Chapter 5: Ethernet

Introduction to Networks
Chapter 5

5.0 Introduction
5.1 Ethernet Protocol
5.2 Address Resolution Protocol
5.3 LAN Switches
5.4 Summary
Chapter 6: Objectives

In this chapter, you will learn to:

- Describe the operation of the Ethernet sublayers.
- Identify the major fields of the Ethernet frame.
- Describe the purpose and characteristics of the Ethernet MAC address.
- Describe the purpose of ARP.
- Explain how ARP requests impact network and host performance.
- Explain basic switching concepts.
- Compare fixed configuration and modular switches.
- Configure a Layer 3 switch.
Ethernet

Introduction

This chapter examines the characteristics and operation of Ethernet as it has evolved from a shared media, contention-based data communications technology to today's high bandwidth, full-duplex technology.
5.1 Ethernet Protocol

[Diagram showing the OSI model layers with emphasis on the Data Link and Physical layers, indicating Ethernet is defined by data link layer and physical layer protocols, with 802.2 and 802.3 standards.]
Ethernet Operation

LLC and MAC Sublayers

Ethernet –

• Most widely used LAN technology
• Operates in the data link layer and the physical layer
• Family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards
• Supports data bandwidths of 10, 100, 1000, 10,000, 40,000, and 100,000 Mbps (100 Gbps)

Ethernet standards –

• Define Layer 2 protocols and Layer 1 technologies
• Two separate sub layers of the data link layer to operate - Logical link control (LLC) and the MAC sublayers

Do buttons on 5.1.1.1
Ethernet Operation

LLC and MAC Sublayers

Know the Sub layers of Ethernet:
LLC
MAC

Ethernet is defined by Data Link layer and Physical layer protocols.

Do buttons on 5.1.1.1
Ethernet Operation

LLC and MAC Sublayers

**LLC**
- Handles communication between upper and lower layers
- Takes the network protocol data and adds control information to help deliver the packet to the destination

**MAC**
- Constitutes the lower sublayer of the data link layer
- Implemented by hardware, typically in the computer NIC
- Two primary responsibilities:
  - Data encapsulation
  - Media access control
Ethernet Operation

MAC Sublayer

Data Encapsulation
- Frame delimiting
- Addressing
- Error detection

Media Access Control
- Control of frame placement on and off the media
- Media recovery

Know:
- 10BaseT
- 100BaseTX
- 1000BaseT
- 1000BaseST
- 1000BaseLX
Ethernet Operation

MAC Sublayer

Data encapsulation

• Frame assembly before transmission and frame disassembly upon reception of a frame

• MAC layer adds a header and trailer to the network layer PDU

Provides three primary functions:

• Frame delimiting – identifies a group of bits that make up a frame, synchronization between the transmitting and receiving nodes

• Addressing – each Ethernet header added in the frame contains the physical address (MAC address) that enables a frame to be delivered to a destination node

• Error detection - each Ethernet frame contains a trailer with a cyclic redundancy check (CRC) of the frame contents
Ethernet Operation

MAC Sublayer

Media Access Control

- Responsible for the placement of frames on the media and the removal of frames from the media
- Communicates directly with the physical layer
- If multiple devices on a single medium attempt to forward data simultaneously, the data will collide resulting in corrupted, unusable data
- Ethernet provides a method for controlling how the nodes share access through the use of a Carrier Sense Multiple Access (CSMA) technology
Carrier Sense Multiple Access (CSMA) process

- Used to first detect if the media is carrying a signal
- If no carrier signal is detected, the device transmits its data
- If two devices transmit at the same time - data collision

Be able to describe difference between:
CSMA/CD
CSMA/CA
Ethernet Operation

Media Access Control

Contention-Based Access

<table>
<thead>
<tr>
<th>Method</th>
<th>Characteristics</th>
<th>Example</th>
</tr>
</thead>
</table>
| Contention-Based     | • Stations can transmit at any time  
                       | Access          | • Ethernet  
                       | • Collisions exist   |               |
| Access               | • Mechanisms exist to resolve contention problems  
                       |               | • Wireless  
                       | • CSMA/CD for Ethernet networks |               |
|                      | • CSMA/CA for 802.11 wireless networks                                            |               |

This is CSMA/CD
Ethernet Operation

Media Access Control

The two commonly used methods are:

CSMA/Collision Detection

• The device monitors the media for the presence of a data signal
• If a data signal is absent, indicating that the media is free, the device transmits the data
• If signals are then detected that show another device was transmitting at the same time, all devices stop sending and try again later
• While Ethernet networks are designed with CSMA/CD technology, with today’s intermediate devices, collisions do not occur and the processes utilized by CSMA/CD are really unnecessary
• Wireless connections in a LAN environment still have to take collisions into account
Ethernet Operation

Media Access Control

The two commonly used methods are:

**CSMA/Collision Avoidance (CSMA/CA) media access method**

- Device examines the media for the presence of data signal - if the media is free, the device sends a notification across the media of its intent to use it
- The device then sends the data.
- Used by 802.11 wireless networking technologies
## Ethernet Operation

### Media Access Control

<table>
<thead>
<tr>
<th>Method</th>
<th>Characteristics</th>
<th>Example</th>
</tr>
</thead>
</table>
| Contention-Based Access | • Stations can transmit at any time  
                          • Collisions exist  
                          • Mechanisms exist to resolve contention problems  
                          • CSMA/CD for Ethernet networks  
                          • CSMA/CA for 802.11 wireless networks | • Ethernet  
                           • Wireless                           |

Again understand:  
CSMA/CD  
CSMA/CA
Ethernet Operation

MAC Address: Ethernet Identity

- Layer 2 Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits
  - IEEE requires a vendor to follow two simple rules:
    - Must use that vendor's assigned OUI as the first 3 bytes
    - All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes

<table>
<thead>
<tr>
<th>Organizationally Unique Identifier (OUI)</th>
<th>Vendor Assigned (NIC, Interfaces)</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 Bits</td>
<td>24 Bits</td>
</tr>
<tr>
<td>6 hex digits</td>
<td>6 hex digits</td>
</tr>
<tr>
<td>00-60-2F</td>
<td>3A-07-BC</td>
</tr>
<tr>
<td>Cisco</td>
<td>particular device</td>
</tr>
</tbody>
</table>
Ethernet Operation
Frame Processing

- MAC addresses assigned to workstations, servers, printers, switches, and routers
- Example MACs: 00-05-9A-3C-78-00, 00:05:9A:3C:78:00, or 0005.9A3C.7800.
- Forwarded message to an Ethernet network, attaches header information to the packet, contains the source and destination MAC address
- Each NIC views information to see if the destination MAC address in the frame matches the device’s physical MAC address stored in RAM
- No match, the device discards the frame
- Matches the destination MAC of the frame, the NIC passes the frame up the OSI layers, where the decapsulation process takes place
### Ethernet Operation

#### 5.1.1.6 Activity - MAC and LLC Sublayers

<table>
<thead>
<tr>
<th></th>
<th>MAC</th>
<th>LLC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Controls the network interface card through software drivers</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Works with the upper layers to add application information for delivery of data to higher level protocols</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Works with hardware to support bandwidth requirements – checks for errors in bits sent and received</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Controls access to the media through signaling and physical media standards requirements</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Supports Ethernet technology by using CSMA/CD or CSMA/CA</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Remains relatively independent of physical equipment</td>
<td></td>
</tr>
</tbody>
</table>

Do activity 5.1.1.6 in class
Ethernet Frame Attributes

**Ethernet Encapsulation**

- Early versions of Ethernet were relatively slow at 10 Mbps
- Now operate at 10 Gigabits per second and faster
- Ethernet frame structure adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent

Ethernet II is the Ethernet frame format used in TCP/IP networks.
Ethernet Frame Attributes
Ethernet Frame Size

- Ethernet II and IEEE 802.3 standards define the minimum frame size as 64 bytes and the maximum as 1518 bytes
- Less than 64 bytes in length is considered a "collision fragment" or "runt frame"
- If size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device drops the frame
- At the physical layer, different versions of Ethernet vary in their method for detecting and placing data on the media
The figure displays the fields contained in the 802.1Q VLAN tag.

IEEE 802.1Q added a 4 byte field to the frame.
# Ethernet Frame Attributes

## Introduction to the Ethernet Frame

**IEEE 802.3**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preamble</td>
<td>Used for synchronization between the sending and receiving devices</td>
</tr>
<tr>
<td>Start Frame Delimiter</td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td>Defines the exact length of the frame's data field/describes which protocol is implemented</td>
</tr>
<tr>
<td>Length/Type Field</td>
<td></td>
</tr>
<tr>
<td>Data and Pad Fields</td>
<td>Contain the encapsulated data from a higher layer, an IPv4 packet</td>
</tr>
<tr>
<td>Frame Check Sequence</td>
<td></td>
</tr>
</tbody>
</table>

### Preamble and Start Frame Delimiter Fields

- **Preamble**: Used for synchronization between the sending and receiving devices.

### Length/Type Field

- **Length**: Defines the exact length of the frame's data field.
- **Type**: Describes which protocol is implemented.

### Data and Pad Fields

- **Data**: Contains the encapsulated data from a higher layer, an IPv4 packet.

5.1.2.3 Click on boxes in 5.1.2.3
## Ethernet Frame Attributes

### Introduction to the Ethernet Frame

#### IEEE 802.3

<table>
<thead>
<tr>
<th></th>
<th>7</th>
<th>1</th>
<th>6</th>
<th>6</th>
<th>2</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preamble</strong></td>
<td><strong>Start of Frame Delimiter</strong></td>
<td><strong>Destination Address</strong></td>
<td><strong>Source Address</strong></td>
<td><strong>Length</strong></td>
<td><strong>46 to 1500</strong></td>
<td><strong>Frame Check Sequence</strong></td>
</tr>
<tr>
<td><strong>802.2 Header and Data</strong></td>
<td><strong>5.1.2.3</strong></td>
<td><strong>Click on boxes in 5.1.2.3</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Frame Check Sequence Field

Used to detect errors in a frame with cyclic redundancy check (4 bytes), if calculations match at source and receiver, no error occurred.
Ethernet Frame Attributes
5.1.2.4 Activity - Ethernet Frame Fields

Do activity 5.1.2.4 in class
Ethernet MAC

MAC Addresses and Hexadecimal

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Binary</th>
<th>Hexadecimal</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0001</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0010</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0011</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0100</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>0101</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>0110</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>0111</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>1000</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>1001</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>1010</td>
<td>A</td>
</tr>
<tr>
<td>11</td>
<td>1011</td>
<td>B</td>
</tr>
<tr>
<td>12</td>
<td>1100</td>
<td>C</td>
</tr>
<tr>
<td>13</td>
<td>1101</td>
<td>D</td>
</tr>
<tr>
<td>14</td>
<td>1110</td>
<td>E</td>
</tr>
<tr>
<td>15</td>
<td>1111</td>
<td>F</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Binary</th>
<th>Hexadecimal</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000 0000</td>
<td>00</td>
</tr>
<tr>
<td>1</td>
<td>0000 0001</td>
<td>01</td>
</tr>
<tr>
<td>2</td>
<td>0000 0010</td>
<td>02</td>
</tr>
<tr>
<td>3</td>
<td>0000 0011</td>
<td>03</td>
</tr>
<tr>
<td>4</td>
<td>0000 0100</td>
<td>04</td>
</tr>
<tr>
<td>5</td>
<td>0000 0101</td>
<td>05</td>
</tr>
<tr>
<td>6</td>
<td>0000 0110</td>
<td>06</td>
</tr>
<tr>
<td>7</td>
<td>0000 0111</td>
<td>07</td>
</tr>
<tr>
<td>8</td>
<td>0000 1000</td>
<td>08</td>
</tr>
<tr>
<td>9</td>
<td>0000 1010</td>
<td>09</td>
</tr>
<tr>
<td>10</td>
<td>0000 1111</td>
<td>0A</td>
</tr>
<tr>
<td>11</td>
<td>0001 0000</td>
<td>0B</td>
</tr>
<tr>
<td>12</td>
<td>0001 0001</td>
<td>0C</td>
</tr>
<tr>
<td>13</td>
<td>0001 0010</td>
<td>0D</td>
</tr>
<tr>
<td>14</td>
<td>0001 0011</td>
<td>0E</td>
</tr>
<tr>
<td>15</td>
<td>0001 0100</td>
<td>0F</td>
</tr>
<tr>
<td>16</td>
<td>0001 0101</td>
<td>10</td>
</tr>
<tr>
<td>17</td>
<td>0001 0110</td>
<td>11</td>
</tr>
<tr>
<td>18</td>
<td>0001 0111</td>
<td>12</td>
</tr>
<tr>
<td>19</td>
<td>0001 1000</td>
<td>13</td>
</tr>
<tr>
<td>20</td>
<td>0001 1001</td>
<td>14</td>
</tr>
<tr>
<td>21</td>
<td>0001 1010</td>
<td>15</td>
</tr>
<tr>
<td>22</td>
<td>0001 1011</td>
<td>16</td>
</tr>
<tr>
<td>23</td>
<td>0001 1100</td>
<td>17</td>
</tr>
<tr>
<td>24</td>
<td>0001 1101</td>
<td>18</td>
</tr>
<tr>
<td>25</td>
<td>0001 1110</td>
<td>19</td>
</tr>
<tr>
<td>26</td>
<td>0001 1111</td>
<td>1A</td>
</tr>
</tbody>
</table>

Do buttons on 5.1.3.1 in class
Ethernet MAC

MAC Address Representations

- With Dashes: 00-60-2F-3A-07-BC
- With Colons: 00:60:2F:3A:07:BC
- With Periods: 0060.2F3A.07BC

Command prompt:
```ipconfig /all```

C:\>ipconfig/all

Ethernet adapter Local Area Connection:

- Connection-specific DNS Suffix.: example.com
- Description.: Intel(R) Gigabit Network Connection
- Physical Address.: 00-21-CC-BA-44-C4
- DHCP Enabled.: Yes
- Autoconfiguration Enabled.: Yes
- IPv4 Address.: 192.168.1.67 (Preferred)
- Subnet Mask.: 255.255.255.0
- Lease Obtained.: Monday, November 26, 2012 12:14:48 PM
- Lease Expires.: Saturday, December 01, 2012 12:15:02 AM
- Default Gateway.: 192.168.1.254
- DHCP Server.: 192.168.1.254
- DNS Servers.: 192.168.1.254
Ethernet MAC

Unicast MAC Address

Do animation 5.1.3.3 in class
Ethernet MAC

Broadcast MAC Address

Do animation 5.1.3.4 in class
Ethernet MAC
Multicast MAC Address

Multicast MAC address is a special value that begins with 01-00-5E in hexadecimal

Range of IPV4 multicast addresses is 224.0.0.0 to 239.255.255.255

Do animation 5.1.3.5 in class
MAC and IP

MAC address
- This address does not change
- Similar to the name of a person
- Known as physical address because physically assigned to the host NIC

IP address
- Similar to the address of a person
- Based on where the host is actually located
- Known as a logical address because assigned logically
- Assigned to each host by a network administrator

Both the physical MAC and logical IP addresses are required for a computer to communicate just like both the name and address of a person are required to send a letter

5.1.4.1
## Ethernet MAC

### End-to-End Connectivity, MAC, and IP

A switch examines MAC addresses.

<table>
<thead>
<tr>
<th>Destination MAC Address</th>
<th>Source MAC Address</th>
<th>Source IP Address</th>
<th>Destination IP Address</th>
<th>Data</th>
<th>Trailer</th>
</tr>
</thead>
</table>

A router examines IP addresses.

<table>
<thead>
<tr>
<th>Destination MAC Address</th>
<th>Source MAC Address</th>
<th>Source IP Address</th>
<th>Destination IP Address</th>
<th>Data</th>
<th>Trailer</th>
</tr>
</thead>
</table>

Do buttons and animations on 5.1.4.2
Ethernet MAC

End-to-End Connectivity, MAC, and IP

The Data Link Layer

Data link layer protocols govern how to format a frame for use on different media.

Different protocols may be in use for different media.

At each hop along the path, an intermediary device accepts frames from one medium, de-encapsulates the frame and then forwards the packets in a new frame. The headers of each frame are formatted for the specific medium that it will cross.

5.1.4.2

Do buttons and animations on 5.1.4.2
Ethernet MAC - Labs
5.1.4.3 Lab - Using Wireshark to Examine Ethernet Frames
5.1.4.4 Packet Tracer - Identify MAC and IP Addresses

Do labs 5.1.4.3 and 5.1.4.4 as a lab grade
5.2 Address Resolution Protocol

I need to send information to 192.168.1.7, but I only have the IP address. I don't know the MAC address of the device that has that IP.
ARP

Introduction to ARP

ARP Purpose

- Sending node needs a way to find the MAC address of the destination for a given Ethernet link

The ARP protocol provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining a table of mappings
ARP

Introduction to ARP

I need to send information to 192.168.1.7, but I only have the IP address. I don't know the MAC address of the device that has that IP.
ARP
ARP Functions/Operation

ARP Table –
- Used to find the data link layer address that is mapped to the destination IPv4 address
- As a node receives frames from the media, it records the source IP and MAC address as a mapping in the ARP table

ARP request –
- Layer 2 broadcast to all devices on the Ethernet LAN
- The node that matches the IP address in the broadcast will reply
- If no device responds to the ARP request, the packet is dropped because a frame cannot be created

Static map entries can be entered in an ARP table, but this is rarely done

Do Animation on 5.2.1.2 and 5.2.1.2
ARP

ARP Functions/Operation

The ARP Process — Communicating Remotely

Host A — ARP Cache

Host A
10.10.0.1
00-0d-88-c7-9a-24

Host B
10.10.0.2
00-08-a3-b6-ce-04

Host C
10.10.0.3
00-0d-56-09-fb-d1

Host D
10.10.0.4
00-12-3f-d4-6d-1b

Host A wants to send data to IP address 10.10.0.3, but has no ARP entry.

R1 interface G0/0
10.10.0.254

Do Buttons on 5.2.1.3
ARP Functions/Operation

Broadcasting an ARP Request

Host A — ARP Cache

Host A
10.10.0.1
00-0d-88-c7-9a-24

Host B
10.10.0.2
00-08-a3-b6-ce-04

Host C
10.10.0.3
00-0d-56-09-fb-d1

Host D
10.10.0.4
00-12-3f-d4-6d-1b

Host A sends an ARP request looking for the MAC address associated with IP 10.10.0.3.
ARP Functions/Operation

Broadcasting an ARP Request

Host A — ARP Cache

Host A
10.10.0.1
00-0d-88-c7-9a-24

Host B
10.10.0.2
00-08-a3-b6-ce-04

Host C
10.10.0.3
00-0d-56-09-fb-d1

Host D
10.10.0.4
00-12-3f-d4-6d-1b

Host A sends an ARP request looking for the MAC address associated with IP 10.10.0.3.

R1 interface G0/0
10.10.0.254
00-10-7b-e7-fa-ef

Do Buttons on 5.2.1.3
ARP

ARP Functions/Operation

ARP Reply with MAC Information

Host A — ARP Cache

<table>
<thead>
<tr>
<th>Host A</th>
<th>Host B</th>
<th>Host C</th>
<th>Host D</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.1</td>
<td>10.10.0.2</td>
<td>10.10.0.3</td>
<td>10.10.0.4</td>
</tr>
<tr>
<td>00-0d-88-c7-9a-24</td>
<td>00-08-a3-b6-ce-04</td>
<td>00-0d-56-09-fb-d1</td>
<td>00-12-3f-d4-6d-1b</td>
</tr>
</tbody>
</table>

Host C, with IP address 10.10.0.3 responds with an ARP reply that includes its MAC address.

Do Buttons on 5.2.1.3
ARP

ARP Functions/Operation

Adding MAC-to-IP Map in ARP Cache

Host A — ARP Cache
10.10.0.3 00-0d-56-09-fb-d1

Host A
10.10.0.1
00-0d-88-c7-9a-24

Host B
10.10.0.2
00-08-a3-b6-ce-04

Host C
10.10.0.3
00-0d-56-09-fb-d1

Host D
10.10.0.4
00-12-3f-d4-6d-1b

Host A adds the IP to MAC address map to its ARP cache

Do Buttons on 5.2.1.3
ARP

ARP Functions/Operation

Forwarding Data with MAC Address Information

Host A — ARP Cache
10.10.0.3 00-0d-56-09-fb-d1

Host A
10.10.0.1
00-0d-88-c7-9a-24

Host B
10.10.0.2
00-08-a3-b6-ce-04

Host C
10.10.0.3
00-0d-56-09-fb-d1

Host D
10.10.0.4
00-12-3f-d4-6d-1b

Do Buttons on 5.2.1.3

Host A forwards data directly to Host C via MAC address.
ARP

ARP Role in Remote Communication

- If the destination IPv4 host is on the local network, the frame will use the MAC address of this device as the destination MAC address.

- If the destination IPv4 host is not on the local network, the source uses the ARP process to determine a MAC address for the router interface serving as the gateway.

- In the event that the gateway entry is not in the table, an ARP request is used to retrieve the MAC address associated with the IP address of the router interface.
ARP

Removing Entries from an ARP Table

- ARP cache timer removes ARP entries that have not been used for a specified period of time
- Commands may also be used to manually remove all or some of the entries in the ARP table

Removing MAC-to-IP Address Mappings

<table>
<thead>
<tr>
<th>Host A — ARP Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.3</td>
</tr>
<tr>
<td>00-0d-56-09-fb-d1</td>
</tr>
<tr>
<td>10.10.0.254</td>
</tr>
<tr>
<td>00-10-7b-e7-fa-ef</td>
</tr>
</tbody>
</table>

Host A 10.10.0.1 00-0d-88-c7-9a-24

Host B 10.10.0.2 00-08-a3-b6-ce-04

Host C is removed from the network.

Host D 10.10.0.4 00-12-3f-d4-6d-1b

If Host C's IP and MAC address are not removed from Host A's ARP cache, Host A may still try to communicate with Host C.

R1 interface G0/0 10.10.0.254 00-10-7b-e7-fa-ef
# ARP

## ARP Tables on Networking Devices

**Router**

```
Router#show ip arp
```

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Address</th>
<th>Age</th>
<th>Hardware Addr</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>172.16.233.229</td>
<td>-</td>
<td>0000.0c59.f892</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.16.233.218</td>
<td>-</td>
<td>0000.0c07.ac00</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.16.168.11</td>
<td>-</td>
<td>0000.0c63.1300</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.16.168.254</td>
<td>9</td>
<td>0000.0c36.6965</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
</tbody>
</table>

**C:**

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

<table>
<thead>
<tr>
<th>Interface: 192.168.1.67 --- 0xa</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Address</td>
</tr>
<tr>
<td>192.168.1.254</td>
</tr>
<tr>
<td>192.168.1.255</td>
</tr>
<tr>
<td>224.0.0.22</td>
</tr>
<tr>
<td>224.0.0.251</td>
</tr>
<tr>
<td>224.0.0.252</td>
</tr>
<tr>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>
ARP

5.2.1.7 Packet Tracer - Examine the ARP Table

Optional:
Do Lab 5.2.1.7
Can’t do 5.1.1.8
ARP Issues

How ARP Can Create Problems

ARP broadcasts can flood the local media.

ARP Issues:
- Broadcasts, overhead on the media
- Security
ARP Issues
Mitigating ARP Problems

Switch at the center of a LAN

Each computer has its own collision domain.
5.3 LAN Switches
Switching
Switch Port Fundamentals

Layer 2 LAN switch

- Connects end devices to a central intermediate device on most Ethernet networks
- Performs switching and filtering based only on the MAC address
- Builds a MAC address table that it uses to make forwarding decisions
- Depends on routers to pass data between IP subnetworks

Do Buttons on 5.3.1.1
Switching
Switch MAC Address Table

1. The switch receives a broadcast frame from PC 1 on Port 1.
2. The switch enters the source MAC address and the switch port that received the frame into the address table.
3. Because the destination address is a broadcast, the switch floods the frame to all ports, except the port on which it received the frame.
4. The destination device replies to the broadcast with a unicast frame addressed to PC 1.

Continued…
5. The switch enters the source MAC address of PC 2 and the port number of the switch port that received the frame into the address table. The destination address of the frame and its associated port is found in the MAC address table.

6. The switch can now forward frames between source and destination devices without flooding, because it has entries in the address table that identify the associated ports.
Switching

Duplex Settings

**Half Duplex (CSMA/CD)**
- Unidirectional data flow
- Higher potential for collision
- Hub connectivity

**Full Duplex**
- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled

5.3.1.3
Switching

Auto-MDIX

MDIX auto detects the type of connection required and configures the interface accordingly.
A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.
Switching

Cut-through Switching

Two variants:

**Fast-forward switching:**
- Lowest level of latency immediately forwards a packet after reading the destination address, typical cut-through method of switching

**Fragment-free switching:**
- Switch stores the first 64 bytes of the frame before forwarding, most network errors and collisions occur during the first 64 bytes

A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

Do the animation on 5.3.1.6
Switching
5.3.1.7 Activity - Frame Forwarding Methods

Do the activities on 5.3.1.7 in class
## Memory Buffering on Switches

<table>
<thead>
<tr>
<th>Port-based memory</th>
<th>In port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared memory</td>
<td>Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.</td>
</tr>
</tbody>
</table>
Switching
5.3.1.7 Activity - Frame Forwarding Methods

Do the activities on 5.3.1.9 in class
This is GREAT practice to understanding how switches work
Fixed or Modular

Fixed verses Modular Configuration

Power over Ethernet (PoE)

Click on devices and do the buttons on 5.3.2.1
Fixed or Modular

Fixed verses Modular Configuration

Switch Form Factors

Fixed Configuration Switches

Features and options are limited to those that originally come with the switch.

Modular Configuration Switches

The chassis accepts line cards that contain the ports.

Stackable Configuration Switches
Fixed or Modular
Module Options for Cisco Switch Slots
Layer 3 Switching

Layer 2 verses Layer 3 Switching

Click on buttons on 5.3.3.1
Layer 3 Switching
Cisco Express Forwarding

Two main components:

- Forwarding information base (FIB)
  - Conceptually similar to a routing table
  - A networking device uses this lookup table to make destination-based switching decisions during Cisco Express Forwarding operation
  - Updated when changes occur in the network and contains all routes known at the time

- Adjacency tables
  - Maintain layer 2 next-hop addresses for all FIB entries
Layer 3 Switching
Cisco Express Forwarding
Layer 3 Switching

Types of Layer 3 Interfaces

The major types of Layer 3 interfaces are:

- **Switch Virtual Interface (SVI)** – Logical interface on a switch associated with a virtual local area network (VLAN).

- **Routed Port** – Physical port on a Layer 3 switch configured to act as a router port. Configure routed ports by putting the interface into Layer 3 mode with the `no switchport` interface configuration command.

- **Layer 3 EtherChannel** – Logical interface on a Cisco device associated with a bundle of routed ports.
## Layer 3 Switching

### Configuring a Routed Port on a Layer 3 Switch

#### Routed Port Configuration

```
S1(config)#interface f0/6
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.200.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
*Mar 1 00:15:40,115: %SYS-5-CONFIG_I: Configured from console by console
S1#show ip interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/2</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/3</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/4</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/5</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td><strong>FastEthernet0/6</strong></td>
<td><strong>192.168.200.1</strong></td>
<td><strong>YES manual</strong></td>
<td><strong>up</strong></td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/7</td>
<td>unassigned</td>
<td>YES unset</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/8</td>
<td>unassigned</td>
<td>YES unset</td>
<td>up</td>
<td></td>
</tr>
</tbody>
</table>
```

<output omitted>
Layer 3 Switching
5.3.3.5 Packet Tracer - Configure Layer 3 Switches

Do lab 5.3.3.5 as a lab grade
Chapter 5

Summary

- Ethernet is the most widely used LAN technology used today.
- Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
- The Ethernet frame structure adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent.
- As an implementation of the IEEE 802.2/3 standards, the Ethernet frame provides MAC addressing and error checking.
- Replacing hubs with switches in the local network has reduced the probability of frame collisions in half-duplex links.
Chapter 5
Summary

- The Layer 2 addressing provided by Ethernet supports unicast, multicast, and broadcast communications.
- Ethernet uses the Address Resolution Protocol to determine the MAC addresses of destinations and map them against known Network layer addresses.
- Each node on an IP network has both a MAC address and an IP address.
- The ARP protocol resolves IPv4 addresses to MAC addresses and maintains a table of mappings.
- A Layer 2 switch builds a MAC address table that it uses to make forwarding decisions.
Chapter 5

Summary

- Layer 3 switches are also capable of performing Layer 3 routing functions, reducing the need for dedicated routers on a LAN.
- Layer 3 switches have specialized switching hardware so they can typically route data as quickly as they can switch.
Cisco Networking Academy
Mind Wide Open™