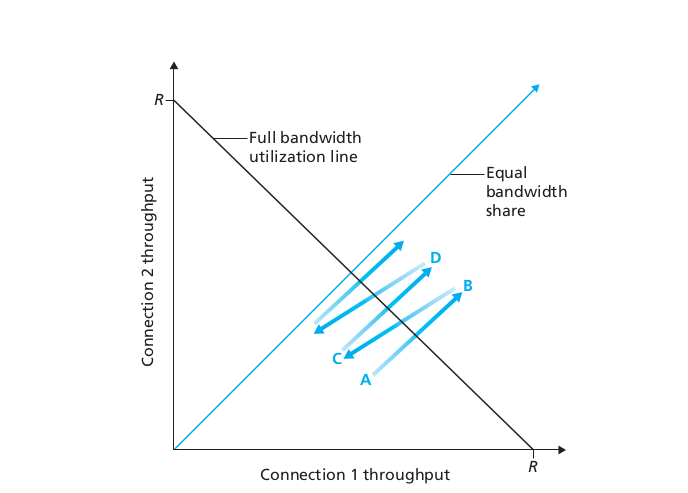
1. a) “TCP(All variations in use today's Internet) uses AIMD(Additive Increase Multiplicative Decrease) algorithm, which ensures fairness. How? Because hosts increase their bandwidth additively, but when congestion occurs they drop their bandwidth multiplicatively. So, the host with higher share, loses most. After that every host increase their share by same amount(additively). As this steps happens again and again, bandwidths converge to fair amounts”

<https://stackoverflow.com/questions/32394730/networking-is-transmission-control-protocoltcp-ensures-fairness-among-multipl>

A more detailed explanation is given in 3.7.1 (pg. 280 - 282) of “Computer Networking - A Top Down Approach” (the course textbook), but it’s too long to paste here. It’s along the same lines of the answer given above though.



b) No we could all remember an ip address of google.com and DNS wouldn’t be needed.  
(But google gives URLs and not direct ips :o)

Necessary given that the Web has become a global construct and it is impractical to have all users remember the IP addresses of all the sites they want to visit. Moreover, these addresses will change over time (e.g. if the site needs to be moved during maintenance). Hence a service that performs the role of DNS will be required for the Web to function today.

c) i. A packet filtering router is a router (forwarding device on the network layer) that controls network traffic

by monitoring incoming and outgoing packets, deciding which ones should halt and which ones should pass.

ii. A circuit level gateway is a kind of firewall between application and transport layer that monitors TCP handshaking between packets to determine whether a requeested session is legitimate. (eg Tor)

“acts like a (non-caching) proxy, viz. it fully takes over the host’s communication with the recipient, and then decides what to allow/block” - Week 5 page 34

iii. An application level gateway is a security component that augments a firewall or NAT. Allows the firewall to look inside packets and see what the application is doing with that packet - e.g can distinguish HTTP for web browsing from HTTP for peer-to-peer file sharing.

d) i. TCP Assuming a separate ACK packet is sent for every packet and no loss: 3 (establish connection) + 1 (send request) + 1 (request ACK) + 2\*n (packets for data and ACKS)t

ii. UDP assuming no loss: 1 (send request) + n (packets for data)

e) UDP is faster to transmit objects like picture or video, but not reliable and may transmit wrong HTML page

f)

i. Max no. sequences = 2^32 –1 so to exceed sequence numbers must send 2^32 bytes.

L therefore no greater than 2^(32) - 1B assuming that segment only contains data, s eq nos begin from 0

ii.

\*Corrected units for data transfer rate\*

1 packet has size 536 + 64 = 600 B

No. of packets = 2^{32}-1/536

Time taken to transmit 1 packet = (600 \* 8) / (50 \* 10^6) s

Hence total time taken = no. of packets \* time taken for 1 packet = 12.8 min (to 3 sf)

2. a) Each item in vector represents (Destination, Next router, Path length). Router looks up destination router then uses the next router as the ‘next hop’ address, forwarding packet there.

b) i) Good news propagates quickly through the network so if a router such as R1 was down and comes back up then the network would realise this quickly. Also costs are calculated dynamically and so account for network cost.

Short, optimal routes

ii) Bad news propagates slowly through the network which means that the network may suffer from a count-to-infinity problem e.g. if R1 goes down, all routers increase their routers up to infinity thinking they know where R1 is.

Each router has to allocate memory for their routing tables => Resource expensive

c) Errors: (R4, R3, 1) -> (R4,R4,1) ; (R5, R3, 7) -> (R5, R3, 6)

d) Believe to be 2: once to 1,3,4 then further to 5,6. 2 as not yet mapped to R7, R6 does not yet have its minimum path length

e) Incorporate changes from C and update R6: **(R6,R3,7)** . R7 would change to **(R7,R4,13)**

f) Anyone care to answer the last part?

Shorter distance fraud -

i) A malicious router claims to have a shorter distance to another router than it actually does.

Other routers will therefore use the malicious router as it is seemingly a shorter path. The malicious router attracts traffic and then drops all the packets so they never reach their destination. This is called a black hole. Alternatively, it could use this method to eavesdrop.

ii) To avoid eavesdropping: encrypt data