Ethernet Switching Basics

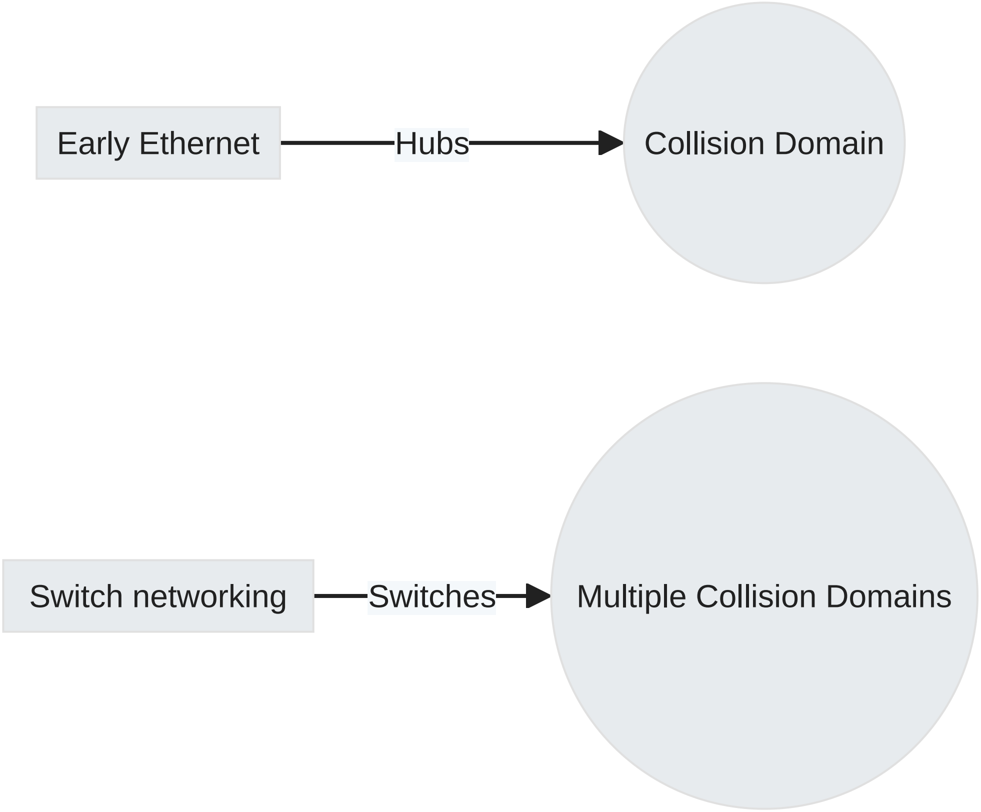
1 Ethernet Switching Basics

1.1 Overview of Ethernet Protocols

Ethernet is the foundational standard for most Local Area Networks (LANs). It specifies the types of cables and signal processing methods used in a LAN environment.

- Ethernet networks are built on the CSMA/CD mechanism.
- Switches have largely replaced hubs in modern networks due to their ability to improve performance by isolating collision domains.

> A collision domain is a segment of a network where packet collisions can occur, typically confined to a single broadcast domain when using a hub.



1.1.1 CSMA/CD Mechanism

- Devices listen for network silence before transmitting.
- If two devices transmit simultaneously, a collision occurs.
- Devices stop sending data and send jam signals upon detecting collisions.
- After waiting for a random delay period, devices attempt to resend data.

1.1.2 Broadcast Domains

> A broadcast domain is the area where a broadcast message can reach all devices in a network at Layer 2 of the OSI model.

- All hosts within the same broadcast domain receive any broadcasted packets.

- Switches send broadcast messages to all devices connected to them, making those devices part of a single communication group.

1.1.3 Ethernet NIC (Network Interface Card)

> **NIC Definition**: Essential hardware component enabling network device connection to an external network. Each port on a networking device corresponds to one NIC. Commonly referred to as network interface or port.

> **Physical ports:** actual interface on your computer where you can connect a cable—like an Ethernet port connected to its respective NIC.

> **Software/network port:** This is a virtual construct used by your computer's operating system to organize and manage network traffic. For example, when you access a website using your web browser, it typically uses port 80 (for HTTP) or port 443 (for HTTPS).

> **Ethernet NICs**: In the context of this document, all NICs referenced are Ethernet compatible. The switches discussed use Ethernet NICs at each port.

> **Data Handling**: Computers or switches send and receive data frames through NICs which process these frames into bitstreams suitable for transmission across physical media.

1.2 Overview of Ethernet Frames

1.2.1 Ethernet Frame Format

- Ethernet frames are the data units used in Ethernet networks.
- Two primary formats: **Ethernet II** and **IEEE 802.3**.
- Frame length: `64–1518 bytes` , where the MTU (Maximum Transmission Unit) is `1500 bytes` .

1.2.1.1 Ethernet II vs IEEE 802.3

Ethernet II Frame Structure	Size (bytes)	Description
Destination MAC (DMAC)	6	Destination Media Access Control address
Source MAC (SMAC)	6	Source Media Access Control address
Type / Ethertype	2	field in an Ethernet frame specifies the protocol of the data contained in the frame's payload (like IPv4, IPv6, ARP, etc.).
User Data	46-1500	Payload containing the encapsulated data from a higher layer protocol
Frame Check Sequence (FCS)	4	Error-checking field used to detect corruption

> - Type
>   - **0x0800:** Internet Protocol Version 4 (IPv4)
>   - **0x0806:** Address Resolution Protocol (ARP)

IEEE 802.3 Frame Structure	Size (bytes)	Description
Destination MAC (DMAC)	6	Destination Media Access Control address
Source MAC (SMAC)	6	Source Media Access Control address

IEEE 802.3 Frame Structure	Size (bytes)	Description
Length field	2	Specifies the length of the payload data
Logical Link Control (LLC)	Variable	Provides additional control information for managing data communication links.
Destination Service Access Point (DSAP)	1 byte	Identifies which application or service on the destination device should handle data.
Source Service Access Point (SSAP)	1 byte	Identifies the application or service on the source device that generated data.
Control	1 byte	Ensures proper sequencing and error checking for frames being transmitted.
SNAP	-	- Extends LLC to allow use of EtherType values for protocol identification.
- Org Code	3 bytes	Specifies an organization that defines the format of following fields in SNAP.
- Type	2 bytes	Indicates which protocol is encapsulated within this Ethernet frame (like IP, ARP).
User data	38-1492B	Contains actual information being transmitted (application data, etc.).
FCS	4 bytes	Error-checking field that helps ensure data integrity during transmission.

1.2.2 MAC Address

- **A media access control (MAC):** address uniquely identifies a NIC on a network. Each NIC must have a globally unique MAC address, defined and standardized in IEEE 802.
  - **Length**: `48 bits` or `6 bytes` .
  - **Format**: Six groups of two hexadecimal digits (`00-AA-BB-CC-DD-EE`).

Criteria	IP Addresses	MAC Addresses
Uniqueness	Unique within a network segment	Globally unique
Changeability	Can be changed	Cannot be changed
Assignment Basis	Based on network topology	Based on the manufacturer
Network Relevance	Used for route selection and networking	Used primarily for local network traffic
Flexibility & Maintenance	Devices can be reassigned IP addresses; helpful for reconfiguration and mobility	MAC addresses are static, but devices can be replaced without affecting IP addressing

1.2.3 OUI and CID

> **Organizationally unique identifier (OUI):** First 3 bytes assigned by IEEE to manufacturers(globally unique).
> **Company ID (CID):** Last 3 bytes assigned by manufacturers to individual devices.

1.2.4 Frame Types

1.2.4.1 Unicast Frame

- Destination MAC = Unicast MAC address
- Sent from one source to one destination only.

> **Format:** XX-XX-XX-XX-XX-X0 | Individual device identification.

1.2.4.2 Broadcast Frame

- Destination MAC = FF:FF:FF:FF:FF:FF
- Sent from one source to all hosts on LAN.

> **Format:** FF-FF-FF-FF-FF-FF | All devices on the LAN.

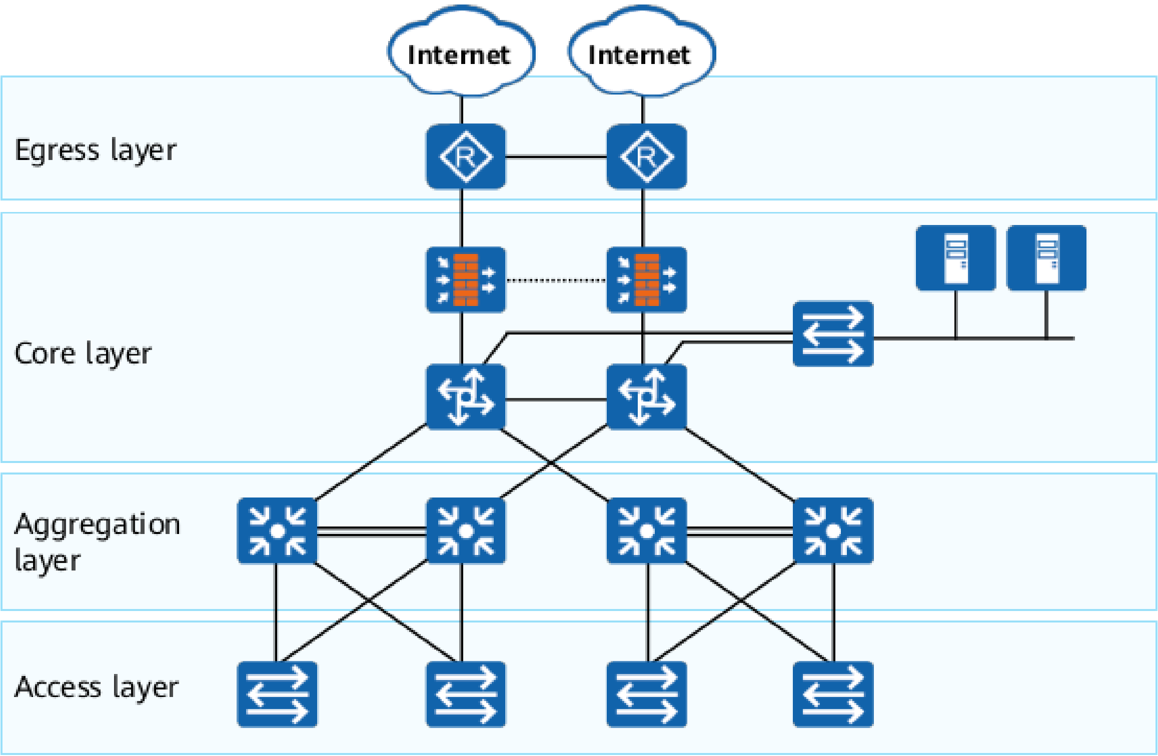
1.2.4.3 Multicast Frame

- Destination MAC = Starts with '01' e.g., 01:80:C2...
- Sent from one source to multiple hosts subscribed to multicast group.

> **Format:** XX-XX-XX-XX-XX-X1 | Group of devices on the LAN.

1.3 Overview of Ethernet Switches

- A campus network typically includes an **access layer**, **aggregation layer**, **core layer**, and **egress layer**.
- Devices involved include routers, switches (Layer 2 & Layer 3), and firewalls.



1.3.1 Switches

1.3.1.1 Layer 2 Ethernet Switch

> - Operates at the Data Link Layer (Layer 2 of the TCP/IP model).
> - Forwards packets based on MAC addresses.

1.3.1.2 Layer 3 Ethernet Switch

> - Capable of high-speed Layer 3 forwarding.
> - Used when routers are insufficient due to high costs or low performance.

1.3.2 Frame Processing Behaviors

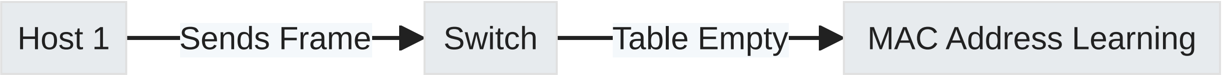
- **Flooding**: If the destination MAC address is unknown or a broadcast address, the frame is sent to all ports except the originating port.
- **Forwarding**: The switch sends the frame to a specific port based on the MAC address table.
- **Discarding**: Frames coming from the same place they arrived are discarded to prevent loops.

1.3.3 MAC Address Table Learning Process

> **Note**
>
> Switches dynamically learn MAC addresses and associate them with interfaces. Entries have an aging time (e.g., Huawei default is 300s).

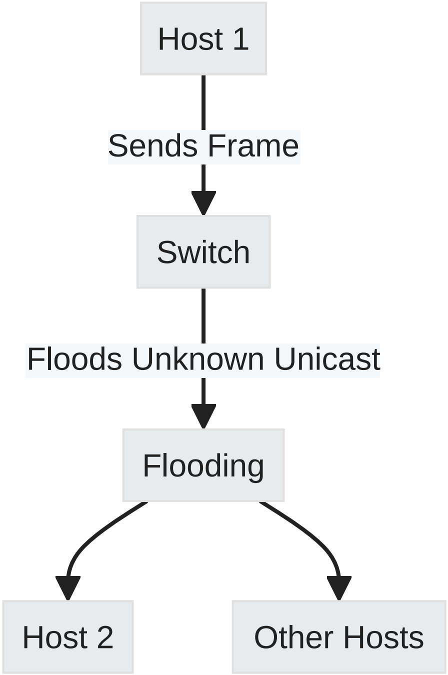
MAC Address	Interface
MAC1	GE0/0/1
MAC2	FE0/1

1.3.3.1 Initial State



> `Host1` sends a frame with its own source IP/MAC to `Host2` .

1.3.3.2 Frame Reception & Flooding

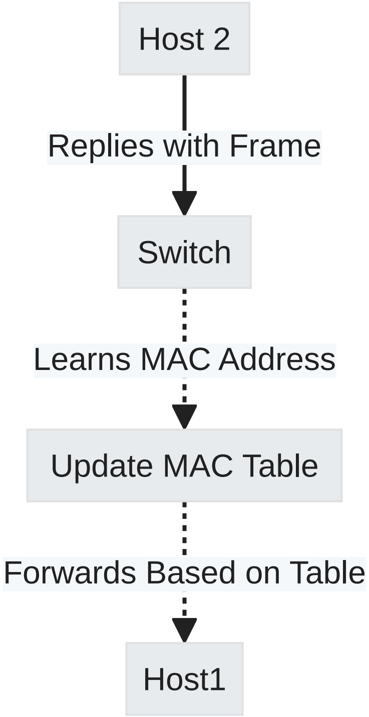


MAC Address	Interface
MAC1	GE0/0/1

> The switch learns `Host1` 's MAC and updates its table linking it to interface GE 0/0/1.

> If no entry for `Host2` 's MAC exists, the switch floods the frame.

1.3.3.3 Update Table & Forwarding



> `Host2` receives and processes the frame since it matches its own MAC address.

> When `Host2` replies, the switch finds an entry in its table and forwards accordingly while learning `Host2` 's interface (GE 0/0/2).

MAC Address	Interface
MAC1	GE0/0/1
MAC2	GE0/0/2

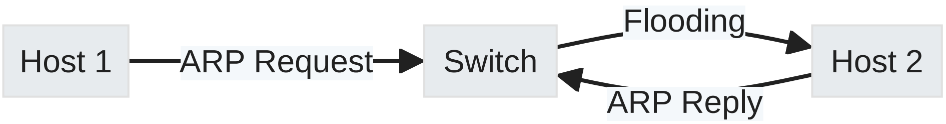
1.4 Process of Data communication Within a Network Segment

1.4.1 Overview

- **Objective**: Host 1 wants to access Host 2 within a network.
- **Hosts**:

  - Both hosts know their own IP and MAC addresses.
  - Assumption: Host 1 has obtained the IP address of Host 2.
- **Switch**: The switch is initially in a powered-on state with an empty MAC address table.

1.4.2 Initialization Process



> ✎ **Note**
>
> Initially, both the ARP cache table on Host 1 and the MAC address table on the switch are empty.

1.4.3 ARP Request and Flooding Frames

- Host 1 sends an **ARP Request** to find MAC2 (Host 2's MAC address).
- The switch floods the frame to all ports except the one it received from because its MAC address table is empty.

1.4.4 MAC Address Learning

- The switch learns MAC1 (Host 1's MAC) when it receives the ARP Request and updates its MAC address table:

MAC Address	Port	Type
`0050-5600-0001`	GE0/0/1	dynamic

> **Tip**
>
> Switches learn source MAC addresses from incoming frames and store them in their tables along with associated ports.

1.4.5 Reply of the Target Host (ARP Reply)

- Host 2 processes the ARP Request and sends an **ARP Reply** back to Host 1 containing its own MAC and IP addresses.
- The switch forwards this reply directly to Host 1 since it now knows where to send packets destined for `0050-5600-0001` .

1.4.5.1 Updated Switch Table after ARP Reply

MAC Address	Port	Type
`0050-5600-0001`	GE0/0/1	dynamic
`0050-5600-0002`	GE0/0/2	dynamic

> **Host 1** updates its ARP cache with the IP-MAC mapping for Host 2.