IKT204 – All Review Question Solutions

# Solutions – chapter 1

## Exercise 1 (R11)

Suppose there is exactly one packet switch between a sending host and a receiving host. The transmission rates between the sending host and the switch and between the switch and the receiving host are ***R1*** and ***R2***, respectively. Assuming the switch uses store-andforward packet switching, what is the total end-to-end delay to send a packet of length L?

(Ignore queuing, propagation delay, and processing delay.

Answer suggestions:

At time ***t0*** the sending host begins to transmit. At time ***t1 = L/R1***, the sending host completes transmission, and the entire packet is received at the switch (no propagation delay). Because the switch has the entire packet at time ***t1***, it can begin to transmit the packet to the receiving host at time ***t1***. At time ***t2 = t1 + L/R2***, the switch completes transmission, and the entire packet is received at the receiving host (again, no propagation delay). Thus, the end-to-end delay is ***L/R1 + L/R2***.

## Exercise 2 (R23)

What are the five layers in the Internet protocol stack? What are the principal responsibilities of each of these layers?

Answer suggestions:

The five layers in the Internet protocol stack are – from top to bottom – the application layer, the transport layer, the network layer, the link layer, and the physical layer. The principal responsibilities are outlined in textbook Section 1.5.1.

Application layer:

* Different applications related to network and corresponding application-layer protocols reside in this layer.
* Some of the protocols that are present in this layer are HTTP (which provides for Web document request and transfer of such between a server on the website being visited and a client) and SMTP (which provides for the transfer of e-mail messages).
* We also find specific network functions, such as translating human-friendly names for Internet end systems like www.uia.no to a 32-bits and/or a 128-bits network address. This is done using a specific application layer protocol, namely the domain name system (DNS).
* The protocols of this layer are distributed over multiple end systems.
* The application in the system of one end will exchange the packets of information with the application present in the system at the other end
* We call a packet of information on the application layer a **message**.

Transport layer:

* The main responsibility of the transport layer is to transport application layer messages between the application endpoints.
* The Internet has two transport protocols, TCP and UDP, both of which can transport application layer messages. TCP provides a connection-oriented service for the applications. This service includes guaranteed delivery of application layer messages to the destination and flow control (i.e., matching the speed between sender and receiver). TCP also divides long messages into shorter segments and has a congestion-control mechanism, so that a source throttles its transmission rate when the network is congested. The UDP protocol provides a connectionless service to its applications. This is a service that does not provide reliability, no flow control, and no congestion control.
* We call a transport layer packet a **segment**.

Network layer:

* The main responsibility of the network layer is to move the data packets, known as datagrams, between two hosts in the network.
* From the transport layer, this layer receives a segment as well as a destination address. The service provided by this team is like the postal service. It moves the datagrams and delivers them based on the destination address.
* An important protocol found in this layer is the IP protocol, which is available in two versions, v4 and v6. All Internet components that have a network layer must run the IP protocol.
* The Internet network layer also contains routing protocols that determine the route or path datagrams take between sources and destinations.
* A packet on the network layer is called a **datagram**.

Link layer:

* The main responsibility of the link layer is to move packets from one node to the next node along the best possible route. A node can be a router, a host, or any other network device.
* The network layer relies on the services of this layer for delivery of datagrams.
* The protocols in this layer are dependent on the specific link that is employed for moving the data packet. Ethernet and WiFi are examples of protocols found on this layer.
* We call a packet on the link layer a **frame**.

Physical layer:

* The main responsibility of physical layer is to move the individual bits within the frame from one node (here node may be a router, a host or any other network device) to the next node through physical transmission media.
* The protocols in this layer are dependent on the specific link that is employed for moving the data packet.
* Different physical media require different protocols. The protocol to transfer the bits using twisted pair is different from the protocol used in wireless transfer. The bits are moved in different ways across the links based on the media used.

## Exercise 3 (R24)

What do encapsulation and de-encapsulation mean? Why are they needed in a layered protocol stack?

Answer suggestions:

Encapsulation means that as application message goes down the Internet protocol stack it is appended with a header at each layer. At the receiving side, each layer removes its header as the same message goes up the protocol stack for its final destination the application layer. Encapsulation and de- encapsulation are needed in a layered protocol stack, because through the Internet link layer switches and network layer routers do not implement the whole protocol stack. They primarily see their own layer header and headers of the layers below. The rest of the packet is just payload.

## Exercise 4 (R25)

Which layers in the Internet protocol stack does a router process? Which layers does a linklayer switch process? Which layers does a host process?

Answer suggestions:

Routers process network, link and physical layers (layers 1 through 3). (This is a little bit of a white lie, as modern routers sometimes act as firewalls or caching components, and process Transport layer as well.) Link layer switches process link and physical layers (layers 1 through 2). Hosts (end systems) process all five layers.

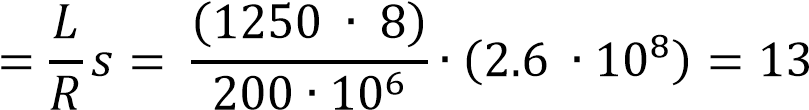
## Exercise 5 (P6)

Propagation delay and transmission delay are two central concepts in data networking. Consider two hosts, A and B, connected by a single link of rate ***R*** bps. Suppose that the two hosts are separated by ***m*** meters, and suppose the propagation speed along the link is s meters/sec. Host A is to send a packet of size ***L*** bits to Host B.

1. Express the propagation delay, ***d*prop**, in terms of ***m***and ***s***.
2. Determine the transmission time of the packet, ***d*trans**, in terms of ***L***and ***R***.
3. Ignoring processing and queuing delays, obtain an expression for the end-to-end delay.
4. Suppose Host A begins to transmit the packet at time ***t* = 0**. At time ***t* = *d*trans**, where is the last bit of the packet?
5. Suppose ***d*prop** is greater than ***d*trans**. At time ***t* = *d*trans**, where is the first bit of the packet?
6. Suppose ***d*prop** is less than ***d*trans**. At time ***t* = *d*trans**, where is the first bit of the packet?
7. Suppose ***s***= 2.6 **.** 108 m/s, ***L***= 1250 bytes, and ***R***= 200 Mbps. Find the distance ***m***so that ***d*prop** equals ***d*trans**.

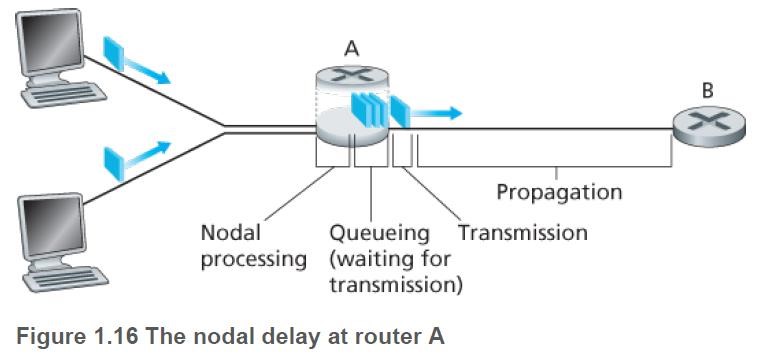
Answer suggestions:

* 1. ***d*prop** = ***m***/***s*** seconds.
  2. ***d*trans** = ***L***/***R*** seconds.
  3. ***d*end-to-end** = (***m***/***s*** + ***L***/***R***) seconds.
  4. The bit is just leaving Host A.
  5. The first bit is in the link and has not reached Host B.
  6. The first bit has reached Host B.
  7. Want ***d*prop** = ***d*trans**

𝑚  km

## Exercise 6 (P10)

Consider the network illustrated in Figure 1.16. Assume the two hosts on the left of the figure start transmitting packets of 1500 bytes at the same time towards Router B. Suppose the link rates between the hosts and the Router A is 10 Mbps. One link has 2.0 milliseconds propagation delay and the other has 2.1 milliseconds propagation delay. Link rate between Router A and Router B is 50 Mbps. Assume negligible processing delay at Router A (***dprocRouterA* ≈ 0**) and its outbound queue towards Router B is currently empty. Will queuing delay occur in Router A? Support your answer with calculations.



Answer suggestions:

Router is store and forward. Packet from host 1 with 2.0 ms propagation delay will be in Router A at:

***d*totalHost1** = ***d*trans** + ***d*propHost1** = (1500 **.** 8) / 10 **.** 106 + 2.0 **.** 10-3 = 3.2 ms and forwarded: ***d*transRouterA** = (1500 **.** 8) / 50 **.** 106 = 0.24 ms later.

Packet from host 2 with 2.1 ms propagation delay will be in Router A at: ***d*totalHost2** = ***d*trans** + ***d*propHost2** = (1500 **.** 8) / 10 **.** 106 + 2.1 **.** 10-3 = 3.3 ms

Since ***d*totalHost1** + ***d*transRouterA** = 3.44 ms is larger than ***d*totalHost2** , the packet from host 2 would be added to queue and ready for forwarding 0.14 ms later.

## Exercise 7 (P24)

Consider a user who needs to upload 125 MB of data to a server. The user has a 100 Mbps Wi-Fi connection. How long is the upload time?

Answer suggestions: ***d*trans,wifi**= L/R = (125 **.** 106 **.** 8) / 100 **.** 106 = 10 seconds.

# Solutions – Chapter 2

## Exercise 1 (R3)

For a communication session between a pair of processes, which process is the client and which is the server?

Answer suggestions:

The process which initiates the communication is the client; the process that waits to be contacted is the server.

## Exercise 2 (R5)

What information is used by a process running on one host to identify a process running on another host?

Answer suggestions:

The IP address of the destination host and the port number of (the socket in) the destination process.

## Exercise 3 (R12)

How can websites keep track of users? Do they always need to use cookies?

Answer suggestions:

When the user first visits the site, the server creates a unique identification number, creates an entry in its back-end database, and returns this identification number as a cookie number. This cookie number is stored on the user’s host and is managed by the browser. During each subsequent visit (and purchase), the browser sends the cookie number back to the site. Thus, the site knows when this user (more precisely, this browser) is visiting the site.

## Exercise 4 (R16)

Suppose Alice, with a Web-based e-mail account (such as Hotmail or Gmail), sends a message to Bob, who accesses his mail from his mail server (using POP or IMAP).

Discuss how the message gets from Alice’s host to Bob’s host. Be sure to list the series of application-layer protocols that are used to move the message between the two hosts.

Answer suggestions:

The message is first sent from Alice’s host to her mail server over TCP. Alice’s mail server then sends the message to Bob’s mail server over TCP. Bob then transfers the message from his mail server to his host over POP or IMAP.

Alice → HTTP → Alice’s mail server → SMTP → Bob’s mail server → POP or IMAP → Bob

## Exercise 5 (R18)

What is the HOL blocking (“først-i-køen”-blokkering) issue in HTTP/1.1? How does HTTP/2 attempt to solve it?

Answer suggestions:

Head of Line (HOL) blocking is often referring to the fact that each client has a limited number of TCP connections to a server (usually 6 connections per hostname) and doing a new request over one of those connections has to wait for the previous request on the same connection to complete before the client can make a new request.

HTTP/1.1 introduced a feature called "pipelining" which allowed a client sending several HTTP requests over the same TCP connection. However, HTTP/1.1 still required the responses to arrive in order and small objects may have to wait behind larger object(s) so it didn't really solve the HOL.

HTTP/2 solves the HOL issue by means of multiplexing requests over the same TCP connection, so a client can make multiple requests to a server without having to wait for the previous ones to complete as the responses can arrive in any order.

HTTP/2 does however still suffer from another type of HOL, as it runs over a TCP connection; and due to TCP's congestion control, one lost packet in the TCP stream makes all streams wait until that package is re-transmitted and received.

The obvious solution would be to run HTTP/2 over UDP (plus an optimized way of managing congestion), and that's precisely what the QUIC protocol does.

## Exercise 6 (P4)

Consider the following string of ASCII characters that were sent when the browser sent an HTTP GET message (i.e., this is the actual content of an HTTP GET message). Answer the following questions, indicating where in the HTTP GET message below you find the answer.

GET /cs453/index.html HTTP/1.1

Host: gaia.cs.umass.edu

User-Agent: Mozilla/5.0 (Windows;U; Windows NT 5.1; en-US; rv:1.7.2)

Gecko/20040804 Netscape/7.2 (ax)

Accept:ext/xml, application/xml, application/xhtml+xml, text/html;q=0.9, text/plain;q=0.8,image/png,\*/\*;q=0.5

Accept-Language: en-us,en;q=0.5

Accept-Encoding: zip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7

Keep-Alive: 300

Connection:keep-alive

*<cr><lf> (empty line)*

1. What is the URL of the document requested by the browser?
2. What version of HTTP is the browser running?
3. Does the browser request a non-persistent or a persistent connection?
4. What is the IP address of the host on which the browser is running?
5. What type of browser initiates this message? Why is the browser type needed in an HTTP request message?

Answer suggestions:

1. The document request was http://gaia.cs.umass.edu/cs453/index.html. The Host : field indicates the server's name and /cs453/index.html indicates the file name.
2. The browser is running HTTP version 1.1.
3. The browser is requesting a persistent connection, as indicated by the Connection: keep-alive.
4. This is a trick question. This information is not contained in an HTTP message anywhere. So there is no way to tell this from looking at the exchange of HTTP messages alone. One would need information from the IP datagrams (that carried the TCP segment that carried the HTTP GET request) to answer this question.
5. Mozilla/5.0. The browser type information is needed by the server to send different versions of the same object to different types of browsers.

## Exercise 7 (P18)

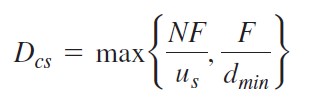
1. What is a *whois* database?
2. Use a *whois* databases on the Internet to obtain the names of two DNS servers (for eksempel navneserverne til uia.no). Indicate which *whois* databases you used.
3. Use *nslookup* on your local host to send DNS queries to three DNS servers: your local DNS server and the two DNS servers you found in part (b). Try querying for Type A, NS, and MX reports. Summarize your findings.
4. Use *nslookup* to find a Web server that has multiple IP addresses. Does the Web server of your institution (school or company) have multiple IP addresses?

## Exercise 8 (P22)

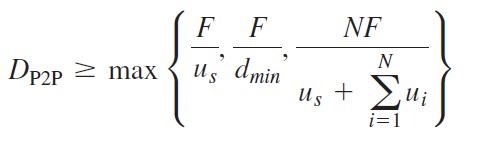
Consider distributing a file of ***F*** = 500 MB to N peers. The server has an upload rate of ***us*** = 1000 Mbps, and each peer has a download rate of ***di*** = 80 Mbps (i.e., ***dmin***= ***di***) and an upload rate of ***ui***. For ***N*** = 15, 300, and 6 000 and ***ui*** = 2 Mbps, 10 Mbps, and 50 Mbps, prepare a table giving the minimum distribution time for each of the combinations of ***N*** and ***ui*** for both client-server distribution and P2P distribution.

Answer suggestions:

For calculating the minimum distribution time for client server distribution, we use this formula from the textbook:



Similarly, for calculating the minimum distribution time for P2P distribution, we use this formula from the textbook:



Where ***dmin***= ***di***= 80 Mbps. Client/server case:

|  |  |  |  |
| --- | --- | --- | --- |
| N | 15 | 300 | 6 000 |
| ***ui*** does not matter | 60 seconds | 1 200 seconds | 24 000 seconds |

P2P case (numbers rounded):

|  |  |  |  |
| --- | --- | --- | --- |
| N | 15 | 300 | 6 000 |
| ***ui =*** 2 Mbps | 58 seconds | 750 seconds | 1 846 seconds |
| ***ui =*** 10 Mbps | 52 seconds | 300 seconds | 393 seconds |
| ***ui =*** 50 Mbps | 50 seconds | 75 seconds | ≈80 seconds |

# Solutions – Chapter 3.1 – 3.3 (UDP)

## Exercise 1 (R3)

How is a UDP socket identified?

Answer suggestions:

UDP: Destination IP and destination port (dest\_IP, dest\_port).

## Exercise 2 (R4)

Describe why an application developer might choose to run an application over UDP rather than TCP.

Answer suggestions:

Simple answer: Speed. An application developer may not want its application to use TCP’s congestion control, which can throttle the application’s sending rate at times of congestion. Often, designers of IP telephony and IP videoconference applications choose to run their applications over UDP because they want to avoid TCP’s congestion control. Also, some applications do not need the reliable data transfer provided by TCP.

## Exercise 3 (R6)

Is it possible for an application to enjoy reliable data transfer even when the application runs over UDP? If so, how?

Answer suggestions:

Yes. The application developer can put reliable data transfer into the application layer protocol. This would require a significant amount of work and debugging, however.

## Exercise 4 A (R7)

Suppose that Host A and Host B send a UDP segment to Host C with destination port number 6789. Will both of these segments be directed to the same socket at Host C?

If so, how will the process at Host C know that these two segments originated from two different hosts?

Answer suggestions:

Yes, both segments will be directed to the same socket. For each received segment, at the socket interface, the operating system will provide the process with the IP addresses to determine the origins of the individual segments.

## Exercise 4 B

Suppose a host having two network application processes, Process A and Process B. Both processes send a UDP segment to a server process with destination port number 6789. How will the server process know that these two segments originated from two different processes?

Answer suggestions:

For each received segment, the operating system will provide the server process with the source port numbers of the received segment. If these differ, this means that the segments originated from different processes. If the source IP addresses of the received segments match, this means that that the processes run on the same host.

## Exercise 5 (P1)

Suppose Client A requests a web page from Server S through HTTP (which uses TCP) and its socket is associated with port 33000.

1. What are the source and destination ports for the segments sent from A to S?
2. What are the source and destination ports for the segments sent from S to A?
3. Can Client A contact Server S using UDP as the transport protocol?

Answer suggestions:

1. The TCP segment sent from the client to the server will have a source port number that is randomly selected from the dynamic port number range. The target port number is 33000.
2. The TCP packets sent from the server to the client will have source port number equal to 33000. The target port number will be equal to the source port number of the received segment (that was randomly selected).
3. The client can contact the server using UDP *only if* the server has a UDP socket assigned to the same port number. However, since HTTP runs on TCP, it is not possible to combine UDP with HTTP.

# Solutions – Chapter 3.4 – 3.8 (TCP)

## Exercise 1

How many sockets does a UDP server need to serve N clients?

Answer suggestions:

One. This is because a UDP socket is identified by only by destination IP and destination port number fields in the UDP header.

## Exercise 2 (R3)

How is a UDP socket fully identified? What about a TCP socket? What is the difference between the full identification of both sockets?

Answer suggestions:

UDP: Destination IP and destination port (dest\_IP, dest\_port).

A TCP socket is identified by the 4-tuple source IP, source port number, destination IP, destination port number fields in the TCP header.

TCP establishes a full duplex bidirectional session between sender and receiver. UDP has no formal procedure for establishing a session between a sender and a receiver.

## Exercise 3 (R26)

If a TCP server were to support N simultaneous connections, each from a different client, how many sockets would the TCP server need?

Answer suggestions:

N sockets (see Exercice 2) + 1. The extra socket is a listening socket.

## Exercise 4 (R10)

What is the purpose of timers in TCP?

Answer suggestions:

To handle losses in the channel. If the ACK for a transmitted packet is not received within the duration of the timer for the packet, the packet (or its ACK) is assumed to have been lost. Hence, the packet is retransmitted.

## Exercise 5 (R15)

Suppose Host A sends two TCP segments back-to-back to Host B over a TCP connection. The first segment has sequence number 90; the second has sequence number 110.

1. How much data is in the first segment?
2. Suppose that the first segment is lost but the second segment arrives at B. In the acknowledgment that Host B sends to Host A, what will be the acknowledgment number?

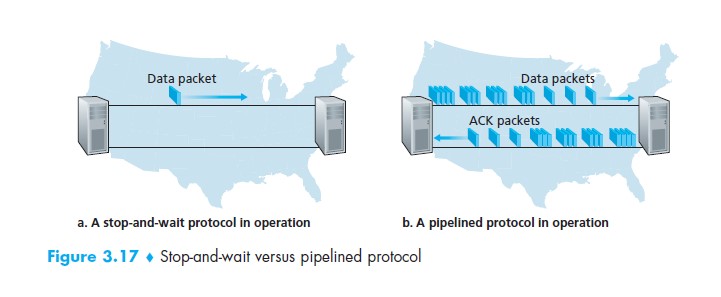
Answer suggestions:

1. 20 bytes.
2. 90

## Exercise 6 (P15)

Consider the cross-country example shown in Figure 3.17. Suppose that the round-trip time RTT is 33 milliseconds, the channel transmission rate ***R*** is 1.2 Gbps, and the size of a packet is 1500 bytes, including both header fields and data. ACK packets are small, and their transmission delay can be ignored.

1. How big is channel utilization (in percent) when a **stop-and-wait protocol** is used?
2. How many unacknowledged segments in transit are permissible to achieve a channel-utilization greater than 98 percent when a **pipelined protocol** is used?
3. What is this in terms of window size, i.e., the range of permissible sequence numbers for transmitted but not yet acknowledged packets?



Answer suggestions:

1. Transmitting one packet takes: 𝑑trans = 𝐿 = 1500 89 = 0.01 𝑚𝑠

𝑅 1.2 10

If we assume small ACK packets and ignoring their transmission time, receiver can send ACK after RTT/2 + dtrans. The ACK will be at sender side RTT/2 later. With a **stopand-wait** protocol, the sender can therefor send next packet at:

𝑡 = 𝑅𝑇𝑇 + 𝑑trans = 33 + 0.01 = 33.01 𝑚𝑠

From textbook the formula for channel utilization using **stop-and-wait** protocol is:

𝐿

𝑈 = 𝑅 𝐿 = 𝑅𝑇𝑇𝑑+trans𝑑trans = 330.01.01  0.0003  0.03% 𝑅𝑇𝑇 + 𝑅

1. Now switch to pipelined protocol and wish channel utilization >=98%:

𝐿

𝑈 = 0.98 = 𝑅  𝑛 𝐿 = 𝑅𝑇𝑇𝑑+trans𝑑trans ⟹ 𝑛 = 0.98 𝑅𝑇𝑇𝑑+trans𝑑trans = 0.98 330.01.01  3235 𝑅𝑇𝑇 + 𝑅

1. The window size needs to be rather large: 3235 packets of 1500 bytes, in total approx. 4 852 500 bytes.

## Exercise 7 (P27)

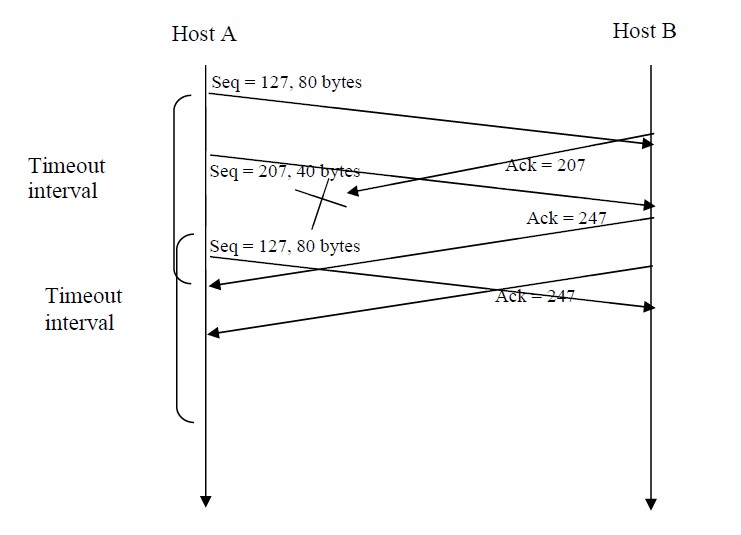
Host A and B are communicating over a TCP connection. Host B has already received from Host A all bytes up through byte 96. Suppose Host A then sends two segments to Host B. The first and the second segments contain 40 and 80 bytes of data, respectively. In the first segment, the sequence number is 97, the source port number is 302, and the destination port number is 80. Host B sends an acknowledgment whenever it receives a segment from Host A.

1. In the second segment sent from Host A to B, what are the sequence number, source port number, and destination port number?
2. If the first segment arrives before the second segment, in the acknowledgment of the first arriving segment, what is the acknowledgment number, the source port number, and the destination port number?
3. If the second segment arrives before the first segment, in the acknowledgment of the first arriving segment, what is the acknowledgment number?
4. Suppose the two segments sent by A arrive in order at B. The first acknowledgment arrives after the first timeout interval. What is the sequence number of the next segment that A will transmit?

Answer suggestions:

a. In the second segment from Host A to B, the sequence number is 207, source port number is 302 and destination port number is 80.

1. If the first segment arrives before the second, in the acknowledgement of the first arriving segment, the acknowledgement number is 207, the source port number is 80 and the destination port number is 302.
2. If the second segment arrives before the first segment, in the acknowledgement of the first arriving segment, the acknowledgement number is 127, indicating that it is still waiting for bytes 127 and onwards. d)



# Solutions – chapter 4

## Exercise 1 (R3)

We made a distinction between the forwarding function and the routing function performed in the network layer. What are the key differences between routing and forwarding?

Answer suggestions:

Forwarding is a router local action of transferring packets from its input link interfaces to its appropriate output link interfaces based on the packet’s destination address. Forwarding is typically implemented in hardware and takes typically a few nanoseconds.

Routing refers to the network-wide process that determines the end-to-end paths that packets take from sources to destinations. Such paths are realized by means of a routing table that is found in each router. This means that routing is the process of computing and updating routing tables.

## Exercise 2 (R17)

Suppose Host A sends Host B a TCP segment encapsulated in an IP datagram. When Host B receives the datagram, how does the network layer in Host B know it should pass the segment (that is, the payload of the datagram) to TCP rather than to UDP or to some other upper-layer protocol?

Answer suggestions:

The 8-bit “protocol” field in the IPv4 datagram specifies the protocol of the encapsulated payload data. Value 6 means TCP and 17 is UDP.

## Exercise 3 (R18)

What field in the IP header can be used to ensure that a packet is forwarded through no more than N routers?

Answer suggestions:

Time-to-live (TTL). When an IP packet passes through a router, the router will decrement the value in TTL by one. If TTL=0, a router will drop the packet, and

## Exercise 4 (R21)

How many IP addresses does a router have?

Answer suggestions:

They have one address for each interface.

## Exercise 5 (R25)

Suppose an application generates 40 bytes of data that gets encapsulated in a TCP segment and then an IP datagram. (Assume that the IP “options” field is 0 bytes.)

1. What percentage of the datagram is overhead and what percentage is application data?
2. What is the overhead percentage if UDP is used instead of TCP?

Answer suggestions:

1. IP packet size = 20 bytes (IP header) + 20 bytes (TCP header) + 40 bytes (data) = 80 bytes. The overhead percentage is 50 %.
2. IP packet size = 20 bytes (IP header) + 8 bytes (UDP header) + 40 bytes (data) = 68 bytes. The overhead percentage is 59 %.

Although the relative overhead is greater in b) than a), the header overhead including IP is less with UDP (28 bytes) than TCP (40 bytes), which therefore gives a better utilization of bandwidth.

## Exercise 6 (P17)

Suppose IP datagrams are limited to 1,500 bytes (including header) between source Host A and destination Host B. The IP header is 20-byte and TCP is used.

How many datagrams would be required to send an MP3 consisting of 5 million bytes?

Answer suggestions:

The MP3 file size is 5million bytes. The data is carried in TCP segments, with each TCP segment also having 20 bytes header. Then each datagram can carry

1500 – 40 = 1460 bytes of the MP3 file. Number of datagrams required: 5**.** 106 / 1460 = 3425.

All but the last datagram will be 1,500 bytes; the last datagram will be 960+40 = 1000 bytes.

## Exercise 7 (R31)

How makes “tunneling” it possible to send IPv6 packets over IPv4 routers?

Answer suggestions:

IPv6 datagram (including header fields) is encapsulated in an IPv4 datagram. IPv4 header will indicate this by having its “protocol” field set to 41, which is the assigned payload type number for IPv6.

## Exercise 8 (P8, P13)

Consider an IP network using 32-bit host addresses. Suppose a router has four links, numbered 0 through 3, and packets are to be forwarded to the link interfaces as follows:

|  |  |
| --- | --- |
| **Destination Address Range** | **Link Interface** |
| 11010000 00000000 00000000 00000000 through  11010000 00111111 11111111 11111111 | 0 |
| 11010000 01000000 00000000 00000000 through  11010000 01000001 11111111 11111111 | 1 |
| 1. 01000010 00000000 00000000 through 2. 11011111 11111111 11111111 | 2 |
| otherwise | 3 |

1. Provide a routing table that has five entries and uses longest prefix matching, and forwards packets to the correct link interfaces. (Hint. The third entry needs to be split to cover the given address range.)
2. Rewrite this routing table using CIDR a.b.c.d/x notation instead of the binary string notation. (P13)
3. Describe how your routing table determines the appropriate link interface for datagrams with the following IP addresses:

Address 1: 11010001 11110111 01110011 00111001

Address 2: 11010000 00001100 10101101 11100100

Address 3: 11010000 01000000 11000011 01110010

Address 4: 11010001 10001111 01100111 00011111

Answer suggestions:

a) We start by identifying the common msb. of the starting and ending addresses in each entry. We can therefore conclude that prefix 11010000 00**/10** shall go to interface 0, and 11010000 0100000**/15** shall go to interface 1.

The address range to interface 2 is a bit trickier, we need two entries in routing table. First a short prefix 1101000**/7** to interface 2. However, since this covers too many addresses, then we add a longer prefix 11010001 111**/11** that captures those “exceeding” addresses, which should go out on interface 3. Because of the **longest prefix-matching rule**, the longer prefix will correctly capture the “exceeding” addresses of the shorter prefix.

The routing table will then look like this:

|  |  |  |
| --- | --- | --- |
| Entry | Prefix | Link interface |
| 1 | 11010000 00 | 0 |
| 2 | 11010000 0100000 | 1 |
| 3 | 1101000 | 2 |
| 4 | 11010001 111 | 3 |
| 5 | otherwise | 3 |

b)

|  |  |  |
| --- | --- | --- |
| Entry | Prefix | Link interface |
| 1 | 11010000 00 → 208.0.0.0/10 | 0 |
| 2 | 11010000 0100000 → 208.64.0.0/15 | 1 |
| 3 | 1101000 → 208.0.0.0/7 | 2 |
| 4 | 11010001 111 → 208.224.0.0/11 | 3 |
| 5 | otherwise | 3 |

c) The first address matches entry 4: link interface 3. The second address matches entry 1:

link interface 0. The third address matches entry 2: link interface 1. The fourth address matches entry 3: link interface 2.

## Exercise 9 (P14 variant)

Consider a subnet with prefix 128.119.40.128/26.

1. How many IP addresses does this prefix represent?
2. What are the starting and ending IP addresses that this prefix represents?

Answer suggestions:

1. Since there are 26 most significant bits in the subnet part, there is 6 bits left for host addresses. There are 2^6 = 64 addresses. (0’s and all 1’ in in the host part is reserved, which gives addresses to 64 interfaces.)
2. 128.119.40.128 to 128.119.40.191, where 128 = 1000 0000 and 191 = 1011 1111. The red bits are the range in the host part.

## Exercise 10 (P14 variant)

Suppose an ISP owns the block of addresses of the form 128.119.40.64/26. Suppose it wants to create four subnets from this block, with each block having the same number of IP addresses. What are the prefixes (on the form a.b.c.d/x) for the four subnets?

Answer suggestions:

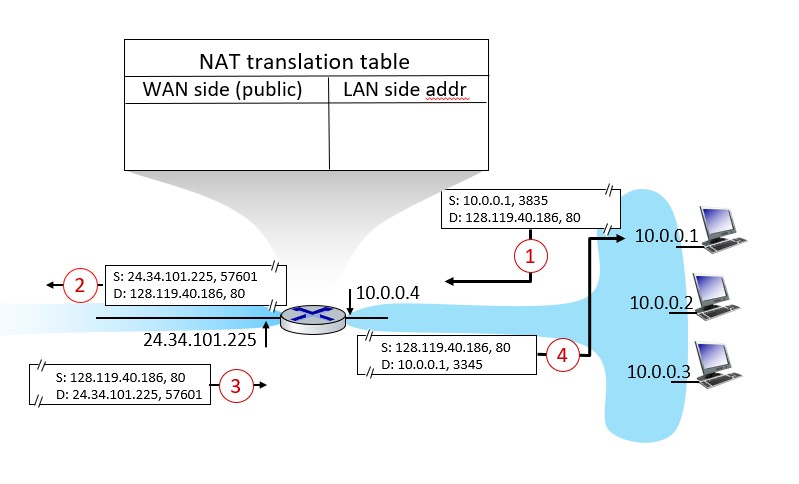
The subnet address 171.136.56.192/26 corresponds to the binary prefix:

|  |  |
| --- | --- |
| 10101011 10001000 00111000 11000000    The four subnet prefixes are: | → 171.136.56.192/26 |
| 10101011 10001000 00111000 11000000 | → 171.136.56.192/28 |
| 10101011 10001000 00111000 11010000 | → 171.136.56.208/28 |
| 10101011 10001000 00111000 11100000 | → 171.136.56.224/28 |
| 10101011 10001000 00111000 11110000 | → 171.136.56.240/28 |

## Exercise 11 (P18 variant)

Consider the network with NAT in the figure below

1. Provide the corresponding entry in the NAT translation table.
2. Suppose that the ISP instead assigns the router the address 143.43.131.225 and that the subnet address of the home network is 192.168.0/24. Assign addresses to all interfaces in the home network.



Answer suggestions:

1. NAT translation table:

|  |  |
| --- | --- |
| WAN side (public) | LAN side (private) |
| NAT IP, port number | Source IP, port number |
| 24.34.112.235, 57601 | 10.0.0.1, 3835 |

1. Home addresses are the private IP addresses on the inside of the NAT, which are 192.168.0.1, 192.168.0.2, 192.168.0.3, and the router interface has 192.168.0.4.

# Solutions – chapter 5

## Exercise 1 (R3)

Compare and contrast the properties of a centralized and a distributed routing algorithm.

Give an example of a routing protocol that takes a centralized and a distributed approach.

Answer suggestions:

A centralized routing algorithm computes the least-cost path between a source and destination by using complete, global knowledge about the network. The algorithm needs to have complete knowledge of the connectivity between all nodes and all links’ costs. The actual calculation can be run at one site or could be replicated in the routing component of each and every router.

A distributed routing algorithm calculates the lease-cost path in an iterative, distributed manner by the routers. With a distributed algorithm, no node has the complete information about the costs of all network links. Each node begins with only the knowledge of the costs of its own directly attached links, and then through an iterative process of calculation and information exchange with its neighboring nodes, a node gradually calculates the leastcost path to a destination or a set of destinations.

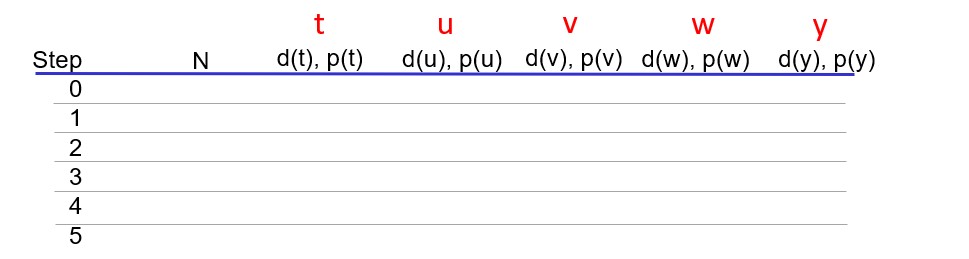
OSPF protocol is an example of centralized routing algorithm, and BGP is an example of a distributed routing algorithm.

Open Shortest Path First (OSPF) is an example that uses a centralized routing algorithm. OSPF is used exclusively within an autonomous system. BGP is an example of a distributed routing protocol.

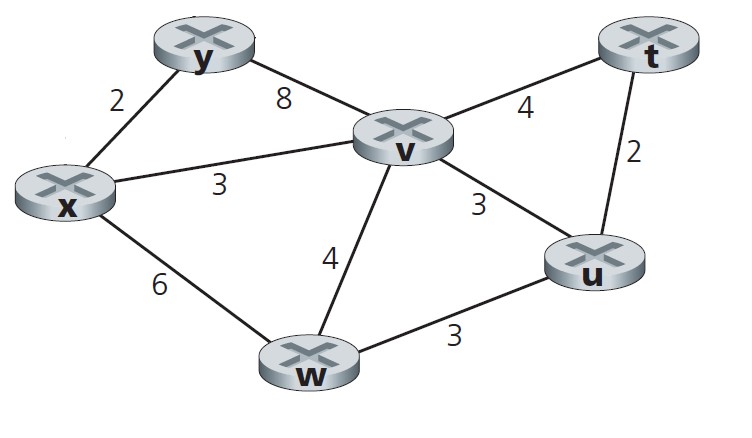
## Exercise 2 (P1, P2 variant)

Consider the following network.

1. Use Dijkstra’s shortest-path algorithm to compute the shortest path from **node** **x** to all network nodes. Show how the algorithm works by computing a table below.



1. Use Dijkstra’s shortest-path algorithm to compute the shortest path from **node** **t** to all network nodes.



Answer suggestions:

## Exercise 3 (R7)

Why are different inter-AS and intra-AS protocols used in the Internet?

Answer suggestions:

Flexibility: An autonomous system is controlled by an ISP. Since the internet consists of many thousand AS’s, each ISP may decide which intra-AS-protocol to use, and how to conduct routing within their AS.

Scale: Since routing must be conducted across the AS’s, a common inter-AS routing is necessary that will act as a “glue”. Routing between large numbers of networks is a critical issue in inter-AS routing.

## Exercise 4 (R8)

When an OSPF router sends its link state information, it is sent only to those routers that are directly attached neighbors or to all routers in the same autonomous system? Justify your answer.

Answer suggestions:

With OSPF, a router broadcasts its link-state information to all other routers in the autonomous system to which it belongs, not just to its neighboring routers. This is because with OSPF, each router needs to construct a complete topological map of the entire AS and then locally runs Dijkstra’s shortest-path algorithm to determine its least-cost paths to all other nodes in the same AS.

## Exercise 5 (R10)

Define and contrast the following terms: subnet, prefix, and “BGP route”.

Answer suggestions:

A **subnet** is a portion of a larger network. A subnet does not contain a router. Its boundaries are defined by the router interface and host interfaces.

A **prefix** is the network portion of a CDIR address; it is written in the form a.b.c.d/x ; A prefix covers one or more subnets.

When a router advertises a prefix across a BGP session, it includes with the prefix the BGP attributes AS-PATH and NEXT-HOP. A BGP route is the prefix and the BGP attributes.

## Exercise 6 (R11)

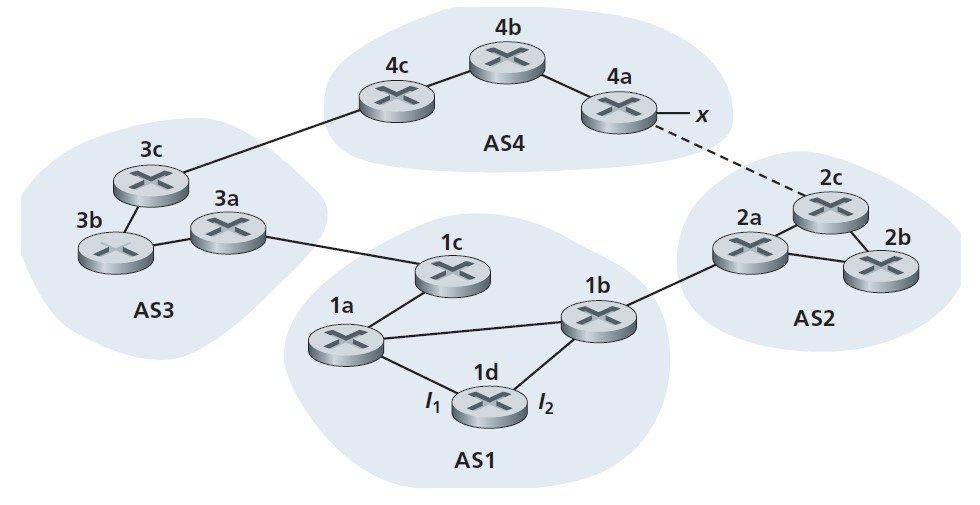
How does BGP use the NEXT-HOP attribute? How does it use the AS-PATH attribute?

Answer suggestions:

Routers use the AS-PATH attribute to detect and prevent looping advertisements; they also use it in choosing among multiple paths to the same prefix. The NEXT-HOP attribute indicates the IP address of the first router along an advertised path (outside of the AS receiving the advertisement) to a given prefix. When configuring its forwarding table, a router uses the NEXT-HOP attribute.

## Exercise 7 (P14)

Consider the network shown below. Suppose that AS1, AS2, AS3 and AS4 are running OSPF for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.



1. Router **3c** learns about prefix ***x*** from which routing protocol: OSPF, eBGP, or iBGP?
2. Router **3a** learns about ***x*** from which routing protocol?
3. Router **1c** learns about ***x*** from which routing protocol?
4. Router **1d** learns about ***x*** from which routing protocol?
5. Once router **1d** learns about prefix ***x***, it will put an entry *(****x,I****)* in its forwarding table, where ***I*** is either interface ***I1*** or ***I2***. Will ***I*** be equal to ***I1*** or ***I2***? Explain why in one sentence.
6. Now suppose that a link between AS2 and AS4 (shown by the dotted line) is established, and that router **1d** learns that prefix ***x*** is accessible via AS2 as well as via AS3. Will ***I*** be set to ***I1*** or ***I2***? Explain why in one sentence.

Answer suggestions:

1. eBGP
2. iBGP
3. eBGP
4. iBGP
5. ***I1*** since AS1 uses RIP and router **1d** has, through an iterative process and assuming identical link costs inside AS1, calculated that interface ***I1*** begins the shortest path towards gateway router **1c** (and NEXT-HOP router **3a**).
6. ***I2*** since both routes to prefix ***x*** has equal AS-PATH length, but interface ***I2*** begins the shortest path towards gateway router **1b** (and NEXT-HOP router **2a**).

# Solutions – chapter 6

## Exercise 1 (R2)

If all the links on the Internet were to provide reliable delivery service, would the TCP reliable delivery service be redundant? Why or why not?

Answer suggestions:

Assuming that reliable delivery means that the Internet delivers packets from sender to receiver without errors and in correct order, then the TCP is reliable delivery service redundant.

## Exercise 2 (R10)

Suppose nodes A, B, and C each attach to the same broadcast LAN (through their adapters).

1. If A sends thousands of IP datagrams to B with each encapsulating frame addressed to the MAC address of B, will C’s adapter process these frames? If so, will C’s adapter pass the IP datagrams in these frames to C’s network layer?
2. How would your answers change if A sends frames with the MAC broadcast address?

Answer suggestions:

1. Node C’s network interface will **process** the frames, but since its MAC address does not match the destination address in the frames, it will **not pass** the datagrams up the protocol stack.
2. If the MAC broadcast address (FF-FF-FF-FF-FF-FF) is used, then node C’s interface will **process** the frames **and pass** the datagrams up the protocol stack.

## Exercise 3

1. Why is an ARP query sent within a broadcast frame?
2. Why is an ARP response sent within a frame with a specific destination MAC address?

Answer suggestions:

1. The querying host does not know which interface address corresponds to the IP address in question and must find the MAC address among all hosts on the local network. It therefore broadcasts this query.
2. The host that has the requested MAC address knows the MAC address of the host that sent the ARP query by looking at the source address. It does therefore not have to broadcast the response.

## Exercise 4 (R15 variant)

Each host and router have an ARP table in its memory (an ARP cache).

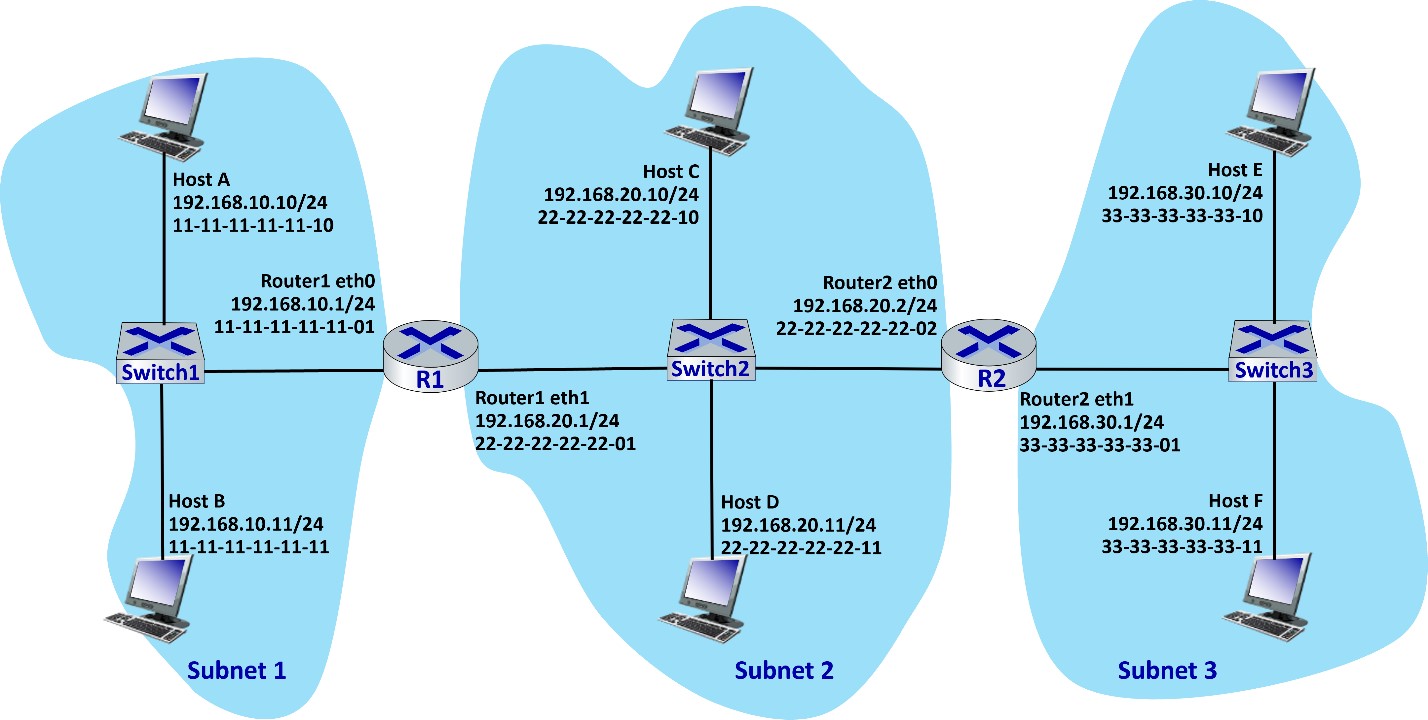
1. What is the content of this table?
2. What is the main reason for having such a table?

Answer suggestions:

1. The ARP table contains mappings of IP addresses and MAC addresses of hosts and routers in a local network.
2. The main reason for having such a table is to reduce the number of ARP requests in the local network. If a relevant ARP entry exists, the host does not need to send an ARP request to first find the MAC address of the destination.

## Exercise 5 (P14 variant)

Consider three LANs interconnected by two routers, as shown in figure below.



1. Host F is sending an IP datagram to Host A. Suppose all ARP tables are up to date. Describe and enumerate all the steps, as done for the single-router example in Section 6.4.1.
2. Assume that the ARP table in the sending host F is empty (and the other tables are up to date). Describe and enumerate all the steps.
3. Subnet 2 is interconnected other networks via two routers. Can the hosts in this subnet have two default gateway routers? Discuss how traffic out of this subnet is handled. (Hint: Can DHCP provide some options?)

Answer suggestions:

1. Sending an IP datagram from Host F to Host A:
   1. The network mask in host F determines that the datagram with destination IP address 192.168.10.10 should be routed to the subnet gateway router interface 192.168.30.1.
   2. Host F creates an Ethernet frame with destination MAC address 33-3333-33-33-01 (found by ARP table lookup).
   3. Router 2 receives the packet and extracts the datagram. The forwarding table in this router indicates that the datagram is to be routed to gateway interface 192.168.20.1.
   4. Router 2 then sends the Ethernet packet with destination MAC address 22-22-22-22-22-01 (found by ARP table lookup) and source MAC address 22-22-22-22-22-02 via its interface with IP address of 192.168.20.2.
   5. Router 1 receives the packet and extracts the datagram. The forwarding table in this router indicates that the datagram is to be delivered to a host in subnet 192.168.10.0/24.
   6. Router 1 then sends the Ethernet packet with destination MAC address 11-11-11-11-11-11 (found by ARP table lookup) and source MAC address 11-11-11-11-11-01 via its interface with IP address of 192.168.10.1.
   7. The packet has reached Host A.
2. ARP in host F must now determine the MAC address of 192.168.30.1:
   1. Host F sends out an ARP query packet within a broadcast Ethernet frame:

“Who has IP address 192.168.30.1?”

* 1. Router 2 receives the query packet and sends to Host F an ARP response packet.
  2. This ARP response packet is carried by an Ethernet frame with MAC source address 33-33-33-33-33-01 and destination address 33-33-33-3333-11.
  3. Then follow the steps in C).

1. A host can only have one default gateway router. If a datagram is to be sent to a destination outside Subnet 2, the datagram would be sent to gateway router which will then forward the packet e.g., to the other router interface in this subnet. However, DHCP has options (33 and 121) that allow hosts to be given static routes. In this case DHCP could e.g., specify default gateway router 192.168.20.2 (option 3) and 192.168.10.0/24 as static route to 192.168.20.1

(option 121). In such a case the hosts will perform an internal routing and send

traffic to Subnet 1 to router interface 192.168.20.1, while all other traffic out of this subnet is sent to default gateway router interface 192.168.20.2.

## Exercise 6 (P26)

Let us consider the operation of a learning switch in the context of a network in which 6 nodes labeled A through F are star connected into an Ethernet switch. Suppose that *(i)* B sends a frame to E, *(ii)* E replies with a frame to B, *(iii)* A sends a frame to B, *(iv)* B replies with a frame to A. The switch table is initially empty. Show the state of the switch table before and after each of these events. For each of these events, identify the link(s) on which the transmitted frame will be forwarded, and briefly justify your answers

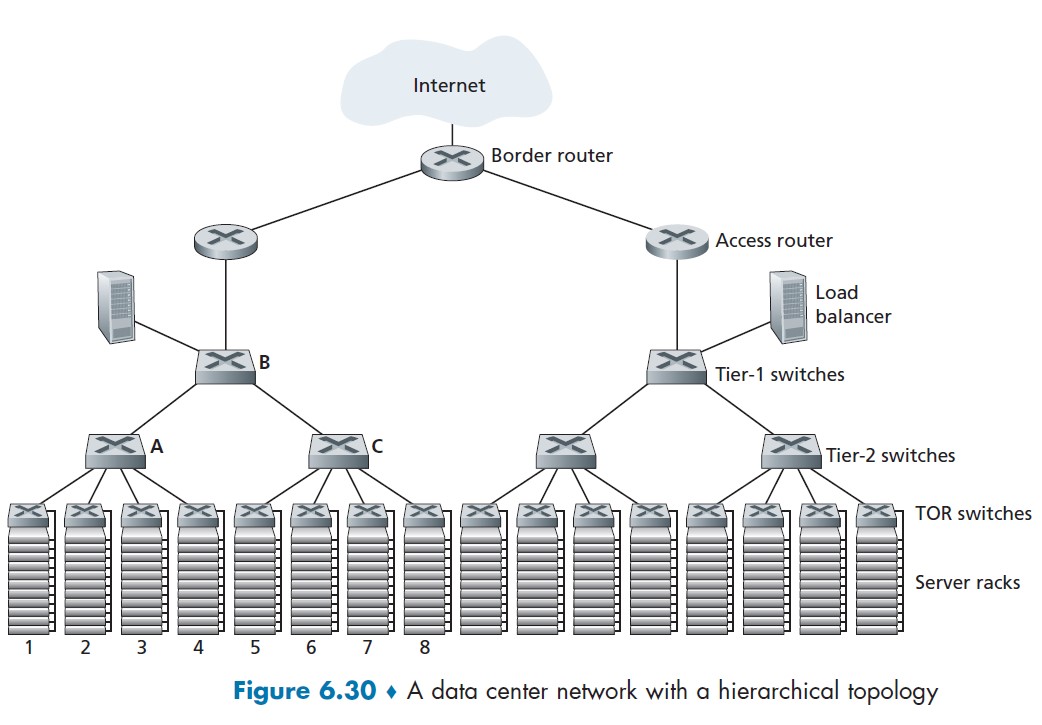
Answer suggestions:

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Switch table state | Link(s) packet is forwarded to | Explanation |
| *(i)* B sends a frame to E | Switch learns interface corresponding to MAC address of B | A, C, D, E, and F | Since switch table is empty, so switch does not know the interface corresponding to MAC address of E |
| *(ii)* E replies with a frame to B | Switch learns interface corresponding to MAC address of E | B | Since switch already knows interface corresponding to MAC address of B |
| *(iii)* A sends a frame to B | Switch learns interface corresponding to MAC address of A | B | Since switch already knows interface corresponding to MAC address of B |
| *(iv)* B replies with a frame to A. | Switch table state remains the same as  before | A | Since switch already knows the interface corresponding to MAC address of A |

## Exercise 7 (P33)

Consider the hierarchical network in Figure 6.30 below and suppose that the data center needs to support e-mail and video distribution among other applications. Suppose *four* racks of servers are reserved for e-mail and *four* racks are reserved for video. For each of the applications, all four racks must lie below a single tier-2 switch since the tier-2 to tier-1 links do not have sufficient bandwidth to support the intraapplication traffic. For the e-mail application, suppose that for 99.9 percent of the time only three racks are used, and that the video application has identical usage patterns.

1. For what fraction of time does the e-mail application need to use a fourth rack? How about for the video application?
2. Assuming e-mail usage and video usage are independent, for what fraction of time do both applications need their fourth rack?



Answer suggestions:

1. Both email and video application uses the fourth rack for 0.1 percent of the time.
2. Probability that both applications need fourth rack is 0.001\*0.001 = 10-6.

# Solutions – Chapter 7

## Exercise 1 (R1)

1. What does it mean for a wireless network to be operating in “infrastructure mode”?
2. If the network is **not** in infrastructure mode, what mode of operation is it in, and what is the difference between that mode of operation and infrastructure mode?

Answer suggestions:

1. In infrastructure mode of operation, each wireless host is connected to the larger network via an access point. In other words, there is no direct communication between the hosts.
2. If not operating in infrastructure mode, a network operates in ad-hoc mode. In ad-hoc mode, wireless hosts do not connect with an access point and infrastructure. The hosts communicate directly with each other, or nodes may forward (relay) messages on behalf of a sender towards a destination node.

## Exercise 2 (R3)

What are the differences between the following types of wireless channel impairments: path loss (norsk: signaltap), multipath propagation, and interference from other sources?

Answer suggestions:

*Path loss* is a reduction in signal strength as the signal travels from a transmitter to a receiver, because of distance and when it travels through matter.

*Multipath propagation* occurs when electromagnetic signals reflect off walls or objects, in which both the direct and reflected signals are received by sender. This results in a blurring of the received signal.

*Interference from other sources* is a disturbance that occurs when another source is transmitting on the same or neighboring channel or frequency as a specific sender.

## Exercise 3 (R4)

As a mobile node gets farther and farther away from a base station, path loss (norsk:

signaltap) occurs causing a reduced signal-to-noise ratio (SNR). What two actions could a base station take so that the loss probability of a transmitted frames does not increase?

Answer suggestions:

1. Ask the mobile node to increase the transmission power in order to improve the signalto-noise ratio (SNR).
2. Reduce the transmission rate by selecting a lower order modulation scheme (i.e., using less bits per symbol).

## Exercise 4 (R5)

Describe the role of the beacon frames in 802.11.

Answer suggestions:

Beacon frames announce the existence of a wireless network and are vital for the proper operation of a network. Access points (APs) transmit beacon frames periodically (usually every 100 millisecond). This let nearby wireless hosts to discover and identify an AP.

## Exercise 5 (R6)

802.11-type access points periodically send beacon frames. What is the content of the beacon frames?

Answer suggestions:

Beacon frames announce the existence of a wireless network and are vital for the proper operation of a network. Beacon frames contain the AP’s MAC address and other parameters (timestamp, beacon interval, capabilities information). It also contains the AP’s Service Set Identifier (SSID), which is the AP’s name used for identifying wireless networks.

## Exercise 6 (R9)

What are the two main purposes of a CTS frame?

Answer suggestions:

In wireless networks all sent messages are broadcast. A wireless host requests the AP for permission to send by sending a request-to-send (RTS) to the AP. The AP grants this station access to the channel by sending (broadcasting) a clear-to-send (CTS) frame. This gives the host explicit permission to send. Since the CTS is broadcast, it is also received by the other hosts within the Basic Service Set (BSS). These are hence instructed not to send during the reserved period.

## Exercise 7

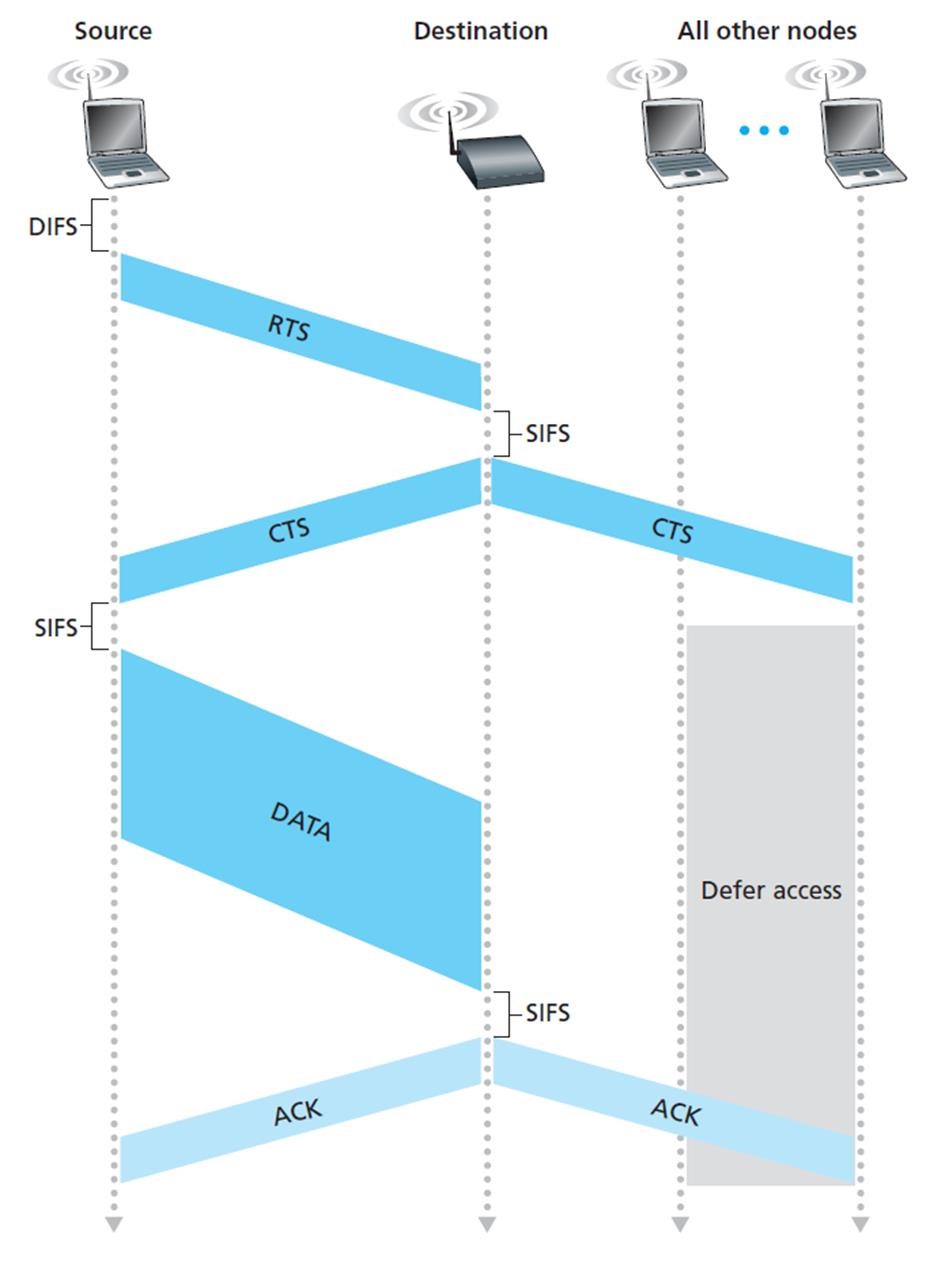
After selecting an AP (by means of its SSID), a wireless host sends a request frame to the AP and the AP responds with a response frame. When connected to an AP, the host will want to join the subnet to which the AP belongs. What does the host do next?

Answer suggestions:

The wireless host will typically send a DHCP discover message (within an UDP segment to port 67 and broadcast IP address 255.255.255.255) into the subnet via the AP to obtain an IP address.

## Exercise 8 (P7 variant)

Suppose an 802.11b wireless host is configured to reserve the channel with the RTS/CTS sequence. Suppose this host wants to transmit 1000 bytes of data, and all other stations are idle at this time.



We have the following assumptions

* The transmission rate in the wireless network is 11 Mbps.
* For 802.11b, DIFS (DCF Interframe Spacing) is 50 microseconds and SIFS (Short Interframe Spacing) is 10 microseconds.
* A 812.11 frame without data is 34 bytes long (see Fig. 7.13 in the textbook). The CTS, RTS and ACK control frames are frames without data.

What will the total time to transmit the frame and receive the acknowledgement as a function of SIFS and DIFS, ignoring propagation delay?

Answer suggestions:

Assumptions:

* Given transmission rate is 11 Mbps.
* Assume that a control frame (such as an RTS frame, a CTS frame, or an ACK frame) is 34 bytes = 272 bits. The time to transmit a control frame is 272 bits/11 Mbps = 25 microseconds.
* The data frame is 1000+34 bytes=1034 bytes = 8272 bits. The time to transmit the data frame is 8272 bits/11 Mbps = 752 microseconds.
* DIFS = 50 microseconds and SIFS =10 microseconds.

From the figure, we have the timing sequence:

## DIFS + RTS + SIFS + CTS + SIFS + FRAME + SIFS + ACK = DIFS + 3 \* SIFS + RTS + CTS + FRAME + ACK

Thus, total time to transmit the frame and receive the acknowledgement is

DIFS + 3 \* SIFS + RTS + CTS + ACK + FRAME = 50 + 3\*10 + 3\*25 + 752 = 907 microseconds

## Exercise 9 (P9)

Power is a precious resource in mobile devices, and thus the 802.11 standard provides power-management capabilities that allow 802.11 nodes to minimize the amount of time that their sense, transmit, and receive functions and other circuitry need to be “on.” In 802.11, a node is able to explicitly alternate between sleep and wake states. Explain in brief how a node communicates with the AP to perform power management.

Answer suggestions:

The node informs the AP that it is going to sleep until next beacon frame. Then the AP will not transmit frames to this node.

The AP sends beacon frames every 100 milliseconds. A beacon frame contains a list of nodes of which the AP has buffered frames for. The node wakes up just before the AP sends the next beacon frame. The node receives the beacon frame. If there are no buffered frames for this node, it will go back to sleep until the next beacon frame.

# Solutions – Chapter 8

## Exercise 1

Explain Kerckhoff's principle with regard to keys and encryption/decryption algorithms.

Answer suggestions:

An encryption algorithm must be known, published, standardized and available to everyone. Security comes solely from the secrecy of the encryption key.

## Exercise 2

What security property is provided by symmetric key and asymmetric key encryption?

Answer suggestions:

Confidentiality

## Exercise 3

1. Consider symmetric key encryption. If an attacker gets hold of both a ciphertext and its underlying encrypted plaintext, can the attacker easily deduce the encryption key?
2. Consider asymmetric key encryption. If an attacker gets hold of both a ciphertext and its underlying encrypted plaintext, can the attacker easily deduce the private key?

Answer suggestions:

No for both

## Exercise 4

All block ciphers and certain public key encryption algorithms are deterministic, meaning that the same plaintext and key produces the same ciphertext.

1. Are block ciphers resistant to chosen plaintext attacks?
2. Are deterministic public key encryption algorithms resistant to chosen plaintext attacks?

Answer suggestions:

Consider chosen plaintext attacks in which an attacker is able to get an encryption for any plaintext. (The ultimate goal may be to obtain the encryption key.)

1. Block ciphers are resistant to such attacks since the attacker does have access to the secret key. (Otherwise, he would have to trick the victim to produce encryptions for him.)
2. For public key encryption algorithms, chosen plaintext attacks is always given, since encryption is carried out using the public key. (However, although this also applies for probabilistic public key encryption algorithms, they produce different ciphertext for a given plaintext.)

## Exercise 5

Checksums and CRC32 codes provide integrity protection concerning transmission errors.

1. Do hash functions provide integrity protection in this regard?
2. Do hash functions provide integrity protection regarding a (passive) eavesdropper?
3. Do hash functions provide integrity protection regarding an active adversary?

Answer suggestions:

1. Yes
2. Not relevant since an eavesdropper does not modify anything
3. No

## Exercise 6

Consider a hash function whose output length is 160 bits. Why is it difficult to find two different input messages that produce the same hash, i.e. h(m1)=h(m2)?

Answer suggestions:

A hash function is a secure one-way function. A hash function whose output length is 160 bits has an output hash space of 2^160 different possible hash values, which is exceedingly large. The probability of finding two distinct messages so that h(m1)=h(m2) is therefore extremely small.

## Exercise 7

What are the different purposes of link-layer MAC and cryptographic MAC?

Answer suggestions:

Link-layer MAC relates to link-layer addressing, where MAC means medium access control, while cryptographic MAC refers to message authentication and message authentication codes.

## Exercise 8 (variant R15)

After being victim of a fraudulent individual, Alice has decided to ensure the integrity of data she sends to her clients.

1. Would integrity protection make the clients confident that Alice is the originator and sender of her data?
2. Regarding protecting against fraudulent individuals, what is suitable of using 1) message digests, 2) MACs, or 3) digital signatures? Explain what is achieved by each alternative.

Answer suggestions:

Integrity protection protects against intended and unintended integrity breeches. However, it does not by itself authenticate the originator of a message.

Message digests do not provide integrity protection nor message authenticity against an adversary. Message authentication codes do this, but are not practical if Alice has many clients. (Why?)

Using digital signatures, it is convenient for her clients to authenticate messages from her. (Why?)

## Exercise 9 (variant R6)

Suppose that a team of 10 people are using symmetric key encryption to communicate securely with the other members of the team, without anybody else in the team being able to decrypt.

1. How many keys need to be shared in total among the team members?
2. Given the pairwise shared keys, how can four people in the group communicate securely together using symmetric key encryption (without anybody else in the team being able to decrypt).
3. Suppose that the group uses public key encryption instead. What is the answer to a) and b) in this case?

Answer suggestions:

1. Each person needs to share one distinct key with each of the 9 other persons. Thus, the total number of keys is 10\*9/2=45. In general, there are N\*(N-1)/2 such pairs and thus there are N\*(N-1)/2 keys.
2. Each person among a subset of four must encrypt the same message with regard to the three other members of that subset. Thus, each person must send three encryptions of the same message.
3. With a public key system, each user has a public key which is known to all. This means that each user must possess the public key of each of the 9 other persons, in addition to his or her own key pair. In total there are 10 public keys to be shared. Similar to b), each person among a subset of four must still encrypt the same message with regard to the three other members of that subset. Thus, each person must send three encryptions of the same message.

## Exercise 10

What are the advantages of using public key encryption compared to secret key encryption? What potential security problem does public keys introduce, and how can this be mitigated?

Answer suggestions:

Using secret key cryptography, Alice and Bob must share a secret key before they can communicate securely. To agree on a secret key over an insecure network can be challenging. Using public keys cryptography, Alice and Bob do not have to share a secret key in advance.

## Exercise 11

Why do digital signatures have a stronger security property (non-repudiation) compared to MACs (message authentication)?

Answer suggestions:

Digital signatures are verified by means of the originator’s public key. This means that they can be verified by anybody, hence non-repudiation, meaning that the originator cannot deny his or her signature.

On the other hand, MACs are computed using a shared secret key, which means that only the other party holding that key can verify the MAC.

## Exercise 12

A digital certificate contains the name of the holder, a public key, and a digital signature. a) Whose signature is it?

1. What is the purpose of digital signature certificates?
2. Does a single digital certificate guarantee this security goal?

Answer suggestions:

* 1. A digital certificate is always signed by a trusted authority.
  2. The purpose of a digital certificate is to authenticate its public key by means of the digital signature.
  3. No, because the signature must be verified by another public key, which has to be trustworthy.

## Exercise 13

Replay attacks are a significant category of attacks.

1. What security property prevents replay attacks?
2. How can replay attacks be prevented?

Answer suggestions:

1. Entity authentication
2. Replay attacks can be prevented using a timestamp, a unique counter, or a nonce. These must be used in conjunction with an encryption, MAC, or digital signature.

## Exercise 14

What is the difference between key transfer and key agreement? Why is key agreement preferable?

Answer suggestions:

Key transfer means that one party generates a symmetric key that he or she securely transmits to another party.

Key agreement means that two parties collaboratively establish a shared key and both contribute to the key value.

## Exercise 15 (R21)

1. What is the purpose of the random nonces in the TLS handshake?
2. How do they achieve this purpose?

Answer suggestions:

1. The purpose of the random nonces in the handshake is to defend against replay attack.
2. During TLS handshake, server and client both send nonces to each other, which are included in a function to create the session keys. This will cause the encryption keys to be unique for every connection, i.e., the connection cannot be re-created in a replay attack.