Homework: Lower Network layers

Tailang Cao u1480633

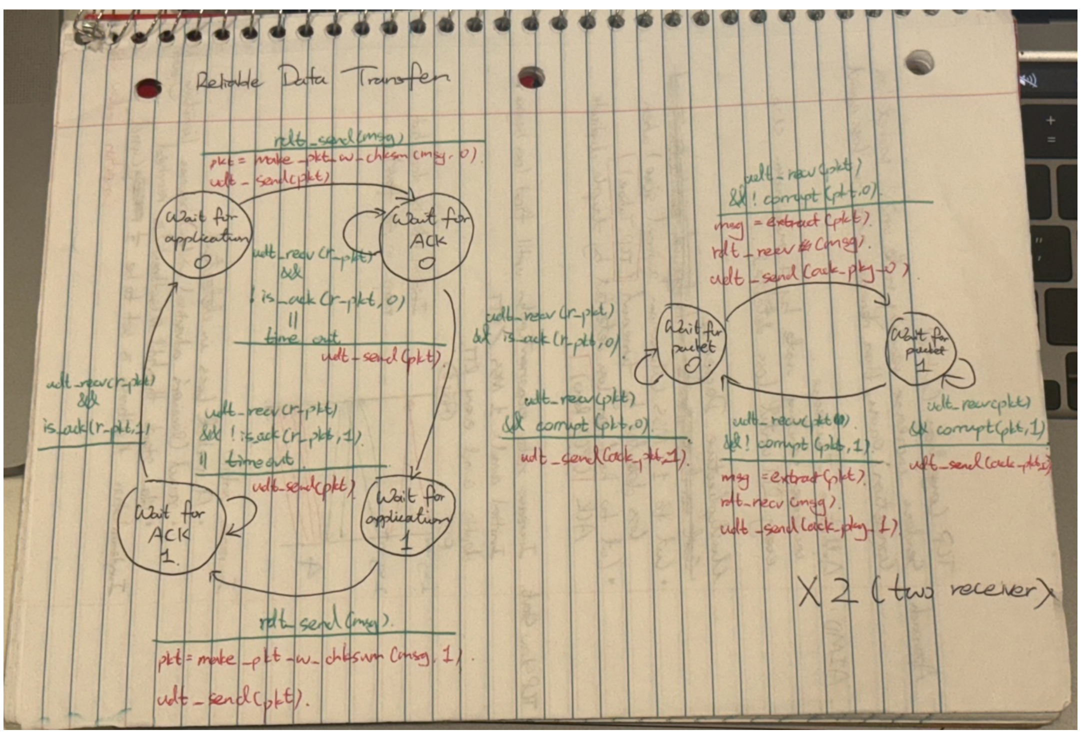
Question 1: Reliable Data Transfer

We want to send data from one node to two other nodes using over a simple broadcast channel. Specifically, we want to design a protocol for reliably sending data from host S to hosts R1 and R2 over this channel. The channel can lose or corrupt packets for independently. For example, a packet sent by S might be received by R1 but not R2.

When there are collisions on the broadcast channel, you can assume that the receiving hosts will detect them as corrupt packets. If data needs to be resent, you can ignore random backoffs, etc, and assume that eventually the colliding hosts will be able to resend their data without interference.

Design the protocol state machines for S and R (both R1 and R2 should use the same protocol).

Use the primitives we discussed in the notes (udt_send and receive, etc). Don't consider pipelining. The RDT protocol we developed with sequence numbers 0 or 1 + timeouts is a good starting point.



Question 2: Throttling
Q: What is the difference between flow control and congestion control? Describe the way TCP implements each of these features.

A:

TCP flow control is a mechanism used to regulate the flow of data between a sender and a receiver to prevent the receiver from being overwhelmed by data it cannot process fast enough. It is achieved through the use of sliding window protocols, where the receiver advertises its available buffer space (receive window) to the sender. The sender adjusts its transmission rate based on this advertised window size, ensuring efficient data transfer without overwhelming the receiver. When the receiver's buffer is full, it advertises a window size of zero, instructing the sender to stop sending data.

TCP congestion control is a mechanism used to manage network congestion, which occurs when there is more data being transmitted through a network than it can handle.

It starts of with a slow flow (transmission) state and increases the amount of data by doubling the cwnd that can be send until it detects packet loss. A lost packet is detected either when the sender gets 3 duplicate ACKs, or when its timeout fires. If a packet is lost (timeout fires), a variable called the "slow start threshold" (ssthresh) is set to cwnd/2. Then the cwnd is reset to 1 and the slow start process begins again. If the cwnd becomes greater than ssthresh, then the connection switches to "congestion avoidance mode”. In this mode, the sender tries to increase its transmission rate more slowly since it's probably within a factor of 2 of its max rate.

Question 3:NAT

Q: Two hosts (IPs **A**: 10.0.0.1 and **B**: 10.0.0.2) sit behind a NAT enabled router (public IP **5.6.7.8**). They're both communicating with a remote host **X**, 1.2.3.4 on port 80. What are *possible* values for the source and destination addresses and ports for packets:

from A to X behind the NAT

Source IP: 10.0.0.1 Source Port: 7777

Destination IP: 1.2.3.4 Destination Port 80

from B to X behind the NAT

Source IP: 10.0.0.2 Source Port: 7778

Destination IP: 1.2.3.4 Destination Port 80

from A to X between the NAT and X

Source IP: 5.6.7.8 Source Port 11111

Destination IP: 1.2.3.4 Destination Port 80

from B to X between the NAT and X

Source IP: 5.6.7.8 Source Port 11111

Destination IP: 1.2.3.4 Destination Port 80

from X to A between X and the NAT

Source IP: 1.2.3.4 Source Port 80

Destination IP: 5.6.7.8 Destination Port 11111

from X to A between the NAT and A

Source IP: 5.6.7.8 Source Port: 11111

Destination IP: 10.0.0.1 Destination Port 7777

	Inside IP	Inside port	Outside port
A	10.0.0.1	7777	11111
B	10.0.0.2	7778	11112

Question 4:

A company has 3 groups that each hava a subnet on the corporate network. Group A uses subnet 1.1.1.0/24. Group B uses 1.1.2.0/24. Group C uses subnet 1.1.3.0/24.

Each group has a router. There is a link between each pair of routers.

A and B have a link: 1.1.4.0 (on A) to 1.1.4.1 (on B) A and C have a link: 1.1.5.0 (on A) to 1.1.5.1 (on C) B and C have a link: 1.1.6.0 (on B) to 1.1.6.1 (on C)

(1) How many subnets are a part of this network, and what is the smallest IP prefix (i.e. most fixed bits) that can be used to describe each one?

There are six subnets.The smallest IP prefix that can be used to describe each one is 255.255.248.0 or 1.1.7.0/21 .

(2) If this network is somehow connected to the internet, what is the cheapest (i.e. smallest number of address) IP prefix the company could have purchased (without using NAT)?

The cheapest IP prefix is /21

(3) Assume the router for group A has 4 ports: port 1 is connected to the group subnet, port 2 is connected to router B, port 3 is connected to router C, and port D is connected to the ISP. Write out router A's forwarding table.

Destination	Interface (Port)
1.1.1.0	Port 1
1.1.2.0	Port 2
1.1.2.0	Port 3
1.1.4.0	Port 2
1.1.5.0	Port 3
0.0.0.0	Port D

Question 5:

Plot the number of messages required to converge as a function of network size.