[CNet - F25]

Computer Networks

<//Lecture-02//>

NETWORK ADDRESSES & COMMUNICATION SETUP

Week 4 - (28 SEPT 2025)

</// Today's agenda //>

01 NETWORK ADDRESSES

Understanding MAC & IP Addresses

02 Address Resolution Protocol

Describing Address Resolution Protocol (ARP)

03 IP CLASSES

Identify and categorize IP classes

04 NETWORK DESIGN

Explaining CIDR and VLSM

05 LEARNING ACTIVITIES

Interactive Discussion, Real-World Case Studies, DEMO Labs, **Quiz#2**, **Assignment#3**

06 Q & A Session

Q&A session for students to ask questions about today's presentation.

</// MAC ADDRESS (Media Access Control Address) //>

Definition: A MAC address is a unique hardware identifier that is assigned to a Network Interface Card (NIC) by its manufacturer. It serves as a permanent “name tag” for a device on a local network.

Format: A MAC address is **48 bits (or 6 bytes)** in length and is typically represented as **12 hexadecimal digits**. These digits are usually grouped into six pairs separated by colons or hyphens. **E.g.:**

00:1A:2B:3C:4D:5E

The first 3 bytes identify the NIC's manufacturer, whereas the last 3 bytes contain a unique number from the manufacturer that identifies each device on a network.

</// MAC ADDRESS (Media Access Control Address) //>

Role in Networking: Operating at the Data Link Layer (Layer 2) of the OSI model, the MAC address is crucial for local network communication. It ensures that data frames are accurately delivered to the correct hardware device within the same network segment.

Permanence: Generally, a MAC address is permanently embedded (or “burned in”) into the NIC during manufacturing. While it is usually fixed, some devices allow the MAC address to be reconfigured or spoofed via software if necessary.

IP ADDRESS (Internet Protocol Address)

Definition: An IP address is a unique logical identifier assigned to a device within a network that uses the Internet Protocol (IP) for communication. It allows devices to send and receive data across local and global networks.

Versions:

- **IPv4 (Internet Protocol Version 4)**
  - **A 32-bit numerical** address represented in dotted decimal format (e.g., **192.168.10.1**). And the **Range** is: From **0.0.0.0** to **255.255.255.255**
  - Supports approximately **4.3 billion** unique addresses, leading to IPv6 adoption due to address exhaustion.
- **IPv6 (Internet Protocol Version 6)**
  - **A 128-bit** hexadecimal address (e.g., **2001:0db8:85a3::8a2e:0370:7334**).
  - Provides a vastly larger address space and improved security features compared to IPv4.

IP ADDRESS (Internet Protocol Address)

Public IP Address

- Assigned by **IANA**, **RIRs,** and Local Internet Service Provider (**ISP**) and is globally routable over the internet.

Private IP Address

- Used within local networks and not routable over the public internet.

Loopback Address

- The loopback address is used for self-testing and communication within the device itself without the need for an active network connection. It confirms that the TCP/IP stack is working correctly.

APIPA (Automatic Private IP Addressing)

- Assigned automatically when DHCP is unavailable to allow limited local communication.
- Useful for troubleshooting network connectivity issues.

IP CLASSES and Ranges

Class	Both Public & Private IP Ranges			Private IP Ranges Only		
A	1.0.0.0	→	126.255.255.255	10.0.0.0	→	10.255.255.255
B	128.0.0.0	→	191.255.255.255	172.16.0.0	→	172.31.255.255
C	192.0.0.0	→	223.255.255.255	192.168.0.0	→	192.168.255.255
D	224.0.0.0	→	239.255.255.255	N/A		
E	240.0.0.0	→	255.255.255.255	N/A		

Link

Local Hosts / Loopback Addresses

IPv4 Loopback Range: 127.0.0.0 to 127.255.255.255

Most Common Address: 127.0.0.1 is typically used as the local host address.

IPv6 Loopback Range: ::1 (Serves the same purpose as the IPv4 loopback in IPv6-enabled systems.)

APIPA Address (Automatic Private IP Addressing)

Range: From 169.254.0.0 to 169.254.255.255 (For IPv4) **and** FE80::/10 (For IPv6)

<// IP Address vs. MAC Address//>

FEATURE	IP ADDRESS	MAC ADDRESS
Definition	A logical address assigned to a device in a network.	A physical address permanently assigned to a network interface card (NIC).
Function	Identifies devices at the network level, allowing routing between different networks.	Identifies devices within the same local network (Layer 2).
Structure	IPv4: 32-bit, IPv6: 128-bit	48-bit hexadecimal (e.g., 00:1A:2B:3C:4D:5E)
Persistence	Can be static (manual) or dynamic (assigned by DHCP).	Permanent and unique per device (unless manually changed via spoofing).
Layer	Network Layer (Layer 3)	Data Link Layer (Layer 2)
Example	192.168.1.10	00:14:22:01:23:45
Scope	Local network segment	Local and Global/internet wide

</// Address Resolution Protocol (ARP) //>

- **Definition:**

  ARP (Address Resolution Protocol) is a network protocol used to map a device's **IP address** to its corresponding **MAC address**. This is necessary for devices within a local area network (LAN) to communicate effectively over the data link layer (Layer 2) of the OSI model.

- **Purpose:**

  ARP allows devices to locate each other in a network using the IP address, which is a Layer 3 address. However, communication at the data link layer requires the MAC address (Layer 2). Without ARP, devices would not know how to send data packets directly to other devices within the same network using their MAC addresses.

HOW ARP WORKS

- **ARP Request (Broadcast):**
  - When a device needs to send data to another device within the same local network, it checks its ARP cache to see if the IP-to-MAC mapping is already stored.
  - If the mapping is not found, the device broadcasts an ARP request to all devices on the local subnet. The ARP request packet contains the sender's IP and MAC address, and it asks, "Who has IP address X.X.X.X? Please send your MAC address.“
- **ARP Reply (Unicast):**
  - The device with the matching IP address responds with an ARP reply. This reply is a unicast message (sent directly to the requesting device) that contains the **MAC address** of the device that owns the IP address in question.
  - This reply updates the ARP cache of the requesting device, allowing it to map the IP address to a MAC address for future communication.

ARP Process Overview

Step	Action	Description
1	**ARP Request**	Sender broadcasts a message asking, “Who has IP X.X.X.X?”
2	**ARP Broadcast**	This ARP request is sent to all devices on the LAN.
3	**ARP Reply**	The device with that IP sends back its MAC address.
4	**Data Transfer**	Sender uses the received MAC to send the actual data frame.

Practical Example Scenario

Let’s imagine two computers on the same LAN:

Device	Hostname	IP Address	MAC Address
PC-A	Alice	192.168.1.10	AA:AA:AA:AA:AA:AA
PC-B	Bob	192.168.1.20	BB:BB:BB:BB:BB:BB

Goal: **PC-A wants to send a message to PC-B (IP: 192.168.1.20).**

ARP Request

If PC-A does not know Bob’s MAC address, so it sends an ARP Request.

The ARP Request asks: “Who has 192.168.1.20? Tell 192.168.1.10.”

Ethernet Header	Destination MAC	Source MAC	Payload
Broadcast Frame	FF:FF:FF:FF:FF:FF	AA:AA:AA:AA:AA:AA	ARP Request asking for 192.168.1.20

Practical Example Scenario

ARP Reply:

PC-B knows the IP is its own, so it replies with its MAC address.

Field	Value
Sender MAC	BB:BB:BB:BB:BB:BB
Sender IP	192.168.1.20
Target MAC	AA:AA:AA:AA:AA:AA
Target IP	192.168.1.10

ARP Reply Message is unicast: Ex: sent directly to PC-A

Real Message

Ethernet Header	Destination MAC	Source MAC	Payload
Data Frame	BB:BB:BB:BB:BB:BB	AA:AA:AA:AA:AA:AA	Actual IP Packet (e.g., TCP/HTTP)

Summary Table: ARP Lifecycle

Step	Type	Source MAC	Destination MAC	Description
1	**ARP Request**	AA:AA:AA:AA:AA:AA	FF:FF:FF:FF:FF:FF	Broadcast asking “Who has 192.168.1.20?”
2	**ARP Broadcast**	-	All devices	All devices receive the request
3	**ARP Reply**	BB:BB:BB:BB:BB:BB	AA:AA:AA:AA:AA:AA	Bob replies with his MAC
4	**Data Transfer**	AA:AA:AA:AA:AA:AA	BB:BB:BB:BB:BB:BB	PC-A sends real data

ARP Table (Cache)

- **Purpose:** ARP tables (or ARP caches) store the IP-to-MAC address mappings for efficient data forwarding.
- **Entries:** When a device performs an ARP request, the corresponding IP-to-MAC pair is stored in its ARP table for future use. Each entry typically includes:
    - IP Address
    - MAC Address
    - Interface (the network interface on the device that holds the mapping)
    - TTL (Time to Live)
- **Commands to View ARP Table:**
    - On **Windows**: arp -a
    - On **Linux**: ip neighbour or arp -n

ARP USE CASES

- **Local Network Communication:**
  - In a typical Ethernet network, ARP ensures devices can map IP addresses to MAC addresses and communicate directly within the same subnet.
- **Routers and Gateways:**
  - Routers use ARP to communicate with devices in the same subnet. If a router needs to forward a packet to a device on the same subnet, it will perform an ARP request to determine the destination’s MAC address.
- **DHCP (Dynamic Host Configuration Protocol):**
  - When a device first connects to a network and obtains its IP address via DHCP, it uses ARP to ensure the IP address is not already in use by another device on the same network.

[CNet-F25]

<//THANK YOU!//>

“For I know the plans I have for you," declares the Lord, "plans to prosper you and not to harm you, plans to give you hope and future.”

Jeremiah 29:11