# SWITCHING ESSENTIALS

PUTERI AZWA BT AHMAD
SITI NURDIANA BINTI ABU BAKAR
MUHAMMAD KHAIRUL EZAD BIN SULAIMAN

# SWITCHING ESSENTIALS

PUTERI AZWA BT AHMAD
SITI NURDIANA BINTI ABU BAKAR
MUHAMMAD KHAIRUL EZAD BIN SULAIMAN

## Author

Puteri Azwa bt Ahmad
Siti Nurdiana binti Abu  Bakar
Muhammad Khairul Ezad bin Sulaiman

## Editor

Puteri Azwa bt Ahmad
Siti Nurdiana binti Abu  Bakar
Muhammad Khairul Ezad bin Sulaiman

## Designer

Puteri Azwa bt Ahmad
Siti Nurdiana binti Abu  Bakar
Muhammad Khairul Ezad bin Sulaiman



## First Published 2024





## Published by:

POLITEKNIK TUANKU SYED SIRAJUDDIN
Pauh Putra
02600 Arau
Perlis
www.ptss.edu.my

Cataloguing-in-Publication Data

Perpustakaan Negara Malaysia

A catalogue record for this book is available from the National Library of Malaysia

eISBN 978-629-7514-58-1

# PREFACE

This e-book is designed to provide a frame of reference for Polytechnic diploma courses in Information Technology or students majoring in related courses. The e-book is alternatively useful to those who wish to keep enhancing their knowledge on the switching technology in computer network.

This e-book consists of three main topics, which cover the topics of **Switching Essentials** adapted by the Malaysian Polytechnics. Students are guided to acquire the required skill and knowledge of attack in switching technology.

Finally, this e-book can also be beneficial to students and other readers using this e-book as reference. Hopefully, students will find this e-book helpful in assisting them to achieve a better knowledge and understanding in switch attacks which can provide readers with a better result and comprehension.

# TABLE OF CONTENTS


## CHAPTER 1 : NETWORK ATTACKS

*Network attacks* 1
*Types of network attack* 1

## CHAPTER 2 : SWITCH ATTACKS

*Switch attack categories* 2
*MAC address table attack* 3
*VLAN hopping attack* 5
*VLAN double tagging attack* 6
*DHCP attack* 8
*Address Resolution Protocol (ARP) attack* 10
*Address spoofing attack* 11
*Spanning Tree Protocol (STP) attack* 12
*CDP reconnaissance attack* 13

## CHAPTER 3: ATTACK PREVENTION

*Disable unused ports on switch* 14
*MAC address table attack prevention* 15
*VLAN attack prevention* 23
*DHCP attack prevention* 24
*Address Resolution Protocol (ARP) attack prevention* 25
*Spanning Tree Protocol (STP) attack prevention* 26

## SWITCH SECURITY ACTIVITIES 28

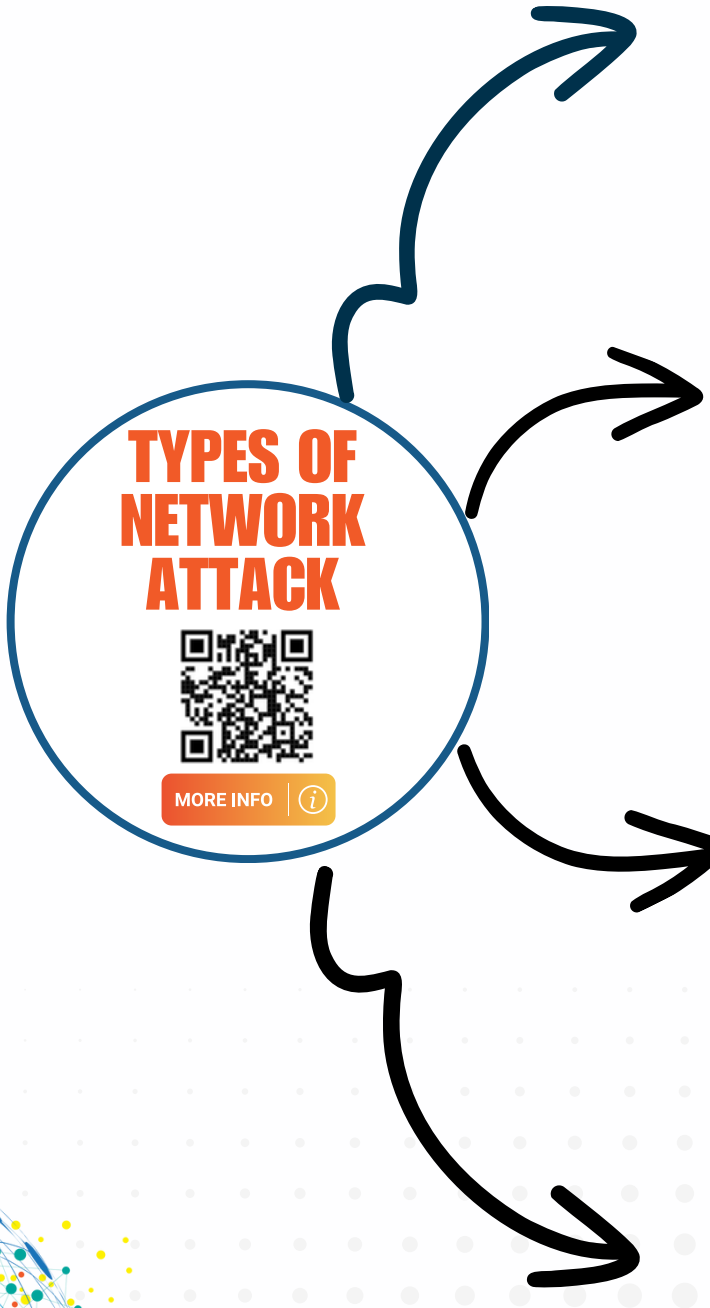
## REAL WORLD ATTACKS AND PREVENTIONS 29

## REFERENCES 31

# NETWORK ATTACKS

# NETWORK ATTACK

**A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity.**




## DDOS ATTACK

This is a coordinated attack from many devices, called zombies, with the intention of degrading or halting public access to an organization's website and resources

## DATA BREACH ATTACK

This is an attack in which an organization's data servers or hosts are compromised to steal confidential information.

## MALWARE ATTACK

This is an attack in which an organization's hosts are infected with malicious software that cause a variety of problems. For example, ransomware such as WannaCry encrypts the data on a host and locks access to it until a ransom is paid.

## DOS ATTACK

Is an attack meant to shut down a machine or network, making it inaccessible to its intended users

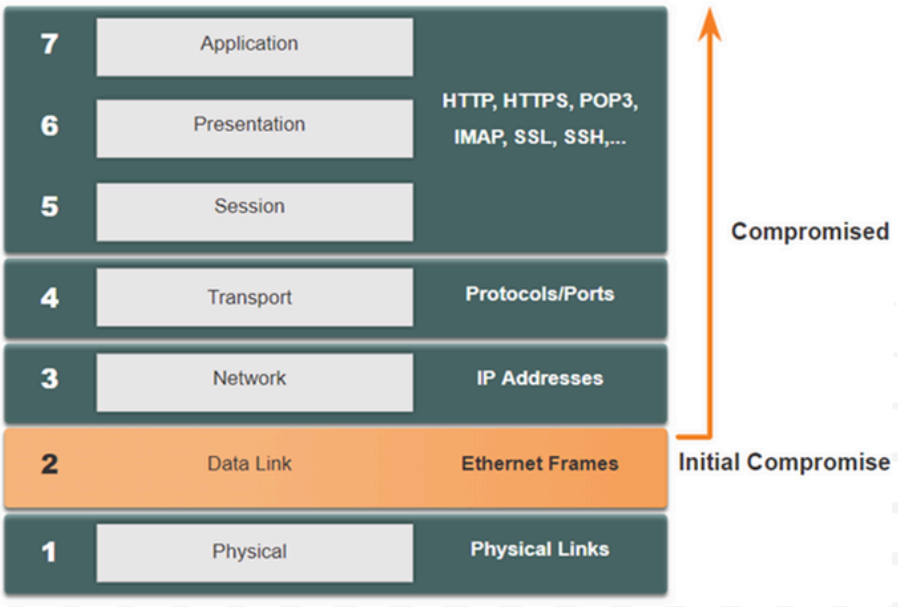
# SWITCH ATTACKS

# SWITCH ATTACK CATEGORIES

Security is only as strong as the weakest link in the system, and Layer 2 (Data Link Layer) is considered to be that weak link. This is because LANs were traditionally under the administrative control of a single organization and this cause a single point of failure. Switch operates at Layer 2 and becomes the target of many attacks.

# TYPES OF SWITCH ATTACKS

- MAC address table attack
- VLAN hopping attack
- VLAN double tagging attack
- DHCP attack
- ARP attack
- Address spoofing attack
- STP attack
- CDP reconnaissance attack



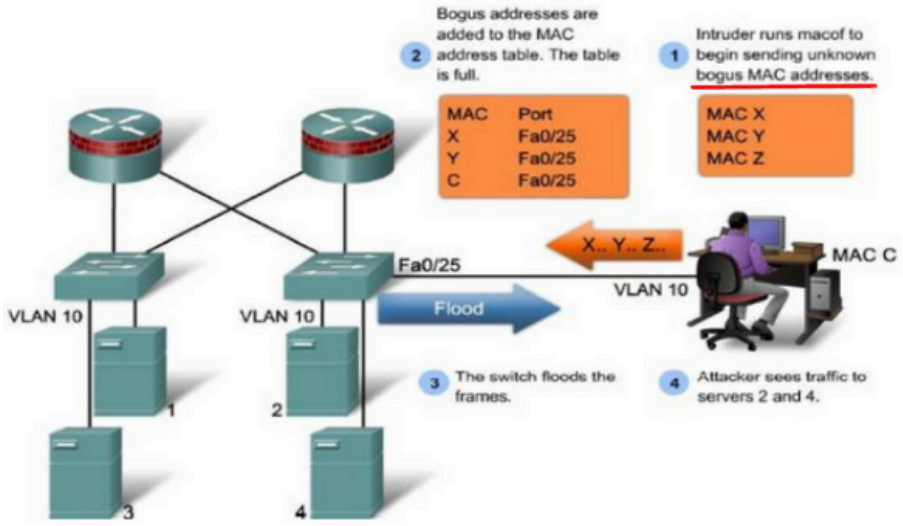
# MAC ADDRESS TABLE ATTACK

All MAC tables have a fixed size and consequently, a switch can run out of resources in which to store MAC addresses.

MAC address flooding attacks take advantage of this limitation by bombarding the switch with fake source MAC addresses until the switch MAC address table is full.

When this occurs, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic out all ports on the same VLAN without referencing the MAC table.

This condition now allows a attacker to capture all of the frames sent from one host to another on the local LAN or local VLAN.




**MAC Address Table Attack**

Note: Traffic is flooded only within the local LAN or VLAN. The attacker can only capture traffic within the local LAN or VLAN to which the attacker is connected.

Another reason why these attack are dangerous because they not only affect the local switch, they can also affect other connected Layer 2 switches. When the MAC address table of a switch is full, it starts flooding out all ports including those connected to other Layer 2 switches.

What makes tools such as "macof" so dangerous is that an attacker can create a MAC table overflow attack very quickly. For instance, a Catalyst 6500 switch can store only 132,000 MAC addresses in its MAC address table. A tool such as "macof" can flood a switch with up to 8,000 bogus frames per second; creating a MAC address table overflow attack in a matter of a few seconds.

WATCH NOW

Switch attacks: MAC flooding and MAC spoofing

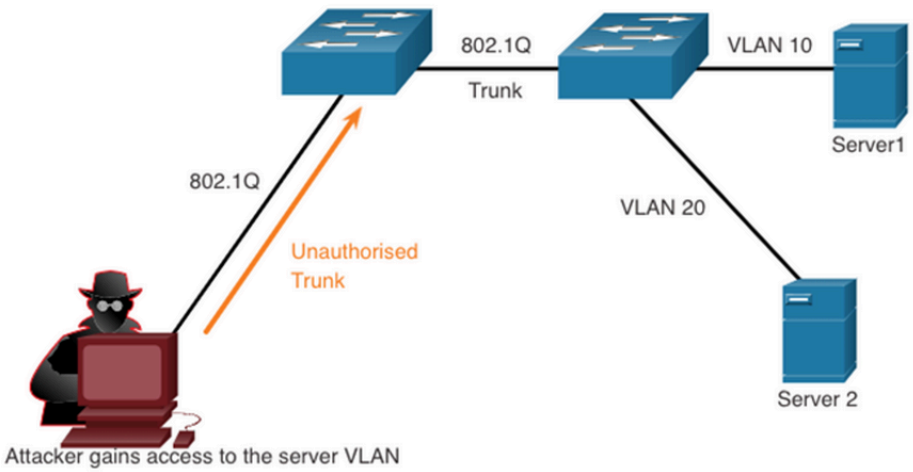
# VLAN HOPPING ATTACK

A VLAN hopping attack enables traffic from one VLAN to be seen by another VLAN without the aid of a router.

In a basic VLAN hopping attack, the attacker configures a host to act like a switch to take advantage of the automatic trunking port feature enabled by default on most switch ports.

The attacker configures the host to spoof 802.1Q signaling and Dynamic Trunking Protocol (DTP) signaling to trunk with the connecting switch. If successful, the switch establishes a trunk link with the host.

Now the attacker can access all the VLANs on the switch. The attackerr can send and receive traffic on any VLAN, effectively hopping between VLANs

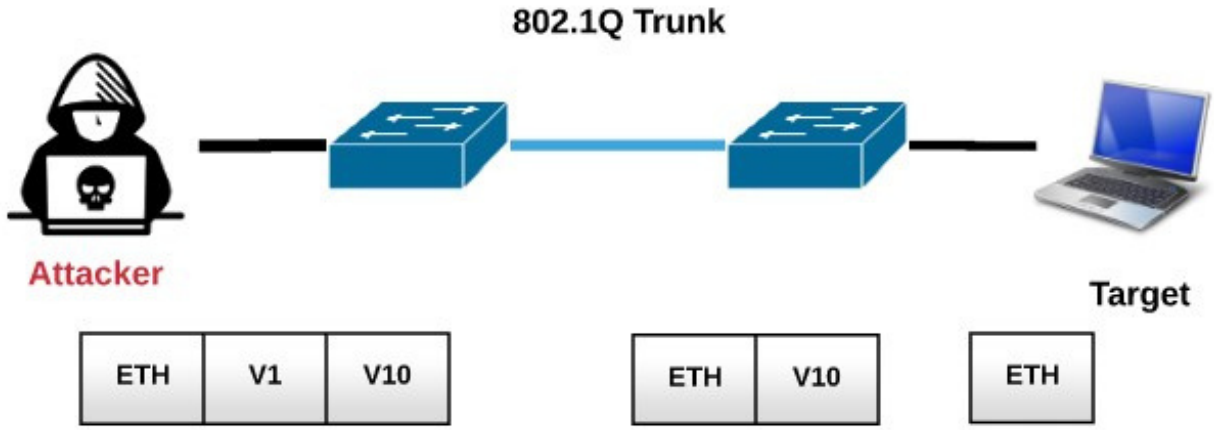



**VLAN Hopping Attack**

WATCH NOW

VLAN hopping explained

# VLAN DOUBLE-TAGGING ATTACK




Attacker could embed a hidden 802.1Q tag inside the frame that already has an 802.1Q tag.

This tag allows the frame to go to a VLAN that the original 802.1Q tag did not specify

STEP 01

The threat actor sends a double-tagged 802.1Q frame to the switch.

STEP 02

The frame arrives on the first switch, which looks at the first 4-byte 802.1Q tag. The switch sees that the frame is destined for the native VLAN. The switch forwards the packet out all native VLAN ports after stripping the VLAN tag. The frame is not retagged because it is part of the native VLAN. At this point, the inner VLAN tag is still intact and has not been inspected by the first switch.

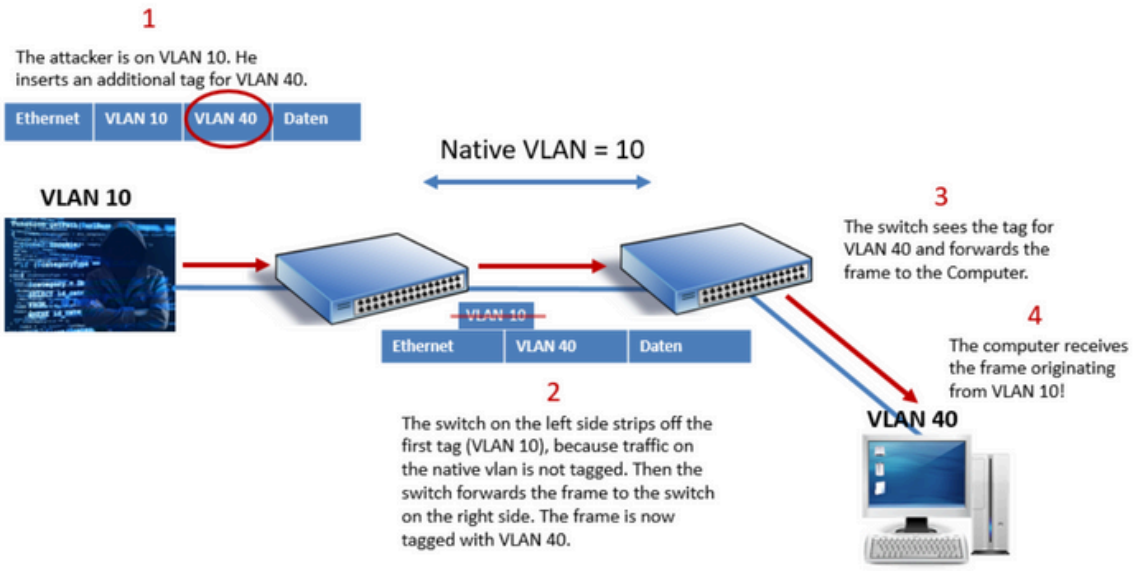
STEP 03

The frame arrives at the second switch which has no knowledge that it was supposed to be for the native VLAN. Native VLAN traffic is not tagged. The second switch looks only at the inner 802.1Q tag that the attacker inserted and sees that the frame is destined to the target VLAN.

The second switch sends the frame on to the target or floods it.

A VLAN double-tagging attack is unidirectional and works only when the attacker is connected to a port residing in the same VLAN as the native VLAN of the trunk port.

This attack allows the attacker to send data to hosts or servers on a VLAN that otherwise would be blocked by some type of access control configuration. Attacker able to communicate with devices on the normally blocked VLAN.




**VLAN Double-Tagging Attack**

WATCH NOW

How to protect Cisco devices against VLAN hopping attack

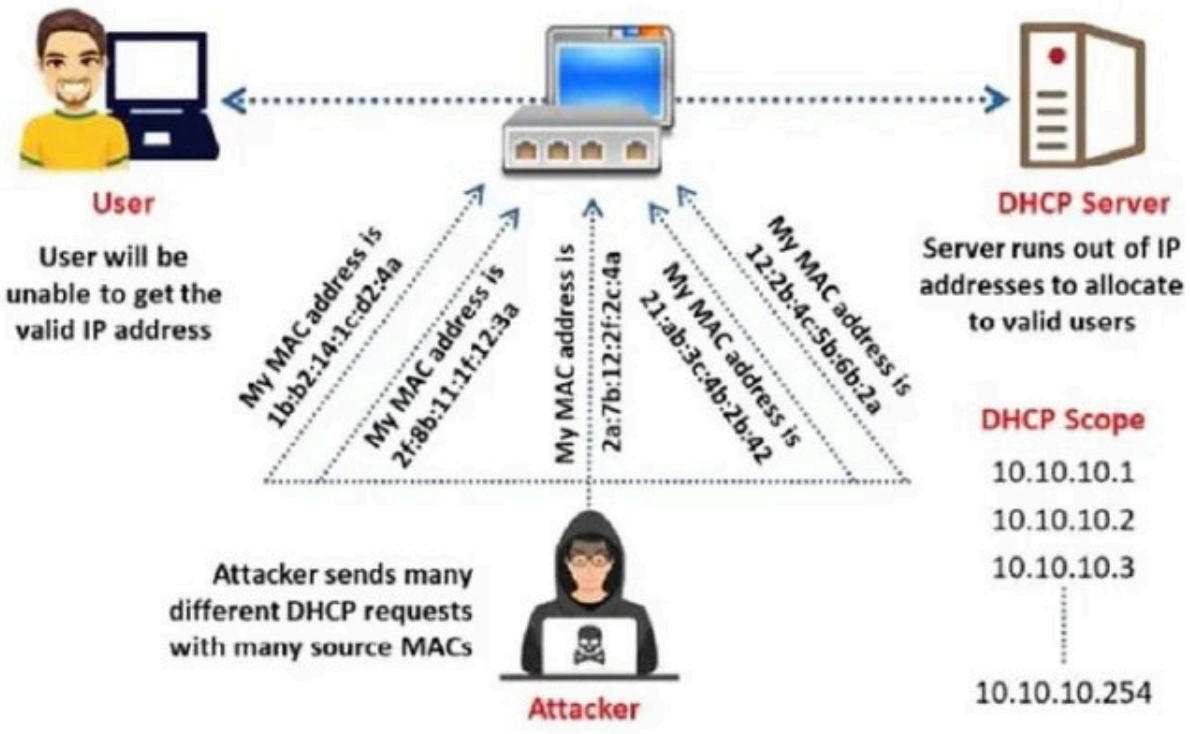
# DHCP ATTACK

## TYPES OF DHCP ATTACKS

- DHCP starvation attack
- DHCP spoofing attack

### DHCP starvation attack

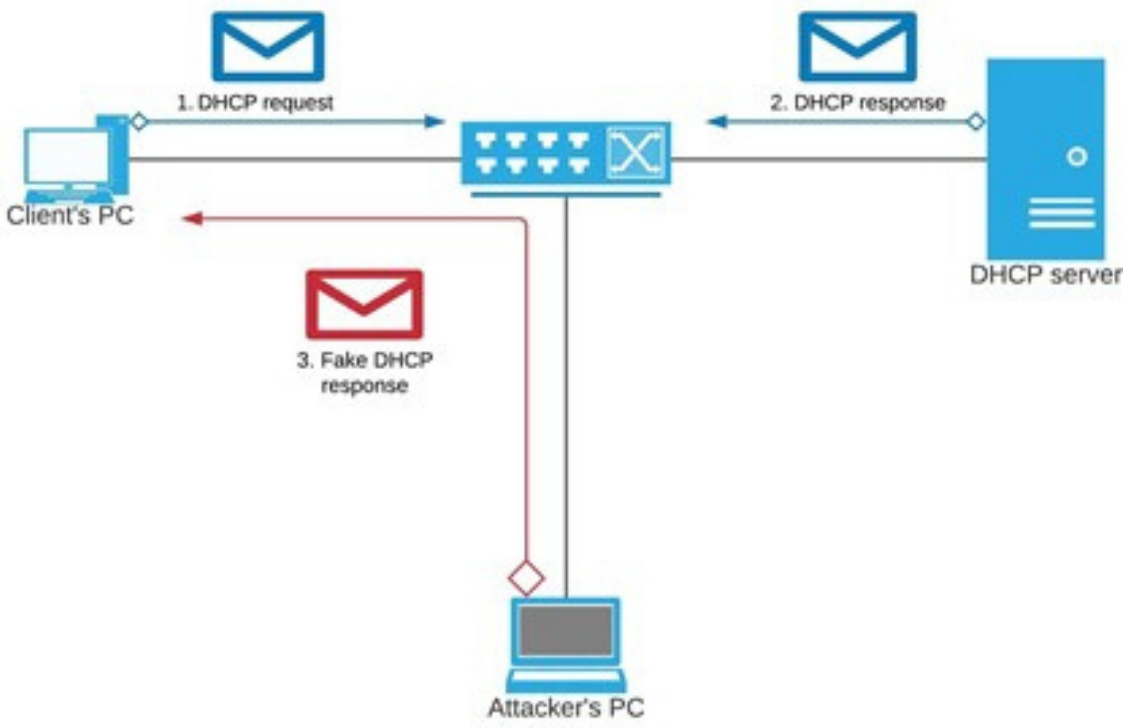
- A DHCP Starvation attack can result in a Denial of Service (DoS) attack. To perform this attack, the attacker sends tons of bogus DHCP Discover messages with spoofed source MAC addresses. The DHCP server tries to respond to all these bogus messages, and as a result, the pool of IP addresses used by the DHCP server is depleted. Hence, a legitimate user won't be able to get an IP address via DHCP.




**DHCP Starvation Attack**

## DHCP spoofing attack

- DHCP spoofing is when a malicious actor sets up an alternate DHCP server on a network to provide false addressing and configuration information to clients. After a client sends a DHCP Discover message, it will typically accept a DHCP Offer from whichever server responds to it the fastest. If the rogue server responds first and the offer is accepted, there are a few incorrect pieces of information that could have negative impacts on clients and the network as a whole.

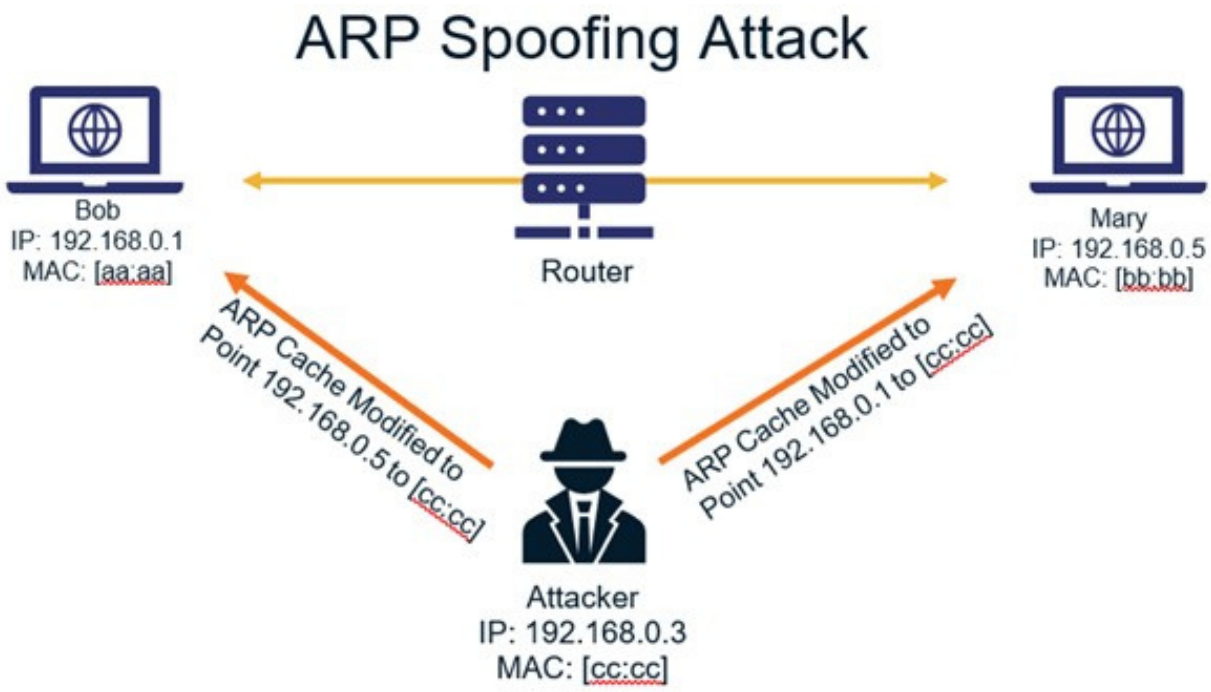



**DHCP Spoofing Attack**

WATCH NOW

What is DHCP attack ?

# ADDRESS RESOLUTION PROTOCOL (ARP) ATTACK



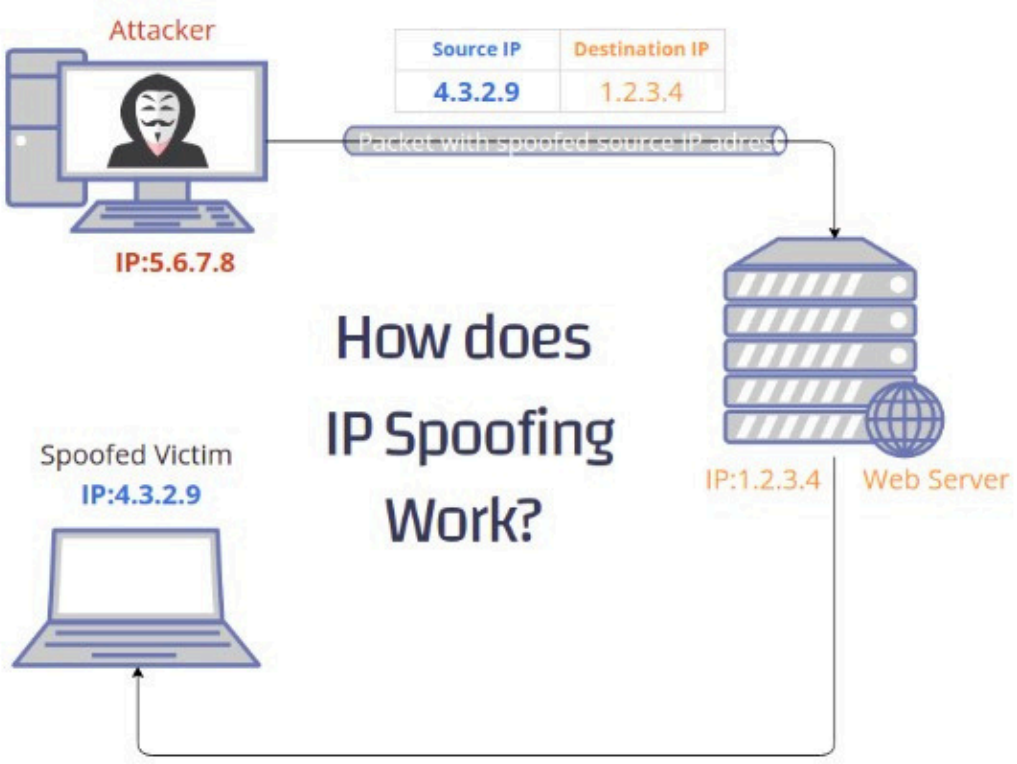

- Hosts broadcast ARP Requests to determine the MAC address of a host with a destination IP address. All hosts on the subnet receive and process the ARP Request. The host with the matching IP address in the ARP Request sends an ARP Reply.

- A client can send an unsolicited ARP Reply called a “gratuitous ARP”. Other hosts on the subnet store the MAC address and IP address contained in the gratuitous ARP in their ARP tables.

- An attacker can send a gratuitous ARP message containing a spoofed MAC address to a switch, and the switch would update its MAC table accordingly.

- There are many tools available on the Internet to create ARP man-in-the-middle attacks.

# ADDRESS SPOOFING ATTACK

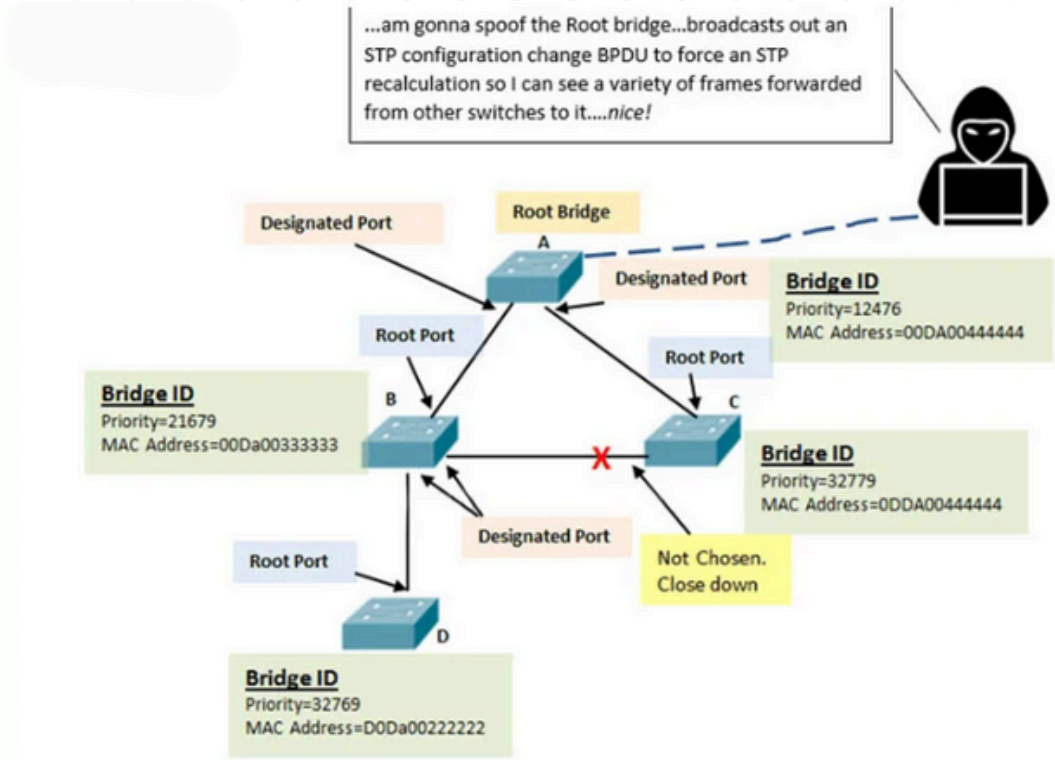



- IP address spoofing is when attacker hijacks a valid IP address of another device on the subnet or uses a random IP address. IP address spoofing is difficult to mitigate, especially when it is used inside a subnet in which the IP belongs.

- MAC address spoofing attacks occur when the attacker alter the MAC address of their host to match another known MAC address of a target host. The switch overwrites the current MAC table entry and assigns the MAC address to the new port. It then inadvertently forwards frames destined for the target host to the attacking host.

- There is no security mechanism at Layer 2 that allows a switch to verify the source of MAC addresses, which is what makes it so vulnerable to spoofing.

# SPANNING TREE PROTOCOL (STP) ATTACK

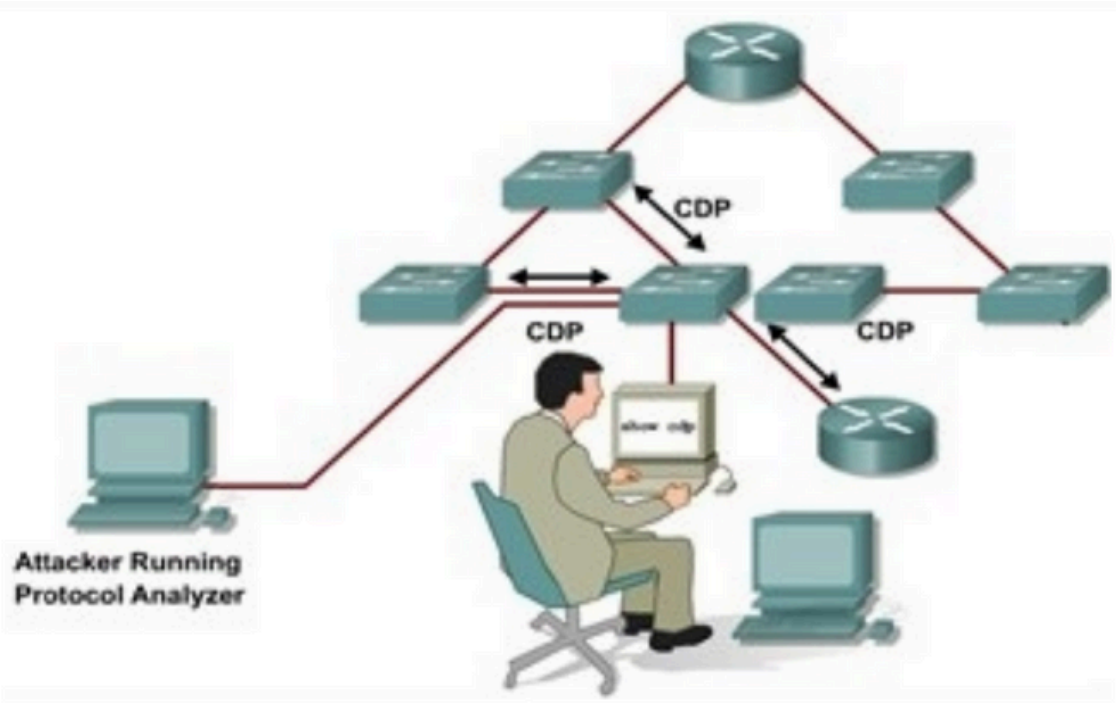



Attackers can manipulate the Spanning Tree Protocol (STP) to conduct an attack by spoofing the root bridge and changing the topology of a network. Attackers can then capture all traffic for the immediate switched domain.

WATCH NOW

STP security (Root Guard and BPDU Guard)

# CDP RECONNAISSANCE ATTACK



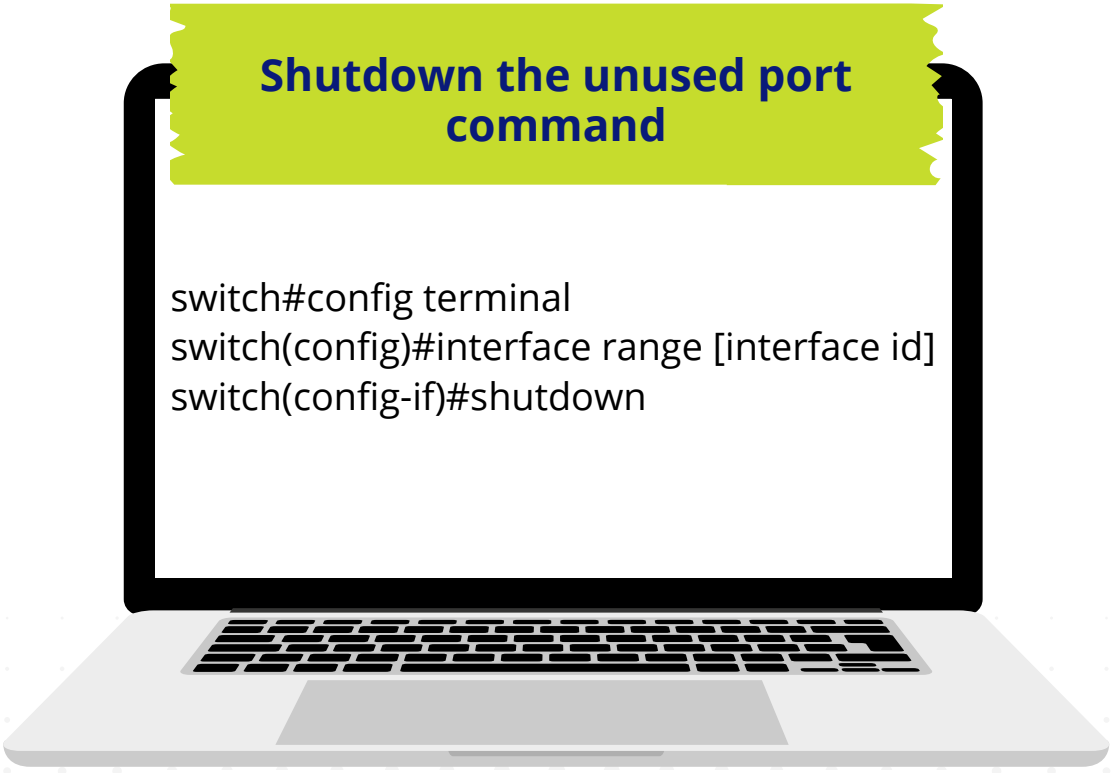

The Cisco Discovery Protocol (CDP) is a proprietary Layer 2 link discovery protocol. It is enabled on all Cisco devices by default. Network administrators also use CDP to help configure and troubleshoot network devices.

CDP information is sent out CDP-enabled ports in periodic, unencrypted, unauthenticated broadcasts. CDP information includes the IP address of the device, IOS software version, platform, capabilities, and the native VLAN.

# ATTACK PREVENTION

# DISABLE UNUSED PORTS ON SWITCH

- Layer 2 attacks are some of the easiest for hackers to deploy but these threats can also be mitigated with some common Layer 2 solutions.
- A simple method that many administrators use to help secure the network from unauthorized access is to disable all unused ports on a switch.
- Navigate to each unused port and issue the Cisco IOS shutdown command. If a port must be reactivated at a later time, it can be enabled with the no shutdown command. To configure a range of ports, use the interface range command.



# MAC ADDRESS TABLE ATTACK PREVENTION

## Port Security

- The simplest and most effective method to prevent MAC address table overflow attacks is to enable port security.

- Port security limits the number of valid MAC addresses allowed on a port. It allows an administrator to manually configure MAC addresses for a port or to permit the switch to dynamically learn a limited number of MAC addresses.

- When a port configured with port security receives a frame, the source MAC address of the frame is compared to the list of secure source MAC addresses that were manually configured or dynamically learned on the port.

- By limiting the number of permitted MAC addresses on a port to one, port security can be used to control unauthorized access to the network.

WATCH NOW

How to prevent MAC spoofing attack

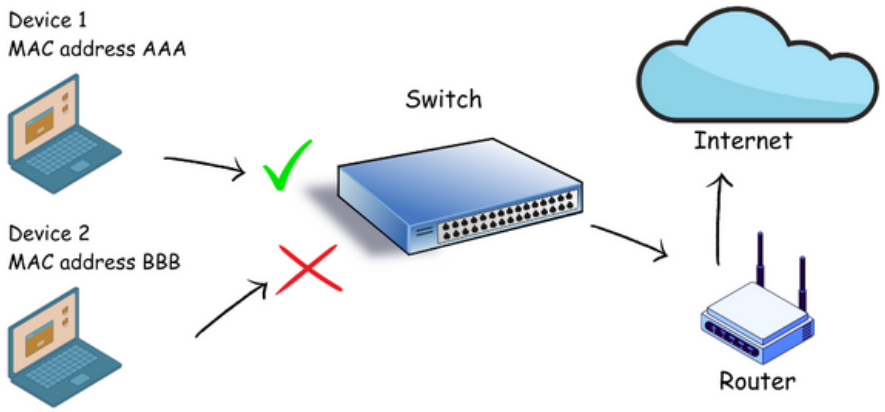
## Port security interface configuration

- The simplest and most effective method to prevent MAC address table overflow attacks is to enable port security.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

- Notice in the example, the switchport port-security command was rejected. This is because port security can only be configured on manually configured access ports or manually configured trunk ports. By default, Layer 2 switch ports are set to dynamic auto (trunking on).

- Therefore, in the example, the port is configured with the switchport mode access interface configuration command.




**Port Security**

- Use the show port-security interface command to display the current port security settings for FastEthernet 0/1.

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

- Notice how port security is enabled, the violation mode is shutdown, and how the maximum number of MAC addresses is 1.

- If a device is connected to the port, the switch will automatically add the device's MAC address as a secure MAC. In this example, no device is connected to the port.

- Note: If an active port is configured with the switchport port-security command and more than one device is connected to that port, the port will transition to the error-disabled state.

- To set the maximum number of MAC addresses allowed on a port, use the following command:

**#switchport port-security [maximum value]**

- The default port security value is 1

- The switch can be configured to learn about MAC addresses on a secure port in one of three ways:

1. Manually configured

- The administrator manually configures a static MAC address(es) by using the following command for each secure MAC address on the port:

**#switchport port-security [MAC address]**

2. Dynamically Learned

- When the switchport port-security command is entered, the current source MAC for the device connected to the port is automatically secured but is not added to the running configuration. If the switch is rebooted, the port will have to re-learn the device's MAC address.

3. Dynamically Learned – Sticky

- The administrator can enable the switch to dynamically learn the MAC address and "stick" them to the running configuration by using the following command:

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

## Port security-aging

- Port security aging can be used to set the aging time for static and dynamic secure addresses on a port and two types of aging are supported per port.

**Absolute** - The secure addresses on the port are deleted after the specified aging time.secure addresses on a port and two types of aging are supported per port.

**Inactivity** **-** The secure addresses on the port are deleted if they are inactive for a specified time.

- Use aging to remove secure MAC addresses on a secure port without manually deleting the existing secure MAC addresses.

- Use the switchport port-security aging command to enable or disable static aging for the secure port, or to set the aging time or type.

**#switchport port-security aging [time]**
**#switchport port-security aging type [aging type]**

## Port security-violation

- If the MAC address of a device attached to a port differs from the list of secure addresses, then a port violation occurs and the port enters the error-disabled state. There are 3 violation mode:

**shutdown** **restrict** **protect**

| Mode | Description |
|---|---|
| shutdown (default) | The port transitions to the error-disabled state immediately, turns off the port LED, and sends a syslog message. It increments the violation counter. When a secure port is in the error-disabled state, an administrator must re-enable it by entering the **shutdown** and **no shutdown** commands. |
| restrict | The port drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value. This mode causes the Security Violation counter to increment and generates a syslog message. |
| protect | This is the least secure of the security violation modes. The port drops packets with unknown MAC source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the maximum value. No syslog message is sent. |

- To set the port security violation mode, use the following command:

**#switchport port-security violation [violation mode]**

**Protect Mode**

**Status After Violation:**

```
S3#show port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0060.3ED7.4636:1
Security Violation Count   : 0
```

Port status is up.

Violation mode Protect (no shutdown even threat actors attempt to compromise) Port only deny traffic from unauthorized MAC address.

Recording of MAC address Threat Actor 3

Port associate with VLAN

No counting attack

## Port err-disabled

- In the example below, the show interface command identifies the port status as err-disabled. The output of the show port-security interface command now shows the port status as secure-shutdown. The Security Violation counter increments by 1.

```
S1# show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : c025.5cd7.ef01:1
Security Violation Count   : 1
S1#
```

- The administrator should determine what caused the security violation If an unauthorized device is connected to a secure port, the security threat is eliminated before re-enabling the port.

- To re-enable the port, first use the shutdown command, then, use the no shutdown command.

**#shutdown**
**#no shutdown**

## Verify port-security

- To display all secure MAC addresses that are manually configured or dynamically learned on all switch interfaces, use the **#show port-security address** command.

```
S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------
Vlan    Mac Address       Type            Ports     Remaining Age
                                                        (mins)
----    -----------       ----            -----     -------------
1       0025.83e6.4b01    SecureDynamic   Fa0/18          -
1       0025.83e6.4b02    SecureSticky    Fa0/19          -
-----------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

- Use the **#show port-security interface** command to view details for a specific interface.

- To display port security settings for the switch, use the **#show port-security** command.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------------
      Fa0/1              1            0                  0         Shutdown
      Fa0/2              1            0                  0         Shutdown
      Fa0/3              1            0                  0         Shutdown
(output omitted)
     Fa0/24              1            0                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

# VLAN ATTACK PREVENTION

Use the following steps to mitigate VLAN hopping attacks:

1. Disable DTP (auto trunking) negotiations on non-trunking ports by using the switchport modeaccess interface configuration command.
2. Disable unused ports and put them in an unused VLAN.
3. Manually enable the trunk link on a trunking port by using the switchport mode trunk command.
4. Disable DTP (auto trunking) negotiations on trunking ports by using the switchport nonegotiate command.
5. Set the native VLAN to a VLAN other than VLAN 1 by using the switchport trunk native vlan vlan_number command.

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

# DHCP ATTACK PREVENTION

**DHCP starvation attacks** can be effectively mitigated by using port security because Gobbler uses a unique source MAC address for each DHCP request sent.

However, mitigating DHCP spoofing attacks requires more protection.

**DHCP spoofing attacks** can be mitigated by using DHCP snooping on trusted ports.

DHCP snooping filters DHCP messages on untrusted ports.

- Devices under administrative control (e.g., switches, routers, and servers) are trusted sources.
- Trusted interfaces (e.g., trunk links, server ports) must be explicitly configured as trusted.
- Devices outside the network and all access ports are generally treated as untrusted sources.

A DHCP table is built that includes the source MAC address of a device on an untrusted port and the IP address assigned by the DHCP server to that device.

- The MAC address and IP address are bound together.
- Therefore, this table is called the DHCP snooping binding table.

# ADDRESS RESOLUTION PROTOCOL (ARP) ATTACK PREVENTION

Dynamic ARP Inspection (DAI) requires DHCP snooping and helps prevent ARP attacks by:

- Not relaying invalid or gratuitous ARP Replies out to other ports in the same VLAN.
- Intercepting all ARP Requests and Replies on untrusted ports.
- Verifying each intercepted packet for a valid IP-to-MAC binding.
- Dropping and logging ARP Replies coming from invalid to prevent ARP poisoning.
- Error-disabling the interface if the configured DAI number of ARP packets is exceeded.

WATCH NOW

ARP Poisoning: Understanding the threat and how to prevent

# SPANNING TREE PROTOCOL (STP) ATTACK PREVENTION

To mitigate STP attacks, use **PortFast** and **Bridge Protocol Data Unit (BPDU) Guard.**

## PortFast

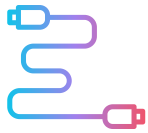
- PortFast immediately brings a port to the forwarding state from a blocking state, bypassing the listening and learning states.
- Apply to all end-user access ports.
- PortFast bypasses the STP listening and learning states to minimize the time that access ports must wait for STP to converge.
- PortFast can be enabled :
  - On an interface – Use the **#spanning-tree portfast interface configuration** command.
  - Globally – Use the **#spanning-tree portfast default global configuration** command to enable PortFast on all access ports.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
```

## BPDU Guard

- Like PortFast, BPDU guard should only be configured on interfaces attached to end devices.
- An access port could receive an unexpected BPDUs accidentally or because a user connected an unauthorized switch to the access port.
- If a BPDU is received on a BPDU Guard enabled access port, the port is put into error-disabled state. This means that the port is shut down and must be manually re-enabled.
- BPDU Guard can be enabled:

  - On an interface – Use the **#spanning-tree bpduguard enable interface configuration** command.



  - Globally – Use the **#spanning-tree portfast bpduguard default global configuration** command to enable BPDU Guard on all access ports.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```

# SWITCH SECURITY ACTIVITIES

Switch security configuration activity 1

Port security activity

Security questions activity

Switch security configuration activity 2

# REAL WORLD ATTACKS AND PREVENTIONS

10 Real world cyber attacks

Every cyber attack type explained in 5 minutes

ARP poisoning and port mirroring attacks

ARP attacks, STP attacks, and CDP reconnaissance

Detecting and preventing the most powerful DDoS attack methods

DoS attack protection

# REFERENCES


Cisco Networking Academy (2020) Switching, Routing and Wireless Essential v7.0 (SRWE) Companion Guide. Indianapolis, US: Cisco Press.

Cisco Networking Academy (2020). Introduction to Networks Companion Guide (CCNAv7). Indianapolis, US: Cisco Press.

Cisco Networking Academy (2020). CCNA 2 v7 Course Booklet. Indianapolis, US: Cisco Press.

Cisco Networking Academy (2020). CCNA 2 v7 Labs & Study Guide. Indianapolis, US: Cisco Press.

Cisco Networking Academy (2020). Introduction To Network Course Booklet (CCNAv7). Indianapolis, US: Cisco Press.

Cisco Networking Academy (2020). CCNA 1 v7 Labs & Study Guide. Indianapolis, US: Cisco Press.

Dean, T. (2021). Network+ Guide to Networks (8th ed.). Cengage Learning.

**SWITCHING ESSENTIALS**

e ISBN 978-629-7514-58-1