EE 3650 **Introduction to Computer Networks** (Total 100 points.) June 21, 2010.

1) (TCP, 20%) Please be brief in answering the following questions.
   a) (2%) In order to support multiple application processes, what are the 4-tuples used as a TCP demux key?
   b) (2%) Describe how TCP uses the AIMD algorithm for congestion control?
   c) (2%) Why do we need the slow start mechanism in AIMD?
   d) (2%) Since TCP is full-duplex, what the two main fields in a TCP header are needed in order to keep packets to be transmitted and received in-order?
   e) (2%) Draw the timeline of the three-way handshake algorithm used in TCP.
   f) (2%) Figure 1 is the state transition diagram of TCP. Please trace the *normal* three-way handshake of both client and server on Figure 1.
   (Please **plot on the graph directly** and **send this sheet back** with your name and your student number.)

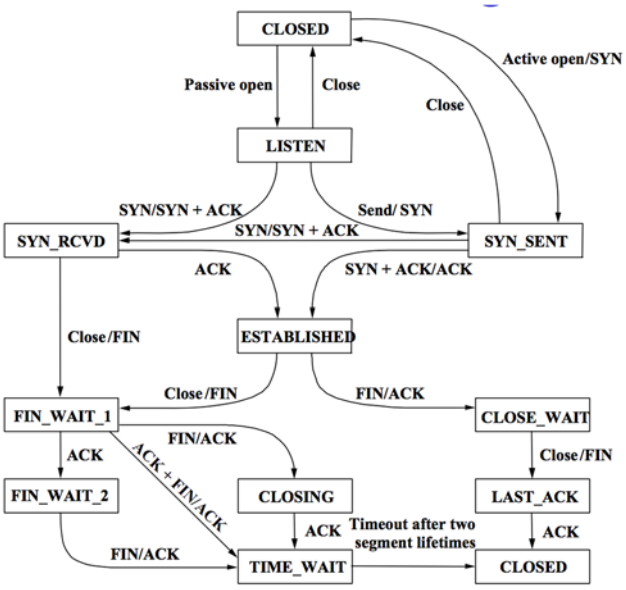


Fig 1. State Transition Diagram of TCP

   g) (2%) Give a reason why TCP has to estimate RTT.
   h) (2%) How does TCP compute AdvertisedWindow? (Hint: use the following pointers and parameters: MaxRcvBuffer, MaxSendBuffer, LastByteRead, NextByteExpected, LastByteRcvd, LastByteAcked, LastByteSent and LastByteWritten.)
   i) (2%) In TCP, how to solve the silly window syndrome problem? Silly window syndrome: If the sender aggressively fills an empty container as soon as it arrives.
   j) (2%) Describe how RED is used in conjunction with TCP to avoid synchronized backoff?

2) (Queuing disciplines and QoS, 10%)
   a) (2%) Describe briefly what a priority queue is.
   b) (2%) Suppose that packet *i* with packet length P_i arrives at the router at time A_i. If the time stamp of packet $i-1$ is F_{i-1}, find the time stamp F_i for packer *i* under the *fair queuing* policy.
   c) (2%) Describe the difference between admission control and policing.
   d) (2%) Describe what RSVP does (including the PATH message and the RESV message).
   e) (2%) Describe briefly how self-clocking is used in TCP?

3) (Security, 14%)
   a) (2%) How can a RSA algorithm be used for digital signature?
   b) Describe the following Internet security attacks.
      i) (2%) Playback attack.

ii) (2%) Man-in-the-middle attack.

c) Answering the following problems for authentication.
   i) (2%) What is *nonce* ?
   ii) (3%) Figure 2 is the timeline of the synchronized public-key authentication. Please explain this figure briefly.
   iii) (3%) Figure 3 is the timeline of the asynchronized public-key authentication. Please explain this figure briefly.

4) (JPEG and MPEG, 6%)
   a) (2%) Consider the DCT(Discrete Cosine Transform) in JPEG, after the transform, it has two parts: the low spatial frequency and the high spatial frequency, which one is more essential? Why?
   b) (2%) In JPEG, which step or steps will lose information?
   c) (2%) There are three kinds of frames in MPEG. Which one of them can be decoded independently?

5) (Application, 10%)
   a) (2%) What does a DNS server do?
   b) (2%) What is the main difference between HTTP 1.0 and HTTP 1.1?
   c) (2%) The original design for e-mails only allows transmitting ASCII characters. Describe how the extended design allows e-mails to transmit multimedia data.
   d) (2%) What is the protocol H.323 designed for?
   e) (2%) Describe briefly how consistent hashing works.

6) (LZ coding, 10%)
   a) (5%) Encode the following sequence using the Lempel-Ziv (LZ) algorithm.
   0101100101110100100010001111001010011000
   Do not bother to put the sequence into its binary form, but simply state it as a sequence of pairs in the format (index, additional bit).
   b) (5%) Consider the following LZ encoded binary sequence.
   0000100011001010000000100001100100001111
   Suppose the indexes are encoded using 4 bits. Please decode it to find the original sequence.

7) (Huffman coding, 10%)
   a) (5%) A sequence of data contains five symbols S_1, S_2, S_3, S_4, and S_5. Suppose that S_1 appears in the data with probability 0.3, S_2 appears in the data with probability 0.25, S_3 appears in the data with probability 0.2, S_4 appears in the data with probability 0.15, and S_5 appears in the data with probability 0.1. Use the Huffman coding to represent these five symbols. (Describe every step in details.)
   b) (5%) Consider a new sequence contains only three symbols S_1, S_2, and S_3 with probabilities 0.5, 0.3 and 0.2 respectively. Now, for achieving better effieciency, each two symbols are concatenated into a new symbol. Use the Huffman coding to represent these symbols. (Describe every step in details.)

8) (Diffie-Hellman key agreement, 5%)
   Consider two (publicly known) parameters 2 and 5. Suppose Bob selects 3 as his secret number and Alice selects 2 as her secret number.
   a) (2%) What number should Bob send to Alice under the Diffie-Hellman key agreement algorithm?
   b) (3%) What is the common secret number (key) between Bob and Alice under the Diffie-Hellman key agreement algorithm?

9) (RSA and security, 15%)
   a) (5%) Consider two primes $p = 3$ and $q = 7$. Choose an encryption key $e = 5$. Find the decryption key d in RSA.
   b) (5%) Consider a message $M = 3$. Find the encrypted message C by using the encryption key e in RSA.
   c) (5%) Show how you decrypt C to get $M = 3$.

Answer :

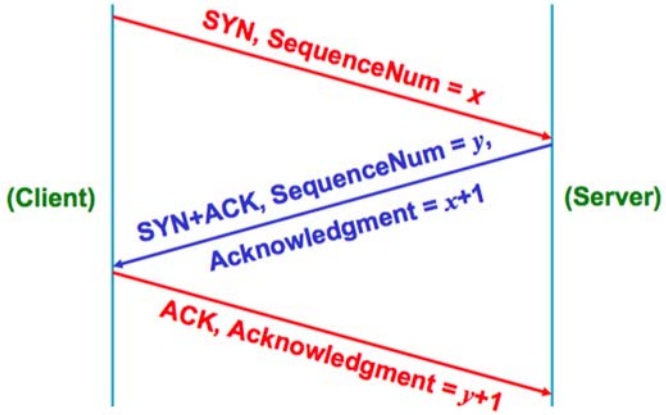
1a. source IP, source port, destination IP, destination port

1b. Additive Increase:
Every time the source successfully sends a CongestionWindow's worth of packets, it adds the equivalent of one packet to CongestionWindow.
Multiplicative Decrease:
Each time a timeout occurs, the source sets CongestionWindow to half of its previous value.

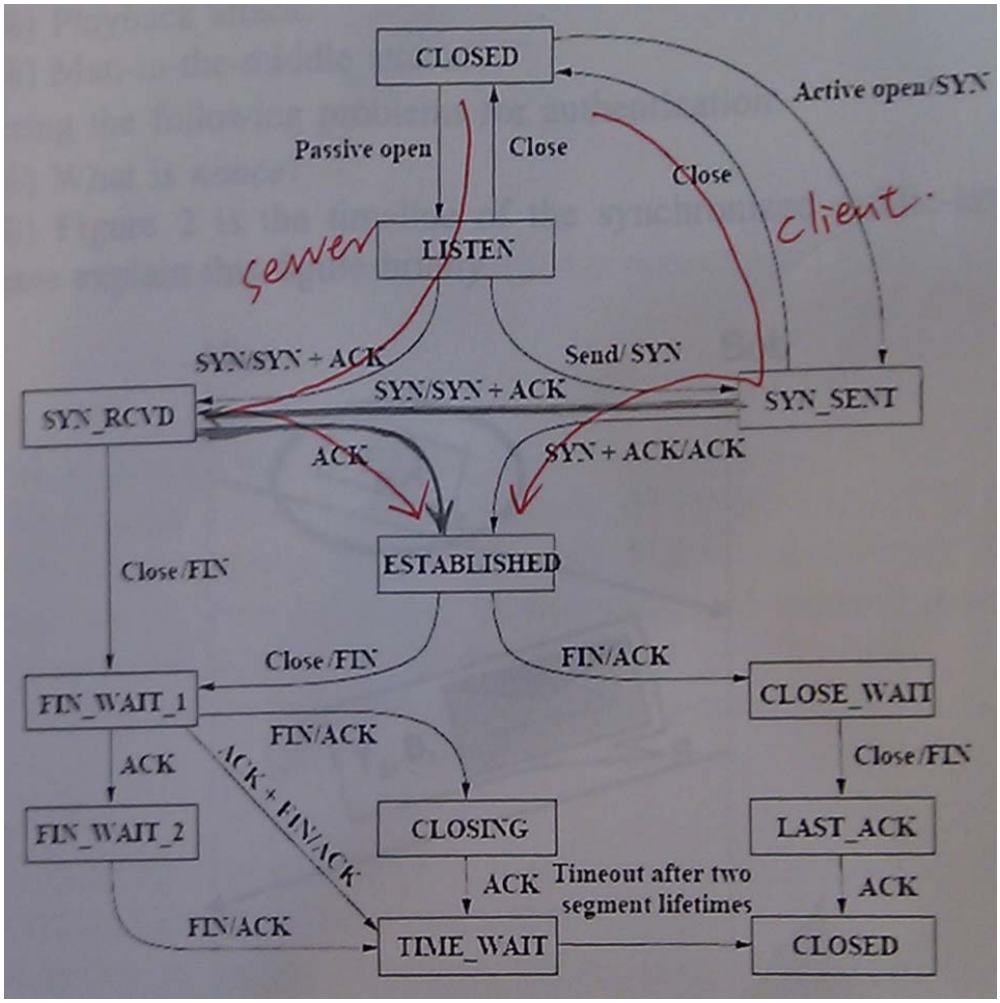
1c. The AIMD takes too long to ramp up a Source connection from its start to the available bandwidth. Increase the congestion wimdow exponentially rather than linearly.

1d. Acknowledgment and AdvertisedWindow

1e.



1f.



1g. TCP sets adaptive retransmit timeout as a function of the RTT it expects between the two ends of the connection.

1h. Rather than having a fixed-size sliding window, the receiver advertises a window size to the sender.
AdvertiseWindow = MaxRcvBuffer –((NextByteExpected – 1) – LastByteRead)

1i. Some mechanisms are also introduced to coalesce small containers. The receiver can do this by delaying ACKs, sending one combined ACK rather than multiple smaller ones. Reply a large window size.

1j. Rather than wait for queue to become full, drop each arriving packet with some drop probability whenever the queue length exceeds some drop level.

2a. Make each packet with priority (carried in the IP Type of Service (TOS) field)
– The router always transmits packets out of the highest- priority queue if the queue is nonempty
– Then moves on to the next priority queue
– Within each priority, packets are still FIFO

2b. $F_i = \max(F_{i-1}, A_i) + P_i$

2c. Admission control:
looks at the TSpec and RSpec of the flow and tries to decide if the desired service can be provided
– Given the currently available resources
– Without causing any previously admitted flow to receive worse service than it had requested
Policing:
is a function applied on a per-packet basis to make sure that a flow conforms to the TSpec that was used to make the reservation
– There are several options, the obvious one being to drop offending packets
– Another option is to drop the offending packets first if any packets are needed to drop

2d. RESV:
The receiver needs to know what traffic the sender is likely to send (to make an appropriate reservation)
PATH:
It needs to know what path the packets will follow (to establish a reservation at each router on the path)

2e. By using ACKs to pace the transmission of packets

3a. Encrypt message with own private key for digital signature and encrypt again with receiver's public key.

3b. (Not in the teaching content of 2015)
- Can generate "raw" IP packets directly from application, putting any value into IP source address field
- receiver can't tell if source is spoofed m
- e.g.: C pretends to be B

3c. i. (Not in the teaching content of 2015) Algorithm combinations

ii.
- In the first protocol, Alice and Bob's clocks are synchronized
- Alice sends Bob a message with a timestamp and her identity in plaintext plus her digital signature
- Bob uses the digital signature to authenticate the message, and the timestamp to verify its freshness
- Bob sends back a message with a timestamp and his identity in plaintext, and a new session key encrypted by Alice's public key, all digitally signed
- Alice can verify the authenticity and freshness of the message

iii.
- The second protocol does not rely on clock synchronization
- Alice sends Bob a digitally signed message with TA and A
- Bob cannot be sure that the message is fresh, since their clocks are not synchronized
- Bob sends back a digitally signed message with TA, TB and B
- Alice can verify the freshness of Bob's reply by comparing her current time
- Alice sends Bob back a signed message with TB and an encrypted new session key
- Bob can verify the freshness of Alice's reply

4a. Low spatial frequency, high-frequency coefficients are increasingly unimportant to the perceived quality of image.
4b. Quantization
4c. I frames

5a. DNS maps domain names into IP-addresses.
5b. HTTP 1.0 established a separate TCP connection for each data item retrieved from server while HTTP 1.1 allows persistent connections.
5c. MIME uses a straight forward encoding of binary data into the ASCII encoding data. This encoding method is called base 64, which map every 3 bytes of the original data into 4 ASCII characters.
5d. H.323 is designed as a protocol for Internet telephony.
5e. Hash server would return the closest match to the URL and only local mapping changes after adding or removing servers.

6a. parsed source:
0 1 01 10 010 11 101 00 100 0100 011 110 0101 001 1000
index:
0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111
codeword string:
(0000,0) (0000,1) (0001,1) (0010,0) (0011,0) (0010,1) (0100,1) (0001,0) (0100,0) (0101,0) (0011,1) (0110,0) (0101,1) (1000,1) (1001,0)
6b. index:
00001 00011 00101 00000 00100 00110 01000 01111
0001 0010 0011 0100 0101 0110 0111 1000
1 11 111 0 110 1110 00 001
answer:
1 11 111 0 110 1110 00 001

7a.

8 $p = 2$, $g = 5$, Alice's key = 2, Bob's key = 3
8a. n = $g^a \bmod p$
$= 5^3 \bmod 2$
$= 125 \bmod 2$
$= 1$
8b. secret key = $g^{ab} \bmod p$
$= 5^{2*3} \bmod 2$
$= (5^2 \bmod 2)^3 \bmod 2$
$= 1$

9. $n = p*q$
9a. $de \bmod ((p-1)*(q-1)) = 1$
$d5 \bmod 12 = 1$
⇨ $d = 5$
9b. $C = M^e \bmod n$
$= 3^5 \bmod 21$
$= 12$
9c. $M = C^d \bmod n$
$= 12^5 \bmod 21$
$= 3$