Week 4 (Networking and the Internet) Exercises

Questions

Q1:: What are the differences between star and bus topologies apart from the physical appereance?

Q2:: Which networking classification would you choose to use if you are creating a network in a school environment? (WAN, MAN, etc)

Q3: Give three examples of network topologies?

Q4: Why do we need protocols in networks?

Q5: How does CSMA/CD work?

Q6: What is the difference between *repeater* and *bridge*?

Q7: How can you combine two incompatible networks together and what is it called?

Q8: How does a router knows which device has which address?

Q9: What are the differences between client/server model and p2p model?

Q10: Why cluster computing is good for high availability?

Q11: What does Domain Name Servers do?

Q12: What is grid computing?

Q13: Why do we use collision avoidance (CSMA/CA) instead of collision detection (CSMA/CD) in WiFi?

Q14: What are the four layers in Internet Protocol? What are their roles, write in detail.

Q15: Why is TCP connection-oriented?

Q16: Why is TCP reliable?

Q17: Why UDP is more suitable in online games compared to TCP?

Q18: In which cases using UDP can be advantageous?

Q19: In case of a congestion or a problem in network, what is used to make sure that the package is not being forwarded infinitely?

Q20: What is DoS (Denial of Service)?

Q21: Name 3 differences between Client/Server model and P2P.

Answers

A1: In star topology, machines are communicating with each other through a central unit. In bus topology, they are communicating with each other over a single bus.

A2: Local Area Network (LAN). If you are talking about a single building or a campus, local area network is the most suitable.

A3: Bus, Star, Mesh, Line, Ring, Tree...

A4: For a network to operate functionally, there must be rules. Otherwise how would the computers communicate with each other? Protocols are rules for a network to function reliably.

A5: Each message is broadcasted to all machines in the bus. When a machine receives the message, it checks whether it is addressed to itself or not. If the message is not addressed to itself, it does not store it. When sending a message, every machine monitors the bus to see if it is silent or not. If it is available, starts transmission but still monitors. If someone else tries to send a message, they both understand there is a collision and pause for a random period before re-transmission.

A6: Repeater does not care about the meaning of the messages. It just passes signals back and forth. Bridge is more complex. It also connects two buses, but it checks the destination address of each message only forwards it when it is addressed to the other side.

A7: You combine two incompatible networks together by using *routers*. It is called *internet*.

A8: Forwarding table helps router to choose directions for the messages.

A9: In client and server model, single server provides services to multiple clients. In P2P, they provide services to each other; peer to peer. In CS model, a server must execute continuously to provide for clients, in P2P it only executes on a temporary basis.

A10: Because in cluster computing, there are several machines working together. Even if one of them fails, the task can be done by other computers in the cluster.

A11: Every machine has an IP address. However, this is hard to memorize. Memorizing and remembering names instead of numbers is easier for most people. That is why, for every website we have a name to remember them. When we try to connect to a website, we send a request. At some point, that request goes to DNS server. At that server, it has a database mapping addresses into IP

addresses. So, DNS servers let us use the name addresses instead of numeric IP addresses.

A12: When our computers are idle, we can use certain software to make them aparticipate in certain initiatives such as medical research etc. It is similar to cluster computing but here the computers are loosely coupled.

A13: CSMA/CD is not compatible with wireless star networks. Because in those networks there is no way to see whether the communication line is busy or not. In CSMA/CD, before sending a message machines check the availability of the bus. Here, this is not possible. In addition, transmission may collide and signals can be blocked because of the environment. That is why wireless networks try to *avoid* collisions rather than *detect* them.

A14: Application Layer, Transport Layer, Network Layer and Link Layer.

1. Application Layer: Deals with messages from the application's point of view.
2. Transport Layer: Converts messages into segments and ensures that they are compatible with the Internet. Adds sequence numbers so that they can be reassembled at the destination. Creates **packets**.
3. Network Layer: Directs segments through the Internet. Decides which direction a packet should be sent by maintaining the *forwarding table*.
4. Link Layer: Handles the actual transmission of the segments. Responsible for transfer of the packet. It deals with the communication details, i.e. uses CSMA/CD or CSMA/CA.

A15: In order to provide reliability. TCP creates a connection because it wants the destination to know that a message is going to be sent. By receiving an *acknowledgment* it knows that the server is up and waiting for a message. This gives TCP certain advantages such as re-transmission of the lost packages.

A16: TCP is reliable because it uses *acknowledgments* and *packet retransmission*. If a packet is lost, origin will know of this and re-send the lost package and therefore provide reliability.

A17: In UDP, there is no retransmission. In addition, in online gaming, it is not logical to retransmit lost packages because online gaming is real time and fast. Therefore, in real time applications UDP is suitable. It is faster because there is no overhead (packet size is smaller).

A18: In real time scenarios such as video streaming, voip, online gaming and situations where re-transmission is not needed such as DNS.

A19: Hop count. When there is a blockage, the traffic must be routed around. However, it should not be infinite. Therefore for every hop in the network, hop count decreases from 64. When it becomes 0, it stops.

A20: When a DoS attack is done, the purpose is to put the remote machine out of service. This is done by sending a large number of messages over a brief

period of time and the remote machine / target computer is overloaded. Because of this, it will be down and no longer available.

A21: In Client/Server models, a single server provides to multiple clients; in P2P machines are providing services to each other. In CS model a server must execute continuously at all times, P2P executes on a temporary basis. P2P distributes the service task over many peers rather than concentrating on one server (think of torrent, you can download the same thing from different peers)