2016

April 20, 2017

Question 1

a

TCP

- Reliable: Yes
- In order delivery: Yes
- Header: 20-60 bytes (src port, dest port, seq num, ack num, data offset, reserved, control flags, window size, checksum, urgent pointer, optional data)
- Connection overhead: Yes

UDP

- Reliable: No
- In order delivery: No
- Header: 8 bytes (src port, dest port, length, checksum)
- Connection overhead: No

IP Telephony & IP Videoconferencing: UDP

- TCP
  - Must buffer for unacknowledged segments
  - Connection dies if too many packets are lost
  - Lines become garbled due to packets trying to recover
- UDP
  - Missing packets don't affect quality that much
    - Slight "slip in words" as packets get lost
  - Faster, better for real time

b

In a persistent connection, socket pairs are used. Each socket pair is identified by

- 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 communicate via this socket. This means the requests from A and B both pass through different sockets. Although the destination identifier is the same (port `80`), A and B will have different source IP addresses, and possibly using different source port numbers, so would be assigned a different socket address.

Answer 1b

c

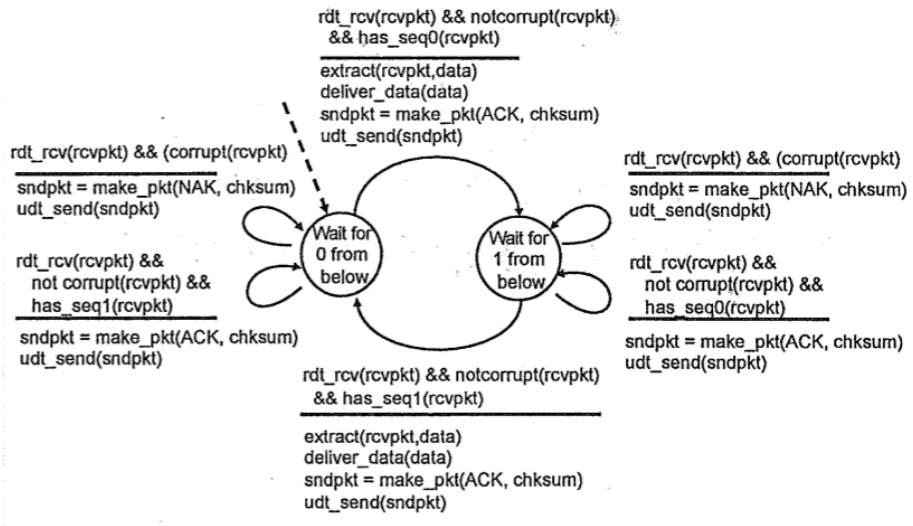

Figure 1: Received Handles Garbled ACK/NAKs

d

- $92 - 65 = 27$ bytes of data is in the first segment

  - Reference
- `ACK 65`

e

- Packets are sent back to back
- Lost segments are detected via duplicate ACKs

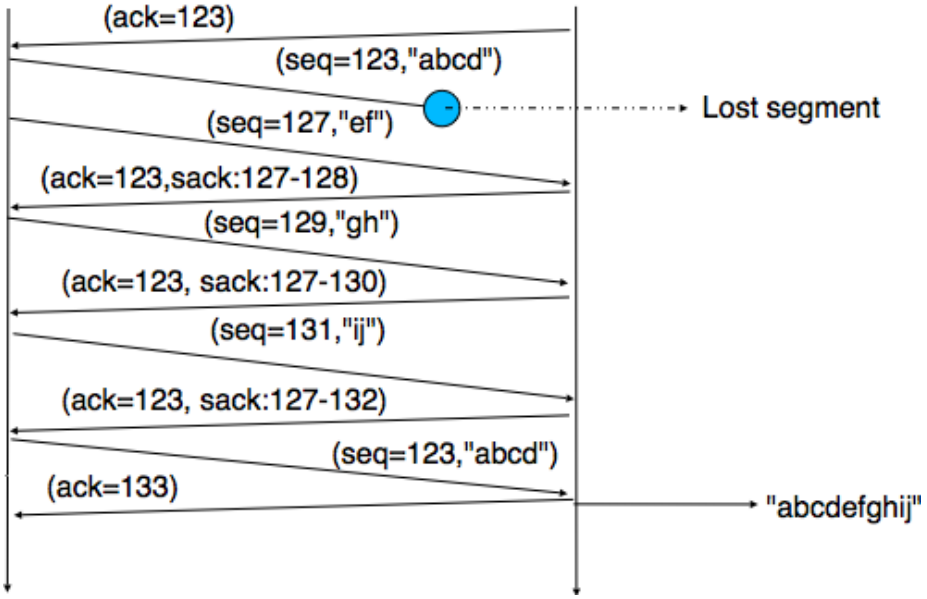

Figure 2: TCP Fast Retransmit Example

- If sender receives 3 ACKs from the same data ("Triple Duplicate ACKs"), resent segment of that sequence number
  - Do not wait for timeout as often relatively long

f

Congestion window determines the number of bytes that can be outstanding at a given time and is set to the maximum segment size (MSS) allowed on the connection. If all the segments are received and the acknowledgements 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.

Round Trip	Sequence Number
1	1
2	2, 3
3	4, 5, 6
4	7, 8, 9, *10*
5	10, 11
6	12, 13, 14
7	15, 16, 17, 18
8	19, 20, 21, 22, 23
9	24, *25*, 26, 27, 28, 29
10	25, 26, 27

Reference

Question 2

a

`HTTP` is an application protocol for transfering hypertext, such as `HTML`. It is a request-response protocol in the client-server computing model. It was designed to permit intermediate network elements to improve or enable communications between clients and servers.

A stateless protocol means that the server maintains no information about past client requests.

b

Cookies maintain the state at the sender/receiver over multiple `HTTP` transactions. They have six parameters

- Name of the cookie
- Value of the cookie
- Expiration date of the cookie
- Path the cookie is valid for
- Domain the cookie is valid for
- The need for a secure connection

This allows sites to identify the user so that they can store information. In the case of the e-commerce website, it can keep a record of purchase history.

c

- Access link rate = $15Mbps$
- LAN rate = $100Mbps$
- Avg Object Size = $960,000bits = 0.96Mb$
- Avg Request Rate = $15r/s$
- RTT: $2s$

i

$\Delta = \frac{\text{avg object size}}{\text{access link rate}} = \frac{0.96}{15} = 0.064s/r$

B = $15r/s$

Avg Access Delay: $\frac{\Delta}{1-\Delta \text{B}} = \frac{0.064}{1-(0.064\times 15)} = 1.6s$

Avg Response Time: $1.6 + 2 = 3.6s$

ii

Miss rate = 0.4

Avg Access Delay: $\frac{\Delta}{1-\text{Miss Rate}\Delta \text{B}} = \frac{0.064}{1-(0.4\times 0.064\times 15)} = 0.104s$

Avg Response Time: $0.104 + 2 = 2.104s$

Total Response Delay: $0.6 \times 0 + 0.4 \times 2.104 = 0.842s$

Answer 8

d

1. Client queries ISP for IP of `somesite.com`
2. ISP queries root server to find IP address of `.com` DNS server
3. ISP queries `.com` server to get IP of `somesite.com` DNS server
4. ISP returns IP address of `somesite.com` to client
5. Client can now access that host

Reference

e

If Alice becomes one of Bob's top-four providers, he will reciprocate if there is a chunk that she is missing.

Every 30 seconds, peers are selected at random. This can provide other peers with chunks when they have nothing to upload and they can begin transfering chunks to other peers.

Question 3

a

Components of a block cipher are

- Deterministic algorithm
- Operates on a fixed-length group of bits (the block)
- Uses a key

The Vigenere Cipher:

- Pick a key
- Build a poly-alphabetic cipher
  - Write the key with a letter per row
  - Begin writing the alphabet starting at that letter and wrap around

Example: key = BLOCK

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

- Repeat your key for the length of the plaintext
- For a given letter in the repeated key, go to the corresponding row in the square
- For a given letter in the plaintext, go to the column where that letter should be
- This is your cipher letter

Example:

- Plaintext: GIVEMEAFIRST
- Key: BLOCKBLOCKBL
- Ciphertext: HTJGNPCGTFUD

b

Electronic code book mode encodes each 64-bit block independently. This causes repetitive part-blocks of ciphertext to emerge, or the information can be replicated. For example, a repeated request for withdrawal of $1bn could be made, or blocks can be moved around, such as swapping bonuses in an encrypted spreadsheet.

For cipher block chaining, the plaintext is XOR'd with an initialisation vector before being encrypted. The result of this is then passed into the next 64-bit block to be XOR'd against that before being encrypted. This make each ciphertext block dependent on all the plaintext blocks processed up to that point.

This means that parts of the requests can't be shifted around, since the cipher at a given point is dependent on the previous cipher. The initialisation vector also prevents repeated requests as this value changes each time.

c

A group G is cyclic if it contains an element a which can generate the entire group, i.e. $\text{ord}(a) =\mid G \mid$

A primitive element of group G is an element that can generate the entire group.

$a^{10} = 2014 \mod 10 \equiv 1 \mod 11$, i.e. $\text{ord}(a) = 10 =\mid \mathbb{Z}_{11}^* \mid$

$a^1 = 2, a^2 = 4, a^3 = 8, a^4 = 16 \equiv 5 \mod 11, a^5 = 32 \equiv 10 \mod 11, a^6 = 64 \equiv 9 \mod 11, a^7 = 128 \equiv 7 \mod 11, a^8 = 256 \equiv 3 \mod 11, a^9 = 512 \equiv 6 \mod 11, a^{10} = 2014 \equiv 1 \mod 11$

2 is a primitive element of $\mathbb{Z}_{11}^*$, which is a cyclic group.

d

- $p = 467$
- $\alpha = 2$
- $a = 228$
- $b = 57$

1. $A \equiv \alpha^a \equiv 4.313591467 \times 10^{68} \mod 467 = 394$
    - This is Alice's public key
    - Sent to Bob
2. $= B \equiv \alpha^b \equiv 1.441151881 \times 10^{17} \mod 467 = 313$
    - This is Bob's public key
    - Sent to Alice
3. $B^a \mod 467 = 206$
4. $A^b \mod 467 = 206$

i.e. $(\alpha^a)^b \mod p = (\alpha^b)^a \mod p$

- Trudy intercepts Alice's public key and sends hers to Bob
- Trudy generates the shared key between herself and Bob
- Trudy does the same for Bob's public key to Alice.
- She can now access and modify messages between Bob and Alice

Reference

e

1. Client sends list of algorithms it supports and a client nonce
2. Server chooses algorithm and sends back choice, certificate and server nonce
3. Client verifies certificate, extracts server's public key, generates a `pre_master_secret`, encrypts it with the server's public key and sends that to the server
4. Client and server compute encryption and MAC keys from `pre_master_secret` and nonces
5. Client sends a MAC of all handshake messages
6. Server sends a MAC of all handshake messages

Message Authentication: Bob wants to ensure messages originally came from Alice

Message Integrity: Bob wants to ensure messages from Alice haven't been changed

The nonce is used to prevent against replay attacks. Trudy can't attempt to use the same messages that were used in the previous connection as a new key will be generated with unique nonces.