Question 1: Reliable Data Transfer

Question 2: Throttling

Flow Control: flow control prevents the sender from overwhelming the receiver. It ensures that the sender doesn't send data faster than the receiver can process and accept it.

How it is Implemented: (rwnd && window < rwnd)

- Window-based Mechanism: TCP uses a sliding window mechanism for flow control. The window size can change based on the receiver's buffer capacity and how quickly it can process incoming data.
- Acknowledgements and window updates: receiver sends ACKs back to the sender, indicating sequence number of next expected byte and sometimes updating the window size. This makes it so it can adjust transmission rate to match the receiver's current capacity.

Congestion Control: it prevents too much data from being injected into the network, causing network resources to become overwhelmed. Its main concern is with the overall network health and tries to avoid packet loss and long delays during times when there are so busy.

How it is Implemented: (cwnd && window < cwnd)

- Slow start: cwnd starts with low value and grows exponentially until it meets the threshold or there's packet loss. It allows TCP to quickly reach capacity without causing too much congetsion
- Congestion Avoidance: once cwnd reaches the threshold, TCP increases it linearly
- Fast Retransmit and Fast Recovery: when there is packet loss/there are three duplicate ACKs, then the TCP resends the missing segment before its timeout. If it enters fast recovery, cwnd is reduced to half of its current size and then increases linearly, and doesn't slow start
- Additive Increase/Multiplicative Decrease (AIMD): TCP increases cwnd to probe for available bandwidth and decreases cwnd more significantly when congestion is detected. This proactively defends against congestion.

Key Differences:

- Flow control (rwnd) focuses on the receiver's capacity to handle incoming data. Congestion control (cwnd) focuses on the overall network and its capacity in regards to traffic.

Question 3: NAT

From A or B to X Behind the NAT:
The source IP addresses are their private IPs and the destination is host X IP.

Source (Host A): IP 10.0.0.1, Source Port: Assigned by Host A (e.g., 12345)
Destination (Host X): IP 1.2.3.4, Destination Port: 80
Source (Host B): IP 10.0.0.2, Source Port: Assigned by Host B (e.g., 23456)
Destination (Host X): IP 1.2.3.4, Destination Port: 80

From A or B to X between the NAT and X;
Once packets from and A/B reach the NAT router, the source IP addresses are replaced by the router's public IP

Source (from A through NAT): IP 5.6.7.8, Source Port: Unique port (e.g., 10001)
Destination (Host X): IP 1.2.3.4, Destination Port: 80
Source (from B through NAT): IP 5.6.7.8, Source Port: Unique port (e.g., 10002)
Destination (Host X): IP 1.2.3.4, Destination Port: 80

From X to A or B between X and the NAT:
Responses from X to A or B have the NAT's public IP as their destination and the source port indicates specific NAT translation entry.

Source (Host X): IP 1.2.3.4, Source Port: 80
Destination (to A through NAT): IP 5.6.7.8, Destination Port: 10001
Source (Host X): IP 1.2.3.4, Source Port: 80
Destination (to B through NAT): IP 5.6.7.8, Destination Port: 10002

From X to A or B between the NAT and A or B:
After the NAT router receives responses from X, it translates the destination IP back to the privat one.

Source (Host X): IP 1.2.3.4, Source Port: 80
Destination (to A): IP 10.0.0.1, Destination Port: 12345 (original source port from A)
Source (Host X): IP 1.2.3.4, Source Port: 80
Destination (to B): IP 10.0.0.2, Destination Port: 23456 (original source port from B)

NAT TABLE:

Internal IP	Internal Port	External IP	External Port	Destination IP	Destination Port
10.0.0.1	12345	5.6.7.8	10001	1.2.3.4	80
10.0.0.2	23456	5.6.7.8	10002	1.2.3.4	80

Question 4: Routers

There are 6 subnets in this network. Group A, B and C are group subnets which are 256 addresses. Link subnets have 4 addresses each, 2 of which are usable for router-to-router links. Here are the subnets listed with the smallest possible prefix given:

1. Group A subnet: 1.1.1.0 (24 bits)
2. Group B subnet: 1.1.2.0 (24 bits)
3. Group C subnet: 1.1.3.0 (24 bits)
4. A-B Link subnet: 1.1.4.0 (30 bits)
5. A-C link subnet: 1.1.5.0 (30 bits)
6. B-C link subnet: 1.1.6.0 (30 bits)

Because we can't use NAT, we need to make sure that every divide has a unique global IP address. The subnets range from 1.1.1.0 to 1.1.6.0. The smallest CIDR block that can encompass all these addresses would start at 1.1.1.0 and go to 1.1.6.255. This could be covered by a /21 subnet that would extend to all of these addresses and for subnets/links.

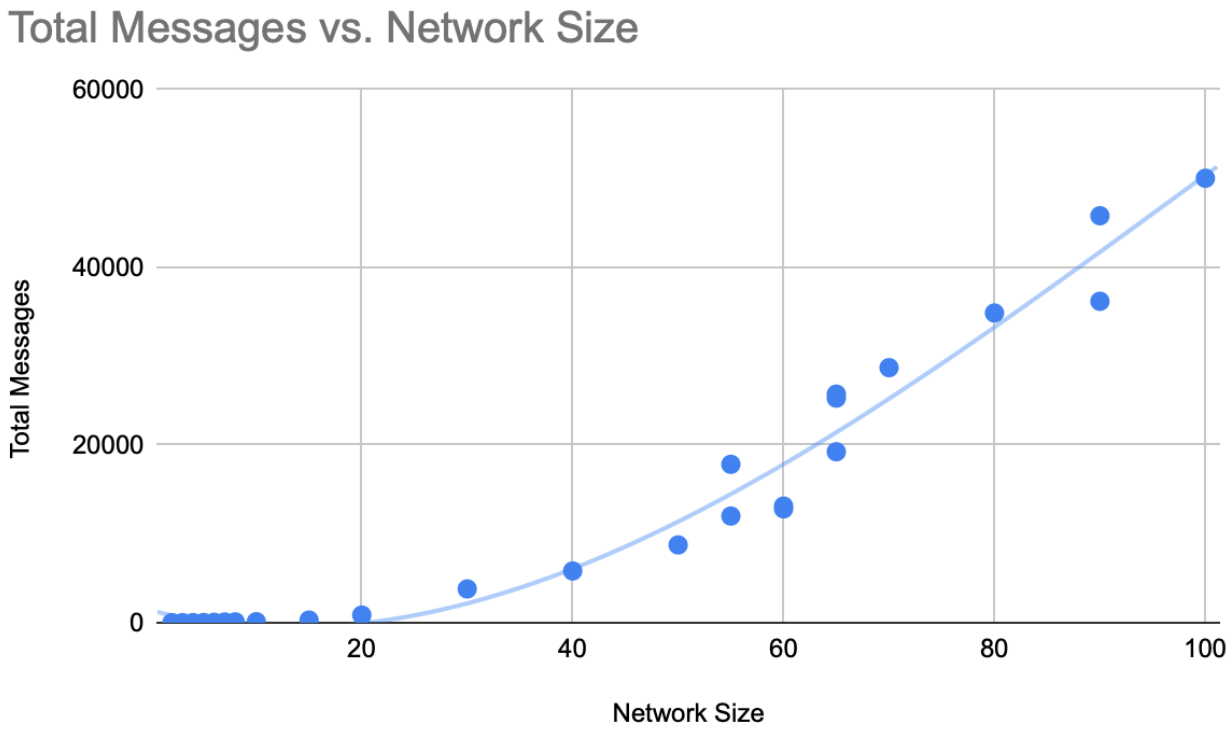
Assume the router for group A has 4 ports: port 1 is connected to the group subnet, port 2 is connected to router B, port 3 is connected to router C, and port D is connected to the ISP. Write out router A's forwarding table.

Destination	Subnet Mask	Next Hop (Interface)	Port
1.1.1.0	255.255.255.0	Directly connected	1
1.1.2.0	255.255.255.0	1.1.4.1	2
1.1.3.0	255.255.255.0	1.1.5.1	3
1.1.4.0	255.255.255.252	Directly connected	2
1.1.5.0	255.255.255.252	Directly connected	3

1.1.6.0	255.255.255.252	1.1.4.1(via B) or 1.1.5.1(via C)	2 or 3
0.0.0.0	0.0.0.0	ISP's router IP	4

Question 5: Routing

My code for this question is in the homework folder. I plotted different network sizes against the total number of messages. I then found that it followed a cubic graph. The trendline is a cubic function against the dots, which are my data points.



Network Size	Total Messages
5	16
6	45
4	9
3	6
2	2

7	74
8	88
20	852
10	112
15	290
50	8748
30	3799
40	5819
100	50016
80	34854
70	28700
60	13121
65	25721
65	19238
65	25276
60	12807
55	17820
55	12001
90	36173
90	45798