ABHYASMITRA.IN

STUDY NOTES

COMPUTER NETWORKS

Unit III — Network Layer

Topics Covered (09 Hours)

Network Layer Services & Design Issues
Datagram (Connectionless) vs. Virtual Circuits
Store-and-Forward Switching Architecture
Quality of Service (QoS) & Congestion Control
Routing Algorithms (Dijkstra, Flooding, Link State)
Distance Vector Routing & Count-to-Infinity Problem
IP Addressing (IPv4 Classes, Subnets, and CIDR)
Comparison of IPv4 vs. IPv6 Datagram Formats
Core Network Protocols: ICMP, ARP, RIP, and OSPF

Compiled in a simple, easy-to-understand, book style format
for students of Computer Science and Engineering

TABLE OF CONTENTS

3.1 Network Layer Services & Design Issues

The Network Layer is responsible for routing packets from a source host to a destination host, potentially crossing many intermediate routers along the path. It is the lowest layer that handles end-to-end transmission across the entire network.

Store-and-Forward Packet Switching

The network layer operates on a store-and-forward architecture. When a host sends a packet, it travels to the nearest router. The router stores the entire packet in its buffer, checks it for errors, and then forwards it to the next router along the path according to its internal routing table. This decoupling is essential for linking heterogeneous networks.

Connectionless vs. Connection-Oriented Services

The network layer can offer two different styles of services to the transport layer above it:

- **1. Connectionless Service (Datagram Networks):** Each packet is treated as an independent unit (a datagram) carrying the full destination address. Routers route each datagram individually. Packets may arrive out of order or take different paths. (Example: The Internet/IP).
- **2. Connection-Oriented Service (Virtual-Circuit Networks):** A path from source to destination is established before any data is sent. This path is called a Virtual Circuit (VC). All packets follow the same path in strict sequential order. (Example: ATM, Frame Relay).

VC vs. Datagram Networks Detailed Comparison

Issue	Datagram Subnet (Connectionless)	Virtual-Circuit Subnet (Connection-Oriented)
Circuit Setup	Not required. Packets are injected immediately.	Required before any data packets can be sent.
Addressing	Each packet contains full source and destination IP.	Packets contain a short VC identifier instead of IPs.
State Information	Routers hold no state about active connections.	Each router must store a table mapping incoming to outgoing VCs.
Routing	Each packet is routed independently.	Routing path is chosen at setup; all packets follow it.
Router Failure	Robust. Routers route around failed nodes.	Fatal. All active connections crossing the failed node die.

Congestion Control & QoS

When too many packets are present in a part of the network, performance degrades—a state called Congestion. Routers fail to handle the load, leading to buffer overflows and packet drops. Congestion control techniques prevent this. Common methods include:

- **Leaky Bucket Algorithm:** Smooths out bursty traffic by storing packets in a queue (the bucket). The bucket leaks packets at a constant, fixed rate. If packets arrive too quickly and the bucket overflows, the excess packets are discarded. This is ideal for traffic shaping.
- **Token Bucket Algorithm:** Allows controlled bursts of traffic. The bucket accumulates tokens at a constant rate. When a packet is transmitted, it must consume a token. If the bucket is full of tokens, a burst of packets can be sent immediately, providing better flexibility for bursty applications.

3.2 Routing Algorithms

Routing is the primary function of the network layer. A routing algorithm determines which output line an incoming packet should be sent on. We classify algorithms into Non-Adaptive (static routing, determined in advance) and Adaptive (dynamic routing, adapting to traffic changes).

1. Shortest Path Routing (Dijkstra's Algorithm)

A static routing algorithm that computes the absolute shortest path between nodes. The network is represented as a graph, with nodes representing routers and links representing communication channels. Each link has a cost (based on distance, bandwidth, or latency). Dijkstra's algorithm finds the shortest path from a source node to all other nodes by incrementally selecting the node with the lowest path cost.

Step-by-Step Calculation Trace: Let node A be the source. Initially, we mark A's distance as 0, and all other nodes as infinity. A is marked as permanent. We look at A's neighbors (e.g., B and C). If link A-B has cost 2, we update B's temporary distance to 2. If link A-C has cost 5, we update C's temporary distance to 5. We select the smallest temporary node (B) and mark it permanent. We look at B's neighbors (e.g., C). If link B-C has cost 2, then path A-B-C has cost 4. Since 4 is smaller than C's current temporary distance (5), we update C's distance to 4. We repeat until all nodes are permanent.

2. Flooding

A simple static routing algorithm where every incoming packet is duplicated and sent out on all outgoing links except the one it arrived on. Flooding generates massive numbers of duplicate packets, so hop counts or sequence databases are used to terminate packets. It is highly robust and is used for network discovery and routing updates.

3. Distance Vector Routing (Bellman-Ford)

A dynamic routing algorithm. Each router maintains a routing table (vector) containing the shortest distance to every destination, and the next-hop router. Routers periodically share their entire vector with their immediate neighbors. While simple, it suffers from the Count-to-Infinity Problem: bad news (link failures) propagates extremely slowly through the network, causing routing loops.

4. Link State Routing (OSPF Core)

Replaced Distance Vector in large networks. Each router monitors its links to immediate neighbors, measures costs, and packages this data into a Link State Packet (LSP). The LSP is flooded to the entire network. Once every router has the identical LSP database, they run Dijkstra's algorithm locally to construct their routing tables. It converges extremely fast and prevents routing loops.

3.3 Internet Architecture and Protocols

The global Internet is built on the Internet Protocol (IP), which acts as the universal layer bridging different physical network standards.

IP Addressing (IPv4)

Every host on the internet is assigned a unique 32-bit logical IP address. IPv4 addresses are written in dotted-decimal format (e.g., 192.168.1.1).

- **Classful Addressing:** Historically divided into Classes A, B, C, D, and E based on the leading bits. Class A (huge networks), Class B (medium networks), Class C (small networks, up to 254 hosts). This division wasted many addresses.
- **CIDR (Classless Inter-Domain Routing):** Replaced classful addressing. It allows arbitrary prefix lengths. An address is followed by a slash and the number of network bits (e.g., 192.168.1.0/24). Subnet masks identify the boundary between the network prefix and host bits.

Detailed Subnetting Math Walkthrough

Suppose we are assigned the network block 192.168.1.0/26. The /26 prefix indicates that the first 26 bits represent the network portion, leaving 6 bits (32 - 26 = 6) for hosts.

- **Subnet Mask:** The binary mask has 26 ones followed by 6 zeros: 11111111.11111111.11111111.11000000. In decimal, this is 255.255.255.192.
- **Total Subnets:** This creates 4 subnets within the class C block: 0 to 63, 64 to 127, 128 to 191, and 192 to 255.
- **Host Capacity:** Each subnet has 2^6 = 64 addresses. We subtract 2 (one for the network address and one for the broadcast address), leaving 62 usable host addresses per subnet.
- **Example Allocation:** For the first subnet: Network Address is 192.168.1.0, Usable Host Range is 192.168.1.1 to 192.168.1.62, and Broadcast Address is 192.168.1.63.

IPv4 vs. IPv6

Due to the exhaustion of 32-bit IPv4 addresses, IPv6 was introduced, utilizing 128-bit addresses.

Feature	IPv4	IPv6
Address Size	32 bits (4 Billion addresses)	128 bits (Undecillions of addresses)
Address Format	Dotted-decimal (e.g., 192.30.250.1)	Hexadecimal-colon (e.g., 2001:db8::ff00:42)
Header Size	Variable size (20 to 60 bytes)	Fixed size (40 bytes), speeding up router processing

Feature	IPv4	IPv6
Auto-Configuration	Requires DHCP or manual setup	Supports Stateless Address Autoconfiguration (SLAAC)

Core Protocols

- **IP Datagram:** The basic packet format, containing header fields like Version, TTL (Time-To-Live, preventing infinite looping), Protocol, Source IP, and Destination IP.
- **ICMP (Internet Control Message Protocol):** Used by routers and hosts to send error messages and operational information (e.g., used by 'ping' and 'traceroute').
- **ARP (Address Resolution Protocol):** Maps a logical IP address to a physical MAC address on a local area network.
- **RIP & OSPF:** Routing protocols. RIP (Routing Information Protocol) is a simple Distance Vector protocol. OSPF (Open Shortest Path First) is a powerful, hierarchical Link State protocol used inside enterprise networks.

Unit Summary

This unit examined the protocols and routing of the Network Layer.

- The Network Layer is responsible for end-to-end packet routing across multiple subnets.
- Store-and-forward switching stores packets locally on routers before forwarding them.
- Datagram networks are connectionless (IP), while Virtual-Circuit networks are connection-oriented.
- Congestion occurs when subnets are overloaded. Leaky and Token bucket algorithms shape traffic.
- Routing algorithms include Dijkstra's shortest path, Flooding, Distance Vector, and Link State.
- IPv4 uses 32-bit addresses and classful/CIDR subnetting, while IPv6 uses 128-bit hex addresses.
- Core internet protocols are ICMP (diagnostics), ARP (IP-to-MAC mapping), and routing protocols like OSPF and RIP.