Kalinga University

Department of Computer Science &Information Technology

Course:BCAAIML **Semester: IV**

Subject: Computer Network **Subject Code: BCAAIML403**

UNIT – IV

Networks Layer Functions and Protocols

The Network Layer is responsible for routing data between devices on different networks. Its main functions include:

1. Routing: Determining the best path for data to travel from the source to the destination.
2. Addressing: Providing logical addresses to devices on a network.
3. Congestion Control: Managing network traffic to prevent congestion.
4. Error Handling: Detecting and correcting errors that occur during data transmission.

Some common Network Layer protocols include:

1. IP (Internet Protocol): Provides logical addressing and routing for data on the internet.
2. ICMP (Internet Control Message Protocol): Provides error handling and diagnostic functions for IP.
3. IGMP (Internet Group Management Protocol): Manages multicast groups and membership.

Routing Algorithms

Routing algorithms determine the best path for data to travel from the source to the destination. Some common routing algorithms include:

1. Distance Vector Routing: Each router maintains a table of distances to all possible destinations.
2. Shortest Path Routing: Each router determines the shortest path to the destination based on the distance vector table.
3. Link State Routing: Each router maintains a map of the network topology and calculates the shortest path to the destination.

IP Protocol

The IP protocol provides logical addressing and routing for data on the internet. Its main functions include:

1. Addressing: Providing logical addresses to devices on a network.
2. Routing: Determining the best path for data to travel from the source to the destination.
3. Fragmentation: Breaking down large packets of data into smaller packets for transmission.

Internet Control Protocols

Internet Control Protocols provide error handling and diagnostic functions for IP. Some common Internet Control Protocols include:

1. ICMP (Internet Control Message Protocol): Provides error handling and diagnostic functions for IP.
2. IGMP (Internet Group Management Protocol): Manages multicast groups and membership.

Unicasting, Multicasting, Broadcasting

Unicasting, multicasting, and broadcasting are methods of transmitting data on a network:

1. Unicasting: Transmitting data to a single device on a network.
2. Multicasting: Transmitting data to a group of devices on a network.
3. Broadcasting: Transmitting data to all devices on a network.

ISDN (Integrated Services Digital Network)

ISDN is a digital communication standard that provides integrated services for voice, data, and video transmission. Its main features include:

1. PRI (Primary Rate Interface): Provides 23 B-channels (64 kbps each) and 1 D-channel (64 kbps) for signaling and control.
2. BRI (Basic Rate Interface): Provides 2 B-channels (64 kbps each) and 1 D-channel (16 kbps) for signaling and control.
3. Services: ISDN provides a range of services, including voice, data, and video transmission, as well as fax and telex services.

Historical Outline of ISDN

ISDN was first developed in the 1970s and 1980s as a replacement for traditional analog telephone networks. Its development involved the collaboration of several international organizations, including the ITU (International Telecommunication Union) and the ISO (International Organization for Standardization).

Network Layer Functions

The Network Layer is responsible for routing data between devices on different networks. Its main functions include:

1. Routing: Determining the best path for data to travel from the source to the destination.
2. Addressing: Providing logical addresses to devices on a network.
3. Congestion Control: Managing network traffic to prevent congestion.
4. Error Handling: Detecting and correcting errors that occur during data transmission.
5. Packet Forwarding: Forwarding packets of data between networks.
6. Packet Filtering: Filtering packets of data based on security policies.

Network Layer Protocols

Some common Network Layer protocols include:

1. IP (Internet Protocol): Provides logical addressing and routing for data on the internet.
2. ICMP (Internet Control Message Protocol): Provides error handling and diagnostic functions for IP.
3. IGMP (Internet Group Management Protocol): Manages multicast groups and membership.
4. RIP (Routing Information Protocol): A distance-vector routing protocol used to exchange routing information.
5. OSPF (Open Shortest Path First): A link-state routing protocol used to exchange routing information.
6. BGP (Border Gateway Protocol): A path-vector routing protocol used to exchange routing information between autonomous systems.

IP Protocol

The IP protocol provides logical addressing and routing for data on the internet. Its main functions include:

1. Addressing: Providing logical addresses to devices on a network.
2. Routing: Determining the best path for data to travel from the source to the destination.
3. Fragmentation: Breaking down large packets of data into smaller packets for transmission.
4. Reassembly: Reassembling fragmented packets of data at the destination.

ICMP Protocol

The ICMP protocol provides error handling and diagnostic functions for IP. Its main functions include:

1. Error Reporting: Reporting errors that occur during data transmission.
2. Diagnostic Functions: Providing diagnostic functions, such as ping and traceroute.

IGMP Protocol

The IGMP protocol manages multicast groups and membership. Its main functions include:

1. Multicast Group Management: Managing multicast groups and membership.
2. Multicast Routing: Routing multicast traffic between networks.

Routing Protocols

Routing protocols are used to exchange routing information between networks. Some common routing protocols include:

1. RIP (Routing Information Protocol): A distance-vector routing protocol.
2. OSPF (Open Shortest Path First): A link-state routing protocol.
3. BGP (Border Gateway Protocol): A path-vector routing protocol.

Network Layer Devices

Network Layer devices include:

1. Routers: Devices that forward packets of data between networks.
2. Gateways: Devices that connect a network to another network or to the internet.
3. Firewalls: Devices that filter packets of data based on security policies.

Routing Algorithms

Routing algorithms determine the best path for data to travel from the source to the destination. The main goals of routing algorithms are:

1. Optimality: Find the best path to the destination.
2. Simplicity: Minimize computational overhead.
3. Scalability: Handle large networks with many nodes.

4. Flexibility: Adapt to changing network conditions.

Distance Vector Routing

Distance Vector Routing is a type of routing algorithm that uses a distance vector to determine the best path to the destination. A distance vector is a table that lists the distance to each destination node in the network.

How Distance Vector Routing Works

1. Initialization: Each node initializes its distance vector with the distance to its directly connected neighbors.
2. Exchange: Each node exchanges its distance vector with its neighbors.
3. Update: Each node updates its distance vector based on the information received from its neighbors.
4. Routing: Each node uses its updated distance vector to determine the best path to the destination.

Distance Vector Routing Protocols

Some common distance vector routing protocols include:

1. RIP (Routing Information Protocol): A simple distance vector routing protocol used in small networks.
2. IGRP (Interior Gateway Routing Protocol): A more advanced distance vector routing protocol used in larger networks.

Advantages of Distance Vector Routing

1. Simple to implement: Distance vector routing is relatively simple to implement.
2. Low computational overhead: Distance vector routing requires minimal computational overhead.

Disadvantages of Distance Vector Routing

1. Slow convergence: Distance vector routing can take a long time to converge to the optimal routing solution.
2. Routing loops: Distance vector routing can create routing loops, where packets are forwarded in a loop.

Examples of Distance Vector Routing

1. RIP routing: RIP is a simple distance vector routing protocol used in small networks.
2. IGRP routing: IGRP is a more advanced distance vector routing protocol used in larger networks.

Comparison with Other Routing Algorithms

Distance vector routing is compared with other routing algorithms, such as:

1. Link state routing: Link state routing uses a different approach to determine the best path to the destination.
2. Path vector routing: Path vector routing uses a different approach to determine the best path to the destination.

Shortest Path Routing

Shortest Path Routing is a type of routing algorithm that determines the best path to the destination by finding the shortest path.

How Shortest Path Routing Works

1. Initialization: Each node initializes its routing table with the distance to its directly connected neighbors.
2. Exchange: Each node exchanges its routing table with its neighbors.
3. Calculation: Each node calculates the shortest path to the destination using the information received from its neighbors.
4. Routing: Each node uses its calculated shortest path to forward packets to the destination.

Shortest Path Routing Algorithms

Some common shortest path routing algorithms include:

1. Dijkstra's Algorithm: A popular algorithm for finding the shortest path in a graph.
2. Bellman-Ford Algorithm: An algorithm for finding the shortest path in a graph with negative weight edges.
3. A Algorithm*: An algorithm for finding the shortest path in a graph with heuristic information.

Advantages of Shortest Path Routing

1. Optimal routing: Shortest path routing ensures that packets are forwarded along the optimal path.
2. Low latency: Shortest path routing minimizes latency by avoiding unnecessary hops.
3. High throughput: Shortest path routing maximizes throughput by avoiding congestion.

Disadvantages of Shortest Path Routing

1. Complexity: Shortest path routing can be computationally expensive, especially in large networks.
2. Scalability: Shortest path routing can be challenging to scale in very large networks.

Examples of Shortest Path Routing

1. OSPF (Open Shortest Path First): A popular link-state routing protocol that uses shortest path routing.
2. IS-IS (Intermediate System to Intermediate System): A link-state routing protocol that uses shortest path routing.

Comparison with Other Routing Algorithms

Shortest path routing is compared with other routing algorithms, such as:

1. Distance vector routing: Distance vector routing uses a different approach to determine the best path.
2. Link state routing: Link state routing uses a different approach to determine the best path.

Network Layer Protocols

Network Layer protocols are responsible for routing data between devices on different networks. The main functions of Network Layer protocols include:

1. Routing: Determining the best path for data to travel from the source to the destination.
2. Addressing: Providing logical addresses to devices on a network.
3. Packet Forwarding: Forwarding packets of data between networks.

Types of Network Layer Protocols

1. Connectionless Protocols: Protocols that do not establish a connection before sending data.
2. Connection-Oriented Protocols: Protocols that establish a connection before sending data.

Examples of Network Layer Protocols

1. IP (Internet Protocol): A connectionless protocol that provides logical addressing and routing for data on the internet.
2. ICMP (Internet Control Message Protocol): A connectionless protocol that provides error reporting and diagnostic functions for IP.
3. IGMP (Internet Group Management Protocol): A connectionless protocol that manages multicast groups and membership.

IP Protocol

The IP protocol is a connectionless protocol that provides logical addressing and routing for data on the internet. The main functions of IP include:

1. Addressing: Providing logical addresses to devices on a network.
2. Routing: Determining the best path for data to travel from the source to the destination.
3. Packet Forwarding: Forwarding packets of data between networks.

IP Packet Structure

An IP packet consists of:

1. Header: Contains control information, such as source and destination addresses.
2. Payload: Contains the actual data being transmitted.

IP Addressing

IP addresses are used to uniquely identify devices on a network. The main types of IP addresses include:

1. IPv4 Addresses: 32-bit addresses that are commonly used on the internet.
2. IPv6 Addresses: 128-bit addresses that are designed to provide a larger address space.

ICMP Protocol

The ICMP protocol is a connectionless protocol that provides error reporting and diagnostic functions for IP. The main functions of ICMP include:

1. Error Reporting: Reporting errors that occur during data transmission.
2. Diagnostic Functions: Providing diagnostic functions, such as ping and traceroute.

IP Protocol

The IP protocol is a connectionless protocol that provides logical addressing and routing for data on the internet.

Functions of IP Protocol

1. Addressing: Providing logical addresses to devices on a network.
2. Routing: Determining the best path for data to travel from the source to the destination.
3. Packet Forwarding: Forwarding packets of data between networks.
4. Fragmentation: Breaking down large packets of data into smaller packets for transmission.
5. Reassembly: Reassembling fragmented packets of data at the destination.

IP Packet Structure

An IP packet consists of:

1. Header: Contains control information, such as source and destination addresses.
2. Payload: Contains the actual data being transmitted.

IP Header Format

The IP header format includes:

1. Version: Indicates the version of the IP protocol.
2. Header Length: Indicates the length of the IP header.
3. Type of Service: Indicates the type of service required for the packet.
4. Total Length: Indicates the total length of the packet.
5. Identification: Identifies the packet and its fragments.
6. Flags: Indicates whether the packet is fragmented and whether more fragments are to follow.
7. Fragment Offset: Indicates the offset of the fragment in the original packet.
8. Time to Live: Indicates the maximum number of hops the packet can take.
9. Protocol: Indicates the protocol used by the packet's payload.
10. Header Checksum: Verifies the integrity of the IP header.
11. Source Address: Indicates the IP address of the packet's source.
12. Destination Address: Indicates the IP address of the packet's destination.

IP Addressing

IP addresses are used to uniquely identify devices on a network. The main types of IP addresses include:

1. IPv4 Addresses: 32-bit addresses that are commonly used on the internet.
2. IPv6 Addresses: 128-bit addresses that are designed to provide a larger address space.

IPv4 Address Format

The IPv4 address format includes:

1. Network ID: Identifies the network.
2. Host ID: Identifies the host on the network.

IPv6 Address Format

The IPv6 address format includes:

1. Global Routing Prefix: Identifies the global routing prefix.
2. Subnet ID: Identifies the subnet.
3. Interface ID: Identifies the interface.

Internet Control Protocols

Internet Control Protocols are used to manage and control the flow of data on the internet. These protocols provide error reporting, diagnostic functions, and other control functions.

Types of Internet Control Protocols

1. ICMP (Internet Control Message Protocol): Provides error reporting and diagnostic functions for IP.
2. IGMP (Internet Group Management Protocol): Manages multicast groups and membership.
3. ICMPv6 (Internet Control Message Protocol version 6): Provides error reporting and diagnostic functions for IPv6.

ICMP (Internet Control Message Protocol)

ICMP is a connectionless protocol that provides error reporting and diagnostic functions for IP. ICMP messages are used to report errors and provide diagnostic information.

Types of ICMP Messages

1. Error Messages: Used to report errors, such as destination unreachable or time exceeded.
2. Query Messages: Used to request information, such as ping or traceroute.

3. Informational Messages: Used to provide information, such as echo reply.

ICMP Header Format

The ICMP header format includes:

1. Type: Identifies the type of ICMP message.
2. Code: Provides additional information about the ICMP message.
3. Checksum: Verifies the integrity of the ICMP message.
4. Data: Contains the data being carried by the ICMP message.

IGMP (Internet Group Management Protocol)

IGMP is a protocol used to manage multicast groups and membership. IGMP is used by hosts to report their multicast group membership to nearby routers.

Types of IGMP Messages

1. Membership Report: Used by hosts to report their multicast group membership.
2. Membership Query: Used by routers to query hosts about their multicast group membership.
3. Leave Group: Used by hosts to leave a multicast group.

ICMPv6 (Internet Control Message Protocol version 6)

ICMPv6 is a protocol used to provide error reporting and diagnostic functions for IPv6. ICMPv6 is similar to ICMP, but it has some additional features and message types.

Types of ICMPv6 Messages

1. Error Messages: Used to report errors, such as destination unreachable or time exceeded.
2. Query Messages: Used to request information, such as ping or traceroute.
3. Informational Messages: Used to provide information, such as echo reply.

ICMPv6 Header Format

The ICMPv6 header format includes:

1. Type: Identifies the type of ICMPv6 message.
2. Code: Provides additional information about the ICMPv6 message.
3. Checksum: Verifies the integrity of the ICMPv6 message.

4. Data: Contains the data being carried by the ICMPv6 message.

Unicasting

Unicasting is a communication technique where a single sender transmits data to a single receiver. It is a one-to-one communication method, where the sender and receiver have a dedicated connection.

How Unicasting Works

1. Connection Establishment: The sender and receiver establish a dedicated connection.
2. Data Transmission: The sender transmits data to the receiver through the established connection.
3. Data Receipt: The receiver receives the data and sends an acknowledgement to the sender.

Types of Unicasting

1. Connection-Oriented Unicasting: The sender and receiver establish a dedicated connection before data transmission.
2. Connectionless Unicasting: The sender transmits data to the receiver without establishing a dedicated connection.

Advantages of Unicasting

1. Reliability: Unicasting provides reliable data transmission, as the sender and receiver have a dedicated connection.
2. Security: Unicasting provides secure data transmission, as the data is transmitted through a dedicated connection.
3. Quality of Service: Unicasting provides Quality of Service (QoS) guarantees, as the sender and receiver have a dedicated connection.

Disadvantages of Unicasting

1. Scalability: Unicasting is not scalable, as it requires a dedicated connection for each sender-receiver pair.
2. Resource Intensive: Unicasting is resource-intensive, as it requires dedicated connections and bandwidth.

Examples of Unicasting

1. TCP (Transmission Control Protocol): TCP is a connection-oriented protocol that uses unicasting for reliable data transmission.
2. HTTP (Hypertext Transfer Protocol): HTTP is a connectionless protocol that uses unicasting for data transmission.

Comparison with Other Communication Techniques

Unicasting is compared with other communication techniques, such as:

1. Multicasting: Multicasting is a one-to-many communication technique, where a single sender transmits data to multiple receivers.
2. Broadcasting: Broadcasting is a one-to-all communication technique, where a single sender transmits data to all receivers on a network.

Multicasting

Multicasting is a communication technique where a single sender transmits data to multiple receivers. It is a one-to-many communication method, where the sender sends a single copy of the data to a group of receivers.

How Multicasting Works

1. Group Membership: Receivers join a multicast group to receive data from the sender.
2. Data Transmission: The sender transmits data to the multicast group.
3. Data Receipt: Receivers in the multicast group receive the data.

Types of Multicasting

1. IP Multicasting: IP multicasting uses IP addresses to identify multicast groups.
2. Ethernet Multicasting: Ethernet multicasting uses MAC addresses to identify multicast groups.

Advantages of Multicasting

1. Efficient Use of Bandwidth: Multicasting reduces bandwidth usage by sending a single copy of the data to multiple receivers.
2. Scalability: Multicasting is scalable, as it can support a large number of receivers.
3. Reduced Latency: Multicasting reduces latency, as data is transmitted simultaneously to multiple receivers.

Disadvantages of Multicasting

1. Complexity: Multicasting is complex, as it requires routers to manage multicast groups and forward data to multiple receivers.
2. Security: Multicasting raises security concerns, as data is transmitted to multiple receivers.

Examples of Multicasting

1. Video Streaming: Multicasting is used in video streaming applications, such as online TV and video conferencing.
2. Online Gaming: Multicasting is used in online gaming applications, such as multiplayer games.
3. File Distribution: Multicasting is used in file distribution applications, such as software updates and file sharing.

Protocols Used in Multicasting

1. IGMP (Internet Group Management Protocol): IGMP is used to manage multicast group membership.
2. PIM (Protocol Independent Multicast): PIM is used to forward multicast data between routers.
3. DVMRP (Distance Vector Multicast Routing Protocol): DVMRP is used to forward multicast data between routers.

Broadcasting

Broadcasting is a communication technique where a single sender transmits data to all receivers on a network. It is a one-to-all communication method, where the sender sends a single copy of the data to all receivers on the network.

How Broadcasting Works

1. Data Transmission: The sender transmits data to the network.
2. Data Receipt: All receivers on the network receive the data.

Types of Broadcasting

1. Network Broadcasting: Broadcasting to all devices on a network.
2. Limited Broadcasting: Broadcasting to a limited number of devices on a network.

Advantages of Broadcasting

1. Simple Implementation: Broadcasting is simple to implement, as it does not require complex routing or addressing.

2. Efficient Use of Bandwidth: Broadcasting can be efficient in terms of bandwidth usage, as a single copy of the data is transmitted to all receivers.
3. Low Latency: Broadcasting can provide low latency, as data is transmitted simultaneously to all receivers.

Disadvantages of Broadcasting

1. Security Concerns: Broadcasting raises security concerns, as data is transmitted to all receivers on the network.
2. Network Congestion: Broadcasting can cause network congestion, as a large amount of data is transmitted to all receivers on the network.
3. Unnecessary Data Transmission: Broadcasting can result in unnecessary data transmission, as data is transmitted to all receivers on the network, regardless of whether they need it or not.

Examples of Broadcasting

1. DHCP (Dynamic Host Configuration Protocol): DHCP uses broadcasting to assign IP addresses to devices on a network.
2. ARP (Address Resolution Protocol): ARP uses broadcasting to resolve IP addresses to MAC addresses.
3. Network Announcements: Broadcasting is used to make network announcements, such as network maintenance or outages.

Protocols Used in Broadcasting

1. UDP (User Datagram Protocol): UDP is a transport-layer protocol that supports broadcasting.
2. IP (Internet Protocol): IP is a network-layer protocol that supports broadcasting.

ISDN Services

ISDN provides a range of services, including:

1. Basic Rate Interface (BRI): Provides two 64 kbps B-channels and one 16 kbps D-channel.
2. Primary Rate Interface (PRI): Provides 23 B-channels and one D-channel.
3. Bearer Services: Provide transparent, circuit-switched connections for voice, data, and video.
4. Teleservices: Provide enhanced services, such as video conferencing and multimedia.
5. Supplementary Services: Provide additional features, such as call forwarding and call waiting.

Historical Outline of ISDN

ISDN was developed in the 1970s and 1980s as a replacement for traditional analog telephone networks.

1. 1970s: ISDN was first proposed by the International Telecommunication Union (ITU).
2. 1980s: ISDN was standardized by the ITU, and the first ISDN networks were deployed.
3. 1990s: ISDN became widely available, and its use expanded to include data and video services.
4. 2000s: ISDN began to decline, as newer technologies, such as DSL and VoIP, became more popular.

Key Features of ISDN

1. Digital Transmission: ISDN uses digital transmission, which provides higher quality and reliability than analog transmission.
2. Integrated Services: ISDN provides integrated services, including voice, data, and video.
3. Circuit-Switched Connections: ISDN provides circuit-switched connections, which provide a dedicated path for data transmission.
4. Multiple Channels: ISDN provides multiple channels, which allow for simultaneous transmission of multiple data streams.

Applications of ISDN

1. Video Conferencing: ISDN was widely used for video conferencing, as it provided high-quality, real-time video transmission.
2. Remote Access: ISDN was used for remote access, as it provided fast and reliable connections for dial-up users.
3. Data Transmission: ISDN was used for data transmission, as it provided high-speed, reliable connections for data transfer.
4. Telecommuting: ISDN was used for telecommuting, as it provided remote workers with fast and reliable connections to the office.

PRI (Primary Rate Interface)

PRI is a type of ISDN interface that provides a high-speed connection for large organizations or businesses. PRI is typically used for:

1. High-speed data transfer: PRI provides a high-speed connection for transferring large amounts of data.
2. Multiple phone lines: PRI provides multiple phone lines, allowing for simultaneous voice calls.
3. Video conferencing: PRI provides a high-quality connection for video conferencing.

Characteristics of PRI:

1. Speed: PRI provides a speed of 1.544 Mbps (T1) or 2.048 Mbps (E1).
2. Channels: PRI provides 23 B-channels (64 kbps each) and 1 D-channel (64 kbps).
3. Distance: PRI can support distances of up to 4 km (2.5 miles).

BRI (Basic Rate Interface)

BRI is a type of ISDN interface that provides a lower-speed connection for small businesses or home users. BRI is typically used for:

1. Low-speed data transfer: BRI provides a lower-speed connection for transferring smaller amounts of data.
2. Single phone line: BRI provides a single phone line, allowing for a single voice call.
3. Internet access: BRI provides a connection for internet access.

Characteristics of BRI:

1. Speed: BRI provides a speed of 128 kbps.
2. Channels: BRI provides 2 B-channels (64 kbps each) and 1 D-channel (16 kbps).
3. Distance: BRI can support distances of up to 5 km (3.1 miles).

Comparison of PRI and BRI

1. Speed: PRI is faster than BRI, with a speed of 1.544 Mbps (T1) or 2.048 Mbps (E1) compared to BRI's 128 kbps.
2. Channels: PRI provides more channels than BRI, with 23 B-channels and 1 D-channel compared to BRI's 2 B-channels and 1 D-channel.
3. Distance: PRI and BRI have different distance limitations, with PRI supporting up to 4 km (2.5 miles) and BRI supporting up to 5 km (3.1 miles).
4. Cost: PRI is typically more expensive than BRI, due to the higher speed and number of channels.