IP Addressing (IPv4):

Structure: 32-bit address divided into 4 octets (e.g., 192.168.1.1).

Binary Representation: 11000000.10101000.00000001.00000001.
Classes & Ranges:

Class	Range	Default Subnet Mask	CIDR Notation	Purpose
A	1.0.0.0 to 126.255.255.255	255.0.0.0	/8	Large Networks (16M Hosts)
B	128.0.0.0 to 191.255.255.255	255.255.0.0	/16	Medium Networks (65K Hosts)
C	192.0.0.0 to 223.255.255.255	255.255.255.0	/24	Small Networks (256 Hosts)
D	224.0.0.0 to 239.255.255.255	-	-	Multicasting
E	240.0.0.0 to 255.255.255.255	-	-	Experimental

CIDR Notation (Classless Inter-Domain Routing):

Format: <IP Address>/<Prefix Length> — Example: 192.168.1.0/24.
Prefix Length (/24): Represents the number of bits used for the **Network ID**.
/24 → First 24 bits are **Network**; last 8 bits are **Hosts**.
Subnet Mask Equivalent: 255.255.255.0.
CIDR Flexible subnetting (no strict class boundaries), More efficient IP address allocation.
Example Calculation:
192.168.10.0/28:
Network Bits: 28
Host Bits: 4 → $2^4-2==14$ usable addresses.
Subnet Mask: 255.255.255.240.

Subnetting:

Purpose: Divides a large network into smaller subnetworks for better traffic management.
Formulas: Number of Subnets: 2^n, where n = number of subnet bits.
Hosts per Subnet: 2^h-2, where h = number of host bits.

Example:

IP Address: 192.168.20.0/26
Subnet Mask: 255.255.255.192
Subnets: 4 subnets
Hosts per Subnet: 62 (64 - 2 for Network & Broadcast)

VLSM

Purpose: VLSM allows subnetting a network into **variable-sized** subnets to **avoid IP wastage** based on actual host needs.

You're given a **network: 192.168.1.0/24**, You need to subnet it for:

Dept A: 100 hosts, Dept B: 50 hosts, Dept C: 25 hosts, Dept D: 10 hosts

Subnet creation using VLSM	
1. Dept A – Needs 100 hosts: Closest power of 2: 128 → 7 host bits Subnet: 192.168.1.0/25 Range: 192.168.1.0 – 192.168.1.127	3. Dept C – Needs 25 hosts: Closest power of 2: 32 → 5 host bits Subnet: 192.168.1.192/27 Range: 192.168.1.192 – 192.168.1.223
2. Dept B – Needs 50 hosts: Closest power of 2: 64 → 6 host bits Subnet: 192.168.1.128/26 Range: 192.168.1.128 – 192.168.1.191	4. Dept D – Needs 10 hosts: Closest power of 2: 16 → 4 host bits Subnet: 192.168.1.224/28 Range: 192.168.1.224 – 192.168.1.239

First & Broadcast Address

Network Address: The first IP in the subnet (all host bits = 0)
First Usable Address: Network Address + 1
Broadcast Address: The last IP in the subnet (all host bits = 1)
Last Usable Address: Broadcast Address – 1

Super netting:

Purpose: Combines multiple subnets into a larger address space to reduce routing entries.
Example: Networks: 192.168.1.0/24, 192.168.2.0/24 → Super net: 192.168.0.0/23.
Usage: Commonly used by ISPs to simplify routing.

Routing – Routing is the process of **selecting a path** for traffic in a network to reach its destination.

Static Routing:

Manually Configured:
Command: ip route <destination> <subnet mask> <next hop>
Example: ip route 192.168.1.0 255.255.255.0 192.168.2.1.
Pros: Simple, secure, no overhead.
Cons: Not scalable, requires manual updates.

Dynamic Routing:

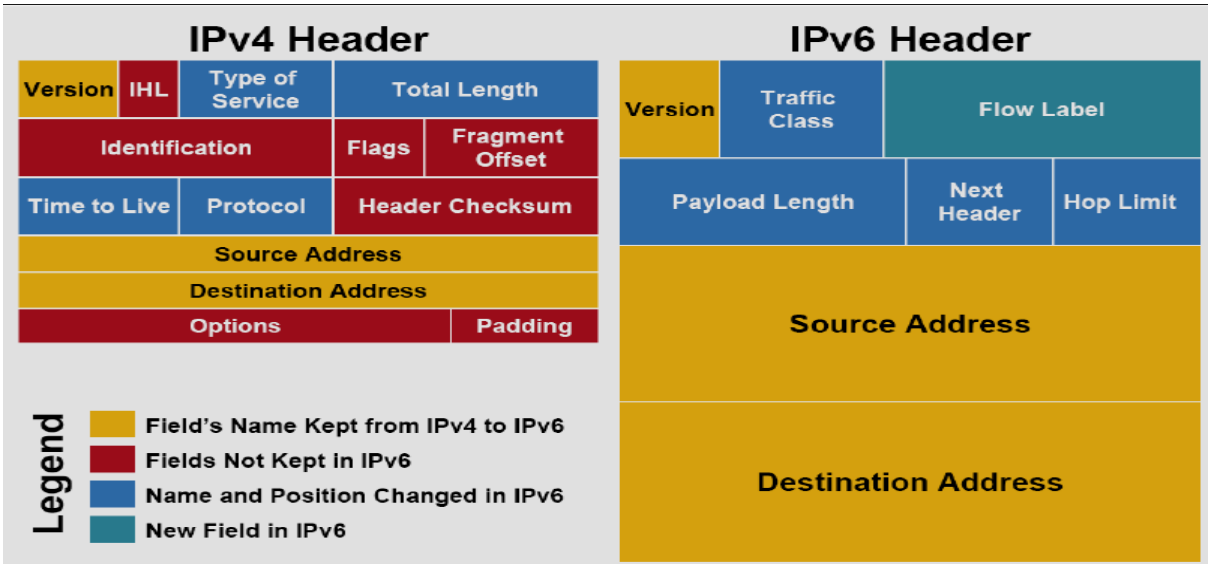
Automatically Configures Routes:
Protocols: OSPF, RIP, EIGRP.
Learns routes and adjusts based on network changes.

Distance Vector vs. Link State

Feature	Distance Vector (e.g., RIP, RIPv2)	Link State (e.g., OSPF, IS-IS)
Routing Method	Hop Count	Cost (Bandwidth-based)
Update Mechanism	Periodic (every 30s), to neighbours only	Triggered (when changes occur), to all
Convergence Time	Slow	Fast
Algorithm Used	Bellman-Ford	Dijkstra's Shortest Path First
Loop Prevention	Split Horizon, Poison Reverse	Sequence Numbers, LSA Synchronization

Bandwidth Usage	High (regular updates)	Efficient (only topology changes)
Usage Scenario	Small networks	Large, scalable enterprise networks

IP (Internet Protocol)



Field and its Description IP V 4	
Version – IP version (always 4 for IPv4)	Time to Live (TTL) – Limits packet lifespan (max hops)
Header Length – Header size in 32-bit words	Protocol – Indicates next layer protocol (e.g., TCP)
Type of Service – Defines priority & QoS	Header Checksum – Ensures header integrity
Total Length – Size of entire packet	Source Address – Sender's IP address
Identification – ID for fragment reassembly	Destination Address – Receiver's IP address
Flags – Control flags for fragmentation	Options – Optional control info
Fragment Offset – Fragment's position in original data	Padding – Fills to 32-bit alignment
Field and its Description IP V 6	
Version – IP version (always 6 for IPv6)	Next Header – Identifies type of next header (e.g., TCP, UDP, extension)
Traffic Class – Packet priority & QoS (like IPv4 ToS)	Hop Limit – Max hops before packet is discarded (like TTL in IPv4)
Flow Label – Marks packet flows for special handling	Source Address – 128-bit sender's IP address
Payload Length – Size of payload after the header	Destination Address – 128-bit receiver's IP address

IPv4: 32-bit, fragmented at routers.
IPv6: 128-bit, fragmentation handled by the sender.
Example of IPv6: 2001:0db8:85a3::8a2e: 0370:7334.

ICMP (Internet Control Message Protocol):

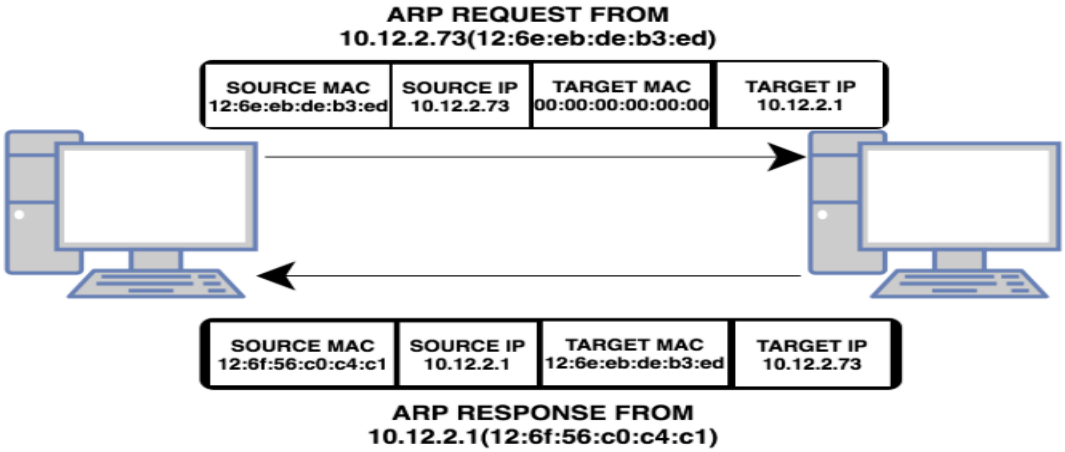
Purpose: Error reporting and diagnostics.

Usage: ping, traceroute

Common Messages:

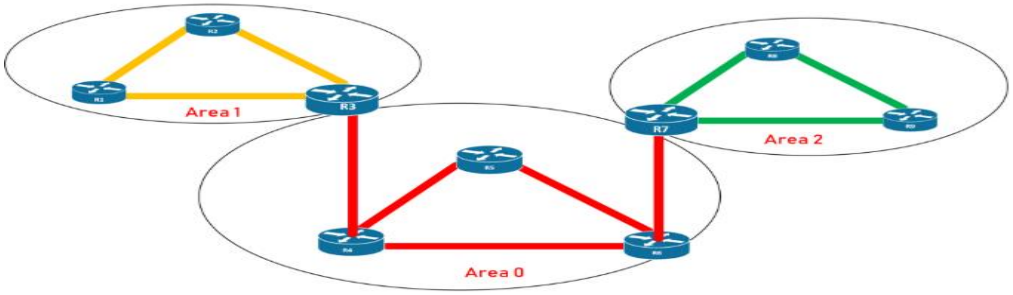
Type	Message	Description
0	Echo Reply	Response to ping request
3	Destination Unreachable	Network/Host unreachable
8	Echo Request	Ping to test reachability
11	Time Exceeded	TTL expired in transit

ARP (Address Resolution Protocol):



Function: Resolves IP addresses to MAC addresses.
Process: Broadcasts a request → Receives a unicast response.

OSPF (Open Shortest Path First):



Type: Link-State Protocol.
Metric: Cost based on bandwidth.
Area-based Design: Divides large networks into smaller areas (e.g., Area 0 - Backbone).
Usage Scenarios: Large enterprise networks, Fast convergence and loop-free topology

RIPv2 (Routing Information Protocol v2):**Type:** Distance Vector Protocol.

Max Hop Count: 15 (16 = Unreachable).
Updates: Sent every 30 seconds to neighbours.
Usage: Small networks with simple routing, Easy configuration but poor scalability.