Computer Networks - Study Guide

Preparation for Test 3

Peijun Hou

Contents

1 Foundational Concepts in Networking

1.1 IP Header and Addressing

Concept:

- The IP protocol is a core component of the network layer, responsible for delivering packets between hosts.
- The IPv4 datagram consists of a header and a payload; the header includes fields such as source and destination IP addresses, TTL, and header checksum.
- IP addresses are 32-bit identifiers assigned to interfaces. Subnets divide address space into a network (subnet) and host part.
- Fragmentation allows large datagrams to be split into smaller pieces to accommodate link-layer MTU limitations.
- Classless Inter-Domain Routing (CIDR) enables flexible subnetting using a.b.c.d/x notation.

Explanation:

- **IP Datagram Format:** The header contains key fields such as:
  - `version, header length, total length, TTL, protocol, source IP, destination IP, header checksum`.
- **Header Checksum:** IP includes its own checksum for the header only, since IP may run over protocols without their own checksums. The checksum must be recomputed at every router due to TTL changes.
- **Fragmentation and Reassembly:** When a datagram exceeds the link MTU, it is fragmented. Each fragment contains:
  - The same identifier, a fragment offset, and a flag indicating whether more fragments follow.

  Reassembly occurs only at the final destination.
- **IP Addressing:** An IP address identifies an interface, not a device. Interfaces on the same subnet (same high-order bits) can communicate without routing.
- **CIDR:** Allows specifying subnets of arbitrary size using notation like `192.168.1.0/24`. This replaced rigid classful addressing (Class A, B, C).
- **Limitations:** IPv4 binds addresses to interfaces, complicating mobility and multihoming. Techniques like LISP and Mobile IP aim to decouple identity from location.

1.2 DHCP, NAT, and IPv6

Concept:

- **DHCP (Dynamic Host Configuration Protocol):** Enables hosts to obtain IP addresses dynamically in a plug-and-play fashion.
- **NAT (Network Address Translation):** Allows multiple devices in a local network to share a single public IP address.
- **IPv6:** New version of the IP protocol with a larger address space (128 bits) and improved header design.

Explanation:

- **DHCP Operation:** DHCP uses a four-step client-server interaction:

1. DHCP Discover (broadcast by client)
2. DHCP Offer (from server)
3. DHCP Request (from client)
4. DHCP ACK (from server)

It can also provide additional configuration such as DNS server, default gateway, and subnet mask.

- **NAT Mechanism:** Translates private IP addresses inside a local network to a single public IP address. Each outgoing packet's source address and port are replaced with NAT's public IP and a new port number. The NAT device maintains a translation table to reverse the mapping for incoming responses.
- **NAT Benefits:**
  - Reduces the need for globally unique IP addresses.
  - Increases security by hiding internal network structure.
  - Allows IP renumbering and ISP changes without affecting internal devices.
- **NAT Limitations:**
  - Violates the end-to-end principle.
  - Makes peer-to-peer applications and direct incoming connections more difficult.
  - Controversial because it involves layer 4 (ports) at routers.
- **IPv6 Motivation:**
  - Exhaustion of 32-bit IPv4 address space.
  - IPv6 simplifies header processing and supports better QoS.
- **IPv6 Features:**
  - Fixed 40-byte header (no fragmentation by routers).
  - No header checksum (to reduce processing time).
  - New addressing modes including anycast.
  - ICMPv6 enhancements.
- **Transition to IPv6:** Tunneling allows IPv6 packets to be encapsulated within IPv4 for routing across legacy networks. Deployment has been slow but is ongoing.

1.3 Generalized Forwarding Software Defined Networking (SDN)

Concept:

- **Middleboxes:** Devices operating at the network layer that perform functions beyond basic routing, e.g., NAT, firewalls, load balancers.
- **SDN (Software Defined Networking):** Separates the control and data planes; control logic is centralized in a controller that programs forwarding devices.
- **OpenFlow:** A standard protocol enabling SDN by allowing external controllers to define forwarding rules in network switches.
- **Generalized Forwarding:** Uses a match-plus-action abstraction where rules are based on packet header fields, allowing flexible and programmable forwarding.

Explanation:

- **Problem with Traditional Middleboxes:**

  - Increased complexity in network management.
  - Violation of the end-to-end principle.

- **OpenFlow Flow Table Entries:**
  - Each rule includes a header match, an action (e.g., forward, drop, modify), and counters.
  - Priorities are used to resolve conflicts in overlapping rules.

- **Match-Action Abstraction:**
  - Matches can include Layer 2, 3, and 4 header fields (e.g., IP src/dst, TCP port).
  - Actions may involve forwarding, dropping, sending to controller, or field modification.

- **Flow Setup Process:**
  - Upon a table miss, the switch sends a `Packet-IN` to the controller.
  - Controller replies with `Packet-OUT` and/or `Flow-MOD` to define a new rule.
  - The new flow is cached in the switch to speed up future packets.

- **Programmable Data Planes (P4):**
  - Evolved from OpenFlow to support run-time programmable match+action pipelines.
  - Helps reduce complexity while enabling flexibility in packet processing.

1.4 Link-State Routing and Dijkstra's Algorithm

Concept:

- Link-state routing protocols allow each router to build a complete map of the network and compute the shortest path to all other nodes.
- Dijkstra's algorithm is used to compute the least-cost path from a source to all other nodes in the network based on the global topology information.

Explanation:

Link-State Routing Principles:

- Each router discovers its directly connected neighbors and the cost to reach them.
- It constructs a link-state packet (LSP) containing this information and floods it to all other routers in the network.
- All routers collect LSPs from every other router and construct an identical graph of the network.
- Using the complete network graph, each router independently computes the shortest-path tree rooted at itself.

Dijkstra's Algorithm (Centralized Version):

- Each router runs Dijkstra's algorithm on the graph:
  - Let $D(v)$ be the current known shortest distance from the source node to node v.
  - Maintain a set N' of nodes whose shortest distance is finalized.
  - At each step, add the node with the smallest tentative distance to N'.
  - Update distances of all neighbors of the newly added node.
- The process repeats until all nodes are in N', meaning the shortest paths from the source to all nodes are known.

1.5 Distance Vector Routing and Bellman-Ford

Concept:

- Distance vector routing protocols enable routers to determine shortest paths to all destinations by exchanging vectors of distance estimates with their neighbors.
- The Bellman-Ford algorithm is the foundation for distance vector routing and uses an iterative, distributed method to compute minimum-cost paths.

Explanation:

Distance Vector Principles:

- Each router maintains a **distance vector**, which is a table containing the estimated minimum cost to each destination in the network.
- Routers periodically send their distance vectors to all directly connected neighbors.
- Upon receiving a neighbor's distance vector, a router updates its own table using the **Bellman-Ford equation**:

$$D_x(y) = \min_{v \in \text{Neighbors}(x)} \{c(x,v) + D_v(y)\}$$

  where $D_x(y)$ is the cost from node x to destination y, and $c(x,v)$ is the cost to neighbor v.

Algorithm Characteristics:

- **Distributed:** Routers operate independently and exchange information only with immediate neighbors.
- **Iterative:** Updates occur over time as new distance vectors are received.
- **Asynchronous:** No global clock or synchronization is required.
- Routers only send updates when their distance vector changes (triggered updates).

1.6 Intra-AS Routing: OSPF

Concept:

- OSPF (Open Shortest Path First) is a link-state routing protocol used for routing within a single autonomous system (AS).
- It uses Dijkstra's algorithm to compute shortest paths based on a complete view of the intra-AS topology.

Explanation:

- OSPF is a link-state protocol: each router floods link-state advertisements (LSAs) containing information about its links and their costs.
- Routers receiving LSAs build a full map of the network and independently run Dijkstra's algorithm to compute the shortest-path tree rooted at themselves.
- OSPF divides an AS into **areas** to enhance scalability:
  - All routers in an area have identical LSDBs (link-state databases).
  - Area 0 is the backbone area; all inter-area traffic must go through it.
  - Area Border Routers (ABRs) connect different areas.
- OSPF supports multiple equal-cost paths (ECMP), making load balancing possible.

- Each router is assigned a unique router ID (typically the highest IP address of any of its interfaces).
- OSPF uses **Hello** messages to discover neighbors and maintain adjacencies.
- Routing updates are reliable and sent over IP using protocol number 89 (not UDP/TCP).
- Authentication can be enabled to secure OSPF message exchanges.
- OSPF allows route summarization at ABRs to reduce LSA flooding between areas.

1.7 Inter-AS Routing: BGP and Policy-based Routing

Concept:

- BGP (Border Gateway Protocol) is the de facto inter-domain routing protocol used to exchange routing information between autonomous systems (ASes).
- Unlike intra-AS routing, BGP is policy-driven: routing decisions are based on operator-defined policies rather than solely on shortest path metrics.

Explanation:

- BGP is a path-vector protocol: it maintains the AS-level path for each route and avoids loops by rejecting paths that contain the local AS.
- Each BGP route advertisement includes:
  - **NEXT-HOP:** IP address to reach the destination.
  - **AS-PATH:** ordered list of ASes the route has passed through.
  - **PREFIX:** destination IP prefix being advertised.
- BGP operates in two modes:
  - **eBGP (External BGP):** between routers in different ASes.
  - **iBGP (Internal BGP):** within the same AS, for internal propagation of external routes.
- BGP sessions run over long-lived TCP connections (port 179) and exchange four types of messages: OPEN, UPDATE, KEEPALIVE, and NOTIFICATION.
- BGP uses routing policies to control:
  - Which routes to accept from neighbors (import policies).
  - Which routes to advertise to neighbors (export policies).
  - Preference of paths based on attributes (e.g., local preference, AS path length).
- Policy-based routing allows ISPs to enforce business relationships, such as:
  - Prefer customer routes over peer or provider routes.
  - Do not transit traffic between two peers or two providers.
- Routers maintain a routing information base (RIB), selecting the best route per prefix based on policy and exporting it to the forwarding information base (FIB).

1.8 Link Layer Services and Error Detection

Concept:

- The link layer provides node-to-node communication over a physical link and is responsible for framing, addressing, error detection, and optionally reliable delivery.
- It acts as the interface between the physical layer and the network layer.

Explanation:

- A link-layer protocol operates on a single link connecting two adjacent nodes and is responsible for encapsulating network-layer datagrams into frames.
- **Link Layer Services:**
  - **Framing:** Encapsulate datagrams into frames with headers and trailers.
  - **Link Access:** Determines how multiple devices share a link (especially important in broadcast links like Ethernet or Wi-Fi).
  - **Reliable Delivery:** Uses acknowledgments and retransmissions on unreliable links (e.g., wireless).
  - **Flow Control:** Regulates the pace of transmission between two nodes.
  - **Error Detection:** Detects bit errors introduced by noise or interference.
- **Error Detection Mechanisms:**
  - **Parity Check:** Adds a single parity bit (even or odd) to detect single-bit errors.
  - **Checksums:** Used in TCP/UDP/IP headers; calculates a sum of data words.
  - **Cyclic Redundancy Check (CRC):**
    - Uses polynomial division on frame contents.
    - Appends a CRC remainder to the frame.
    - Receiver performs the same division to check correctness.
- Error detection does not correct errors; it simply allows the receiver to detect corruption and discard bad frames or request retransmission.
- Link-layer addressing uses **MAC addresses**, which are flat and globally unique identifiers assigned to network interfaces.
- The link layer is typically implemented in hardware (e.g., NIC card or chip) but may involve some software logic.

1.9 MAC Protocols: TDMA, FDMA, CSMA, ALOHA, CDMA, OFDMA

Concept:

- Medium Access Control (MAC) protocols regulate how multiple devices share a common communication medium in a broadcast link (e.g., Ethernet, Wi-Fi).
- MAC protocols are essential in the link layer for avoiding or resolving collisions when multiple nodes contend for access to the channel.

Explanation:

Goals of a MAC Protocol:

- Efficient and fair use of the channel.
- Minimize collisions and idle time.

- Enable distributed access without centralized scheduling.

MAC Protocol Categories:
1. Channel Partitioning:

- Divide the channel into distinct resources: time, frequency, or codes.
- Each device gets exclusive access to its portion.
- **TDMA (Time Division Multiple Access):**
  - Time is divided into slots; each device transmits in its assigned slot.
  - Eliminates collisions but leads to idle time if a device has no data.
- **FDMA (Frequency Division Multiple Access):**
  - Spectrum is divided into frequency bands; each device transmits on its own band.
  - Guard bands are used to prevent interference.
- **CDMA (Code Division Multiple Access):**
  - Each device is assigned a unique code to modulate its signal.
  - Multiple users can transmit simultaneously using orthogonal codes.

2. Random Access:

- Devices transmit at will and detect or recover from collisions.
- More efficient when network load is low.
- **ALOHA:**
  - Transmit whenever ready; resend after random backoff if collision occurs.
  - Slotted ALOHA improves efficiency by enforcing time slot boundaries.
- **CSMA (Carrier Sense Multiple Access):**
  - Listen before transmitting; defer if channel is busy.
  - **CSMA/CD (Collision Detection):** Used in Ethernet; detect collisions and abort.
  - **CSMA/CA (Collision Avoidance):** Used in Wi-Fi; avoid collisions using backoff timers and RTS/CTS.

3. Taking Turns:

- Devices take turns to transmit using controlled access.
- **Polling:** Central controller polls each device for permission to transmit.
- **Token Passing:** A token is passed among devices; only the holder can transmit.

4. Hybrid Techniques:
OFDMA (Orthogonal Frequency Division Multiple Access):

- Used in modern wireless systems (e.g., LTE, Wi-Fi 6).
- Combines frequency and time division with orthogonal subcarriers.
- Allows multiple users to transmit simultaneously in different time-frequency resource blocks.

2 Practice and Sample Test Questions

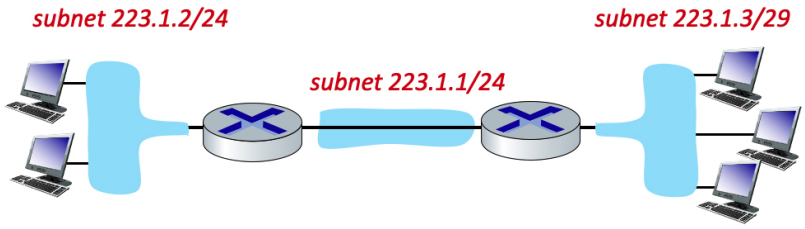
Test 3 may include questions on all topics covered in class, and it will mostly cover topics covered after test 2, but this study guide focuses only on selected topics covered after test 2.

1. Explain how IP fragmentation works. Where is fragmentation done, and where is reassembly done? Name and explain the three key IP header fields involved.

2. What is the purpose of the Header Checksum field in the IP header? Why must it be updated by each router?

3. NAT is often used to conserve IP addresses. Describe how NAT modifies packet headers and maintains mappings. What are some downsides of using NAT?

4. Consider the three subnets in the diagram below. Which of the following addresses can not be used by an interface in the 223.1.3/29 network? Check all that apply.
   a) 223.1.3.16



   b) 223.1.3.28
   c) 223.1.3.2
   d) 223.1.3.6
   e) 223.1.2.6

5. We've seen that there are two approaches towards implementing the network control plane - a per-router control-plane approach and a software-defined networking (SDN) control-plane approach. Which of the following actions occur in a per-router control-plane approach? The other actions that you don't select below then correspond to actions in an SDN control plane.
   a) Routers send information about their incoming and outgoing links to other routers in the network.
   b) A control agent in router receives a complete forwarding table, which it installs and uses to locally control datagram forwarding.
   c) All routers in the network send information about their incoming and outgoing links to a logically centralized controller.
   d) A router exchanges messages with another router, indicating the cost for it (the sending router) to reach a destination host.

6. List three key differences between IPv4 and IPv6. What benefits does IPv6 offer over IPv4 with NAT in terms of scalability and security?

7. Which of the following fields occur ONLY in the IPv6 datagram header (i.e., appear in the IPv6 header but not in the IPv4 header)? Check all that apply.
   a) The flow label field.
   b) The header checksum field.
   c) The header length field.
   d) The upper layer protocol (or next header) field.
   e) The time-to-live (or hop limit) field.
   f) The IP version number field.

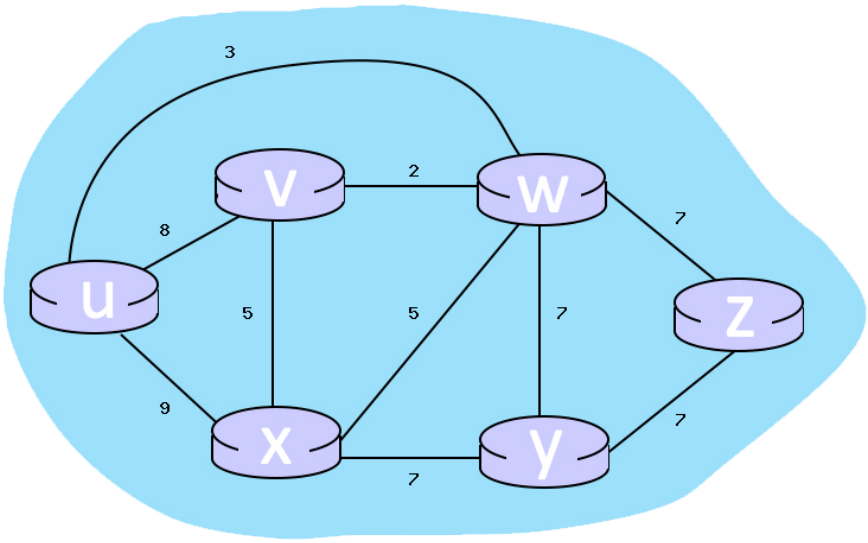
g) 128-bit source and destination IP addresses.
h) The options field.

8. Explain the match-plus-action model in SDN's generalized forwarding. What fields can be matched in an OpenFlow flow table entry?

9. What is meant by generalized forwarding (as opposed to destination-based forwarding) in a router or switch?
a) Any of several actions (including drop (block), forward to a given interface, or duplicate-and-forward) can be made based on the contents of one or more packet header fields.
b) None of the other answers is a correct definition of generalized forwarding.
c) The decision about which output port to forward a packet to can be made based on the link-type of the outgoing port (e.g., Ethernet versus WiFi).
d) In addition to performing forwarding, the device can generalize its services, also performing hop-by-hop reliable data transfer and per-hop congestion control.

10. Write the Bellman-Ford update equation used in distance vector routing. Explain how routers use this equation in a distributed and iterative fashion.

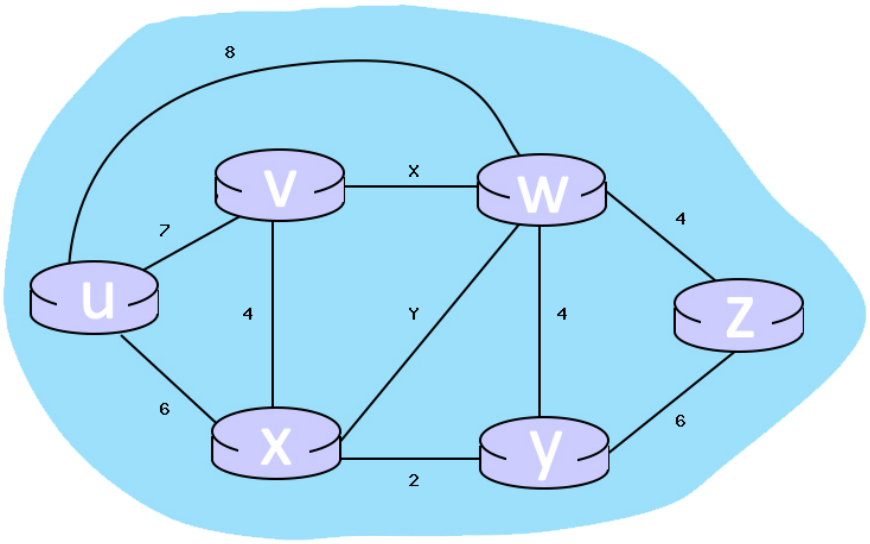
11. Consider the 6-node network shown below, with the given link costs. Using Dijkstra's algorithm, find the least cost path from source node U to all other destinations and answer the following questions.
a) What is the shortest distance to node z and what node is its predecessor?



b) What is the shortest distance to node x and what node is its predecessor?
c) What is the shortest distance to node w and what node is its predecessor?

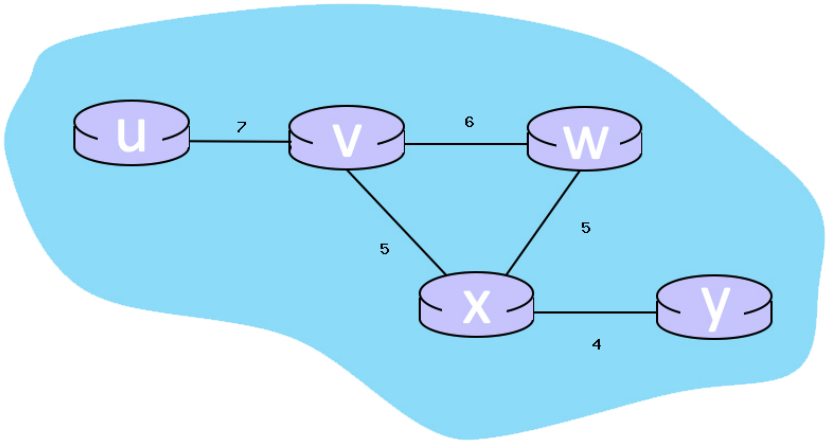
12. Consider the incomplete 6-node network shown below, with the given link costs.
a) For link X, what is the cost associated with this link? If the answer can't be determined given the

Node	Shortest distance from X	Previous Node
X	0	n/a
W	2	X
Y	2	X
V	4	X
U	6	X
Z	6	W



information, respond with 'n/a'.
b) For link Y, what is the cost associated with this link? If the answer can't be determined given the information, respond with 'n/a'.

13. Consider the 6-node network shown below, with the given link costs:
a) When the algorithm converges, what are the distance vectors from router 'V' to all routers? Write



your answer as u,v,w,x,y.
b) What are the initial distance vectors for router 'X'? Write your answer as u,v,w,x,y and if a distance is ∞, write 'x'.
c) The phrase 'Good news travels fast' is very applicable to distance vector routing when link costs decrease; what is the name of the problem that can occur when link costs increase?

14. What are the primary services provided by the link layer? Briefly describe the purpose of framing and error detection.

15. Explain how Cyclic Redundancy Check (CRC) is used to detect errors in frames. What happens when an error is detected?

16. What type of routing protocol is OSPF: link-state or distance-vector? Briefly explain how routers in OSPF learn about the full network topology.

17. What is the purpose of the AS-PATH attribute in BGP route advertisements? How does it help avoid routing loops?

18. Briefly describe how TDMA, FDMA, and CDMA divide the communication medium among multiple users.

19. Consider the figure below, which shows the arrival of 9 messages for transmission at different multiple access wireless nodes at times t = (0.1, 0.3, 0.6, 1.4, 2.3, 3.4, 3.7, 4.8, 4.9) and each transmission requires exactly one time unit. What protocol is it?
    a) Aloha

    b) Slotted-Aloha
    c) CSMA
    d) CSMA-CD

20. What are the primary services provided by the link layer? Briefly describe the purpose of framing and error detection.

21. Describe the main role of the communication layer, the network-wide state-management layer, and the network-control application layer in an SDN controller.

22. Is it necessary that every autonomous system use the same intra-AS routing algorithm? Why or why not?

23. Why do we need another checksum when TCP and UDP already have one?

24. How to prevent oscillations when using congestion or delay-link metric in Dijkstra's algorithm?

25. List three error detection methods and explain.

Use these questions to guide your studying. Focus on understanding the ***concepts*** *and* ***explanations*** *in each subsection, then apply them to these practice problems. Good luck!*