UNIT III

The Network Layer

The **network layer** is the **3rd layer** of the OSI (Open Systems Interconnection) model. Its main job is to **move data (packets) from the source device to the destination device across multiple networks**.

1. Main Purpose of the Network Layer

The network layer is responsible for:

a) **Logical addressing**

- Assigns **IP addresses** to devices
- Example: 192.168.1.1

b) **Routing**

- Determines the **best path** for data to travel from sender to receiver
- Works across **multiple networks (internetworking)**

c) **Packet forwarding**

- Moves packets from one router to another until they reach the destination

2. Key Functions of Network Layer

i. **Logical Addressing (IP Addressing)**

Every device gets a unique IP address.

Two types:

- **IPv4** → e.g., 192.168.0.1
- **IPv6** → e.g., 2001:db8::1

ii. Routing (Path Determination)

Routing decides:

"Which path should this packet take?"

Routers use:

- **Routing tables**
- **Routing algorithms**

Example:

- If multiple paths exist, router picks the **shortest or fastest path**

iii. Packetizing (Encapsulation)

- Data from transport layer is divided into **packets**
- Each packet contains:
  - Source IP
  - Destination IP
  - Data

iv. Fragmentation and Reassembly

- If packet is too large for a network:
  - It is **split into smaller fragments**
- At destination:
  - Fragments are **reassembled**

v. Internetworking

- Connects different types of networks
- Example:
  - Wi-Fi network → ISP → Internet → another network

3. Devices Used in Network Layer

Routers (Main Device)

- Operate at network layer
- Forward packets based on IP addresses

Other devices:

- Layer 3 switches (advanced networks)

4. Protocols of Network Layer

a. IP (Internet Protocol)

- Core protocol
- Responsible for addressing and delivery

b. ICMP (Internet Control Message Protocol)

- Used for error messages and diagnostics
- Example: ping

c. ARP (Address Resolution Protocol)

- Converts:
  - IP address → MAC address

d. Routing Protocols

Used by routers:

- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- BGP (Border Gateway Protocol)

5. Types of Delivery

Unicast

- One sender → one receiver

Broadcast

- One sender → all devices in network

Multicast

- One sender → group of devices

6. Connection Types

Connectionless (IP)

- No prior connection needed
- Each packet travels independently

Best-effort delivery

- No guarantee of:
  - Delivery
  - Order
  - Duplication

7. Example of Network Layer in Action

1. You open a website (e.g., google.com)
2. Your device sends request with destination IP
3. Router checks routing table
4. Packet travels through multiple routers
5. Reaches destination server
6. Response comes back the same way

8. Difference from Other Layers

Layer	Role
Transport	End-to-end communication (TCP/UDP)
Network	Path selection & IP addressing
Data Link	Local delivery (MAC address)

9. Simple Analogy

Think of sending a letter

- Transport layer → Writes the message
- **Network layer → Writes the destination address and chooses route**
- Data link → Delivers to next post office

Routing Algorithm

What is a Routing Algorithm?

A **routing algorithm** is a method used by routers to determine the **optimal path** for forwarding packets across a network.

Goals:

- Find shortest/fastest path
- Avoid congestion
- Adapt to failures
- Minimize delay and cost

Classification of Routing Algorithms

Routing algorithms are mainly divided into two broad categories:

1. Static Routing (Non-Adaptive)

- Routes are **manually configured**
- Do not change automatically

Features:

- Simple to implement
- No overhead
- Not suitable for large networks

Example: Small office networks

2. Dynamic Routing (Adaptive)

- Routes are updated **automatically**
- Routers exchange information

Features:

- Adapts to network changes
- More complex
- Used in large networks (like the Internet)

Main Types of Routing Algorithms

1. Distance Vector Routing

Concept:

- Each router shares its routing table with neighbors
- Uses **distance (cost) + direction (next hop)**

Algorithm Used:

- Bellman-Ford Algorithm

Example Protocol:

- RIP (Routing Information Protocol)

Advantages:

- Simple
- Easy to configure

Disadvantages:

- Slow convergence
- Routing loops (count-to-infinity problem)

2. Link State Routing

Concept:

- Each router builds a **complete map of the network**
- Uses shortest path algorithm

Algorithm Used:

- Dijkstra’s Algorithm

Example Protocol:

- OSPF (Open Shortest Path First)

Advantages:

- Fast convergence
- Accurate routing

Disadvantages:

- Requires more memory and CPU
- Complex to implement

3. Path Vector Routing

Concept:

- Maintains the **entire path (list of routers/AS)**

Example Protocol:

- BGP (Border Gateway Protocol)

Used in:

- Internet (between Autonomous Systems)

Advantages:

- Prevents loops
- Policy-based routing

Disadvantages:

- Complex
- Slower convergence

4. Flooding

Concept:

- Every incoming packet is sent to **all outgoing links**

Features:

- No routing table needed
- Guarantees delivery (if path exists)

Disadvantages:

- Massive redundancy
- Congestion risk

Controlled using:

- TTL (Time To Live)
- Sequence numbers

5. Hierarchical Routing

Concept:

- Network divided into **regions or areas**

Example:

- OSPF areas
- Internet divided into Autonomous Systems

Advantages:

- Scalable
- Reduces routing table size

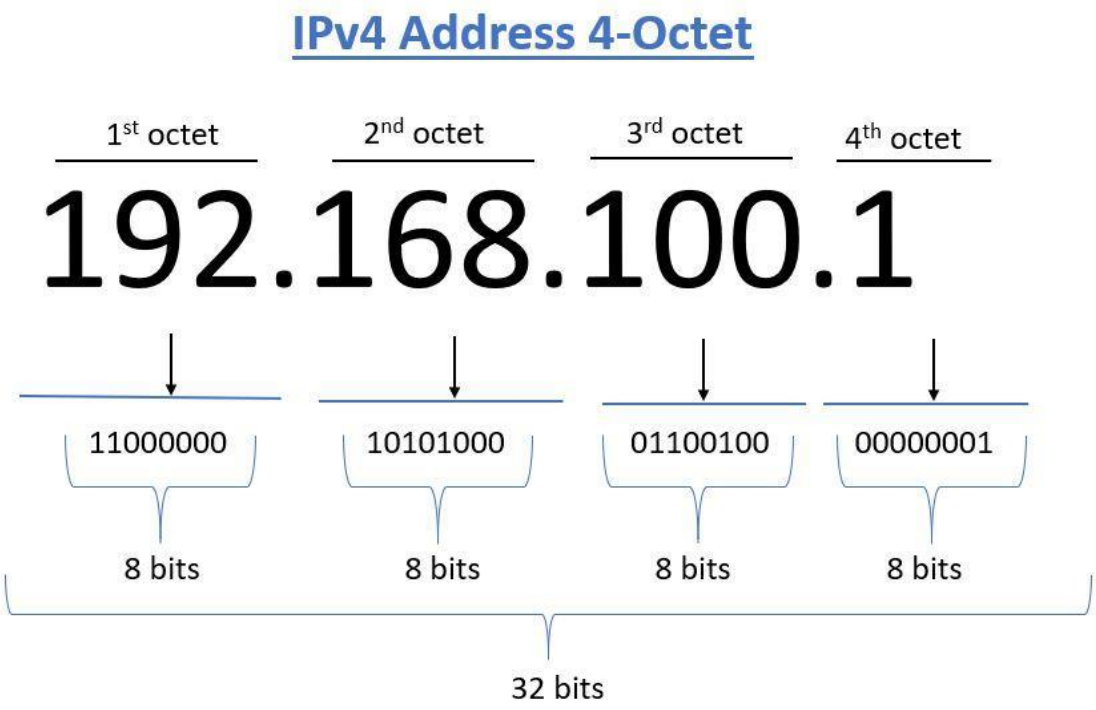
What are IP Addresses?

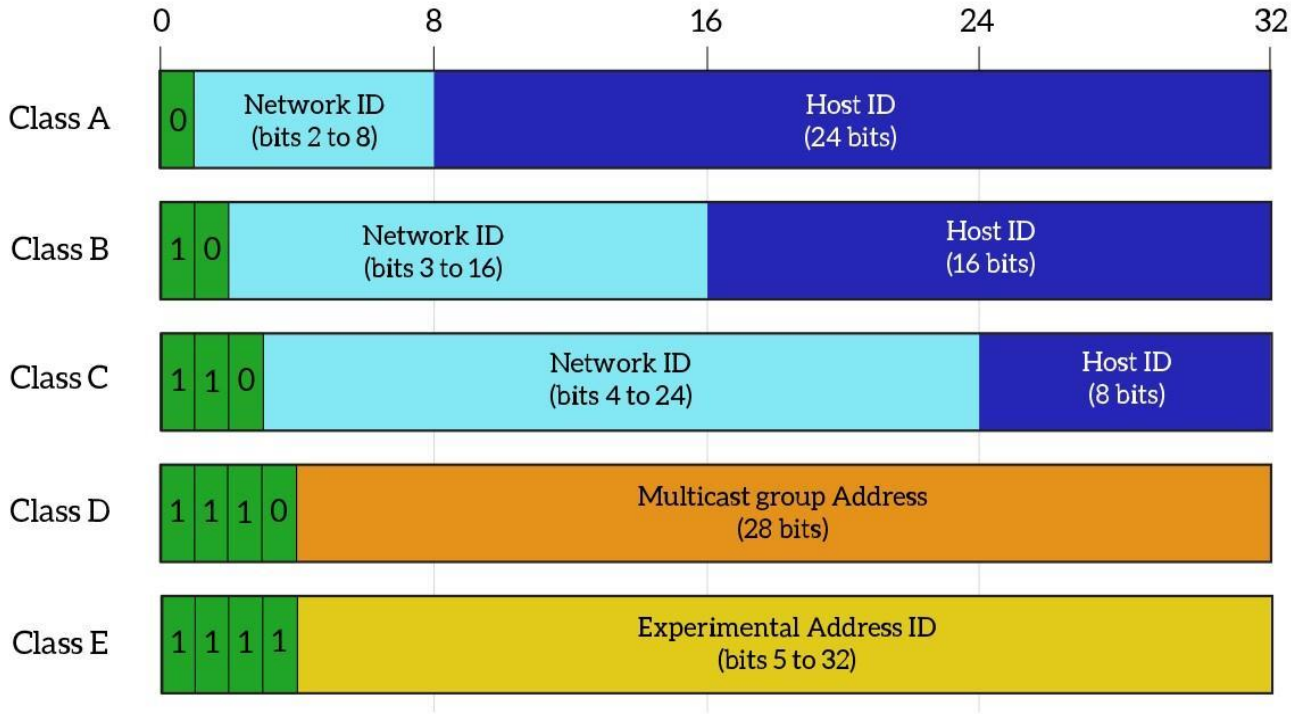
An **IP address (Internet Protocol address)** is a unique numerical identifier assigned to every device connected to a network. It allows devices to **communicate, send, and receive data** over networks like the Internet.

Think of it like a **home address**—it tells data where to go.

Types of IP Addresses

1. IPv4 (Internet Protocol version 4)





Network Host

192.168.001.123 IP Address

255.255.255.192 Subnet Mask

11000000.10101000.00000001.01111011 IP Address (Binary)

11111111.11111111.11111111.11000000 Subnet Mask (Binary)

11000000.10101000.00000001.01000000 Network ID (Binary)

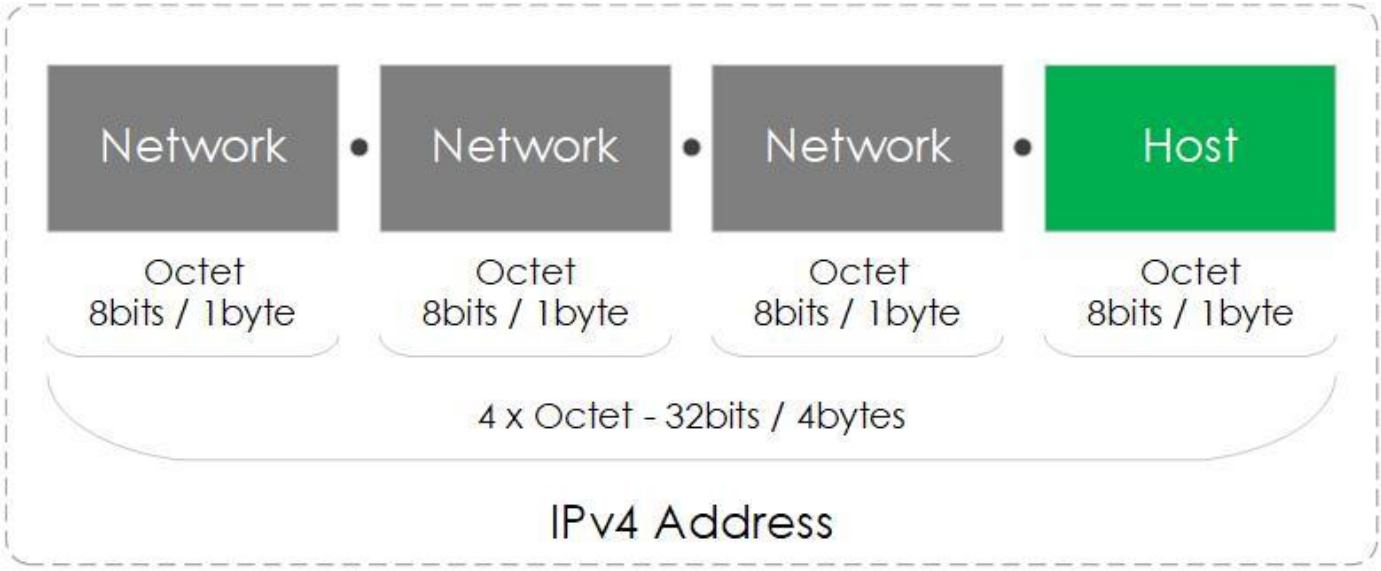
11000000.10101000.00000001.01111111 Broadcast (Binary)

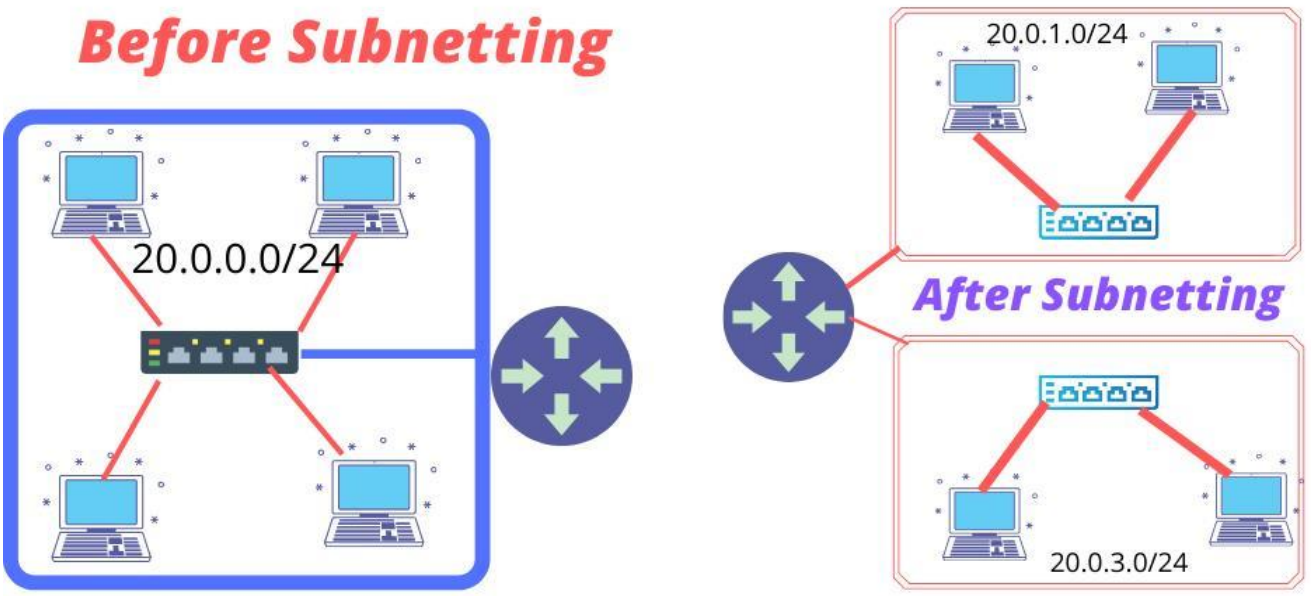
192.168.001.64 Network ID

192.168.001.1 First Host Address

192.168.001.126 Last Host Address

192.168.001.127 Broadcast





Features:

- 32-bit address
- Written in **dotted decimal format**
  Example: `192.168.1.1`

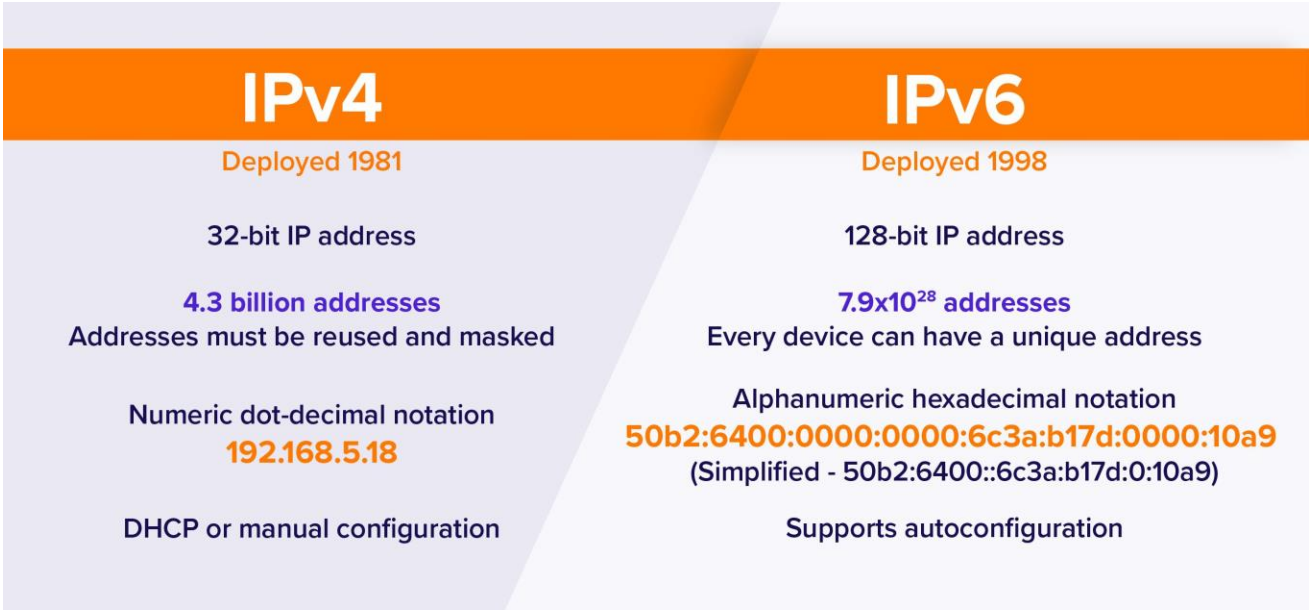
Structure:

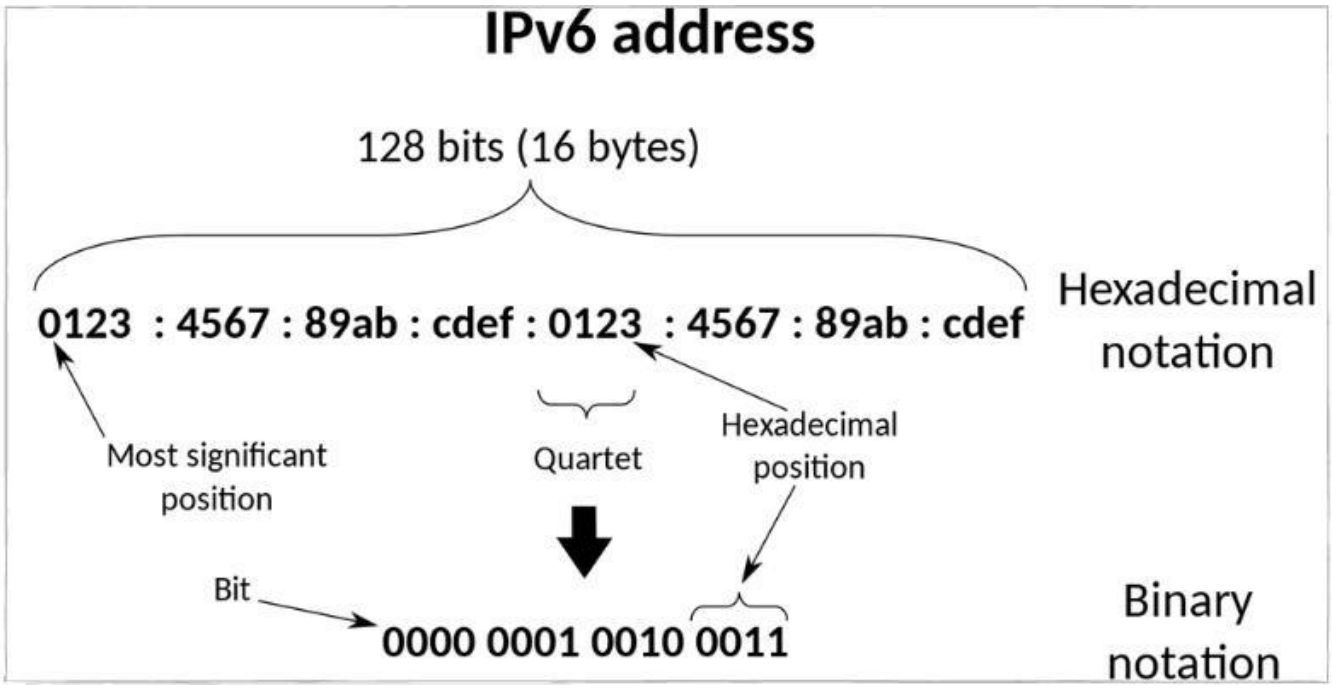
- Divided into **4 octets (8 bits each)**
- Range: `0.0.0.0` → `255.255.255.255`

Example:

- `192.168.10.5`

2. IPv6 (Internet Protocol version 6)





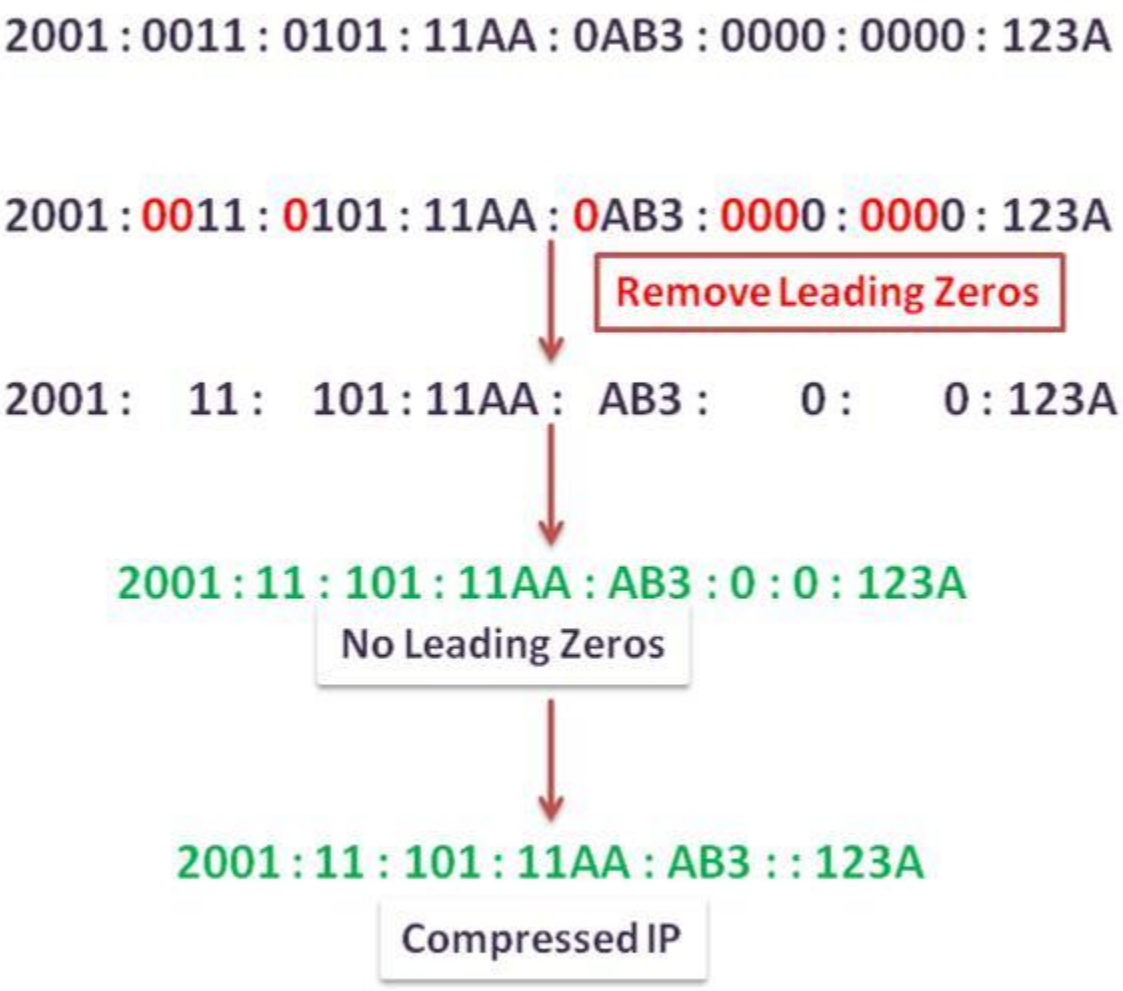
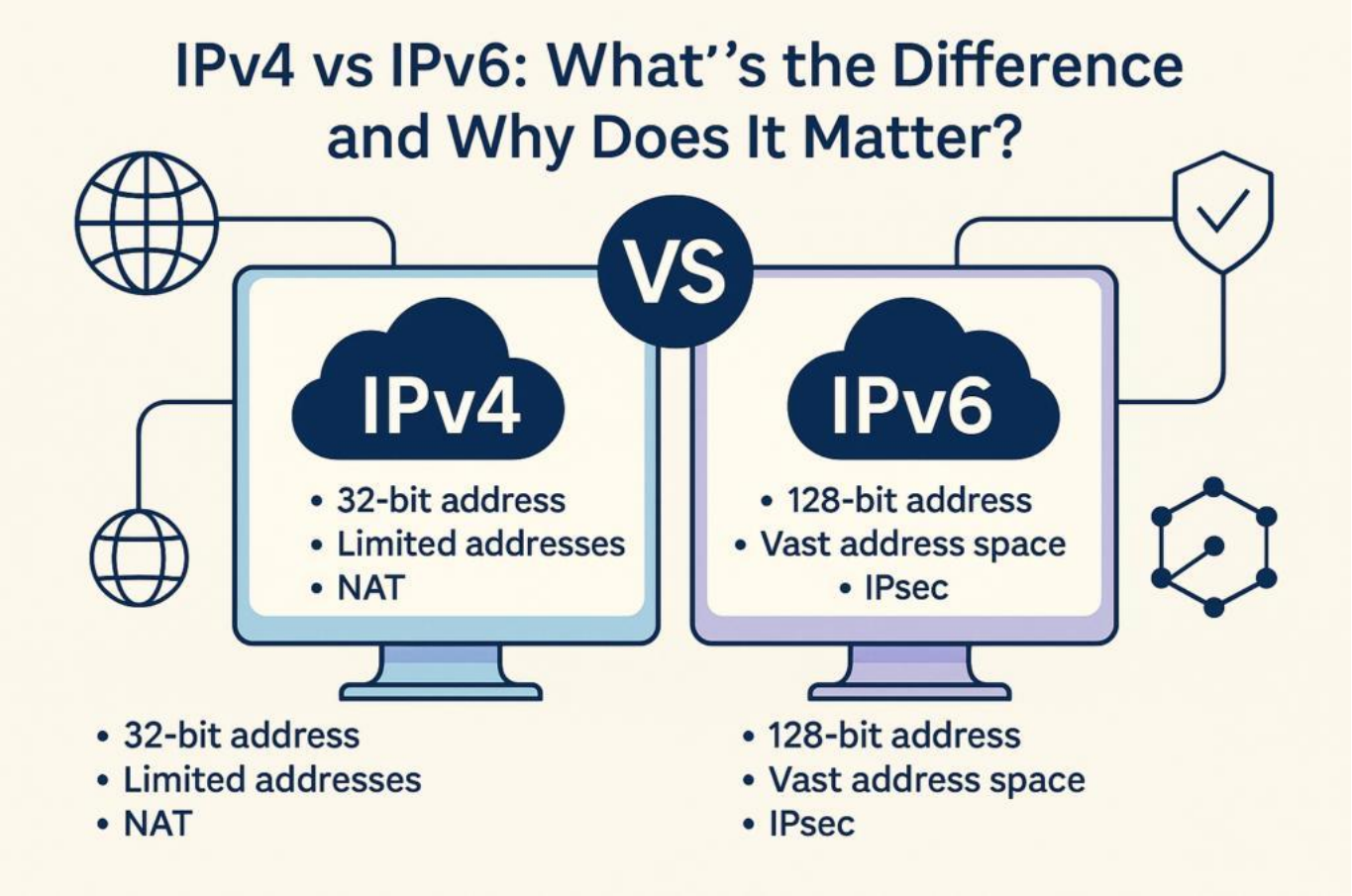


Figure 10: Rules to Shorten the IPv6 Address



Features:

- 128-bit address
- Written in **hexadecimal format**
  ☞ Example: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`

Advantages:

- Huge number of addresses
- Better security and efficiency

Classes of IPv4 Addresses

Class	Range	Usage
A	1.0.0.0 – 126.255.255.255	Large networks
B	128.0.0.0 – 191.255.255.255	Medium networks
C	192.0.0.0 – 223.255.255.255	Small networks
D	224.0.0.0 – 239.255.255.255	Multicasting
E	240.0.0.0 – 255.255.255.255	Experimental

Types of IP Address Based on Usage

1. Public IP Address

- Assigned by Internet Service Provider (ISP)
- Used on the Internet
- Unique globally

2. Private IP Address

- Used inside local networks
- Not accessible from the Internet

Private IP 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`

3. Static vs Dynamic IP

Static IP:

- Fixed address
- Does not change
- Used for servers

Dynamic IP:

- Assigned automatically (via DHCP)
- Changes over time

Special IP Addresses

- **Loopback Address:** `127.0.0.1` (used for testing)
- **Broadcast Address:** Sends data to all devices in network
- **Network Address:** Identifies the network
- **Default Gateway:** Router IP (e.g., `192.168.1.1`)

Subnet Mask

A **subnet mask** divides the IP into:

- Network part
- Host part

Example:

- IP: `192.168.1.10`
- Subnet Mask: `255.255.255.0`

Why IP Addresses are Important

- Identify devices
- Enable communication
- Help in routing data
- Support internet services

Simple Example

When you open a website:

1. Your device has an IP address
2. The server has an IP address
3. Data is sent using these addresses

How to Calculate Subnet Mask

What is a Subnet Mask?

A **subnet mask** determines:

- Which part of an IP address is the **network**
- Which part is the **host**

Example:

- IP: `192.168.1.10`
- Subnet Mask: `255.255.255.0`

Method 1: Using CIDR Notation (Most Important)

CIDR uses "/number" to show how many bits are for the network.

Step-by-Step Example: `/24`

Step 1: Understand the number

- `/24` means **24 bits are 1s (network part)**

Step 2: Convert to binary

```
11111111.11111111.11111111.00000000
```

Step 3: Convert to decimal

```
11111111 = 255
11111111 = 255
11111111 = 255
00000000 = 0
```

Final Subnet Mask:
255.255.255.0

Common CIDR to Subnet Mask

CIDR	Subnet Mask
/8	255.0.0.0
/16	255.255.0.0
/24	255.255.255.0
/25	255.255.255.128
/26	255.255.255.192
/27	255.255.255.224
/28	255.255.255.240
/29	255.255.255.248
/30	255.255.255.252

Method 2: Quick Shortcut (No Binary Needed)

Use this trick:

Look at the last octet:

Bits	Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

Example: `/27`

- /24 already gives: `255.255.255.0`
- Remaining bits = 3 bits

From table:

- 3 bits = **224**

Final answer:
255.255.255.224

Method 3: Based on Number of Hosts

Formula:

```
2^n - 2 = number of hosts
```

Where:

- n = number of host bits

Example: Need 30 hosts

Step 1:

```
2^5 - 2 = 30
```

So:

- Host bits = 5
- Total bits = 32

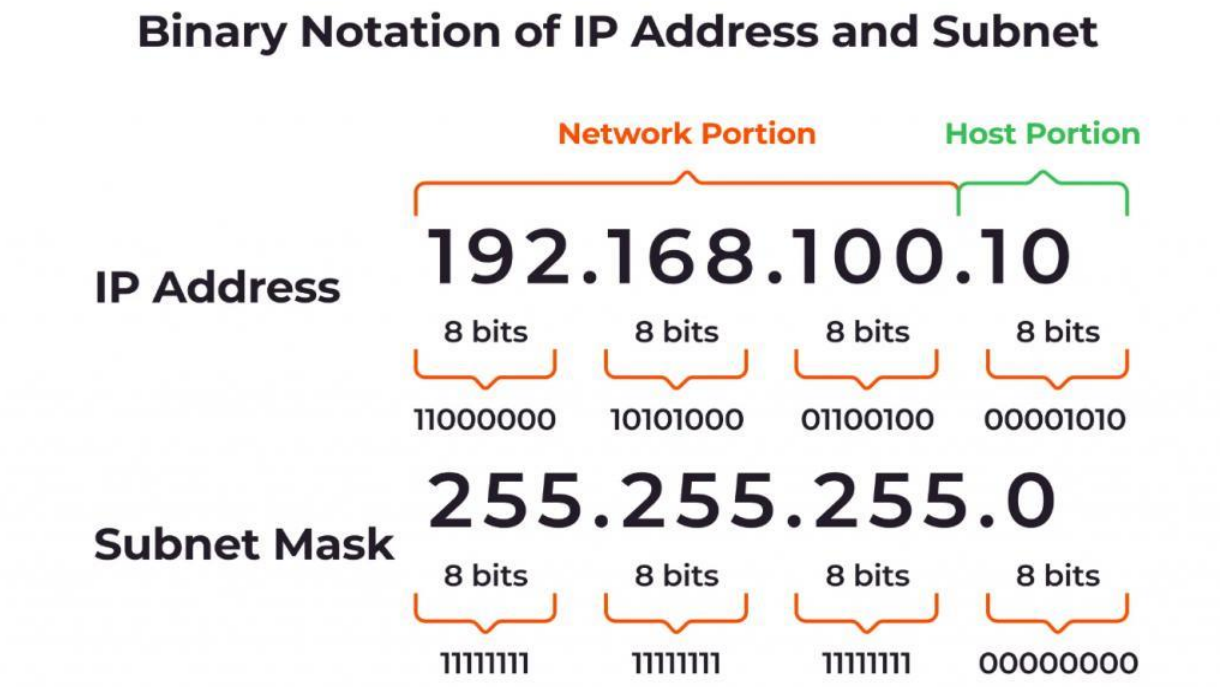
Step 2:

`32 - 5 = 27`

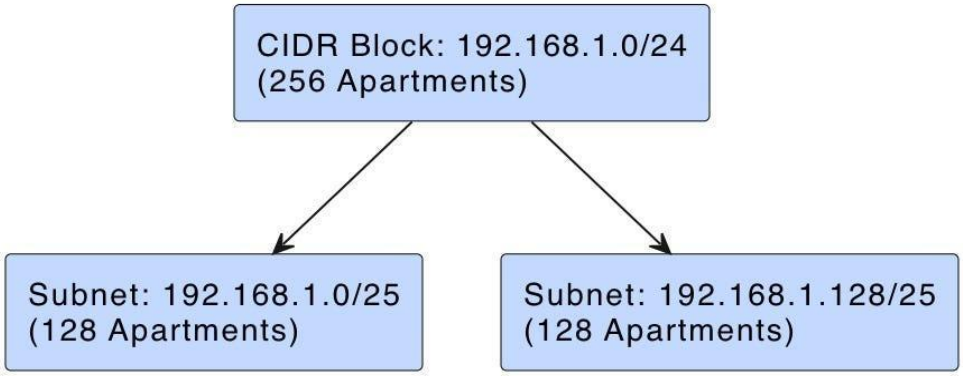
CIDR = `/27`

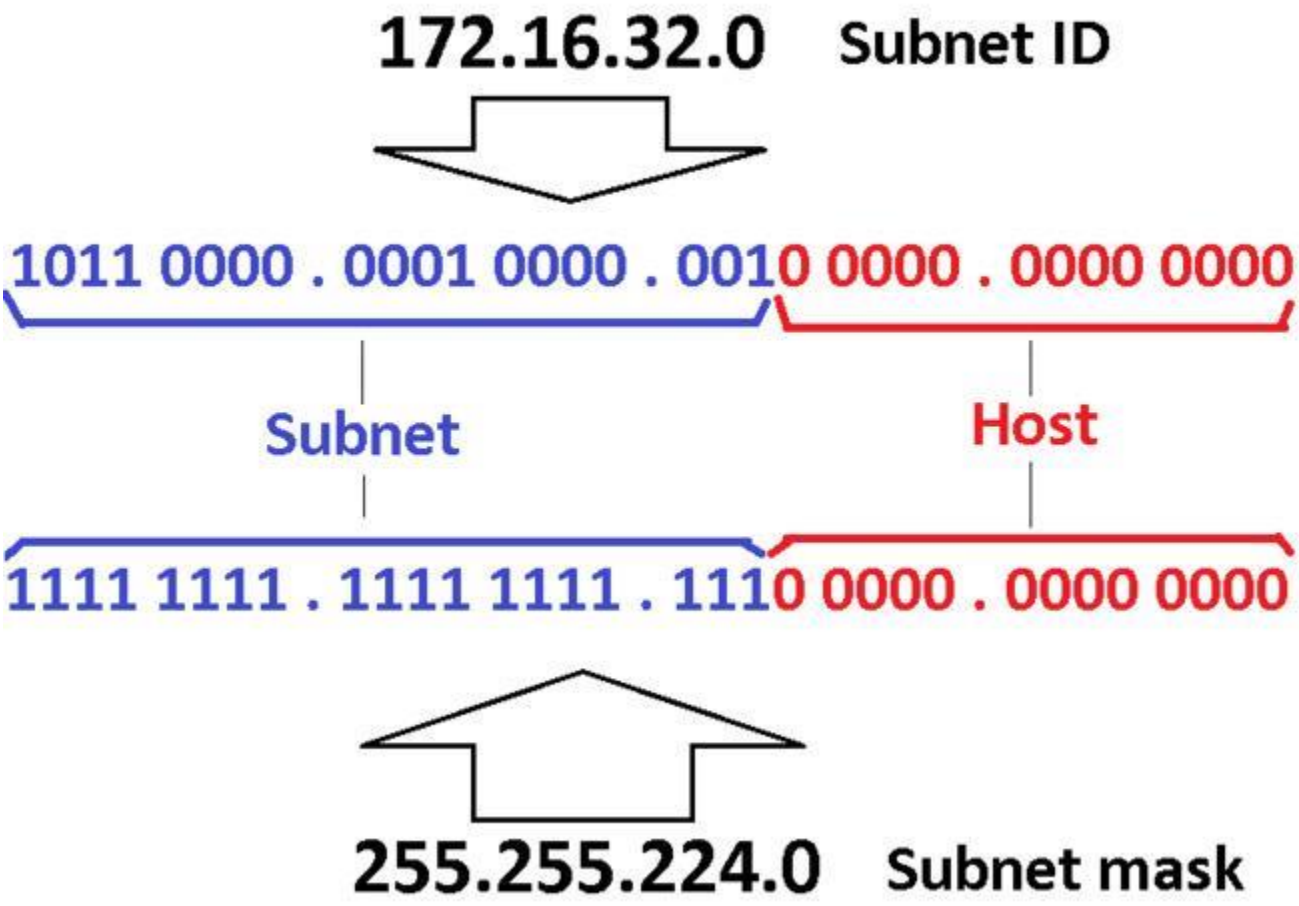
Subnet Mask: **255.255.255.224**

Visual Understanding



CIDR and Subnet Division

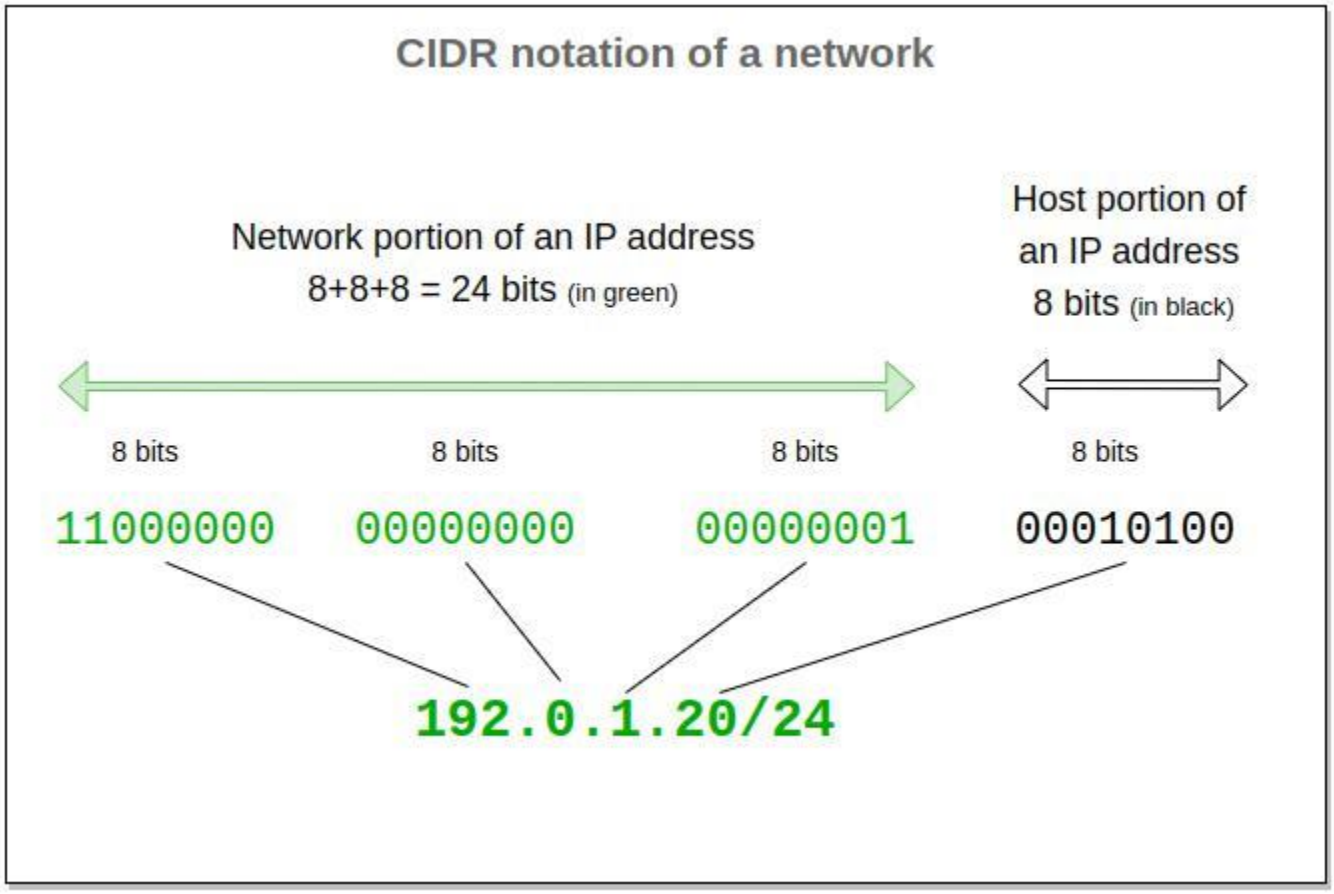


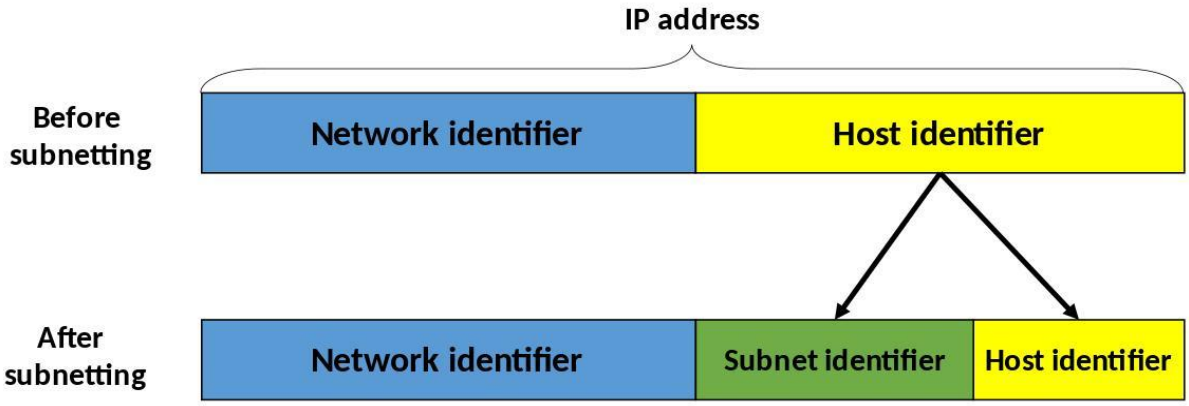


Subnet Masks - Binary

	1st octet	2nd octet	3rd octet	4th octet
172.0.0.0	Network	Host	Host	Host
Subnet Mask	11111111	00000000	00000000	00000000
192.4.0.0	Network	Network	Host	Host
Subnet Mask	11111111	11111111	00000000	00000000
192.168.1.0	Network	Network	Network	Host
Subnet Mask	11111111	11111111	11111111	00000000

- A "1" bit in the subnet mask means that the corresponding bit in the IP address should be read as a network number
- A "0" bit in the subnet mask means that the corresponding bit in the IP address should be read as a host bit.





Key Tips (Exam Focus)

- Always remember:
  - **/24 = 255.255.255.0**
- Learn last octet values (128,192,224,240…)
- Practice host calculation:
- `Hosts = 2^n - 2`
- Smaller subnet = fewer hosts but more networks

Final Summary

- Subnet mask = defines network & host portion
- CIDR (/number) makes it easy
- Use:
  - Binary method (accurate)
  - Shortcut method (fast in exams)
  - Host formula (for design questions)

SUBNETTING

What is Subnetting?

Subnetting = dividing one large network into **smaller sub-networks (subnets)**.

Why?

- Better performance
- Efficient IP usage
- Improved security

Key Concepts You MUST Know

- IP Address = Network part + Host part
- Subnet mask decides the split
- Formula:

```
Hosts per subnet = 2^n - 2
```

Where **n = number of host bits**

Step-by-Step Subnetting (Main Method)

Let’s use a real example

✅ Example:

Subnet this network:

`192.168.1.0/24` into **4 subnets**

Step 1: Understand given network

- `/24` → Subnet mask = `255.255.255.0`
- Total IPs:

```
2^(32-24) = 256 addresses
```

Step 2: Determine number of bits to borrow

We need **4 subnets**

```
2^2 = 4
```

Borrow **2 bits**

Step 3: New subnet mask

```
24 + 2 = /26
```

New subnet mask:
255.255.255.192

Step 4: Find block size

Formula:

```
Block size = 256 - last octet
256 - 192 = 64
```

So subnets increase by **64**

Step 5: List all subnets

Subnet	Network Address	First IP	Last IP	Broadcast
1	192.168.1.0	192.168.1.1	192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65	192.168.1.126	192.168.1.127
3	192.168.1.128	192.168.1.129	192.168.1.190	192.168.1.191
4	192.168.1.192	192.168.1.193	192.168.1.254	192.168.1.255

Visual Understanding

1st Subnet		
11000000 . 10101000 . 00000001	001	00000

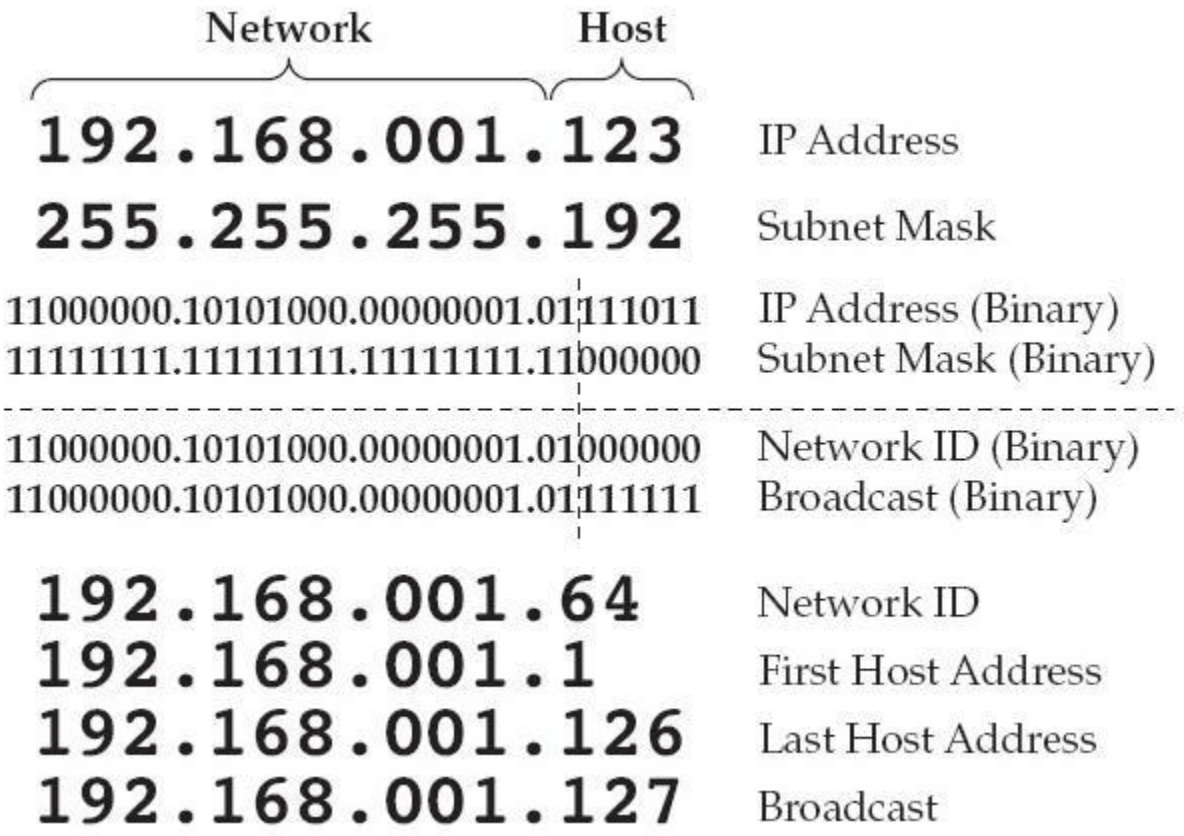
192.168.1.32

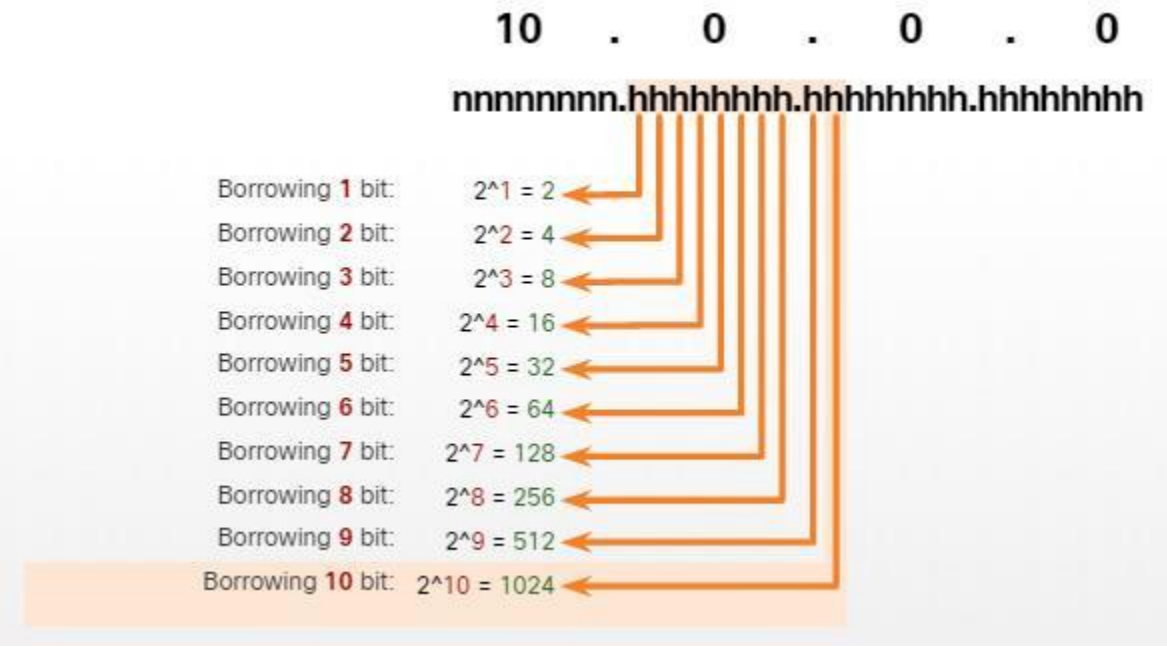
2nd Subnet		
11000000 . 10101000 . 00000001	010	00000

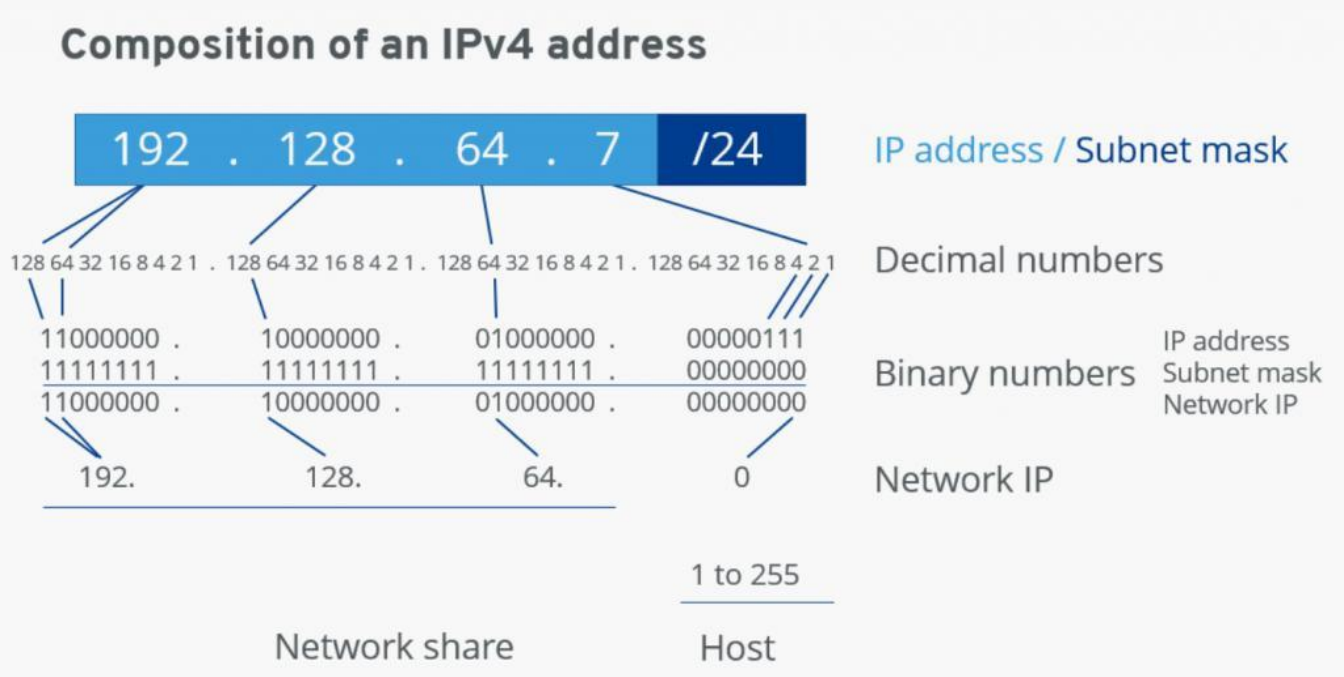
192.168.1.64

3rd Subnet		
11000000 . 10101000 . 00000001	011	00000

192.168.1.96




10 . 0 . 0 . 0
nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
Borrowing 1 bit: 2^1 = 2
Borrowing 2 bit: 2^2 = 4
Borrowing 3 bit: 2^3 = 8
Borrowing 4 bit: 2^4 = 16
Borrowing 5 bit: 2^5 = 32
Borrowing 6 bit: 2^6 = 64
Borrowing 7 bit: 2^7 = 128
Borrowing 8 bit: 2^8 = 256
Borrowing 9 bit: 2^9 = 512
Borrowing 10 bit: 2^10 = 1024


Composition of an IPv4 address
192 . 128 . 64 . 7 /24
IP address / Subnet mask
128 64 32 16 8 4 2 1 . 128 64 32 16 8 4 2 1 . 128 64 32 16 8 4 2 1 . 128 64 32 16 8 4 2 1
Decimal numbers
11000000 . 10000000 . 01000000 . 00000111
11111111 . 11111111 . 11111111 . 00000000
11000000 . 10000000 . 01000000 . 00000000
Binary numbers
IP address
Subnet mask
Network IP
192. 128. 64. 0
Network IP
1 to 255
Network share
Host

Shortcut Method (VERY IMPORTANT)

1. Find new subnet mask

Add bits based on number of subnets

2. Use block size

```
Block size = 256 - subnet value
```

3. Count subnets

Start from 0:

```
0, 64, 128, 192
```

Another Example (Exam Type)

Subnet: `192.168.10.0/24` into **8 subnets**

Step 1:

```
2^3 = 8 → borrow 3 bits
```

Step 2:

```
24 + 3 = /27
```

Step 3:

Subnet mask:
255.255.255.224

Step 4:

```
256 - 224 = 32
```

Subnets:

```
0, 32, 64, 96, 128, 160, 192, 224
```

Final Summary

Subnetting steps:

1. Identify network (CIDR)
2. Determine required subnets
3. Borrow bits
4. Calculate new subnet mask
5. Find block size
6. List all subnets

Supernetting

Supernetting is the opposite of subnetting.

Subnetting = divide one network into smaller ones

Supernetting = combine multiple smaller networks into **one larger network**

It's also called **route aggregation** or **CIDR (Classless Inter-Domain Routing)**.

Why Supernetting is used

- Reduces routing table size
- Improves router performance
- Makes networks easier to manage
- Used heavily in the Internet backbone

Basic Idea

Combine **contiguous (continuous)** networks into one summary network.

Example:

- 192.168.0.0/24
- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

These can be combined into:

192.168.0.0/22

Step-by-Step Supernetting

Example:

Combine these 4 networks:

- 192.168.0.0/24
- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

Step 1: Convert to Binary (last octet)

```
0   = 00000000
1   = 00000001
2   = 00000010
3   = 00000011
```

Step 2: Find Common Bits

All share the same first **22 bits**

So new prefix = **/22**

Step 3: Write Supernet

192.168.0.0/22

Subnet mask:
255.255.252.0

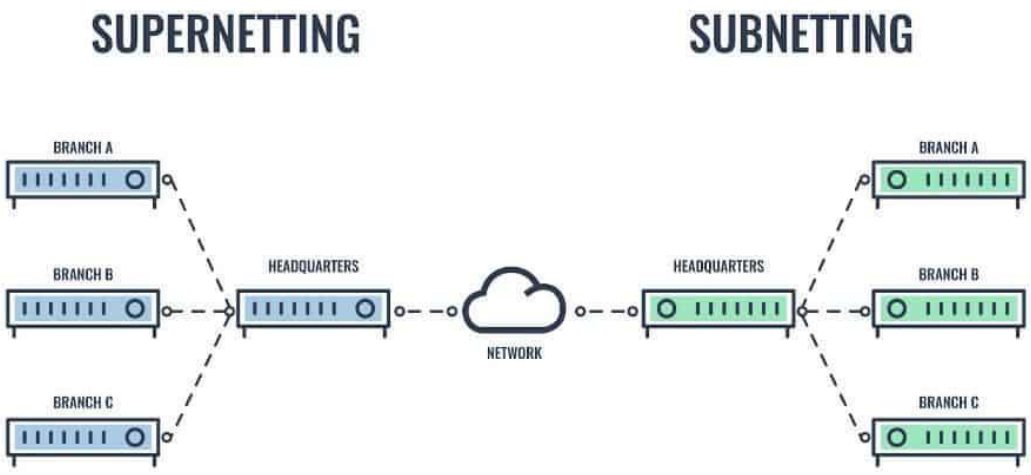
Visual Understanding

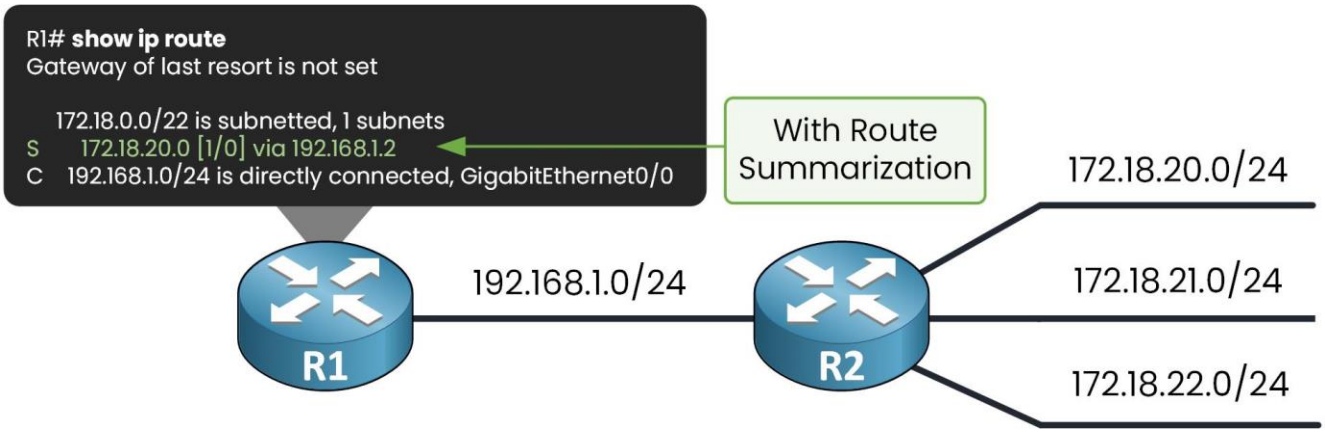
Route summarization (2/3)

Addresses	First Octet	Second Octet	Third Octet	Fourth Octet
192.168.98.0	11000000	10101000	01100010	00000000
192.168.99.0	11000000	10101000	01100011	00000000
192.168.100.0	11000000	10101000	01100100	00000000
192.168.101.0	11000000	10101000	01100101	00000000
192.168.102.0	11000000	10101000	01100110	00000000
192.168.105.0	11000000	10101000	01101001	00000000

Summary route is 192.168.96.0/20

192.168.96.0	11000000	10101000	01100000	00000000





Conditions for Supernetting

To combine networks, they must:

1. Be **contiguous (sequential)**
2. Have the **same subnet mask**
3. Number of networks must be **power of 2** (2, 4, 8, 16…)

Quick Shortcut Method

Step 1:

Count number of networks
Example: 4 networks

```
2^2 = 4 → remove 2 bits
```

Step 2:

Original = /24

```
24 - 2 = /22
```

Step 3:

Write first network address

Final:
192.168.0.0/22

Another Example

Combine:

- 10.0.0.0/24
- 10.0.1.0/24

Step:

```
2 networks → 2^1
24 - 1 = /23
```

Result:
10.0.0.0/23

Supernet vs Subnet

Feature	Subnetting	Supernetting
Purpose	Divide network	Combine networks
Prefix	Increases (/24 → /26)	Decreases (/24 → /22)
Usage	LAN design	Internet routing

Mobile Network Architecture

Mobile network architecture is the structure that allows mobile phones to **connect, communicate, and access services** like calls, SMS, and the internet while moving.

It is used in systems like:

- 2G (GSM)
- 3G
- 4G LTE
- 5G

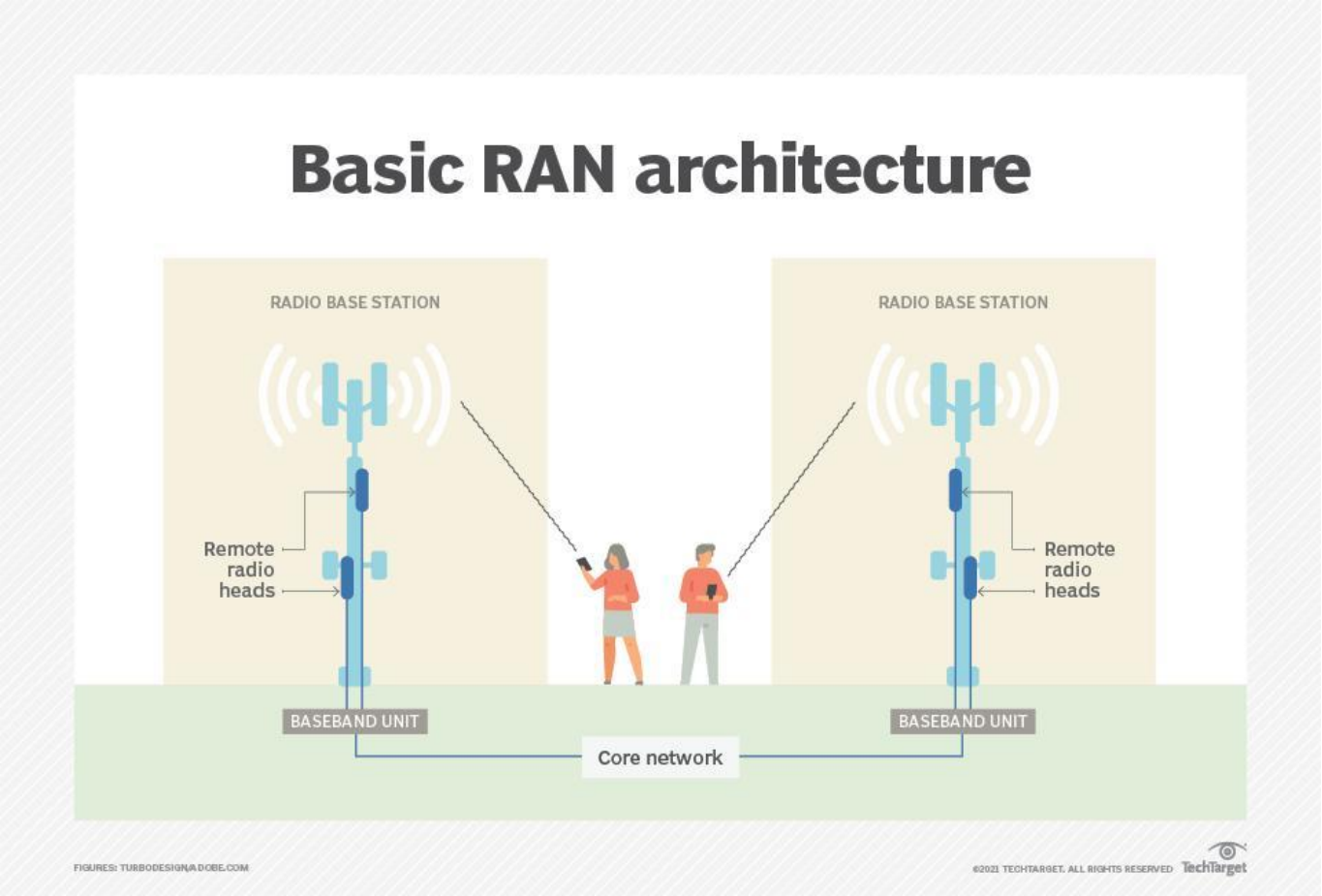
Main Idea

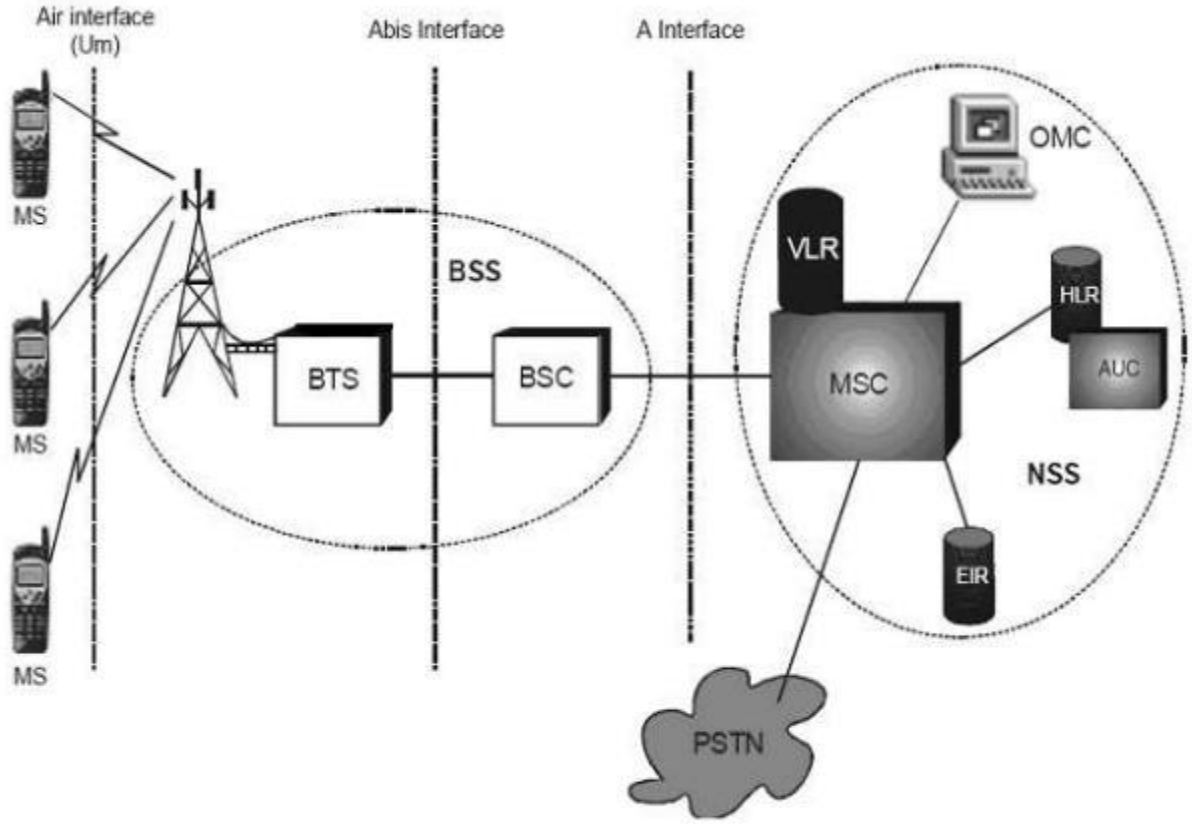
A mobile network is divided into **three major parts**:

1. **Radio Access Network (RAN)**

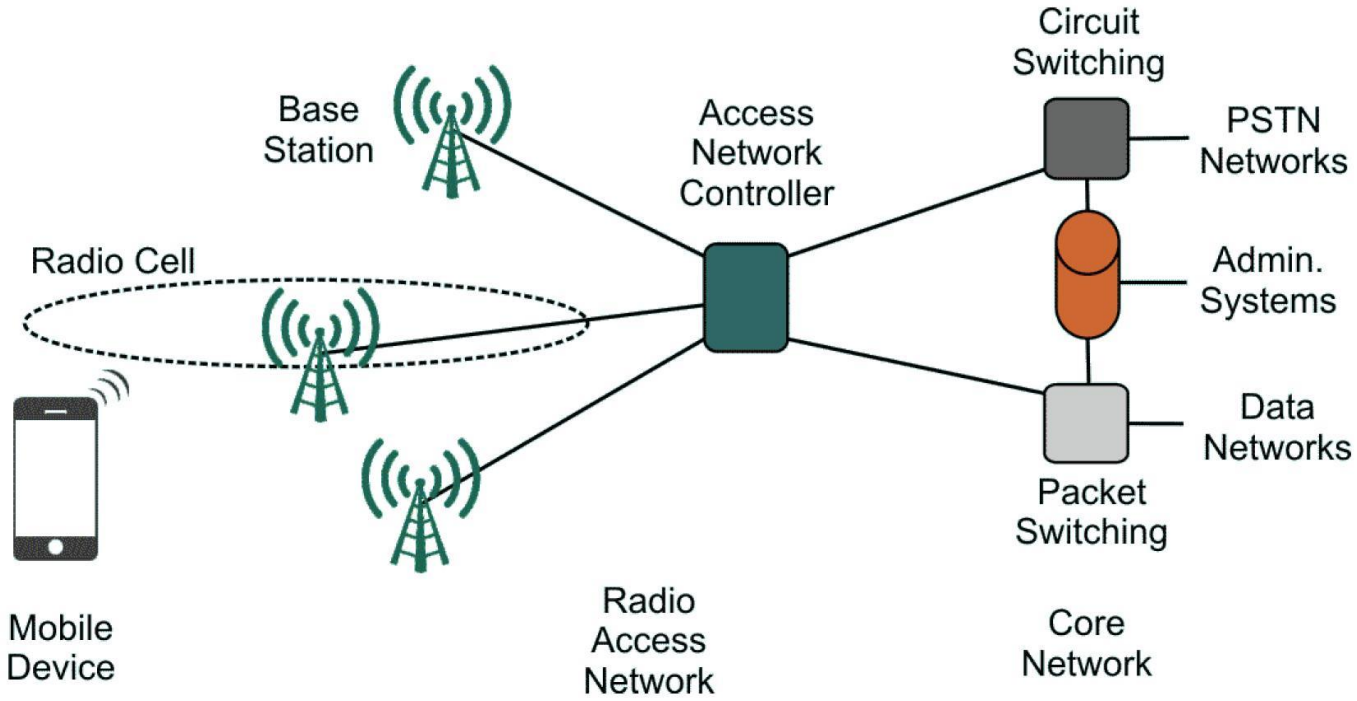
2. **Core Network (CN)**
3. **Backhaul Network**

1. Radio Access Network (RAN)





GSM Architecture overview



This is the part that connects your phone to the network.

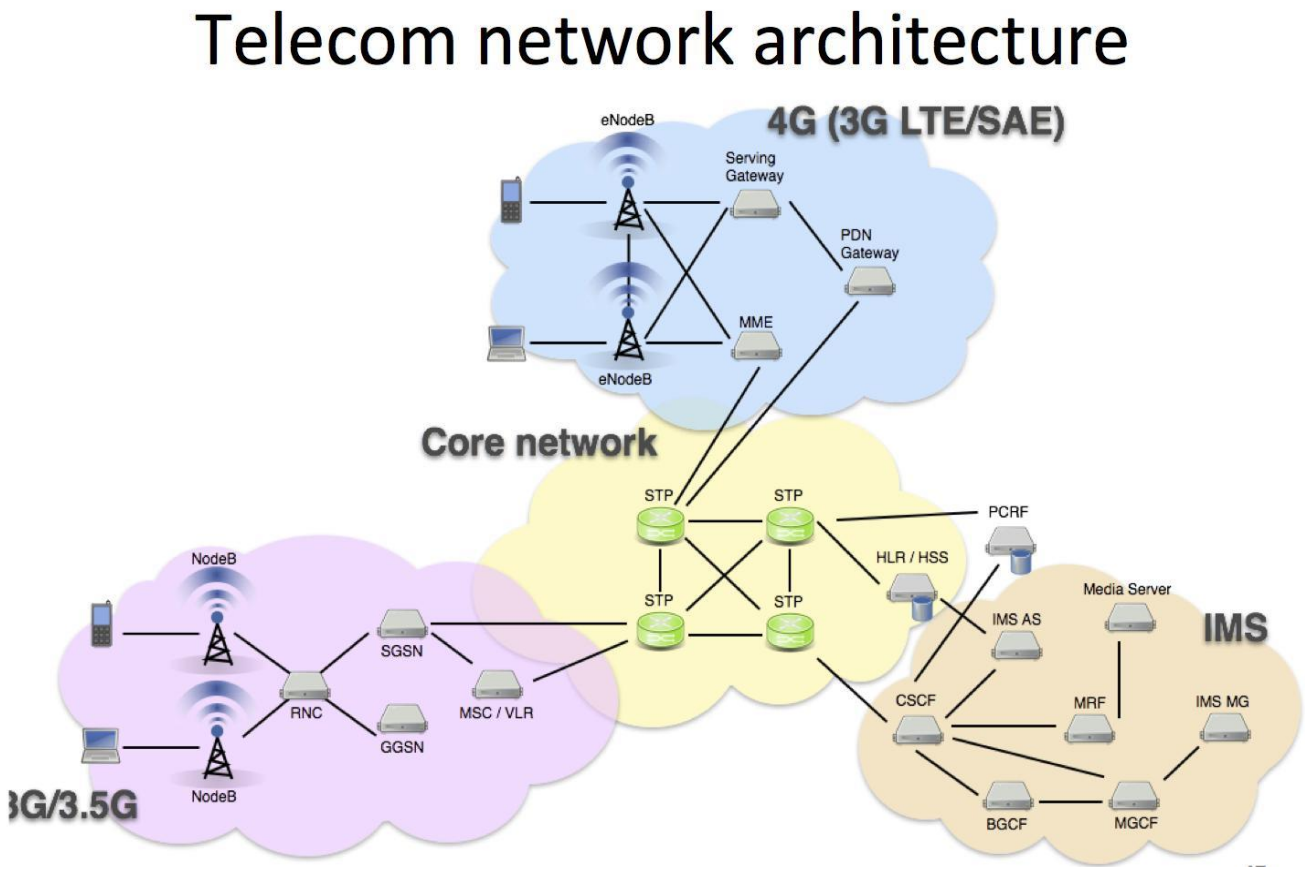
Components:

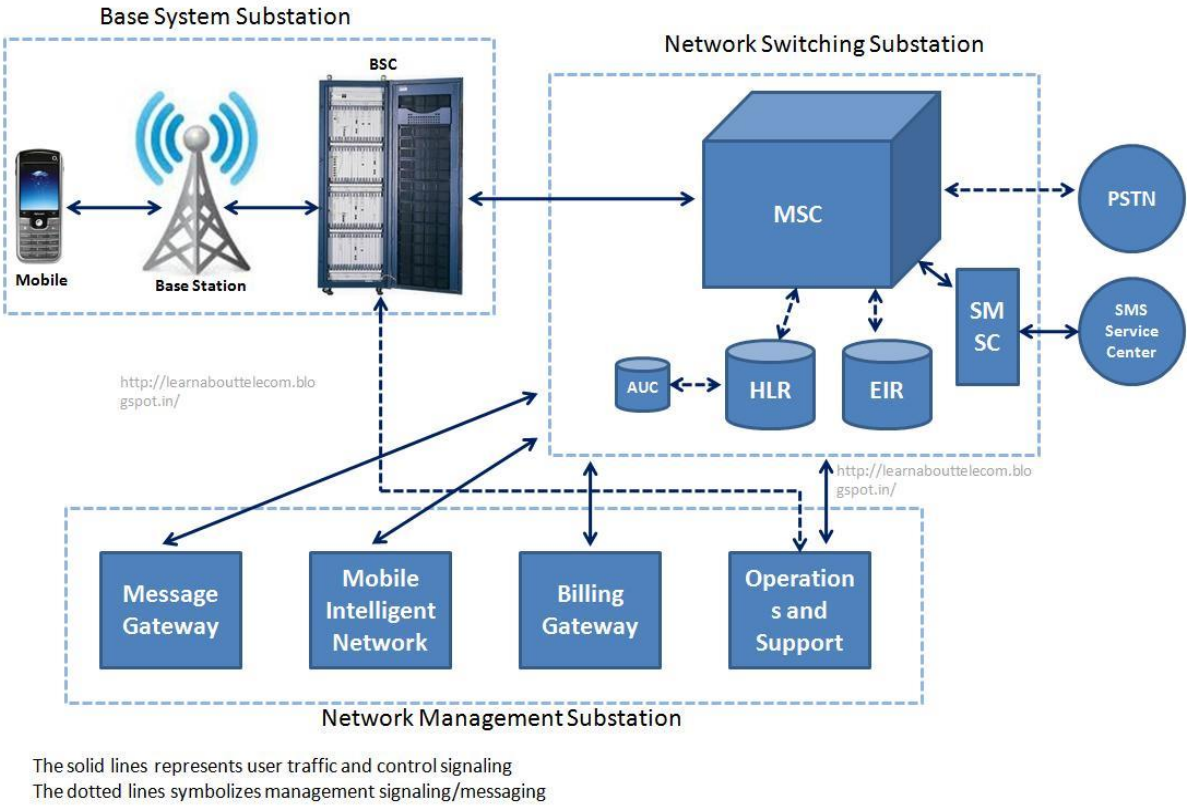
- **Mobile Device (UE – User Equipment)** → Your phone
- **Base Station**:
  - 2G → BTS (Base Transceiver Station)
  - 3G → Node B
  - 4G → eNodeB
  - 5G → gNodeB

Functions:

- Sends/receives radio signals
- Manages cell coverage
- Handles handover between towers

2. Core Network (CN)





This is the “brain” of the network.

Functions:

- Call routing
- Internet connectivity
- Authentication
- Mobility management

Key Elements (GSM example):

- **MSC (Mobile Switching Center)** → Handles calls
- **HLR (Home Location Register)** → Stores subscriber info
- **VLR (Visitor Location Register)** → Temporary user data
- **AuC (Authentication Center)** → Security
- **GGSN/SGSN** → Data services (internet)

3. Backhaul Network

Connects RAN to the Core Network.

Technologies:

- Fiber optic cables
- Microwave links
- Satellite (in remote areas)

How It Works (Simple Flow)

1. Your phone sends signal → nearest base station
2. Base station → Core Network
3. Core Network:
    - Authenticates user
    - Finds destination
4. Data/call routed to:
    - Another phone OR
    - Internet server

Architecture Evolution

2G (GSM)

- Circuit switching (voice only)

3G

- Introduced data + internet

4G LTE

- All IP-based network
- High-speed internet

5G

- Ultra-low latency
- Massive device support (IoT)

Key Features of Mobile Architecture

- **Mobility management** → works while moving
- **Handover** → switch between towers seamlessly
- **Scalability** → supports millions of users
- **Security** → authentication & encryption

Real-Life Example

When you make a call:

- Phone → nearest tower (RAN)
- Tower → Core Network
- Core routes call → destination user
- If you move → handover to another tower

Modulation Schemes — Analog vs Digital

Modulation is the process of **encoding information onto a carrier signal** (usually a high-frequency wave) so it can travel long distances.

Without modulation, signals (voice/data) cannot be transmitted efficiently over networks.

Types of Modulation

There are **two main categories**:

1. **Analog Modulation**
2. **Digital Modulation**

1. Analog Modulation

Parameters of Comparison	Analog Modulation	Digital Modulation
Value Range	It can represent any value that is between the specified range	It will represent only a set of values within the specified range
Signal separation	It is difficult to separate them	It can be easily separated
Wave	Sine Wave	Square wave
Definition	It is a continuous signal that can be changed over some time	It is a discrete signal carrying the information in binary form
Triggering	Single-stage triggering	Sequential triggering

Definition:

Analog modulation uses a **continuous signal** to modify the carrier wave.

Types of Analog Modulation

1. Amplitude Modulation (AM)

- Amplitude of carrier changes
- Frequency remains constant
-

Used in:

- AM radio broadcasting

2. Frequency Modulation (FM)

- Frequency of carrier changes
- Amplitude remains constant

Used in:

- FM radio
- High-quality audio transmission

3. Phase Modulation (PM)

- Phase of carrier changes

Less common, but forms the basis for digital schemes

Advantages of Analog Modulation

- Simple to implement
- Requires less bandwidth (in some cases)

Disadvantages

- Noise sensitive
- Lower quality over long distances

2. Digital Modulation

Definition:

Digital modulation uses **discrete (binary) signals (0s and 1s)** to modify the carrier.

Types of Digital Modulation

1. Amplitude Shift Keying (ASK)

- Amplitude changes between binary values

2. Frequency Shift Keying (FSK)

- Frequency switches between two values

3. Phase Shift Keying (PSK)

- Phase changes to represent bits

Example:

- BPSK, QPSK

4. Quadrature Amplitude Modulation (QAM)

- Combines amplitude + phase
- Very efficient

Used in:

- Wi-Fi
- 4G/5G networks
- Digital TV

Advantages of Digital Modulation

- More resistant to noise
- Higher data rates
- Better security

Disadvantages

- More complex
- Requires more bandwidth (sometimes)