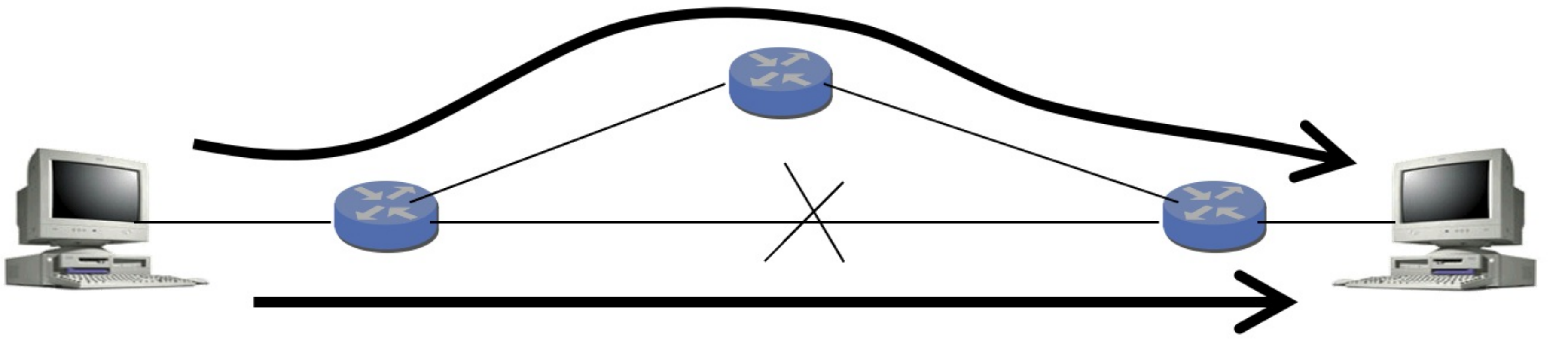
[redacted]

Suppose two hosts have a long-lived TCP session over a path with a 100 msec round-trip time (RTT). Then, a link fails, causing the traffic to flow over a longer path with a 500 msec RTT. This scenario is depicted in the figure below. The original path is the straight path at the bottom. The new path is at the top.



Answer the following two questions.

1 TCP Path Change Q1

Suppose the router on the left recognises the failure immediately and starts forwarding data packets over the new path, without losing any packets. (Assume also that the router on the right recognises the failure immediately and starts directing ACKs over the new path, without losing any ACK packets.) Why might the TCP sender retransmit some of the data packets anyway?

Fill in your answer here

TCP bases its retransmission timeout (RTO) on an estimate of the round-trip time between the sending and receiving hosts. In this example, the RTT is 100 msec before the failure. As this connection has been active for some time, the sender's RTT estimate should pretty accurate and close to 100 msec. The DevRTT should be a very low value (close to 0) The RTO will thus be very similar to the RTT estimate. When the failure occurs, the increase in the actual round-trip time implies that the ACK packets will not arrive before the RTO expires. This causes the sender to presume the data packets have been lost, leading to retransmissions, despite the fact that no packets were actually lost.

Maximum marks: 1.5

2 TCP Path Change Q2

Suppose instead that the routers do not switch to the new paths all that quickly, and the data packets (and ACK packets) in flight are all lost. What new congestion window size does the TCP sender use? Explain your answer.

Fill in your answer here

The TCP sender's adjustment of the congestion window depends on how the packet losses were detected. If a triple-duplicate-ACK occurs, the congestion window would be divided in half. However, in this case, all packets in flight are lost, so no ACKs are received, forcing the sender to detect the loss via a timeout. Timeout-based loss detection leads the sender to set the congestion window to 1 (i.e., 1 MSS).

Maximum marks: 1.5

3 **TCP SYN**

Why does a TCP sender use a very large retransmission timeout (e.g., several seconds) for the SYN segment? Answer in 2 sentences at most.

Fill in your answer here

The TCP sender does not have any initial estimate of the round-trip time (RTT). Starting with a conservative retransmission timeout (RTO) of several seconds prevents the excessive retransmissions that would result from using an RTO that is smaller than the actual RTT.

Maximum marks: 1

4 TCP 3 Way Handshake

Why is it necessary to have a 3 way handshake for connection establishment in TCP? Why is a 2 way handshake not sufficient?

Fill in your answer here

Maximum marks: 2

TCP is a bi-directional communication protocol, which means either end ought to be able to send data reliably. Both parties need to establish an Initial Sequence Number (ISN), and both parties need to acknowledge the other's ISN. Thus a two-way handshake is required in each direction as follows:
1) Alice picks an ISN and SYNchronises it with Bob.
2) Bob ACKnowledges the ISN.
3) Bob picks an ISN and SYNchronises it with Alice.
4) Alice ACKnowledges the ISN.
Steps 2 and 3 can be combined in a SYN-ACK segment, which reduces this to a 3 way handshake.
A two way handshake would only allow one party to establish an ISN, and the other party to acknowledge it. Which means only one party can send data.

Assume that the SendBase for a TCP Reno sender is currently 4000. The TCP sender has sent four TCP segments with sequence numbers 4000, 4500, 5500 and 7000. The sender then receives a segment with an acknowledgement number 7500 and a receive window 6000. The congestion window, CongWin, is set to 10000 bytes after this ACK is processed. Answer the first three questions assuming that this ACK is processed and no further ACKs are received.

5

TCP Sequence Q1

What is the value of SendBase? Only enter the numeric value in the space provided: (7500).

Maximum marks: 0.75

The sender has received an ACK for 7500, so the sender would have moved the base of the window up to that point. Thus SendBase = 7500.

6 TCP Sequence Q2

How many bytes in total are sent in the four TCP segments? Only enter the numeric value in the space provided: ____ (3500).

Maximum marks: 0.75

The first segment carries 500 bytes, the second segment carries 1000 bytes, the third one carries 1500 bytes and the last segment carries 500 bytes. Thus, the total data in the four segments is 3500 bytes.

7
TCP Sequence Q3

What is the last byte (number) that the TCP sender can send with certainty that the receiver's buffer will not overflow? Assume that the sender always has data to send. Explain your answer in 1-2 sentence.

Fill in your answer here

The window size is set to the minimum of the congestion window and receive window. Hence, the window size will now be set to 6000 bytes. Since current SendBase is 7500, this implies that the last byte that the sender can send with certainty is 13499.

Maximum marks: 1

8

TCP Sequence Q4

Now assume that the sender receives three more TCP segments, such that all three segments have TCP acknowledgement number 7500.

Answer the this question and the next question assuming that all three ACKs are processed and no further ACKs are received.

What is the value of CongWin and why?

Fill in your answer here

Since the sender receives three duplicate ACKs, the CongWin is reduced to half the current value (current value = 10000 bytes), which is 5000 bytes.

Maximum marks: 1

9 TCP Sequence Q5

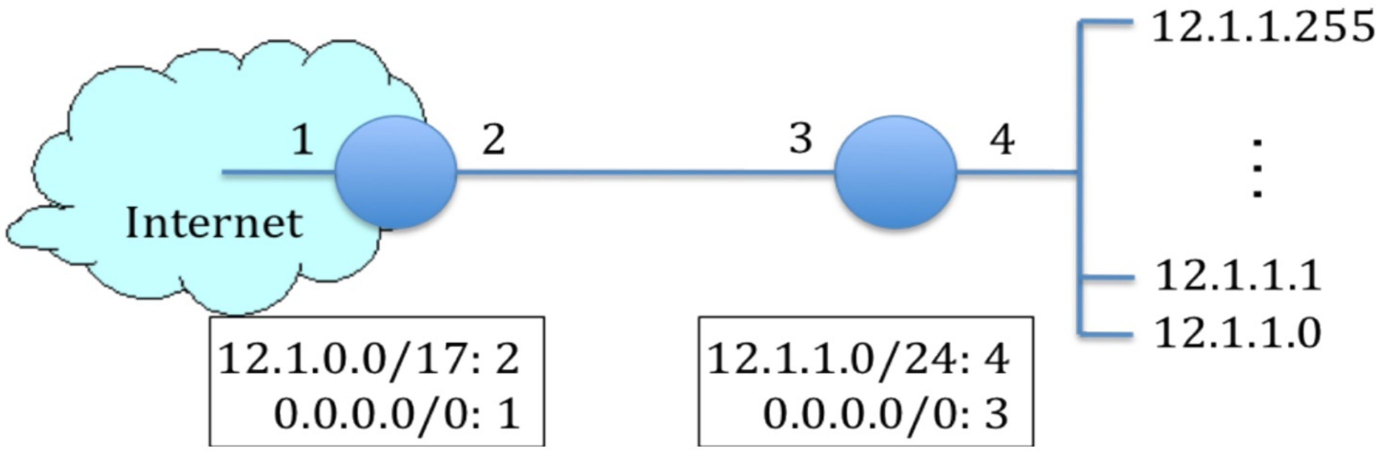
What is the sequence number of the next segment that will be transmitted by the sender? Explain your answer in 1 sentence.

Fill in your answer here

Since the sender received three duplicate ACKs for 7500, it will now retransmit the segment with sequence number 7500.

Maximum marks: 1

A small university campus is assigned a large address block 12.1.0.0/17, but is only using a portion of these addresses (in 12.1.1.0/24) to number its computers. The campus uses a single Internet Service Provider (ISP) to reach the rest of the Internet. The picture below shows the forwarding tables on the ISP's router (on the left) and the campus edge router (on the right).



For example, the ISP forwards all packets with destination addresses in 12.1.0.0/17 to link #2 toward the campus edge router. Both routers include a default forwarding entry (i.e., 0.0.0.0/0) that can match any destination IP address.

Answer the following 4 questions.

10 IP Addressing Q1

How many IP addresses does the campus “own” in its 12.1.0.0/17 block? You can represent your answer as a power of two.

Fill in your answer here

The 17-bit subnet mask leaves 15 bits to identify the addresses within the block. As such, the block contains 2^15 or 32,768 addresses.

Maximum marks: 0.5

11 IP Addressing Q2

What are the smallest and largest IP addresses that the campus “owns”? Do these addresses have special meaning and if so what do they signify?

Fill in your answer here

The smallest IP address would be 12.1.0.0. This is usually referred to as the network address (i.e. to refer to the entire network). The largest address would be 12.1.127.255 and it is the broadcast address for the network.

Maximum marks: 1

12 IP Addressing Q3

Suppose the ISP router receives a packet from the Internet with destination IP address 12.1.20.1? What path does this packet follow (indicate the path using link numbers from the above figure)? What is the ultimate outcome for this packet?

Fill in your answer here

The packet flows over the path, 1 -> 2 -> 3 -> 2 -> 3 ……. It keeps looping. Match the destination IP with the forwarding table entries at each router.
The looping packet is eventually discarded once it’s TTL equals to zero.

Maximum marks: 1.5

13 IP Addressing Q4

Suppose the ISP router receives a packet from the Internet with destination IP address 12.1.1.1? What path does this packet follow (indicate the path using link numbers from the figure above)?

Fill in your answer here

The packet flows over the path 1 -> 2 -> 3 -> 4

Maximum marks: 1.5

14 **NAT**

When an IP datagram containing a transport segment is going from a private network onto the public Internet through a Network Address Translation (NAT) router, which of the following network and transport layer header fields might the router change? You can select multiple options.

Select one or more alternatives

- Protocol field in IP header
- Source IP address ✔
- IP checksum ✔
- Destination IP address
- Transport checksum ✔
- Source port number ✔
- None of the provided choices
- Destination port number

Maximum marks: 1

A NAT router would modify the source IP, source destination, and the transport and IP checksums for outgoing datagrams.

15 DV MCQ

Which of the following statements about distance vector routing are true? Multiple statements may be true.
Select one alternative:

- Every router in the network knows the entire network topology.
- Poison reverse may not always resolve the count to infinity problem. ✔
- None of the other choices are true.
- The distance vector sent by each router is propagated to all other routers in the network.
- A reduction in the cost of a link connected to a router will always trigger a distance vector update to be sent from this router.

Maximum marks: 1

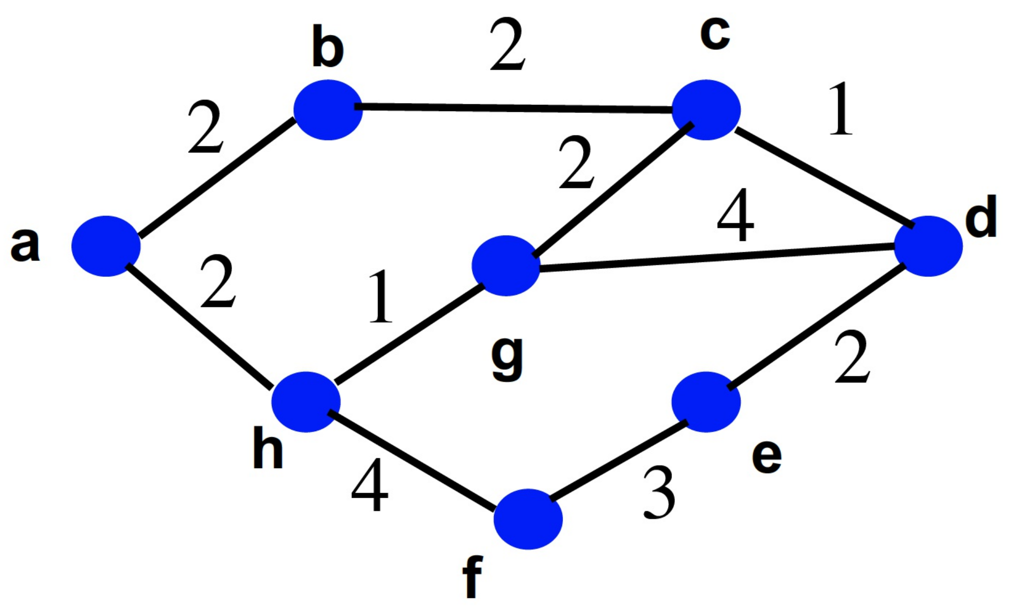
In DV, routers do not have knowledge of the entire topology, just their direct neighbours.

A reduction in the cost of a link will always trigger the execution of the DV algorithm at the node. However, a DV update will only be sent if there is a change in the DV as a result of this execution, which may not always be the case.

A DV from a node is only sent to its direct neighbours. These neighbours do not propagate the DV further. So the correct answer is that Poison Reverse may not always solve county to infinity problem. An example was shown in the lecture.

[redacted]

Consider the 8-node network shown in the figure below with link costs as shown. Note that each link shown in this network is bidirectional and has the same cost in either direction.



Answer the following two questions.

16 # Dijkstra

Execute Dijkstra's algorithm at Node **a** to determine the shortest path from Node **a** to every other node in the network. You will have to draw an appropriately sized table using the table option in the menu at the top of the text area below (similar to the one shown in the lecture notes on Dijkstra's algorithm) You are required to show all steps.

Fill in your answer here

Step	N	D(b), p(b)	D(c), p(c)	D(d), p(d)	D(e), p(e)	D(f), p(f)	D(g), p(g)	D(h), p(h)
0	a	2, a	-	-	-	-	-	2, a
1	ab		4, b	-	-	-	-	2, a
2	abh		4, b	-	-	6, h	3, h	
3	abhg		4, b	7, g	-	6, h		
4	abhgc			5, c	-	6, h		
5	abhgcd				7, d	6, h		
6	abhgcdf				7, d			
7	abhgcdfe							

Since there is a tie at step 1, either b or h could be chosen as the node to be added to N. The other node would be added in Step 2. In the answer provided b is added first, followed by h. However, you could have added h first, followed by b. The end result would still be the same.

Words: 0

Maximum marks: 4

17

Forwarding Table

Based on the execution of the Dijkstra's algorithm in the above question, draw the forwarding table for node **a**, which contains the outgoing link for reaching every other node in the network. A link between two nodes x and y should be denoted as (x, y).

Fill in your answer here

Destination	Outgoing link
b	(a, b)
c	(a, b)
d	(a, b)
e	(a, b)
f	(a, h)
g	(a, h)
h	(a, h)

Maximum marks: 1.5

18 # CRC Q1

Assume that the data bits D being transmitted over a link are 100010 and that CRC is being used to provide error detection. Suppose that a generator, G = 111 is being used and known to both the sender and receiver.

1) What are the CRC bits (R) as computed (and included with the message) by the sender? You are not required to show your calculations. Simply note down R in the space provided. [ ] (11)

2) Continuing with the previous question. Assume that the sender transmits <D, R>. Neglect any other headers. Assume that 2nd, 3rd and 4th bits of this sequence are flipped as the frame is transmitted through the link. Will the receiver be able to detect the error?

Select an alternative

- True
- False ✔

Maximum marks: 1.5

1) R = 11 (NOTE: you cannot add leading or trailing zeros, so 011 or 110 are not valid answers)

```
      110101                 110101
111√10001000           111√10001011
    111                    111
     110                    110
     111                    111
       110                    110
       111                    111
         100                    111
         111                    111
          11                      0 ← perfectly divided
```

The computation on the left which shows how R is computed by the sender. The computation on the right side shows you that if there are no errors while transmission, then dividing <D, R> by G will result in a zero remainder at the receiver.

2) False.

```
      100101
111√11111011
    111
      110
      111
        111
        111
          0 ← perfectly divided, CRC returns 'no error detected'
```

The computation is for the case when the ordering is left to right (i.e. 2nd, 3rd and 4th bits are counted from the left). I have not shown the computation if you count the order right to left but the answer would still be the same - False.

19

CRC Q2

Now assume that the data bits D are the same as the previous two questions (100010) but that a generator G = 1111 is used.

1) What will be the CRC bits (R) as computed (and included with the message) by the sender? You are not required to show your calculations. Simply note down R in the space provided.

(000)

2) Continuing with the previous question. Assume that the sender transmits <D, R>. Neglect any other headers. Assume that 2nd, 3rd and 4th bits of this sequence are flipped as the frame is transmitted through the link. Will the receiver be able to detect the error?

Select an alternative

- True ✔
- False

Maximum marks: 1.5

1) R = 000. (NOTE: There MUST be 3 zeros in your answer, so 0 or 00 or 0000 are not valid answers)

```
       110000                 110000
1111√100010000        1111√100010000
     1111                  1111
      1111                  1111
      1111                  1111
         00000                 00000 ← perfectly divided
```

The computation on the left shows how R is computed by the sender. The computation on the right shows the corresponding computation at the receiver assuming there are no errors in transmitting <D, R>

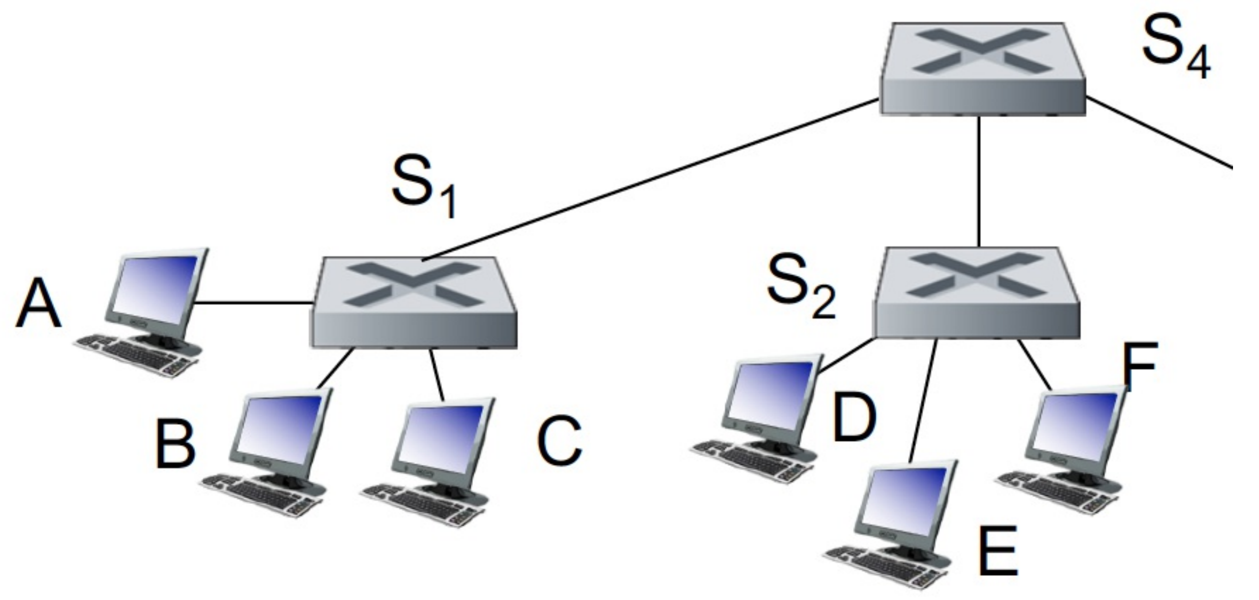
2)

```
          100011
    1111√111110000
         1111
           01000
            1111
             1110
             1111
               001 ← not perfectly divided, CRC returns 'error detected'
```

The computation shown is for the case when the ordering is left to right (i.e. 2nd, 3rd and 4th bits are counted from the left). I have not shown the computation if you count the order right to left but the answer would still be the same - True.

[redacted]

Consider the network shown in the figure below. You may assume that all switch tables are empty at the start.



Answer the following three questions. To represent links you can use notations such as A-S1 (the link connecting A to S1) and S1-S4 (the link connecting S1 to S4).

20 Switch Q1

Assume that host A sends a frame to Host F. Indicated all links in the network that this frame is transmitted on and explain why.

Fill in your answer here

The frame is first sent on the link A-S1. When it arrives at S1 since the switch table is empty, the frame will be broadcast by S1 on all other links: S1-B, S1-C, and S1-S4.

When the frame reaches S4, since the switch table is empty, S4 would send it to all other links, i.e., S4-S2.

When the frame arrives at S2 since the switch table is empty, the frame will be broadcast by S2 on all other links: S2-D, S2-E, and S2-F.

Maximum marks: 1.5

21
Switch Q2

Assume that host F now sends a frame to Host A. Indicated all links in the network that this frame is transmitted on and explain why.

Fill in your answer here

The frame would be transmitted on F-S2. When the frame reaches S2, it would now have learnt that host A is reachable along the link S2-S4. So S2 would selectively forward the frame on this link (i.e., S2-S4).
When the frame reaches S4, S4 would have learnt that host A is reachable along the link S4-S1. So S4 would selectively forward the frame on this link (i.e., S4-S1).
When the frame reaches S1, S1 would have learnt that host A is reachable along the link S1-A. So S1 would selectively forward the frame on this link (i.e. S1-A).

Maximum marks: 1.5

22 ARP

Suppose Host C wants to send an IP datagram to Host F. Assume that Host C only knows the IP address of Host F but does not know its MAC address. Describe how Host C proceeds to send the IP datagram (i.e., outline the sequence of events leading to transmission of this datagram).

Fill in your answer here

Host C will first send an ARP query requesting for the MAC address that corresponds to F's IP address. This query will be sent to switch S1 which will send it on all outgoing links. Switches S4 and S2 will do the same. So all hosts will receive this query. Only Host F will respond with an ARP response containing its own MAC Address. When Host C receives this MAC address, it will encapsulate the IP datagram in an Ethernet frame with F's MAC address as the destination and transmit the frame to Switch S1. Depending on the switch table entries of the switches this frame will either get selectively forwarded towards F or broadcast.

Maximum marks: 1.5

Consider the wireless network composed of four nodes in the figure below, which has a linear topology deployed along a highway. The distance between neighbouring nodes is equal. Assume all nodes are using 802.11 MAC with RTS/CTS enabled. The radio range for each node is fixed, and this radio range is slightly longer than the inter-node distance, i.e., each node can reach only its left and right neighbours. Assume that if there are two simultaneous transmissions within the radio range of the receiver, both transmissions will be unsuccessful.

Answer the following three questions.

23 WiFi Q1

Assume that node A is currently sending a data frame (not an ACK, an RTS, or a CTS) to node B. Node C wants to send a packet to node D. Assume that node C (and only C) ignores the 802.11 MAC and sends the packet. Would C's packet arrive successfully at D? Would A's packet arrive successfully at B? Explain your reasoning.

Fill in your answer here

C's packet would indeed arrive successfully at D since D cannot hear A's transmission. Hence, there is no interference from the perspective of the receiver (i.e. D). However, A's packet would not arrive successfully at B, since there will be a collision at B due to interference from C's transmission.

Maximum marks: 1

24 WiFi Q2

Consider the same situation as in the previous questions except that all nodes are using the 802.11 MAC. Will C start transmission while A is sending the data packet? Why or why not? If not, how does C know that A is transmitting a data frame?

Fill in your answer here

C will not transmit while A is transmitting. This is because C would have overhead the CTS frame sent by B (in response to the RTS request from A). The CTS frame will contain the duration of time for which the ongoing transmission between A and B will go on. Thus, C will know when A is transmitting

Maximum marks: 1

25

WiFi Q3

Is there any way for C to know when A’s transmission will end? Explain.

Fill in your answer here

Same reason as stated in the answer to the previous question. The CTS contains the time and hence, C will know when A’s transmission will end. C will also receive the ACK from B to signal the end of transmission from A.

Maximum marks: 1

26

Keys

Suppose *N* people want to communicate with each of *N* – 1 other people using symmetric key encryption. All communication between any two people, *i* and *j*, is visible to all other people in this group of *N,* and no other person in this group should be able to decode their communication. How many keys are required in the system as a whole?

Now suppose that public key encryption is used. How many keys are required in this case?

Provide a short explanation for your answers in the space below.

Fill in your answer here

Symmetric Key Encryption:
A symmetric key would be required between each pair of people. So Person 1 would require (N-1) keys to communicate with others. Person 2 would require (N-2), Person 3 would require (N-3) and so on. Thus total keys required = (N-1) + (N -2) + (N-3) .... + 1 = N(N-1)/2.

Public Key Encryption:
Each person would only require a public, private key pair. So the total keys required = N pairs of public, private key pairs.

Maximum marks: 2

27

CA

What is the role of a Certification Authority (CA) in Public Key Infrastructure (PKI)?
Select one alternative:

- Issues a session key to both end parties for communication
- Guarantee that the public key of the registered user is authenticated by issuing a digital certificate ✔
- Maintain private keys of all authenticated users
- CA's are not used in PKI

Maximum marks: 1

The role of the CA is to certify the public keys of users who register with it. The CA does so by adding a digital signature (signed by the CA's private key) to the public key of the user. Others can verify the certificate by applying the CA's public key.

28

Email

SuperMail wants every email to be authenticated and protected from modification or tampering while it is transit from the sender to the receiver. Suppose Alice is sending an email *M* to Bob. Assume that a SuperMail employee proposes the following solution: Alice's software should encrypt M using Bob's public key. In other words, Alice's software should send E_{KB+} (M) to Bob. Can you comment on whether the employee's solution meets the requirement stated above. Justify your answer.

Fill in your answer here

Encryption does not provide authenticity/integrity. Anyone other than Alice can send the exact same message to Bob Bob won't be able to distinguish who the sender was..

Maximum marks: 1

29 Putting it together

You walk into a room, connect your laptop to an Ethernet outlet, and type in your web browser a URL of a web page. List all the messages/packets that you expect your laptop to send or receive until you download the web page. Assume that your laptop is configured with the IP address of a local DNS server, as well as the IP address of a default gateway (a router through which traffic from your laptop will exit the local IP subnet).

Fill in your answer here

Since your computer's ARP cache is initially empty, your computer will use ARP protocol to get the MAC addresses of the first-hop router and the local DNS server.
Your computer will first query the local DNS server to find the IP address of the Web page you would like to download.
Once your computer has the IP address of the Web page, then it will establish a TCP connection and send out a HTTP request via the first hop router (assuming the Web server does not reside inside the local network). The HTTP request message will be encapsulated in a TCP segment, and then further encapsulated in an IP datagram and then an Ethernet frame.
Your computer sends the Ethernet frame destined to the first-hop router. Once the router receives the frame, it passes the encapsulated IP datagram up to the IP layer, checks its routing table, and then sends the IP datagram encapsulated in an Ethernet frame to the next-hop (the interface corresponding to the next-hop in the routing table). Then the IP datagram will be routed through the Internet until they reach the Web server.
The server hosting the Web page will send back the Web page to your computer via HTTP response messages. Those messages will be encapsulated in TCP segments and then further into IP datagrams and link layer frames. Those IP datagrams follow the routes (as per the routing algorithms used) and finally reach your first-hop router, and then the router will forward them to your computer by encapsulating them into Ethernet frames.

Words: 0

Maximum marks: 3