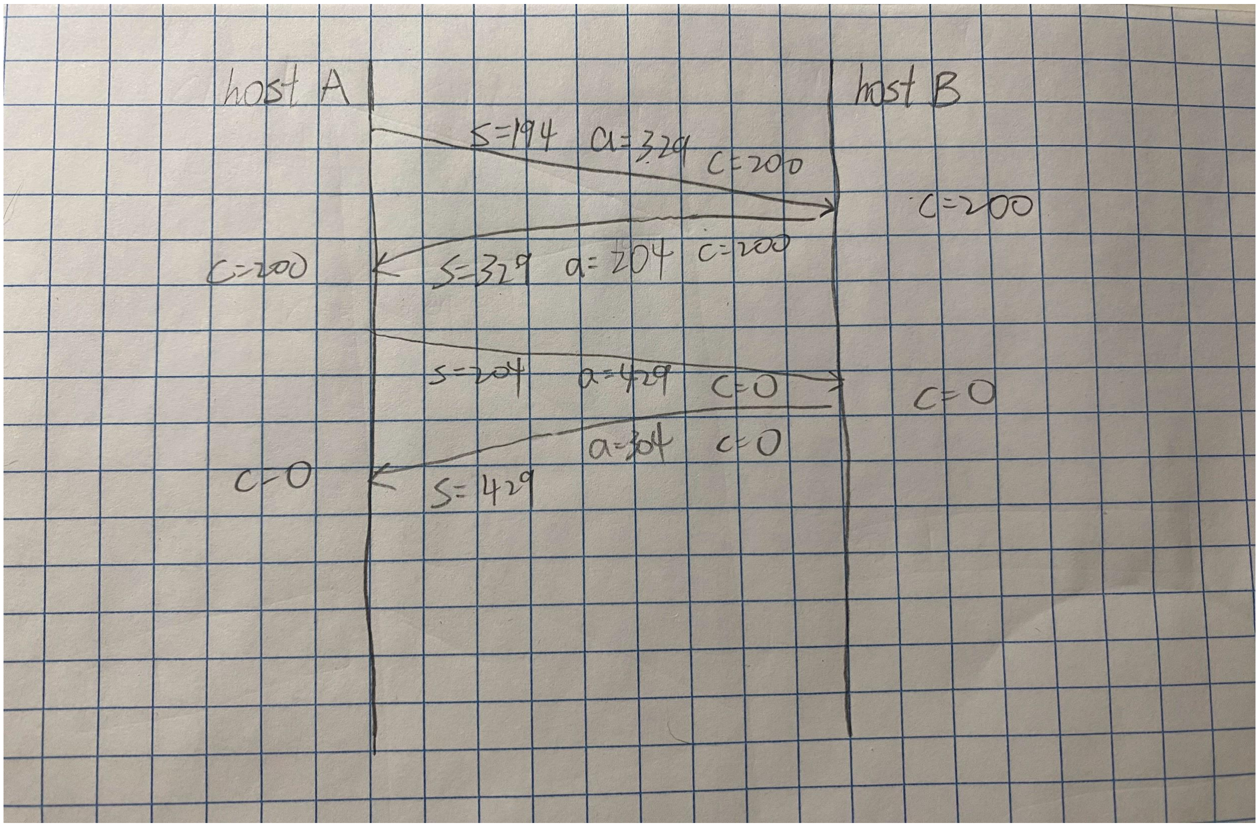
1. It is possible to allow intermediate servers as a part of the mail server communication. The main advantages in doing so is that the mail would be stored on multiple servers. So, in case of a failure of one server, mails can still be retrieved from other servers. Also, different receivers can be connected to different mail servers in order to balance the load. But, in doing so security and confidentiality of the mails can be compromised, as mails are stored at more than one unreliable server. So, the chances of security breach increase with the increase in the number of the mail servers between the sender and the receiver. b) SMTP between mail servers cannot be replaced by HTTP. HTTP is not appropriate for E-mail; they're quite different. The E-mail protocol suite is for implementation of a store & forward messaging system. HTTP is a nearly stateless file retrieval protocol (some state was shoehorned into HTTP late in the game as a matter of efficient use of TCP/IP).
2. In client-server architecture, only the server can upload the files. Depending on the number of files in transmission, the server needs to update the same number of files. Whereas in P2P architecture, all hosts participate in file uploading. When only transmit one file between server to one host, P2P is not better than client-server, if transmitting between many hosts, P2P is better than client-server.
3. Go-back-N window size limit is to avoid packets being recognized incorrectly. If the window size is greater than half the sequence number space, then if an ACK is lost, the sender may send new packets that the receiver believes are retransmissions. For example, if our sequence number range is 0-3 and the window size is 3, this situation can occur.
   [initially] (B's window = [0,1,2])
   A -> 0 -> B (B's window = [1,2,3])
   A -> 1 -> B (B's window = [2,3,0])
   A -> 2 -> B (B's window = [3,0,1])
   [lost] ACK0
   [lost] ACK1
   A <- ACK2 <- B
   A -> 3 -> B
   A -> 0 -> B [retransmission]
   A -> 1 -> B [retransmission]
   After the lost packet, B now expects the next packets to have sequence numbers 3, 0, and 1. But, the 0 and 1 that A is sending are actually retransmissions, so B receives them out of order. By limiting the window size to 2 in this example, we avoid this problem because B will be expecting 2 and 3, and only 0 and 1 can be retransmitted.
   When network has no lost and ACK each packet in order without delay, GBN could produce the same performance of the unrestricted protocol
4. UDP has no congestion control, if there is network congestion, UDP still sends packets the UDP frames keep congesting the network. TCP detects the network congestion and stops sending packets.
5. Send 24 bits chucks data: 000000000000100000000000

Chuck1: 000000000000
Chuck 2: 100000000000
Sum: 100000000000
Checksum 011111111111
If on the receiver side, receive: 100000000000000000000000
Chuck1: 100000000000
Chuck 2: 000000000000
Sum: 100000000000
Checksum 011111111111
If errors are detected by checksum, it’s guaranteed that errors must have occurred.

6.



7. End to end congestion controls have no explicit feedback from the network, congestion inferred from the system observed loss and delay. In network assisted congestion control, the router provides feedback to the end system. TCP must use end-to-end congestion control rather than network-assisted congestion control, since the IP layer provides no feedback to the end systems regarding network congestion
8. In virtual circuits, each packet carries VC identifies. Link, router may be allocated to VC. VC maintains forwarding table in router which combine incoming interface and incoming

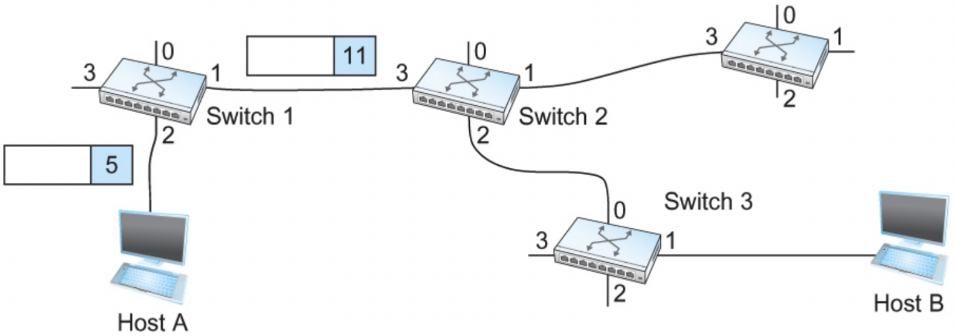
VC numbers with outgoing interface and outgoing VC number

Switch 1 Table

Incoming Interface	Incoming VC	Outgoing Interface	Outgoing VC
2	5	1	11

Switch 2 Table

Incoming Interface	Incoming VC	Outgoing Interface	Outgoing VC
3	11	2	7



9. CIDR, which stands for Classless Inter-Domain Routing, is an IP addressing scheme that improves the allocation of IP addresses. It replaces the old system based on classes A, B, and C. This scheme also helped greatly extend the life of IPv4 as well as slow the growth of routing tables. CIDR also allows the amalgamation of subnets into a supernet for more efficient network routing. One routing table entry represents the entire aggregation of networks. One issue is that CIDR is no longer possible to determine by looking at the first octet to determine how many bits of an IP address represent the network ID and how many the host ID.
10. NAT router remember (in NAT translation table) every (source IP address, port #) to (NAT IP address, new port #) translation pair. For outgoing datagrams, replace source IP address and port with NAT IP address and new port. For incoming datagrams, replace NAT IP address and new port with corresponding source IP address and port stored in NAT table. For P2P applications, there are three solutions: 1. Statically configure NAT to forward incoming connection requests at a given port to the server. 2. Universal Plug and Play, Internet Gateway Device protocol. Application running in a host request NAT mapping its private IP and port to public IP and port. 3. Relaying, both NATed client and external client connects to relay, relay bridges packets between two connections.