CS168 Midterm

Oct. 20, 2015

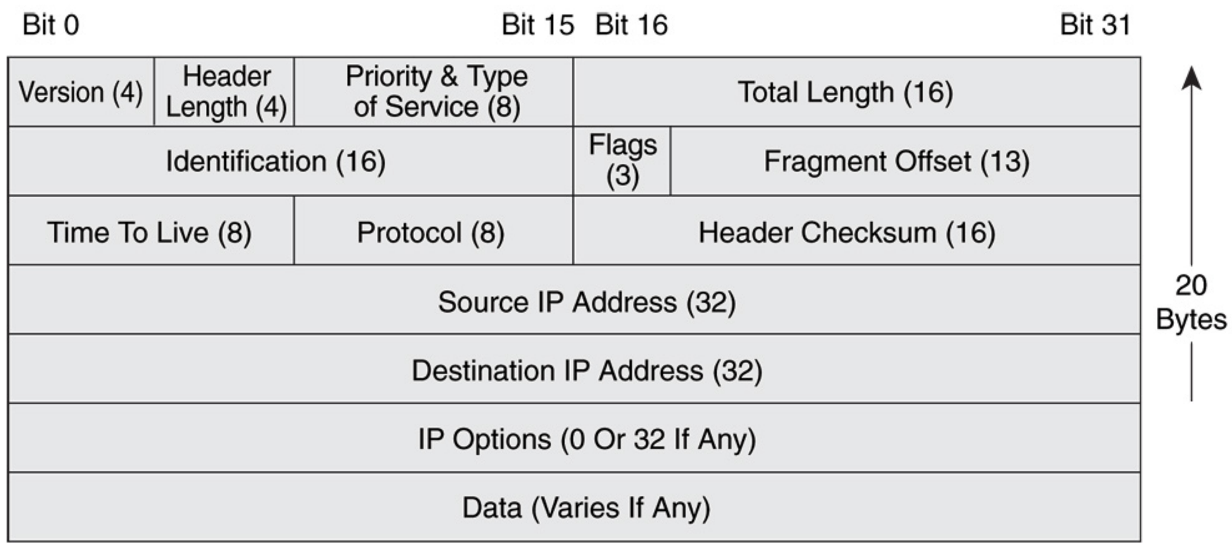
Abandon all hope, ye who enter here
–Dante

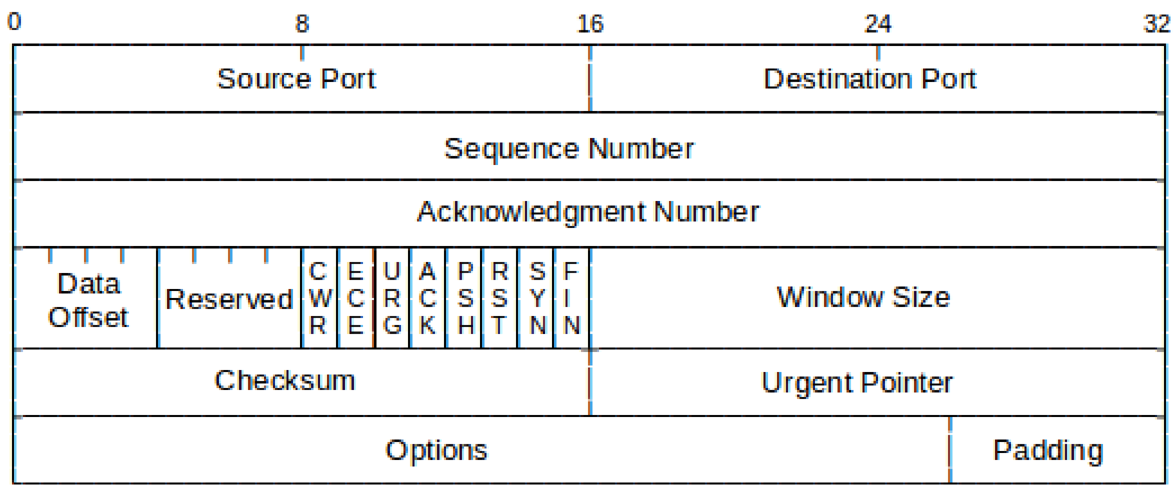
Instructions: Read them NOW!

- **Please detach the last page of this test, and use it to enter all your answers.**
- **Write your name and SID on the answer sheet!**
- You may write on the test itself, but only the answer sheet will be graded. In addition, there are blank pages at the end for you to use as scratch paper.
- This examination is CLOSED BOOK/CLOSED NOTES.
- You will not require a calculator, iPhone, laptop computer, or other calculation aid. Please put them away right now! Using electronics of any kind during the test will be considered cheating, and you will be excused from the room.
- You MAY use one 8.5"x11" double-sided crib sheet, packed with **handwritten** notes, formulas, and diagrams.

Fun Facts to Remember

- 1 TB $= 10^{12}$ bytes; 1 GB is 10^9 bytes; 1 MB is 10^6 bytes
- 1Gbps is 10^9 bits/sec; 1Mbps is 10^6 bits/sec
- 1 msec is 10^{-3} seconds; 1 μsec is 10^{-6} seconds.
- The IPv4 header and TCP header are depicted below.





(26) 1. **Acronym Olympics**

Match each acronym to its corresponding description. Use each of these acronyms once and only once:

ACK	HTTP	MSS	SYN
ARP	IANA	MTU	TCP
C	ICMP	MX	TLD
DHCP	IETF	NAT	TTL
DNS	IPv4	NS	UDP
E2E	IPv6	RST	
FIN	ISN	RTO	

(1) (a) This flag is often set on the second packet of a TCP exchange.

(1) (b) When this reaches zero, the packet is dropped.

(1) (c) This limits the size of a packet.

(1) (d) This is the transport protocol most often used by DNS.

(1) (e) This is how TCP abruptly terminates a connection.

(1) (f) This makes traceroute work.

(1) (g) The protocol that underlies the web.

(1) (h) This protocol normally has a 20-byte header, and can have options.

(1) (i) This determines how long TCP waits before retransmitting a packet.

(1) (j) This enables many hosts to share a single IP address.

(1) (k) This flag is typically set on the first packet in a TCP exchange.

(1) (l) This principle provides the rationale for not making IP service reliable.

(1) (m) This class of address (in classful addressing) is what CIDR calls a /24.

(1) (n) This limits the size of a TCP payload.

(1) (o) This protocol has a Next Header field.

(1) (p) This body is where protocol standards are handled.

(1) (q) This is how a TCP connection terminates gracefully.

(1) (r) This resource record maps a domain name to the name of the mail server.

(1) (s) This is often how a host finds out where its local DNS server is.

(1) (t) This is how a host finds out the MAC address of another host.

(1) (u) This body handles all Internet policy issues related to numbering and names.

(1) (v) This resource record maps a domain name to the name of the authoritative name server.

(1) (w) This infrastructure has a root located in Reston, VA.

(1) (x) This is the transport protocol used by HTTP.

(1) (y) This is what .com, .edu, and .fr are.

(1) (z) This value is carried in a SYN packet.

(51) 2. **Short Question Sprint**

(3) (a) **Principles**: Our discussion of modularity led us to three networking principles: (A) Layering, (B) End-to-End, and (C) Fate-Sharing. Below please indicate which principle best fits each description by writing the associated letter (A, B, or C).

(1) i. Gives guidance about which functionality goes in the network.

(1) ii. Gives guidance about where state should be stored.

(1) iii. Gives guidance about how functionality is modularized.

(3) (b) **IPv4 vs IPv6**: Consider the following protocol fields: (A) Identification, (B) Flow-Label, and (C) Source Address. Please indicate your answers below using the associated letters A, B, and C.

(1) i. Which of these is in both IPv4 and IPv6?

(1) ii. Which of these is in IPv4 but not IPv6?

(1) iii. Which of these is in IPv6 but not IPv4?

(6) (c) **Fragmentation**: An IP packet of size 5000B arrives at a link with an MTU of 1500B. The packet is broken up into four fragments (numbered 1, 2, 3, 4), the first three of which are 1500B.

(2) i. How big (total IP packet size in bytes) is the last fragment?

(2) ii. Which (if any) of the four fragments have the MF field set?

(2) iii. What is the value of the offset field for the second fragment?

(6) (d) **LPM**: Consider the following CIDR routing table:

default $\Rightarrow$ port 1
64.0.0.0/2 $\Rightarrow$ port 2
80.0.0.0/4 $\Rightarrow$ port 3

For each arriving packets with the given destination address below, please write the port they are sent to.

(2) i. `01110101 01001100 11001010 11011001`

(2) ii. `10101010 10101001 11011100 00001100`

(2) iii. `01011101 01100101 10010110 01110001`

(6) (e) **Subnets**: Consider the following address assignments:
Host A has IP address `01001101 01100101 10010110 01110001` and is on a subnet with netmask `11111111 11111110 00000000 00000000`.
Host B has IP address `01001101 01100100 01001101 01100101`.
Host C has IP address `01101101 01100101 10010110 01110001`.

(2) i. Is Host B on the same subnet as Host A? (Yes or No)

(2) ii. Is Host C on the same subnet as Host A? (Yes or No)

(2) iii. Is Host B on the same subnet as Host C? (Yes or No)

(4) (f) **NAT**: Which of the following fields does Network Address Translation overwrite on outgoing packets? List all that apply.

A. Source IP Address
B. Destination IP Address
C. Source MAC Address
D. Destination MAC Address
E. Source Port
F. Destination Port

(4) (g) **Filling the pipe**: Host A is sending packets to Host B. The RTT between A and B is 0.2sec, and the bandwidth of the link is 120Mbps. What is the minimal value of the window W (in bytes) that can use the available bandwidth?

A. 1MB
B. 2MB
C. 3MB
D. 4MB

(2) (h) **L2 Broadcast**: The L2 broadcast address is:

A. 255.255.255.255
B. GG:GG:GG:GG:GG:GG
C. FF:FF:FF:FF:FF:FF
D. 0.0.0.0

(4) (i) **DNS**: When the local DNS resolver does an iterative lookup on the name www.cs.stanford.edu and contacts the TLD server for .edu, what information is the resolver asking for?

A. Where is the root?
B. Where is the DNS server for .edu?
C. Where is the DNS server for stanford.edu?
D. Where is the DNS server for cs.stanford.edu?

(3) (j) **Header Fields**: Consider the following possibilities: (A) source IP address, (B) Checksum, (C) source port.

(1) i. Which field appears in IPv4, UDP, and TCP, but not in IPv6?
(1) ii. Which field appears in UDP and TCP, but not in IPv4 or IPv6?
(1) iii. Which field appears in IPv4 and IPv6, but not in UDP or TCP?

(10) (k) **True or False**: (Indicate your answer with T or F)

(1) i. The IP Checksum helps detect corruption of the packet payload.

(1) ii. The calculation of timeout values is improved if you estimate both the RTT and the Deviation in the RTT.

(1) iii. A TCP segment can be an ACK and carry Data.

(1) iv. The DF field is used to provide Quality-of-Service.

(1) v. The TCP source determines the size of the Advertised Window.

(1) vi. Link-State routing can have temporary loops during convergence.

(1) vii. One cannot do MTU discovery with IPv4.

(1) viii. The typical difference between MTU and MSS is 20 bytes.

(1) ix. The IPv6 header is always the same size.

(1) x. The UDP header contains source and destination addresses.

(15) 3. **TCP Timeouts and Retransmissions**

Assume that the current value of the RTO for a cross-country TCP connection is 0.2sec (and the estimates that go into the RTO remain constant during the events below). The advertised window is 400 bytes, and the ISN is 99. At time $t = 0$ the TCP source sends 100B packets with sequence numbers 100, 200, 300, and 400, and sets the timeout timer (which starts at RTO and begins to count down).

(5) (a) At time $t = 0.1$sec the source receives an ACK expecting the next byte to be 400. What does the TCP do then? (List all that apply.)

A. Retransmit the packet with sequence number 100
B. Retransmit the packet with sequence number 400
C. Send packets with sequence numbers 500, 600, 700
D. Reset the timeout timer (to RTO), which then begins counting down
E. Reset the timeout timer (to 2RTO), which then begins counting down
F. Nothing

(5) (b) No additional packets have arrived at the source by time $t = 0.3$sec. What does the TCP do then? (List all that apply.)

A. Retransmit the packet with sequence number 100
B. Retransmit the packet with sequence number 400
C. Send packets with sequence numbers 500 and 600
D. Reset the timeout timer (to RTO), which then begins counting down
E. Reset the timeout timer (to 2RTO), which then begins counting down
F. Nothing

(5) (c) At time $t = 0.4$sec the source receives an ACK expecting the next byte to be 500 (and has received no other packets in the meantime). What does the TCP do then? (List all that apply.)

A. Retransmit the packet with sequence number 100
B. Retransmit the packet with sequence number 400
C. Send packet with sequence number 800
D. Reset the timeout timer (to RTO), which then begins counting down
E. Reset the timeout timer (to 2RTO), which then begins counting down
F. Nothing

(12) 4. **TCP ACK Acrobatics**

Consider a TCP sender who sends 100B packets with seq numbers 100, 200, 300, 400, 500. After it has sent these packets (and before it sends any more), it receives a string of TCP ACKs (with no more to follow). We use the notation that A100 means that the receiver has received all bytes up to 99 and the next byte it is expecting is 100. If the network were acting perfectly, the resulting string of ACKs would be A200, A300, A400, A500, A600.

However, the network is not always perfect! Below we show you four possible streams of ACKs and ask you whether this was caused by Data packets being dropped and/or reordered (i.e., not received in the order they were sent), and/or ACK packets being dropped and/or reordered. We are asking for the *minimal* cause (which may involve more than one of these possibilities). To be more specific, if you could produce the stream of ACKs by (i) dropping an ACK packet, or (ii) dropping a Data packet and reordering the ACK packets, then choose the first cause. Write the letter or letters corresponding to the minimal cause (if there are multiple equally-minimal causes, choose only one for your answer).

(3) (a) If the ACKs coming back are (in sequence) A200, A300, A300, A300. List the minimal set of events that could have caused this.

A. A Data packet was dropped.
B. An ACK packet was dropped.
C. Some Data packets arrived out of order.
D. Some ACK packets arrived out of order.

(3) (b) If the ACKs coming back are (in sequence) A200, A300, A300, A300, A600. List the minimal set of events that could have caused this.

A. A Data packet was dropped.
B. An ACK packet was dropped.
C. Some Data packets arrived out of order.
D. Some ACK packets arrived out of order.

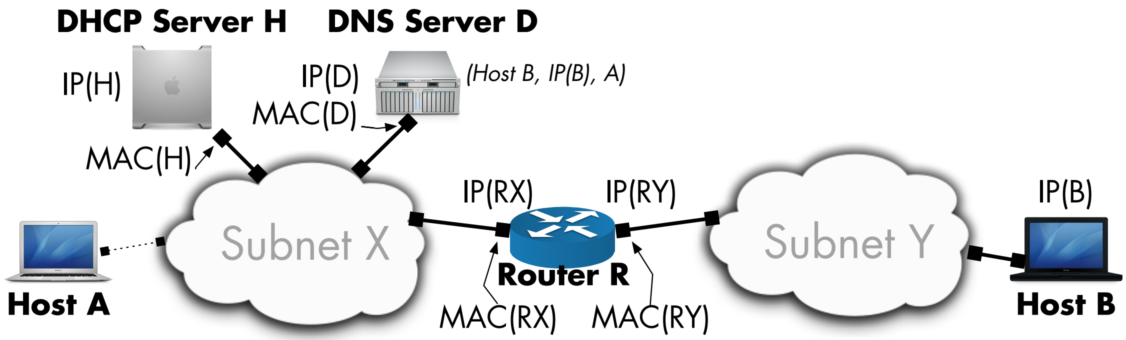
(3) (c) If the ACKs coming back are (in sequence) A200, A200, A300, A600. List the minimal set of events that could have caused this.

A. A Data packet was dropped.
B. An ACK packet was dropped.
C. Some Data packets arrived out of order.
D. Some ACK packets arrived out of order.

(3) (d) If the ACKs coming back are (in sequence) A200, A500, A300, A400, A600. List the minimal set of events that could have caused this.

A. A Data packet was dropped.
B. An ACK packet was dropped.
C. Some Data packets arrived out of order.
D. Some ACK packets arrived out of order.

(21) 5. **Fun at L2 and L3**



Consider the following scenario:

- Host A (a laptop) arrives on Subnet X and wants to send a PING packet to Host B, which is on Subnet Y.
- On subnet X are a DHCP server H (with IP address IP(H) and MAC address MAC(H)) and a DNS server D (with IP address IP(D) and MAC address MAC(D)). Host A will eventually be assigned IP address IP(A).
- Subnet X and Y are connected by Router R, which has an interface on Subnet X with IP address IP(RX) and MAC address MAC(RX) and an interface on Subnet Y with IP address IP(RY) and MAC address MAC(RY).
- We assume that all ARP caches are empty, but that the DNS server on Subnet X has host B's IP address cached.

We now want to construct what messages are sent in the process from Host A arriving until its message arrives at Host B. On the next page we have listed (in alphabetical order) a set of possible messages (some of which are part of the actual sequence, and some of which are not). You will be asked several questions about these, in terms of their order, their addresses, and their existence. We have put them on a separate page so the questions and the messages are both visible at the same time.

Please turn the page for the rest of this question.....

Alphabetical listing of messages (possibly) used in this scenario:

A) ARP asking for the MAC address associated with IP(A)
B) ARP asking for the MAC address associated with IP(B)
C) ARP asking for the MAC address associated with IP(D)
D) ARP asking for the MAC address associated with IP(RX)
E) ARP asking for the MAC address associated with IP(RY)
F) ARP response providing the MAC address associated with IP(A)
G) ARP response providing the MAC address associated with IP(B)
H) ARP response providing the MAC address associated with IP(D)
I) ARP response providing the MAC address associated with IP(RX)
J) ARP response providing the MAC address associated with IP(RY)
K) DHCP ACK
L) DHCP Discover message
M) DHCP Offer
N) DHCP Request
O) DNS query to find B's IP address
P) DNS query to find R's IP address
Q) DNS response with B's IP address
R) DNS response with R's IP address
S) PING packet being forwarded by R to B on subnet Y
T) PING packet being sent by A

This list is a strict superset of the messages needed to accomplish the task of sending the PING packet. You will be asked to identify the superfluous messages. In the other questions, please list all messages that apply (whether or not they are needed for the task) by using the letters above to identify the messages:

(3) (a) Which of these are broadcast over one of the subnets?

(3) (b) Which of these have destination IP address 255.255.255.255?

(3) (c) For which of these does the Source IP address refer to a different host or router than the Source MAC address? (Ignore packets that do not include an IP address, or use one that does not refer to a specific host.)

(3) (d) For which of these does the Destination IP address refer to a different host or router than the Destination MAC address? (Ignore packets that do not include an IP address, or use one that does not refer to a specific host.)

(3) (e) Which is sent first, Message B or Message T?

(3) (f) Which is sent first, Message Q or Message C?

(3) (g) Which messages would not be sent in this scenario?

(15) 6. **Variations on HTTP**

Host A wants to download two files from Server S. In doing so, it would take the following steps (listed alphabetically):

A) A initiates TCP Handshake (A sends SYN, S sends SYN-ACK, A sends ACK)

B) A initiates TCP Teardown (A sends FIN, S sends FIN-ACK, A sends ACK)

C) A sends HTTP request for file1

D) A sends HTTP request for file2

E) S responds with file1

F) S responds with file2

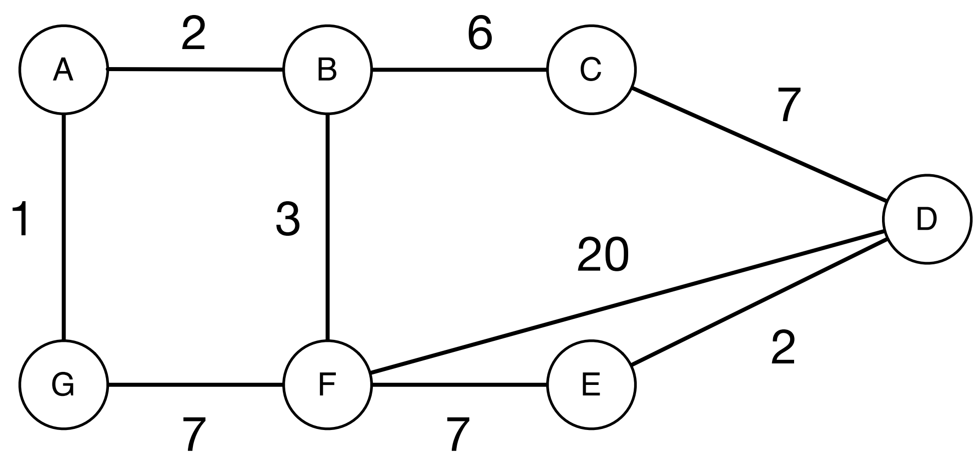
Please write down the order these steps would be taken for three variants of HTTP (using the letters associated with each step). In each case, assume that messages do not get reordered on the network and that the server processes requests in a first-in-first-out manner.

(5) (a) The simple one-object-at-a-time version of HTTP

(5) (b) Persistent HTTP

(5) (c) Pipelined HTTP

(15) 7. **Routing**



Consider the above graph, which should be familiar to you from Homework #2, where the routers are using distance-vector routing (where the path cost is the sum of the costs along the path up to the advertising router; it is up to the receiving router to add the cost of the link between them). Someone has misconfigured router F so that it advertises a distance of 3 to all destinations, and drops all packets sent to it. Thus, packets either reach their intended destination or are dropped by F. Please answer the following questions with Yes or No.

(3) (a) Would a packet sent by G to A reach A?

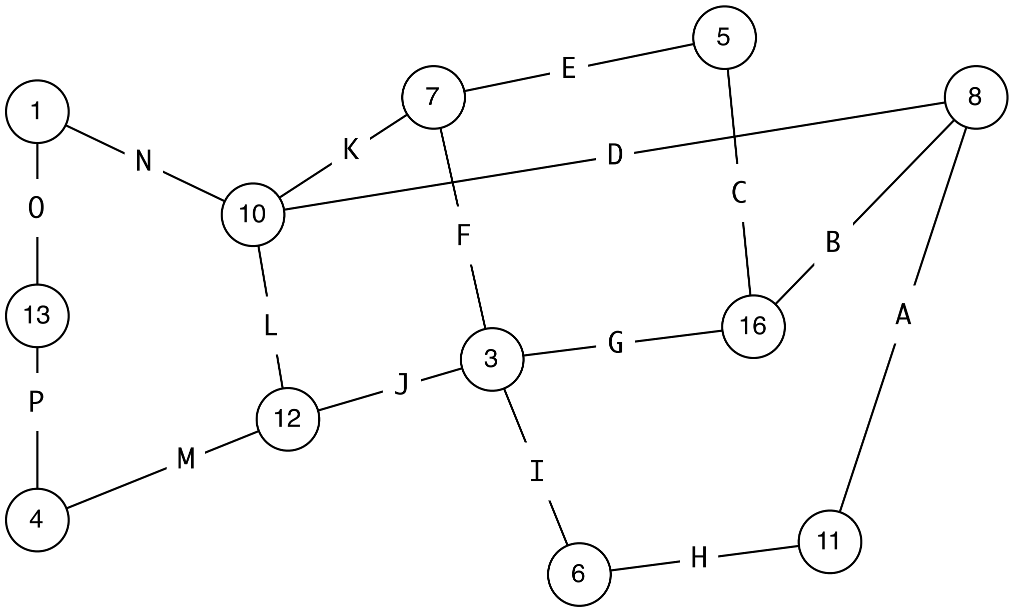
(3) (b) Would a packet sent by D to G reach G?

(3) (c) Would a packet sent by D to E reach E?

(3) (d) Would a packet sent by B to E reach E?

(3) (e) Is there any destination (besides F) such that if C sent a packet to that destination, it would end up being dropped by F?

(15) 8. **Spanning Tree Trials**



Here we apply the Spanning Tree Protocol (STP) described in class to the above graph (with the node IDs shown for each node, and links labeled with letters). As you know, the result of the STP protocol is that links are either "on" (part of the spanning tree, and used by the switches) or "off" (not used for forwarding packets other than for the STP protocol itself).

(5) (a) After the STP protocol has converged, which of the links are "off" (i.e., not used in the spanning tree)? Write down the letters associated with these links (in alphabetical order would be preferred).

(5) (b) Now assume that node 16 has been hacked, and that it acts as if it now has ID=1 (so there are two nodes with ID 1). The spanning tree protocol runs until it has converged. Which of the links are "off"? Write down the letters associated with these links (in alphabetical order would be preferred).

(5) (c) What is wrong with the resulting set of "on" links? List all that apply.

A) The resulting set of links has a loop.

B) The resulting set of links is disconnected.

C) The resulting set of links does not span all nodes.

1. **Acronyms**
   (a) ________________
   (b) ________________
   (c) ________________
   (d) ________________
   (e) ________________
   (f) ________________
   (g) ________________
   (h) ________________
   (i) ________________
   (j) ________________
   (k) ________________
   (l) ________________
   (m) ________________
   (n) ________________
   (o) ________________
   (p) ________________
   (q) ________________
   (r) ________________
   (s) ________________
   (t) ________________
   (u) ________________
   (v) ________________
   (w) ________________
   (x) ________________
   (y) ________________
   (z) ________________

2. **Short Questions**
   (a) Principles
      i. ________________
      ii. ________________
      iii. ________________
   (b) IPv4 vs IPv6
      i. ________________
      ii. ________________
      iii. ________________
   (c) Fragmentation
      i. ________________
      ii. ________________
      iii. ________________
   (d) LPM
      i. ________________
      ii. ________________
      iii. ________________
   (e) Subnets
      i. ________________
      ii. ________________
      iii. ________________
   (f) NAT
      ____
   (g) Filling the pipe
      ____
   (h) L2 Broadcast
      ____
   (i) DNS
      ____
   (j) Header Fields
      i. ________________
      ii. ________________
      iii. ________________
   (k) True or False
      i. ________________
      ii. ________________
      iii. ________________
      iv. ________________
      v. ________________
      vi. ________________
      vii. ________________
      viii. ________________
      ix. ________________
      x. ________________

3. **TCP Timing**
   (a) ________________
   (b) ________________
   (c) ________________

4. **TCP ACKs**
   (a) ________________
   (b) ________________
   (c) ________________
   (d) ________________

5. **Fun at L2 and L3**
   (a) ________________
   (b) ________________
   (c) ________________
   (d) ________________
   (e) ________________
   (f) ________________
   (g) ________________

6. **HTTP**
   (a) ________________
   (b) ________________
   (c) ________________

7. **Routing**
   (a) ________________
   (b) ________________
   (c) ________________
   (d) ________________
   (e) ________________

8. **Spanning Tree**
   (a) ________________
   (b) ________________
   (c) ________________