**2016 Question 1**

Q1(a)

|  |  |  |
| --- | --- | --- |
|  | **TCP** | **UDP** |
| **Reliable?** | Very reliable | Unreliable |
| **Delivery?** | In-order | Unordered |
| **Header?** | 20-60 bytes (src port, dest port, seq num, ack num, data offset, reserved, control flags, window size, checksum, urgent pointer, optional data) | 8 bytes (src port, dest port, length, checksum) |
| **Connection Overhead?** | Yes | No |

**For IP telephony and videoconferencing**

|  |  |
| --- | --- |
| **TCP** | **UDP** |
| Must buffer for unacknowledged segments | Missing packets don’t affect quality that much, slight \*slip of words\* as packets get lost |
| Connection dies if too many packets are lost | Faster and better for real time |
| Line becomes garbled due to too many packets trying to recover |  |

(b)

For a persistent connection, socket pairs are used, each socket pair is identified by the following..

* Source IP address
* Source port number
* Destination IP address
* Destination port number

And assigned a socket address. Once a host has received this numerical descriptor it can only then start communicating via this socket. For this reason, requests from A and B will always pass through different sockets. Although the destination port number (port 80) will be the same for A and B, the source IP address and possibly the port number will be different so would be given different socket addresses.

(c)

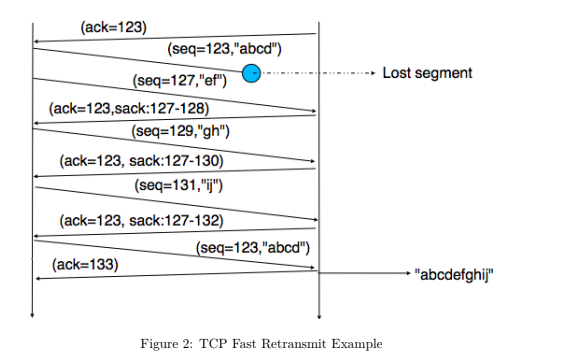
To be answered

(d)

* 65 as it is the first segment
* ACK 93 as Host B is expecting 92+1=93

(e)

Packets are sent back to back and lost packets are determined via duplicate ACKs

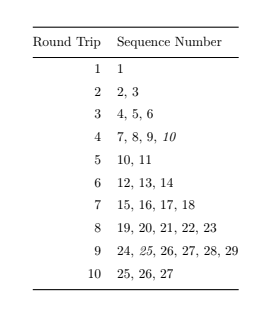


If sender received 3 ACKs from the same data commonly referred to as Triple Duplicate ACKs, resent segment of that sequence number, do not wait for the timeout as can be relatively long.

(f)

The congestion window determines the maximum amount of bytes that can be outstanding at any given time and is set to the Maximum segment size (MSS) allowed on the connection.

If all segments are received and ACKs reach the sender on time the congestion window is increased by 1 MSS. If a packet is lost the congestion window is cut in half.



**2015 Question 1**

1. - (c) NOT on course anymore

(d)

* Firstly, the client queries the ISP of the IP of [www.somesite.com](http://www.somesite.com)
* The ISP queries the root server to find IP address of .com DNS server
* ISP queries .com server to find IP address of somesite.com DNS server
* ISP queries somesite.com to find IP address of [www.somesite.com](http://www.somesite.com) DNS server
* ISP returns IP address of [www.somesite.com](http://www.somesite.com) to the client
* Client is now able to access the host.

(e)

Yes, an organization's web server and mail server can have the same alias for a host name eg. foo.com. The MX resource record type contains the host name of the mail server.

2014 Question 3

(a)

|  |  |  |
| --- | --- | --- |
|  | **TCP** | **UDP** |
| **Connection** | P2P connection oriented | Connectionless |
| **Function** | Connection based | Used for message transport and transfer |
| **Usage(Suitable for)** | High reliability transmission | Fast, efficient transmission time |
| **Reliability** | Yes, (RDT) | None |
| **Packet Ordering** | In-Order | Out-Of-Order |
| **Speed of Transfer** | Slow | Fast(best-effort) |
| **Data Flow Control** | Set window size | None |
| **Error Checking** | Yes and recovery | Yes and no recovery |
| **Handshake examples(eg. HTTP = TCP)** | 3 way handshake (SYN, SYN-ACK, ACK) | None as connectionless |
| **Examples** | HTTP, telnet, ssh, ftp, smtp | VoIP, DHCP, DNS |

(b)

Domain name system is a hierarchical decentralised naming system for resources connected to the internet. It assigns a hierarchy of names to IP addresses.

Eg. Google.ie = 209.85.203.94

* Root servers resolve top level domains (.ie, .com, .net etc.)
* TLD servers are responsible for their respective subdomains (google.ie, amazon.ie, etc.)
* Authoratize servers are responsible for their subdomains (foo.bar.net etc.)

If all of the DNS servers in the world went down at the same time, domain names would be unresolvable, however if you knew the exact IP address of the domain you could still access it.

(c)

CDN’s were built to relieve some of the pressure that is on the internet, it was never built to handle live HD video streaming, online flash sales or the demands of massive amounts of data so CDN’s work by caching links to certain content. For example if a user in Japan wanted to access a site in Milan that was having a sale before CDN’s the user in Japan would need their connection to hop around the world to get to the endpoint for the Milan site. However, now with CDN’s the CDN server nearest the user in Japan will have cached the Milan site’s content and deliver it to the Japan user without having their connection travel around the globe saving much needed time and resulting in much greater performance.

Benefits of a business using a CDN include

* Performance
* Availability
* Intelligence
* Security

(d)

To be answered

TCP or UDP for multimedia applications and why?

UDP would be the preferred method for multimedia communications as it is

* Faster
* Reliability, in order transfer and error recovery isn’t as important
* Doesn’t need to be connection oriented