Ex NO : 01 DATE : 17.11.23	DEVELOP CLIENT SERVER BASED TCP APPLICATIONS USING UNIX SOCKET PROGRAMMING FUNCTION

AIM:

To develop client server based TCP applications using UNIX socket programming function.

THEORY:

TCP sockets are used for communication between a server and a client process. The server's code runs first, which opens a port and listens for incoming connection requests from clients. Once a client connects to the same (server) port, the client or server may send a message. Once the message is sent, whenever receives it (server or client) will process it accordingly.

PROCEDURE:

* Server side:

Step 1: Create a socket that returns a socket descriptor.

Step 2: Initialize the server address by the port and IP.

Step 3: Bind the socket descriptor to the server address.

Step 4: Turn on the socket to listen for incoming connections.

Step 5: Store the client's address and socket

descriptor by accepting an incoming connection.

step 6: Communicate with the client using send() and recv().

step 7: close the server and client socket to end communication.

* Client-side:

step 1: Create a socket, and initialize the server's address information in a variable. similar to how it was done at the server side.

step 2: Send a connection request to the server, which is waiting at accept().

step 3: Communicate with the server using send() and recv().

step 4: Close the socket.

EXP NO: 02 DEVELOP CLIENT SERVER BASED UDP APPLICATIONS USING LINUX SOCKET PROGRAMMING FUNCTION

DATE: 21.11.23

AIM:

To develop client server based UDP applications using LINUX socket programming function.

THEORY:

In UDP, the client does not form a connection with the server like in TCP and instead sends a datagram. similarly, the server need not accept a connection and just waits for datagram to arrive. Datagrams upon arrival contain the address of the sender which the server uses to send data to the correct client.

PROCEDURE:

* Server-side:

step 1: Create a UDP socket.

step 2: Bind the socket to the server address by the port and IP.

step 3: Wait untill the datagram arrives from the client.

step 4: Process the datagram packet and send a reply to the client.

~~step 5~~:

* Client-side:

Step 1: Create a UDP socket.

Step 2: Send a message to the server.

Step 3: wait until response from server is received.

Step 4: Close socket descriptor and exit.

EX.No:04	PERFORMANCE ANALYSIS OF TCP AND UDP PROTOCOL USING STIMULATION TOOL.
DATE: 29.11.23	

AIM:

To analysis of the performance of TCP protocol and UDP protocol using the stimulation tool.

THEORY:

TCP - Transmission Control Protocol is a communication standard that enables the application program and computing device to exchange messages over network.

UDP- User Datagram Protocol refers to protocol used for communication throughout internet. It is specifically chosen for time sensitive application like DNS

PROCEDURE:

Step 1: Open cisco Packet Tracer tool and arrange the components.

Step 2: Use 'Copper straight Through' cables to

connect PC_s, servers and switch among the device.

Step 3: Configure every device from PC_s to server [PC_0, PC_1, PC_2, PC_3, server].

(Data)

→ DNS server – 192.162.10.5

→ subnet – 255.255.255.0

→ PC – 192.162.10.–

Step 4: Configure the server – sevice – DNS.

Step 5: Configure the server – service – HTTP.

Step 6: On PC_2, at cmp using ns lookup view address details.

Step 7: Launch PC_2 web browser. Go to URL and do search.

EX. NO: 05	PERFORMANCE ANALYSIS OF ROUTING
DATE: 11.12.23	PROTOCOLS USING STIMULATION TOOL.

AIM:

To analyse the performance of the routing protocols using the stimulation tool.

THEORY:

i) RIP:

Routing Information protocol is dynamic routing protocol and one of oldest protocol in service that uses hop count as routing metric to choose best path [hop - 15 max].

ii) OSPF:

Open shortest path first in link state routing protocol which one of family of IP protocol used to find best path using its own shortest path first. [hop - No limit].

PROCEDURE :

RIP PROTOCOL:

Step 1: Open cisco packet tracer and get arrange the components.

Step 2: Use " copper Straight Through" cables to connect PC, server, switches.

Step 3 : connect 3 router using serial DTE.

Step 4 : Configure all PCs as per order from $PC_0, PC_1, \ldots$

Step 5 : Establish the connections in routers as $(R_0, R_1, R_2, \ldots)$.

Step 6 : By using clr router RIP is introduced to the routers on network with command of network (address).

Step 7: Now decide the source and destination system to transfer data.

OSPF PROTOCOL:

Step 1: Open cisco packet Tracer tool and arrange the components.

Step 2: Use "Automatic choose connection type" cables to connect PC, , server, routers.

Step 3: Configure all PCs as per order from PC_0, PC_1 with gateway.

Step 4: Establish the connections in all ports of routers as R_1, R_2 ...

Step 5: By using CLI terminal the routers are assigned for OSPF protocol with the command, network (address) followed by router OSPF 1, for router 1.

Step 6: After assigning protocol, the network ready to transfer the data.

EXP NO : 06

DATE: 14.12.23

DEMONSTRATE THE WORKING OF NETWORK TOOLS SUCH AS PING, TCP DUMP, TRACEROUTE AND NETSTAT.

AIM:

To demonstrate the working of network tools such as ping, TCP,dump, traceroute and netstat.

THEORY:

Network tools are used to perform a variety of tasks such as obtaining information about other systems on your network, accessing other systems, and communicating directly with other users. Network information can be obtained using utilities such as ping, traceroute etc. These are useful for smaller networks and enable to access remote systems directly.

PING COMMAND:

The ping command in linux is a utility that helps to test connectivity between two devices on a network.

TCP DUMP COMMAND:

The TCP dump is a packet sniffing and analyzing tool for a system Administrator to troubleshoot connectivity issues in linux.

TRACEROUTE COMMAND:

The traceroute command in linux prints the route that a packet takes to reach the host.

NETSTAT COMMAND:

This command prints network connections, routing tables, interface statistic and multicast memberships.

EX. NO: 07	ANALYZE THE NETWORK TRAFFIC USING
DATE: 9.1.24	WIRESHARK OR PACKET TRACER TOOL.

AIM:

To analyze the network traffic using the wire shark or packet tracer tool.

THEORY:

The packet tracer tool is cross platform visual sitmulation tool designed by cisco system that allows were to create network topologies and initate modern computer networks. The software allows users to sitmulate the configuration of cisco routers and switches using stimulated command line.

PROCEDURE:

Step 1: Launch packet tracer tool on PC.

Step 2: Add network devices to workspace by dragging and dropping them to create a topology.

step 3: configure the network devices.

step 4: verify connectivity and set IP address for network devices.

step 5: configure a switch or hub and make the required connection.

step 6: Try sending files within the network to analyze the network traffic.

step 7: Save the file and close packet tracer tool.