1)Page (260)

Mechanism – use, comments

Checksum – Used to detect bit errors in a transmitted packet

Timer – used to timeout/retransmit a packet, possibly because the packet was lost within the channel. Because timeouts can occur when a packet is delayed but not lost, or when a packet has been received by the receiver but the receiver-to-sender ack has been lost, duplicate copies of a packet may be received by a receiver

Sequence number – used for sequential numbering of packets of data flowing from sender to receiver. Gaps in the sequence numbers of received packets allow the receiver to detect a lost packet. Packets with duplicate sequence numbers allow the receiver to detect duplicate copies of a packet

Acknowledgment – used by the receiver to tell the sender that a packet or set of packets has been received correctly. Acknowledgments carry sequence number

Negative Acknowledgement – Used by the receiver to tell the sender that a packet was not received correctly. Negative ACK will typically carry the sequence number of the packet that was not received correctly

Window - the sender may be restricted to sending only packets with sequence numbers that fall within a given range. By allowing multiple packets to be transmitted but not yet acknowledged, sender utilization can be increased over a stop-and-wait mode of operation.

2) UDP Segment structure – 32 bits or 4 fields each 2 bytes = 8bytes (Page 232)

Source Port and Destination Port – Host to pass the application data to the correct process running on the destination end system

Length – specifies the number of bytes in the UDP segment header (header + data)

Checksum – used by the receiving host to check whether errors have been introduced into the segment

Application Data – contains content we are passing or receiving such as message, query, audio files etc.

3) TCP Segment structure – 20bytes and like UDP, it contains Source/Destination Port and checksum.

32-bit Sequence number field and 32-bit acknowledgment number field – (See number 1) reliable data transfer service.

16-bit Receive window – number of bytes user is willing to receive

4-bt Header Length – length of the TCP header in 32-bit words.

Options field – used when sender and receiver negotiate the maximum segment size or as window scaling factor for use in high-speed networks.

6-bit Flag field – contains Ack bit which contains an acknowledgment for a segment that has been successfully received. (see number 1 for better understanding)

4) Forwarding – Routing Page (page 337)

Forwarding – router-local action of transferring a packet from an input link interface to the appropriate output link interface.

Routing – network wide process that determines the end-to-end paths that packets take from source to destination.

Traditional approach - each router has a routing component that communicates with the routing components of other routers.

SDN Approach – remote controller computes and distributes the forwarding tables to be used by each and every router

5) Packet Scheduling/Queue management methods (page 353)

FIFO – selects packets for link transmission in the same order in which they arrived at the output link queue.

Priority – packets arriving at the output link are classified into priority classes upon arrival. Priority class typically has its own queue

Round Robin – packets are sorted into classes and a round robin scheduler alternates service among the classes.

Weighted fair queuing – arriving packets are classified and queued in the appropriate per-class waiting area. WFQ will serve classes in a circular manner

6) CIDR and IPv4 (page 364)

7)IPv6 Header (page 378)

Version – which IP version number

Traffic class – gives priority to certain datagrams

Flow label – identify a flow of datagrams

payload length – number of bytes in the IPv6 datagram

next header – identifies the protocol to which the contents of this datagram will be delivered

hop limit – the contents of this field are decremented by 1 by each router that forwards the datagram

source and destination addresses – formats of the IPv6 128-bit address

data – payload of the datagram. Removed once it reaches destination

8) IPv4 (page 358)

Version - IP protocol version of the datagram

Header length – where in the IP datagram the payload begins

Type of service – distinguish between different types of IP datagrams

Datagram length – total length of the IP datagram

Time to live – ensure that datagrams do not circulate forever

Protocol – indicates the specific transport layer protocol to which the data portion of this IP datagram should be passed

Header checksum – aids router in detecting bit errors in a received IP datagram.

Source and destination IP address – stores IP of the final destination and your IP address

Options – allow an IP header to be extended.

Data – contains content such transport layer segments or messages to be delivered.