Chapter 7: The Network Layer (Layer 3) Exam Notes

These notes cover the initial sections of Chapter 7, focusing on the Network Layer, IPv4, and its special addresses, as requested.

7.1 Introduction to the Network Layer

- **Primary Function:** The network layer is responsible for routing packets from a source node to a destination node across a network.
- **Key Protocol Example:** The Internet Protocol (IP) is the primary example of a network layer protocol.
- **Core Topic:** Addressing is a fundamental aspect of the network layer due to its routing function.

7.2 IPv4

- **Prevalence:** IPv4 is the most widely deployed version of IP, though IPv6 is its intended successor. The transition to IPv6 has been predicted for many years but has not fully occurred, although IPv6 is used in large parts of the internet.
- **Service Type:** IP provides an unreliable, best-effort connectionless service. Its packets are known as datagrams. UDP (User Datagram Protocol) essentially adds Layer 4 functionality to IP.
- **Basic IPv4 Routing Algorithm:**
    1. If the destination node (B) is on the same network as the current node (A), A delivers the datagram directly to B.
    2. If A and B are on different networks, A consults its routing table. If an entry exists for B, A forwards the datagram to the specified next hop (router).
    3. If no specific route to B is found in the routing table, A sends the datagram to its default gateway (default router).
    4. If no default gateway is specified and no other route is found, A discards the datagram (reflecting IP's unreliable nature).
- **IPv4 Header (Figure 7.1):**
    - **Source and Destination Addresses:** Essential for routing.
    - **Checksum:** Covers only the header, meaning payload changes are not detected by IP. This is indicative of its unreliable nature.
    - **Time to Live (TTL):** Indicates the maximum number of hops a packet can traverse before being discarded. Each router decrements the TTL by 1. When TTL reaches 0, the datagram is discarded. This prevents packets from looping indefinitely in routing loops, which could congest networks.
    - **Version:** For IPv4, this field is 4. It indicates the header structure. (IPv6 will have a value of 6 here).
    - **IHL (Internet Header Length):** Not explicitly detailed in the provided snippet but is part of the standard header.
    - **Type of Service:** Originally intended for quality of service, but rarely used. Newer

RFCs reassigned it as the Differentiated Services field.
    - **Total Length:** Indicates the total length of the datagram (header + payload).
    - **Identification:** A number that helps identify the datagram, not used for sequencing.
    - **Flags:** Discussed later in the chapter (not in this summary).
    - **Fragment Offset:** Discussed later in the chapter (not in this summary).
    - **Protocol:** Indicates the Layer 4 protocol used at the origin (e.g., TCP, UDP). This allows the destination's Layer 3 to pass the payload to the correct Layer 4 protocol.
    - **Options:** Discussed later in the chapter (not in this summary).
    - **Padding:** Adds bits to ensure the header ends on a 32-bit word boundary; often not required.

7.2.1 IPv4 Addresses

- **Size:** IPv4 addresses are 32 bits long.
- **Notation:** Usually written in dotted decimal notation (e.g., 1.2.3.4), where each of the four bytes is converted to decimal and separated by dots.
- **Structure:** Divided into a **network portion** (identifies the network) and a **host portion** (identifies a specific host on that network).
- **Address Classes (Original System):** The class determines the split between network and host portions, identified by the initial bits of the address.
    - **Class A:** Starts with '0'. First byte is the network portion, remaining three bytes are the host portion. Max $2^8-1=128$ networks.
    - **Class B:** Starts with '10'. First two bytes are the network portion, final two bytes are the host portion. Max $2^{16}-2=16,384$ networks.
    - **Class C:** Starts with '110'. First three bytes are the network portion, last byte is the host portion. Max $2^{24}-3=2,097,152$ networks.
    - **Class D:** Starts with '1110'. Used for multicast addressing (discussed later). No network/host portion distinction.
    - **Class E:** Starts with '1111'. Reserved for future use and currently unused.
- **Special Host Numbers:**
    - **Host number of all 0s:** Identifies the network itself, not a specific host (e.g., 10.0.0.0 refers to the network 10.0.0.0). Used in routing tables.
    - **Host number of all 1s (binary):** Broadcast address for all hosts on that specific network (e.g., for network 10.0.0.0, the broadcast address is 10.255.255.255).
    - Since these two addresses cannot be assigned to hosts, a host field of n bits can address 2^n-2 hosts.
- **Netmask:**
    - Indicates which bits form the network portion (1s) and which form the host portion (0s). It's a sequence of 1s followed by 0s.
    - Represented in dotted decimal notation.
        - Class A: 255.0.0.0
        - Class B: 255.255.0.0

        - Class C: 255.255.255.0
- **CIDR (Classless Inter-Domain Routing) Notation:**
    - Specifies the number of bits in the network portion, separated from the address by a slash (e.g., 10.0.0.0/8 means the leftmost 8 bits are the network portion).
    - Useful when deviating from standard class definitions, such as in subnetting and supernetting.
- **Subnetting:**
    - Dividing a larger network into smaller subnetworks.
    - An organization with a Class A address (e.g., 10.0.0.0/8) might use some of the host bits to define subnets (e.g., use the second byte, making it 10.1.0.0/16 for sales, 10.2.0.0/16 for production).
    - The outside world still sees the original classful address (e.g., 10.0.0.0/8); the extended netmask is used internally.
    - The split need not occur on a byte boundary (e.g., a Class C address can be split with a netmask like 255.255.255.240 or /28).
    - The network address of a host is found by a logical AND of the host's IP address and the netmask.
- **Supernetting:**
    - Combining multiple smaller network addresses into a larger network, primarily to simplify routing tables on the internet.
    - Example: If an ISP is assigned 256 Class C networks from 192.168.0.0 to 192.168.255.0, these can be advertised as a single supernet 192.168.0.0/16 to the rest of the internet.
    - Affects routers outside the organization rather than inside.

7.2.2 Special IPv4 Addresses

A number of IPv4 addresses are reserved for special purposes.

- **127.0.0.1 (localhost):**
    - Refers to the computer on which it is used (the local machine).
    - Part of the 127.0.0.0/8 network, known as localnet.
    - The associated interface is the loopback interface.
    - Used for testing networking software on the local machine (e.g., ping 127.0.0.1).
- **0.0.0.0:**
    - Also used to refer to the local computer, but primarily as a placeholder, especially when a computer doesn't yet have an IP address.
    - Never used as a destination address for traffic.
    - Example: A computer requesting an IP address via DHCP might use 0.0.0.0 as its source address to indicate "me". The DHCP response wouldn't be sent to 127.0.0.1 (that's the server itself) or 0.0.0.0. Communication often relies on broadcasts.
- **255.255.255.255 (Limited Broadcast):**
    - Reserved for broadcasting "on the wire" – to all computers connected directly on the same local area network, not through a router.

- **Private Addresses:**
  - Blocks of addresses for use within private networks; not routed on the public internet. Public addresses are used on the public internet.
  - Allows organizations to build internal networks without needing globally unique public IP addresses for every device.
  - Network Address Translation (NAT) is used to allow devices with private addresses to communicate with the public internet, typically by translating the private source IP to a public IP of a NAT device (router).
  - The three reserved private address blocks are:
    - **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) (The range 172.16.0.0 to 172.31.0.0 refers to the networks within this block).
    - **192.168.0.0/16:** (192.168.0.0 – 192.168.255.255)
  - These ranges include network addresses, broadcast addresses, and usable private host addresses.
- **100.64.0.0/10 (Shared Address Space / Carrier-Grade NAT - CGN/CGNAT):**
  - A private address block reserved for use by ISPs and similar large connectivity providers (RFC 6598).
  - Helps ISPs manage IP address allocation to customers, often using CGNAT to share public IPs among many customers with private IPs from this range.
  - Addresses from this space are routable within an ISP's network but not on the public internet.
- **0.0.0.0/0 (Default Route):**
  - Used in routing tables to specify a default gateway or default "next hop".
  - An entry of 0.0.0.0/0 will match any destination address because it requires 0 bits to match, effectively acting as a catch-all for traffic not matching more specific routes.
  - Example from routing table (Figure 7.2): 0.0.0.0/0 directs traffic to 100.127.127.113.
- **Distinguishing 0.0.0.0 Uses:**
  - **0.0.0.0/0**: Found only in routing tables to mark a default route.
  - **0.0.0.0 (placeholder, often written as 0.0.0.0/32 in literature):** Used where a real address is not available or doesn't make sense (e.g., DHCP source, or as a "next hop" in a routing table when the destination is directly connected via an interface). The /32 notation suggests all 32 bits are network bits, which is counter-intuitive for a placeholder that should only match itself, but it is used.
- **169.254.0.0/16 (Link-Local Addresses / APIPA - Automatic Private IP Addressing):**
  - Used for communication between devices on a single network segment (link) when no DHCP server is available to assign addresses.
  - Devices automatically pick an address from this range and can communicate with other devices on the same link that have also self-assigned addresses from this block.
  - Example: A computer directly connected to a printer without being part of a larger managed network, or a laptop connected to a mobile phone hotspot where DHCP

might be overkill.

Summary Table of Common Special IPv4 Addresses (Table 7.1):

- **0.0.0.0/0:** Default gateway entry
- **0.0.0.0/32:** Placeholder for ‘this’ computer
- **10.0.0.0/8:** Private address block
- **100.64.0.0/10:** The shared address space (for CGN)
- **169.254.0.0/16:** Link-local addresses
- **172.16.0.0/12:** Private address block
- **192.168.0.0/16:** Private address block
- **255.255.255.255/32:** ‘Local’ broadcast

This concludes the notes up to and including the section on special IPv4 addresses as requested.