Here are your exam summary notes for Chapter 7: The Network Layer.

Network Layer (Layer 3) Fundamentals

- **Primary Function**: Routes packets from a source node to a destination node across multiple networks.
- **Primary Protocol**: **IP (Internet Protocol)** is the main example.
- **Key Element**: Addresses are crucial for routing.

IPv4 (Internet Protocol version 4)

- **Deployment**: Most widely deployed version of IP, though IPv6 is its intended successor.
- **Service Type**: Provides an **unreliable, best-effort connectionless service**. Packets are called **datagrams**.
- **Basic Routing Algorithm**:
    1. If destination (B) is on the same network as current node (A), A delivers directly to B.
    2. Else, A consults its routing table. If an entry for B's network exists, A forwards the datagram to the next hop router.
    3. Else, if no specific entry, A sends the datagram to its default gateway.
    4. Else, if no default gateway, A discards the datagram.

IPv4 Header

Key fields include (see Figure 7.1):

- **Version**: 4 for IPv4.
- **IHL (Internet Header Length)**: Length of the header in 32-bit words.
- **Total Length**: Total length of the datagram (header + payload).
- **Identification**: Helps identify fragments of a datagram.
- **Flags & Fragment Offset**: Used for fragmentation. Fragment Offset indicates where a fragment fits in the original datagram.
- **TTL (Time-to-Live)**: Limits packet lifetime; decremented by each router. If TTL reaches 0, packet is discarded (prevents infinite loops).
- **Protocol**: Identifies the Layer 4 protocol of the payload (e.g., TCP=6, UDP=17).
- **Header Checksum**: Error detection for the header only.
- **Source Address**: 32-bit address of the sender.
- **Destination Address**: 32-bit address of the recipient.
- **Options**: Optional parameters, e.g., for source routing (rarely used).
- **Padding**: Ensures header ends on a 32-bit boundary.

IPv4 Addressing

- **Format**: 32-bit addresses, usually written in **dotted decimal notation** (e.g., 1.2.3.4).

- **Structure**: Divided into a **network portion** and a **host portion**.
- **Address Classes** (Original scheme, often superseded by CIDR):
    - **Class A**: Leading bit 0. 1st byte is network, next 3 are host. Network mask: 255.0.0.0 (/8).
    - **Class B**: Leading bits 10. First 2 bytes are network, next 2 are host. Network mask: 255.255.0.0 (/16).
    - **Class C**: Leading bits 110. First 3 bytes are network, last 1 is host. Network mask: 255.255.255.0 (/24).
    - **Class D**: Leading bits 1110. Used for multicast.
    - **Class E**: Leading bits 1111. Reserved/experimental.
- **Special Host Numbers**:
    - Host portion of all 0s: Represents the network itself (e.g., 10.0.0.0).
    - Host portion of all 1s: Broadcast address for that network (e.g., 10.255.255.255 for network 10.0.0.0).
    - Number of usable hosts on a network with n host bits: $2^n - 2$.
- **Netmask**: A 32-bit value with 1s for the network portion and 0s for the host portion.
- **CIDR (Classless Inter-Domain Routing)**: Notation like address/prefix_length (e.g., 10.0.0.0/8). Indicates number of bits in the network portion.

Subnetting & Supernetting (Practical Application of CIDR)

Subnetting

- **Purpose**: Divides a large network into smaller, manageable subnetworks.
- **How it works**: "Borrows" bits from the host portion to create a subnet identifier. This extends the network portion.
- **Example (Class A subnetted using the second byte)**:
    - Organization has 10.0.0.0/8.
    - They decide to use the second byte for subnets (e.g., Sales: 10.1.0.0, Production: 10.2.0.0).
    - Effectively, the network portion becomes 16 bits (/16).
    - The subnet mask used internally is 255.255.0.0.
    - Sales network: 10.1.0.0/16.
    - Externally, it's still seen as 10.0.0.0/8.
- **Example (Subnetting a Class C address)**:
    - An owner of a Class C address (8 host bits) wants to create subnets.
    - Decision: Use 4 bits for subnet ID, leaving 4 bits for host ID.
    - Original prefix: /24. New subnet prefix: 24(original)+4(subnet bits)=/28.
    - **New Subnet Mask Calculation**:
        - Original mask (binary for last octet): 00000000
        - Borrow 4 bits for subnet: 11110000
        - This becomes 240 in decimal.
        - Full subnet mask: 255.255.255.240.
    - Number of subnets: $2^4=16$.

    - Number of usable hosts per subnet: 24−2=14.
- **Finding the Network Address**: Perform a logical **AND** operation between the host's IP address and its subnet mask.
    - E.g., IP Address 192.168.10.37, Subnet Mask 255.255.255.240 (/28)
        - IP: 11000000.10101000.00001010.00100101
        - Mask: 11111111.11111111.11111111.11110000
        - AND Result: 11000000.10101000.00001010.00100000 -> 192.168.10.32
        - Network address is 192.168.10.32/28.

Supernetting (Route Aggregation/Summarization)

- **Purpose**: Combines multiple smaller network addresses into a single, larger network entry in routing tables to reduce table size.
- **How it works**: Shortens the network prefix.
- **Example**: An ISP is assigned 256 Class C networks from 192.168.0.0 to 192.168.255.0.
    - These can be summarized as a single supernet: 192.168.0.0/16.
    - External routers only need one entry for this block, pointing to the ISP.

Special IPv4 Addresses

(See Table 7.1 for a good summary)

- 127.0.0.1: **Loopback address** (localhost). Network 127.0.0.0/8 is localnet.
- 0.0.0.0:
    - As a **source address**: Placeholder for "this computer" when its IP is unknown (e.g., DHCP request).
    - In routing tables (gateway column): Indicates a directly connected network or no specific next hop.
    - In CIDR notation: Often written as 0.0.0.0/32 when used as a placeholder for a specific host value of zero.
- 0.0.0.0/0: **Default route** in routing tables. Matches any destination IP address.
- 255.255.255.255: **Local broadcast** ("on the wire") to all directly connected computers.
- **Private IP Addresses** (not routable on the public Internet):
    - 10.0.0.0/8 (10.0.0.0 – 10.255.255.255)
    - 172.16.0.0/12 (172.16.0.0 – 172.31.255.255)
    - 192.168.0.0/16 (192.168.0.0 – 192.168.255.255)
- 100.64.0.0/10: **Shared Address Space** (for Carrier-Grade NAT - CGN). Used by ISPs.
- 169.254.0.0/16: **Link-Local Addresses**. Used for automatic IP configuration when no DHCP server is available, for communication on a single link.

IPv4 Routing Tables

- **Content**: Destination network, Netmask (or CIDR prefix), Next Hop (Gateway), Interface, Metric (cost).
- **Directly Connected Networks**: Gateway is often 0.0.0.0 or blank, interface is specified.

- **Remote Networks**: Gateway is the IP address of the next router, interface often derived from next hop's reachability.
- **Default Route**: Destination 0.0.0.0/0, Gateway is the default router's IP.

IPv4 Fragmentation

- **Reason**: IP datagram larger than the Maximum Transmission Unit (MTU) or PDU size of the underlying Layer 2 protocol (e.g., Ethernet MTU is 1500 bytes).
- **Process**: Original datagram is split into smaller fragments.
- **Header Fields Used**:
  - **Identification**: Same value for all fragments of the original datagram.
  - **Flags**: "Do not fragment" (DF) bit can prevent fragmentation. "More fragments" (MF) bit indicates if more fragments follow.
  - **Fragment Offset**: Specifies where this fragment belongs in the original datagram.
- **Reassembly**: Occurs at the final destination IP layer.

Obtaining IP Addresses

- **Hierarchy**: IANA -> Regional Internet Registries (RIRs) -> ISPs -> End users/organizations.
- **RIRs**: AfriNIC (Africa), ARIN (USA, Canada, etc.), APNIC (Asia-Pacific), LACNIC (Latin America & Caribbean), RIPE NCC (Europe, Russia, West/Central Asia).
- **IPv4 Exhaustion**: RIRs have largely exhausted their pools of "new" IPv4 addresses. Policies exist for managing remaining blocks.

Support Protocols (Layer 3)

ICMP (Internet Control Message Protocol)

- **Purpose**: Sends control, status, and error messages for IP.
- **Transport**: Carried as the payload of an IP packet.
- **Structure**: ICMP Type number (8 bits) indicates message type, possibly a payload.
- **Common ICMP Types** (Figure 7.11):
  - Type 0: Echo Reply (ping response)
  - Type 3: Destination Unreachable
  - Type 8: Echo Request (ping request)
  - Type 10 (or 11 in practice): Time Exceeded (used by traceroute)
- **Commands**:
  - ping: Uses Echo Request/Reply to test reachability.
  - traceroute (or tracert): Sends packets with increasing TTLs to map the route; relies on Time Exceeded messages from routers.

ARP (Address Resolution Protocol)

- **Purpose**: Resolves an IP address to its corresponding Layer 2 MAC (hardware) address for delivery on a local network segment.
- **Process**:
    1. Host A wants to send to IP B on the same local network. Host A broadcasts an ARP request: "Who has IP B? Tell IP A."
    2. Host B recognizes its IP address and sends an ARP reply (unicast) to Host A: "IP B is at MAC address Z."
    3. Host A caches this mapping and can now send frames directly to MAC Z.

Unicasting, Multicasting, Broadcasting

- **Unicast**: One-to-one communication.
- **Broadcast**: One-to-all nodes on a specific network.
- **Multicast**: One-to-many (a group of interested nodes).
    - Uses Class D IPv4 addresses.
    - Routers can use protocols like IGMP (Internet Group Management Protocol) to manage multicast group membership and efficiently forward multicast streams only where interested listeners exist (e.g., for internet radio/TV).

Network Address Translation (NAT)

- **Purpose**: Allows multiple devices on a private network (using private IP addresses) to share one or a few public IP addresses for internet access. Key for mitigating IPv4 address exhaustion.
- **How it works**:
    1. Internal host (private IP) sends a packet to an external destination via the NAT router.
    2. NAT router replaces the private source IP with its own public IP address and typically assigns a unique source port number. It records this mapping (private IP:port <-> public IP:new_port).
    3. When a response arrives at the NAT router's public IP and the new_port, the router uses its mapping table to translate the destination IP/port back to the original private IP:port and forwards it to the internal host.

Boundary, Ingress, Egress Routers

- **Boundary Router**: Connects a network (often an Autonomous System - AS) to another

network or the Internet. Often a point for deploying firewalls.
- **Ingress Router**: Router where traffic *enters* a specific network or part of a network.
- **Egress Router**: Router where traffic *leaves* a specific network or part of a network.
- Ingress and egress can be the same physical router if there's a single point of entry/exit. These terms can also refer to functionality rather than strict topology.

IPv6 (Internet Protocol version 6)

- **Goal**: Successor to IPv4, primarily addressing IPv4 address exhaustion.
- **Adoption**: Slow but ongoing.

IPv6 Headers

- **Simpler** than IPv4 header.
- **Key Fields**:
  - **Version**: 6.
  - **Traffic Class**: For QoS.
  - **Flow Label**: For identifying packets belonging to the same flow.
  - **Payload Length**: Length of the payload.
  - **Next Header**: Identifies type of the first extension header or Layer 4 protocol.
  - **Hop Limit**: Similar to IPv4 TTL.
  - **Source Address**: 128-bit address.
  - **Destination Address**: 128-bit address.
- **Extension Headers**: Optional headers placed between the IPv6 header and payload for additional functionality (e.g., routing, fragmentation).

IPv6 Addressing

- **Size**: 128 bits.
- **Notation**: Eight groups of four hexadecimal digits, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- **Zero Compression**:
  - Leading zeros in a group can be omitted (e.g., 0db8 becomes db8).
  - One sequence of consecutive zero-blocks can be replaced by :: (e.g., 2001:0db8:0000:0000:1234::5678 becomes 2001:db8::1234:0:5678 or 2001:db8::1234::5678 is incorrect, only one ::). Example from text: 2001:0db8:0000:0000:0000:0000:0000:0123 becomes 2001:db8::123.
- **Structure**: Typically split into a **prefix** (network part) and an **interface identifier** (host part). Usually a /64 prefix, leaving 64 bits for the interface ID.
- **Multiple Addresses per Interface**: Common and normal.

IPv6 Address Types & Scopes

- **Scope**: Defines the region where an address is unique and valid (e.g., link-local, global).

- **Unicast**: To a single interface.
    - **Global Unicast Address (GUA)**: Publicly routable on the Internet. Typically starts with 2000::/3. ISPs assign these (e.g., a /48 or /56 to an organization, which then subnets to /64 for links).
    - **Link-Local Address**: fe80::/10 prefix. Automatically configured on interfaces (SLAAC). Used for communication on the same local link only; not routed. Often includes a scope/zone ID (e.g., fe80::1234%eth0 or fe80::1234%3).
    - **Unique Local Address (ULA)**: fc00::/7 prefix (specifically fd00::/8 is used for locally assigned ULAs). Private addresses, not routed on the global Internet but can be routed within a set of cooperating sites. Requires a 40-bit globally unique random ID to make the prefix.
- **Multicast**: ff00::/8 prefix. Delivers a packet to all interfaces in a multicast group. Replaces broadcast.
- **Anycast**: A unicast address assigned to multiple interfaces. Packets sent to an anycast address are routed to the "nearest" interface (in routing terms).
- **Special Addresses**:
    - ::1/128: Loopback address (like 127.0.0.1).
    - ::/128: Unspecified address (source IP when host doesn't have one yet, e.g., DHCP).
    - ::/0: Default route in IPv6 routing tables.
    - 2001:db8::/32: Reserved for documentation and examples.

Moving to IPv6 (Transition Mechanisms)

- **Dual Stack**: Devices and routers run both IPv4 and IPv6 protocol stacks simultaneously. They can communicate using either protocol. This is the most common approach.
- **Tunnelling**: Encapsulating IPv6 packets within IPv4 packets (or vice-versa) to traverse parts of the network that only support one protocol. Examples:
    - 6to4 (2002::/16 prefix)
    - Teredo (2001::/32 prefix)

Layer 3 Commands (Diagnostic Tools)

- ping <ip_address_or_hostname>: Tests reachability using ICMP echo requests/replies.
- traceroute <ip_address_or_hostname> (Linux/macOS) or tracert <ip_address_or_hostname> (Windows): Displays the path (sequence of routers) to a destination. traceroute6 or tracert /6 for IPv6.
- route print (Windows) or netstat -r or ip route show (Linux): Displays the IP routing table.
- arp -a: Displays the ARP cache (IP to MAC address mappings).
- netstat (various options): Shows network connections, listening ports, interface statistics.
- ipconfig (Windows) or ifconfig / ip addr (Linux): Displays and configures IP addresses,

netmasks, gateways for network interfaces.

ATM (Asynchronous Transfer Mode) - Alternative Routing Model

- **Layers**: Operates across Layers 1-3.
- **Packets**: Uses fixed-size 53-byte "cells" (5-byte header, 48-byte payload). Allows for efficient router processing and low jitter.
- **Connection-Oriented**: A path, called a Switched Virtual Circuit (SVC), is established before data transmission.
- **Forwarding**: Uses Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) in the cell header to determine the next hop and new VPI/VCI values for that link. This is a lookup and swap, not a complex routing table search.
- **Ideal for**: Multimedia (voice, video) due to predictable forwarding and low jitter.
- **Layer 3**: ATM Adaptation Layer (AAL).