



# Module 10: LAN Security Concepts

Switching, Routing and Wireless  
Essentials v7.0 (SRWE)



# Module Objectives

**Module Title:** LAN Security Concepts

**Module Objective:** Explain how vulnerabilities compromise LAN security

Topic Title	Topic Objective
Endpoint Security	Explain how to use endpoint security to mitigate attacks
Access Control	Explain how AAA and 802.1x are used to authenticate LAN endpoints and devices
Layer 2 Security Threats	Identify Layer 2 vulnerabilities
MAC Address Table Attack	Explain how a MAC address table attack compromised LAN security
LAN Attacks	Explain how LAN attacks compromise LAN security

# 10.1 Endpoint Security

## Endpoint Security

# Network Attacks Today

The news media commonly covers attacks on enterprise networks. Simply search the internet for “latest network attacks” to find up-to-date information on current attacks. Most likely, these attacks will involve one or more of the following:

- **Distributed Denial of Service (DDoS)** – 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** – This is an attack in which an organization’s data servers or hosts are compromised to **steal confidential information**.
- **Malware** – 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.

## Endpoint Security

# Network Security Devices

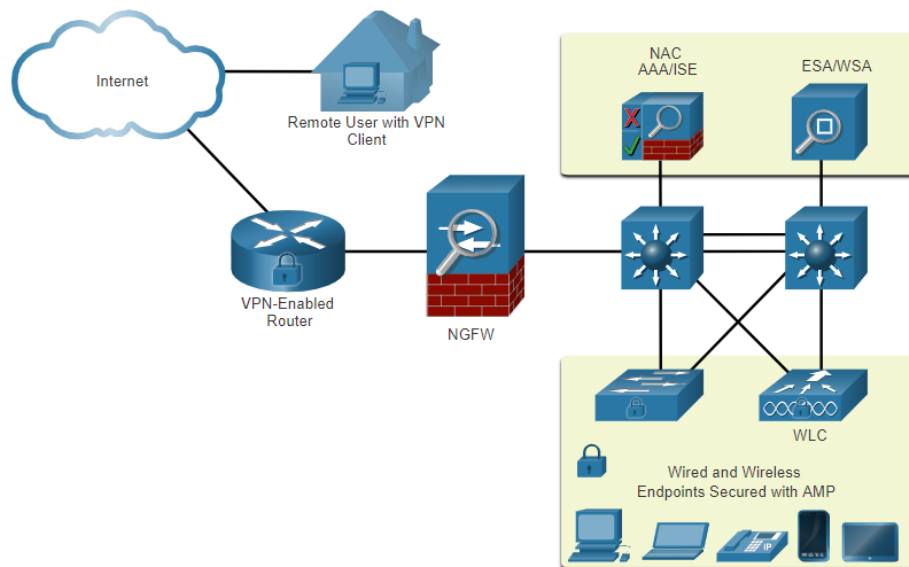
**Various network security devices are required to protect the network perimeter from outside access. These devices could include the following:**

- **Virtual Private Network (VPN)** enabled router - provides a secure connection to remote users across a **public network** and into the enterprise network. VPN services can be integrated into the **firewall**.
- **Next-Generation Firewall (NGFW)** - provides **stateful** packet inspection, application visibility and control, a next-generation intrusion prevention system (**NGIPS**), advanced malware protection (**AMP**), and **URL** filtering.
- **Network Access Control (NAC)** - includes authentication, authorization, and accounting (**AAA**) services. In larger enterprises, these services might be incorporated into an appliance that can manage access policies across a wide variety of users and device types. The Cisco Identity Services Engine (**ISE**) is an example of a NAC device.

# Endpoint Security

## Endpoint Protection

- Endpoints are hosts which commonly consist of laptops, desktops, servers, and IP phones, as well as employee-owned devices. Endpoints are particularly susceptible to malware-related attacks that originate through email or web browsing.
- Endpoints have typically used traditional host-based security features, such as **antivirus/antimalware, host-based firewalls, and host-based intrusion prevention systems (HIPSs)**.
- Endpoints today are best protected by a combination of **NAC, AMP software, an email security appliance (ESA), and a web security appliance (WSA)**.



## Endpoint Security

# Cisco Email Security Appliance (ESA)

The Cisco **ESA** device is designed to monitor Simple Mail Transfer Protocol (SMTP). The Cisco ESA is constantly updated by real-time feeds from **the Cisco Talos**, which detects and correlates threats and solutions by using a worldwide database monitoring system. This threat intelligence data is pulled by the Cisco ESA every three to five minutes.

These are some of the functions of the Cisco ESA:

- Block known **threats**
- Remediate against **stealth malware** that evaded initial detection
- Discard emails with **bad links**
- Block access to **newly infected sites**.
- Encrypt **content** in outgoing email to prevent data loss.

# Cisco Web Security Appliance (WSA)

- The Cisco Web Security Appliance (WSA) is a mitigation technology for web-based threats. It helps organizations address the challenges of securing and controlling web traffic.
- The Cisco WSA combines advanced malware protection, application visibility and control, acceptable use policy controls, and reporting.
- Cisco WSA provides complete control over how users access the internet. Certain features and applications, such as chat, messaging, video and audio, can be allowed, restricted with time and bandwidth limits, or blocked, according to the organization's requirements.
- The WSA can perform blacklisting of URLs, URL-filtering, malware scanning, URL categorization, Web application filtering, and encryption and decryption of web traffic.



# 10.2 Access Control

# Authentication with a Local Password

Many types of authentication can be performed on networking devices, and each method offers varying levels of security.

The simplest method of **remote access authentication** is to configure a login and password combination on console, vty lines, and aux ports.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

**SSH** is a more secure form of remote access:

- It requires a **username and a password**.
- The username and password can be **authenticated locally**.

The local database method has some limitations:

- User accounts must be configured locally **on each device** which is not scalable.
- The method provides no fallback authentication method.

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

# Access Control

## AAA Components

AAA stands for Authentication, Authorization, and Accounting, and provides the primary framework to set up access control on a network device.

AAA is a way to control who is permitted to access a network (**authenticate**), what they can do while they are there (**authorize**), and to audit what actions they performed while accessing the network (**accounting**).

# Access Control

## Authentication

Local and server-based are two common methods of implementing AAA authentication.

### Local AAA Authentication (look in Netacad.com):

- Method stores **usernames and passwords** locally in a network device (e.g., Cisco router).
- Users authenticate against **the local database**.
- Local AAA is ideal for **small networks**.

### Server-Based AAA Authentication (look in Netacad.com):

- With the server-based method, the router accesses a **central AAA server (NAC)**.
- The **AAA server** contains the usernames and password for all users.
- The router uses either the Remote Authentication Dial-In User Service (**RADIUS**) or Terminal Access Controller Access Control System (**TACACS+**) protocols to communicate with the AAA server.
- When there are **multiple routers and switches**, server-based AAA is more appropriate.

# Authorization(look in Netacad.com)

- AAA authorization is automatic and does not require users to perform additional steps after authentication.
- Authorization governs what **users can and cannot** do on the network after they are authenticated.
- Authorization uses a set of attributes that describes the user's access to the network. These attributes are used by the AAA server to determine privileges and restrictions for that user.

## Accounting(look in Netacad.com)

AAA accounting collects and reports usage data. This data can be used for such purposes **as auditing or billing**. The collected data might include the **start and stop connection times, executed commands, number of packets, and number of bytes**.

A primary use of accounting is to combine it with AAA authentication.

- The AAA server keeps a detailed log of exactly what the authenticated user does on the device, as shown in the figure. This includes all EXEC and configuration commands issued by the user.
- The log contains numerous data fields, including the username, the date and time, and the **actual command that was entered by the user**. This information is useful when **troubleshooting devices**. It also provides **evidence** for when individuals perform malicious acts.

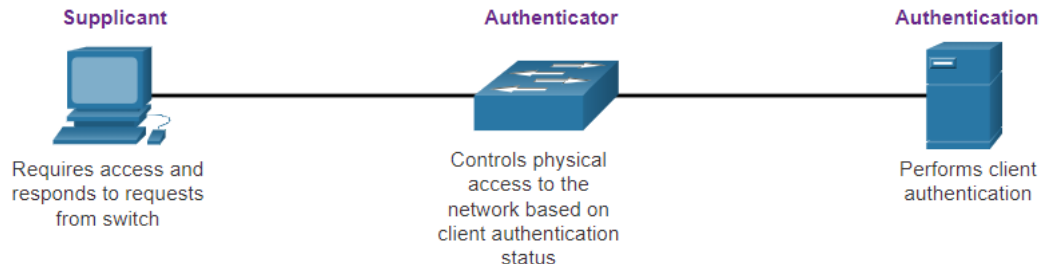
# Access Control

## 802.1X

The IEEE **802.1X** standard is a port-based access control and authentication protocol. This protocol restricts unauthorized workstations from connecting to a LAN through publicly accessible switch ports. The authentication server authenticates each workstation that is connected to a switch port before making available any services offered by the switch or the LAN.

With 802.1X port-based authentication, the devices in the network have specific roles:

- **Client (Supplicant)** - This is a device running 802.1X-compliant client software, which is available for wired or wireless devices.
- **Switch (Authenticator)** –The switch acts as an intermediary between the client and the authentication server. It requests identifying information from the client, verifies that information with the authentication server, and **relays a response** to the client. Another device that could act as authenticator is a **wireless access point**.
- **Authentication server** –The server validates the identity of the client and notifies the switch or wireless access point that the client is or is not authorized to access the LAN and switch services.



# 10.3 Layer 2 Security Threats

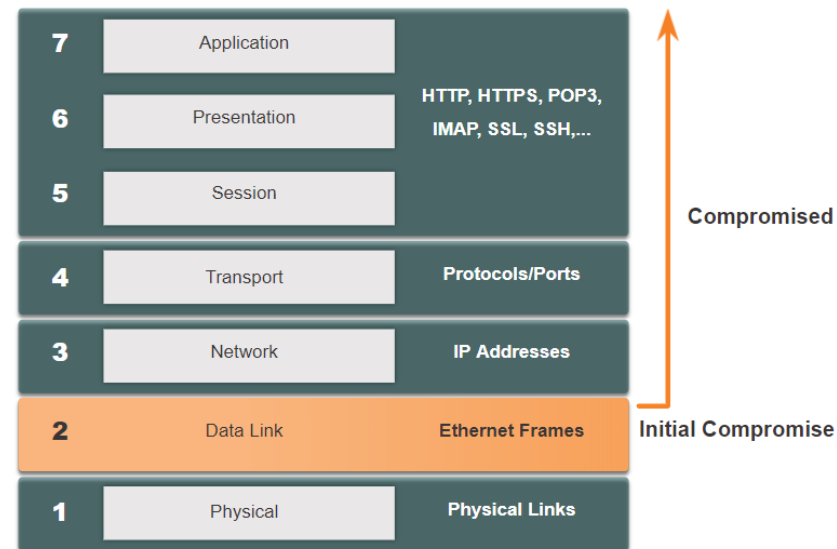


# Layer 2 Security Threats

## Layer 2 Vulnerabilities

Recall that the OSI reference model is divided into **seven layers** which work independently of each other. The figure shows the function of each layer and the core elements that can be exploited.

Network administrators routinely implement security solutions to protect the elements in **Layer 3 up through Layer 7**. They use **VPNs, firewalls, and IPS devices** to protect these elements. However, if **Layer 2 is compromised**, then all the layers above it are also affected. For example, if a threat actor with access to the internal network captured Layer 2 frames, then all the security implemented on the layers above would be useless. The threat actor could cause a lot of damage on the Layer 2 LAN networking infrastructure.



## Layer 2 Security Threats

# Switch Attack Categories

Security is only as strong as the weakest link in the system, and Layer 2 is considered to be that weak link. This is because LANs were traditionally under the administrative control of a single organization. We inherently trusted all persons and devices connected to our LAN. Today, with BYOD and more sophisticated attacks, our LANs have become more vulnerable to penetration.

Category	Examples
<b>MAC Table Attacks</b>	Includes MAC address flooding attacks.
<b>VLAN Attacks</b>	Includes VLAN hopping and VLAN double-tagging attacks. It also includes attacks between devices on a common VLAN.
<b>DHCP Attacks</b>	Includes DHCP starvation and DHCP spoofing attacks.
<b>ARP Attacks</b>	Includes ARP spoofing and ARP poisoning attacks.
<b>Address Spoofing Attacks</b>	Includes MAC address and IP address spoofing attacks.
<b>STP Attacks</b>	Includes Spanning Tree Protocol manipulation attacks.

## Layer 2 Security Threats

# Switch Attack Mitigation Techniques

Solution	Description
Port Security	Prevents many types of attacks including MAC address flooding attacks and DHCP starvation attacks.
DHCP Snooping	Prevents DHCP starvation and DHCP spoofing attacks.
Dynamic ARP Inspection (DAI)	Prevents ARP spoofing and ARP poisoning attacks.
IP Source Guard (IPSG)	Prevents MAC and IP address spoofing attacks.

These Layer 2 solutions will not be effective if the management protocols are not secured. The following strategies are recommended:

- Always use secure variants of management protocols such as **SSH**, **Secure Copy Protocol (SCP)**, **Secure FTP (SFTP)** → **FTP plus SSH to encrypt. data and works on port 22 only** → **IOSXE**, and **Secure Socket Layer/Transport Layer Security (SSL/TLS)**.
- Consider using **out-of-band** management network to manage devices.
- Use a **dedicated management VLAN** where nothing but management traffic resides.
- Use **ACLs** to filter unwanted access.

# 10.4 MAC Address Table Attack

# MAC Address Table Attack

## Switch Operation Review

Recall that to make forwarding decisions, a Layer 2 LAN switch builds a **table** based on the **source MAC addresses** in received frames. This is called a MAC address table. MAC address tables are stored in memory and are used to more efficiently switch frames.

```
S1# show mac address-table dynamic
      Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       0001.9717.22e0    DYNAMIC     Fa0/4
1       000a.f38e.74b3    DYNAMIC     Fa0/1
1       0090.0c23.ceca    DYNAMIC     Fa0/3
1       00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

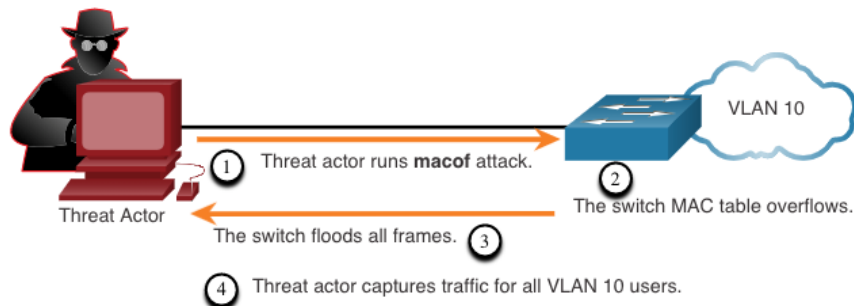
# MAC Address Table Attack

## MAC Address Table Flooding

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 threat actor to capture all of the frames sent from one host to another on the local LAN or local VLAN.

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



## MAC Address Table Attack

# MAC Address Table Attack Mitigation

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 **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.

Another reason why these attack tools are dangerous is 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.

To mitigate MAC address table overflow attacks, network administrators must implement port security. **Port security** will only allow a specified number of source MAC addresses to be learned on the port. Port security is further discussed in another module.

# 10.5 LAN Attacks

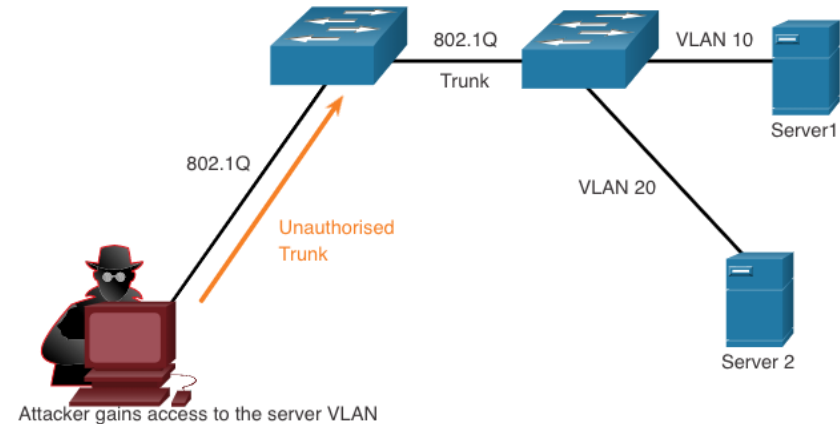


# LAN Attacks

## VLAN Hopping Attacks

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 threat actor 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 threat actor configures the host to **spoof 802.1Q signaling** and Cisco-proprietary Dynamic Trunking Protocol (**DTP**) signaling to trunk with the connecting switch. If successful, the switch establishes **a trunk link** with the host, as shown in the figure. Now the threat actor can **access all the VLANs** on the switch. The threat actor can send and receive traffic on any VLAN, effectively hopping between VLANs.



# VLAN Double-Tagging Attacks (look in Netacad.com)

A threat actor in specific situations 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 1:** The threat actor sends a double-tagged 802.1Q frame to the switch. The outer header has the VLAN tag of the threat actor, which is **the same as the native VLAN** of the trunk port.
- **Step 2:** 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 3:** 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 by the sending switch as specified in the 802.1Q specification. The second switch looks only at **the inner 802.1Q** tag that the threat actor inserted and sees that the frame is destined the target VLAN. The second switch sends the frame on to the target or floods it, depending on whether there is an existing MAC address table entry for the target.

## VLAN Double-Tagging Attacks (Cont.)

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. The idea is that double tagging 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. Presumably the return traffic will also be permitted, thus giving the attacker the ability to communicate with devices on the normally blocked VLAN.

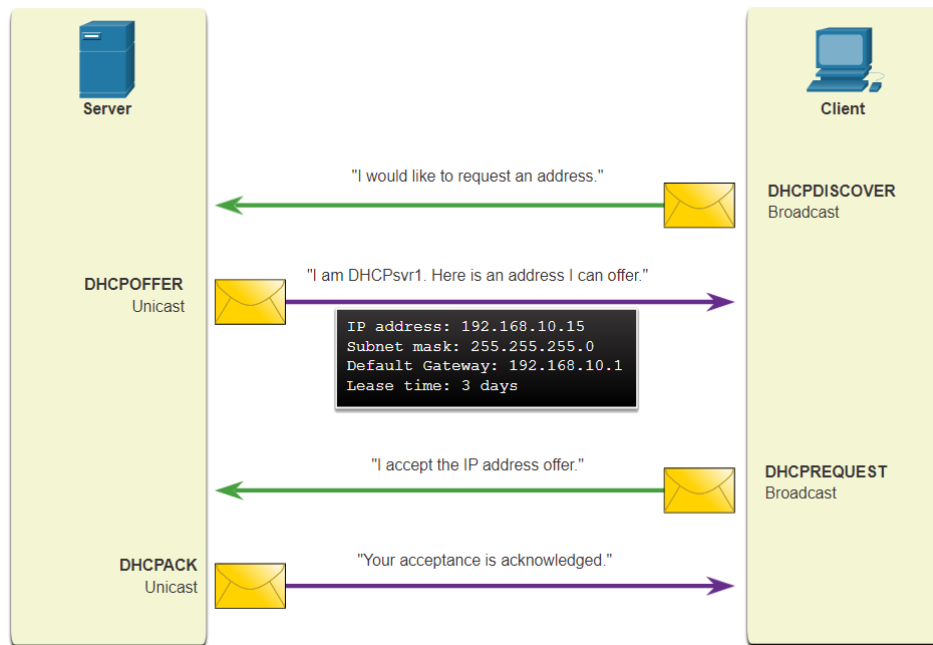
**VLAN Attack Mitigation** - VLAN hopping and VLAN double-tagging attacks can be prevented by implementing the following trunk security guidelines, as discussed in a previous module:

- Disable trunking on **all access ports**.
- Disable **auto trunking** on trunk links so that trunks must be manually enabled.
- Be sure that the **native VLAN** is only used for trunk links.

# LAN Attacks

## DHCP Messages

DHCP servers dynamically provide IP configuration information including **IP address, subnet mask, default gateway, DNS servers, and more to clients**. A review of the sequence of the DHCP message exchange between client and server is show in the figure.



# DHCP Attacks (look in Netacad.com)

Two types of DHCP attacks are **DHCP starvation** and **DHCP spoofing**. Both attacks are mitigated by implementing DHCP snooping.

- **DHCP Starvation Attack** – The goal of this attack is to create a **DoS for connecting clients**. DHCP starvation attacks require an attack tool such as **Gobbler**. Gobbler has the ability to look at the entire scope of leasable IP addresses and tries to lease them all. Specifically, it creates DHCP discovery messages with bogus MAC addresses.
- **DHCP Spoofing Attack** – This occurs when a **rogue DHCP server** is connected to the network and provides **false IP configuration** parameters to legitimate clients. A rogue server can provide a variety of misleading information, including the following:
  - **Wrong default gateway** - The rogue server provides an **invalid gateway** or the IP address of its host to create a man-in-the-middle attack. This may go entirely undetected as the intruder intercepts the data flow through the network.
  - **Wrong DNS server** - The rogue server provides an incorrect DNS server address pointing the user to a **nefarious website**.
  - **Wrong IP address** - The rogue server provides an invalid IP address effectively creating a DoS attack on the DHCP client.

# Video – ARP Attacks, STP Attacks, and CDP Reconnaissance

This video will cover the following:

- ARP Spoofing Attack
- ARP Poisoning Attack
- STP Attack
- CDP Reconnaissance

# LAN Attacks

## ARP Attacks

- 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. In a typical attack, a threat actor sends unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway, effectively setting up a man-in-the-middle attack.
- There are many tools available on the internet to create ARP man-in-the-middle attacks.
- IPv6 uses ICMPv6 **Neighbor Discovery Protocol** for Layer 2 address resolution. IPv6 includes strategies to mitigate Neighbor Advertisement spoofing, similar to the way IPv6 prevents a spoofed ARP Reply.
- ARP spoofing and ARP poisoning are mitigated by implementing **Dynamic ARP Inspection (DAI)**.

# Address Spoofing Attacks (look in Netacad.com)

- IP address spoofing is when a threat actor **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 threat actors **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.
- When the target host sends traffic, the switch will correct the error, realigning the MAC address to the original port. To stop the switch from returning the port assignment to its correct state, the threat actor can create a program or script that will constantly send frames to the switch so that the switch maintains the incorrect or spoofed information.
- 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.
- IP and MAC address spoofing can be mitigated by implementing **IP Source Guard (IPSG)**.



## STP Attack (look in Netacad.com)

- Network 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.
- To conduct an STP manipulation attack, the attacking host **broadcasts STP bridge protocol data units (BPDUs)** containing configuration and topology changes that will force spanning-tree recalculations. The BPDUs sent by the attacking host announce a **lower bridge priority** in an attempt to be elected as the root bridge.
- This STP attack is mitigated by implementing **BPDU Guard** on all access ports. BPDU Guard is discussed in more detail later in the course.

## LAN Attacks

# CDP Reconnaissance

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. The device receiving the CDP message updates its CDP database.

To mitigate the exploitation of CDP, limit the use of CDP on devices or ports. For example, **disable CDP on edge ports that connect to untrusted devices.**

- To disable CDP globally on a device, use the **no cdp run** global configuration mode command. To enable CDP globally, use the **cdp run** global configuration command.
- To disable CDP on a port, use the **no cdp enable** interface configuration command. To enable CDP on a port, use the **cdp enable** interface configuration command.

**Note:** **Link Layer Discovery Protocol (LLDP)** is also vulnerable to reconnaissance attacks. Configure **no lldp run** to disable LLDP globally. To disable LLDP on the interface, configure **no lldp transmit** and **no lldp receive**.

# 10.6 Module Practice and Quiz