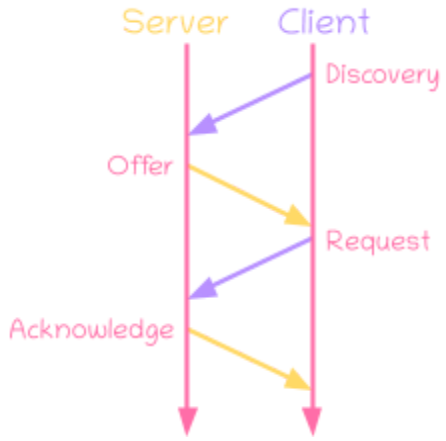
What is DHCP? Using a timeline diagram, show an example of a client getting its IP address from a DHCP server. (10 Points)



DHCP stands for Dynamic Host Configuration protocol, and it is a way for organisations or other institutions with a block of IP addresses to assign each individual host on their network with an IP address dynamically. A DHCP server runs on UDP port 67 and offers IP addresses to hosts using the timeline shown in the diagram. Hosts first send a discovery packet looking for a DHCP server to respond, then the server responds offering an IP address. The host responds requesting the offered IP address, and the server acknowledges that it has given the host the IP address, and also sends the name of the first-hop router, name and IP address of the DNS server, and a network mask which shows the host portion of the network address.

What is NAT? Clearly explain how the translation is done. Describe at least two solutions for a client which wants to connect to a server within a NAT subnet. (12 Points)

NAT is a temporary solution to the problem that eventually we will run out of IPv4 addresses, so in some scenarios, a subnet will be created with a gateway router which has a unique IP address, but the hosts behind it will not and will not be visible to the outside network. All the communication will happen through the gateway router using Network Address Translation. The gateway router maps each of its hosts to a port number on the gateway router's IP address and stores the information in a NAT translation table.

When a host wants to send a packet to an outside address, the NAT router stores the LAN address and host port number in a table in the same row as the router's address and router's outgoing port number, and sends the packet using the router's address and port number. When the remote address responds, the router uses the NAT table to find the entry corresponding with the router's address and specific port number that was used, which will return the LAN address and host port number of the actual host which sent the packet. The router will then send the packet received from the internet to the actual host using the LAN address and host port number stored in the table.

If an outside client wants to connect to a server within a NAT subnet, we can either statically configure the NAT router to always forward data on a specific port of the router to the LAN address of the server within the NAT address. Another solution is to allow the NATed servers to request that the router connect the private address and port number to the address and chosen port number of the router. If the router allows it, then the private server knows its new public address and port number and can advertise to remote hosts to connect to this public address and port number which will then be forwarded to the NATed server using the NAT table. This last one is called universal plug and play.

List the fields in IPv6 datagram format. What is the purpose of each field? (10 Points)

Version: 4 bit field which identifies the IP protocol version number. Will be 6 in IPv6
Traffic class: can distinguish between different kinds of data traffic like real time, non realtime, etc
Flow label: loose definition of a flow, but can group packets as different "flows" like audio video, and other loose categorisations of kinds of packets
Payload length: number of bytes of data in the packet not including the fixed length header
Next header: identifies the kind of protocol the data within this packet is using (TCP, UDP, etc)
Hop limit: value decremented by one each time the packet is processed. If it reaches zero, the packet is discarded. Same as time to live in IPv4
Source address: IPv6 address that the packet was sent from
Destination address: IPv6 address that the packet is going to
Data: the actual data being sent in the packet

Differentiate (at least three differences) between IPv4 and IPv6. (6 Points)

IPv4 uses 32 bit addresses meaning there can be 2^{32} IPv4 addresses, and we are running out of them. IPv6 has 128 bit addresses, so there are 2^{128} addresses, so a whole lot of them, almost too many to comprehend. IPv4 uses only numbers separated by dots, but IPv6 is alphanumeric separated by colons, where each 4 character section is hexadecimal. IPv6 has 8 header fields where IPv4 has 12, but the total header length for v6 is longer than v4.

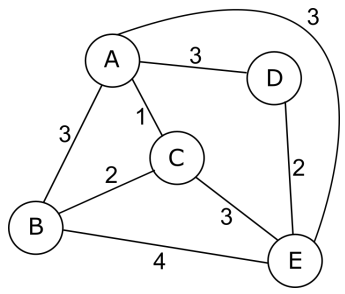
What is tunneling? How and why is it done? (4 Points)

Tunneling is done when trying to send IPv6 across a path which contains an IPv4 router. When the v6 packet needs to cross the v4 router, the entire v6 packet including header is wrapped in a v4 header as the data payload of a v4 packet. Once that packet has passed the v4 router, the next v6 router it hits will unwrap the v4 header and continue sending the v6 packet as normal. This is done because not all routers will immediately become v6 routers. People will gradually change to v6, but for a long while there will still be v4 routers that have not been replaced, and these could be required on paths that packets need to take.

What is the functionality of the data plane and the control plane in the router? (4 Points)

The control plane is where the best path between a source and destination is determined via routing algorithms. In per router algorithms, each router works with each other to compute the forwarding tables. The forwarding tables within each router however, are actually part of the data plane because this is where they are used to choose the correct port to forward incoming packets to.

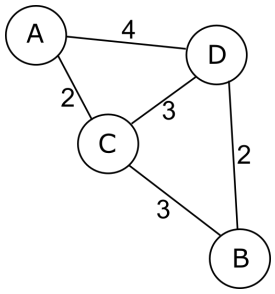
Using Dijkstra's algorithm and using the table shown in lecture videos, compute the shortest path from B to all the network nodes and find the routing table at router B for the network shown in Figure 1 (10 Points)



Step	N'	D(A)	D(C)	D(D)	D(E)
0	B	3, B	**2, B**	∞	4, B
1	BC	**3, C**		∞	4, B
2	BCA			6, A	**4, B**
3	BCAE			**6, E**	
4	BCAED				

B to A: B, A for 3
B to C: B, C for 2
B to E: B, E for 4
B to D: B, E, D for 6

Using the Distance-Vector algorithm, compute the shortest path from A to all the network nodes and find the routing table at router A for the network shown in Figure 2. (20 Points)



	A	B	C	D
A	**0**	**5**	**2**	**4**
B	5	0	3	2
C	2	3	0	3
D	4	2	3	0

What is hierarchical routing? Differentiate between (at least two differences) intra-AS and inter-AS routing. (6 Points)

Hierarchical routing is splitting the entire internet into different subgroups of subgroups, and each of these subgroups and levels of subgroups use their own routing algorithms that don't necessarily need to know the details of any other group. This is because at some point the larger and more complex a network becomes, the less effective it is to try and manage all the hosts as a single network, and it's better to break the network up into independently routed subnetworks which then communicate with each other. These are then called autonomous networks. Each of these autonomous networks routes within itself using intra AS routing algorithms. Then, each of these ASs communicate with each other and route between each other using inter AS routing. The routers within an AS all run the

same routing algorithm. One example is Open Shortest Path First. The routers all must use the same inter AS routing algorithm. This is called Border Gateway Protocol

What are the two commonly used intra-AS routing protocols? Describe the OSPF protocol. (6 Points)

Two commonly used protocols are Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). OSPF is using Dijkstra's algorithm or link-state routing algorithm. Once the routing table is calculated for the entire AS that table is broadcast to each router in the AS

Describe the BGP routing protocol. What do the eBGP and iBGP protocols do? (6 Points)

BGP is how separate ASs transport packets from one to another. eBGP is obtaining the reachability of other subnets from the neighboring ASs, and iBGP is broadcasting that reachability to all the ASs internal routers.

What is the use of ICMP protocol? Describe how the traceroute application uses the ICMP protocol? (6 Points)

ICMP is used to communicate network layer information between hosts. This is used for error reporting such as dropped packets due to TTL where the router where the packet was dropped sends an ICMP packet to the source router. This can be used by a traceroute program to compute round trip time on all the routers on the way to the destination router.