Domain Name Space (DNS)

- DNS is a hierarchical, distributed naming system that translates domain names to IP addresses.
- DNS servers store DNS records for each domain, including information like IP address, mail server information, and more.
- DNS uses a client-server model, with DNS servers responding to requests from client devices.
- Common DNS record types include A records (which map domain names to IP addresses), MX records (which specify mail servers), and CNAME records (which create aliases for domain names).

Transport Layer: Process to Process Communication

- The Transport Layer is responsible for establishing end-to-end connections between processes running on different devices.
- Transport Layer protocols include User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Stream Control Transmission Protocol (SCTP).
- The Transport Layer adds a header to the data sent by the application layer that includes information like port numbers, sequence numbers, and checksums.
- The Transport Layer also handles flow control, congestion control, and error recovery.

User Datagram Protocol (UDP)

- UDP is a connectionless, unreliable Transport Layer protocol.
- UDP does not establish a connection before sending data and does not guarantee that data will be delivered.
- UDP is useful for applications that need low latency and do not require reliable delivery of data, such as video and audio streaming.

Transmission Control Protocol (TCP)

- TCP is a connection-oriented, reliable Transport Layer protocol.
- TCP establishes a connection before sending data and guarantees that data will be delivered.

- TCP uses mechanisms like window-based flow control, congestion control, and error recovery to ensure reliable delivery of data.
- TCP is used for applications that require reliable data delivery, such as web browsing and file transfers.

SCTP Congestion Control

- SCTP is a Transport Layer protocol that provides both reliable and unordered delivery of messages between hosts.
- SCTP congestion control algorithms ensure that the network is not overloaded and that packets are not lost.
- SCTP uses a variety of mechanisms to handle congestion, including fast retransmit and slow start.

Quality of Service (QoS)

- QoS refers to the ability to prioritize different types of traffic on a network to ensure that critical applications receive sufficient bandwidth and low latency.
- QoS can be implemented at different levels of the network stack, including the application layer, Transport Layer, and network layer.
- QoS techniques can include packet classification, traffic shaping, and congestion control.

Leaky Bucket and Token Bucket algorithm

- Leaky Bucket and Token Bucket algorithms are QoS techniques used to control traffic on a network.
- The Leaky Bucket algorithm limits the rate at which data is sent by discarding excess packets.
- The Token Bucket algorithm controls traffic by regulating the rate at which packets are sent and discarding packets when the bucket is empty.

Logical addressing - IPV4

- IPV4 is a protocol used to identify devices on a network.
- IPV4 addresses are 32-bit numbers, divided into four octets, with each octet separated by a period.
- IPV4 addresses consist of a network portion and a host portion.
- IPV4 addresses are assigned by Internet Assigned Numbers Authority (IANA) and distributed to regional registries.

Hamming code

- Hamming code is a technique used to detect and correct errors in data transmission.
- Hamming code adds redundant bits to the original data to create a code word that can be checked for errors.
- If an error is detected, the code word can be corrected using the redundant bits.

Domain Name Space (DNS)

- DNS is a hierarchical, distributed naming system used to translate domain names to IP addresses.
- DNS servers store DNS records for each domain, including information like IP address, mail server information, and more.
- DNS operates in a client-server model, with DNS servers responding to requests from client devices.
- The DNS hierarchy starts with the root domain, represented by a single dot (.) and includes top-level domains like .com, .org, .net, and country-specific domains like .us, .uk, and .jp.
- DNS queries use the domain name system to locate the correct DNS server to ask for the IP address.
- Common DNS record types include A records (which map domain names to IP addresses), MX records (which specify mail servers), and CNAME records (which create aliases for domain names).
- DNS operates on both UDP and TCP, with UDP used for small queries and TCP used for large queries or zone transfers.

Transport Layer: Process to Process Communication

- The Transport Layer is responsible for establishing end-to-end connections between processes running on different devices.
- Transport Layer protocols include User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Stream Control Transmission Protocol (SCTP).
- The Transport Layer adds a header to the data sent by the application layer that includes information like port numbers, sequence numbers, and checksums.
- The Transport Layer is responsible for flow control, congestion control, and error recovery.
- Flow control is used to manage the rate at which data is sent to prevent buffer overflow and packet loss.
- Congestion control is used to ensure that the network is not overloaded with traffic, which can lead to packet loss and reduced performance.
- Error recovery is used to detect and retransmit lost or damaged packets.

User Datagram Protocol (UDP)

-
- UDP is a connectionless, unreliable Transport Layer protocol.
- UDP does not establish a connection before sending data and does not guarantee that data will be delivered.
- UDP is useful for applications that need low latency and do not require reliable delivery of data, such as video and audio streaming.
- UDP is also used for simple request/response protocols like DNS and DHCP.
- Applications using UDP must handle error detection and recovery.

Transmission Control Protocol (TCP)

- TCP is a connection-oriented, reliable Transport Layer protocol.
- TCP establishes a connection before sending data and guarantees that data will be delivered.
- TCP uses mechanisms like window-based flow control, congestion control, and error recovery to ensure reliable delivery of data.
- TCP is used for applications that require reliable data delivery, such as web browsing and file transfers.

- TCP provides flow control through the use of sliding windows and congestion control through the use of slow start, congestion avoidance, and fast retransmit algorithms.

SCTP Congestion Control

- SCTP is a Transport Layer protocol that provides both reliable and unordered delivery of messages between hosts.
- SCTP congestion control algorithms ensure that the network is not overloaded and that packets are not lost.
- SCTP uses a variety of mechanisms to handle congestion, including fast retransmit and slow start.
- SCTP is used in applications that require reliable data delivery, such as telephony and multimedia streaming.

Quality of Service (QoS)

- QoS refers to the ability to prioritize different types of traffic on a network to ensure that critical applications receive sufficient bandwidth and low latency.
- QoS can be implemented at different levels of the network stack, including the application layer, Transport Layer, and network layer.
- QoS techniques can include packet classification, traffic shaping, and congestion control.
- QoS can be used to ensure that high-priority traffic like voice and video are given sufficient bandwidth and low latency, while lower-priority traffic like email or file transfers can be limited to ensure that they do not interfere with critical traffic.

QoS improving techniques: Leaky Bucket and Token Bucket algorithm

- The Leaky Bucket algorithm is a QoS technique that limits the rate at which traffic can be sent by smoothing out traffic bursts.
- The algorithm works by treating a network link as a virtual bucket with a fixed capacity. When traffic arrives, it is added to the bucket. If the bucket is full, traffic is discarded.
- The Token Bucket algorithm is a similar QoS technique that also limits the rate at which traffic can be sent but allows for short bursts of traffic.

- The algorithm works by adding tokens to a bucket at a fixed rate. When traffic arrives, tokens are removed from the bucket to allow the traffic to be sent. If there

QoS improving techniques: Leaky Bucket and Token Bucket algorithm (continued)

- The Leaky Bucket algorithm can be used to limit the rate at which traffic is sent by a network device or application by smoothing out traffic bursts. It allows a maximum burst of traffic to be sent at a certain rate, after which any excess traffic is discarded.
- The Token Bucket algorithm is similar to the Leaky Bucket algorithm but allows for short bursts of traffic. It uses tokens that are added to the bucket at a fixed rate. When traffic arrives, tokens are removed from the bucket to allow the traffic to be sent. If there are no tokens in the bucket, the traffic is discarded.
- Both algorithms are used to improve QoS by ensuring that network traffic is sent at a controlled rate, preventing congestion and allowing critical traffic to be given priority over less important traffic.

Other QoS improving techniques include:

- Traffic shaping: This technique is used to limit the amount of traffic that can be sent from a device or application to a network. It allows network administrators to control the bandwidth used by different types of traffic, prioritizing critical traffic over less important traffic.
- Packet scheduling: This technique is used to prioritize traffic when there is congestion on a network. It determines which packets should be sent first based on their importance or priority level.
- Network segmentation: This technique is used to divide a network into smaller segments or subnets, allowing traffic to be isolated and prioritized within each subnet. It can improve QoS by reducing congestion and allowing critical traffic to be given priority over less important traffic.

Logical addressing – IPV4

- IP (Internet Protocol) is a network layer protocol used for communicating between devices on a network.
- IP provides logical addressing, which allows devices to be identified by their IP address rather than their physical MAC address.

- IPv4 is the most widely used version of IP and uses 32-bit addresses.
- IPv4 addresses are expressed as four octets separated by dots (e.g. 192.168.0.1).
- IPv4 addresses are divided into two parts: network address and host address. The network address identifies the network to which the device belongs, while the host address identifies the device on the network.
- Subnet masks are used to divide an IP address into network and host portions.
- Private IP addresses are reserved for use on local networks and are not routable on the public internet.

Hamming code

- Hamming codes are a type of error-correcting code used in digital communication.
- Hamming codes add extra bits to the data being transmitted to allow for the detection and correction of errors.
- Hamming codes use a mathematical formula to determine which bits should be added to the data.
- Hamming codes can detect and correct single-bit errors, but are less effective at detecting and correcting multiple bit errors.
- Hamming codes are widely used in computer memory and storage systems, as well as in satellite communication and other digital communication systems.