EXPERIMENT- 1

Study CAT6 UTP EIA/TIA568A/B straight and cross-over cable crimp and test and verify its connectivity.

CAT6 UTP Cable :

It supports Gigabit Ethernet (1000 Base-T) standard. Operates at a bandwidth up to 250MHz. The cable well exceeds the requirements of TIA/EIA-568.C.2 category 6ISD/IEL class E. It means cable consists of 4 unshidded twisted pairs and no outer shielding.

RJ45 Connector :

A RJ45 connector is a modular 8 position, 8 pin connector used for terminating CAT5e patch cable or CAT6 cable.

Straight through Cable :

A straight through cable is a type of twisted pair cable that is used in local area network to connect a computer to a network hub such as a router.

Crossover through Cable

A crossover ethernet cable is a type of Ethernet cable used to connect computing devices together directly. Unlike straight through cable, the RJ45 cross over cable uses two different wiring standards.

NOTE :

1. The cable color code is the 568B standard on each end of a straight through cable.
2. If a crossover cable is needed, use the 568A standard on one end and 568B on the other end.

TIA/EIA-568-A T568A Wiring

Pin	Color
1.	white/green
2.	green
3.	white/orange
4.	blue
5.	white/blue
6.	orange
7.	white/brown
8.	brown

TIA/EIA-568-B T568B Wiring

Pin	Color
1.	white/orange
2.	orange
3.	white/green
4.	blue
5.	white/blue
6.	green
7.	white/brown
8.	brown

REQUIREMENT

1. Crimping tool
2. Wire cutter
3. RJ45 connector
5. CAT6 cable

PROCEDURE

1. Strip CAT6 cable to considerable length so that it can be crimped to RJ45 connector.
2. Arrange the wires of CAT6 cable in class B color coding.
3. Insert the wires into RJ45 connector
4. Now crimp the wires with RJ45 connector using crimping tool. Repeat the above steps for the other end.
5. The Ethernet cable is now redy for connecting.

EXPERIMENT- 2

Install and configure network devices like hub, switch and router and create a LAN and perform connectivity test.

HUB

The hubs link various networking devices. A network also functions as amplification by amplifying signals that deteriorate over cables after long distances.

Hubs do not process or address packets, they only send data packets to all connected devices.

There are two types of Hubs Active Hubs and Passive Hubs.

Active HUB

These are hubs that can clean, raise and distribute the signal together with the network with their power supply. It is both a repeater and a cable hub. The total distance between nodes can be increased.

Passive HUB

These are hubs that collect cable from active network nodes are electricity. These hubs relay signals to the guid without being cleaned and improved nor can the distance between nodes be increased.

ROUTER

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

SWITCH

A switch is a multiport bridge with a buffer and a design that can boost its efficiency and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.

To Verify LAN Connectivity

On Desktops : follow these below steps

Step 1 : On desktop 1 go to "Open Network and sharing center" by right clicking on connection.

Step 2 : Go to Ethernet → Properties → Internet Protocol Version 4

Step 3 : Change IPv4 settings, to
- ⊙ Use the following IP address
  IP address : 192.168.100.1
- ● Subnet mask : 255.255.255.0

Step 4 : Press "OK"

Step 5 : Repeat step 1 and step 2 on desktop 2

Step 6 : Now change IPv4 setting on desktop 2, to
- ⊙ Use the following IP address
  IP address : 192.168.100.2
- ● Subnet mask : 255.255.255.0

Step 7 : Press "OK"

Step 8 : Press "Windows button + R" and type "ping 192.168.100.1 -t" on desktop 2.

Step 9 : In command prompt we get reply from 192.168.100.1 if the connection is successful, Else it throws "Request timeout" or "General Failure"

EXPERIMENT - 3

Configure host IP, subnet mask and gateway in LAN

STUDY OF NETWORK IP

Each device connected to the internet has a unique identifier. Most networks today, including all computers on the internet use the TCP/IP as a standard to communicate on the network. In the TCP/IP protocol, this unique identifier is the IP Address. There two kinds of IP Adress are IPV4 and IPv6.

IPV4

It uses 32 binary bits to create a single unique address on the network. An IPV4 address is expressed by four numbers separated by dots. Each number is the decimal (base-10) representation for an eight-digit binary (base-2) number, also called an octet.

IPV6

It uses 128 binary bits to create a single unique address on the network. An IPV6 address is expanded by eight groups of hexadecimal (base-16) numbers separated by colons. Groups of numbers that contain all zeroes are often omitted to save space, leaving a colon seperator to mask the gap.

SUBNET MASK

A subnet mask is a smaller network of computers connected to a larger network through a router.

Every devices has an IP address with two pieces; the client / host address and the server / network address. IP address are either configured by a DHCP server / manually configured (static IP address). The subnet mask splits the IP address into the host and network addresses, thereby defining which part of IP address belongs to the device and which part belongs to the network.

The

GATEWAY

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

Configure Static Address

Step 1 : On Desktop go to "open, Network and Sharing center" by right clicking on connection

Step 2 : Go to Ethernet → Properties → IPv4

Step 3 : Change IPv4 settings to

- ⊙ Use the following IP address
  - IP address : 192.168.100.1
  - Subnet mask : 255.255.255.0
- ⊙ Use the following DNS server address

Step 4 : Press "OK"

Step 5 : Press "Windows button + R", type "ping 192.168.100.2 -t"

Step 6 : In command Prompt we get reply from 192.168.100.2. This step is used to verify connectivity.

Configure Dynamic Address

Step 1 : On Desktop go to "open Network & Sharing center" by right clicking on connection.

Step 2 : Go to Ethernet → Properties → Internet Protocol version 4

Step 3 : In IPv4 change settings to
- ⊙ Obtain an IP address automatically.
- ⊙ Obtain DNS server address automatically.

Step 4 : Press "OK"

Step 5 : Press "Windows + R" button, type ping followed by ip address to verify connectivity.

Step 6 : Go to Ethernet → Details, we can see
IPv4 Address : 172.16.12.231
IPv4 subnet mask : 255.255.240.0

EXPERIMENT – 4

Study of basic Network configuration commands and utilities to debug the network issues.

Networking Commands

1. **Ping** :

It is used to testing a network host capacity to interact with another host. Just enter the command ping, followed by target hosts name or IP address. This is performed by using internet control message protocol which allows echo packet to be sent to destination host and a linking mechanism.

If destination host reply to requesting host that means host is reachable. This utility usually gives a basic image of where there may be a specific networking issue.

Options : target, -a, -t, -ncount, -rcount

2. **Netstat** :

It is a common TCP-IP networking command line method in most windows, linux, UNIX and other OS. It provides the statistics and information in the use of current TCP-IP connection network about protocol.

Options : -a, -b, -c, -o, -v, -r

3. IP Config :

The command IP config will display basic commands about the device IP address configuration. It is used inorder to resolve DNS and DHCP issues.

4. Hostname :

To communicate with each other, the computer needs a unique address and hostname can be alphabetic / alphanumeric and specific symbols to define a specific node / device.

5. Tracert :

This command is a command prompt and to get the network packet being sent and received and no of hops required for that packet to reach to target. It is also referred to tracerroute.

6. Nslookup :

It stands for Name server lookup command. It is a network utility command to obtain information about internet servers. It provides name server for DNS and IP address.

7. Route :

In IP networks, routing tables are used to direct packets from one subnet to another. The route command provides the devices routing tables.

8. ARP :

It stands for address resolution protocol. It depends on MAC address. It provides information like address, flags, mask and IFace.

9. Path Ping :

This command provides a combination of best aspects of Tracert and Ping.

Options : -w timeout, target etc.

EXPERIMENT : 5

Case study of Campus Network Operation Center.

A campus area network is a computer area network that spans a limited geographic area. CANs interconnect multiple local area networks within an educational / corporate campus. Most CANs connect to public internet CANs are smaller than Metropolitan Area Network (MANs) and wide area networks WANs which stretch over large geographic area. The organization that owns the campus also owns and operators all the networking infrastructure for the CAN.

CANs provide internet access for students and faculty. CANs also enable connected users to quickly share files and data within the network. Since data does not have to leave the CAN, users experience far less latency than they would when sending and receiving data within MAN / WAN.

Benefits of CAN

- Speed :

Communication within a CAN takes place over Local Area Network (LAN) so data transfer rate between systems is little bit fast than Internet.

- **Security :**

Network administrators of campus take care of network by continuous monitoring, tracking and limiting access. To protect network from unauthorized access firewall is placed between network & internet.

- **Cost :**

With a little effort and maintenance, network works well by providing fast data transfer rate with multi-departmental network access. It can be enabled wirelessly, where wiring and cabling costs can be managed. So to work with in a campus using CAN is cost-effective in view of performance.

Different Networks can be connected into a CAN.

Within distance of 300 feet switch can be used to connect the nodes and above 300 feet fiber cables can be used.

There are 5 Servers. Among 5 two are IBM servers. Total of about 1000 systems are in the campus. The campus is equipped with 1000 Mbps network card.

- **Campus Network**

  - 10 G Network
  - Supports 1200 systems
  - Used Cat 6 UTP cabling for inside the Departments and fiber cable if the distance is more than 100 meters or 300 feet.

- Wifi with more than 25 hotspots.

- Two Internet leased lines are available
  → 100 Mbps bank (BSNL)
  → 100 Mbps Airtel

- Servers

  - Private Cloud Server
  - Data Server
  - Remote Service Access Server
  - SMB server
  - Network Management Service.

EXPERIMENT- 6

Packet capture and header analysis by wire-shark (TCP- UDP, IP)

Installing Wireshark on Ubuntu

The wireshark utility is available on all major desktop platforms i.e; Linux, Microsoft Windows, FreeBSD, MacOS, Solaris and many more.

Following are the steps to install wireshark on Ubuntu

Step 1 : Update APT

First, as always, update and upgrade your APT through the following command

```
$ sudo apt update
$ sudo apt upgrade
```

Step 2 : Download and Install Wireshark

Now that wireshark's latest version has been added to the APT, you can download and install it with the following command.

```
$ sudo apt install wireshark
```

Step 3 : Enable Root Privilegs

When wireshark installs on your system you will be prompted by the following window. As wireshark requires super user / root privileges to operate, this option asks to enable / disable permissions for all every user on the system. Press the "Yes" button to allow other users, or press the "No" button to restrict other users from using wireshark.

Step 4 : Launch Wireshark

In the terminal window, type the following command to start the wireshark application

$ sudo wireshark

Step 5 : To start capture press on wireshark icon

Step 6 : Capturing packets from multiple interfaces

To capture packets from multiple interfaces press and hold <ctrl> and click on the interfaces that you want to capture packets to and from and then click on the start capturing packets icon.

Note : There are three sections on Wireshark GUI

1. List of Packets captured
2. Information of packets captured
3. Raw data in the packets.

Step 7 : Stopping packet capture in Wireshark

Click on the red icon to stop capturing wireshark packets.

EXPERIMENT : 7

Implement client server communication using sockets.

```
# server.py

import socket

def server_program :

    host = socket.hostname ()
    port = 8080

    server_socket = socket.socket ()
    server_socket.bind ((host, port))

    server_socket.listens (2)
    conn, address = server_socket.accept ()
    print (" Connection from ", str (address))

    while True :
        data = conn.recv (1024).decode ()
        if not data :
            break
        print (" From connected user : ", data)
        data = input (" → ")
        conn.send (data.encode ())
    conn.close ()

if __name__ == '__main__' :
    server_program
```

```
# client.py

import socket

def client_program :

    host = socket.hostname ()
    port = 8080

    client_socket = socket.socket()
    client_socket.connect ( (host, port))

    message = input ("→ ")

    while message.tolower.strip() != "bye" :
        client_socket.send (message.encode)
        data = client_socket.recv(1024).decode()
        print ("Received from server", data)

        message = input ("→ ")

if __name__ == "__main__"
    client_program ()
```

OUTPUT :

Client

→ hi

Received from server : hello

→ Bye

Server

Connection from : ('127.0.0.1', 57406)

from Connected user : hi

→ hello