AKTU · 3RD YEAR · SEMESTER 6 · BCS603

Computer Networks

Unit 3 — Network Layer

- Point-to-point networks
- Logical addressing
- Basic internetworking (IP, CIDR, ARP, RARP, DHCP, ICMP)
- Routing, forwarding and delivery
- Static and dynamic routing
- Routing algorithms and protocols
- Congestion control algorithms
- IPv6



DECODED BY

Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

theycotes.com

Point-to-Point Networks in Network Layer

POINT-TO-POINT NETWORK

A networking model where a dedicated physical or logical communication link directly connects exactly two network nodes without intermediate broadcast sharing.

- Packets are transmitted directly from source host/router to destination host/router across a dedicated link.
- No media access control (MAC) addressing is required on simple point-to-point links like PPP (Point-to-Point Protocol).
- Provides predictable bandwidth, low latency, and simplified packet processing at the network layer.
- Store-and-forward switching is utilized when packets traverse multiple point-to-point hops.

Logical Addressing: IPv4 Structure

IPv4 uses a 32-bit unique binary address formatted into four decimal octets separated by dots.

- Address Space: Contains a total of $2^{32} \approx 4.3 \times 10^9$ unique addresses.
- Address Composition: Divided into a Network Identifier (NetID) and a Host Identifier (HostID).
- Classful Addressing Scheme
  - Class A: NetID 8 bits (starts with 0), HostID 24 bits. Range: 1.0.0.0 to 127.255.255.255
  - Class B: NetID 16 bits (starts with 10), HostID 16 bits. Range: 128.0.0.0 to 191.255.255.255
  - Class C: NetID 24 bits (starts with 110), HostID 8 bits. Range: 192.0.0.0 to 223.255.255.255
  - Class D & E: Class D reserved for Multicast (224-239), Class E reserved for Research (240-255).

Classless Inter-Domain Routing (CIDR)

CIDR (CLASSLESS INTER-DOMAIN ROUTING)

An addressing scheme introduced to replace classful addressing, allowing variable-length subnet masking (VLSM) to prevent IP address exhaustion.

- Notation: Expressed as $\text{IP_Address}/n$, where n specifies the network prefix length in bits.
- Subnet Mask: An 32-bit mask with n contiguous 1s followed by $32 - n$ contiguous 0s.
- Number of Hosts: A block with prefix $/n$ provides 2^{32-n} total addresses and $2^{32-n} - 2$ usable host addresses.
- Aggregation: Allows route summarization (supernetting) to minimize the size of global routing tables.

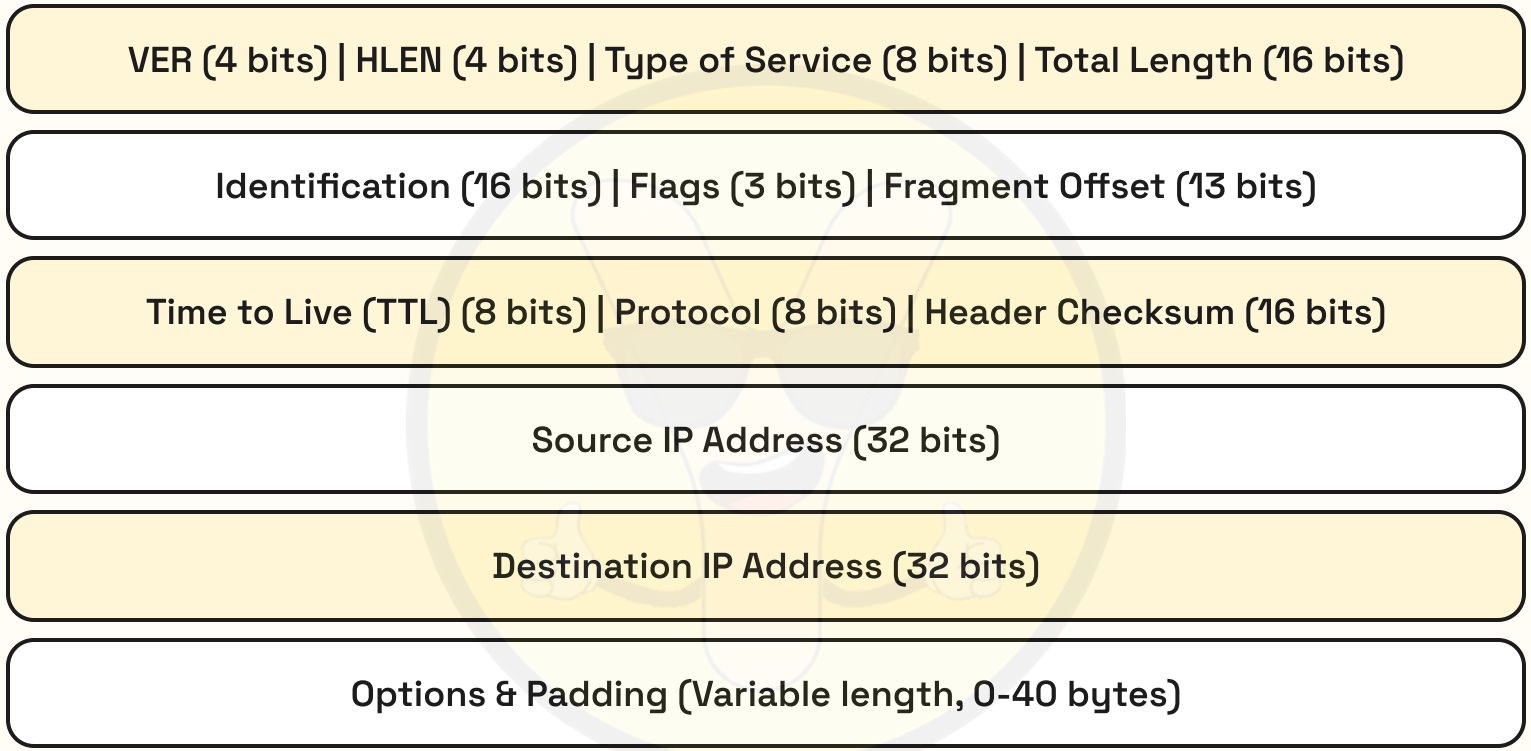
Worked Example: CIDR Subnet Calculation

An organization is assigned the block 192.168.10.0/26. Find the subnet mask, total addresses, usable host range, and broadcast address.

1. Step 1: Prefix length $n = 26$. Number of host bits $h = 32 - 26 = 6$.
2. Step 2: Subnet mask has 26 ones: 11111111.11111111.11111111.11000000, which equals 255.255.255.192.
3. Step 3: Total addresses = $2^6 = 64$. Usable addresses = $64 - 2 = 62$.
4. Step 4: Network Address (first IP) = 192.168.10.0.
5. Step 5: Broadcast Address (last IP) = 192.168.10.63 (setting all 6 host bits to 1).
6. Step 6: First usable host = 192.168.10.1; Last usable host = 192.168.10.62.

Subnet Mask: 255.255.255.192 | Total IP: 64 | Usable Hosts: 192.168.10.1 to 192.168.10.62 | Broadcast: 192.168.10.63

IPv4 Datagram Header Structure



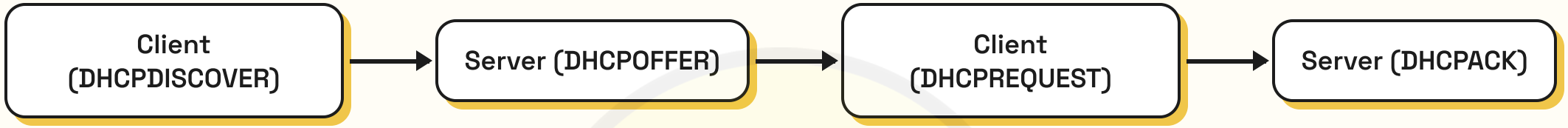
IPv4 Header Format: Standard minimum length is 20 bytes (HLEN = 5), maximum length is 60 bytes (HLEN = 15).

Address Resolution Protocol (ARP) and RARP

Protocols operating between Network and Data Link layers to map logical IP addresses to physical MAC addresses.

- ARP Function: Translates a known target IPv4 address into its corresponding physical MAC address.
- ARP Operation: Source broadcasts ARP Request (FF:FF:FF:FF:FF:FF). Target host responds with a unicast ARP Reply.
- ARP Cache: Dynamic table maintained by hosts to store recent IP-to-MAC mappings and reduce broadcast traffic.
- RARP (Reverse ARP): Maps a known physical MAC address to a dynamic logical IP address.
- RARP Limitation: Used historically by diskless workstations; largely replaced by BOOTP and DHCP.

DHCP DORA Process Flow



DHCP 4-Way Handshake: Enables dynamic, automated IP address allocation, subnet mask configuration, default gateway, and DNS configuration.

Internet Control Message Protocol (ICMP)

A supporting protocol in the IPv4 suite used by network devices to send error reports and operational information.

- Encapsulation: ICMP messages are directly encapsulated inside IPv4 datagrams (Protocol field = 1).
- ICMP Message Categories
  - Error-Reporting Messages: Destination Unreachable, Source Quench, Time Exceeded (TTL expired), Parameter Problem.
  - Query Messages: Echo Request / Echo Reply (used by ping), Router Solicitation / Advertisement.
- Ping Utility: Uses ICMP Echo Request (Type 8) and Echo Reply (Type 0) to test network layer reachability.
- Traceroute Utility: Uses ICMP Time Exceeded (Type 11) messages with incrementing TTL values to map packet paths.

Routing, Forwarding, and Delivery

The core responsibilities of the network layer for transmitting packets end-to-end across interconnected networks.

- Delivery: The process of handling a packet by lower layers (Direct Delivery to local host, Indirect Delivery via router).
- Forwarding: The local action of placing a packet on an outgoing interface based on routing table lookups.
- Routing: The global process of determining optimal paths from source to destination across network topology.
- Connectionless Delivery: Each IPv4 datagram is treated independently and routed separately (Datagram Approach).
- Longest Prefix Matching: Forwarding rule where the router selects the routing table entry with the longest prefix matching the destination IP.

Comparison: Static Routing vs. Dynamic Routing

Parameter	Static Routing	Dynamic Routing
Route Determination	Manually configured by administrator	Automatically computed via routing protocols
Adaptability to Failures	No auto-rerouting on link failure	Automatically updates and reroutes paths
Overhead & CPU Usage	Zero dynamic processing overhead	Requires router CPU, memory, and bandwidth
Routing Protocols Used	None required	RIP, OSPF, BGP, EIGRP
Scalability	Suitable for small networks only	Highly scalable for large/complex networks
Security	High (no protocol traffic exchanged)	Requires authentication mechanisms

Distance Vector Routing Algorithm

An iterative, asynchronous, decentralized algorithm based on the Bellman-Ford equation.

- Bellman-Ford Formula: $D_x(y) = \min_v\{c(x,v) + D_v(y)\}$, where $c(x,v)$ is cost to neighbor v.
- Vector Exchange: Each node periodically sends its entire distance vector table to its immediate neighbors only.
- Convergence: Iterates until no node receives updated cost estimates from its neighbors.
- Count-to-Infinity Problem: Slow convergence when a link breaks, leading to routing loops.
- Mitigation Techniques: Split Horizon, Poison Reverse, and Triggered Updates.

Link State Routing Algorithm

A centralized algorithm where every router possesses complete topological knowledge of the entire network.

- Link State Advertisement (LSA): Each router floods information about its local connected links to all routers.
- Dijkstra's Shortest Path Algorithm: Computes lowest-cost paths from the source node to all other nodes.
- Dijkstra's Algorithm Steps
  - Initialization: Set distance to source = 0, distance to all other nodes = ∞. Set empty visited set S.
  - Node Selection: Select unvisited node u with minimum tentative distance.
  - Update Neighbors: For each unvisited neighbor v of u, update $D(v) = \min(D(v), D(u) + c(u, v))$.
  - Repeat: Add u to S until all nodes are visited.
- Key Feature: Fast convergence and immunity to count-to-infinity problems.

Comparison: RIP vs. OSPF vs. BGP

Feature	RIP	OSPF	BGP
Type	Interior Gateway (IGP)	Interior Gateway (IGP)	Exterior Gateway (EGP)
Algorithm	Distance Vector	Link State	Path Vector
Metric	Hop Count (Max 15)	Cost / Bandwidth	Path attributes / Policy
Transport Protocol	UDP (Port 520)	IP Direct (Protocol 89)	TCP (Port 179)
Scope	Small enterprise networks	Large enterprise / Autonomous System	Inter-domain Internet routing
Convergence	Slow	Fast	Variable (Policy driven)

Principles of Congestion Control

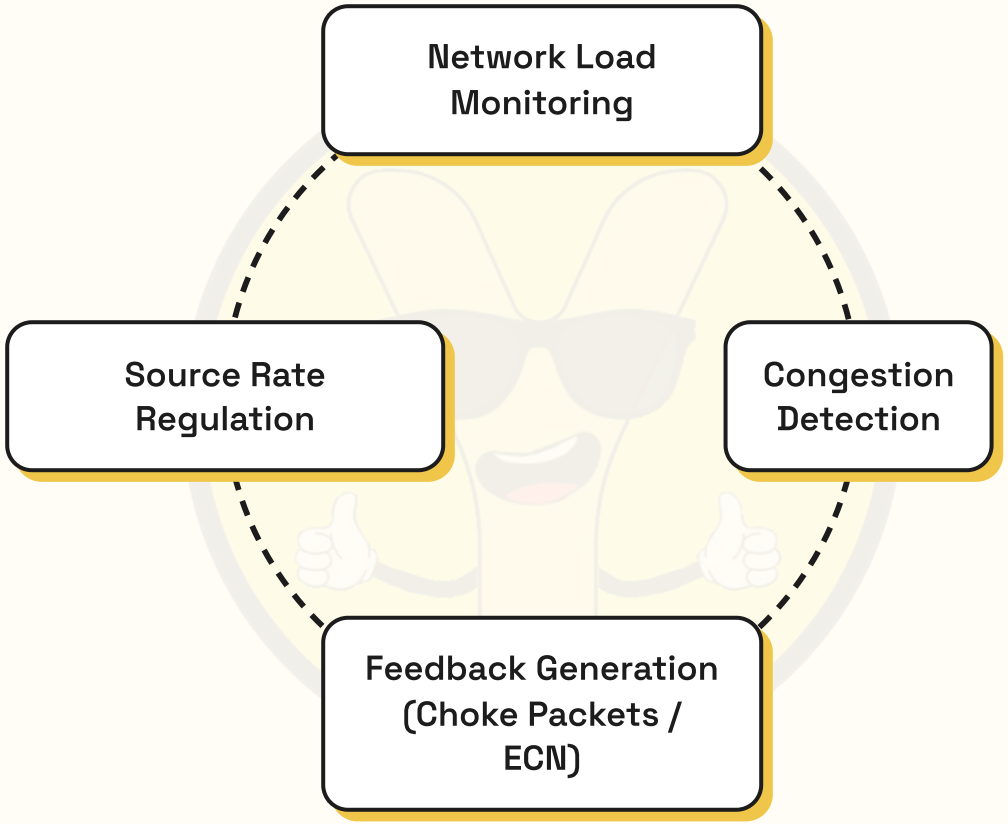
Congestion occurs when incoming traffic to a network region exceeds available router buffer and link bandwidth capacity.

- Congestion Effect: Packet delays increase dramatically; when buffer space is exhausted, packets are dropped.
- Open-Loop Control (Prevention): Policies designed to prevent congestion before it happens (e.g., traffic shaping, admission control).
- Closed-Loop Control (Removal): Dynamic mechanisms operating on active feedback to clear congestion.
- Explicit Feedback: Network devices send explicit notification signals back to source (e.g., Choke Packets, ECN bits).
- Implicit Feedback: Source infers congestion from network performance degradation (e.g., packet timeouts, duplicate ACKs).

Congestion Control: Leaky Bucket vs. Token Bucket

Parameter	Leaky Bucket Algorithm	Token Bucket Algorithm
Output Rate	Strictly constant / rigid output rate	Allows bursty traffic up to bucket capacity
Token Storage	No tokens; packets stored in bucket	Tokens accumulate at constant rate r
Packet Handling	Fails/drops packets if bucket overflows	Transmits burst equal to available tokens
Application	Traffic policing / rigid shaping	Traffic shaping with burst tolerance
Idle Period Impact	Idle time is lost (bucket empties)	Tokens accumulate for future bursts
Max Burst Calculation	Not allowed (constant outflow)	Max Burst Size $S = b + r \times t$

Congestion Prevention and Recovery Flow



Closed-Loop Feedback System: Continuously monitors load, detects congestion thresholds, and signals end systems to reduce transmission rates.

IPv6 Architecture and Header Format

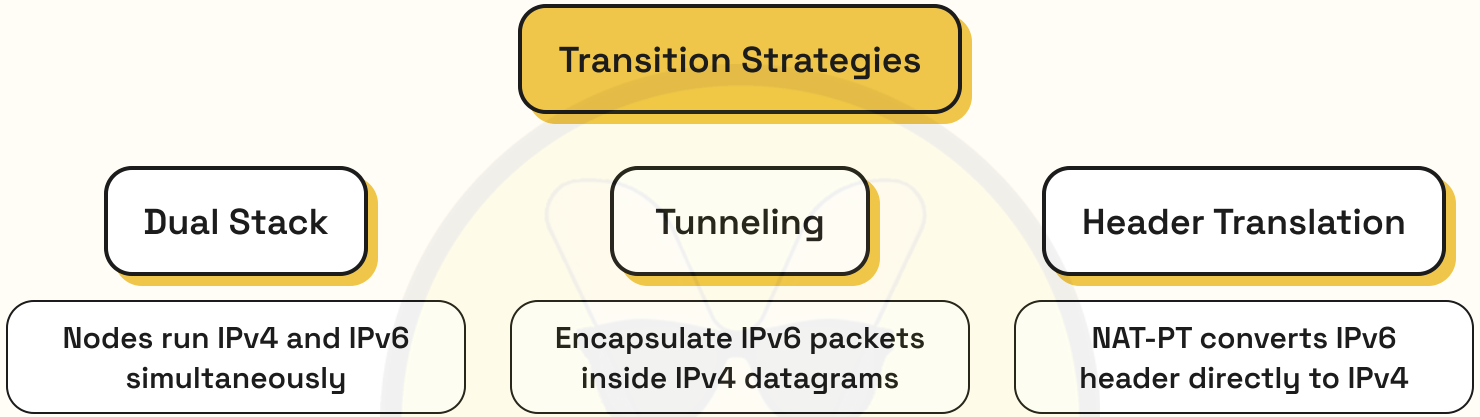
IPv6 was developed to replace IPv4, offering a massive 128-bit address space and streamlined header processing.

- Address Length: 128 bits long, represented as 8 groups of 4 hexadecimal digits separated by colons.
- Address Capacity: Provides $2^{128} \approx 3.4 \times 10^{38}$ total addresses.
- Fixed Header Size: Base header size fixed at 40 bytes (8 fields), accelerating router processing speed.
- Simplified Fields: IPv4 fields like HLEN, Identification, Flags, Fragment Offset, and Header Checksum were removed or modified.
- Extension Headers: Optional information is inserted between the fixed IPv6 base header and payload.

Comparison: IPv4 vs IPv6

Feature	IPv4	IPv6
Address Length	32 bits (4 bytes)	128 bits (16 bytes)
Header Size	Variable (20 - 60 bytes)	Fixed (40 bytes base header)
Header Checksum	Present (recomputed per hop)	Removed (handled by L2 and L4)
Fragmentation	Done by routers and source host	Done by source host only (Path MTU Discovery)
Configuration	Manual or DHCP	Stateless Autoconfiguration (SLAAC) or DHCPv6
Security (IPsec)	Optional add-on	Mandatory / Built-in support

IPv4 to IPv6 Transition Strategies



Three standardized techniques used to ensure smooth migration from legacy IPv4 infrastructure to IPv6.

AKTU Exam Corner: Likely Questions

Q1 Q1. Differentiate between IPv4 and IPv6 headers with neat diagrams. Explain the role of extension headers in IPv6. [10 Marks]

Q2 Q2. Explain Classless Inter-Domain Routing (CIDR). Given an IP address 198.16.0.0/20, find the subnet mask, total hosts, first usable address, and broadcast address. [7 Marks]

Q3 Q3. Describe the working of Address Resolution Protocol (ARP) and DHCP DORA process with suitable flow sequence. [7 Marks]

Q4 Q4. State and explain Dijkstra's Link State Routing algorithm with steps. Compare Distance Vector Routing and Link State Routing. [10 Marks]

Q5 Q5. Write short notes on: (a) ICMP Messages (b) Count-to-Infinity Problem (c) Split Horizon Technique. [7 Marks]

Q6 Q6. Differentiate between Leaky Bucket and Token Bucket algorithms for congestion control with diagrams and examples. [7 Marks]

Q7 Q7. Explain IPv4 to IPv6 transition mechanisms: Dual Stack, Tunneling, and Header Translation. [7 Marks]

Unit 3 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 4 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

