Question 1

0 / 1 pts

How is network congestion signaled between hosts on a TCP/IP connection.

- By setting the congested flag in the IP header.
- You Answered — By signaling a Window size of 0

  Incorrect
- Internet routers monitor their links and signal the hosts using out-of-band connections.
- Correct answer — As a side-effect of requests to re-transmit undelivered packets.

Question 2

1 / 1 pts

How is the route which data flows between two hosts in a circuit switched network determined?

- It is laid down in the CCITT guidelines for host connectivity.
- Each data packet sent between the two hosts can take any route through the network.
- Correct! — It is setup at the start of the connection and cannot change.

  Correct
- Servers in the cloud compute the best route between the hosts and inform the intermediary routers.

Question 3

1 / 1 pts

If one host on a TCP/IP link signals that its Window size is 0, what does this mean?

- The host sending the Window=0 is opening the connection.

Correct!

- The host sending the Window=0 has a full buffer and the other host should stop sending.

  Correct

- The host sending the Window=0 is now ready to receive data again.
- The host sending the Window=0 segment is closing down the connection.

Question 4

1 / 1 pts

Which of the following are unreliable protocols?

- Ethernet

You Answered

- Multicast

  Correct

Correct!

- UDP

  Correct

- TCP/IP

Correct. Issues with question setup.

Question 5

0 / 1 pts

You are asked to audit a real time networked system with a full mesh topology. Each node can process a maximum of 10 messages/second from the network. If all messages sent by a single node have to be sent to all members of the network including itself, what is the maximum size of of the mesh?

You Answered

- 11

Incorrect

- 100

Correct answer

- 10

- 25

Question 6

1 / 1 pts

What is the Internet Control Message Protocol (ICMP) used for.

Correct!

- End to end signaling of error messages.

Correct

- To bridge between IP and MAC addresses.
- To provide a key exchange mechanisms for asymmetric encryption protocols.
- To allocate IP addresses dynamically to hosts.

Question 7

1 / 1 pts

What protocol layer does ARP belong to?

- Layer 10
- Correct! Layer 2 and 3

  Correct
- Layer 4
- Layer 2

Question 8

1 / 1 pts

What is jitter?

- Variations in the rate of packet loss.
- Variation in the bandwidth on a route.
- Variation in signal amplitude that can burn out fibre optic cables
- Correct! Variations in packet arrival latency that can cause quality issues for real time traffic such as audio.

  Correct

Question 9

1 / 1 pts

What does Nagle's algorithm do when it is enabled on a connection?

- Piggy backs acks onto other traffic
- Prevents buffer from getting too small in order to prevent silly window syndrome
- Forces routers to preferentially drop TCP traffic
- Correct! Buffers data to be sent until it has a full segment or has not received a previous ack

Correct

Question 10

1 / 1 pts

How does Wireshark know the manufacturer of a device sending data?

- Correct! It uses the part of the MAC address which identifies the manufacturer.

Correct

- It uses a dynamically updated database maintained by the IEEE
- It uses the IP address manufacturer code.
- The device identifies itself with a string.

Question 11

1.5 / 2 pts

Distributed Hash Tables are used as a efficient algorithm in peer-to-peer networks to provide an [Select] to [Select] content on each node in the network.

Answer 1:

You Answered — efficient

Correct answer — scalable

Answer 2:

Correct! — peer-to-peer

Answer 3:

Correct! — index

Answer 4:

Correct! — local

Question 12

2 / 2 pts

The Fisher Consensus problem states that it is impossible to guarantee that any number of asynchronously con hosts can agree on even a single bit value.

Answer 1:

Correct! — impossible

Answer 2:

You Answered — asynchronously connected

Correct answer — guarantee

Correct. Issues with question setup.

Question 13

0 / 2 pts

If an application problem requires consensus between nodes, they must use some form of _____ topology.

You Answered

mesh

Correct Answers

partial mesh

hierarchical

full mesh

Question 14

2 / 2 pts

You are asked to design a real time audio application, streaming information from microphones across the Internet. Describe briefly whether you would use TCP/IP or UDP for your application, and the pros and cons of this choice vs. the alternative. (Note: either choice is fine, this question is asking for the design considerations of your choice.

Your answer:

TCP/IP deliveres/receives an ordered and error-checked stream of information packets over a network. **UDP**, however, delivers a faster stream of information by excluding error-checking.

With this in mind, I would prefer to design a real time audio application with **UDP**, as the main purpose is to deliver soundbites to the user. If a few seconds of audio is missing (assuming that the audio information is continuous and not only a few seconds long), it will not interfere with the quality for the end-user, but instead provide the user with fast stream of audio instead - therefore providing the user with the main purpose of the application, real time audio.

Pros: No excessive latency (UDP), skipping communication and error-checking back and forth between devices (TCP). Therefore, resulting in faster communication between the devices with UDP.

Cons: Data (packets) can/may be lost with UDP, versus not lost with TCP.

Question 15

2 / 2 pts

What is a goodput collapse?

Your answer:

Goodput is the useful user traffic transmitted by a network. That is, packets sent per second (packets/sec). In a congestion collapse, network becomes unusable, as transmission of dropped packets increases load, which causes more packets to be dropped. Therefore, resulting in a goodput collapse, as the network is still carrying its full load of traffic, but has been driven out by error recovery traffic. This may in the end result in the network crashing, as you shall not do.

Something something Lord of the Rings joke.

Question 16

2 / 2 pts

Why is flow control important at all levels of the network stack?

Your answer:

Too much traffic from hosts will cause blocking, therefore it is necessary to control the flow of traffic between sender and receiver on the network stack.

If this is not done, data can be sent too quickly, leading to that the receiver is overwhelmed by the amount of data that it starts dropping packets and data gets lost and/or the network collapses due too error handling.

Also, the data transfer can be too slow, resulting in an inefficient network and slow connection between hosts (which equals frustrating users).

Therefore, the flow control for all levels of the network stack is highly important, which (should) result in the most efficient and fast network possible between hosts - making everybody happy.

Question 17

2 / 2 pts

What is the advantage of TCP Selective Acknowledgements (SACK) over the original cumulative acknowledgement scheme?

Your answer:

In the original cumulative acknowledgement scheme, the client sends some requests to the server, and the server formulates a response. For this example, lets say the response is four packets.

The server transmits all four packets in response to the request, but the second response packet is lost somewhere in the network and never reaches the client.

This results in the inefficiency that the server has sent all the packets, but the client only acknowledges receiving packet number one - resulting in that the server has to send again packets 2-4 to the client.

With selective acknowledgement (SACK), the client is allowed to say (for this particular example) that it only has received packet number one in order, but has also received packet 3-4.

This allows the server to re-transmit only the packet (no.2) lost, which then is received by the client.

Question 18

1.5 / 2 pts

Explain the differences between symmetric and asymmetric encryption.

Your answer:

Symmetric encryption: Same key is used to encrypt and decrypt.

Plaintext --> Encryption (key) --> Ciphertext --> Decryption (key) --> Plaintext

Asymmetric encryption: Two different keys, one to encrypt, and to decrypt.

Plaintext --> Encryption (key1) --> Ciphertext --> Decryption (key2) --> Plaintext

Are these all private? Public? Combination?

Question 19

2 / 2 pts

Multicast is a protocol designed to allow the same data to be broadcast between computers on the same multicast group. Each time a host in the group sends a datagram to the multicast group, the network routers ensure that that datagram is sent to all members of the group.

Considering the SEQ/ACK methods used by TCP/IP to guarantee reliable delivery of data between nodes, what fundamental issues will be created when trying to implement reliable multicast to large groups of hosts?

Your answer:

Excessive traffic.

By using TCP/IP when dealing with multicast, you are consequently crashing the network very very quickly, as TCP/IP sends packets and waits for acknowledgement from the client(s) before sending the next packet.

If an error occurs, that is a packet has not been received by the client, a sequence of error handling is then processed - meaning packets are being sent again over the network, which does not lead to an ideal multicast to large groups of hosts.

Question 20

2 / 2 pts

You are asked to improve a real time network application's performance. Examining the code you notice that it sending 1653 byte messages across the network, the Nagle algorithm is enabled on both sides, and the application is using a 2 Mb. buffer. What do you recomend?

Your answer:

According to **Nagle's Algorithm**, it attempts to limit the number of small packets / connections. As long as there is a sent packet outstanding (no ACK) - Sender will buffer data arriving to be sent. Data is then sent, when segment amount of data has been received, and ACK arrives for previous segment.

With a real time network application, the Nagle's Algorithm is exactly what you do not want to be happening, as there are a lots of small real time update packets being sent (not the **excessively large messages** that are being sent over this network). Connections can be dropped, whilst Nagle is delaying traffic. As well as the algorithm can create a deadlock with delayed ACKs.

With **too big buffers**, latency can be caused as well.

So, my recommendation is the following:

- Adapt an algorithm that is more suited to real-time network application performance (not Nagle's Algorithm).

- Decrease the size of the application buffer.

- Decrease the size of the messages being sent over the network.

Correct. Though if we disable Nagle's algorithm, the buffer size doesn't matter much.