6.033
COMPUTER SYSTEMS ENGINEERING
HANDS ON 5: TCP DUMP

JOHN WANG

(1) The ip address for willow is 128.30.4.222 and the address for maple is 128.30.4.223, this can be obtained by using the "-n" option which stops *tcpdump* from converting ip addresses to names.

(2) The largest sequence number that was acked was 1,572,889. Since the sequence numbers represent bytes, there were 1572 kilobytes that were transferred. The last communication occurred at 0:34:44.339015 and the first communication occurred at 00:34:41.473036. Thus, 2.866 seconds elapsed from the first to the last communication. This means the rate of message sending was $1,572,889 bytes/2.866s = 549 KiloBytes/s$.

(3) Packet 1473:2921 was sent out at 00:34:41.474225, while the acknowledgement came at 00:34:41.482047. Thus, the round trip time was 0.007822 seconds. Packet 13057:14505 was sent at 00:34:41.474992 and the acknowledgement came at 00:34:41.499373. The round trip time was 0.024381 seconds, which is much larger than the round trip time for packet 1473:2921. The reason for this is because the 1473:2921 packet was sent in the initial startup and it was one of the first packets to get sent. Because of this, it was received by the receiver pretty quickly after it was sent and an ack was sent quickly as well. However, for packet 13057:14505, the packet had to wait for the queue of packets before it to be processed before the ack could be sent.

1. TIME SEQUENCE GRAPH

(4) The white arrows occur after the transition (to the right) of the green lines. This is because as soon as an ack is received, the sender can slide the window and send more packets. Therefore, receiving an ack allows the sender to transmit more packets.

2. PACKET LOSS AND RETRANSMISSION

(5) 4000. This is first time that 3 duplicate acks are received.

(6) 18000. This is the first time that there is a retransmission and 3 duplicate acks were not received.

3. TCP CONGESTION CONTROL

(7) The reason the white arrows are approximately on a line are because once TCP finds its correct window value, packets are sent at an approximately constant rate. When an ack is received, a packet is sent out. Thus, TCP sends out packets in a linear fashion, since after the window has been saturated, there are more packets sent out from the receiver than acks that the receiver obtains. Therefore, the round trip time will govern the throughput of the packets in the formula $throughput = window\_size/RTT$.

(8) The slope of the line is given by $|W|/RTT$ where $|W|$ is the congestion window size and RTT is the round trip time. This makes sense because the rate of increase of packets is given by the throughput, which is determined by how many acks are received per round trip time. Clearly, there are $|W|$ of these acks received.