A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No-1

AIM:-

Setup a wired LAN using layer 2 Switch. It includes preparation of cable, testing a cable using line tester, configuration machine using IP addresses, testing using PING utility and demonstrating the PING packets captured traces using Lilishark Packet Analyser Tool.

Objectives:-

To understand the structure and working of various networks including the interconnecting devices used in them.

To get hands on experience of making and testing cables

Outcomes:-

After completion of this experiment, students will be able to -

Setup wired and wifi network.

Learn to setup wired and wifi office/ organisation network

Theory Concepts:-

LAN (Local Area Network).

LAN stands for "Local Area Network" and is pronounced as "LAN". A LAN is a network of connected devices that exists within a specific location. LANS may be found in homes, offices, educational institution, or other areas.

A LAN may be wired, wireless or a combination of the two. A standard LAN uses Ethernet to connect devices together (e.g. installers LANS are typically created using a Wifi signal. If a router supports both Ethernet and Li-fi connections, it can be used to create a LAN with both

wired and wireless devices

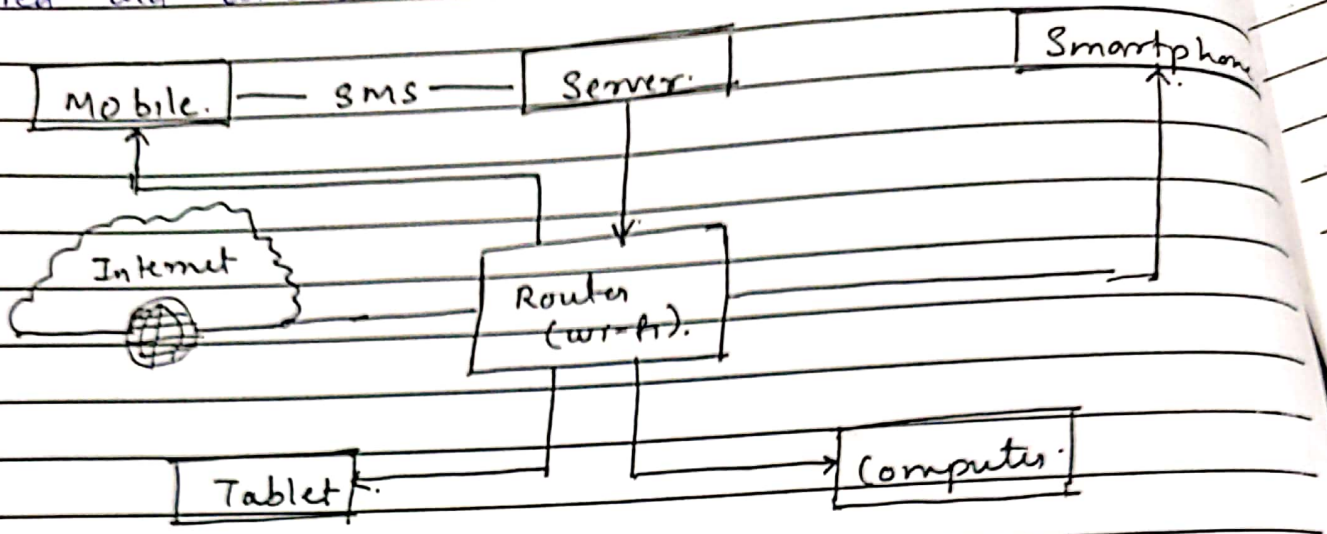


fig- LAN.

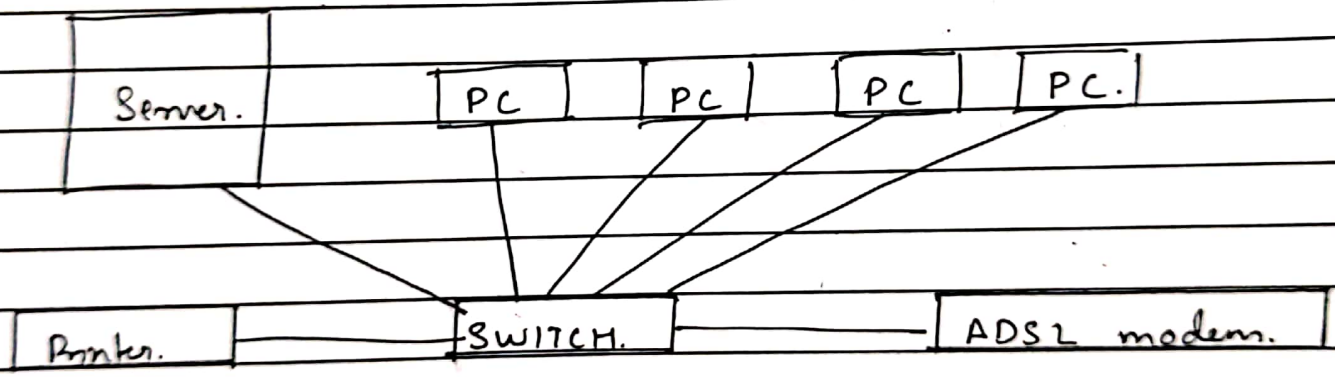


fig-2. Switch.

Switch :-

Switch are networking devices operating at layer 2 or a data link layer of OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination addresses, performs necessary checks and sends the frames to corresponding devices. It supports unicast, multicast as well as broad-cast communications

Types of Switch are :-

1. Unmanged Switch.
2. Managed Switch.
3. LAN Switch.
4. PoE Switch.

Networking Cables :-

Networking Cables are networking hardware used to connect one networking device to other network devices or to connect two or more computers to share printers, scanners etc. Different types of cables, such as, co-axial cable, optical fiber cable and twisted pair cables are used depending on the network's physical layer, topology and size.

1. Coaxial Cable :- A coaxial cable is an electrical cable with copper conductor and insulation shielding around it and braided metal mesh that prevents signal interference and crosstalk.
2. Twisted Pair Cable :- Twisted pair cable have two conductors the are generally made up of copper and each conductor insulation
3. Optical fiber Cable :- The cable is a cylindesical fiber class which is hour thin size or any transparent dielectric medium.

Cable Tester :-
A cable tester is an electronic device used to verify electrical connections in a signal cable or other wired assembly.

1) Basic cable tester - verify the correct wiring of connections on the cable.
2) Advanced cable tester - verify properties of cable such as noise, resistance, signal attenuation and interference.

IP Address :-
The Internet Protocol Addresses (or IP Address) is a unique address that computing devices such as personal computers tablets and smartphones use to identify itself and communicate with each devices in the IP network

1. Static IP - Address never change. They serve a permanent Internet addresses and provide a simple & reliable way for remote computers to contact you.

2. Dynamic IP - Address are temporary and are assigned each turn a computer access the Internet.

Ping Command :-
The ping command is a Command Prompt command. used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used to simple way to verify that a computer can communicate over the network with another computer or network devices.

Eg - ping 192.168.2.106.

Libreshark :-

Libreshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and education.

Examples :-

Network administrations use it to troubleshoot network problems
Network security engineers use it to examine security problems
Developers use it to debug protocol implementation
People use it to learn network protocol internals.

Con

Conclusions :-

Successfully set a wired LAN connection for minimum PC's and analyzed the packets using Libre Shark Packet Analyzer Tool.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

PRACTICAL NO-2.

Aim:- Demonstrate the different types of topologies and types of transmission media by using a packet tracer tools.

Objective:- i) To study different types of topology.
ii) To study transmission media by using packet tracer tools.

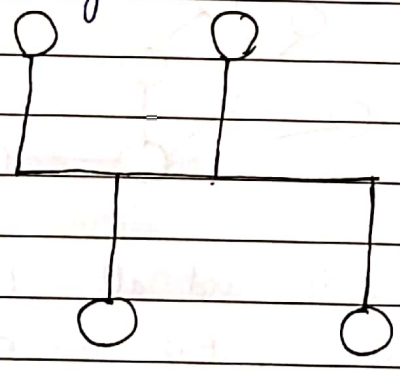
Theory:-

* **Network Topology:-**

To build a network we need network topology. The network topology can be summerized like.

1. **Bus Topology:-**

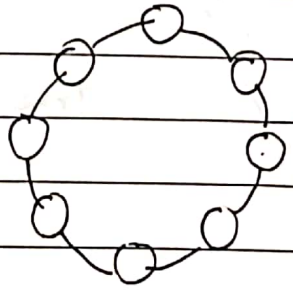
With bus topology, all the network nodes are connected to a common network media and only one node can receive and transmit data at any time.



Bus Topology.

2. **Ring Topology:-**

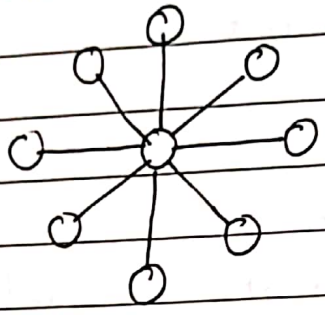
All the nodes are connected on a medium and frames are travels through on direction. If a node wants to send data, then it adds to the frame.



Ring Topology.

Star Topology :-

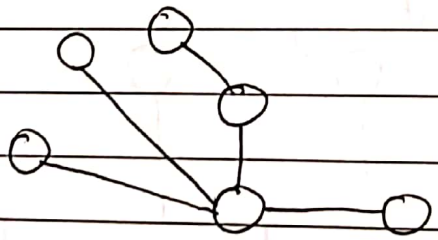
It is the topology that all the other nodes are connected to central node. This is widely used topology but is has disadvantages that if the central device fails, the other nodes can not communicate.



Star topology

Mesh Topology :-

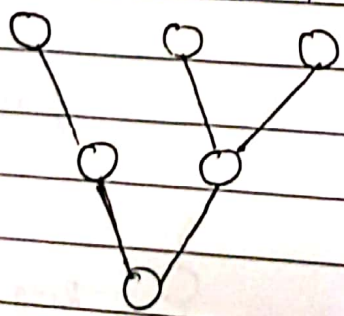
It has a unique network design in which each computer on the network connected to every other. It offers high level of redundancy, so even if one network cable fails, still data has a alternate path to reach destination.



Mesh topology.

Tree Topology :-

It has root node, and all other nodes are connected which form a hierachy. So, it is also know as hierachical topology. This topologies integrates various star topologies together is single bus, so it is known as star topology.



Tree topology

* TRASMISSION MEDIA :-

A trasmission media is a physical path between the trasmit and receiver. It is channel through which data is sent from one place to another. They are classified into 3 types.

1. Guided Media :-

It is also referred as cured / Bounced trasmission media. Signals being trasmitted are directly and confined in narrow pathway by using physical links.

There are 3 major types of Gurde Media.

a) Trusted Pair Cable :-

It consists of 2 separately insulated conducter wires wound about each other. Generally, several such pairs are burdled together in protective sheath.

b) Conial Cable :-

It has an outer plastic covering containing an insulation layer made of PVC / Teflon and 2 parallel conductors each having a separate insulated protection cover.

The coaxial Cable trasmits information in two modes- Baseband mode and Broad band mode.

Cable TVs and analog television networks widely use conial cables.

c) Optical fiber Cable :-

It uses the concept of reflection of light through a core made up of glass and plastic. The core is surrounded by less dense glass covering called the cladding. It is used for trasmission of large volumes of data. The cable can be directional.

or undirectional.

Conclusion :-

In this way, we studied different type of topologies and transmission media.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No-3.

Aim :- Write a program for error detection and correction of 7/8 bits ASCII codes using Hamming codes or CRC.

Objective :- To study error detection and error correction of 7/8 bits ASCII codes.

Theory :-

The hamming code technique, which is an error-detection and error-correction technique was proposed by R.W. hamming. Whereever data packet is transmitted over a network, there are possibilities that the data bits may get lost or damage during transmission.

Error Detection :

Errors in the received frames are detected by means of parity check and cyclic redundancy check (CRC). In both cases, few extra bits are set along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver end fails, the bits are considered corrupted.

Error Correction :-

It can be done in two ways :-

i) Backward ERROR Correction :-
When the receiver detects an error in the data received, it requests back the sender to retransmits the data unit.

ii) Forward ERROR Correction :-
When the receiver detects some error in the data received, it executes error-correcting code, which help to auto-recover and to correct some kind of errors.

Conclusions :-
In this way, we studied error correction and detection using hamming code of CRC.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No-4.

Aim :-

Write a program to simulate Go back N and selective Repeat Modes of sliding window Protocol in Peer - to Peer mode.

Objective:-

To study Goback N and selective Repeat modes of sliding window protocol.

Theory :-

In computer Network sliding window protol is a method to transmit data on network. Sliding Window Protocol is applied on Data link layer of OSI model. At data link layer data is in form of frames.

In networking, window simply means a buffer which has data frames that needs to be transmitted.

Both sender and receiver agrees on some window size. If window size = w then after sending w frames sender waits for the acknowledgement (ack) of first frame.

As soon as sender receives the acknowledgement of a ~~frame~~ frame it is replaced by next frame to be transmitted by sender. If receiver sends a collective cumulative acknowledgement to sender then it understands that more than one frame are properly received.

For eg- If ack of frame 3 is received. it understands that frame 1 and frame 2 are received properly.

Conclusion:-
In this way, we studied sliding window protocol in peer-to peer mode.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No- 5.

Aim :-
Write a program to demonstrate subnetting and find. Subnet mask.

Objective :-
To study subnetting and find subnet mask.

Theory :-

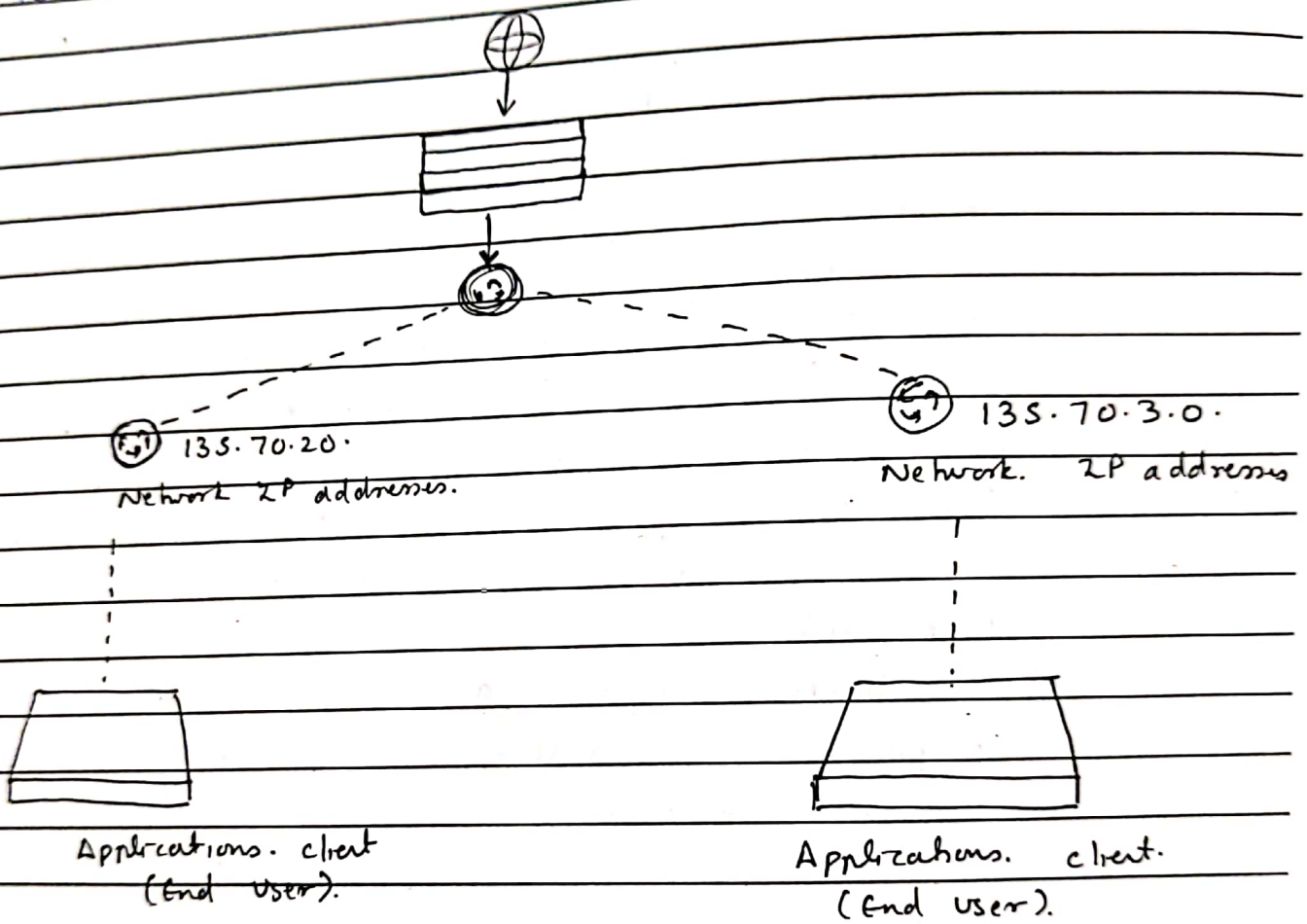
Subnetting :-
Subnetting is used in IPV4 networks. when an organization with a single logical IP network addresses has multiple physical networks. A subnetted domain further divides the last number portion of the classful address into two parts, a subnet number and a host number on that subnet.

Subnetting enables an organization to conceal network complexity and reduce network traffic by adding subnets without a new network number.

Subnet Mask :-
Every device has an IP address with two pieces : the client or host address and the server on network address IP addresses are either configured by DHCP server. or manually configured.

The subnet mask splits the IP addresses, there by defining which part of IP addresses belongs to the device and which part belongs to the network.

The device called a gateway. This means that when a local device wants to send information to device at an IP address on another network, it first sends it packets to the gateway, which then forwards the data on its destination outside of the local network.



Conclusions:-

In this way, we studied Subnetting.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No - 6.

Aim :- W

Write a program to implement link state Distance vector routing protocol to find suitable path for transmission.

Objective :-

To study Distance vector routing protocol.

Theory :-

DISTANCE VECTOR ROUTING PROTOCOL :-

A distance vector routing (DVR) protocol requires that a router inform its neighbours of topology changes periodically. Each router maintains a distance vector table containing the distance between itself and All possible destination nodes, Distance, based on a chosen matric, are computed using information from the neighbour's distance vectors.

Each router has an ID.

Associated with each link connected to a router, there is a link cost (Static / Dynamic)

Intermediate loops.

Distance Vector Table Initialization :-

Distance to itself = 0.

Distance to All other routers = infinity number.

Distance Vector Algorithm :-

1. A router transmits its distance vector to each of its neighbour in routing packets.
2. Each router receives and saves the most recently received distance vector from each of its neighbour.
3. A router recalculates its distance vector when.
   - It receives ~~recalculates its distance vector when~~
   - It receives a distance vector program from a neighbour containing different info than before
   - It discovers that a link to neighbour has gone down.

Conclusion :-

In this way, we studied distance vector Routing (DVR) Protocol.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No. 7

Aim :- Use packet tracer tool for configuration of 3 routes network using one of following protocol. RIP, OSPF / BGP.

Objective :- To study RIP / BGP protocol

Theory :-

Packet Transfer. BGP Configuration :-

In the configuration we will use two AS. (Autonomous System) with 3 routers for each. We will use private As block (64512 - 65535) for this configuration, but in interact public As numbers are used.

→ you can download the Packet Tracer with .pkt format.

→ you can also download all the packet tracer examples with .pkt format in Packet tracer labs section.

For Packet Tracer BGP configuration, firstly we need to configure the IP addresses of interface.

Packet Tracer OSPF Configuration :-

1. Build the network topology.
2. Configure IP address on PC's and router interface.
3. Configure OSPF on the routers.
4. Verify OSPF configuration.

Conclusion :-

In this way, we studied Packet Tracer BGP and OSPF configuration.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No - 8.

Aim :- Write a program using TCP socket for wired network for following -

a. Say Hello to each other.
b. File transfer.
c. Calculation.

Theory :-

TCP Socket :-

The Transmission Control Protocol is a standard for exchanging data between different devices in computer network.

It allows two endpoints in a shared computer to establish connection that enables two way transmission of data. They data loss is detected and automically corrected which is why TCP is also called reliable protocol.

Together with UDP and SCTP, TCP forms the groups of transmission protocol belonging to internet protocol suite that are located at transport layer in network architecture according to OSI model.

The term TCP / IP protocol stack is also commonly used to refer internet protocol.

TCP allows for transmission of information in both direction. This means that computer system that communicate over TCP can send and receive data at same time.

The protocol uses segments as basic or unit of data transmission.
Segments can also contain control info and are limited to 1,500 bytes.

Conclusions:-
In this way, we studied TCP socket.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No- 9.

Aim :-

Write a program using UDP sockets to enable file transfer. (Scripts, Text, Audio and Videos one file each) between two machine.

Theory :-

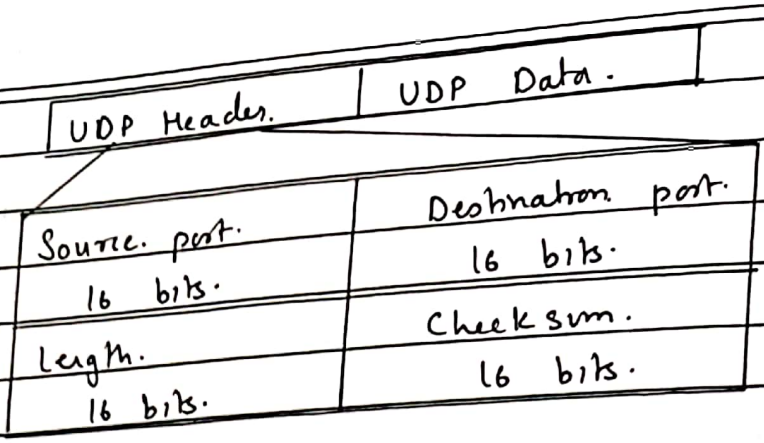
User Datagram Protocol (UDP):-

UDP is transport layer protocol UDP is a part of Internet Protocol suite, referred to UDP / IP suite unlike TCP it is unreliable and connectionless protocol. So, there is no need to establish a connection prior to data transfer.

UDP Header :-

UDP Header is an 8 bytes fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 bytes contain all necessary header information and remaining part consists of data. UDP port number fields are each 16 bits long, therefore the range for port no is defined from 0 - 65535. port no 0 is measured.

Port numbers helps to distinguish different user requests on processes.



Source Port :-
It is 2 byte long field used to identify the port no of the source.

Destination Port :-
It is 2 byte long field, used to identify port of destined packet.

Length :-
Length of UDP including the ~~headline~~ header and the data - It is 16 - bit field.

Checksum :-
It is 2 byte long field - It is the 16- bit one's complement of one's complement sum of UDP header, the pseudo - header of info from IP header, and the data, padded with zero octets at the end to make a multiple of two octets.

Conclusions :-
In this way, we studied UDP sockets.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No-10.

AIM:- Write a program for DNS lookup. Given an IP address as input, it should return URL and vice-versa.

Theory:-

DOMAIN NAME SYSTEM (DNS):-

DNS is a host name to IP addresses translation service. DNS is a distributed database implemented in a hierachy of name servers. It is an application layer protocal for message exchange between client and servers.

Every host is identified by the IP address but remembering number is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of websites to their numerical IP addresses.

Domain:-

There are various kind of domain:-

General Domain:-

• com (commercial) • edu (educational) • org (non-profit organization) all these are generic domain.

Country Domain:-

• in (india) • us • uk.

- Inverse Domain :-
If we want to know what is domain name of the web
IP to domain name mapping. So DNS can provide both
the mapping for eg-
to find the IP addresses for geeks.for geeks org then
we have to type lookup.

Conclusion :-
In this way, we studied DNS loop up.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No - 11.

Aim :-

Installing and configure DHCP server and write a program to install the software on remote machine.

Theory :-

Installing DHCP SERVER :-

Choose Start → Administrative Tools → Server Manager.
Click the Roles link and then click Add a Role.
Click Next to get wizard started.
Select DHCP server from the list of roles and then click Next
Click Next.
Select the static IP address you want to use for DHCP Server. Then click Next.
Enter the domain name and DNS Servers. To enters a DNS server, type its address in IP address text box and click Add.
Click Next.
To create a new scope, click the Add scope button.
Enter the information for new scope.
Select the Activate this scope check box the click O
When you finish creating scopes, click Next.
Click Install.
Click Close.

CONFIGURING DHCP SERVERS :-

1. Open server Manager : click the start button then click server manager.
2. Add roles and features.
3. Select Role-based or feature-based installation.
4. Select destination server.
5. Select server roles.
6. Feature, DHCP server.
7. Confirmation.

Conclusion :-
In this way, we studied to install and configure DHCP server.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No - 13.

Aim:- Study and Analyze the performance of HTTPs, HTTP and FTP protocol using packets tracer tools.

Objective :-

To study HTTP, HTTP's and FTP protocol.

Theory :-

HTTP (Hyper Text Transfer Protocol) :-

- HTTP offers set of rules and standards which govern how many information can be transmitted on WWW.
- HTTP provides standard rules for web browser and servers to communicate.
- HTTP is an application layer network protocol which is built on top of TCP.
- HTTP uses Hyper text structured text which establish the logical link between nodes containing text.
  It is also known as stateless protocol.

HTTPs (Hyper Text Transfer Protocol Secure) :-

- It is highly advanced and secure vision can HTTP.
- It uses the port no 443 for data communication.
- It allows the secure transaction by encripting the entire communication with SSL.
- It is a combination of SSL / TLS protocol and HTTP.
- It provides encrypted and secure identification of network server.
- HTTP also allows you to create a secure encrypted connection between the server and the browser.

- It offers the bi-directional security of data.
- This helps to protect potentially sensitive information from being stolen.
- In HTTPs protocol 852 transaction are negotiated with the help of Key-based encryption algorithm.
- This key is generally either 40/128 bits in strength.

FTP (File Transfer Protocol):-
- FTP is an application layer protocol which moves files between local and remote file systems.
- It runs on the top of TCP, like HTTP.
- To transfer a file, 2 TCP connection are used by FTP in parallel: control connection and data connection.

FTP Session:-
When FTP session is started between a client and server, the client initiates a control TCP connection with the server side. The client sends control information over this.

When the server receives this, it initiates a data connection to client side. ~~control information over this~~ Only one file can be sent over one data connection. But the control connection remains active throughout the user session.

As the we know HTTP is stateless. i.e it does not have to keep track of any user state. But FTP needs to maintain a state about its users throughout the session. FTP allows 3 types of data structure

1. File Structure :- In file structure there is no internal structure and file is considered to be continuous sequence of data types.

2. Record Structure :-
In record - structure the file is made up of sequential records.

3. Page Structure :-
In Page - structure the file is made up independent indexed pages.

Conclusion :-
In this way, we studied HTTP, HTTPS and FTP protocol.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Experiment No- 14.

AIM :- To study the IPsec (ESP and AH) protocol by capturing the packet using wireshark tool.

Objective :- To study IPsec Protocol

Theory :-

AH and ESP protocols :-

IPsec uses two distinct protocols, Authentication Header (AH) and Encapsulating security Payload (ESP) which are defined by IETF.

AH. (Authentication Header) Protocol :-

IP Authentication Header is used to provide connection-less integrity and data origin authentication. There are two main advantages that authentication Header provides :-

Message Integrity :-

It means, message is not modified while coming from source.

Source Authentication :-

It means, source is exactly source from whom we were expecting data.

When packet is sent from source A to Destination B, it consists of data that we need to send and however header which consists of information regarding packet AH verifies origin of data and also payload to confirm

if there are has been modification done in between, during transmission between source and destination.

However, it basic values of some IP header fields might change. So, values of such fields cannot be protected from Authentication header. AH cannot protect every field of IP header. It provides protection to fields which are essential to be protected.

MAC Header.	IPv4 / IPv6 Header.	Authentication Header.	Payload.

Next Header. (8 bit).	Payload. (8 bit) length.	Reserved. (16 bit).
Security Parameter Index. (32 bit).		
Sequence. Number. (32 bit).		
Authentication Header. (32 bit).		

* Encapsulating Security Payload (ESP):-

ESP is a member of IPS set of protocols that encrypt and authenticate the packets of data between computers using a virtual private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely.

The enhanced version of IPsec in use on Internet -layer. security protocol. It is pre-programmed for IP-layer application security whereas other protocols such as TLS and SSH function on application layer.

Security Authentication Header (AH) is another IPSec member protocol. ESP and AH can operate between hosts and between networks. They can also operate in two modes that encrypts the data packets, for use between work stations that are running a VPN client and Tunnel Mode which are more secure.

Conclusions :-

In this way, we studied AH and ESP IPsec protocol.