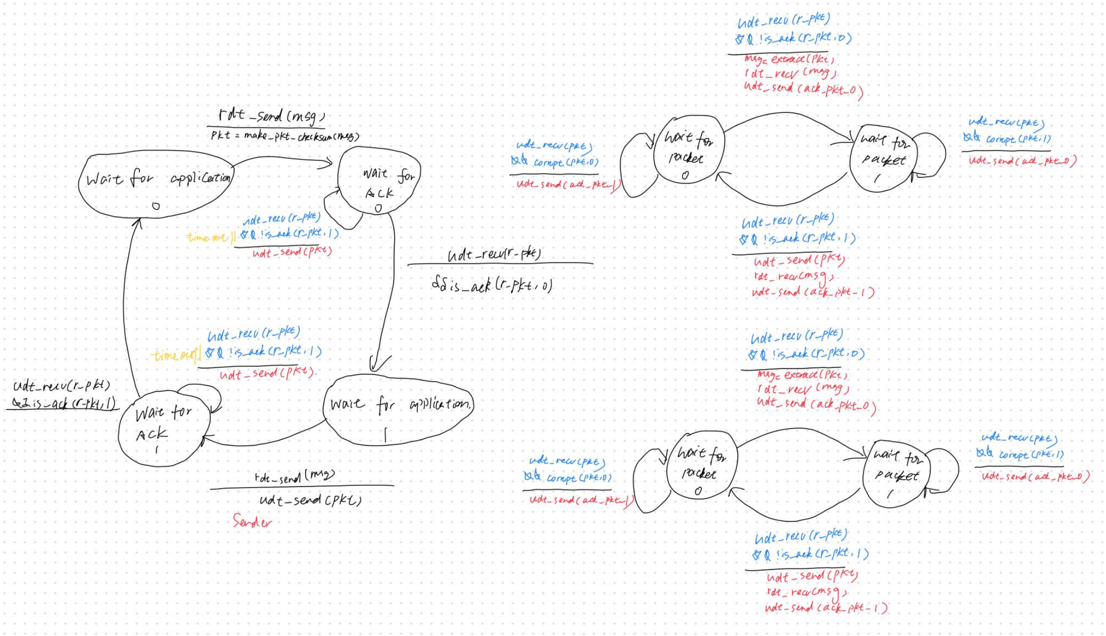
Homework : Lower Network Layers

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:

What is the difference between flow control and congestion control? Describe the way TCP implements each of these features.

Flow control and congestion control are two essential mechanisms in network communication, especially in TCP (Transmission Control Protocol), to ensure reliable data transfer and efficient network utilization. While they aim to optimize network performance and prevent packet loss, they operate at different levels and address different problems.

Flow Control

Purpose: Flow control is a mechanism to match the speed at which the sender is transmitting data with the receiver's ability to process and acknowledge the received data. It prevents the sender from overwhelming the receiver's buffer, ensuring that the receiver can handle incoming data without losing any packets due to buffer overflow.

How TCP Implements Flow Control:

Window-Based Mechanism: TCP uses a sliding window mechanism for flow control. The receiver specifies a window size in the TCP header of each ACK packet, informing the sender of the amount of data it is prepared to receive (the size of the receiver's buffer). This window size is dynamically adjusted based on the receiver's capacity to process data.
Receiver Advertised Window: The receiver tells the sender how much space is left in its buffer (the receive window), which limits the amount of data the sender can transmit before receiving further acknowledgment. This mechanism ensures that the sender does not send more data than the receiver can handle at any given time.
Congestion Control

Purpose: Congestion control aims to prevent network congestion by controlling the rate at which data is sent into the network. It is concerned with the overall network's ability to transport data and tries to avoid overwhelming the network capacity, which can lead to packet loss, long delays, and network collapse.

How TCP Implements Congestion Control:

Slow Start: When a connection is established, TCP starts with a low rate of data transmission and increases the rate exponentially until it detects packet loss or until it reaches a threshold called the slow start threshold.

Congestion Avoidance: Once the slow start threshold is reached, TCP enters congestion avoidance mode, where it increases the congestion window more cautiously (typically by one maximum segment size per round-trip time) to avoid congestion.
Fast Retransmit and Fast Recovery: Upon detecting packet loss (indicated by three duplicate ACKs), TCP performs a fast retransmit of the lost packet and enters fast recovery mode. In fast recovery, the congestion window is reduced to half of its current size (but not below the slow start threshold) to decrease the network load quickly, and then congestion avoidance is used.

Congestion Window (cwnd): A key component in TCP's congestion control, it limits the amount of data the sender can have in flight before receiving ACKs. The size of the congestion window is adjusted dynamically based on network conditions, independent of the receiver's advertised window.
Differences Summarized:

Scope: Flow control is concerned with the point-to-point communication capacity between the sender and receiver, while congestion control deals with the overall network capacity and aims to prevent network congestion.

Controlled By: Flow control is managed by the receiver's ability to process data, whereas congestion control is determined by the network's current state of congestion and packet loss signals.

Mechanisms: Flow control uses the receiver's advertised window to control the sender's rate, and congestion control uses algorithms like slow start, congestion avoidance, fast retransmit, and fast recovery, adjusting the congestion window based on network conditions.

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
from B to X behind the NAT
from A to X between the NAT and X
from B to X between the NAT and X
from X to A between X and the NAT
from X to A between the NAT and A
What there corresponding contents of the router's NAT translation table?

A:
1. From A to X Behind the NAT
Source Address and Port: 10.0.0.1 and a dynamically assigned source port (e.g., 12345)
Destination Address and Port: 1.2.3.4 and 80

2. From B to X Behind the NAT

Source Address and Port: 10.0.0.2 and a dynamically assigned source port (e.g., 54321)

Destination Address and Port: 1.2.3.4 and 80

3. From A to X Between the NAT and X

Source Address and Port: The public IP 5.6.7.8 and a translated source port (e.g., 10001)

Destination Address and Port: 1.2.3.4 and 80

4. From B to X Between the NAT and X

Source Address and Port: The public IP 5.6.7.8 and a different translated source port (e.g., 10002)

Destination Address and Port: 1.2.3.4 and 80

5. From X to A Between X and the NAT

Source Address and Port: 1.2.3.4 and 80

Destination Address and Port: The public IP 5.6.7.8 and the translated source port corresponding to A's session (e.g., 10001)

6. From X to A Between the NAT and A

Source Address and Port: 1.2.3.4 and 80

Destination Address and Port: 10.0.0.1 and the original source port assigned to A's session (e.g., 12345)

7. From X to B Between X and the NAT

The scenario isn't explicitly asked, but it's similar to "From X to A between X and the NAT."

Source Address and Port: 1.2.3.4 and 80

Destination Address and Port: The public IP 5.6.7.8 and the translated source port corresponding to B's session (e.g., 10002)

8. From X to B Between the NAT and B

Similarly, this wasn't asked but completes the scenarios.

Source Address and Port: 1.2.3.4 and 80

Destination Address and Port: 10.0.0.2 and the original source port assigned to B's session (e.g., 54321)

NAT Translation Table Contents:

For packets from A to X and from B to X, the NAT router's translation table would include entries to keep track of the internal and external mappings. Here's what the entries might look like:

For A's communication with X:
Internal Source: 10.0.0.1:12345 -> External Source: 5.6.7.8:10001
Destination (remains the same): 1.2.3.4:80
For B's communication with X:
Internal Source: 10.0.0.2:54321 -> External Source: 5.6.7.8:10002
Destination (remains the same): 1.2.3.4:80

Question 4: Routers

A: 1.1.1.0/24 subnet B: 1.1.2.0/24 subnet C:1.1.3.0/24 subnet
AB: 1.1.4.0 (on A)/1.1.4.1 (on B)/31 subnet (all but last 2 bits masked)
AC: 1.1.5.0 (on A) to 1.1.5.1 (on C)/31 subnet
BC: 1.1.6.0 (on B) to 1.1.6.1 (on C)/31 subnet

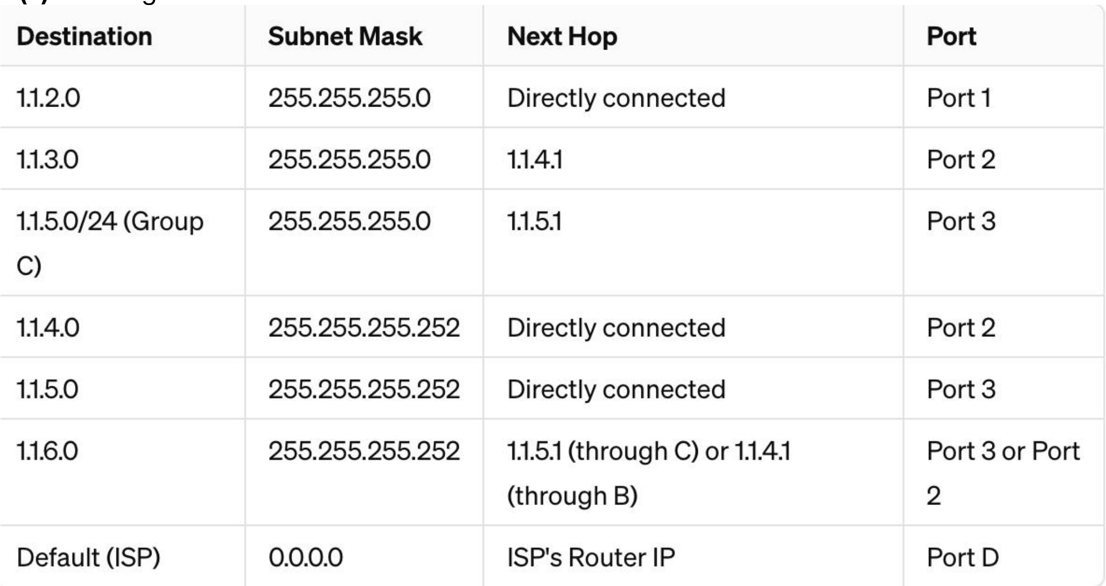
	Inside Ip	Inside port	Outside port
A	10.0.0.1	7777	11111
B	10.0.0.2	7778	11112

5

A (1) 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 .

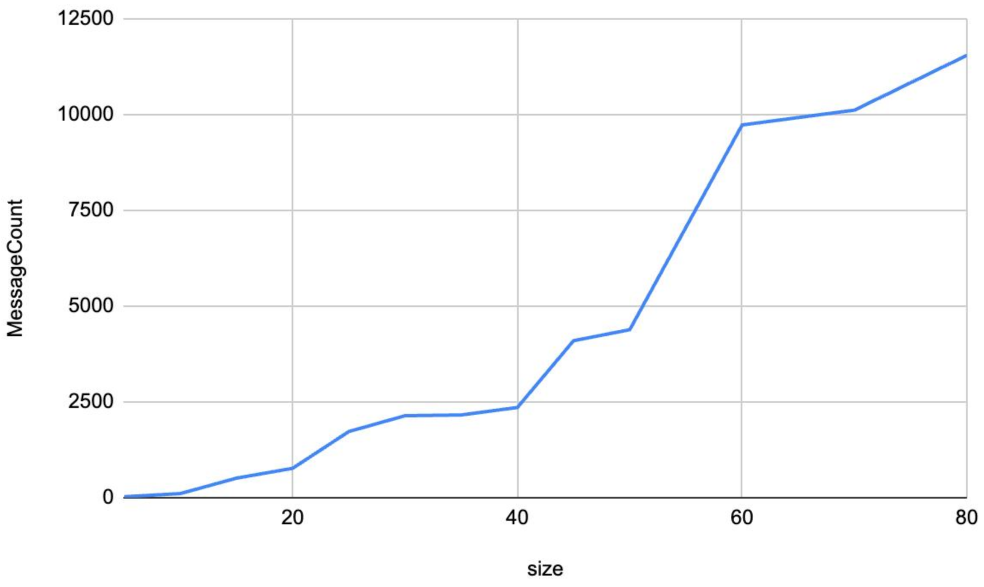
A(2) The cheapest IP prefix is /21. In order to buy a prefix for anything over the use of 1.1.3.0 you have to get the first 21 bits masked.

A(3): Routing table



Destination	Subnet Mask	Next Hop	Port
1.1.2.0	255.255.255.0	Directly connected	Port 1
1.1.3.0	255.255.255.0	1.1.4.1	Port 2
1.1.5.0/24 (Group C)	255.255.255.0	1.1.5.1	Port 3
1.1.4.0	255.255.255.252	Directly connected	Port 2
1.1.5.0	255.255.255.252	Directly connected	Port 3
1.1.6.0	255.255.255.252	1.1.5.1 (through C) or 1.1.4.1 (through B)	Port 3 or Port 2
Default (ISP)	0.0.0.0	ISP's Router IP	Port D

Question 5: Routing


MessageCount
size