Name - Jasleen kaur
class - T5
Rollno - 03915603122

Computer Networks
Assignment - 3

Ques 1: Differentiate b/w classful addressing and classless addressing. Give Examples.

Sol

Classful Addressing :- In classful addressing, IP addresses are divided into predefined classes (A, B, C, D, E) Each class has a fixed subnet mask, which determines the number of network and host bits.

IP address are defined as:-

(1) Class A:- (0.0.0.0 to 126.255.255.255)
(2) Class B:- (128.0.0.0 to 191.255.255.255)
(3) Class C:- (192.0.0.0 to 223.255.255.255)
(4) Class D:- (224.0.0.0 to 239.255.255.255)
(5) Class E:- (240.0.0.0 to 255.255.255.255)

Limitation :- It wastes IP addresses by allocating a fixed number of addresses per network.

Classless Addressing :- In classless Addressing, IP addresses are assigned without fixed classes and use a variable-length subnet mask. It allows the network to be divided into subnets of different size, which optimizes IP address utilization.

Classless Inter-Domain Routing (CIDR) notation. ~~Eg. IP address~~ specifies the number of bits for the network prefix.
It is more flexible and efficient in terms of address allocation and routing.

Example :- IP address → 192.168.1.0/24

Ques 2: What is Routing in a network layer? Explain any two Routing Algorithms.

Ans: Routing is the process of determining the path for data to travel across interconnected networks from a source to destination. It involves selecting optimal routes and forwarding data packets through intermediate routers based on routing tables.

Routing Algorithms:-

(1) Distance Vector Routing:- Routers share information with their neighbours about the distance to reach certain networks. Each routers maintains a table of distances to other networks updating it periodically.

- Routers use algorithms like Bellmanford to calculate paths and determine the shortest paths route

(2) Link state Routing:- Each router has a complete map of the network topology and calculates the best path using algorithms like Dijkstra's shortest path.

Routers periodically send information about the state of their links to all other routers.

Suitable for large networks with frequent topology changes

Ques: What are supernetting and subnetting?

Sol Subnetting is the process of dividing a single IP address network into smaller segments called subnets.

It allows for better management of IP address space and isolates network traffic within smaller domains.

Subnetting increases the number of network segments while reducing the number of hosts per segment.

Ex:- Dividing a class B network (172.16.0.0/16) into small subnets like 172.16.1.0/24, 172.16.2.0/24.

Supernetting:- It is the process of combining multiple smaller networks into a larger, contiguous address space.

It reduces the number of routing entries in a router's routing table and is commonly used in CIDR.

- Supernetting is used to aggregate routes and simplify routing tasks, particularly useful for ISPs.

Example:- Combining four class C networks (eg. 192.168.0.0/24, 192.168.1.0/24) into one supernet 192.168.0.0/22.

Ques 4:- Explain the following Algorithms.

(a) Leaky bucket Algorithm.

→ The leaky bucket Algorithms is used for traffic shaping to control the flow rate of data.

→ It uses a fixed size buffer (bucket) that releases packets at a constant rate, discarding any excess packets when the bucket is full

→ This algorithm ensures a steady output rate but can lead to packet loss if too much traffic enters at once.

(b) Token bucket Algorithm.

→ The token bucket Algorithm allows for bursty data transmission but still controls the maximum data rate.

→ Tokens accumulate in the bucket over time at a fixed rate, and each token permits the transmission of a packet.

→ When packets arrive, they can only be transmitted if there are enough tokens otherwise they wait until tokens are available.

Name- Jasleen kaur Assignment-4
class- T5 Computer Networks
Rollno.→ 03915603122

Ques1: How is process-to process communication established in TCP? Explain the use of Sending and Receiving buffers.

Sol. TCP is a connection-oriented protocol used for reliable, process-to process communication between applications on networked computers. It uses three way handshake process to establish connection:

(1) SYN: The sender sends a synchronization packet to initiate the connection.

(2) SYN-ACK:- The receiver responds with an acknowledgement packet.

Use of Sending and Receiving buffer

- Sending buffer → Stores data that has application wants to send but has not yet been acknowledgement by the receiver Ensures reliable transmission, as data in the buffer can be retransmitted if packets are lost or damaged.

- Receiving buffer:- Stores incoming data packets until they are processed by the receiving application. Ensures data is received in the correct order, allowing TCP to reassemble out of order packets and handle any missing packets by requesting transmission.

Ques2:- How is Checksum Calculation Done in UDP and TCP?

Sol. In UDP UDP uses a simple checksum that provides error check for data integrity.

- The checksum is calculated by adding together segments of the packet (header and data) as 16-bit words.

If the sum has more than 16 bits, any overflow bits are [illegible]

TCP | 80 | HTTP

added to the 16 bit.
finally, the sum is inverted resulting in the checksum. This
Checksum is included in the UDP header and if data corru
on occurs, the checksum at the receiver will not match
prompting error handling.

In TCP

→ In TCP checksum calculation is similar to UDP but include
the concept of a pseudoheader.
The Pseudo-header contains parts of the IP header
The TCP checksum is computed by summing up the pseudo-
header, the TCP header and the data, treating them as
16 bit words. Any overflow bits are wrapped around and added
and the result is inverted to get final checksum.

Ques 3. Explain UDP in Detail. List all well-known ports
reserved for UDP and TCP.

Ans UDP is a connectionless and stateless protocol designed
for applications that need fast, low-overhead data transmiss
without reliability or order guarantees.
Unlike TCP, UDP does not establish a connection instead it
sends packets independently.
It is suitable for applications like video streaming, online gaming
and DNS where speed is prioritized over reliability.

Protocol	Port	Service
TCP	20	FTP Data
TCP	21	FTP control
TCP	23	Telnet
TCP/UDP	25	SMTP
UDP	53	DNS
UDP	67	DHCP

TCP	80	HTTP
TCP	110	POP3
TCP	143	IMAP
UDP	161	SNMP
TCP/UDP	514	Syslog.

Ans 4: Write short note on

(1) Proxy Server:- A proxy server acts as an intermediary between client device and external servers, forwarding client requests to desired resources on behalf of the client. It provides security, caching and privacy by masking client IP addresses and filtering web requests.

Types include forward proxies (used by client to access external resources) and reverse proxies (used by servers to manage client requests and improve load balancing.

Proxy servers are commonly used for content filtering, access control, load balancing and anonymity on the Internet.

(2) DNS (Domain Name System): DNS translates human readable domain names into IP addresses that computers use to identify each other on the network.

It acts like an internet phonebook, allowing users to make easy memorable domain names instead of numerical IP addresses.

DNS follows a hierarchical structure with different types of servers such as root servers, TLD servers and authoritative DNS servers

DNS works through queries that are resolved in multiple steps to retreive IP addresses or specific record types.