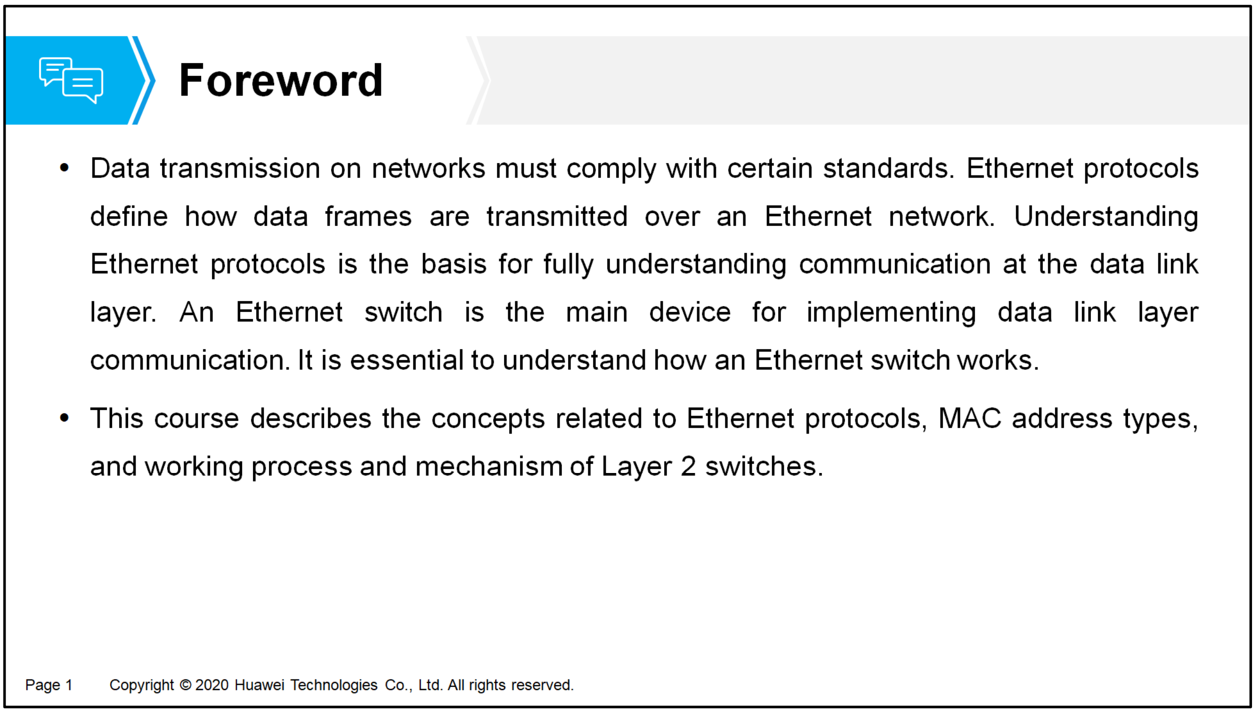
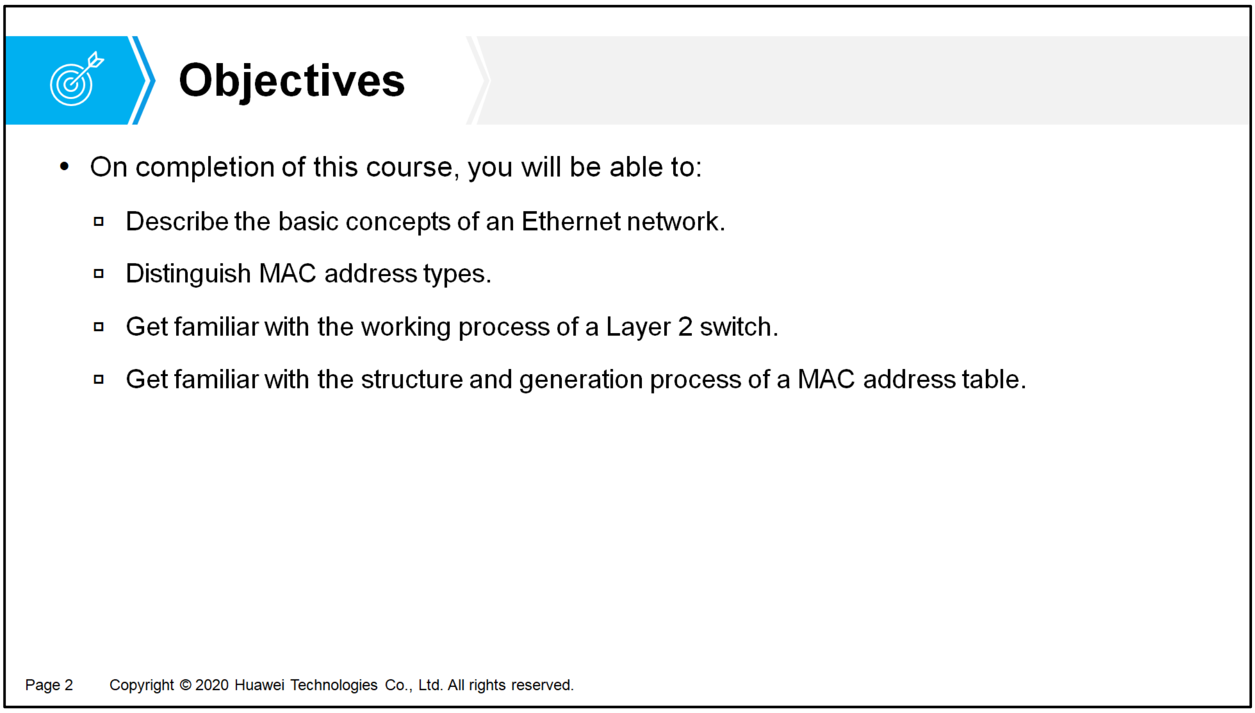


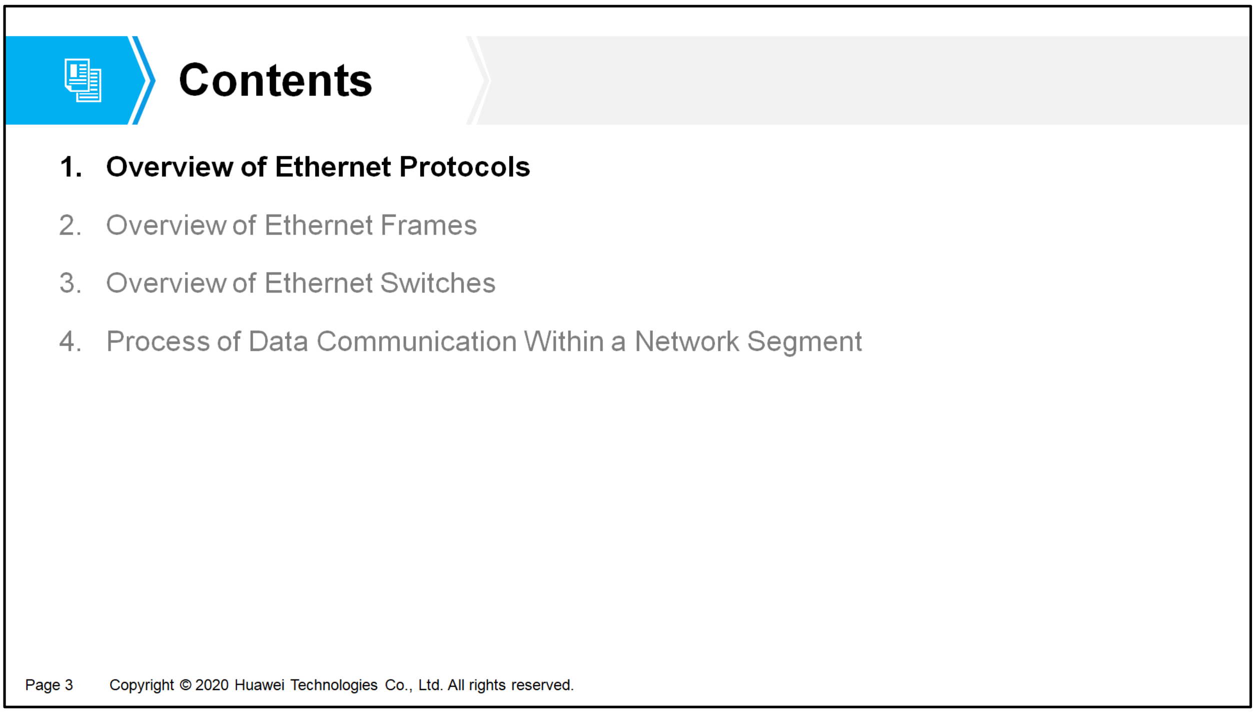
Foreword

- Data transmission on networks must comply with certain standards. Ethernet protocols define how data frames are transmitted over an Ethernet network. Understanding Ethernet protocols is the basis for fully understanding communication at the data link layer. An Ethernet switch is the main device for implementing data link layer communication. It is essential to understand how an Ethernet switch works.
- This course describes the concepts related to Ethernet protocols, MAC address types, and working process and mechanism of Layer 2 switches.



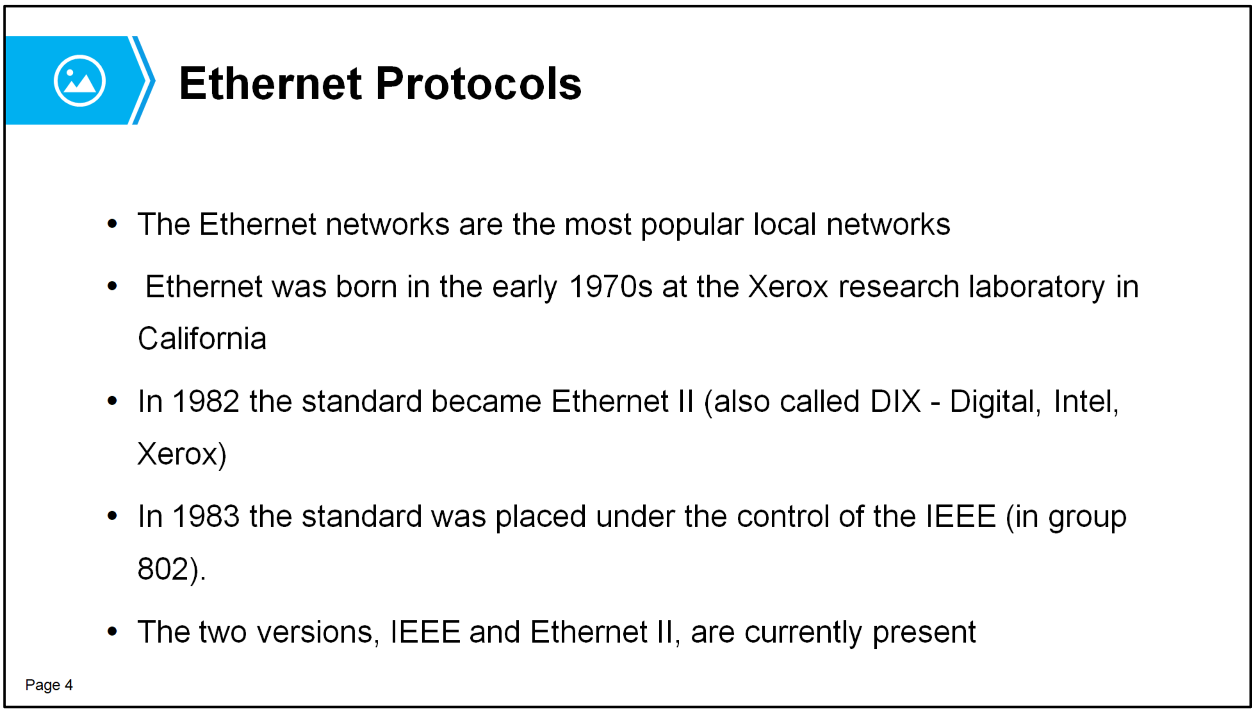
Objectives

- On completion of this course, you will be able to:
  - Describe the basic concepts of an Ethernet network.
  - Distinguish MAC address types.
  - Get familiar with the working process of a Layer 2 switch.
  - Get familiar with the structure and generation process of a MAC address table.



Contents

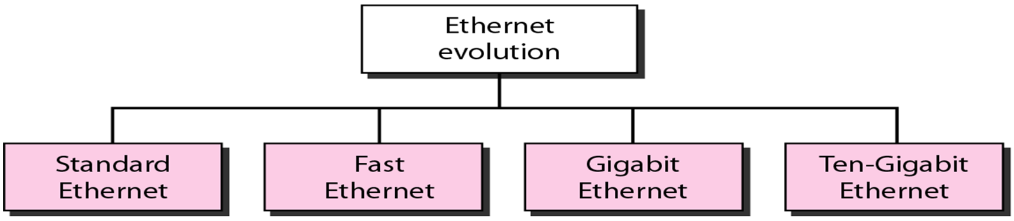
1. **Overview of Ethernet Protocols**
2. Overview of Ethernet Frames
3. Overview of Ethernet Switches
4. Process of Data Communication Within a Network Segment



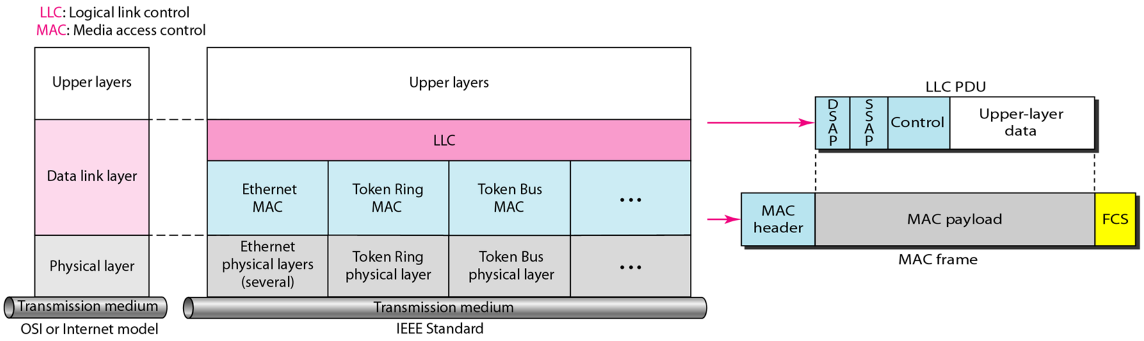
Ethernet Protocols

- The Ethernet networks are the most popular local networks
- Ethernet was born in the early 1970s at the Xerox research laboratory in California
- In 1982 the standard became Ethernet II (also called DIX - Digital, Intel, Xerox)
- In 1983 the standard was placed under the control of the IEEE (in group 802).
- The two versions, IEEE and Ethernet II, are currently present

Ethernet Protocols

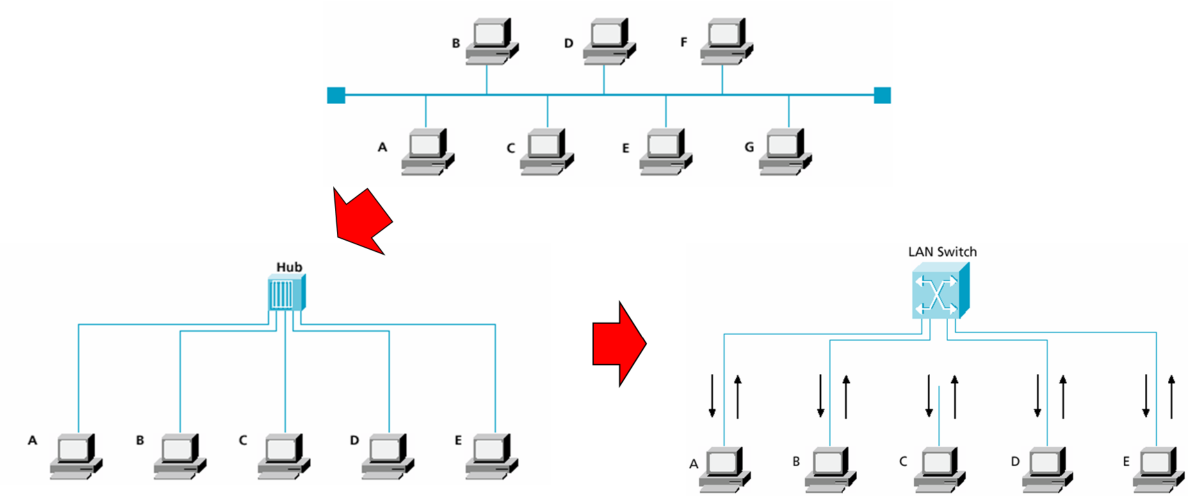


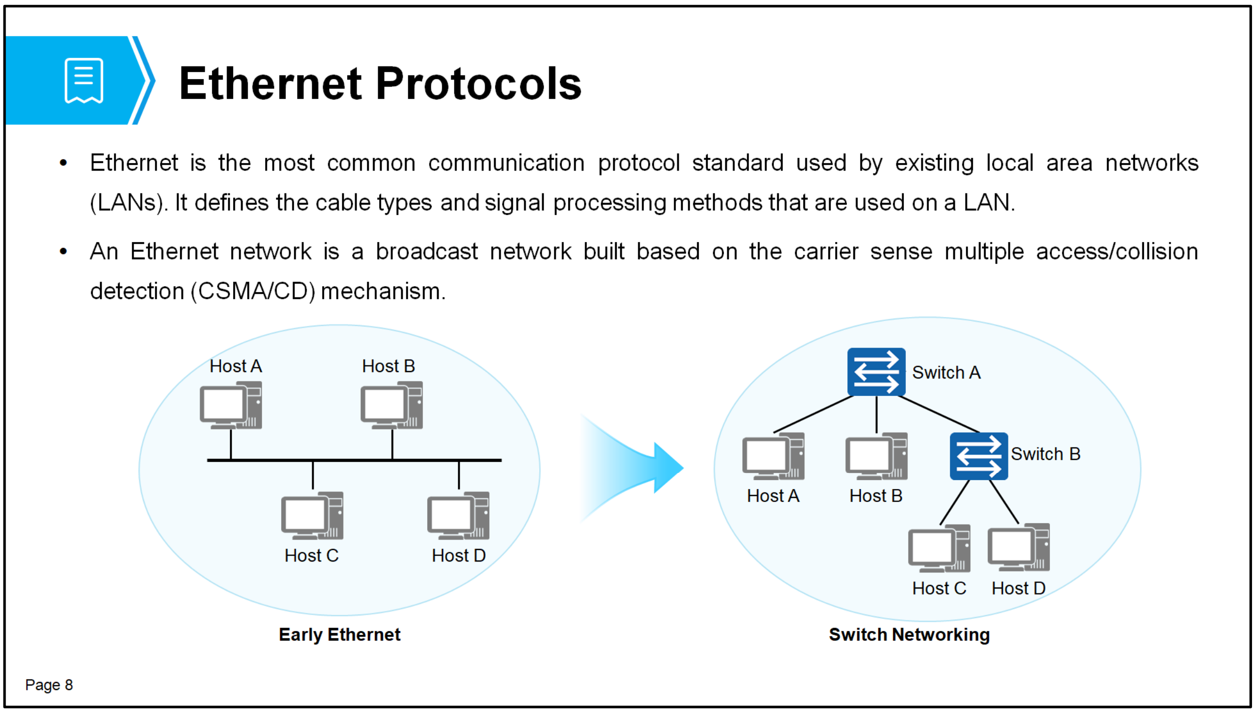
The IEEE 802 standard



- 802.1 definisce le caratteristiche generali degli standard per le reti locali e metropolitane e per l'interoperabilità tra reti diverse.

Ethernet Topologies





Ethernet Protocols

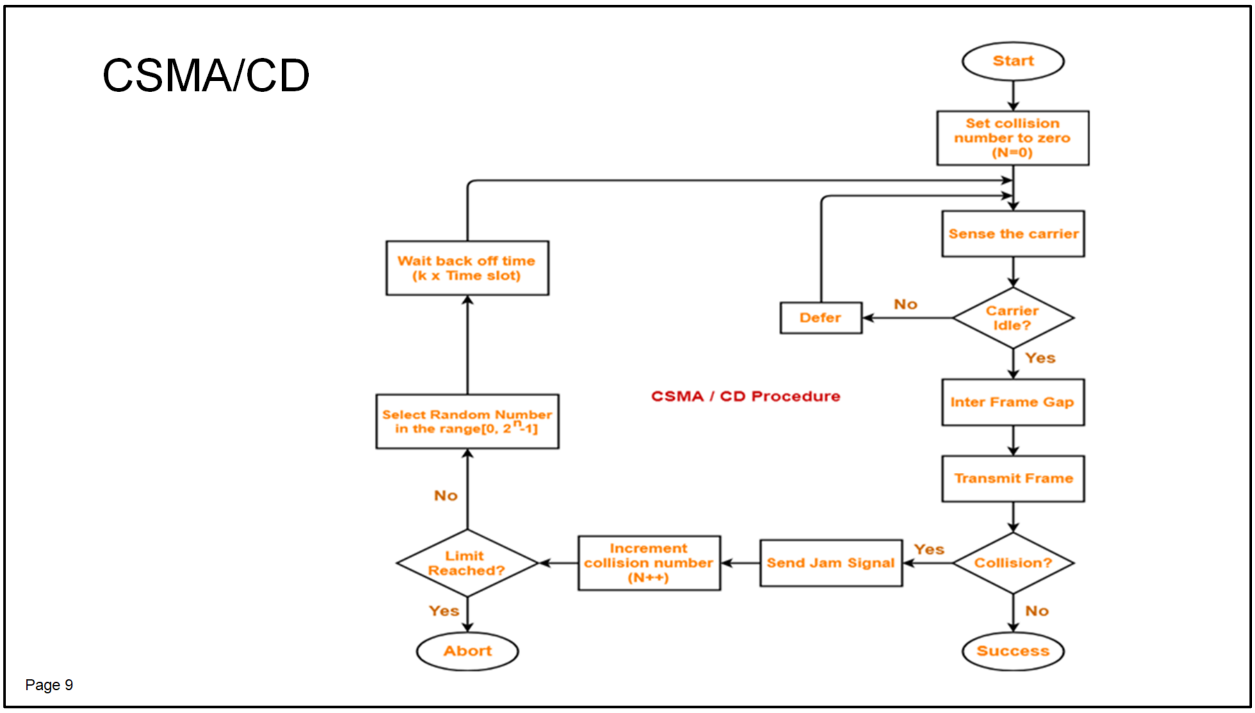
- Ethernet is the most common communication protocol standard used by existing local area networks (LANs). It defines the cable types and signal processing methods that are used on a LAN.
- An Ethernet network is a broadcast network built based on the carrier sense multiple access/collision detection (CSMA/CD) mechanism.

Host A
Host B
Host C
Host D
Switch A
Switch B
Host A
Host B
Host C
Host D

Early Ethernet

Switch Networking

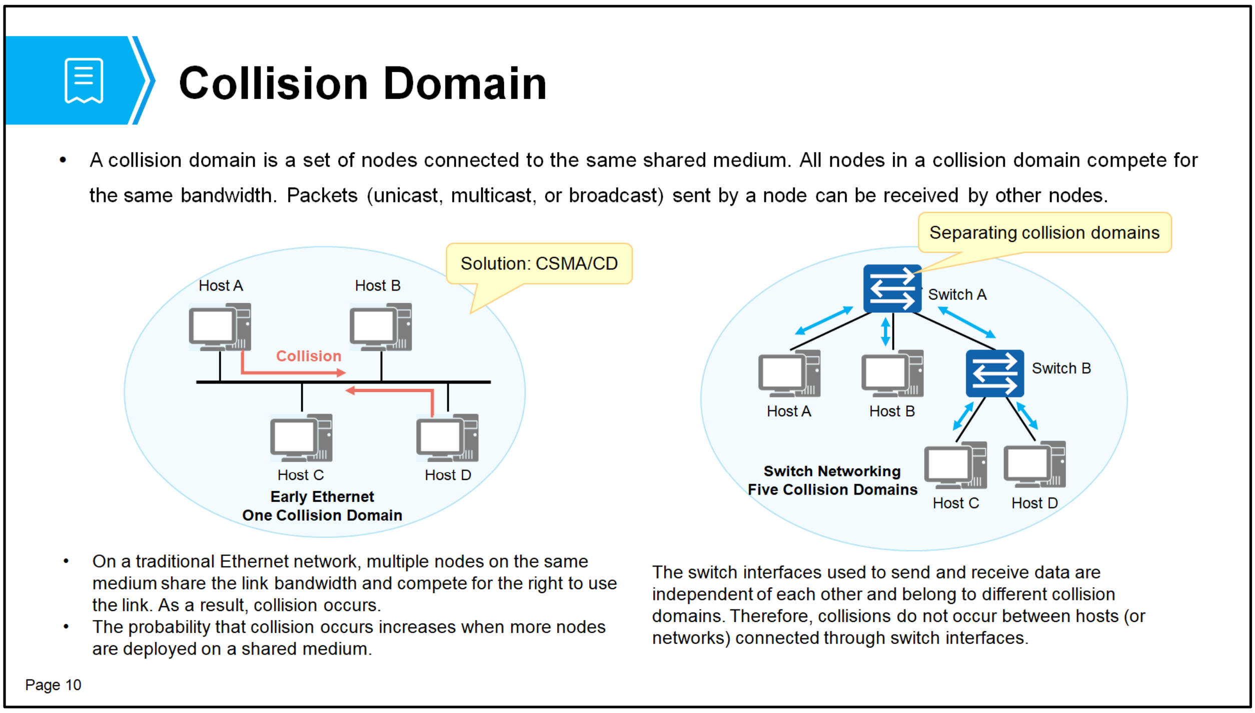
- Early Ethernet:
  - Ethernet networks are broadcast networks established based on the CSMA/CD mechanism. Collisions restrict Ethernet performance. Early Ethernet devices such as hubs work at the physical layer, and cannot confine collisions to a particular scope. This restricts network performance improvement.
- Switch networking:
  - Working at the data link layer, switches are able to confine collisions to a particular scope. Switches help improve Ethernet performance and have replaced hubs as mainstream Ethernet devices. However, switches do not restrict broadcast traffic on the Ethernet. This affects Ethernet performance.



CSMA/CD

Page 9

- binary exponential backoff: K=2^(n-1), with n=min(m,10), m number of collisions.



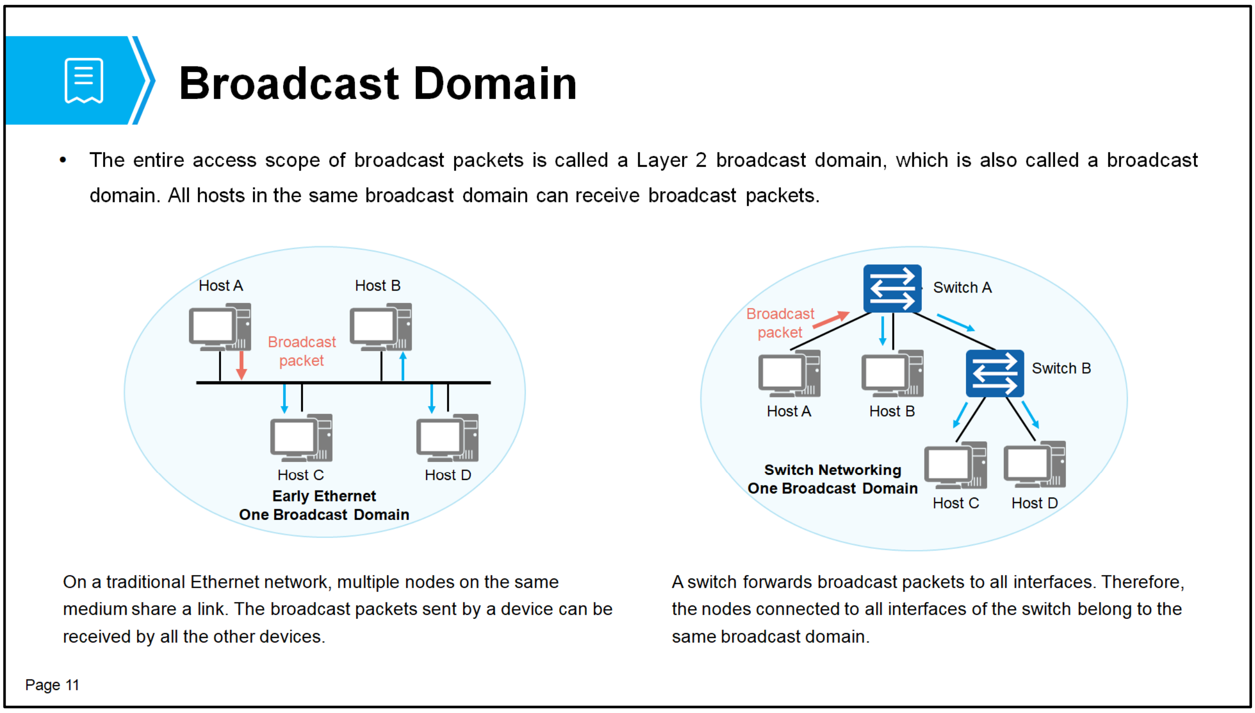
Collision Domain

- A collision domain is a set of nodes connected to the same shared medium. All nodes in a collision domain compete for the same bandwidth. Packets (unicast, multicast, or broadcast) sent by a node can be received by other nodes.

- On a traditional Ethernet network, multiple nodes on the same medium share the link bandwidth and compete for the right to use the link. As a result, collision occurs.
- The probability that collision occurs increases when more nodes are deployed on a shared medium.

The switch interfaces used to send and receive data are independent of each other and belong to different collision domains. Therefore, collisions do not occur between hosts (or networks) connected through switch interfaces.

- On a shared network, the Ethernet uses the CSMA/CD technology to avoid collisions. The CSMA/CD process is as follows:
  - A terminal continuously detects whether the shared line is idle.
    - If the line is idle, the terminal sends data.
    - If the line is in use, the terminal waits until the line becomes idle.
  - If two terminals send data at the same time, a collision occurs on the line, and signals on the line become unstable.
  - After detecting the instability, the terminal immediately stops sending data.
  - The terminal sends a series of disturbing pulses. After a period of time, the terminal resumes the data transmission. The terminal sends disturbing pulses to inform other terminals, especially the terminal that sends data at the same time, that a collision occurred on the line.
- The working principle of CSMA/CD can be summarized as follows: listen before send, listen while sending, stop sending due to collision, and resend after random delay.



Broadcast Domain

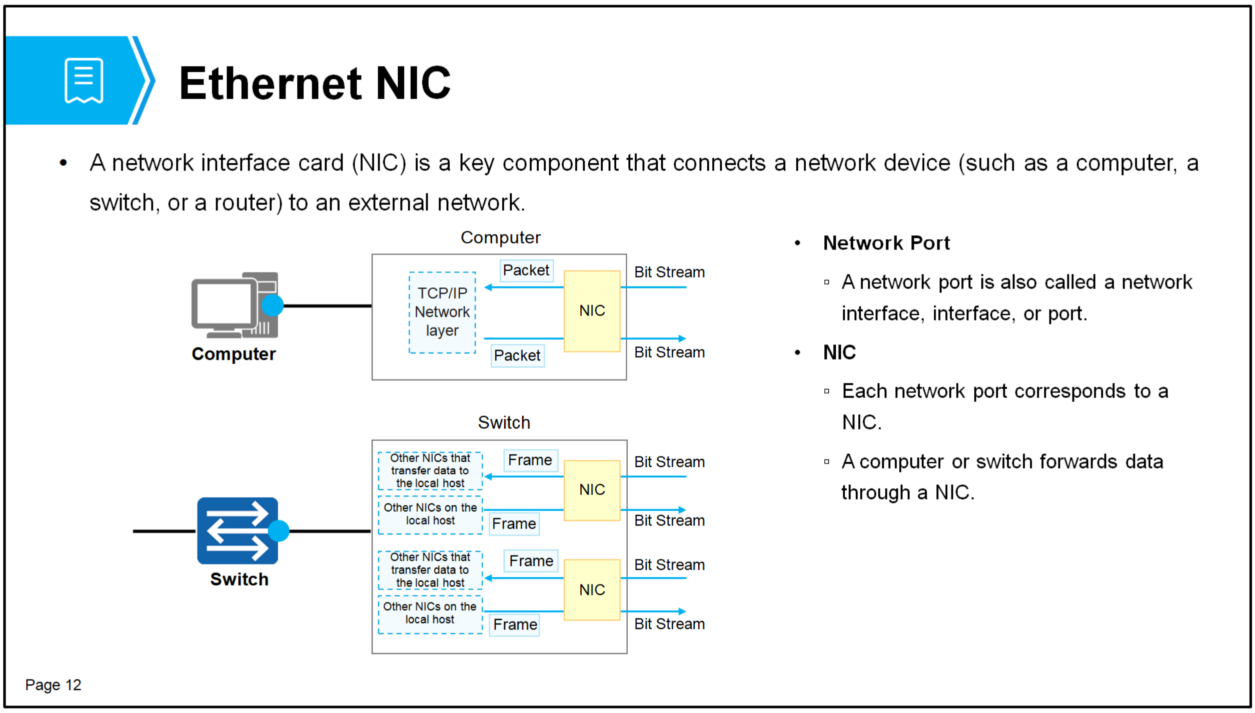
- The entire access scope of broadcast packets is called a Layer 2 broadcast domain, which is also called a broadcast domain. All hosts in the same broadcast domain can receive broadcast packets.

On a traditional Ethernet network, multiple nodes on the same medium share a link. The broadcast packets sent by a device can be received by all the other devices.

A switch forwards broadcast packets to all interfaces. Therefore, the nodes connected to all interfaces of the switch belong to the same broadcast domain.

- An all-1 MAC address (FF-FF-FF-FF-FF-FF) is a broadcast address. All nodes process data frames with the destination address being a broadcast address. The entire access range of the data frames is called a Layer 2 broadcast domain, which is also called a broadcast domain.

- Note that a MAC address uniquely identifies a network interface card (NIC). Each network adapter requires a unique MAC address.



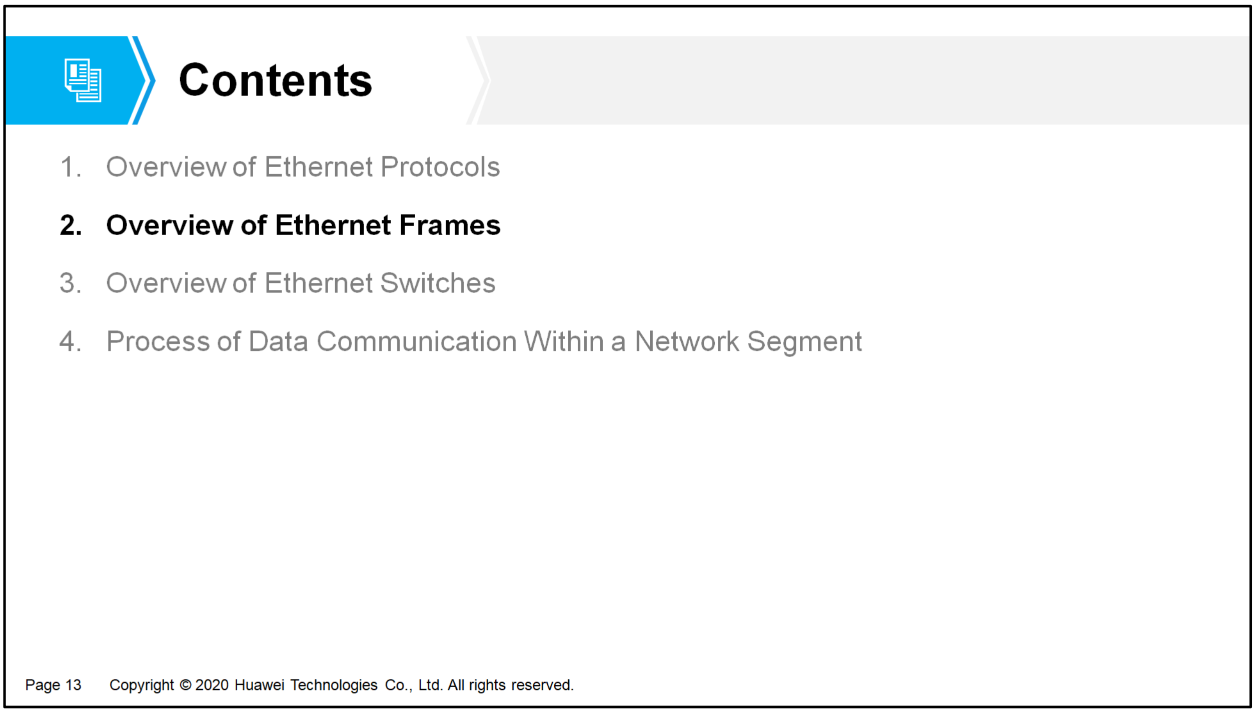
Ethernet NIC

- A network interface card (NIC) is a key component that connects a network device (such as a computer, a switch, or a router) to an external network.

Computer
Packet
TCP/IP Network layer
NIC
Bit Stream
Packet
Bit Stream
Computer
Switch
Other NICs that transfer data to the local host
Frame
NIC
Bit Stream
Other NICs on the local host
Frame
Bit Stream
Other NICs that transfer data to the local host
Frame
Bit Stream
NIC
Other NICs on the local host
Frame
Bit Stream
Switch

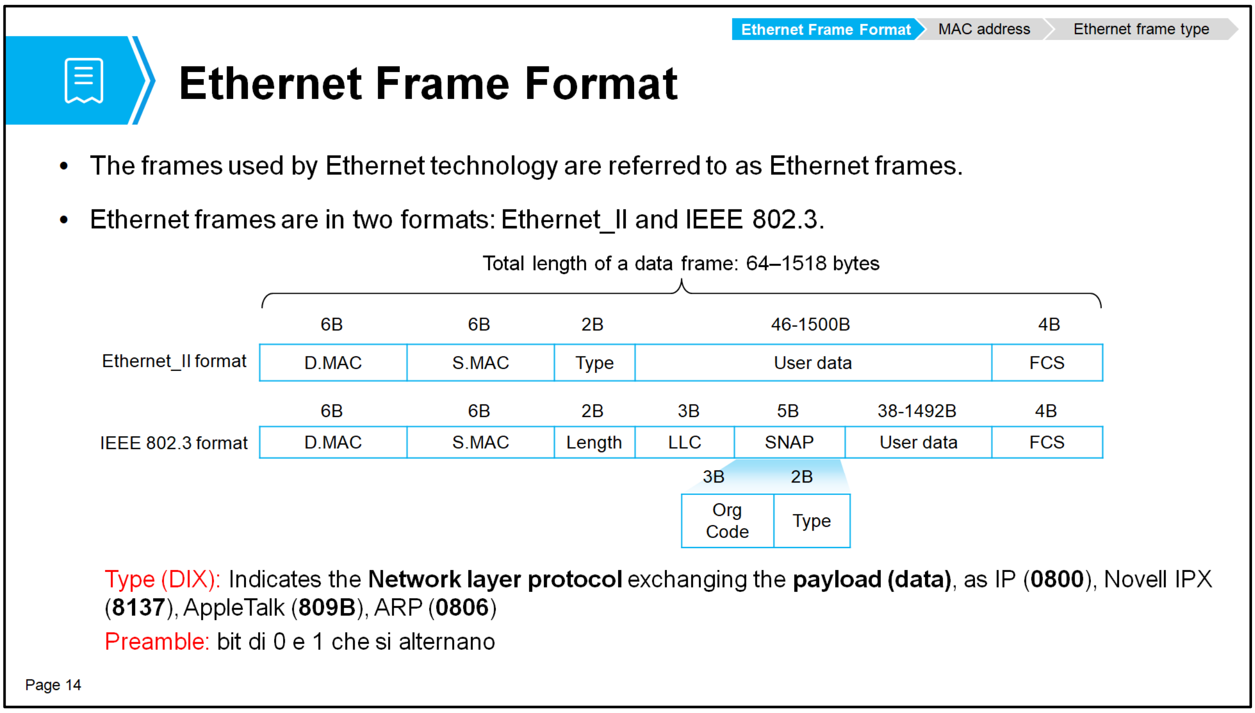
- **Network Port**
  - A network port is also called a network interface, interface, or port.
- **NIC**
  - Each network port corresponds to a NIC.
  - A computer or switch forwards data through a NIC.

- There are many types of NICs. In this document, all the NICs mentioned are Ethernet NICs.
- The switches mentioned in this document are Ethernet switches. The NICs used by each network port on a switch are Ethernet NICs.



Contents

1. Overview of Ethernet Protocols
2. **Overview of Ethernet Frames**
3. Overview of Ethernet Switches
4. Process of Data Communication Within a Network Segment



Ethernet Frame Format > MAC address > Ethernet frame type

Ethernet Frame Format

- The frames used by Ethernet technology are referred to as Ethernet frames.
- Ethernet frames are in two formats: Ethernet_II and IEEE 802.3.

Total length of a data frame: 64–1518 bytes

	6B	6B	2B	46-1500B	4B
Ethernet_II format	D.MAC	S.MAC	Type	User data	FCS

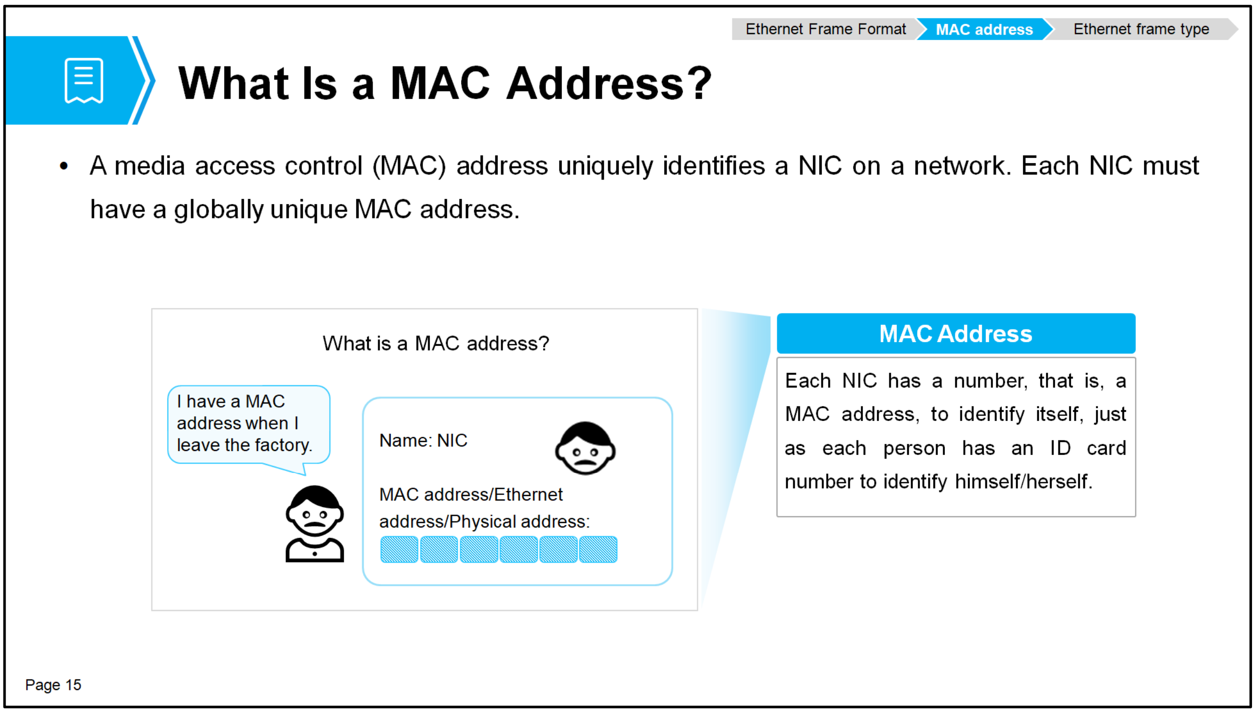
	6B	6B	2B	3B	5B	38-1492B	4B
IEEE 802.3 format	D.MAC	S.MAC	Length	LLC	SNAP	User data	FCS

3B	2B
Org Code	Type

Type (DIX): Indicates the **Network layer protocol** exchanging the **payload (data)**, as IP (**0800**), Novell IPX (**8137**), AppleTalk (**809B**), ARP (**0806**)

Preamble: bit di 0 e 1 che si alternano

- Frame is the unit of data that is transmitted between network nodes on an Ethernet network. Ethernet frames are in two formats, namely, Ethernet_II and IEEE 802.3, as illustrated in the figure shown in this slide.
- Ethernet II frame:
  - DMAC: 6 bytes, destination MAC address. This field identifies which MAC address should receive the frame.
  - SMAC: 6 bytes, source MAC address. This field identifies which MAC address should send the frame.
  - Type: 2 bytes, protocol type. Common values are as follows:
    - 0x0800: Internet Protocol Version 4 (IPv4)
    - 0x0806: Address Resolution Protocol (ARP)
- IEEE 802.3 LLC Ethernet frame:
  - Logical link control (LLC) consists of the destination service access point (DSAP), source service access point (SSAP), and Control field.
    - DSAP: 1 byte, destination service access point. If the subsequent type is IP, the value is set to 0x06. The function of a service access point is similar to the Type field in an Ethernet II frame or the port number in TCP/UDP.
    - SSAP: 1 byte, source service access point. If the subsequent type is IP, the value is set to 0x06.
    - Ctrl: 1 byte. This field is usually set to 0x03, indicating unnumbered IEEE 802.2 information of a connectionless service.
  - The Subnetwork Access Protocol (SNAP) field consists of the Org Code field and the Type field.
    - The three bytes of the Org Code field are all 0s.



Ethernet Frame Format › MAC address › Ethernet frame type

What Is a MAC Address?

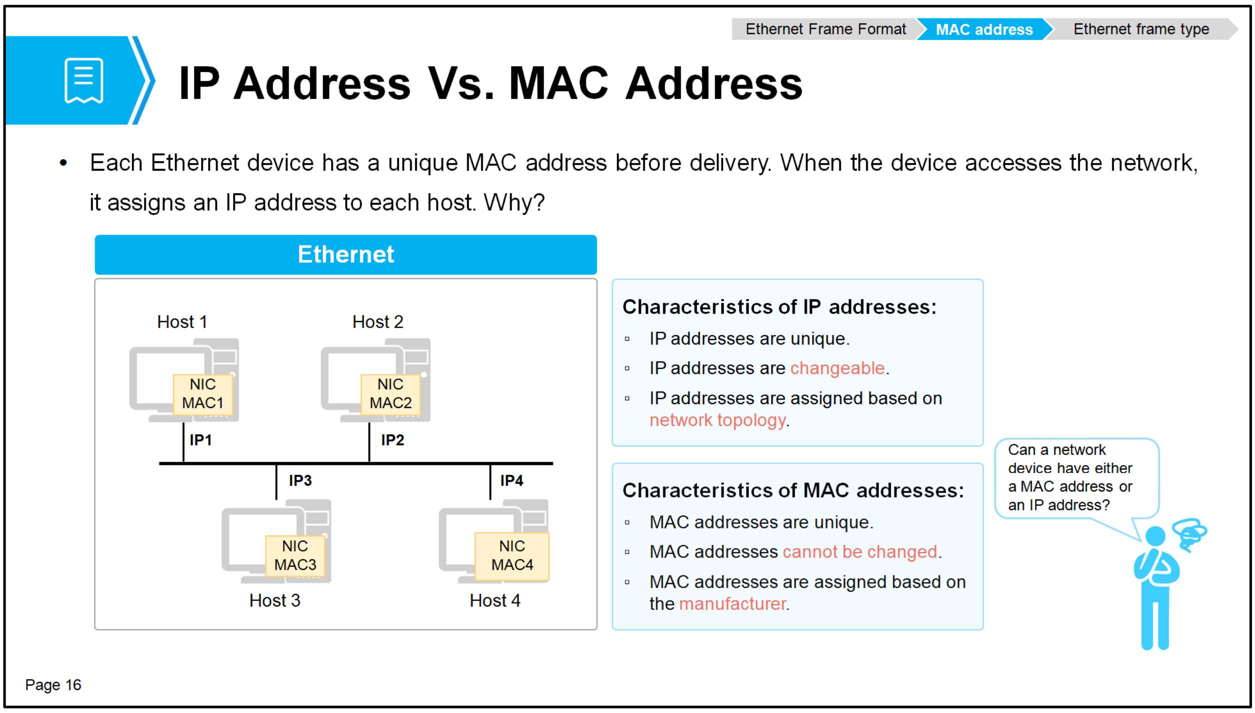
- A media access control (MAC) address uniquely identifies a NIC on a network. Each NIC must have a globally unique MAC address.

What is a MAC address?
I have a MAC address when I leave the factory.
Name: NIC
MAC address/Ethernet address/Physical address:

MAC Address

Each NIC has a number, that is, a MAC address, to identify itself, just as each person has an ID card number to identify himself/herself.

- A MAC address, as defined and standardized in IEEE 802, indicates the position of a network device. All Ethernet NICs that comply with the IEEE 802 standard must have a MAC address. The MAC address varies according to the NIC.



Ethernet Frame Format > MAC address > Ethernet frame type

IP Address Vs. MAC Address

- Each Ethernet device has a unique MAC address before delivery. When the device accesses the network, it assigns an IP address to each host. Why?

Characteristics of IP addresses:

- IP addresses are unique.
- IP addresses are changeable.
- IP addresses are assigned based on network topology.

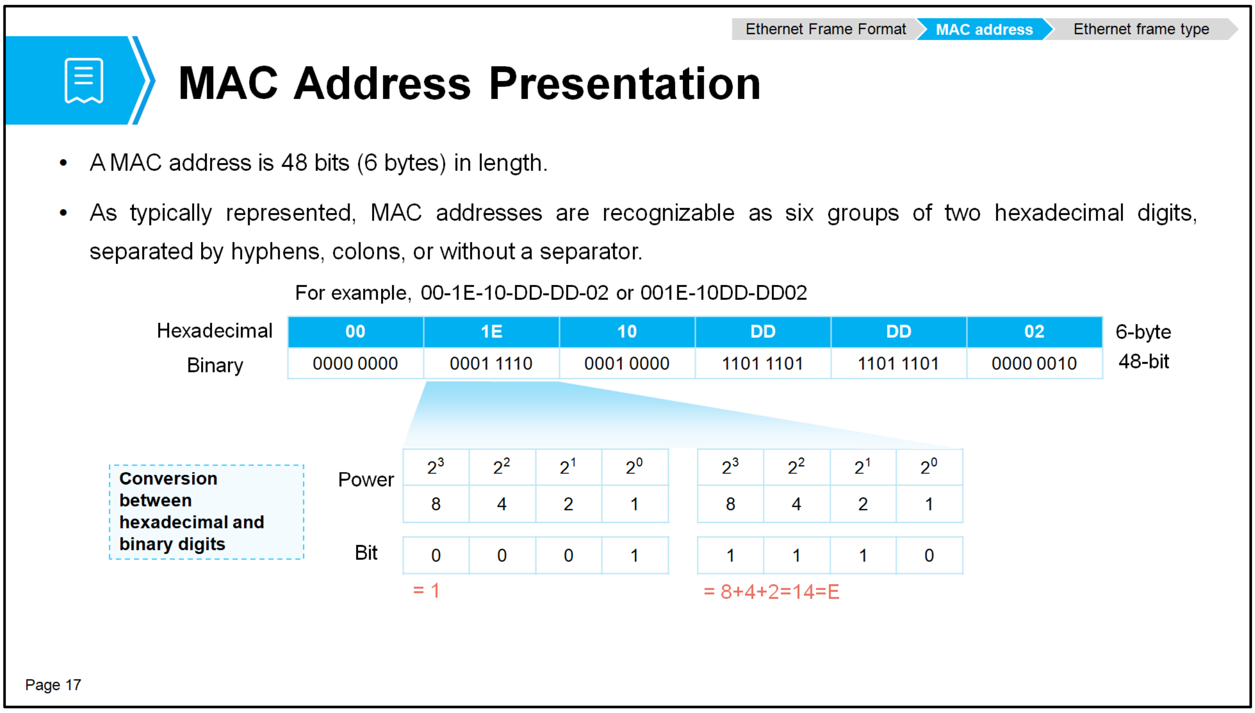
Characteristics of MAC addresses:

- MAC addresses are unique.
- MAC addresses cannot be changed.
- MAC addresses are assigned based on the manufacturer.

Can a network device have either a MAC address or an IP address?

Page 16

- Each Ethernet device has a unique MAC address before delivery. Then, why is an IP address assigned to each host? In other words, if each host is assigned a unique IP address, why does a unique MAC address need to be embedded in a network device (such as a NIC) during production?
- The main causes are as follows:
  - IP addresses are assigned based on the network topology, and MAC addresses are assigned based on the manufacturer. If route selection is based on the manufacturer, this solution is not feasible.
  - When two-layer addressing is used, devices are more flexible and easy to maintain.
    - For example, if an Ethernet NIC is faulty, you can replace it without changing its IP address. If an IP host is moved from one network to another, a new IP address can be assigned to the IP host with no need for replacing the NIC with a new one.
- Conclusion:
  - An IP address uniquely identifies a network node. Data on different network segments can be accessed using IP addresses.
  - A MAC address uniquely identifies a NIC. Data on a single network segment can be accessed using MAC addresses.



MAC Address Presentation

- A MAC address is 48 bits (6 bytes) in length.
- As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator.

For example, 00-1E-10-DD-DD-02 or 001E-10DD-DD02

Hexadecimal	00	1E	10	DD	DD	02	6-byte
Binary	0000 0000	0001 1110	0001 0000	1101 1101	1101 1101	0000 0010	48-bit

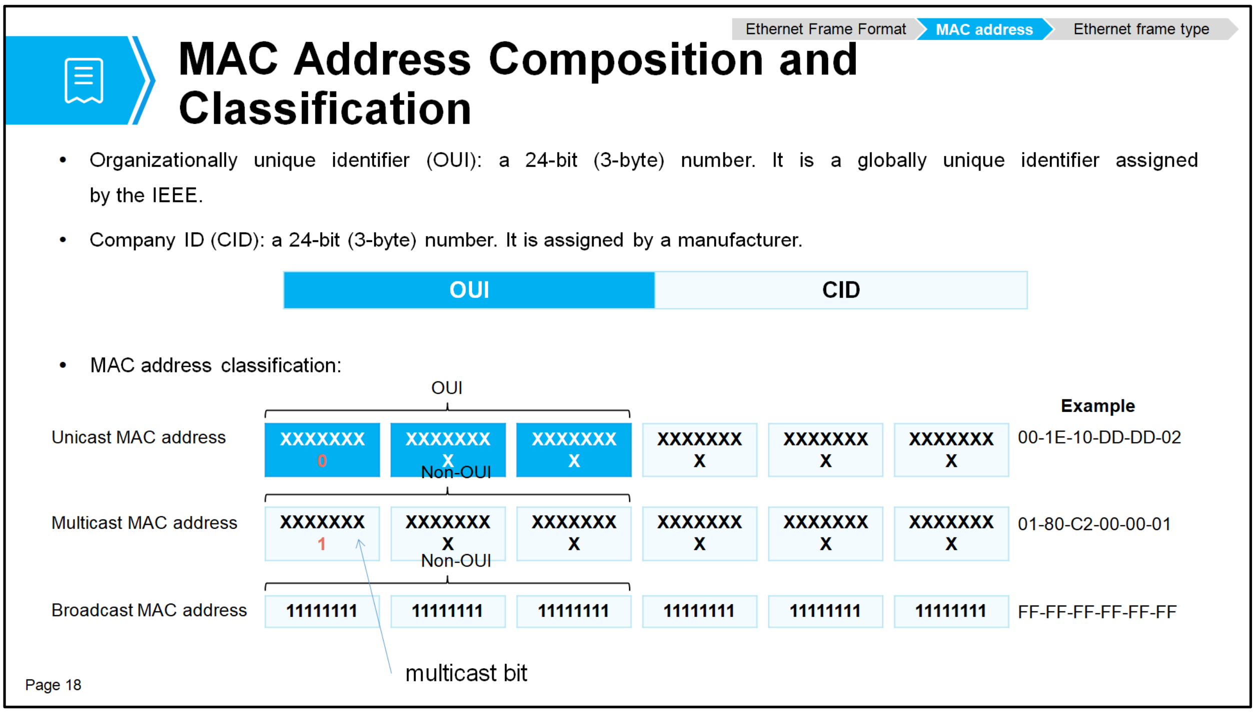
Conversion between hexadecimal and binary digits

Power	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
	8	4	2	1	8	4	2	1
Bit	0	0	0	1	1	1	1	0

= 1

= 8+4+2=14=E

- A MAC Address, which is 48 bits (6 bytes) in length, is a 12-digit hexadecimal number.



Ethernet Frame Format > MAC address > Ethernet frame type

MAC Address Composition and Classification

- Organizationally unique identifier (OUI): a 24-bit (3-byte) number. It is a globally unique identifier assigned by the IEEE.
- Company ID (CID): a 24-bit (3-byte) number. It is assigned by a manufacturer.

OUI	CID

- MAC address classification:

OUI

Non-OUI

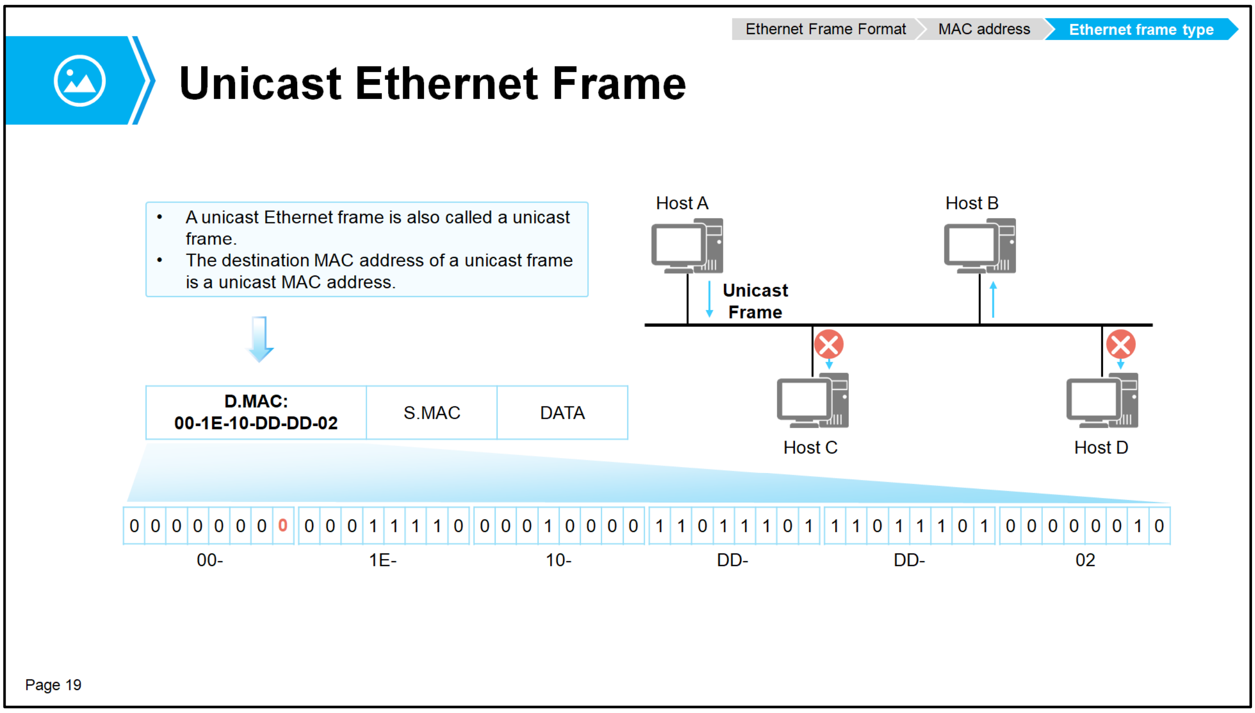
Non-OUI

							Example
Unicast MAC address	XXXXXXX 0	XXXXXXX X	XXXXXXX X	XXXXXXX X	XXXXXXX X	XXXXXXX X	00-1E-10-DD-DD-02
Multicast MAC address	XXXXXXX 1	XXXXXXX X	XXXXXXX X	XXXXXXX X	XXXXXXX X	XXXXXXX X	01-80-C2-00-00-01
Broadcast MAC address	11111111	11111111	11111111	11111111	11111111	11111111	FF-FF-FF-FF-FF-FF

multicast bit

Page 18

- A manufacturer must register with the IEEE to obtain a 24-bit (3-byte) vendor code, which is also called OUI, before producing a NIC.
- The last 24 bits are assigned by a vendor and uniquely identify a NIC produced by the vendor.
- MAC addresses fall into the following types:
  - Unicast MAC address: is also called the physical MAC address. A unicast MAC address uniquely identifies a terminal on an Ethernet network and is a globally unique hardware address.
    - A unicast MAC address identifies a single node on a link.
    - A frame whose destination MAC address is a unicast MAC address is sent to a single node.
    - A unicast MAC address can be used as either the source or destination address.
    - Note that unicast MAC addresses are globally unique. When two terminals with the same MAC address are connected to a Layer 2 network (for example, due to incorrect operations), a communication failure occurs (for example, the two terminals fail to communicate with each other). The communication between the two terminals and other devices may also fail.
  - Broadcast MAC address: an all-1 MAC address (FF-FF-FF-FF-FF-FF), which indicates all terminals on a LAN.
    - A broadcast MAC address can be considered as a special multicast MAC address.



Ethernet Frame Format > MAC address > Ethernet frame type

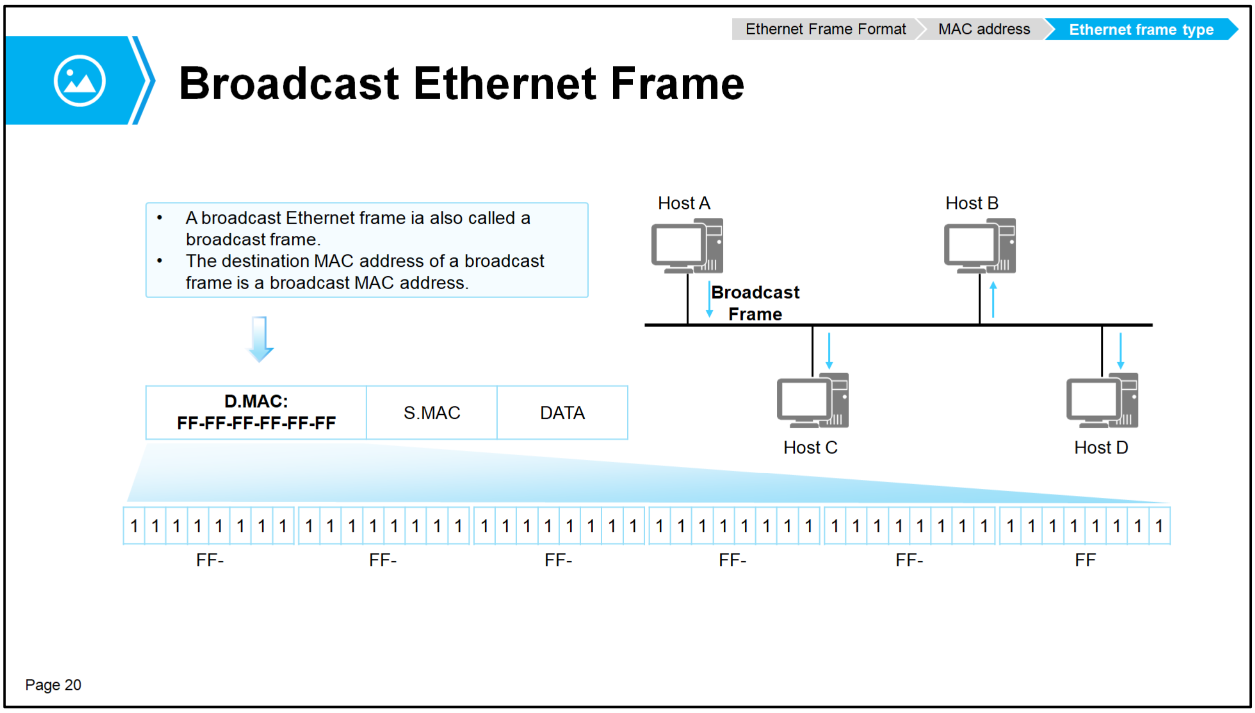
Unicast Ethernet Frame

- A unicast Ethernet frame is also called a unicast frame.
- The destination MAC address of a unicast frame is a unicast MAC address.

D.MAC: 00-1E-10-DD-DD-02	S.MAC	DATA

0 0 0 0 0 0 0 0	0 0 0 1 1 1 1 0	0 0 0 1 0 0 0 0	1 1 0 1 1 1 0 1	1 1 0 1 1 1 0 1	0 0 0 0 0 0 1 0
00-	1E-	10-	DD-	DD-	02

- Frames on a LAN can be sent in three modes: unicast, broadcast, and multicast.
- In unicast mode, frames are sent from a single source to a single destination.
  - Each host interface is uniquely identified by a MAC address. In the OUI of a MAC address, the eighth bit of the first byte indicates the address type. For a host MAC address, this bit is fixed at 0, indicating that all frames with this MAC address as the destination MAC address are sent to a unique destination.



Ethernet Frame Format › MAC address › **Ethernet frame type**

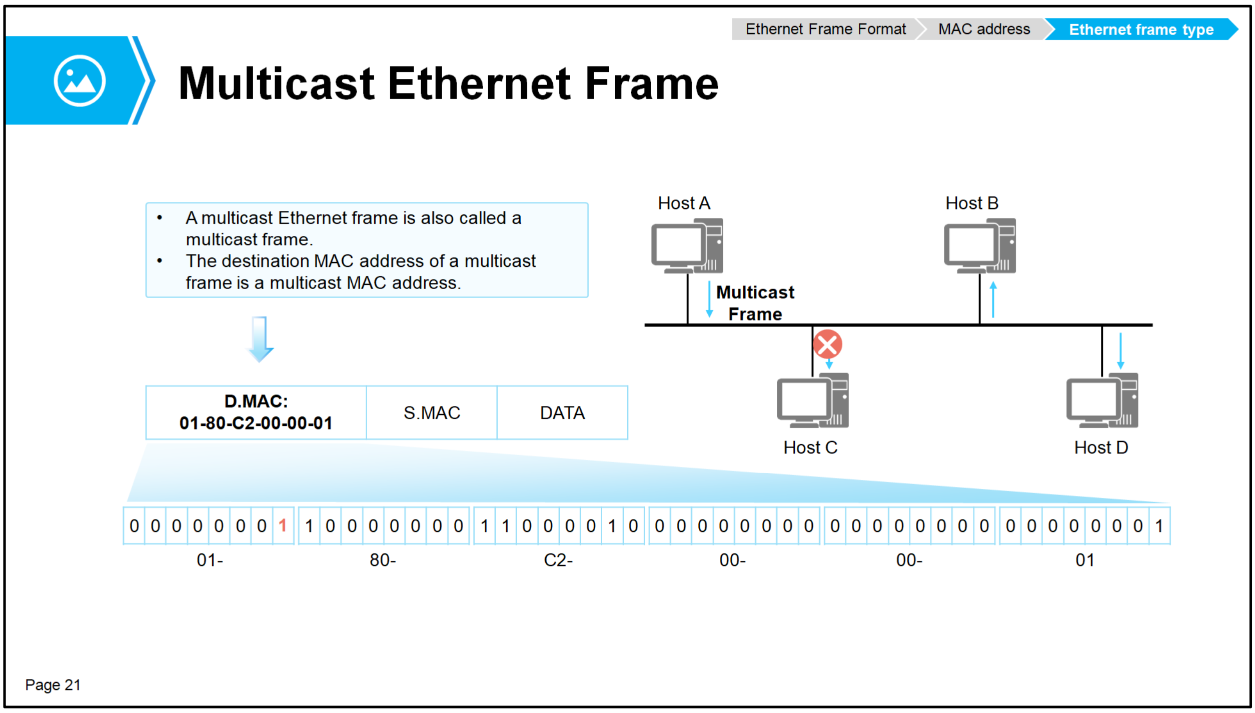
Broadcast Ethernet Frame

- A broadcast Ethernet frame ia also called a broadcast frame.
- The destination MAC address of a broadcast frame is a broadcast MAC address.

D.MAC: **FF-FF-FF-FF-FF-FF**	S.MAC	DATA

1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1
FF-	FF-	FF-	FF-	FF-	FF

- In broadcast mode, frames are sent from a single source to all hosts on the shared Ethernet.
  - The destination MAC address of a broadcast frame is a hexadecimal address in the format of FF-FF-FF-FF-FF-FF. All hosts that receive the broadcast frame must receive and process the frame.
  - In broadcast mode, a large amount of traffic is generated, which decreases the bandwidth utilization and affects the performance of the entire network.
  - The broadcast mode is usually used when all hosts on a network need to receive and process the same information.



Ethernet Frame Format | MAC address | **Ethernet frame type**

Multicast Ethernet Frame

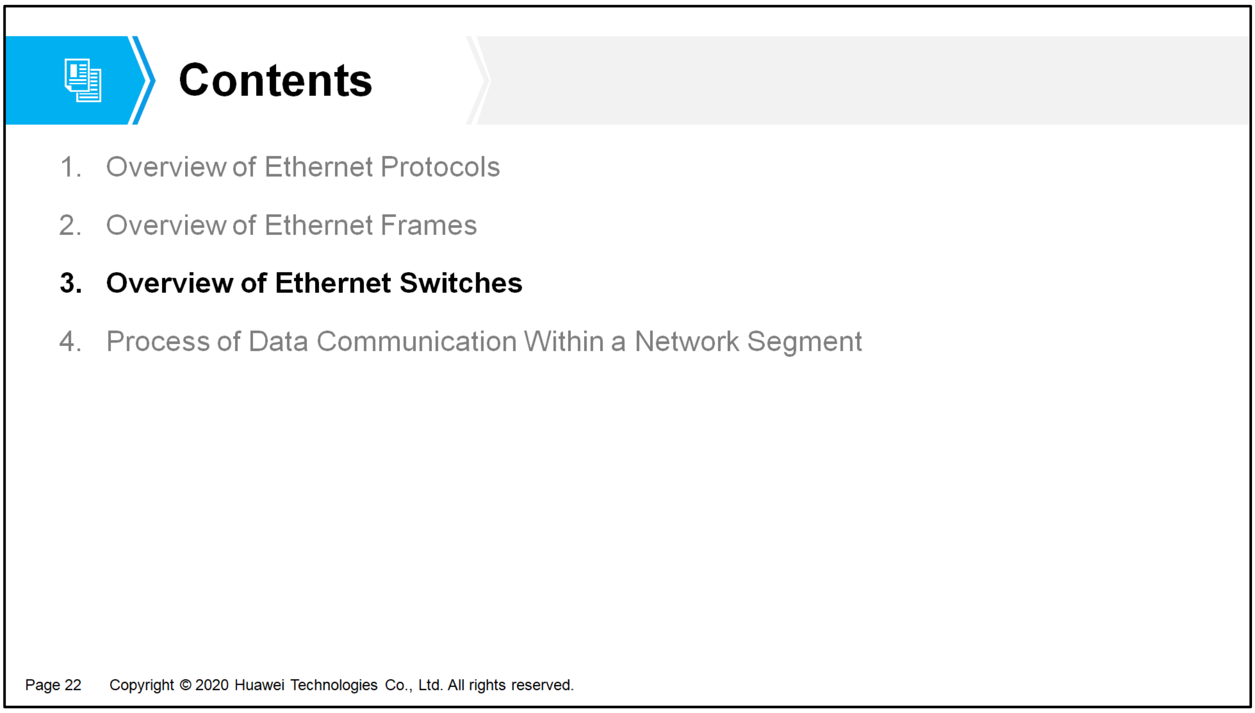
- A multicast Ethernet frame is also called a multicast frame.
- The destination MAC address of a multicast frame is a multicast MAC address.

D.MAC: **01-80-C2-00-00-01**	S.MAC	DATA

0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

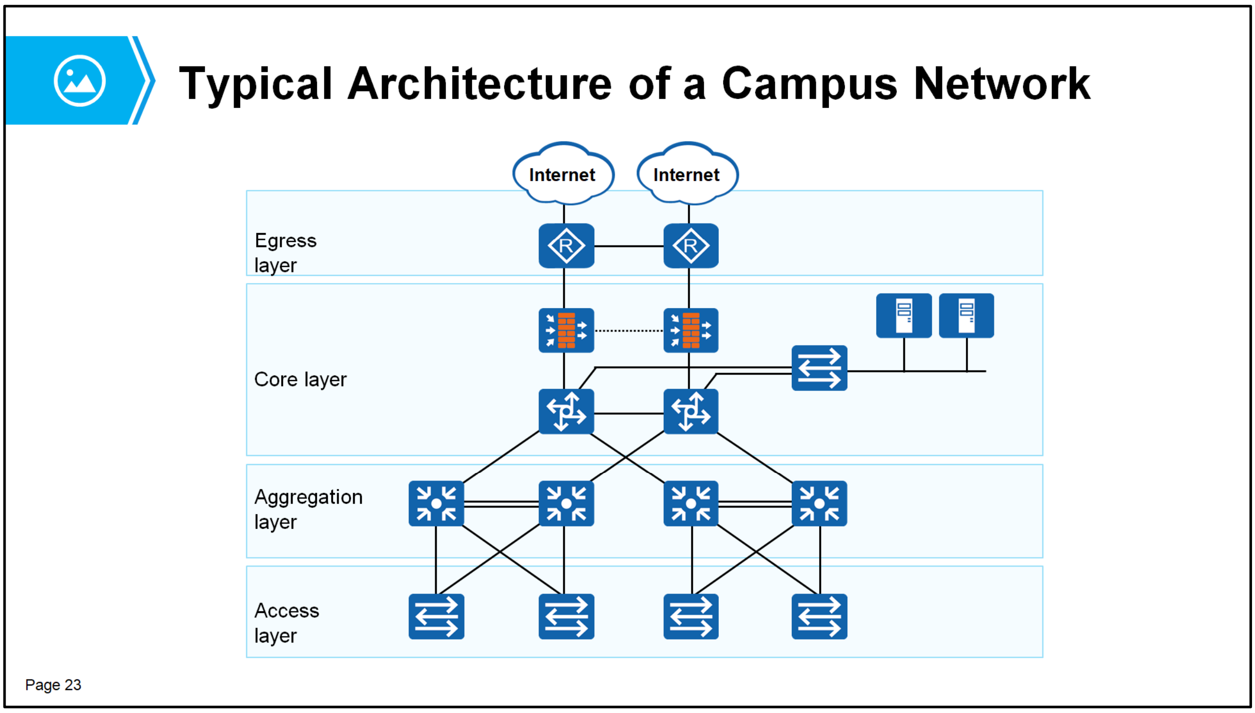
01- 80- C2- 00- 00- 01

- The multicast mode is more efficient than the broadcast mode.
  - Multicast forwarding can be considered as selective broadcast forwarding. Specifically, a host listens for a specific multicast address, and receives and processes frames whose destination MAC address is the multicast MAC address.
  - A multicast MAC address and a unicast MAC address are distinguished by the eighth bit in the first byte. The eighth bit of a multicast MAC address is 1.
  - The multicast mode is used when a group of hosts (not all hosts) on the network need to receive the same information and other hosts are not affected.



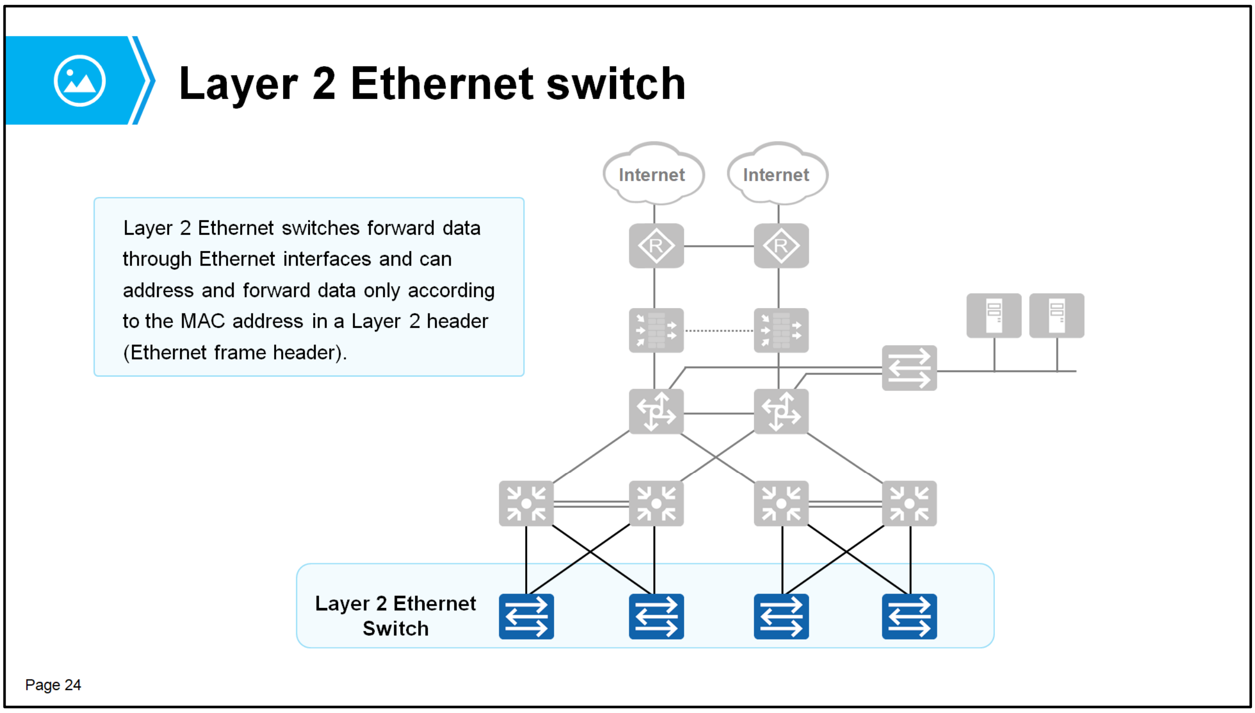
Contents

1. Overview of Ethernet Protocols
2. Overview of Ethernet Frames
3. **Overview of Ethernet Switches**
4. Process of Data Communication Within a Network Segment



Typical Architecture of a Campus Network

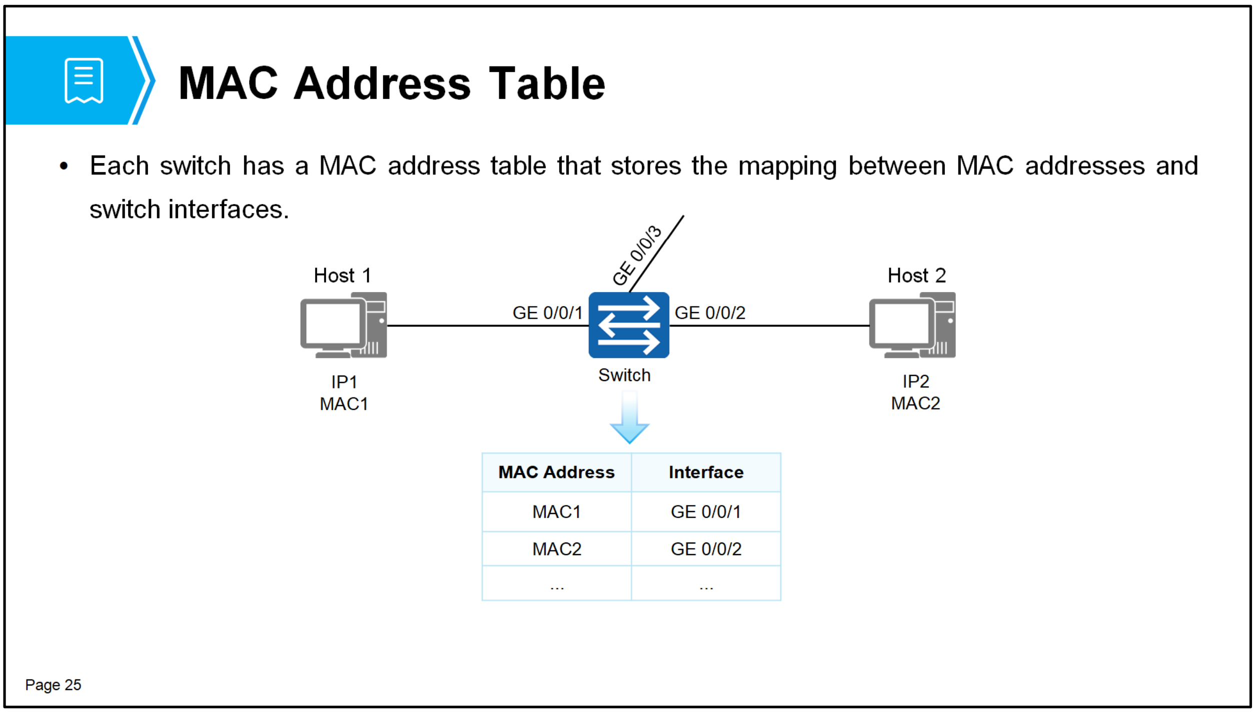
- A typical campus network consists of different devices, such as routers, switches, and firewalls. Generally, a campus network adopts the multi-layer architecture which includes the access layer, aggregation layer, core layer, and egress layer.



Layer 2 Ethernet switch

Layer 2 Ethernet switches forward data through Ethernet interfaces and can address and forward data only according to the MAC address in a Layer 2 header (Ethernet frame header).

- Layer 2 Ethernet switch:
  - On a campus network, a switch is the device closest to end users and is used to connect terminals to the campus network. Switches at the access layer are typically Layer 2 switches.
  - A Layer 2 switch works at the second layer of the TCP/IP model, which is the data link layer, and forwards data packets based on MAC addresses.
- Layer 3 Ethernet switch:
  - Routers are required to implement network communication between different LANs. As data communication networks expand and more services emerge on the networks, increasing traffic needs to be transmitted between networks. Routers cannot adapt to this development trend because of their high costs, low forwarding performance, and small interface quantities. New devices capable of high-speed Layer 3 forwarding are required. Layer 3 switches are such devices.
- Note that the switches involved in this course refer to Layer 2 Ethernet switches.

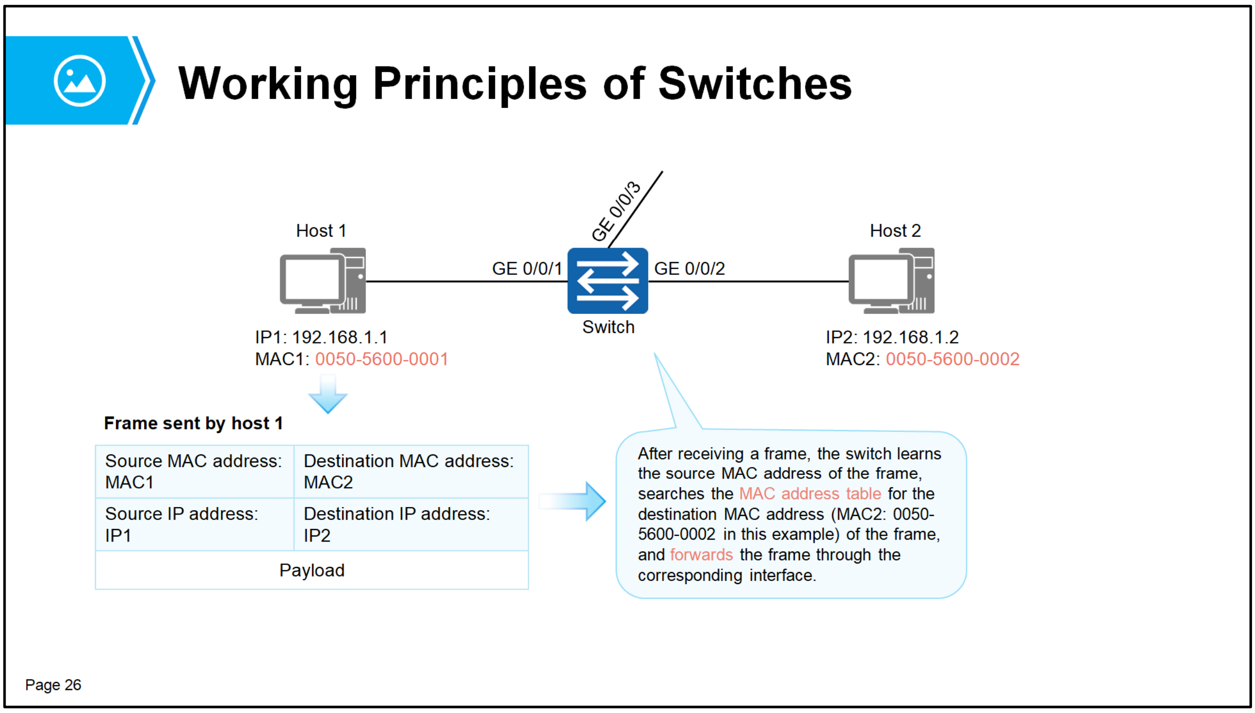


MAC Address Table

- Each switch has a MAC address table that stores the mapping between MAC addresses and switch interfaces.

MAC Address	Interface
MAC1	GE 0/0/1
MAC2	GE 0/0/2
...	...

- A MAC address table records the mapping between MAC addresses and interfaces of other devices learned by a switch. When forwarding a frame, the switch looks up the MAC address table based on the destination MAC address of the frame. If the MAC address table contains the entry corresponding to the destination MAC address of the frame, the frame is directly forwarded through the outbound interface in the entry. If the MAC address table does not contain the entry corresponding to the destination MAC address of the frame, the switch floods the frame on all interfaces except the interface that receives the frame.



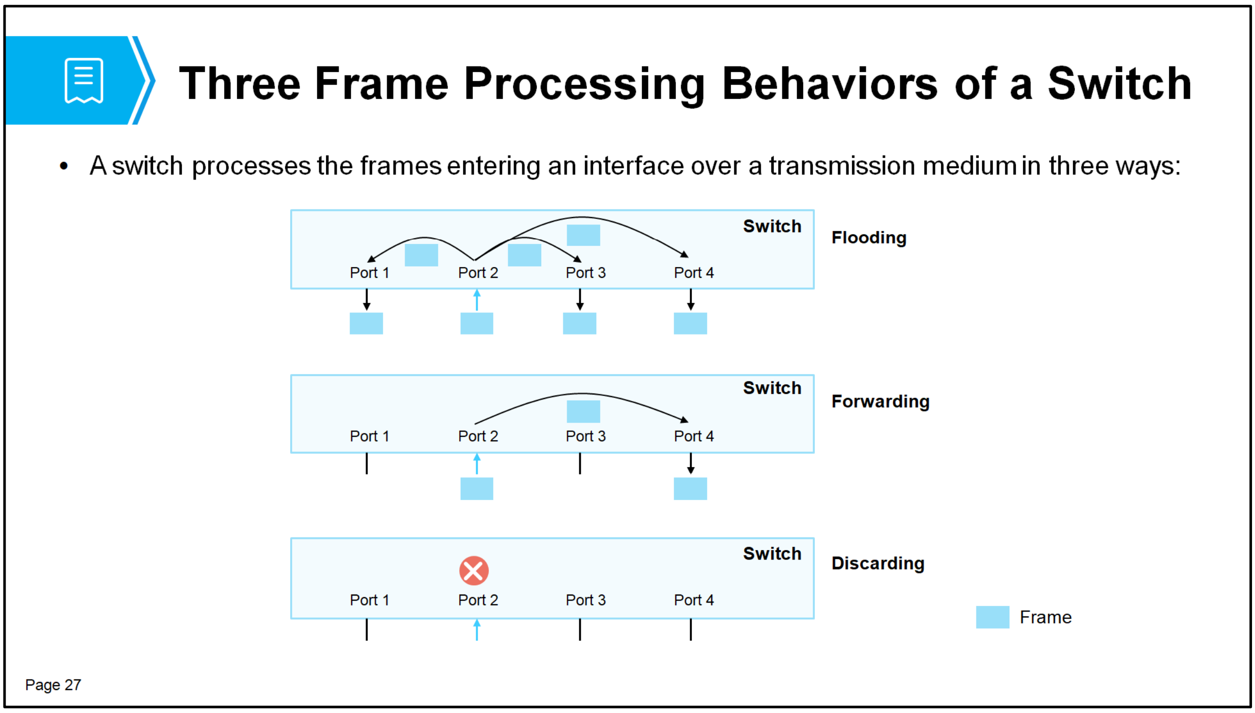
Working Principles of Switches

Frame sent by host 1

Source MAC address: MAC1	Destination MAC address: MAC2
Source IP address: IP1	Destination IP address: IP2
Payload	

After receiving a frame, the switch learns the source MAC address of the frame, searches the MAC address table for the destination MAC address (MAC2: 0050-5600-0002 in this example) of the frame, and forwards the frame through the corresponding interface.

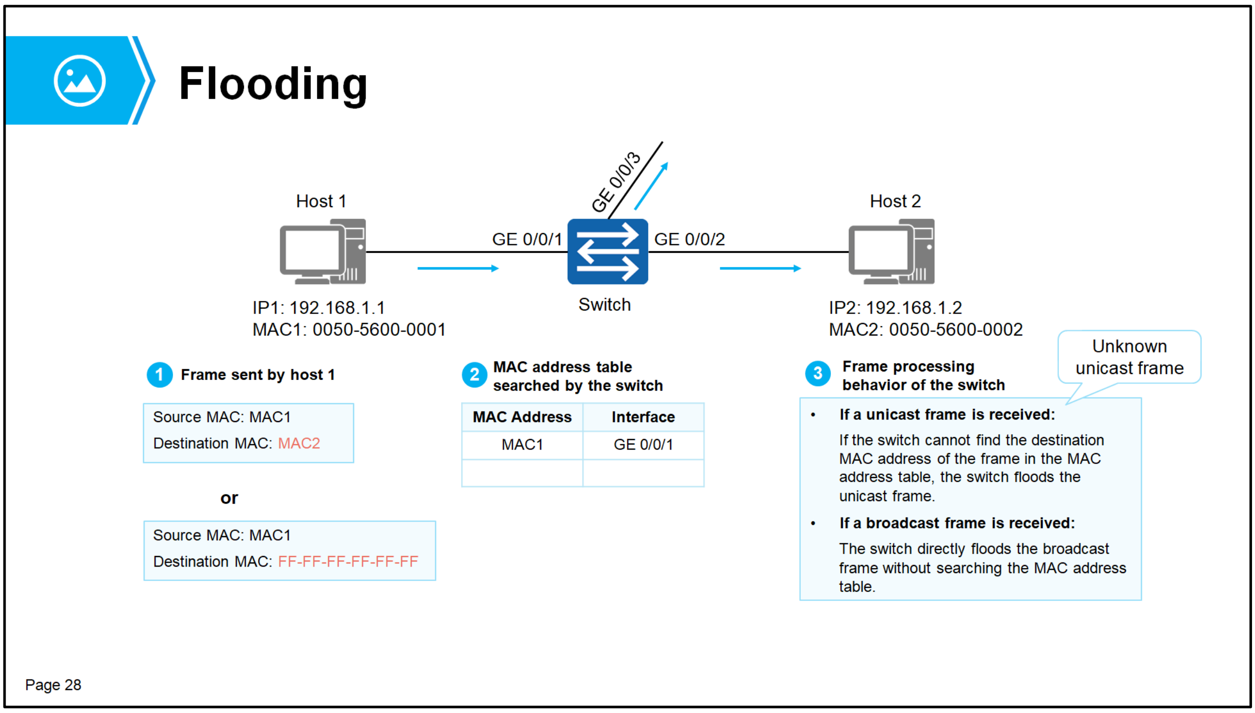
- Layer 2 switches work at the data link layer and forward frames based on MAC addresses. Switch interfaces used to send and receive data are independent of each other. Each interface belongs to a different collision domain, which effectively isolates collision domains on the network.
- Layer 2 switches maintain the mapping between MAC addresses and interfaces by learning the source MAC addresses of Ethernet frames. The table that stores the mapping between MAC addresses and interfaces is called a MAC address table. Layer 2 switches look up the MAC address table to determine the interface to which frames are forwarded based on the destination MAC address.



Three Frame Processing Behaviors of a Switch

- A switch processes the frames entering an interface over a transmission medium in three ways:

- A switch forwards each frame that enters an interface over a transmission medium. The basic function of a switch is to forward frames.
- A switch processes frames in three ways: flooding, forwarding, and discarding.
  - Flooding: The switch forwards the frames received from an interface to all other interfaces.
  - Forwarding: The switch forwards the frames received from an interface to another interface.
  - Discarding: The switch discards the frames received from an interface.



Flooding

1 **Frame sent by host 1**

Source MAC: MAC1
Destination MAC: MAC2

or

Source MAC: MAC1
Destination MAC: FF-FF-FF-FF-FF-FF

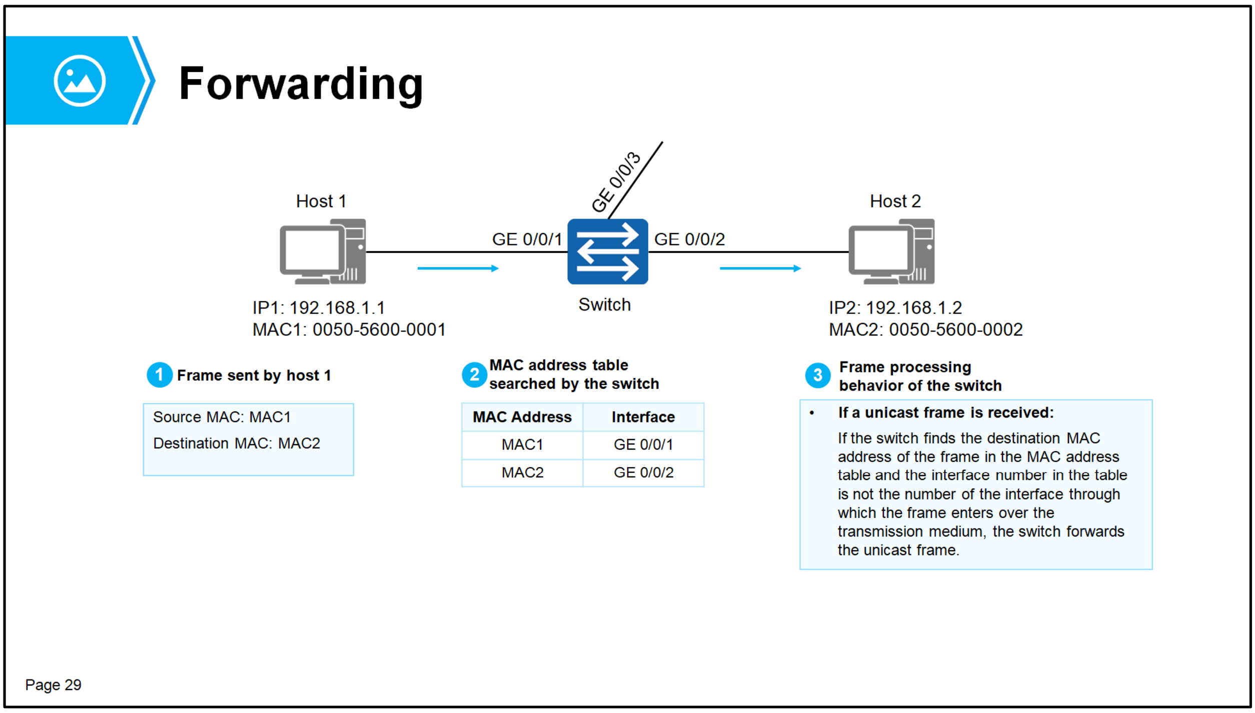
2 **MAC address table searched by the switch**

MAC Address	Interface
MAC1	GE 0/0/1

3 **Frame processing behavior of the switch**

- **If a unicast frame is received:**
  If the switch cannot find the destination MAC address of the frame in the MAC address table, the switch floods the unicast frame.
- **If a broadcast frame is received:**
  The switch directly floods the broadcast frame without searching the MAC address table.

- If a unicast frame enters a switch interface over a transmission medium, the switch searches the MAC address table for the destination MAC address of the frame. If the MAC address cannot be found, the switch floods the unicast frame.
- If a broadcast frame enters a switch interface over a transmission medium, the switch directly floods the broadcast frame instead of searching the MAC address table for the destination MAC address of the frame.
- As shown in this figure:
  - Scenario 1: Host 1 wants to access host 2 and sends a unicast frame to the switch. After receiving the unicast frame, the switch searches the MAC address table for the destination MAC address of the frame. If the destination MAC address does not exist in the table, the switch floods the frame.
  - Scenario 2: Host 1 wants to access host 2 but does not know the MAC address of host 2. Host 1 sends an ARP Request packet, which is a broadcast frame to the switch. The switch then floods the broadcast frame.



Forwarding

1 **Frame sent by host 1**

Source MAC: MAC1
Destination MAC: MAC2

2 **MAC address table searched by the switch**

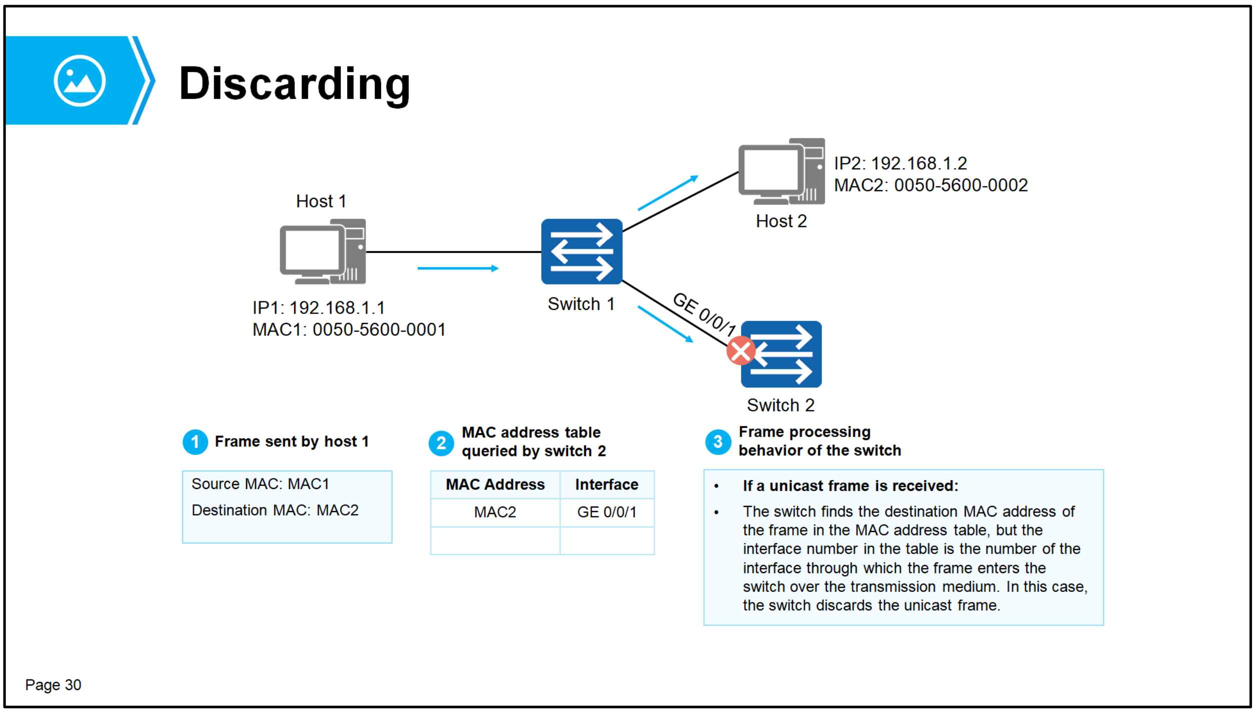
MAC Address	Interface
MAC1	GE 0/0/1
MAC2	GE 0/0/2

3 **Frame processing behavior of the switch**

- **If a unicast frame is received:**

  If the switch finds the destination MAC address of the frame in the MAC address table and the interface number in the table is not the number of the interface through which the frame enters over the transmission medium, the switch forwards the unicast frame.

- If a unicast frame enters a switch interface over a transmission medium, the switch searches the MAC address table for the destination MAC address of the frame. If the corresponding entry is found in the MAC address table, the switch checks whether the interface number corresponding to the destination MAC address is the number of the interface through which the frame enters the switch over the transmission medium. If not, the switch forwards the frame to the interface corresponding to the destination MAC address of the frame in the MAC address table. The frame is then sent out from this interface.
- As shown in this figure,
  - host 1 wants to access host 2 and sends a unicast frame to the switch. After receiving the unicast frame, the switch finds the corresponding entry in the MAC address table and forwards the frame in point-to-point mode.



Discarding

1 **Frame sent by host 1**

Source MAC: MAC1
Destination MAC: MAC2

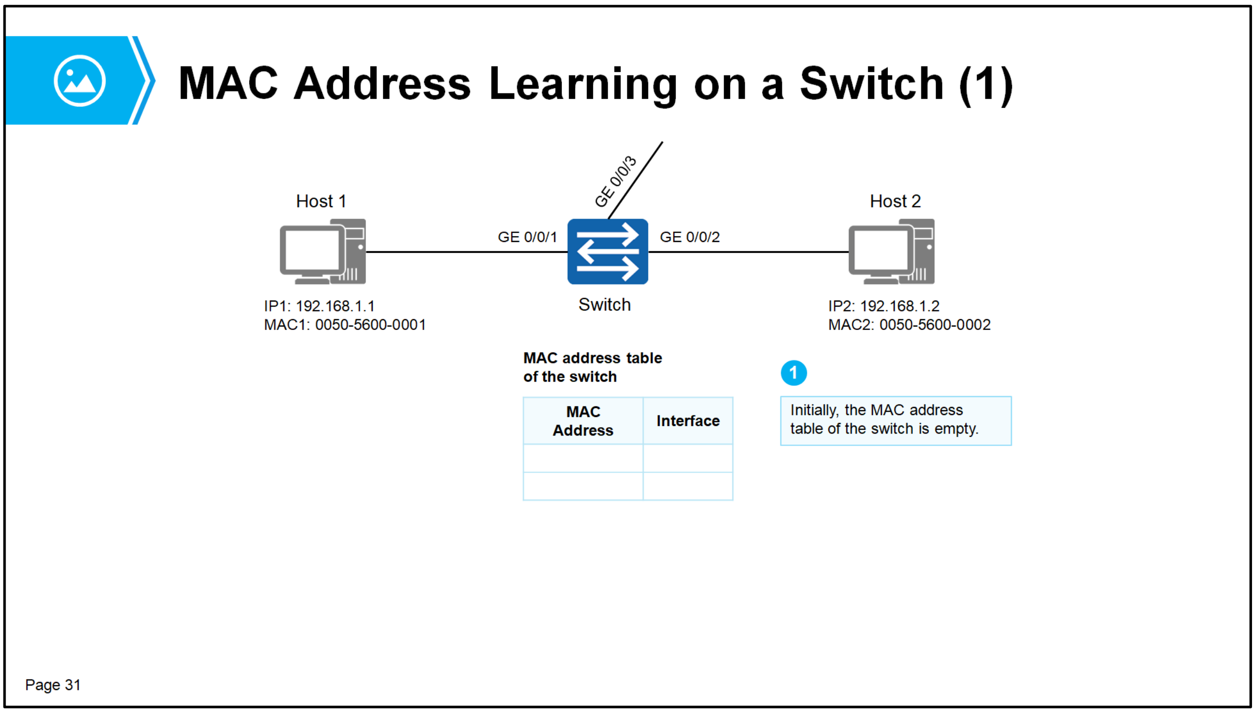
2 **MAC address table queried by switch 2**

MAC Address	Interface
MAC2	GE 0/0/1

3 **Frame processing behavior of the switch**

- **If a unicast frame is received:**
- The switch finds the destination MAC address of the frame in the MAC address table, but the interface number in the table is the number of the interface through which the frame enters the switch over the transmission medium. In this case, the switch discards the unicast frame.

- If a unicast frame enters a switch interface over a transmission medium, the switch searches the MAC address table for the destination MAC address of the frame. If the corresponding entry is found in the MAC address table, the switch checks whether the interface number corresponding to the destination MAC address in the MAC address table is the number of the interface through which the frame enters the switch over the transmission medium. If yes, the switch discards the frame.
- As shown in this figure:
    - Host 1 wants to access host 2 and sends a unicast frame to switch 1. After receiving the unicast frame, switch 1 searches the MAC address table for the destination MAC address of the frame. If the destination MAC address does not exist in the table, switch 1 floods the frame.
    - After receiving the frame, switch 2 finds that the interface corresponding to the destination MAC address is the interface that receives the frame. In this case, switch 2 discards the frame.



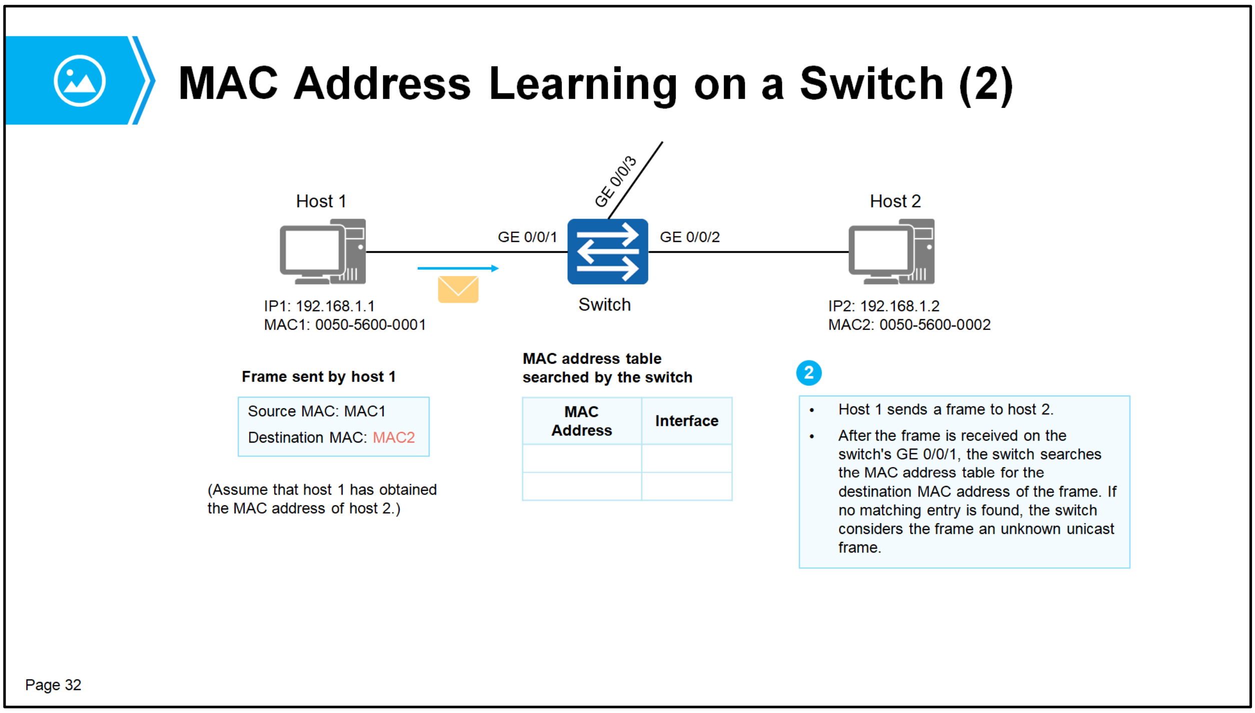
MAC Address Learning on a Switch (1)

MAC address table of the switch

MAC Address	Interface

1 Initially, the MAC address table of the switch is empty.

- In the initial state, a switch does not know the MAC address of a connected host. Therefore, the MAC address table is empty.



MAC Address Learning on a Switch (2)

Frame sent by host 1

Source MAC: MAC1

Destination MAC: MAC2

(Assume that host 1 has obtained the MAC address of host 2.)

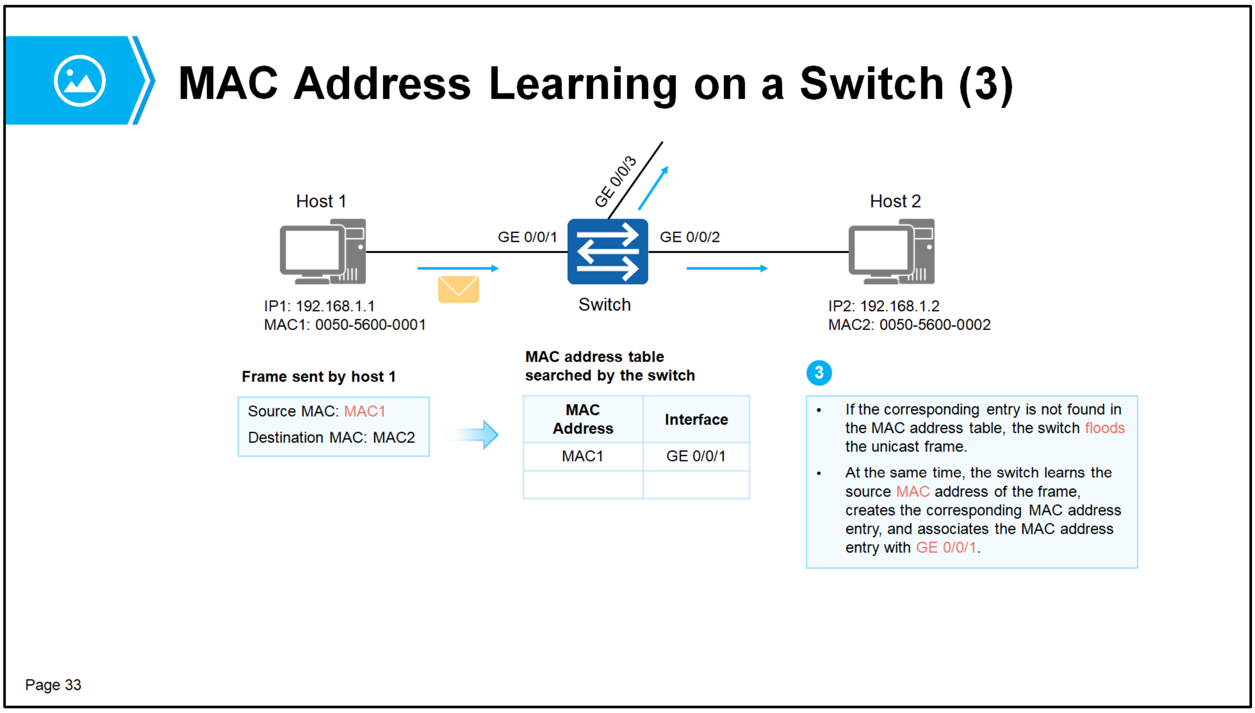
MAC address table searched by the switch

MAC Address	Interface

2

- Host 1 sends a frame to host 2.
- After the frame is received on the switch's GE 0/0/1, the switch searches the MAC address table for the destination MAC address of the frame. If no matching entry is found, the switch considers the frame an unknown unicast frame.

- If host 1 wants to send data to host 2 (assume that host 1 has obtained the IP address and MAC address of host 2), host 1 encapsulates the frame with its own source IP address and source MAC address.
- After receiving the frame, the switch searches its own MAC address table. If no matching entry is found in the table, the switch considers the frame an unknown unicast frame.



MAC Address Learning on a Switch (3)

Host 1

IP1: 192.168.1.1
MAC1: 0050-5600-0001

GE 0/0/1

Switch

GE 0/0/3

GE 0/0/2

Host 2

IP2: 192.168.1.2
MAC2: 0050-5600-0002

Frame sent by host 1

Source MAC: MAC1
Destination MAC: MAC2

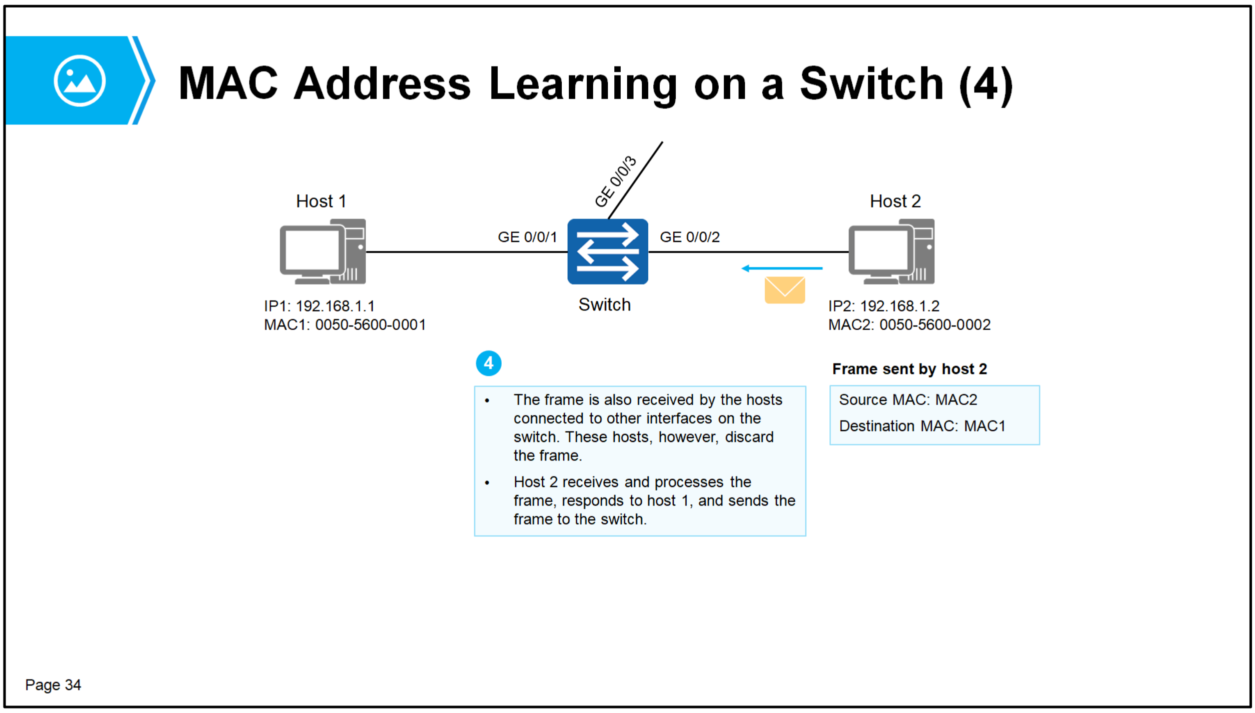
MAC address table searched by the switch

MAC Address	Interface
MAC1	GE 0/0/1

3

- If the corresponding entry is not found in the MAC address table, the switch floods the unicast frame.
- At the same time, the switch learns the source MAC address of the frame, creates the corresponding MAC address entry, and associates the MAC address entry with GE 0/0/1.

- The switch floods the received frame because it is an unknown unicast frame.
- In addition, the switch records the source MAC address and interface number of the received frame in the MAC address table.
- Note that the dynamically learned entries in a MAC address table are not always valid. Each entry has a lifespan. If an entry is not updated within the lifespan, the entry will be deleted. This lifespan is called the aging time. For example, the default aging time of Huawei S series switches is 300s.



MAC Address Learning on a Switch (4)

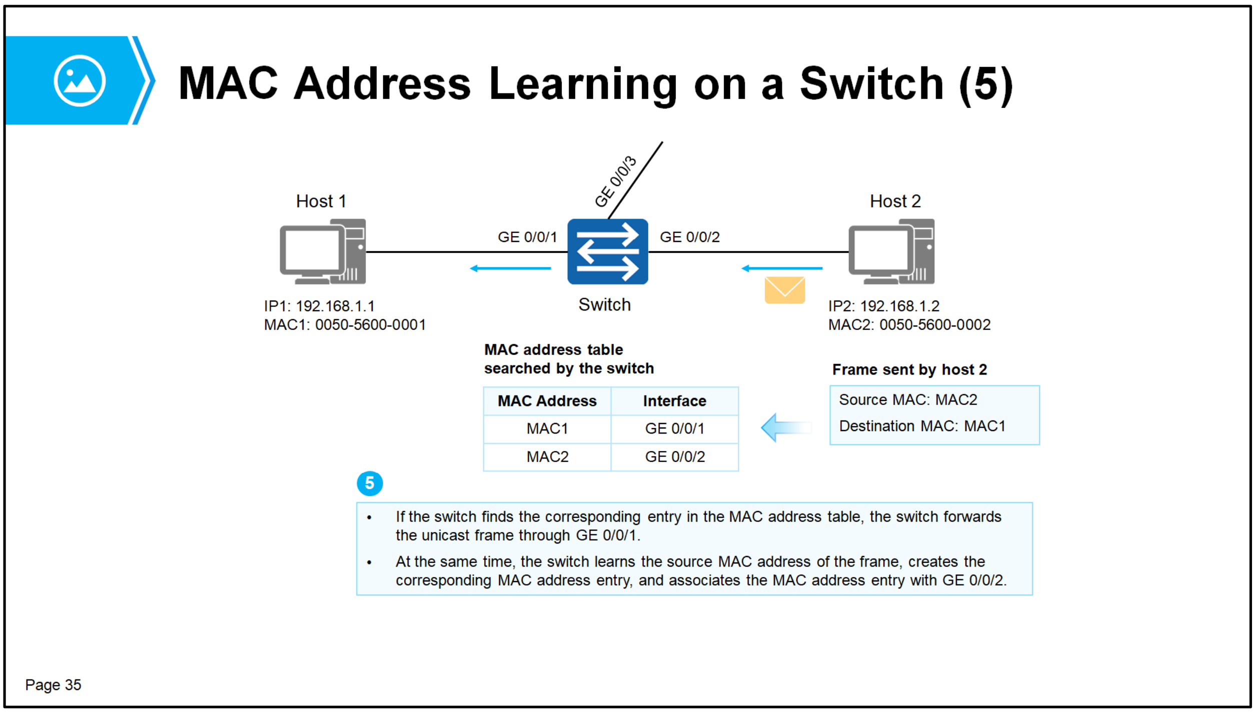
- The frame is also received by the hosts connected to other interfaces on the switch. These hosts, however, discard the frame.
- Host 2 receives and processes the frame, responds to host 1, and sends the frame to the switch.

Frame sent by host 2

Source MAC: MAC2

Destination MAC: MAC1

- All hosts on a broadcast network receive the frame, but only host 2 processes the frame because the destination MAC address is the MAC address of host 2.
- Host 2 sends a reply frame, which is also a unicast data frame, to host 1.



MAC Address Learning on a Switch (5)

MAC address table searched by the switch

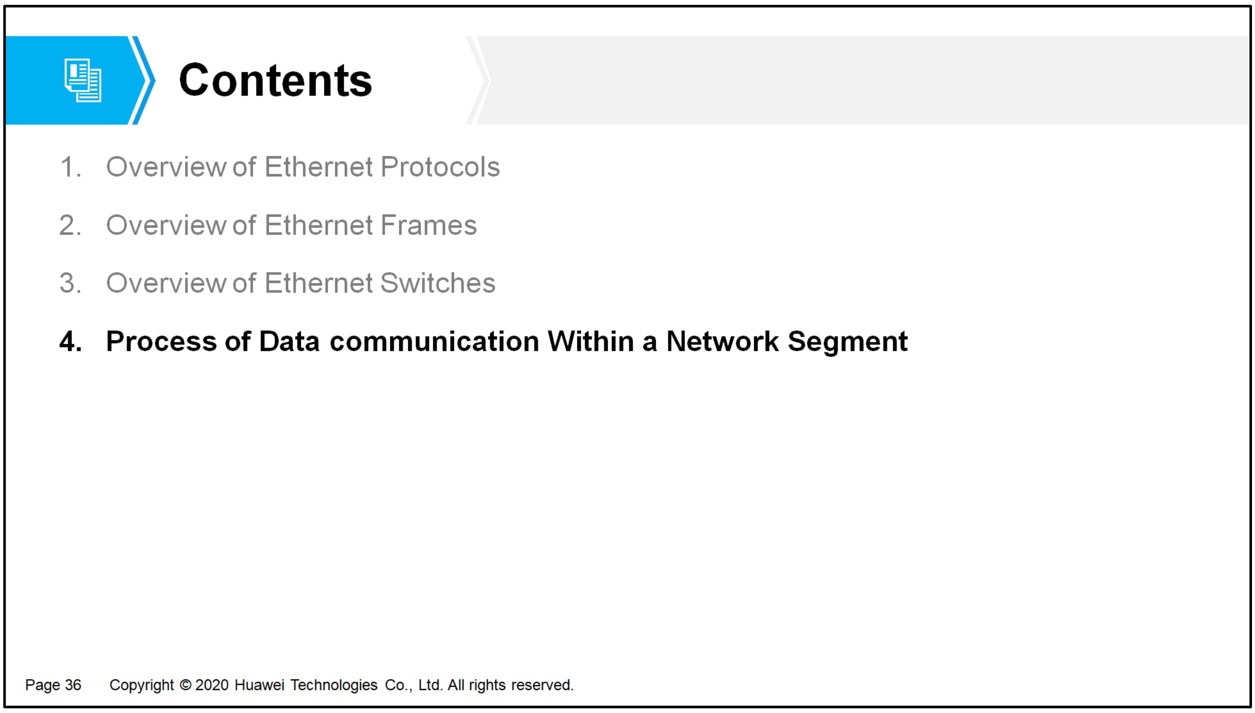
MAC Address	Interface
MAC1	GE 0/0/1
MAC2	GE 0/0/2

Frame sent by host 2

Source MAC: MAC2
Destination MAC: MAC1

- If the switch finds the corresponding entry in the MAC address table, the switch forwards the unicast frame through GE 0/0/1.
- At the same time, the switch learns the source MAC address of the frame, creates the corresponding MAC address entry, and associates the MAC address entry with GE 0/0/2.

- After receiving the unicast frame, the switch checks its MAC address table. If a matching entry is found, the switch forwards the frame through the corresponding interface.
- In addition, the switch records the source MAC address and interface number of the received frame in the MAC address table.

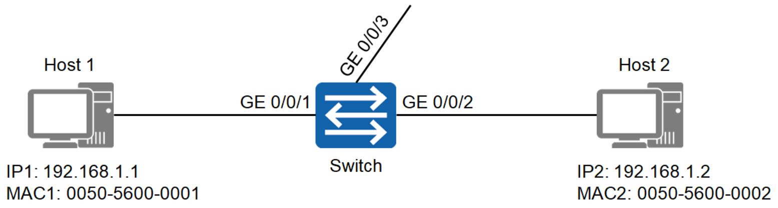


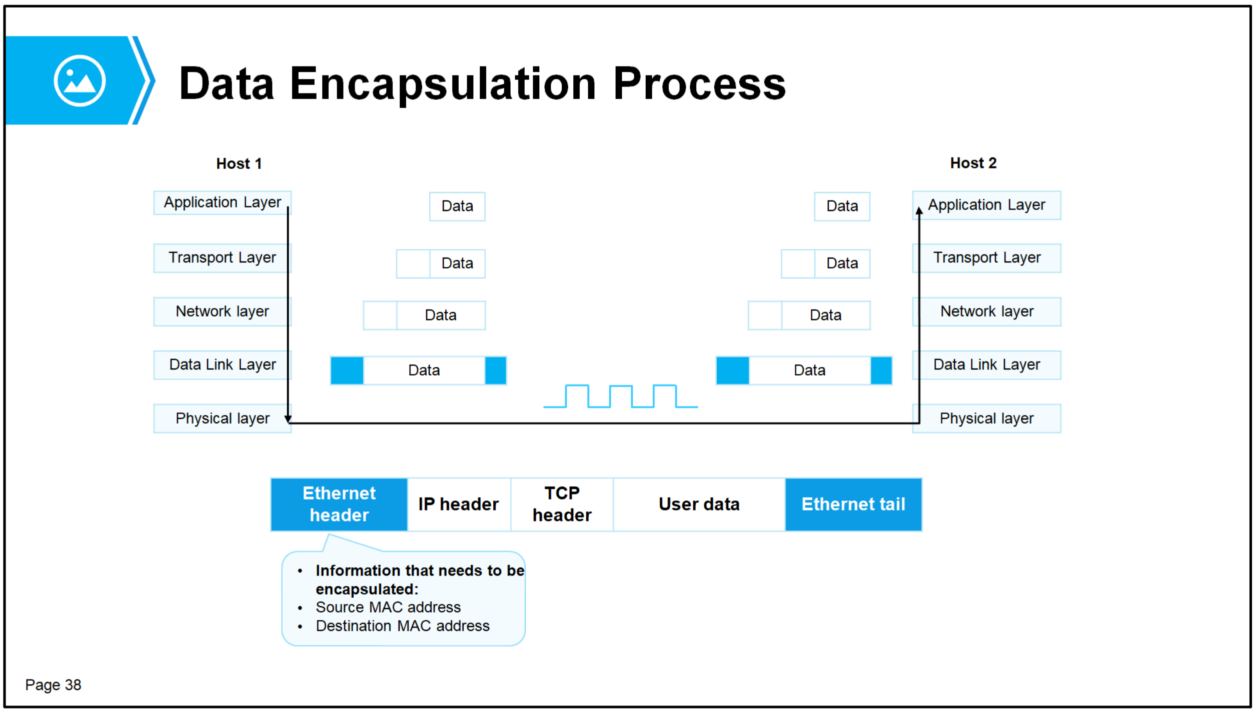
Contents

1. Overview of Ethernet Protocols
2. Overview of Ethernet Frames
3. Overview of Ethernet Switches
4. **Process of Data communication Within a Network Segment**

Process of Data Communication Within a Network Segment

- Scenario description:
  - Task: Host 1 wants to access host 2.
  - Host: The host is in the initialized state and only knows its own IP address and MAC address (assume that the IP address of the peer host has been obtained).
  - Switch: The switch is just powered on and in the initialized state.



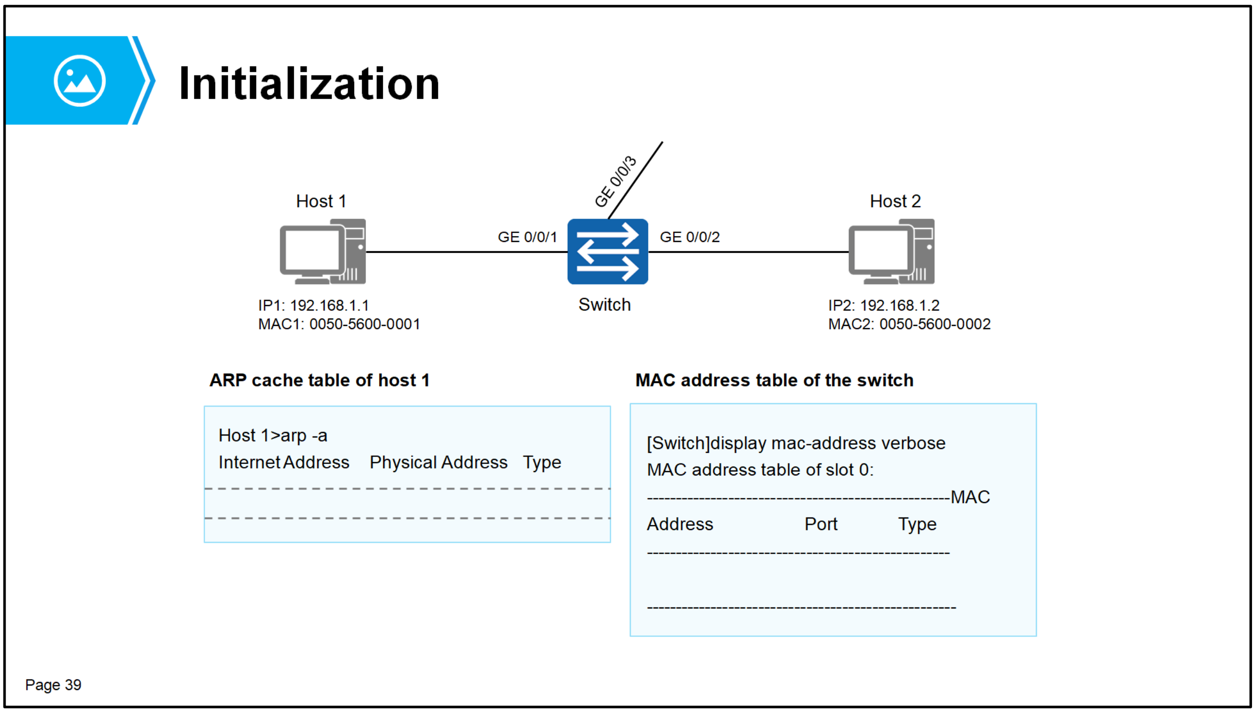


Data Encapsulation Process

Ethernet header	IP header	TCP header	User data	Ethernet tail

- **Information that needs to be encapsulated:**
- Source MAC address
- Destination MAC address

- Before sending a packet, host 1 needs to encapsulate information, including the source and destination IP addresses and the source and destination MAC addresses, into the packet.



Initialization

ARP cache table of host 1

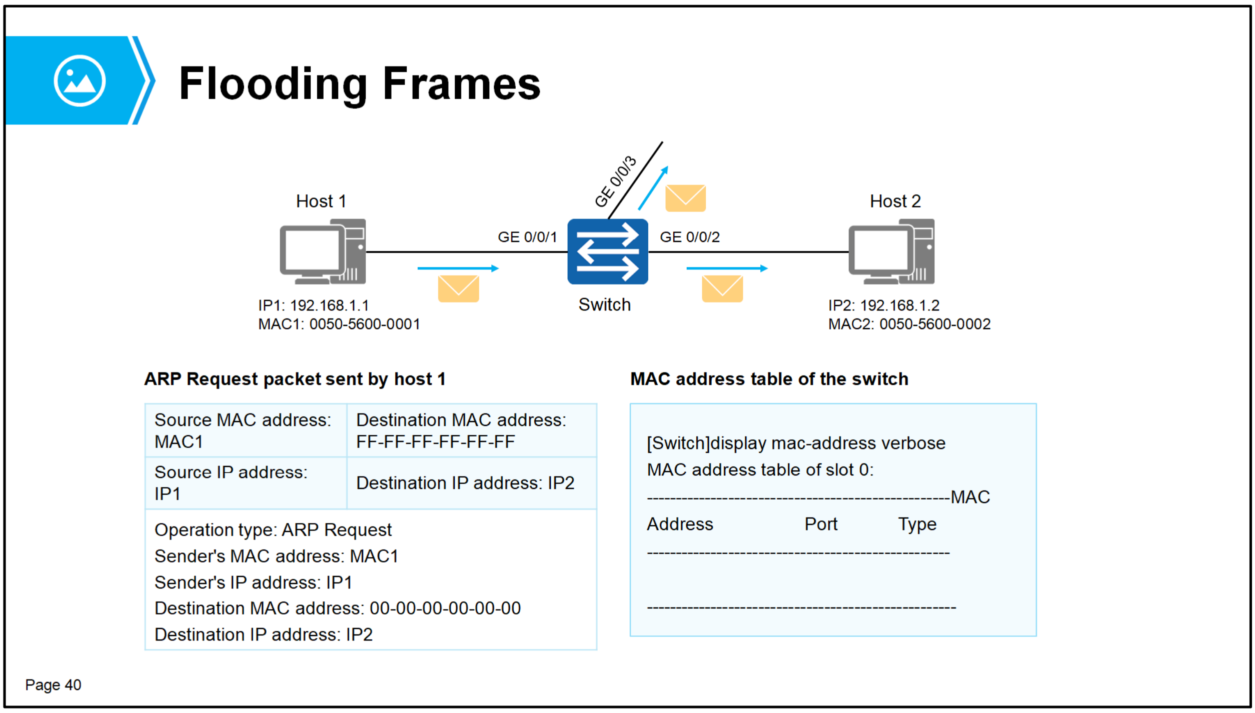
```
Host 1>arp -a
Internet Address    Physical Address   Type
-------------------------------------------------
-------------------------------------------------
```

MAC address table of the switch

```
[Switch]display mac-address verbose
MAC address table of slot 0:
-------------------------------------------------MAC
Address                 Port          Type
-------------------------------------------------


---------------------------------------------------
```

- To encapsulate packet, host 1 searches the local ARP cache table. In the initial state, the ARP cache table of host 1 is empty.
- For the switch that is just powered on, in the initial state, the MAC address table is also empty.



Flooding Frames

ARP Request packet sent by host 1

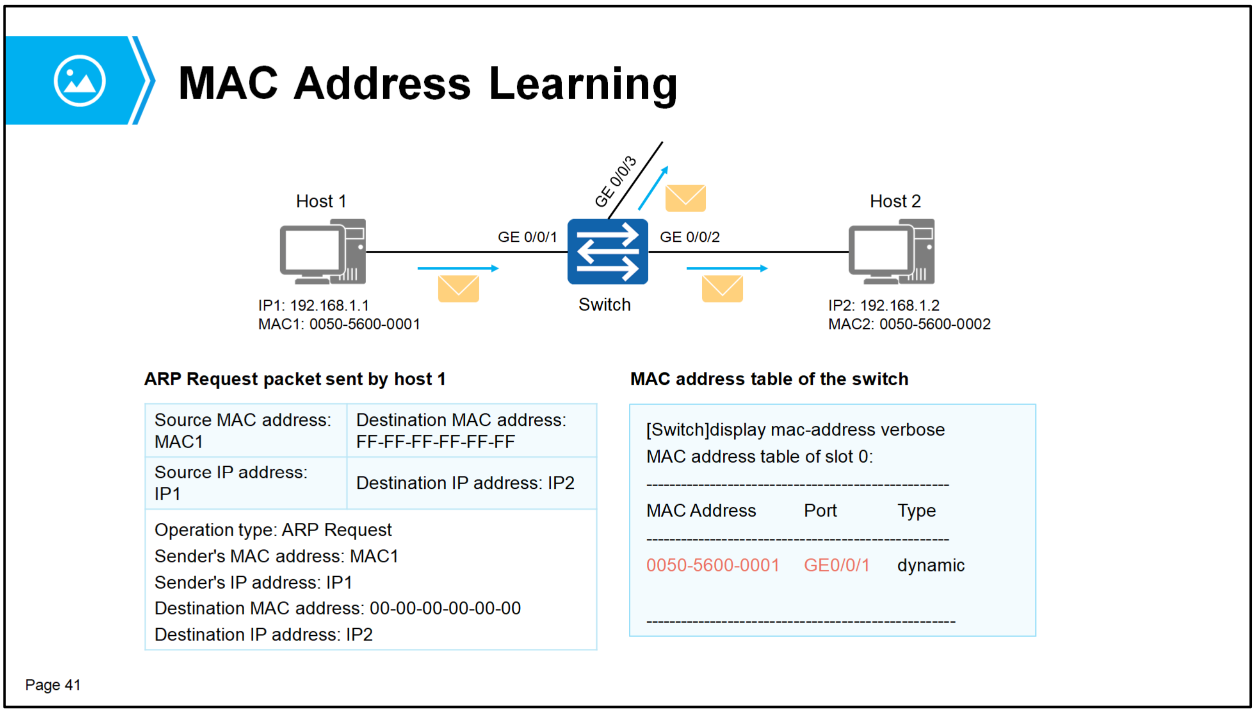
Source MAC address: MAC1	Destination MAC address: FF-FF-FF-FF-FF-FF
Source IP address: IP1	Destination IP address: IP2
Operation type: ARP Request Sender's MAC address: MAC1 Sender's IP address: IP1 Destination MAC address: 00-00-00-00-00-00 Destination IP address: IP2	

MAC address table of the switch

```
[Switch]display mac-address verbose
MAC address table of slot 0:
-------------------------------------------------MAC
Address              Port          Type
-------------------------------------------------


--------------------------------------------------
```

- Host 1 sends an ARP Request packet to request for the destination MAC address.
- After receiving a frame, the switch searches the MAC address table. If no matching entry is found in the table, the switch floods the frame to other interfaces other than the interface receiving the frame.



MAC Address Learning

ARP Request packet sent by host 1

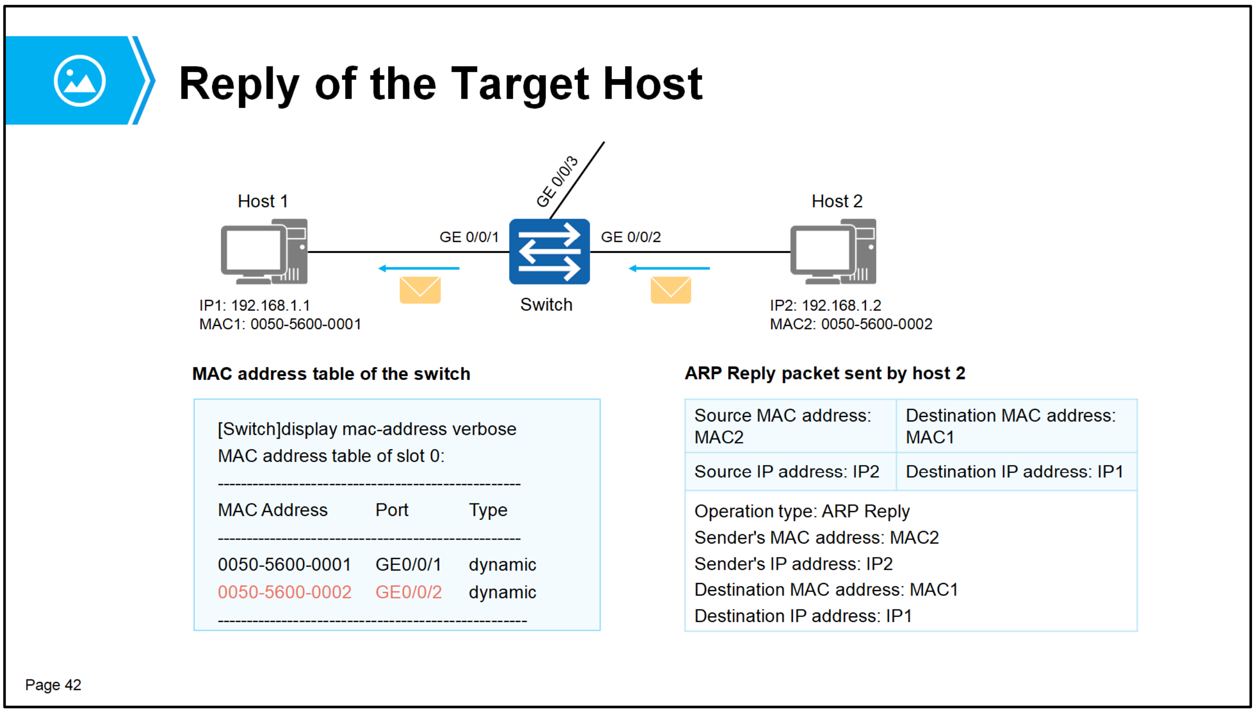
Source MAC address: MAC1	Destination MAC address: FF-FF-FF-FF-FF-FF
Source IP address: IP1	Destination IP address: IP2
Operation type: ARP Request Sender's MAC address: MAC1 Sender's IP address: IP1 Destination MAC address: 00-00-00-00-00-00 Destination IP address: IP2	

MAC address table of the switch

```
[Switch]display mac-address verbose
MAC address table of slot 0:
---------------------------------------------------
MAC Address        Port          Type
---------------------------------------------------
0050-5600-0001     GE0/0/1       dynamic

----------------------------------------------------
```

- The switch records the source MAC address and interface number of the received frame in the MAC address table.



Reply of the Target Host

MAC address table of the switch

```
[Switch]display mac-address verbose
MAC address table of slot 0:
-----------------------------------------------------
MAC Address         Port        Type
-----------------------------------------------------
0050-5600-0001    GE0/0/1    dynamic
0050-5600-0002    GE0/0/2    dynamic
-----------------------------------------------------
```

ARP Reply packet sent by host 2

Source MAC address: MAC2	Destination MAC address: MAC1
Source IP address: IP2	Destination IP address: IP1

Operation type: ARP Reply
Sender's MAC address: MAC2
Sender's IP address: IP2
Destination MAC address: MAC1
Destination IP address: IP1

- After receiving the ARP Request packet, host 2 processes the packet and sends an ARP Reply packet to host 1.
- After receiving a frame, the switch searches the MAC address table. If the corresponding entry is found in the table, the switch forwards the frame to the corresponding interface and records the source MAC address and interface number of the received frame in the MAC address table.
- After receiving the ARP Reply packet from host 2, host 1 records the corresponding IP address and MAC address in its ARP cache table and encapsulates its packets to access host 2.