Ph.D. Preliminary Examination

Computer Networking

January 2008

1. (10 pts) Sketch the five-layer TCP/IP protocol stack. Which layer does the HTTP protocol belong to?

2. (15 pts) Explain in details the *Exponential Backoff* algorithm used in the CSMA/CD protocol.

3. (20 pts) Calculate the latency (from the first bit sent from node A to the last bit received at node B) for the following scenario: a 10-Mbps Ethernet with a single store-and-forward switch S in the path from A to B, and a packet size of 512 bytes. There are two links in the path, i.e., from A to S, and from S to B. Assume that the length of each link is 2.5 km, the signal propagation speed is 2.3×10^8 m/s, and the switch begins retransmitting immediately after it has finished receiving the packet.

4. (15 pts) A token ring has a total wire length of L meters. Assume that the signal propagation rate is R m/s, there is only a single active host, and the packet size is P bits. What is the effective throughput rate that can be achieved if the ring has a bandwidth of B bps (assuming that L, R, P and B are positive numbers, and that delayed token release is used)? Give the expression in terms of L, R, P and B.

5. (20 pts) Suppose that a TCP message contains 4096 bytes of data and 20 bytes of TCP header. This TCP message is passed to IP for delivery across a network. Assume that all IP headers are 20 bytes. The network uses 8-byte headers with a maximum transmission unit (MTU) of 1024 bytes. The MTU gives the total network packet size that may be sent, including the network header. Give the offsets of the sequence of fragments delivered to the network layer at the destination host.

6. (20 pts) A wants to ensure the integrity of the message *m* to be sent to B. So A signs the SHA1 digest of the message, *SHA1(m)*, with its RSA private key. Then A sends $m + E(SHA1(m), private_A)$ to B. Suppose the message *m* was modified so that a different message m_1 was received by B. List the major steps for B to detect the modification.

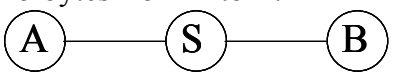
Computer Networking
October 2008

1. (15 pts) A voice communication system is operating at a sampling rate of 8000 samples per second with each sample being quantized to 24 bits. What is the bit rate of this system? And how "wide" is a bit (in seconds) with such a bit rate?

2. (15 pts) If we want to send data at a rate of 8000 bps through a channel with bandwidth of 1000 Hz.What is the minimum SNR (signal to noise ratio) required?

3. (15 pts) Consider a satellite channel with 250ms propagation delay. Stop-and-wait ARQ protocol is employed with a frame size of 1000 bits and a bit rate of 1Mbps. Calculate the utilization of the link (assuming there are no error and no processing delay).

4. (20 pts) Hosts A and B are each connected to a store-and-forward switch S via 10-Mbps links as shown in the figure below. The propagation delay on each link is 10 μs. S implements "cut-through" switching: It is able to begin retransmitting the packet after the first 200 bits have been received. Calculate the total time required to transmit a packet of 625 bytes from A to B.



5. (20 pts) A disavantage of the contention approach for the Ethernet is the capacity wasted due to multiple stations attempting to access the channel at the same time. Suppose there are only three active stations (A, B and C) that are accessing the Ethernet, and that time is divided into discrete slots, with each of the three stations attempting to transmit at the beginning of a slot with a given probability (as shown in the table below). What is the probability of a slot being wasted due to multiple simultaneous transmission attempts?

Station	Probability of Transmission
A	0.5
B	0.5
C	0.8

6. (15 pts) If we want to encrypt a plaintext message *m* using the AES cipher, we need to provide a password *p*. After we run the AES encryption algorithm, we obtain a ciphertext $c_1 = AES\ (m, p)$. By using the same plaintext *m* and the same password *p*, we run the AES encryption algorithm again. This time, however, we might obtain a totally different ciphertext $c_2 = AES\ (m, p)$. That is, $c_1 \neq c_2$. Explain why the same password would produce different ciphertexts.

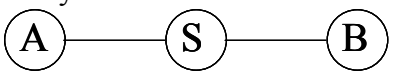
Ph.D. Preliminary Examination
Computer Networking
January 2009

1. (15 pts) If we want to send data at a rate of 8000 bps through a channel with bandwidth of 1000 Hz. What is the minimum SNR (signal to noise ratio) required?

2. (15 pts) Consider a satellite channel with 250ms propagation delay. Stop-and-wait ARQ protocol is employed with a frame size of 1000 bits and a bit rate of 1Mbps. Calculate the utilization of the link (assuming there are no error and no processing delay).

3. (15 pts) A voice communication system is operating at a sampling rate of 8000 samples per second with each sample being quantized to 24 bits. What is the bit rate of this system? And how "wide" is a bit (in seconds) with such a bit rate?

4. (20 pts) Hosts A and B are each connected to a store-and-forward switch S via 10-Mbps links as shown in the figure below. The propagation delay on each link is 10 μs. S implements "cut-through" switching: It is able to begin retransmitting the packet after the first 200 bits have been received. Calculate the total time required to transmit a packet of 625 bytes from A to B.



5. (20 pts) A disavantage of the contention approach for the Ethernet is the capacity wasted due to multiple stations attempting to access the channel at the same time. Suppose there are only three active stations (A, B and C) that are accessing the Ethernet, and that time is divided into discrete slots, with each of the three stations attempting to transmit at the beginning of a slot with a given probability (as shown in the table below). What is the probability of a slot being wasted due to multiple simultaneous transmission attempts?

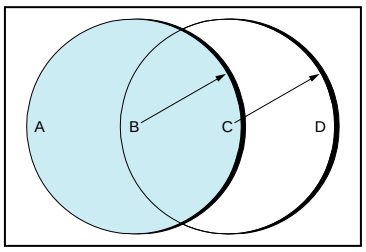
Station	Probability of Transmission
A	0.5
B	0.5
C	0.8

6. (15 pts) If we want to encrypt a plaintext message *m* using the AES cipher, we need to provide a password *p*. After we run the AES encryption algorithm, we obtain a ciphertext $c_1 = AES(m, p)$. By using the same plaintext *m* and the same password *p*, we run the AES encryption algorithm again. This time, however, we might obtain a totally different ciphertext $c_2 = AES(m, p)$. That is, $c_1 \neq c_2$.

Explain why the same password would produce different ciphertexts.

April 2009
Preliminary Examination
Computer Networking

1. (15 pts) Explain in details how the MACA (multiple access with collision avoidance) Algorithm can be used to resolve the problem of *hidden nodes* (A and C) in a 802.11 network shown below.



2. (15 pts) Consider a satellite channel with 250ms propagation delay. Stop-and-wait ARQ protocol is employed with a frame size of 1000 bits and a bit rate of 1Mbps. Calculate the utilization of the link (assuming there are no error and no processing delay).

3. (15 pts) A voice communication system is operating at a sampling rate of 8000 samples per second with each sample being quantized to 24 bits. What is the bit rate of this system? And how "wide" is a bit (in seconds) with such a bit rate?

4. (20 pts) Hosts A and B are each connected to a store-and-forward switch S via 10-Mbps links as shown in the figure below. The propagation delay on each link is 10 μs. S implements "cut-through" switching: It is able to begin retransmitting the packet after the first 200 bits have been received. Calculate the total time required to transmit a packet of 625 bytes from A to B.

5. (20 pts) A disavantage of the contention approach for the Ethernet is the capacity wasted due to multiple stations attempting to access the channel at the same time. Suppose there are only three active stations (A, B and C) that are accessing the Ethernet, and that time is divided into discrete slots, with each of the three stations attempting to transmit at the beginning of a slot with a given probability (as shown in the table below). What is the probability of a slot being wasted due to multiple simultaneous transmission attempts?

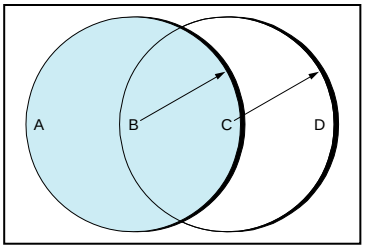
Station	Probability of Transmission
A	0.5
B	0.5
C	0.8

6. (15 pts) If we want to encrypt a plaintext message *m* using the AES cipher, we need to provide a password *p*. After we run the AES encryption algorithm, we obtain a ciphertext $c_1 = AES(m,$

p). By using the same plaintext *m* and the same password *p*, we run the AES encryption algorithm again. This time, however, we might obtain a totally different ciphertext $c_2 = AES(m, p)$. That is, $c_1 \neq c_2$. Explain why the same password would produce different ciphertexts.

Ph.D. Preliminary Examination
Computer Networking
October 2009

1. (15 pts) Explain in details how the MACA (multiple accesses with collision avoidance) Algorithm can be used to resolve the problem of *incorrectly exposed nodes* (A and D) in an 802.11 network shown below.



2. (15 pts) Describe in details the three-way handshake procedure used by the Transmission Control Protocol to establish a connection.

3. (15 pts) Explain in details the *Exponential Backoff* algorithm used in the CSMA/CD protocol.

4. (10 pts) What does the term "Flow Control" mean? Is flow control provided by the User Datagram Protocol?

5. (10 pts) In a Token Ring network, how can a monitor station detect a missing token?

6. (20 pts) A disavantage of the contention approach for the Ethernet is the capacity wasted due to multiple stations attempting to access the channel at the same time. Suppose there are N active stations that are accessing the Ethernet, where N is a positive integer greater than 1, and that time is divided into discrete slots, with each of the three stations attempting to transmit at the beginning of a slot with the same probability p. What is the probability of a slot being wasted due to multiple simultaneous transmission attempts?

7. (15 pts) Explain how to generate digitial signatures for a message using the RSA algorithm.

Ph.D. Preliminary Examination

Computer Networking
Spring 2010

1. (10 pts) Sketch the five-layer TCP/IP protocol stack. Which layer does the Internet Control Message Protocol (ICMP) belong to?

2. (15 pts) How many half-duplex links are required to connect 200 nodes in a fully connected configuration (i.e., each node has a direct link to other nodes)?

3. (15 pts) Explain in details the *Early Token Release Scheme* as used by Token Ring networks.

4. (20 pts) Calculate the latency (from the first bit sent from node A to the last bit received at node B) for the following scenario: a 10-Mbps Ethernet with a single store-and-forward switch S in the path from A to B, and a packet size of 512 bytes. There are two links in the path, i.e., from A to S, and from S to B. Assume that the length of each link is 2.5 km, the signal propagation speed is 2.3×10^8 m/s, and the switch begins retransmitting immediately after it has finished receiving the packet.

5. (20 pts) Use pseudo codes to illustrate the Internet's Checksum Algorithm used to calculate the checksum field in headers of IP packet.

6. (20 pts) Explain what are the protocols the network tool *traceroute* uses, and the mechanism by which *traceroute* forces a router that is **two** hops away to report its IP address.