List of Experiments:-

1(a). Study different types of Network cables (Copper and Fiber) and prepare cables (Straight and Cross) to connect Two or more systems. Use crimping tool to connect jacks. Use LAN tester to connect the cables.

1(b). Install and configure Network Devices: HUB, Switch and Routers. Consider both manageable and non-manageable switches. Do the logical configuration of the system. Set the bandwidth of different ports.

1(c). Install and Configure Wired and Wireless NIC and transfer files between systems in Wired LAN and Wireless LAN. Consider both adhoc and infrastructure mode of operation.

2. Work with the commands Ping, Tracert, Ipconfig, pathping, telnet, ftp, getmac, ARP, Hostname, Nbtstat, netdiag, and Nslookup

3. Find all the IP addresses on your network. Unicast, Multicast, and Broadcast on your network.

4. Use Packet tracer software to build network topology and configure using Distance vector routing protocol.

5. Use Packet tracer software to build network topology and configure using Link State routing protocol.

6. Using JAVA RMI Write a program to implement Basic Calculator

7. Implement a Chatting application using JAVA TCP and UDP sockets.

8. Hello command is used to know whether the machine at the other end is working or not. Echo command is used to measure the round trip time to the neighbour. Implement Hello and Echo commands using JAVA.

9. Using Wireshark perform the following operations:

- Inspect HTTP Traffic

- Inspect HTTP Traffic from a Given IP Address,

- Inspect HTTP Traffic to a Given IP Address,

- Reject Packets to Given IP Address,

- Monitor Apache and MySQL Network Traffic.

10. Install Network Simulator 2/3. Create a wired network using dumbbell topology. Attach agents, generate both FTP and CBR traffic, and transmit the traffic. Vary the data rates and evaluate the performance using metric throughput, delay, jitter and packet loss.

11. Create a static wireless network. Attach agents, generate both FTP and CBR traffic, and transmit the traffic. Vary the data rates and evaluate the performance using metric throughput, delay, jitter and packet loss.

12. Create a mobile wireless network. Attach agents, generate both FTP and CBR traffic, and transmit the traffic. Vary the data rates and evaluate the performance using metric throughput, delay, jitter and packet loss.

Experiment-1(A)

**Aim:-** **Study different types of Network cables(Copper and Fiber) and prepare cables (Straight and Cross) to connect two or more systems. Use crimping tool to connect jacks. Use LAN testers to connect the cables.**

# Types of Network Cables:-

There are three types of Network cables: **coaxial, twisted pair, and fiber-optic cabling**. In modern [Local Area Networks](https://computernetworktopology.com/local-area-network/), twisted pair cable cabling is the most popular type of cabling, but fiber-optic cabling usage is increasing, especially in high-end networks. Coaxial cabling is usually used for cable over the Internet. Let’s explain all three Types of Ethernet Cables in detail.

### **1: Coaxial Cabling:-**

A coaxial cable has an internal conductor that runs down the middle of the cable. The conductor is surrounded by a layer of insulation which is then surrounded by another carrying conductor shield, which makes this type of cable resistant to external obstruction. This type of cable comes in two types – thinnet and thicknet. Each type has a maximum transmission speed of 10 Mbps. Coaxial cables were previously used in computer networks, but are now replaced by twisted pair cables.

A **single-core** coaxial cable uses a single central metal (usually copper) conductor, while a **multi-core** coaxial cable uses multiple thin strands of metal wires. The following image shows both types of cable.

### **2: Twisted-pair Cabling:-**

The twisted-room has four pairs of wires. These wires are twisted almost to each other to reduce crosstalk and external interference. This type of cabling is common in current LANs.

Twisted pair cables can be used for telephone and network cables. It comes in two versions: **UTP (Unshielded Twisted-Pair)** and **STP (Shielded Twisted-Pair)**. The difference between these is that the STP cable has an additional layer of protection to protect the data from external interference.

### Similarities and differences between STP and UTP cables

* Both STP and UTP can transmit data over 10Mbps, 100Mbps, 1Gbps, and 10Gbps.
* STP cables are more expensive than UTP cables because they contain more material.
* Both cables use the same RJ-45 (registered slot) module connector.
* STP provides more noise and EMI resistance than UTP cable.
* The maximum length of the two cable segments is 100 meters or 328 feet.
* The two cables can accommodate a maximum of 1,024 nodes per segment.

The following image shows both types of twisted-pair cable.

### **3: Fiber-optic Cabling:-**

This type of cable uses optical fibers to transmit data in the form of a light signal. The cables have fiberglass strands surrounded by cladding material.

The core is wrapped in cladding; The cladding is wrapped in a buffer, and the buffer is wrapped in a jacket.

1. The key is to transmit information signals in the form of light.
2. The cladding reflects light back into the core.
3. The buffer prevents light from leaking.
4. This jacket protects the cable from physical damage.

Fiber optic cables are fully immune to EMI and RFI. This cable can transmit data over long distances at maximum speed. It can transmit 40 km of data at 100Gbps.

Fiber optic cables use light to transmit data. It reflects light from one point to another. There are two types of fiber optic cables based on how much light they transmit at a given time; SMF to MMF.

This type of cable can support longer cable lengths than other cable types (a few miles). The cable has no electromagnetic interference. As you can see, this cable method has many advantages over other methods, but its main disadvantage is that it is more expensive.

There are two types of fiber-optic cables:

* **Single-mode fiber (SMF)** – uses only one light beam to transmit information. Used for longer distances.
* **Multi-mode fiber (MMF)** – uses multiple light beams to transmit data. Less expensive than SMF.

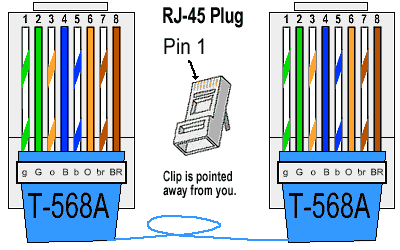
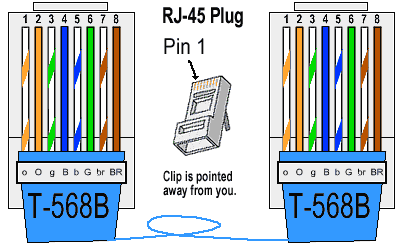
**prepare cables (Straight and Cross):-**

**Components:** RJ-45 connector, Crimping Tool, Twisted pair Cable

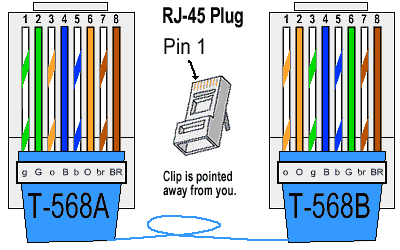
**Procedure: To do these practical following steps should be done:**

* 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 ½ 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 ½ 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.

**Diagram show you how to prepare Straight wired connection**

**Diagram show you how to prepare Cross wired connection**



**LAN testers:-**

A [LAN cable tester](http://dataworld.com.au/network-tools/cable-tools/cable-tester/) is a tool that is used for testing LAN cables. It has the capability to find certain problems associated with the cable. Any defect can easily be detected with this small but very useful instrument. Generally, a LAN cable tester consists of a source of electric current, a voltmeter and switching matrix that is used to connect the source and the voltmeter to the contact points.

Usually, the testing process is done in two stages. The first stage is called the open test, and this stage makes sure that every planned connections is properly set. The second, called the short test, helps find unintended connections. The LAN cable testers are not only used for testing LAN cables, but for telecommunication and data communication cables as well. In short, a LAN cable tester is a tool that offers a lot and is a must-have network testing tool.

Experiment-1(B)

**Aim:-** **Install and configure Network Devices: HUB, Switch and Routers. Consider both manageable cand non-manageable switches. Do the logical configuration of the system. Set the bandwidth of  
different ports.**

**Hub:**

An Eathernet hub, active hub, network hub, repeater hub, hub or concentrator is a device for connecting multiple twisted pair or optic fiber Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer(layer1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

**Switch:**

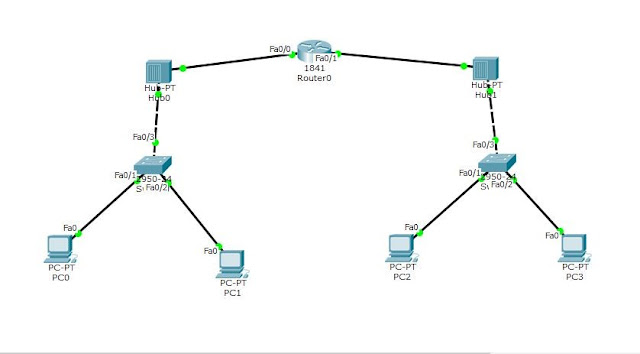
A network switch connects devices within a network (often a [local area network, or LAN](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/)) and forwards [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) to and from those devices. Unlike a [router](https://www.cloudflare.com/learning/network-layer/what-is-a-router/), a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices.

An unmanaged switch simply creates more Ethernet ports on a LAN, so that more local devices can access the Internet. Unmanaged switches pass data back and forth based on device MAC addresses.

A managed switch fulfills the same function for much larger networks, and offers network administrators much more control over how traffic is prioritized. They also enable administrators to set up Virtual LANs (VLANs) to further subdivide a local network into smaller chunks.

**Router:**

A Router is an electronic device that interconnects two of more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network. Or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

0[](https://1.bp.blogspot.com/-Rwp5amQY5Bc/Xo2mGalki3I/AAAAAAAAAAM/PSJ03iHXLwMScYP4hl5XFg5qbxLcb4ZFwCLcBGAsYHQ/s1600/Install+and+configure+network+devices+HUB+Switch+and+Router.jpg)

**Step 1**: Take a router of model 1841.

**Step 2**: Take two hub of model Hub-PT.

**Step 3**: Take two switch of model 2950-24.

**Step 4**: Take pc0, pc1 for switch0, take pc2, pc3 for switch1.

**Step 5:**Connect pc0, pc1 to Switch0 with Straight through cable, connect pc2, pc3 to Switch1 with straight through cable, and connect Switch0 to Hub0 with cross over cable, connect Switch1 to Hub1 with cross over cable. Connect Hub0, Hub1 to Router0 with straight through cable.

**Step 6:**Router configuration:

Go to**Router0**→**CLI**

Router>enable

Router#configure terminal

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 10.10.1.1  255.0.0.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip address 192.168.1.1  255.255.255.0

Router(config-if)#no shutdown

**Step 7:**All pcConfiguration:

Go to **PC0** → **Desktop** → **IP Configuration** → **Static**

|  |  |
| --- | --- |
| IP Address | 10.10.1.5 |
| Subnet Mask | 255.0.0.0 |
| Default Gateway | 10.10.1.1 |

Go to **PC1** → **Desktop** → **IP Configuration** → **Static**

|  |  |
| --- | --- |
| IP Address | 10.10.1.6 |
| Subnet Mask | 255.0.0.0 |
| Default Gateway | 10.10.1.1 |

Go to**PC2** → **Desktop** → **IP Configuration** → **Static**

|  |  |
| --- | --- |
| IP Address | 192.168.1.5 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.1.1 |

Go to **PC3** → **Desktop** → **IP Configuration** → **Static**

|  |  |
| --- | --- |
| IP Address | 192.168.1.6 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 192.168.1.1 |

Experiment-1(c)

Aim:- install and configure wired and wireless NIC and transfer files between systems in wired LAN and wireless LAN. Consider both adhoc and infrastructure mode of operation.hn

Install and Configure of wired LAN:-

* After connecting A computer to an ethernet cable, click the **Start** button, and select **Settings**.
* Select **Network and Internet**.
* In **Status,** click **Network and Sharing Center**.
* Choose **Change adapter settings** on the left side menu.
* Right-click Ethernet and then choose Properties.
* Select**Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**.
* Set up the IP to use, then click **OK** to save your settings. You may want to restart your computer.
* Open a web browser to test your connection. In some instances, you may be asked to [register your computer onto CU Boulder's network](https://oit.colorado.edu/node/1731/). If you register your computer, you should [clear your web browser's cache](https://oit.colorado.edu/node/739) after registration.

Install and Configure of wireless LAN:-

* The optimal placement is in a central location, free from obstructions that could cause wireless interference..
* Plug an [Ethernet cable](https://www.lifewire.com/what-is-an-ethernet-cable-817548) (typically provided with the router) into the router [WAN port](https://www.lifewire.com/what-is-an-ethernet-port-817546). Then, connect the other end of the Ethernet cable to the modem.
* plug one end of another Ethernet cable into the router LAN port (any port will work) and the other end of the Ethernet cable into the Ethernet port of a laptop.
* It's best if you turn on these devices in the proper order. Turn on the modem first. When the modem lights are all on, turn on the router. When the router is on, turn on the computer.
* Configure the router name, static or dynamic ip addresses and security password to the router and save configuration.
* After saving the router's configuration settings, unplug the cable that connects the computer to the router. Then, plug a USB or PC card wireless adapter into the laptop if it doesn't have a wireless adapter installed or built-in.
* Your computer may automatically install the drivers, or you may have to use the setup CD that came with the adapter.
* On your computer and other wireless-enabled devices, find the new network you set up and [connect to the network](https://www.lifewire.com/wi-fi-tutorial-how-to-connect-to-a-wireless-network-2378222).

# Ad-Hoc Mode & Infrastructure Mode

• Infrastructure mode is the most common mode to operate and is the factory default setting.

• Infrastructure mode is used when a PC is connected to a wireless access point or to a wireless router.

• If the hosts are connected to the network via a base station or an access point (fixed infrastructure), then the network is said to be operating in infrastructure mode.

• Cellular networks work in infrastructure mode because all the cell phones connect to the network through the base stations (cell towers).

When a network is not in infrastructure mode, then it is said to be operating in Ad hoc mode of operation.

• In an Ad hoc mode of operation, the wireless hosts can communicate with each other without an access point.

• No fixed infrastructure such as access point is required for the wireless hosts.

Experiment-2

Aim:-Work with the commands Ping, Tracert, Ipconfig, pathping, telnet, ftp, getmac, ARP, Hostname, nbtstaff, netdiag, and nslookup.

**Basic networking commands:-**

C:\>ping: Ping is the most basic TCP/IP command, and it’s the same as placing a phone call  
to your best friend. You pick up your telephone and dial a number, expecting your best friend  
to reply with “Hello” on the other end. Computers make phone calls to each other over a  
network by using a Ping command. The Ping commands main purpose is to place a phone  
call to another computer on the network, and request an answer. Ping has 2 options it can use  
to place a phone call to another computer on the network. It can use the computers name or  
IP address.

C:\>tracert: The tracert command displays a list of all the routers that a packet has to go  
through to get from the computer where tracert is run to any other computer on the  
internet.

C:\>ipconfig: The ipconfig command displays information about the host (the computer  
your sitting at)computer TCP/IP configuration.

C:\>ipconfig /all: This command displays detailed configuration information about your  
TCP/IP connection including Router, Gateway, DNS, DHCP, and type of Ethernet  
adapter in your system.

C:\>Ipconfig /renew: Using this command will renew all your IP addresses that you are  
currently (leasing) borrowing from the DHCP server. This command is a quick problem  
solver if you are having connection issues, but does not work if you have been configured  
with a static IP address.

C:\>Ipconifg /release: This command allows you to drop the IP lease from the DHCP  
server.

C:\>ipconfig /flushdns: This command is only needed if you’re having trouble with your  
networks DNS configuration. The best time to use this command is after network  
configuration frustration sets in, and you really need the computer to reply with flushed.

C:\>pathping: Pathping is unique to Window’s, and is basically a combination of the Ping  
and Tracert commands. Pathping traces the route to the destination address then launches a  
25 second test of each router along the way, gathering statistics on the rate of data loss along  
each hop.

C:\telnet

Telnet is a text-based program you can use to connect to another computer using the Internet. You'll be able to access programs and services that are on the remote computer as if you were sitting right in front of it.

C:\ftp

It is a protocol

C:\ getmac: This is the simplest of all TCP/IP commands. It simply displays the MAC or physical address of  
your computer.

C:\>arp –a: ARP is short form of address resolution protocol, It will show the IP address of  
your computer along with the IP address and MAC address of your router.

C:\>hostname: This is the simplest of all TCP/IP commands. It simply displays the name of  
your computer.

C:\>nbtstat –a: This command helps solve problems with NetBIOS name resolution.  
(Nbt stands for NetBIOS over TCP/IP)

C:\>netdiag: Netdiag is a network testing utility that performs a variety of network diagnostic  
tests, allowing you to pinpoint problems in your network. Netdiag isn’t installed by default,  
but can be installed from the Windows XP CD after saying no to the install. Navigate to the  
CD ROM drive letter and open the support\tools folder on the XP  
CD and click the setup.exe icon in the support\tools folder.

C:\>netstat: Netstat displays a variety of statistics about a computers active TCP/IP  
connections. This tool is most useful when you’re having trouble with TCP/IP applications  
such as HTTP, and FTP.

C:\>nslookup: Nslookup is used for diagnosing DNS problems. If you can access a  
resource by specifying an IP address but not it’s DNS you have a DNS problem.  
5  
C:\>route: The route command displays the computers routing table. A typical  
computer, with a single network interface, connected to a LAN, with a router is fairly  
simple and generally doesn’t pose any network problems. But if you’re having trouble  
accessing other computers on your network, you can use the route command to make sure the  
entries in the routing table are correct.