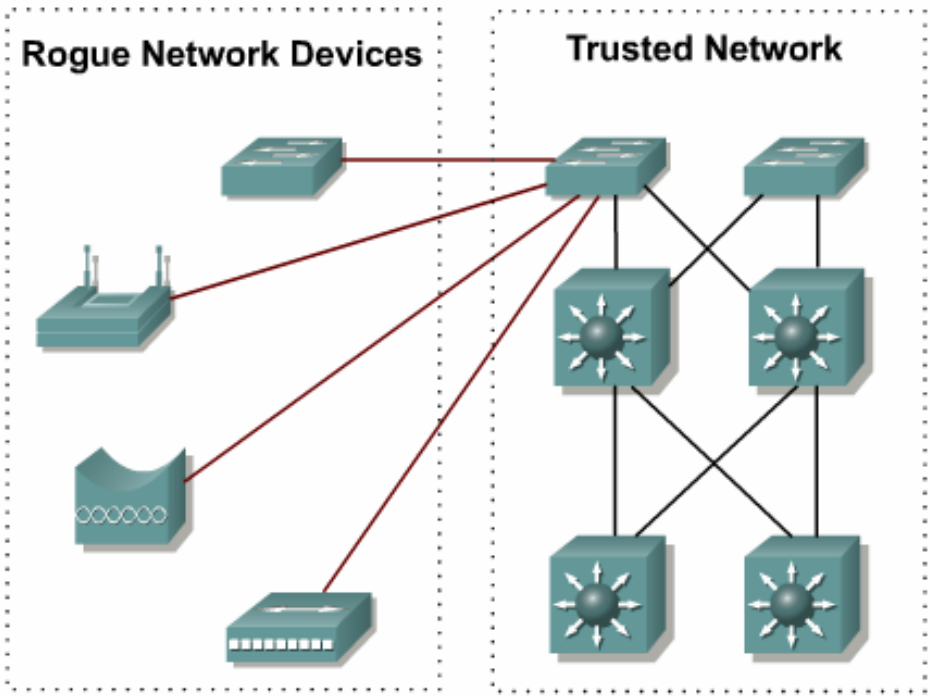
CCNP 3 - Module 08

Minimizing Service Loss and Data Theft in a Campus Network

Objectives

Upon completion of this module, the student will be able to perform tasks related to the following:	
8.1	Understanding Switch Security Issues
8.2	Protecting against VLAN Attacks
8.3	Protecting against Spoof Attacks
8.4	Describing STP Security Mechanisms
8.5	Preventing STP Forwarding Loops
8.6	Securing Network Switches
8.7	Security Lab Exercises

Unauthorized Access by Rogue Devices



- Rogue network devices can be:
  - Wireless hubs
  - Wireless routers
  - Access switches
  - Hubs
- These devices are typically connected at access level switches.

Switch Attack Categories

- Layer 2 malicious attacks are typically launched by a device connected to the campus network.
- This can be a physical rogue device placed on the network or an external intrusion that takes control of and launches attacks from a trusted device.
- In either case, the network sees all traffic as originating from a legitimate connected device.
- The following lists the types of attacks launched against switches and Layer 2:

  MAC layer attacks

  VLAN attacks

  Spoof attacks

  Switch device attacks

MAC layer attacks

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

Attack Method	Description	Steps to Mitigation
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 may need protection from one another, even though they are on a common VLAN. This is especially true on service provider segments supporting devices from multiple customers.	Implement private VLANs (PVLANs).

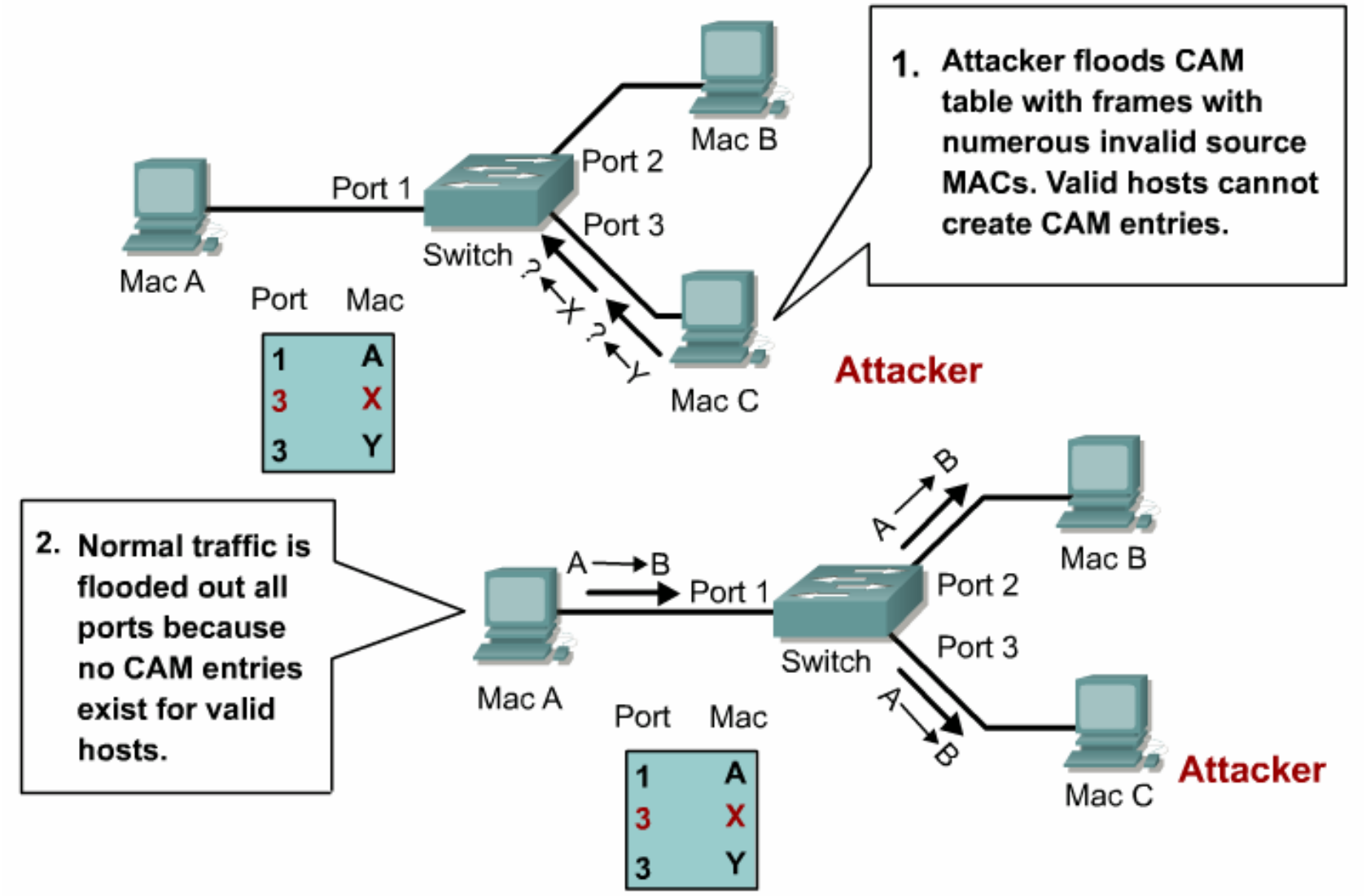
Spoof attacks

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. 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. DHCP snooping, port security.

Switch device attacks

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 virtual terminal (vty) ACLs.

MAC layer attacks



Port Security

- Cisco Catalyst switches include port security as a feature.
- 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 then provides access only to frames from those addresses.
- If the number of addresses is limited to four but no specific MAC addresses are configured, the port allows any four MAC addresses to be learned dynamically, and port access is then limited to those four dynamically learned addresses.

Port Security

- A Port Security feature called “sticky learning,” which is available on some switch platforms, combines the features of dynamically learned and statically configured addresses.
- When this feature is configured on an interface, the interface converts dynamically learned addresses to “sticky secure” addresses.
- The addresses are added to the running configuration as if they were configured using the switchport port-security mac-address command.

Port Security Configuration Commands

Step	Description
1	Enables port security. `Switch(config-if)#switchport port-security`
2	Sets a maximum number of MAC addresses that will be allowed on this port. Default is one. `Switch(config-if)#switchport port-security maximum value`
3	Specifies which MAC addresses will be allowed on this port (optional). `Switch(config-if)#switchport port-security mac-address mac-address`
4	Defines which 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 Show Commands

```
Switch#show port-security interface type mod/port
```

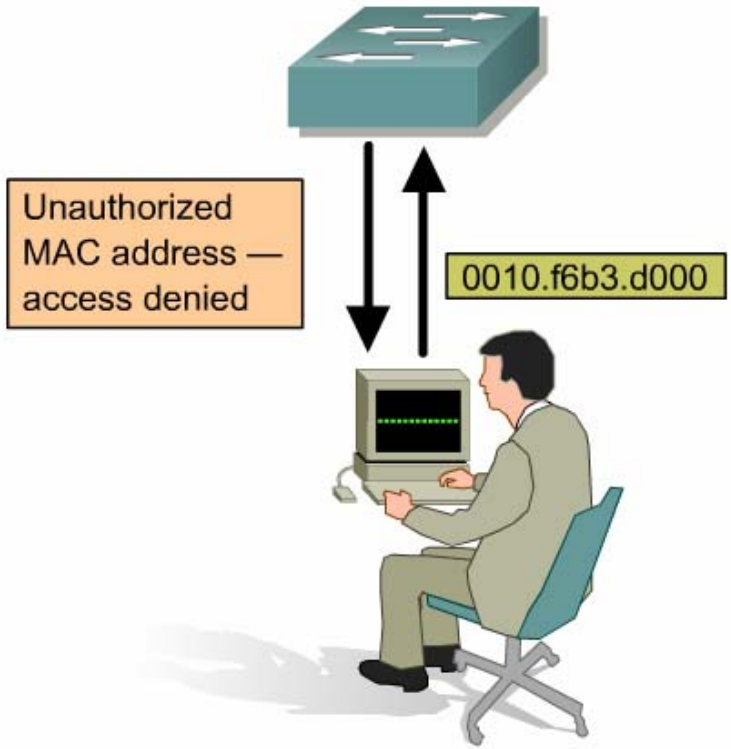
- Displays security information for a specific interface

```
Switch#show port-security interface fastethernet 5/1

Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

Port Security – Sticky configuration

- **switchport port-security mac-address sticky**

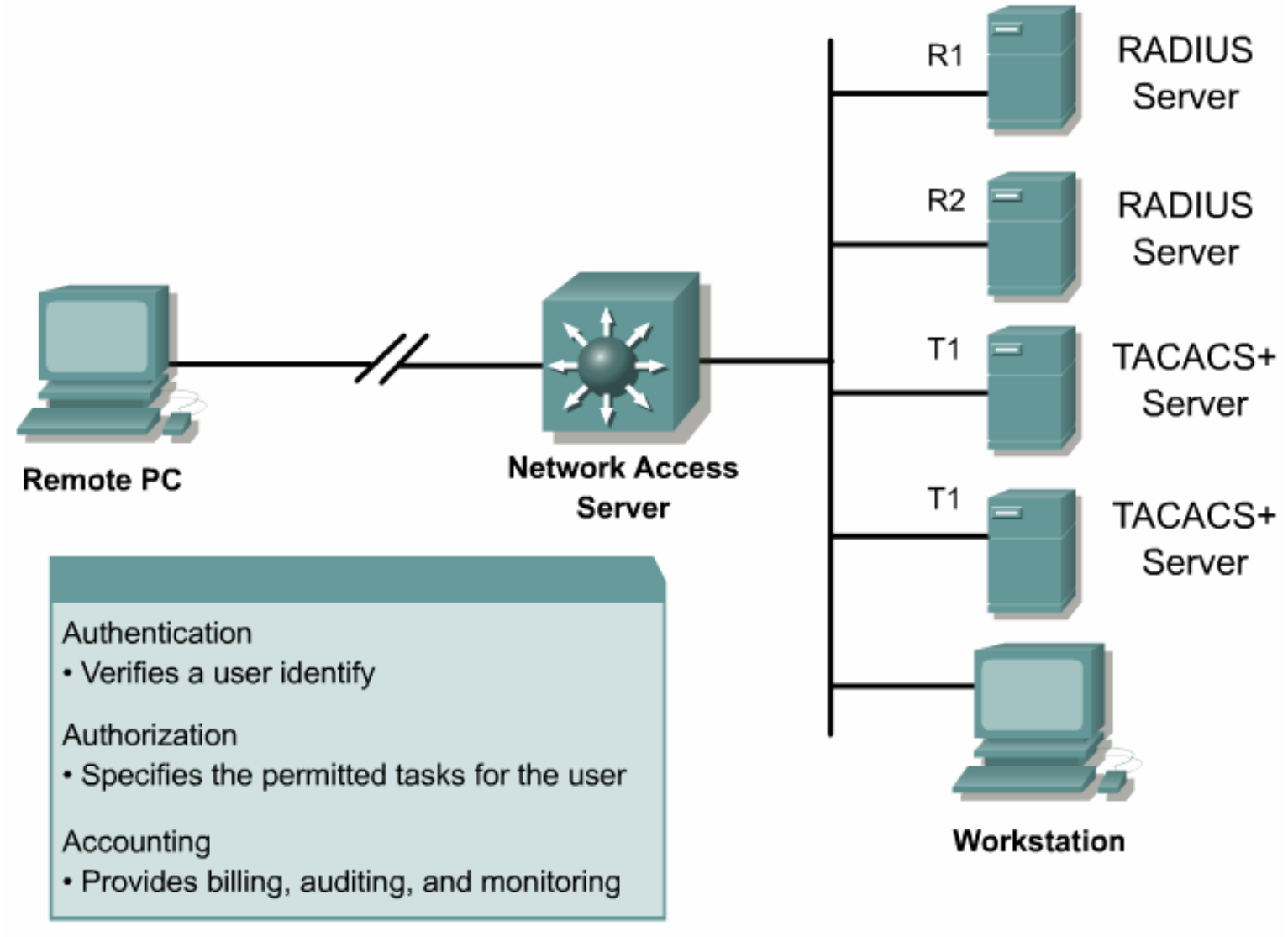


Sticky MAC stores dynamically learned MAC addresses.

AAA
Authentication, authorization, and accounting

- Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which access control is set up on a switch.
- AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner.
- AAA provides a modular way of performing these services.
- For purposes of this course, only authentication is discussed.

AAA
Authentication, authorization, and accounting



Authentication

- Authentication is the way a user is identified before being allowed access to the network and network services.
- AAA authentication is configured by defining a list of named authentication methods and then applying that list to various interfaces.
- The method list defines the types of authentication to be performed and in which sequence they are performed.
- The method list must be applied to a specific interface before any of the defined authentication methods are performed.
- If there is no defined method list, the default method list (named “default”) is applied. A defined method list overrides the default method list.

Authentication

- **In many circumstances, AAA uses protocols such as RADIUS, TACACS+, or 802.1x to administer security functions.**
- **If the switch is acting as a network access server, AAA is the means through which a switch establishes communication between the network access server and the RADIUS, TACACS+, or 802.1x security server.**

AAA Configuration

Step	Description
1.	Enable AAA by using the **`aaa new-model`** global configuration command.
2.	If a separate security server is used, configure security protocol parameters such as RADIUS, TACACS+, or Kerberos.
3.	Define the method lists for authentication by using an **`aaa authentication`** command.
4.	Apply the method lists to a particular interface or line, if required.

AAA Configuration

```
Switch(config)#aaa authentication login {default |
list-name} method1 [method2...]
```

- Creates a local authentication list

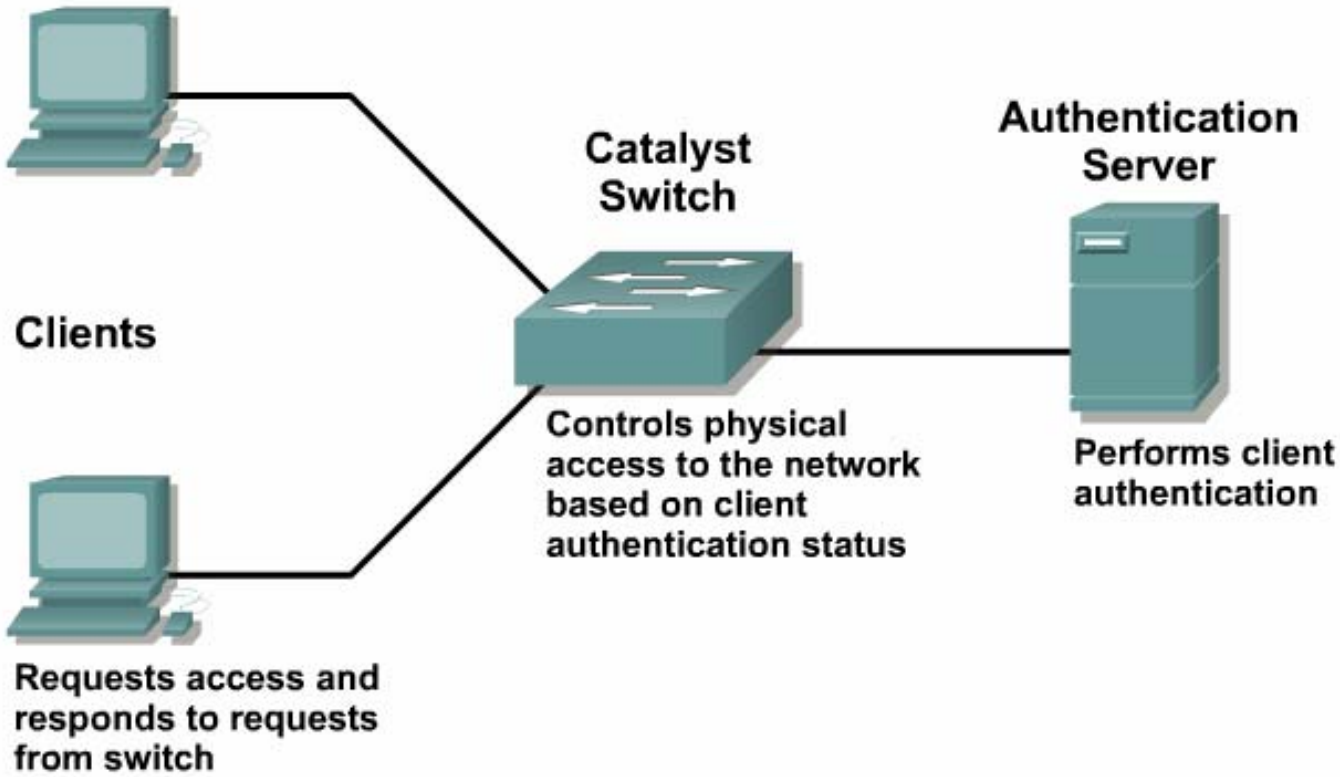
Cisco IOS AAA supports these authentication methods:

- Enable password
- Kerberos 5
- Kerberos 5-Telnet authentication
- Line password
- Local database
- Local database with case sensitivity
- No authentication
- RADIUS
- TACACS+

802.1x Port-Based Authentication

- The IEEE 802.1x standard defines a port-based access control and authentication protocol that restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports.
- The authentication server authenticates each workstation connected to a switch port before making available any services offered by the switch or the LAN.
- Until the workstation is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the workstation is connected.
- After authentication succeeds, normal traffic can pass through the port.

802.1x Port-Based Authentication



Network access through switch requires authentication.

802.1x Configuration Commands

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

- Enables AAA

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

- Creates an 802.1x port-based authentication method list

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

- Globally enables 802.1x port-based authentication

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

- Enters interface configuration mode

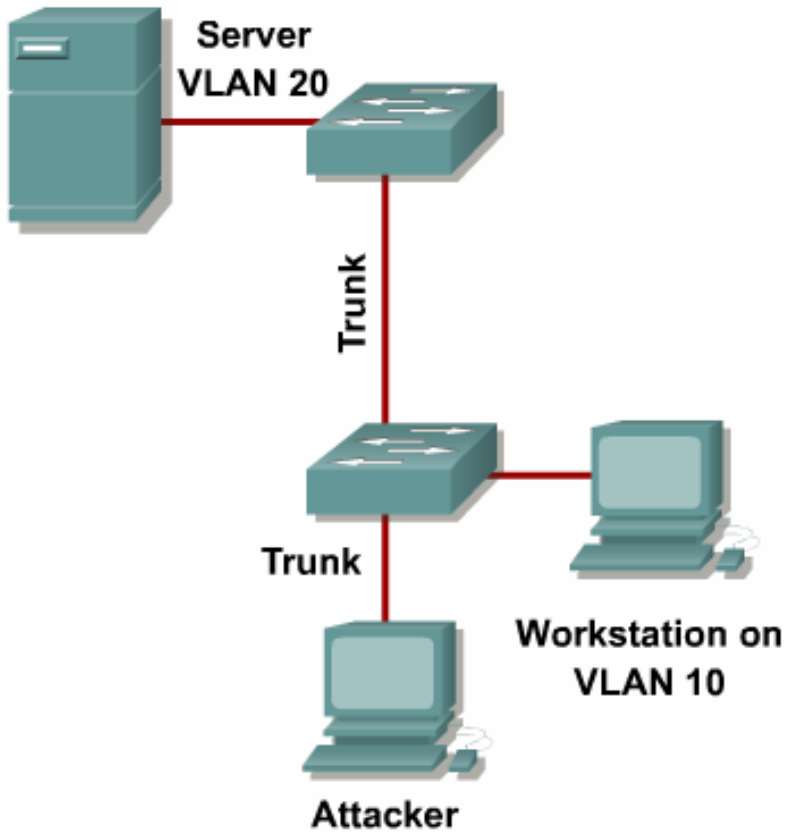
```
Switch(config-if)#dot1x port-control auto
```

- Enables 802.1x port-based authentication on the interface

802.1x Configuration Example

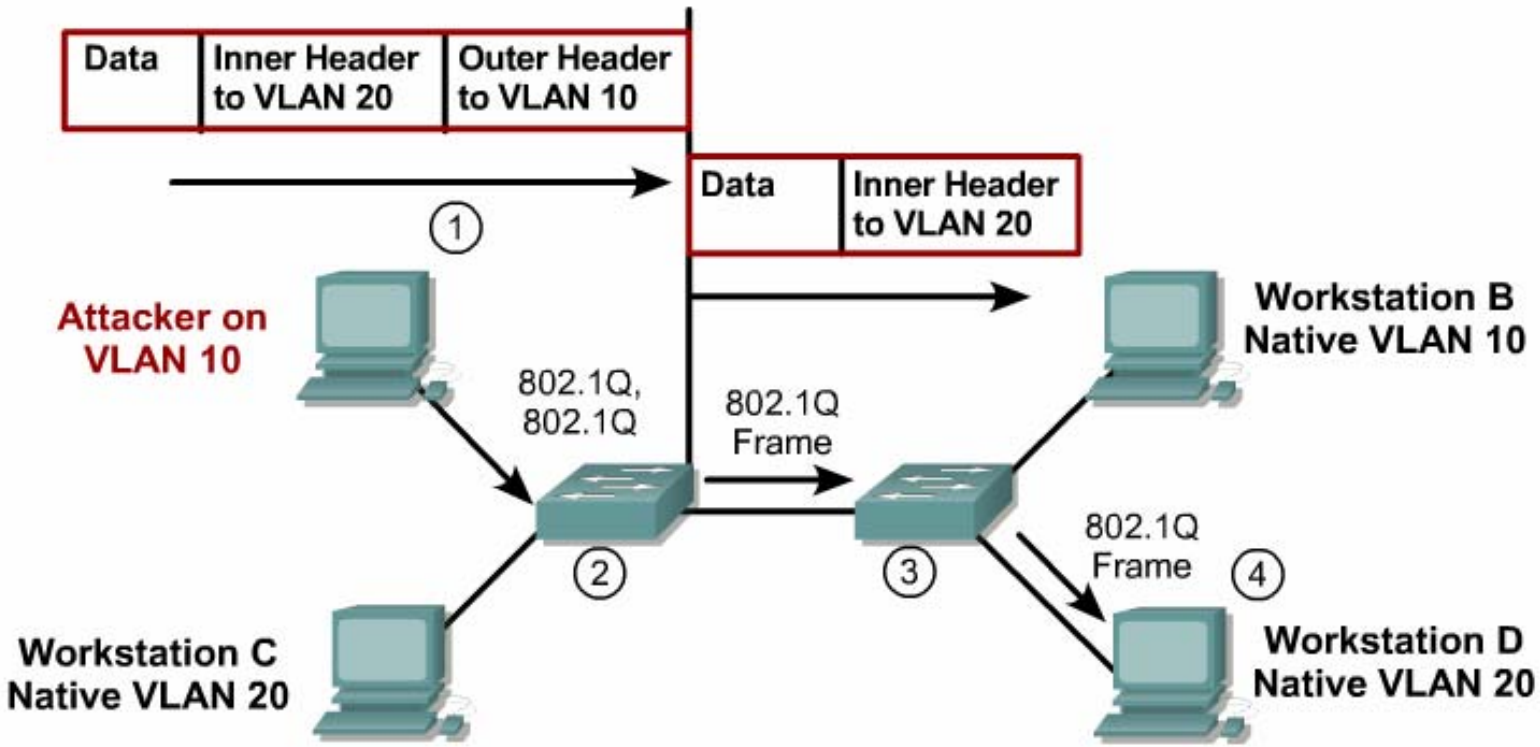
```
Switch#configure terminal
Switch(config)#aaa new-model
Switch(config)#radius-server host 172.120.39.46 auth-
port 1812 key rad123
Switch(config)#aaa authentication dot1x default group
radius
Switch(config)#dot1x system-auth-control
Switch(config)#interface fastethernet 5/1
Switch(config-if)#dot1x port-control auto
Switch(config-if)#end
```

VLAN Hopping



- Attacking system spoofs itself as a legitimate trunk negotiating device.
- Trunk link is negotiated dynamically.
- Attacking device gains access to data on all VLANs carried by the negotiated trunk.

VLAN Hopping



Double tagging allows a frame to be forwarded to a destination VLAN other than the source's VLAN.

Mitigating VLAN Hopping

- **The measures to defend the network from VLAN hopping consist of a series of best practices for all switch ports and a set of parameters to follow when establishing a trunk port:**

  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 with a VLAN designated only for unused ports, carrying no user data traffic.

- **When establishing a trunk link, configure the following:**

  Make the native VLAN different from any data VLANs

  Set trunking as “on,” rather than negotiated

  Specify the VLAN range to be carried on the trunk

Access Control Lists

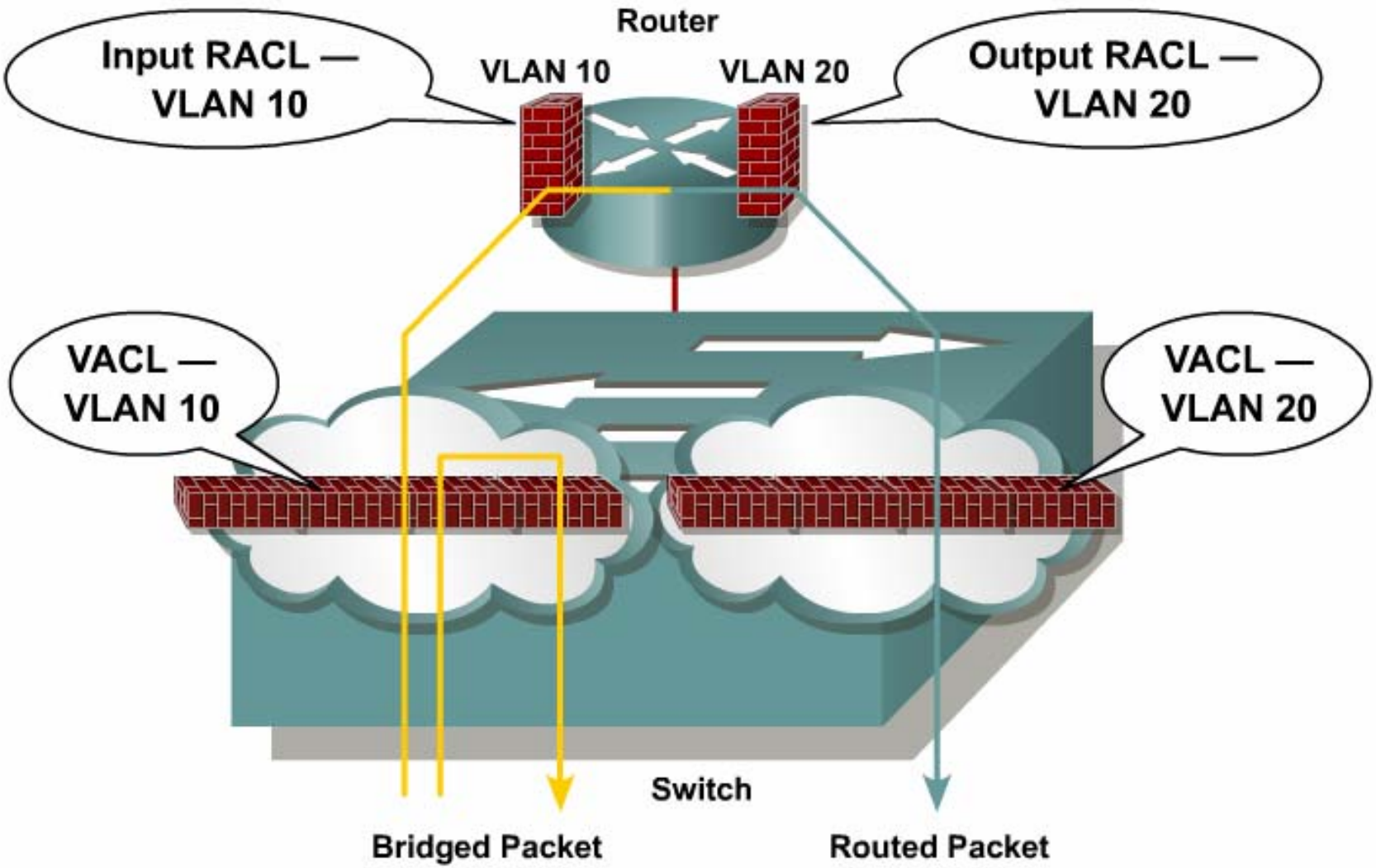
- **Cisco multilayer switches support three types of ACLs:**

  Router access control list (RACL): Applied to Layer 3 interfaces such as SVI or L3 routed ports. It controls the access of routed traffic between VLANs. RACLs are applied on interfaces for specific directions (inbound or outbound). You can apply one access list in each direction.

  Port access control list (PACL): Applied on a Layer 2 switch port, trunk port, or EtherChannel port. PACLs perform access control on traffic entering a Layer 2 interface. With PACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses.

  VLAN access control list (VACL): Supported in software on Cisco multilayer switches. Filtering based on Layer 2 or Layer 3 parameters within a VLAN. Unlike RACLs, VACLs are not defined by direction (input or output).

Access Control Lists



VLAN ACL

- VACLs (also called VLAN access maps in Cisco IOS software) apply to all traffic on the VLAN.
- You can configure VACLs for IP and MAC-layer traffic.VACLs follow route-map conventions in which map sequences are checked in order.
- Three VACL actions are permitted:

  Permit (with capture, Catalyst 6500 only)

  Redirect (Catalyst 6500 only)

  Deny (with logging, Catalyst 6500 only)

VLAN ACL

- **Two features are supported only on the Cisco Catalyst 6500:**

  VACL capture: Forwarded packets are captured on capture ports. The capture option is only on permit ACEs. The capture port can be an IDS monitor port or any Ethernet port. The capture port must be in an output VLAN for Layer 3 switched traffic.

  VACL redirect: Matching packets are redirected to specified ports. You can configure up to five redirect ports. Redirect ports must be in a VLAN where the VACL is applied.

VLAN ACL Configuration

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

- Defines a VLAN access map

```
Switch(config-access-map)# match {ip address {1-199 |
1300-2699 | acl_name} | ipx address {800-999 |
acl_name}| mac address acl_name}
```

- Configures the match clause in a VLAN access map sequence

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

- Configures the action clause in a VLAN access map sequence

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

- Applies the VLAN access map to the specified VLANs

VLAN ACL Configuration Example

```
Switch(config)# vlan access-map PxR1 10
Switch(config-access-map)# match ip address 1
Switch(config-access-map)# action drop
Switch(config-access-map)# vlan access-map PxR1 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter PxR1 vacl vlan-list 1-4094
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255

!
vlan access-map PxR1 10
 action drop
 match ip address 1
vlan access-map PxR1 20
 action forward
vlan filter PxR1 vlan-list 1-4094
vlan internal allocation policy ascending
```

Private VLANs

- Internet service providers (ISPs) often have devices from multiple clients, as well as their own servers, on a single Demilitarized Zone (DMZ) segment or VLAN.
- As security issues proliferate, it becomes necessary to provide traffic isolation between devices, even though they may exist on the same Layer 3 segment and VLAN.
- Catalyst 6500/4500/3750/3560 switches implement private VLANs to keep some switch ports shared and some isolated, although all ports exist on the same VLAN.
- The 2960 supports “protected ports,” which is functionally similar to PVLANs on a per-switch basis.

Private VLANs

- The traditional solution to address these ISP requirements is to provide one VLAN per customer, with each VLAN having its own IP subnet. A Layer 3 device then provides interconnectivity between VLANs and Internet destinations.
- These are the challenges with this traditional solution:

  Supporting a separate VLAN per customer may require a high number of interfaces on service provider network devices.

  Spanning tree becomes more complicated with many VLAN iterations.

  Network address space must be divided into many subnets, which wastes space and increases management complexity.

  Multiple ACL applications are required to maintain security on multiple VLANs, resulting in increased management complexity.

Private VLANs

- **PVLANs and protected ports provide Layer 2 isolation between ports within the same VLAN.**
- **This isolation eliminates the need for a separate VLAN and IP subnet per customer.**

Protected Port

- A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port.
- Traffic cannot be forwarded between protected ports at Layer 2; all traffic passing between protected ports must be forwarded through a Layer 3 device.
- The forwarding behavior between a protected port and a non-protected port is not affected and proceeds normally.

```
Switch#configure terminal
Switch(config)#interface fa0/1
Switch(config-if)#[no] switchport protected
Switch(config-if)#end
Switch#show interfaces fa0/1 switchport

Name: Fa0/1

Switchport: Enabled
<output truncated>

Protected: True
```

Private VLANs

- **A port in a PVLAN can be one of three types:**

  Isolated: Has complete Layer 2 separation from other ports within the same PVLAN, except for the promiscuous port. PVLANs block all traffic to isolated ports, except the traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports.

  Promiscuous: Communicates with all ports within the PVLAN, including the community and isolated ports. The default gateway for the segment would likely be hosted on a promiscuous port, given that all devices in the PVLAN need to communicate with that port.

  Community: Communicate among themselves and with their promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities, or in isolated ports within their PVLAN.

Private VLANs

- **PVLAN ports are associated with a set of supporting VLANs that are used to create the PVLAN structure. A PVLAN uses VLANs in three ways:**

  As a primary VLAN: Carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same primary VLAN.

  As an isolated VLAN: Carries traffic from isolated ports to a promiscuous port.

  As a community VLAN: Carries traffic between community ports and to promiscuous ports. You can configure multiple community VLANs in a PVLAN.

- **Isolated and community VLANs are called secondary VLANs.**

  You can extend PVLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support PVLANs.

Private VLANs Configuration

```
Switch(config-vlan)#private-vlan [primary | isolated |
community]
```

- Configures a VLAN as a private VLAN

```
Switch(config-vlan)#private-vlan association
{secondary_vlan_list | add svl | remove svl}
```

- Associates secondary VLANs with the primary VLAN

```
Switch#show vlan private-vlan type
```

- Verifies private VLAN configuration

Private VLANs Configuration

```
Switch(config-if)#switchport mode private-vlan {host |
promiscuous}
```

- Configures an interface as a private VLAN port

```
Switch(config-if)#switchport private-vlan host-
association {primary_vlan_ID secondary_vlan_ID}
```

- Associates an isolated or community port with a private VLAN

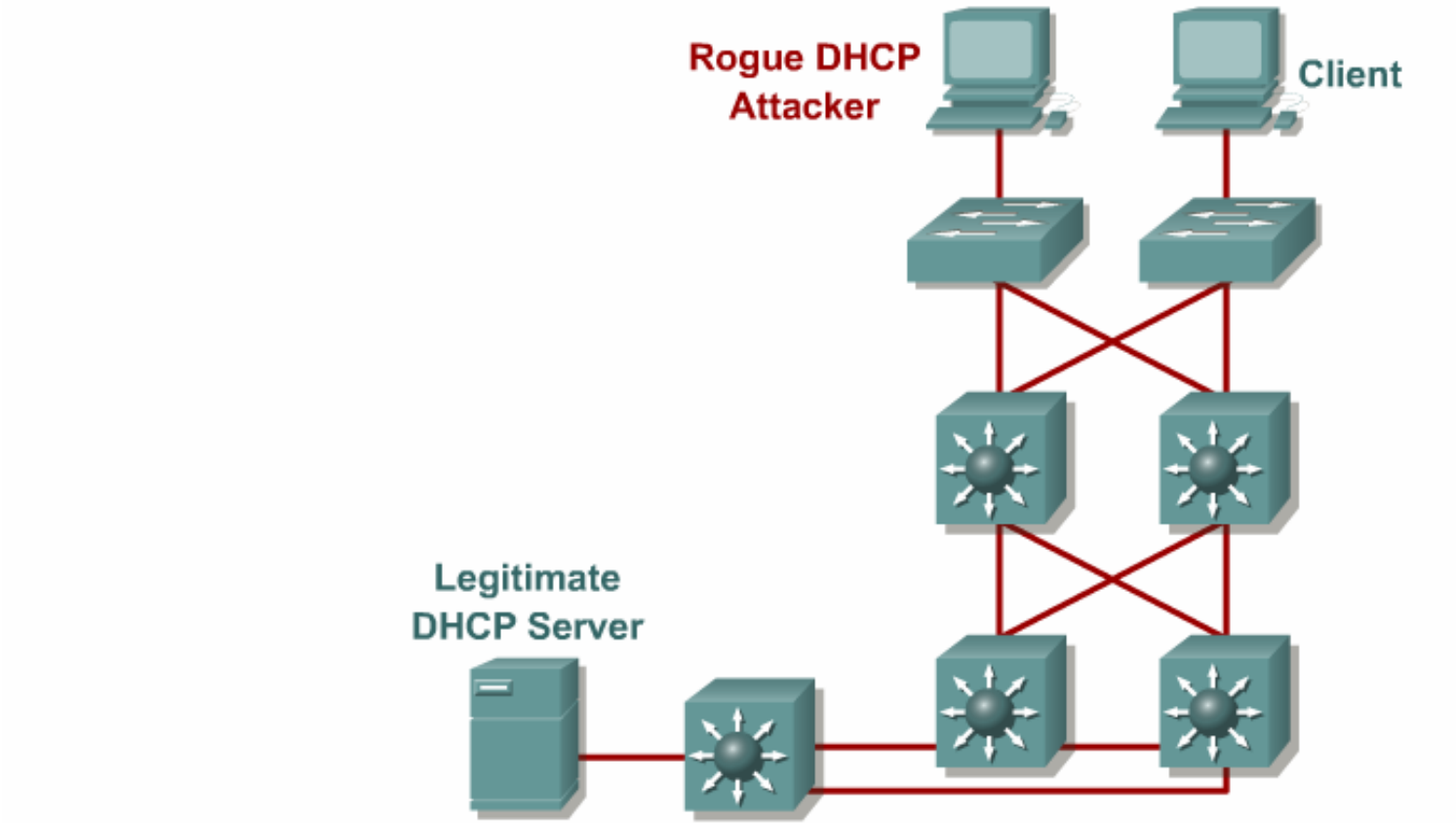
```
Switch(config-if)#private-vlan mapping primary_vlan_ID
{secondary_vlan_list | add svl | remove svl}
```

- Maps a promiscuous PVLAN port to a private VLAN

```
Switch#show interfaces private-vlan mapping
```

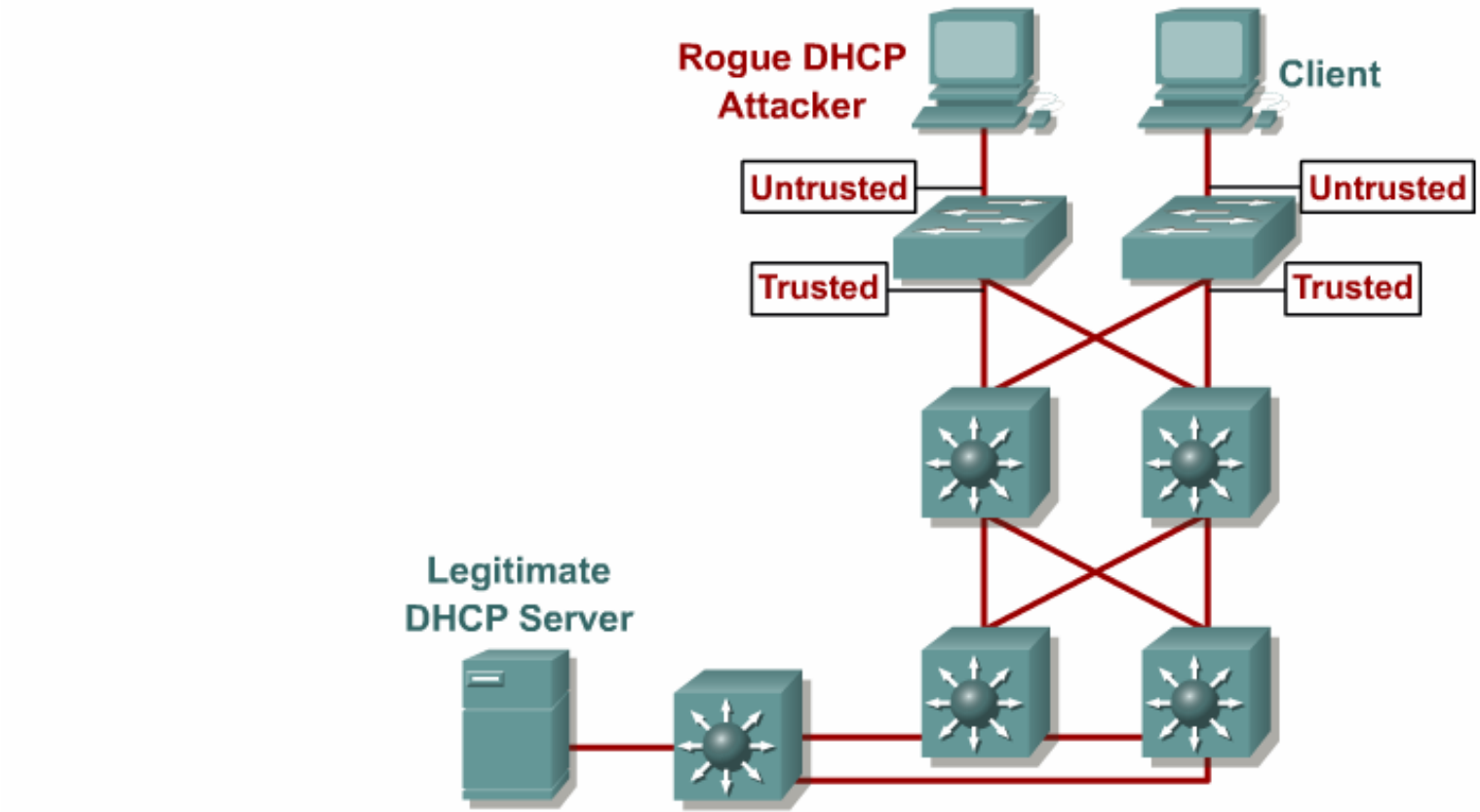
- Verifies private VLAN port configuration

Describing a DHCP Spoof Attack



- Attacker activates DHCP server on VLAN.
- Attacker replies to valid client DHCP requests.
- Attacker assigns IP configuration information that establishes rogue device as client default gateway.
- Attacker establishes "man-in-the-middle" attack.

DHCP Snooping



- DHCP snooping allows the configuration of ports as trusted or untrusted.
- Untrusted ports cannot process DHCP replies.
- Configure DHCP snooping on uplinks to a DHCP server.
- Do not configure DHCP snooping on client ports.

DHCP Snooping

- Untrusted ports are those not explicitly configured as trusted.
- A DHCP binding table is built for untrusted ports.
- Each entry contains the client MAC address, IP address, lease time, binding type, VLAN number, and port ID recorded as clients make DHCP requests.
- The table is then used to filter subsequent DHCP traffic.
- From a DHCP snooping perspective, untrusted access ports should not send any DHCP server responses, such as DHCPOFFER, DHCPACK, or DHCPNAK.

DHCP Snooping

- With the DHCP option-82 feature enabled on the switch, port-to-port DHCP broadcast isolation is achieved when the client ports are within a single VLAN.
- During client-to-server exchanges, broadcast requests from clients connected to VLAN access ports are intercepted by a relay agent running on the switch and are not flooded to other clients on the same VLAN.
- The relay agent inserts additional information inside the DHCP request packet, such as which port the request originated from, and then forwards it to the DHCP server.
- During server-to-client exchanges, the DHCP (option-82 aware) server sends a broadcast reply that contains the option-82 field.
- The relay agent uses this information to identify which port connects to the requesting client and avoids forwarding the reply to the entire VLAN

DHCP Snooping Configuration

```
Switch(config)# ip dhcp snooping
```

- Enables DHCP snooping globally

```
Switch(config)# ip dhcp snooping information option
```

- Enables DHCP option-82 data insertion

```
Switch(config-if)# ip dhcp snooping trust
```

- Configures a trusted interface

```
Switch(config)# ip dhcp snooping limit rate [rate]
```

- Number of packets per second accepted on a port

```
Switch(config)# ip dhcp snooping vlan number [number]
```

- Enables DHCP snooping on your VLANs

DHCP Snooping Configuration

```
Switch# show ip dhcp snooping
```

- Verifies the DHCP snooping configuration

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP Snooping is configured on the following VLANs:
    10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface            Trusted        Rate limit (pps)
---------            -------        ----------------
FastEthernet2/1      yes            none
FastEthernet2/2      yes            none
FastEthernet3/1      no             20
Switch#
```

IP Source Guard

- IP source guard is a security feature that prevents IP source address spoofing.
- This feature is enabled on a DHCP snooping untrusted Layer 2 port. All IP traffic on the port is blocked, except for DHCP packets that are allowed by the DHCP snooping process.
- When a client receives a valid IP address from the DHCP server, a per-port VLAN Access Control List (PVACL) is installed on the port.
- 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 ability to attack the network by claiming a neighbor host's IP address.

IP Source Guard

- **IP source guard supports only the Layer 2 ports, including both access and trunk.**
- **For each untrusted Layer 2 port, there are two levels of IP traffic security filtering, as follows:**

  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.

  Source IP and MAC address filter: IP traffic is filtered based on its source IP address as well as its MAC address. Only IP traffic with source IP and MAC addresses matching the IP source binding entry are permitted.

IP Source Guard Configuration

```
Switch(config)# ip dhcp snooping
```

- Enables DHCP snooping globally

```
Switch(config)# ip dhcp snooping vlan number [number]
```

- Enables DHCP snooping on a specific VLAN

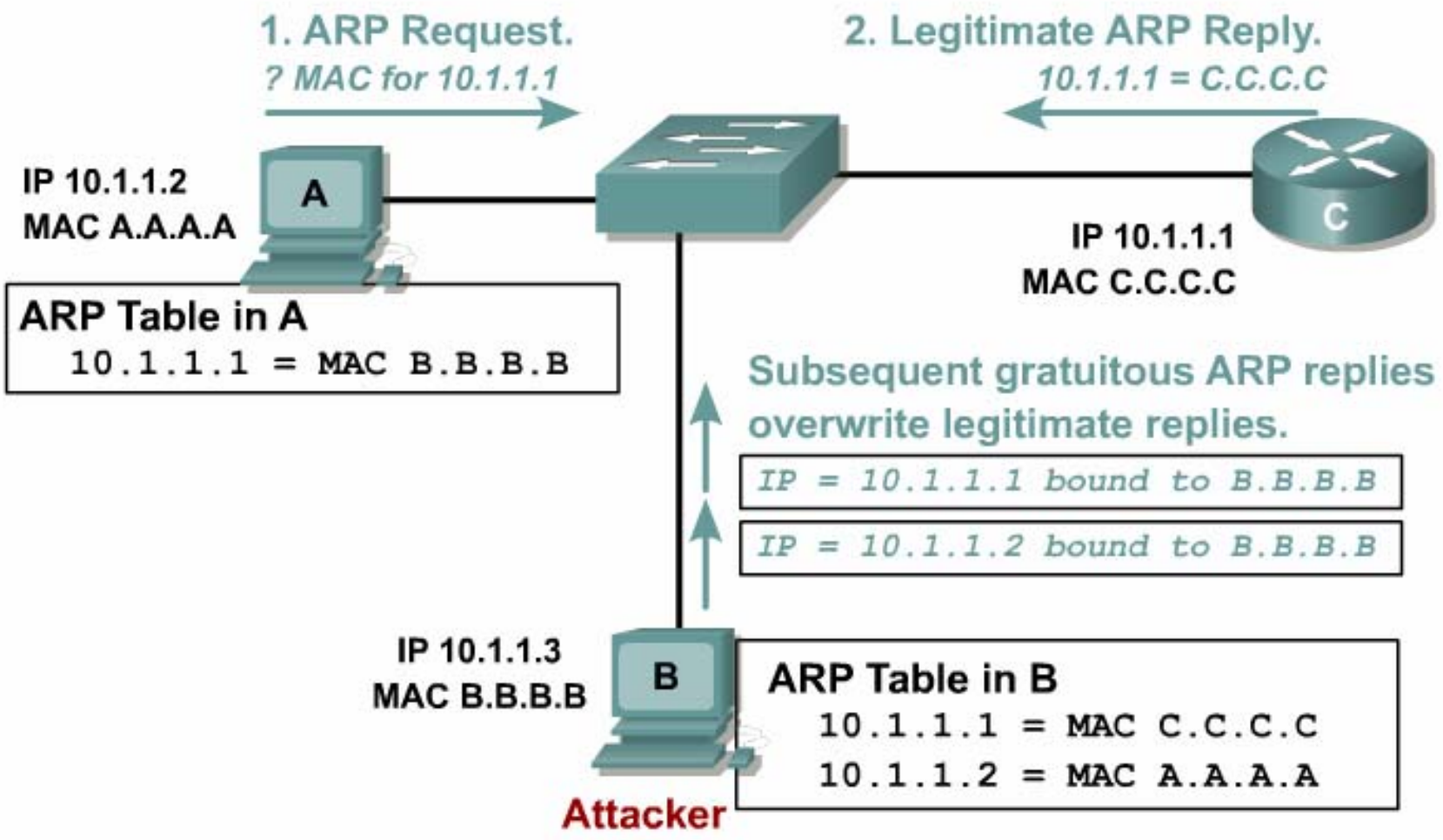
```
Switch(config-if)# ip verify source vlan
dhcp-snooping port-security
```

- Enables IP source guard, source IP and source MAC address filter on a port

- **A static IP source binding may be configured on a port via the following global command:**

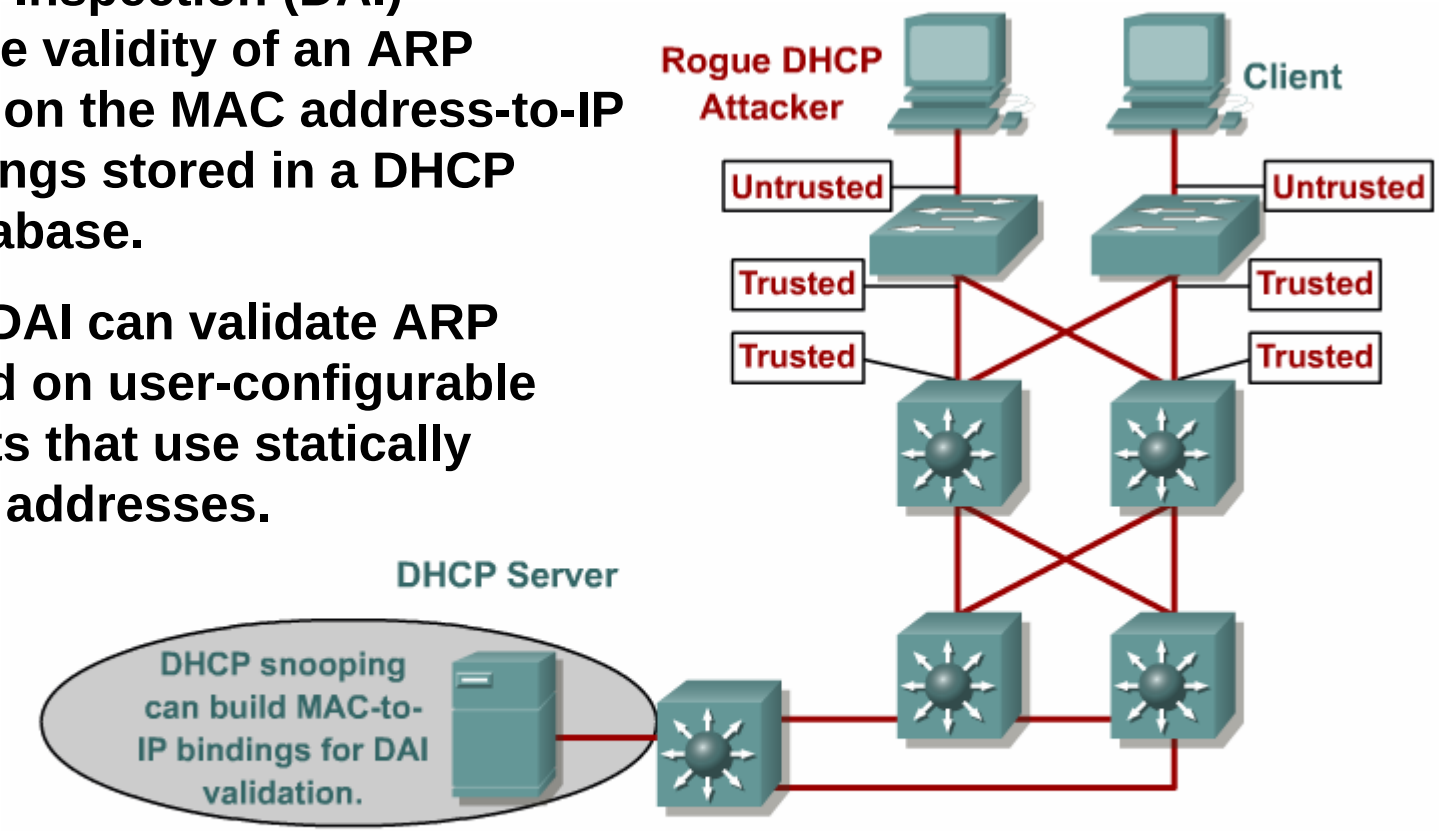
  Switch(config)#ip source binding ip-addr *ip* vlan *number* interface *inter*

Describing ARP Spoofing



Dynamic ARP Inspection

- **Dynamic ARP Inspection (DAI) determines the validity of an ARP packet based on the MAC address-to-IP address bindings stored in a DHCP snooping database.**
- **Additionally, DAI can validate ARP packets based on user-configurable ACLs for hosts that use statically configured IP addresses.**



Dynamic ARP Inspection

- **To prevent ARP spoofing or "poisoning," a switch must ensure that only valid ARP requests and responses are relayed. To ensure that only valid ARP requests and responses are relayed, DAI takes the following 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, logs, or drops and logs ARP packets with invalid IP-to-MAC address bindings**

Dynamic ARP Inspection

- Generally, all access switch ports should be cofigured as untrusted and all switch ports connected to other switches as trusted.
- All ARP packets traversing the network from an upstream distribution or core switch could bypass the security check requiring no further validation.
- You can also use DAI to set the rate limit of ARP packets and then err-disable the interface if the rate is exceeded.

Dynamic ARP Inspection Configuration

```
Switch(config)#ip arp inspection vlan vlan_id[,vlan_id]
```

- Enables DAI on a VLAN or range of VLANs

```
Switch(config-if)#ip arp inspection trust
```

- Enables DAI on an interface and sets the interface as a trusted interface

```
Switch(config-if)#ip arp inspection validate {[src-mac]
[dst-mac] [ip]}
```

- Configures DAI to drop ARP packets when the IP addresses are invalid

Protecting the Operation of STP

- Cisco provides features to protect spanning tree from loops being created on ports where PortFast has been enabled.
- In a proper configuration, PortFast would be enabled only on ports supporting end devices such as servers and workstations.
- It is anticipated that BPDUs from a switch device should not be received on a PortFast interface.
- However, should this happen, BPDU guard and BPDU filtering provide protection.
- Both BPDU guard and BPDU filtering can be configured globally on all PortFast-configured ports or on individual ports.

Protecting the Operation of STP

- BPDU guard protects the switched network from the problems that may be caused by the receipt of BPDUs on ports that should not be receiving them. The receipt of unexpected BPDUs may be accidental or may be part of an unauthorized attempt to add a switch to the network.
- PortFast BPDU filtering affects how the switch acknowledges BPDUs seen on PortFast-configured ports. Its functionality differs if it is configured globally or on a per-port basis.
- Root guard protects against a switch outside the designated network attempting to become the root bridge by blocking its access until the receipt of its BPDUs ceases.

BPDU Guard Configuration

- You can enable BPDU guard on PortFast-enabled ports at the global level. In a valid configuration, PortFast-enabled ports do not receive BPDUs.
- Receiving a BPDU on a PortFast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in an error-disabled state.

```
Switch(config)#spanning-tree portfast bpduguard default
```

- You can also enable BPDU guard on any port at the interface level without enabling the PortFast feature. When the port receives a BPDU, it is put in an error-disabled state.

```
Switch(config-if)#spanning-tree bpduguard enable
```

BPDU Filtering Global Configuration

- **BPDU global filtering has these attributes:**

  It affects all operational PortFast ports on a switch that do not have BPDU filtering configured on the individual ports.

  If BPDUs are seen, the port loses its PortFast status, BPDU filtering is disabled, and STP sends and receives BPDUs on the port like any other STP port on the switch.

  At startup, the port transmits ten BPDUs. If this port receives any BPDUs during that time, PortFast and PortFast BPDU filtering are disabled.

- **Switch(config)#spanning-tree portfast bpdufilter default**

BPDU Filtering Interface Configuration

- **BPDU filtering has these attributes when enabled on an individual port:**

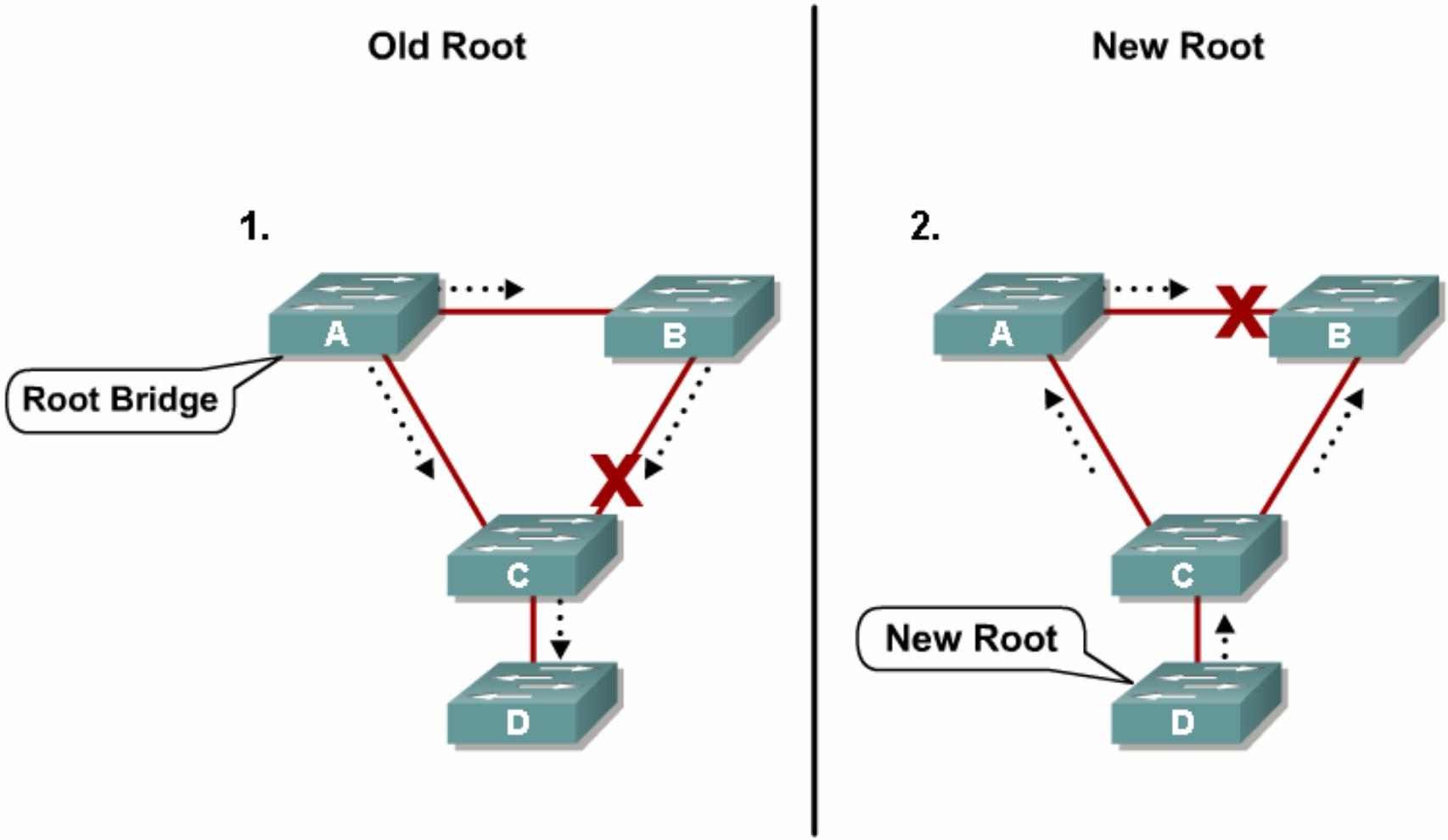
  It ignores all BPDUs received.

  It sends no BPDUs.

- **Switch(config-if)#spanning-tree bpdufilter enable**

CAUTION: Explicit configuration of PortFast BPDU filtering on a port not connected to a host station can result in bridging loops.

Root Guard



Root Guard

- Root guard limits the switch ports out of which the root bridge may be negotiated.
- If a root guard–enabled port receives BPDUs that are superior to those being sent by the current root bridge, that port is moved to a root-inconsistent state, which is effectively equal to an STP listening state.
- No data traffic will be forwarded across this port.
- Root guard is configured on a per-port basis.
- When switch stops sending superior BPDUs, the port is unblocked again and transitions through STP states like any other port. Recovery requires no intervention.

Root Guard Configuration

```
Switch(config-if)#spanning-tree guard root
```

- Configures root guard

```
Switch#show spanning-tree inconsistentports
```

- Displays information about ports in inconsistent states

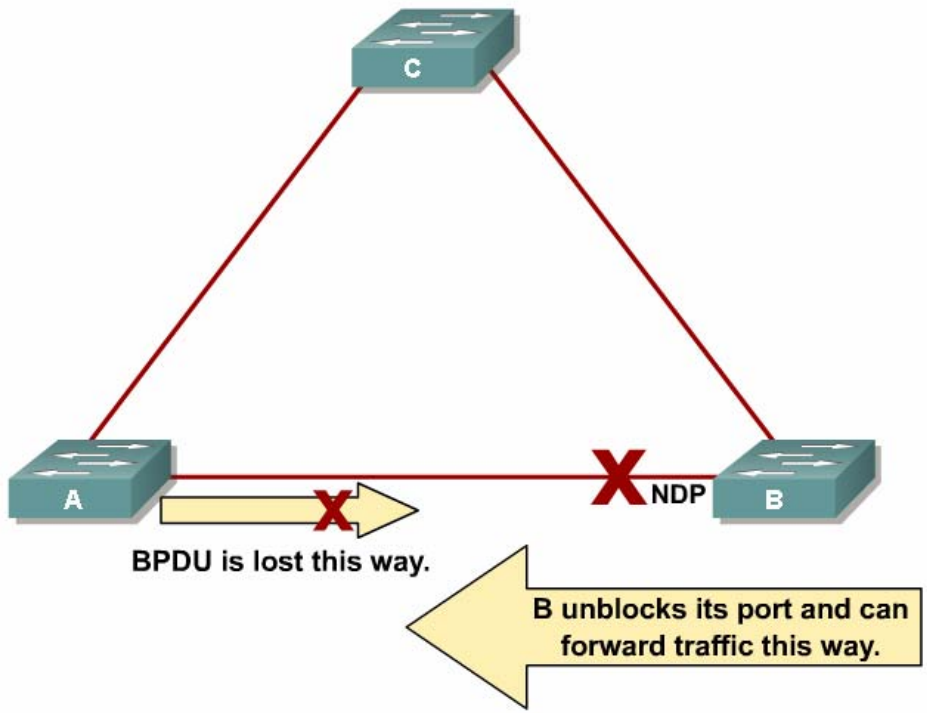
```
!
interface FastEthernet5/8
switchport mode access
spanning-tree guard root
Switch#show spanning-tree inconsistentports
Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
VLAN0001             FastEthernet3/1        Port Type Inconsistent
VLAN0001             FastEthernet3/2        Port Type Inconsistent
VLAN1002             FastEthernet3/1        Port Type Inconsistent

Number of inconsistent ports (segments) in the system :3
```

UDLD - Unidirectional Link Detection

- A unidirectional link occurs when traffic is transmitted between neighbors in one direction only. Unidirectional links can cause spanning tree topology loops. Unidirectional Link Detection (UDLD) allows devices to detect unidirectional link conditions when Layer 1 mechanisms do not, and provides the ability to shut down the affected interface.

- The switch periodically transmits UDLD packets on an interface with UDLD enabled. If the packets are not echoed back within a specific time frame, the link is flagged as unidirectional, and the interface is shut down. Devices on both ends of the link must support UDLD for the protocol to successfully identify and disable unidirectional links.



UDLD - Unidirectional Link Detection

- **UDLD can be configured in two modes:**

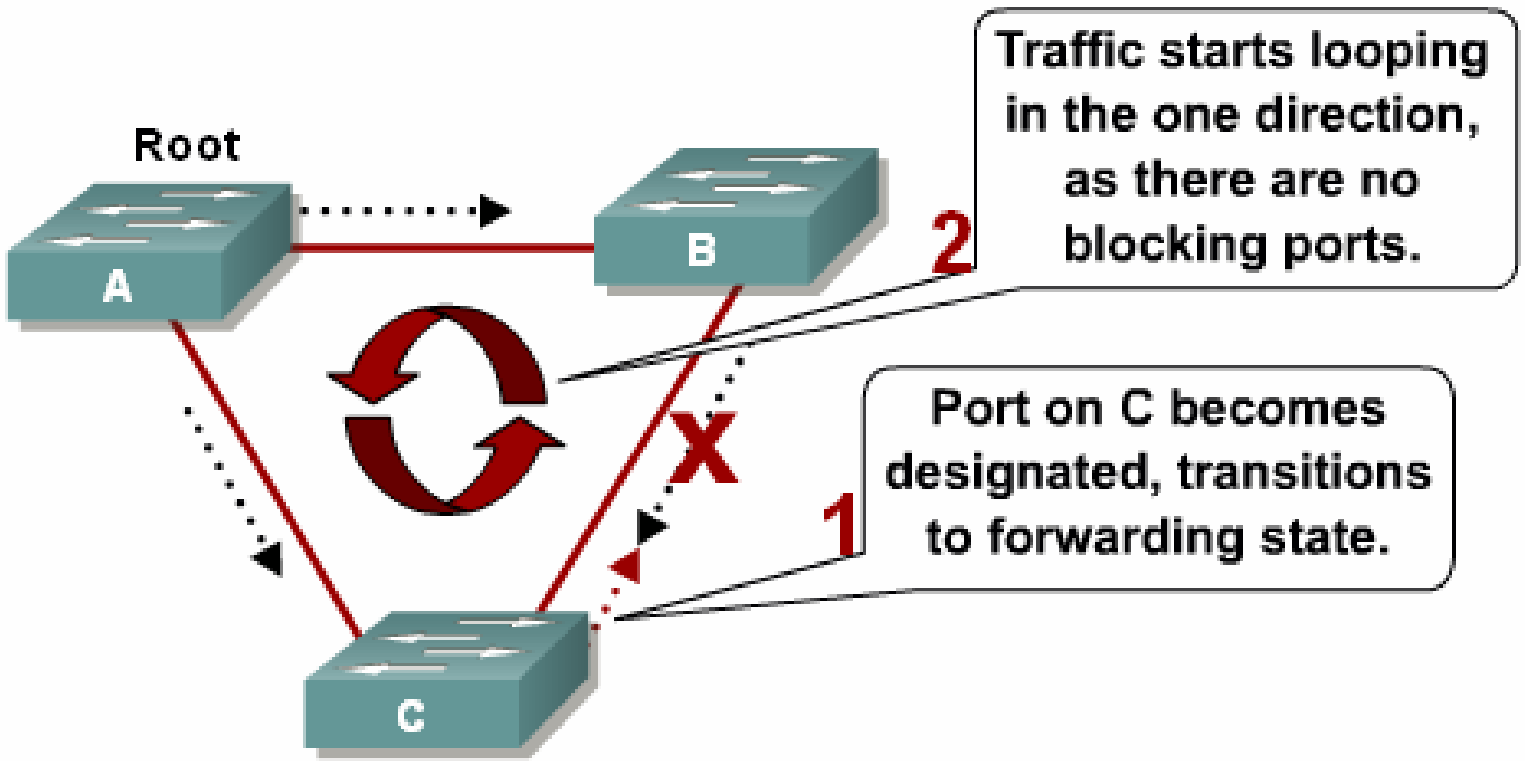
  Normal mode changes the UDLD-enabled port to an undetermined state when it stops receiving UDLD messages from its directly connected neighbor.

  Aggressive mode makes eight attempts to re-establish the UDLD neighbor relation before error disabling the port. Aggressive mode is the preferred method of configuring UDLD and is the only mode that can detect a UDLD condition on twisted-pair cable.

- **UDLD uses destination MAC 01-00-0c-cc-cc-cc with SNAP HDLC protocol type 0x0111.**

Loop Guard

- Like UDLD, loop guard provides protection for STP when a link is unidirectional and BPDUs are being sent, but not received, on a link that is considered operational.
- Without loop guard, a blocking port transitions to forwarding if it stops receiving BPDUs.



Loop Guard

- If loop guard is enabled and the link is not receiving BPDUs, the interface moves into the STP loop-inconsistent blocking state. When loop guard blocks a port, this message is generated to the console or log file:

```
SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port
3/2 in vlan 3. Moved to loop-inconsistent state.
```

- When a BPDU is received on a loop guard port that is in a loop-inconsistent state, the port transitions to the appropriate state as determined by the normal functioning of spanning tree. The recovery requires no user intervention. After the recovery, this message is logged:

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

UDLD Configuration

```
Switch(config)#udld enable
```

- Enables UDLD globally on all fiber-optic interfaces

```
Switch(config-if)#udld port
```

- Enables UDLD on an individual interface

```
Switch(config-if)#no udld port
```

- Disables UDLD on an individual non-fiber-optic interface

```
Switch# udld reset
```

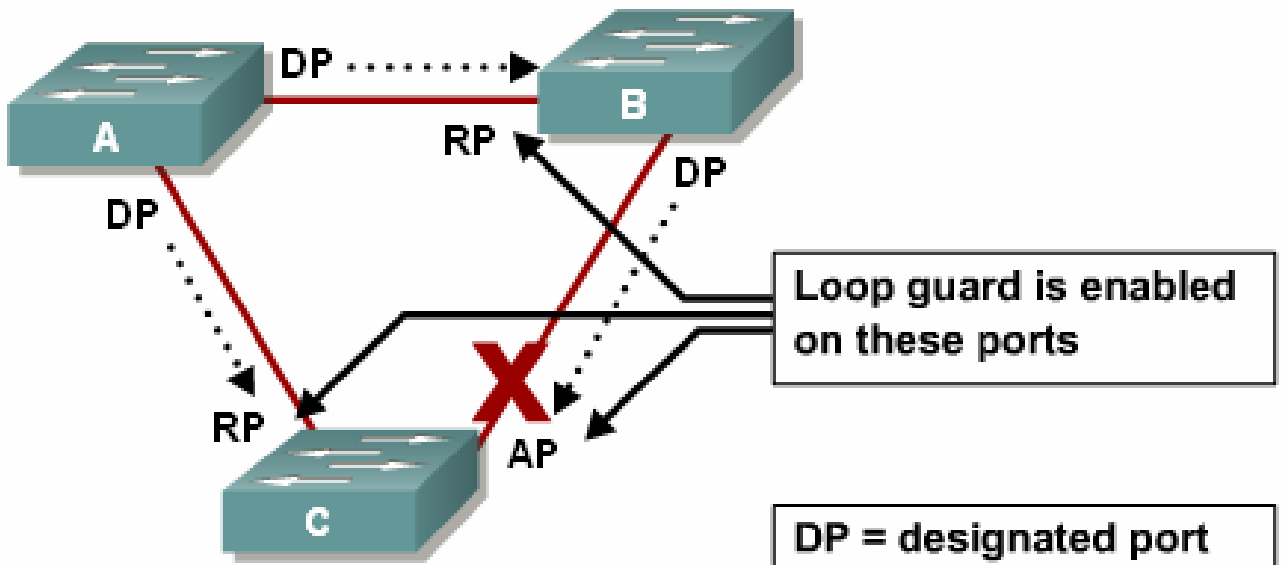
- Resets all interfaces that have been shut down by UDLD

```
Switch#show udld interface
```

- Displays UDLD information for a specific interface

Loop Guard Configuration

```
Switch(config-if)spanning-tree guard loop
```

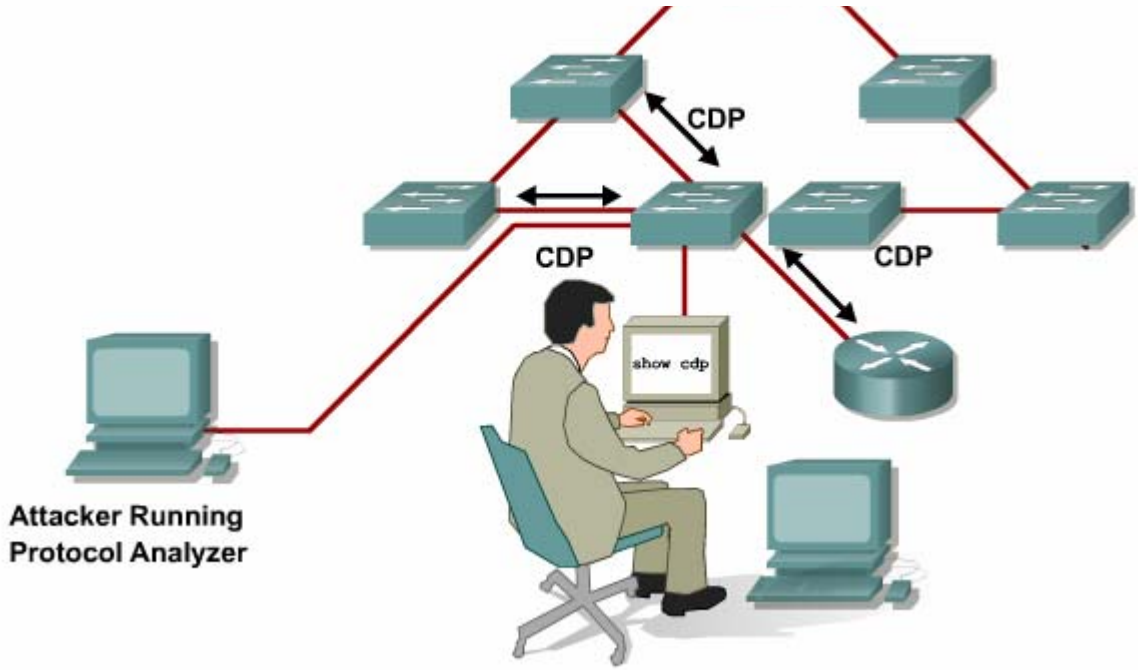


Comparing Loop Guard and UDLD

	Loop Guard	UDLD
Configuration	Per port	Per port
Action granularity	Per VLAN	Per port
Autorecovery	Yes	Yes, with error-disable timeout feature
Protection against STP failures caused by unidirectional links	Yes, when enabled on all root and alternative ports in redundant topology	Yes, when enabled on all links in redundant topology
Protection against STP failures caused by problem in software, resulting in designated switch not sending BPDU	Yes	No
Protection against miswiring	No	Yes

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.



Telnet Protocol Vulnerabilities

- **Telnet has the following 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.

  A remote attacker could find an enabled guest account that may be present anywhere within the trusted domains of the server.

SSH Protocol

- SSH is a client and server protocol used to log in to another device over a network, execute commands in a remote machine, and move files from one machine to another.
- It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, rdist, and Telnet.
- When using the SSH login (instead of Telnet), the entire login session, including password transmission, is encrypted; therefore, it is almost impossible for an outsider to collect passwords.
- Cisco's implementation of SSH requires Cisco IOS to support RSA authentication and minimum DES encryption.

SSH Protocol

- **Although SSH is secured, many vendors' implementations of SSH contain vulnerabilities that could allow a remote attacker to execute arbitrary code with the privileges of the SSH process or cause a denial of service.**
- **Most of the SSH vulnerabilities have been addressed in the latest Cisco IOS software and in other vendors' SSH server and client software.**

CAUTION: SSH version 1 implementations are vulnerable to various security compromises. Whenever possible, use SSH version 2.

Configuring SSH

- **SSH requires a local username database, ip domain, and RSA key to be generated.**

```
Switch(config)# username Joe password User
Switch(config)# ip domain-name sshtest.lab
Switch(config)# crypto key generate key
Switch(config)# line vty 0 15
Switch(config-line)# login local
Switch(config-line)# transport input ssh
```

- **You will need an application on the workstation that supports SSH, such as SecureCRT or PuTTY.**

Applying ACLs to vty Lines

```
Switch(config)#access-list access-list-number {permit |
deny | remark} source [mask]
```

- Configure a standard IP access list.

```
Switch(config)#line vty {vty# | vty-range}
```

- Enter configuration mode for a vty or vty range.

```
Switch(config-line)#access-class access-list-number in|out
```

- Restrict incoming or outgoing vty connections to addresses in the ACL.

Best Practices for Switch Security

- **Set system passwords:** Use the enable secret command to set the password that grants enabled access to the Cisco IOS system. Because the enable secret command simply implements a Message Digest 5 (MD5) hash on the configured password, that password still remains vulnerable to dictionary attacks.
- Therefore, apply standard practices in selecting a feasible password. Try to pick passwords that contain letters, numbers, and special characters, for example, “$pecia1$” instead of “specials,” where the “s” has been replaced by “$,” and the “l” has been replace with "1" (one).

Best Practices for Switch Security

- **Secure access to the console:** Console access requires a minimum level of security both physically and logically. An individual who gains console access to a system can recover or reset the system-enable password, thus allowing that person to bypass all other security implemented on that system. Consequently, it is imperative to secure access to the console.
- **Secure access to vty lines:** The minimum recommended steps for securing Telnet access are:

  Apply the basic ACL for in-band access to all vty lines.

  Configure a line password for all configured vty lines.
- **Use SSH:** The SSH protocol and application provide a secure remote connection to a switch. It encrypts all traffic, including passwords, between a remote console and a switch.

Best Practices for Switch Security

- **Configure system-warning banners:** For both legal and administrative purposes, displaying a system-warning banner prior to login is a convenient and effective way of reinforcing security and general usage policies. By clearly stating the ownership, usage, access, and protection policies before a login, you provide more solid backing for potential future prosecution.
- **Disable unneeded services:** By default, Cisco devices implement multiple TCP and User Datagram Protocol (UDP) servers to facilitate management and integration into existing environments. For most installations, these services are typically not required, and disabling them can greatly reduce overall security exposure.

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no service config
```

Best Practices for Switch Security

- **Disable the integrated HTTP daemon if not in use:** Although Cisco IOS software provides an integrated HTTP server for management, it is highly recommended that it be disabled to minimize overall exposure. If HTTP access to the switch is absolutely required, use basic ACLs to permit access from only trusted subnets.
- **Configure basic logging:** To assist and simplify problem troubleshooting and security investigations, monitor the switch subsystem information received from the logging facility. View the output in the on-system logging buffer memory. To render the on-system logging useful, increase the default buffer size.

Best Practices for Switch Security

- **Use CDP only as needed:** CDP does not reveal security-specific information, but it is possible for an attacker to exploit this information in a reconnaissance attack, whereby an attacker learns device and IP address information for the purpose of launching other types of attacks. Two practical guidelines should be followed for CDP.
- **Secure the spanning tree topology:** It is important to protect the STP process of the switches that compose the infrastructure. Inadvertent or malicious introduction of STP BPDUs could potentially overwhelm a device or pose a DoS attack.

Best Practices for Switch Security

- **Proactively configure unused router and switch ports:**

  Execute the shut 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.

- **Disable automatic trunk negotiation: By default, Cisco Catalyst switches running Cisco IOS software are configured to automatically negotiate trunking capabilities.**

- **Monitor physical device access: Avoid rogue device placement in wiring closets with direct access to switch ports.**

- **Establish port-based security: Specific measures should be taken on every access port of any switch placed into service.**

CCNP 3 - Module 08

Minimizing Service Loss and Data Theft in a Campus Network