# Exam 2014, Questions and answers - Lots of questions!

Computer Networks I (University of Queensland)

# Odd Questions

**A hub in an Ethernet like a network is replaced by a switch. What impact will this replacement have on the network throughput? Explain**

A switch directs packets only to the intended recipient whereas a hub transmits the packets through all of its ports. Using a hub increases collisions and reduces throughput but has no processing delay since it does not have to look at the destination address to forward packets. A Switch is more efficient in that it can transmit on different ports in parallel and there changing to a switch will increase network throughput. [igs, wadey]

**Show similarities and differences between the MAC and IP addresses.**

Similarities:
- Both identify the computer uniquely in a network

Differences
- MAC address shouldn't be changed and is embedded into hardware at the manufacturer
- IP Address can be changed and is not embedded into hardware
- MAC addresses should be globally unique
- IP address may or may not be unique on globally

**Explain the term *Broadcast Network*.**

A network in which all devices on the network receive every sent packet.

**Are there any MAC layer protocols for which it makes sense to use the stop-and-wait protocol?**

Wireless LAN because it cannot send and receive simultaneously. It also has a high transmission error rate.

Stop-and-Wait is ineffective if the RTT is high. Due to Wi-Fi having a low range, the RTT is very short. Knowing that the RTT will always be very short and that Wi-Fi has a right rate of transmission errors, the stop-and-wait protocol makes sense to be used in Wi-Fi. [Alison, David, mdn]

**Explain the terms *multicast* and *broadcast* with respect to frames or packets. Is Ethernet capable of broadcasting and/or multicasting frames?**
**Explain your answer.**

Multicast is a type of address which sends a frame to multiple entities (a.k.a a group) on the network.

Broadcast sends the frame to all nodes in the network.

Ethernet is able to do a multicast and a broadcast. Ethernet normally is not able to distinguish between the two as a broadcast is a special case of multicast in that it sends to all nodes in the network.

**Is every "read" operation an idempotent operation? Explain why. (2 marks)**

No. As if you are reading from say, the Physical Layer's buffer, upon reading that data it is removed from the buffer therefore "reading" again will give a different result.

A read operation can be idempotent if it specifies which index to read from however.

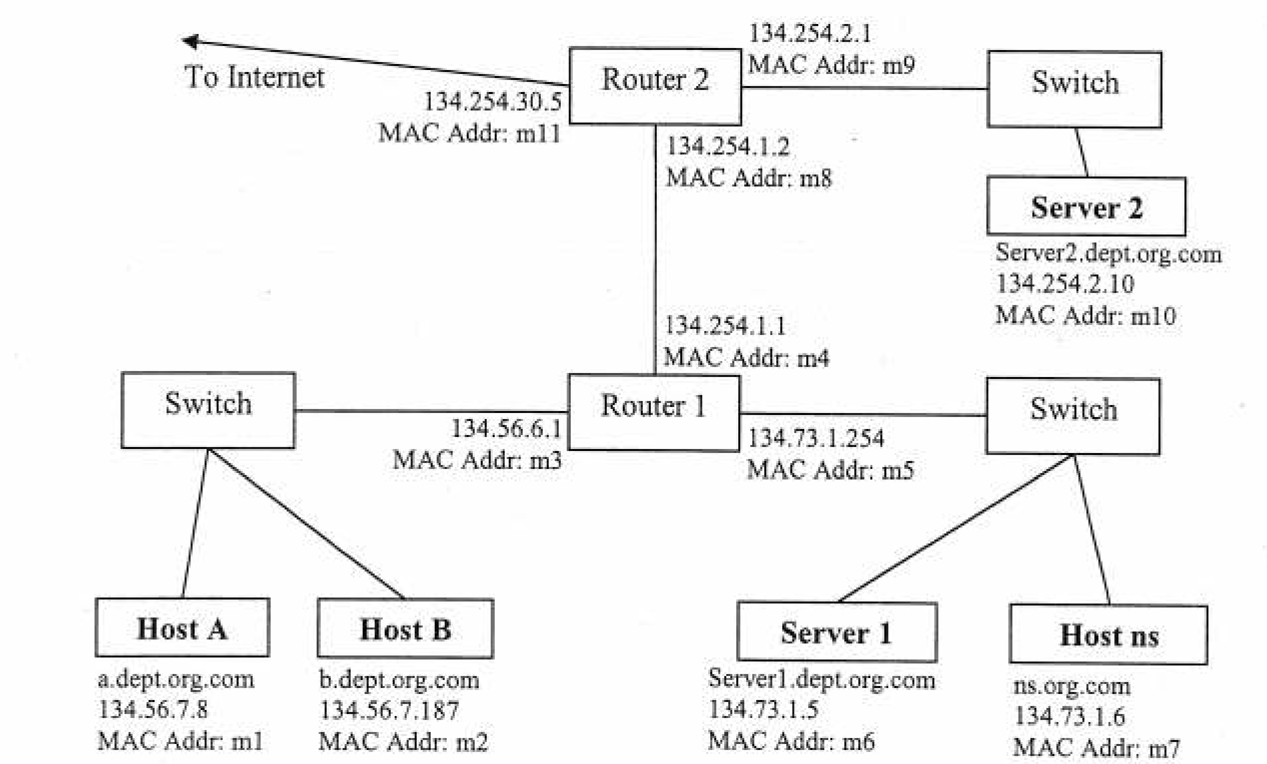
**Explain why the CSMA/CD protocol used in Ethernet-like networks is not suitable for Wireless LANs. (3 marks)**

It's expensive to build wireless hardware that can send and receive on the same frequency at the same time, which is required for CD. Also Wireless LANs give rise to the Hidden Station Problem, which results in two or more Nodes not being able to "see" one another; This can lead to issue where both Nodes think the channel is free and transmit at the same time and as they cannot "see" one another they cannot detect the collision.

**The Stop-and-wait protocol is known for its poor performance. Are there any current network technologies in which using this protocol at the data link layer makes sense? Explain why. (3 marks)**

Yes; In current WiFi networks the Stop and wait protocol is used because it does not result in packet collision. The stop and wait protocol also does not allow sending and receiving of packets simultaneously which directly corresponds to the properties of wireless transmission making it a suitable protocol choice. As wireless cannot achieve the performance gains prominent in other protocols (Sliding windows, etc) the poor performance of stop and wait protocols is acceptable/ unavoidable.

The performance is also typically not as bad as in other situation as in wireless transmission the RTT tends to be very low (due to the low range).



**Hosts have the names, IP addresses and (simplified) MAC addresses shown. *Host ns* servers as the authoritative DNS server for org.com. Each host is aware of its subnet mask, the IP address of the gateway (i.e. the particular router interface**

**address), and the IP address of the DNS server. Assume that at the beginning of the communication exchange described below no host/router has ARP or DNS information cached (other than *Host ns* knowing DNS information for the whole domain), however once it acquires such information it will be cached.**

**Consider a client process on host A sending a request to Server 1. The address (Server1.dept.org.com) is given to the client process as an argument. Assume that TCP is used at the transport layer. Write down the sequence (in time) of ARP and IP packets that will be transferred to complete this request. You should clearly specify which host (and interface) sends each packet, which hosts(s) receive (i.e. process) each packet and what the contents of the packet are. You may assume that no transport or IP level fragmentation is necessary and that no packets are lost. You may also assume that the client request will be successful and a response will come from the server.**

**As an example of the level of detail required, the first frame in the sequence is provided for you. Your answer should be a table with the headings shown below. You do not need to repeat this first frame.**

| **Sender(Interface)** | **Receiver(s)** | **Content** |
|---|---|---|
| Host A (m1) | All on Network 1 | ARP request: "Who owns 134.56.6.1?<br>My IP address is 134.56.7.8"<br>(Host a needs to find the MAC address of Router 1.) |
| Router 1 (m3) | Host A (m1) | ARP reply: "MAC address of 134.56.6.1 is m3"<br>[Router 1 replies to ARP request from Host A with MAC address] |
| Host A (m1) | Router 1 (m3) | UDP DNS Request: "Who owns Server1.dept.org.com? Please tell me: 134.56.7.8" |
| Router 1 (m5) | Host ns (m7) | ARP request: "Who owns 134.73.1.6?<br>My IP address is 134.73.1.254"<br>[Router 1 needs to find the MAC address of Host ns] |
| Host ns (m7) | Router 1 (m5) | ARP reply: "MAC address of 134.73.1.6 is m7"<br>[Host ns replies to ARP request from Router 1 with MAC address] |
| Router 1 (m3) | Router 1 (m5) | Forwarding message |

| | | |
|---|---|---|
| | | [Router 1 forwards the packet from Host A to Host ns] |
| Host ns (m7) | Router 1 (m5) | UDP DNS response: “134.73.1.5 owns Server1.dept.org.com”<br>[Host ns replies to DNS request from Host A] |
| Router 1 (m5) | Router 1 (m3) | Forwarding message<br>[Router 1 forwards packet from Host ns to Host A] |
| Host A (m1) | Router 1 (m3) | TCP SYN: “Hi 134.73.1.5, I’m 134.56.7.8, I would like to chat.”<br>[Host A wants to establish communication with Server 1] |
| Router 1 (m3) | Router 1 (m5) | Forwarding message<br>[Router 1 forwards the packet from Host A to Server 1] |
| Router 1 (m5) | All on Network 2 | ARP Request: “Who owns 134.73.1.5? My IP address is 134.73.1.254.”<br>[Router 1 needs to know the MAC address of Server 1] |
| Server 1 (m6) | Router 1 (m5) | ARP Reply: “MAC Address of 134.73.1.5 is m6.”<br>[Server 1 replies to ARP request from Router 1 with MAC address] |
| Router 1 (m5) | Router 1 (m3) | Forwarding message<br>[Router 1 forwards the packet from Server 1 to Host A] |
| Server 1 (m6) | Router 1 (m5) | TCP SYN-ACK: “Hi 134.56.7.8, yeah, I’m up for a chat!”<br>[Server 1 accepts the connection from Host A] |
| Router 1 (m3) | All on Network 1 | ARP Request: “Who owns 134.56.7.8? My IP Address is 134.56.6.1”<br>[Router 1 needs to know the |

| | | |
|---|---|---|
| | | MAC address of Host A” |
| Router 1 (m5) | Router 1 (m3) | Forwarding message<br>[Router 1 forwards the packet from Server 1 to Host A] |
| Host A (m1) | Router 1 (m3) | ARP Reply: “MAC address of 134.56.7.8 is m1.”<br>[Host A replies to ARP request from Router 1 with MAC address.] |
| Host A (m1) | Router 1 (m3) | TCP ACK: “I heard you agreed to the chat, just so you know, I heard you: 134.73.1.5. Yours truly: 134.56.7.8.”<br>[Host A needs to Acknowledge the SYN-ACK from Server 1] |
| Router 1 (m3) | Router 1 (m5) | Forwarding message<br>[Router 1 forwards the packet from Host A to Server 1] |
| Host A (m1) | Router 1 (m3) | TCP: “I have a request for you: 134.73.1.5, here it is.”<br>[Host A sends the request to Server 1] |
| Router 1 (m3) | Router 1 (m5) | Forwarding message<br>[Router 1 forwards the packet from Host A to Server 1] |
| Server 1 (m6) | Router 1 (m5) | TCP: “Here is my response for: 134.56.7.8.”<br>[Server 1 sends the response to Host A] |
| Router 1 (m5) | Router 1 (m3) | Forwarding message<br>[Router 1 forwards the packet from Server 1 to Host A] |
| Host A (m1) | Router 1 (m3) | TCP FIN: “I’ve finished chatting with: 134.56.7.8.”<br>[Host A doesn’t want to communicate anymore] |
| Router 1 (m3) | Router 1 (m5) | Forwarding message |

| | | |
|---|---|---|
| | | [Router 1 forwards the packet from Host A to Server 1] |
| Server 1 (m6) | Router 1 (m5) | TCP ACK: “I heard you finished chatting? Okay!”<br>[Server 1 acknowledges that Host A doesn’t want to chat anymore] |
| Router 1 (m5) | Router 1 (m3) | Forwarding message<br>[Router 1 forwards the packet from Server 1 to Host A] |
| Server 1 (m6) | Router 1 (m5) | TCP FIN: “Okay, I’ve said all I needed to say.”<br>[Server 1 agrees that the communication is finished] |
| Router 1 (m5) | Router 1 (m3) | Forwarding message<br>[Router 1 forwards the packet from Server 1 to Host A] |
| Host A (m1) | Router 1 (m3) | TCP ACK: “Okay, thanks for letting me know. Communication is over.”<br>[Host A acknowledges that Server 1 agreed the communication is over] |
| Router 1 (m3) | Router 1 (m5) | Forwarding message<br>[Router 1 forwards the packet from Host A to Server 1] |

# TCP/IP Questions

**Explain why TCP original 16-bit window size is not suitable for use in high bandwidth product networks**

Due to the high bandwidth, a large amount of packets will be sent before the expiry of the maximum segment lifetime. This becomes an issue since the sequence number will be wrapped around and two packets could have the same sequence number. [anon, Alison]

**Explain how the TCP flow control mechanism supports congestion control. Discuss the impact of the mechanism on the TCP performance for the end-to-end paths that include wireless hops (eg, the last hop is wireless)**

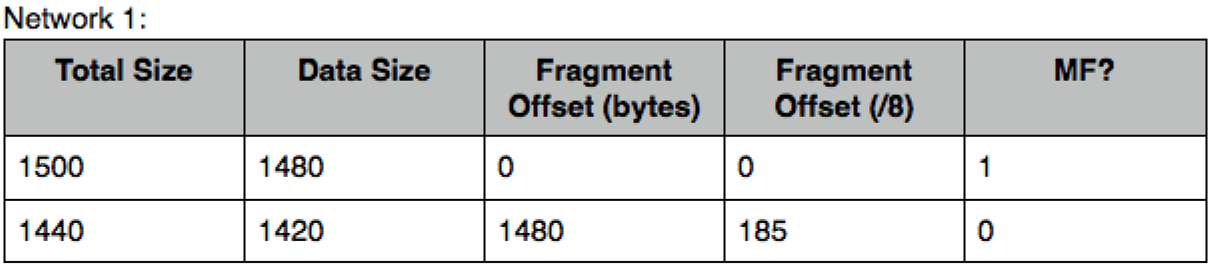
1. TCP sender starts with one segment window
2. Effective window grows exponentially with each successfully received ACK until it reaches threshold
3. After reaching threshold, effective window grows by one (additive increase)
4. If timeout happens: half threshold, time doubled, Sender returns to slow start

If the last hop is wireless, then the speed will drop to nearly 0, due to the high number of packets being lost and slow start.

**Explain why TCP is not suitable for real-time video streaming. List as many reasons as possible**

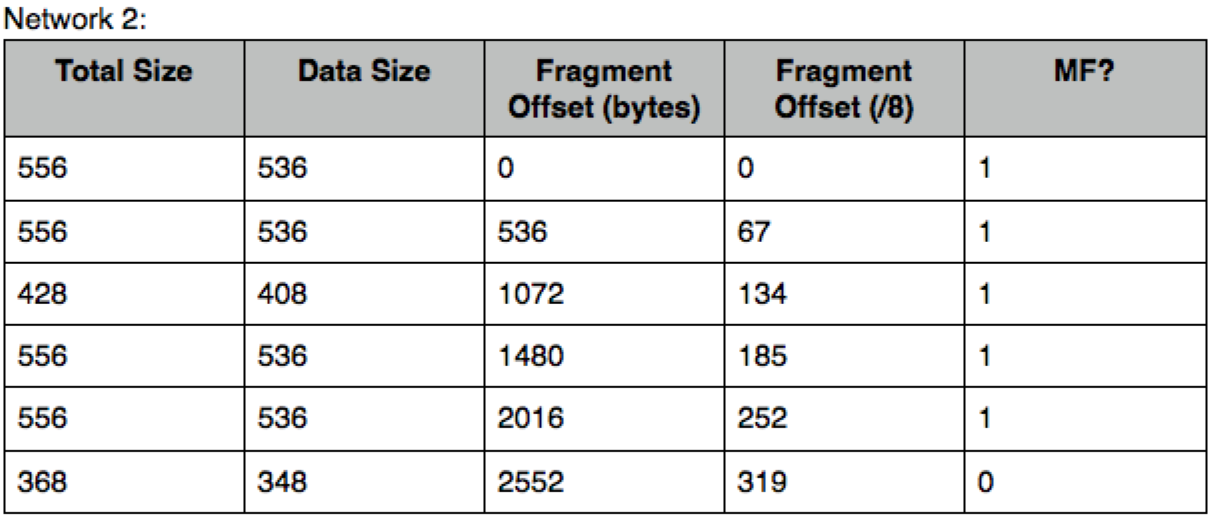
- TCP congestion control (slow start) meaning that it will take a significant length of time to achieve the required speed for video streaming
- If a packet is lost, it will return to slow start and due to real-time video streaming using a large amount of bandwidth, this is inefficient
- TCP uses error detection, meaning there will be delays
- TCP retransmissions cause skew and jitter between packets
- TCP ensures all data is received by the client and is inefficient for video streaming as it does not require older packets [c.fullelove]
- TCP is reliable meaning all packets are ACK'd or resent otherwise, this would cause delay when live streaming because of the waiting for lost packets to be retransmitted.
- IP multicast significantly reduces video bandwidth requirements for large audiences; TCP prevents the use of IP multicast.
- When using TCP all packets must be ACK'd before they are removed from the sending buffer; This coupled with a constant input stream from the data source could cause the buffer to fill quickly resulting in data being dropped by the buffer and causing parts of the live stream to never even be sent.
- TCP has a small window size and therefore arises the issue of the wrapping around of sequence numbers within the small window

**A message of 2900 bytes (application data + transport header) is to be transmitted over two IP networks. the first network has an MTU of 1500 bytes and the second network has an MTU of 560 bytes. How many fragments are expected at the network destination.**



Network 1:

| Total Size | Data Size | Fragment Offset (bytes) | Fragment Offset (/8) | MF? |
|---|---|---|---|---|
| 1500 | 1480 | 0 | 0 | 1 |
| 1440 | 1420 | 1480 | 185 | 0 |



Network 2:

| Total Size | Data Size | Fragment Offset (bytes) | Fragment Offset (/8) | MF? |
|---|---|---|---|---|
| 556 | 536 | 0 | 0 | 1 |
| 556 | 536 | 536 | 67 | 1 |
| 428 | 408 | 1072 | 134 | 1 |
| 556 | 536 | 1480 | 185 | 1 |
| 556 | 536 | 2016 | 252 | 1 |
| 368 | 348 | 2552 | 319 | 0 |

**An IP datagram that has "1" in the Protocol field is received by the IP protocol. This value represents the ICMP protocol. How is this information used by the IP protocol?**

The IP Protocol uses this information to identify the higher-level protocol carried within the datagram and in this case is passed to ICMP service.

ICMP Information is used for:

- Hosts or Routers being unreachable
- Telling the sender to **SLOW DOWN**
- Packets being too large (requiring fragmentation)
- Packets containing errors (requiring retransmission)

**Name two mechanisms used in today's Internet that ease the problem of IPv4 address shortage.**

NAT - Network Address Translation

Routers see the same thing

Violates End-To-End semantics (Problem for P2P applications)

CIDR - Classless InterDomain Routing

All Routers must be aware of the netmask used

Means changing structure of internet

**The receiving side of a TCP connection has a maximum buffer size of 50,000 bytes. The receiver has received 100,000 contiguous bytes, 70,000 of which have been consumed by the receiving application. What window size will be advertised by this side of the connection?**

AdvWindow = MaxRcvBuffer - (LastByteRcvd - LastByteRead)
= 50000 - (100000 - 70000)
= 20000

**Consider a TCP segment arriving with the following header field values:**
**Sequence number = 1000**
**Acknowledgement number = 56789**
**URG = 0**
**ACK = 1**
**PSH = 0**
**RST = 0**
**SYN = 1**
**FIN = 0**

**Write down the value of these headers for the segment that would get sent in reply to this.**

The first thing to notice is that the SYN is 1 which means it is in the TCP handshake stage. More specifically you notice that ACK is also 1 which means the current state is the ACCEPT_CONNECTION state. This means the next packet to send is from the server to the host [see diagram below]

[For future possible questions, the follow stages are]

1. SYN(SEQ = x)
2. SYN(SEQ = y, ACK = x + 1)
3. SEQ = x + 1, ACK = y + 1

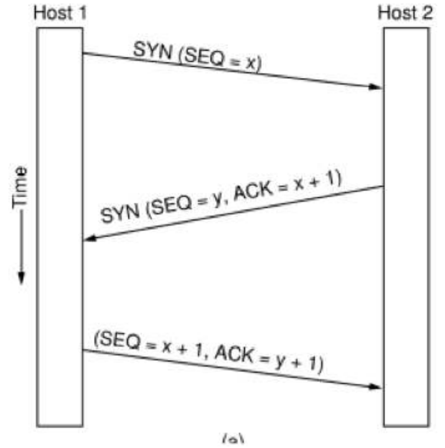
The packet in the question is two and we are sending three.

We can then read that:
x - 56788
y - 1000

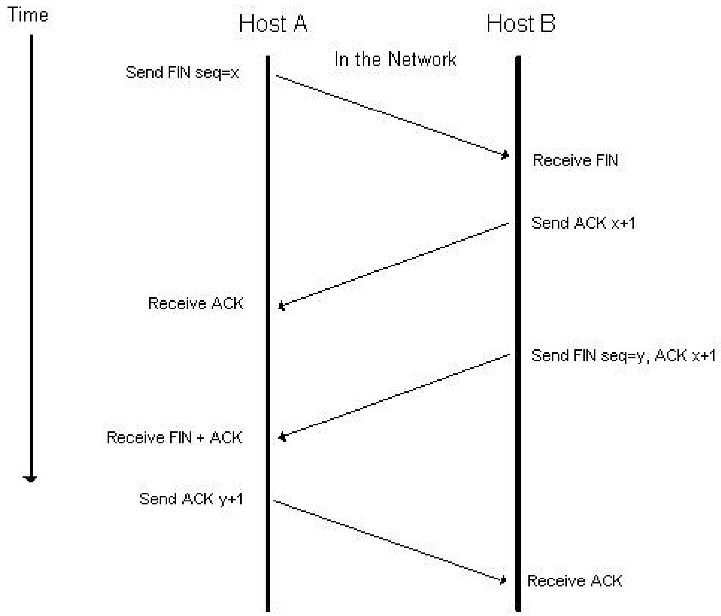
That means that in the return message:
SEQ = 56789 and ACK is 1001

**NOTE: Notice SYN is not set in packet 3**

Seq = 56789
Ack No = 1001
URG = 0
ACK = 1 /* Want to inform TCP receiver we have an Ack No set */
PSH = 0
RST = 0
SYN = 0
FIN = 0



**Consider a TCP segment arriving with the following header field values:**
**Sequence number = 3150**
**Acknowledgement number = 2621**
**URG = 0**
**ACK = 1**
**PSH = 0**
**RST = 0**
**SYN = 0**
**FIN = 1**
**Write down the value of these and all other header fields which need to be set for the segment that would be sent in reply to this. If there is more than one possibility, explain why. (4 marks)**



Sequence number = Old sequence number + 1
Acknowledgement number = 3151
URG = 0
ACK = 1

| | |
|---|---|
| PSH | = 0 |
| RST | = 0 |
| SYN | = 0 |
| FIN | = 1 |

Yes there is more than one possibility; If we still had data to send than we would stick ACK the FIN request but we would not yet terminate the connection(FIN set to 0 in reply), instead we would send the remaining data before closing the connection with the final FIN(and returned ACK).

**What is the role of a window in TCP? What does affect its size? (4 marks)**

The role of the window in TCP is to indicate the amount of data available to be received by the buffer for said TCP connection. Because TCP has a window it allows it to implement a sliding window protocol which increases the performance of TCP. The windows size is affected by how big the buffer is for the TCP connection and how much data is currently in the buffer.

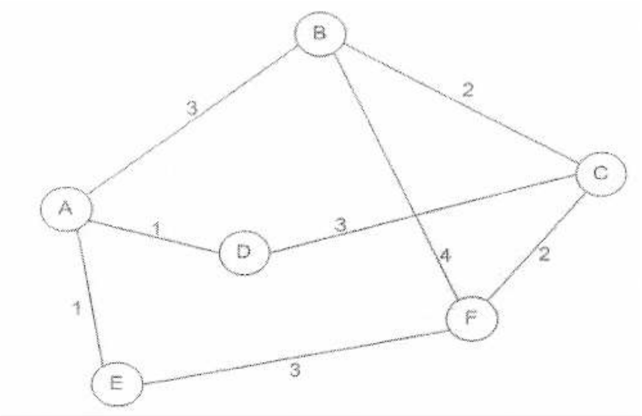
Ben: I would add that the window size is (sort of) affected by the transmission rate and read rate of the sender and receiver respectively.

**Is TCP's original 16-bit window size suitable for all kinds of networks? Explain. (2 marks)**

No. It is not suitable for high bandwidth product networks (e.g. Gigabit Ethernet) as due to the extremely high number of Frames being transmitted the sequence number could "wrap" around or allow two identical sequence numbers on the network simultaneously, which could potentially cause the receiver to accept incorrect data.

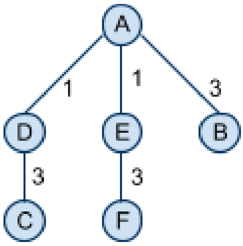
# Routing/Switching Questions

## Dijkstra’s Algorithm



**For the network shown above with the given link cost, use Dijkstra's algorithm to determine the shortest path from A to all other nodes. Show all of your working and show your result as a spanning tree rooted at A**

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| A | [0, A] | -<br>(3, A) | - | -<br>(1, A) | -<br>(1, A) | - |
| D, E | | | (4, D) | [1, A] | [1, A] | (4, E) |
| B | | [3, A] | ~~(5, B)~~ | | | ~~(7, B)~~ |
| C, F | | | [4, D] | | [4, E] | |



[DO NOT use Summative Values, DOES NOT require numbers]

**Consider the link-state routing algorithm applied to this network. show what routing information will be periodically sent by node C. Be sure to mention the recipient**

This question relates to this network, so I think they are looking for figures. i.e. (B, 2),(F,2),(D,3) along with the router ID, a sequence number and TTL, will be sent to all nodes on the network. - Carl

| A |
|---|

| |
|---|
| SEQ |
| AGE |
| B  2 |
| F  2 |
| D 3 |

**Consider the distance-vector routing algorithm applied to this network**
**Show the *initial* forwarding tables for nodes B,C,F and D (i.e. when each node is only aware of its immediate neighbours)**

Node B

| Destination node | Cost | Next Hop |
|---|---|---|
| A | 3 | A |
| F | 4 | F |
| C | 2 | C |

Node C

| Destination node | Cost | Next Hop |
|---|---|---|
| B | 2 | B |
| D | 3 | D |
| F | 2 | F |

Node F

| Destination node | Cost | Next Hop |
|---|---|---|
| B | 4 | B |
| C | 2 | C |
| E | 3 | E |

Node D

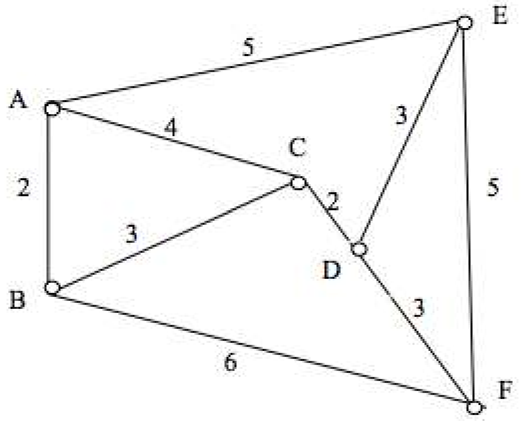
| Destination node | Cost | Next Hop |
|---|---|---|
| A | 1 | A |
| C | 3 | C |

**Show the forwarding table for node C after the first exchange of forwarding information between neighbours.**

Node C

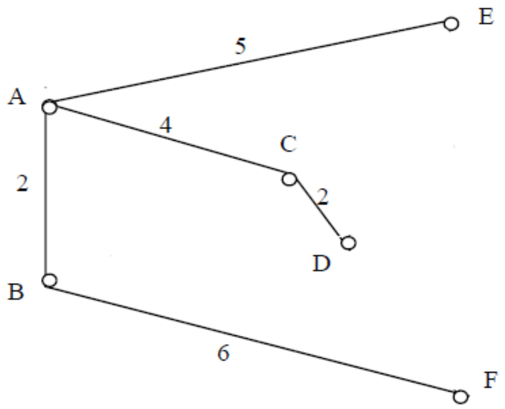
| Destination node | Cost | Next Hop |
|---|---|---|
| A | 4 | D |
| B | 2 | B |
| D | 3 | D |

| | | |
|---|---|---|
| E | 5 | F |
| F | 2 | F |



**For the network shown above (and assuming the given link costs), use Dijkstra's algorithm to determine the shortest path from A to all other nodes. Show all of your working and show your result as a spanning tree rooted at A.**

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| A | [0,A] | - | - | - | - | - |
| | | (2, A) | (4, A) | | (5, A) | |
| B | | [2,A] | | | | |
| | | | ~~(5, B)~~ | | | (8,B) |
| C | | | [4,A] | | | |
| | | | | (6,C) | | |
| E | | | | | [5,A] | |
| | | | | | | ~~(10, E)~~ |
| D | | | | [6,C] | | |
| | | | | | | ~~(9, D)~~ |
| F | | | | | | [8,B] |



**Consider the link-state routing algorithm applied to this network. Show what routing information will be periodically sent by node A. Be sure to mention the recipient.**

Sent to B, C and E (with the intent of sharing it with D and F also).

| | |
|---|---|
| A | |
| SEQ | |
| AGE | |
| B | 2 |
| C | 4 |
| E | 5 |

**Consider the distance-vector routing algorithm applied to this network.**

**i) Show the *initial* forwarding tables for nodes A, B and C (i.e. when each node is only aware of its immediate neighbours.)**

Node A

| Destination | Cost | Next Hop |
|---|---|---|
| B | 2 | B |
| C | 4 | C |
| E | 5 | E |

Node B

| Destination | Cost | Next Hop |
|---|---|---|
| A | 2 | A |
| C | 3 | C |

| | | |
|---|---|---|
| F | 6 | F |

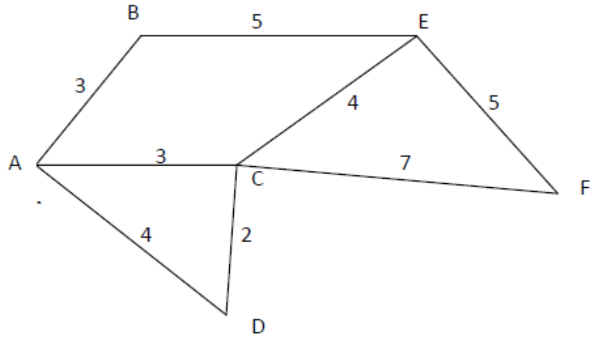
Node C

| Destination | Cost | Next Hop |
|---|---|---|
| A | 4 | A |
| B | 3 | B |
| D | 2 | D |

**ii) Show the forwarding table for node A after the first exchange of forwarding information between neighbours.**

**Node A**

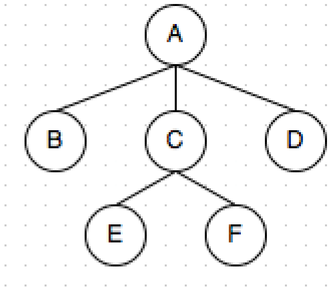
| Destination | Cost | Next Hop |
|---|---|---|
| B | 2 | B |
| C | 4 | C |
| E | 5 | E |
| D | 6 | C |
| F | 8 | B |



**For the network shown above (and assuming the given link costs), use Dijkstra’s algorithm to determine the shortest path from A to all other nodes. Show all of your working and show your result as a spanning tree rooted at A. (6 marks)**

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| A | [0, A] | -<br>(3, A) | -<br>(3, A) | -<br>(4, A) | - | - |
| B, C | | [3, A] | [3, A] | ~~(5, C)~~ | ~~(8, B)~~<br>(7, C) | (10, C) |

| | | | | | | |
|---|---|---|---|---|---|---|
| D | | | | [4, A] | | |
| E | | | | | [7, C] | ~~(12, C)~~ |
| F | | | | | | [10, C] |



**Consider the link-state routing algorithm applied to this network. Show what routing information will be periodically sent by node C. Be sure to mention the recipient. (2 marks)**

| |
|---|
| C |
| SEQ |
| AGE |
| A 3 |
| D 2 |
| E 4 |
| F 7 |

Consider the distance-vector routing algorithm applied to this network.

**a.** Show the initial forwarding tables for nodes A, B, C, and D (i.e. when each node is only aware of its immediate neighbours). (3 marks)

Node A

| Destination | Cost | Next Hop |
|---|---|---|
| B | 3 | B |
| C | 3 | C |
| D | 4 | D |

Node B

| Destination | Cost | Next Hop |
|---|---|---|
| A | 3 | A |
| E | 5 | E |

Node C

| Destination | Cost | Next Hop |
|---|---|---|
| A | 3 | A |
| D | 2 | D |
| E | 4 | E |
| F | 7 | F |

Node D

| Destination | Cost | Next Hop |
|---|---|---|
| A | 4 | A |
| C | 2 | C |

**b.** Show the forwarding table for node A after the first exchange of forwarding information between neighbours. (3 marks)

| Destination | Cost | Next Hop |
|---|---|---|
| B | 3 | B |
| C | 3 | C |
| D | 4 | D |
| E | 7 | C |
| F | 10 | C |

## Other routing/switching questions

**Which of the two routing protocols, OSPF or AODV, is more suitable for ad-hoc networks? Explain why.**

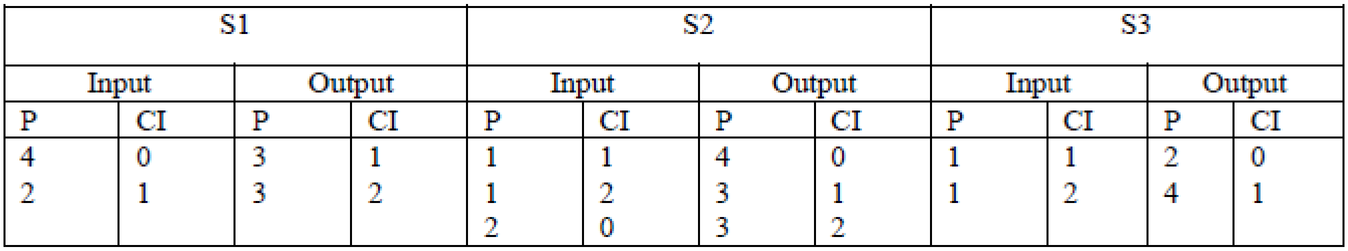
OSPF is similar to Link-State routing in that it keeps routing tables and is designed for static ad-hoc networks.

AODV is on demand, no table storage. When something needs to be sent a packet is broadcasted asking for the destination, everyone who receives this also broadcasts looking for the destination until it is found (flooding). Temporary tables are created for this and the data can be sent through to the destination.

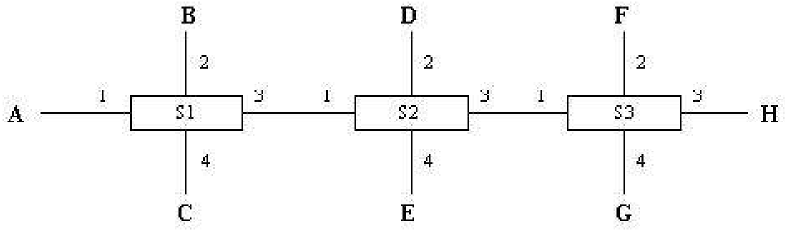
AODV is likely more suitable as ad-hoc networks tend to be very dynamic, batteries die, hosts move out of range and new hosts are added to the network constantly. It also takes into account the reduced bandwidth by not storing routing tables.

[Combined from Nathan’s Comment and the Previous Answer - Ben]
~~AODV takes into account limited bandwidth and low battery life by not storing a routing table. AODV must discover and maintain routes. (Also; A in AODV stands for Ad-Hoc!)~~

**Consider a connection-oriented routing protocol. The figure below shows the routing tables for three switches/routers and the network of these switches/routers. The table shows what <port, CI> pairs are connected to what other. List all endpoint-to-endpoint connections. (6 marks)**



| S1 | | | | S2 | | | | S3 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Input | | Output | | Input | | Output | | Input | | Output | |
| P | CI | P | CI | P | CI | P | CI | P | CI | P | CI |
| 4 | 0 | 3 | 1 | 1 | 1 | 4 | 0 | 1 | 1 | 2 | 0 |
| 2 | 1 | 3 | 2 | 1 | 2 | 3 | 1 | 1 | 2 | 4 | 1 |
| | | | | 2 | 0 | 3 | 2 | | | | |



C -> E *Explained: C > S1[4,0] > S1[3,1] > S2[1,1] > S2[4,0] > E
B -> F *Explained: B > S1[2,1] > S1[3,2] > S2[1,2] > S2[3,1] > S3[1,1] > S3[2,0] > F
D -> G *Explained: D > S2[2,0] > S2[3,2] > S3[1,2] > S3[4,1] > G

# Physical Layer Questions

**Nyquist's** $C = 2W \log_2 Mt$
**Shannon's** $C = W \log_2(1+S/N)$
**W = Bandwidth[Hz]**
**C = channel capacity, max data rate [bps]**
**S/N = Signal-to-Noise ratio**
**M = No. symbols**
**t = ?**

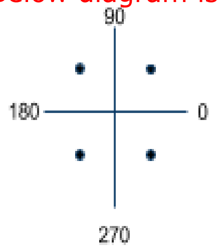
**ADSL and dial-up modems both transmit on the same physical medium. Use Shannon's theorem to explain why ADSL can achieve much higher data rates the modems**

Shannon says:
$C=W \log_2(1+S/N)$
If the same physical medium is used, then S/N is the same, so for the data rate to increase, the W value (bandwidth) must be greater in ADSL. Dialup modems make use of 3000Hz of bandwidth offered by copper telephone wires, however these copper wires can handle a significantly higher range of frequencies, which ADSL makes use of. This means ADSL has a greater available bandwidth, and thus, with a greater W value (bandwidth) in Shannon's equation, ADSL's C value (max data rate) also increases.

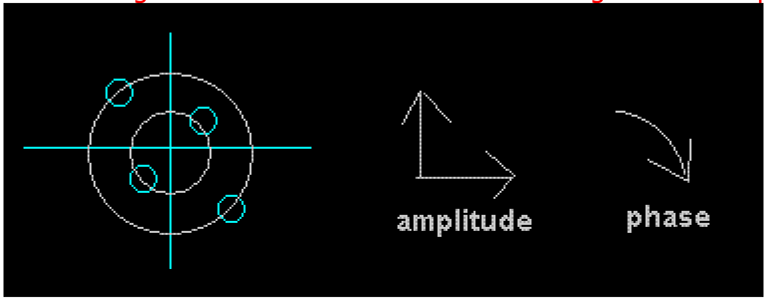
**A modem has a baud rate of 2400 symbols/s. Draw a constellation diagram that uses amplitude and phase modulation that enables a 4800 bps data rate**

4800bps = 2400 * bits per symbol
bits per symbol = 4800/2400 = 2 => 2 bits per symbol
bits per symbol = log2(number of symbols)
number of symbols = 2^(bits per symbol) = 2^2 = 4

Below diagram is INCORRECT because it changes only phase.



Below diagram is CORRECT because it changes both amplitude and phase.



**Explain why analog telephone signals are sampled at a rate of 8000 samples per second when converted for digital transmission**

Nyquist's theorem says that when converting an analog signal for digital transmission, the sample rate must be twice the highest frequency (to prevent waste and to get good reproduction of the signal), which is 4000Hz in telephone lines, as most speech occurs below this frequency.

**ADSL and dial-up modems both transmit on the same physical medium, i.e. telephone copper wire. Use Shannon's theorem to explain why ADSL can achieve much higher data rates.**

Simple:

Same medium with same environment, so S/N is the same, but W is increased due to higher frequencies, thus C increases.

Justified:

Shannon says:

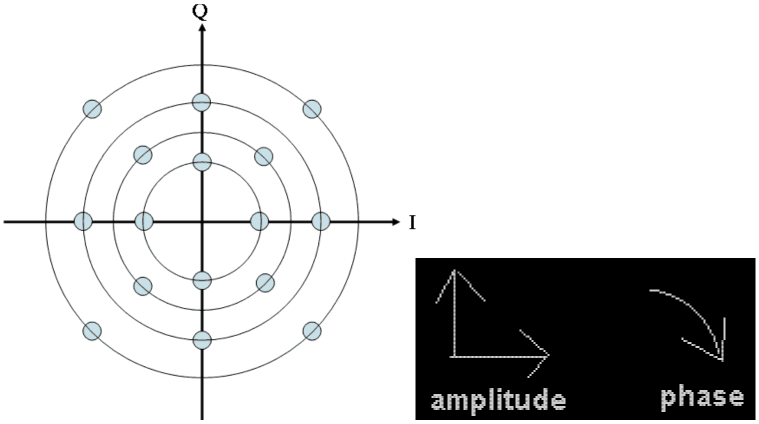
$C=W \log_2(1+S/N)$

If the same physical medium is used, then S/N is the same, so for the data rate to increase, the W value (bandwidth) must be greater in ADSL. Dialup modems make use of 3000Hz of bandwidth offered by copper telephone wires, however these copper wires can handle a significantly higher range of frequencies, which ADSL makes use of. This means ADSL has a greater available bandwidth, and thus, with a greater W value (bandwidth) in Shannon's equation, ADSL's C value (max data rate) also increases.

**Draw a modulation pattern using amplitude and phase modulation that allows sending 3 bits per baud**

No. of symbols = $2^{\text{number of bits}} = 2^3 = 8$

Sample (more than the required for this question but to help with other possible questions):



**Why may ADSL give a higher data rate for users than a cable modem?**

Contention ratios: A cable modem has a higher bandwidth but uses a shared medium and therefore the data rate is dependent on the other users using the same medium. ADSL does not have this issue as it uses different channels.

**Compare the ADSL and cable modem technology. (4 marks)**

- ADSL has a downstream rate of 8Mbps whereas cable modem has 40Mbps
- ADSL has an upstream rate up to 1Mbps whereas cable modem has 20Mbps
- ADSL Uses same telephone copper wire as dial-up modems with same SNR whereas cable modem uses the same cables for cable TV
- ADSL uses divided frequency range (giving more consistent speeds)

- Cable modem has a higher bandwidth but is a shared medium (more fluctuation in speeds)

**Explain why analog telephone signals are sampled at a rate of 8000 samples per second when converted for digital transmission. (2 marks)**

For a good reproduction of an analog signal it must be sampled at 2x the highest frequency in the signal (Nyquist theorem), sampling any higher is a waste of bandwidth.

As most human speech occurs below 4000Hz, this is chosen as the highest frequency, so 8000 samples/sec.

**Explain why early modems had low data rates like 2400 bps, 4800 bps, 9600 bps, etc. (2 marks)**

This was before channel coding was employed in modem transmissions, so errors rates were high and this limited speeds.

Once channel coding was invented and the Hamming-Distance discovered, modem speeds reached 19.2kbps.

# Data Link Layer Questions

**In CRC, what is the remainder obtained by dividing $x^7$+$x^5$+1 by the generator polynomial $x^3$+1**

$x^7 + x^5 + 1$ = 10100001
$x^3 + 1$ = 1001

CRC division is simply XORing the remainder each step of the way.
As part of CRC division, you must add the highest degree, of the generator, zeros to the end of the number to be divided. In this case, the highest degree is 3 and therefore, three zeros are added to the end of **10100001** to get **10100001000** **do not forget this step.**

***10100001000 : 1001***

```
1001
  0110001000
  0000
          110001000
          1001
          10101000
          1001
          0111000
          0000
          111000
          1001
          11100
          1001
          1110
          1001
                    0111 = x2 + x + 1
```

**Using the CRC method, what remainder is obtained by dividing**
**x6 +x4+x1+1 by the generator polynomial x3 + x +1? (5 marks)**

$x^6 + x^4 + x + 1$ = 1010011
$x^3 + x + 1$: 1011

As stated at the start of the previous question, we need to add the highest degree of the generator zeros to the end. So **1010011** becomes **1010011000**

1010011000:1011
1011
0001011000
~~000~~1011
~~000~~0000000
Remainder is 0.

**Using the CRC method, what remainder is obtained by dividing $x^7 + x^4 + x + 1$ by the generator polynomial $x^3 + x + 1$?**

$x^7 + x^4 + x + 1 = 10010011$
$x^3 + x + 1 = 1011$

As stated at the start of the previous question, we need to add the highest degree of the generator zeros to the end. So **10010011** becomes **10010011000**

10010011 before the division.
**NOTE: Crossed out 0's are not required - they're used as padding to keep everything inline.**
10010011000 : 1011
1011
00100011000
~~00~~1011
~~00~~001111000
~~0000~~1011
~~0000~~0100000
~~00000~~1011
~~00000~~001100
~~0000000~~1011
~~0000000~~0111
Therefore, the remainder is 111 OR $x^2 + x + 1$.

**Explain why not all errors are detected by the CRC method.**

Enough errors may occur to move to a different set that the given polynomial would again work out correctly for (i.e. the received word is a different polynomial but still valid a codeword).

Ben: If the Error Polynomial is a multiple of the Generator polynomial then the error can go undetected. However, clever choice of polynomials can minimize the risk of this.

**The sender sends the following frame: 10011101 which is received by the receiver as 10101101. Odd parity bit is used as the error detection method. Will this transmission error be detected? Explain why.**

No, because the parity is correct for the received frame. (i.e. both sent and receive have odd numbers of 1s).

**Find the performance of the go-back-n protocol working under the following assumptions:**

**If a question on selective repeat happens to be in it, just remember that the number of outstanding packets = (MaxSeqNo + 1) / 2**

**A)**

- frames are 600 bytes long

- data rate is 10 Mbps
- propagation delay is 5 μsec/km
- 2 bits are allocated for the seq num
- the distance is 2000km

data rate = 10Mbps = 10 * $10^6$ bps = 1 * $10^7$ bps

time to send frame = size / speed = (600 bytes * 8) / $10^7$ bps = 4.8 * $10^{-4}$ seconds

propagation delay = (5 * $10^{-6}$ seconds) * (2000km) * 2 + 4.8*$10^{-4}$ seconds = 0.02048seconds

number of outstanding packets = $2^{\text{bits allocated for sequence number}}$ - 1 = $2^2$ - 1 = 3

efficiency = (3 * 4.8*$10^{-4}$) / 0.02048 = 0.0703 = 7.03%

**B)**

- frames are 500 bytes long
- data rate is 10 Mbps
- propagation delay is 5 usec/km
- 3 bits are allocated for the frame sequence number
- the distance is 1000 km

Assume that no frames are lost. Assume that transmission time for ACK is negligible.

total propagation = time/distance * distance = 5x$10^{-6}$ * $10^3$ = 0.005 = 5ms

RTT = 5ms x 2 = 10ms

Frame send time = bits/bit-rate = (500*8)/$10^7$ = 0.4ms

Total transmission time = total propagation + frame send time = 10ms + 0.4ms = 10.4ms

Window Size: 3 bits of sequence = $2^3$ - 1 = 7

Line utilisation = window size * frame send time / total transmission time = 7 * 0.4/10.4 = 27% utilisation

Performance: 10Mbps x 27% = 2.7Mbps almost

**C)**

- frames are 200 bytes long
- data rate is 10 Mbps
- propagation delay is 5 μsec/km
- 3 bits are allocated for the frame sequence number
- the distance is 1000 km

Assume that no frames are lost. Assume that transmission time for ACK is negligible. (6 marks)

Total Propagation = time/distance * distance = 5 * $10^{-6}$ * $10^3$ = 0.005 = 5ms

Frame send time = bits/bit-rate = (200 * 8)/$10^7$ = 0.00016 = 0.16ms

RTT = total propagation * 2 = 5ms * 2 = 10ms

Total transmission time = total propagation + frame send time = 10ms + 0.16ms = 10.16ms

Window Size: 3 bits of sequence = $2^3$ - 1 = 7

Line utilisation = window size * frame send time / total transmission time = 7 * 0.16/10.16 = 11% utilisation

Performance: 10Mbps * 11% = 1.1Mbps

## Security Questions

**In a two way dialogue, how many different keys are used for encryption and decryption in symmetric key encryption?**

Only one key is used here to encrypt and decrypt the message by both parties, i.e., $K_{A-B}$

**How many different keys are used for encryption and decryption in a two-way dialogue using public key cryptography?**

We use 2 public key $K^+_A$ for encryption and 2 private key $K^-_A$ for decryption, one for each entity.

**What is the main purpose of a public key certificate. What does it say about the trustworthiness of the person/entity named in the certificate?**

Its main purpose is to bind together a public key with an identity.

It verifies that a certain public key belongs to the person/entity named in the certificate.

**Compare the SSL and IPsec protocols. Show as many similarity and differences as possible.**

1. IPsec operates at Network Layer whereas SSL operates above Transport Layer (below Application Layer, Applications must be aware)
2. IPsec is optional in IPv4, standard in IPv6 whereas SSL has to implemented and is independent of the network layer
3. SSL protects the application data whereas IPSec protects either the payload of the original packet or the entire IP packet
4. IPsec does not require a handshake but requires hosts to implement IPsec (if in Transport mode, not Tunneling mode) whereas SSL requires a handshake

**Alice creates an Internet store and advertises her public key which can be used by clients to securely send purchasing requests (including the client's credit card number) to the store. Alice will decrypt the requests using her private key.**

**i) Briefly outline problems that Alice could have with the distribution of her public key and suggest how they could be solved.**

No guarantee for a shopper that the distributed public key is Alices. By using a certificate signed by a CA the authenticity of the key can be guaranteed.

**ii) Compare Alices approach to current practices for providing security for Internet shopping. If possible, suggest how her approach might be improved.**

SSL is used to encrypt application-specific data before it is sent over a network. This would work well with Internet shopping as the application-specific data would include any payment details. SSL is a secure connection (created through a handshake) between the host and the server and is therefore more secure than publicly distributing her public key.

**Explain why both public and private key cryptography are used in current practices for providing security for Internet shopping. (4 marks)**

Public and private key cryptography work together and be useless without each other. A public key is used for the client to encrypt all data allowing for all clients to use the same public key. The private key is the only key that is able to decrypt the public-key encrypted information and is therefore known only to the shop/company. This means that any encrypted information is only decryptable by the people knowing the private key and is fully secure.

This allow the shopper's browser to encrypt their purchase information and this can only be decrypted by the shop server.

**What is the main purpose of a public key certificate? What does it say about the trustworthiness of the person/entity named in the certificate? (3 marks)**

Its main purpose is to bind together a public key with an identity. It verifies that a certain public key belongs to the person/entity named in the certificate.

They are typically issued by a Certificate Authority (CA) who are in turn, certified by a Root body of authentication.

**List the differences between Virtual Private Networks (VPN) and virtual LANs.**

VLANs are hardware based and implemented in hardware. VPNs are implemented in software and act as a tunnel between two connections whereas a VLAN is a connection accessible through lines.

VLAN:

- Partitions / Groupings of hosts on a network (Connected on the Data-Link Layer)
- Implemented through Routers/Switches that are VLAN aware (pretty sure this is software level)
- Basically, can be within a building etc.

VPN:

- Secure network between hosts that can be remote
- Works through the Internet (VLAN does not)
- Tunnels information between hosts

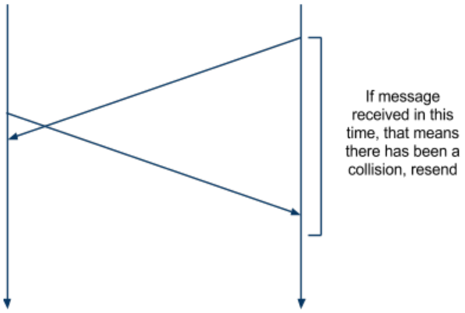
# MAC Layer Questions

**Are there any MAC layer protocols for which it makes sense to use the stop-and-wait protocol? Explain why or why not.**

Stop-and-Wait is ineffective if the RTT is high. Due to Wi-Fi having a low range, the RTT is very short. Knowing that the RTT will always be very short and that Wi-Fi has a right rate of transmission errors, the stop-and-wait protocol makes sense to be used in Wi-Fi. [Alison, David, mdn]

**Explain, using words and a time diagram, why the 10 Mb Ethernet like network(IEEE 802.3) has a minimum frame size. Discuss the applicability of the shortest frame for computers connected to hubs or switches. Explain how it was possible to keep the same shortest frame size for the 100 Mb Ethernet like network.**

It has a minimum frame size so that the sender is still transmitting in the event of a collision on the far end of the cable. This allows the sender to know the longest it should wait to tell if there has been a collision or not. The minimum frame size is selected such that the transmission time is equal to 2*propagation delay.

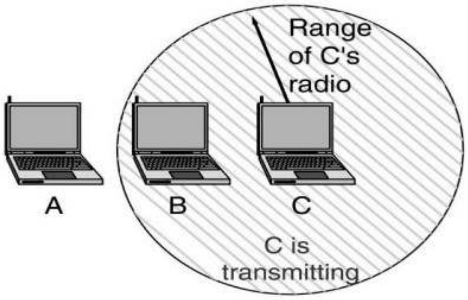

If message received in this time, that means there has been a collision, resend

It is possible to keep the same minimum packet size by reducing the propagation delay 10 times, e.g. reduce the maximum length of the cable to 1/10th of 10Mb

**Explain, using words and a time diagram, why Ethernet (IEEE 802.3) has a minimum frame size. How would the minimum frame size change if the maximum network size doubled? Explain why.**

**See first half of previous question**

If the network size doubled, the potential delay increases, thus the minimum frame size should also increase. Assuming network size doubled means t is doubled, then minimum frame size would quadruple as the sender has to wait 2 * t.



**Three stations illustrated above communicate using the IEEE 802.11 protocol. Stations A, B and C have the same transmission range. Station A and C cannot hear each other. Station C needs to send a message, as three fragments, to station B. Station A needs to send a message, as two fragments, to station B as well. Analyse the following snapshots of protocol behaviours. Show which of these snapshots represents the correct behaviours for the protocol (IE. the order of the listed operations does not violate the protocol rules) Explain why in each case.**

> **A sends RTS to B, B responds with CTS to A, A sends its first fragment, B responds with ACK, A sends its second fragment, B responds with ACK**
> OK. The original RTS will show how many fragments A will send
>
> **A sends RTS to B, C sends RTS to B**
> OK, b would then broadcast a CTS allowing A to send, and C would calculate NAV and wait until A is finished
>
> **C sends RTS to B, B responds with CTS to C, A sends RTS to B, B responds with CTS to A**
> Violates. C must send frame that the RTS was requested before A should even send an RTS, let alone have B send out a CTS
>
> **A sends RTS to C, C responds with CTS to A, A sends its first fragment to C, C responds with ACK**
> Incorrect, as A cannot see C, it could not send an RTS to C.

**Answer the following question related the network where A and C can see B but not each other: How does a station that can hear CTS and RTS know for how long it should refrain from transmitting?**

By calculating the NAV, which is how long the frame will take to be sent (including any ACKs that will need to be sent)

**An application uses TCP/IP to send a short message of 10 byes over a 10Base-T LAN. What is the length of the frame at the MAC layer? Explain why. What is the length of the frame if UDP/IP is used to send this short message? Explain why.**

TCP/IP: 20 bytes of TCP + 20 bytes of IP + 10 bytes of data = 50 bytes but min length of frame = 64 bytes. This is because minimum frame size for ethernet is 64 bytes.
UDP/IP: 8 bytes of UDP + 20 bytes of IP + 10 bytes of data = 38 bytes but min length of frame = 64 bytes due to min frame size for ethernet.

**Three stations illustrated below [refer to above three-laptop diagram] communicate using the IEEE 802.11 protocol. Station B needs to send a message, as two fragments, to station A. Station C needs to send a message, as three fragments, to station B. Analyse the following snapshots of the protocol behaviour. Show which of these snapshots represents the correct behaviour for the protocol (i.e. the order of the listed operations does not violate the protocol rules). Explain why in each case.**

**i) C sends RTS to B, B responds with CTS, C sends its first fragment, B responds with ACK.**

Correct.

**ii) B sends RTS to A, C sends RTS to B**

INCORRECT: C could hear the RTS from B, so would not follow with a RTS of it's own

POSSIBLE: If the RTS's were transmitted at the same time, or the first had not yet reached C.

**iii) B sends RTS to A, A responds with CTS, C sends RTS to B, B responds with CTS**

INCORRECT: B would not send to C a CTS as B is still sending to A

**iv) A sends RTS to C, C responds with CTS, A sends its first fragment to B, B responds with ACK**

INCORRECT: C can't send to A, A is outside of C's range

**Three stations illustrated below [refer to three laptop diagram above] communicate using the IEEE 802.11 protocol.**
**Stations A, B and C have the same transmission range. Station A and C cannot hear each other. Station C needs to send a message, as three fragments, to station B. Station A needs to send a message, as two fragments, to station B as well. Analyse the following snapshots of the protocol behaviour. Show which of these snapshots represents the correct behaviour for the protocol (i.e. the order of the listed operations does not violate the protocol rules). Explain why in each case.**

**a**. A sends RTS to C, C responds with CTS, A sends its first fragment to C, C responds with ACK

Incorrect, A anc C are out of range of one another

**b.** A sends RTS to B, C sends RTS to B

Correct, just not good!

**c.** C sends RTS to B, B responds with CTS, C sends its first fragment, B responds with ACK

Correct

**d.** C sends RTS to B, B responds with CTS, A sends RTS to B, B responds with CTS (4 marks)

Incorrect, C must must finish sending and be ACKed by B before A can RTS (NAV)

## Quality of Service

**Assume that a stream of video frames is sent over three networks that use the IntServ, DiffServ and MPLS QoS models, respectively. Please show the differences in how the stream of packets will be treated. In particular discuss flow identification, Qos requirement specification and whether QoS is guaranteed. for the latter explain why.**

I talked to the lecturer about this today and this is what she said:
IntServ needs flow identification, QoS specification and QoS is guaranteed because the person trying to send something has to talk to the routers who then make sure the can fulfill the requirements of the QoS the person has asked for. If they can, then they reserve those resources for that person, else, they deny it.

DiffServ does not have flow identification, does not guarantee QoS, it has small requirement specification, it only needs to know whether the traffic is real time or normal. It will treat real time better and give them better speeds, but if there is a lot of real time traffic then it will slow down heaps and be terrible. This is because the internet community that made this just wanted to know that their real time traffic were getting priority but they didn't care if it was guaranteed on time delivery.

MPLS almost changes routing to switching. The routers communicate and have the same routing tables, so each packet contains a label in front of it which points to the position in the routing table that will tell the router where to send it next. This means the routers do not have to search the routing table each time a packet comes in. This improves speed but doesn't guarantee QoS. It is often used with DiffServ.

**Which of the IntServ and DiffServ Quality of Service models is easier to implement in the Internet? Explain.**

- DiffServ (Differentiated Services) is scalable
- IntServ (Integrated Services) requires fundamental changes to the Internet structure
  - Routers need to all be changed to understand (requires complex software)
- DiffServ aims to provide classes in existing structure
- DiffServ's philosophy is minimal change
- DiffServ does not guarantee QoS as it does not have to reserve resources
  - Which is considerably more complicated

Answer: DiffServ is easier to implement due to less changes to the structure of the internet

**What are the main differences between DiffServ and IntServ? Show at least three differences. (3 marks)**

DiffServer does not have flow identification, it does not guarantee QoS and it only needs to know whether the traffic real time or normal. If it is real time traffic, it will give them better speeds and slow down normal traffic.

IntServ needs flow identification, QoS is guaranteed because the person trying to send something has to talk to the routers who then make sure they can fulfill the requirements of the QoS. IntServ then reserves the resources for that person.

**Which fields in the IPv6 header can be used to support provisioning of communication Quality of Service. Explain. (3 marks)**

*Traffic Class (8 bits)* 6 most significant bits are used for DiffServ

*Flow Label* (20 bits) indicates packets should stay on the same path as one another.