CHAPTER 2:SECTION-IP ADDRESS & RELATED NETWORKING CONCEPTS

1) WHAT IS AN IP ADDRESS?

An IP Address (Internet Protocol Address) is a unique numerical identifier assigned to every device connected to a network that uses the Internet Protocol for communication. It's like a digital postal address—helping data find the right device on a network.

---

2) TYPES OF IP ADDRESSES

2.1 BASED ON VERSION

IPv4 (Internet Protocol version 4)

32-bit address

Written in dotted-decimal form (e.g., 192.168.1.1)

Total addresses: 4,294,967,296 (2^{32})

IPv6 (Internet Protocol version 6)

128-bit address

Written in hexadecimal groups separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)

Total addresses: ~3.4×10^{38}

2.2 BASED ON USAGE

Public IP Address

- Used on the internet
- Globally unique
- Assigned by ISP

Private IP Address

1. Used within local networks (LAN)
2. Not globally unique (can repeat across different networks)

Common ranges:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Static IP Address

- Fixed; does not change over time
- Often used for servers

Dynamic IP Address

- Changes periodically
- Assigned automatically by DHCP servers

STRUCTURE OF AN IPV4 ADDRESS

Total: 32 bits

Divided into 4 octets (each = 8 bits)

Format: A.B.C.D where each part is 0–255

Two logical parts:

Network ID – identifies the network

Host ID – identifies the device within that network

Example: 192.168.1.10

Network part: 192.168.1

Host part: 10

IP ADDRESS CLASSES (IPV4)

Class	First Octet Range	Default Subnet Mask	Purpose	Example
A	1 – 126	255.0.0.0	Large networks	10.0.0.1
B	128 – 191	255.255.0.0	Medium networks	172.16.0.1
C	192 – 223	255.255.255.0	Small networks	192.168.1.1

Class	First Octet Range	Default Subnet Mask	Purpose	Example
D	224 – 239	N/A	Multicasting	224.0.0.1
E	240 – 255	N/A	Experimental	250.1.1.1

Special notes

0.x.x.x → Reserved

127.x.x.x → Loopback (localhost)

HOW TO IDENTIFY AN IP ADDRESS

IPv4 validity rules

Four octets separated by dots (.)

Each octet: 0–255

No letters/spaces/special characters (other than dots)

Examples

Valid: 192.168.0.1

Invalid: 192.168.256.1 (256 out of range)

Invalid: 192.168.one.1 (contains words)

IPV6 VALIDITY RULES

Eight groups of 1–4 hexadecimal digits

Groups separated by colons (:)

:: may be used once to replace a consecutive sequence of zero groups

---

IPV6 ADDRESS FORMAT BASICS & COMPRESSION

6.1 Format Basics

Length: 128 bits

Written as 8 groups (blocks) of 1–4 hex digits

Separator: :

Hex digits: 0–9, A–F (case-insensitive)

Example (full):
2001:0db8:0000:0000:0000:ff00:0042:8329
Each block is 16 bits → 8 × 16 = 128 bits.

6.2 Why :: Exists

IPv6 addresses can contain long runs of 0000.

:: denotes “one or more consecutive groups of 0000”.

Only once per address (to avoid ambiguity).

6.3 Examples of Compression

Full → remove leading zeros:
2001:0db8:0000:0000:0000:0000:0000:0001
→ 2001:db8:0:0:0:0:0:1

Use :: to replace consecutive zero groups:
2001:db8:0:0:0:0:0:1 → 2001:db8::1

More examples of ::

Middle compression
fe80:0:0:0:2aa:ff:fe9a:4ca2 → fe80::2aa:ff:fe9a:4ca2

At the start
0:0:0:0:0:0:0:1 → ::1 (IPv6 loopback)

At the end
2001:db8:1234:5678:0:0:0:0 → 2001:db8:1234:5678::

Rules to remember

Leading zeros can be removed (e.g., 00ab → ab).

:: can appear only once.

Using :: twice is invalid.

PARAMETERS THAT DEFINE AN IP ADDRESS

When configuring networking you typically specify:

IP Address (e.g., 192.168.1.10)

Subnet Mask (defines network vs host part, e.g., 255.255.255.0)

Default Gateway (router IP, e.g., 192.168.1.1)

DNS Server (name → IP translation, e.g., 8.8.8.8)

NETWORK ID

Identifies the specific network.

Devices in the same network share this ID.

Routers use it to deliver packets to the right network.

HOST ID

Identifies the specific device within that network.

Must be unique inside the network.

HOW THEY'RE SPLIT (SUBNET MASK)

Bits covered by 1s in the subnet mask → Network ID

Bits covered by 0s in the subnet mask → Host ID

Example

IP: 192.168.1.10

Mask: 255.255.255.0

IP Address: 11000000.10101000.00000001.00001010

Subnet Mask: 11111111.11111111.11111111.00000000

Network ID: 11000000.10101000.00000001.00000000 → 192.168.1.0

Host part: 00001010 → .10

So:

Network ID = 192.168.1.0

Host ID = .10

Why it matters

Network ID: “Send this packet to Network X.”

Host ID (inside Network X): “Deliver to Device Y.”

Analogy

Network ID = street name

Host ID = house number

SUBNET MASK

WHAT IS A SUBNET MASK?

A 32-bit number (IPv4) that divides an IP address into:

Network ID (which network)

Host ID (which device in that network)

It doesn’t travel with packets; it is used locally for routing decisions.

HOW IT WORKS

Written like an IPv4 address: e.g., 255.255.255.0

In binary: a sequence of 1s followed by 0s

1 → bit belongs to Network ID

0 → bit belongs to Host ID

Example (AND operation)

IP: 192.168.1.10 → 11000000.10101000.00000001.00001010

Mask: 255.255.255.0 → 11111111.11111111.11111111.00000000

Net: 192.168.1.0 → 11000000.10101000.00000001.00000000

Result: Network ID = 192.168.1.0; Host ID = .10

Usable hosts per subnet

If n = number of host bits (zeros in the mask):
Usable hosts = $(2^n) – 2$
(Subtract network ID and broadcast address.)

Network ID → name of the network segment

Host bits in the mask → how many devices it can hold

RELATIONSHIP BETWEEN IP & SUBNET MASK

IP Address: where you are

Subnet Mask: how much of the IP is network vs host

Together, they determine who is in the same subnet (no routing) and who is outside (needs routing).

DEFAULT SUBNET MASK (CLASSFUL)

Class	First Octet	Default Mask	CIDR	Network Bits	Host Bits	Usable Hosts
A	1–126	255.0.0.0	/8	8	24	16,777,214
B	128–191	255.255.0.0	/16	16	16	65,534
C	192–223	255.255.255.0	/24	24	8	254

Classful examples

10.25.8.7 → Class A → mask 255.0.0.0 (/8)
Network ID: 10 | Host ID: 25.8.7

172.16.5.100 → Class B → mask 255.255.0.0 (/16)
Network ID: 172.16 | Host ID: 5.100

192.168.1.10 → Class C → mask 255.255.255.0 (/24)
Network ID: 192.168.1 | Host ID: 10

 Today we use CIDR (Classless Inter-Domain Routing), so masks can be any length, not just class defaults. Knowing defaults still helps with exams/legacy docs.

STATIC IP ADDRESS

A static IP does not change (manually assigned).

Uses

Hosting (web/email/FTP)

Remote access (CCTV, home office)

VPNs

Any device that must be reliably reachable

ADVANTAGES

Consistent/reliable address

Good for DNS mapping

Often lower latency for gaming/VoIP

Easy remote access targeting

DISADVANTAGES

May cost extra

Easier to target (predictable)

Requires manual configuration

Less private (easier to track)

DYNAMIC IP ADDRESS

A dynamic IP changes periodically (assigned by DHCP).

Uses

Everyday internet access (phones, laptops, home users)

ISP customer management at scale

Situations where constant remote access isn’t needed

ADVANTAGES

No manual setup (plug-and-play)

More private/harder to target

Usually cheaper/included

Conserves IPv4 address pool

DISADVANTAGES

Can change unexpectedly (bad for hosting)

Can disrupt remote connections

DNS updates may be needed

Minor setup frictions for some features (e.g., port forwarding)

10.1 Quick Comparison: Static vs Dynamic

Feature	Static IP	Dynamic IP
Assignment	Manual	Automatic (DHCP)
Change	Never (unless reconfigured)	Periodically
Cost	Usually extra	Usually included
Security	Easier to track/attack	More private/harder to target
Best for	Servers/hosting/remote access	Everyday browsing/home users

Rule of thumb

Use Static if you run services that must be found at the same address.

Use Dynamic for normal use when fixed remote access isn't required.

MAC ADDRESS

WHAT IS A MAC ADDRESS?

MAC = Media Access Control address

Unique hardware identifier assigned to a network interface card (NIC) by the manufacturer

OSI Layer 2 (Data Link)

Format: 6 groups of two hex digits, separated by colons or hyphens

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

First half: OUI (manufacturer)

Second half: unique device ID

Unlike IP (logical, changeable), MAC is tied to the physical hardware (though it can be spoofed)

USES OF MAC ADDRESSES

Local LAN communication (switches deliver frames by MAC)

Device identification (security systems)

MAC filtering (allow/block specific devices)

Asset tracking/inventory in enterprises

Data transmission across Ethernet/Wi-Fi/Bluetooth

ADVANTAGES

Unique per device

Usually fixed (no config needed)

Reliable for LAN delivery

Useful for certain security controls

DISADVANTAGES

Not encrypted; visible on the LAN

Can be spoofed

Works only within LAN scope (not routed across the internet)

Can impact privacy (device tracking)

Finite (though large) address space

KEY DIFFERENCE FROM IP ADDRESS

Feature	MAC Address	IP Address
Type	Hardware (physical)	Logical (software)
OSI Layer	Layer 2 (Data Link)	Layer 3 (Network)
Scope	Local network (LAN)	Global/network-wide
Change	Hardcoded (spoofable)	Easily changeable
Example	00:1A:2B:3C:4D:5E	192.168.1.10

DNS (DOMAIN NAME SYSTEM)

WHAT IS DNS?

DNS is the phone book of the internet—it translates human-friendly domain names (e.g., www.google.com) into machine-friendly IP addresses (e.g., 142.250.183.206). Without DNS you'd have to remember IPs like 172.217.22.14 to visit sites.

WHAT DNS DOES IN A NETWORK (BASIC FLOW)

Your device asks: "What's the IP for this domain?"

A DNS server looks it up and replies with the IP.

Your device uses that IP to connect to the server.

DNS IS A SYSTEM, NOT JUST ONE MACHINE

A global hierarchy of DNS servers working together

They store records mapping domain names → IP addresses

WHERE DNS CAN LIVE

A) DNS servers on the internet (hold the records or know where to find them)
Examples:

Google DNS → 8.8.8.8, 8.8.4.4

Cloudflare DNS → 1.1.1.1

OpenDNS → 208.67.222.222

Your ISP's DNS

B) DNS resolver in your router

Home routers often act as a DNS forwarder

Forwards your device's queries to ISP/custom DNS

Often caches results for faster repeats

C) DNS cache on your device

OS/browser caches recent answers to avoid repeat lookups

How They Work Together (full resolution path)

Device checks local cache (OS/browser)

If not found → asks router

Router forwards to ISP DNS or custom (e.g., Google/Cloudflare)

If unknown, resolver queries root → TLD → authoritative servers for the final answer

In Short

Is DNS a server? Yes—served by specialized DNS servers.

Is DNS in my router? Often yes—as a forwarder/cache.

Where is DNS really? Distributed worldwide in a hierarchy of servers.