1. i. No, intermediate servers cannot use in email, because SMTP protocol is used in E-mail which is a push protocol. So, between sender and receiver all router should always be up and working. If any one of the between router is down, protocol will fail.

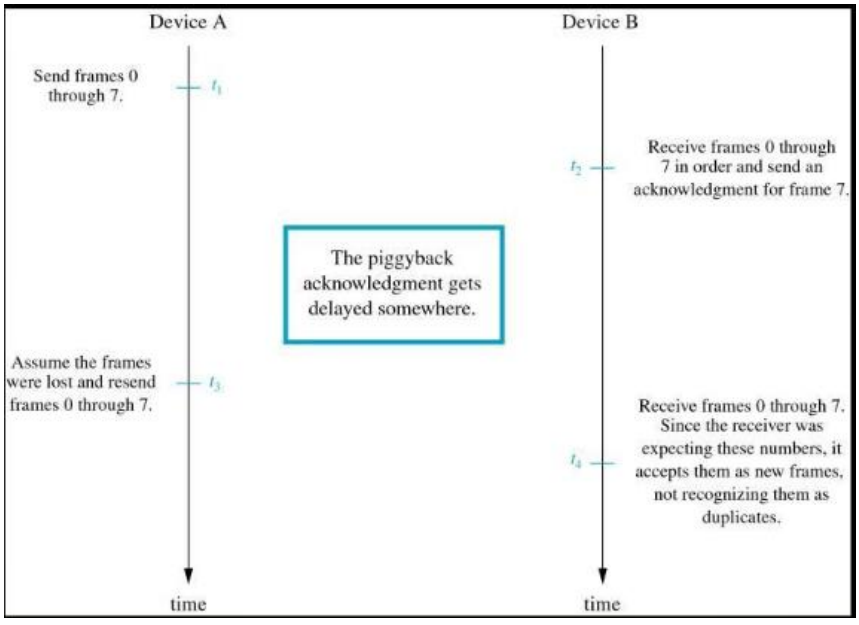
   ii. No protocol can be used other than SMTP. For example, if we use HTTP, then the receiver mail server must check sender mail server periodically if there is any data to be sent.

2. In Client-Server Architecture, the total time for distribution of File size F increases as the no. of clients increase. But in P2P, the upload speed of each Peer is added in the overall upload speed as number of peers, as number of peers increases. Due to this, there is decrease in total time for file distribution. Hence, In File Transfer P2P performs better than Client-Server architecture.

   In client server architecture the total time for transfer file of size F from one server to N clients depends on the no of clients/peers. The distribution time of data increases exponentially with the increase in number of peers. The same also happens in P2P architecture, but whenever number of peers increase the upload speed is also added in the overall upload speed, due to which the overall time for transfer of data is decreased. P2P performs better in every case as compared to client server architecture.

3. Consider k = 3, 2^k - 1 = 7 and Window size= 8 i.e., 0,1…7

In this protocol, problem of duplicates occurs. So, GBN fails under the window size greater than 2^k - 1.



With the same performance, GBN can perform as unrestricted protocol when the ACK is received before the whole window is transmitted and the window will slide down according to the ack received and sends the data.

4. In UDP, it doesn't have acknowledgement mechanism, it just sends data without waiting for ACK of previously send Packets. If any one of the send packets is lost, it doesn't resend lost

packet. While in TCP if packet lost or network is congested then it holds back and does not send the new packet until it gets ACK for previously send Packet. So, UDP can end up TCP frames being delayed indefinitely.

Flow Control mechanism in UDP can mitigate this problem.

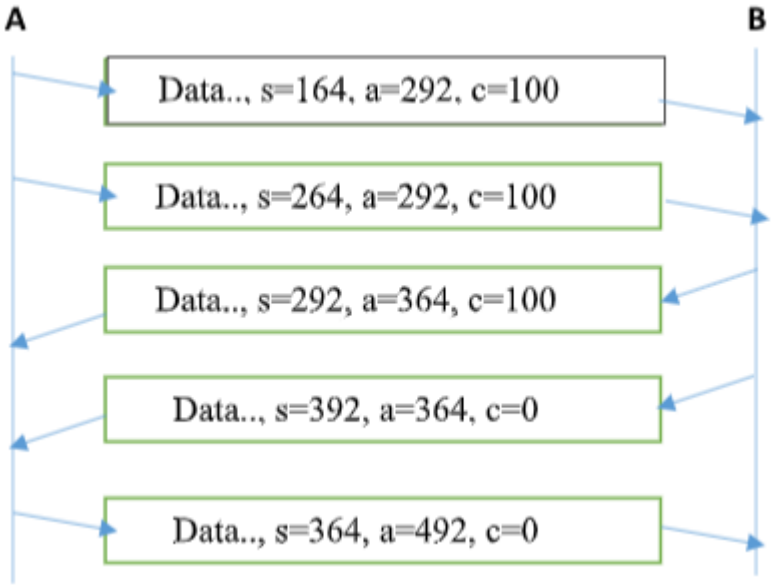
5. Consider the Checksum of 16-bits string: 1010100000110011**10101000**

String1 = 10101000
String2 = 00110011

	10101000	10101001
	+ 00110011	+ 00110010
	---	---
Sum	11011011	11011011
	+ 10101000	+ 10101000
	---	---
	10000011	10000011
Checksum :	01111100	Checksum: 01111100

Both Checksums is same as before

6. Flow is mention below



7. In network assisted congestion control, they are Various drawbacks:

Network elements such as routers must implement the congestion control mechanisms i.e. the network should be smart, which has additional functionality over the network which will affect the overall performance.

Sometimes network providers don't provide congestion control i.e. if this happens then the whole it is of no use and end to end congestion control will have to be again applied.

There might be chances that path from router to sender can also be congested. Due to this, there might be chances that choke packet may or may not reach the sender. If it doesn't reach the sender, the sender will be sending at its usual rate which is doing further harm.

Due to the above reasons TCP uses end-to-end congestion control.

8. In VC network each of the packet in the VC network has a Virtual number instead of the destination address and all router maintains tables which contain information about links associated with router and their outgoing interface. Virtual number is assigned to the dedicated VC network and all the packets consists of this number. Whenever a sender must send the data a VC is established and given a number. All the routers on that VC update their tables with that number and whenever a packet consisting of that number arrives at the router it already knows the destination address of that router and will route that packet accordingly.

9. CIDR – Classless Inter-Domain Routing is a method which is used for allocating IP addresses and IP routing. It is a compact representation of IP address and its routing prefix.

   Advantage: It can be used to manage IP address space effectively and help to reduce the routing table entries.

   Disadvantage: configure with prefix smaller than the classful mask is not possible. For Example, for class C, a mask less than 24 bits cannot be summarized by network.

   Example:

   CIDR looks like 192.168.100.25/24 under IPv4 address with network address being 192.168.100.0 with subnet mask 255.255.255.0 which has 24 leading 1-bits

10. Consider two host are connected to a router with NAT. Due to this, each device is assigned with two addresses on Network. One address is Public (External) Address and other is Private (Internal) address.

    To communicate between two devices that are connected to router, Internal IP address is used and for all devices on network, these addresses are different.

    Public IP address is used to connect to Internet and by default routers with NAT assign same public address to all devices under its network. So, whenever router gets a request from outside it investigates its NAT translation table and maps the WAN address to LAN Address and sends the request to particular host on the network.

References:

[1] Referred Textbook, Lecture Notes, Discussion Done during lecture and Wikipedia Pages of the topics used in above Question.
[2] https://searchnetworking.techtarget.com/definition/CIDR
[3] https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing
[4] https://en.wikipedia.org/wiki/Network_address_translation
[5] https://ieeexplore.ieee.org/document/983548
[6] https://en.wikipedia.org/wiki/TCP_congestion_control