Homework 3, David Rasoly.

Question 1:

A) The application of Host A will use UDP service at the transport layer, this will be done by building a UDP packet format which includes source port, destination port, length, checksum and data payload.
Then, the UDP packet will pass to the Network layer, where an IP datagram will be built. The IP datagram will be divided by header and payload, and contains the payload type (UDP), length of header, length of datagram, TTL, source destination, protocol, and checksum.
Since the 8 MSB are are the same for both source and destination, we know that both the source and target addresses are at the same network, the Link layer MAC address destination should be found using ARP, which can provide the mapping of the MAC address using the I.P. destination address.
If the cache of the ARP has the mac address for the destination IP address, it will be resolved instantly.
However, if the ARP cache isn't familiar with that I.P., then the ARP will initiate a broadcast frame request which asks which computer at the network has the MAC address that matches the destination I.P. address.
Host B will response that it has the matching MAC address,and the cache of the ARP will be updated with the new MAC to IP address mapping.Now that we have the mapping, The original IP datagram will be built as an Ethernet frame and will be passed to the Link Layer. The frame will contain a header and a source - the header will contain the source and destination MAC addresses, and the payload will contain the source IP address and the original payload, as in most datagrams, it will contain a checksum at the end.
The Ethernet frame will be sent to the Network layer, building again the I.P. datagram back to the Transport layer and the host of the destination source, host B.

B) The application of Host A will use UDP service at the transport layer, this will be done by building a UDP packet format which includes source port, destination port, length, checksum and data Payload.
The UDP packet will pass to the Network layer, where an IP datagram will be built. The IP datagram will be divided by header and payload, and contains the payload type (UDP), length of header, length of datagram, TTL, source destination, protocol, and checksum.
This time,the 8 MSB of the source and target addresses (13 and 18, respectively) are not at the same network, this means that the destination IP address will be introduced to the routing layer of the 13.0.0.0/8 at the Network Layer. This means that 13.0.0.0/8

Network Layer now understand that in order to reach 18.0.0.0/8 it has to pass through 13.0.0.1. Which is now mapped to 18.0.0.1.
The Network Layer will check whether the ARP's cache has an address for the router, therefore a broadcast will be sent by the Physical Layer to ARP at the Link Layer to check which host has the MAC address that I.P. that matches 13.0.0.1.
The router host response with its MAC address at the ARP's cache will be updated with the new mapping to its' I.P.
Now that we have the mapping, The original IP datagram will be built as an Ethernet frame and will be passed to the Link Layer. The frame will contain a header and a source - the header will contain the source and destination MAC addresses, and the payload will contain the source IP address and the original payload, as in most datagrams, it will contain a checksum at the end.
The Ethernet frame will be sent to the Network layer, building again the I.P. datagram. The address will be resolved by the routing table to Router 2.
The Network Layer will check whether the ARP's cache has an address for the destination host, therefore a broadcast will be sent by the Physical Layer to ARP at the Link Layer to check which host has the MAC address that I.P. that matches 13.0.0.8.
The destination host response with its MAC address at the ARP's cache will be updated with the new mapping to its' I.P.
Now that we have the mapping at 18.0.0.0/8 network, the original IP datagram will be built as an Ethernet frame and will be passed to the Link Layer.
The frame will contain a header and a source - the header will contain the source and destination MAC addresses, and the payload will contain the source IP address and the original payload, as in most datagrams, it will contain a checksum at the end.
The Ethernet frame will be sent to the Network layer, building again the I.P. datagram back to the Transport layer and the host of the destination source, host D.

Question 2

A) The tuple is used to create a set of five connection characteristics that together creates a unique combination of connection between peers. The five Tuple characteristics are :
    a) Protocol - Could be either UDP or TCP.
    b) Local I.P. Address.
    c) Local Port.
    d) Remote I.P. Address.
    e) Remote Port.

   The ports are provided by the local and remote operating systems, and the I.P.s are the address of the local and remote hosts, the port suggests the process of which the packet is designated arrival or source to depart from. The IP address and destinations are part of the TCP or UDP request headers.

B) I will assume for the question that both the web and email connections are done using TCP protocol. The connection at TCP is initiated with SYN command, and once the connection is established and packages can be sent over the two connections.
The operating system of the client will arbitrary choose free ports for both the connection, let's assume port 101 for web connection and port 102 for email.
The I.P. addresses of both the client and the server are the same, so the server's operating system will allocate two ports of its own that are used for both the services, assuming 201 for web connection and 202 for email connection.

The 5 tuple table connection, under the port number assumption :

Protocol	Local I.P.	Remote I.P.	Local Port	Remote Port
TCP	18.19.20.21	129.103.104.105	101	102
TCP	18.19.20.21	129.103.104.105	201	202

Because both Local Port and Remote Port are different, the connections are unique even though the I.P.s and the protocol of the two different connections are the same.

Question 3 :

A) The column heading of a RIP distance vector routing table are:
   a) Destination Network and Mask - IP of the destination network address that matches the network mask.
   b) Metric - the number of hops to the final destination. A metric value of 1 indicates that the final address is connected to the directly.
   c) Next Hop I.P. address - the next I.P address of the router at the path for the final destination.
   d) Port - The port that used by the router to send packets.

B) The routing protocol to choose for a large network would rather be OPSF over RIPv2. The reason for this is due to the "mathematical" nature of of a network - a network is a graph (depending on topology, but it is a graph anyway) , and the bigger a graph, the more unique paths it will have. Considering features of OPSF, The reason that I'd think that OPSF is more ideal are :
   a) For a bigger network, it is important not to be bound to the RIPv2 constraint of 16 maximum hops.
   b) PSPF allows dividing the network to areas using partitions, this could shorten the path depending on the areas.
   c) A larger network would probably be a corporate or other big organization that might need security feature that could be supported better by OPSF.

Question 4 :

The UDP pseudo-header contains the following fields:

1. Source Host IP address.
2. Destination Host IP address.
3. UDP protocol number.

The checksum is a function that takes into calculation the I.P address information, and once it is sent to its' source destination with the correct protocol, it is calculated again to verify that it indeed arrived to the correct address with the correct protocol.
The problem that can arise with this checksum mechanism is that should the checksum is wrong, than the assumption is that the problem was the I.P. address number, where in fact it could be the wrong port number, as they both used to calculate the checksum.

Question 5 :

Flow control is the way to control the amount of data that passes between the sender to the receiver, this needs control to prevent receiving more data than the receiver can handle. The Control flow is measured by a sliding window, this window is implemented as a field at the TCP protocol and adjusts itself to the ideal sliding number which represents the best maximum amount of packets that can be sent in a stream until an ack is sent. The higher a sliding window is - the more efficiently a data could be sent and received.
Congestion control is a mechanism that helps determine what should be the ideal sliding window. Once connection is acknowledged, the sliding window grows and gets double after each acknowledgement. Once one packet or more stopped arriving due to heavy load, the sliding window is divided by half, this deemed as Congestion Avoidance Algorithm.
Both Congestion Control and Flow Control help achieving an optimal usage of the network between the peers.

Question 6 :

A) NAT or NAPT allows mapping between private network host connecting to an external public host. Because private network has an I.P. address (or address) that are known to a public network, the external address of the private network is not enough information to access a specific host within the private network. Therefore, additional two columns will be added to the 5 tuple :
    a) Unique NAT source port number - a mapped port number.
    b) Public source I.P address - the I.P. of the NAT box.

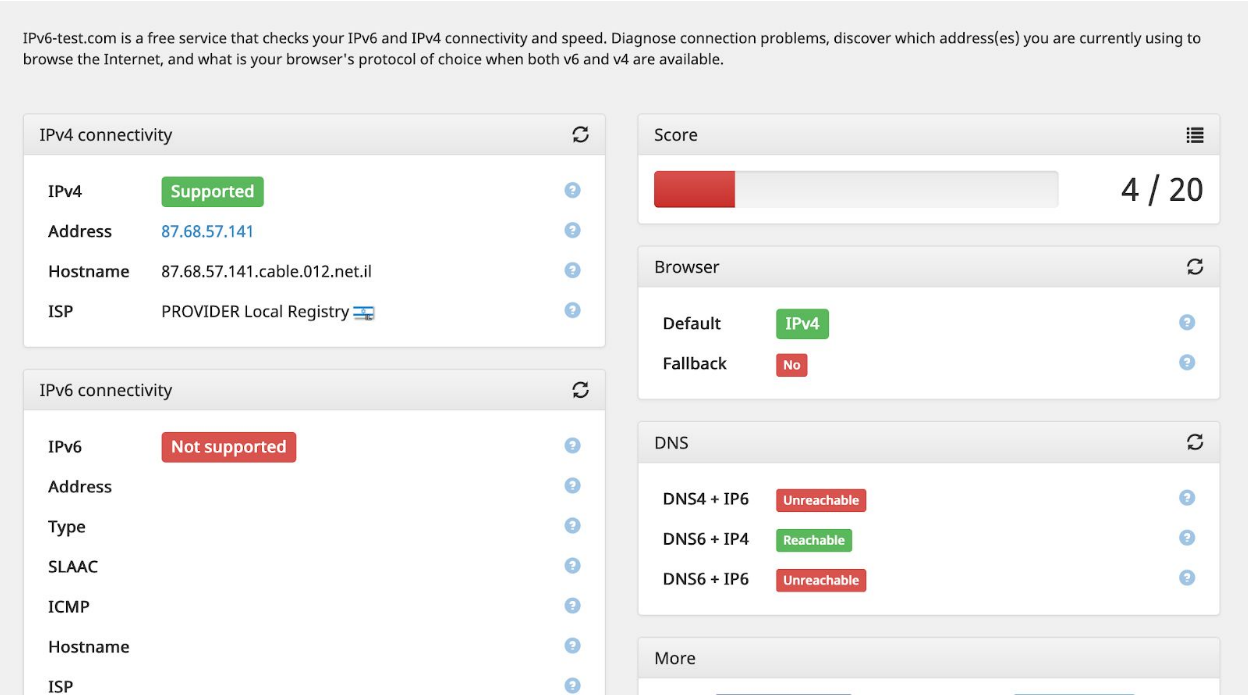
The NAT source I.P address and the port numbers are used as a mediator between the internal endpoint and the actual external destination endpoint. The checksum calculation occurs every time a packet arrives to the NAT box, thus, the final destination host will not be aware of the actual I.P. of the sender host.

B) Because the destination address doesn't know the actual I.P. of the internal source host, I'd assume that any UDP protocol affiliated at the application layer wouldn't be ideal, simply because the checksum mechanism at UDP can mistakenly calculated wrongly, and thus more prone to miss the the source address - if a packet could sometimes be dropped due to wrong checksum calculation at UDP (because of the protocol and I.P. calculation), then when a NAT box is involved, this could occur more often, and statistically more packets are likely to be dropped.

Question 7 :

A) I'd say that in order to establish a connection between a source and destination that would support IPv6, then all of the components within this network should support it. This means all of the host machines operating systems, the routers, the I.S.P infrastructure, the routing protocols and related software that support the hardware - simply because in a network, multiple paths could be taken into consideration to establish a connection between peers. I could think of a bypass when not all nodes support IPv6, is if the network routing protocol is OPSF, and some areas and partition are designed to be purely IPv6 by configuration, then within these areas, IPv6 could work between peers, even if not all of the network items support IPv6.

B) Using www.test-ipv6.com, I can say that my home network does not support IPv6 :



IPv6-test.com is a free service that checks your IPv6 and IPv4 connectivity and speed. Diagnose connection problems, discover which address(es) you are currently using to browse the Internet, and what is your browser's protocol of choice when both v6 and v4 are available.

IPv4 connectivity

IPv4	Supported
Address	87.68.57.141
Hostname	87.68.57.141.cable.012.net.il
ISP	PROVIDER Local Registry

IPv6 connectivity

IPv6	Not supported
Address	
Type	
SLAAC	
ICMP	
Hostname	
ISP	

Score

4 / 20

Browser

Default	IPv4
Fallback	No

DNS

DNS4 + IP6	Unreachable
DNS6 + IP4	Reachable
DNS6 + IP6	Unreachable

More

In my country, Israel, the internet service is provided by two companies, the infrastructure (who owns the local cables and routers and connection at a region of a city) and service provider, the ISP which acts as an actual ISP.

From the diagram above we can see that luckily I have an internet connection, using IPv4, but IPv6 connection is not supported, and therefore an address, hostname and ISP couldn’t even be provided. There is a support of DNS6 over IPv4, which means that it is possible to connect to IPv4 hosts which served by IPv6-only name server, but not the other way around.