Network Design and Advanced Data Security Questions

1) Layered Reference models are often used when designing the protocols of a communication network. What are the layers in the protocol stack of an Internet reference model and state the protocol data units that can be associated with each layer of the model?

Layers		Protocol Data Units
Application	-	Message
Transport	-	Segment
Network	-	Datagram
Data Layer	-	Frame
Physics	-	Bits on the Wire

2) Calculate the total time required to send a 640,000 bits file from host A to host B. Assume that all links in the network use Time Division Multiplexing with 24 slots. All links have a bit rate of 1.536Mbps. In addidtion, the network requires 200 ms to establish end-to-end circuit before host A can transmit to host B.

Speed of Connection / No of Slots = Speed Per Slot

1536000(Bits)/24 = 64000 bits/s = 64 Kbs

Size of File/Speed per Slot (Channel Speed) + Establishing Time = Time Taken

640000/64000 + 200ms = 10.2 Seconds

3) Briefly describe the two connection services that are provided to applications by the transport layer of the internet. Give an example application and specific protocol that uses each connection service.

TCP (Connection Based) : File Transfer Protocol

UDP (Connectionless) : Dynamic Name Service

4) Message segmentation is an important consideration when designing a packet switched network. State two advantages and two disadvantages of message segmentation in a packet switched network.

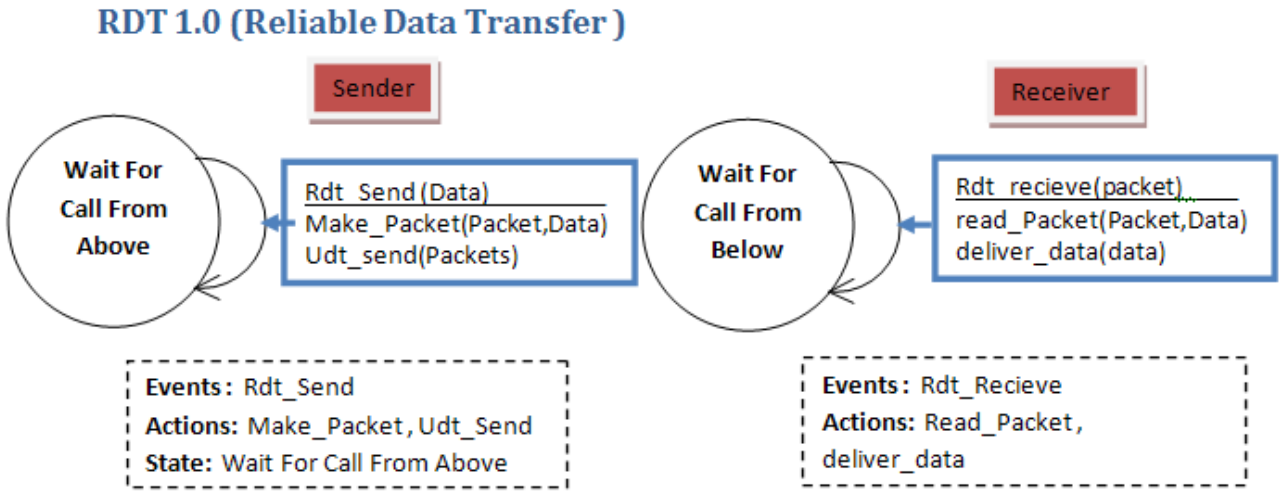
<u>Advantages</u>

- If failure of delivery , only a small chunk has to be resent not the whole message
- Segmented Packets can be sent different routes depending on congestion

<u>Disadvantages</u>

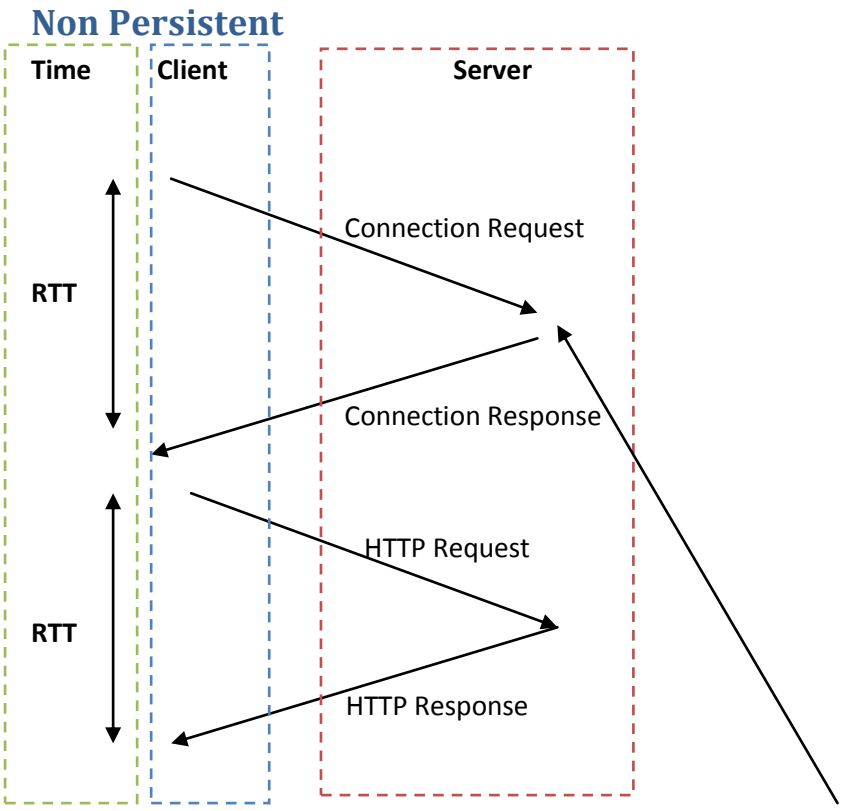
- If one segmented packet is missing , then the overall file cannot be read
- Need's a queuing and rebuilding system for segmented packets
- Nodal Processing
- More Bandwidth of Overhead

5) Finite state machines can be used when designing a reliable data transfer protocol between a sender and receiver. Assuming the simplest case of reliable data transfer over a perfectly reliable one-way data channel. Draw FSM diagrams for both the sender and receiver and clearly describe the states and transitions that are involved in the design.



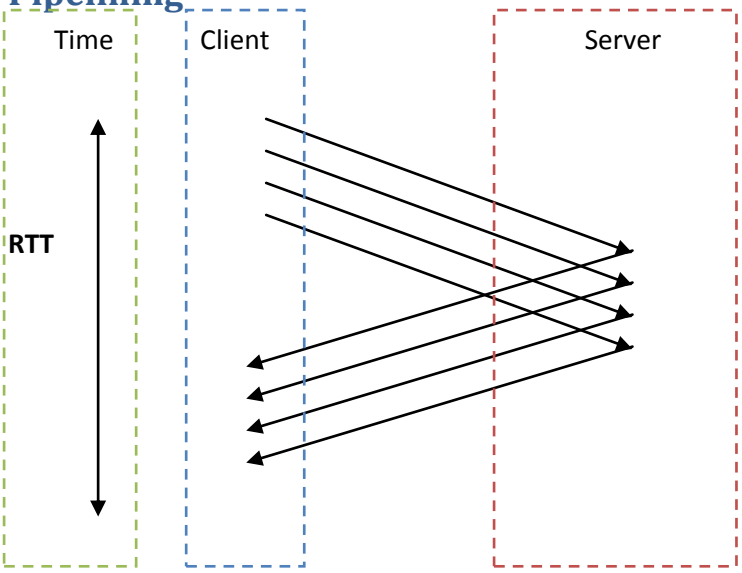
6) Describe and quantify persistent, non-persistent and pipeline connections with regard to the round trip time (RTT) of a client-server application such as HTTP -> Needs to Establish

Time Sequence Diagram



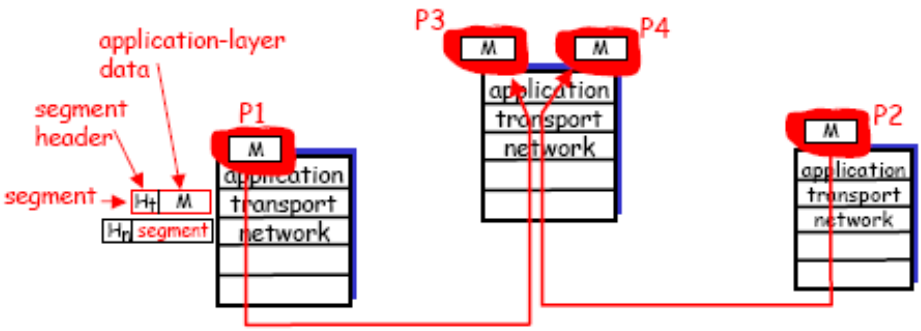
Persistent Connection is open all the time so no need for initial TCP request

Pipelining



7) Describe the essential difference between the services provided by the transport and network layers of the Internet. Briefly describe the purposes of multiplexing and de-multiplexing with regard to application layer process sockets and transport layer protocols

The network layer is responsible for end to end packet delivery which is usually performed connectionless. Whereas the transport layer is connection oriented service usually handled by host's on the sender or receiver. The network layer doesn't guarantee that the packets will arrive in the order they where sent , but the transport layer can do this by numbering the packets. Multiplexing is the method , of gathering up data from multiple application process's into a segment and header for delivery. De-multiplexing is delivering these segment's header's to the correct application layer process.



Transport = Process to Process Connection

Network = Host to Host Connection

Multiplexing and de-multiplexing are done via port numbers. When a packet arrives the OS will know what application it is using for which port number

8)A translation cipher is given by:

Plaintext : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher text : E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

Explain how the encryption procedure may be expressed in terms of modular arithmetic. Give the corresponding decrypting transformation in terms of modular arithmetic.

Encryption procedure (4 Away from A)

Cipher Mapping: $a \mapsto a + 4 \bmod 26$
Where R = X Mod M
Encryption Integer G
X = GM + R
$0 \leq \boldsymbol{r} < \boldsymbol{m}$
Key = 4

Decryption procedure

$a \mapsto a +_{26} 22$

9) Describe the role of the Key Distribution Centre (KDC) with regard to network security. Outline the steps required to establish a secure communication between two network entities A and B using a KDC.

A key distribution centre is part of a cryptosystem whose purpose is to reduce the risk of malicious Key Exchange. A user A needing to access a service on Server B with authenticate with the third party KDC as them self (A) , the KDC will check if the user (A) has a right to access the service on B, and if so the KDC will issue a key with the permissions to A . A will then take this key to the needed machine (B).

10) A Message digest can be used to create a digital signature. Explain the term message digest and describe hot it can be used with public key cryptography to provide a digital signature.

The term message digest is a number that is created with algorithms from a file to uniquely represent the file and changes that happen to it. A message digest can be used to create a digital signature of a user by hashing a message with the Sender's Private Key (K_B-)(m), this then get's sent to the intended recipient who check the message with the Sender's Public Key(K_{B+})(K_B-)(m) = m, to retrieve the message. If it decodes this proves the message was from the initial sender and no one else has signed it.