

Contents

EXPERIMENT NO. 1	2
AIM: Study of Data Communication and Networking. Identify five components of Data communication system.	2
EXPERIMENT NO. 2	5
AIM: Study of computer network OSI model layered architecture.	5
EXPERIMENT NO. 3	7
AIM: Installation of TC/IP protocol configuration and study the classification of addresses employing TCP/IP protocols.	7
EXPERIMENT NO. 4	9
AIM: Write a C program to determine if the IP address is in Class A, B, C, D, or E.	9
EXPERIMENT NO. 5	11
AIM: Write a C program to translate dotted decimal IP address into 32 bit address.	11
EXPERIMENT NO. 6	13
AIM: Study of basic network commands: ipconfig, hostname, ping <ip_address>, tracert <ip_address>, netstat<ip_address> etc.	13
EXPERIMENT NO. 7	16
AIM: To establish a straight over and a cross over cable in LAN.	16
Straight Cable	16
Crossover Cable	16
EXPERIMENT NO. 8	19
AIM: To establish a peer-to-peer connection and share files between two PCs using a crossover LAN cable.	19

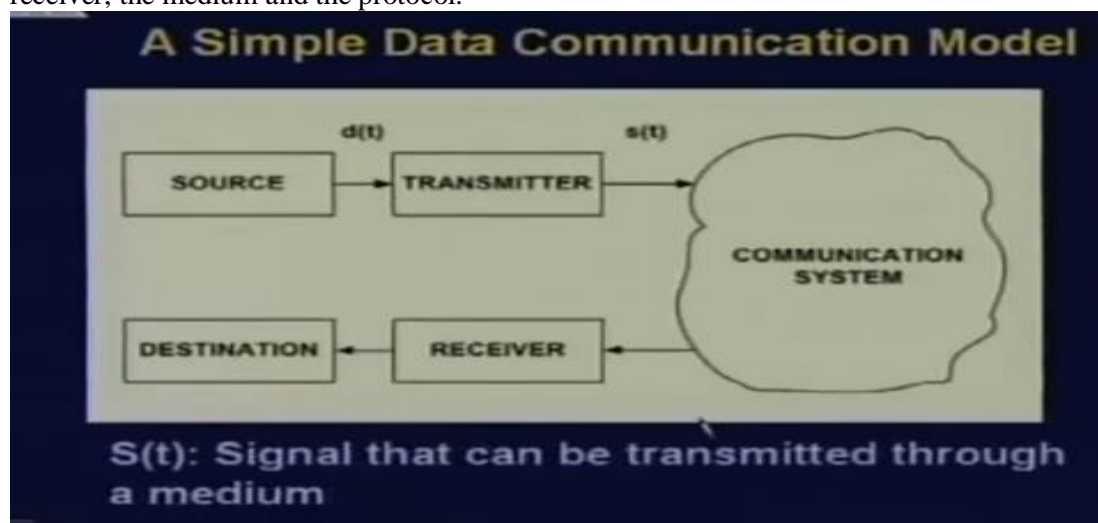
EXPERIMENT NO. 1

AIM: Study of Data Communication and Networking. Identify five components of Data communication system.

THEORY:

Introduction:

Data communication is the moving or transferring of data between two electronic devices using a transmission medium of some kind. Data Communication is a system consisting of carries and related devices used to transport data from one point to another. Communication means to convey a message, an idea, a picture or speech that is received and understood clearly and correctly by the person for whom it is conveyed. Data communication has five basic components: the message, the sender, the receiver, the medium and the protocol.



Communication Systems:

A Communication system is the combination of hardware, software and data transfer links that make up a communication facility for transferring data in a cost effective and efficient manner. A communication system itself can be either analog or digital. The technique by which a digital signal is converted to its analog form is known as Modulation

The reverse process i.e. conversion of analog signal to digital signal is known as Demodulation. These processes of conversions carried out by a special device called Modem.

Components of Data Communications:

i. Message

In a data communication system, the message is the information sent out through the system. The message may include numbers, words, photos, other graphics, sounds, video or a combination of any of these.

Messages in a data communication system are put together in analog or digital form and broken into groups or segments of data called packets. Each packet has a payload -- the actual data being sent -- and a header -- information about the type of data in the payload, where it came from, where it is going, and how it should be reassembled so the message is clear and in order when it arrives at the destination.

ii. Sender

The sender in a data communication sequence is the device that generates the messages. Sometimes these devices are called sources or transmitters instead of senders. Some sending devices are desktop and laptop

computers, netbooks, smartphones, video cameras, workstations, telephones, fax machines and tablets. Television stations, radio stations, short wave radios and walkie talkies are also considered senders -- or transmitters -- in a data communication system.

iii. Receiver

The receiver is the device on the other end of the data communication transmission that gets the message and reassembles it. Many of the same devices that function as receivers also function as senders, such as computers, smart phones and telephone handsets. Some, however, are only receivers, such as radios, printers, or televisions.

iv. Medium

The medium is the means by which the message travels from the sender to the receiver. In a data communication system this includes the wire, twisted wire, local area network (LAN) cable, fiber optic cable, microwave signal, satellite signal or any other transmission medium used in a network. A point to point connection is comprised of only two devices connected by a dedicated medium. On the other hand, multiple devices may be connected through mediums into networks. The Internet is a collection of many different networks creating a distributed network. Other networks include LANs, Metropolitan Area Networks (MANs) and Wide Area Networks (WANs).

v. Protocol

A protocol is a set of rules that guides how data communication is carried out. Every device that wants to communicate with each other must use the same protocol in order to exchange messages. Every device on the Internet, for example, uses the TCP/IP protocol. AppleTalk is another protocol. The keys to protocol are syntax, semantics and timing. All the rules and standards are necessary so that devices manufactured by many different companies can still communicate with each other.

Computer network:

A computer network, or simply a network, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information. Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. Simply, more than one computer interconnected through a communication medium for information interchange is called a computer network.

Networks may be classified according to a wide variety of characteristics, such as the medium used to transport the data, communications protocol used, scale, topology, benefit, and organizational scope. Classification of Computer Network:

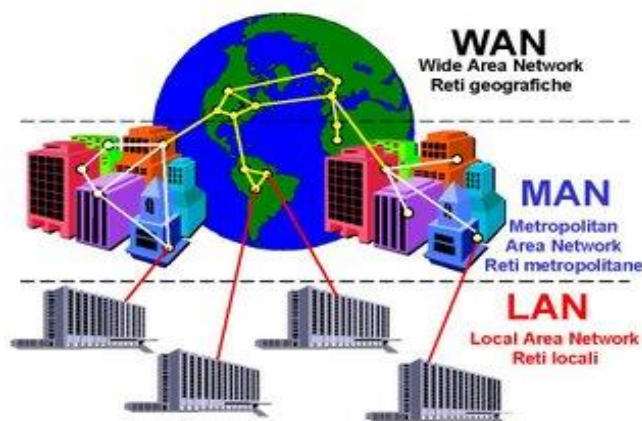


Figure 1: Classification of computer network

Judging from the geographical range covered by a network, usually divided into three types, LAN, MAN, and WAN.

Local Area Network (LAN)

LAN is a computer network that covers an area in one room, one building, or several adjacent buildings. For example, the network in a single integrated campus or at a company location is classified as a LAN. LAN transmission media generally use a cable (UTP, coaxial cable, or fiber optics). But some are not using a cable and is referred to as Wireless LAN (WLAN). LAN speeds ranging from 10 Mbps to 1 Gbps.

According to the LAN type can be either a client / server (network model that has a client and server) or peer-to-peer (network model that gives equal footing to all computers).

Metropolitan Area Network (MAN)

MAN is a network that covers an area of one town or with a range of about 10-45 km. Network connecting several banks located in one city or campus that is spread in several locations classified as a MAN. Such networks generally use transmission media by micro waves or radio waves. But there also are using leased lines (leased line).

Wide Area Network (WAN)

Network which includes inter-city, inter-provincial, inter-state, and even between continents called the WAN. Example of a WAN is a network that connects the ATM (Automatic Teller Machine). Another example is the internet.

CONCLUSION: In this experiment we studied simple data communication model along with components, also seen computer network and different types of computer networks.

EXPERIMENT NO. 2

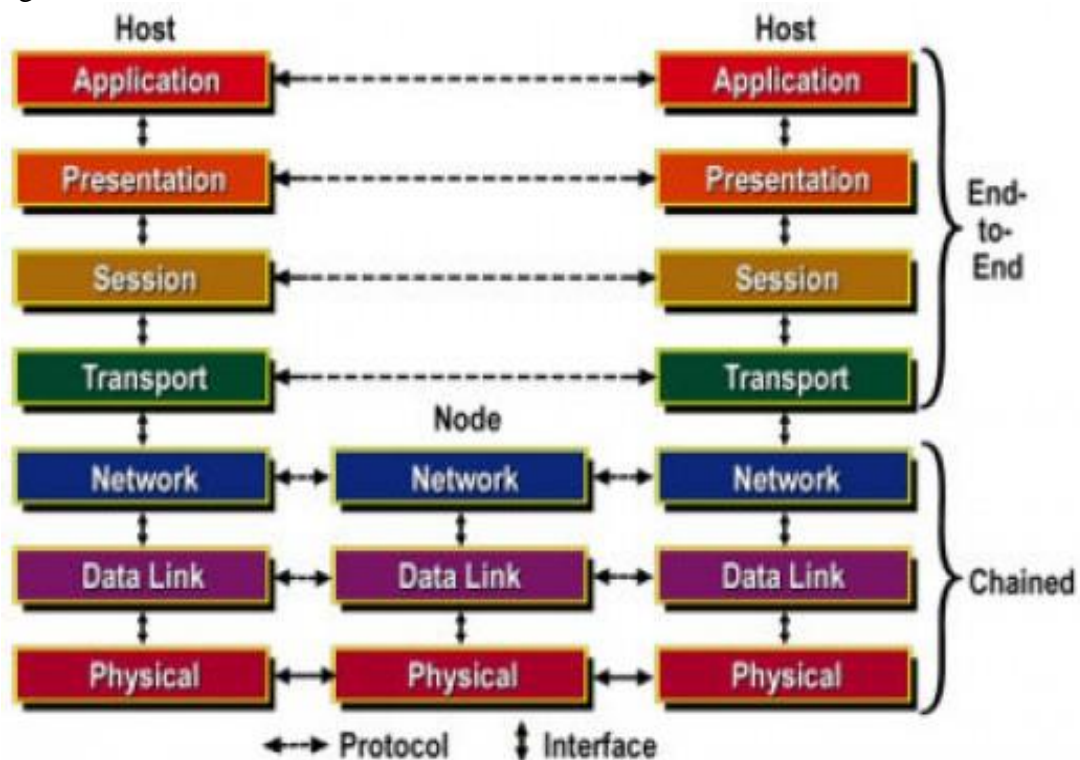
AIM: Study of computer network OSI model layered architecture.

THEORY:

OSI MODEL:

Open Systems Interconnection (OSI) model is a reference model developed by ISO (International Organization for Standardization) in 1984, as a conceptual framework of standards for communication in the network across different equipment and applications by different vendors. It is now considered the primary architectural model for inter-computing and internetworking communications. Most of the network communication protocols used today have a structure based on the OSI model. The OSI model defines the communications process into 7 layers, which divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.

The seven layers of the OSI model can be divided into two groups: upper layers (layers 7, 6 & 5) and lower layers (layers 4, 3, 2, 1). The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the wires, for example) and is responsible for placing data on the medium.



The specific description for each layer is as follows:

Layer 7: Application Layer

Defines interface to user processes for communication and data transfer in network
Provides standardized services such as virtual terminal, file and job transfer and operations

Layer 6: Presentation Layer

Masks the differences of data formats between dissimilar systems
Specifies architecture-independent data transfer format
Encodes and decodes data; Encrypts and decrypts data; Compresses and decompresses data

Layer 5: Session Layer

Manages user sessions and dialogues
Controls establishment and termination of logic links between users
Reports upper layer errors

Layer 4: Transport Layer

Manages end-to-end message delivery in network
Provides reliable and sequential packet delivery through error recovery and flow control mechanisms
Provides connectionless oriented packet delivery

Layer 3: Network Layer

Determines how data are transferred between network devices
Routes packets according to unique network device addresses
Provides flow and congestion control to prevent network resource depletion

Layer 2: Data Link Layer

Defines procedures for operating the communication links
Frames packets
Detects and corrects packets transmit errors

Layer 1: Physical Layer

Defines physical means of sending data over network devices
Interfaces between network medium and devices
Defines optical, electrical and mechanical characteristics

CONCLUSION: In this experiment we have studied network topologies & OSI Model in detail.

EXPERIMENT NO. 3

AIM: Installation of TC/IP protocol configuration and study the classification of addresses employing TCP/IP protocols.

THEORY:

TCP/IP

TCP/IP is the communication protocol for communication between computers on the Internet. TCP/IP stands for **T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol. TCP/IP defines how electronic devices (like computers) should be connected to the Internet, and how data should be transmitted between them.

Inside TCP/IP

Inside the TCP/IP standard there are several protocols for handling data communication:

- TCP (Transmission Control Protocol) communication between applications
- UDP (User Datagram Protocol) simple communication between applications
- IP (Internet Protocol) communication between computers
- ICMP (Internet Control Message Protocol) for errors and statistics
- DHCP (Dynamic Host Configuration Protocol) for dynamic addressing

IP is Connection-Less

- IP is for communication between computers.
- IP is a "connection-less" communication protocol.
- IP does not occupy the communication line between two computers. IP reduces the need for network lines. Each line can be used for communication between many different computers at the same time.
- With IP, messages (or other data) are broken up into small independent "packets" and sent between computers via the Internet.
- IP is responsible for "routing" each packet to the correct destination.

TCP/IP

- TCP/IP is TCP and IP working together.
- TCP takes care of the communication between your application software (i.e. your browser) and your network software.
- IP takes care of the communication with other computers.
- TCP is responsible for breaking data down into IP packets before they are sent, and for assembling the packets when they arrive.
- IP is responsible for sending the packets to the correct destination.

To configure TCP/IP, you must be logged on as a member of the **Administrators** group on the local computer.

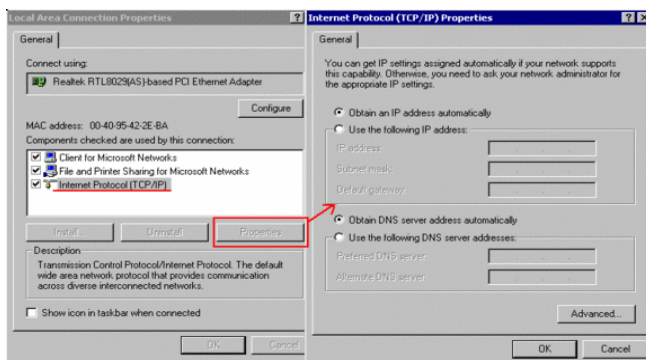
Complete the following steps to install and configure the TCP/IP protocol.

1. [Open](#) the Network utility.
2. Right-click the connection to which you want to add a network component, and then click **Properties**.
3. If **Internet Protocol (TCP/IP)** is listed, skip to Step 6. If **Internet Protocol (TCP/IP)** is not listed, click **Install**.
4. In the **Select Network Component Type** dialog box, click **Protocol**, and then click **Add**.

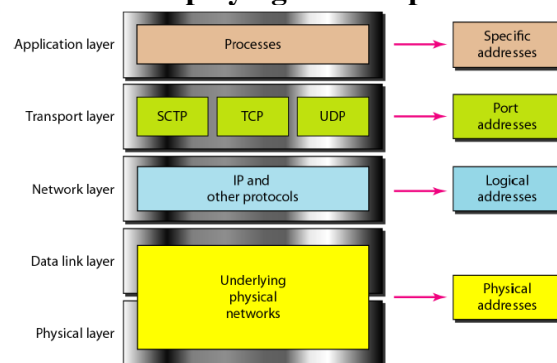
5. From the **Network Protocol** list, select **TCP/IP Protocol** and click **OK**.
6. From the **General** tab (for local area connections) or the **Networking** tab (for all other connections), select **Internet Protocol (TCP/IP)**, and then click **Properties**.
7. Configure TCP/IP either automatically or manually.

Contact your network administrator to find out if there is a DHCP server installed on your network.

- **Automatically** – You can automatically configure TCP/IP services if you have a DHCP server on your network. This automatic process ensures easy and accurate installation of TCP/IP because your local computer is configured with the correct IP address, subnet mask, and default gateway.
To configure automatically, select **Obtain an IP address automatically**, and then click **OK**.
- **Manually** – You must configure TCP/IP manually if you do not have a DHCP server on your network, or if you are configuring a Windows server to be a DHCP server. In this case, you must manually enter valid addressing information after the TCP/IP protocol software is installed on your computer. To avoid duplicate addresses, be sure to use the values for IP addresses and subnet masks that are supplied by your network administrator.



Addresses employing TCP/IP protocols



Through logical address the system identify a network (source to destination). After identifying the network physical address is used to identify the host on that network. The port address is used to identify the particular application running on the destination machine.

Logical Address:

An IP address of the system is called logical address. This address is the combination of Net ID and Host ID. This address is used by network layer to identify a particular network (source to destination) among the networks. This address can be changed by changing the host position on the network. So it is called logical address.

Physical address:

Each system having a NIC (Network Interface Card) through which two systems physically connected with each other with cables. The address of the NIC is called Physical address or MAC address. This is specified by the manufacture company of the card. This address is used by data link layer.

Port Address:

There are many applications running on the computer. Each application run with a port no. (Logically) on the computer. This port no. for application is decided by the Kernel of the OS. This port no. is called port address.

CONCLUSION: In this way we had studied TCP/IP in detail.

EXPERIMENT NO. 4

AIM: Write a C program to determine if the IP address is in Class A, B, C, D, or E.

THEORY:

Internet Protocol address

IP address is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "*A name indicates what we seek. An address indicates where it is. A route indicates how to get there.*"

The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995.

IPv4 addresses

In IPv4 an address consists of 32 bits which limits the address space to 4294967296 (2^{32}) possible unique addresses.

Address classes

The first class, designated as *Class A*, contained all addresses in which the most significant bit is zero. The network number for this class is given by the next 7 bits, therefore accommodating 128 networks in total, including the zero network, and including the existing IP networks already allocated. A *Class B* network was a network in which all addresses had the two most-significant bits set to 1 and 0. For these networks, the network address was given by the next 14 bits of the address, thus leaving 16 bits for numbering host on the network for a total of 65536 addresses per network. *Class C* was defined with the 3 high-order bits set to 1, 1, and 0, and designating the next 21 bits to number the networks, leaving each network with 256 local addresses. The leading bit sequence *111* designated an "*escape to extended addressing mode*", which was later subdivided in to Class D (*1110*) for multicast addressing, while leaving as reserved for future use the *1111* block designated as Class E.

This addressing scheme is illustrated in the following table:

Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

ALGORITHM:

1. Start
2. Read IP in dotted decimal form
Check IP is in correct form
If the first value is in between 0-127, display Class A
If the first value is in between 128-191, display Class B
If the first value is in between 192-223, display Class C
If the first value is in between 224-239, display Class D
If the first value is in between 240-255, display Class E
3. Exit
4. Stop

CODE:

```
#include<stdio.h>
#include<conio.h>
int main()
{
char ip[20];
int fstoct;
printf("Enter IP Address""(""ipv4"")::");
scanf("%s", ip);
fstoct= atoi(strtok(ip, "."));
if (fstoct >= 1 && fstoct<=126){
printf("Given IP Address Belongs to Class: A");
}
else if (fstoct >= 127 && fstoct<=191){
printf("Given IP Address Belongs to Class: B");
}
else if (fstoct >= 192 && fstoct<=223){
printf("Given IP Address Belongs to Class: C");
}
else if (fstoct >= 224 && fstoct<=239){
printf("Given IP Address Belongs to Class: D");
}
else if (fstoct >= 240 && fstoct<=255){
printf("Given IP Address Belongs to Class: E");
}
else {
printf("----Invalid IP----");
}
return 0;
}
```

Input: Enter IP Address(ipv4)::92.56.1.1

Output: Given IP Address Belongs to Class A

CONCLUSION: Hence we have successfully performed the program to display the class of entered IP address.

EXPERIMENT NO. 5

AIM: Write a C program to translate dotted decimal IP address into 32 bit address.

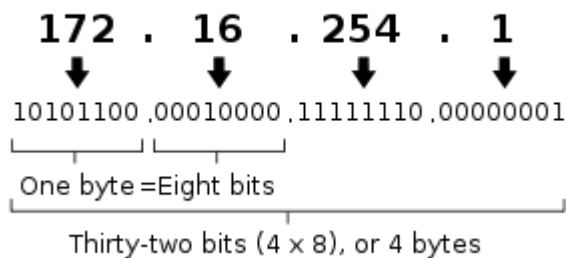
THEORY:

Two versions of the Internet Protocol (IP) are in use: IP Version 4 and IP Version 6. Each version defines an IP address differently. Because of its prevalence, the generic term *IP address* typically still refers to the addresses defined by IPv4. In IPv4 an address consists of 32 bits which limits the address space to 4294967296 (2^{32}) possible unique addresses. IPv4 reserves some addresses for special purposes such as private networks (~18 million addresses) or multicast addresses (~270 million addresses).

IPv4 addresses are canonically represented in dot-decimal notation, which consists of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 172.16.254.1. Each part represents a group of 8 bits (octet) of the address. In some cases of technical writing, IPv4 addresses may be presented in various hexadecimal, octal, or binary representations.

IPv4 addresses

An IPv4 address (dotted-decimal notation)



Decomposition of an IPv4 address from dot-decimal notation to its binary value.

ALGORITHM:

1. Start
2. Read IP Address in dotted decimal format
3. Check IP ,whether it is correct or incorrect
4. If incorrect IP , display message for wrong IP
5. For correct IP
Convert each decimal number into 8-bit binary format
6. display the conversion i.e. 32 bit binary format
7. Stop.

Input:

Enter IP in dotted decimal format

172.16.254.1

Output:

Binary conversion

10101100 00010000 11111110 00000001

CONCLUSION: Hence we have successfully performed the program to convert entered dotted decimal IP address into 32-bit binary format.

EXPERIMENT NO. 6

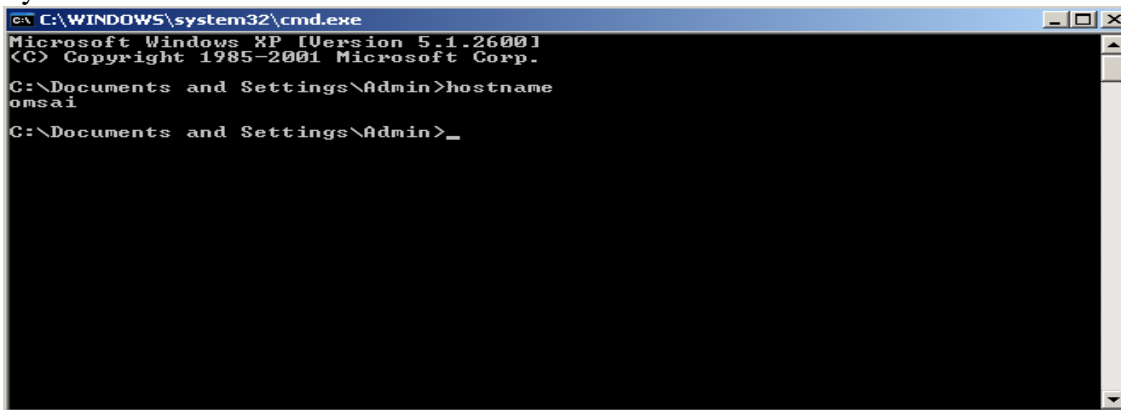
AIM: Study of basic network commands: ipconfig, hostname, ping <ip_address>, tracert <ip_address>, netstat<ip_address> etc..

THEORY:

hostname:

The hostname command displays the host name of the Windows XP computer currently logged into.

Syntax:



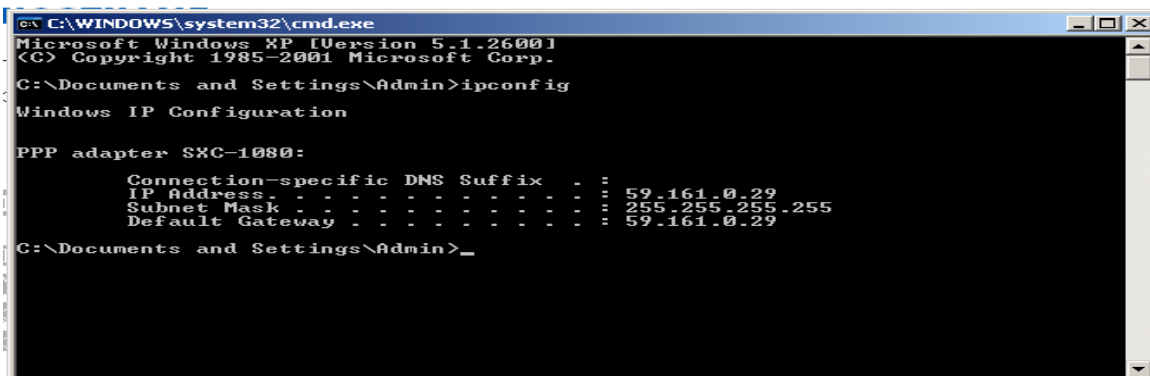
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Admin>hostname
omsai

C:\Documents and Settings\Admin>_
```

ipconfig:

Ipconfig is used to display the network settings currently assigned and given by a network. This command can be utilized to verify a network connection as well as to verify your network settings.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Admin>ipconfig

Windows IP Configuration

PPP adapter SXC-1080:

    Connection-specific DNS Suffix . : 
    IP Address . . . . . : 59.161.0.29
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 59.161.0.29

C:\Documents and Settings\Admin>_
```

ping :

The ping command is used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used as a simple way verify that a computer can communicate over the network with another computer or network device.

The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides.

Ping Command Syntax:

ping -a 192.168.1.22

In this example I'm asking the ping command to find the hostname assigned to the *192.168.1.22* IP address but otherwise ping it as normal.

Pinging J3RTY22 [192.168.1.22] with 32 bytes of data:

Reply from 192.168.1.22: bytes=32 time<1ms TTL=64

Reply from 192.168.1.22: bytes=32 time<1ms TTL=64

Reply from 192.168.1.22: bytes=32 time=1ms TTL=64

Reply from 192.168.1.22: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.22:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

tracert :

The tracert command is used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify.

You might also sometimes see the tracert command referred to as the *trace route command* or *traceroute command*.

Tracert Command Syntax:

Tracing route to 192.168.1.1 over a maximum of 30 hops

1 <1 ms <1 ms <1 ms 192.168.1.254

2 <1 ms <1 ms <1 ms 192.168.1.1

Trace complete.

In this example, you can see that tracert found a network device using the IP address of *192.168.1.254*, let's say a network switch, followed by the destination, *192.168.1.1*, the router.

tracert www.google.com

Using the tracert command as shown above, we're asking tracert to show us the path from the local computer all the way to the network device with the hostname *www.google.com*.

Tracing route to www.l.google.com [209.85.225.104]

over a maximum of 30 hops:

1 <1 ms <1 ms <1 ms 10.1.0.1

2 35 ms 19 ms 29 ms 98.245.140.1

3 11 ms 27 ms 9 ms te-0-3.dnv.comcast.net [68.85.105.201]

...

13 81 ms 76 ms 75 ms 209.85.241.37

14 84 ms 91 ms 87 ms 209.85.248.102

15 76 ms 112 ms 76 ms iy-f104.1e100.net [209.85.225.104]

Trace complete.

In this example we can see that tracert identified fifteen network devices including our router at *10.1.0.1* and all the way through to the *target* of *www.google.com* which we now know uses the public IP address of *209.85.225.104*.

NETSTAT

The netstat command is used to display *very* detailed information about how your computer is communicating with other computers or network devices. Specifically, the netstat command can show details about individual network connections, overall and protocol-specific networking statistics, and much more, all of which could help troubleshoot certain kinds of networking issues.

Netstat Command Syntax:

netstat -f

In this first example, I execute netstat to show all active TCP connections. However, I do want to see the computers I'm connected to in FQDN format [-f] instead of a simple IP address.

Here's an example of what you might see: Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:5357	VM-Windows-7:49229	TIME_WAIT
TCP	127.0.0.1:49225	VM-Windows-7:12080	TIME_WAIT
TCP	192.168.1.14:49194	75.125.212.75:http	CLOSE_WAIT
TCP	192.168.1.14:49196	a795sm.avast.com:http	CLOSE_WAIT
TCP	192.168.1.14:49197	a795sm.avast.com:http	CLOSE_WAIT
TCP	192.168.1.14:49230	TIM-PC:wsd	TIME_WAIT
TCP	192.168.1.14:49231	TIM-PC:icslap	ESTABLISHED
TCP	192.168.1.14:49232	TIM-PC:netbios-ssn	TIME_WAIT
TCP	192.168.1.14:49233	TIM-PC:netbios-ssn	TIME_WAIT
TCP	:::1]:2869	VM-Windows-7:49226	ESTABLISHED
TCP	:::1]:49226	VM-Windows-7:icslap	ESTABLISHED

As you can see, I had 11 active TCP connections at the time I executed netstat. The only protocol (in the *Proto* column) listed is TCP, which was expected because I did not use -a.

You can also see three sets of IP addresses in the *Local Address* column - my actual IP address of 192.168.1.14 and both IPv4 and IPv6 versions of my loopback addresses, along with the port each connection is using. The *Foreign Address* column lists the FQDN (75.125.212.75 didn't resolve for some reason) along with that port as well.

Finally, the *State* column lists the TCP state of that particular connection.

netstat -o :- In this example, I want to run netstat normally so it only shows active TCP connections, but I also want to see the corresponding process identifier [-o] for each connection so I can determine which program on my computer initiated each one.

Here's what my computer displayed:

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	192.168.1.14:49194	75.125.212.75:http	CLOSE_WAIT	2948
TCP	192.168.1.14:49196	a795sm:http	CLOSE_WAIT	2948
TCP	192.168.1.14:49197	a795sm:http	CLOSE_WAIT	2948

You probably noticed the new *PID* column. In this case, the PIDs are all the same, meaning that the same program on my computer opened these connections.

CONCLUSION: In this way we have performed the basic networking commands successfully.

EXPERIMENT NO. 7

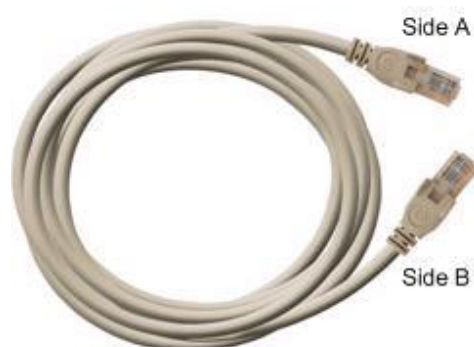
AIM: To establish a straight over and a cross over cable in LAN.

THEORY:

Common Ethernet network cable are straight and crossover cable. This Ethernet network cable is made of 4 pair high performance cable that consists twisted pair conductors that used for data transmission. Both end of cable is called RJ45 connector.

The cable can be categorized as **Cat 5, Cat 5e & Cat 6 UTP cable**. Cat 5 UTP cable can support 10/100 Mbps Ethernet network, whereas Cat 5e and Cat 6 UTP cable can support Ethernet network running at 10/100/1000 Mbps. You might heard about Cat 3 UTP cable, it's not popular anymore since it can only support 10 Mbps Ethernet network.

Straight and crossover cable can be Cat3, Cat 5, Cat 5e or Cat 6 UTP cable, the only difference is each type will have different wire arrangement in the cable for serving different purposes.



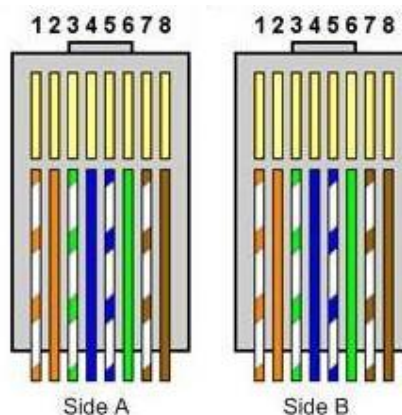
Straight Cable

You usually use straight cable to connect different type of devices. This type of cable will be used most of the time and can be used to:

- 1) Connect a computer to a switch/hub's normal port.
- 2) Connect a computer to a cable/DSL modem's LAN port.
- 3) Connect a router's WAN port to a cable/DSL modem's LAN port.
- 4) Connect a router's LAN port to a switch/hub's uplink port.(normally used for expanding network)
- 5) Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.

If you need to check how straight cable looks like, it's easy. **Both side (side A and side B) of cable have wire arrangement with same color.** Check out different types of straight cable that are available in the market here.

Pin ID	Side A	Side B
1	Orange-white	Orange-white
2	Orange	Orange
3	Green-white	Green-white
4	Blue	Blue
5	Blue-white	Blue-white
6	Green	Green
7	Brown-white	Brown-white
8	Brown	Brown

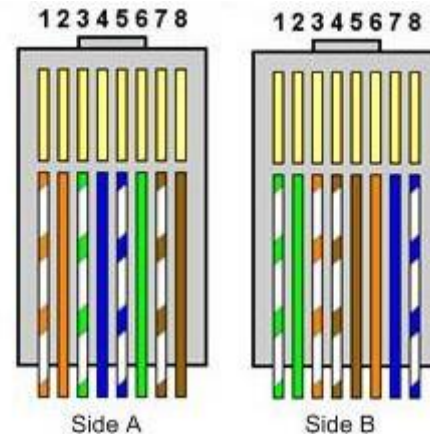


Crossover Cable

Sometimes you will use crossover cable, it's usually used to connect same type of devices. A crossover cable can be used to:

- 1) Connect 2 computers directly.
 - 2) Connect a router's LAN port to a switch/hub's normal port. (Normally used for expanding network)
 - 3) Connect 2 switches/hubs by using normal port in both switches/hubs.
- In you need to check how crossover cable looks like, **both side (side A and side B) of cable have wire arrangement with following different color.**

Pin ID	side A	side B
1	Orange-white	green-white
2	Orange	green
3	green-white	orange-white
4	blue	brown-white
5	blue-white	Brown
6	green	orange
7	brown-white	Blue
8	brown	blue-white



Step 1:

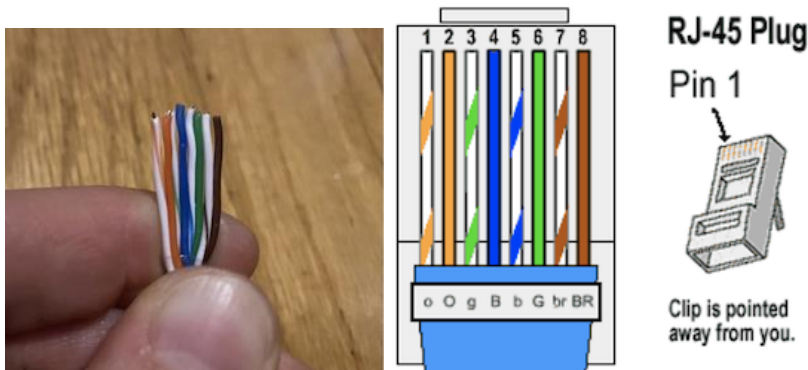


Cut the shielding off the cable, which will expose the 4 pairs of wires. Blue, Green, Orange and Brown. When it comes to creating a straight through cable the color combination does not matter. Whatever the color of the first end is, make the second end the same.

When it comes to RJ45 Standards it's different. The standard rj45 colors are:

White Orange, Orange, White Green, Blue, White Blue, Green, White Brown, Brown

Step 2:

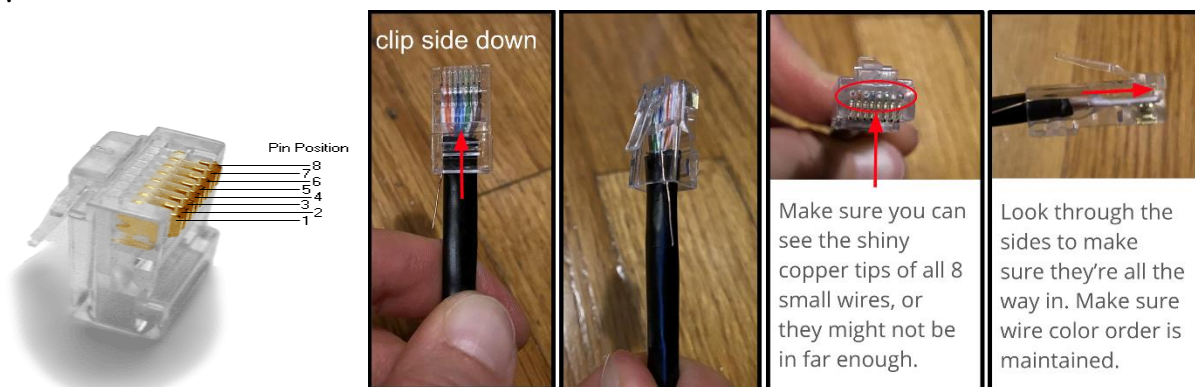


Line the wires according to the image below. This is the rj45 straight through standard colors. This will be the same color on both ends of the cable.

Cut the excess wire off, usually leave half inch. This usually fits in the head perfect.



Above is the final cut. The White Orange is Pin 1 and Brown is Pin 8



Pin Outs (tab facing down and pins away)

Step 3:

RJ45 Head, when placing the wires into the head try to line it up length wise. Similar to what is shown couple images above.

Make sure the wires reach the copper / gold pins. This is important because its what connect the wires to whatever you plug the cable into.

Now, used the crimper to crimp the wire and finished making a LAN Cable.



CONCLUSION: In this experiment we have learned how to create LAN cable.

EXPERIMENT NO. 8

AIM: To establish a peer-to-peer connection and share files between two PCs using a crossover LAN cable.

Equipment Required

- Two PCs
- Ethernet crossover cable
- Operating system: Windows or Linux

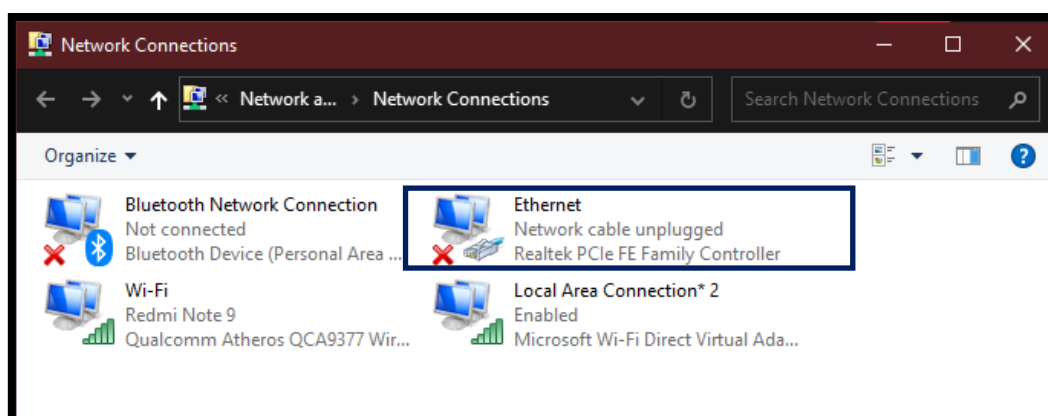
Theory

A peer-to-peer network is a type of network in which all computers are equal and can communicate directly with each other without the need for a central server. Peer-to-peer networks are often used in small offices and homes to share resources such as files, printers, and internet access.

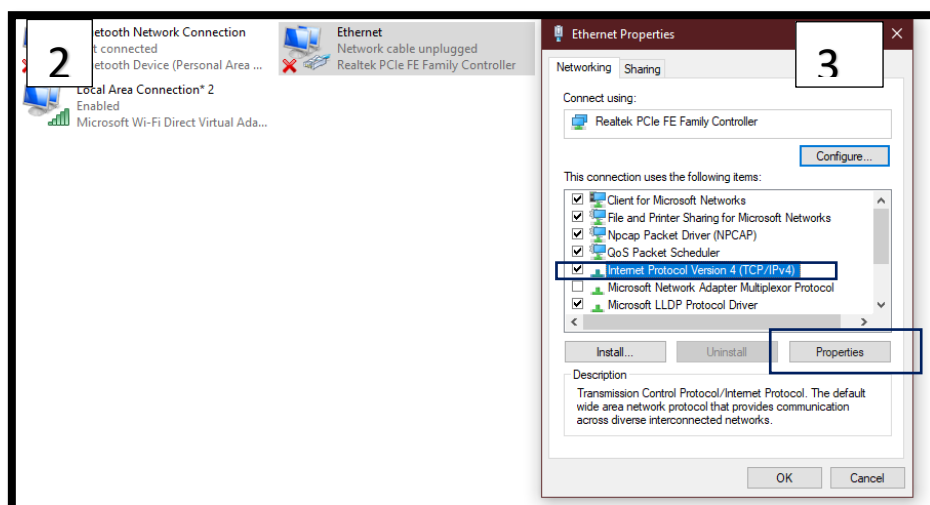
To establish a peer-to-peer connection between two PCs using a crossover LAN cable, follow these steps:

1. Connect one end of the crossover LAN cable to the Ethernet port on PC1.
2. Connect the other end of the crossover LAN cable to the Ethernet port on PC2.
3. Configure the IP addresses of PC1 and PC2 to be in the same subnet. For example, you could configure PC1 to have the IP address 192.168.1.1 and PC2 to have the IP address 192.168.1.2.

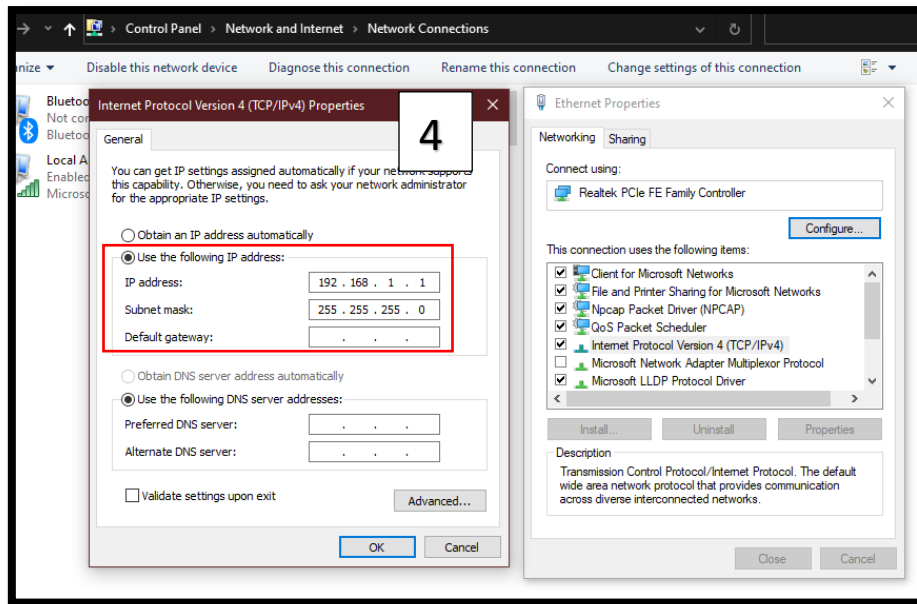
1



2



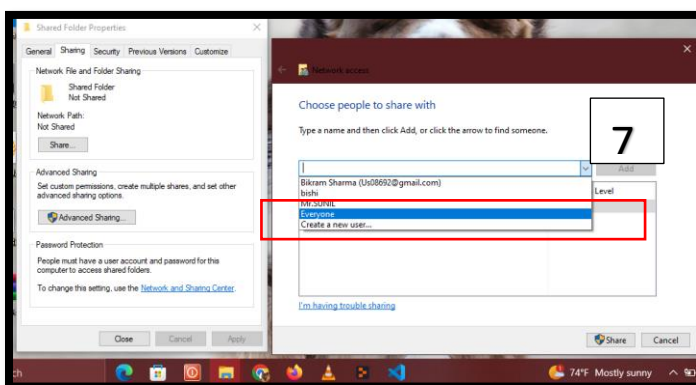
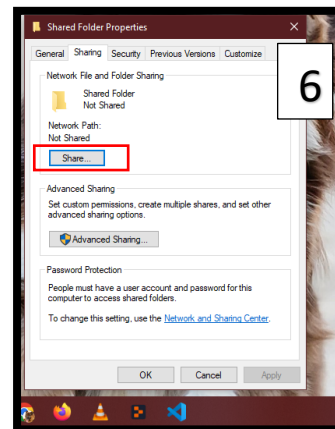
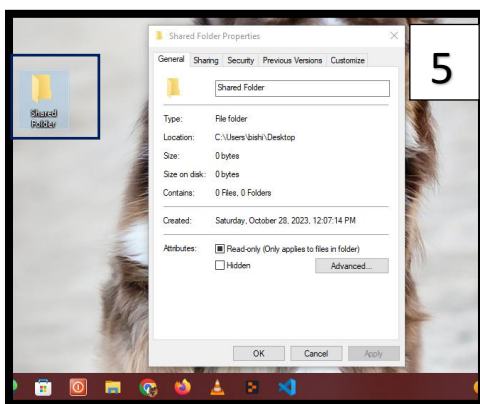
3

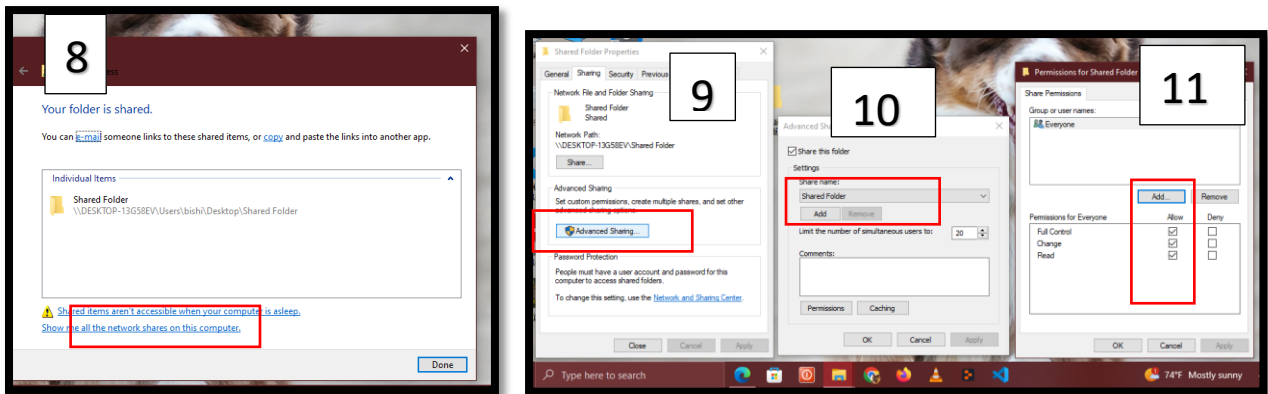


Disable the firewall on both PCs.

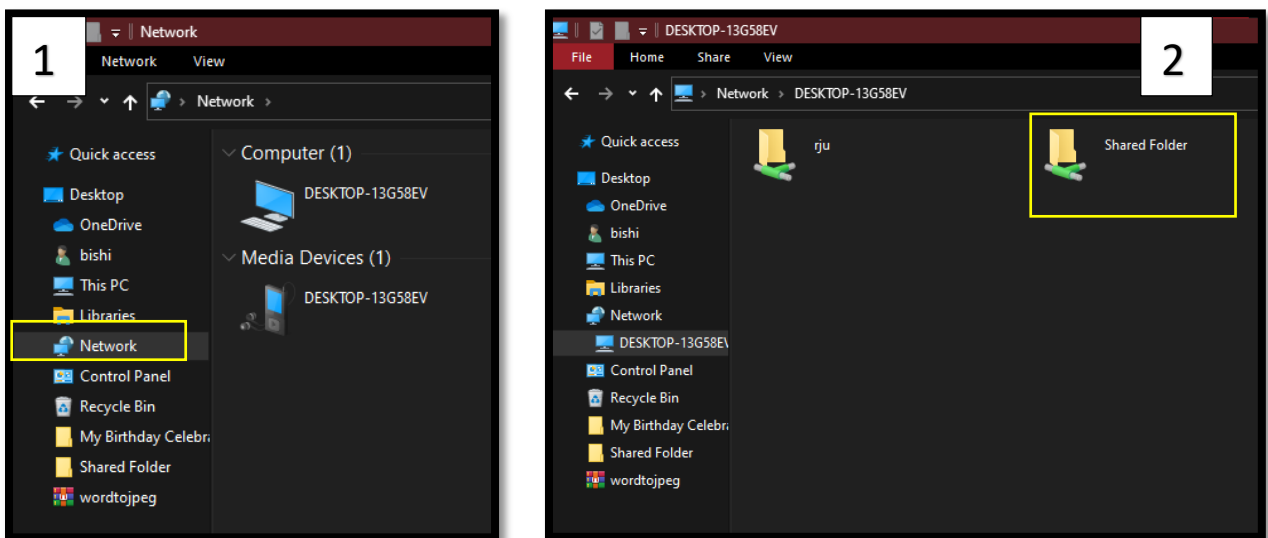
To share files between PC1 and PC2, follow these steps:

1. On PC1, create a shared folder. Right-click on the folder and select Properties. Click on the Sharing tab and select Share. Click on the Add button and enter the username of the user on PC2 who you want to share the folder with provide the necessary permissions of folder control. Click on the OK button.





2. On PC2, open File Explorer and navigate to the Network tab. You should see PC1 listed in the list of devices. Click on PC1 and then click on the Shared folder that you created on PC1. You should now be able to access the files in the shared folder.



CONCLUSION:

In this lab, we successfully established a peer-to-peer connection between two PCs using a crossover LAN cable and shared files between the two PCs. Peer-to-peer networks are a simple and effective way to share resources between a small numbers of computers.