Zhuang Jianning
A0214561M

1. As a communication systems engineer, what are the metrics you would use in system design?

Some performance metrics include delay, throughput and packet loss.

Delay specifies the latency of data traveling across the network from one end to another. It is usually divided into processing delay, queuing delay, transmission delay and propagation delay.

Throughput measured in bits per second (bps) is the rate at which data is successfully transferred over a communication channel.

Packet loss refers to the number of data packets that were successfully sent out from one point in a network, but were dropped during data transmission due to errors or congestion.

2. Describe the layers and corresponding functions of the OSI reference model. What layers comprise the TCP/IP stack?

There are 7 layers in the OSI reference model.

Physical Layer
The physical layer deals with the physical characteristics of the transmission medium. It defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems. Such characteristics include voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes.

Data Link Layer
At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer. Media Access Control (MAC) provides flow control and multiplexing for device transmissions over a network while the Logical Link Control (LLC) provides flow and error control over the physical medium as well as identifies line protocols. The data link layer uses the MAC address to define a hardware or data link address in order for multiple stations to share the same medium and still uniquely identify each other. It also frames the data in a way that is meaningful to the receiver using special bit patterns, adds physical addresses of both sender and receiver in every frame, and controls error by detecting and retransmitting frames.

Network Layer
The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). It also decides the ideal route for information transfer from source to destination. This process is known as routing.

Transport Layer
The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts to ensure end to end reliability. Layer 4 protocols include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Session Layer
The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and terminated at Layer 5. Session layer services also include authentication and reconnections.

Presentation Layer
The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. This layer can also handle the encryption and decryption required by the application layer.

Application Layer
The application layer is the OSI layer that is closest to the user. It provides network services to the user's applications. At this layer, both the end user and the application layer interact directly with the software application.

The TCP/IP Model is made up of the Application Layer, Transport Layer, Network Layer, Data Link Layer and Physical Layer.

3. What are the pros and cons of cross layer design?

Cross Layer design refers to protocol design done by actively exploiting the dependence between protocol layers to obtain performance gains compared to layered design where protocols at different layers are designed independently, architecture forbids direct communication between nonadjacent layers, and communication between adjacent layers are also limited to procedure calls and responses.

Pros of Cross Layer design include performance gains by exploiting the dependence between protocol layers or by violating the layered architecture. Examples include a new interface between non adjacent layers, viewing layers as a superlayer, designing protocols with other layers in mind, having a shared database across all layers or a completely new abstraction. Cross Layer design can also fully utilize opportunistic communications offered by wireless networks which cannot be sufficiently exploited in layered design.

Cons of Cross Layer design include excessive architecture violations which accumulate over time. This may cause the original architecture to completely lose its meaning and have a detrimental effect on system longevity, maintenance and innovation.

4. I characterized Packet Switching and the End-to-End principle as the two key design choices for the Internet. Describe them.

Packet Switching uses statistical multiplexing where bandwidth is shared based on demand from each user. This results in greater utilization and efficiency as bandwidth is not wasted when there is demand. It also allows for more users to use the network. However, there could be issues such as congestion and delay when aggregate resource demand exceeds the amount available which leads to packet loss and delay and a need for protocols for reliable data transfer.

End to End principle is used to determine where a function should be implemented in a communication system. It is based on the argument that the function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible.

5. At what layer does ARQ exist? At what layer does TCP exist? Compare them in terms of how they provide reliability.

ARQ exists in the Data Link Layer while TCP exists in the Transport Layer. ARQ ensures reliable transmission of frames over the link at the hop by hop level while TCP ensures end to end reliability.

6. Describe the hierarchical structure and addressing of the Internet.

The internet is a hierarchical global network which uses the standard internet protocol suite (TCP/IP) for routing. IP addresses have a hierarchy that makes it easier to route data around the Internet. The IPv4 addressing hierarchy includes network, subnet, and host components in an IPv4 address. IPv6, with its 128-bit addresses, provides globally unique and hierarchical addressing based on prefixes rather than address classes. Hierarchical IP addresses allow multiple addresses with the same prefix to be grouped together which keeps routing tables small and routing efficient.

7. Explain the tradeoff between Packet Switching and Circuit Switching?

Packet Switching uses statistical multiplexing where bandwidth is shared dynamically based on demand from each user. This results in greater utilization and efficiency as bandwidth is not wasted when there is demand and resources are used as needed. It also allows for more users to use the network. However, there could be issues such as congestion and delay when aggregate resource demand exceeds the amount available which leads to packet loss and delay and a need for protocols for reliable data transfer.

Circuit Switching uses Frequency Division Multiplexing or Time Division Multiplexing which allocates dedicated resources statically and can provide guaranteed bandwidth and performance. However, it is less efficient compared to Packet Switching and also requires call setup time.

8. Why do we have both MAC & IP Addresses?

MAC and IP addresses operate on different layers and allow for layers to be independent. MAC addresses are used by the link layer within a LAN while IP addresses are used by the network layer for routing. A MAC address is a globally unique ID for a device and is used for local communications. An IP Address is hierarchical to group and organize different networks into subnets and they are changeable so they indicate where you are and not who you are.

9. In setting up a network, should you use a switch or a router? Describe the pros and cons.

Switches are “plug-and-play” devices as they don’t require any intervention or configuration from network administrators and users. On the other hand routers are not plug-and-play meaning that configurations of IP addresses are needed when hosts are connected to the routers.

The packet forwarding rates are higher in switches than routers as switches process frames only up to layer 2 while routers need to process up to layer 3 incurring more overhead and delay. Routers do more intelligent routing than switches as the latter use spanning trees for packet routing whereas routing is more flexible in routers as they can select good routes based on routing protocols and dynamic state of the network.

Generally switches are preferred for interconnecting small networks and LANs whereas routers are preferred for interconnecting large networks.

10. Think about security in layer 2 and layer 3. What kind of attacks are there at layer 2 and layer 3? Hint: Lookup the broadcast storm, ARP/switch poisoning, and Denial of Service.

Broadcast storm is an abnormally high number of broadcast packets within a short period of time. A broadcast storm can overwhelm switches and endpoints as they struggle to keep up with processing the flood of packets. When this happens, network performance degrades.

ARP poisoning is a Man in the Middle attack on Layer 2 that allows attackers to intercept communication between network devices. It involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table.

Layer 2 DDoS attacks include MAC Flooding which consumes memory and floods the MAC address table of the switch. This forces legitimate MAC table contents out of the switch and forces a unicast flooding behavior potentially sending sensitive information to portions of the network where it is not normally intended to go. Layer 3 DDoS attacks include Ping Flood which sends multiple ping requests to a server at once, Smurf Attack, where the target’s IP address in the ping request is spoofed.