6. Ethernet Technologies

Ethernet Frame

An **Ethernet frame** operates at the Data Link Layer (Layer 2) of the OSI model. The structure of a Layer 2 PDU (Protocol Data Unit) is as follows:

```
L2 Header | Data | L2 Trailer
```

The L2 header and trailer are further divided into sub-parts:

L2 Header

1. **Preamble (7 Bytes)**
    - Length: 7 bytes (56 bits)
    - Alternating 1's and 0's (10101010 repeated 7 times)
    - Purpose: Synchronizes the receiving device's clock with the incoming data.
2. **SFD (Start Frame Delimiter) (1 Byte)**
    - Length: 1 byte (8 bits)
    - Value: 10101011
    - Purpose: Marks the end of the preamble and the beginning of the frame.
3. **Destination MAC Address (6 Bytes)**
    - A 6-byte (48-bit) field specifying the MAC address of the intended recipient.
4. **Source MAC Address (6 Bytes)**
    - Indicates the MAC address of the sending device.
5. **EtherType/Length (2 Bytes)**
    - Specifies either the type of protocol in the payload (EtherType) or the length of the payload data.
    - Values of 1500 or less indicate the length of the encapsulated packet.
    - Values of 1536 or greater indicate the type of packet (e.g., IPv4 or IPv6).

L2 Trailer

- **FCS (Frame Check Sequence)**: Detects corrupted data using a CRC (Cyclic Redundancy Check) algorithm.

Total Header + Trailer Size: 26 bytes (18 bytes for header + 8 bytes for trailer).

Ethernet frame payload minimum size

The preamble + SFD is usually not considered part of the
Ethernet header. but it sent always.

Therefore the size of ethernet header + trailer is 18 bytes (6+6+2+4)

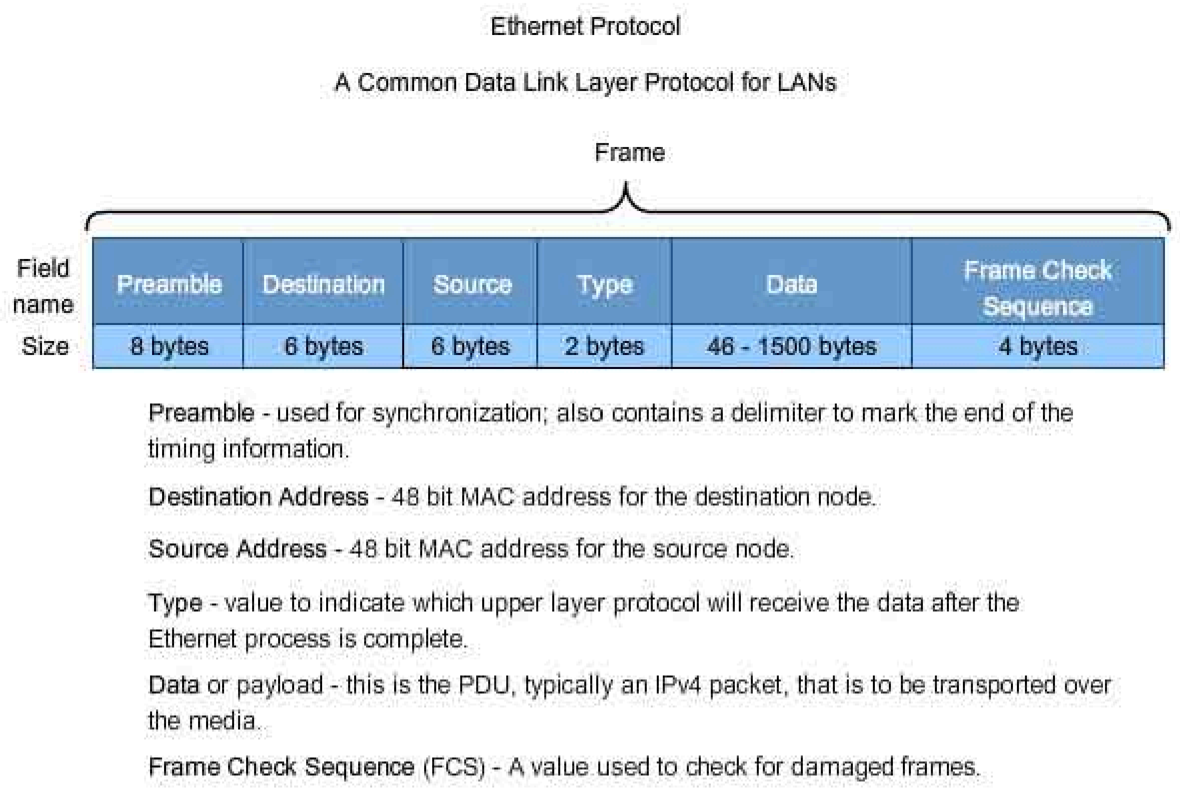
> The minimum size or an Ethernet frame (Header + Payload(Packet) + Trailer is **64 bytes**.

64 bytes - 18 bytes (header - trailer size) = 46 bytes

what if we send payload is less than 46 bytes?

> padding bytes are added , they all are 0.

i.e 34byte packet is send so 12 byte padding will add to make it of 46bytes.



Ethernet Protocol

A Common Data Link Layer Protocol for LANs

Field name	Preamble	Destination	Source	Type	Data	Frame Check Sequence
Size	8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes

Preamble - used for synchronization; also contains a delimiter to mark the end of the timing information.

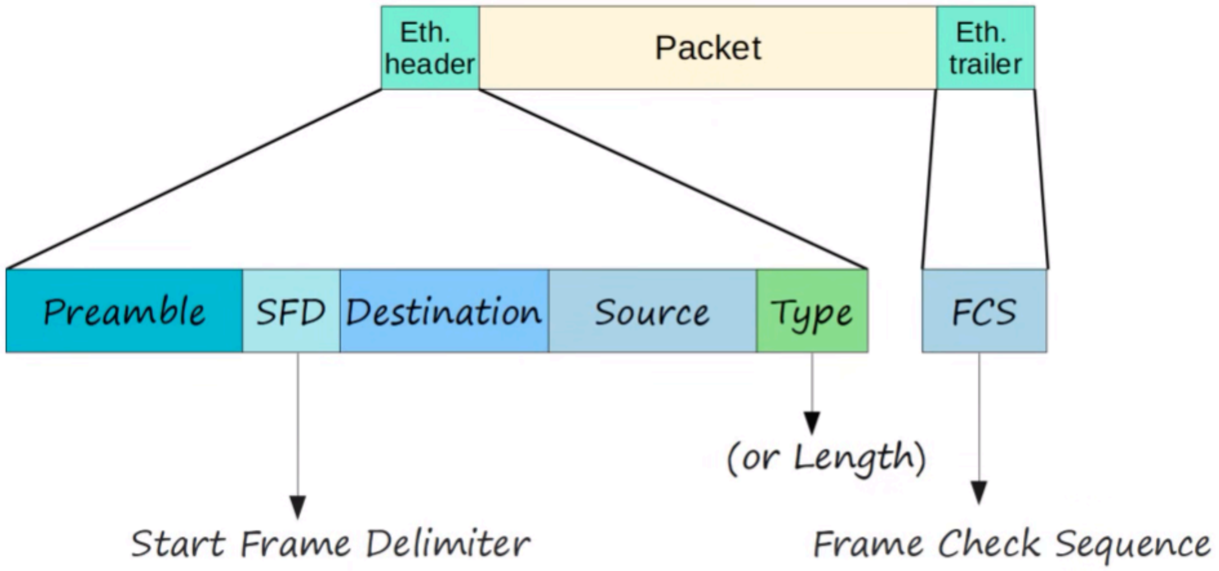
Destination Address - 48 bit MAC address for the destination node.

Source Address - 48 bit MAC address for the source node.

Type - value to indicate which upper layer protocol will receive the data after the Ethernet process is complete.

Data or payload - this is the PDU, typically an IPv4 packet, that is to be transported over the media.

Frame Check Sequence (FCS) - A value used to check for damaged frames.



There are three types of Ethernet addresses:

1. **Unicast Addresses**: These addresses identify a single unique device on the network. A packet sent to a unicast address is received only by the device with that specific MAC address.

- **Unknown Unicast frame:** Fooled the frame to find which pc.
  When switch OR router don't have the destination mac address so how switch handle now?

  To handle unknown unicast frames, the switch will flood the frame out of all ports except the one it was received on. This means that the frame is sent to all devices on the same network segment in an attempt to reach the intended recipient.
- **Known unicast Frame :** Forwarded directly.
  forwarded to the destination mac address directly without flooded as it already stored the MAC address .

2. **Multicast Addresses**: These addresses are used to send packets to a group of devices. A multicast packet is delivered to all devices that are subscribed to that particular multicast address.

3. **Anycast Addresses:**

- Anycast addresses are a special type of address where a single address can be assigned to multiple devices across geographically dispersed locations. When a packet is sent to an anycast address, it is delivered to the nearest device using that address. This is useful for services like load balancing or content delivery networks (CDNs).

5. **Reserved Addresses:**

- A few special IPv6 address blocks are reserved for specific purposes: Loopback Address (::1): Used for internal communication within a single device, similar to the loopback address in IPv4 (127.0.0.1). Unspecified Address (::): Represents an unspecified or non-existent interface.

3. **Broadcast Addresses**:

This type of address is used to send packets to all devices on a local network segment. A broadcast packet is received by every device within the broadcast domain.

- **Broadcast address is always the last address of network.**
- The broadcast address CANNOT be assigned to a host.
- Host portion of the address is all 1'es = Broadcast Address
- **Broadcast Address**: `FFFF.FFFF.FFFF`
- **Ethernet broadcast address**: **FF:FF:FF:FF:FF**
- **IP broadcast address**: Typically the last IP address in the subnet (e.g., **192.168.1.255** for a /24 subnet).

Both serve the purpose of sending messages to all devices within their respective layers of the network.

broadcasting

Broadcast Domain: This is a logical division of a network where any broadcast sent by a device can be received by all other devices in the same domain. Routers typically separate broadcast domains.

- **Broadcast Addresses**: In IPv4, the broadcast address for a subnet allows communication with all devices in that subnet. For example, in a subnet with the address 192.168.1.0 and a subnet mask of 255.255.255.0, the broadcast address would be 192.168.1.255.
- **Protocols**: Various network protocols use broadcasting, including:
  - **ARP (Address Resolution Protocol)**: To resolve IP addresses to MAC addresses.
  - **DHCP (Dynamic Host Configuration Protocol)**: Often uses broadcasting to assign IP addresses to devices on a network.
- **Impact on Network Performance**: Excessive broadcasting can lead to network congestion, known as a broadcast storm, which can degrade performance. This is why network design often aims to limit broadcast traffic.

- **Switches and Broadcasts**: In Ethernet networks, switches forward broadcast frames to all ports (except the port it originated from), while routers do not forward broadcasts, effectively separating broadcast domains.

How a Switch Finds a Device by Broadcasting address

When PC1 sends a message to PC2 in a local network, the message first goes to the switch. The switch needs to determine the MAC address of PC2 to forward the message correctly. There are two main methods the switch uses to find the MAC address:

1. **Manually Configured MAC Address Table**:
    - Network administrators can manually add MAC addresses and their corresponding switch interfaces to the MAC address table. This allows the switch to know exactly where to send traffic for specific MAC addresses.
2. **Dynamically Learned MAC Address**:
    - The switch can learn MAC addresses dynamically. When it receives a frame from PC1, it will flood the frame to all devices on the network (except the port it came from). Any device that recognizes its own MAC address will respond, allowing the switch to learn the MAC address and the port it is connected to. This information is then added to the MAC address table.

How PC1 Finds PC3's MAC Address

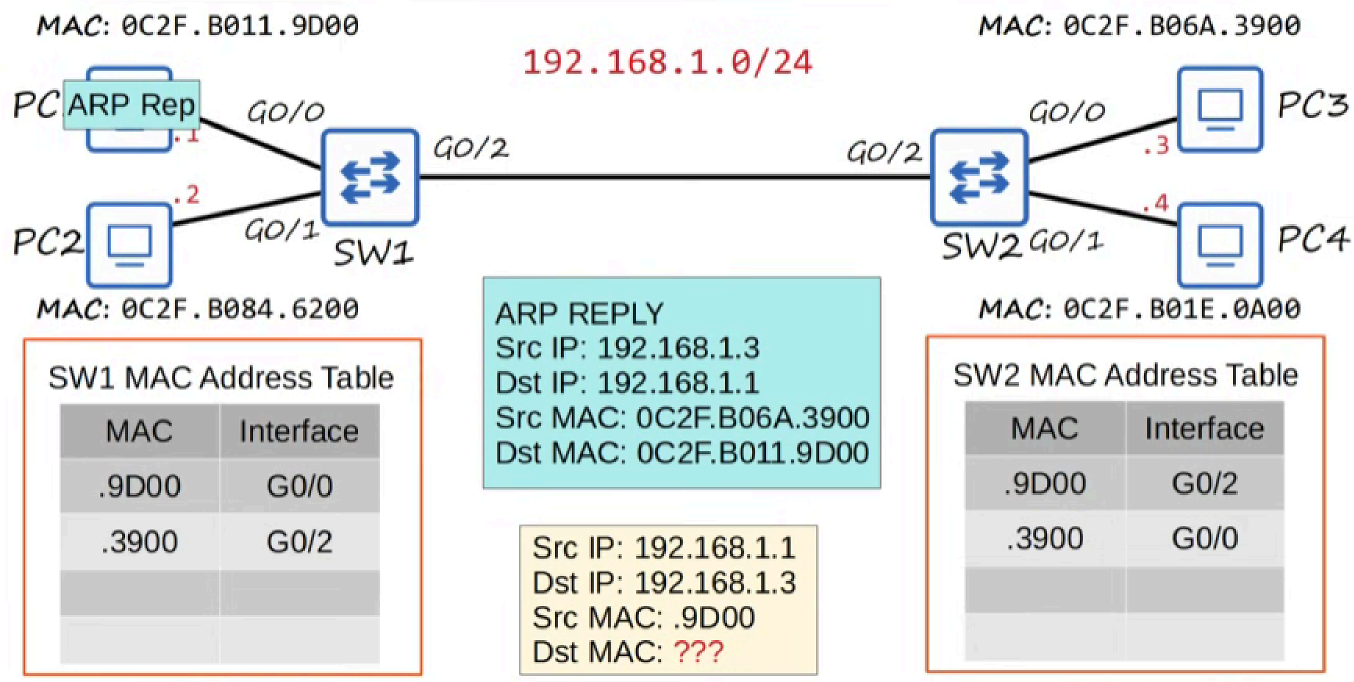
If PC1 knows PC3's IP address but not its MAC address, it will use the Address Resolution Protocol (ARP) to discover it:

1. **ARP Request**:
    - PC1 sends an ARP request to the switch, asking for the MAC address corresponding to PC3's IP address. This ARP request is broadcast to all devices on the local network.
2. **Flooding the Request**:
    - Since the switch does not initially know the MAC address of PC3, it floods the ARP request to all interfaces except the one from which it was received.
3. **ARP Reply**:

- PC3 receives the ARP request, recognizes that it is the intended recipient, and sends back an ARP reply directly to PC1 with its MAC address.

4. **Updating ARP Table**:
    - Upon receiving the ARP reply, PC1 adds PC3's MAC address to its ARP table for future reference.

Note: When PC1 sends the ARP request, it sets the destination MAC address to `FF:FF:FF:FF:FF:FF`, which signifies a broadcast to all devices in the network.



SW1 MAC Address Table

MAC	Interface
.9D00	G0/0
.3900	G0/2

ARP REPLY
Src IP: 192.168.1.3
Dst IP: 192.168.1.1
Src MAC: 0C2F.B06A.3900
Dst MAC: 0C2F.B011.9D00

Src IP: 192.168.1.1
Dst IP: 192.168.1.3
Src MAC: .9D00
Dst MAC: ???

SW2 MAC Address Table

MAC	Interface
.9D00	G0/2
.3900	G0/0

ARP

Address Resolution Protocol (ARP)

- **ARP**: Used to discover the MAC address of a known IP address.
- Consists of two messages:
    1. **ARP Request**: Broadcast to all hosts on the network.
    2. **ARP Reply**: Unicast to the requesting host.

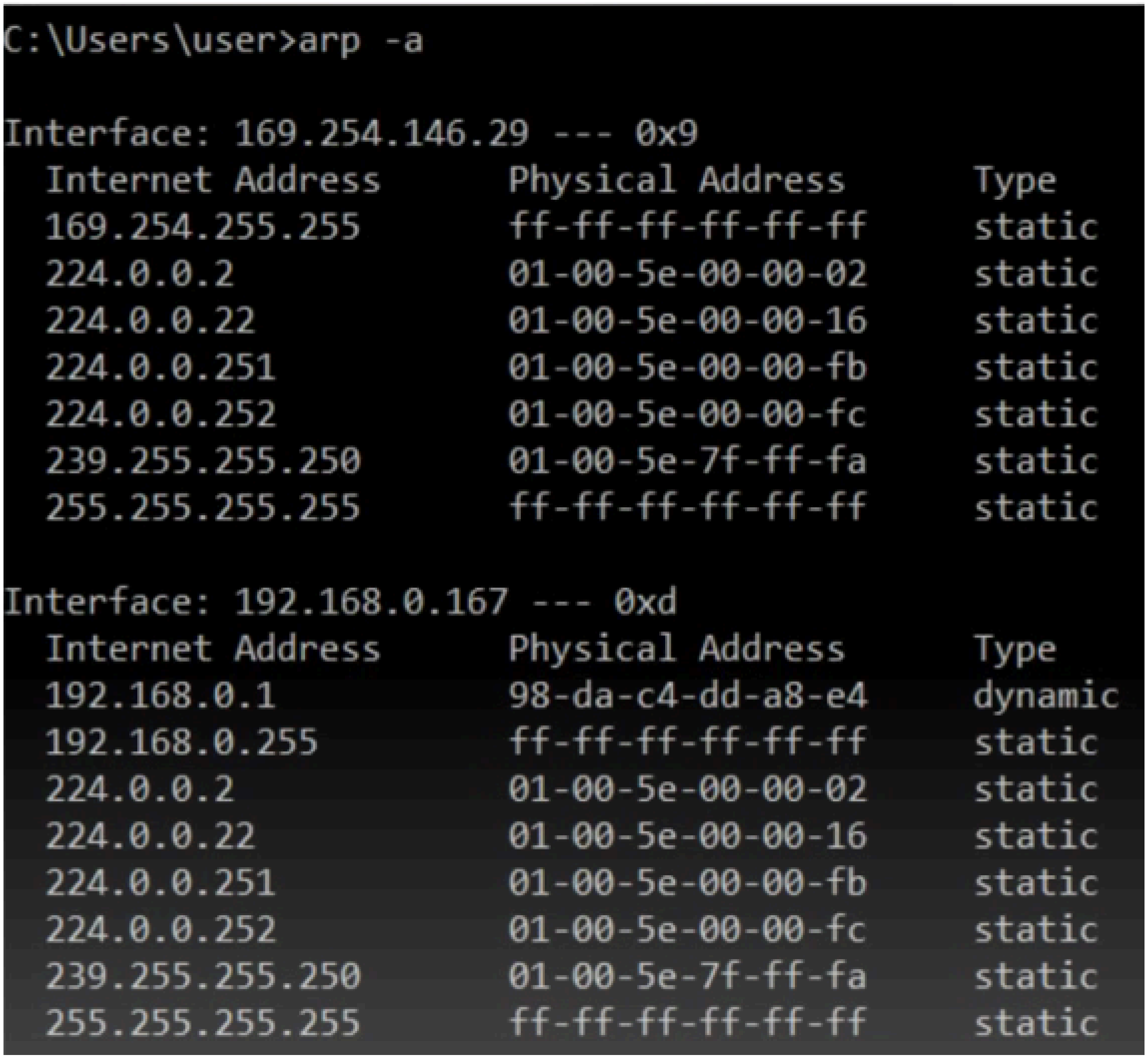
ARP Process

1. If PC1 needs PC3's MAC address, it sends an ARP request.
2. The switch floods the request, and PC3 replies with its MAC address, which PC1 then adds to its ARP table.

ARP Table: View using `arp -a` in Windows, Linux, or Mac.

- **Types**:

- **Static**: Default entry.
- **Dynamic**: Learned via ARP.



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

Interface: 169.254.146.29 --- 0x9
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.167 --- 0xd
  Internet Address      Physical Address      Type
  192.168.0.1           98-da-c4-dd-a8-e4     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

ping

- A network utility that is used to test reachability
- Measures round -trip time
- Uses two messages:
  1. ICMP Echo Request
  2. ICMP Echo Reply
- Command: `ping (ip-address)`

MAC address (media access control)

- 6-byte (48 -bit) physical address assigned to the device when it is made
- A.K.A. (Burned -In Address' (BIA)

- Is globally unique
- The first 3 bytes are the OUI (Organizationally Unique Identifier, which is assigned to the company making the device.
- The last 3 bytes are unique to the device itself.
- Written as 12 hexadecimal characters.

Mac addressing spoofing

MAC spoofing involves changing the MAC address of a network interface to a different address. This can be done temporarily or permanently.

- **How It Works**: The device is configured to report a different MAC address to the network, which can be achieved through software or configuration settings.

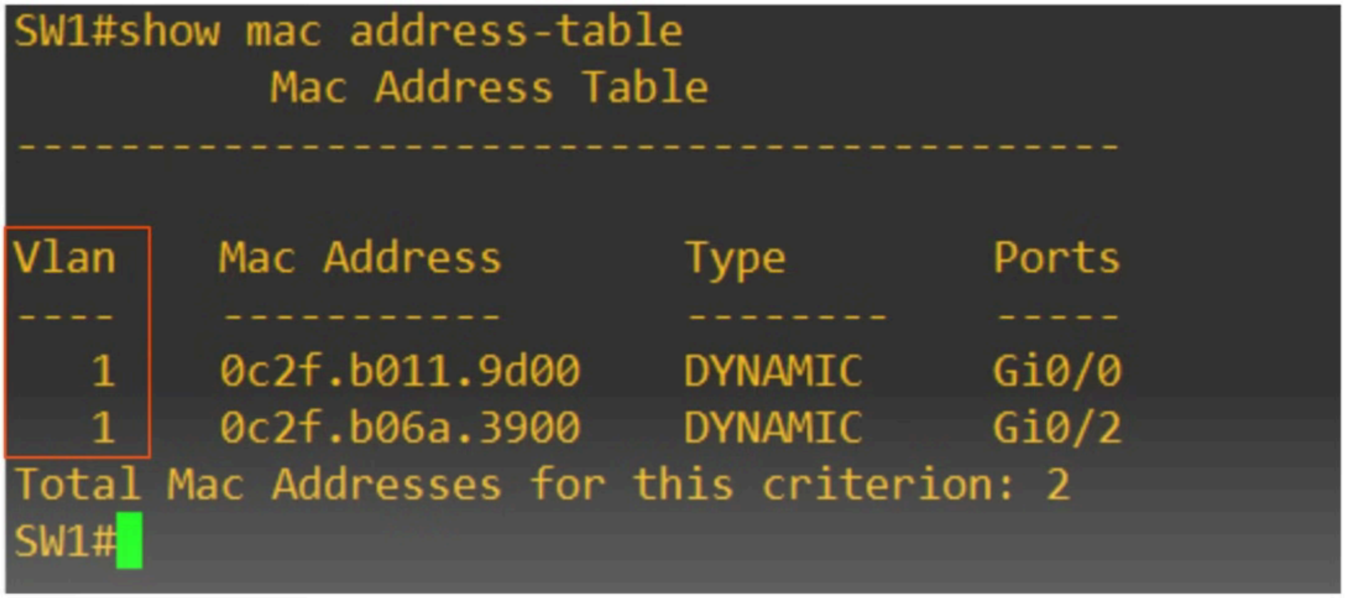
How to protect mac spoofing.

1. MAC Address Filtering
   Allow only specific MAC addresses on your network.
2. 802.1X Authentication
   Implement port-based access control requiring devices to authenticate before connecting.
3. Network Access Control (NAC)
   Use NAC solutions to enforce security policies and assess device health.
4. Regular Monitoring and Auditing
   Continuously monitor network traffic for unusual MAC addresses.
5. Segmentation and Isolation
   Use VLANs to separate sensitive systems from less secure devices.
6. Security Policies and User Education
   Develop policies and educate users about the risks of MAC spoofing.
7. Intrusion Detection Systems (IDS)
   Employ IDS to monitor for unauthorized MAC address changes and alert on suspicious activity.

MAC Address Table for Cisco Switches

- View MAC address table using: `show mac address-table`.
- Entries are dynamic, learned via ARP.
- Dynamically learned MAC addresses auto-clear after 5 minutes of inactivity (Aging).
- To manually clear entries:
  - `clear mac address-table dynamic interface interface_id`
  - Example: `clear mac address-table dynamic interface Gi0/0`.

MAC Address Table



```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0c2f.b011.9d00    DYNAMIC     Gi0/0
   1    0c2f.b06a.3900    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 2
SW1#
```