CSC 138-03
12/17/2020
Quinn Roemer

quinnroemer@csus.edu

Short Answer

1. Application, Transport, Network, Link, & Physical Layer

2. Persistent HTTP can recieve multiple objects over the same connection, Non-persistent cannot.

3. TCP provides reliable data transfer while UDP does not.

4. DDOS stands for Distributed Denial of Service & occurs when a resource is overwhelmed with invalid requests.

5. Three duplicate ACKs

6. HTTP → Application
TCP → Transport
UDP → Transport
IP → Network
FTP → Application
SMTP → Application
DNS → Application
FDMA → Link
TDMA → Link
DHCP → Application

7. HTTP = Port 80
SMTP = Port 25
DNS = Port 53
Telnet = Port 23

8. DASH stands for Dynamic Adaptive Streaming & is used to stream videos, It works by replicating files at various encoding on distributed servers, providing the client with a manifest file allowing it to pick the best server/encoding for its bandwidth adaptively

9. A standard IP address has 32 bits. The "/21" means the 21 high-orders bits are a <u>subnet</u>

10. A MAC address has 48bits. It is portable as the address is generally linked to the hardware.

11. IP addresses are used in routing tables & MACS in switch tables.

12. Slotted ALOHA transmits frames in time slots, if a collision occurs retransmission of the colliding frame takes place in a later frame. In pure ALOHA, no timeslots are used & transmission occurs immediately with the same collision handling technique. In CSMA/CD the channel is sensed. If busy transmission is defered, else transmission occurs. If a collision occurs, transmission is aborted.

13. In Step 1: SYN bit = 1
In Step 2: SYN bit = 1 & ACK bit = 1
In Step 3: ACK bit = 1

14. Congestion controls aim is to prevent overloading the network as a whole, while flow control attempts to not overload the reciever. TCP is more fair since it has flow & Congestion control & UDP does not.

15. Packet Sniffing - Reading a packets contents over the wire.
IP Spoofing - Injecting a packet with a false source address.

Multiple Choice

1. D: SMTP uses 2 ports like FTP does
2. A: L/R
3. B: Slow-Start phase, window grows expenentially
4. C: There are no issues using it.
5. D: All of the above
6. A: The dst IP is irrevalent when it comes to routing & forwarding
7. B: Packet switching uses "store & fwd" to deliver packets
8. B: IP fragmentation is performed in both IPv6 & IPv4
9. B: Error detection
10. A: RIP & OSPF are generally used within an AS

Long Answer

1.1: A checksum is used in rdt 2.0 to detect error & a NAK is sent back to sender informing them of the error so retransmission can occur

1.2: Sequence numbers are used to avoid duplicate packets.

1.3: A timeout timer is used. If no ACK is sent within that period retransmission occurs.

1.4: Pipelined protocols such as Go-Back-N & Selective Repeat can be used.

2.1: Source IP = 111.111.111.111
Destination IP = 222.222.222.222
Source MAC = 74-29-9C-E8-FF-55
Destination MAC = E6-E9-00-17-BB-4B

2.2: Using the destination IP, the destination MAC will be exchanged for that of B & the source MAC will be exchanged for the SRC of the outgoing interface

2.3: Source IP = 111.111.111.111
Destination IP = 222.222.222.222
Source MAC = 1A-23-F9-CD-06-9B
Destination MAC = 49-BD-D2-C7-56-2A

2.4 The headers will be cached for later use (sending a reply) & the packet payload demuxed & passed to the below layer

3. Slow Start: 1, 2, 3, 7, 8, 9
Congestion Avoidance: 10-23, 25-31, 33-40
Fast Recovery: 24, 32

Packet loss at 6 detected with timeout
Packet loss at 23 detected by triple duplicate ACK
Packet loss at 31 detected by triple duplicate ACK

Ssthreash changes to ~5 at time 7
Ssthreash changes to ~11 at time 24
Ssthreash changes to ~10.5 at time 32

4. G = 1001 D = 1001 1000 and R = 3

$1001\ 1000 \cdot 2^3 = 1001\ 1000\ 000$

```
            1 0001 001
1001 ) 1001 1000 000
       1001  ↓     |
       0000        ↓
          1000
          1001
          0001
              1000
              1001
            R = 001
```

Non-Zero remainder, therefore an error has been detected & the packet recieved is not correct.

5.1: The request is sent to a DHCP server. This request is an application layer DHCP request encapsulated in UDP (transport layer), IP datagram (Network Layer), & ethernet frame Link layer

5.2: The MAC address FFF FFF FFF FFF will be used because the correct MAC address is unknown. This essentially floods the network allowing the request to be recieved by all.

5.3: The IP address translation request goes to a DNS server. This is an application layer DNS request sent through UDP (transport) layer, encapsulated in an IP datagram (Network layer) & encapsulated in an ethernet frame (Link layer)

5.4: ARP (Address resolution protocol) can be used. This is a network wide request for the MAC associated with an IP. The MAC is then sent back to the originator of the request

5.5: An HTTP (Application Layer) request is sent through TCP (Transport Layer), encapsulated in a IP datagram (Network layer), in an ethernet frame (Link layer). The transport layer protocol is different (TCP vs UDP). As a result, a 3 way handshake must occur between the client & Google's web server. This involves the client sending a SYN request, google replying with a SYNACK, & the client sending an ACK to that possibly with the first request for the server.