.1 has MAC 00:00:aa:aa:fa:fa
10.1.1.2 has MAC 00:00:aa:aa:fa:fa
IP 10.1.1.3
MAC 00:00:aa:aa:fa:fa
ARP Table
10.1.1.1 has MAC 00:00:ff:ff:00:00
10.1.1.2 has MAC 00:00:10:00:00:20
Attacker

ARP Spoofing

- **Step 1.** PCA sends an ARP request for MAC address of R1.
- **Step 2.** R1 replies with its MAC and IP address. It also updates its ARP cache.
- **Step 3.** PCA binds MAC address of R1 to R1's IP address in its ARP cache.
- **Step 4.** Attacker sends its ARP reply to PCA, binding its MAC address to the IP of R1.
- **Step 5.** PCA updates ARP cache with MAC address of attacker bound to IP address of R1.
- **Step 6.** Attacker sends its ARP reply to R1, binding its MAC address to the IP of PCA.
- **Step 7.** R1 updates ARP cache with MAC address of attacker bound to IP address of PCA.
- **Step 8.** Packets are diverted through attacker.

Dynamic ARP Inspection

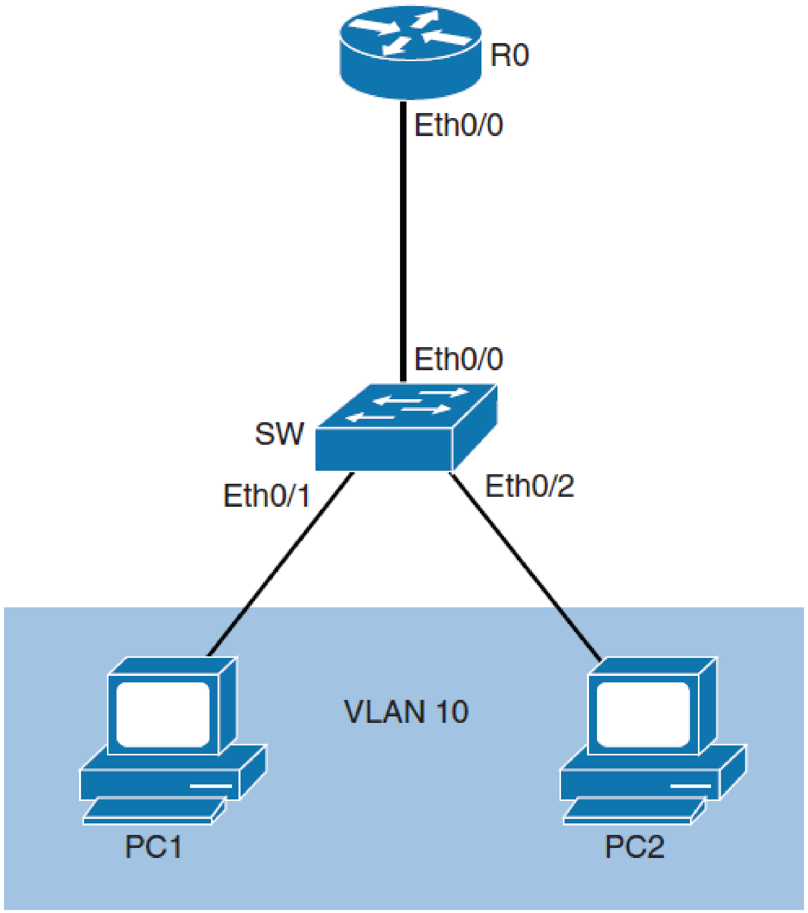
- Dynamic ARP inspection (DAI) helps prevent such attacks by not relaying invalid or gratuitous ARP replies out to other ports in the same VLAN.
- DAI intercepts all ARP requests and all replies on the untrusted ports.
- Each intercepted packet is verified for valid IP-to-MAC binding similar to IPSG.
- ARP replies coming from invalid devices are either dropped or logged by the switch for auditing so that ARP poisoning attacks are prevented.
- You can also use DAI to rate-limit the ARP packets and then err-disable the interface if the rate is exceeded.
- DAI determines the validity of an ARP packet based on a valid MAC-address-to-Ip address bindings database that is built by DHCP snooping.
- In addition, to handle hosts that use statically configured IP addresses, DAI can validate ARP packets against user configured ARP ACLs.

DAI Configuration Steps

- **Step 1.** Implement protection against DHCP spoofing:
  - **a.** Enable DHCP snooping globally.
  - **b.** Enable DHCP snooping on selected VLANs.
- **Step 2.** Enable DAI: Enable ARP inspection on selected VLANs.
- **Step 3.** Configure trusted interfaces for DHCP snooping and ARP inspection (untrusted is default).

DAI Configuration

```
SW(config)# ip dhcp snooping
SW(config)# ip dhcp snooping vlan 10
SW(config)# ip arp inspection vlan 10
SW(config)# interface Ethernet 0/0
SW(config-if)# ip dhcp snooping trust
SW(config-if)# ip arp inspection trust
```



DAI Commands

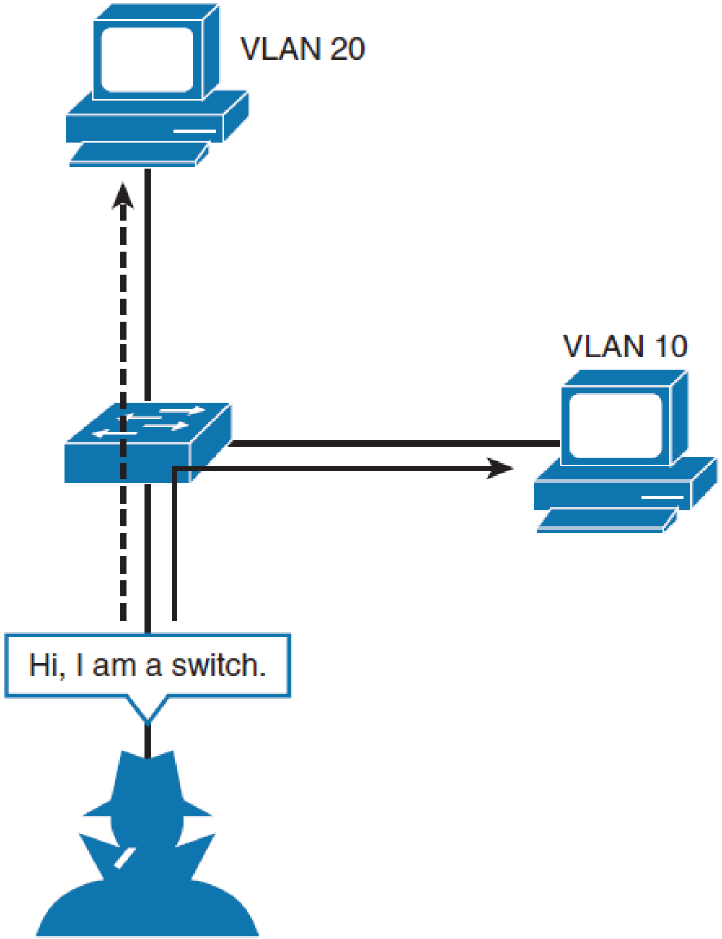
- **ip arp inspection vlan** *vlan-id* [, *vlan-id*]
  - Enables DAI on a VLAN or range of VLANs
- **ip arp inspection trust**
  - Sets the interface as a trusted interface
- **ip arp inspection validate** {[*src-mac*] [*dst-mac*] [*ip*]}
  - Configures DAI to drop ARP packets when the IP addresses are invalid, or when the MAC addresses in the body of the ARP packets do not match the addresses that are specified in the Ethernet header

Securing VLAN Trunks

Securing VLAN Trunks

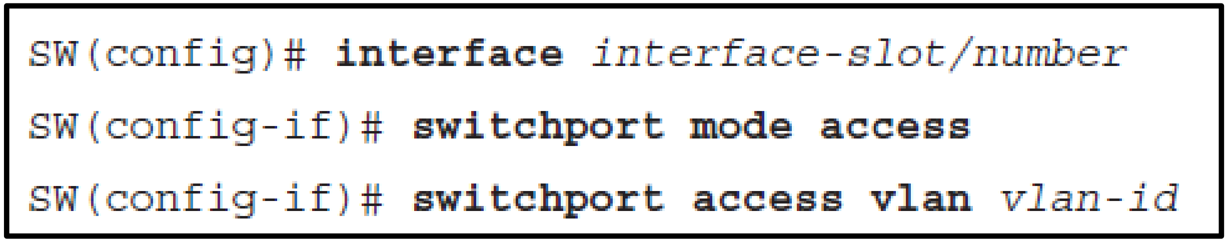
- Describe the switch spoofing attack associated with VLAN trunks
- Protect your network against switch spoofing
- Describe the VLAN hopping attack
- Protect your network against the VLAN hopping attack
- Describe the need for VLAN access lists
- Describe how VLAN access lists interact with standard and port access lists
- Configure the VLAN access lists

Switch Spoofing

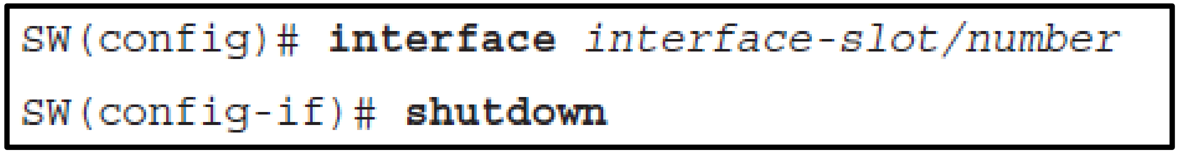


- There are several mechanisms or best practices to minimize authorized access to trunk ports and switch spoofing, including the following
  - Manually configure access and trunk ports
  - Shut down unused interfaces
  - Restrict VLANs on trunk ports

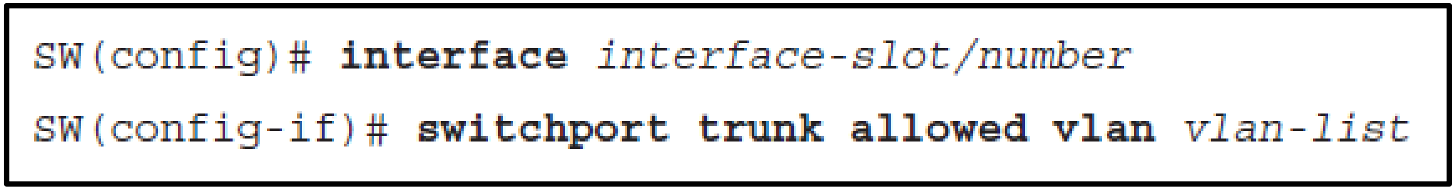
Switch Spoofing



```
SW(config)# interface interface-slot/number
SW(config-if)# switchport mode access
SW(config-if)# switchport access vlan vlan-id
```

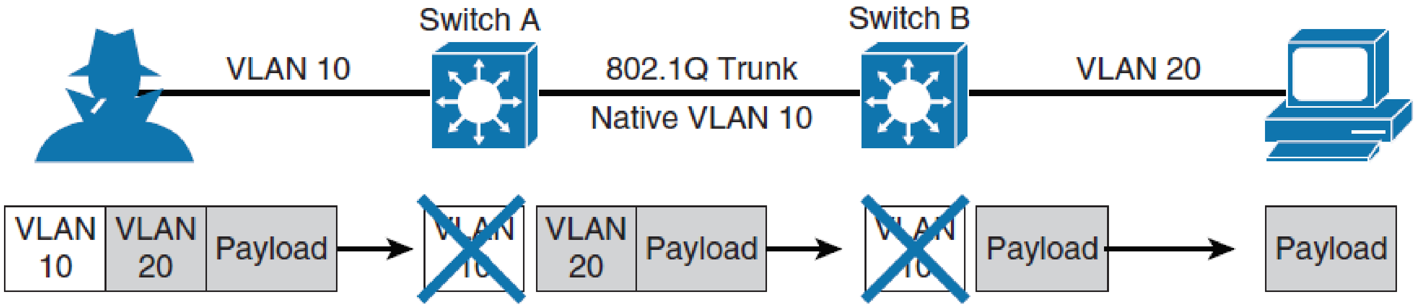


```
SW(config)# interface interface-slot/number
SW(config-if)# shutdown
```



```
SW(config)# interface interface-slot/number
SW(config-if)# switchport trunk allowed vlan vlan-list
```

VLAN Hopping



- The IP-enabled device the attacker is using must be connected to an access port.
- The IP-enabled device must send a double-tagged frame.
- The first-hop switch must be configured to accept 802.1Q frames.
- The first-hop switch must be connected to another switch with an 802.1Q truck, and its native VLAN must match the attackers outer VLAN tag.

Protecting Against VLAN Hopping

- Because an attacker’s port VLAN must match the native VLAN of a trunk, the simple solution is to configure the native VLAN of all trunk ports to an unused VLAN.

```
SW(config)# interface interface-slot/number
SW(config-if)# switchport trunk native vlan vlan-id
SW(config-if)# switchport trunk allowed vlan remove vlan-id
```

- Yet another option is to tag all frames on trunk ports by default. The command to configure this option is as follows:

```
SW(config)# vlan dot1q tag native
```

VLAN Access Lists

- VACLs can provide access control for all packets that are bridged within a VLAN or packets that are routed into or out of a VLAN or a WAN interface.
- VACLs can configured for IP or MAC layer traffic with some limitations depending on platform and software version.
- VLAN access lists (VACLs) on Catalyst switches serve the following two distinct purposes:
  - With certain limitations, filter traffic at Layer 2
  - Overcome VLAN Switch Port Analyzer (SPAN) limitations via use of the Capture Port feature

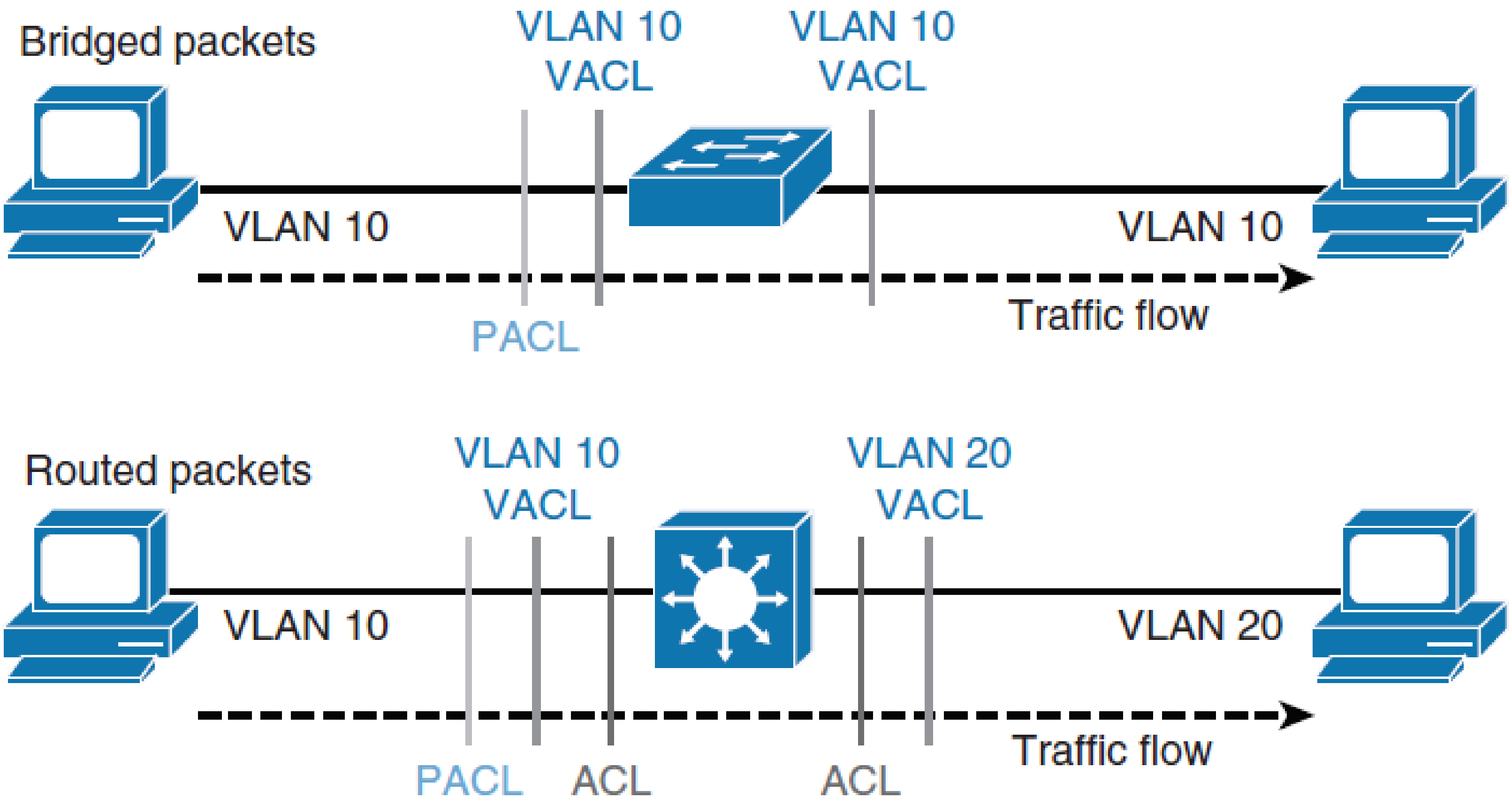
VACLs Process

- Each VLAN access map can consist of one or more map sequences; each sequence has a match clause and an action clause.
- The match clause specifies IP or MAC ACLs for traffic filtering, and the action clause specifies the action to be taken when a match occurs.
- When a flow matches a permit ACL entry, the associated action is taken, and the flow is not checked against the remaining sequences.
- When a flow matches a deny ACL entry, it will be checked against the next ACL in the same sequence or the next sequence.
- If a flow does not match any ACL entry and at least one ACL is configured for that packet type, the packet is denied.

Advantage of VACL Capture Port usage over VSPAN

- **Granular traffic analysis**
  - VACLs can match based on source IP address, destination IP address, Layer 4 protocol type, source and destination Layer 4 ports, and other information.
- **The number of sessions**
  - VACLs are enforced in hardware..
- **Destination port oversubscription**
  - Granular traffic identification reduces the number of frames to be forwarded to the destination port and thereby minimizes the probability of their oversubscription.
- **VACLs are enforced in hardware**

VACL Interaction with ACLs and PACLs



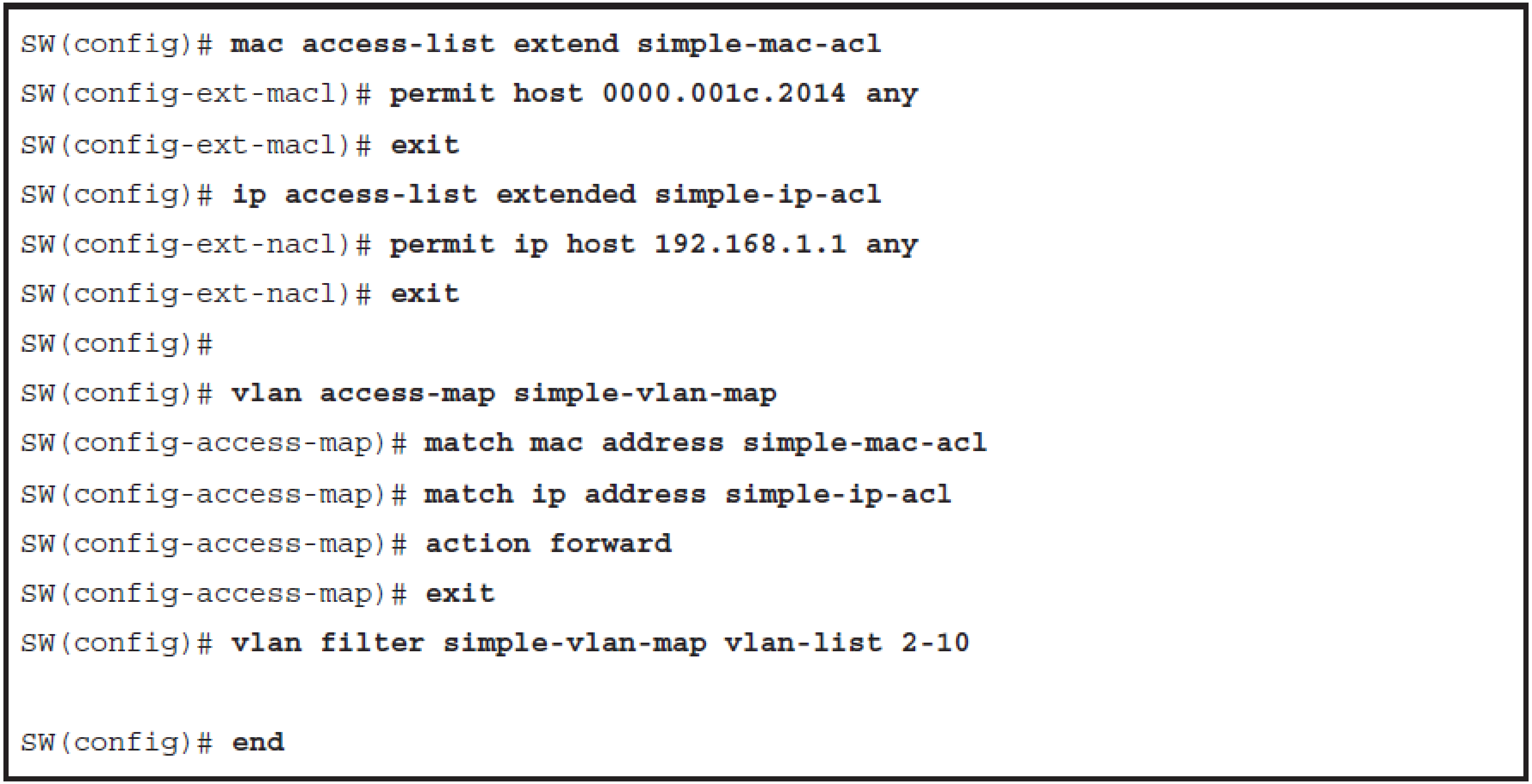
Configuring VACLs

- SW(config)# **mac access-list extended** *acl-name*
- SW(config-ext-macl)# **permit host** [*source-mac* | **any**] [*destination-mac* | **any**]
- SW(config)# **ip access-list** *acl-type acl-name*
- SW(config-ext-nacl)# **permit protocol** [*source-address* | **any**] [*destination-address* | **any**]

- SW(config)# **vlan access-map** *map-name*
- SW(config-access-map)# **match** [**mac** | **ip**] **address** *acl-name*
- SW(config-access-map)# **action** [**drop**|**forward**|**redirect**][**log**]

- SW(config)# **vlan filter** *map-name* **vlan-list** [*vlan-list* | **all**]

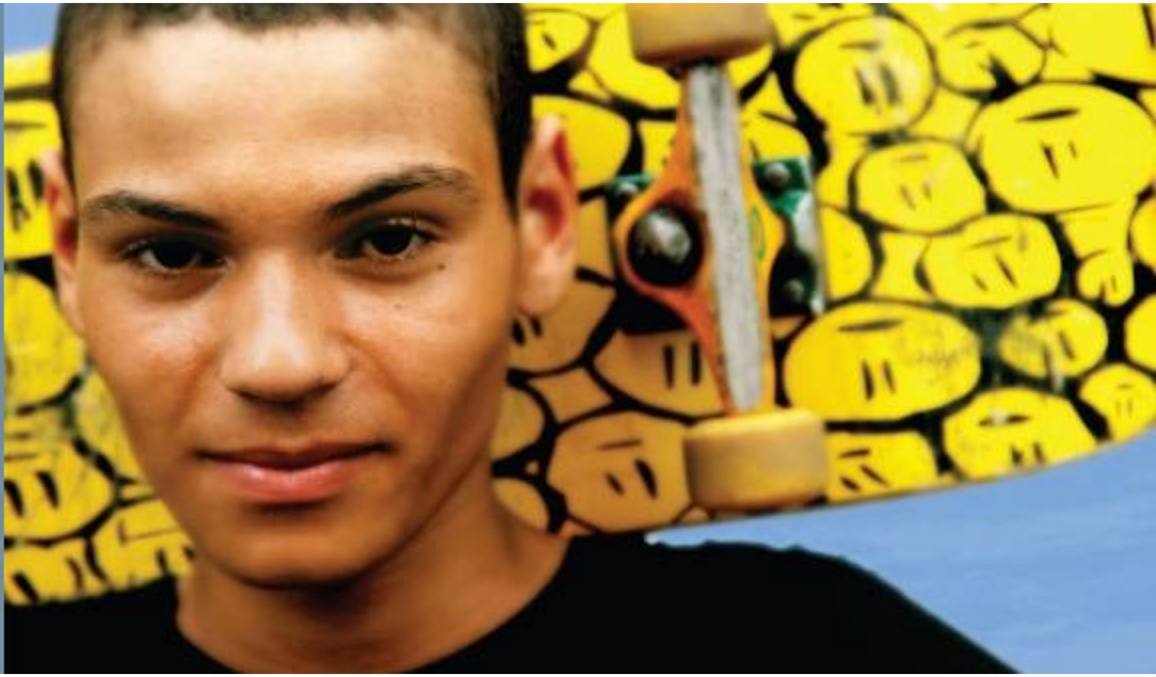
VACL examples



```
SW(config)# mac access-list extend simple-mac-acl
SW(config-ext-macl)# permit host 0000.001c.2014 any
SW(config-ext-macl)# exit
SW(config)# ip access-list extended simple-ip-acl
SW(config-ext-nacl)# permit ip host 192.168.1.1 any
SW(config-ext-nacl)# exit
SW(config)#
SW(config)# vlan access-map simple-vlan-map
SW(config-access-map)# match mac address simple-mac-acl
SW(config-access-map)# match ip address simple-ip-acl
SW(config-access-map)# action forward
SW(config-access-map)# exit
SW(config)# vlan filter simple-vlan-map vlan-list 2-10

SW(config)# end
```

Private VLANs



Private VLANs

- Introduction to private VLANs
- Describe the private VLAN feature
- Describe the private VLAN port types
- Configure private VLANs
- Verify private VLAN configuration
- Describe private VLANs across multiple switches
- Describe the protected port feature

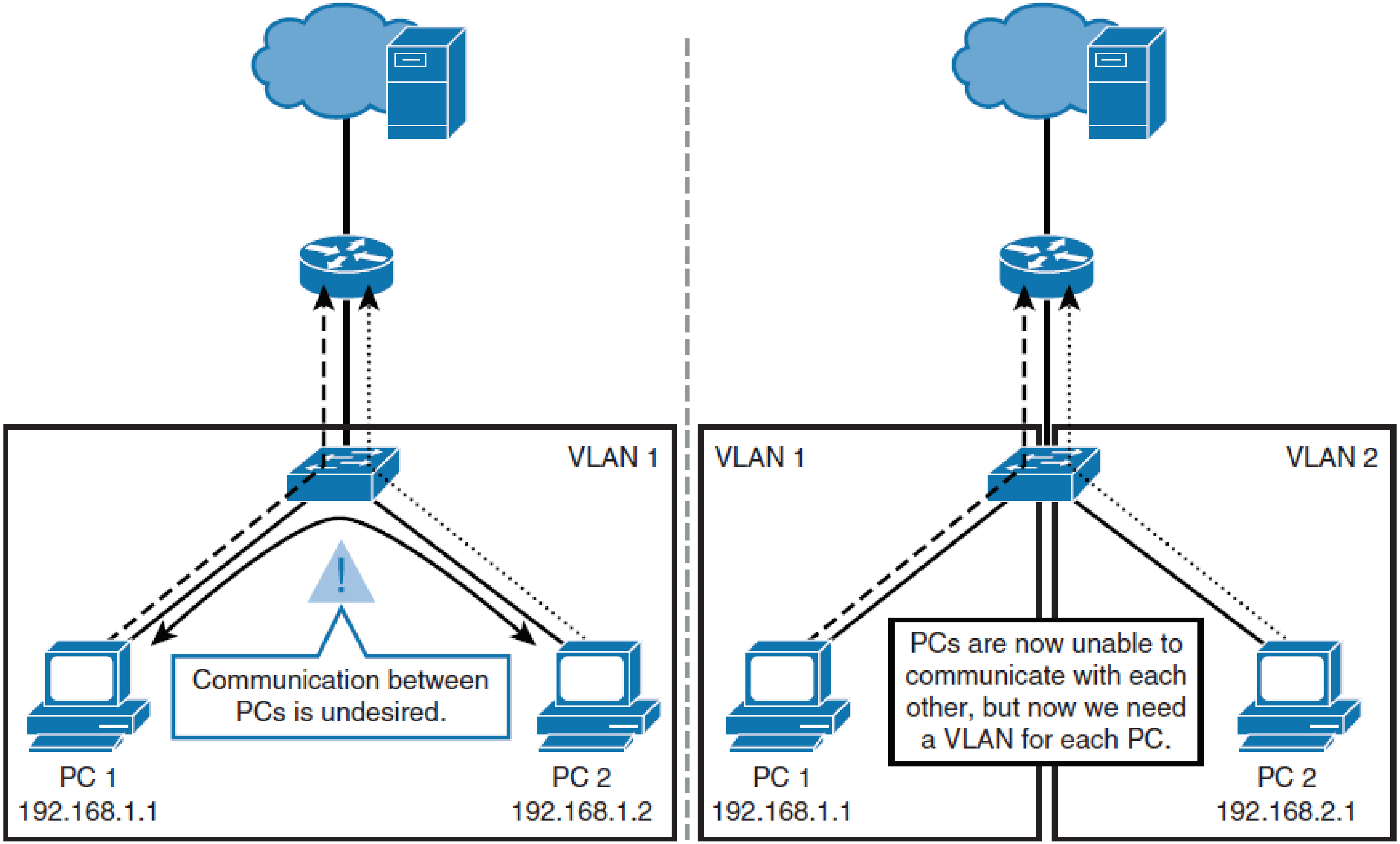
Introduction to PVLANs

- PVLANs restrict end-user devices such as PCs and mobile devices from communicating with each other, but still allow communication to router ports and network services.
- The end-user devices will behave as normal but cannot communicate to other devices in the same Layer 2 domain.
- This mechanism provides a level of security.
- Assigning every single end device its own VLAN would accomplish the same security method as PVLANs; however, switches have a limit on the number of VLANs supported, and a large number of VLANs creates scalability issues.

Introduction to PVLANs

- PVLANs are essentially VLANs inside a VLAN.
- A Layer 3 device is needed to route packets between different PVLANs.
- When a VLAN is partitioned into PVLANs, devices in different PVLANs still belong to the same IP subnet, but are unable to communicate with each other on Layer 2.
- PVLANs are an elegant solution when you need to keep multiple devices in the same IP subnet yet provide port isolation on Layer 2.

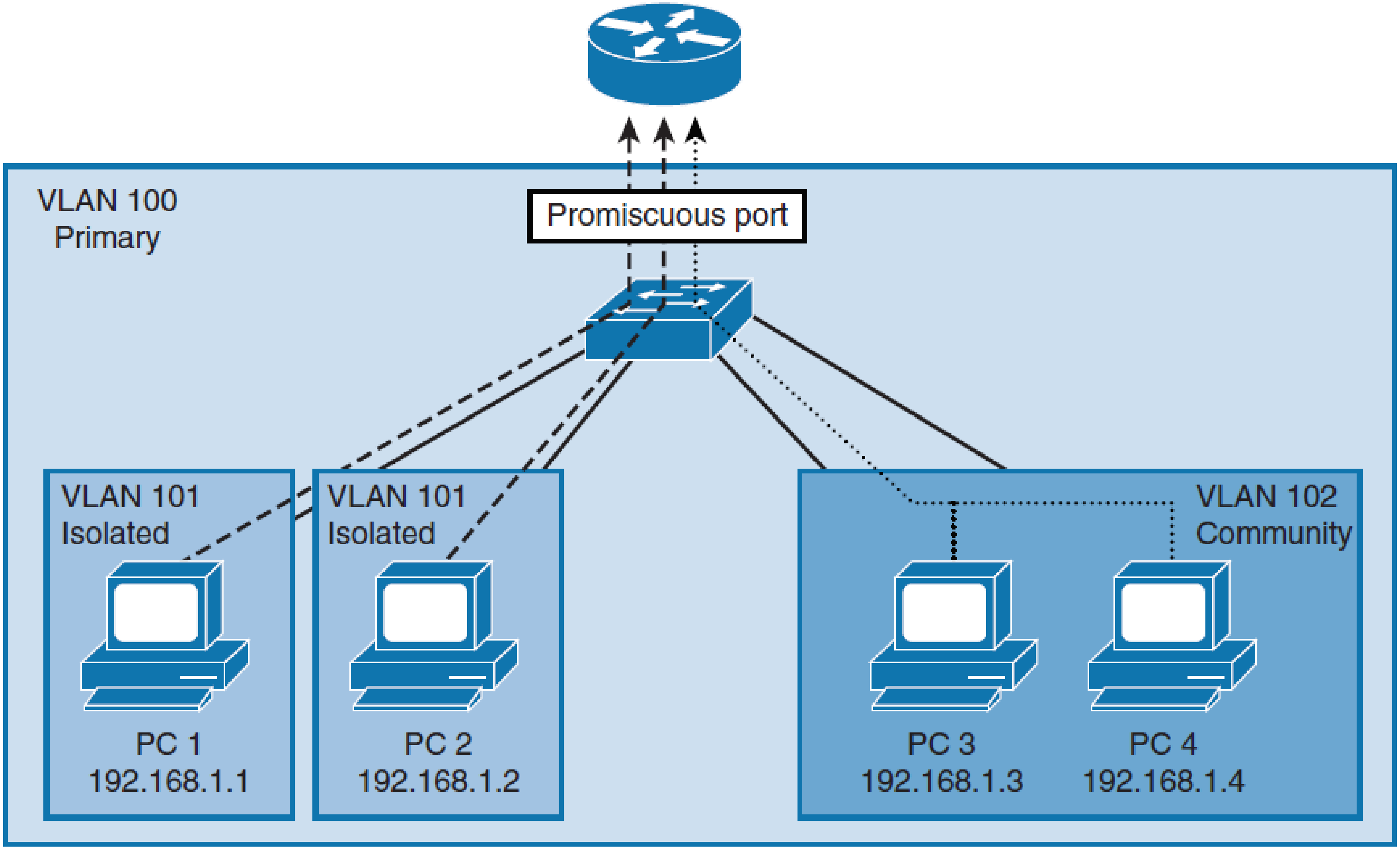
Introduction to PVLANs


VLAN 1
Communication between PCs is undesired.
PC 1
192.168.1.1
PC 2
192.168.1.2
VLAN 1
VLAN 2
PCs are now unable to communicate with each other, but now we need a VLAN for each PC.
PC 1
192.168.1.1
PC 2
192.168.2.1

PVLAN Port Types

- A PVLAN domain has one primary VLAN.
- Each port in a private VLAN domain is a member of the primary VLAN; the primary VLAN is the entire private VLAN domain.
- Secondary VLANs are subdomains that provide isolation between ports within the same private VLAN domain.
- There are two types of secondary VLANs: isolated VLANs and community VLANs.
  - Isolated VLANs contain isolated ports, which cannot communicate between each other in the isolated VLAN.
  - Community VLANs contain community ports that can communicate between each other in the community VLAN.

PVLAN Port Types

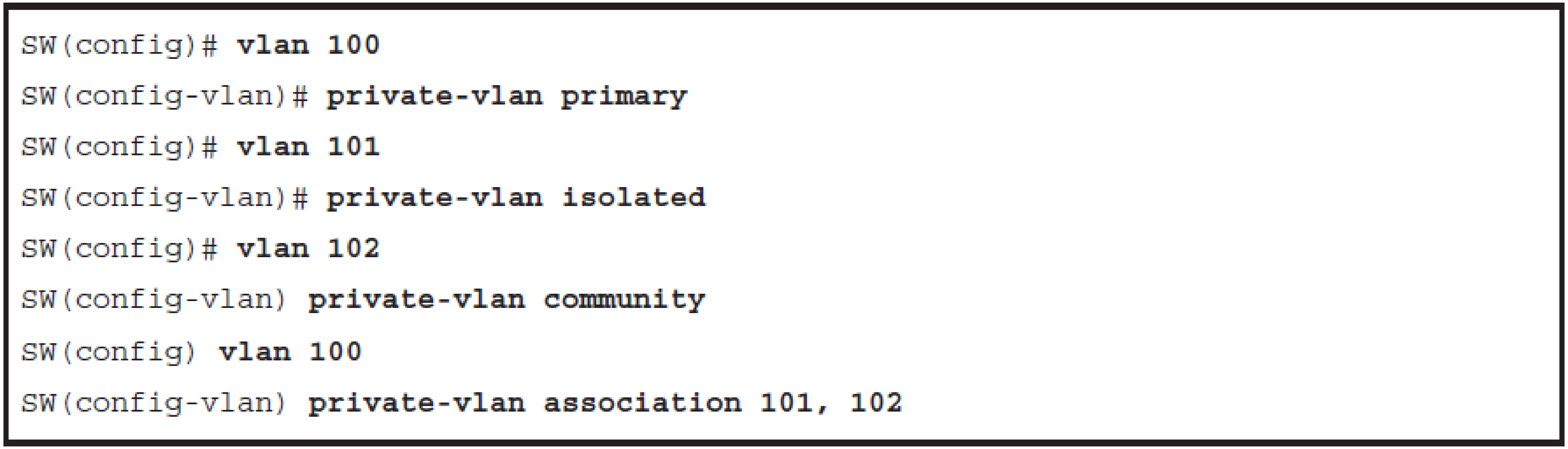


PVLAN Port Types

- **Promiscuous**
  - A promiscuous port belongs to the primary VLAN and can communicate with all mapped ports in the primary VLAN, including community and isolated ports.
  - There can be multiple promiscuous ports in a primary VLAN.
- **Isolated**
  - An isolated port is a host port that belongs to an isolated secondary VLAN.
  - An isolated port has complete isolation from other ports, except with associated promiscuous ports.
  - You can have more than one isolated port in a specified isolated VLAN.
- **Community**
  - A community port is a host port that belongs to a community secondary VLAN.
  - Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.
  - They are isolated from all ports in other community VLANs and all isolated ports.

PVLAN Configuration

- VTP must be set to transparent or off (v1, v2 and v3 supp).
- Configure the primary VLAN.
- Configure the secondary VLANs and apply the configuration of these PVLANs as isolated or community.
- Associate the primary VLAN with the secondary VLANs



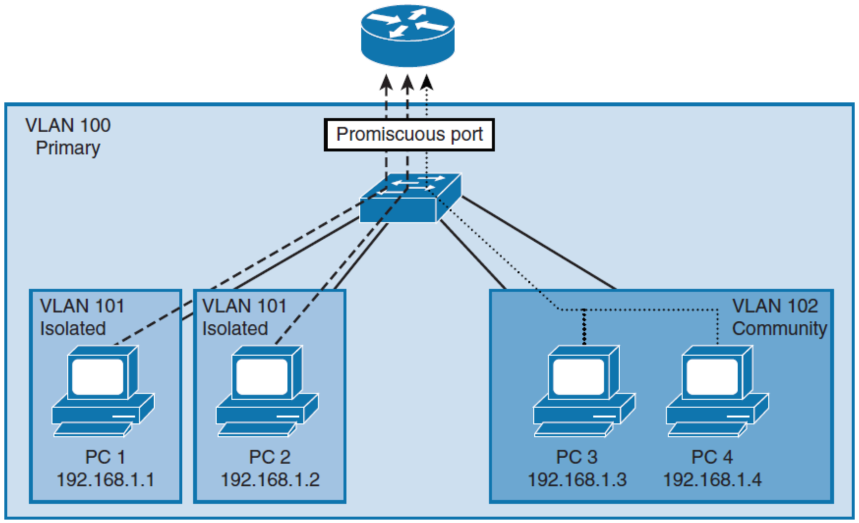
```
SW(config)# vlan 100
SW(config-vlan)# private-vlan primary
SW(config)# vlan 101
SW(config-vlan)# private-vlan isolated
SW(config)# vlan 102
SW(config-vlan) private-vlan community
SW(config) vlan 100
SW(config-vlan) private-vlan association 101, 102
```

Assign Ports

- Promiscuous Ports
- SW(config)# **interface** *interface-slot/number*
- SW(config-if)# **switchport mode private-vlan promiscuous**
- SW(config-if)# **switchport private-vlan mapping** *primary-vlan-id* **add** *secondary-vlanid* {, *secondary-vlan-id* }

- Community or Isolated Ports
- SW(config)# **interface range** *interface-range*
- SW(config-if-range)# **switchport mode private-vlan host**
- SW(config-if-range)# **switchport private-vlan host-association** *primary-vlan-id secondary-vlan-id*

Assign Ports



```
SW(config)# interface GigabitEthernet 0/1
SW(config-if)# switchport description Interface-to-Router
SW(config-if)# switchport mode private-vlan promiscuous
SW(config-if)# switchport private-vlan mapping 100 add 101, 102
SW(config-if)# interface range GigabitEthernet 0/2-3
SW(config-if-range)# switchport description End-User-Ports-In-Isolated-PVLAN
SW(config-if-range)# switchport mode private-vlan host
SW(config-if-range)# switchport private-vlan host-association 100 101
SW(config-if)# interface range GigabitEthernet 0/4-5
SW(config-if-range)# switchport description End-User-Ports-In-Community-PVLAN
SW(config-if-range)# switchport mode private-vlan host
SW(config-if-range)# switchport private-vlan host-association 100 102
```

Using the Protected Port Feature

- The PVLAN feature is not available on all switches.
- Protected port, also known as the PVLAN edge, is a feature that (unlike PVLANs) has only local significance to the switch.
- Protected ports do not forward any traffic to protected ports on the same switch.

- SW(config)# **interface** *interface-slot/number*
- SW(config-if)# **switchport protected**

Chapter 10 Summary

- Configure port security to limit and filter MAC addresses on ports; port security supports features that reduce the overhead of assigning MAC addresses per port.
- Use PVLANs to restrict traffic within a VLAN with simple configuration.
- Leverage DHCP snooping, DAI, and IPSG to prevent spoofing attacks.
- Consider VACLs when appropriate to block unnecessary traffic and known traffic attacks.
- Always adhere to basic security configurations such as AAA on all Cisco devices.
- Stay current on all vulnerabilities and security notices from Cisco.
- Keep current on Cisco Catalyst software versions because new software versions address known vulnerabilities.

Chapter 10 Labs

- **CCNPv7.1 SWITCH Lab 10.1 Securing Layer2**
- **CCNPv7.1 SWITCH Lab 10.2 Securing VLANs**

Cisco | Networking Academy®
Mind Wide Open™

Acknowledgment

- *Some of the images and texts are from Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: (CCNP SWITCH 300-115)* by Richard Froom and Erum Frahim (1587206641)
- Copyright © 2015 – 2016 Cisco Systems, Inc.
- Special Thanks to *Bruno Silva*