Tutorial 5 Solutions

Instructions

1. Form ad-hoc groups of 2 to 3 students to solve this week's exercise.
2. Each group must answer the following review Q's
3. Each group will use shared google docs to work with all group members and tutor. The document must include the group member's names and the tutorial sheet number.

Review Questions

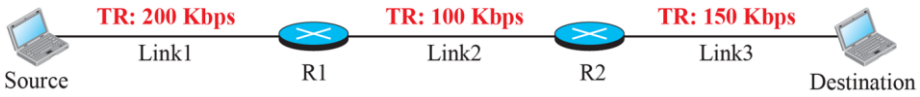
1. Q4-1. Why does the network-layer protocol need to provide packetizing service to the transport layer? Why can't the transport layer send out the segments without encapsulating them in datagrams?

   Answer: The transport layer communication is between two ports; the network layer communication is between two hosts. This means that each layer has a different source/destination address pair; each layer needs a different header to accommodate these pair of addresses. In addition, there are other pieces of information that need to be separately added to the corresponding header.

2. Q4-3. Distinguish between the process of routing a packet from the source to the destination and the process of forwarding a packet at each router.

   Answer: Forwarding is delivery to the next node. A router uses its forwarding table to send a packet out of one of its interfaces and to make it to reach to the next node. In other words, forwarding is the decision a router makes to send a packet out of one of its interfaces. Routing, on the other hand, is an end-to-end delivery resulting in a path from the source to the destination for each packet. This means a routing process is a series of forwarding processes. To enable each router to perform its forwarding duty, routing protocols need to be running all of the time to provide updated information for forwarding tables. Although forwarding is something, we can see in the foreground, in the background, routing provides help to the routers to do forwarding.

3. Q4-9. In Figure 4.10, assume that the link between R1and R2 is upgraded to 170 Kbps and the link between the source host and Rl is now downgraded to 140 Kbps. What is the throughput between the source and destination after these changes? Which link is the bottleneck now?



a. A path through three links

   Answer: The throughput is the smallest transmission rate, or 140 Kbps. The bottleneck is now the link between the source host and R1.

4. Q4-11. A host is sending 100 datagrams to another host. If the identification number of the first datagram is 1024, what is the identification number of the last?

   Answer: The identification numbers need to be contiguous. The identification number of the last datagram should be 1024 + 100 - 1 = 1123.

5. Q4-13. In classless addressing, we know the first and the last address in the block. Can we find the prefix length? If the answer is yes, show the process.

   Answer: If the first and the last addresses are known, the block is fully defined. We can first find the number of addresses in the block (N) and then find the prefix length (n).

   N = (last address) - (first address) + 1
   $n = 32 - \log_2 N$
   Block: (first address)/n

6. Q4-15. In classless addressing, can two different blocks have the same prefix length? Explain.

   Answer: Many blocks can have the same prefix length. The prefix length only determines the number of addresses in the block, not the block itself. Two blocks can have the same prefix length but start in two different points in the address space. For example, the following two blocks have the same prefix length, but they are definitely two different blocks. The length of the blocks is the same, but the blocks are different.

   127.15.12.32/27 **174.18.19.64/27**

7. Q4-21. Compare and contrast the protocol field at the network layer with the port numbers at the transport layer. What is their common purpose? Why do we need two port-number fields but only one protocol field? Why is the size of the protocol field only half the size of each port number?

   Answer: The protocol field and the port numbers both have the same functionality: multiplexing and demultiplexing. Port numbers are used to do these tasks at the transport layer; the protocol field is used to do the same at the network layer. We need only one protocol field at the network layer because payload taken from a protocol at the source should be delivered to the same protocol at the destination. The client and server processes, on the other hand, normally have different port numbers (ephemeral and well-known), which means we need two port numbers to define the processes. The size of the protocol field defines the total number of different protocols that use the service of the network layer, which is a small number (eight bits is enough for this purpose). On the other hand, many new applications may by added every day that needs a larger size of the port number field (sixteen bits is assigned).

8. Q4-27. In a graph, if we know that the shortest path from node A to node G is (A→B→E→G), what is the shortest path from node G to node A?

   Answer: According to the principle mentioned in the text, the shortest path is the inverse of the original one. The shortest path is G → E → B →A.

9. Q4-33Assume that we have an isolated Autonomous System (AS) running RIP. We can say that we have at least two different kinds of datagram traffic in this AS. The first kind carries the messages exchanged between hosts; the second carries messages belonging to RIP. What is the difference between the two kinds of traffic when we think about source and destination IP addresses? Does this show that routers also need IP addresses?

Answer: The source and destination IP addresses in datagrams carrying payloads between the hosts are the IP addresses of the hosts; the IP addresses carrying routing update packets between routers are IP addresses of the routing inter- faces from which the packets are sent or received. This shows that a router needs as many IP addresses as it has interfaces.

10. Q4-35. At any moment, a RIP message may arrive at a router that runs RIP as the routing protocol. Does it mean that the RIP process should be running all the time?

    Answer: Although RIP is running as a process using the service of the UDP, the process is called a daemon because it is running all the time in the background. Each router acts both as a client and a server; it acts as a client when there is a message to send; it acts as a server when a message arrives.

11. Q4-37. We say that OSPF is a hierarchical intra-domain protocol, but RIP is not. What is the reason behind this statement?

    Answer: OSPF divides an AS into areas, in which routing in each area is independent from the others; the areas only exchange a summary of routing information between them. RIP, on the other hand, considers the whole AS as one single entity.

12. Q4-39. Why do you think we need only one update RIP message, but several OSPF update messages?

    Answer:

    ***In RIP**, each router just needs to share its distance vector with its neighbor. Since each router has one type of distance vector, we need only one update message.*

    ***In OSPF**, each router needs to share the state of its links with every other router. Since a router can have several types of links (a router link, a network link, …), we need several update messages.*

13. Q4-41. OSPF messages and ICMP messages are directly encapsulated in an IP datagram. If we intercept an IP datagram, how can we tell whether the payload belongs to OSPF or ICMP?

    *Answer: The **type of payload** can be determined from the value of the protocol field. The protocol field value for ICMP is 01; for OSPF, it is 89.*

14. Q4-65. List three protocols in the 1Pv4 network layer that are combined into a single protocol in IPv6.

    Answer: The three protocols IGMP, ICMP, and ARP in IPv4 have been combined into a single protocol, ICMPv6 can also be delivered out of order to the receiving process. The responsibility again is on the receiving process to reorder the packets.

15. P4-3. Which fields of the IPv4 main header may change from router to router?

    Answer: The following fields can be changed from one router to another:

    a) HLEN: If there is option change
    b) Total length: If fragmented or options change
    c) Flags: If fragmented
    d) Fragmentation Offset: If fragmented

e) Time-to-Live; Decremented at each router
f) Header Checksum: Need to change because of other changes

16. P4-5. Briefly describe how we can defeat the following security attacks:
a. packet sniffing b. packet modification c. IP spoofing

Answer: Let us discuss each case separately:

a. ***Packet sniffing*** *can be defeated if the datagram is encrypted at the source and decrypted at the destination using an unbreakable scheme.*
b. ***Packet modification*** *can be defeated using a strong message integrity scheme.*
c. ***IP spoofing*** *can be defeated using a strong entity authentication scheme.*

17. P4-9. Find the class of the following Classful IP addresses:
a. 130.34.54.12 b. 200.34.2.1 c. 245.34.2.8

Answer: The class can be defined by looking at the first byte (see figure 4.31):

a. Since the first byte is between 128 and 191, the class is B.
b. Since the first byte is between 192 and 223, the class is C.
c. Since the first byte is between 240 and 255, the class is E.

18. P4-13. In classless addressing, what is the value of prefix length (n) if the size of the block (N) is one of the following?
a. N= 1 b. N= 1024 c. N= 2^{32}

Answer: The prefix can be found as $n = 32 - \log_2 N$:

a. $n = 32 - \log_2 1 = 32$
b. $n = 32 - \log_2 1024 = 22$
c. $n = 32 - \log_2 2^{32} = 0$

19. Give some reasons for using fragmentation and reassembly at the network layer?

Answer:

- *The communications network may only accept blocks of data up to a certain size.*
- *Error control may be more efficient with a smaller PDU size. With smaller PDUs, fewer bits need to be retransmitted when a PDU suffers an error.*
- *More equitable access to shared transmission facilities, with shorter delay, can be provided.*
- *A smaller PDU size may mean that receiving entities can allocate smaller buffers.*
- *An entity may require that data transfer come to some sort of "closure" from time to time, for checkpoint and restart/recovery operations.*