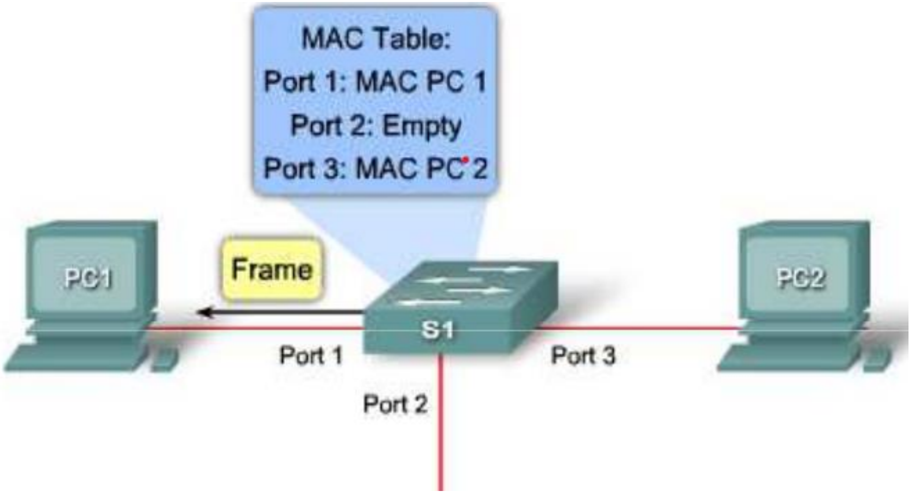
Layer2 attack and how to mitigate it.

The attack

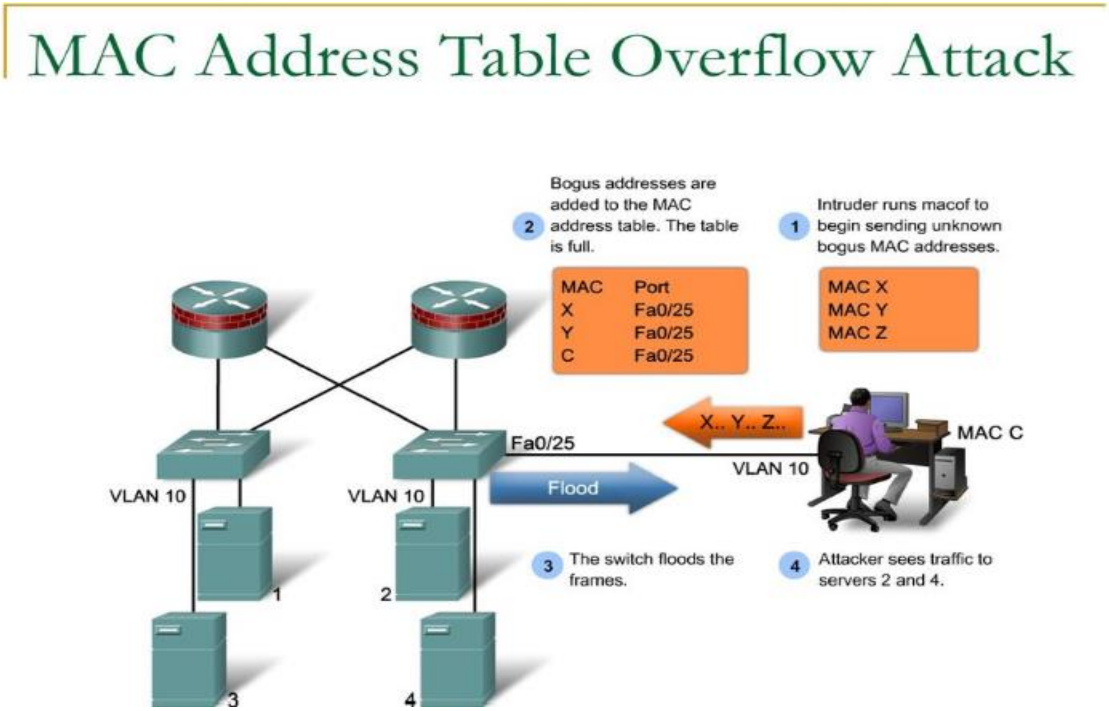
Mac address table overflow attack (mac address flood)

(Normal Switch Operation)

The switch can forward frames between PC1 and PC2 without flooding because the MAC address table contains port-to-MAC-address mappings in the MAC address table for these PCs.



A CAM Overflow attack relies on flooding the switch with many invalid source MAC addresses until the table is full. When the attack causes the switch to act as a hub, the threat actor can monitor traffic passing through it.



MAC Address Table Overflow Attack

2 Bogus addresses are added to the MAC address table. The table is full.

MAC	Port
X	Fa0/25
Y	Fa0/25
C	Fa0/25

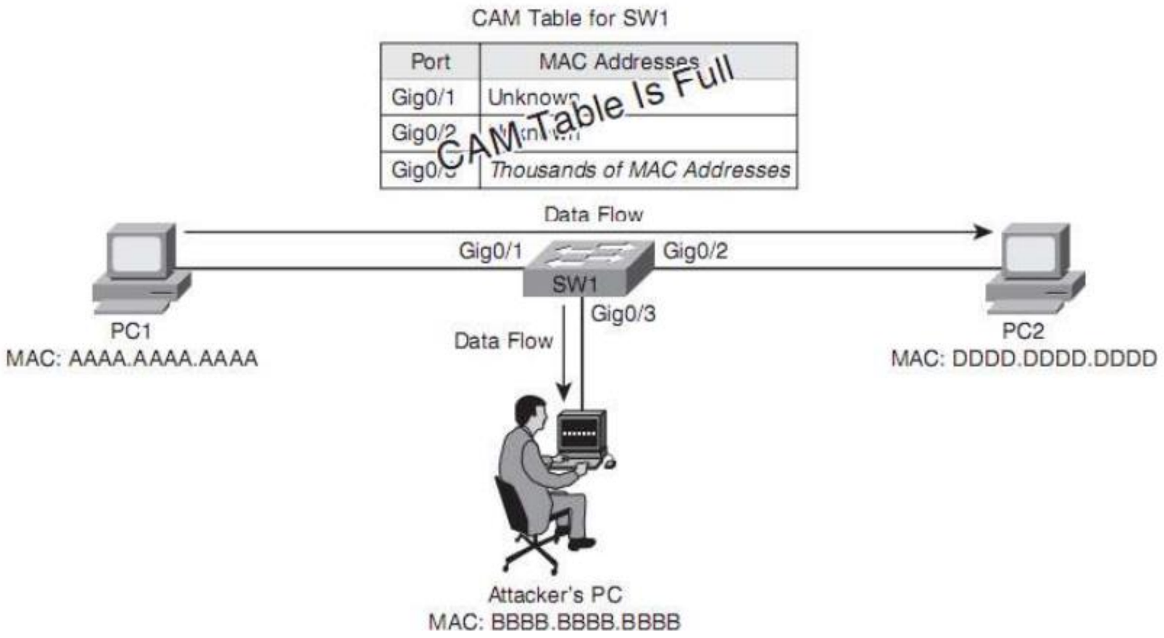
1 Intruder runs macof to begin sending unknown bogus MAC addresses.

MAC X
MAC Y
MAC Z

3 The switch floods the frames.

4 Attacker sees traffic to servers 2 and 4.

Flooding Behavior After a CAM Table Overflow Attack



Port	MAC Addresses
Gig0/1	Unknown
Gig0/2	Unknown
Gig0/3	Thousands of MAC Addresses

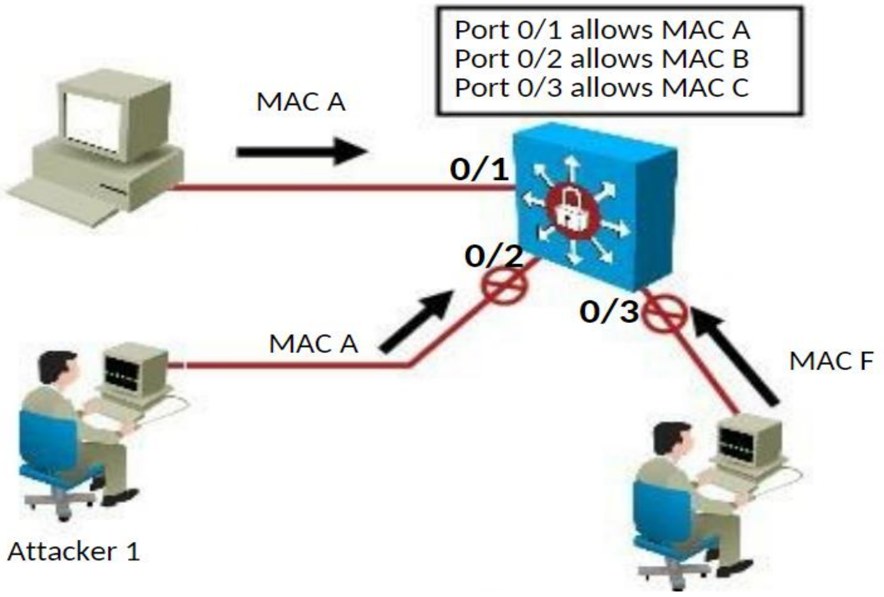
The Mitigation

Port security

- Allows an administrator to statically specify MAC Addresses for a port or to permit the switch to dynamically learn a limited number of MAC addresses.

- Limits the number of MAC addresses to be learned on an access switch port.

- Port security controls how many MAC addresses can be learned on a single switch port.



The violation: -

When the number of secure MAC addresses reaches the limit allowed on the port:

1. **protect**: -packets with unknown source addresses are dropped. You are not notified that a security violation has occurred.
2. **restrict**: - packets with unknown source addresses are dropped. you are notified that a security violation has occurred. The counter increases by one.
3. **shutdown**: - packets with unknown source addresses are dropped. you are notified that a security violation has occurred. The counter increases by one.

   The interface dropped in error-disable state.
4. **shutdown per VLAN**: - only the VLAN on which the violation occurred is error-disabled.

Once the counter reaches a predefined threshold, the device might trigger an alert.

The configuration: -

port security can't be set on the dynamic mode

```
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 shutdown

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

Switch(config-if)# switchport port-security aging time 120
```

- The aging command allows MAC-Addresses on the Secure switchport to be deleted after the set aging time.

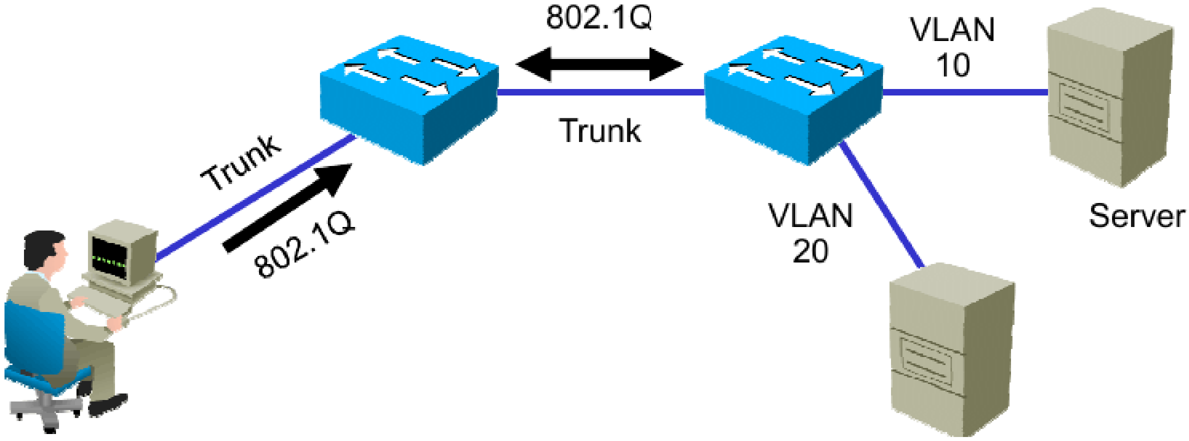
Aging Parameters

static	**Enable aging for statically configured secure addresses on this port.**
time (time)	**Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.**
type absolute	**All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.**
type inactivity	**The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time.**

The attack

VLAN Hopping attack.

Switch spoofing



-Spoofing DTP Messages from the attacking host to cause the switch to enter trunking mode.

-The attacker uses tools like Yersinia.

-Attacking device gains access to data on all VLANs carried by the negotiated trunk.

step	Description
1.	Attacker gains access to a switch port and sends DTP negotiation frames toward a switch with DTP running and auto negotiation turned on.
2.	Attacker and switch negotiate trunking over the port.
3.	Switch allows all VLANs to traverse the trunk link.
4.	Attacker sends data to, or collects it from, all VLANs carried on that trunk.

The Mitigation

The best way to prevent a basic VLAN hopping attack is to turn off trunking on all ports, except the ones that specifically require trunking. On the required trunking ports, disable DTP (auto trunking) negotiations and manually enable trunking.

-enable access on the access ports manually.

-disable the DTP.

The attack

Double-Tagging VLAN Attack

-An important characteristic of the double encapsulated VLAN hopping attack is that it

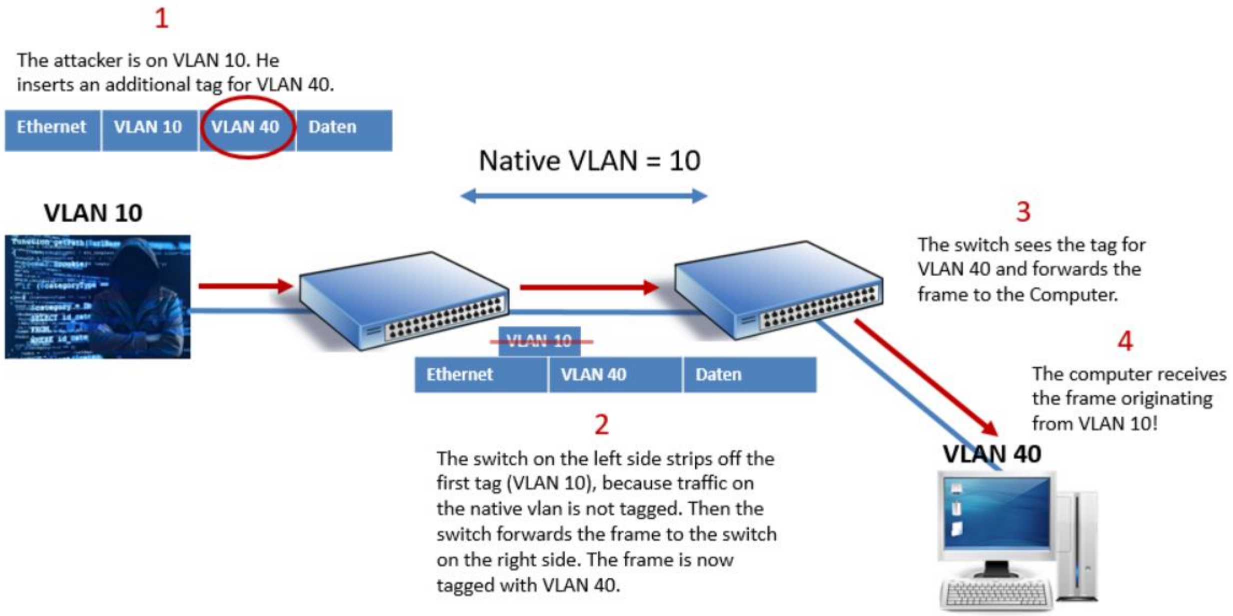
works even if trunk ports are disabled.

-the attacker must be in the native VLAN.

-**one way attack. (can use to send malicious).**

-this attack is unidirectional.

-**the attacker uses tools like Yersinia.**


1
The attacker is on VLAN 10. He inserts an additional tag for VLAN 40.
Ethernet
VLAN 10
VLAN 40
Daten
Native VLAN = 10
VLAN 10
~~VLAN 10~~
Ethernet
VLAN 40
Daten
2
The switch on the left side strips off the first tag (VLAN 10), because traffic on the native vlan is not tagged. Then the switch forwards the frame to the switch on the right side. The frame is now tagged with VLAN 40.
3
The switch sees the tag for VLAN 40 and forwards the frame to the Computer.
4
The computer receives the frame originating from VLAN 10!
VLAN 40

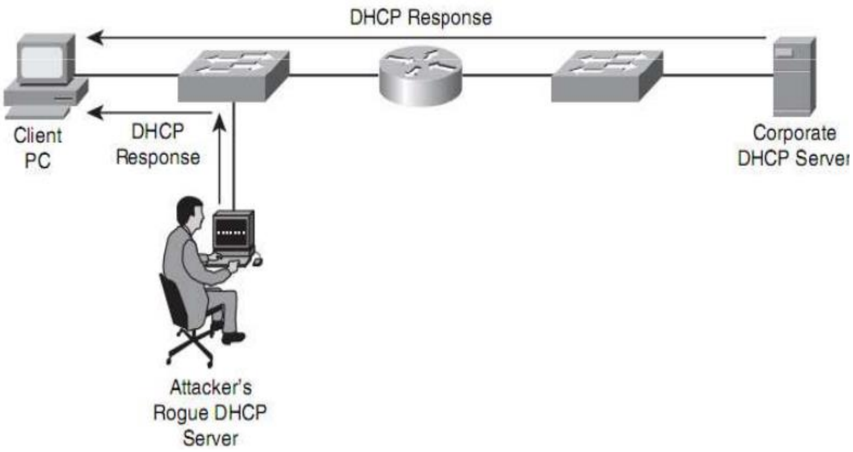
The Mitigation

Change the native VLAN and don’t put any device on the native VLAN.

The attack

DHCP Server Spoofing

If an attacker connects a rogue DHCP server to the network, the rogue DHCP server can respond to a client’s DHCP request. Even though both the rogue DHCP server and the actual DHCP server respond to the request, the client uses the rogue DHCP server’s response if it reaches the client before the response from the actual DHCP server.



The Mitigation

DHCP Snooping

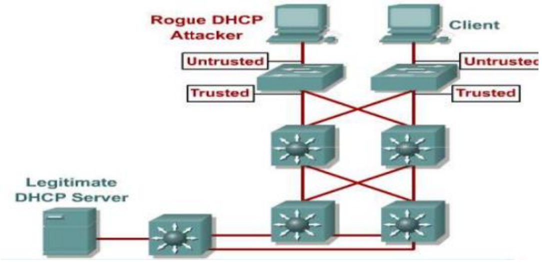
DHCP snooping provides an additional layer of security to ensure that DHCP services are only provided by trusted servers, preventing unauthorized devices from causing disruptions or potential security risks on the network.(Prevents rogue DHCP servers from impacting the network.)

The switch build the DHCP **snooping binding table** contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch. (show ip dhcp snooping binding)

-**DHCP snooping is enabled on a per-VLAN basis.**

-DHCP snooping prevents DHCP spoofing and DHCP starvation.

The configuration:-



```
sw2(config)# ip dhcp snooping

sw2(config)# ip dhcp snooping vlan 10

sw2(config)# interface Gi1/0

sw2(config-if)# ip dhcp snooping trust

sw2(config)# interface Gi1/1

sw2(config-if)# ip dhcp snooping limit rate 3
```

sw2(config)# no ip dhcp snooping information option ➔ means don’t send option 82

dhcp-server (config-if)# ip dhcp relay information trusted ➔ means accept the clear option 82➔under trusted interface

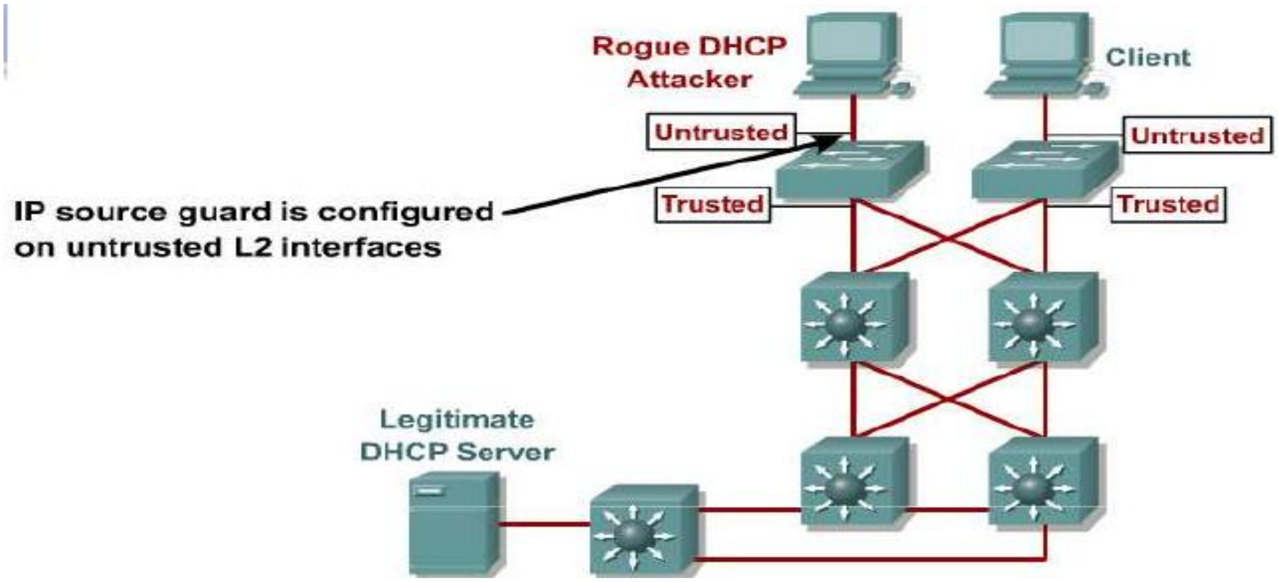
Sw2(config)#ip dhcp snooping database flash

the option 82 (relay agent or giadder) is clear so we must write one of this commend. Why clear it depend on the firmware of the switch or some another reasons.

Option 82 → it contains information about the switch and the client who ask for ip.

IP Source Guard

IP source guard is a security feature on Cisco devices that prevents IP address spoofing. It ensures that only IP traffic with source IP addresses that match valid IP/MAC bindings are forwarded by the device.



The configuration

```
sw2(config)# ip dhcp snooping
sw2(config)# ip dhcp snooping vlan 10
sw2(config)# interface Gi1/0/24
sw2(config-if)# ip verify source vlan dhcp-snooping port-security
```

Enables IP Source guard, source ip and source MAC address filter on a port.

DHCP snooping binding table protects me from some kind of attack such as ARP Spoofing.

Eng.Ahmed Shawky

The attack

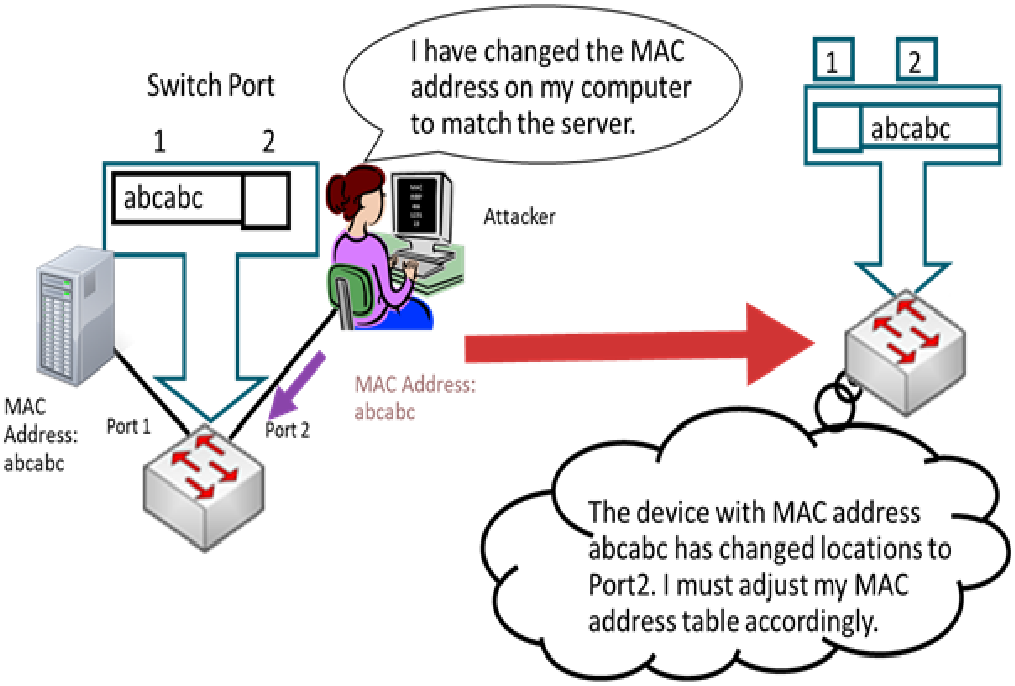
MAC address spoofing (ARP spoofing)

The mac address spoofing depends on the **Gratuitous ARP**. The Gratuitous ARP used to remove the cache on the switch to update data that cashed (this happened if I change the gateway or change the ip for interface or change the router ……)

-the aim is to associate the attacker's MAC address with the IP address of another node

(such as the default gateway).

- The attacker could then choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (MITM)


Switch Port
1
2
abcabc
I have changed the MAC address on my computer to match the server.
Attacker
MAC Address: abcabc
Port 1
Port 2
MAC Address: abcabc
1
2
abcabc
The device with MAC address abcabc has changed locations to Port2. I must adjust my MAC address table accordingly.

The Mitigation

Dynamic ARP inspection (DAI)

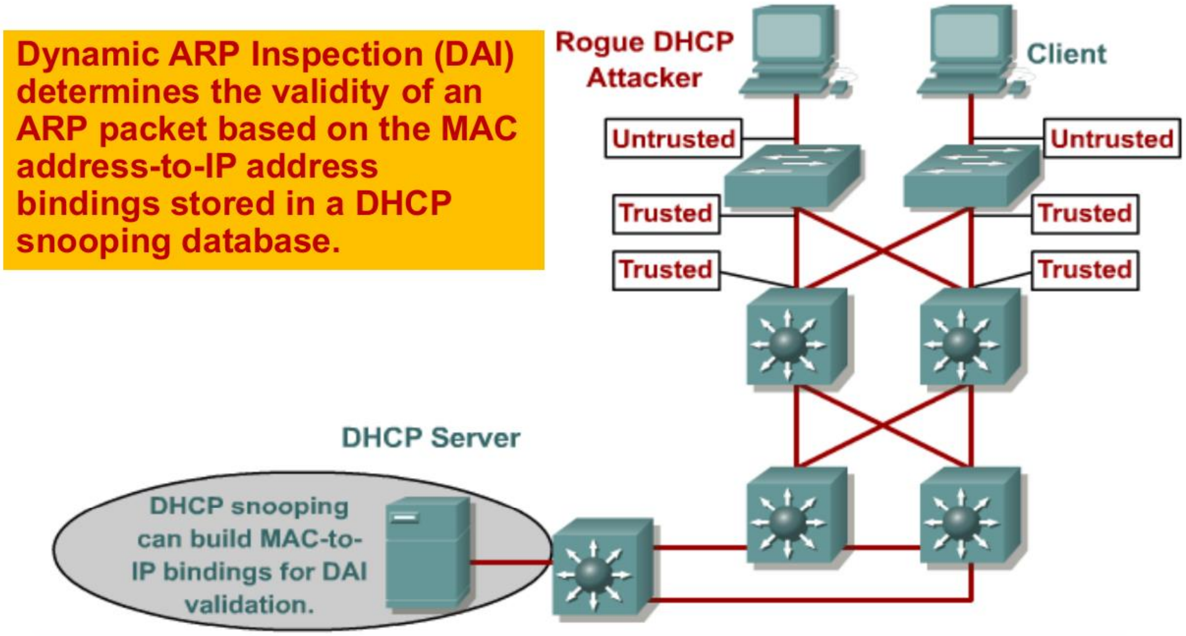
The mitigation depends on DHCP snooping.

-DAI works by inspecting and validating the ARP packets on the network. It maintains an ARP binding table that contains valid IP-to-MAC address mappings.

-**DAI works by using the DHCP snooping binding database**

- **DAI can also be used to prevent ARP cache poisoning attacks**

Configuration: -



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.

This configuration based on DHCP Snooping binding table so you should run the dhcp snooping first.

Switch (config) #ip arp inspection vlan10

After this command all interfaces become untrust you should trust the interfaces you want.

Switch (config-if)# ip arp inspection trust

You should trust the dhcp snooping interface also.

ip arp inspection trust

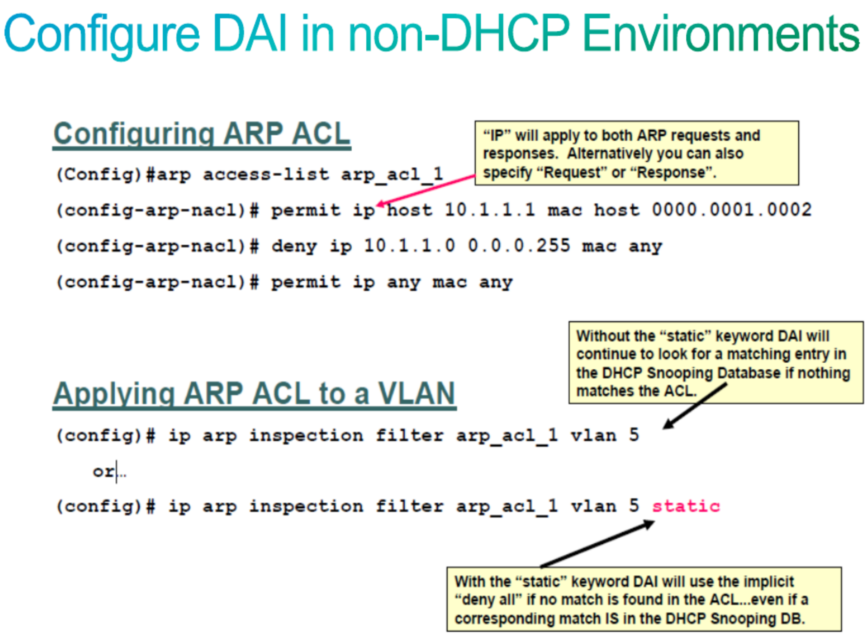
ip dhcp snooping trust

-you can determine the number of packets

The interface will receive in one second .

-To avoid the dos attack.

-If some one make a dos attack to me the interface drop in error- disable.



Configure DAI in non-DHCP Environments

Configuring ARP ACL

```
(Config)#arp access-list arp_acl_1
(config-arp-nacl)# permit ip host 10.1.1.1 mac host 0000.0001.0002
(config-arp-nacl)# deny ip 10.1.1.0 0.0.0.255 mac any
(config-arp-nacl)# permit ip any mac any
```

"IP" will apply to both ARP requests and responses. Alternatively you can also specify "Request" or "Response".

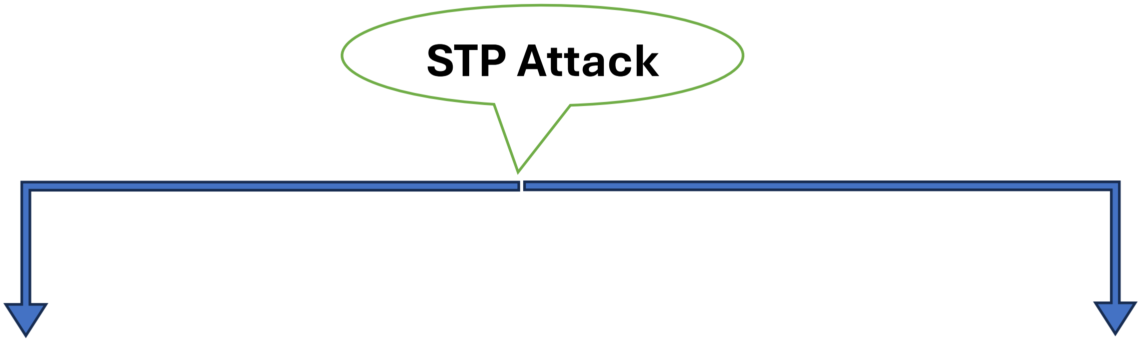
Applying ARP ACL to a VLAN

```
(config)# ip arp inspection filter arp_acl_1 vlan 5
    or..
(config)# ip arp inspection filter arp_acl_1 vlan 5 static
```

Without the "static" keyword DAI will continue to look for a matching entry in the DHCP Snooping Database if nothing matches the ACL.

With the "static" keyword DAI will use the implicit "deny all" if no match is found in the ACL...even if a corresponding match IS in the DHCP Snooping DB.

Spanning tree protocol



STP Attack

Unexpected BPDU (STP filter)

-Root guard

-BPDU guard

-BPDU filter

Sudden loss of BPDU

- skew detection

- loop guard

- UDLD

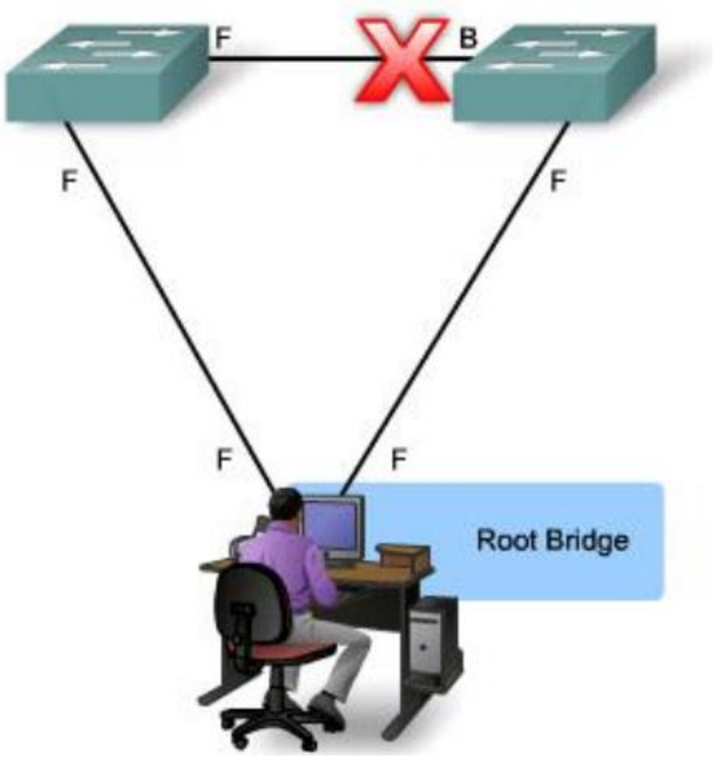
The attack

An STP attack typically involves the creation of a bogus Root bridge.

-The attacking host broadcasts STP configuration and topology change BPDUs to force spanning-tree recalculations.

- The BPDUs sent by the attacking host announce a lower bridge priority to be elected as the root bridge.

-If successful, the attacking host becomes the root bridge and sees a variety of frames that otherwise, are not accessible.



The Mitigation

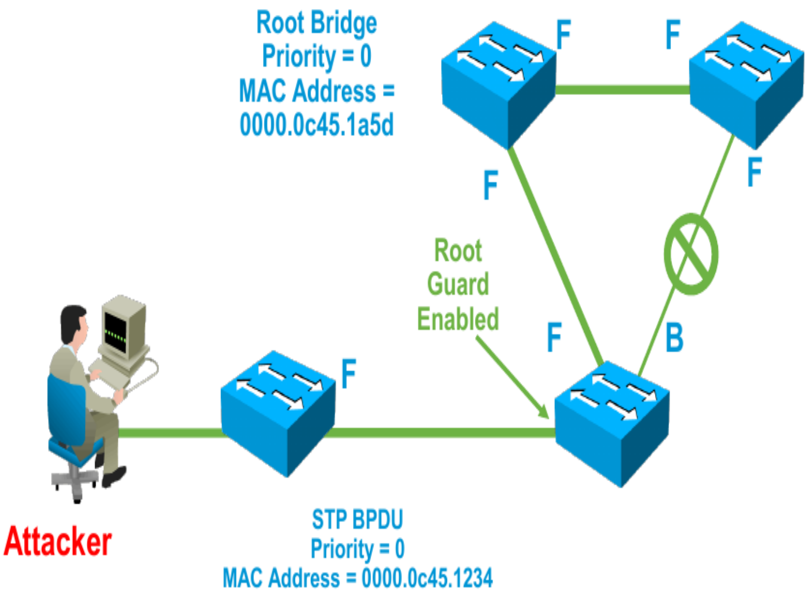
Unexpected BPDU

Root guard

-If a root-guard-enabled port receives BPDUs that are superior to those that the current root bridge is sending, that port is moved to a root-***inconsistent state***.

– This effectively is equal to an STP listening state, and no data traffic is forwarded across that port.

- If an attacking host sends out spoofed BPDUs to become the root bridge, the switch, upon receipt of a BPDU, ignores the BPDU and puts the port in a root-inconsistent state.



– The port recovers as soon as the offending BPDUs cease.

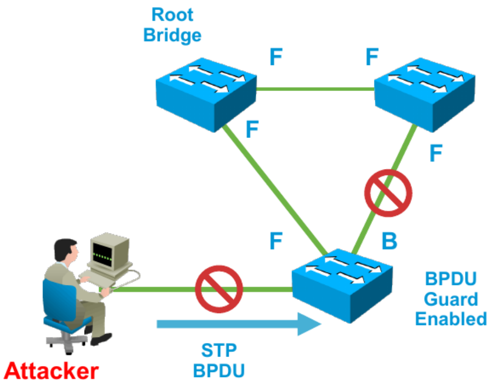
The configuration

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

BPDU guard

-It protects a switched network from receiving BPDUs on ports that should not be receiving them.

-If a port configured with Port Fast and BPDU Guard receives a BPDU, the switch will put the port into the **disabled state. (error-disable)**.



The configuration

Switch(config)#spanning-tree portfast bpduguard default

If I want to disable it under interface you can do it under that interface.

Switch(config-if) #Spanning tree portfast (bpduguard) disable

Eng.Ahmed Shawky

BPDU Filter

-can configure in per interface or globally

per interface: - means doesn't send BPDU and doesn't received BPDU

Globally: - means doesn't send BPDU and process BPDU(receive).

doesn't drop the interface if it receives the bpdu.

Switch (config-if) spanning-tree bpdu filter (edge) enable

Switch(config)# spanning-tree portfast bpdufilter default

Sudden loss of BPDU

skew detection

-not supported right now.

-if the switch didn’t receive BPDU the syslog appears.

loop guard

-common in the fiber cable.

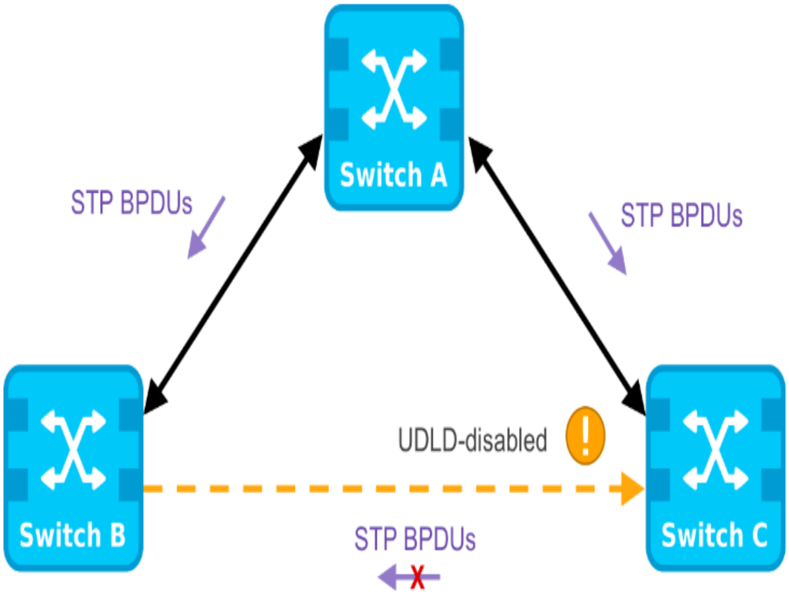
Loop guard is a Cisco feature that helps prevent Layer 2 loops in Spanning Tree Protocol (STP) enabled network. When enabled on a port, loop guard monitors the port to check for any loop conditions. If a loop is detected, loop guard puts the port into a loop-inconsistent state rather than transitioning it to a forwarding state.

Loop guard can be configured globally on all ports using the "**spanning-tree loopguard default**".

command, or it can be configured on specific ports using the "**spanning-tree guard loop**" command.

Unidirectional Link Detection (UDLD)

-common in the fiber.



-Unidirectional Link Detection (UDLD) is a Cisco proprietary layer 2 protocol used to determine the physical status of a link. The purpose of Unidirectional Link Detection (UDLD) is to detect and deter issues that arise from Unidirectional Links. UDLD helps to prevent forwarding loops and blackholing of traffic by identifying and acting on logical one-way links that would otherwise go undetected.

There are two modes: -

1) **Normal**

-send syslog when a problem is appears. (like skew detection).

Configuration

udld enable

2) **Aggressive**

-send syslog

-put the interface in error disable.

configuration

```
udld aggressive
```

port fast

-if you enable port fast on the 'access port' this port "transitions from blocking to forwarding state immediately".

- if you enable port fast on a port connecting to another switch , you risk creating a spanning tree loop.

Configuration

```
s1(config)# interface fastethernet 0/1
s1(config-if) # spanning-tree portfast
```

storm control

-limits the amount of broadcast or multicast traffic flowing through the switch.

-Prevents traffic from being disrupted by an excessive broadcast, multicast, or unicast storm on a port.

-Bandwidth-based or packet-based traffic activity measurement.

configuration

```
interface fastethernet0/1

storm-control broadcast level 60 50

storm-control action shutdown
```

my LinkedIn

https://linkedin.com/in/ahmed-shawky-0003a4259