THE COPPERBELT UNIVERSITY

COMPUTER SCIENCE DEPARTMENT

Internet Technologies I Test one
Time allowed 2 hrs min
Answer all questions
All questions have equal marks
Date: 23rd November 2017
Prepared by Dr DB Ntalasha

Question one

a) Explain how TCP handles congestion, you should cover:

i. how the sending window size changes as a result of lost messages [2 marks]
ii. the use of retransmission timeout and how it is determined [2 marks]
iii. how routers discard datagrams as a result of increased traffic [2 marks]
iv. how deadlocks are prevented when acknowledgments are lost [2 marks]

Answer

One of the most important aspects of TCP is a mechanism for congestion control. In most modern internets, packet loss or extreme long delays are more likely to be caused by congest ion than a hardware failure. Interestingly, transport protocols that retransmit can exacerbate the problem of congest ion by injecting additional copies of a message.
To avoid such a problem, TCP always uses packet loss as a measure of congestion and responds to congest ion by reducing the rate at which it retransmits data.
TCP does not compute an exact transmission rate. Instead, TCP bases transmission on buffers. That is, the receiver advertises a window size and the sender can transmit data to fill the receiver 's window before an ACK is received.
To control the data rate, TCP imposes a restrict ion on the window size – by temporarily reducing the window size , the sending TCP effectively reduces the data rate. TCP congest ion control takes over when a message is lost. Instead of retransmitting enough data to fill the receiver 's buffer (the receiver's window size), TCP begins by sending a single message containing data. If the acknowledgement arrives without additional loss, TCP doubles the amount of data being sent and sends two additional messages. If acknowledgements arrive for those two, TCP sends four more and so on.

b) what is the difference between Direct broadcast and limited broadcast [2 marks]

Answer
Broadcast is a way to send a packet to al l the stat ions on a particular network at once. Broadcast systems al low the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This is called direct broadcasting. The directed broadcast address for a network is formed by adding a suffix that consists of all 1 bits to the network prefix. The limited broadcast refers to a broadcast on a local physical network. Limited broadcast is used during system startup by a

computer that dosed not yet know the network number. The IP limited Broadcast address is found by setting all 32 bits of the IP address to a value of 1.

Question two

a) What is the maximum number of fragments that can result from a single IP Datagram? Explain.[3 marks]

Answer

To fragment a datagram for transmission across a network, a router uses the network MTU (Maximum Transmission Unit) and the datagram header size to calculate the maximum amount of data that can be sent in each fragment and number of fragment that will be needed. The router than creates the fragments. A datagram cannot be larger than the MTU of a network over which it is sent. If a fragment eventually reaches another network that has a smaller MTU then fragment is further divided in to smaller fragments. IP does not distinguish between original fragments and sub fragments. So the maximum number of fragments from a single datagram will depend on size of datagram and MTU of the networks over which i t is sent along its path.

b) Give a brief comparison of routing and bridging. Your answer should cover topics like forwarding, layering, addressing, complexity, and scalability. [5 marks]

Answer

Bridging is layer 2 forwarding based on the MAC address. MAC addresses have a flat structure and layer 2 networks with many nodes leads to large forwarding tables. No aggregation is possible. Loops can be detected through the spanning tree protocol.

The scalability of bridging is limited since a large number of nodes results in large forwarding tables and a large amount of broadcast traffic. Bridged networks are easy to configure, easy to manage, and the equipment is cheap compared to layer 3 products.

Routing is layer 3 forwarding based on IP addresses. IP addresses can be aggregated so that forwarding tables can be kept reasonably small even for very large networks. Loops can be detected through routing protocols and TTL decrementation. Routing is more complicated to configure and manage compared to bridging, and layer 3 equipment is normally more expensive. Routing scales far better than bridging

c) What is the structure and use of internet addresses? [2 marks]

Answer

Each IP address is 32 bit long. In human language the IP addresses are written in dotted decimal notation. These are then converted to binary by the computer. Each IP address has two parts: Network identifier or a network ID and host ID. The current internet protocol standard is IPV4. The IP addresses are divided into three classes: a class A network, a class B network, and a class C network. Class A being the largest. The four digit numbers in an IPV4 address, each network of class A will have different first number, and then its network will be addressed by the rest of the three numbers, or three bytes. The IP addresses identify a machine to deliver packets and load web pages.

Question three

a) Reassembling of IP fragments at the ultimate destination is advantageous. Give reasons. [2 marks]

Answer
Routers need not bother about whether the datagram is fragment or not. The fragments may travel to the destination through different routes.

- It reduces the amount of state information in routers. When forwarding a datagram, a router does not need to know whether the datagram is a fragment.
- It allows routers to change dynamically. If an intermediate router reassembles fragments, all fragments would need to reach that router. By postponing reassembly until the ultimate destination, IP is free to pass some fragments from a datagram along a different route than other fragments.

b) How many responses does a computer expect to receive when it broadcast an ARP request? Why? [3 marks]

Answer
An ARP request message is placed in a hardware frame and broadcast to all computer on the network. Each computer receives the request and examines the IP address. The computer mentioned in the request sends a response, all other computers process and discard the request without sending a response. So response will be obtained only from the machine for which request is being sent not from the other machines on the network.

c) Suppose you wanted to establish a communication network between earth and a star light years away in space. Would Sliding Window be an appropriate protocol, in the presence of errors? What would be the recommended sending window size? Justify your answer. [2 marks]

Answer
No. The round trip delay would be several years. Therefore any protocol using retransmission is inappropriate. If you use sliding window, the only reasonable window size is one that is larger than the size of the message to be sent. otherwise, a smaller window would permit only part of the message to be sent, after which the sender would wait several years before receiving an ack that would permit the window to be advanced.

d) Explain how a specific technology uses configurable addressing in which a network interface can be assigned a specific hardware address.[3 marks] gtbk

Answer
For such networks, it is possible to choose addresses that make a closed-form address resolution possible. A resolver that uses a closed-form method computes a mathematical function that maps an IP address to a hardware address. If the relationship between an IP address and the corresponding hardware address is straightforward, the computation requires only a few arithmetic operations.

To understand why closed-form computation can be especially efficient for a network with configurable addresses, remember that both the hardware and IP addresses can be changed. Thus, values can be chosen to optimise the translation. In fact, the host portion

of a computer's IP address can be chosen to be identical to the computer's hardware address, making the translation trivial.

As an example, suppose a configurable network has been assigned the class C network number 220.123.5.0. As computers are added to the network, each computer is assigned an IP address suffix and a matching hardware address. The first host is assigned IP address 220.123.5.1 and hardware address 1. The second host is assigned IP address 220.123.5.2 and hardware address 2. The suffixes need not be sequential. If a router attached to the network is assigned IP address 220.123.5.101, the router is assigned hardware address 101. Given the IP address of any computer on the network, the computer's hardware address can be computed by a single Boolean *and* operation:

Hardware_address = ip_address & 0xff

Question four

a) Explain that the lost acknowledgement does not necessarily enforce retransmission of the packet [3 marks]

Answer

To guarantee reliable transfer, protocols use positive acknowledgement with retransmission. When receiver gets the packet an acknowledgement is sent. If an acknowledgement is lost, generally packet is retransmitted.

Retransmission can not succeed if a hardware failure has permanently disconnected the network or if receiving computer has crashed. Therefore, protocols retransmitting the messages bound the maximum number of transmissions. When the bound has been reached, the protocol stops retransmission of packet even if acknowledges is not received. So a lost acknowledgement does not necessarily enforce retransmission of packet.

b) What are the main differences between OSI and TCP/ IP reference models? Explain briefly. [4 marks]

Answer

We will be focusing only on the key differences between the two references models. Three concepts are central to OSI model: services, inter faces and protocols. OSI model makes the clear distinct ion between these three concepts.

The TCP/ IP model did not originally clearly distinguish between services, interface, and protocol. For example the only real services offered by the Internet layer are SEND IP packet and RECEIVE IP packet.

The OSI reference model was devised before the protocols were invented. This ordering means that model was not biased towards one particular set of protocols, which made it quite general.

With TCP/ IP reverse was true: the protocol came first, and the model was really just a descript ion of the existing protocols. So problem was model did not fi t for any other protocol stack.

Another difference is in the area of connectionless versus connection oriented communication. The OSI model supports both connectionless and connect ion oriented communication in network layer , but only connection oriented in the transport layer. The

TCP/ IP model has only connect ion less mode in network layer but supports both the mode in transport layer.

c) In your view, how can you implement the use of proxy in ARP? [3 marks]

Answer

Proxy ARP is the process in which one system responds to the ARP request for another system. For example, host A sends an ARP request to resolve the IP address of host B. Instead of Host B, Host C responds to this ARP request.

Question five

a) Explain how TCP/ IP decide the size of an IP fragment? [3 marks]

Answer

TCP/IP protocol uses the name IP datagram to refer to an Internet packet. The amount of data carried in a datagram is not fixed. The sender chooses an amount of data that is appropriate for a particular purpose. If size of a datagram is larger than network MTU than fragmentation is performed.

When a datagram is larger than the MTU of a network over which it is sent, the router divides the datagram into smaller pieces called fragments and sends each fragment independently. To fragment a datagram for transmission across the network, a router uses the network MTU and datagram header size to calculate maximum amount of data that can be sent in each fragment and number of fragment that will be needed.

b) Consider the following network running the distance vector routing protocol. In the diagram, vertices represent routers and edges (arcs) represent links between routers. The numerical annotation on the links represents link costs. Higher costs indicate worse links

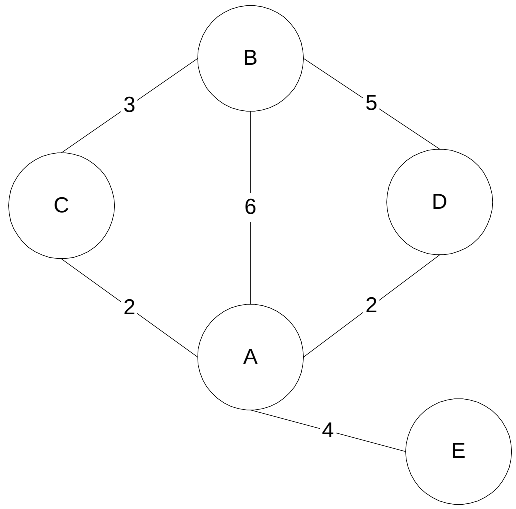
i. Show the routing table at node A when the distance vector routing algorithm stabilizes. [4 marks]

Answer

(a) Routing Table at Node A:

Destination	Next Hop	Cost
B	C	5
C	A	2
D	A	2
E	A	4

ii. Suppose the link between node A and node E fails, show the routing table at node B when the distance vector algorithm stabilizes. Show all important steps in your analysis.[3 marks]



answer

The distance vector routing algorithm never stabilizes. The failure of the link from A to E initiates a count to infinity problem since every other node relies on A to get to E.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!ALL THE BEST!!!