UNIVERSITY OF CHAKWAL
DEPARTMENT OF COMPUTER SCIENCE
(Computer Communication Networks CS-324)

Lab 01

Basic Introduction

Pre-Requisites for Lab

- Basic knowledge of computer

Objectives:

- Introduction to Network cables and devices

- Introduction to IP addressing

- Set IP addresses and subnet mask to and use basic utilities used for IP addressing.

1.1 Network Cables

There are many types of network cables used in the real-world applications. Some of them are given below:

1. **Unshielded twisted pair:** As the name indicates, the wires are twisted with one another and there is no shield.
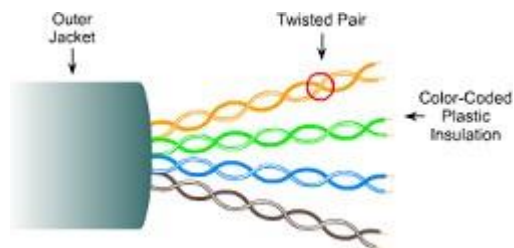

Figure 1.3: Unshielded twisted pair cable.

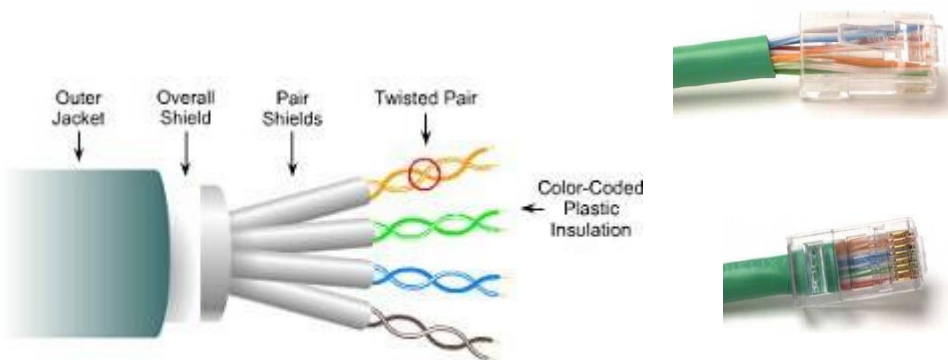2. **Shielded twisted pair:** Shield with twisted pair.

Figure 1.4: Shielded twisted pair cable.

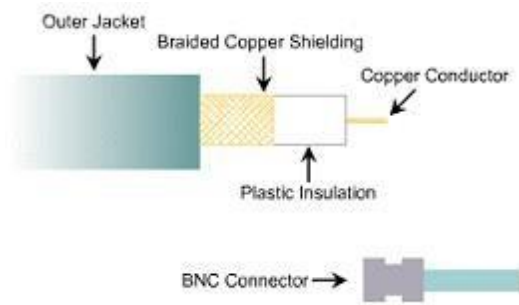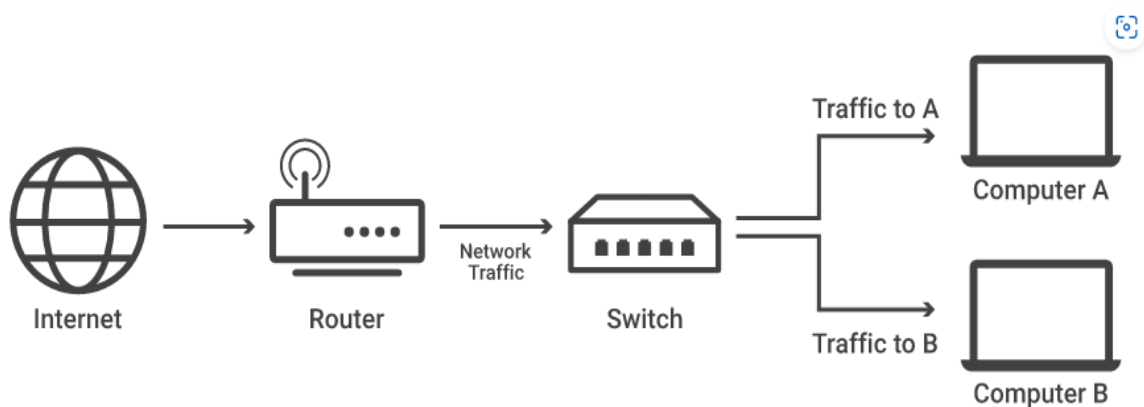3. **Coaxial cable:** Similar to our cable TV cables.

Figure 1.5: Coaxial Cable.

1.2 Introduction to network devices:

1.2.1 Network Switch:

A network Switch connects existing 10/100 Mbps devices like NICs etc. We can combine it with any other standard switch as our network grows. A network switch can have 4, 8, 16, 24 or 32 connection ports.

A network switch has the following hardware features:

1. There are 24 Fast Ethernet auto-negotiating 10Base-T/100Base-TX ports.

2. Connect two units back-to-back using a single Cable

3. Port status LEDs that show status of each port on the switch.

The front view of a switch along with various LED information is provided below:
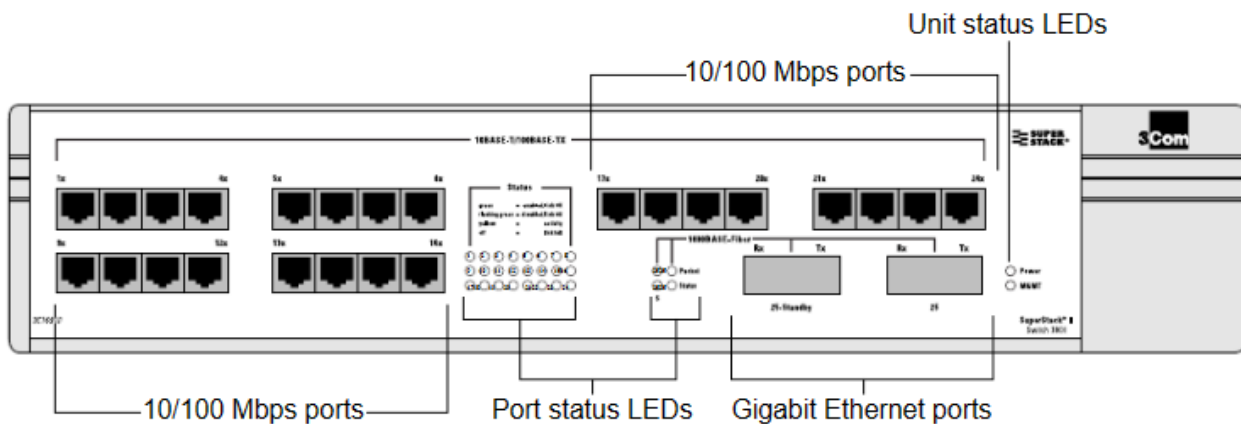
Figure 1.6: Front view of 3COM switch.

1.2.2 Routers

The front view of router has LEDs, that indicates the following:

1. Power: Indicates the router's operating status. Comes on when power is supplied to the router and the router is operational.

2. RPS [Redundant Power System]: Off—No RPS is attached; On—RPS is attached and operational; Blinking—RPS is attached, but has a failure.

3. Activity: Off—In the Cisco IOS software, but no network activity; Blink (500 ms ON, 500 ms OFF)—In ROMMON, no errors; Blink (500 ms ON, 500 ms OFF, 2 seconds between codes)— In ROMMON, error detected; Blink (less than 500 ms)—In the Cisco IOS software, the blink rate reflects the level of activity.

The back view of our router: The router has serial and fast Ethernet ports. These ports are mostly used for data transfer. It has console and auxiliary ports, which are used for management purposes.
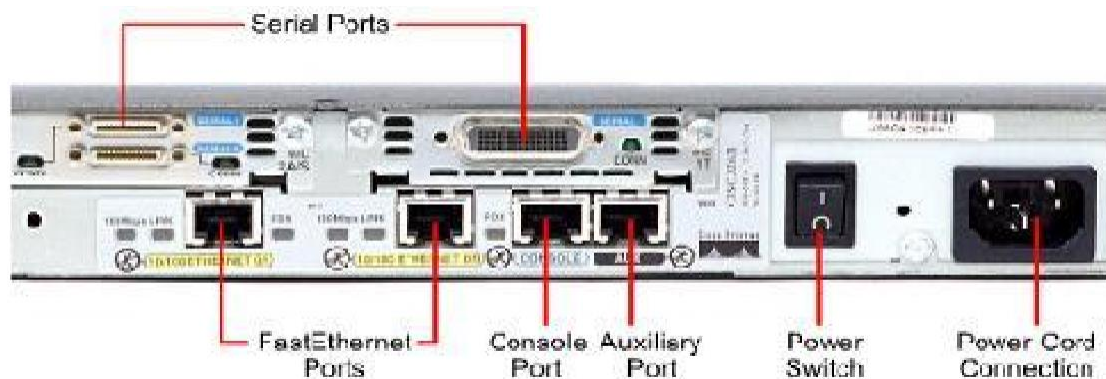
Introduction to IP Addressing

Each Network Interface Card (NIC or Network card) present in a PC is assigned one Network address called **as IP address** [or Network address]. This IP address is assigned by the **administrator of the network**. No two PCs can have the same IP address. IP address is **32bits or 4 bytes.**

There is a burned-in address on the NIC called as Physical Address [or **MAC address or Hardware address**]. The MAC address of a network card indicates the vendor of that card and a unique serial number.

2.1   Rules of IPv4 addressing

1. Format of IP address

2. IPv4 is made up of four parts, in the pattern as w.x.y.z. Each part has 8 binary bits and the values in decimal can range from 0 to 255.

IP address classes

1. IP addresses are divided into different classes. These classes determine the maximum number of hosts per network ID. Only three classes are actually used for network connectivity. The following table lists all of the address class.

IP address class	First Octet Value
Class A	0-127 (127 is loopback address)
Class B	128-191
Class C	192-223
Class D	224-239
Class E	240-255

2. Grouping of IP addresses into different classes.

   a) Class A, B, C, D, E

   b) Class A

      i. 0.0.0.0 to 127.255.255.255

      ii. **First 8 bits** are used for network part and the remaining for host part.

      iii. **127** is loopback address to test whether your NIC is working properly

      iv. **0** is invalid address

   c) Class B

      i. 128.0.0.0 to 191.255.255.255

      ii. **First 16 bits** for network part and remaining host part

   d) Class C

      i. 192.0.0.0 to 223.255.255.255

      ii. **First 24 bits** for network part and last 8 bits for host part.

   e) Class D

      i. 224.0.0.0 to 247.255.255.255

      Used for **multicast**

   f) Class E: future use or experimental purposes.
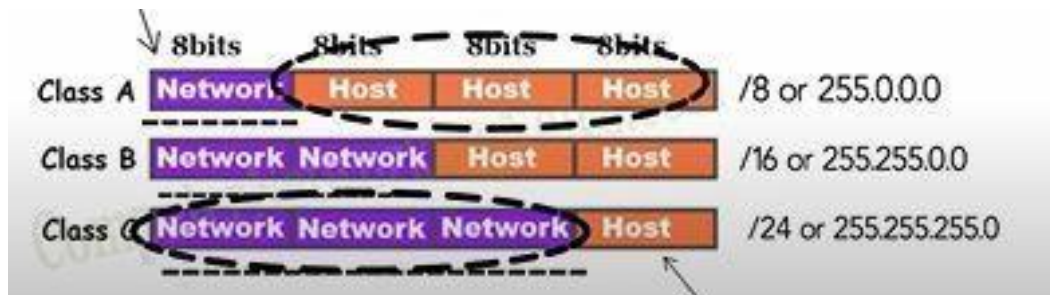
Consider the following IP addresses:

- **10.50.120.7** – because this is a Class A address, the first number (10) represents the network part, while the remainder of the address represents the host part (50.120.7). This means that, in order for devices to be on the same network, the first number of their IP addresses has to be the same for both devices. In this case, a device with the IP address of **10.47.8.4** is on the same network as the device with theIP address listed above. The device with the IP address 11.5.4.3 is not on the same network, because the first number of its IP address is different.

- **172.16.55.13** – because this is a Class B address, the first two numbers (172.16) represent the network part, while the remainder of the address represents the host part (55.13). A device with the IP address of **172.16.254.3** is on the same network, while a device with the IP address of 172.55.54.74 isn't.

3. **Default Subnet mask**

It is used to identify the network part from the host part. Put binary one for the parts that represent network part and zero for the part that represent host part.

   a. Class A: 255.0.0.0

   b. Class B: 255.255.0.0

   c. Class C: 255.255.255.0

   d. We can't have mix of 1s and 0s in subnet mask. Only consecutive 1s is followed by consecutive 0s

4. Invalid IP address.

   a. If the **network part is all 0s**, the address belongs to class A. But this is an invalid ip address because for an ip address all the network or host part should not be all 1s or all 0s.

      i. **0.0.0.0 is not valid**. Routers use it internally.

   b. If the **network part is all 1s**, this address belongs to class E. But due to presence of all 1s, it is not valid. This represent broadcast to all networks.

      i. **255.255.255.255** is not valid.

If the host part is all 0s, this represents network address. This is not a valid ip address.

If the host part is all 1s, this represents broadcast address. This is not a valid ip address.

We can't use the ip address represented within private address range as part of public ip address.

Class A: **10**.0.0.0 to 10.255.255.255

Class B: **172**.16.0.0 to 172.31.255.255

Class C: **192**.168.0.0 to 192.168.255.255

127.0.0.0 network address is used for loop-back testing. This will help you to check the network card of your own PC [localhost].

The validity of the IP address is also based on the subnet mask used provided.

Default subnet masks for standard IP address classes

UNIVERSITY OF CHAKWAL
DEPARTMENT OF COMPUTER SCIENCE
(Computer Communication Networks CS-324)

The following table lists the default subnet masks for each available class of

TCP/IP networks.

Address Class	Bits for Subnet Mask	Subnet Mask
Class A	11111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

UNIVERSITY OF CHAKWAL
DEPARTMENT OF COMPUTER SCIENCE
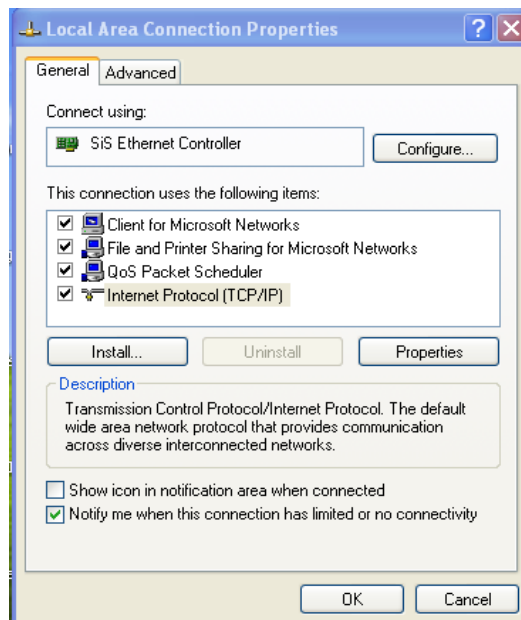**(Computer Communication Networks CS-324)**

Exercises for lab

Exercise 1:

Students are required to configure static IP address and subnet mask to network computer. The steps to assign IP address are:

1. Right click on My Network Places icon present at desktop.

2. Click on Properties

3. Right click on local area network connection

4. Local area connection properties will be opened.

5. Double click on Internet Protocol (TCP/IP)

6. Select use the following IP address radio button

Exercise 2:

1. Write the address class next to each IP address.

Address	Class
131.107.2.89	
3.3.57.0	
200.200.5.2	
191.107.2.10	
127.0.0.1	

UNIVERSITY OF CHAKWAL
DEPARTMENT OF COMPUTER SCIENCE
(Computer Communication Networks CS-324)

2. Identify invalid IP address: Circle the portion of the IP address that would be invalid if it were assigned to a host, and then explain why it is invalid.

1. 131.107.256.80

2. 222.222.255.222

3. 231.200.1.1

4. 126.1.0.0

5. 0.127.4.100

6. 190.7.2.0

7. 127.1.1.1

8. 198.121.254.255

9. 255.255.255.255