04- Network Infrastructure Protection

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Identifying Network Device Planes

- Effective network security demands an integrated defense-in-depth approach.
- The first layer of a defense-in-depth strategy is the enforcement of the fundamental elements of network security.
- The security of a network device requires all three device planes secured.
- Configuring secure access to the network device, routing protocols, and other control features along with guaranteeing the security of the forwarded data mean to operate on three different planes: control plane, management plane, and data plane.

Identifying Network Device Planes (cont.)

- **The following are some of the expected threats to the network infrastructure:**
  - Denial of service (DoS)
  - Distributed denial of service (DDoS)
  - Unauthorized access
  - Session hijacking
  - Man-in-the-middle attack
  - Privilege escalation
  - Intrusions and Botnets
  - Routing protocol attacks
  - Spanning tree attacks
  - Layer 2 attacks

Identifying Network Device Planes (cont.)

- **It is often beneficial to think of network devices in three separate contexts, as identified by their functionality planes:**

Data Plane	Provide Traffic Forwarding Functions: Switched and Routed Data
Control Plane	Builds Control Structures Required for Traffic Forwarding
Management Plane	Provides Device Management Functions

Identifying Network Device Planes (cont.)

- **It is often beneficial to think of network devices in three separate contexts, as identified by their functionality planes (cont.)**

  - Data Plane functions are data switching and data routing. The data plane allows the device to forward network traffic and apply services (such as security, QoS, accounting, and optimization) to it as it is forwarded.
  - Control Plane allows the device to build all of the required control structures (such as the routing table, forwarding table, and MAC address table) that will allow the data plane to operate correctly.
  - Management Plane provides devices with all of the functions that administrators need to provision the configuration and monitor the operation of the device.

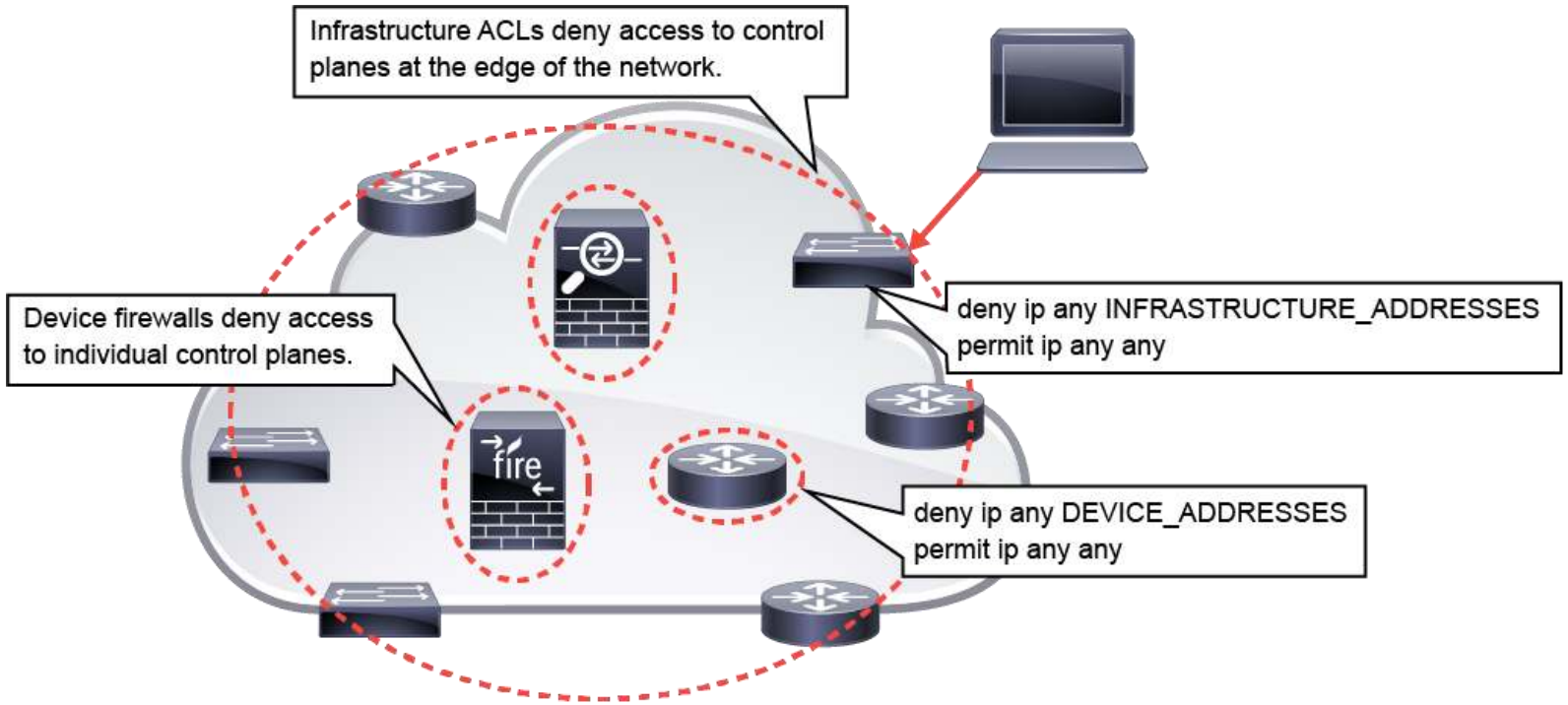
4.1- Control Plane Security Controls

Infrastructure ACLs

- Because the CPU is shared among the three functions (control plane, management plane, slow data path), excessive traffic to one of these three functions can, by default, overwhelm the entire CPU and influence the behavior of the other two functions.
- This setup can lead to flooding attacks, in which the attacker can disable these three functions by sending a high rate of packets to the CPU.
- There are multiple possible countermeasures that guard against this threat, and one of them is the infrastructure access control list (ACL).

Infrastructure ACLs (cont.)

- Infrastructure ACLs filter traffic on the network edge of access OSI Layer 3 devices that accept IP traffic from network users or external networks.

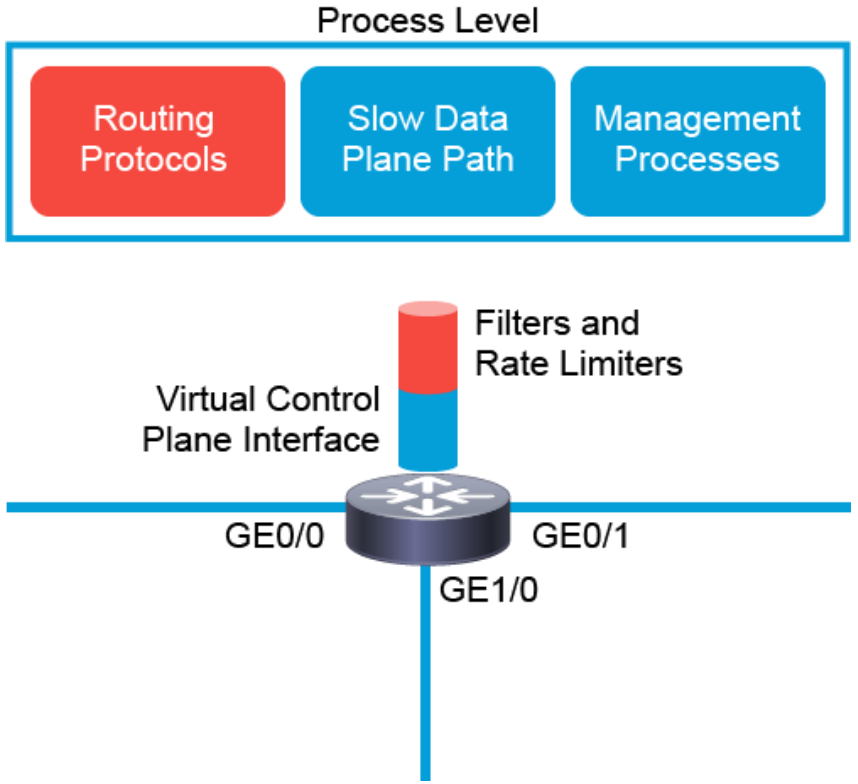


Infrastructure ACLs (cont.)

- Infrastructure ACLs are typically applied in the input direction on the interface that connects to the network users or external networks with the following policies:
  - All traffic to the IP addresses of network infrastructure devices is dropped and logged.
  - All other traffic is permitted and allows all transit traffic over the network.

Control Plane Policing

- One more countermeasure that guards against control plain targeting threats is CoPP

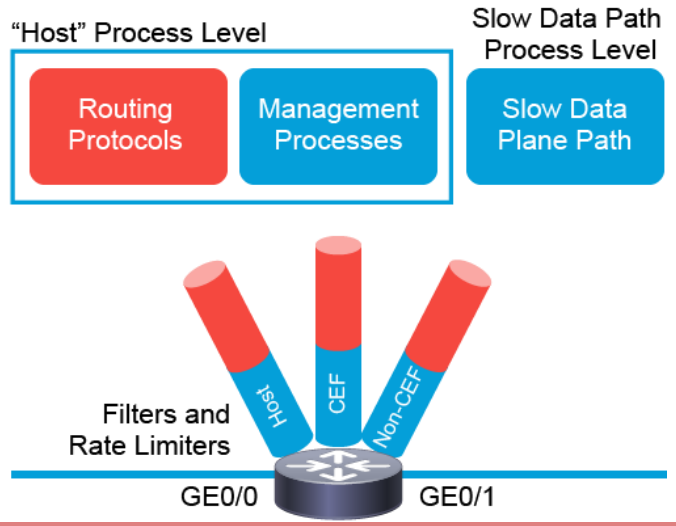


Control Plane Policing (cont.)

- CoPP uses early rate limiting and drops traffic that is destined for the central processor of the network device by applying QoS policies to a virtual aggregate CPU-bound queue, called the "control plane interface."
- This queue receives all aggregated traffic that is destined for the control plane (which includes the routing protocols), the management plane (management processes), and the slow data plane path traffic of the network device.
- CoPP can granularly permit, drop, or rate-limit traffic to the CPU using a Modular QoS (MQC) CLI.
- Because CoPP aggregates all traffic that is forwarded to the CPU of the network device, it is independent of interfaces.

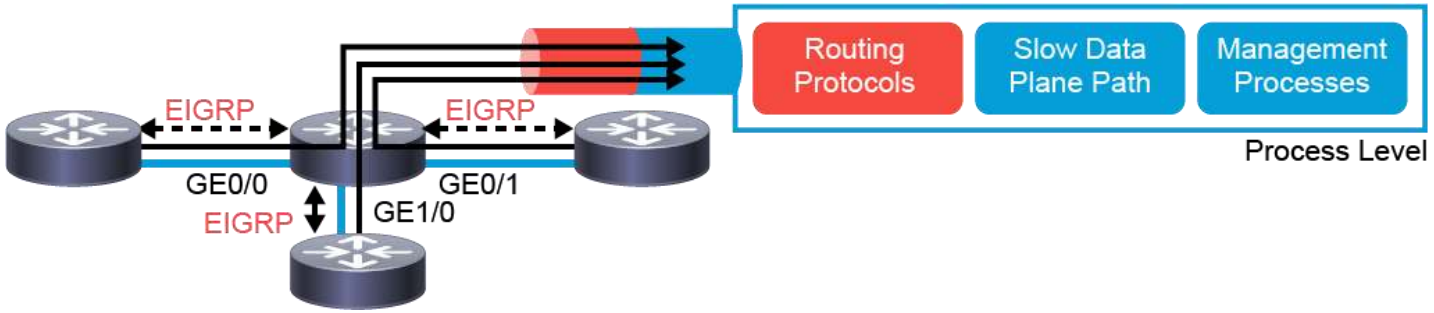
Control Plane Protection

- CPPr extends the CoPP functionality by automatically classifying all CPU-bound traffic into three queues (or subinterfaces) under the aggregate control plane interface.
- Each subinterface receives and processes a specific type of CPU-bound traffic, and each subinterface has a separate traffic policy that is attached to it, which makes the limit configuration easier.



Control Plane Protection (cont.)

- To configure CPPr, complete the following tasks:
  - Create traffic classes that describe valid control plane traffic. You can configure as many traffic classes as you need, depending on the required granularity of your policy.
  - Create a traffic policy that will permit, deny, or rate-limit the configured traffic classes and therefore conserve process layer resources, or even act as a device firewall by hiding most device resources from the network.
  - Apply the configured traffic policy to a required CPPr subinterface.



Configure Control Plane Protection

The protected device uses the EIGRP routing protocol with three EIGRP peers. All peers are connected to subnets of the **10.0.0.0/8** network and, together, produce no more than 200 EIGRP packets per second. All other traffic for the control plane should not produce more than 50 packets per second.

```
ip access-list extended CPPR-EIGRP
permit eigrp 10.0.0.0 0.255.255.255 any
!
class-map CPPR-EIGRP-CLASS
match access-group  name CPPR-EIGRP
!
policy-map CPPR-POLICY
class CPPR-EIGRP-CLASS
police rate 200 pps conform-action transmit exceed-action drop
class class-default
police rate 50 pps conform-action transmit exceed-action drop
!
control-plane host
service-policy input CPPR-POLICY
```

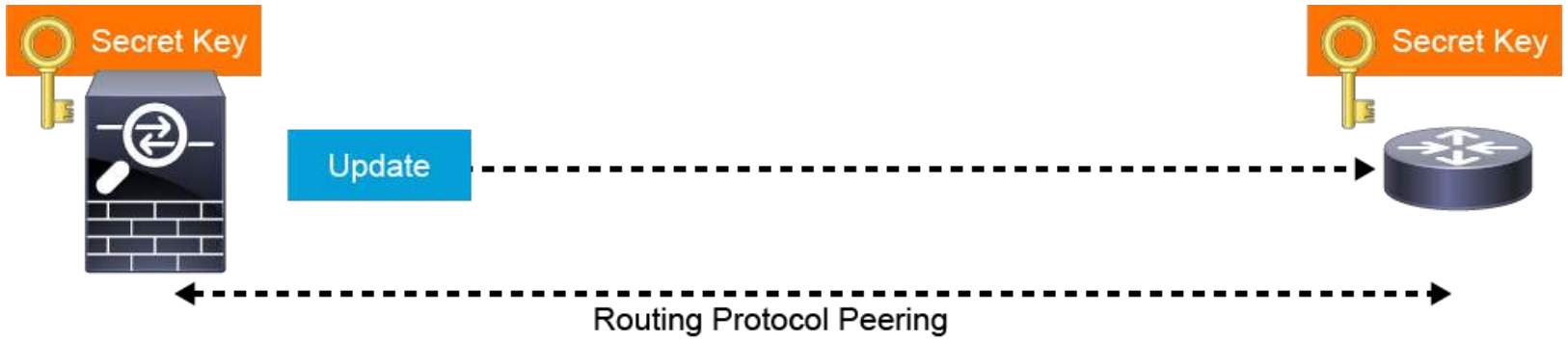
Routing Protocol Security

- Attackers can use malicious routing information to redirect or black-hole sensitive traffic and therefore violate its confidentiality, integrity, or ability to perform a denial-of-service attack. These risks can be mitigated by the following:

  - Use data plane ACLs to limit who can send routing protocol information to network devices.
  - Use the CoPP and CPPr features to locally limit the authorized routing protocol peers by their IP address.
  - Use routing protocol authentication, in which a cryptographic integrity and authenticity proof is embedded within each routing protocol message that prevents routing adjacency and routing update spoofing.
  - Use routing protocol filtering, which prevents injection of malicious routing information from known, authenticated peers.

Routing Protocol Security (cont.)

- A routing protocol often needs to be protected to prevent access to unknown peers and to reject forged routing updates through routing protocol peer and update authentication.
- This allows only trusted routers to participate in routing, but does not prevent injection of malicious routing information in case of trusted device compromise.

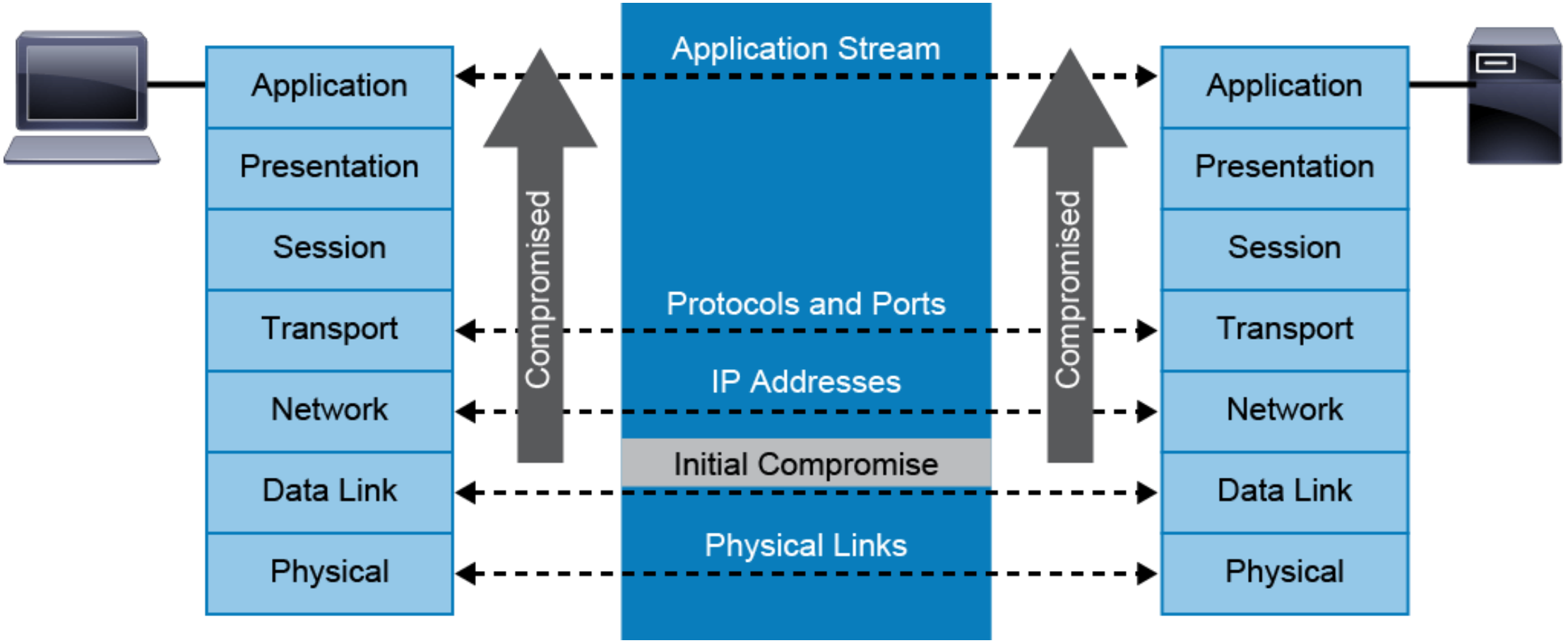


Routing Protocol Security (cont.)

- Most routing protocols support both cleartext passwords (that is, the password is included in the routing update in cleartext) and the MD5 HMAC algorithm to produce the message authentication code that is sent with the update.
- HMAC-MD5 or SHA combines the shared secret password and the information in the packet itself, and MD5 or SHA is a "one way" function.
- Therefore, knowing the packet contents and the resulting hash does not enable the reverse calculation of the original secret password.
- However, if the shared secret is not changed for a long time, then the risk that it could still be revealed somehow increases.

4.2- Layer 2 & 3 Data Plane Security Controls

Overview of Layer 2 Data Plane Security Controls



Overview of Layer 2 Data Plane Security Controls (cont.)

- Take the example of the previous image of a web browser and a web server communicating with each other.
- The two applications communicate with each other via a socket that is provided by the transport layer.
- Neither application is concerned with the complexity of the transport layer or any layer beneath the transport layer.
- Similarly, the transport layer depends on the network layer to carry packets to and from other systems based on IP addresses.
- The transport layer does not need to deal with the complexity of subnetting and routing.

Overview of Layer 2 Data Plane Security Controls (cont.)

- Also, the network layer depends on the data link layer to move frames between systems on the same broadcast domain, based on MAC addresses.
- Imagine, in this example, if Layer 2 is compromised at some point. Frames which should be passed between two neighboring routers are instead sent to a man-in-the-middle within that broadcast domain. Now, all traffic between the web browser and the web server is intercepted by man-in-the-middle, and none of the higher layers have any indication of the security breach.

Overview of Layer 2 Data Plane Security Controls (cont.)

Attack	Switched Infrastructure Countermeasure
VLAN hopping	Static access ports, disabling of Dynamic Trunking Protocol (DTP), avoidance of trunk native VLAN on access ports
STP spoofing	BPDU Guard/Root Guard
MAC spoofing	Port security
CAM flooding	Port security (MAC limit)
DHCP spoofing	DHCP snooping
DHCP starvation	Port security (MAC limit) or DHCP snooping rate limit
ARP spoofing	ARP inspection
LAN storm	Storm control

VLAN-Based Attacks Mitigation

- The VLANs are one of those networking features that are most commonly used in the networks today.
- Their usage provides many benefits, such as easy segmentation of the network, improved security and flexibility.
- However, improper configuration and deployment can lead to many potential problems in the network, such as basic and double-tagging VLAN hopping attacks.
- Appropriate implementation of mitigation techniques is required for protecting the networks from VLAN-based attacks.

VLAN-Based Attacks Mitigation (cont.)

- Once the VLANs are created on the switches, the interfaces are assigned to the required VLANs.
- The interfaces that participate in those VLANs and connect to the end devices are configured as access interfaces.
- On the other side, the links between the switches should not belong to just a single VLAN, but should transfer data from many different VLANs that are available in the networks, For that purpose, the interfaces that connect the switches to each other, must operate as trunk ports.
- The access or trunk mode on the switch interfaces can be configured manually or dynamically by using the DTP.
- DTP is enabled on Cisco switches, by **default** and it is used to negotiate a trunk or access link between the interconnecting switches.

VLAN-Based Attacks Mitigation (cont.)

- A trunk is a point-to-point link between two devices that is capable of carrying multiple VLANs.
- Trunks between switches allow many VLANs to be shared between switches using minimal physical connections.
- There are two protocols that are used to implement trunks in Ethernet environments, the Cisco proprietary protocol called Inter-Switch Link (ISL) and the IEEE ratified 802.1Q standard. In modern networks, almost all trunking is implemented with the 802.1Q protocol.

VLAN-Based Attacks Mitigation (cont.)

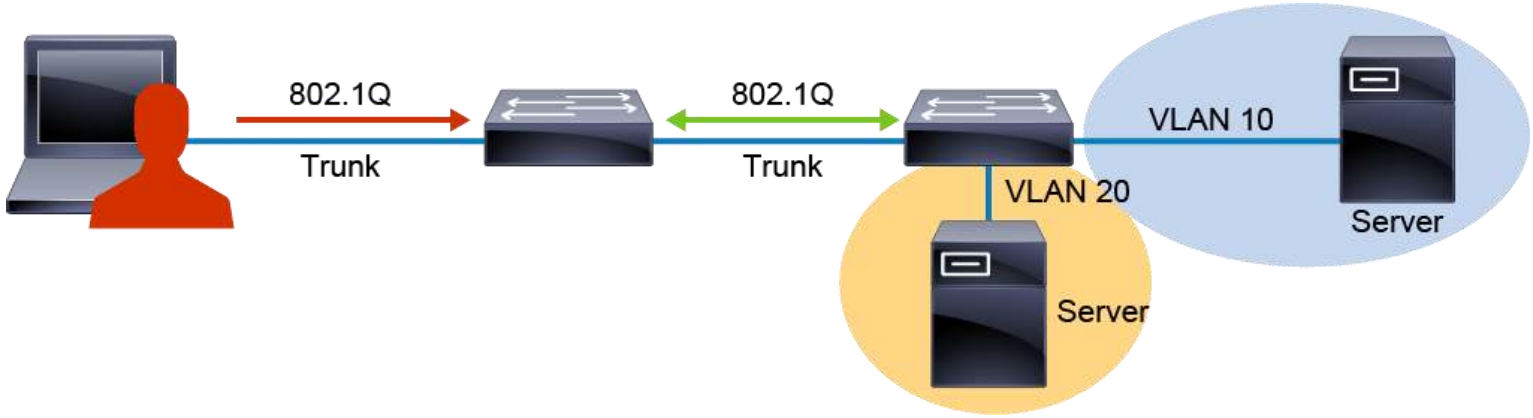
- The 802.1Q protocol introduces a tag into the Ethernet header which specifies the VLAN to which the frame should be contained.
- The 802.1Q tag is inserted into the frame header when a frame is sent out a trunk port.
- The 802.1Q tag is stripped from the frame when a receiving switch forwards the frame out an access (nontrunking) port.
- 802.1Q uses the concept of a native VLAN, therefore a trunk port is assigned a native VLAN.
- Most network devices assign **VLAN 1** as the native VLAN on trunks by **default**.

VLAN-Based Attacks Mitigation (cont.)

- Traffic that is associated with the native VLAN is untagged.
- That is, on egress, if the frame belongs to the native VLAN of the trunk port, an 802.1Q tag is not imposed.
- In contrast, if the frame belongs to any other VLAN, the appropriate 802.1Q tag is imposed.
- On ingress, if a frame arrives without a tag, it is assigned to the native VLAN, but if it arrives with an 802.1Q tag, the frame is assigned to the VLAN specified by the tag.
- Care must be taken to configure **the same native VLAN on both ends** of a trunk link.

VLAN-Based Attacks Mitigation (cont.)

- **VLAN hopping** allows traffic from one VLAN to be seen by another VLAN.
- The attack works by taking advantage of an incorrectly configured trunk port.
- By default, trunk ports have access to all VLANs and pass traffic for multiple VLANs across the same physical link, generally between switches.
- The data moving across these links may be encapsulated with the 802.1Q or ISL protocols.

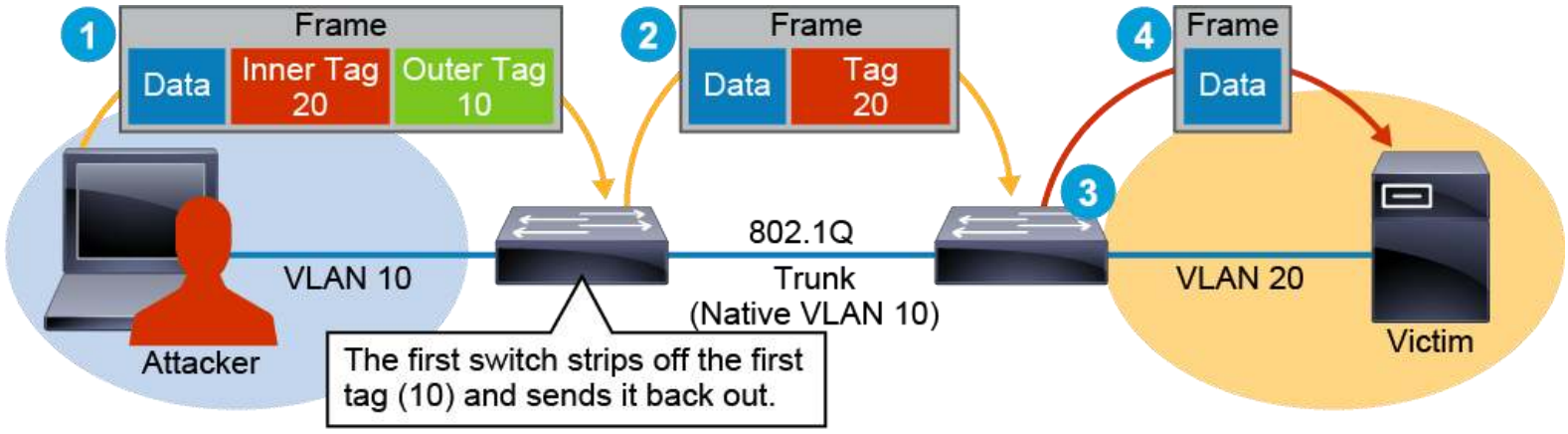


VLAN-Based Attacks Mitigation (cont.)

- In a basic **VLAN hopping attack**, the attacker takes advantage of the fact that DTP is enabled by default on most switches.
- The network attacker configures a system to use DTP to negotiate a trunk link to the switch.
- As a result, the attacker is a member of all the VLANS that are trunked on the switch and can hop between VLANs.
- In other words, the attacker can send and receive traffic on all those VLANs.

VLAN-Based Attacks Mitigation (cont.)

- **double-tagging** (or double-encapsulated) VLAN hopping attack takes advantage of the way that hardware operates on some switches.
- Some switches perform only one level of 802.1Q decapsulation and allow an attacker, in specific situations, to embed a second 802.1Q tag inside the frame.
- This tag allows the frame to go to a VLAN that the outer 802.1Q tag did not specify.



VLAN-Based Attacks Mitigation (cont.)

- A double-tagging VLAN hopping attack follows these steps, as illustrated in the figure:

1. The attacker sends a double-tagged 802.1Q frame to the switch. The outer header has the VLAN tag of the attacker, which is the same as the native VLAN of the trunk port. For the purposes of this example, assume that this is VLAN 10. The inner tag is the victim, VLAN 20.

2. The frame arrives on the switch. The switch sends it out to all VLAN 10 ports (including the trunk), because there is no CAM table entry. On egress out of the trunk link, the switch sees that the frame has an 802.1Q tag for the native VLAN, and it strips that tag. (This is because 802.1Q specifies that native VLAN traffic is not tagged.) The inner tag to VLAN 20 remains.

VLAN-Based Attacks Mitigation (cont.)

- A double-tagging VLAN hopping attack follows these steps, as illustrated in the figure (cont.)

3. The frame arrives at the second switch, which has no knowledge that it was supposed to be for VLAN 10. The second switch looks only at the 802.1Q tag (the former inner tag that the attacker sent) and sees that the frame is destined for VLAN 20 (the victim VLAN). The second switch strips tag 20 and checks the mac-address table for the exit interface.

4. The switch sends the packet on to the victim port, or floods it, depending on whether there is an existing CAM table entry for the victim host.

VLAN-Based Attacks Mitigation (cont.)

- Several mitigation techniques can be implemented on Cisco switches to protect against VLAN-based attacks, such as basic or double-tagging VLAN hopping attacks.
- These mitigation techniques includes:

1. Explicitly assigning access or trunk mode to all interfaces
2. Disabling of the DTP protocol on those interfaces
3. Explicitly defining a dedicated native VLAN on the trunk links

VLAN-Based Attacks Mitigation (cont.)

- The following configuration provides an example of the steps required for protecting against VLAN hopping attacks:

```
Switch(config)# vlan 999
Switch(config-vlan)# name native-trunkonly
Switch(config-vlan)# interface FastEthernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport trunk native vlan 999
Switch(config-if)# interface range FastEthernet0/22-24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport nonegotiate
```

STP Attacks Mitigation

- Enterprise voice and data networks are designed with physical component redundancy to eliminate the possibility of any single point of failure causing a loss of function for an entire switched network.
- However, redundant OSI Layer 2 switch topologies require planning and configuration to operate without introducing loops.
- For that purpose, loop-avoiding protocols are implemented in the networks. Unfortunately, these protocols like any other protocols are susceptible to malicious attacks.
- Therefore, appropriate features must be additionally implemented to prevent the networks from any potential attacks that might occur, while providing network availability at the same.

STP Attacks Mitigation (cont.)

- **Some of the problems that can occur with redundant links and devices in switched networks are as follows:**

1. **Broadcast storms:** Without some loop-avoidance process in operation, each switch floods broadcasts endlessly. This situation is commonly called a broadcast storm.

2. **Multiple frame transmission:** Multiple copies of unicast frames may be delivered to destination stations. Many protocols expect to receive only a single copy of each transmission. Multiple copies of the same frame can cause unrecoverable errors.

3. **MAC database instability:** Instability in the content of the MAC address table results from copies of the same frame being received on different ports of the switch.

STP Attacks Mitigation (cont.)

- STP offers a solution. It determines the optimal path back to a root switch from any point in the Layer 2 network, and allows forwarding on the optimal paths while blocking on suboptimal paths that would introduce loops into the topology.
- If there is a failure in the network, STP will reconverge using a new set of optimal paths given the current conditions.

STP Attacks Mitigation (cont.)

- To mitigate STP manipulation, you can use several security features, such as:

1. PortFast
2. BPDU Guard
3. Root Guard

- Any of these features has a different purpose and should be used according to the requirements in the network.
- Redundant designs can mitigate the possibility of a single point of failure, which causes a loss of function for the entire switched or bridged network.
- However, you must consider problems that redundant designs can cause.

STP Attacks Mitigation (cont.)

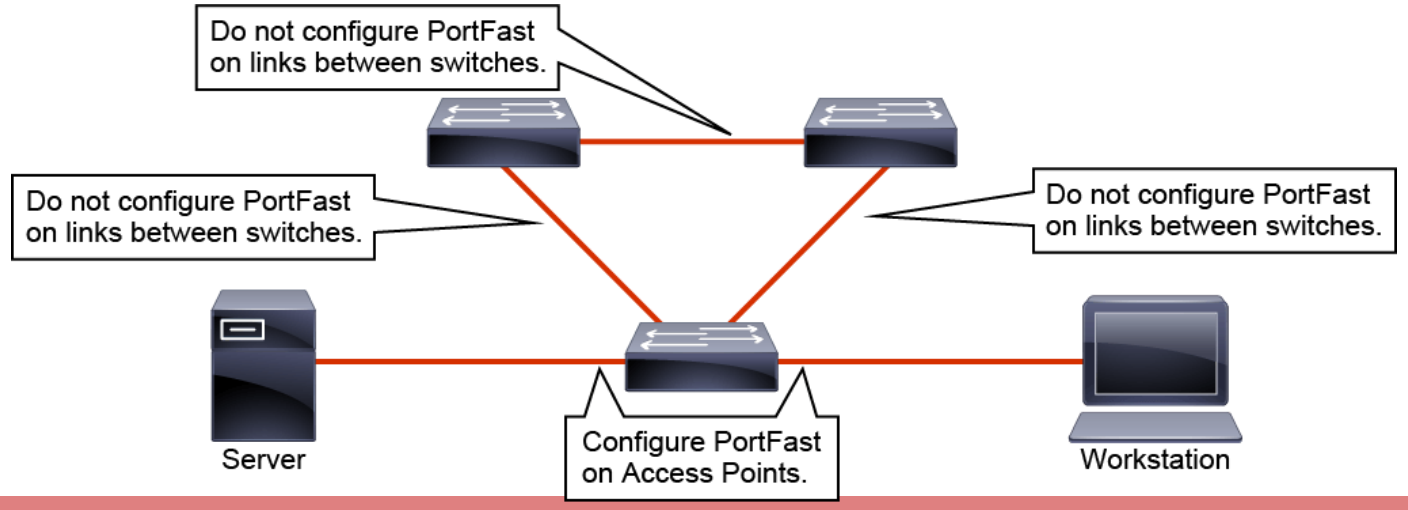
- When an end-user PC connects to an access layer switch, by default it does not get network access immediately.
- First the STP protocol will have to go through all the states—blocking, listening, learning, and forwarding, which in turn will result with some extended delay.
- With the default STP timers, this total transition will take about 30 seconds—15 seconds from listening to learning state, and 15 seconds from learning to forwarding state.

STP Attacks Mitigation (cont.)

- During this process, the PC will not be able to transmit or receive data.
- Once the switch interface transitions the port to the forwarding state, the PC will become operational in the network.
- This default behavior extends the duration of the total time required for the PC to acquire an IP address from the DHCP server and get network access.
- As a solution for this default behavior that produces delay, the PortFast feature can be implemented on the switches.

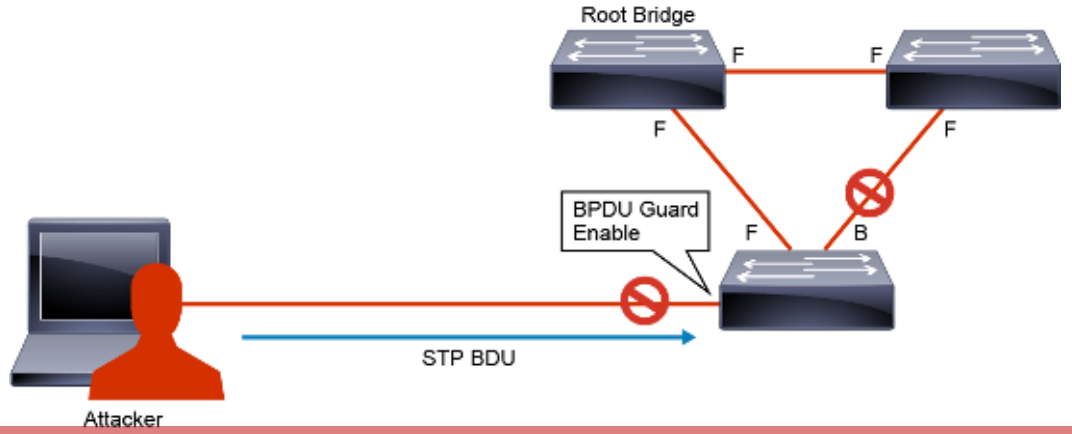
STP Attacks Mitigation (cont.)

- The STP PortFast feature causes an interface that is configured as a Layer 2 access port to transition from a blocking to forwarding state immediately, bypassing the listening and learning states.
- You can use PortFast on Layer 2 access ports that connect to a single workstation or server to allow those devices to connect to the network immediately without any delay produced by the switch.



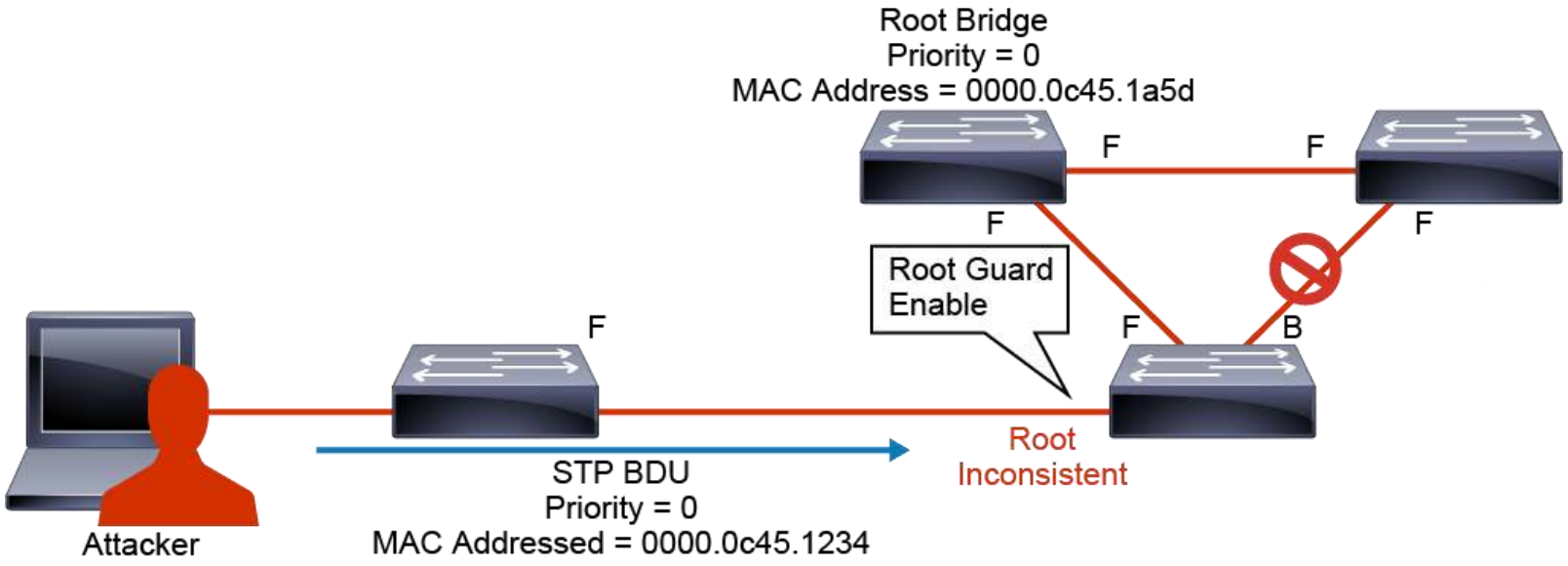
STP Attacks Mitigation (cont.)

- The STP BPDU Guard feature is designed to allow network designers to maintain predictability of the active network topology.
- In a properly configured network, interfaces that are configured with the PortFast feature should never receive any BPDUs.
- Enabling the BPDU guard feature, will always protect the interface by simply logically disabling it when a BPDU is received.



STP Attacks Mitigation (cont.)

- The Root Guard feature of Cisco switches prevents a switch from becoming a root bridge on configured ports.



STP Attacks Mitigation (cont.)

- **Configuration example of enabling the PortFast, BPDU Guard and Root Guard mitigation features in interface mode includes the following commands:**

```
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# spanning-tree guard root
In addition, the PortFast and BPDU Guard can also be enabled in global mode and apply to all
nontrunking ports:
Switch(config)# spanning-tree portfast default
Switch(config)# spanning-tree portfast bpduguard default
```

Port Security

- The port security feature restricts a switch port to a specific set or number of MAC addresses.
- The switch can learn these MAC addresses dynamically, or you can configure them statically on the device.
- Once an interface is configured with the port security feature, it accepts frames only from secure MAC addresses.
- When a violation occurs, the defined action applies to the interface.

Port Security (cont.)

- Due to these functionalities provided by the port security feature, it can be used for protection against:

1. MAC spoofing
2. MAC flooding Layer 2 attacks

- The reason for that is both these attacks operate by manipulating the MAC addresses of the frames when being sent to the switches.
- Therefore, the Port Security feature can deny any of those frames sent by the attacker with issues related to the MAC addresses.

Port Security (cont.)

- When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or dynamically learned on the port.
- If the arriving MAC address is on the list, it is processed normally.
- However, if the arriving MAC address is not on the list, but dynamic learning is enabled and there is room for an additional MAC address, it is added to the list and processed normally.

Port Security (cont.)

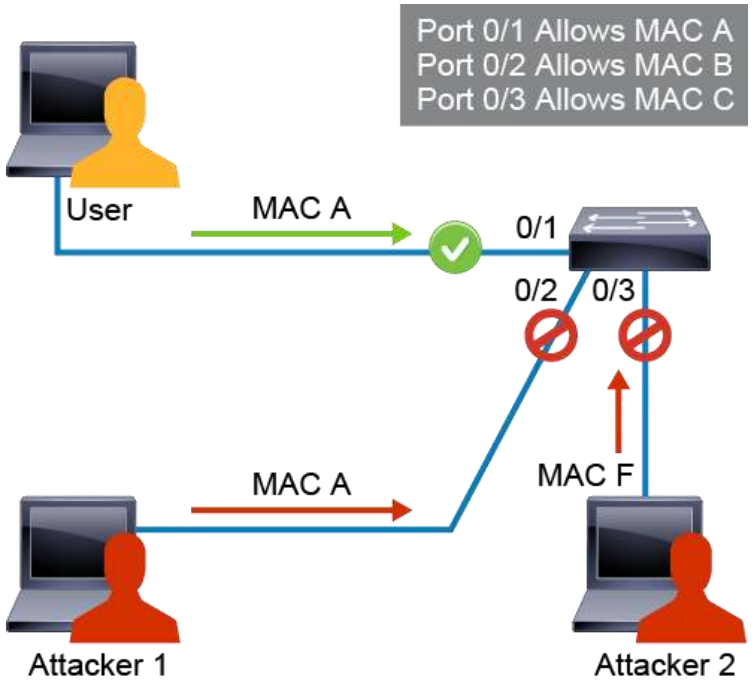
- If the MAC address is not on the list and learning is disabled or the maximum number of MAC addresses is already reached, one of three actions is taken based on the configured violation mode:
  - **Protect:** The offending frame is dropped. The security violation count number is not increased when a violation occurs.
  - **Restrict:** The offending frame is dropped and a Simple Network Management Protocol (SNMP) trap or Syslog message is generated. The security violation count number is increased by one when a violation occurs.
  - **Shutdown:** The interface is placed in an error-disabled state and a SNMP trap or Syslog message is generated. The port is inactive while in an error-disabled state. Administrative action is required to return the port to a normal state. The security violation count number is increased by one when a violation occurs. **Shutdown is the default violation mode**.

Port Security (cont.)

- MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames that are destined for the remote host to the network attacker.
- By sending a single frame with the source MAC address of the other host, the network attacker overwrites the CAM table entry so that the switch forwards packets that are destined for the host to the network attacker.
- Until the host sends traffic, it does not receive any traffic. When the host sends out traffic, the CAM table entry is rewritten once more, so that it moves back to the original port.

Port Security (cont.)

- In the figure, traffic from Attacker 1 and Attacker 2 will be dropped at the switch because the source MAC addresses of the frames that are sent do not match the MAC addresses in the list of secured (allowed) addresses defined on the switch interfaces.



Port Security (cont.)

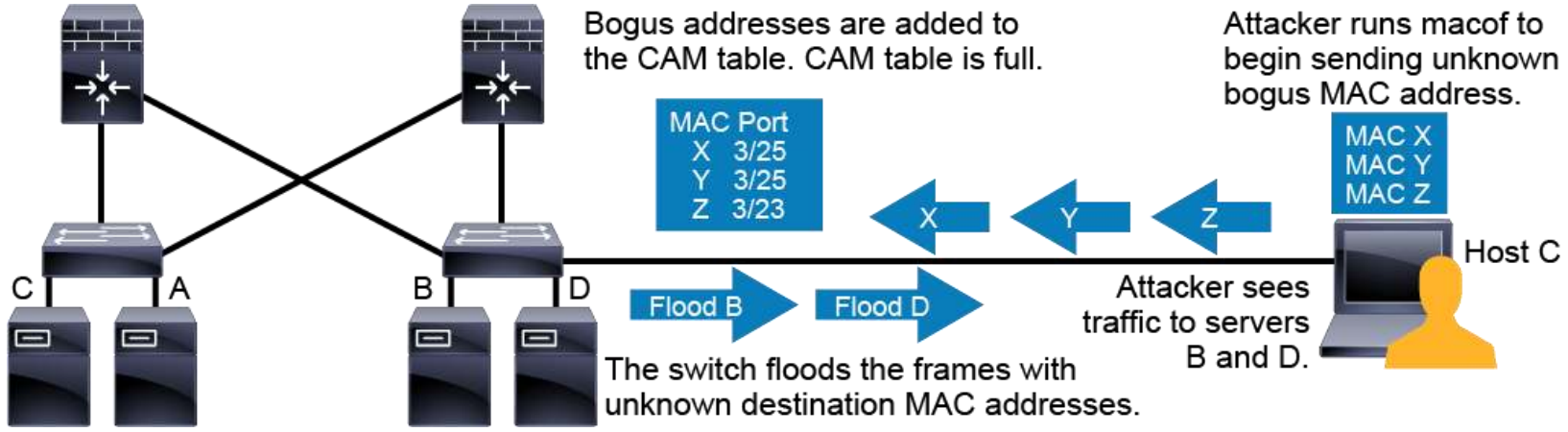
- The most important point to understanding how CAM overflow attacks work is to know that CAM tables are limited in **size**.
- MAC flooding takes advantage of this limitation by bombarding the switch with fake source MAC addresses until the switch CAM table is full.
- If enough entries are entered into the CAM table, the CAM table fills up to the point that no new entries can be accepted.
- Note that this attack will not cause legitimate entries that were in the CAM table before the attack to be removed.
- The attack will quickly consume the freed spot in the CAM table and the legitimate MAC address will not be relearned.

Port Security (cont.)

- In a MAC flooding attack (CAM table overflow attack), a network attacker can use a tool such as the macof program and flood the switch with many invalid source MAC addresses until the CAM table fills up.
- When that occurs, the switch begins to flood traffic for unknown MAC addresses to all ports because there is no room in the CAM table to learn any legitimate MAC addresses.
- The switch acts like a ***hub,*** As a result, the attacker can see all the frames that are sent from a victim host to another host without a CAM table entry.
- CAM table overflow floods traffic only within the local VLAN, so the intruder will see only traffic within the local VLAN to which the attacker is connected.

Port Security (cont.)

- In the figure, the macof program is running on host C.
- The macof program is one of many tools that can flood a switch with packets that contain randomly generated source and destination MAC addresses. Over a short period, the CAM table in the switch fills up until it cannot accept new entries.



Port Security (cont.)

- **The configuration example below shows a typical port security configuration for a voice port:**

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
```

Port Security (cont.)

- To view port security settings for the switch, including violation count, configured interfaces, and security violation actions, you should use:

```
Switch # show port-security
```

- In addition, you can specify the interface for which you want to view the port security settings:

```
Switch# show port-security interface FastEthernet0/1
```

Private VLANs

- Service providers often have devices from multiple clients, as well as their own servers, on a single demilitarized zone (DMZ) segment or VLAN.
- It becomes necessary to provide traffic isolation between devices even though they may exist on the same Layer 3 segment or VLAN.
- 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 and access control between VLANs and Internet destinations.
- Similar to the ISPs, the same requirements can also be demanded in organizations that often support many different network endpoints, Like with the ISPs, one VLAN can be provided per device type, with each VLAN having its own IP subnet.

Private VLANs (cont.)

- **However, there are several challenges with the traditional solution:**

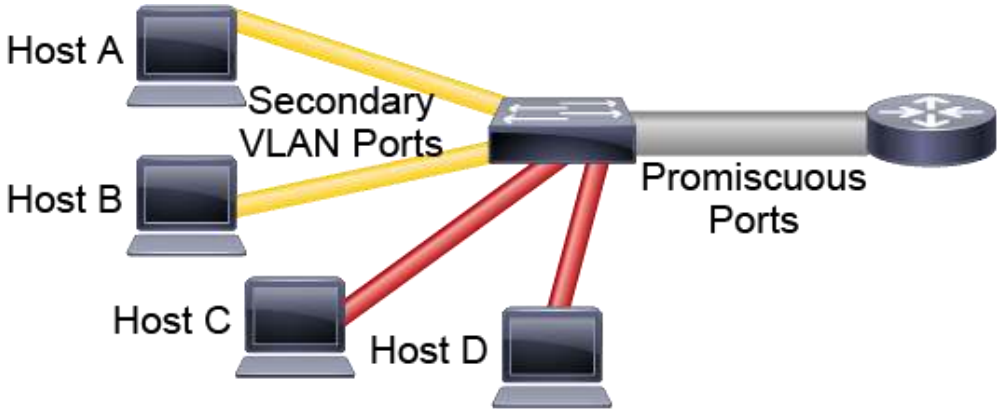
1. Supporting a separate VLAN per customer or device type can require a high number of interfaces on network devices.

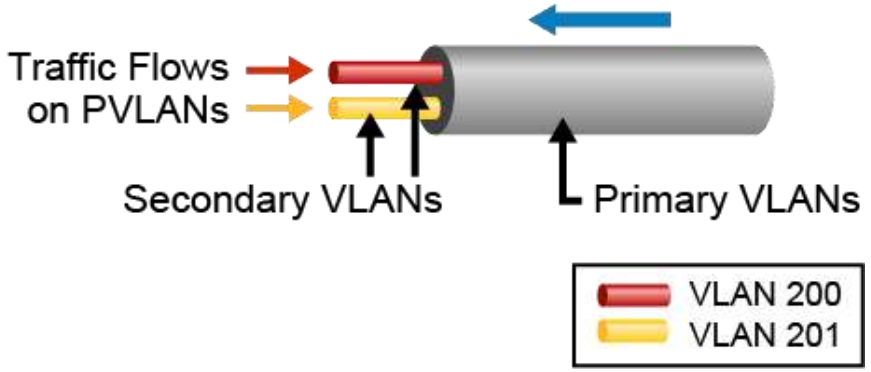
2. The network address space must be divided into many subnets, which wastes space and increases management complexity.

3. Multiple access control list (ACL) applications are required to maintain security on multiple VLANs, resulting in increased management complexity.

Private VLANs (cont.)

- Private VLAN (PVLAN) feature provides a Layer 2 isolation between ports within the same VLAN.
- This isolation eliminates the need for a separate VLAN and IP subnet per customer.





Private VLANs (cont.)

- With PVLANs, a common subnet is subdivided into multiple segments or PVLANs.
- This feature introduces a concept of a primary VLAN, which is the VLAN to which all devices and users belong, and hosts a particular Layer 3 subnet.
- Inside this primary VLAN, you can create as many secondary community VLANs as required to define host groups (or communities) or just one isolated secondary VLAN to isolate devices or users from one another within the primary VLAN.
- The implementation of secondary VLANs still provides classic Layer 3 routing into and out of the primary VLAN.
- The communication between the hosts is controlled by whether their switchport is configured as isolated, community, or promiscuous.

Private VLANs (cont.)

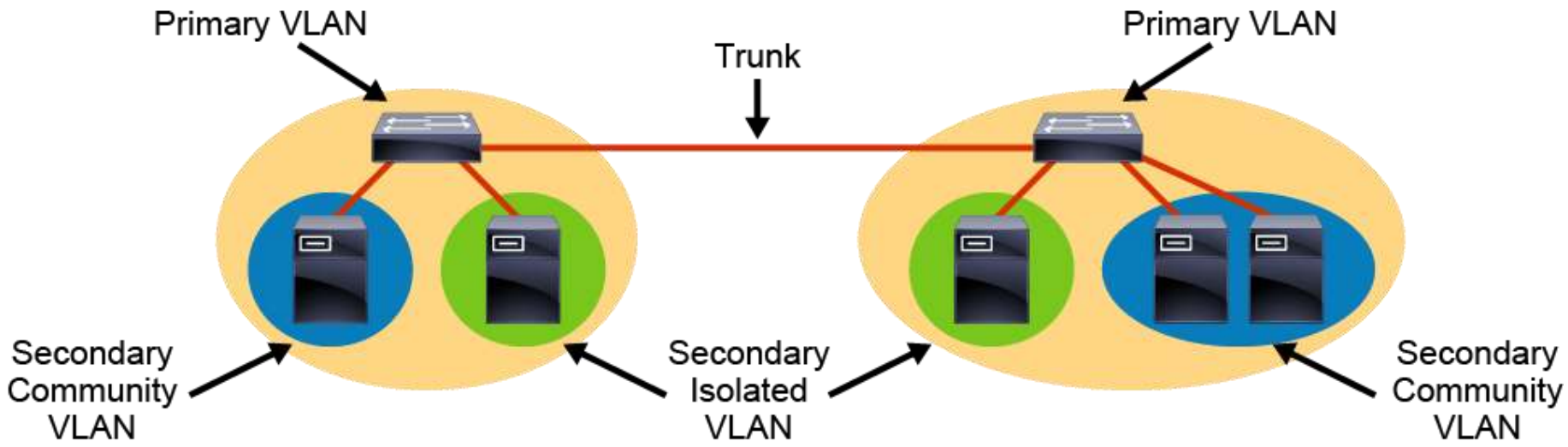
- **Private VLANs**

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

- **As a primary VLAN:** This type of VLAN carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same primary VLAN.
- **As an isolated VLAN:** This type of VLAN carries traffic from isolated ports to a promiscuous port.
- **As a community VLAN:** This type of VLAN carries traffic between community ports and to promiscuous ports. You can configure multiple community VLANs in a PVLAN.

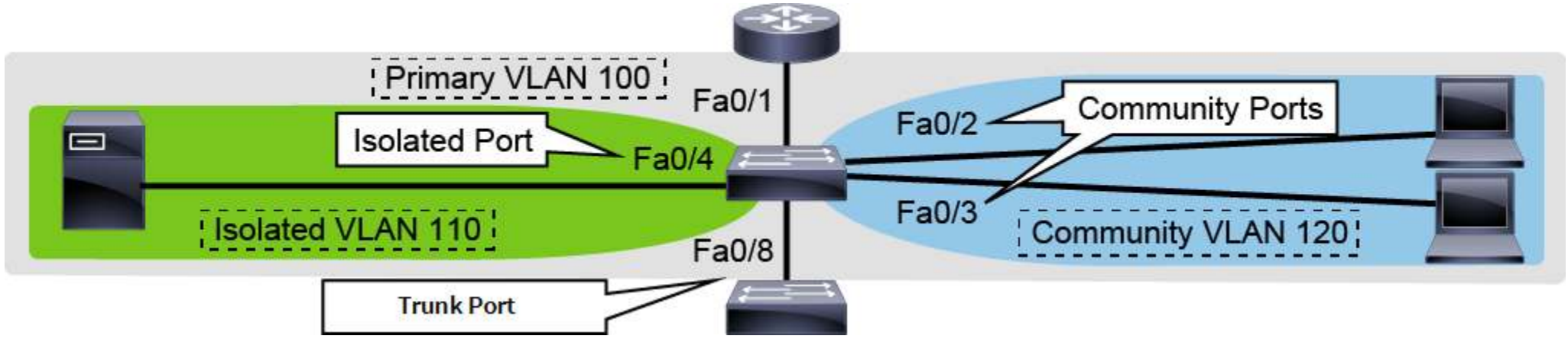
Private VLANs (cont.)

- Isolated and community VLANs are called secondary VLANs and can have only one primary VLAN associated with it.



Private VLANs (cont.)

- **In the figure, there is an example topology in which the PVLAN feature should be implemented. Two secondary VLANs should be used for the server and computers in the topology:**



Private VLANs (cont.)

- Configuration of VLANs 110, 120 and 100 and defining them as secondary isolated, secondary community, and primary VLAN, respectively. The secondary VLANs 110 and 120 are associated with the primary VLAN 100.

```
Switch(config)# vlan 110
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# vlan 120
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# vlan 100
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 110,120
```

Private VLANs (cont.)

- Configures interface FastEthernet 0/4 as an isolated port and associates it to isolated VLAN 110.

```
Switch(config-vlan)# interface FastEthernet 0/4
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 100, 110
```

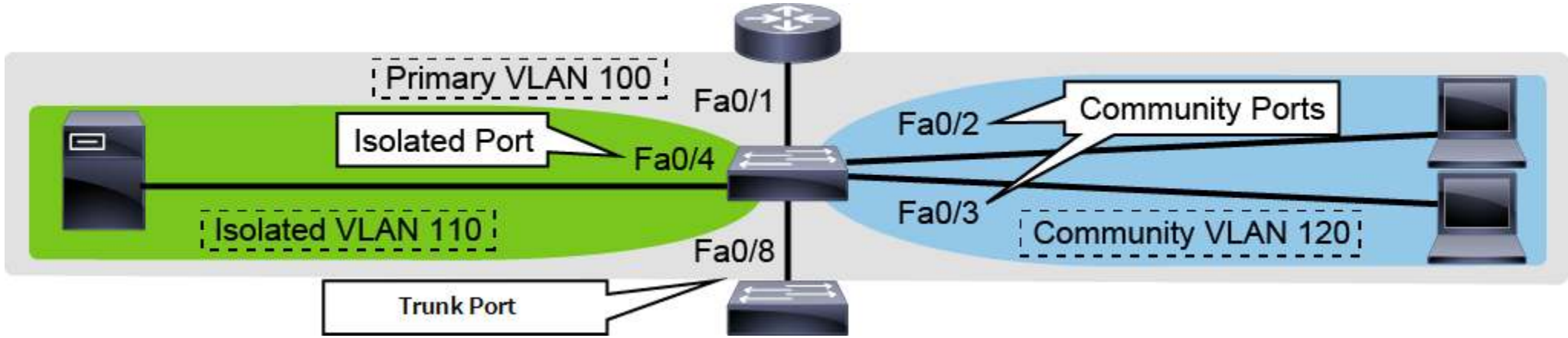
- Configures interfaces FastEthernet 0/2 and 0/3 as community ports and associate them to community VLAN 120

```
Switch(config-if)# interface range FastEthernet 0/2 - 3
Switch(config-if-range)# switchport mode private-vlan host
Switch(config-if-range)# switchport private-vlan host-association 100, 120
```

Private VLANs (cont.)

- Configures interface FastEthernet 0/1 as a promiscuous port and associates it to the primary, isolated and community VLANs.

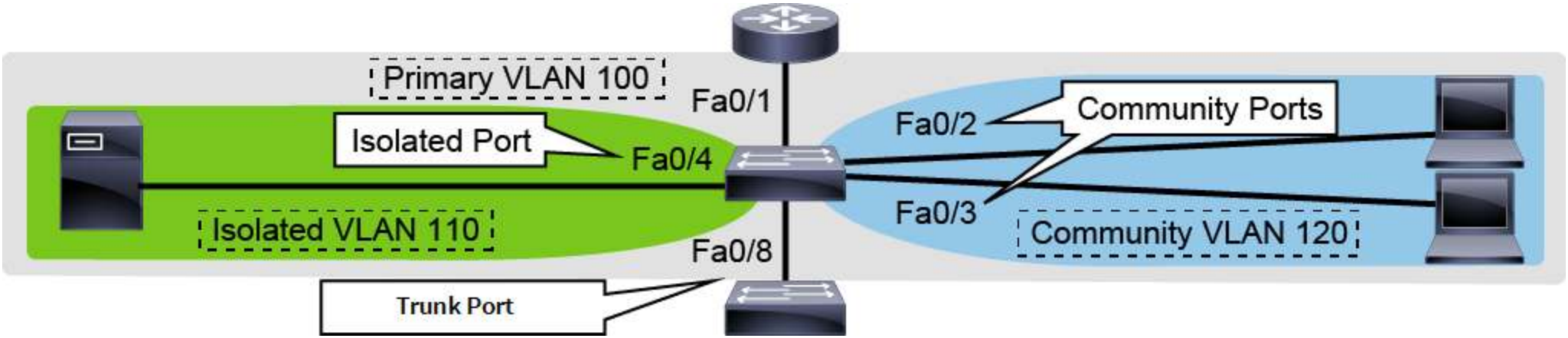
```
Switch(config-if-range)# interface FastEthernet 0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 100,110,120
```



Private VLANs (cont.)

- Configures interface FastEthernet 0/8 as a trunk port.

```
Switch(config-if)# interface FastEthernet 0/8
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
```



Private VLANs (cont.)

- **Private VLANs Verification**

PVLAN Verification Commands	Description
# show vlan private-vlan type	Verifies PVLAN types.
# show vlan private-vlan	Verifies PVLAN associations.
# show interfaces if_name switchport	Verifies Private VLAN Edge.

DHCP Snooping

- DHCP automatically assigns an IP address from an IP address pool that is defined by the administrator.
- However, DHCP is much more than just an IP address allocation mechanism.
- A DHCP server can push other initial configuration parameters to the client devices, such as the addresses of the default gateway and the DNS servers.
- Because DHCP protocol does not use any security mechanism for protecting the communications between the clients and the server, two DHCP related attacks can be performed at Layer 2:

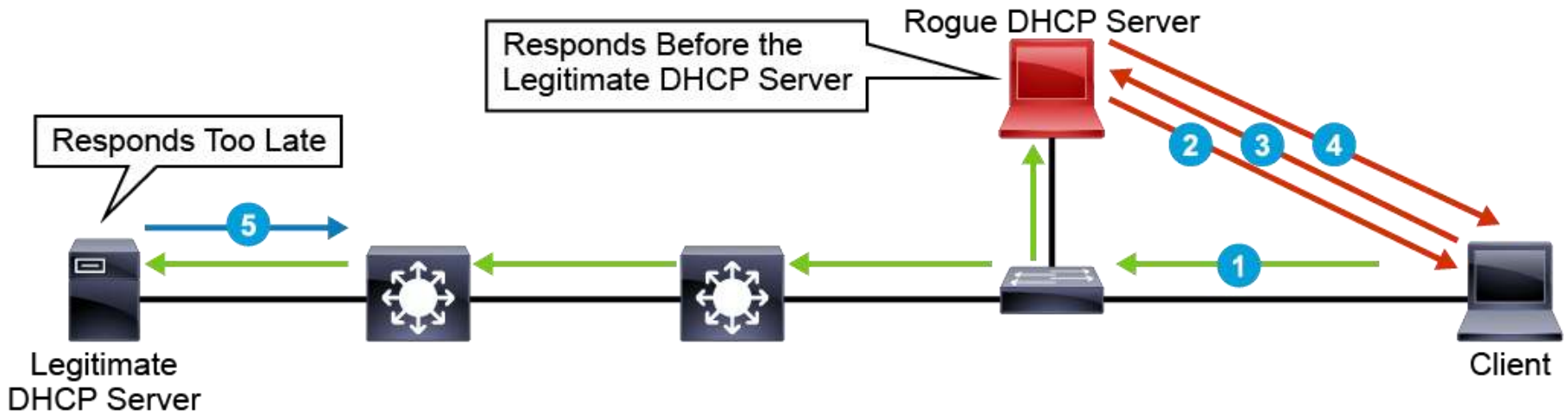
1. DHCP spoofing attacks
2. DHCP starvation attacks.

DHCP Snooping (cont.)

- DHCP does not include authentication and is therefore easily vulnerable to spoofing attacks.
- DHCP Server Spoofing, In this attack the attacker runs a DHCP server software and replies to DHCP requests from legitimate clients.
- As a rogue DHCP server, the attacker can cause a denial of service (DoS) by providing invalid IP information.
- The attacker can also perform confidentiality or integrity breaches via a man-in-the-middle attack.
- The attacker can assign itself as the default gateway or DNS server in the DHCP replies, later intercepting IP communications from the configured hosts to the rest of the network.

DHCP Snooping (cont.)

- There is an example of how the DHCP spoofing attack works.



DHCP Snooping (cont.)

1. When the client needs to get an IP address and other complimentary settings from the DHCP server, sends a DHCP discover (broadcast) message.
2. When the access switch receives the message, it forwards it on every other port, so the message can eventually reach the DHCP server.
3. Because the rouge DHCP server is closer to the client than the legitimate DHCP server, it receives the discover message first.
4. Upon receipt, it responds back with a DHCP offer message.
5. In the offer, all required parameters by the client are included, such as IP address, default gateway, DNS server and so on.

DHCP Snooping (cont.)

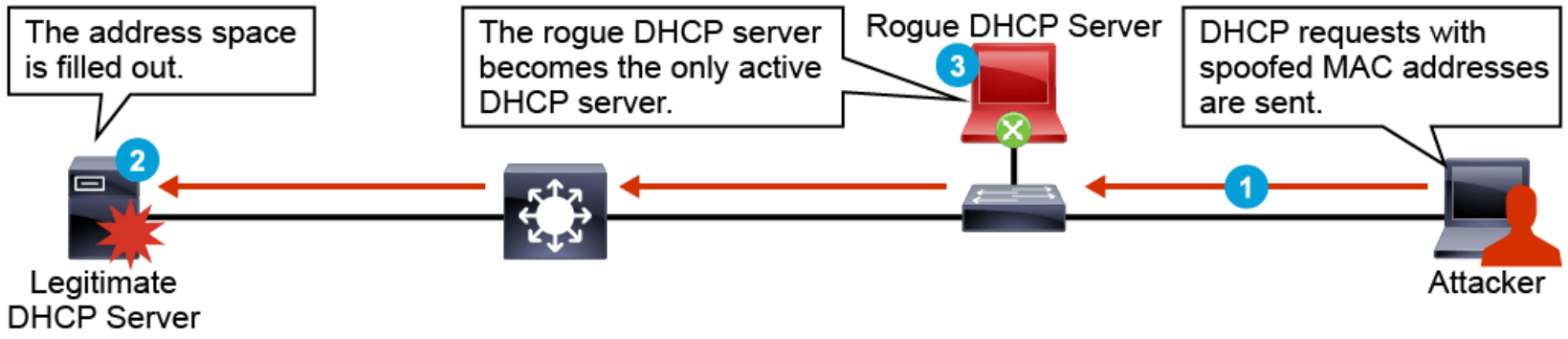
6. Because the client does not have a method to verify the validity of the DHCP server, continues the negotiation with the rogue DHCP server by responding to the offer message with a DHCP request.
7. Once this message is received by the rogue DHCP, the attacker system responds to the request message with a DHCP acknowledgement.
8. Now, the DHCP negotiation process is finished and the client is using the parameters provided by the rogue DHCP server.

DHCP Snooping (cont.)

- To mitigate DHCP spoofing threats, you can use static IP addresses, but static IP addresses are obviously not scalable in large environments.
- On the other hand, as a better solution, you can enable DHCP snooping to control DHCP traffic in the infrastructure.

DHCP Snooping (cont.)

- A DHCP starvation attack works by sending a flood of DHCP requests with spoofed MAC addresses.
- If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers.
- This flooding would cause a loss of network availability to new DHCP clients as they connect to the network.

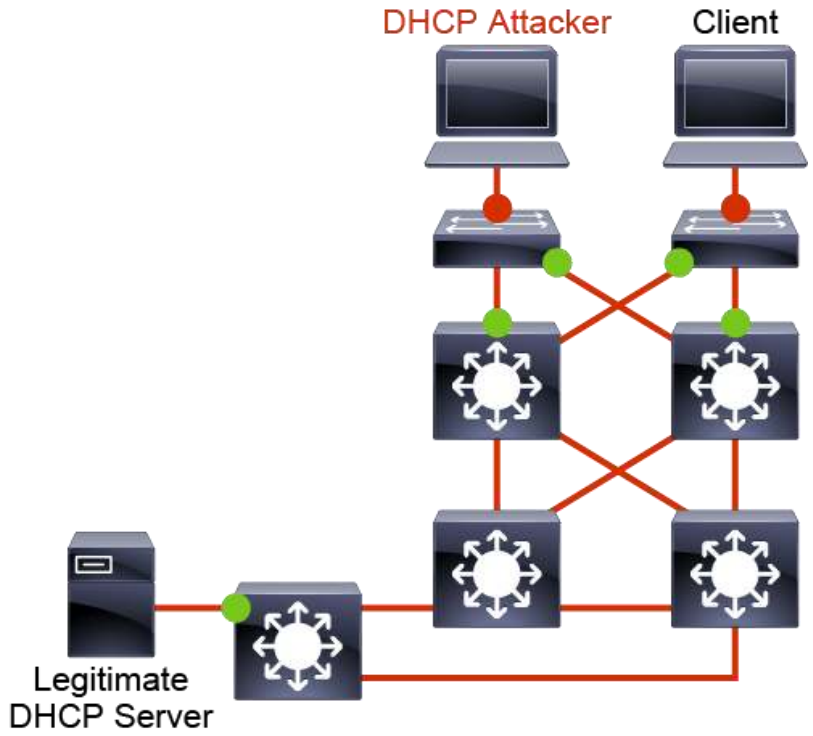


DHCP Snooping (cont.)

- To mitigate DHCP address starvation attacks, you can deploy Port Security address limits, which set an upper limit of MAC addresses that will be accepted into the CAM table from any single interface.
- DHCP snooping is a Layer 2 security feature that specifically prevents DHCP server spoofing attacks and mitigates DHCP starvation to a degree.
- DHCP snooping provides DHCP control by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, which is also referred to as a DHCP snooping binding table.

DHCP Snooping (cont.)

- For DHCP snooping to work, each switch port must be labeled as trusted or untrusted.



DHCP Snooping (cont.)

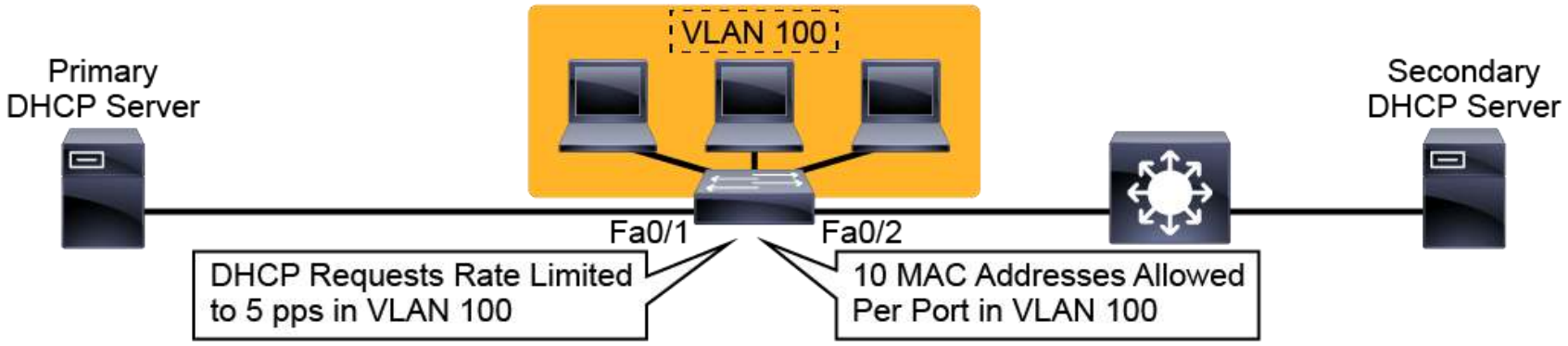
- Trusted ports are the ports over which the DHCP server is reachable and that will accept DHCP server replies.
- All other ports should be labeled as untrusted ports and can only source DHCP requests.
- **By default**, when the DHCP feature is enabled, all interfaces are designated as **untrusted**.

DHCP Snooping (cont.)

- The configuration process of the DHCP snooping feature consists of several steps.
- First, you have to enable it globally on the switch, and then explicitly for the VLAN for which you want the feature to operate.
- **By default**, the DHCP snooping database is only kept in RAM, thus it is lost when the switch reboots.
- Therefore, you have to specify a location-locally on the device or on a remote server-to make the database persistent through reloads.
- Because all interfaces are designated as untrusted by default, you have to configure only the appropriate interfaces as trusted.

DHCP Snooping (cont.)

- In addition, you can rate limit the number of DHCP packets per second that will be allowed on the interfaces to protect against DHCP starvation attacks.
- It is generally preferable to use Port Security with an address limit to resolve DHCP address starvation attacks instead of, or in addition to, rate limiting.



DHCP Snooping (cont.)

- An example of a DHCP snooping configuration will contain the following steps:

Enabling the DCHP snooping feature globally and explicitly for VLAN 100, and defining the location for the persistent database.

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping database flash:/dhcp-snooping.db
Switch(config)# ip dhcp snooping vlan 100
```

DHCP Snooping (cont.)

- An example of a DHCP snooping configuration will contain the following steps (cont.)

Designating FastEthernet 0/1 and FastEthernet 0/2 interfaces as trusted.

```
Switch(config)# interface range FastEthernet 0/1 - 2
Switch(config-if-range)# ip dhcp snooping trust
```

DHCP Snooping (cont.)

- An example of a DHCP snooping configuration will contain the following steps (cont.)

Configuring rate limit on the DHCP messages to 5 packets per second for interfaces in VLAN 100, as well as enabling port security and limiting the maximum number of allowed MAC addresses to 10.

```
Switch(config)# interface range FastEthernet 0/3 - 24
Switch(config-if-range)# ip dhcp snooping limit rate 5
Switch(config-if-range)# switchport port-security
Switch(config-if-range)# switchport port-security maximum 10
```

DHCP Snooping (cont.)

show ip dhcp snooping binding

- to display the dynamically discovered bindings in the DHCP snooping binding database.
- To filter which addresses are displayed, provide either a MAC address or an IP address for the address parameter.

ARP Inspection

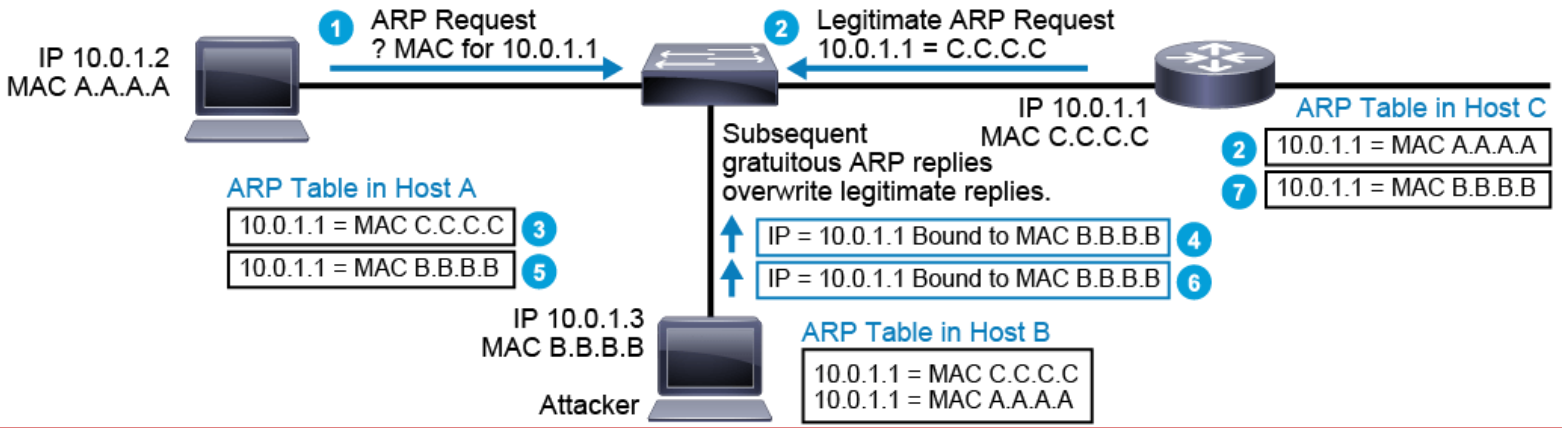
- Devices that use IP addresses need ARP to map IP network addresses to MAC hardware addresses.
- Before a device sends a datagram to another device on the same subnet, it looks in its ARP cache to see if there is a MAC address that corresponds to the destination IP address.
- If there is no entry, the source device sends a broadcast ARP request to every device on the network.
- Each device compares the IP address to its own.

ARP Inspection (cont.)

- The device with the matching IP address sends an ARP reply containing its MAC address.
- The source device adds the destination device MAC address to its ARP table (ARP cache) for future reference, and will use that MAC address in the Layer 2 header for subsequent communication.
- ARP protocol does not provide any protection on its own.
- Therefore, the protocol itself is very susceptible to ARP attacks.

ARP Inspection (cont.)

- ARP spoofing attack, also known as ARP cache poisoning target hosts, switches, and routers that are connected to your Layer 2 network.
- This targeting is achieved by poisoning the ARP caches of systems that are connected to the subnet and by intercepting traffic that is intended for other hosts on the subnet.
- An ARP spoofing attack can result in a man-in-the-middle situation.



ARP Inspection (cont.)

- This ARP vulnerability in the infrastructure can be addressed in several ways:
  1. Static ARP inspection or Dynamic ARP Inspection (DAI) enabled on network switches.
  2. Static ARP entries on infrastructure devices; therefore, no use of ARP at all on critical segments.
- To prevent ARP spoofing, or poisoning, a switch can process transit ARP traffic to ensure that only valid ARP requests and responses are relayed.
- The Dynamic ARP inspection (DAI) feature of Cisco switches prevents ARP spoofing attacks by intercepting and validating all ARP requests and responses.
- Each intercepted ARP reply is verified for valid MAC-to-IP address bindings before it is forwarded.
- ARP replies with invalid MAC-to-IP address bindings are dropped.

ARP Inspection (cont.)

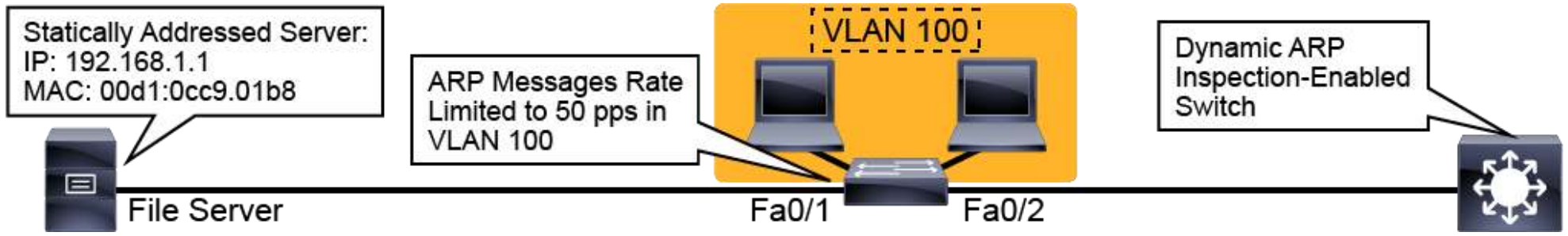
- ARP inspection can determine the validity of an ARP reply that is based on bindings that are stored in a DHCP snooping database for DHCP-addressed hosts.
- As with DHCP snooping, ARP inspection labels all switch ports as trusted or untrusted.
- In a typical network configuration, define all access switch ports that are connected to host ports as untrusted and all switch ports that are connected to other switches as trusted.

ARP Inspection (cont.)

- The configuration process of the DAI feature consists of several steps.
- First, you have to **enable the DHCP snooping feature**, because it is required for all the mappings that will be required by the DAI engine when will inspect ARP messages received on the interfaces.
- Then, you need to enable ARP inspection on the desired VLANs.
- By default all ports are designated as untrusted.
- You should configure all interfaces as trusted, except the access interfaces that connect to hosts.
- Optionally, you can rate limit the amount of ARP messages received on the interfaces.

ARP Inspection (cont.)

- In the figure, an example shows the topology in which the ARP inspection feature should be applied



ARP Inspection (cont.)

- An example of a DAI configuration will contain the following steps:

```
Configuring exception for the statically addressed server, by using an ARP ACL.
Switch(config)# arp access-list ARP-INSPECTION-EXCEPTIONS
Switch(config-arp-nacl)# permit ip host 192.168.1.1 mac host 00d1.0cc9.01b8
Switch(config-arp-nacl)# exit

Enabling ARP inspection for VLAN 100 and applying the ARP ACL to this VLAN.
Switch(config)# ip arp inspection vlan 100
Switch(config)# ip arp inspection filter ARP-INSPECTION-EXCEPTIONS vlan 100
```

ARP Inspection (cont.)

- An example of a DAI configuration will contain the following steps (cont.)

```
Configuring inter-switch link to other ARP-inspecting switch as trusted.
Switch(config)# interface FastEthernet 0/2
Switch(config-if)# ip dhcp snooping trust
```

ARP Inspection (cont.)

- An example of a DAI configuration will contain the following steps (cont.)

```
Specifying ARP inspection rate limit of 50 to specific range of IP addresses.
Switch(config-if)# interface range FastEthernet 0/3 - 24
Switch(config-if-range)# ip arp inspection limit rate 50
```

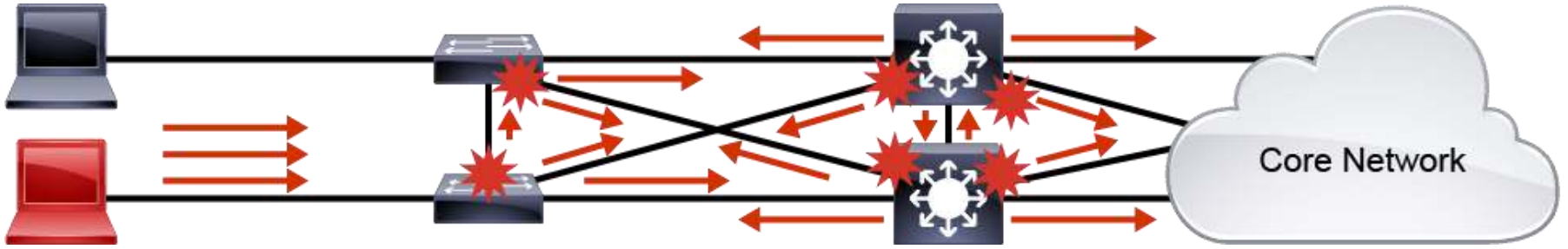
- Use the **show ip arp inspection** command to display the general ARP inspection configuration for a switch.

Storm Control

- An excessive amount of uncontrolled traffic flooded across the network can be very harmful to the deployment and the limited hardware resources of the devices.
- Broadcast storms caused by misconfigured network configurations or even unicast storms caused by faulty network interface cards (NICs) can easily exhaust all available bandwidth of the links and running resources of the Cisco switches.
- For that reason, appropriate protection features should be applied on the switches.

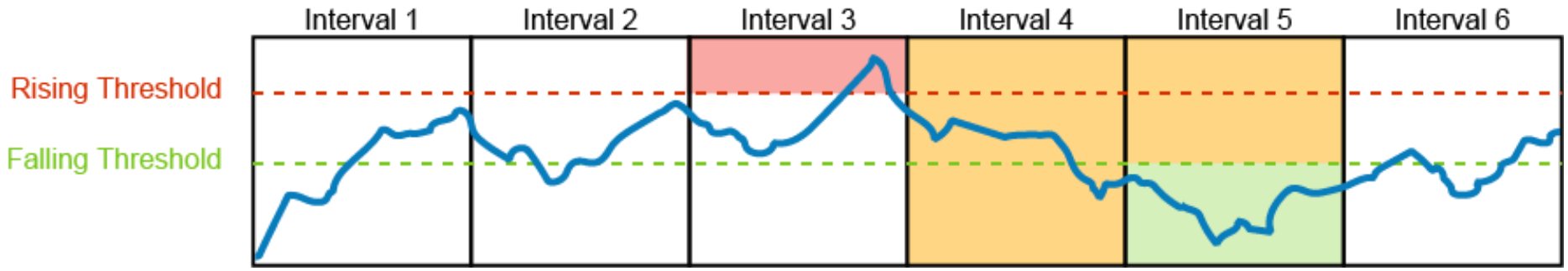
Storm Control (cont.)

- A LAN storm occurs when packets flood the LAN, create excessive traffic, and degrade network performance.
- Errors in protocol-stack implementation, mistakes in network configuration, such as spanning-tree misconfiguration, users issuing a DoS attack, or simply presence of a malfunctioning NIC can cause some sort of a storm in the network.



Storm Control (cont.)

- Switch uses the bandwidth-based method, the rising threshold is the percentage of total available bandwidth that is associated with multicast, broadcast, or unicast traffic before forwarding is blocked.
- The falling threshold is the percentage of total available bandwidth below which the switch resumes normal forwarding.



Storm Control (cont.)

- For example, if incoming traffic on an interface exceeds the specified rising threshold during a polling interval of one second, traffic gets blocked until the incoming rate drops below the configured falling interval on the interface.
- Storm control is configured for the switch as a whole, but operates on a per-port basis. By default, the storm control feature is disabled on Cisco switches.

Storm Control (cont.)

- An example of a storm control configuration contains the following steps:

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# storm-control broadcast level 60 50
Switch(config-if)# storm-control action shutdown
```

- When the broadcast traffic exceeds the configured level of 60 percent of the available bandwidth of the port, the switch puts the port into the error-disable state.
- When the broadcast traffic falls below 50 percent of the available bandwidth of the port, the port resumes normal forwarding.

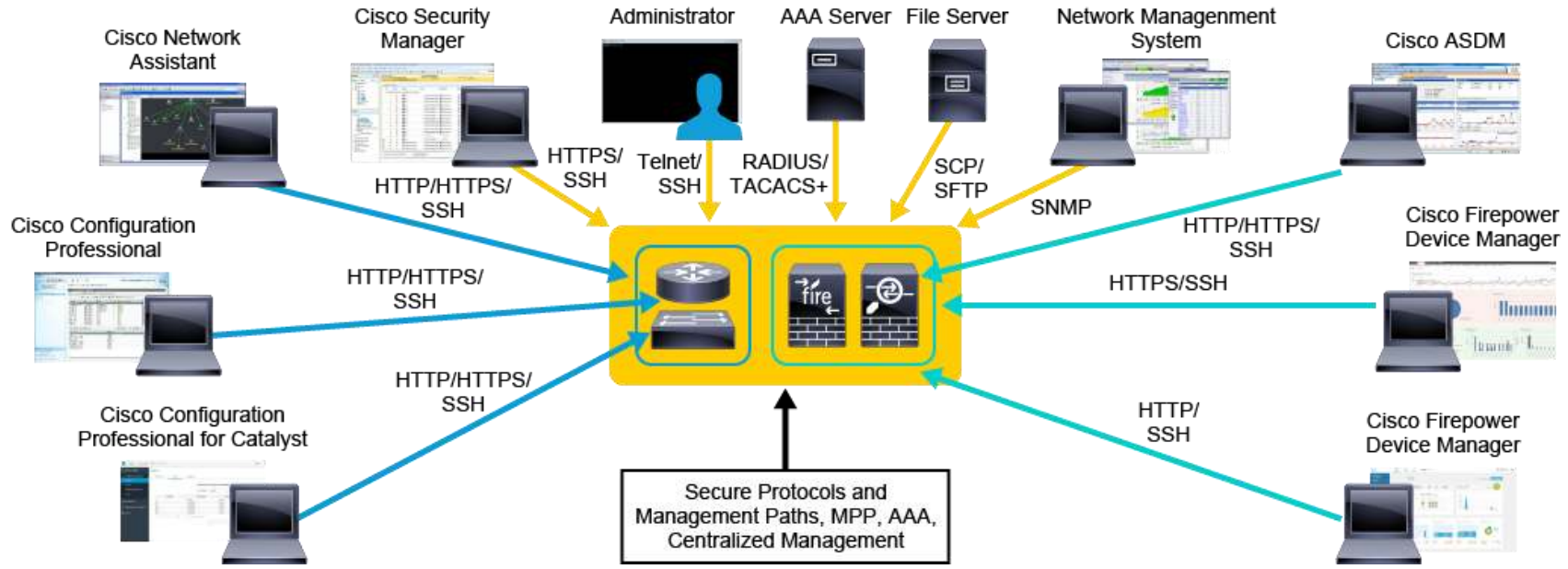
4.3- Management Plane Security Controls

Cisco Secure Management Access

- **The management plane** performs all of the management functions for a device, and coordinates functions between the control and data planes.
- These functions make the management plane a prime target for attacks.
- Management access to a device can be established locally or through a central management deployment.
- Either way, it is required an appropriate management system for performing management functions on the device.
- These management methods are platform dependent and can be used for managing only appropriate devices.

Cisco Secure Management Access (cont.)

- For performing management operations, Cisco IOS routers and switches, along with Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Next-Generation Firewall (NGFW) appliances can be remotely accessed by using various protocols, such as HTTP, HTTPS, Telnet, SSH, and SNMP.



Cisco Secure Management Access (cont.)

- You can use several protocols to remotely access the management functions of the network devices:
  - **Telnet:** A cleartext terminal, CLI access protocol that authenticates administrators before getting access to the devices,The Telnet protocol should not be used over untrusted networks and is generally considered obsolete for security device management.
  - **SSH:** A strongly encrypted and authenticated protocol that allows CLI access to the network devices, This protocol can be used over untrusted networks, if appropriate care is taken when managing the public key. This means not blindly accepting it over an untrusted network, but having a preprovisioned authentic copy that is already stored on the client system.

Cisco Secure Management Access (cont.)

- You can use several protocols to remotely access the management functions of the network devices (cont.)

  - **HTTP:** An unsecure protocol that allows GUI access to the network devices, for different management applications such as Cisco Network Assistant, Cisco Configuration Professional (also for Catalyst), Cisco Adaptive Security Device Manager (ASDM), and so on. The HTTP protocol does not provide any protection of the data sent, and because the communications operate in clear text it is not recommended over untrusted networks.

Cisco Secure Management Access (cont.)

- You can use several protocols to remotely access the management functions of the network devices (cont.)
  - **HTTPS:** A strongly encrypted and authenticated protocol that allows GUI access and file copy access to the networking devicesm, The HTTPS protocol authenticates the devices using public-key-based authentication (in the form of X.509 certificates), and administrators using passwords, or client certificates, The HTTPS protocol is recommended over the unsecure HTTP protocol, and can be used over untrusted networks, if appropriate care is taken when managing the device public key (certificate) in the same manner as with SSH. Every management application supports HTTPS, such as Cisco Network Assistant, Cisco Configuration Professional (also for Catalyst), Cisco ASDM, Cisco Content Security Management Appliance (SMA), Cisco Firepower Management Center (FMC) and Cisco Firepower Device Manager (FDM).

Cisco Secure Management Access (cont.)

- You can use several protocols to remotely access the management functions of the network devices (cont.)

  - **SNMP:** This protocol allows monitoring and configuration of various Cisco device parameters for performance and logging of system events, Cisco SNMP server implementations support all versions of the protocol (1, 2c, and 3), SNMP version 1 and 2c use cleartext authentication and transmission and are therefore not suitable for use over untrusted networks. SNMPv3 uses strong cryptographic authentication and transmission protection, and therefore can be deployed over untrusted network paths.

Simple Network Management Protocol Version 3

- In the complex network consisting of large amounts of different types of network devices, it can seem like a daunting task to manage all these devices and make sure that they are not only up and running but also performing optimally.
- This area is where SNMP can help.
- It was introduced to meet the growing need for a standard of managing IP devices.
- SNMP has evolved through three versions, but SNMPv3 is the only one that provides authentication, integrity and confidentiality of the data exchanged.
- Versions 1 and 2 support community strings as only methods for protection.

Simple Network Management Protocol Version 3 (cont.)

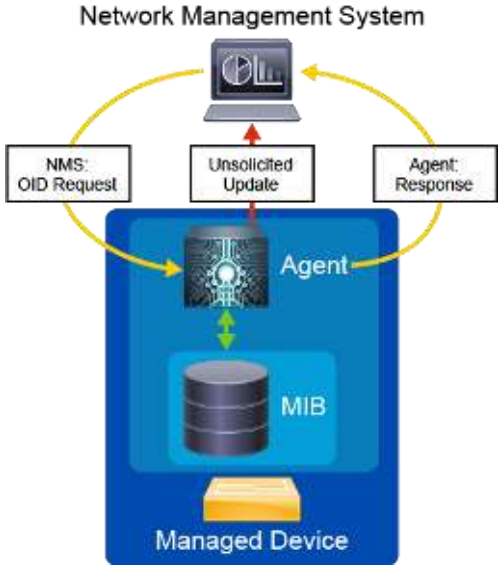
- SNMP exposes the environment and performance parameters of a network device, allowing a network management station (NMS) to collect and process data.
- Network devices keep statistics about the information of their processes and interfaces locally.
- SNMP on a device runs a special process that is called an agent.
- SNMP is typically used to gather environment and performance data such as device CPU usage, memory usage, interface traffic, interface error rate, and so on.
- The NMS polls devices periodically to obtain the values of the MIB objects that it is set up to collect.

Simple Network Management Protocol Version 3 (cont.)

- SNMP is an application layer protocol that defines how SNMP managers and SNMP agents exchange management information.
- SNMP uses the UDP protocol as a transport mechanism to retrieve and send management information, such as Management Information Base (MIB) variables.
- SNMPv3 provides secure access to devices

  by authenticating and encrypting packets

  when transferred over the network.



Simple Network Management Protocol Version 3 (cont.)

- SNMPv3 is broken down into three components or entities and each one contains different applications:

1. **SNMP manager:** The SNMP entity on an NMS includes an SNMP manager and SNMP applications, The manager implements the SNMP protocol, periodically polls the SNMP agents on managed devices by querying the device for data, and sends instructions to them when required. The SNMP applications are software applications that are used to manage the network, The SNMP manager can be part of an NMS such as Cisco Prime Infrastructure.

Simple Network Management Protocol Version 3 (cont.)

- SNMPv3 is broken down into three components or entities and each one contains different applications (cont.)

2. **SNMP agent:** Each managed device (SNMP entity) includes an SNMP agent and an SNMP MIB, The agent runs directly on the managed device, implements the SNMP protocol and allows a managed node to provide information to the NMS and accept instructions from it. The MIB defines the information that can be collected and used to control the managed node. Information exchanged using SNMP takes the form of objects from the MIB.

Simple Network Management Protocol Version 3 (cont.)

- SNMPv3 is broken down into three components or entities and each one contains different applications (cont.)

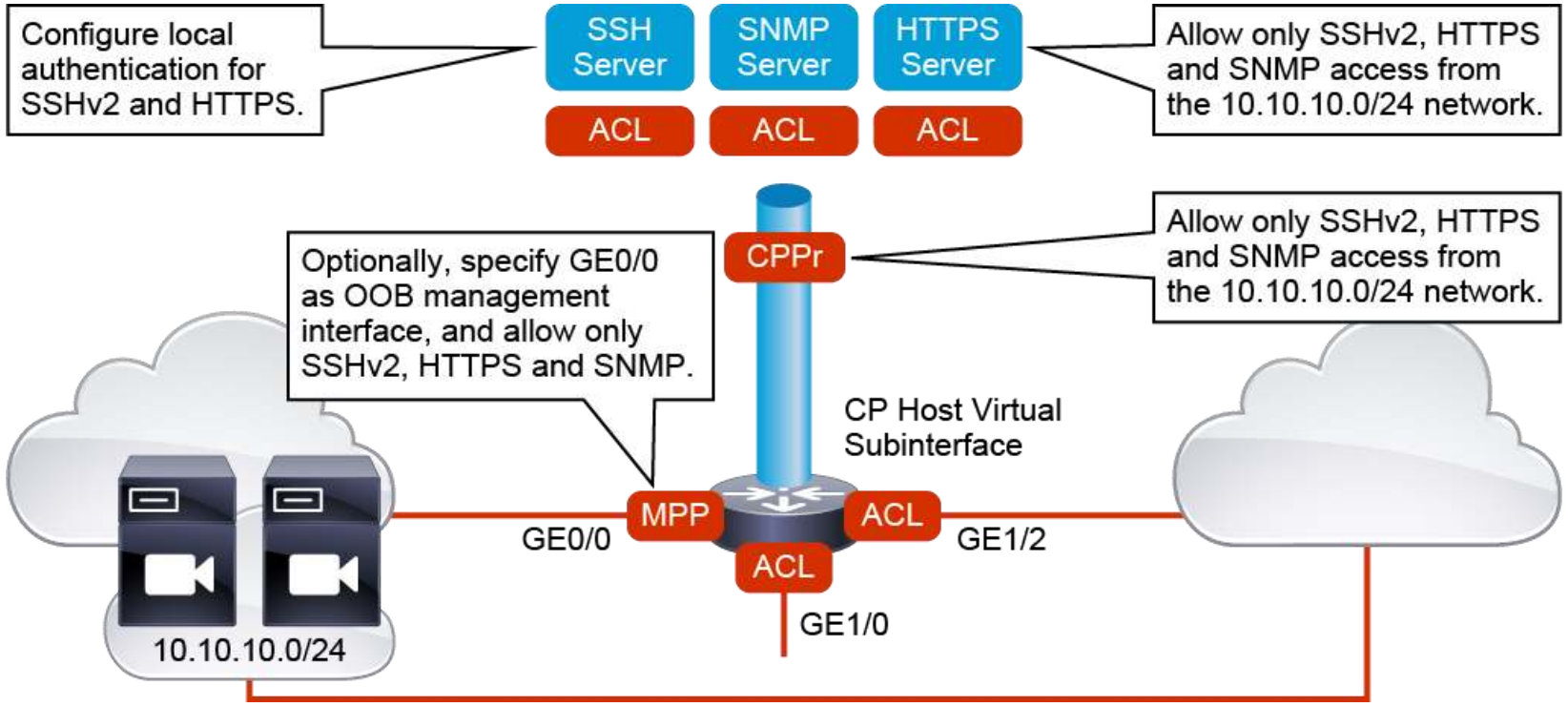
3. **MIB:** Represents a virtual information storage location that contains collections of managed objects, Within the MIB, there are objects that relate to different defined MIB modules (for example, the interface module), Objects in the MIB are referenced by their Object Identifiers (OID), They can define information about many different variables, such as interface status, CPU usage and so on.

Secure Access to Cisco Devices

Access Control Feature	Benefit	Limitation
Interface ACLs	Can limit access to any service	Not scalable with a large number of interfaces
Service-specific ACLs	Easy to configure, manageable	Cannot limit access to all services
Control Plane Protection	Easy to configure, manageableCan limit access to any service	Not available on all platforms
Management Plane Protection	Easy to configure Supports OOB access	Requires OOB access

Secure Access to Cisco Devices (cont.)

Use Case for Secure Access to Cisco Router



Secure Access to Cisco Devices (cont.)

Use Case for Secure Access to Cisco Router (cont.)

- When implementing management plane access control, use one or more of the following configuration tasks will be defined:

1. Enable use of secure management protocols (SSHv2, HTTPS, and SNMPv3) and enable local authentication.
2. It is recommended that you always deploy service-specific access rules to specify the management sources that can access a specific Cisco IOS Software management process.
3. Optionally, or alternatively, you can use CPPr to limit access to management processes using a simple, centralized policy.
4. Optionally, or alternatively, you can also configure MPP, if your network design allows you to dedicate a local interface to management traffic.

Secure Access to Cisco Devices (cont.)

Configuring SSHv2 Access (steps)

1. Configuring a hostname and domain name on the device
2. Generating public RSA (Rivest-Shamir-Adleman) key pair for establishing session (symmetric) key between communicating devices
3. Configuring local accounts (username and password) for user authentication in the local user database of the device
4. Enabling local authentication on the vty lines of the device
5. Enabling SSH access on the vty lines of the device
6. Enabling SSHv2, so no older versions are accepted, but version 2

Secure Access to Cisco Devices (cont.)

Configuring SSHv2 Access (lab)

```
Router(config)# hostname HQ-ISR
HQ-ISR(config)# ip domain-name example.com
HQ-ISR(config)# crypto key generate rsa modulus 1024
HQ-ISR(config)# username admin secret Admin$Secret
HQ-ISR(config)# line vty 0 4
HQ-ISR(config-line)# login local
HQ-ISR(config-line)# transport input ssh
HQ-ISR(config-line)# exit
HQ-ISR(config)# ip ssh version 2
```

Secure Access to Cisco Devices (cont.)

HTTPS Configuration and Operation (lab)

```
HQ-ISR(config)# no ip http server
HQ-ISR(config)# ip http secure-server
```

Secure Access to Cisco Devices (cont.)

Filtering Management Access with ACLs (Lab)

```
HQ-ISR(config)# access-list 90 permit 10.10.10.0 0.0.0.255
HQ-ISR(config)# access-list 90 deny any log

HQ-ISR(config)# line vty 0 15
HQ-ISR(config-line)# access-class 90 in

HQ-ISR(config)# ip http access-class 90
```

Secure Access to Cisco Devices (cont.)

Configuring CPPr and MPP (steps)

- CPPr configures Quality of Service (QoS) features for the management plane.
- It is configured with the IOS Modular QoS CLI (MQC) framework:
  - **Class maps:** Define characteristics to categorize traffic into classes using ACL.
  - **Policy maps:** Define actions that should be taken on particular classes of traffic.
  - **Service policies:** Specifies a statement where a policy map should be implemented.

Secure Access to Cisco Devices (cont.)

Configuring CPPr and MPP (Lab)

- Defining an **extended ACL** that allows the management protocols for accessing the device, The following extended ACL named 'CPPR-MGMT" will permit HTTPS, SSH, and SNMP connections from hosts on the 10.10.10.0/24 network. All other traffic will be implicitly denied.

```
HQ-ISR(config)# ip access-list extended CPPR-MGMT
HQ-ISR(config-ext-nacl)# permit tcp 10.10.10.0 0.0.0.255 any eq 443
HQ-ISR(config-ext-nacl)# permit tcp 10.10.10.0 0.0.0.255 any eq 22
HQ-ISR(config-ext-nacl)# permit udp 10.10.10.0 0.0.0.255 any eq 161
```

Secure Access to Cisco Devices (cont.)

Configuring CPPr and MPP (Lab cont.)

- Configuring a **class map** that will use an ACL as a matching criteria for categorizing the management traffic into the class. In this case the class map named 'CPPR-MGMT-CLASS" will reference the 'CPPR-MGMT" ACL.

```
HQ-ISR(config)# class-map CPPR-MGMT-CLASS
HQ-ISR(config-cmap)# match access-group name CPPR-MGMT
```

Secure Access to Cisco Devices (cont.)

Configuring CPPr and MPP (Lab cont.)

- Configuring a **policy map** that references the configured class, and police the class to a rate that is not exceeded by legitimate traffic.

```
HQ-ISR(config)# policy-map CPPR-POLICY
HQ-ISR(config-pmap)# class CPPR-MGMT-CLASS
HQ-ISR(config-pmap-c)# police rate 50 pps conform-action transmit exceed-action drop
HQ-ISR(config-pmap-c)# class class-default
HQ-ISR(config-pmap-c)# drop
```

Secure Access to Cisco Devices (cont.)

Configuring CPPr and MPP (Lab cont.)

- **Applying the policy map to the appropriate interface**. The policy map 'CPPR-POLICY" is applied on the control-plane host subinterface.

```
HQ-ISR(config)# control-plane host
HQ-ISR(config-cp)# service-policy input CPPR-POLICY
```

Secure Access to Cisco Devices (cont.)

Configuring CPPr and MPP (Lab cont.)

- Configuring a local interface as a dedicated management interface using MPP.

```
HQ-ISR(config-cp)# management-interface GE0/0 allow ssh snmp https
```