Midterm 1

1) a) Ethernet addresses are unique and a part of the hardware; it is burned into ROM when the node is created.

b) Requesting 5.6.7.8
R1 will receive it

c) Collision avoidance would be unfeasible. Exponential backoff could lead to very long wait-times, as there would be significantly more traffic. If you tried to counter this with switches, there would be exponetially more switches!

d) The first part of the IP is the prefix and specifies the network. Since packets first try and find the network, and then the device, and because computers can switch networks, it's necessary for computers to have different IP prefixes (depending on the network it's in) and thus have different addresses.

e) There is more structure to IP addresses, as we can seek out networks instead of individual devices. So, we don't need to broadcast packets as widely; we can have them forwarded towards different networks, and then towards individual computers.

2) a)

	After	NAT
	Src	Dest
IP	105.10.2.5	201.20.4.7
TCP Port	5555	20

We need to modify the IP source address to that of the NAT's public address, since the outside server doesn't know about the 192.168.4.2 address (it's not routable on the internet).

* b) The forwarding table should keep track of the remote host, remote port, outside source port, inside host, and inside port.

c) Address 192.168.4.2 is not routable on the broader internet and it is impossible for an external host to initiate a connection.

d) Again, it's not possible for an external host to establish a connection to a client within a NAT. When the server sends information back, it'll reach the outside address, but there will be no information in the NAT's table that will allow the packet to reach the client itself.

e) Layers should only communicate with the layers directly above or below it. FTP is the application layer, but is interacting with the IP layer, which it shouldn't do.

Bonus When the NAT external port recieves an outgoing PORT message, it should save all the information described in part (b) in its routing table, and treat responses from the server as responses to any other packet.

3) a) A can advertise 100.20/16

b) B will advertise 100.20.128/17

c) B will advertise 100.20/16

d) False, as peers only export routes to customers (not to their peers' customers).

e) No, it won't. X will export all of its own routes to its neighbors, but not routes it knows only from its provider (otherwise X would provide free transport from B to Y).

4) a) ~ A-B link fails
~ B advertises distance of infinity to A
~ D and C advertise distance of 2 to A
~ D decides it can reach A in 3 hops thru C
~ B decides it can reach A in 4 hops thru D
~ C decides it can reach A in 5 hops thru B

This continues! Now we have a count-to-infinity scenario

b) This would not work, as this loop relies on three nodes. D advertises to B a route that it learned thru C, B advertises to C, and C advertises to D. This isn't prevented by poison reverse

c) In link-state routing, each node keeps a full map of all directly connected nodes. When links fail, all nodes can immediately recalculate. Since all nodes (eventually) have complete information, count-to-infinity can't happen (since that depends on incomplete information).

d) Path vector gives each node the explicit path to reach another node, not just the distance. Upon link failure, nodes will update paths, and can avoid adding paths that include failed links

5) a) Using Shannon's law for channel capacity:

$$C = B\log_2(S/N) = 4\times10^6(\log_2(512)) =$$
$$= 36\times10^6$$
$$= \boxed{3.6\times10^7 \text{ bps}}$$

b) $\sqrt{512} = 22.63 \Rightarrow \boxed{22 \text{ levels}}$

c) ~noise power

~channel bandwidth