תקשורת ומחשוב חלק ג

1. DHCP server formulates DHCP ACK containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server, encapsulation at DHCP server, frame forwarded through LAN, demultiplexing at client, DHCP client receives DHCP ACK reply, DNS query created, encapsulated in UDP, encapsulated in IP, encapsulated in Eth. To send frame to router, need MAC address of router interface: ARP, ARP query broadcast, received by router, which replies with ARP reply giving MAC address of router interface, client now knows MAC address of first hop router, so can now send frame containing DNS query, IP datagram containing DNS query forwarded via LAN switch from client to 1st hop router, IP datagram forwarded from campus network into Comcast network, routed (tables created by RIP, OSPF, IS-IS and/or BGP routing protocols) to DNS server, demuxed to DNS server, DNS server replies to client with IP address of the local computer, to send HTTP request, client first opens TCP socket to web server, TCP SYN segment (step 1 in 3-way handshake) inter-domain routed to web server, web server responds with TCP SYNACK (step 2 in 3-way handshake), TCP connection established!, HTTP request sent into TCP socket, IP datagram containing HTTP request routed to the local computer, web server responds with HTTP reply (containing web page), IP datagram containing HTTP reply routed back to client
2. CRC is the most powerful method for Error-Detection and Correction. It is given as a kbit message and the transmitter creates an (n – k) bit sequence called frame check sequence. The out coming frame, including n bits, is precisely divisible by some fixed number.

3. **http 1.0 vs http 1.1:** Since http 1.0 is not persistent and you have to request each HTML object individually , there for http 1.0 is not efficient , http 1.0 helps with this problem , it allows requesting multiple HTML objects within one TCP request , for the client to save time and for the TCP not to wait for the client's response , http 1.1 allows requesting all of the objects without waiting for the client response. http 1.1 allows multiple server hosting by including the host in the header , http 1.0 doesn't. http 1.1 allows resuming downloads, using http 1.0 you will have to download the file from the beginning. **http 1.0 vs http 2.0:** http 1.0 requests and responses in a stop-and-wait way which is low efficient , to improve this method http 2.0 uses multiplexing and tags each frame. the client can construct multiple request streams in parallel over one TCP connection. **http 1.1 vs http 2.0:** Since http 2.0 is more flexible with data transfer due to the binary format , it easier for http 2.0 to deal with the robustness (the ability to withstand failures) , then http 1.1. Since http 1.1 is using pipelining a Head Of Line blocking might occur (HOL blocking is when a packet arrives to it's destination the destination port doesn't know how to work with the packet so it blocks all of the other packets from being processed). To fix this issue http 2.0 uses Multiplexing and tags each frame , it transfers the packets parallerly over one TCP connection , the tag allows breaking the packets apart and then reassembling them at the destination which allows to send packets parallerly without blocking the behind packets. **http 1.1 vs QUIC vs http 2.0 vs http 1.0:** Quic runs on UDP, http runs on TCP. Quic is easy to control and performing changes. for example: changing the CC algorithm , you don't have to change the underlying network stack.
4. When you connect to a device, you connect to its IP address. However, that device may be running any number of services, like a web server, an authentication server, a file server, etc. The port number is a way to identify the SERVICE to which you intend to connect. Logically, the different software services "listen" to specific ports.
5. subnet, is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments. we need subnet because, the segmentation of a network address space, improves address allocation efficiency and consequently increasing network speeds.

6. MAC address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. The mac address ONLY identifies the LAN adapter in the ethernet layer (Layer 2 Simplified OSI model).The IP address (TCP and/or UDP) ONLY works in the IP layer (Layer 3). Not all communication using IP goes via ethernet. IP can be send over other Layer2 layers where there are no MAC-addresses, And Ethernet can carry other Layer3 traffic, besides IP, which don't use IP-addresses at all. In case of IP over ethernet you need BOTH identifiers, simply because both the layers involved require each their own ID system.
7. **Router vs Switch:** 1. Routers operate at Layer 3 (Network) of the OSI model, where Switch operates at layer 2 (Data link layer). 2. Router operations revolve around IP addresses , where Switches work with MAC addresses as it operates within the borders of a single network. 3. Routers can work within both wired and wireless network situations , where Switch are restricted to wired network connections. 4. Router help users to take the faster routing decision, Switch will more likely take a more complicated routing decision. **Router vs Nat:** NAT is a way to have multiple internal devices use a single public address to reach the internet. It's like having multiple people sharing an apartment, so they all have the same mailing address, but inside, everyone knows whose room is whose. Routing is literally transferring packets from one place to another until it reaches the target destination. **Switch vs Nat:** Switching connects hosts at layer-2, while NAT is a kludge that is designed to extend IPv4 layer-3 addresses until IPv6 can become ubiquitous. NAT breaks the IP promise of unique addresses for every host and end-to-end connectivity.
8. **Using IPv6 addresses**, which is having large address space, more unique addresses are available, so IPv6 addressing resolves shortage of IPv4 addresses. **Network address Translation:** In this mechanism, NAT router translate the public address to private address. single IP address is used to represent group of connected devices. So shortage of addresses can be resolved in this mechanism.
9. We will detail in general about the OSPF, RIP, BGP protocols

OSPF - works within ASS, uses the cost of data transfer to calculate the distance, and will always choose the cheapest path to transfer a packet from source to destination - usually more dynamic than other protocols.
RIP - Counts the shortest number of steps on one router to another router.
BGP - Managed using a table of the networks connected to it, and the connections between them and other networks, and executes routing decisions based on the

connections between the networks and policies dictated manually by the network administrator.

In general when different routers learn about a particular subnet sitting behind a router, then the same router sends to its neighbors in the same AS messages depending on the protocol, i.e. choosing the route that is best to reach so that all their neighbors know them, once all its AS neighbors know it .

We will see in this question the integration and connectivity of the protocols.

Let us look at and explain the value of X in all the last four sections. X represents what is the last protocol he sees.

Router C3 - Because it is the external router in 3AS then it speaks in BGP with the 4AS, according to figure (d).

Router A3 - This router learns from C3 router. After C3 learned from OSPF, after the last protocol he saw is OSPF.

Router C1 - learns after a3 and from what he talks to, according to figure (d), the protocol is BGP.

Router C2 - learns within 2AS, according to data (a), in the OSPF protocol.