LABORATORY MANUAL
ON
NETWORKING LAB.

FOUTH SEMESTER

DEPARTMENT OF INFORMATION TECHNOLOGY

GOVERNMENT POLYTECHNIC, BHUBANESWAR
Government of Odisha
ସରକାରୀ ବହୁବୃତ୍ତି ଅନୁଷ୍ଠାନ, ଭୁବନେଶ୍ୱର

VISION AND MISSION OF THE INSTITUTE

VISION

The Vision of the Government Polytechnic, Bhubaneswar is to be a premier Diploma Institution in the Eastern India by transforming the learners into competent technocrats by imparting technical education in multiple disciplines.

MISSION

The mission of the Government Polytechnic, Bhubaneswar is to:

- Focus on quality teaching and learning by providing better academic environment for both faculties and students.
- Develop professionally and technically skilled students who work for betterment of the society
- Nurture positive attitude and social values amongst the students and staff.

VISION AND MISSION OF THE DEPARTMENT

DEPARTMENT OF INFORMATION TECHNOLOGY

VISION

The Vision of the Department of Information Technology is to develop knowledge and skill of students by quality education to make responsible and competent technocrats who will work for the needs of industries and betterment of the society.

MISSION

The Mission of the Department of Information Technology is to:

M-1. Provide an excellent learning environment for the students to be technically efficient in solving problems.

M-2. Prepare the students with strong fundamental concepts, analytical capability and programming skills.

M-3. Create a nurturing environment for lifelong learning.

M-4. Generate social awareness and responsibility within the students to serve the mankind and protect the environment.

Program Educational Objectives (PEOs)

Program Educational Objective of Diploma in Information Technology:

The Program Educational Objectives (PEOs) of the Department of Information Technology are:

PEO-1: ***Strong Fundamentals & Technically skilled:*** *To equip the students with sound knowledge in mathematics, science and basic engineering fundamentals and develop skill to solve engineering problems.*

PEO-2: ***Higher study and Professional responsibilities:*** *To enable students to pursue higher studies for professional growth and/or work as an entrepreneur for successful professional career.*

PEO-3: ***Teamwork and lifelong learning:*** *To inculcate soft skill, professional and ethical attitude, teamwork, leadership skills and multidisciplinary approach within the students which will enable them to correlate societal issue with engineering solution and pursue lifelong learning.*

Program Outcomes and Program Specific Outcomes (PSOs)

Program Outcomes for an Engineering diploma graduate:

i) **Basic and Discipline specific knowledge:** Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the engineering problems

ii) **Problem analysis:** Identify and analyze well-defined engineering problems using codified standard methods.

iii) **Design/ development of solutions:** Design solutions for well-defined technical problems and assist with the design of systems components or processes to meet specified needs.

iv) **Engineering Tools, Experimentation and Testing:** Apply modern engineering tools and appropriate technique to conduct standard tests and measurements.

v) **Engineering practices for society, sustainability and environment:** Apply appropriate technology in context of society, sustainability, environment and ethical practices.

vi) **Project Management:** Use engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about well-defined engineering activities.

vii) **Life-long learning:** Ability to analyze individual needs and engage in updating in the context of technological changes.

Program Specific Outcome of Diploma in Information Technology:

PSO-1: Ability to design and develop methodologies in computer programming and apply those skills in the field of Information Technology.

PSO-2: Develop potentiality to apply the skills learnt for betterment of the society by updating it on the basis of the advanced technological changes and effectively communicate about well-defined engineering activities.

NETWORKING LAB PR-2

Lab. Period	6 period/week	Term works	50 marks
Examination	3hrs	End semester examination	50 marks
Total period	90	Maximum marks	100 marks

Exp. No.	Subject
1	Recognize the physical topology and cabling (coaxial, ofc, Utp, stp) of a network.
2	Recognition and use of various types of connectors rj-45, rj-11, bnc and scst
3	Making of cross cable and straight cable
4	Install and configure a network interface card in a workstation
5	Identify the IP address of a workstation and the class of the address and configure the IP address on a workstation
6	Managing user accounts in windows and linux
7	Sharing of hardware resources in the network.
8	Use of netstat and its options.
9	Connectivity troubleshooting using ping, IPconfig
10	Installation of network operating system (nos)
11	Create a network of at least 6 computers.
12	Study of layers of network and configuring network operating system
13	Study of routing and switching, configuring of switch and routers, troubleshooting of networks
14	Study of scaling of networks, design verities of lan and forward of traffic
15	Study wan concepts and configure and forward traffic in wan
16	Configure IPv4 and IPv6 and learn quality, security and other services
17	Learn network programming
18	Troubles shoot networks

COURSE OUTCOMES:

After completion of this course the student will be able to

1. recognize the physical topology and cabling of a network
2. identify the IP address and configure the IP address on a workstation and Managing user accounts in windows and linux
3. use of netstat and its options, connectivity troubleshooting using ping, IPconfig and Installation of network operating system
4. configuring network operating system, routing, switching and configuring of switch and routers
5. Create a network of at least 6 computers and troubleshooting of networks

COs, POs and PSOs Mapping

Cos, Pos and PSOs mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2
CO1	2	2	1	2	2	-	2	1	2
CO2	2	2	-	2	2	-	2	1	2
CO3	2	1	1	2	2	-	2	1	2
CO4	2	2	-	1	1	-	2	1	1
CO5	2	2	-	1	1	1	2	1	2
Total	10	9	2	8	8	1	10	5	9
Average	2	1.8	1	1.6	1.6	1	2	1	1.8

Experiment No-1

1. **Context**
   - **1.1 Subject: - Computer Network**
   - **1.2 Expt: - 1**
   - **1.3 Topic: - Physical topology and cabling**
   - **1.4 Sub-topic: - Networks**
   - **1.5 Title of the experiment: - recognize the physical topology and cabling (coaxial, ofc, utp, stp) of a network.**
   - **1.6 Environment/location: computer lab**
2. **Aim of the experiment: -** recognize the physical topology and cabling (coaxial, ofc, Utp, stp) of a network.
3. **Objective of the experiment: -**
   On the completion of the experiment the student will be able to:
   1. what is topology?
   2. Know types of topology
   3. What is cabling?
   4. Know types of cabling.
   5. Like: - coaxial, ofc, Utp, stp
4. **Procedure: -**

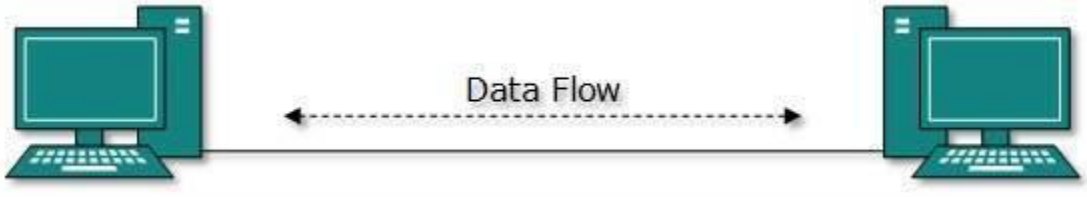
What is topology: -a network topology describes the arrangement of systems on a computer network. It defines how the computers, or nodes, within the network are arranged and connected to each other. Some common network topologies include star, ring, line, bus, and tree configurations.

Or

A network topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

point-to-point

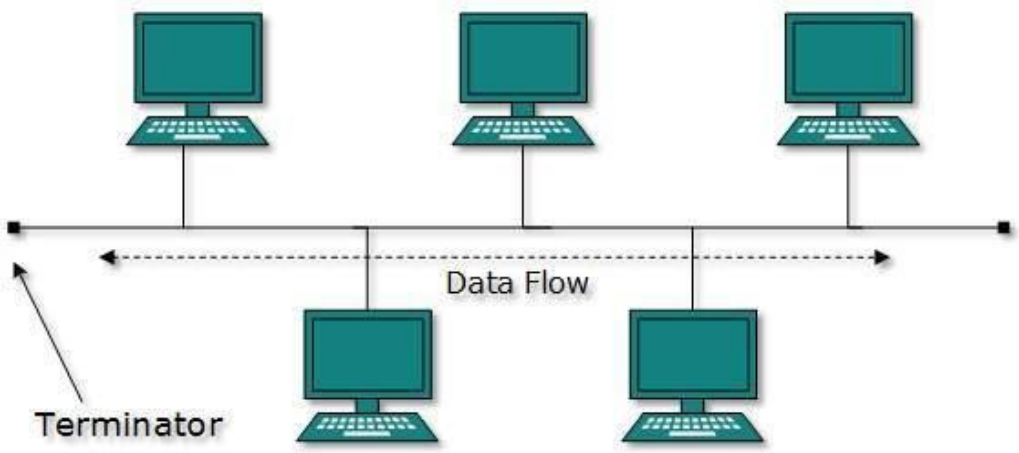
Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa.



If the hosts are connected point-to-point logically, then may have multIPle intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

Bus topology

In case of bus topology, all devices share single commuNICation line or cable. Bus topology may have problem while multIPle hosts sending data at the same time. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared commuNICation line can make all other devices stop functioning.

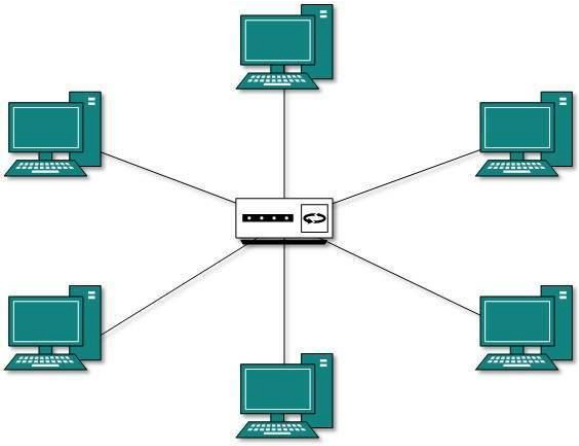


Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

Star topology

All hosts in star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

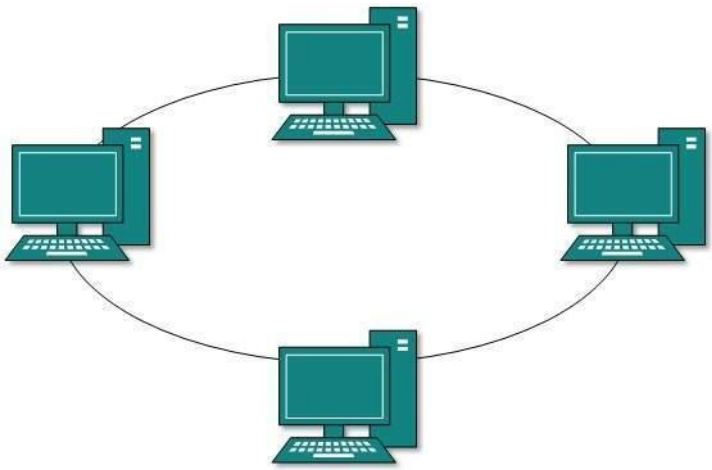
- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway



As in bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every commuNICation between hosts, takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

Ring topology: -

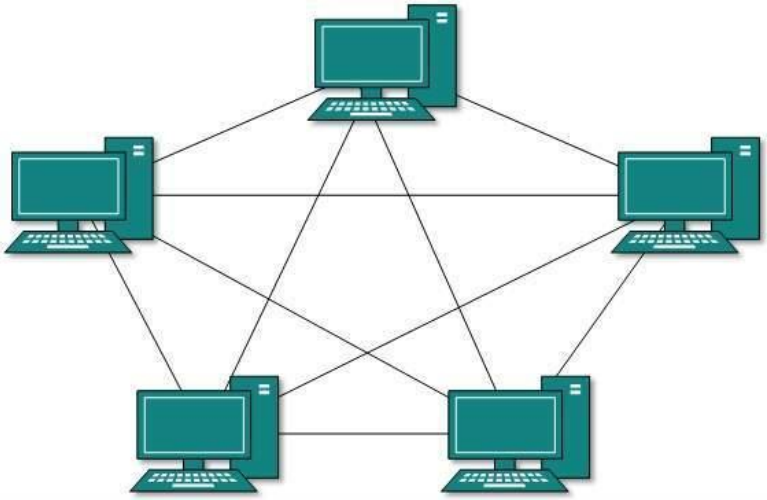
In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to commuNICate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.



Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

Mesh topology: -

In this type of topology, a host is connected to one or multIPle hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.



Hosts in mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

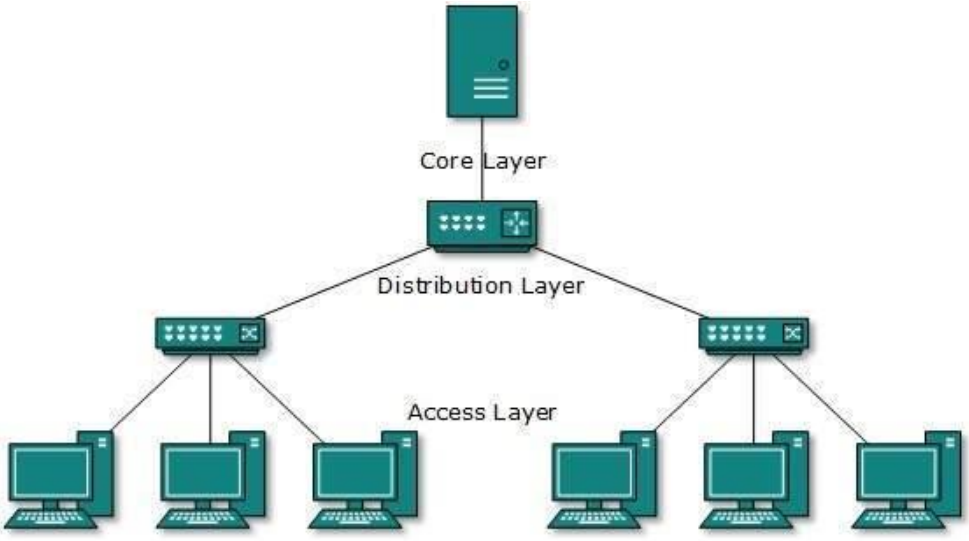
- **Full mesh**: all hosts have a point-to-point connection to every other host in the network. Thus, for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.

- **Partially mesh**: not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

Tree topology: -

Also known as hierarchical topology, this is the most common form of network topology in use presently. This topology imitates as extended star topology and inherits properties of bus topology.

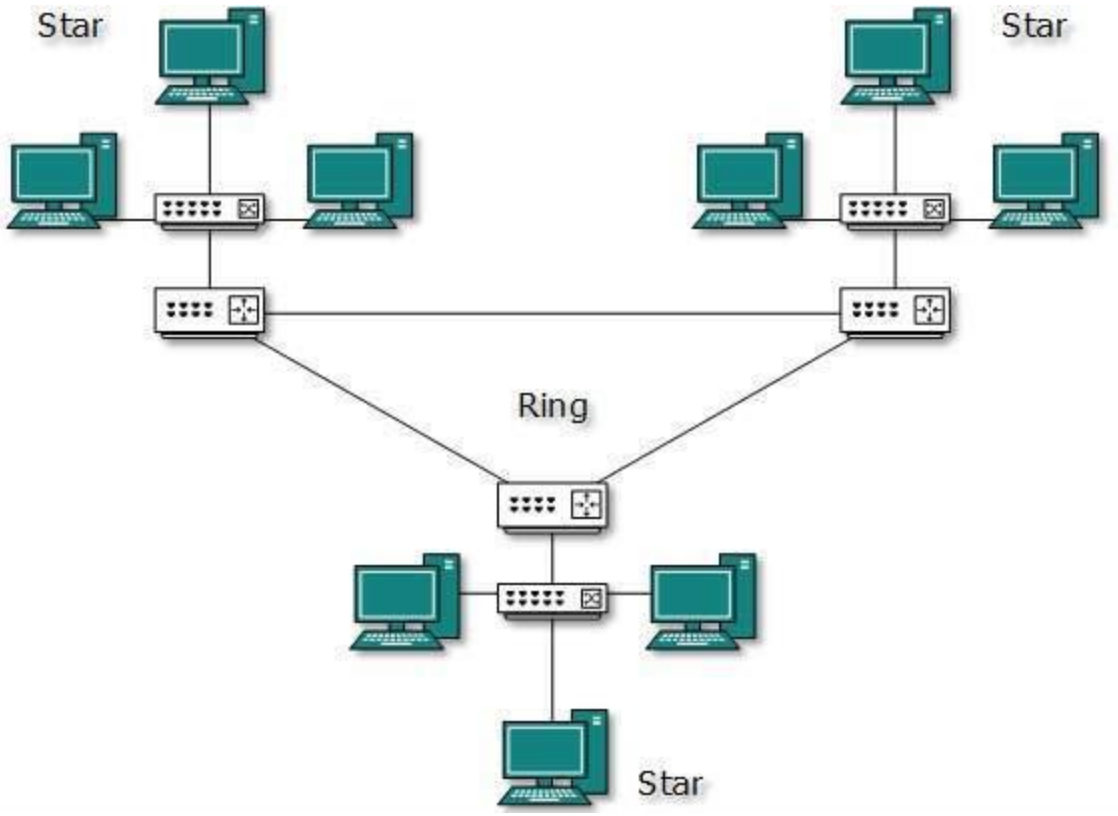
This topology divides the network in to multIPle levels/layers of network. Mainly in lans, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. Root of the tree from which all nodes fork.



All neighboring hosts have point-to-point connection between them. Similar to the bus topology, if the root goes down, then the entire network suffers even. Though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.

Hybrid topology: -

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.



The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of star, ring, bus, and daisy-chain topologies. Most wans are connected by means of dual-ring topology and networks connected to them are mostly star topology networks. Internet is the best example of largest hybrid topology.

What is network cabling?

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with lens. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded twisted pair (Utp) cable
- Shielded twisted pair (stp) cable
- Coaxial cable
- Fiber optic cable
- Cable installation guides
- Wireless lans

Unshielded twisted pair (Utp) cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (Utp) is the most popular and is generally the best option for school networks (see fig. 1).

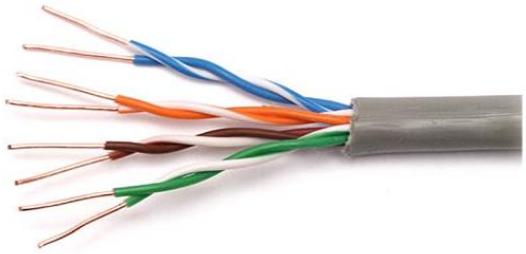


Fig.1. Unshielded twisted pair

The quality of Utp may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The eia/tie (electroNIC industry association/telecommuNICation industry association) has established standards of Utp and rated six categories of wire (additional categories are emerging).

Categories of unshielded twisted pair

UTP Categories - Copper Cable				
UTP Category	**Data Rate**	**Max. Length**	**Cable Type**	**Application**
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Firewall.cx

Unshielded twisted pair connector

The standard connector for unshielded twisted pair cabling is an rj-45 connector. This is a plastic connector that looks like a large telephone-style connector (see fig. 2). A slot allows the rj-45 to

be inserted only one way. Rj stands for registered jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

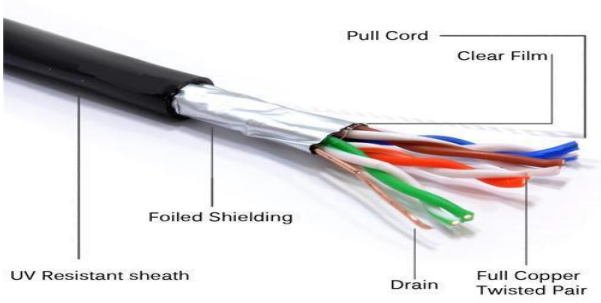
Fig. 2. Rj-45 connector

Shielded twisted pair (stp) cable

Although Utp cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).



Coaxial cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (see fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

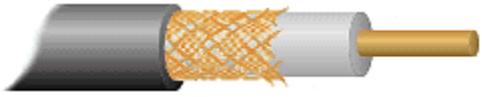


Fig. 3. Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinner. 10base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thick net. 10base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial cable connectors

The most common type of connector used with coaxial cables is the bay one-neill-concelman (bnc) connector (see fig. 4). Different types of adapters are available for bnc connectors, including a t-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the bnc connectors that crimp, rather screw, onto the cable.

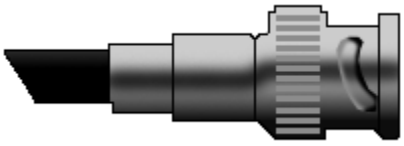


Fig. 4. Bnc connector

Fiber optic cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (see fig. 5). It transmits light rather than electroNIC signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens commuNICation possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10basef refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and Kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of Teflon or pvc.

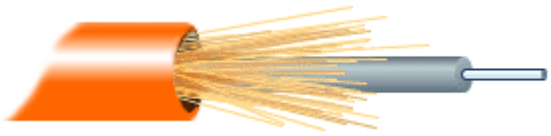


Fig. 5. Fiber optic cable

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

Specification	Cable type
10baset	Unshielded twisted pair
10base2	Thin coaxial
10base5	Thick coaxial
100baset	Unshielded twisted pair
100basefx	Fiber optic
100basebx	Single mode fiber
100basesx	Multimode fiber
1000baset	Unshielded twisted pair
1000basefx	Fiber optic
1000basebx	Single mode fiber
1000basesx	Multimode fiber

Installing cable - some guidelines

When running cable, it is best to follow a few simple rules:

- use more cable than you need. Leave plenty of slack.

- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

Wireless LANs

More and more networks are operating without cables, in the wireless mode. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations, servers, or hubs. Each workstation and file server on a wireless network have some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers, portable devices, or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network. Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

5. Conclusion: - From the above experiment we are able to know about what is topology and what are the different type of topology. We are also able to knowabout different type of cable like fiber optic cable, twisted pair cable, different type of twisted pair of cable, coaxial cable

6. Safety and precautions

1. **Remove your watch and jewelry and secure loose clothing.**
2. **Turn off the power and unplug equIPment before performing service.**
3. **Cover sharp edge inside the computer case with tape.**

4. **Never open a power supply or a CRT monitor.**
5. **Do not touch areas in printers that are hot or that use high voltage.**

7.Review of questions

1. What is topology?
2. What are different types oftopologies?
3. What iscabling?
4. What are different types ofcabling?
5. Where they are used?
6. Give example of coaxial, ofc, Utp and stp.

Experiment No – 2

1. Context

1.1 **Subject: -** computer network

1.2 Expt: - 2

1.3 Topic: - various type of connector.

1.4 **Sub-topic: -** networking

1.5 **Title of the experiment: -** recognition and use of various type of connectors rj-45, rj-11, bnc and scst.

1.6 **Environment/location: -** computer lab.

2. **Aim of the experiment:** recognition and use of various types of connectors rj-45, rj-11, bnc and scst.

3. **Objective of the experiment: -**

On completion of the experiment the students will able to:

1. **What is RJ?**
2. **Different type of RJ.**
3. **What is BNC connector and use**
4. **SCST connector.**

4.Procedure: -

An "**RJ connector**" in a computer network refers to a "Registered Jack" connector, which is a standardized physical interface used to connect data and telecommunication equipment, most commonly recognized as the 8-pin RJ45 connector used for Ethernet cables, allowing devices like computers and routers to communicate on a network; "RJ" stands for "Registered Jack" and the number "45" signifies the specific connector type within the standard.

Types of RJ Connectors:

1. RJ11 Connector:

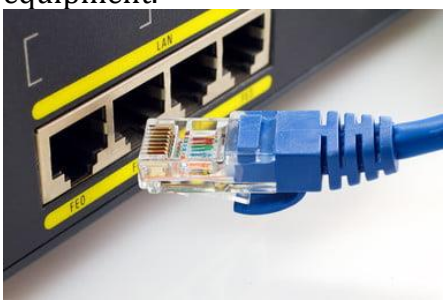
It is an abbreviation for Registered Jack11, which has a four-wire or six-wire telephone-type connection for connecting telephones to wall plates.
It does, however, accommodate up to six wires; most older wired telephone lines connect to ISPs through twisted-pair connections with four wires.

- **Use**: Connects telephone lines for voice and DSL broadband services.
- **Application**: Used in landline telephones and ADSL modems.
- Example: Connecting a telephone to a wall socket for voice communication.

2. RJ45 Connector:

It is a common form of registered jack connector found in Ethernet cables and network equipment. It is comparable to a telephone jack or connection in that it allows data to be shared via a local area network.
RJ45 cables or Ethernet cables are wider than telephone jacks or RJ11, 14, 21, and 25. It is used in the star topology of the Ethernet network to link shielded twisted pair (STP) and unshielded twisted pair (UTP) cabling.

RJ45 connections are typically 8P8C modular connectors with separate twisted pairs for connecting computer and telephone lines, wall plates, patch panels, and other networking equipment.



- **Use**: Connects Ethernet cables (CAT5, CAT6, CAT7) in wired networks.
- **Application**: Used in LANs, office networks, and home networking.
- **Example**: Connecting a computer to a router or switch using an Ethernet cable.

Bayonet neill concelman (bnc) connector

The **bnc connector** (acronym of "bayonet neill–concelman") is a miniature quick connect/disconnect radio frequency connector used for coaxial cable.

Interface specification

The interface specifications for the bnc and many other connectors are referenced in mil-std-348. it features two bayonet lugs on the female connector; mating is fully achieved with a quarter turn of the coupling nut. Bnc connectors are used with miniature-to-subminiature coaxial cable in radio, television, and other radio-frequency electroNIC equIPment, test instruments, and video signals. The bnc was commonly used for early computer networks, including arc net, the IBM pc network, and the 10base2 variant of Ethernet. Bnc connectors are made to match the characteristic impedance of cable at either 50 ohms or 75 ohms. They are usually applied for frequencies below 4 ghz and voltages below 500 volts.

 Use: Used with coaxial cables for networking and video applications.

 Application: Used in CCTV systems, old Ethernet networks (10BASE2), and radio frequency (RF) applications.

 Example: Connecting a coaxial cable to a CCTV camera or RF device.

Fiber Optic Connectors

Fiber optic connectors play a crucial role in the world of telecommunications and data networking, acting as the critical interface between fiber optic cables and the devices or networks they connect. These connectors are designed to align microscopic glass fibers perfectly to ensure that light signals can pass between cables or from cables to equipment with minimal loss.

SC Connectors

SC (Subscriber Connector) connectors, also known as square connectors or standard connectors, are widely used in fiber optic networks for their excellent performance and reliability.

 Use: Fiber optic connector for high-speed data transmission.

 Application: Used in telecommunications and high-speed internet connections.

 Example: Connecting fiber optic cables to network switches or internet service provider (ISP) equipment.

ST Connectors

ST (Straight Tip) connectors are another key player in the fiber optic connector arena, renowned for their reliability and durability. They were one of the first connector types widely implemented in fiber optic networking.

 Use: Fiber optic connector used for high-speed data transmission.
 Application: Used in networking and telecommunications.

 Example: Connecting fiber optic cables in industrial and military networks.

5.Conclusion: - From the aboveexperiment we are able to know about different type of connector like RJ45, RJ11 and BNC connector.How to use them in different place. We also know about the color combination of RJ45.

6. Safety and precautions

1. **Remove your watch and jewelry and secure loose clothing.**
2. **Turn off the power and unplug equIPment before performing service.**
3. **Cover sharp edge inside the computer case with tape.**
4. **Never open a power supply or a CRT monitors.**
5. **Do not touch areas in printers that are hot or that use high voltage.**

7. Review of questions.

1. What is RJ?
2. Different type of rj?
3. What is the use of rj 45?
4. What is the use of rj 11?
5. What is bnc?
6. What is the use of bnc?

Experiment No – 3

1. **Context**
   - **1.1 Subject: - computer network**
   - **1.2 Expt: - 3**
   - **1.3 Topic: - cross cable and straight cable.**
   - **1.4 Sub-topic: - networking**
   - **1.5 Title of the experiment: - Making of cross cable and straight cable.**
   - **1.6 Environment/location: - computer lab**
2. **Aim of the experiment:** making of cross cable and straight cable.
3. **Equipment's Required** (components): rj-45 connector, clamping tool, twisted pair cable.
4. **Objective of the experiment: -**

On completion of the experiment the students are able to:

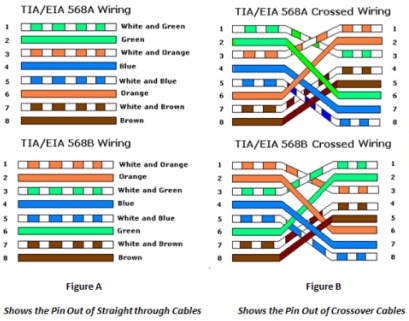
They got to know how to make cross cable and straight cable.

5. Procedure:

1. Start by strIPping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not NICk or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for NICks or cuts. If there are any, just whack the whole end off, and start over.

2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have a lot more than 1/2 of an inch of un-twisted wire.

3. You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.



6. Conclusion:

I use the cable made with the changed rj-45 connectors. The cable showed positive result. The new connectors had borders inside for each wire to guide them to and secure them to the proper pins. This cable was more stable and had no faulty connections, therefore it was a success.

7. Safety and precautions

1. **Remove your watch and jewelry and secure loose clothing.**
2. **Turn off the power and unplug equIPment before performing service.**
3. **Cover sharp edge inside the computer case with tape.**

4. **Never open a power supply or a CRT monitors.**
5. **Do not touch areas in printers that are hot or that use high voltage.**

8. Review of questions.

1. What is cross cable?

2. What is straight cable?

3. What is color code for connecting?

4. What is clamping tool?

Experiment No– 4

1. **Context: -**
   - **1.1 Subject: - computer network**
   - **1.2 Experiment: - 4**
   - **1.3 Topic: - configure network interface card**
   - **1.4 Sub topic: - Networking**
   - **1.5 Title of the experiment: - install and configure network interface card in work station.**
   - **1.6 Environment/location: - computer lab.**
2. **Aim of the experiment**: install and configure network interface card in work station.
3. **Equipments required:**

- NIC card
- Screwdriver
- Ethernet wire

- Installation software procedure

4. **Procedure: -**

NIC card installation

Step 1: unplug the pc from its electrical source, and remove all cords.

Step 2: open the case of the CPU with a screwdriver. Be careful of sharp metal edges. If the case doesn't open easily, check your operator's manual. There may be a release button that will open the case after the screws are undone.

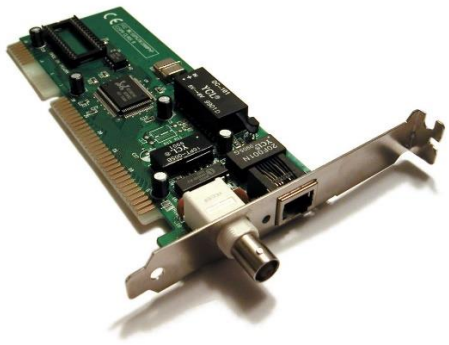
Step 3: lay the cape on its side. Locate the NIC slot. Align the NIC with the rj45 jack facing the outside of the case. Firmly seat the card into the slot. You may have to rock it gently to get it to fit. The gold contacts should not be visible, and the NIC card should be level.

Step 4: secure the mounting bracket with screws. They should come with the NIC card.

Step 5: replace the cover. Securely reattach all cords.

Step 6: connect the rj45 connection to the internet modem using the Ethernet wire. Not all NIC cards come with an Ethernet wire. Sometimes you will need to purchase the Ethernet wire separately.

Step 7: reboot the computer, and install the software that comes with the NIC card. This will install the necessary drivers. There will be prompts as the hardware installs. Simply follow the directions.



Network connection installation

Step 1: open the control panel. Go to start, then click control panel. Click network to open the network control panel.

Step 2: choose TCP/IP. It is probably loaded into your system as a protocol. If not, add it by following the prompts. After verifying the computer has TCP/IP protocol, click TCP/IP one time. Then click properties.

Step 3: pick both obtain an IP address automatically and the obtain DNS server address automatically. Then click the advanced button.

Step 4: select the DNS tab in the advanced TCP/IP settings window. Uncheck the box for register this connection's addresses in DNS. It is toward the bottom of the screen.

Step 5: click ok to close all the open windows. Restart your computer if you are asked to do so.

Manually configuring a network card for TCP/IP in windows xp

•click start, click control panel, click network and internet connections, and then click network connections.

• right-click the network connection that you want to change, and then click properties.

•on the general tab, double-click internet protocol TCP/IP in the "this connection uses the following items" list, and then click properties.

•on the general tab, click use the following IP address. Configure the entries as follows:

•IP address: the IP address you chose for this client (for example, 192.168.0.165).

•subnet mask: 255.255.255.0

•default gateway: 192.168.0.1 note: your router is almost always your gateway

•click use the following DNS server addresses, and then type 192.168.0.1 in the preferred DNS server box. Note: you may need to use your isp's DNS server address (es) here if your gateway device does not relay DNS lookups

•click ok.

6. Conclusion: By following the above experiment, we can install and configure network interface card in workstation.

7. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.

2. Turn off the power and unplug equIPment before performing service.

3. Cover sharp edge inside the computer case with tape.

4. Never open a power supply or a CRT monitors.

5. Do not touch areas in printers that are hot or that use high voltage.

8.review of questions.

1. What is NIC card?

2. Why the NIC card is used?

3. What is the Ethernet wire?

4. How it is used to connect the internet?

EXPERIMENT: - 5

1. Context

1.1 Subject: - computer network

1.2 Experiment: - 5

1.3 Topic: - IP address and class of computer

1.4 Sub-Topic: - Networking

1.5 **Title of the experiment: -**identifying IP address of a workstation and the class of the address and configure the IP information

2. AIM OF THE EXPERIMENT: -

identifying IP address of a workstation and the class of the address and configure the IP information.

3. Objective of the experiment: -

On the completion of the experiment the students will able to:

1. What is IP address?
2. How to find the IP address of a computer?
3. How to configure the IP address of a computer?

4. PROCEDURE: -

An IP Address or **I**nternet **P**rotocol address is a commutation configuration that is set up on a workstation that enables the

workstation to see/be seen by others. It consists of 4 numbers (ranging from 0 - 255) separated by periods called octets. An example is 192.168.0.10.

To find your workstation's IP address you can perform the following actions:

1. Click the Start button, then Run
2. In the text box type **cmd** and press the Enter key
3. Type **IPconfig**
4. Under Local Area Connection, to the right of the row labeled “IP Address” you will find the computer's IP Address
5.

Looking at the first octet of an IP address, you can identify the class of that address: Class A =1-126 Class B =128 -191 Class C =192 -223 Class D =224 –239 Class E =240 –254 Looking at the first octet to determine the class: 64.192.29.2 = Class A =64.0.0.0 172.16.32.4 = Class B =172.16.0.0 208.16.14.1 = Class C =208.16.14.0

Set a static IP address in Windows 7, 8, and 10:

1. Click **Start Menu** > **Control Panel** > **Network and Sharing Centre** or **Network and Internet > Network and Sharing Centre.**
2. Click **Change adapter settings**.
3. Right-click on **Wi-Fi** or **Local Area Connection.**
4. Click **Properties**.
5. Select **Internet Protocol Version 4 (TCP/IPv4)**.
6. Click **Properties**.
7. Select **Use the following IP address**.
8. Enter the **IP address**, **Subnet mask**, **Default gateway**, and **DNS server**.
9. Click **OK**.

Your computer displays a static IP address

5. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.

2. Turn off the power and unplug equipment before performing service.

3. Cover sharp edge inside the computer case with tape.

4. Never open a power supply or a CRT monitors.

5. Do not touch areas in printers that are hot or that use high voltage.

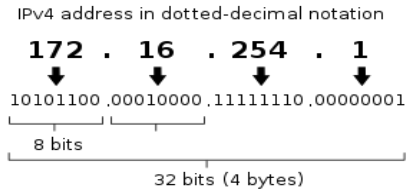
6. Review of questions.

1. What is IP address?

2. What are the different classes of IP address?

3. How to find the IP address of a computer?

4. How to configure the IP address of a computer?



EXPERIMENT No: - 6

1. **Context**
   - **1.1 Subject: -** computer network
   - **1.2 Experiment: -** 6
   - **1.3 Topic: -** user account in windows and LINUX
   - **1.4 Sub-Topic: -** Networking
   - **1.5 Title of the experiment: -** managing user accounts in windows and LINUX
   - **1.6 Environment/location: - computer lab**

2. AIM OF THE EXPERIMENT: - Managing user accounts in windows and LINUX.

3. Objective of the experiment: -

On the completion of the experiment students are able to know: -

1. **What is user account?**
2. **How to manage user account in windows and linux?**

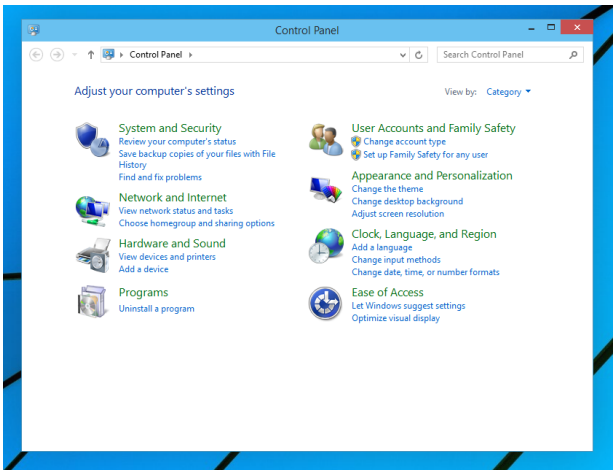
4. PROCEDURE: -

LINUX: -

1. To add a user account, use the add user command. See the add user command page for additional information about this command.
2. To remove a user account, use the del user command. See the del user command page for additional information about this command.
3. To change the user settings, such as group membership, default login shell, and home directory, use the user mod command. See the user mod command page for additional information about this command.

WINDOWS 10: -

1. Open the Control Panel.
2. Select User Accounts.
3. In the User Accounts window, you can add or remove user accounts. You can also select a user account and make any necessary changes, including changing the user account name.



5. Conclusion: - From the above experiment we got to know the use of control panel in windows and Linux.

6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.

2. Turn off the power and unplug equipment before performing service.

3. Cover sharp edge inside the computer case with tape.

4. Never open a power supply or a CRT monitors.

5. Do not touch areas in printers that are hot or that use high voltage.

7. Review of questions.

1. What is user account?

2. How can we add the user account in windows?

3. How can we delete the user account in windows?

4. How can we add the user account in LINUX?

5. How can we delete the user account in LINUX?

EXPERIMENT No: - 7

1. Context

- **1.1 Subject: -** computer network
- **1.2 Experiment: -** 7
- **1.3 Topic: -** hardware resource
- **1.4 Sub-Topic: - Networking**
- **1.5 Title of the experiment: -** sharing of hardware resources in the network
- **1.6 Environment/location: - computer lab**

2. AIM OF THE EXPERIMENT: -Sharing of hardware resources in the network.

3. Objective of the Experiment: -

On completion of the experiment students are able to: -

1. **What is shared resources**
2. **How does networking help share hardware resource**

4. PROCEDURE: -

Definition - What does Shared Resources mean?

Shared resources, also known as network resources, refer to computer data, information, or hardware devices that can be easily accessed from a remote computer through a local area network (LAN) or enterprise internet. Successful shared resource access allows users to operate as if the shared resource were on their own computer. The most frequently used shared network environment objects are files, data, and multimedia and hardware resources like printers, fax machines and scanners.

How does networking help share hardware resources?

We can share Hardware of computers via networking. When we are connected to a same LAN network then we can use the same printer to print anything we want. Resources provided include data files, printers, software, or any other items used by clients on the network.

5. Conclusions: - From the above experiment we are able to learn what shared hardware is and how network helps in this process.

6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.

2. Turn off the power and unplug equipment before performing service.

3. Cover sharp edge inside the computer case with tape.

4. Never open a power supply or a CRT monitors.

5. Do not touch areas in printers that are hot or that use high voltage.

7. Review of questions.

1. What is NIC card?

2. Why the NIC card is used?

3. What is the Ethernet wire?

4. How it is used to connect the internet?

Experiment No: - 8

1. Context

1.1 Subject: - Computer network

1.2 Experiment: - 8

1.3 Topic: -

1.4 Sub-Topic: - networking

1.5 Title of the experiment: -use of netstat and its options

1.6 Environment/location: - Computer lab

2. Aim of the experiment: -Use of netstat and its options.

3. Objective of the experiment: -

On completion of this experiment students will be able to: -

1. Know what netstat is.
2. How to use netstat.
3. What are the different options of netstat.

4. Procedure: -

Netstat — derived from the words *network* and *statistics* — is a program that's controlled via commands issued in the command line. It delivers basic statistics on all network activities and informs users on which **portsand addresses** the corresponding connections (TCP, UDP) are running and which ports are open for tasks. In 1983, netstat was first implemented into

the **Unix** derivative BSD (Berkley Software Distribution), whose version 4.2 supported the first internet protocol family, TCP/IP

How to use netstat?

In Windows operating systems, you can use the netstat services via the command line (cmd.exe). You can find them in the start menu under “All Programs” -> “Accessories” -> “Command Prompt”. Alternatively, you can search directly for “Command Prompt” in the **start menu’s search field** or start the command line via “Run” (Windows key + press “R” and enter “cmd”). The syntax of the netstat commands follows the following pattern:

```
netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p Protocol] [-r] [-s] [-t] [-x] [-y] [Interval]
```

The combination of the individual options works by stringing the individual parameters together, each separated by a space:

```
netstat [-OPTION1] [-OPTION2] [-OPTION3] …
```

The parameters are typically preceded by a **hyphen (-)**, but if you want to combine several options, you only have to place this hyphen in front of the first element. Instead of the variant shown above, you can also link different parameters as follows:

```
netstat [-OPTION1][OPTION2][OPTION3] …
```

netstat commands for Windows

[OPTION]	Command	DescrIPtion
	netstat	Standard listing of all active connections
-a	netstat -a	Displays all active ports
-b	netstat -b	Displays the executable file of a connection or listening port (requires administrator rights)
-e	netstat -e	Shows statistics about your network connection (received and sent data packets, etc.)
-f	netstat -f	Displays the fully qualified domain name (FQDN) of remote addresses
-i	netstat -i	Brings up the netstat overview menu

-n	netstat -n	Numerical display of addresses and port numbers
-o	netstat -o	Displays the process identifier (PID) associated with each displayed connection
-p Protokoll	netstat -p TCP	Displays the connections for the specified protocol, in this case TCP (also possible: UDP, TCPv6, or UDPv6)
-q	netstat -q	Lists all connections, all listening TCP ports, and all open TCP ports that are not listening
-r	netstat -r	Displays the IP routing table
-s	netstat -s	Retrieves statistics about the important network protocols such as TCP, IP, or UDP
-t	netstat -t	Shows the download status (TCP download to relieve the main processor) of active connections
-x	netstat -x	Informs about all connections, listeners, and shared endpoints for NetworkDirect
-y	netstat -y	Displays which connection templates were used for the active TCP connections
Interval	netstat -p 10	Displays the respective statistics again after a selected number of seconds (here 10); can be combined as required (here with –p), [CTRL] + [C] ends the interval display

5. **Conclusion: -** From the above experiment we are able to learn how to use netstats and different function of it.

6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.

2. Turn off the power and unplug equipment before performing service.

3. Cover sharp edge inside the computer case with tape.

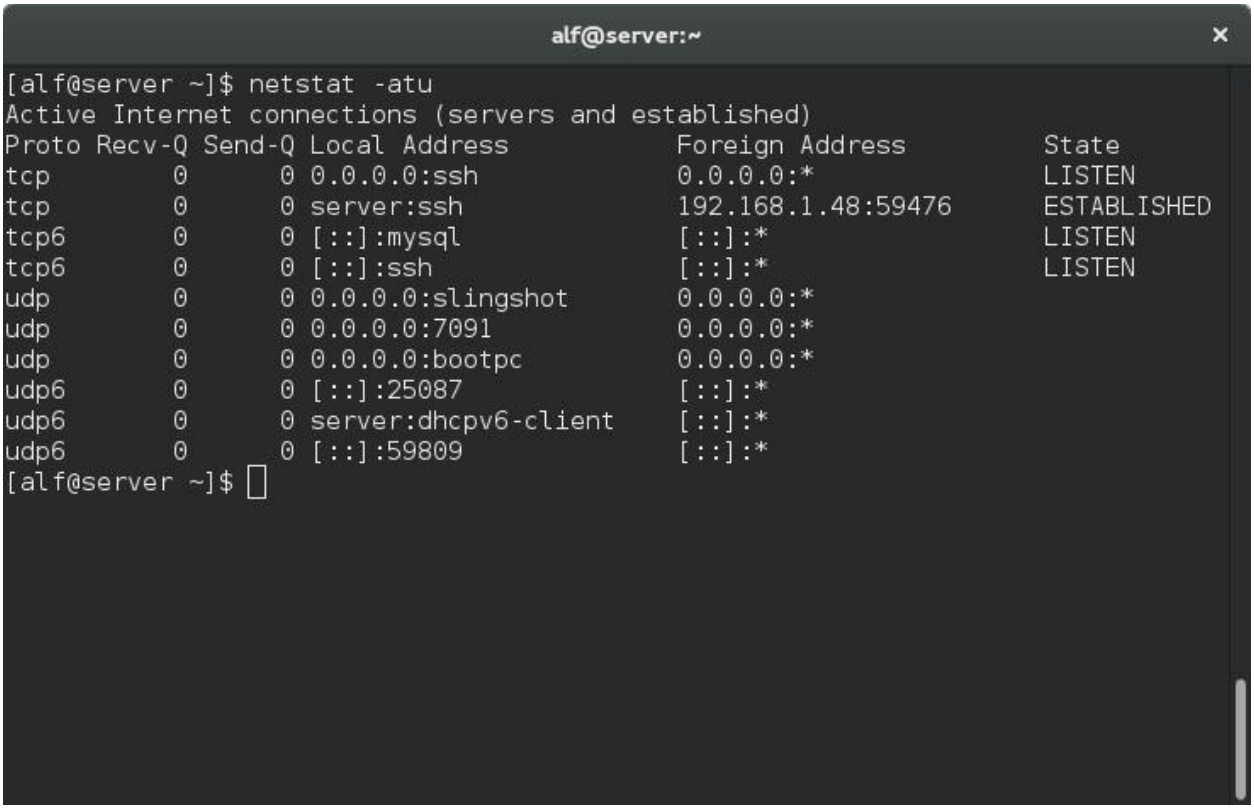
4. Never open a power supply or a CRT monitors.

5. Do not touch areas in printers that are hot or that use high voltage.

7. Review of questions.

1. What is netstat ?

2. How to use netstat?
3. What are the different option of netstat ?



Experiment No: - 9

1. **Context**
   - **1.1 Subject: -** Computer Network
   - **1.2 Experiment: -** 9
   - **1.3 Topic: -** Troubleshooting using ping, IP config
   - **1.4 Sub-Topic: -** networking
   - **1.5 Title of the experiment: -** Connectivity troubleshooting using ping, IPconfig.
   - **1.6 Environment/location: -** Computer lab
2. **Aim of the experiment: -** Connectivity troubleshooting using ping, IPconfig.
3. **Objective of the experiment: -**

   On completion of the experiment the students will able to: -

4. What are the connectivity problems?
5. How to find that the computer is connected to a network?
6. How to find the IP address using command prompt?

4. Procedure: -

IP config and ping can be used to analyze, test, troubleshoot, and configure IPv4 and IPv6 connections. Before moving to more advanced TCP/IP commands, it is important to master these commands by learning what each of the commands and their options do, as well as why you would use those options in a real-world scenario.

The following steps show how you can troubleshoot the problem with ping IPconfig:

You don't have to use the same order shown in these steps. You can use any order desired as long as you are able to identify the problem.

1. Enter ping local host or ping 127.0.0.1.
   By pinging the local host or the loopback address (127.0.0.1), you can verify that TCP/IP is functioning correctly on Joe's local system. You should get four successful replies. You can also use ping -4 local host or ping -6 local host to check IPv4 or IPv6, respectively.
2. Enter ping 192.168.1.5.
   This checks connectivity through a switch (or a hub) but not the router. You

can also ping any other computer with the same network ID. If these pings fail, the problem is on this side of the router.

3. Enter ping 192.168.1.1.
   This pings the default gateway. Remember, you can use IPconfig to determine the IP address of the default gateway.
   You may choose to do step 3 first to reduce troubleshooting steps. If it fails, the problem is on Joe's side of the router (or the router itself).
4. Enter ping 192.168.3.1.
   This is the far side of the router. If successful, it indicates the router is successfully routing traffic. If it fails but you can ping 192.168.1.1 (the default gateway for 192.168.1.1), it indicates the router is causing the connectivity problem and may be misconfigured or faulty.
5. Enter ping 192.168.3.10.
   This pings the IP address of the server named FS1. If this succeeds, it indicates that the server is up and operational. Remember, though, if it fails, it could be because the server is blocking ICMP traffic.
6. Enter ping fs1.The first step of the ping should be to resolve the name fs1 to the IP address of 192.168.3.10.

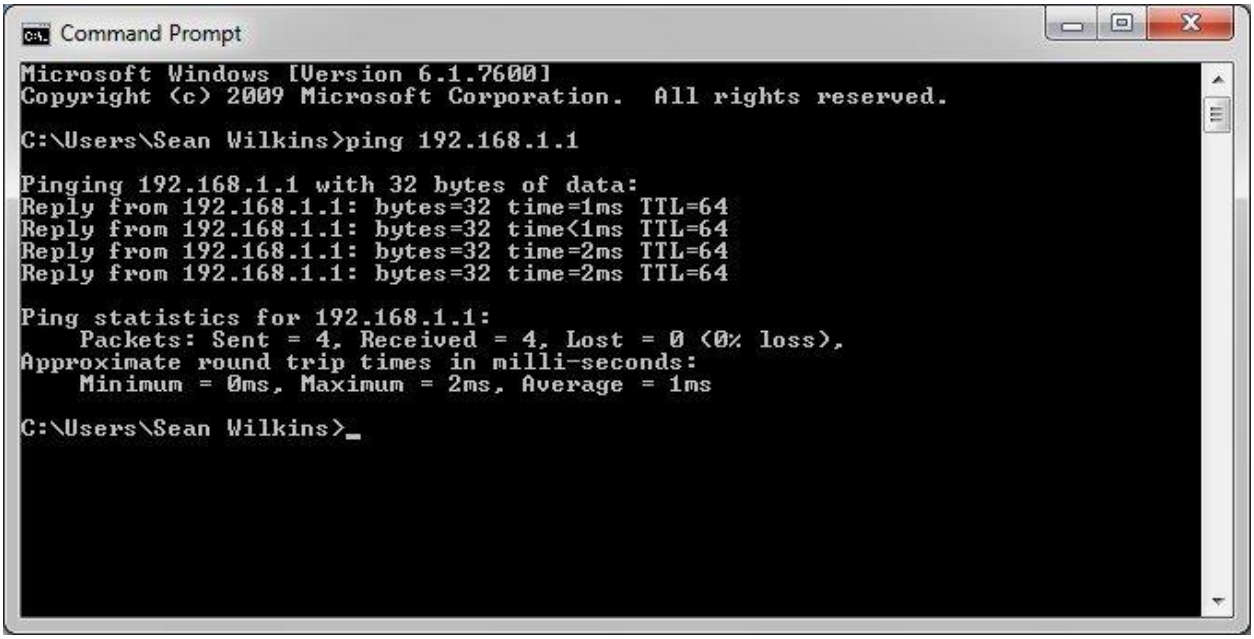
5. Conclusion: - From the above experiment we are now able to troubleshoot about the network connection problems in our system.

6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.
2. Turn off the power and unplug equipment before performing service.
3. Cover sharp edge inside the computer case with tape.
4. Never open a power supply or a CRT monitors.
5. Do not touch areas in printers that are hot or that use high voltage.

7. Review of questions.

1. What is ping?
2. Why ping is used?
3. What is IPconfig?
4. Why IPconfig is used?


Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Sean Wilkins>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 1ms
C:\Users\Sean Wilkins>_

Experiment No: - 10

1. **Context**
   - 1.1 **Subject: -** Computer Network
   - **1.2 Experiment: -** 10
   - **1.3 Topic: -** Network OS
   - **1.4 Sub-Topic: -** Networking
   - 1.5 **Title of the experiment: -** Installation of the network OS
   - **1.6 Environment/location**: - computer lab
2. **Aim of the experiment: -** Installation of network operating system (NOS)
3. **Objective of the experiment: -**
   On completion of the experiment student are able to: -
   Install network operating system
4. **Procedure: -**

A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations, personal computers and, in some instances, older terminals that are connected on a local area network (LAN). The software behind a NOS allows multiple devices within a network to communicate and share resources with each other. The composition of hardware that typically uses NOS includes a number of personal computers, a printer, a server and file server with a local network that connects them together. The role of the NOS is to then provide basic network services and features that support multiple input requests simultaneously in a multiuser environment.

Due to earlier versions of basic operating systems not being designed for network use, network operating systems emerged as a solution for single-user computers.

Types of network operating systems

There are two basic types of network operating systems, the peer-to-peer NOS and the client/server NOS:

1. Peer-to-peer network operating systems allow users to share network resources saved in a common, accessible network location. In this architecture, all devices are treated equally in terms of functionality. Peer-to-peer usually works best for small to medium LANs and is cheaper to set up.
2. Client/server network operating systems provide users with access to resources through a server. In this architecture, all functions and applications are unified under one file server that can be used to execute individual client actions regardless of physical location. Client/server tends to be most expensive to implement and requires a large amount of technical maintenance. An advantage to the client/server model is that the network is controlled centrally, makes changes or additions to technology easier to incorporate.

Common features of network operating systems

Features of network operating systems are typically associated with user administration, system maintenance and resource management functionality. This includes:

- Basic support for operating systems like protocol and processor support, hardware detection and multiprocessing.
- Printer and application sharing.
- Common file system and database sharing.
- Network security capabilities such as user authentication and access control.
- Directory
- Backup and web services.
- Internetworking.

Examples of network operating systems

True network operating systems are categorized as software that enhances the functionality of operating systems by providing added network features. A few examples of these network operating systems and their service providers are:

- Artisoft's LANtastic- This is a simple, user-friendly NOS that supports most PC operating systems.
- Banyan's VINES- This uses client-server architecture to request specific functions and services.
- Novell's NetWare- This was the first network operating system to be released and is designed based on XNS protocol architecture.
- Microsoft's LAN Manager- This operates as a server application and was developed to run under the Microsoft OS. Now, most of the functionality of LAN Manager is included in the Windows OS itself.

In addition, some multi-purpose operating systems, such as Windows NT and Digital's OpenVMS come with capabilities that enable them to be described as a network operating system. Further, the most popular operating systems like Windows, UNIX, Linux and Mac include built-in networking functions that may not require additional network services.

5. **Conclusion: -** From the above experiment we are able to know what the Network OS is and how to install and use it.

6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.
2. Turn off the power and unplug equipment before performing service.
3. Cover sharp edge inside the computer case with tape.
4. Never open a power supply or a CRT monitors.

5. Do not touch areas in printers that are hot or that use high voltage.

7. Review of questions.

1. What is network operating system?
2. How to install network operating system?
3. How to use network operating system?

Experiment No: - 11

1. **Context**
   - **1.1 Subject: -** Computer network
   - **1.2 Experiment: -** 11
   - **1.3 Topic: -** create a network
   - **1.4 Sub-Topic: -** networking
   - **1.5 Title of the experiment: -**Create a network of at least 6 computers.
   - **1.6 Environment/location: -** Computer lab
2. **Aim of the experiment: -** Create a network of at least 6 computers.
3. **Objective of the experiment: -**

   On the completion of the experiment student will able to: -

   Create a network of at least 6 computers.
4. **Apparatus required: -** broadband internet service provider, Ethernet card, 10-port router, Ethernet cable.
5. **Procedure: -**

   Are there individuals in your home who want to have Internet access but they can't because there is only one computer in your house that is Internet-ready? Because there is only one Internet-ready computer, everyone has to wait their turn to use it. This can quickly become a headache. Setting up a home network could be the answer to your problems.

Step 1

Establish broadband Internet service with an Internet service provider of your choice. Your Internet service provider will send you a broadband modem if you don't already have one.

Step 2

Check to ensure that your primary computer has an Ethernet card installed. If it doesn't, purchase one and install it.

Step 3

Purchase a 10-port router. Netgear, D-Link and Linksys are three companies from which you can purchase 10-port routers. Procure nine additional Ethernet (Cat 5) cables. If the router does not come with the extra cables, purchase the cables from an electroNICs or computer store.

Step 4

Power on your computer. Connect one end of the Ethernet cable that came with your router into the router's WAN port. Connect the other end of the Ethernet cable into the modem port labelled "Internet," "WAN" or "WLAN." Turn off your computer.

Step 5

Connect another Ethernet cable from your modem's Ethernet port to the Ethernet port on the back of your computer. Power on your computer. Your Internet connection will be recognized.

Connect the remaining Ethernet cables to the Ethernet ports that are on the other computers that you desire to network. One end of the cables should be connected to the computers. The other end of the cables should be connected to a port that is on the back of the router. After you power off each of the computers and reboot them, the Internet connection will be recognized.

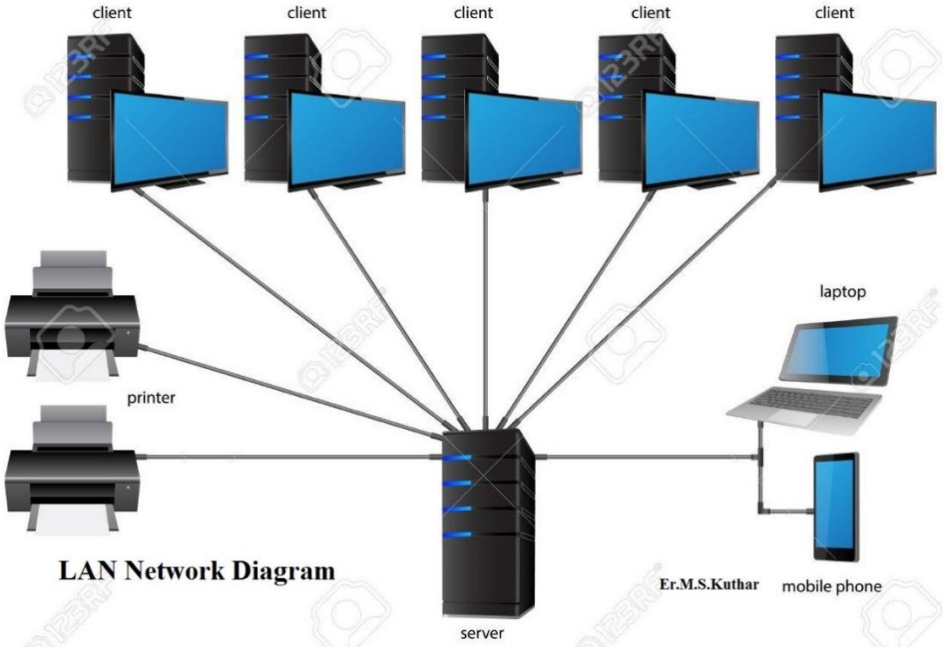
6. **Conclusion: -** From the above experiment we are able to create a network using 6 or more computers.

7. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.
2. Turn off the power and unplug equipment before performing service.
3. Cover sharp edge inside the computer case with tape.
4. Never open a power supply or a CRT monitors.
5. Do not touch areas in printers that are hot or that use high voltage.

8. Review of questions.

1. How to create network?
2. What are the apparatus required to create?
3. How to use network operating system?



LAN Network Diagram

Er.M.S.Kuthar

Experiment No: - 12

1. Context

1.1 **Subject: -** Computer network

1.2 Experiment: - 12

1.3 Topic: - layers of network

1.4 Sub-Topic: - networking

1.5 Title of the experiment: - Study of layers of network and configuring network operating system

1.6 Environment/location: - computer lab

2. Aim of the experiment: - Study of layers of network and configuring network operating system

3. Objective of the experiment: -

On the completion of the experiment students will able to: -

Know different layers of OS and how to use them.

4. Procedure: -

Who Developed the IOS Model?

The International Standards Organization (ISO) developed the Open Systems Interconnection (OSI) model. It divides network communication into seven layers. In this model, layers 1-4 are considered the lower layers, and mostly concern themselves with moving data around. Layers 5-7, called the upper layers, contain application-level data. Networks operate on one basic principle: "pass it on." Each layer takes care of a very specific job, and then passes the data onto the next layer.

The 7 Layers of the OSI Model

In the OSI model, control is passed from one layer to the next, starting at the application layer (Layer 7) in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. The OSI model takes the task of inter-networking and divides that up into what is referred to as a *vertical stack* that consists of the following 7 layers.

- Layer 7 - Application
- Layer 6 - Presentation
- Layer 5 - Session
- Layer 4 - Transport
- Layer 3 - Network

- Layer 2 - Data Link
- Layer 1 - Physical

Application (Layer 7)

OSI Model, Layer 7, supports application and end-user processes. CommuNICation partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

Layer 7 Application examples include WWW browsers, NFS, SNMP, Telnet, HTTP, FTP

Presentation (Layer 6)

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Layer 6 Presentation examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.

Session (Layer 5)

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Layer 5 Session examples include NFS, NetBios names, RPC, SQL.

Transport (Layer 4)

OSI Model, Layer 4, provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Layer 4 Transport examples include SPX, TCP, and UDP.

Network (Layer 3)

Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Layer 3 Network examples include AppleTalk DDP, IP, IPX.

Data Link (Layer 2)

At OSI Model, Layer 2, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Layer 2 Data Link examples include PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, Frame Relay.

Physical (Layer 1)

OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

Layer 1 Physical examples include Ethernet, FDDI, B8ZS, V.35, V.24, RJ45.x

5. **Conclusion: -** From the above experiment we got to know what is OSI model and different layers of OSI model.

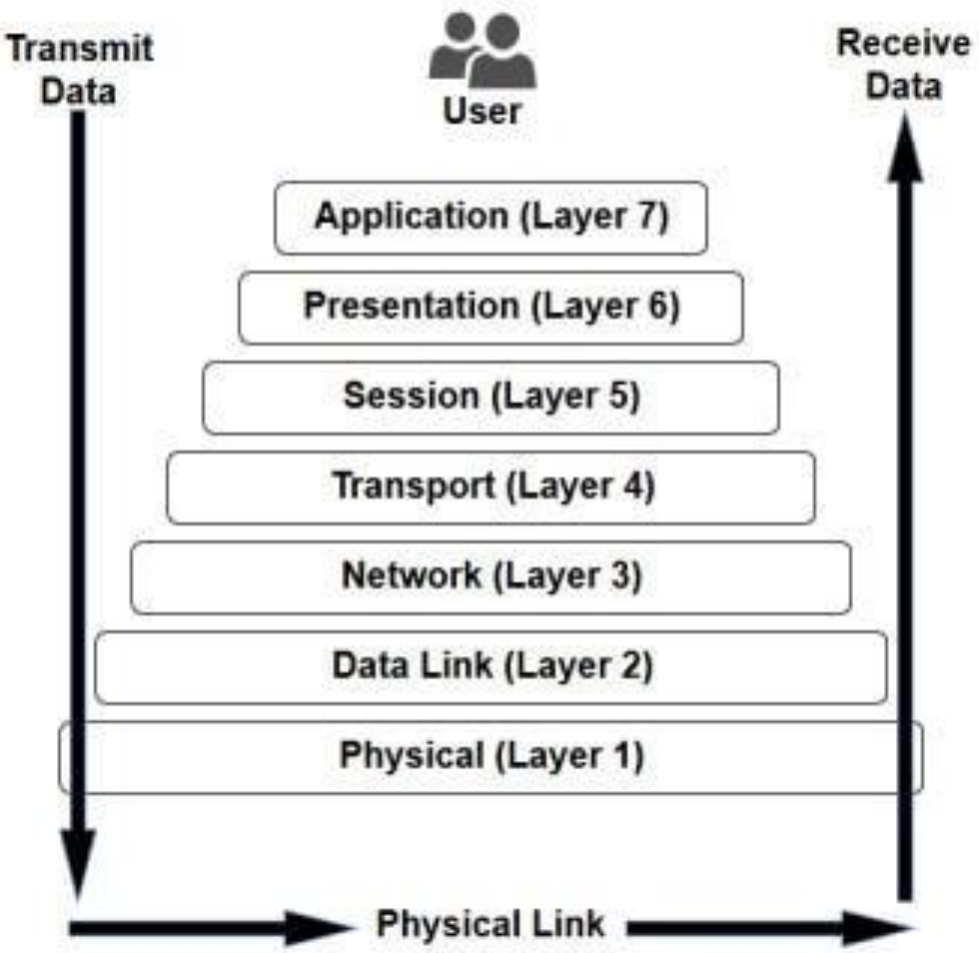
6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.
2. Turn off the power and unplug equipment before performing service.
3. Cover sharp edge inside the computer case with tape.
4. Never open a power supply or a CRT monitors.
5. Do not touch areas in printers that are hot or that use high voltage.

7. Review of questions:

1. What is OSI model?
2. Who developed OSI model?
3. What is the different layer of OSI model?
4. Explain the function of each layer.

The 7 Layers of OSI



Experiment No: - 13

1. Context

1.1 Subject: - computer network

1.2 Experiment: - 13

1.3 Topic: - routing and switching

1.4 Sub-Topic: - networking

1.5 Title of the experiment: - Study of routing and switching, configuring of switch and routers, troubleshooting of networks

1.6 Environment/location: - computer lab

2. Aim of the experiment: - Study of routing and switching, configuring of switch and routers, troubleshooting of networks

3. Objective of the experiment: -

On the completion of the experiment the students will able to: -

Know about routing and switching

4. Procedure: -

What is router?

A **router** is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.

What Is Routing?

Routing is the process of selecting a path for traffic in a network or between or across multIPle networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet. In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task.

What is switch?

A switch is used to network multiple computers together. Switches made for the consumer market are typically small, flat boxes with 4 to 8 Ethernet ports. These ports can connect to computers, cable or DSL modems, and other switches. High-end switches can have more than 50 ports and often are rack mounted. It is also called switching.

How to configure the switch: -

This is a step by step guide for configuring the switch.

STEP1: Connect to the device via console

Use a terminal emulation software such as Putty and connect to the console of the switch. You will get the initial command prompt "**Switch>**"

Type "**enable**" and hit enter. You will get into privileged EXEC mode ("**Switch#**")

Now, get into Global Configuration Mode:

Switch# configure terminal
Switch(config)#

Note: The switch will not ask you for a password when entering into Privileged EXEC mode (i.e after typing "enable") if it has the default factory configuration. See Step 3 below about setting up a password for the Privileged EXEC mode.

STEP2: Set up a hostname for the particular switch to distinguish it in the network

Switch(config)# hostname access-switch1
access-switch1(config)#

STEP3: Configure an administration password (enable secret password)

access-switch1(config)# enable secret *somestrongpass*

The password above will be used to enter into Privileged EXEC mode as described in Step 1 above.

STEP4: Configure a password for Telnet and Console access

It is a very good security practice to lock-down all access lines of a switch with a password. Although it is much better to configure an external AAA server (for centralized Authentication Authorization and Accounting), in this article we will just configure a password on each access line (VTY lines for Telnet and Console line):

access-switch1(config)# line vty 0 15
access-switch1(config-line)# password *strongtelnetpass*
access-switch1(config-line)# login
access-switch1(config-line)# exit
access-switch1(config)#

access-switch1(config)# line console 0
access-switch1(config-line)# password *strongconsolepass*
access-switch1(config-line)# login
access-switch1(config-line)# exit
access-switch1(config)#

STEP5: Define which IP addresses are allowed to access the switch via Telnet

access-switch1(config)# IP access-list standard TELNET-ACCESS
access-switch1(config-std-nacl)# permit 10.1.1.100
access-switch1(config-std-nacl)# permit 10.1.1.101
access-switch1(config-std-nacl)# exit

!Apply the access list to Telnet VTY Lines
access-switch1(config)# line vty 0 15
access-switch1(config-line)# access-class TELNET-ACCESS in
access-switch1(config-line)# exit
access-switch1(config)#

STEP6: Assign IP address to the switch for management

!Management IP is assigned to Vlan 1 by default
access-switch1(config)# interface vlan 1
access-switch1(config-if)# IP address 10.1.1.200 255.255.255.0
access-switch1(config-if)# exit
access-switch1(config)#

STEP7: Assign default gateway to the switch

access-switch1(config)# IP default-gateway 10.1.1.254

STEP8: Disable unneeded ports on the switch

! This step is optional but enhances security
! Assume that we have a 48-port switch and we don't need ports 25 to 48

access-switch1(config)# interface range fe 0/25-48
access-switch1(config-if-range)# shutdown
access-switch1(config-if-range)# exit
access-switch1(config)#

STEP9: Configure Layer2 VLANs and assign ports to the them

By default, all physical ports of the switch belong to the native VLAN1. One of the most important functions of an Ethernet switch is to segment the network into multIPle Layer2 VLANs (with each VLAN belonging to a different Layer3 subnet).

In order to do the above Layer2 segmentation you need to create additional VLANs from the default VLAN1 and then assign physical ports to these new vlans. Let's create two new VLANS (VLAN2 and VLAN3) and assign two ports to each one.

! First create the Layer2 VLANs on the switch

access-switch1(config)# vlan 2
access-switch1(config-vlan)# name TEACHERS
access-switch1(config-vlan)# exit

access-switch1(config)# vlan 3
access-switch1(config-vlan)# name STUDENTS
access-switch1(config-vlan)# exit

! Now assign the physical ports to each VLAN. Ports 1-2 are assigned to VLAN2 and ports 3-4 to VLAN3

access-switch1(config)# interface range fe 0/1-2
access-switch1(config-if-range)# switchport mode access
access-switch1(config-if-range)# switchport access vlan 2
access-switch1(config-if-range)# exit

access-switch1(config)# interface range fe 0/3-4
access-switch1(config-if-range)# switchport mode access
access-switch1(config-if-range)# switchport access vlan 3
access-switch1(config-if-range)# exit

STEP10: Save the configuration

access-switch1(config)# exit
access-switch1# wr

How to configure the router: -

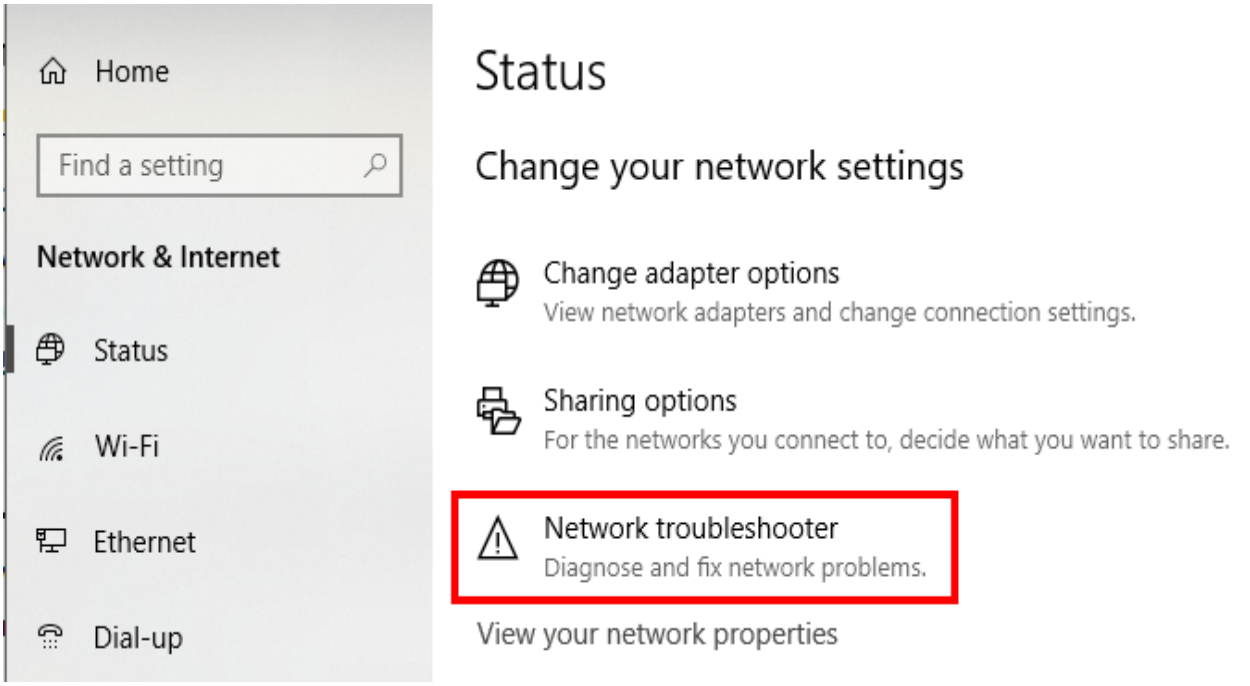
Step 1: Place your wireless **router**. ...
Step 2: **Configure** your wireless **router** gateway. ...
Step 3: Connect your gateway to your new **router**. ...
Step 4: Change your wireless **router's** admin password. ...
Step 5: Update the **router's** firmware. ...
Step 6: Establish a password for your Wi-Fi network. ...
Step 7: Enjoy your Wi-Fi network!

How to troubleshoot the networks

Follow these network troubleshooting tIPs and you'll be up and running in no time.

1. Check Your Settings. First, check your Wi-Fi settings. ...
2. Check Your Access Points. ...
3. Go Around Obstacles. ...
4. Restart the Router. ...
5. Check the Wi-Fi Name and Password. ...
6. Check DHCP Settings. ...

7. Update Windows. ...
8. Open Windows **Network** Diagnostics.



5. Conclusion: -

From the above experiment we can now configure the switch and router at our place, if we face an problem we can also troubleshoot to know about problems.

6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.
2. Turn off the power and unplug equipment before performing service.
3. Cover sharp edge inside the computer case with tape.
4. Never open a power supply or a CRT monitors.
5. Do not touch areas in printers that are hot or that use high voltage.

7. Review of the questions:

1. What is router?
2. What is routing?
3. What is switch?
4. What is switching
5. How to configure router.

Experiment No: - 14

1. Context

1.1 Subject: - computer network

1.2 Experiment: - 14

1.3 Topic: - Scaling of network

1.4 Sub-Topic: - Networking

1.5 Title of the experiment: - Study of scaling of networks, design verities of LAN and forward of traffic

1.6 Environment/location: - computer lab

2. Aim of the experiment: -Study of scaling of networks, design verities of LAN and forward of traffic

3. Objective of the experiment:

- On the completion of the experiment the student will able to: -
- Know what is scaling of network

4. Procedure: -

Implementing a Network Design (1.1)

Effective network design implementation requires a solid understanding of the current state of recommended network models and their ability to scale as the network grows. Hierarchical Network Design (1.1.1) The hierarchical network model and the Cisco Enterprise Architecture are models to consider when designing a network. This section reviews the importance of scalability and how these models can effectively address that need. The Need to Scale the Network (1.1.1.1) Businesses increasingly rely on their network infrastructure to provide mission critical services. As businesses grow and evolve, they hire more employees, open branch offices, and expand into global markets. These changes directly affect the 01_SNCH_3282_r2a.indd 3 2/13/14 10:30 AM 4 Scaling Networks Companion Guide requirements of a network. A large business environment with many users, locations, and systems is referred to as an enterprise. The network that is used to support the business enterprise is called an enterprise network. In Figure 1-1, the following steps occur as the network grows from a small company to a global enterprise:

1. The company begins as a small, single-location company.
2. The company increases its number of employees.
3. The company grows to multiple locations in the same city.

4. The enterprise grows to multiple cities.
5. The enterprise hires Tele workers.
6. The enterprise expands to other countries (not all enterprises are international).
7. The enterprise centralizes network management in a Network Operations Center (NOC).

Hierarchical Network Design (1.1.1.3)

To optimize bandwidth on an enterprise network, the network must be organized so that traffic stays local and is not propagated unnecessarily onto other portions of the network. Using the three-layer hierarchical design model helps organize the network. This model divides the network functionality into three distinct layers, as shown in Figure 1-3:

Access layer
Distribution layer
Core layer

You finally have the consulting project you've been waiting for: A customer is building a new office and has asked you to design their entire local area network (LAN), as their present infrastructure is outdated and has ports failing by the day.

This is a consultant's dream! However, it can become a nightmare for you and your company if you design the network improperly.

The following network design checklist examines some of the big network design issues to consider when designing a new LAN for your customers.

Plan the network's complexity to be in line with the customer's IT expertise

Switches and routers come with hundreds of features and functions. However, engineering too many bells and whistles into the network can create support problems in the future if the customer's IT staff does not have some basic understanding of the features and functions you implement. Recognize the business's needs without making the network overly complex.

To PoE, or not to PoE?

More and more customers are deploying wireless network technology and IP telephony. Wireless LAN access points are easiest to install when Power over Ethernet (PoE) is available. IP telephony utilizes phones that connect to and draw power from the LAN. The days of the traditional private branch exchange (PBX) system are numbered; every vendor out there is moving toward IP PBX systems and handsets. Many customers will tell you "We are not using wireless," or "We will never move to IP telephony." They may not now -- at least as far as their manager knows -- but if you do a good job on this project, your customer will keep their equipment for at least three to five years. You'll do a great service to your customer if you can convince them to purchase PoE switches now. Then, when the CIO decides to move to wireless LAN or IP telephony in 18 months, the non-PoE switches won't have to be replaced.

Figuring out network needs

Just because 10 gigabit Ethernet is here today and higher speeds are coming does not mean that you need those ports all over the LAN. All too often, customers purchase the fastest equipment possible thinking they need it, even though their existing 100 Mbps network is only running at 5% capacity. While it is definitely prudent to ensure that core switches can support these higher speeds, you may be advising the customer to waste a lot of money if you tell them that 10 Gb switches are needed everywhere

5. Conclusion: - from the above experiment we can know about scaling of networks.

6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.
2. Turn off the power and unplug equipment before performing service.
3. Cover sharp edge inside the computer case with tape.
4. Never open a power supply or a CRT monitors.
5. Do not touch areas in printers that are hot or that use high voltage.

7. Review of question:

1. What is Hierarchical Network Design
2. What is Implementing a Network Design
3. What is PoE?
4. What is not PoE?

Experiment No: - 15

1. **Context**
   - 1.1 **Subject: -** computer network
   - 1.2 **Experiment: -** 15
   - 1.3 **Topic: -** wan concept
   - 1.4 **Sub-Topic: -** networking
   - 1.5 **Title of the experiment: -**Study wan concepts and configure and forward traffic in wan
   - 1.6 **Environment/location: -** computer lab
2. **Aim of the experiment:** -Study wan concepts and configure and forward traffic in wan
3. **Objective of the experiment:**

   On completion of the experiment the student will able to: -
   Know what is wan and how to configure it.
4. **Procedure: -**

   Introducing

   Wide-Area Networks (WANs) One way to categorize networks is to divide them into local-area networks (LAN) and wide-area networks (WAN). LANs typically are connected workstations, printers, and other devices within a limited geographic area such as a building. All the devices in the LAN are under the common administration of the owner of that LAN, such as a company or an educational institution. Most LANs today are Ethernet LANs. WANs are networks that span a larger geographic area and usually require the services of a common carrier. Examples of WAN technologies and protocols include Frame Relay, ATM, and DSL. What Is a WAN? A WAN is a data communications network that operates beyond the geographic scope of a LAN. Figure 1-1 shows the relative location of a LAN and WAN.WANs differ from LANs in several ways. Whereas a LAN connects computers, peripherals, and other devices in a single building or other small geographic area, a WAN allows the transmission of data across greater geographic distances. In addition, an enterprise must subscribe to a WAN service provider to use WAN carrier network services. LANs typically are owned by the company or organization that uses them. WANs use facilities provided by a service provider, or carrier, such as a telephone or cable company, to connect the locations of an organization to each other, to locations of other organizations, to external services, and to remote users. WANs provide network capabilities to support a variety of mission-critical traffic such as voice, video, and data. Here are the three major characteristics of WANs:

■ WANs generally connect devices that are separated by a broader geographic area than can be served by a LAN.

■ WANs use the services of carriers, such as telephone companies, cable companies, satellite systems, and network providers.

■ WANs use serial connections of various types to provide access to bandwidth over large geographic areas

Why Are WANs Necessary?

LAN technologies provide both speed and cost efficiency for the transmission of data in organizations over relatively small geographic areas. However, other business needs require communication among remote sites, including the following:

■ People in the regional or branch offices of an organization need to be able to communicate and share resources with the central site.

■ Organizations often want to share information with other organizations across large distances. For example, software manufacturers routinely communicate product and promotion information to distributors that sell their products to end users.

■ Employees who frequently travel on company business need to access information that resides on their corporate networks. In addition, home computer users need to send and receive data across increasingly larger distances. Here are some examples:

■ It is now common in many households for consumers to communicate with banks, stores, and a variety of providers of goods and services via computers.

■ Students do research for classes by accessing library catalogs and publications located in other parts of their country and in other parts of the world.

Because it is obviously not feasible to connect computers across a country or around the world in the same way that they are connected in a LAN with cables, different technologies have evolved to support this need. The Internet has become and continues to be an inexpensive alternative for WAN connectivity. New technologies are available to businesses to provide security and privacy for their Internet communications and transactions. WANs used by them, or in concert with the Internet, allow organizations and individuals to meet their wide-area communication needs.

How to Configure WAN Interfaces

By default, ports p2 and p3 are preconfigured. If you want to configure a WAN interface for either of these ports, you might need to remove the default configurations:

- **Port p2** – Initially, the network interface for port p2 is configured as a dynamic network interface named **dhcp**. If you want to configure either a static or other dynamic connection besides DHCP (PPTP or PPPoE) on port p2, delete the default **DHCP** interface.
- **Port p3** – Initially, port p3 is bridged to port p1. Both interfaces are also configured as management ports in the LAN. To use port p3 for another connection, delete the P1-P3 bridge. However, you might lose connectivity to the network from your administrative PC.

After removing the default configurations for ports p2 and p3, you can reconfigure them as WAN interfaces. For any other ports, just begin configuring the WAN interface. You can configure the WAN interface with either static or dynamic IP address assignment.

Be sure to add the gateway to create the default route over the WAN interface, either when you add or edit a static network interface, or on the **NETWORK > Routing** page.

Remove the default configurations for port p2 and port p3

If you want to use port p2 or p3, first remove their default configurations.

1. If you want to use port p2:
    a. Go to the **NETWORK > IP Configuration** page.
    b. Delete the default DHCP interface from the **Dynamic Interface Configuration** section.
2. If you want to use port p3:
    a. Go the **NETWORK > Bridging** page and delete the P1-P3 bridge.
    b. Go the the **FIREWALL > Firewall Rules** page. Delete the P1-P3-BRIDGE firewall rule.

Configure a WAN interface

To configure a WAN interface:

1. Go to the **NETWORK > IP Configuration** page.
2. If your WAN interface has a static IP address:
    a. In the **Static Interface Configuration** section, click **Add Static Network Interface**.
    b. Configure the static interface settings, including the gateway address.
    c. Click **Add**.
3. If you have a dynamic connection such as PPTP or PPPoE:
    a. In the **Dynamic Interface Configuration** section, click **Add Dynamic Network Interface**.
    b. Configure the dynamic interface settings.
    c. Click **Add**.
4. At the top of the page, click on the warning message to execute the new network configuration.
5. **Conclusion: -** From the above experiment we know about WAN and how to configure it.
6. **Safety and precautions**

1. Remove your watch and jewelry and secure loose clothing.

2. Turn off the power and unplug equipment before performing service.

3. Cover sharp edge inside the computer case with tape.

4. Never open a power supply or a CRT monitors.

5. Do not touch areas in printers that are hot or that use high voltage.

7. **Review of questions:**
    1. What is a WAN?
    2. Why Are WANs Necessary?
    3. How to configure it?

Experiment No: - 16

1. Context

- **1.1 Subject: -** Computer network
- **1.2 Experiment: -** 16
- **1.3 Topic: -** IPv4 and IPv6
- **1.4 Sub-Topics: -** networking
- **1.5 Title of the experiment: -**Configure IPv4 and IPv6 and learn quality, security and other services
- **1.6 Environment/location: -** computer lab

2. Aim of the experiment: -Configure IPv4 and IPv6 and learn quality, security and other services

3. Objective of the experiment: -

On the completion of the experiment students will able to: -
Know what is IPv4 and IPv6 how to configure.

4. Procedure: -

Steps to configure IPv4.

Step 1 Open control panel.
Step 2 Click on Network and Sharing Center
Step 3 Click on Change Adapter Settings
Step 4 Right click on Local Area Connection and click Properties
Step 5 Click Internet Protocol Version 4 (TCP/IP) then click Properties

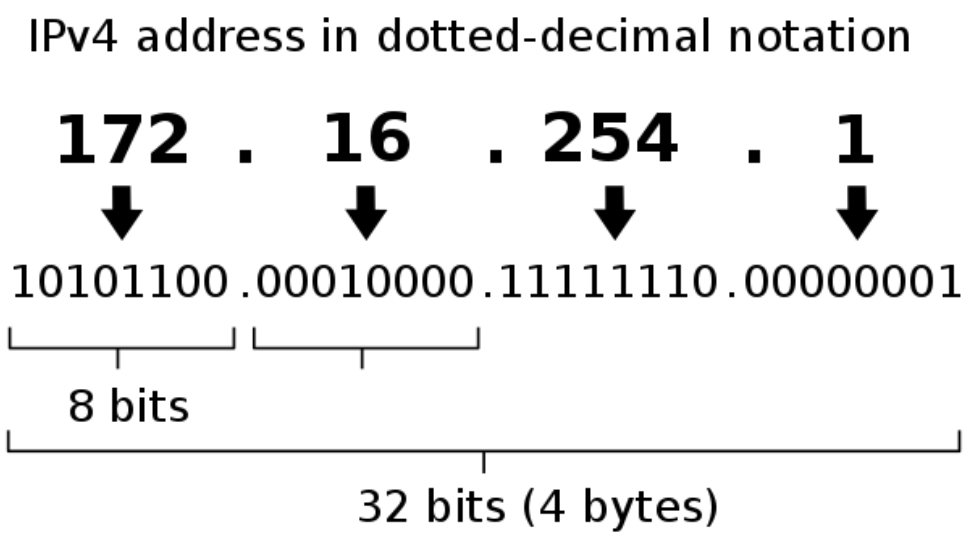
Step 7 Change 'Dot' to Use the following IP address and input your IP and DNS information.

Step 8 Click OK to save and apply your settings.

Security of IPv4: -

1. **It is deployed in 1981.**
2. **It uses 32-bit IP address**
3. **It has 4.3 billion addresses**
4. **Addresses must be reused and masked**
5. **It is numeric dot-decimal notation**

   Eg: -192.168.5.18



Steps to configure IPv6.

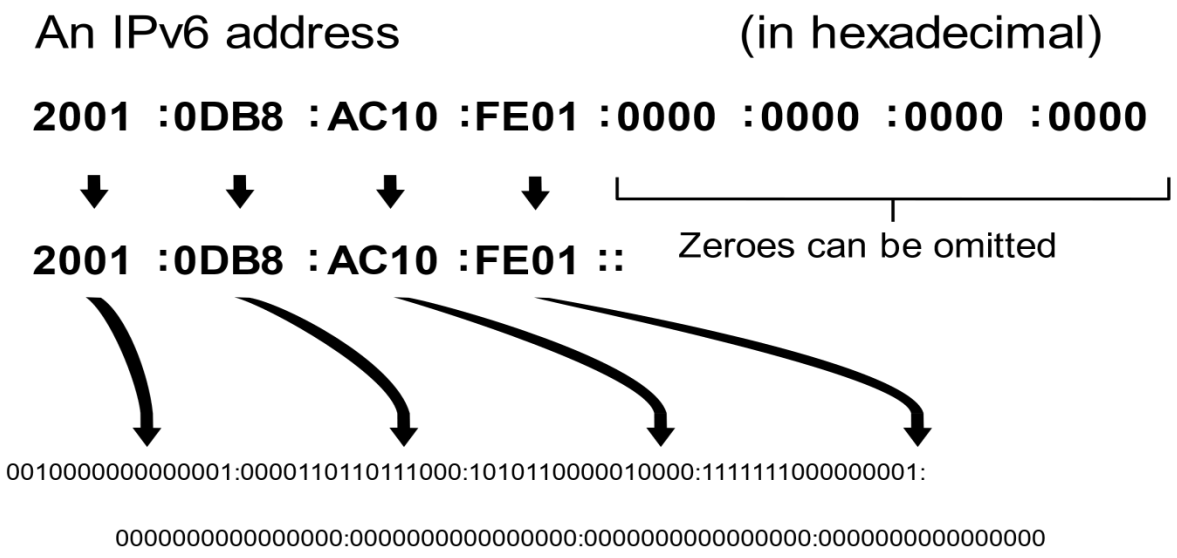
Step 1 Open control panel.
Step 2 Click on Network and Sharing Centre
Step 3 Click on Change Adapter Settings
Step 4 Right click on Local Area Connection and click Properties
Step 5 Click Internet Protocol Version 6 (TCP/IP) then click Properties

Step 7 Change 'Dot' to Use the following IP address and input your IP and DNS information.

Step 8 Click OK to save and apply your settings.

Security of IPv6: -

1. **It is deployed in 1998.**
2. **It uses 128-bit IP address**
3. **It has $7.9x10^{28}$ addresses**
4. **Every device have a unique address**
5. **It is alphanumeric hexadecimal notation**
6. **Eg: -50b2:6400:0000:0000:6c3a:b17d:0000:10a9**



5. Conclusion: - From the above experiment we are able to learn what is IPv4 and IPv6 and how to configure it.

6. Safety and Precautions

1. Remove your watch and jewelry and secure loose clothing.
2. Turn off the power and unplug equipment before performing service.
3. Cover sharp edge inside the computer case with tape.
4. Never open a power supply or a CRT monitors.
5. Do not touch areas in printers that are hot or that use high voltage

7. Review of questions

1. What is IPv4?
2. What is IPv6?
3. How to configure both IPv4 and IPv6?
4. Which is more secure?

Experiment No:-17

1. **Context**
   - **1.1 Subject: -** computer network
   - **1.2 Experiment: -** 16
   - **1.3 Topic: -** network programming
   - **1.4 Sub-Topics: -** networking
   - **1.5 Title of the experiment:** Learn network programming
   - **1.6 Environment/location: -** computer lab

2. Aim of the experiment: -Learn network programming**3. Objective of the experiment:** -

On the completion of the experiment students will able to: -

Know what is IPv4 and IPv6 how to configure.

4. Procedure: -

Connection-oriented and connectionless communications

Very generally, most of communications can be divided into connection-oriented, and connectionless. Whether a communication is a connection-oriented, or connectionless, is defined by the communication protocol, and not by application programming interface (API). Examples of the connection-oriented protocols include Transmission Control Protocol (TCP) and Sequenced Packet Exchange (SPX), and examples of connectionless protocols include User Datagram Protocol (UDP), "raw IP", and Internetwork Packet Exchange (IPX).

Clients and Servers

For connection-oriented communications, communication parties usually have different roles. One party is usually waiting for incoming connections; this party is usually referred to as "server". Another party is the one which initiates connection; this party is usually referred to as "client".

For connectionless communications, one party ("server") is usually waiting for an incoming packet, and another party ("client") is usually understood as the one which sends an unsolicited packet to "server".

Popular protocols and API

Network programming traditionally covers different layers of OSI/ISO model (most of application-level programming belongs to L4 and up). The table below contains some examples of popular protocols belonging to different OSI/ISO layers, and popular APIs for them.

OSI/ISO Layer	Protocol	API
L3 (network)	IP	Raw socket
L4 (transport)	TCP, UDP, SCTP	Berkeley Sockets
L5 (session)	TLS	Open SSL
L7 (application)	HTTP	Various

5.Conclusion: - From the above experiment we are ableto know about network programming**.**

6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.

2. Turn off the power and unplug equipment before performing service.

3. Cover sharp edge inside the computer case with tape.

4. Never open a power supply or a CRT monitors.

5. Do not touch areas in printers that are hot or that use high voltage

7. Review of question:

1. What are the different types of protocols?
2. What is client-server model?

Experiment No: - 18

1. **Context**
   - **1.1 Subject: -** computer network
   - **1.2 Experimentt: -** 18
   - **1.3 Topic: -** Troubles shoot networks
   - **1.4 Sub-Topics: -** Networking
   - **1.5 Title of the experiment:** Troubles shoot networks
   - **1.6 Environment/location: -** Computer lab
2. **Aim of the experiment: -**Troubles shoot networks
3. **Objective of the experiment: -**

On the completion of the experiment students will able to: -

Know list of Troubles shoot networks.

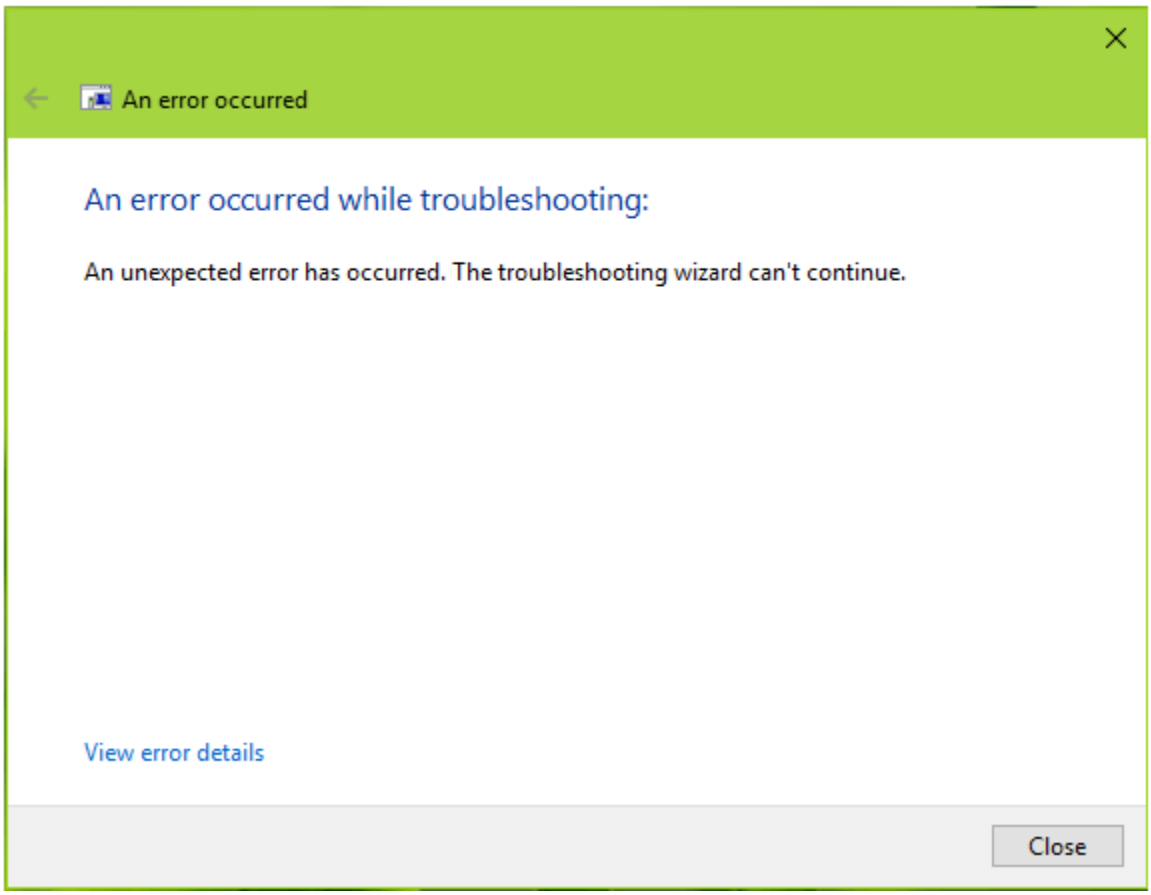
4. Procedure: -

An Error Occurred While Troubleshooting Windows 10/8/7

Computer troubleshooting can be a tricky thing. But in Windows 10/8/7, there are built-in Troubleshooters that can help you to resolve most of the common Windows problems automatically in a few clicks.

For example, if you can't add a new piece of hardware, or there are problems like unexpected keyboard behavior, program compatibility issues, search and indexing problems, Windows update issues, etc., Windows Troubleshooters can be helpful.

However, the Troubleshooters are not always working well. Sometimes, when you try to fix computer issues, the error "An error occurred while troubleshooting" will appear on your computer screen in Windows 10/8/7, followed by an additional message.



The additional message may be:

- A problem is preventing the troubleshooter from starting.
- An unexpected error has occurred. The troubleshooting wizard can't continue.

Usually, there is a random error code in the interface of "An error occurred", like 0x80070057, 0x8000FFF, 0x80070005, 0x80070490, 0x80070002, 0x8e5e0247, 0x803c0103, etc.

It is annoying when Windows Troubleshooters doesn't work, especially if you are solving a problem that has been bugging you for a while. How to fix troubleshooting? Follow the solutions below to find out how to fix it.

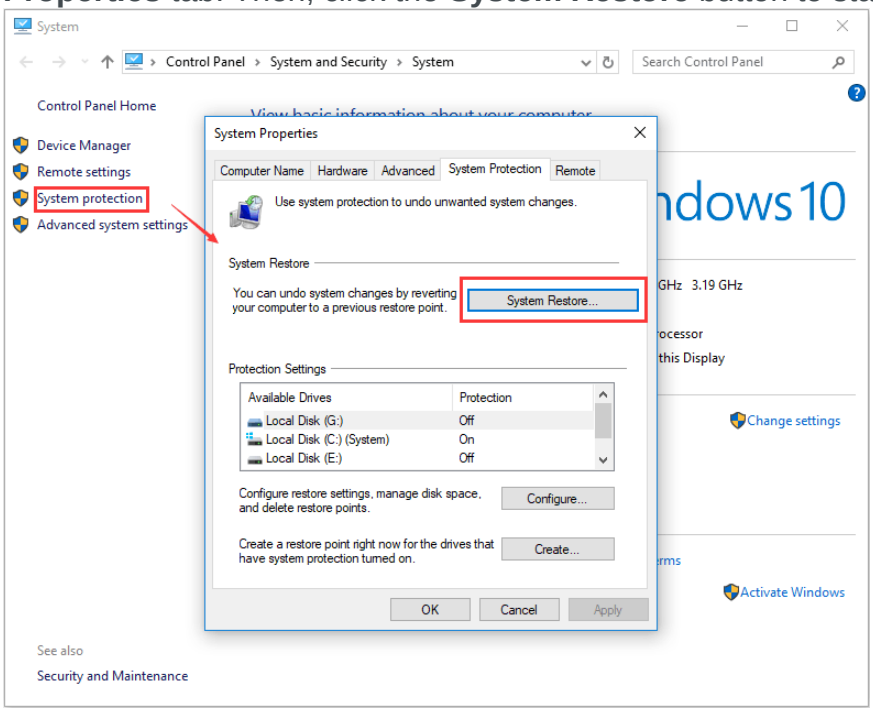
How to Fix Troubleshoot Problems in Windows 10/8/7

Solution 1: Perform a System Restore

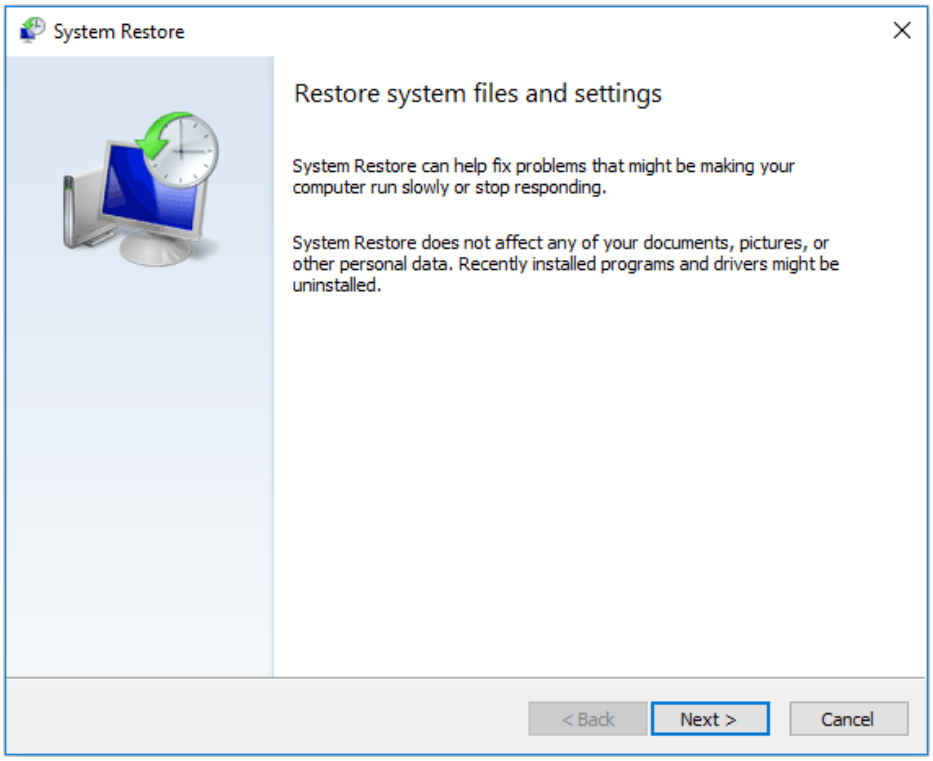
When troubleshooting error happens on your Windows 7/8/10 screen, if you have created a system restore point beforehand, you can solve this issue by using System Restore feature to revert your computer to a previous restore point to undo system changes.

Step 1: Right-click on **This PC** or **Computer** and click **Properties**.

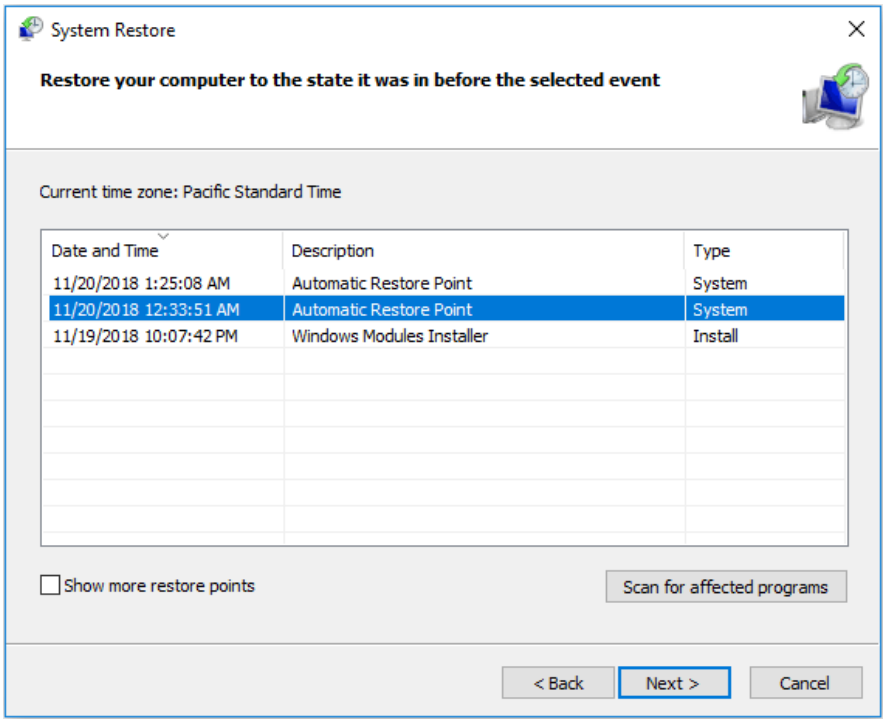
Step 2: In the pop-up window, click **System protection** to enter the **System Properties** tab. Then, click the **System Restore** button to start a system restore.



Step 3: After entering the System Restore window, click the **Next** button to continue.



Step 4: The created system points will be listed, just choose the desired restore point and click the **Next** button.



Step 5: Confirm your restore point and complete the restoration process by following the instructions on the screen.

5. **Conclusion: -** From the above experiment we are to ways to handle different types of troubleshooting problems.

6. Safety and precautions

1. Remove your watch and jewelry and secure loose clothing.
2. Turn off the power and unplug equipment before performing service.
3. Cover sharp edge inside the computer case with tape.
4. Never open a power supply or a CRT monitors.
5. Do not touch areas in printers that are hot or that use high voltage

7. Review of question:

1. What are various types of error occurred in pc.
2. How to handle the troubleshooter Program?
3. How to restore a System?
4. What is troubleshooting wizard?