Implementing Secure Network Design

MNU-2025

Dr. Ahmed Samy

Lecture 02

Module Contents

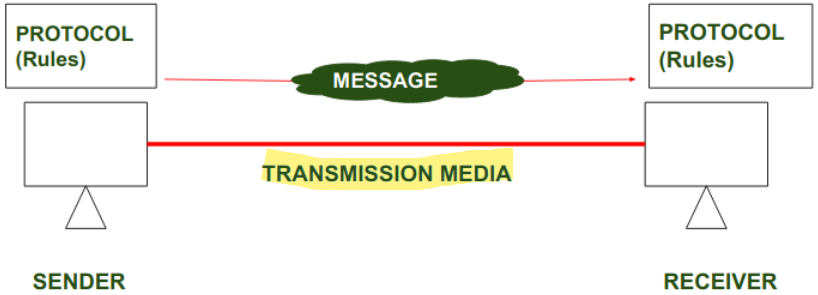
In this module, we will cover the below topics:

- TCP/IP and OSI Protocol Suites
- Network Devices
- Layer2 Attacks and Mitigation
- Layer3 Attacks and Mitigation
- Layer4 Attacks and Mitigation
- Virtual Private Network (VPN)

TCP/IP and OSI Protocol Suites

Communication Fundamentals

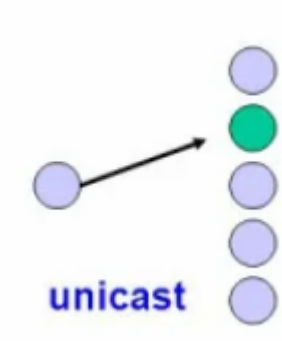
- Networks can vary in size and complexity.
- It is not enough to have a connection, devices must agree on “how” to communicate.
- There are three elements to any communication:
  - There will be a source (sender).
  - There will be a destination (receiver).
  - There will be a channel (media) that provides for the path of communications to occur.

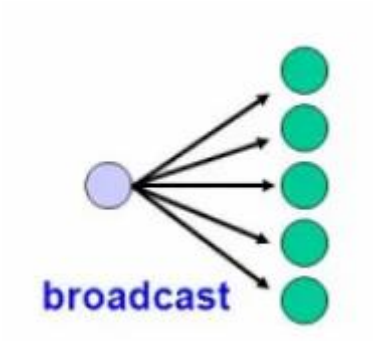


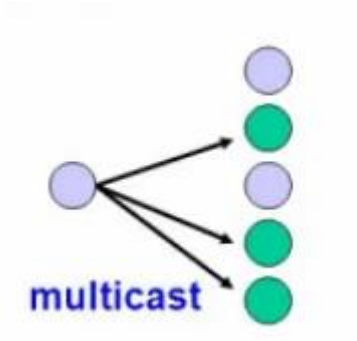
- All communications are governed by protocols.
- Protocols are the rules that communications will follow.

Message Delivery Options

- Message delivery may one of the following methods:
- Unicast – one to one communication
- Broadcast – one to all
- Multicast – one to many, typically not all

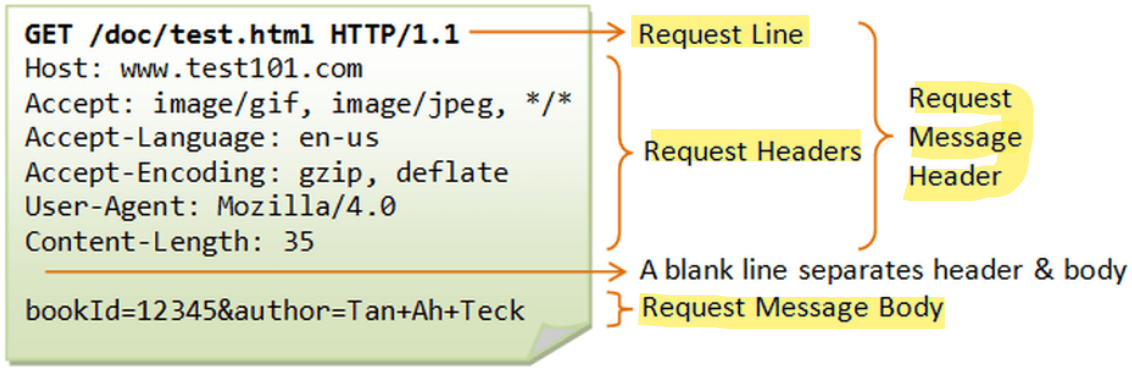






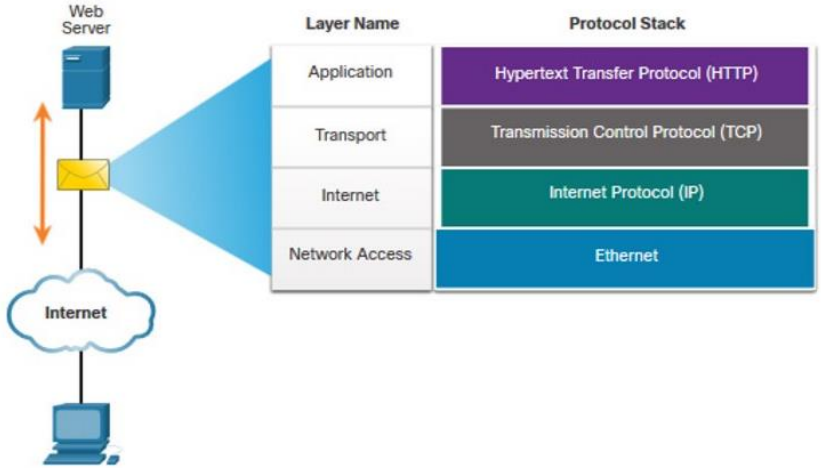
Network Protocol Overview

- Network protocols define a common format and set of rules for exchanging messages between devices.
- Can be implemented on devices in:
  - Software
  - Hardware
  - Both
- Protocols have their own:
  - Function
  - Format
  - Rules



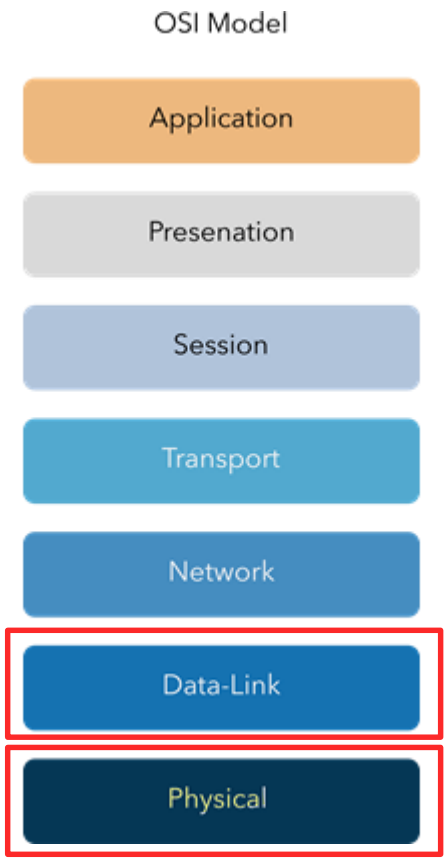
Network Protocol Suites

- Protocols must be able to work with other protocols.
- Protocol suite: is a group of inter-related protocols necessary to perform a communication function
- There are several protocol suites.
- Internet Protocol Suite or TCP/IP- The most common protocol suite and maintained by the Internet Engineering Task Force (IETF)
- Open Systems Interconnection (OSI) protocols- Developed by the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU)



OSI Reference Model

- The OSI (Open Systems Interconnection) Reference Model is a conceptual framework used to understand and standardize how different networking protocols and technologies interact.
- The OSI model divides the communication process into **seven layers**, each with specific functions and responsibilities.
- **Physical Layer:** Deals with the physical connection between devices and the transmission of raw bit streams over a physical medium, handles signaling, voltage levels, and data rates.
- **Data Link Layer:** Ensures reliable data transfer across a physical link and handles error detection/correction at the frame level.
- **Protocols**: Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), PPP (Point-to-Point Protocol).



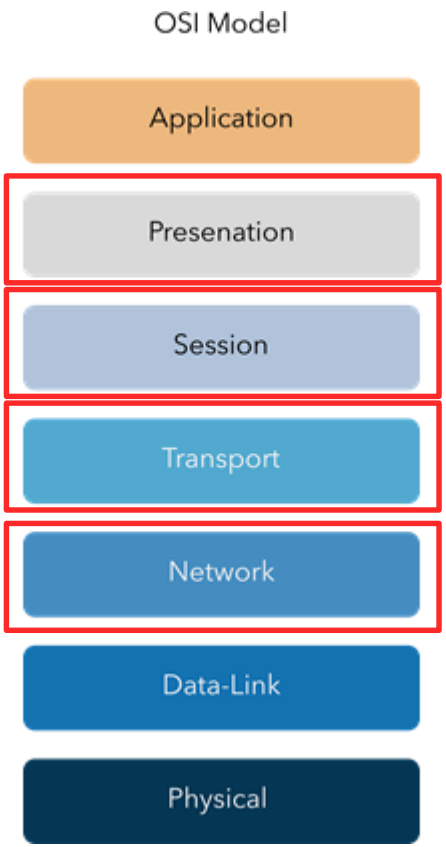
OSI Reference Model

- **Network Layer:** Handles logical addressing and routing of data packets between devices across different networks.
- **Protocols:** IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol)

- **Transport Layer:** Ensures reliable, end-to-end communication between devices, including error recovery and flow control.
- **Protocols:** TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and SCTP (Stream Control Transmission Protocol).

- **Session Layer:** Manages sessions (connections) between applications on different devices.
- **Protocols:** NetBIOS, RPC (Remote Procedure Call), and PPTP (Point-to-Point Tunneling Protocol).

- **Presentation Layer:** Translates data into a format that the application layer can understand, ensuring compatibility between systems.
- **Examples**: Translates data into a format that the application layer can understand, ensuring compatibility between systems.

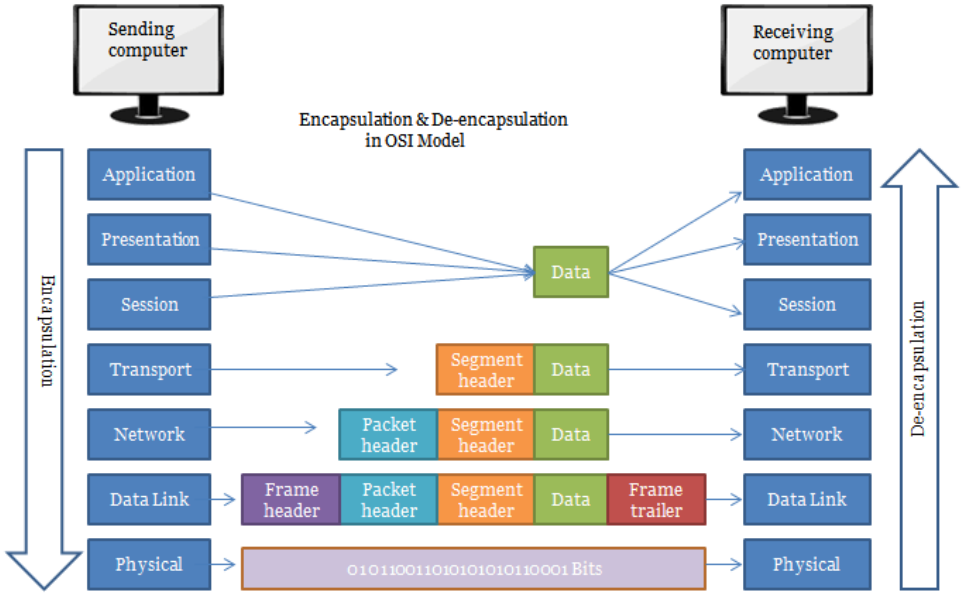


OSI Reference Model

- **Application Layer:** Provides network services directly to end-user applications.
- **Protocols:** HTTP/HTTPS (web browsing), FTP (file transfer), SMTP (email), DNS (domain name resolution), DHCP (Assign Dynamic IP), and Telnet.

- **Data Encapsulation**: As data moves down the layers, each layer adds its own header (and sometimes a trailer) to the data.

- **Decapsulation**: At the receiving end, each layer removes its corresponding header and processes the data before passing it up to the next layer.



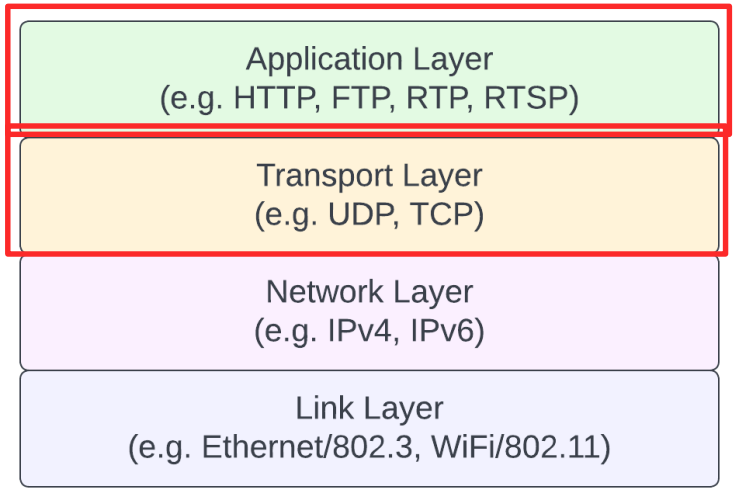
TCP/IP Protocol Suite

- TCP/IP protocol suite provides end-to-end data communication by specifying how data should be packetized, addressed, transmitted, routed, and received.

- The TCP/IP model is organized into four abstraction layers, each with specific functions:

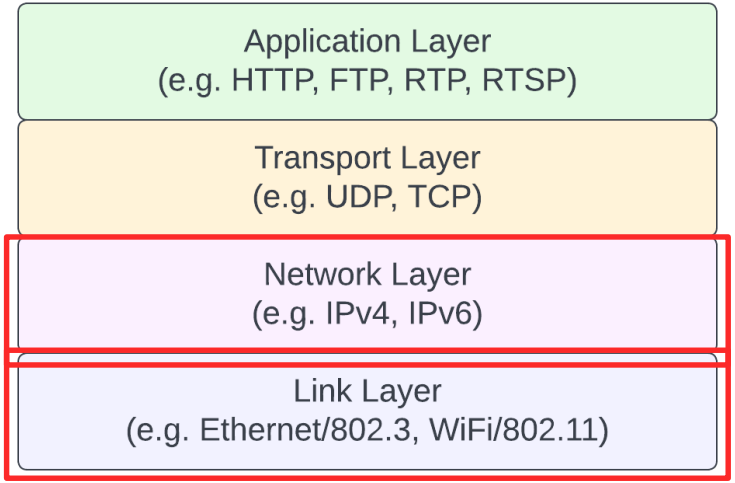
- **Application Layer:** Provides network services directly to end-user applications.
  - **Protocols**: HTTP, FTP, SMTP, DNS, Telnet, SSH, etc.

- **Transport Layer**: Ensures reliable data transfer between devices.
  - **Protocols**: TCP, UDP (User Datagram Protocol).



TCP/IP Protocol Suite

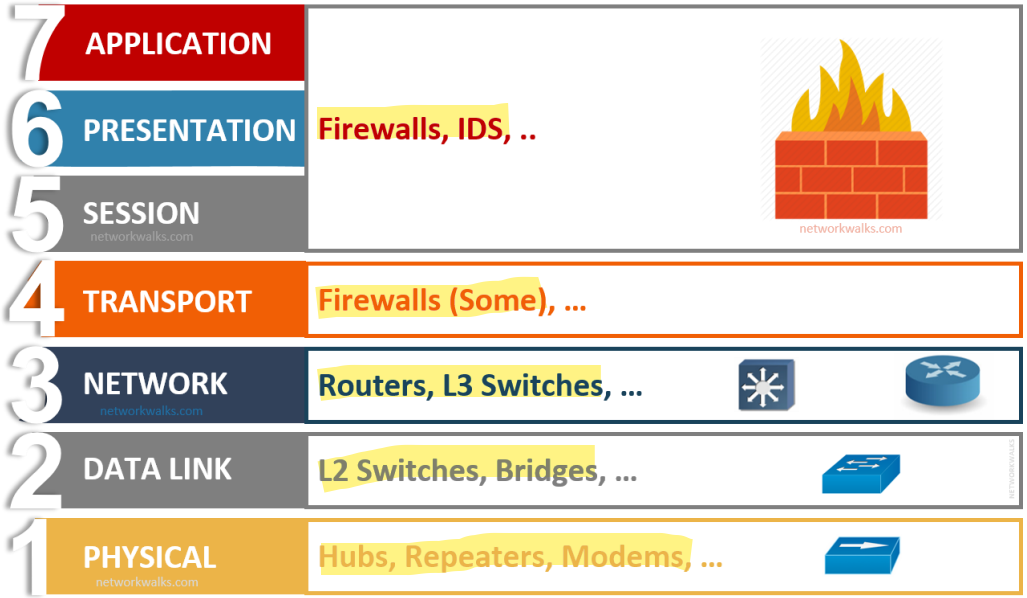
- **Internet Layer:** Handles logical addressing and routing of data packets.
    - **Protocols**: HTTP, FTP, SMTP, DNS, Telnet, SSH, etc.
- **Network Access Layer (Link Layer):** Manages the physical transmission of data over network hardware.
    - **Protocols**: Ethernet, Wi-Fi (IEEE 802.11), PPP (Point-to-Point Protocol).



Network Devices

- Network devices are hardware components that facilitate communication, data transfer, and resource sharing within a network.

- Switches
- Wireless Access Point
- Routers
- Firewalls
- Load Balancers



Layer 2 Attacks

How Switch Works?

- A network switch is a layer2 device and used to connect devices within a local area network (LAN) and forward data packets between them efficiently.

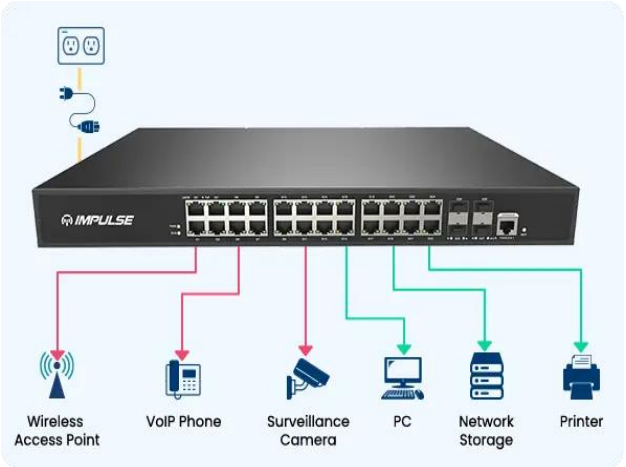
- **Switch Key Functions**

1. **MAC Address Learning:** maintain a MAC address table (also called a CAM table) that maps MAC addresses to the corresponding switch ports.

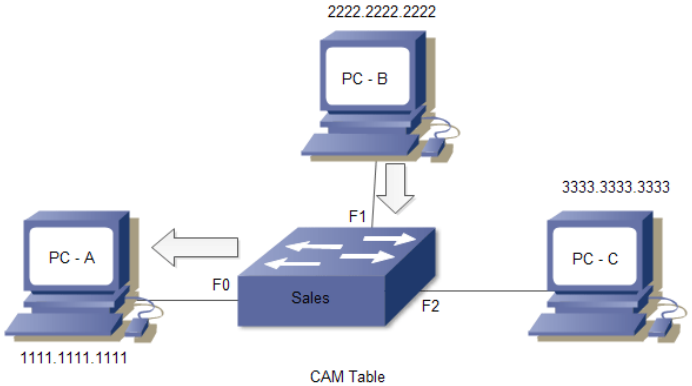
    - **MAC Address:** is a physical address for your network-connected device (NIC). It is a 48-bit hexadecimal number (e.g., 00:1A:2B:3C:4D:5E).

- When a device sends a frame, the switch learns the source MAC address and associates it with the incoming port.

2. **Frame Forwarding:** A switch receives data frames from connected devices and forwards them to the appropriate destination based on the MAC address.

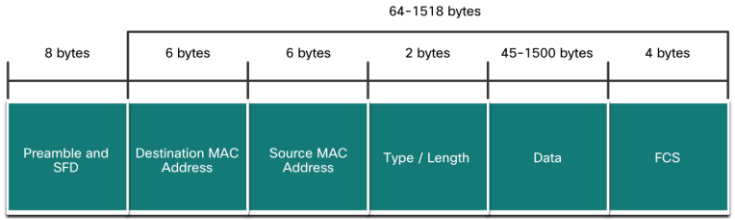


How Switch Builds MAC Table?

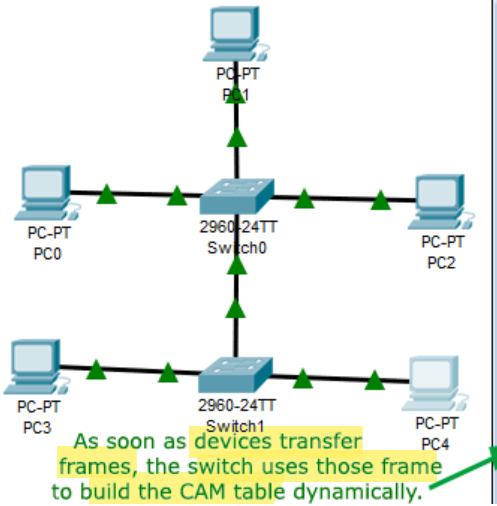


CAM Table

MAC Address	Port Number
1111.1111.1111	F0
2222.2222.2222	F1



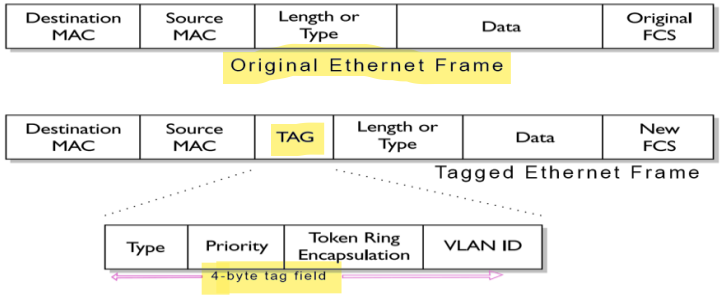
Ethernet Frame

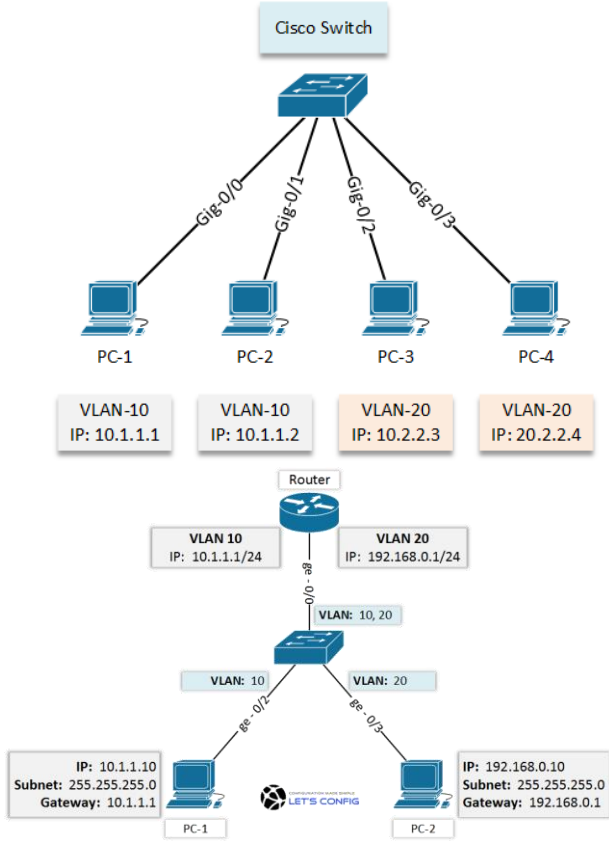



```
changed state to up
When the switch starts, the CAM table is empty.

Switch>enable
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.6462.12ce    DYNAMIC     Fa0/3
   1    0001.c965.b519    DYNAMIC     Gig0/1
   1    0007.ecdd.4128    DYNAMIC     Fa0/2
   1    0060.3e7d.d194    DYNAMIC     Gig0/1
   1    0090.2b22.9cc1    DYNAMIC     Gig0/1
   1    00e0.8fad.629a    DYNAMIC     Fa0/1
Switch#
```

Virtual LANs (VLANs)

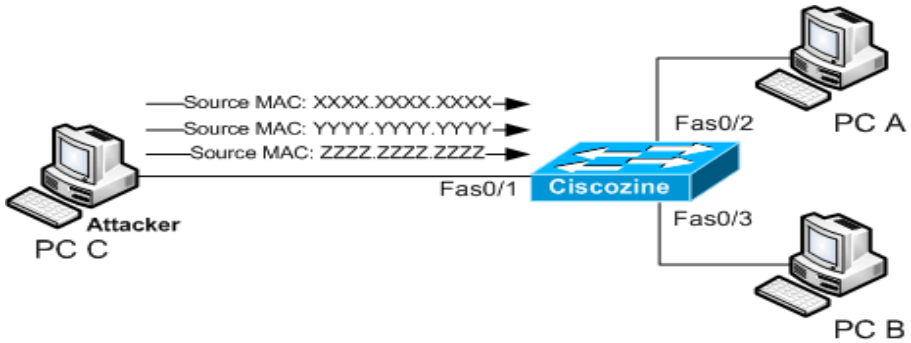
- It is a feature of network switches that allow you to segment a physical network into multiple logical networks.
- Devices in the same VLAN can communicate as if they are on the same physical network, even if they are connected to different switches.
- Switches use a VLAN tag (12 bits added to Ethernet frames) to identify which VLAN a frame belongs to.
- Devices in different VLANs cannot communicate directly. A Layer 3 device (e.g., a router or Layer 3 switch) is required to route traffic between VLANs.





MAC Flooding Attack

- A MAC flooding attack, also known as a MAC table overflow attack, is a type of network security attack that targets network switches.
- It involves overwhelming a switch's MAC address table by flooding it with a massive amount of spoofed Ethernet frames, each containing a unique source MAC address.
- Once the table is full, the switch goes into fail-open mode and behaves like a hub instead of a switch. In this mode, the switch broadcasts all incoming traffic to all ports, regardless of the destination MAC address.



MAC Flooding Attack Prevention

1. **Port Security:** to limit the number of MAC addresses that can be learned on a port.
    1. Set a MAC Address Limit
    2. Sticky MAC Addressing
    3. Actions for Violations (shutdown, limit traffic, generate alert)

2. **MAC address filtering:** Configure switches to permit only specific MAC addresses on each port. It can restrict unauthorized devices from connecting to the network.

3. **Network segmentation:** separate the management and critical VLANs from other VLANs.

4. **Network Monitoring:** Implement network monitoring tools and Intrusion Detection Systems (IDS) to detect and alert unusual patterns of MAC address traffic behavior.

Cisco Catalyst 2960 Series

```
SwitchX(config-if)#switchport port-security [  mac-address
mac-address | mac-address sticky [mac-address] | maximum
value | violation {restrict | shutdown}]
```

```
SwitchX(config)#interface fa0/5
SwitchX(config-if)#switchport mode access
SwitchX(config-if)#switchport port-security
SwitchX(config-if)#switchport port-security maximum 1
SwitchX(config-if)#switchport port-security mac-address sticky
SwitchX(config-if)#switchport port-security violation shutdown
```

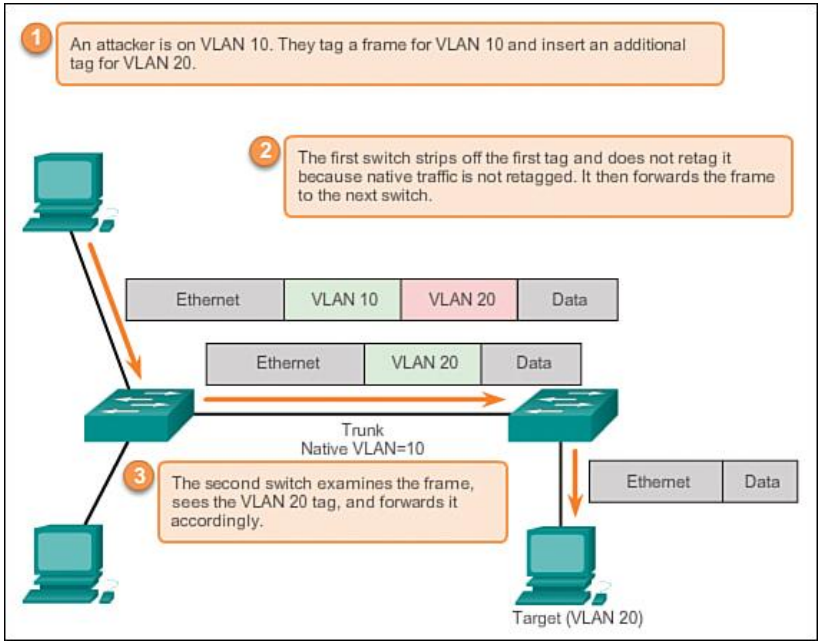
IOS Command Line Interface

```
Cisco_Switch#show port-security interface GigabitEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Double Tagging Attack

- The attacker sends packets with two VLAN tags. The outer tag corresponds to the VLAN of the attacker's access port, and the inner tag corresponds to the target VLAN.
- When the packet reaches the first switch, it removes the outer tag and forwards the packet based on the inner tag, believing it has reached the appropriate VLAN.
- As a result, the packet is sent to the target VLAN, bypassing the intended network segmentation
- **How to Mitigate this attack?**

  1. Change the Native VLAN
  2. Disable Dynamic Trunking Protocol (DTP)
  3. Enable Port Security



MAC Address Spoofing Attack

- MAC address spoofing is a technique where an attacker changes the MAC address of their network interface to impersonate another device on the network.

1. The attacker identifies the MAC address of a legitimate device on the network using tools like arp -a (ARP table) or network scanners.

2. The attacker changes their device's MAC address to match the target's MAC address using software or operating system commands.

```
C:\Users\aaborady>arp -a

Interface: 192.168.1.10 --- 0x19
  Internet Address      Physical Address      Type
  192.168.1.1           30-42-40-ba-66-5c     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

- Windows: Use Device Manager or the netsh command, and Technitium MAC Address Changer.

```bash
netsh interface set interface "<Interface Name>" newmac=<New MAC Address>
```

Example:

```bash
netsh interface set interface "Ethernet" newmac=00-1A-2B-3C-4D-5E
```

- Linux: Use the ifconfig or ip command.
- macOS: Use the ifconfig command.
- Once the MAC address is spoofed, the attacker's device can impersonate the target device, potentially intercepting or redirecting traffic intended for the legitimate device.

MAC Address Spoofing Attack Prevention

1. **Port Security:** to limit the number of MAC addresses that can be learned on a port.
    1. Set a MAC Address Limit
    2. Sticky MAC Addressing
    3. Actions for Violations (shutdown, limit traffic, generate alert)

2. **Use Static ARP entry:** Configure static ARP entries for critical devices to prevent spoofing.

3. **Encryption:** Use encryption protocols (e.g., IPsec, TLS) to protect data from interception.

4. **Dynamic ARP Inspection (DAI):** se DAI to validate ARP packets and prevent ARP spoofing attacks.

Cisco Catalyst 2960 Series

```
SwitchX(config-if)#switchport port-security [  mac-address
mac-address | mac-address sticky [mac-address] | maximum
value | violation {restrict | shutdown}]
```

```
SwitchX(config)#interface fa0/5
SwitchX(config-if)#switchport mode access
SwitchX(config-if)#switchport port-security
SwitchX(config-if)#switchport port-security maximum 1
SwitchX(config-if)#switchport port-security mac-address sticky
SwitchX(config-if)#switchport port-security violation shutdown
```

Address Resolution Protocol (ARP)

- ARP is used to map IP addresses to MAC addresses on a local network.
- ARP enables a host to send an IPv4 packet to another node in the local network by providing a protocol to get the MAC address associated with an IP address.
- **ARP packets:**

ARP Request

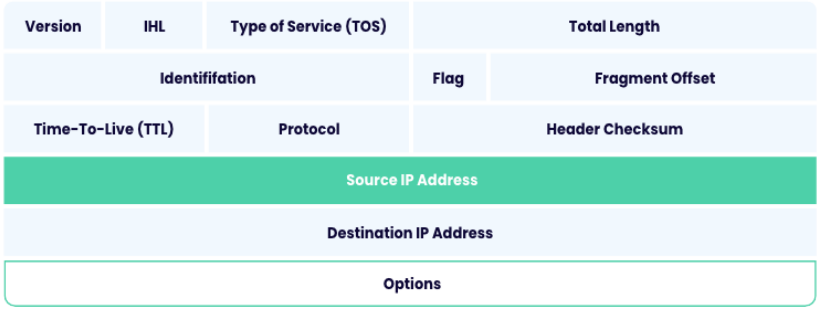
Ethernet II Frame
- **Src:** AAAA-AAAA-AAAA
- **Dst:** FFFF-FFFF-FFFF

Address Resolution Protocol (request)
- **Sender MAC:** AAAA-AAAA-AAAA
- **Sender IP:** 10.1.1.1
- **Target MAC:** 0000-0000-0000
- **Target IP:** 10.1.1.3

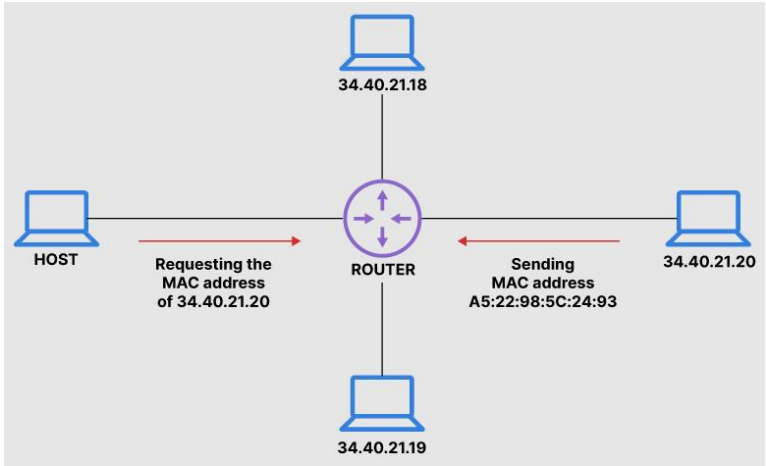
ARP Reply

Ethernet II Frame
- **Src:** CCCC-CCCC-CCCC
- **Dst:** AAAA-AAAA-AAAA

Address Resolution Protocol (request)
- **Sender MAC:** CCCC-CCCC-CCCC
- **Sender IP:** 10.1.1.3
- **Target MAC:** AAAA-AAAA-AAAA
- **Target IP:** 10.1.1.1

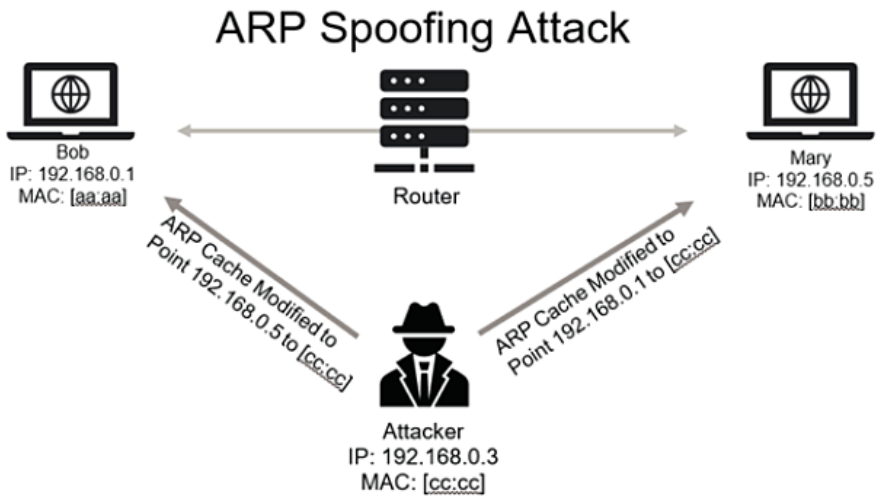


IPv4 Packet Header



ARP Spoofing Attack

- The attacker uses tools like nmap or arp-scan to identify active devices and their IP/MAC addresses.
- The attacker sends falsified ARP responses to the target devices, associating their MAC address with the IP address of a legitimate device.
- Once the ARP cache of the target devices is poisoned, he attacker can intercept, modify, perform DOS and Malware Injection.
- **ARP Spoofing Mitigation:**
- ARP Spoofing Detection Tools: se tools like ARPwatch, XArp, or Cain & Abel to monitor and detect ARP spoofing.
- Enable Port Security.
- Enable Dynamic ARP Inspection (DAI).
- Use Static ARP entries.
- Use Cryptographic protocols.



Thanks!

Do you have any questions?