CSCI 466 Final **Name: _____**
Networks
Fall 2011

This exam consists of 10 problems on the following 13 pages.

You may use your two-sided hand-written 8 ½ x 11 note sheet during the exam and a calculator.
No other computers or communication devices of any kind are permitted.

If you have a question, raise your hand and I will stop by.
Since partial credit is possible, **please write legibly and show your work**.

Problem	Points	Score
1	22	
2	8	
3	5	
4	9	
5	8	
6	7	
7	15	
8	12	
9	12	
10	12	
Total	110	

1. **Multiple choice** (22 points). Circle the single best answer.

I. Which of the following network devices operates at the highest layer of the OSI model?
   a) Switch / bridge
   b) Repeater
   c) Router
   d) Hub

II. Which of the following is **NOT** something that helps networks scale?
   a) Routing areas
   b) Switched Ethernet
   c) SYN flooding
   d) Virtual LANs (VLANs)

III. Which of the following best describes DNS (Domain Name System)?
   a) Maps a domain name to an IP address
   b) Maps a network adapter's MAC address to an IP address
   c) Translates a host's private IP address to a public IP address
   d) Translates a host's IPv6 address to an IPv4 address

IV. In the original deployment of TCP, the sender could immediately send as much data as allowed by the receiver's window size. This resulted in which of the following?
   a) Widespread server outages due to exposure to Smurf attacks
   b) A catastrophic decrease in network goodput (i.e. congestion collapse)
   c) Excessive consumption of IPv4 addresses (necessitating the transition to IPv6)
   d) Increased packet round trip times due to reduced pipelining

V. Which of the following does **NOT** use an overlay network (IP tunneling)?
   a) Virtual Private Networks (VPNs)
   b) IPv6 communication across IPv4 networks
   c) Mobile IP
   d) Network Address Translation (NAT)

VI. TCP employs a 3-way handshake in which both sides inform the other of their starting sequence number. Why can't both sides simply start at 0?
   a) The sequence number must be unique among all TCP connections on both hosts.
   b) It helps avoid a late arriving segment from a previous connection (between the same hosts on the same ports) from corrupting the current connection.
   c) The TCP specification requires hosts increment the starting sequence by one every time a new connection is started on a given port.
   d) Using a small sequence number reduces the size of the TCP segment headers.

VII. Which of the following does **NOT** use the ICMP protocol (Internet Control Message Protocol)?

a) ping
b) traceroute
c) DNS (Domain Name System)
d) Path MTU (Maximum Transmission Unit) discovery

VIII. Wireless protocols such as 802.11 typically provide reliability mechanisms such as Forward Error Correction (FEC) and retransmission. Why is this important to the TCP protocol?

a) Helps prevent TCP congestion control from throttling connections using the wireless link due to mistakenly thinking packet loss is due to congestion.
b) It increases the ratio: TCP segment payload bytes / TCP segment header bytes.
c) Decreases the number of window probe frames required by TCP.
d) Prevents TCP flow control from opening up too large a window size.

4 4

IX. RFC 822 and MIME are associated with which of the following?

a) Format of web pages
b) Format of real-time data (e.g. audio or video data)
c) Format of BGP router updates
d) Format of email messages

X. Which of the following is **true** about how routers handle traffic?

a) If a packet arrives and the router's queue is full, the OSI model requires the arriving packet be dropped.
b) A router may use random early detection (RED), dropping a packet before its queue is actually full.
c) A router with a FIFO queuing disciples must send the packet that has been waiting the least amount of time.
d) If the traffic is secure (e.g. using IPSec), the router cannot inspect the IP header fields.

XI. Which of the following is **true** about the HTTP protocol?

a) HTTP is a binary encapsulated RPC protocol optimized for web content delivery.
b) HTTP is a simple request-response protocol operating in plaintext over TCP.
c) HTTP clients request page elements using parallel UDP messages. Servers may or may not consolidate the results into a single UDP response.
d) HTTP/1.1 must establish and tear down a TCP connection for every page element retrieved.

2. **Network layers** (8 points). The OSI model consists of a 7-layer stack. For the specified layers, give 1-2 examples of a protocol associated with that layer.

Application	**Example 1: HTTP, RTP, SMTP, IMAP, FTP, …** **Example 2:**
Presentation	
Session	
Transport	**Example 1: TCP, UDP** **Example 2:**
Network	**Example 1: IPv4, IPv6**
Data link	**Example 1: 802.11, Ethernet, …** **Example 2:**
Physical	**Example 1: 4B5B, Manchester, NRZI, …**

3. **Host addressing** (5 points). Your friend (who hasn't taken this course), is puzzled by this XKCD comic:

http://xkcd.com/742/

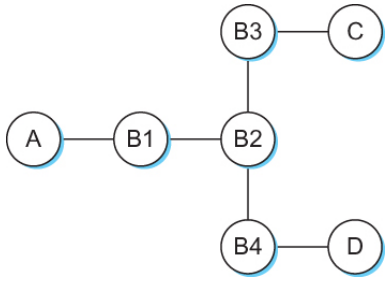
a) Explain to your friend why the children are gasping.

192.168/16 is a private IP space, thus "she" and the killer are on the same home network!

b) How many possible addresses does 192.168/16 (192.168.0.0/16) represent?

2^{16} = 65536

4. **Bridging / switching** (9 points). Consider the arrangement of four learning bridges shown below. Assume all bridge's forwarding tables are empty. Fill out the forwarding tables showing which hosts (A, C, D) are reachable from each interface on each bridges (B1-B4) after each transmission.



a) Transmission: **D → C**

Bridge B1	A-interface	B2-interface
	-	**D**

Bridge B2	B1-interface	B3-interface	B4-interface
	-	-	**D**

Bridge B3	C-interface	B2-interface
	-	**D**

Bridge B4	D-interface	B2-interface
	D	-

b) Transmissions: D → C, **C → D**

Bridge B1	A-interface	B2-interface
	-	**D**

Bridge B2	B1-interface	B3-interface	B4-interface
	-	**C**	**D**

Bridge B3	C-interface	B2-interface
	C	**D**

Bridge B4	D-interface	B2-interface
	D	**C**

c) Transmissions: D → C, C → D, **A → C**

Bridge B1	A-interface	B2-interface
	A	**D**

Bridge B2	B1-interface	B3-interface	B4-interface
	A	**C**	**D**

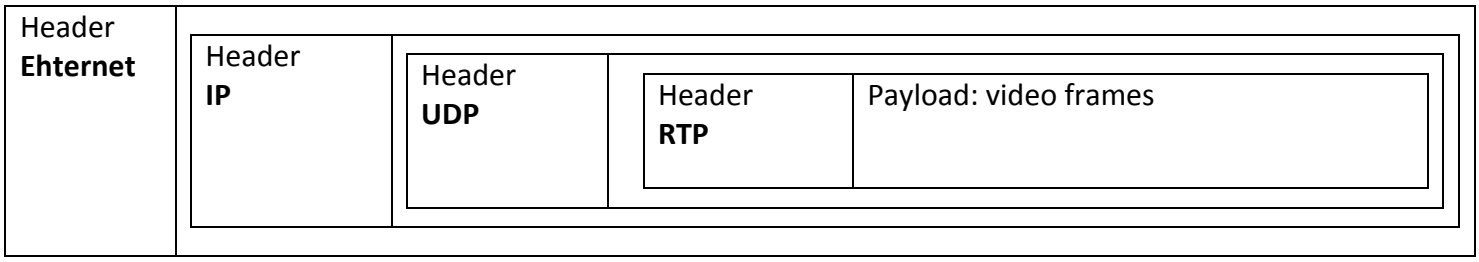
Bridge B3	C-interface	B2-interface
	C	**A, D**

Bridge B4	D-interface	B2-interface
	D	**C**

5. **Real-time data, protocol stacks** (8 points).

a) You are in a video conference with a colleague at a remote office. You are connected to your network using a wired Ethernet connection. Your two offices are connected via a number of Ethernet routers connected via cat-5 cable. The bottom diagram shows your video frames encapsulated in a nesting of different protocols. Label the 4 headers with the most likely protocol from this set:

802.11	WiFi	IMAP	Internet Message Access Protocol
ARQ	Automatic Repeat-reQuest	IP	Internet Protocol
ARP	Address Resolution Protocol	MIME	Multipurpose Internet Mail Extensions
BGP	Border Gateway Protocol	NAT	Network Address Translation
CDMA	Code Division Multiple Access	OSPF	Open Shortest Path First OSPF
DHCP	Dynamic Host Configuration Protocol	RPC	Remote Procedure Call
DNS	Domain Name System	RTP	Real-time Transport Protocol
Ethernet	-	RTCP	Real-time Transport Control Protocol
ECN	Explicit Congestion Notification	SOAP	Simple Object Access Protocol
FTP	File Transfer Protocol	TCP	Transmission Control Protocol
ICMP	Internet Control Message Protocol	UDP	User Datagram Protocol

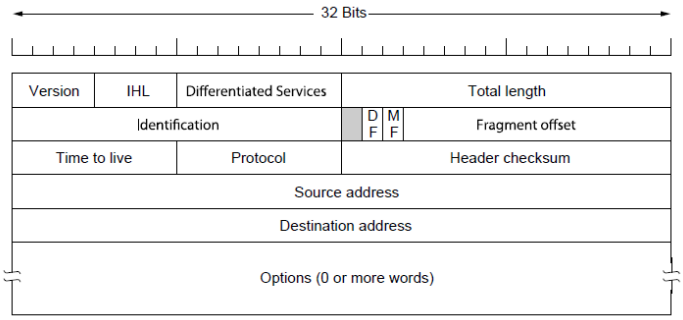


b) Discuss how what is required from the network differs for a real-time video conference versus watching a movie on Netflix. In each case, discuss what an application might do to cope with suboptimal network performance in an effort to improve the user experience.

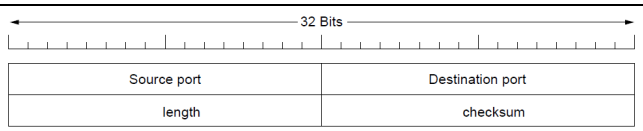
Video conference: low latency, drop to lower quality (high compression or lower resolution)

Netflix: high bandwidth, higher latency is acceptable, increase buffering to account for jitter, lower quality

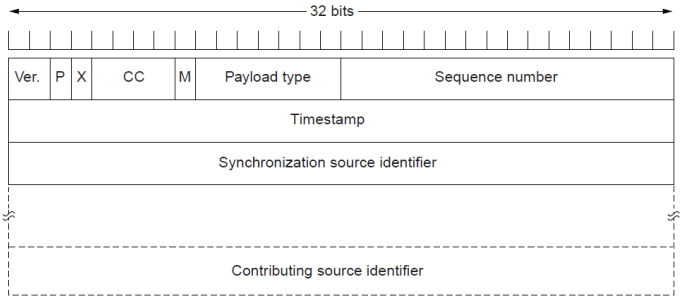
6. **Networking protocols** (7 points). On this page are the header diagrams for a number of networking protocols. Label them using the following: **802.11, Ethernet, IPv4, IPv6, RTP, TCP, UDP.**



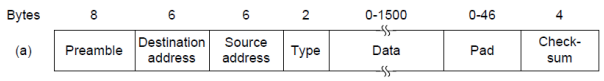
IPv4



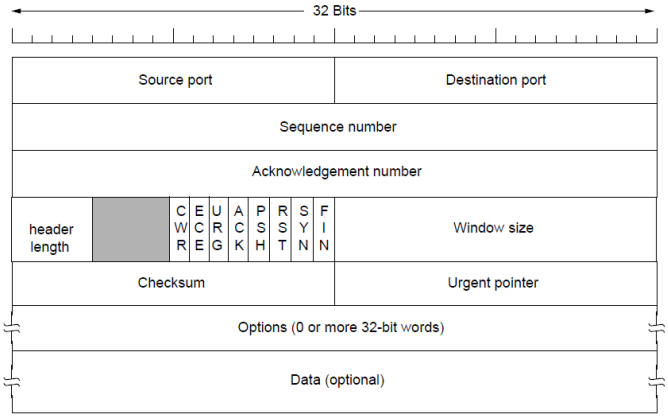
UDP



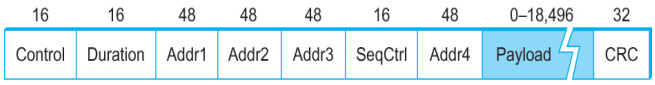
RTP



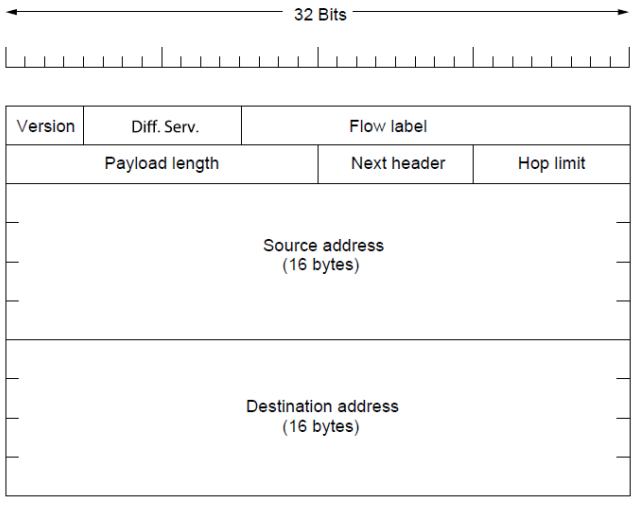
Ethernet



TCP



802.11



IPv6

7. **Short answer** (15 points).

a) Wired Ethernet is a Carrier Sense, Multiple Access with Collision Detection (CSMA/CD) technology. 802.11 (WiFi) is Carrier Sense, Multiple Access with Collision Avoidance (CSMA/CA) technology. Give two reasons why frame collisions can't necessarily be detected in a 802.11 wireless network.

Reason 1: Radios can't transmit and listen for collisions at the same time

Reason 2: Can't hear all other stations (hidden node problem)

b) A home wireless router is at times a DHCP server and at times a DHCP client. Explain when it is a server and when it is a client.

When a server: When new laptop is turned on and needs a new private IP address

When a client: Obtaining a public IP from the ISP

c) DNS lookups run over UDP. Give two reasons UDP is a good choice for performing DNS lookups.

Reason 1: No connection setup

Reason 2: Low header overhead, well suited for small request/response style interaction

d) Explain why 48-bit Ethernet MAC addresses would not work well as a replacement for IP addresses on the global Internet.

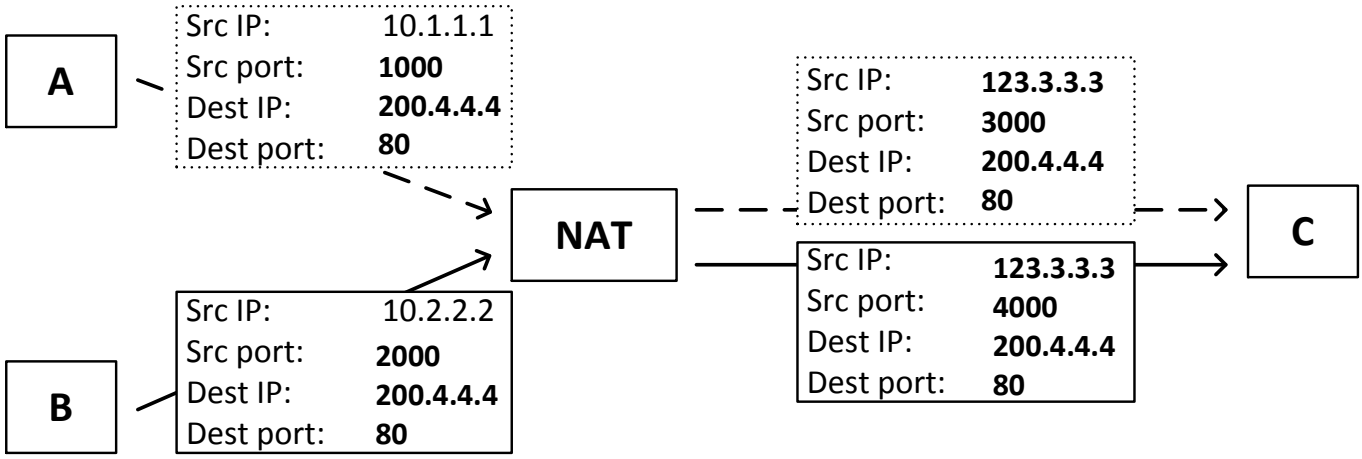
No hierarchy in MAC addresses, so no way to consolidate entries in routing tables.
MAC is tied to the physical device, not say some logical entity like a particular web server.

e) Describe how a router is different from a switch/bridge.

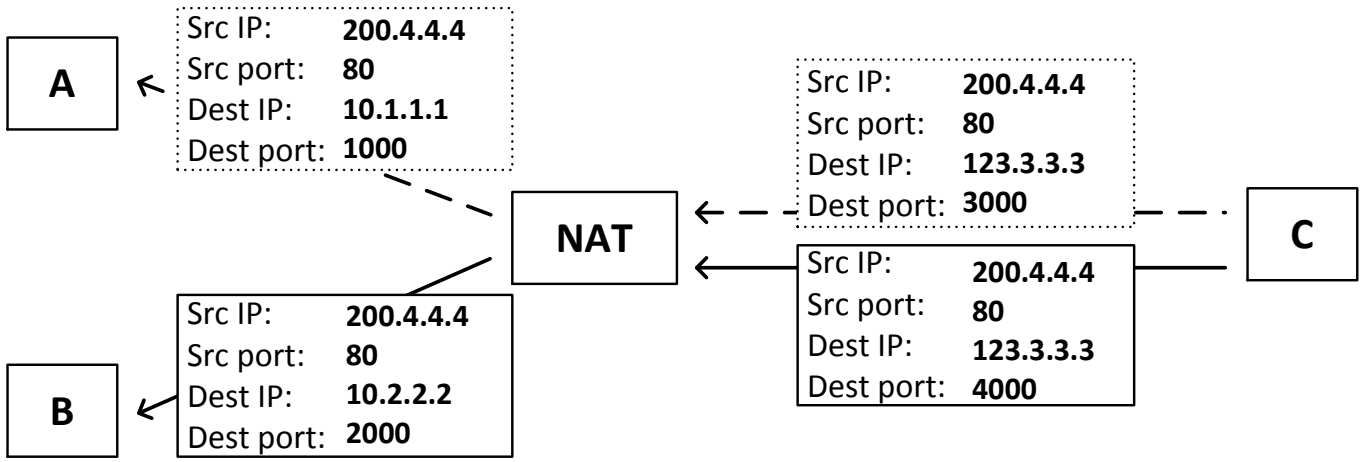
Routers operate at network layer, looking at IP header and forwarding on. A switch operates at the data link layer on a homogeneous small network.

8. **NAT, Network Address Translation** (12 points).

a) A company has its computers behind a NAT box that utilizes a single public IP address 123.3.3.3. The company's computers use private IP addresses in 10.0.0.0/8. Recall that requests to web servers are made on port 80. In the following diagram, host A and B are both making requests to a web host C. Host C has an IP address of 200.4.4.4. Fill in plausible values for the missing fields in the outbound TCP/IP packets.



Host C is now sending back responses to A and B's queries. Fill in the values for the missing fields.



8. **NAT, Network Address Translation (continued)**

b) Host A is using a persistent HTTP connection to host C. The user of host A has taken a 5-minute coffee break. Explain why A's TCP connection may need to be reestablished when the user returns to browsing.

The NAT box's translation table entry for that connection may have timed out and been deleted.

c) If the company in part a) has 100,000 computer behind its NAT box and many of the computers are busy browsing the web, what problem might the NAT box run into?

The NAT box would run out of the 64K available port numbers.

d) Give an advantage afforded to the Internet at large by the organization's use of a NAT box.

Conserves limited IPv4 addresses.

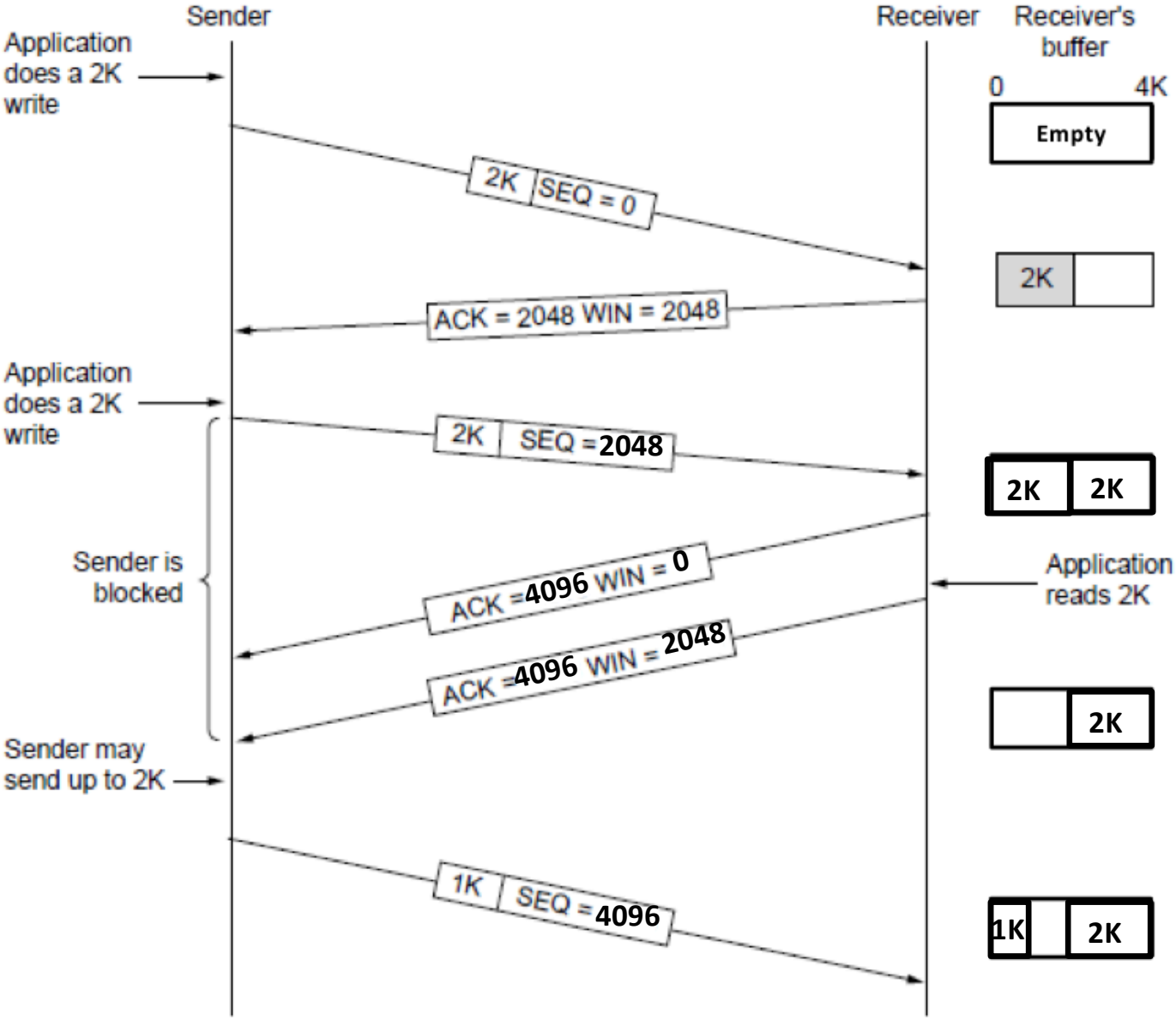
e) Give an advantage afforded to the organization by using a NAT box.

Some measure of security.

Easy to manage and migrate to new ISP or external IP address.

9. **TCP** (12 points).

a) The following timeline diagram shows a TCP conversation. Fill in the missing acknowledgement and window size values in the segments. Also show the state of the receiver's 4KB buffer.

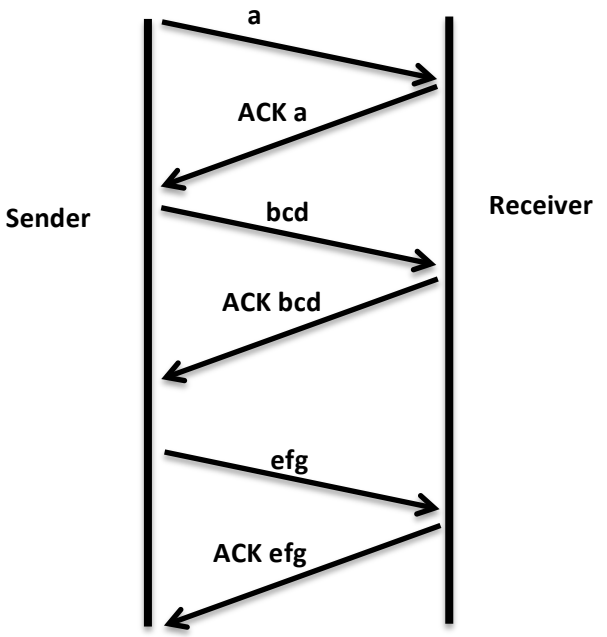


b) Assume the last ACK went missing. Describe the mechanism that prevents communication from permanently stalling out.

The sender periodically sends window probes to see if the received window has opened up.

9. **TCP** (continued)

c) Assume the sending host uses Nagle's algorithm to send the letters `abcdefg` one letter per second over a TCP connection with an RTT of 3.1 seconds. Draw a timeline diagram showing: when each packet is sent, what each sent packet contains, and when the ACK for each packet is returned.



t=0.0, "a" sent

t=1.0, "b" put in buffer

t=2.0, "c" put in buffer

t=3.0, "d" put in buffer

t=3.1, ACK for "a" arrives, "bcd" sent

t=4.0, "e" put in buffer

t=5.0, "f" put in buffer

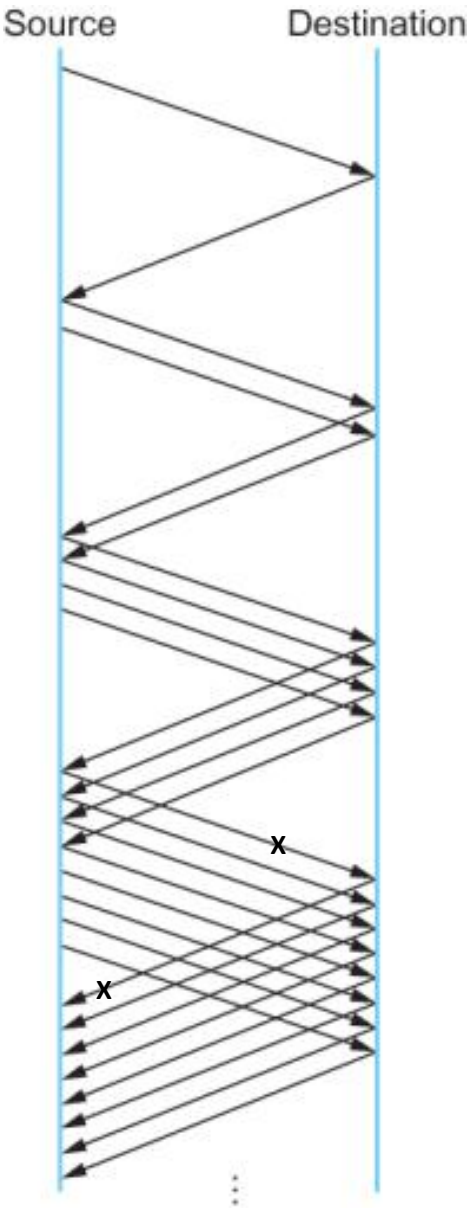
t=6.0, "g" put in buffer

t=6.2, ACK for "bcd" arrives, "efg" sent

t=9.3, ACK for "efg" arrives

10. **Congestion control** (12 points).

a) The diagram shows a new connection using TCP slow start. The source is sending 1K segments with an initial slow start threshold of 64K. The destination is responding with ACKs. Assume the first outbound segment in the last group of 8 disappears. Assume TCP fast retransmission and fast recovery are ***NOT*** being used.



How does the source detect something went wrong?

Times out waiting for ACK of 1st segment in group

What is the new slow start threshold?

4K (8K were in window at time of packet loss)

Draw a timeline diagram showing the first ***5 groups*** of outbound segments sent once the missing packet is detected. Assume all segments (including ACKs) are transmitted without problem.

Similar to diagram at left, starting with 1 sent packet and 1 returned ACK. Then 2 outbound packets, 2 returned ACKs, 4 outbound packets, 4 returned ACKs, 8 outbound packets, 8 returned ACKs, and finally 16 outbound packets and 16 returned ACKs.

10. **Congestion control (continued)**

c) How does explicit congestion notification (ECN) differ from traditional ways of detecting congestion on Internet paths? Give one benefit of ECN. Give one reason deployment of ECN has been slow.

ECN differs in that it relies on Internet routers setting a bit in the packet to indicate things are starting to get congested rather than waiting for congestion to actually occur (with packets being dropped).

ECN may benefit interactive applications that are sensitive to loss of one or more packets.

Deployment has been slow since it requires ECN-capable routers.

d) Assume host A is sending data via TCP to host B. A is connected to a fast 1-Gbps network connection. Somewhere between A and B is a slow 1-Mbps link. Host A initially sends a burst of 4 packets in quick succession. Explain how A can space future transmissions to avoid overwhelming the router at the slow link.

Only sent new packets at the rate the ACKs are received (an ACK clock). Since the ACKs have to traverse the slow link, they provide a measure of how fast the sender can put data into the connection without packets piling up at the slow connection.