

Lab Assignment on Unit I

Aim – To Setup a wired LAN using Layer 2 Switch and then IP switch of minimum four computers.

Prerequisites:

Knowledge of components such Ethernet card, Cable type, Connections, topologies.

Theory:

Types of LAN:

A **local area network (LAN)** is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building and has its network equipment and interconnects locally managed. By contrast, a wide area network(WAN) not only covers a larger geographic distance, but also generally involves leased telecommunication circuits or Internet links. An even greater contrast is the Internet, which is a system of globally connected business and personal computers.

Ethernet and Wi-Fi are the two most common transmission technologies in use for local area networks.

- **Ethernet LAN:**

Ethernet is the most popular physical layer LAN technology in use today. It defines the number of conductors that are required for a connection, A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

- **Fast Ethernet**

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster

throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

- **Gigabit Ethernet**

Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Also known as “gigabit-Ethernet-over-copper” or 1000Base-T, GigE is a version of Ethernet that runs at speeds 10 times faster than 100Base-T. It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.

- **10 Gigabit Ethernet**

10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.

Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing. As it is still very new, which of the standards will gain commercial acceptance has yet to be determined.

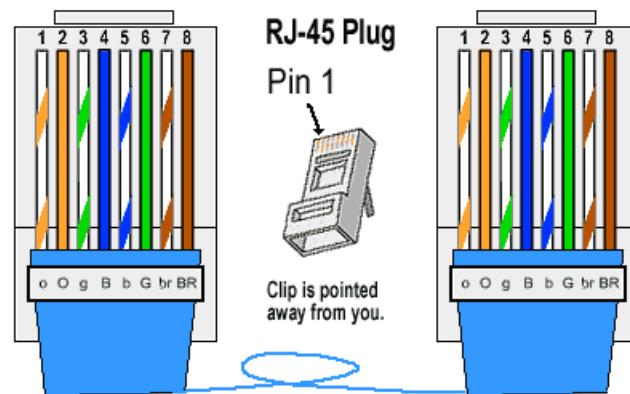
Steps for setting up LAN:

- Installation of Ethernet card in machine.
- Crimping of Ethernet cable
- Make Straight cable in order to form Star topology network to connect 2 different types of components eg. PC to switch or PC to router
- Make Cross cable in order to form Star topology network to connect 2 Similar types of components eg. PC to PC or router to router.

here are two kinds of Ethernet cables you can make, **Straight Through** and **Crossover**.

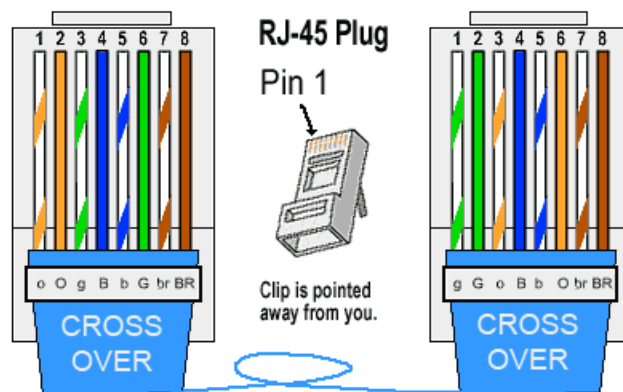
- **STRAIGHT THROUGH**

Ethernet cables are the standard cable used for almost all purposes, and are often called "patch cables". It is highly recommend you duplicate the color order as shown on the left. Note how the green pair is not side-by-side as are all the other pairs. This configuration allows for longer wire runs.



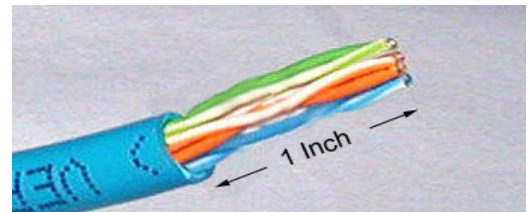
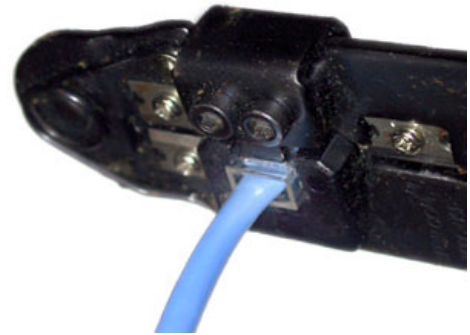
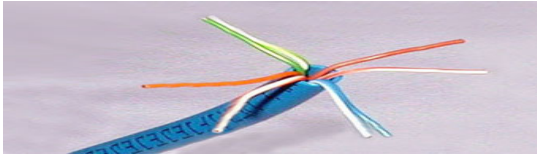
- **CROSSOVER CABLES**

The purpose of a Crossover Ethernet cable is to directly connect one computer to another computer (or device) without going through a router, switch or hub.



- **Crimping:**

Required components:



5) Connect the cable to switch and from switch to the machine. Thus it forms STAR Topology.

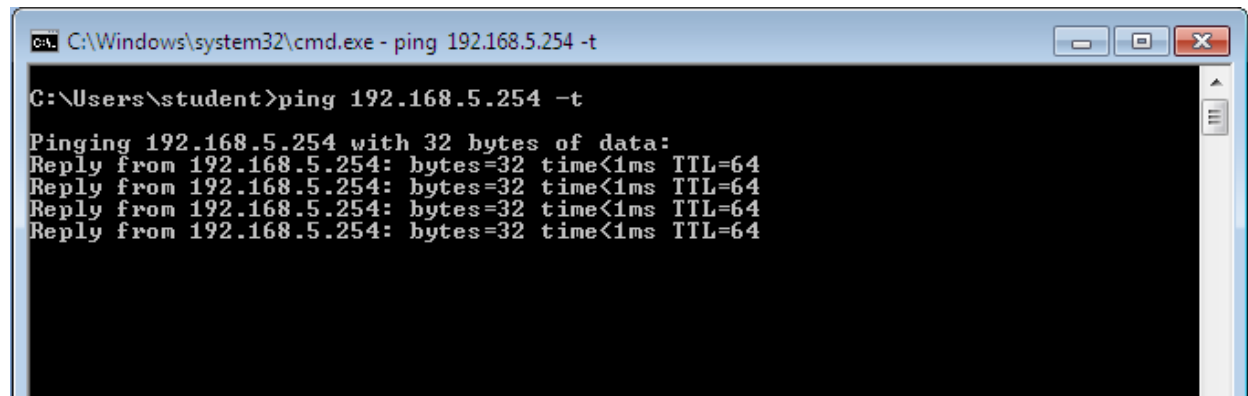
6) Assign IP address
ping from one machine
message is displayed.

to machine 1,2,3 and machine 4 and
to other machine. Following



P:F-LTL-UG/03/R1

7)



```
C:\Windows\system32\cmd.exe - ping 192.168.5.254 -t

C:\Users\student>ping 192.168.5.254 -t

Pinging 192.168.5.254 with 32 bytes of data:
Reply from 192.168.5.254: bytes=32 time<1ms TTL=64
Reply from 192.168.5.254: bytes=32 time<1ms TTL=64
Reply from 192.168.5.254: bytes=32 time<1ms TTL=64
Reply from 192.168.5.254: bytes=32 time<1ms TTL=64
```

Definition - What does Internet Protocol Switching (IP Switching) mean?

Internet Protocol switching, far more commonly referred to as IP Switching, is a routing technique which routes data packets faster than traditional routing by using Layer 3 Switches.

IP Switching is performed by implementing Layer 3 switches which employ Application Specific Integrated Circuit (ASIC) hardware and transferring via Asynchronous Transfer Mode (ATM) Switches. This speeds up the whole routing process. IP Switching establishes a virtual circuit in ATM switches whenever it needs to route packets that are high priority or packets that are destined for an external network.

- **Filtering Packets Cable Testing**

As networks evolve, so do the requirements of the cabling infrastructure to support them. New standards are continuously being developed to provide guidelines for cabling professionals when installing, testing, troubleshooting, and certifying either copper and fiber. Whether it's 10BASE-T, 100BASE-TX or 1000BASE-T, there are specific requirements and potential pitfalls in Filtering Packetsimplementing these technologies. With 10GBASE-T, it becomes even more critical to keep current with the latest proliferations in cabling and cable testing.

- **Types of Cable Testers**

Cable test instruments are designed with a variety of focused features for particular field tasks. They vary in price, performance, and application. Depending on the task the field test instrument performs, it can be classified into one of the three hierarchical groups: certification, qualification, or verification. While some features overlap between test tools, each group answers a unique testing need and provides a different level of operational assurance.

- **Wireshark Packet Analyzer Tool**

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other the other packets on the network.

- **Color Coding**

You'll probably see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.

- **Filtering Packets**

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

Conclusion :

Thus, after successfully completing this assignment, Layer 2 switches and IP switching.