Computer Networks, IT-304

Autumn Semester 2024

Lab-02A

Aim: To study and prepare LAN cables.

Theory:

Local Area Network

A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link. Typically, connected devices share the resources of a single processor or server within a small geographic area such as home, school, computer laboratory, office building, or closely positioned group of buildings**.**

Transmission Medium

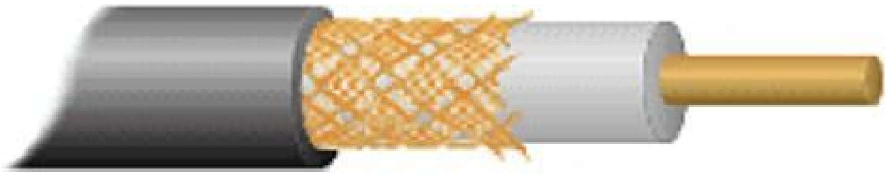
The means through which data is transformed from one place to another is called transmission or communication media. There are two categories of transmission media used in computer communications:

a) Guided Media
b) Unguided Media

1. **Guided Media**: Guided media are the physical links through which signals are confined to narrow path. These are also called guide media. Guided media are made up of a external conductor (Usually Copper) bounded by jacket material, which are called as cables. 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 LANs. 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. Three common types of cables that are used for data transmission are:
    - Coaxial Cable
    - Twisted Pairs Cable
    - Fiber Optics Cable

Coaxial Cable:

Coaxial cable is very common & widely used commutation media. It got its name because it contains two conductors that are parallel to each other. The center conductor in the cable is usually copper. The copper can be either a solid wire or stranded material. Outside this central Conductor is a non-conductive material. It is usually white, plastic material used to separate the inner Conductor form the outer Conductor. The other Conductor is a fine mesh made from Copper. It is used to help shield the cable form EMI. Outside the copper mesh is the final protective cover.



Coaxial cable

Twisted Pair Cable:

The most popular network cabling is twisted pair. It is light weight, easy to install, inexpensive and support many different types of network. It also supports the speed of 100 mps. Twisted pair cabling is made of pairs of solid or stranded copper twisted along each other. The twists are done to reduce vulnerably to EMI and cross talk. The number of pairs in the cable depends on the type. Twisted pair cabling comes in two varieties: shielded and unshielded.

UTP (Unshielded Twisted Pair 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.

Unshielded twisted pair

In the context of the 100-ohm UTP (Unshielded Twisted Pair) type of cable used for Ethernet wiring the only categories of interest are Cat3, Cat4, Cat5, Cat5e, Cat6, and Cat7. CATx is an abbreviation for the category number that defines the performance of building telecommunications cabling as outlined by the Electronic Industries Association (EIA) standards. Some specifications for these categories are shown further down.

Category	Type	Spectral B/W	Length	LAN Applications	Notes
Cat3	UTP	16 MHz	100m	10Base-T, 4Mbps	Now mainly for telephone cables
Cat4	UTP	20 MHz	100m	16Mbps	Rarely seen
Cat5	UTP	100MHz	100m	100Base-Tx,ATM, CDDI	Common for current LANs
Cat5e	UTP	100MHz	100m	1000Base-T	Common for current LANs
Cat6	UTP	250MHz	100m		Emerging
Cat7	ScTP	600MHz	100m		

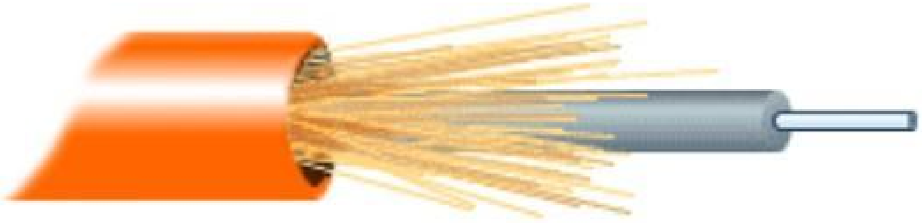
Shielded twisted pair (STP):

It is similar to UTP but has a mesh shielding that's protects it from EMI which allows for higher transmission rate. 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).

Fiber Optic Cable:

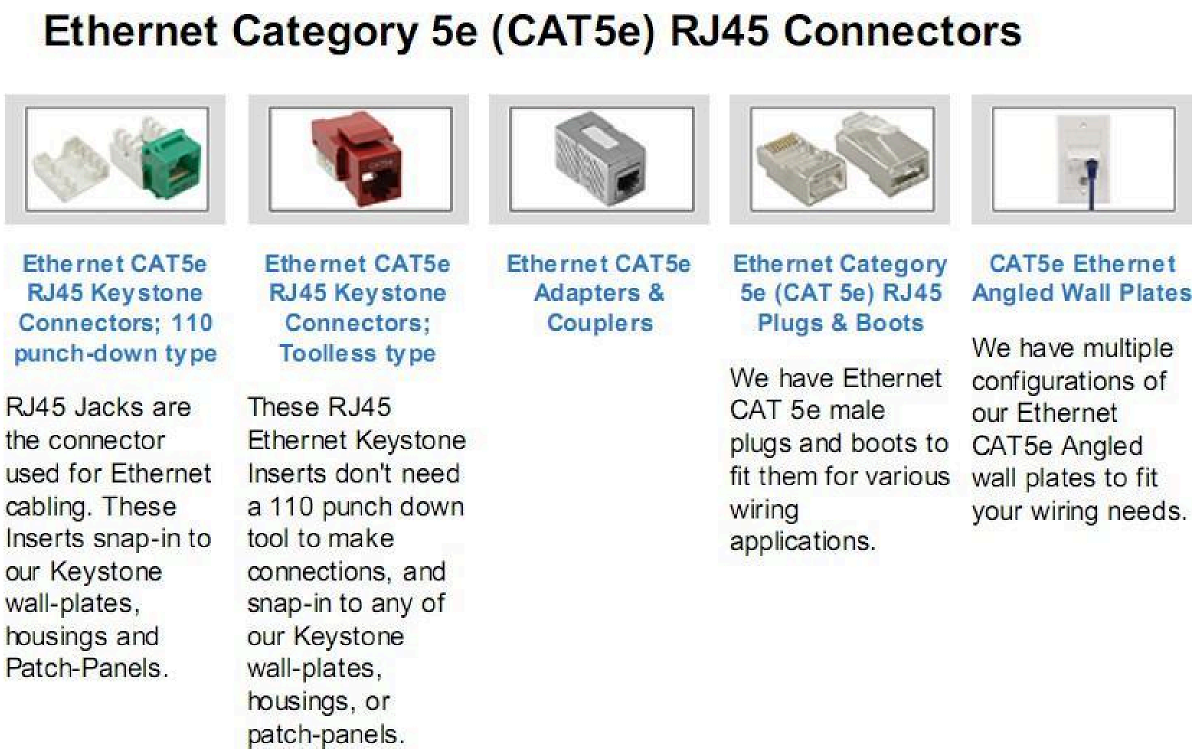
Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. 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 center core of fiber cables is made from glass or plastic fibers. 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.



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.

Connectors:



Ethernet Category 5e (CAT5e) RJ45 Connectors

Ethernet CAT5e RJ45 Keystone Connectors; 110 punch-down type

RJ45 Jacks are the connector used for Ethernet cabling. These Inserts snap-in to our Keystone wall-plates, housings and Patch-Panels.

Ethernet CAT5e RJ45 Keystone Connectors; Toolless type

These RJ45 Ethernet Keystone Inserts don't need a 110 punch down tool to make connections, and snap-in to any of our Keystone wall-plates, housings, or patch-panels.

Ethernet CAT5e Adapters & Couplers

Ethernet Category 5e (CAT 5e) RJ45 Plugs & Boots

We have Ethernet CAT 5e male plugs and boots to fit them for various wiring applications.

CAT5e Ethernet Angled Wall Plates

We have multiple configurations of our Ethernet CAT5e Angled wall plates to fit your wiring needs.

RJ-45 connector

Crossover Cables vs Straight Through Cables:

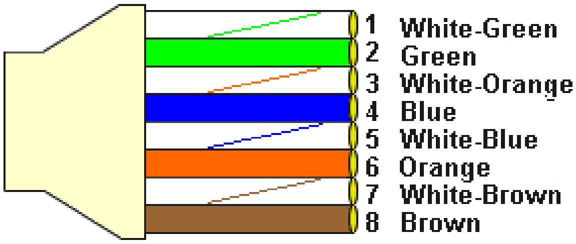
Ethernet patch cables can be wired in three different ways; the two main ways are called straight through and crossover. The third type is called rolled and has only specialized applications.

Generally speaking, straight through cables are used to patch between different types of equipment; for example, PCs to a hub. Conversely, crossover cables are generally used to patch between similar types of equipment; a PC to another PC for example Inside the UTP patch cable there are 8 physical wires although the network only uses 4 of them. The 8 wires are arranged in what's known as pairs and one pair is used to send information whilst the other pair is used to receive information.

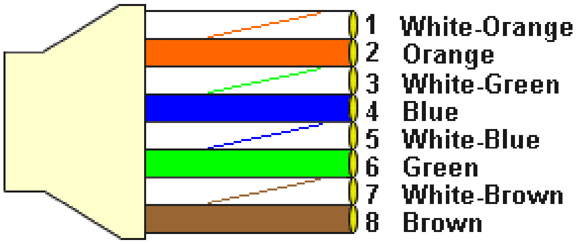
On a PC, the pair on pins 1 and 2 of the connector send information, while the pair on pins 3 and 6 receive the information. To make PCs talk to each we therefore need to connect the send pair of one PC to the receive pair of the other PC (and vice-a-versa). That means we need a crossover cable. If we used a straight through cable the both be listening on the one pair - and hearing nothing, and sending on the one pair - achieving nothing.

Color Codes

The standards say that Ethernet connectors should be cabled with specific colors on specific pins. There are two standard layouts - if a cable has the same layout on both ends it's a straight through cable. If a cable has one layout on one end and the other layout on the other end then it's a crossover cable. Whilst not universal, the color codes shown below are generally used on professional cables.



568A CABLE END



568B CABLE END

If a cable has 568A color wiring on both ends then it's a straight through cable

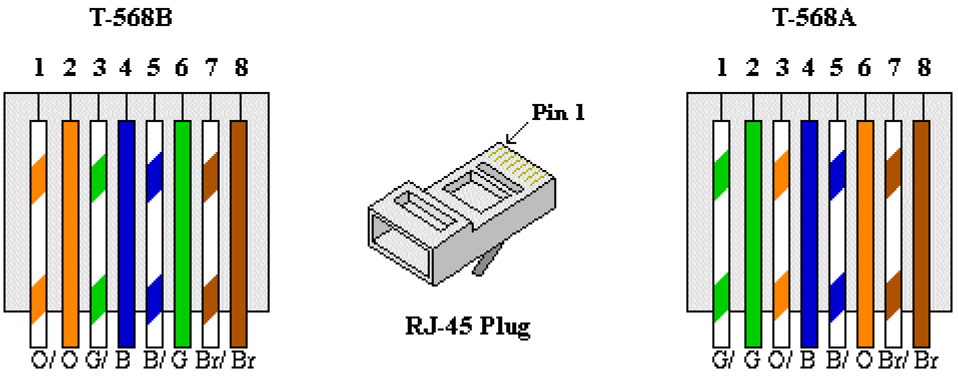
If a cable has 568B color wiring on both ends then it's also a straight through cable.

If a cable has 568A color wiring on one end and 568B color coded wiring on the other end, then it's a crossover cable.

Color Codes for RJ-45 Ethernet Plug :

Eight-conductor data cable (Cat 3 or Cat 5) contains 4 pairs of wires. Each pair consists of a solid color wire and a white and color striped wire. Each of the pairs are twisted together

The pairs designated for 10BaseT Ethernet are orange and green. The other two pairs, brown and blue, are unused. The connections shown are specifically for an RJ45 plug. The wall jack may be wired in a different sequence because the wires may be crossed inside the jack. The jack should either come with a wiring diagram or at least designate pin numbers that you can match up to the color code below.



There are two wiring standards for these cables, called T-568A and T-568B. They differ only in pin assignments, not in uses of the various colors. The illustration above shows both standards. With the T-568B specification the orange and green pairs are located on pins 1, 2 and 3, 6 respectively. **The T-568A specification reverses the orange and green connections, so that the blue and orange pairs are on the center 4 pins, which makes it more compatible with the telco voice connections**.

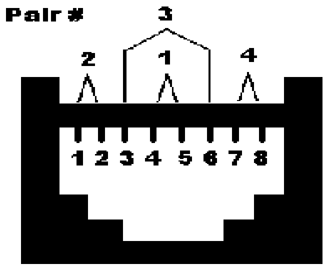
T-568A is supposed to be the standard for new installations, and T-568B is the alternative. However, most off-the-shelf data equipment and cables seem to be wired to T568B.

Pin Number Designations

Here are the pin number designations for both standards:

T-568B

Pin	Color	Pair	Descrtipion
1	white/orange	2	TxData +
2	orange	2	TxData -
3	white/green	3	RecvData +
4	blue	1	Unused
5	white/blue	1	Unused
6	green	3	RecvData -
7	white/brown	4	Unused
8	brown	4	Unused

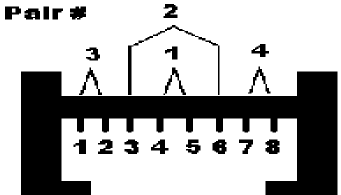


EIA/TIA 568B

T-568A

Pin	Color	Pair	Description
1	white/green	3	RecvData +
2	green	3	RecvData -
3	white/orange	2	TxData +
4	blue	1	Unused
5	white/blue	1	Unused
6	orange	2	TxData -
7	white/brown	4	Unused
8	brown	4	Unused

Note: Odd pin numbers are always the striped wires.



Exercise: To make Straight through and Cross over UTP cable with RJ-45 Connector and test it with Cable Tester.

Suggested Reading:

1. Computer Networks, by Andrew S. Tanenbaum, Fourth edition, section 2.2 – An introduction to various physical media
2. http://hubpages.com/hub/Data-Communication
3. http://www.solutionsandsystems.com/Wiring%20&%20Cable%20Color%20Scheme.htm
4. *highiqsolutions.com/**Wiring**%20&%20**Cable**%20**Color**%20**Scheme**.pdf*

Sample Questions:

Q1. How twists in twisted pair give an advantage over coaxial cable? On what factors no. of twist depends?
Q2. Briefly, discuss about connectors available for coaxial cable and optical fiber?
Q3. List down different uses and applications of Coaxial cable?
Q4. Study about different types of networks: MAN, WAN, PAN, CAN, SAN, TAN?

To Submit: Prepare a log book for all the things done in the network lab. Complete log book with the answers for the above questions

Lab-02-B

Aim: To configure LAN and perform Static Routing

Theory:

Internetworking devices:

1. **NIC(Network Interface Card)**

A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses**.**

2. **Hub**

A network hub contains multiple ports. When a packet arrives at one port, it is copied unmodified to all ports of the hub for transmission. The destination address in the frame is not changed to a broadcast address. It works on the Physical Layer of the OSI model.

3. **Switch**

A network switch is a device that forwards and filters OSI layer 2 datagrams (chunk of data communication) between ports (connected cables) based on the MAC addresses in the packets, is distinct from a hub in that it only forwards the frames to the ports involved in the communication rather than all ports connected. A switch breaks the collision domain but represents itself as a broadcast domain. Switches make forwarding decisions of frames on the basis of MAC addresses. A switch normally has numerous ports, facilitating a star topology for devices, and cascading additional switches.

4. **Router**

A **router** is a device that interconnects two or 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.

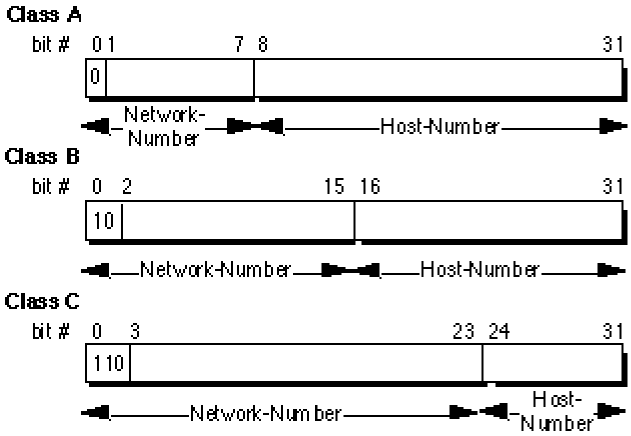
A router is a networking device whose software and hardware are customized to the tasks of routing and forwarding information. A router has two or more network interfaces, which may be to different physical types of network (such as copper cables, fiber, or wireless) or different network standards. Each network interface is a small computer specialized to convert electric signals from one form to another.

IP Address and Hostname:

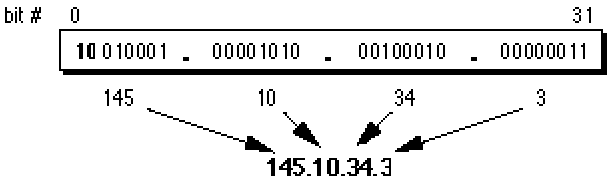
In the Internet, machines are identified by what are known as IP addresses. It is a 4-byte address, and obviously unique for each machine. Since the Internet is a collection of networks, the IP address is composed of two parts.

1. A network part – that identifies which network within the Internet
2. A host part – that identifies which host within the network

   It was foreseen that all networks would not be of the same size, some would consist of a maximum of hundred machines, while others may require capability to accommodate tens of thousands. To cater to this demand, different classes of addresses were constructed. The important ones are classes A, B, and C. An address is identified as belonging to a particular class based on the following:

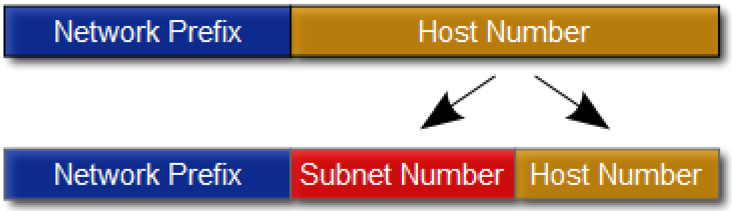


The IP address read as a 4-byte number would appear too big and cumbersome to remember, so the "dotted-decimal" notation is used for reading and writing. In this notation, the 32-bit IP address is divided into 4 8-bit fields and the values are read in the decimal form, each value separated by a dot from the other.



Even though this is in a fairly human-readable form, remembering the IP addresses of hundreds of machines is not entirely easy, that is why hostnames were introduced. A machine is given a name (human-readable) and people can refer to it with this name. The name to address translation has to happen at some point, since the communication at the lower level is always in terms of addresses and not names.

Subnetting: A subnetwork, or subnet, is a logically visible, distinctly addressed part of a single Internet Protocol network. The process of subnetting is the division of a computer network into groups of computers that have a common, designated IP address routing prefix.



Subnetting breaks a network into smaller realms that may use existing address space more efficiently, and, when physically separated, may prevent excessive rates of Ethernet packet collision in a larger network. The subnets may be arranged logically in a hierarchical architecture, partitioning the organization's network address space (see also Autonomous System) into a tree-like routing structure.

Routers are used to interchange traffic between subnetworks and constitute logical or physical borders between the subnets. They manage traffic between subnets based on the high-order bit sequence (routing prefix) of the addresses. A routing prefix is the sequence of leading (most-significant) bits of an IP address that precede both the portion of the address used as host identifier and, if applicable, the set of bits that designate the subnet number In IPv4 networks, the routing prefix is traditionally expressed as a subnet mask, which is the prefix bit mask expressed in quad-dotted decimal representation. For example, 255.255.255.0 is the subnet mask for the 192.168.1.0/24 prefix. All hosts within a subnet can be reached in one routing hop, implying that all hosts in a subnet are connected to the same link**.**

Basic commands for Linux Networking

This section will explain some of the basic commands needed for networking in Linux.

1) ***man***- This command is used to display the text manual for Linux. Manual pages for the Linux commands can be viewed by entering the command man followed by the name of the option.

Syn: ***man*** [command]

2) ***ping***- This command is used to check if a particular device on the network is reachable. Ping stands for Packet Internet Groper.

Syn: ***ping*** [address]

3) ***Ifconfig***-This command is used to report all of the network devices recognized and running on the system.

Syn: ***ifconfig***

This command can be also used to change the IP address and assign a network mask

Syn: ***ifconfig*** [cardname] [address] **netmask** [mask id]

Eg: ***ifconfig*** eth0 192.168.12.1 netmask 255.255.255.0

4) ***route***-This command is used to view the routing table.

Syn: ***route***

This command can also be used to add a new route to the routing table

Syn: ***route*** add [dest.IP] gw [ip address]

Eg: ***route*** add 192 .168.0.1 gw 10.100.68.1 #adds a route to 192.168.0.1 through the gateway 10.100.68.1

In order to add a default route we can use the default keyword along with the route command

Syn: ***route*** add default gw [ip address]

Aim: To setup a Local Area Network with 3 computers where each machine is in a same network

Exercise 1

Connect three machines to a switch and see if they recognize each other using various classes of IP addresses and their respective default subnet mask.

Table shows the scheme of IP addresses to be followed:

Host name	Address Class	IP address	Default Subnet Mask
PC X	Class A	10.0.0.X	255.0.0.0
PC X	Class B	172.1.0.X	255.255.0.0
PC X	Class C	192.168.10.X	255.255.255.0

Where X = PC number

To do:

- Network configurations to be done like setting up the IP address for a machine.
- The IP addresses given to the machines should belong to the same class.
- Ping after connection to see if the nodes in the network can communicate with each other.
- Repeat the necessary steps for all classes of network you make.

Output:

- Steps followed to set up the above configuration.
- Name of the file(s) you have modified (if any).
- Note the modification(s) (if any) done to the file(s).
- The necessary tests that you performed to check if the nodes communicate.

Resources: 3 computers, 1 Switch, data cables

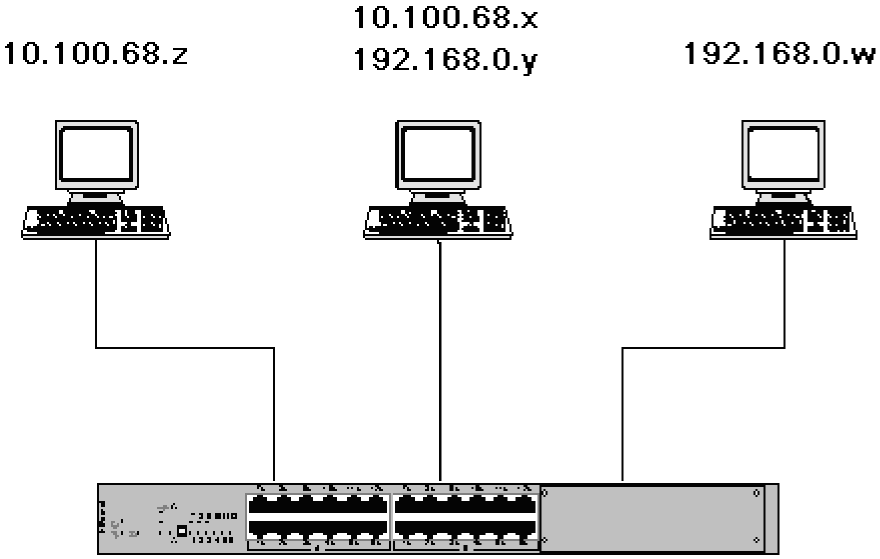
Exercise 2

To create two different class C networks

To do:

1. Start with the Terminal .
2. Configure using the “ifconfig” command, the ip addresses of the computers to reflect the machines in two different LANs.
3. Machine with 2 NICs will have both the IP addresses, one for each card. Thus, as a machine, it will be on both the networks.

(Note: Same figure to be used for exercise 1 and 2)



Output:

1. On pinging the machine on one network to the machine on another network should give the “network unreachable” error.
2. “route” command output should show only two entries on other machines and 3 entries on machine with two NIC cards.

Exercise 3

To make both machines on same networks talk/ ping with each other. This will be the temporary change and will not be effective once the system is rebooted.

To do:

1. Change the ip address of the machines temporarily using commands (As per instruction).
2. Ping the devices and check if they are able to reach each other.

Output:

1. One should be able to ping two machines from each other.

Exercise 4

To learn how to make changes for the address setting to be permanent. To learn about the different options which can be set through the file /etc/sysconfig/network-scripts? (This exercise is similar to Exercise 2 but the only change is we are trying to change the addresses permantly)

Must Do : Create a copy of the file /etc/sysconfig/network-scripts somewhere in your system and at last again use to change the configuration to initial one.

Exercise 5

To learn how to send messages from one machine to another using netcat. Using the static address that we have created, we should be able to message other machines using the same active port.

To do:

1. Use the nc command, communicate with each other.

Output:

To show the output of the messages that you were able to send to eachother.

Exercise 6

Use a switch to try to measure the performance of the LAN by sending file from one machine to the other machine using FTP(max throughput, delay, packet loss rate etc. as a function of total traffic and other relevant parameters) for the switched LAN.

Output:

1. The performance measure obtained for switch should be compared graphically or in the tabular form.
2. Reason out why the particular measurements are obtained.

Sample Questions:-

Q.1 What is MAC address? Give its structure and at which layer MAC address are used?

Q.2 When MAC address exist then what is the requirement of IP addresses?

Q.3 Is IP address really unique?

Q.4 What do you mean by classful and classless addressing?

Q.5 What is the relation between Ping and ICMP?

Q.6 What do you mean by Subnet mask? What are the default subnet mask for class A, B and C?

Q.7 Analyze the time difference between RTT of more than one Ping command's output and why it happens?

Q.8 Analyze the difference between time effects of Ping Command, results from Hub and Switch?

Suggested reading:

1] Linux Network Administrator’s guide, Olaf Kirch, 2nd edition, O’Reilly Publishers

[2] TCP/IP Network Administration, Craig Hunt, 3rd edition, O’Reilly Publishers

[3] Subnetting/Supernetting and Classless Addressing, Tata McGraw hill.

[4] Linux Manual Pages