**2.**

**Difference between flow control and congestion control**

Flow control is a mechanism to ensure that the sender does not overwhelm the receiver by sending data too fast. It focuses on the data transfer rate between two directly communicating entities, ensuring that the sender's data transfer speed does not exceed the receiver's processing capabilities. This helps prevent the receiver from losing data due to buffer overflow.

Congestion control is a mechanism that ensures that data transmission in a network does not cause network congestion. It focuses on data flow throughout the network, trying to avoid increased latency or data loss caused by too many packets passing through the network at the same time. Congestion control is a global problem that attempts to alleviate or avoid congestion by reducing the amount of data sent into the network.

**How TCP implements these features:**

Flow control: TCP implements flow control by using the sliding window protocol. Each TCP segment contains a window size field that indicates the buffer size currently available to the receiver for receiving data. The sender adjusts its sending rate based on this window size to ensure that it does not send more data than the receiver can currently receive.

Congestion control: TCP mainly implements congestion control through four algorithms: slow start, congestion avoidance, fast retransmission and fast recovery.

Slow start: When a connection begins, TCP uses the slow start algorithm to increase the size of its congestion window to detect the network's carrying capacity.

Congestion avoidance: Once the congestion window reaches a threshold, TCP switches to using a congestion avoidance algorithm to avoid network congestion by increasing the window size in a more cautious manner.

Fast retransmit: When the sender receives three duplicate acknowledgments (indicating that the receiver did not receive the packets in order), it immediately retransmits the lost packets instead of waiting for a timeout.

Fast recovery: After a fast retransmission, TCP enters the fast recovery phase, adjusts its congestion window size, and attempts to retransmit lost packets while avoiding increased network congestion.

**3.**

Packet going through NAT from A to X:

Source address and port: 10.0.0.1 and a randomly chosen high-end port

Destination address and port: 1.2.3.4 and 80

Packets going through NAT from B to X:

Source address and port: 10.0.0.2 and a randomly chosen high-end port

Destination address and port: 1.2.3.4 and 80

Packet from A to X between NAT and X:

Source address and port: 5.6.7.8 and a high-end port assigned by the NAT device

Destination address and port: 1.2.3.4 and 80

Packet from B to X between NAT and X:

Source address and port: 5.6.7.8 and a high-end port assigned by the NAT device

Destination address and port: 1.2.3.4 and 80

Packets from X to A between X and NAT:

Source address and port: 1.2.3.4 and 80

Destination address and port: 5.6.7.8 and the corresponding high-end port

Packet from X to A between NAT and A:

Source address and port: 1.2.3.4 and 80

Destination address and port: 10.0.0.1 and 1024

**4.**

Group A Subnet: 1.1.1.0/24, Group B Subnet: 1.1.2.0/24, Group C Subnet: 1.1.3.0/24, A-B Link Subnet: 1.1.4.0/30, A-C Link Subnet: 1.1.5.0/30, B-C Link Subnet: 1.1.6.0/30

The smallest subnet is 1.1.0.0/21, covering addresses from 1.1.0.0 to 1.1.7.255. This allows all of the above subnets to be contained within a single larger subnet. This will be the cheapest IP prefix a company can purchase for direct internet connectivity without the need to employ NAT.

| **Destination** | **Subnet Mask** | **Next Hop** | **Interface** |
| --- | --- | --- | --- |
| 1.1.1.0 | 255.255.255.0 | Directly Connected | Port 1 |
| 1.1.2.0 | 255.255.255.0 | 1.1.4.1 | Port 2 |
| 1.1.3.0 | 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 | 1.1.4.1 (via B) or 1.1.5.1 (via C) | Port 2 or Port 3 |
| 0.0.0.0 | 0.0.0.0 | ISP's Router IP | Port D |