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

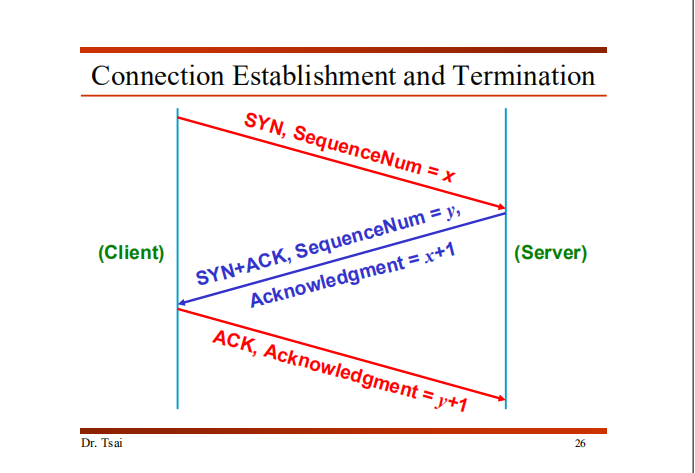
1. (TCP, 20%) Please be brief in answering the following questions.
2. (2%) In order to support multiple application processes, what are the 4-tuples used as a TCP demux key?
3. (2%) Describe how TCP uses the AIMD algorithm for congestion control?
4. (2%) Why do we need the slow start mechanism in AIMD?

Increase the congestion window rapidly from a cold start.

1. (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?

SequenceNum, Acknowledgment.

1. (2%) Draw the timeline of the three-way handshake algorithm used in TCP.



1. (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.)

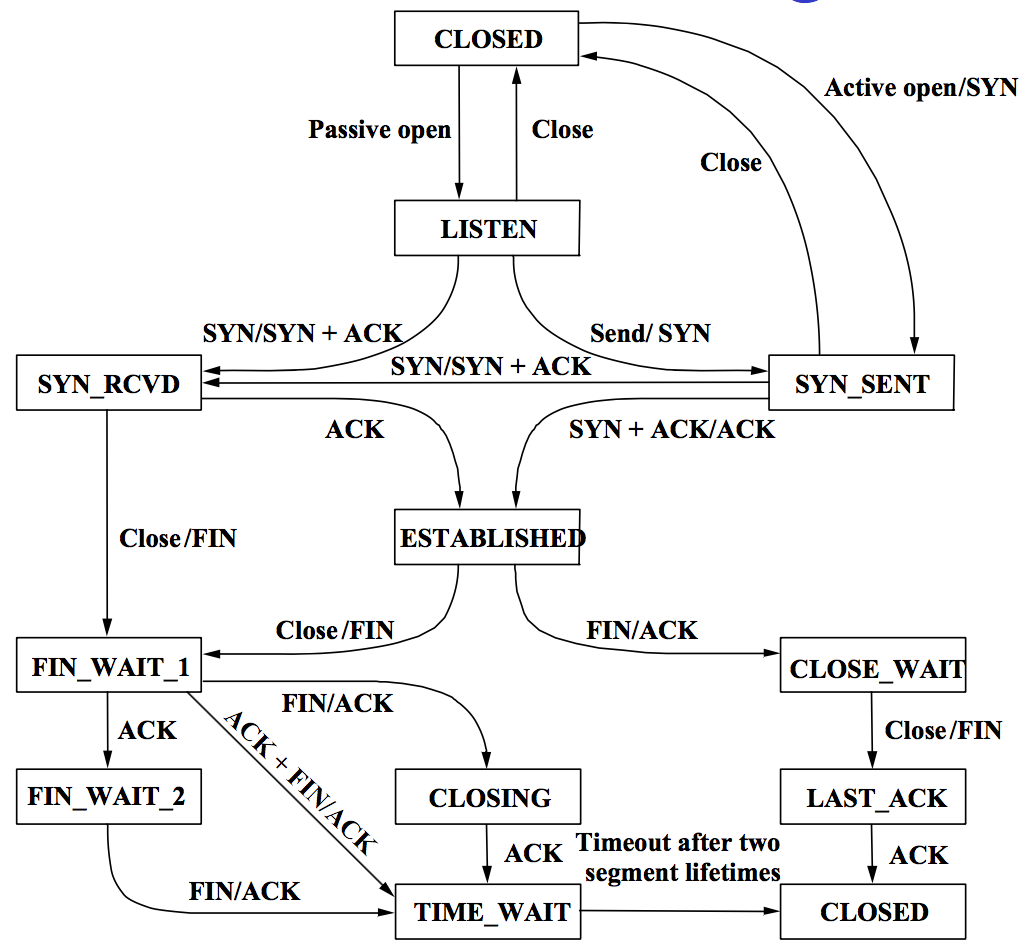
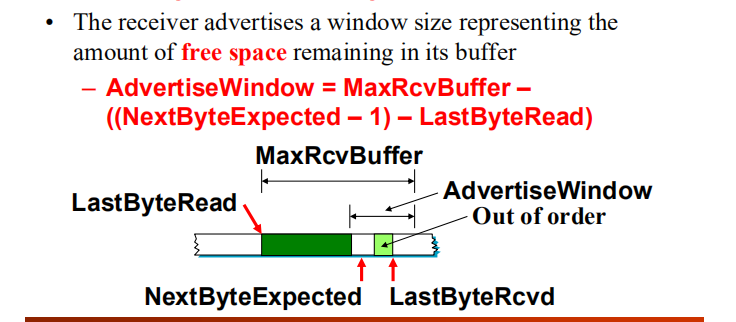


Fig 1. State Transition Diagram of TCP

1. (2%) Give a reason why TCP has to estimate RTT.
2. (2%) How does TCP compute AdvertisedWindow? (Hint: use the following pointers and parameters: MaxRcvBuffer, MaxSendBuffer, LastByteRead, NextByteExpected, LastByteRcvd, LastByteAcked, LastByteSent and LastByteWritten.)



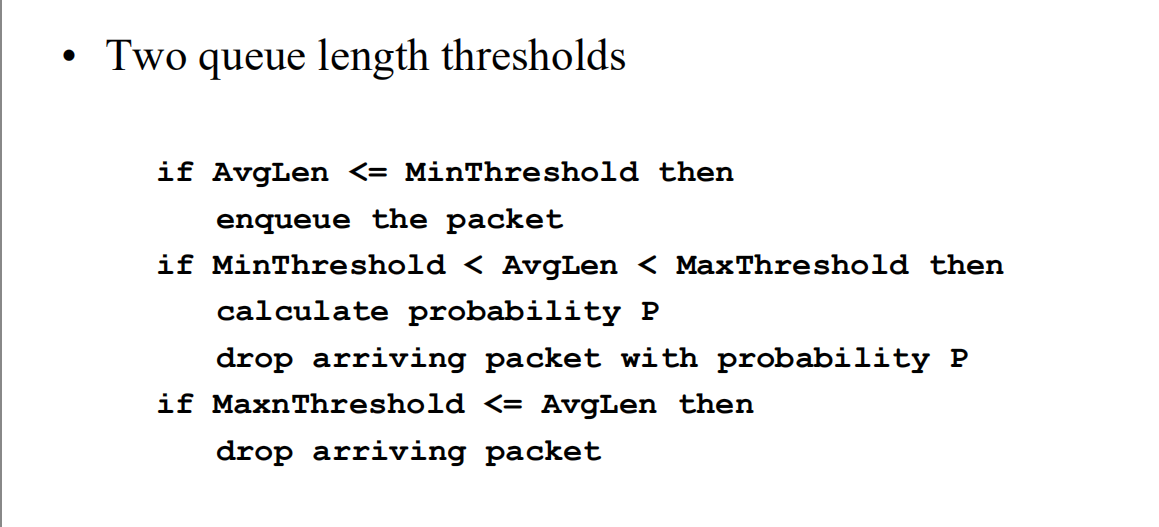
1. (2%) In TCP, how to solve the silly window syndrome problem? Silly window syndrome: If the sender aggressively fills an empty container as soon as it arrives.

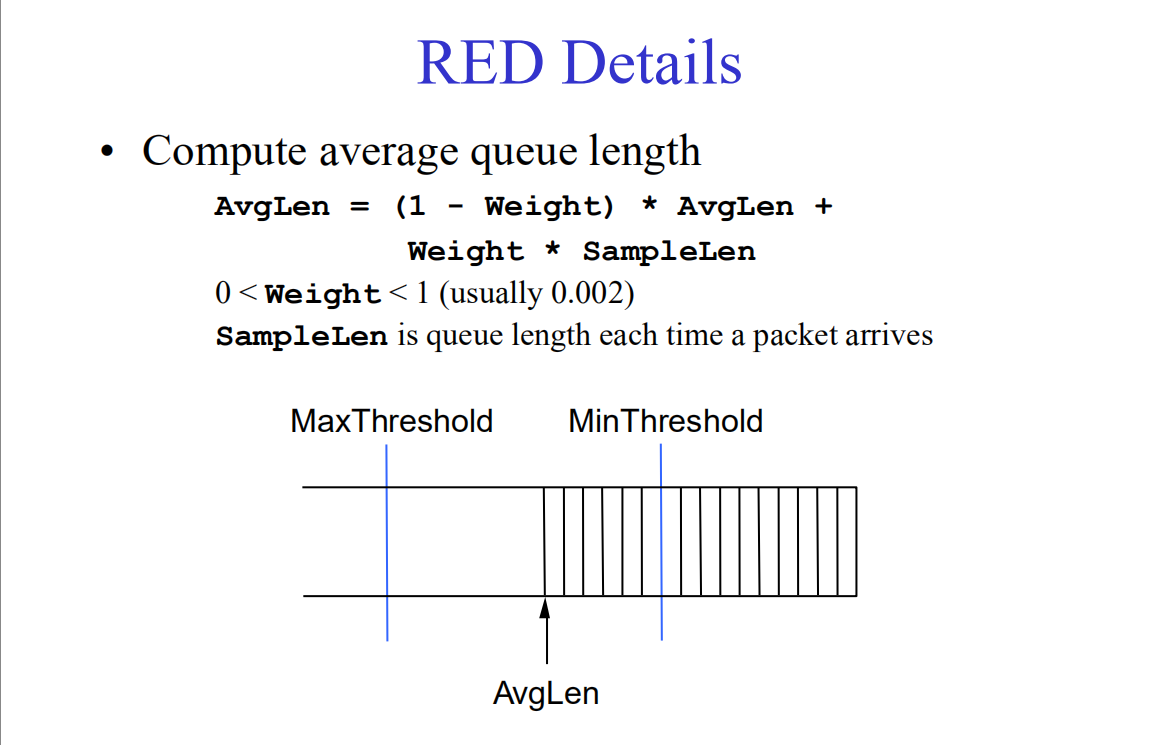
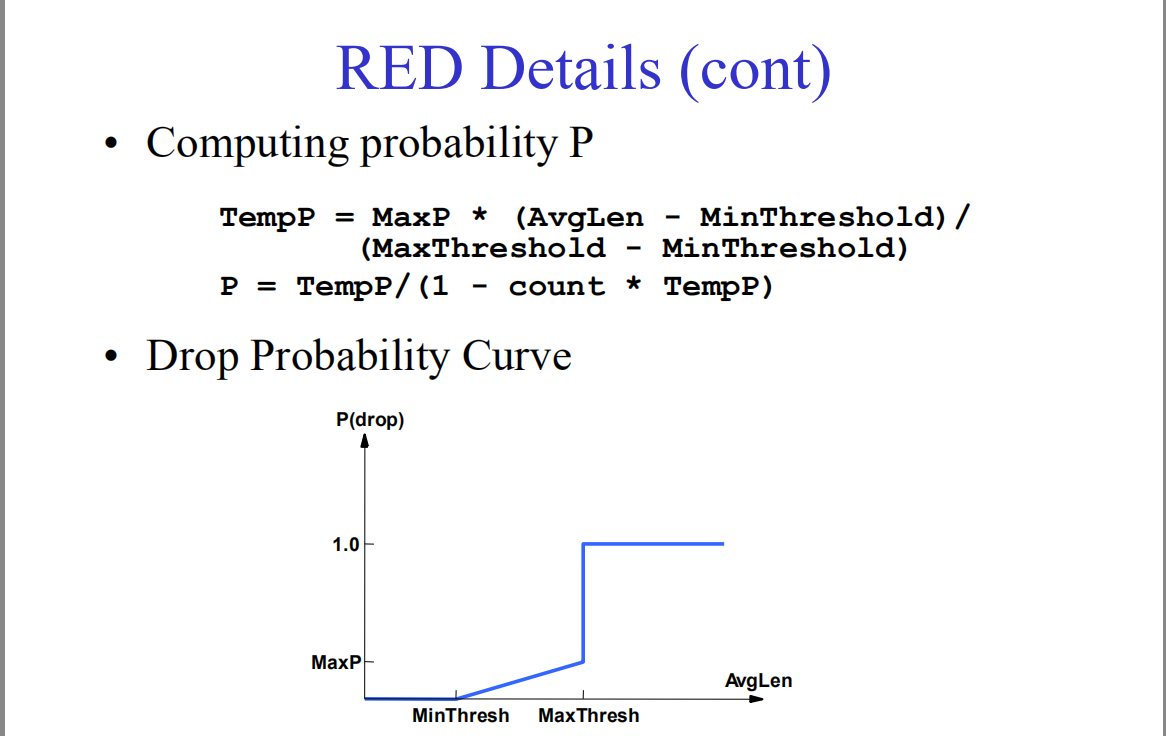
Delaying ACKs: sending one combined ACK rather than multiple smaller ones. Then the receiver will reply with a larger window size.

After advertising a zero window, the receiver must wait for space equal to an MSS before it advertises an open window.

A self-clocking solution: Nagle’s algorithm.

1. (2%) Describe how RED is used in conjunction with TCP to avoid synchronized backoff?



1. (Queuing disciplines and QoS, 10%)
2. (2%) Describe briefly what a priority queue is.

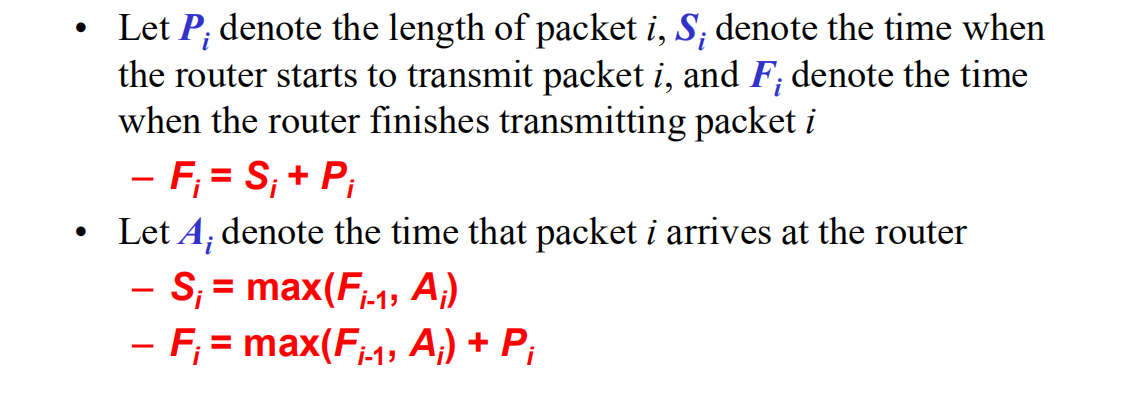
Make each packet with priority (carried in the IP Type of Service (TOS) field)。

The router always transmits packets out of the highestpriority queue if the queue is nonempty.

Then moves on to the next priority queue. Within each priority, packets are still FIFO.

1. (2%) Suppose that packet *i* with packet length arrives at the router at time .

If the time stamp of packet *i* – 1 is , find the time stamp for packer *i* under the *fair queuing* policy.



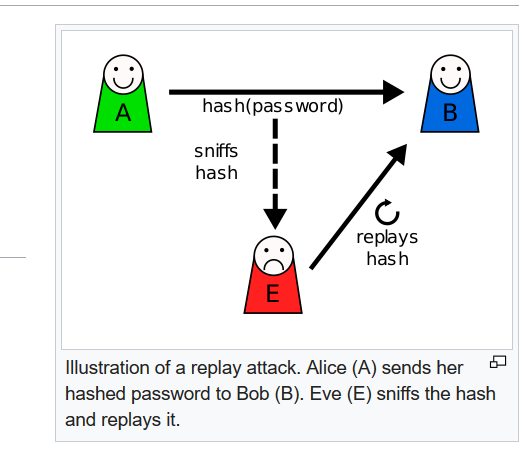
1. (2%) Describe the difference between admission control and policing.
2. (2%) Describe what RSVP does (including the PATH message and the RESV message).

Admission control: the process of deciding when to say no to a requesting user.

Resource reservation: the mechanism by which the users of the network and the components of the network exchange information, such as requests for service.

1. (2%) Describe briefly how self-clocking is used in TCP?
2. (Security, 14%)
3. (2%) How can a RSA algorithm be used for digital signature?
4. Describe the following Internet security attacks.
5. (2%) Playback attack.

This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it.



Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session which Bob accepts, thus granting Eve access

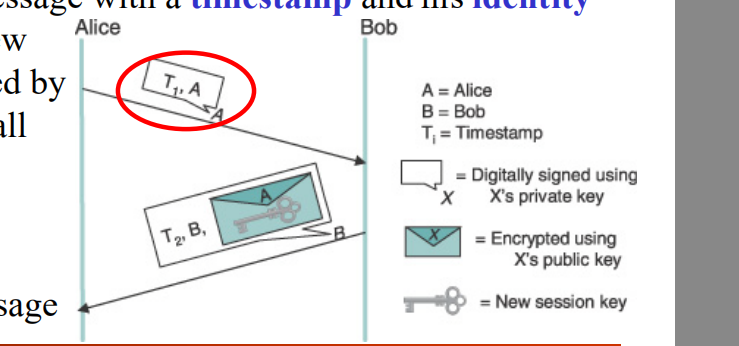
1. (2%) Man-in-the-middle attack.

An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

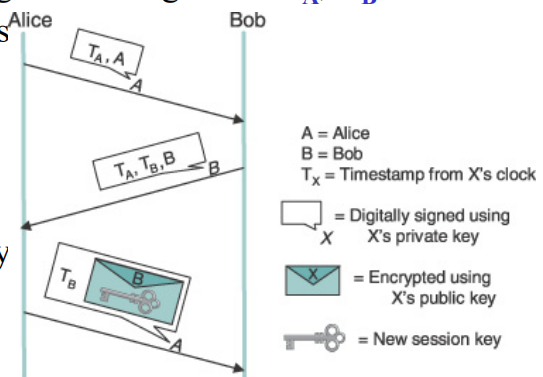
1. Answering the following problems for authentication.
2. (2%) What is *nonce* ?

An arbitrary number that can be used just once. (Anti-replay)

1. (3%) Figure 2 is the timeline of the synchronized public-key authentication. Please explain this figure briefly.



1. (3%) Figure 3 is the timeline of the asynchronized public-key authentication. Please explain this figure briefly.



1. (JPEG and MPEG, 6%)
2. (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?

The low frequencies correspond to the gross features.

The gross features are essential and the fine detail is less essential.

The high-frequency coefficients are increasingly unimportant to the perceived quality of the image.

1. S
2. S
3. S
4. S
5. (RSA and security, 15%)
6. (5%) Consider two primes *p* = 3 and *q* = 7. Choose an encryption key *e* = 5. Find the decryption key *d* in RSA.
7. (5%) Consider a message *M* = 3. Find the encrypted message *C* by using the encryption key *e* in RSA.
8. (5%) Show how you decrypt *C* to get *M* = 3.
9. 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.

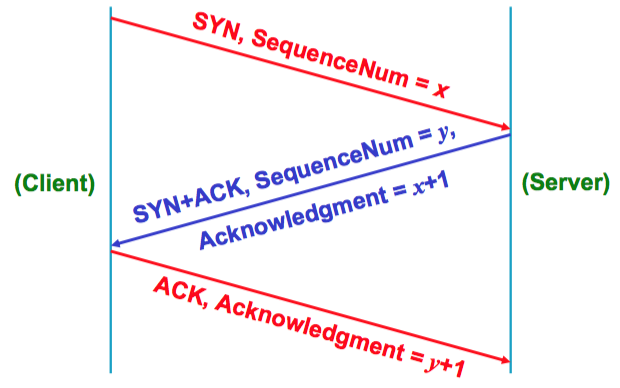
Multiplicative Decrease:

Each time a timeout occurs, the source sets CongestionWindow to half of its previous value.

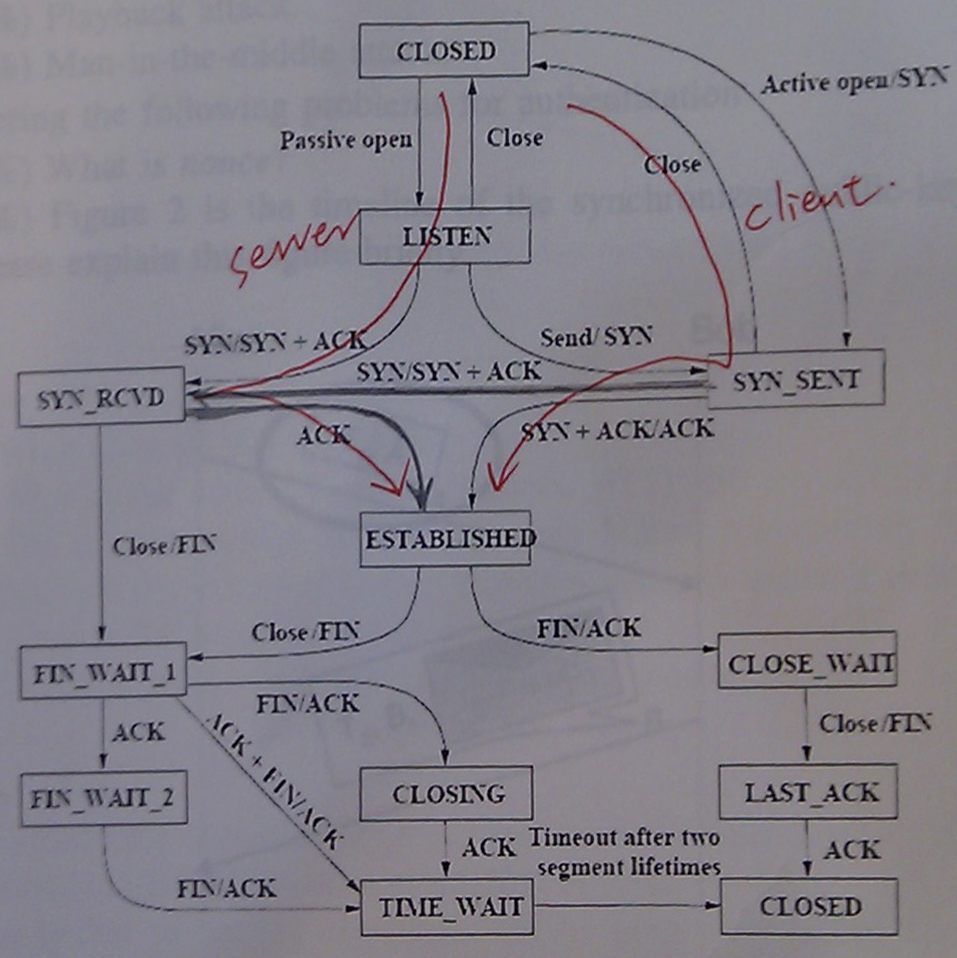
1c. The AIMD takes too long to ramp up a Source connection from its start to the available bandwidth. Increase the congestion wimdow exponentially rather than linearly.

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. = max( , ) +

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

9. *n* = *p*\**q*

9a. *de* mod ((*p*-1)\*(*q*-1)) = 1

*d*5 mod 12 = 1

* *d* = 5

9b. *C* = mod *n*

= mod 21

= 12

9c. *M* = mod *n*

= mod 21

= 3