VALIA COLLEGE
ANDHERI (WEST)

PRESENTS,

Computer Networks Practical

S.Y.B.Sc. I.T. – SEM III

9029120671 / 7021047199

Mumbai University | Course Code: USIT3P3

List of Practical:	
1.	**Colour code for crimping LAN (Cat 5/6/7) cable**
a.	Study of Different color codes
b.	Study of different connecting devices and their differences
c.	Crimping LAN Cable
2.	**Configuring LAN setup**
a.	Planning and Setting IP networks
b.	Configuring subnet
c.	Study of basic network command and Network configuration commands. ipconfig, netstat, ARP, ping, trace route etc.
d.	Basic network troubleshooting.
e.	Configuration of TCP/IP Protocols in Windows / Linux.
f.	Implementation of Drive/file sharing and printer sharing.
3.	**IPv4 Addressing and Subnetting**
a.	Given an IP address and network mask, determine other information about the IP address such as: • Network address • Network broadcast address • Total number of host bits • Number of hosts
b.	Given an IP address and network mask, determine other information about the IP address such as: • The subnet address of this subnet • The broadcast address of this subnet • The range of host addresses for this subnet • The maximum number of subnets for this subnet mask • The number of hosts for each subnet • The number of subnet bits • The number of this subnet
4.	**Designing and configuring a network topology**
a.	Configure IP static routing

5.	Configure IP routing using RIP.
6.	Configuring Simple and multi-area OSPF.
7.	**Configuring server and client.**
a.	Configure DHCP
b.	Configure DNS
c.	Configure HTTP
d.	Configure Telnet
e.	Configure FTP
8.	Configure basic security features for networks
9.	Packet capture and header analysis by wire-shark (TCP, UDP, IP etc.)
10.	**Planning and Design a corporate network for a given scenario.**

Introduction

Networking: Networking is a **connection** that has been established between devices through a transmission media, so that they can communicate to each other to share information and resources.

Host: All devices to which IP address can be assign in networking.

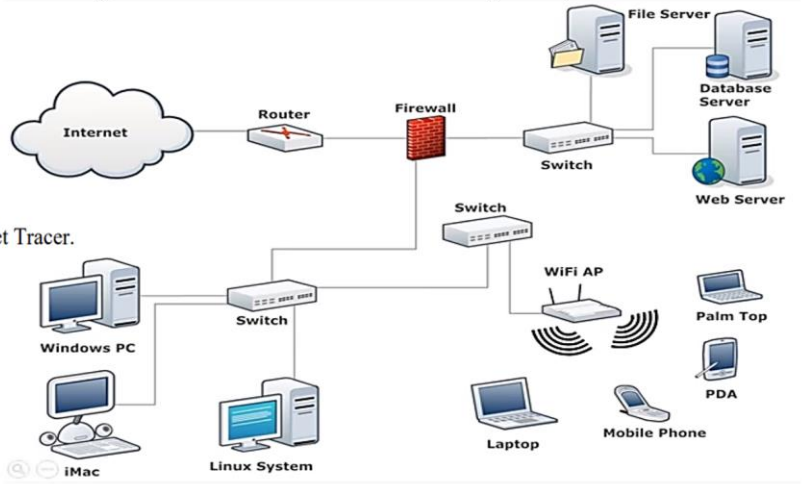
Subnetting: Dividing a large network into a smaller network is known as subnetting i.e. taking bits from host portion to the network portion. It is use to reduce the wastage of IP address. When we subnetted the given IP, it is called Classless IP Address.

Hardware Requirement

RJ-45 connector,
Climping Tool,
Twisted pair Cable

Software Requirement

Command Prompt And Packet Tracer.



Subnet Mask: To separate 32 bits IP address into the network prefix & the host number. It defines which portion is of Network and which is of Host.
Subnet: A subnet (subnetwork) is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same LAN.

Classes in IP Address:

Class	IP Address	Subnet
Class A	1 – 126*	N-H-H-H
Class B	128 – 191	N-N-H-H
Class C	192 – 223	N-N-N-H
Class D	224 – 239	N-N-N-N (Multicasting)
Class E	240 – 255	H-H-H-H (R & D)

Note: 127.0.0.1 to 127.255.255.255 is used for self-pinging or loop-back testing. It used for testing purposes like client-server architecture.

Network Address: If all bits in the host portion is 0's than it is known as Network Address.
For e.g. 172.45.84.15 (Belong to class B: 255.255.0.0); therefore Network Address is 172.45.**0.0**

Broadcast Address: If all bits in the host portion is 1's than it is known as Broadcast Address
For e.g. 172.45.84.15 (Belong to class B: 255.255.0.0); therefore Broadcast Address is 172.45.**255.255**

Private IP Address / Un-registered Addresses / Free of Cost Addresses:
It is non-routable IP Addresses
Class A – **10**.0.0.0 to **10**.255.255.255 (1 Network free)
Class B – 172.**16**.0.0 to 172.**31**.255.255 (16 Network free)
Class C – 192.168.**0**.0 to 192.168.**255**.255 (256 Network free)

Calculation:
1. **Class A (8 bit):**
   No. of Network = $2^7 - 2 = 128 - 2 = 126$
   No. of Host = $2^{24} - 2 = (2^{10} \times 2^{10} \times 2^4) - 2 = 1024x1024x16 - 2 = 16777216 - 2 = 16777214$
2. **Class B (16 bit):**
   No. of Network = $2^{14} - 2 = 16384 - 2 = 16382$
   No. of Host = $2^{16} - 2 = 65536 - 2 = 65534$
3. **Class C (24 bit):**
   No. of Network = $2^{21} - 2 = 2097152 - 2 = 2097150$
   No. of Host = $2^8 - 2 = 256 - 2 = 254$

Practical 1 Colour code for crimping LAN (Cat 5/6/7) cable

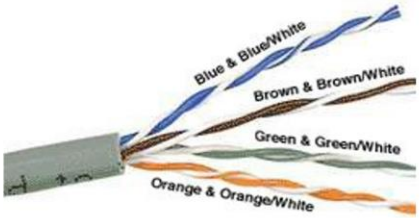
a. Study of Different color codes

AIM: Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using clamping tool.

About the Cable:

You can find bulk supplies of ethernet cable at many computer stores or most electrical or home centers. You want UTP (Unshielded Twisted Pair) ethernet cable of at least Category 5 (Cat 5). Cat 5 is required for basic 10/100 functionality, you will want Cat 5e for gigabit (1000BaseT) operation and Cat 6 or higher gives you a measure of future proofing. You can also use STP (Shielded Twisted Pair) for extra resistance to external interference but I won't cover shielded connectors. Bulk ethernet cable comes in many types, there are 2 basic categories, solid and braided stranded cable. Stranded ethernet cable tends to work better in patch applications for desktop use.

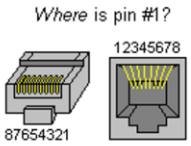
It is more flexible and resilient than solid ethernet cable and easier to work with, but really meant for shorter lengths. Solid ethernet cable is meant for longer runs in a fixed position. Plenum rated ethernet cable must be used whenever the cable travels through an air circulation space. For example, above a false ceiling or below a raised floor. It may be difficult or impossible to tell from the package or labeling what type of ethernet cable it is, so peal out an end and investigate.Here is what the internals of the ethernet cable look like:



Inside the ethernet cable, there are 8 color coded wires. These wires are twisted into 4 pairs of wires, each pair has a common color theme. One wire in the pair being a solid or primarily solid colored wire and the other being a primarily white wire with a colored stripe (Sometimes ethernet cables won't have any color on the striped wire, the only way to tell which is to check which wire it is twisted around). Examples of the naming schemes used are: Orange (alternatively Orange/White) for the solid colored wire and White/Orange for the striped cable. The twists are extremely important. They are there to counteract noise and interference. It is important to wire according to a standard to get proper performance from the ethernet cable. The TIA/EIA-568-A specifies two wiring standards for an 8-position modular connector such as RJ45. The two wiring standards, T568A and T568B vary only in the arrangement of the colored pairs. Tom writes to say "...sources suggest using T568A cabling since T568B is the AT&T standard, but the US Government specifies T568A since it matches USOC cabling for pairs 1 & 2, which allows it to work for 1/2 line phones...". Your choice might be determined by the need to match existing wiring, jacks or personal preference, but you should maintain consistency. I've shown both below for straight through cabling and just T568B for crossover cabling.

About Modular Connector Plugs and Jacks:

The 8P8C modular connectors for Ethernet are often called RJ45 due to their physical resemblance. The plug is an 8-position modular connector that looks like a large phone plug. There are a couple variations available. The primary variation you need to pay attention to is whether the connector is intended for braided or solid wire. For braided/stranded wires, the connector has sharp pointed contacts that actually pierce the wire. For solid wires, the connector has fingers which cut through the insulation and make contact with the wire by grasping it from both sides. The connector is the weak point in an ethernet cable, choosing the wrong one will often cause grief later. If you just walk into a computer store, it's nearly impossible to tell what type of plug it is. You may be able to determine what type it is by crimping one without a cable.



Ethernet Cable Pin Outs: There are two basic ethernet cable pin outs. A straight through ethernet cable, which is used to connect to a hub or switch, and a crossover ethernet cable used to operate in a peer-to-peer fashion without a hub/switch. Generally all fixed wiring should be run as straight through. Some ethernet interfaces can cross and un-cross a cable automatically as needed, a handy feature.

Apparatus (Components): RJ-45 connector, Climping 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 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT 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.

Diagram shows you how to prepare Cross wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Diagram shows you how to prepare straight through wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

UTP Cable Color Coding

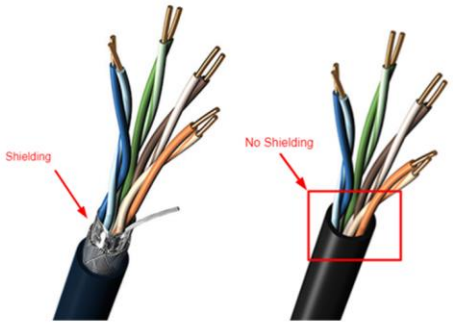
In the Un-Shielded Twisted Pair (UTP) cable, digital signal protection comes from the twists in the wire. The more twists per inch, the farther the digital signal can supposedly travel without interference. For example, categories 5 and 6 have many more twists per inch than category 3 UTP has. The Twists are given to the wire to reduce the Cross talk or interference to electrical signals.

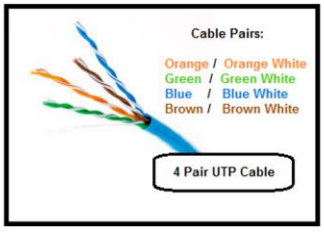
There are 4 twisted pairs with four different colored wires. Each colored wire is twisted with white wire with a strip of same color on it. For example, an Orange color twisted pair would a one wire of Orange color and one of while color with a strip of orange color on it.

Only Two pairs are used with cable numbers 1, 2, 3, and 6 for Tx and Rx signals. You would notice Tx+/Tx- and Rx+/Rx- terms in this blog while reading. + and - terms are the voltages. 10BaseT uses two different voltages i.e. +2.5V and -2.5V.

There are 3 types of cables

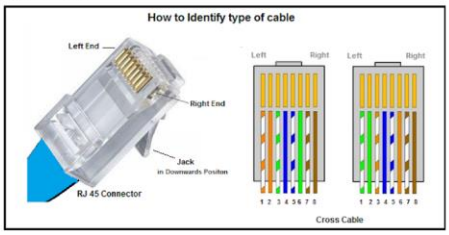
1. **Straight**
2. **Cross**
3. **Rollover or Console**

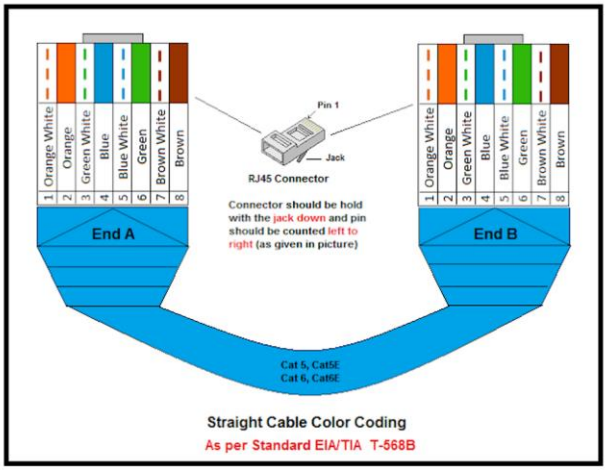




Identifying the Cable type

Hold both ends/RJ-45connectors of cable with their Jack in downward position. Now start matching the color coding from left pin of connector towards right. Below is example to identify a cross cable.





Straight Cable

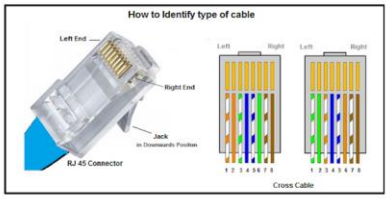
It is used to connect devices having different function. For example:

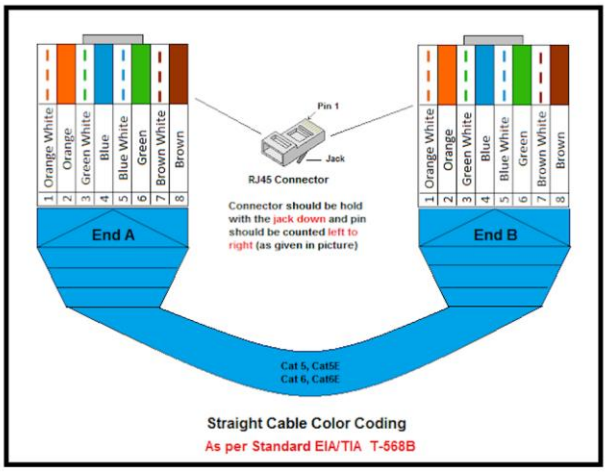
- Connecting a router to a hub or switch.
- Connecting a server to a hub or switch.
- Connecting workstations to a hub or switch.

Copyright © PROF. GUFRAN QURESHI

Identifying the Cable type

Hold both ends/RJ-45connectors of cable with their Jack in downward position. Now start matching the color coding from left pin of connector towards right. Below is example to identify a cross cable.





Straight Cable

It is used to connect devices having different function. For example:

- Connecting a router to a hub or switch.
- Connecting a server to a hub or switch.
- Connecting workstations to a hub or switch.

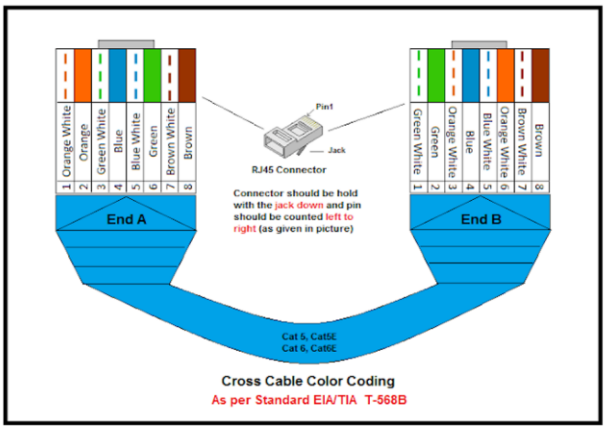
Left	1	Tx+		Rx+	1	Left
	2	Tx-		Rx-	2	
	3	Rx+		Tx+	3	
	4				4	
	5				5	
	6	Rx-		Tx-	6	
	7				7	
Right	8				8	Right

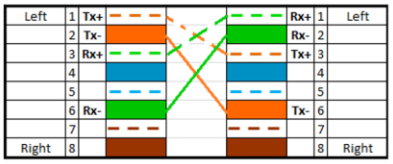
Straight Cable

Cross Cable

It is used to connect devices having same functions or roles. For example:

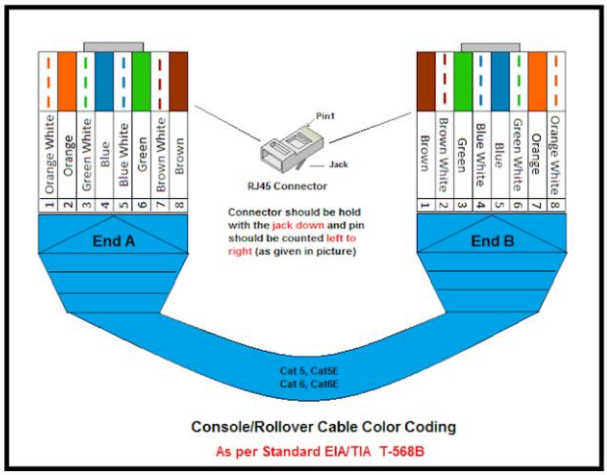
- Connecting uplinks between switches.
- Connecting hubs to switches.
- Connecting a hub to another hub.
- Connecting PC to PC
- Connecting PC to a Router
- Connecting 2 routers together without a hub or a switch.





Console or Rollover cable

It is used for device configuration. For example you have bought a new router and what to configure it with initial config. You need a console cable for same. One end of console cable is connected to console port of the router or a switch and other end would be connected to NIC port of your laptop or PC. Below is the color coding of Console cable. The color coding of both ends are totally reversed.



Practical 1 Colour code for crimping LAN (Cat 5/6/7) cable

b. Study of different connecting devices and their differences

AIM: Study of following Network Devices in Detail

- **Repeater**
- **Hub**
- **Switch**
- **Bridge**
- **Router**
- **Gate Way**

Apparatus (Software): No software or hardware needed.

Procedure: Following should be done to understand this practical.

1. **Repeater:**Functioning at Physical Layer.A **repeater** is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. Repeater have two ports ,so cannot be use to connect for more than two devices

2. **Hub:** An **Ethernet hub**, **active hub**, **network hub**, **repeater hub**, **hub** or **concentrator** is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) 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.

3. **Switch:**A **network switch** or **switching hub** is a computer networking device that connects network segments.The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

4. **Bridge:** A **network bridge** connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term *bridge* formally means a device that behaves according to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports. *Switch* or *Layer 2 switch* is often used interchangeably with *bridge*.Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

5. **Router:** A **router** is an electronic 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.

6. **Gate Way:** In a communications network, a network node equipped for interfacing with another network that uses different protocols.
    - A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.
    - A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

Practical 1 Colour code for crimping LAN (Cat 5/6/7) cable

c. Crimping LAN Cable

AIM: Study of crimping cable with RJ45

Step 0) Slip on the RJ45 boot (optional)

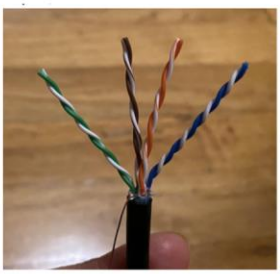
Step 1) Strip the cable

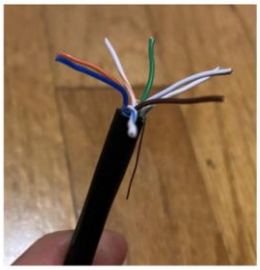
- Push the cable into the razor slot of the strip tool and turn it around the cable to make an even cut around the sheath. Careful not to nick the wires inside!
- Unwrap the blue foil shielding and plastic to uncover the twisted wire pairs.
- Push the copper grounding wire to the side. (Ignore the white string.)

Step 2) Organize the wires

In this step, you'll be taking the 8 colored wires inside the ethernet cable and putting them into the correct ordering of colors.

Note: This is the hardest part of crimping! The wires are small and are hard to control. Take your time and make sure you do this step correctly! Otherwise you might have to go back and restart.





Step 2.1) Untwist the wires

There should be 4 pairs of wires: green, brown, orange, and blue. Each pair has a solid-colored wire and a striped-colored wire. Untwist these pairs and separate them into the 8 wires.

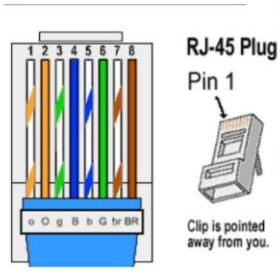
Step 2.2) Straighten out wires

After untwisting the wires, they are probably still kinked and look like they want to be twisted. In this step, you should carefully grab all the wires and try to straighten them out by pulling on them. This will prevent the wires from moving around later on.

Warning: Don't break off the wires!

Step 2.3) Lay out wires in order

With your straightened out wires, put them into the correct order! Make sure that the wires are all flat and in line with each other.



The ordering for these wires is:

1. Striped orange
2. Solid orange
3. Striped green
4. Solid blue
5. Striped blue
6. Solid green
7. Striped brown
8. Solid brown

Tip: After laying them out in order, straighten them out again as a group! This will help keep the wires together.

Step 2.4) Trim the wires

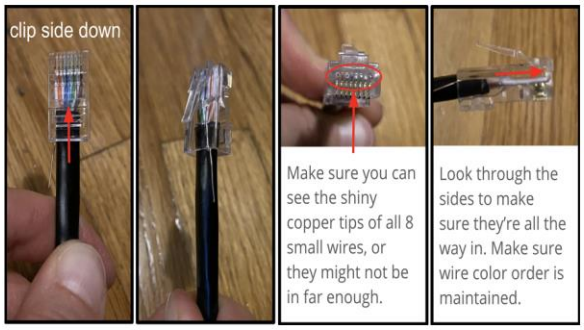
Trim the wires evenly to about 1/2 inch in length using scissors or the blade of your crimping tool. You want to make sure you have enough room for the wires to reach the end of the RJ45 connector. But also try to have room for the shielding of the cable to be inserted into the connector too.

Tip: You can put the wires side-by-side to the RJ45 connector to see how long you should cut it. Look at the next step to see what the final product looks like.

If you don't have the shielding inside of the connector, it makes it easier for the wires to snap off later, which is bad.

Make sure that you cut the wires evenly!

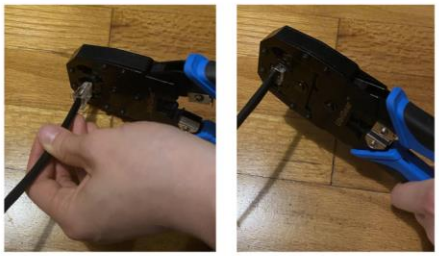
Step 3) Slide wires into RJ45 connector



Carefully slide your 8 wires into the connector. Make sure that the clip is facing away from you! If it is really hard to slide it into the connector, you probably didn't straighten out the wires enough in step 2.2 or 2.3.

Inserting the wires with the clip facing away from you is the standard. However, you could technically do it in 'reverse' and insert the wires with the clip facing you, as long as you do it on both ends of the cable. You shouldn't do this in practice though because others would get confused when looking at your cable.

Step 4) Crimp it



Push the RJ45 connector into the slot of your crimping tool for RJ45 connectors. The slot should be labeled something like "8P" for the 8-pin RJ45 connector that you're using.

In this step, you're doing the actual 'crimping' part and crimping/compressing/stabbing the 8 golden pins on the RJ45 connector into the 8 colored wires.

Tip: Squeeze as hard as you can! You need to make sure that all 8 pins are crimped.

Step 5) Test it

Slide the two pieces of the tester apart and plug each of the cable ends into either piece. Turn the switch to "On" or "Slow." If it's working, all 8 numbers should be flashing green.

If any of them are not showing green, it means something is wrong and you have to redo it! The RJ45 connector can't be reused once it's crimped, so you should just cut the end off and start back at step 1.

If everything is green, then you're done! If you had a cable boot, you can push the boots onto the RJ45 connector now.

Practical 2 Configuring LAN setup

a. Planning and Setting IP networks

AIM: Study of Network IP

As show in figure we teach how the ip addresses are classified and when they are used.

Classification of IP address

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved.

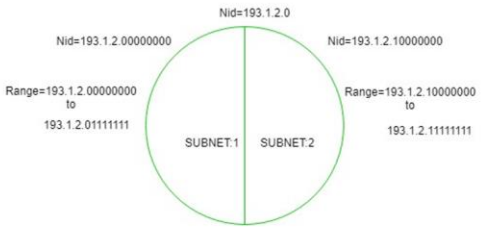
Subnetting:

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks. For example, if we consider a class A address, the possible number of hosts is 224 for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts.

Uses of Subnetting

- Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
- Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
- Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.
- Subnetting is used in increasing network security.

The network can be divided into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.
In the diagram, there are two Subnets.
Note: It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.



Supernetting:

Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.

Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols. More specifically,

- When multiple networks are combined to form a bigger network, it is termed super-netting
- Super netting is used in route aggregation to reduce the size of routing tables and routing table updates.

There are some points which should be kept in mind while supernetting:

1. All the Networks should be contiguous.
2. The block size of every network should be equal and must be in form of 2n.
3. First Network id should be exactly divisible by whole size of supernet.

Practical 2 Configuring LAN setup

b. Configuring subnet

AIM: Working of Subnet

The working of subnets starts in such a way that firstly it divides the subnets into smaller subnets. For communicating between subnets, routers are used. Each subnet allows its linked devices to communicate with each other. Subnetting for a network should be done in such a way that it does not affect the network bits.

In class C the first 3 octets are network bits so it remains as it is.

- **For Subnet-1:** The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.

Thus, the range of subnet 1 is: **193.1.2.0 to 193.1.2.127**
Subnet id of Subnet-1 is : 193.1.2.0
The direct Broadcast id of Subnet-1 is: 193.1.2.127
The total number of hosts possible is: 126 (Out of 128,
2 id's are used for Subnet id & Direct Broadcast id)
The subnet mask of Subnet- 1 is: 255.255.255.128

- **For Subnet-2:** The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111).

Thus, the range of subnet-2 is: **193.1.2.128 to 193.1.2.255**
Subnet id of Subnet-2 is : 193.1.2.128
The direct Broadcast id of Subnet-2 is: 193.1.2.255
The total number of hosts possible is: 126 (Out of 128,
2 id's are used for Subnet id & Direct Broadcast id)
The subnet mask of Subnet- 2 is: 255.255.255.128
The best way to find out the subnet mask of a subnet
is to set the fixed bit of host-id to 1 and the rest to 0.
Finally, after using the subnetting the total number of usable hosts is reduced from 254 to 252.

Note:

- To divide a network into four (22) parts you need to choose two bits from the host id part for each subnet i.e, (00, 01, 10, 11).
- To divide a network into eight (23) parts you need to choose three bits from the host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.
- We can say that if the total number of subnets in a network increases the total number of usable hosts decreases.

Along with the advantage, there is a small disadvantage to subnetting that is, before subnetting to find the IP address first the network id is found then the host id followed by the process id, but after subnetting first network id is found then the subnet id then host id and finally process id by this the computation increases.

Example 1: An organization is assigned a class C network address of 201.35.2.0. It uses a netmask of 255.255.255.192 to divide this into sub-networks. Which of the following is/are valid host IP addresses?

- 201.35.2.129
- 201.35.2.191
- 201.35.2.255
- Both (A) and (C)

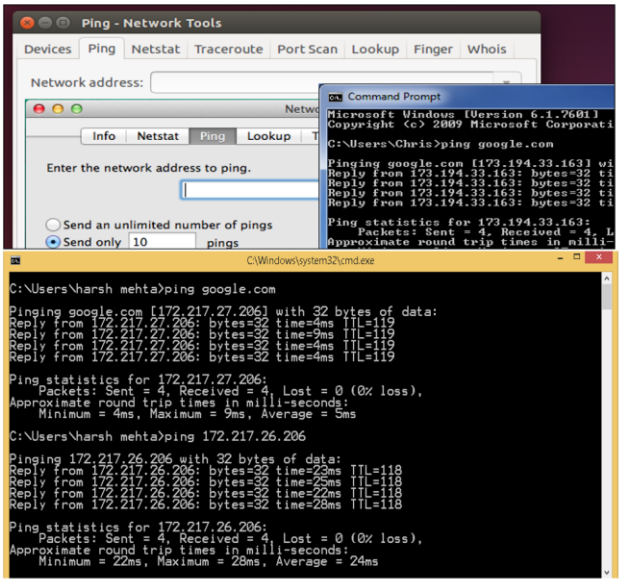
Solution:

Converting the last octet of the netmask into the binary form: 255.255.255.11000000
Converting the last octet of option 1 into the binary form: 201.35.2.10000001
Converting the last octet of option 2 into the binary form: 201.35.2.10111111
Converting the last octet of option 3 into the binary form: 201.35.2.11111111
From the above, we see that Options 2 and 3 are not valid host IP addresses (as they are broadcast addresses of a subnetwork), and OPTION 1 is not a broadcast address and it can be assigned to a host IP.

Practical 2c

AIM: Use of ping & tracert/traceroute, ipconfig/ifconfig, route & arp utilities

Tools like ping, traceroute, lookup, whois, finger, netstat, ipconfig, and port scanners are available on nearly every operating system you can get your hands on. They're used for everything from troubleshooting a connection to looking up information.



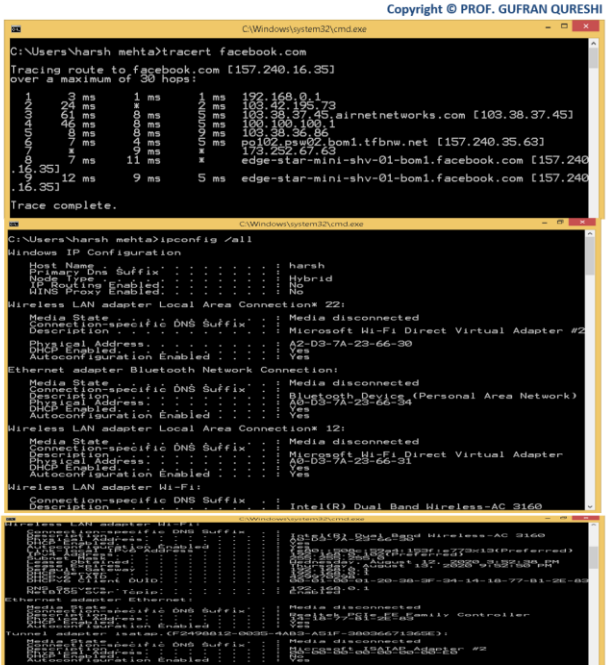
1. Ping

The ping command sends ICMP echo request packets to a destination. For example, you could run **ping google.com** or **ping 172.217.26.206** to ping a domain name or IP address.

These packets ask the remote destination to reply. If the remote destination is configured to reply, it will respond with packets of its own. You'll be able to see how long the round-trip time is between your computer and the destination. You'll see a "request timed out" message if packet loss is occurring, and you'll see an error message if your computer can't communicate with the remote host at all.

2. traceroute / tracert / tracepath

The traceroute, tracert, or tracepath command is similar to ping, but provides information about the path a packet takes. traceroute sends packets to a destination, asking each Internet router along the way to reply when it passes on the packet. This will show you the path packets take when you send them between your location and a destination.



3. ipconfig / ifconfig

- The ipconfig command is used on Windows, while the ifconfig command is used on Linux, Mac OS X, and other Unix-like operating systems. These commands allow you to configure your network interfaces and view information about them.
- For example, you can use the ipconfig /all command on Windows to view all your configured network interfaces, their IP addresses, DNS servers, and other information. Or, you can use the ipconfig /flushdns command to flush your DNS cache, forcing Windows to get new addresses from its DNS servers every time you contact a new hostname. Other commands can force your computer to release its IP address and get a new one from its DHCP server. This utility can quickly display your computer's IP address or help you troubleshoot problems.

4. route: This diagnostic command manipulates network routing tables.

Syntax:

- route [-f] [command [destination] [MASK netmask] [gateway] [METRIC metric]]

Parameters:

- **-f** – Clears the routing tables of all gateway entries. If this parameter is used in conjunction with one of the commands, the tables are cleared prior to running the command.

command – Specifies one of four commands below:

- print: Prints a route.
- add: Adds a route.
- delete: Deletes a route.
- change: Modifies an existing route.

destination – Specifies the host to send command.

MASK – Specifies, if present, that the next parameter be interpreted as the netmask parameter.

netmask – Specifies, if present, the subnet mask value to be associated with this route entry. If not present, this parameter defaults to 255.255.255.255.

gateway – Specifies the gateway.

METRIC – Specifies the route metric (cost) for the destination.

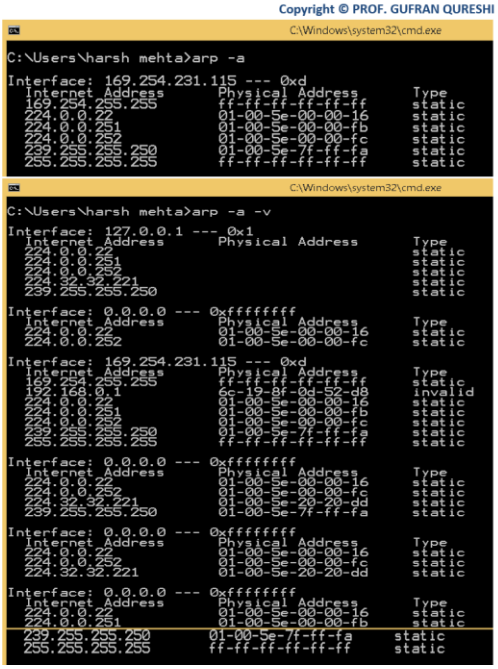
5. **arp:** This diagnostic command displays and modifies the IP-to-Ethernet or Token Ring physical address translation tables used by the Address Resolution Protocol (ARP).

Syntax:

- arp -a [inet_addr] [-N [if_addr]] arp -dinet_addr [if_addr]
- arp -sinet_addrether_addr [if_addr]

Parameters:

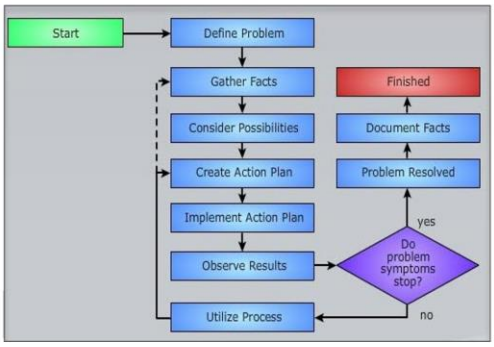
- **-a** – Displays current ARP entries by querying TCP/IP. If inet_addr is specified, only the IP and physical addresses for the specified host are displayed.
- **-d** – Deletes the entry specified by inet_addr
- **-s** – Adds an entry in the ARP cache to associate the IP address inet_addrwith the physical address ether_addr. The physical address is given as 6 hexadecimal bytes separated by hyphens. The IP address is specified using dotted decimal notation. The entry is static. It will not be automatically removed from the cache after the timeout expires and will not exist after a reboot of your computer.
- **-N [if_addr]** – Displays the ARP entries for the network interface specified by if_addr. ether_addr Specifies a physical address. if_addr Specifies, if present, the IP address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used. inet_addr Specifies an IP address in dotted decimal notation.



Practical 2d
AIM: Basic network troubleshooting

Basic network troubleshooting steps

1. Check for local connectivity issues: The first step in troubleshooting network errors is to check cables, devices, switches, and routers for proper functioning. Teams can also try restarting devices such as the modem, PC, and router to resolve simple network issues. Another issue could be LAN connectivity. To identify and troubleshoot LAN connectivity issues, try to ping the destination IP and check configuration settings and source host.
2. Rectify the duplicate entry of IP address: To check whether the computer is receiving a valid IP address or not, type "ipconfig" in the command prompt. If the IP address starts with 169, it's receiving an invalid IP.
3. Perform a DNS check: To determine server issues, use command "nslookup." Results such as refused, timed out or server failure indicate the problem originates from the DNS server of the destination URL.
4. Check malware protection: Check your malware protection tools to ensure they haven't flagged any application, program, or settings affecting network performance.
5. Review logs: Reviewing logs is also one of the best ways to identify and troubleshoot network performance outages and issues. Logs provide elaborated information on each device, application, and program to help track the root cause of the issues.



Following are some essential steps and techniques for basic network troubleshooting:

1. Identify the Problem: Start by gathering information from the user or by observing the issue yourself. Understand what specific problem the user is facing, such as no internet access, slow connection, or inability to access certain resources.
2. Check Physical Connections: Ensure all network cables are securely plugged in, and network devices like routers, switches, and modems have power and functioning indicators.
3. Restart Devices: Sometimes, network issues can be resolved by simply restarting the network devices. Power cycle the router, modem, and any other network equipment to see if it resolves the problem.
4. Check Network Configurations: Verify the network settings on the computer or device experiencing the issue. Look for correct IP configurations, subnet masks, gateway addresses, and DNS server settings.
5. Ping Test: Use the ping command to check the connectivity between the computer and other devices on the network or the internet. For example, try pinging the router, another computer on the network, or an external website.
6. Check for IP Conflicts: Ensure that there are no IP address conflicts on the network. Two devices with the same IP address can cause communication problems.
7. Firewall and Security Software: Temporarily disable any firewall or security software to check if they are blocking network access.
8. Update Network Drivers: Ensure that the network interface card (NIC) drivers are up to date. Outdated drivers can lead to connectivity issues.
9. Test Different Devices: If possible, try connecting the problematic device to a different network or connecting a different device to the same network to see if the issue persists.
10. Check Router and DHCP: Verify that the router is functioning correctly and that the DHCP server is assigning IP addresses to devices on the network.
11. Trace Route: Use the tracert (Windows) or traceroute (macOS and Linux) command to trace the path from your computer to a remote server or website. This can help identify network hops where there might be an issue.
12. Check for Network Outages: Check with your Internet Service Provider (ISP) or network administrator to see if there are any known network outages or maintenance activities in your area.
13. Use Network Troubleshooting Tools: Network troubleshooting tools like ipconfig, ifconfig, nslookup, and netstat can provide valuable information about network configurations and connections.
14. Check Physical Environment: Ensure that there are no physical obstructions or interference (e.g., walls, microwave ovens) that could affect wireless network connectivity.

Practical 2e

AIM: Configuration of TCP/IP Protocols in Windows / Linux

Configuring Windows clients for TCP/IP involves installing and configuring the TCP/IP network protocol.

The following instructions are based on the Configuring TCP/IP function of Windows XP.

1. Click Start > Settings > Control Panel.
2. On the control panel, double-click Network and Dial-Up Connections.
3. Right-click Local Area Connection.
4. Click Properties. If Internet Protocol (TCP/IP) does not appear in the list, do the following:
   a. Click Install.
   b. Select Protocol, and then click Add.
   c. Select Internet Protocol (TCP/IP).
   d. Click OK. This returns you to the Local Area Connection Properties window.
5. Select Internet Protocol (TCP/IP), and then click on Properties.
6. Select Using the Following IP Address. Check with your network administrator to determine the correct settings for this tab. If your PC does not automatically obtain IP and DNS addresses, do the following:
   a. Enter the IP address of your PC (for example, 199.5.83.205).
   b. Enter the subnet mask (for example, 255.255.255.0).
   c. Enter the default gateway (for example, 199.5.83.1).
   d. Enter the preferred DNS server (for example, 199.5.100.75).
   e. Enter the alternate DNS server (for example, 199.5.100.76).

7. If you are using a Windows Internet Name Server, click the Advanced tab, select WINS Address, and do the following:
   a. Click Add.
   b. Enter the primary WINS server (for example, 199.5.83.205).
   c. Enter the secondary WINS server (for example, 199.5.83.206).
   d. The remaining settings should remain as the defaults.
8. Click OK on the Local Area Connection Properties window. It is not necessary to restart your PC.

Practical 2f

AIM: Implementation of Drive/file sharing and printer sharing.

I. Verify that the sharing component is installed

To verify that File and Printer Sharing is on your computer (typically installed by default):

1. Navigate to the Network and Sharing Center.
2. Click Change adapter settings.
3. Right-click the local connection icon and select Properties.
4. In the area below "This connection uses the following items:", look for File and Printer Sharing for Microsoft Networks.
    1. If this component is not available:
        1. Click Install. Select Service, and then click Add....
        2. Select File and Printer Sharing for Microsoft Networks, and then click OK.
        3. Click Close. If a dialog window appears telling you to restart your computer, do so.
    2. If the component is available, make sure it is checked.

II. Share a folder, drive, or printer

Once File and Printer Sharing is installed, to share a folder or drive:

1. Right-click the folder or drive you want to share.
2. Click Properties. From the Sharing tab, click Advanced Sharing.
3. Click Share this folder.

4. In the appropriate fields, type the name of the share (as it appears to other computers), the maximum number of simultaneous users, and any comments that should appear beside it.
5. If you would like to grant access to particular groups or individuals, click Permissions to add the appropriate groups or usernames.
6. If you are using NTFS, check the permissions in the Security tab to ensure that they are properly set to allow access to the share. Because Security settings override Share permissions, it is possible for people on the Permissions list to be denied access to the share because they either are not specified or are denied specifically in the Security list.

Note: FAT32 does not provide the same level of security as NTFS; if you're using FAT32, you will not see the Security tab.

7. Click OK.

To share a printer:

1. From the Control Panel, open Devices and Printers.
2. Right-click the printer you want to share. Click Printer Properties, and then select the Sharing tab.
3. Check Share this Printer. Under Share name, select a shared name to identify the printer. Click OK.

III. Access a shared folder or printer

To find and access a shared folder or printer:

1. Search for Network, and click to open it.
2. Select Search Active Directory at the top of the window; you may need to first select the Network tab on the upper left.
3. From the drop-down menu next to "Find:", select either Printers or Shared Folders.
4. You can now enter search terms in the appropriate fields to modify the search; to start the search, click Find Now. To search for shared printers and folders that match any criteria, click Find Now without entering any search terms.
5. You will see a list of shared printers and folders that are available on the network. Double-click the item to which you want to connect.

If you know the exact name of the computer and the share, or the exact name of the printer, you can enter it directly:

1. Navigate to a search field. Enter two backslashes, the name of the computer, another backslash, and then the name of the share or printer. For example, if the name of the computer is bl-iub-threepio.ads.iu.edu and the name of the share is r2d2, type:

   \\bl-iub-threepio.ads.iu.edu\r2d2

2. Click OK.

If you need to repeatedly access a shared folder or network drive, you can map to it. Mapping creates a persistent link to the share, allowing you to double-click its icon in My Computer whenever you want access.

Practical 3

AIM: IPv4 Addressing and Subnetting

a. Given an IP address and network mask, determine other information about the IP address such as:

1. Network address
2. Network broadcast address
3. Total number of host bits
4. Number of hosts

Given: IP address – 70.12.100.132
Network Mask – 255.255.255.192

Solution:

1. Network Address:

First Address = (any address) AND (Network Mask)
= 70.12.100.132 AND 255.255.255.192
01000110.00001100.01100100.10000100
AND 11111111 .11111111 . 11111111 .11000000
= 01000110.00001100 .01100100.10000000
= 70.12.100.128

2. Network Broadcast Address:

Last Address = (any address) OR (**NOT** Network Mask)
= 70.12.100.132 OR 0.0.0.63
01000110.00001100.01100100.10000100
Complement's → **OR 00000000.00000000.00000000.00111111**
= 01000110.00001100 .01100100.10111111
= 70.12.100.191

3. Total Number of Host Bits = 32 – 26 = 6 bits

4. Number of Host = $2^{32-n} = 2^{32-26} = 2^6 = 64$ host

b. Given an IP address and network mask, determine other information about the IP address such as:

1. The subnet address of this subnet
2. The broadcast address of this subnet
3. The range of host addresses for this subnet
4. The maximum number of subnets for this subnet mask
5. The number of hosts for each subnet
6. The number of subnet bits
7. The number of this subnet

Solution:

- Consider class A IP address 10.0.0.0. It's default subnet mask is 255.0.0.0 which means we can represent it by 10.0.0.0/8. The "/" factor indicates the CIDR (Classless inter-domain routing) values.
- If we decide to block some of the bits to minimize number of host in any given subnet, then that technique is called as variable length subnet masking (VLSM).
- Let us see the examples where we borrow some bits from host part and minimize the count to an extent and create small independent networks of big network. Or even we can say that we want 8 network out of 1 big network then we will observe the following network created with their VLSM 255.224.0.0. (11111111.**11100000**.**00000000.00000000**)

Number of Host per subnet $= 2^{21} = (2^{10} \times 2^{10} \times 2^1) - 2$
$= (1024 \times 1024 \times 2) - 2$
$= 2097152 - 2$
$= 2097150$

Block Size = 256 – Subnet mask = 256 – 224 = 32
OR $2^5 = 32$

ID	Subnet Mask	Broadcast	First Host	Last Host
1	10.0.0.0	10.31.255.255	10.0.0.1	10.31.255.254
2	10.32.0.0	10.63.255.255	10.32.0.1	10.63.255.254
3	10.64.0.0	10.95.255.255	10.64.0.1	10.95.255.254
4	10.96.0.0	10.127.255.255	10.96.0.1	10.127.255.254
5	10.128.0.0	10.159.255.255	10.128.0.1	10.154.255.254
6	10.160.0.0	10.191.255.255	10.160.0.1	10.191.255.254
7	10.192.0.0	10.223.255.255	10.192.0.1	10.223.255.254
8	10.224.0.0	10.255.255.255	10.224.0.1	10.255.255.254

Class	Minimum	Maximum	Subnet Mask
A	0.0.0.0	127.255.255.255	255.0.0.0 (8 N, 24 H)
B	128.0.0.0	191.255.255.255	255.255.0.0 (16 N, 16 H)
C	192.0.0.0	223.255.255.255	255.255.255.0 (24 N, 8 H)
D	**Multicast Add**		(32 N)
E	**Future Reserve (R&D)**		(32 H)

Class	Octet 1	Octet 2	Octet 3	Octet 4
A	Net ID (8 bit)	Host ID (24 bit)		
B	Net ID (16 bit)		Host ID (16 bit)	
C	Net ID (24 bit)			Host ID (8 bit)

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	128
1	1	0	0	0	0	0	0	192
1	1	1	0	0	0	0	0	224
1	1	1	1	0	0	0	0	240
1	1	1	1	1	0	0	0	248
1	1	1	1	1	1	0	0	252
1	1	1	1	1	1	1	0	254
1	1	1	1	1	1	1	1	255

1. What is the subnet mask of:

a. 188.25.45.48 / 16

➢ The subnet mask is 255.255.0.0 because first 2 octet are Net ID

b. 188.25.24.48 / 20

➢ This address belongs to class B. The default subnet mask is 255.255.0.0 / 16

We borrow 4 bits from host portion & then the subnet mask will be

11111111. 11111111. 11110000.00000000

255 . 255 . (128+64+32+16) . 0

255 . 255 . 240 . 0

2. How many subnet does given subnet mask provide?

192.168.1.0 / 27

➢ To calculate subnet we use formula 2^n, where n is the number of the bits borrowed from host bits to create subnet.

The default subnet of class C is 255.255.255.0 / 24

Hence we will borrow (27 – 24) = 3 bits

Therefore our subnet is $2^n = 2^3 = 8$ subnets

3. What is the block size of subnet?

Subnet mask	Block Size
256-128	128
256-192	64
256-224	32
256-240	16
256-248	8
256-252	4
256-254	2
256-255	1

a. 188.25.40.1 / 20

➢ The subnet of the following block is 255.255.0.0 / 20

This address belongs to class B. The default subnet mask is 255.255.0.0 / 16

We borrow 4 bits from host portion & then the subnet mask will be

11111111. 11111111. 11110000.00000000

255 . 255 . 240 . 0

Formula for block size = 256 – Subnet mask = 256 – 240 = 16 **OR** $2^4 = 16$

4. Calculate valid subnet of 192.168.1.0 / 26

➢ Total subnets = $2^n = 2^{2\,(26-24)} = 4$

Subnet mask = 255.255.255.192 (11111111.11111111.11111111.11000000)

Block Size = 256 – 192 = 64

0, 64, 128, 192

5. How many valid hosts are available per subnet?

➢ Valid host = Total host – 2 (Net ID i.e. all 0's and Broadcast i.e. all 1's)

If 64 host are their then 62 host (64 – 2) are valid host.

Commands:

1. **Enable command (en**able**):** It will move us from user mode {>} to privilege mode {#}.
2. **Configure terminal (config t**er**):** It will move us from privilege mode to configuration mode {(config)#}.
3. **Interface Configuration (int**erface **fa0/0):** It will move us from configuration to interface {(config-if)#}.
4. **Change name:** Router(config)# hostname Mumbai

To manage the switch remotely (telnet) we give the IP address to vlan which is in switch

1. **SwitchX(config)#** interface vlan1 {For router interface fa0/0}
2. **SwitchX(config-if)#** ip address 10.5.5.11 255.255.255.0
3. **SwitchX(config-if)#** no shutdown {because vlan is by default shutdown}

Configuring the switch to Default Gateway

SwitchX(config)# ip defaultgateway 172.20.137.1 {It's a router address}

To save the configuration to NVRAM

SwitchX# copy running-config startup-config

To check routing table of Router

1. **RouterX#** show ip route
2. **RouterX#** show ip int brief

Check Router Interfaces

RouterX# show interfaces

Check ARP

Router# show ip arp

Traceroute

Router# Traceroute {protocol} destination

PC> Tracert {protocol} destination

To check whether file is save or not

Router# show startup-config

If not save & to erase all connection

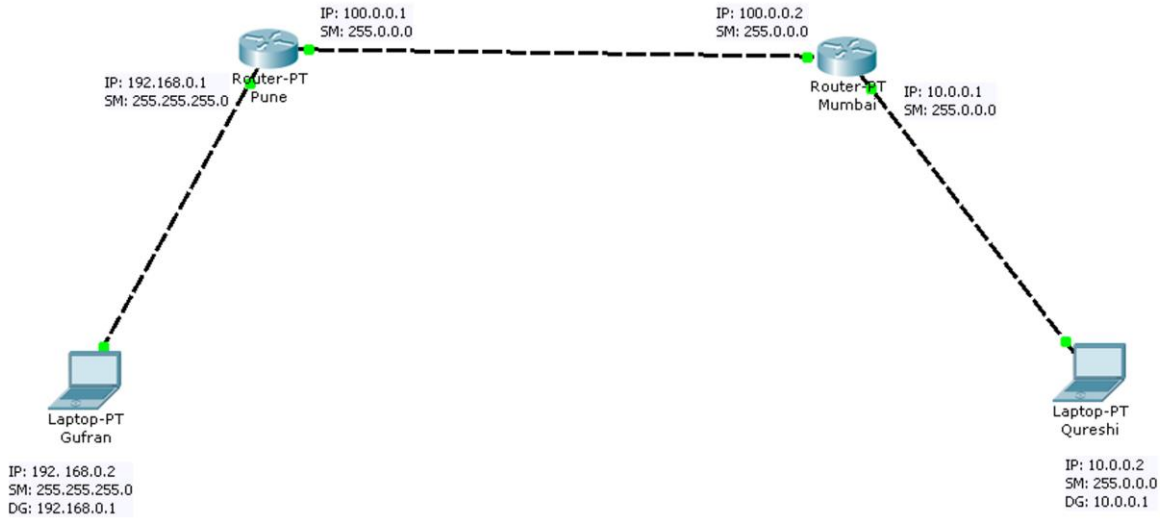
Router# reload

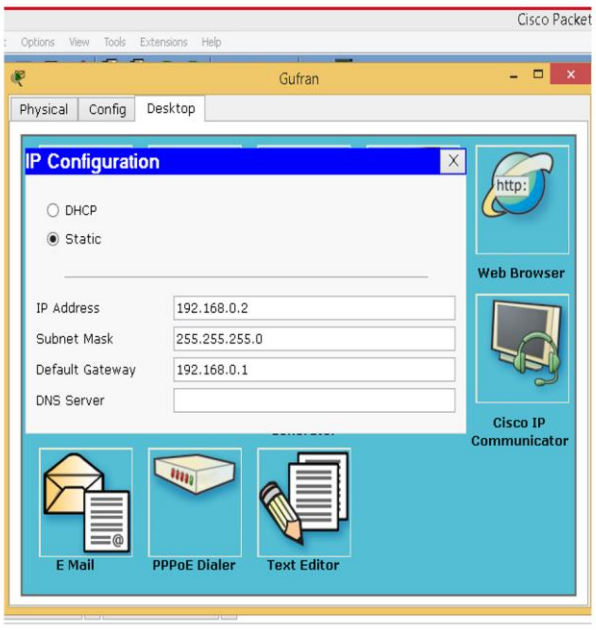
If save & to erase all connection

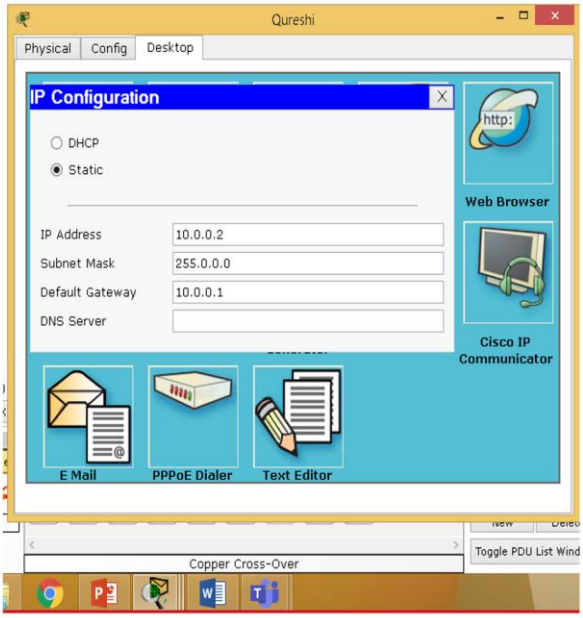
Router# erase startup-config

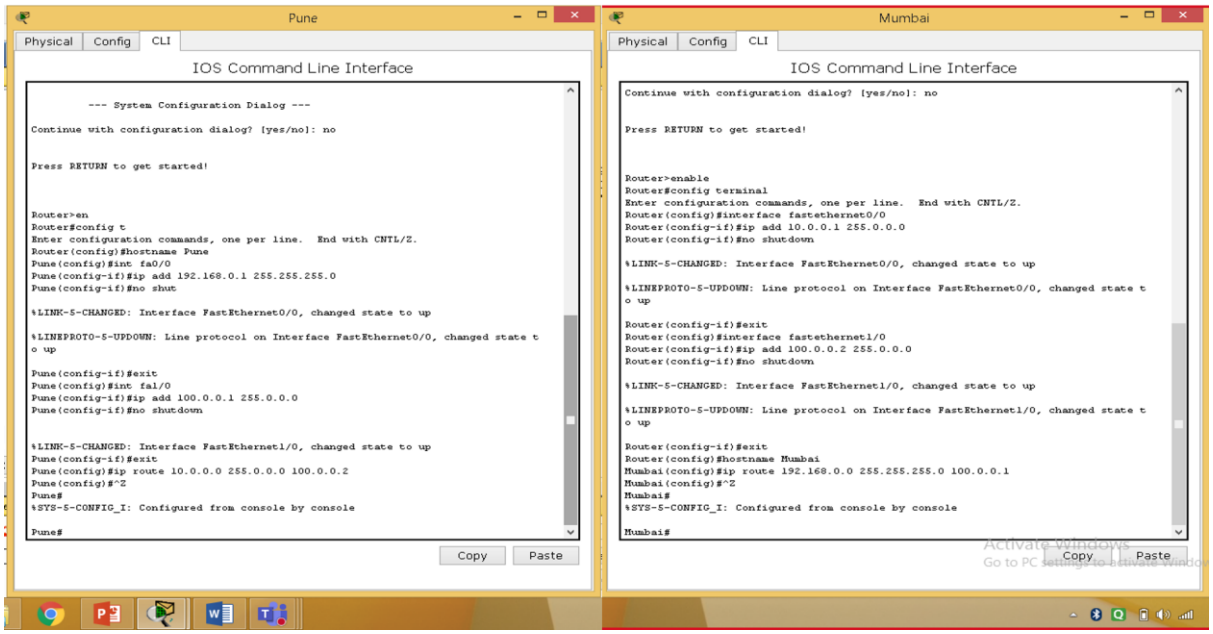
Practical 4

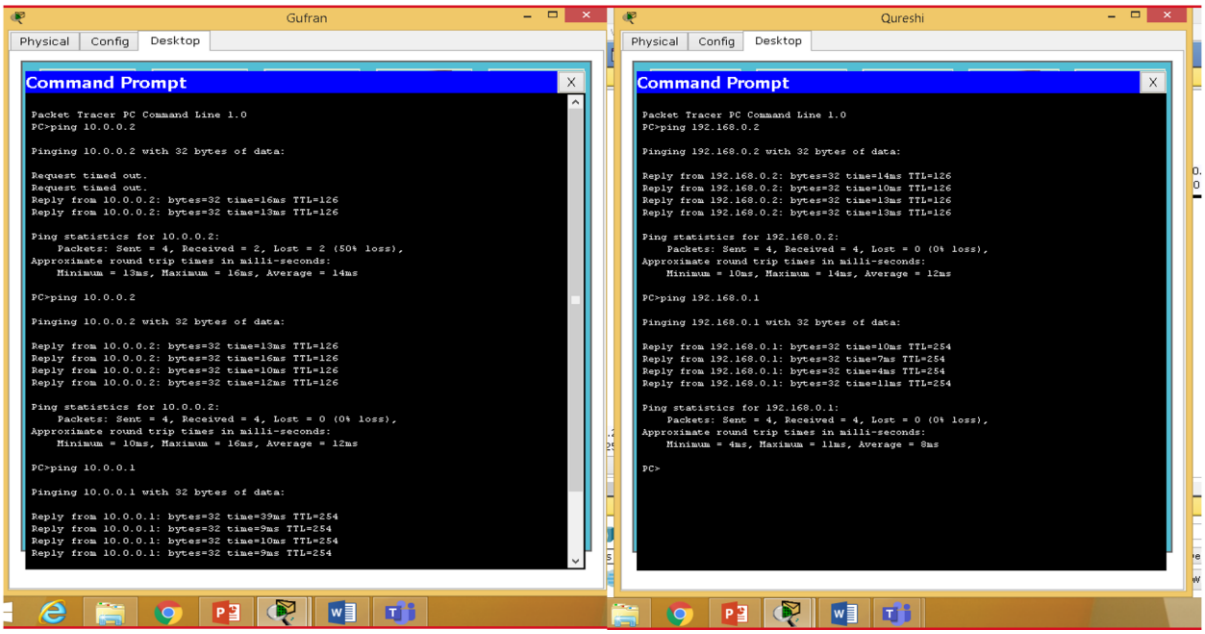
AIM: To Configure IP static routing











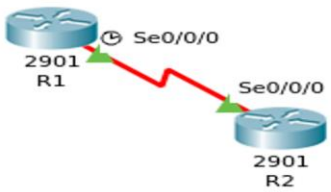
DTE & DCE Connector

DATA TERMINAL EQUIPMENT(DTE)

- DTE is an end instrument that converts user *information into signals or reconverts received signal*. These can also be called tail circuits.
- DTE stands for *data terminal equipment* which generally is a terminal or a computer.

DATA COMMUNICATION EQUIPMENT(DCE)

- (DCE) refers to computer hardware devices used to *establish, maintain and terminate communication network sessions between a data source and its destination.*
- DCE is connected to the data terminal equipment (DTE) and data transmission circuit (DTC) to convert transmission signals.
- DCE stands for *data circuit-terminating, data communications, or data carrier equipment* - this is a modem or more generally, a line adapter.
- Basically, these two are the different ends of a serial line.



- With the DCE cable, (red zigzag with clock) the side you click first will be the DCE, the second will be DTE
- With the DTE cable (red zigzag no clock) the side you click first will be DTE, the second will be DCE

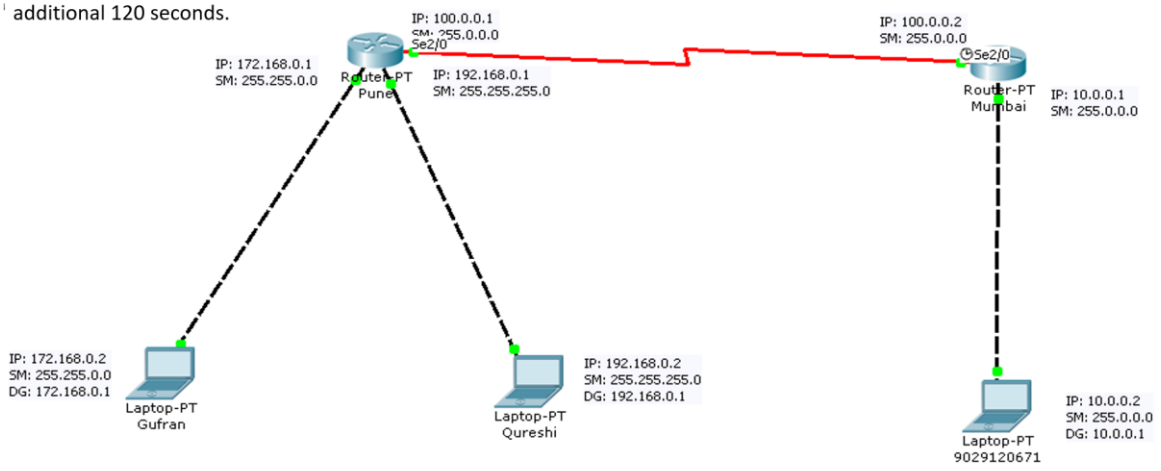
Whichever way you do it, you'll see one side of the cable shows the clock symbol: this is the DCE.

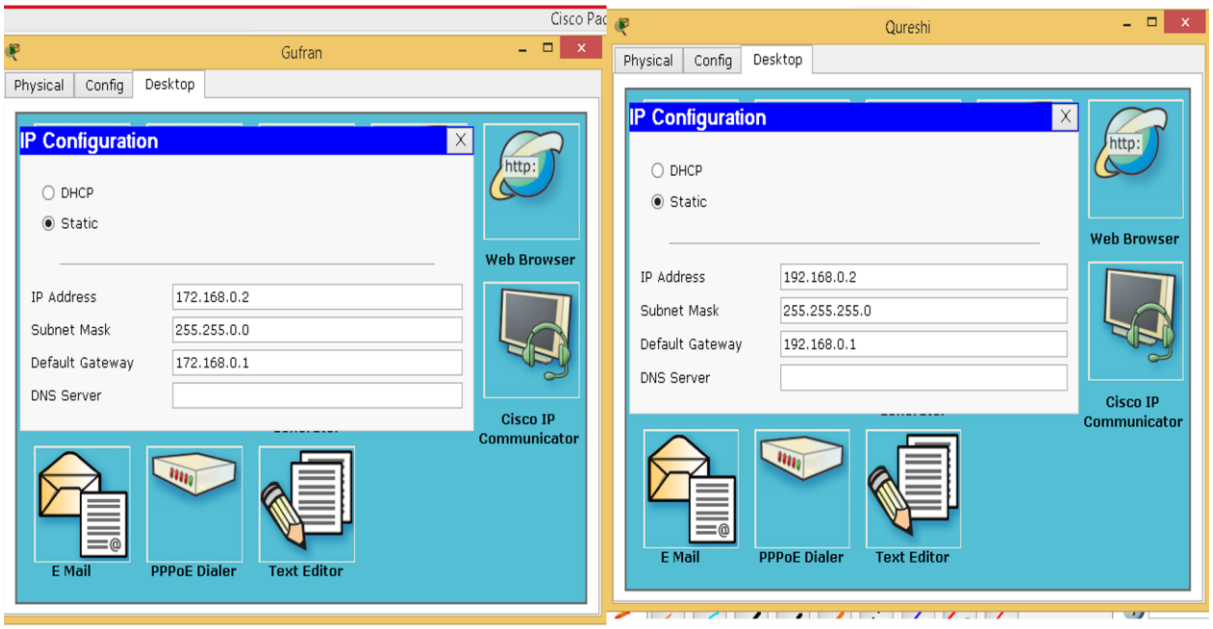
Note: *For serial interface we have to give clock rate 64000 (64 kb) in interface mode at DCE*

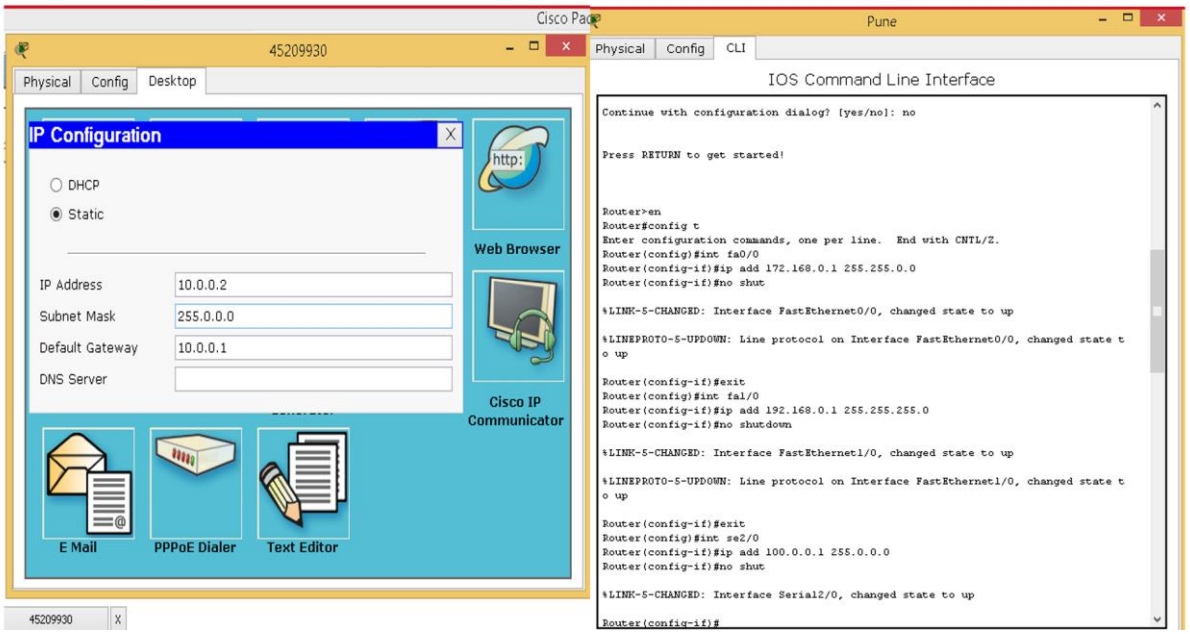
Practical 5

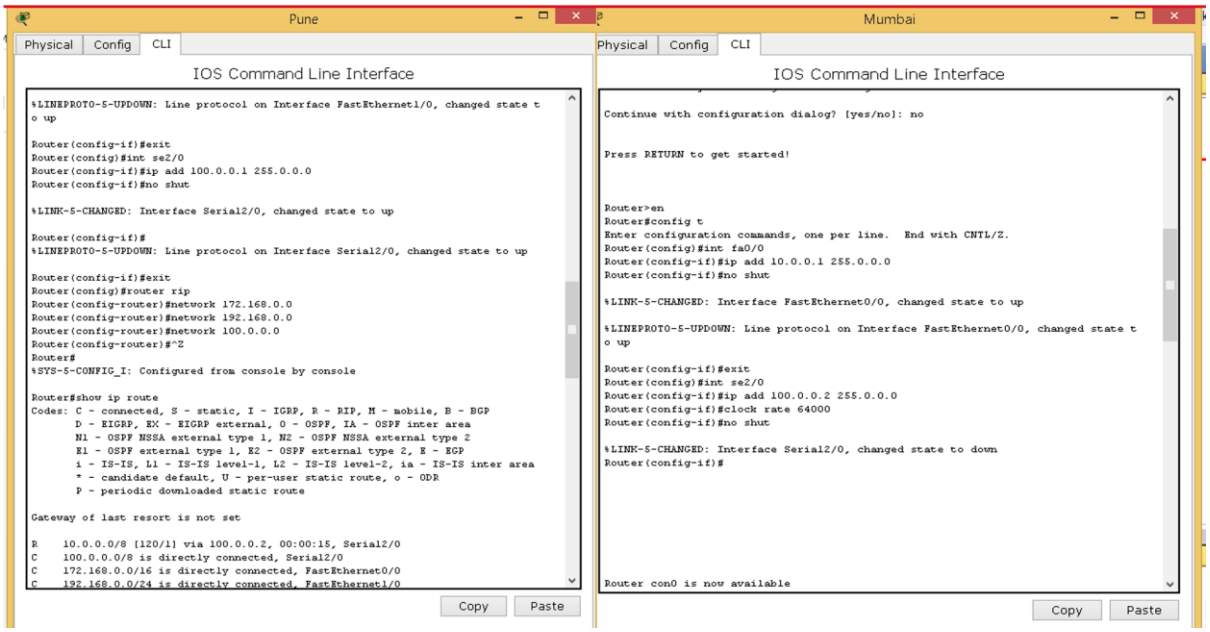
AIM: To Configure IP routing using RIP

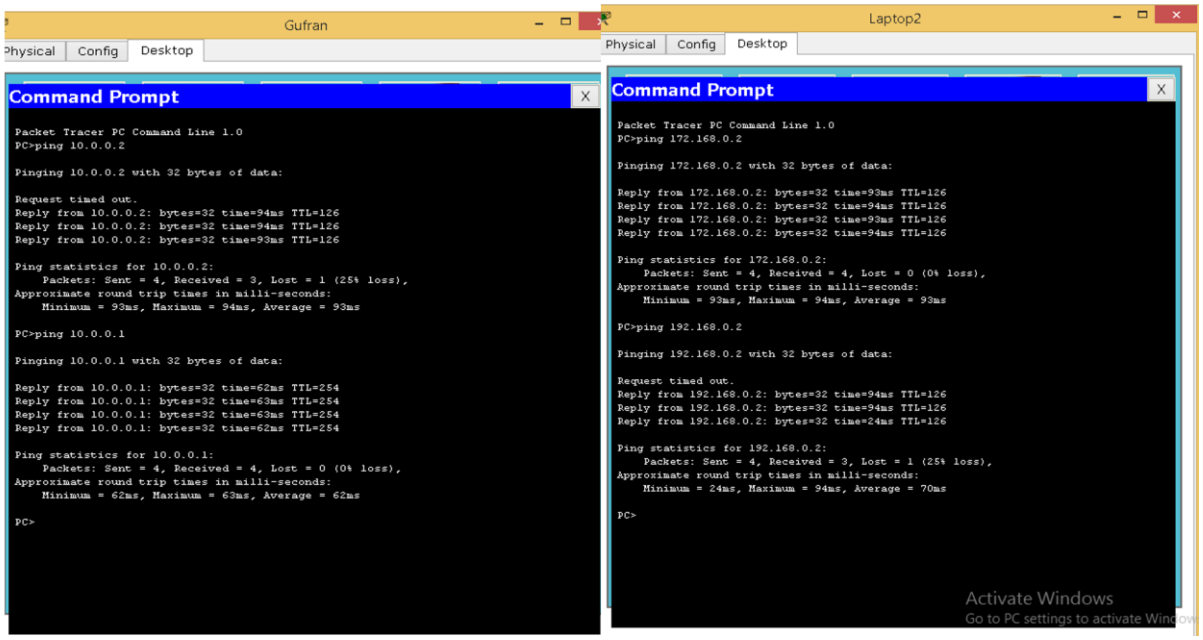
Routing Information Protocol (RIP) is a protocol that routers can use to exchange network topology information. It is characterized as an interior gateway protocol, and is typically used in small to medium-sized networks. A router running RIP sends the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table, it is flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.





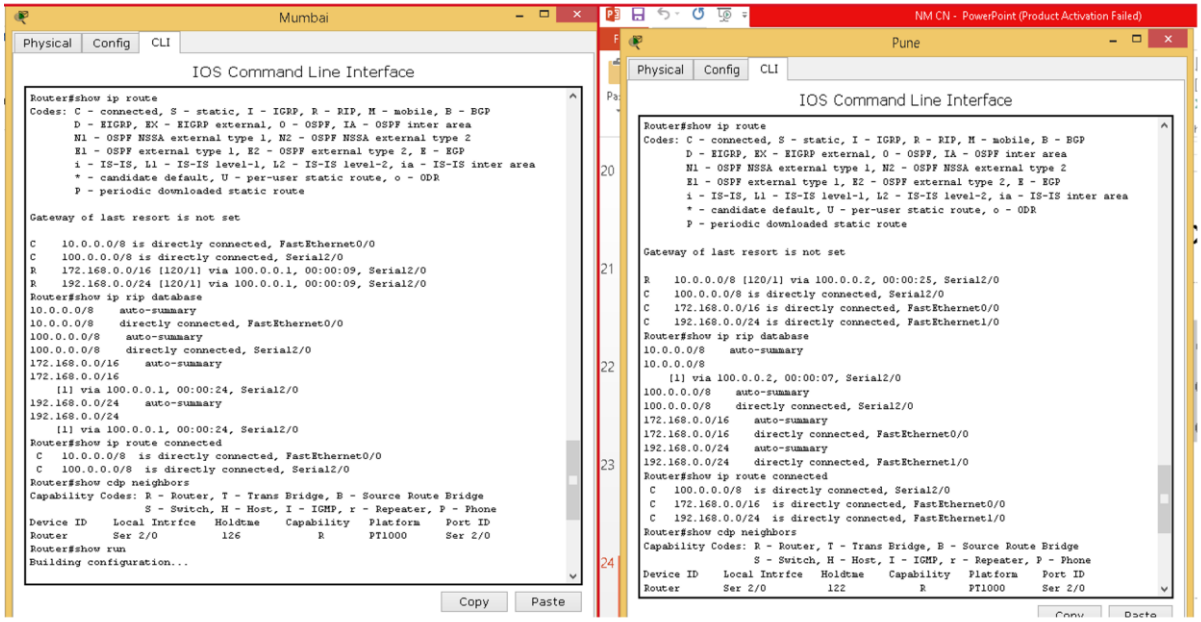






Router Command

1. Show IP Route
2. Show IP RIP Database
3. Show IP Route Connected
4. Show CDP (Cisco Discovery Protocol) Neighbors
5. Show RUN



OSPF

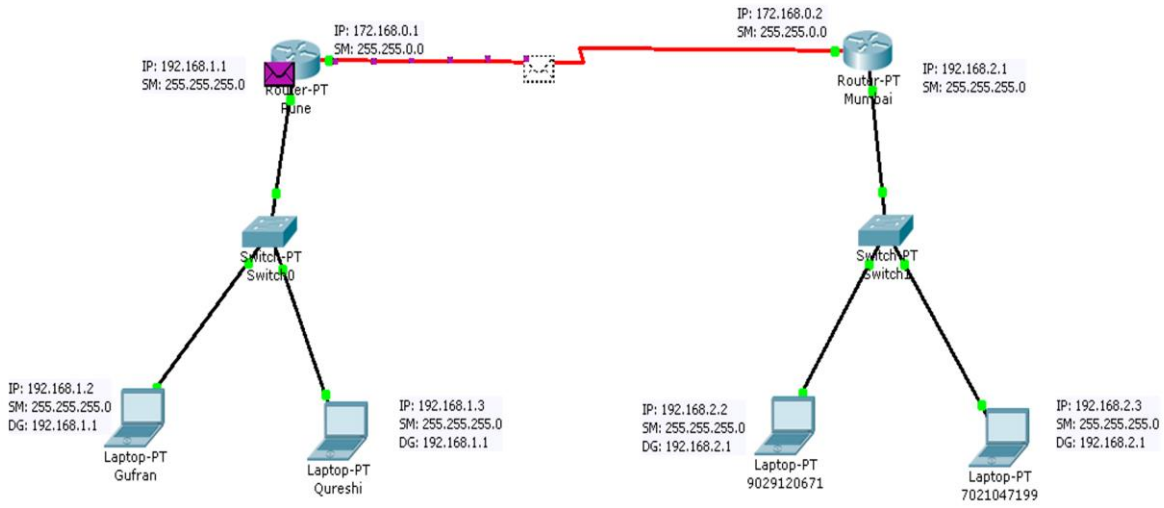
The **OSPF** (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, **used to** distribute IP routing information throughout a single Autonomous System (AS) in an IP network. An OSPF network can be divided into sub-domains called **areas.** An area is a logical collection of OSPF networks, routers, and links that have the same area identification. A router within an area must maintain a topological database for the area to which it belongs. Metric is Cost (Cost = 10^8 / Bandwidth).
The RIP is a distance vector protocol whereas the OSPF is a link state protocol. A distance vector protocol uses the distance or hop counts to determine the transmission path. The link state protocol analyzes different sources like the speed, cost and path congestion while identifying the shortest path (dijkistra algorithm).
Router(config)# router ospf process_ID

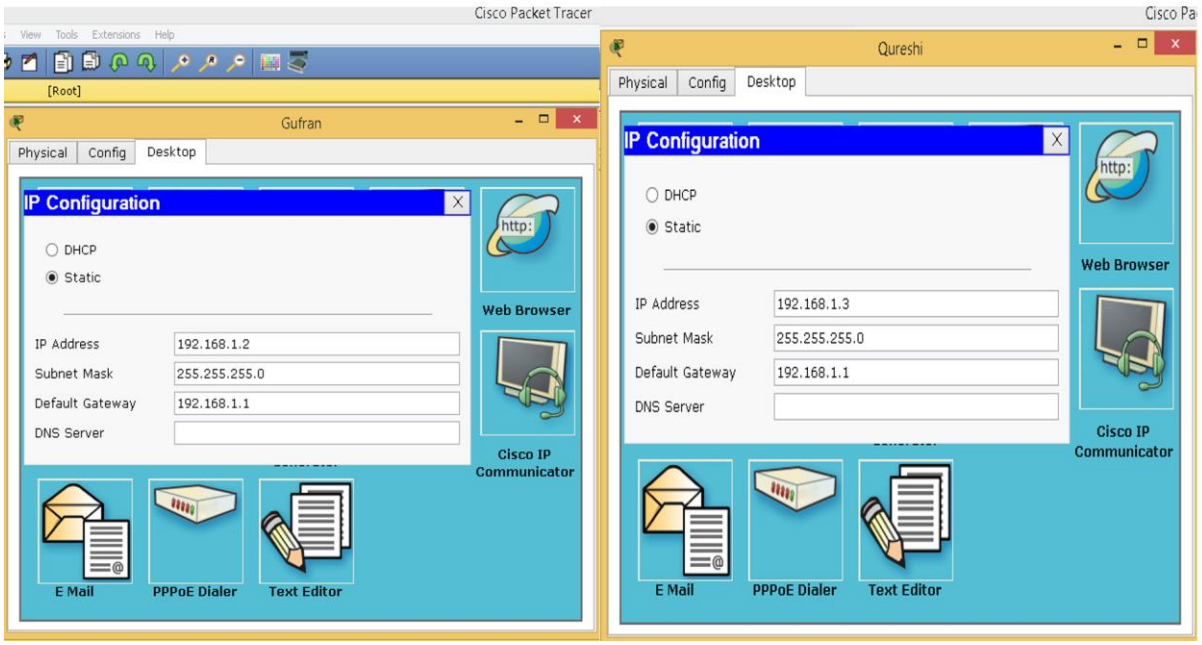
Wildcard Mask: A wildcard mask is a mask of bits that indicates which parts of an IP address are available for examination. In the Cisco IOS, they are used in several places, for example: To indicate the size of a network or subnet for some routing protocols, such as OSPF. At a simplistic level a wildcard mask can be thought of as an inverted subnet mask. For example, a subnet mask of 255.255.255.0 (binary equivalent = 11111111.11111111.11111111.00000000) inverts to a wildcard mask of 0.0.0.255 (binary equivalent = 00000000.00000000.00000000.11111111).

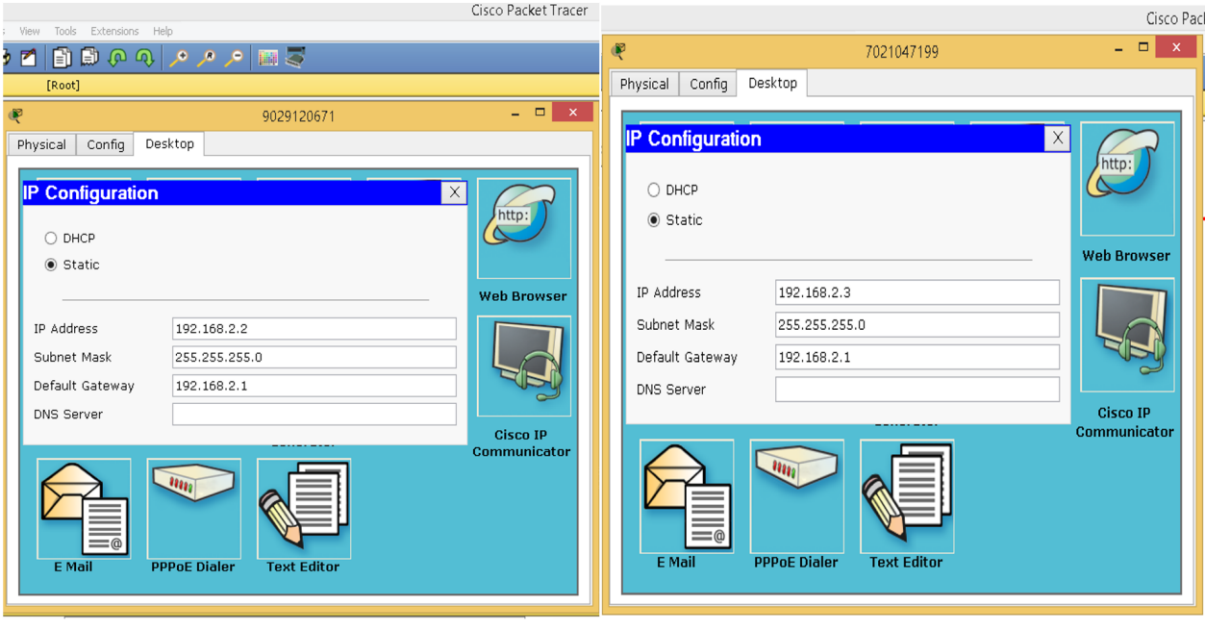
Switches: A network switch (also called switching hub, bridging hub, and by the IEEE MAC bridge) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that **uses MAC addresses to forward data** at the data link layer (layer 2) of the OSI model.

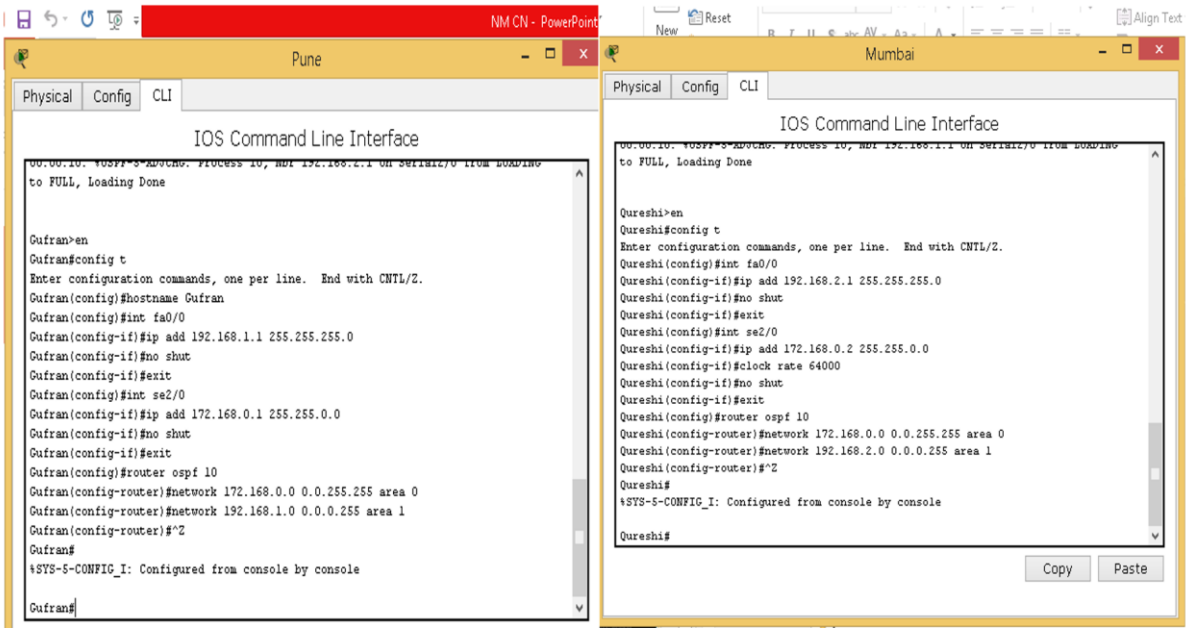
Backbone Area: The backbone area (Area 0) is the core of an OSPF network. All other areas are connected to it and all traffic between areas must traverse it. All routing between areas is distributed through the backbone area. While all other OSPF areas must connect to the backbone area, this connection doesn't need to be direct and can be made through a virtual link.

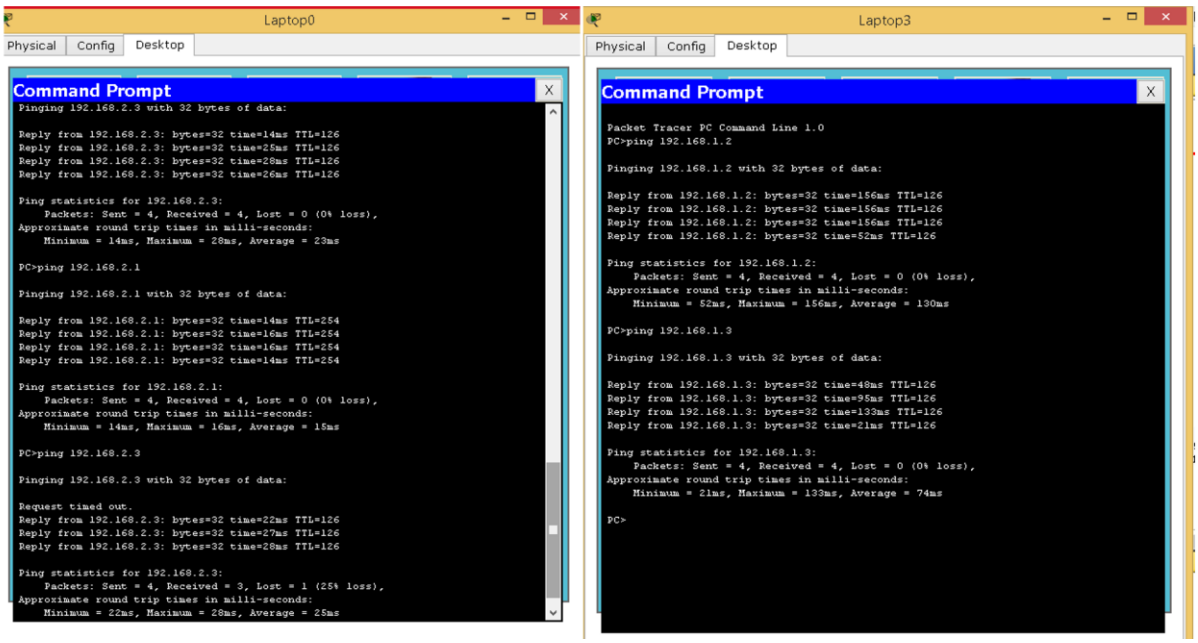
Practical 6a
AIM: To Configure Simple OSPF





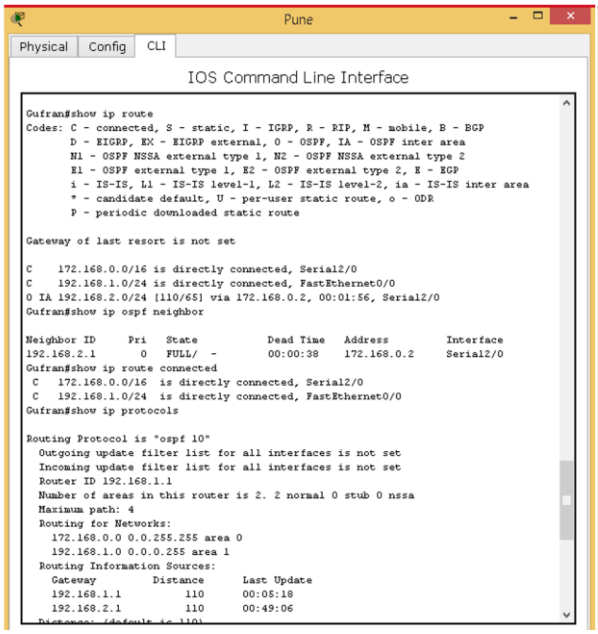


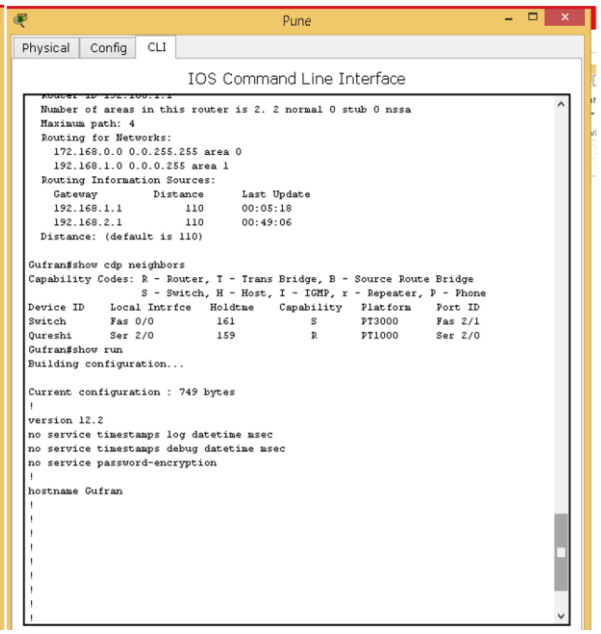


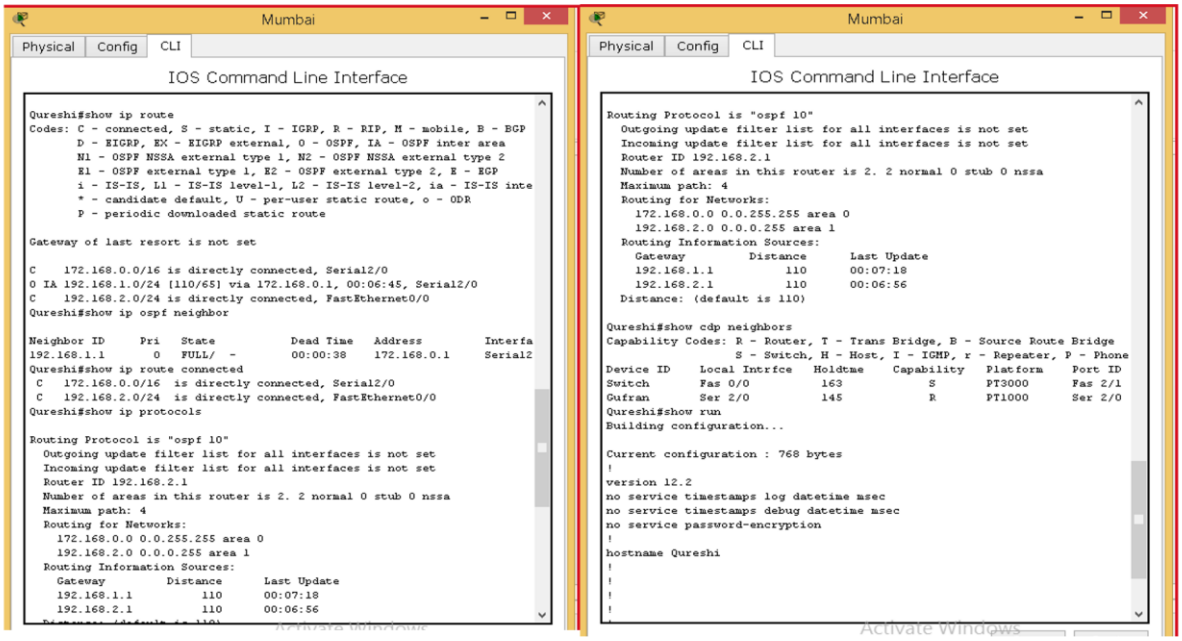


Router Command

1. Show IP Route
2. Show IP OSPF neighbor
3. Show IP Route Connected
4. Show IP protocols
5. Show CDP (Cisco Discovery Protocol) Neighbors
6. Show RUN

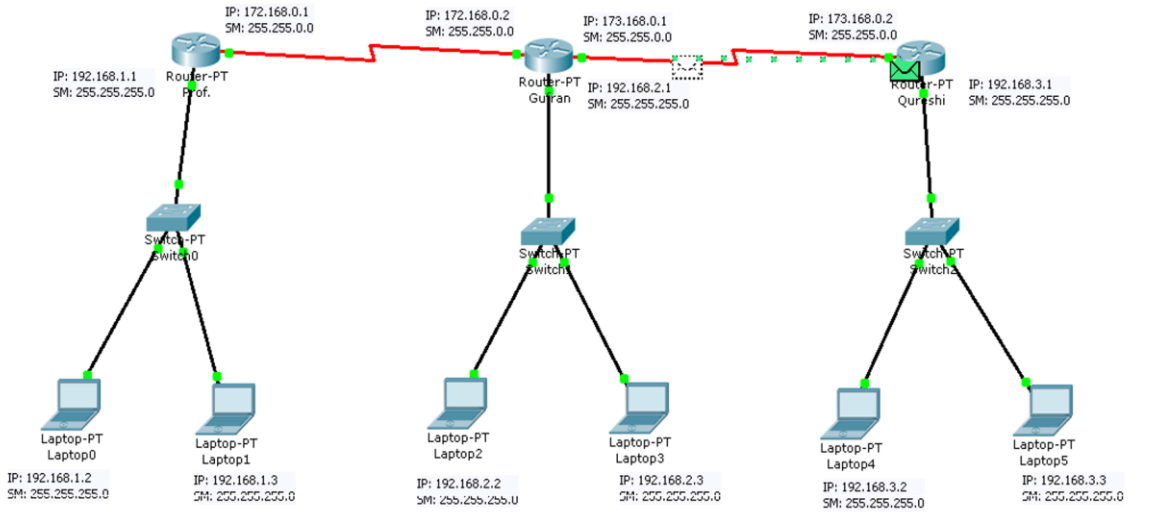


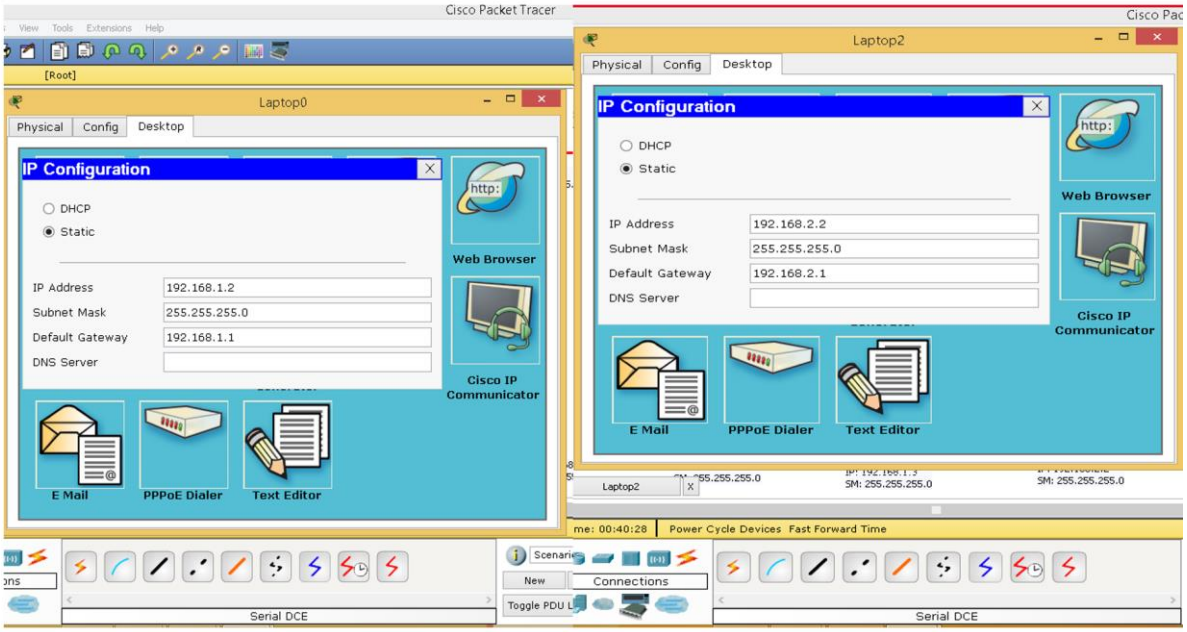


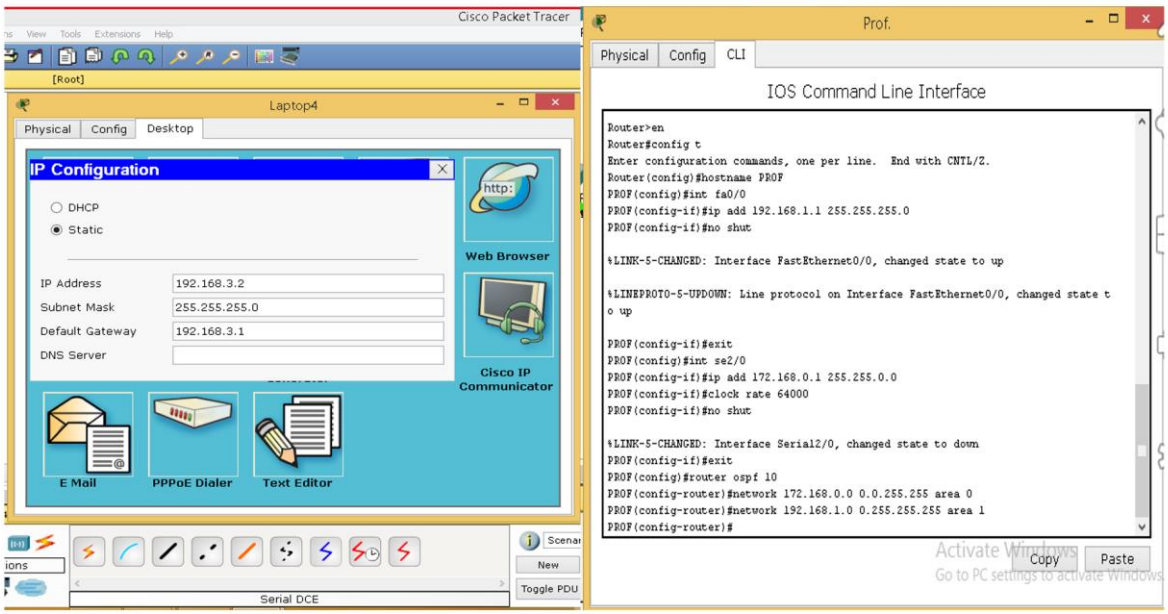


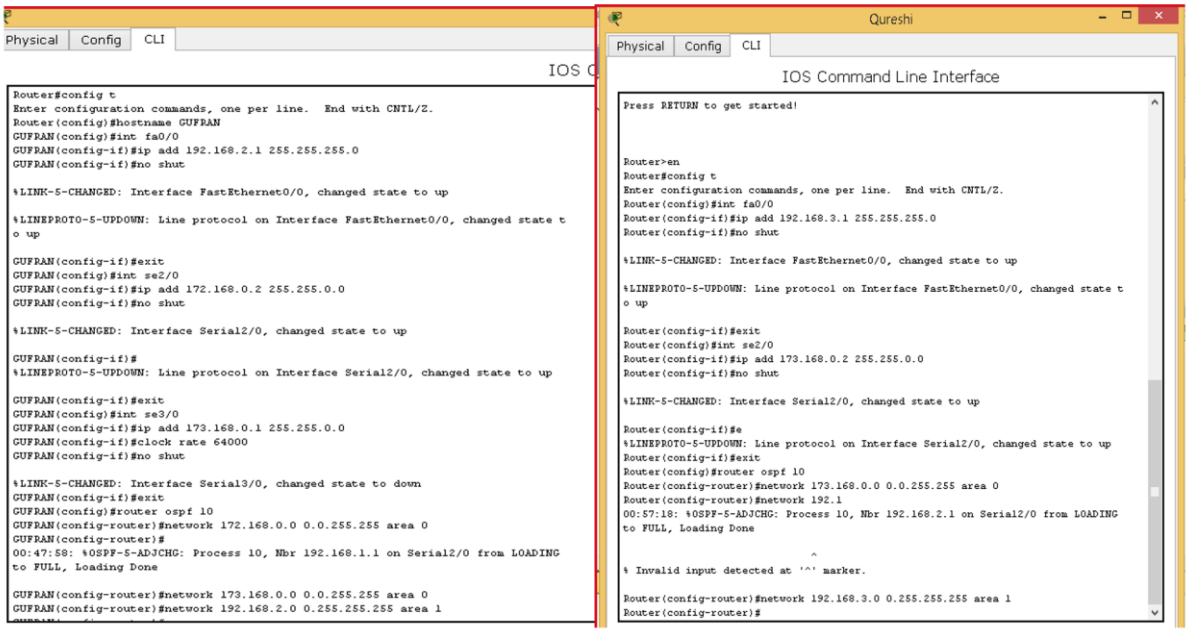
Practical 6b

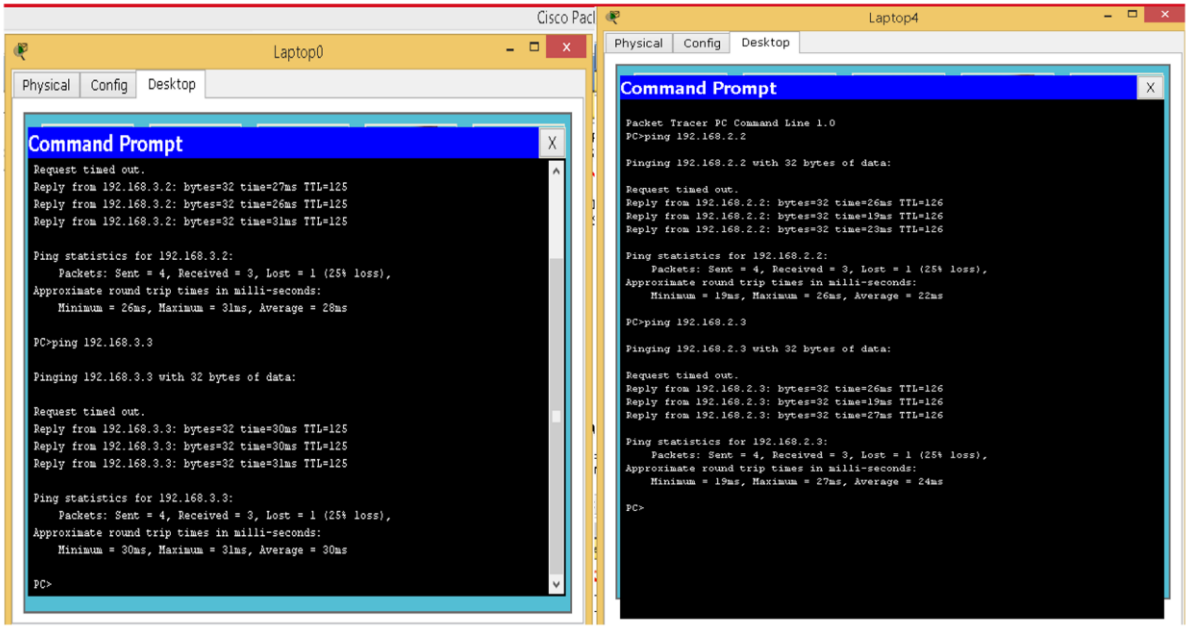
AIM: Configuring OSPF with multiple areas











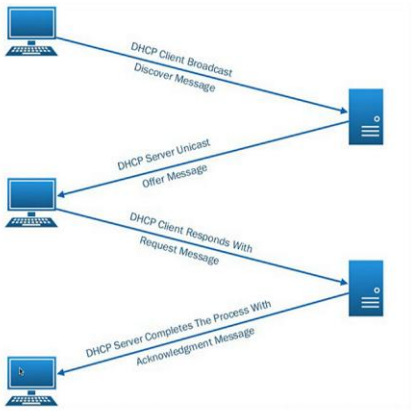
Router Command

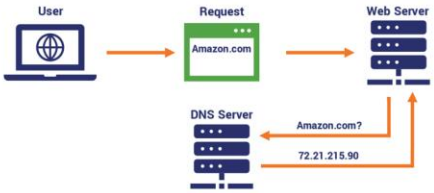
1. Show IP Route
2. Show IP OSPF neighbor
3. Show IP Route Connected
4. Show IP protocols
5. Show CDP (Cisco Discovery Protocol) Neighbors
6. Show RUN

DHCP

DHCP defines the term dynamic host configuration protocol as a network management protocol used on UDP/IP networks. It assigns an IP address and some other configuration parameters to each network device automatically, so that the device will be authorized to communicate with other IP networks. This means users don't need to configure the network, just plug the wire into your computer or connect to the WiFi, your computer will automatically receive the IP address, subnet mask, default gateway and DNS server.

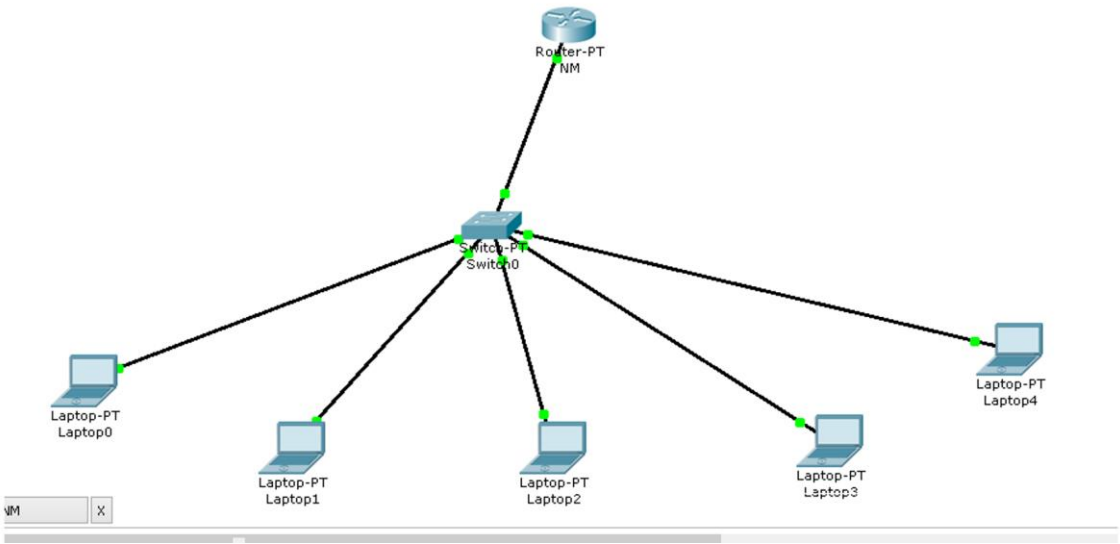
Step one: When a new client wants to join a network, it will broadcast a DHCP discover packet to the servers.
Step two: To answer the request, DHCP servers will send the free DHCP offer packet to the client.
Step three: The client takes the first DHCP offer message from different serves. Then it will send a DHCP request to the Internet to indicate which IP address it has taken.
Step four: DHCP server sends an acknowledge message to make sure the IP address has been used that will not assign to any other client. And now the client can participate on the network.

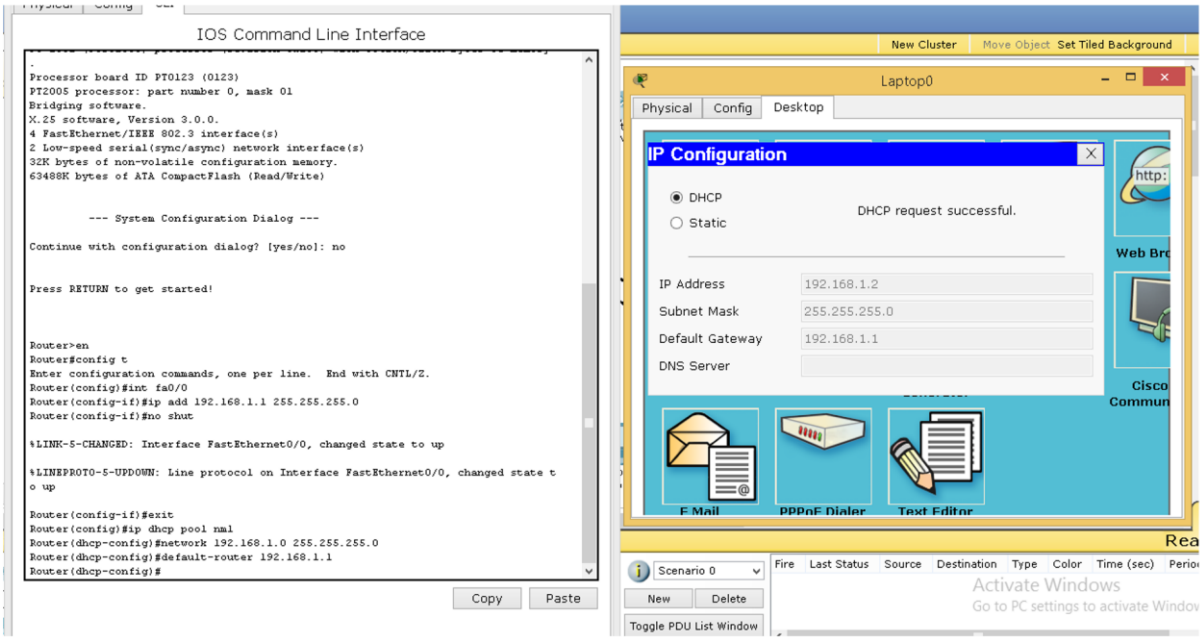


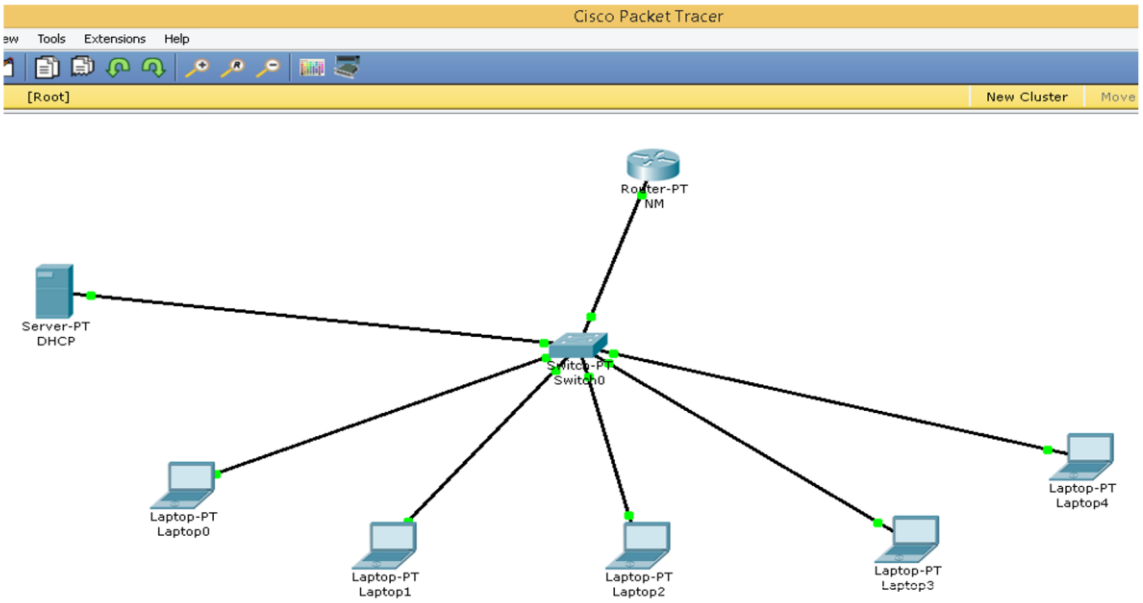


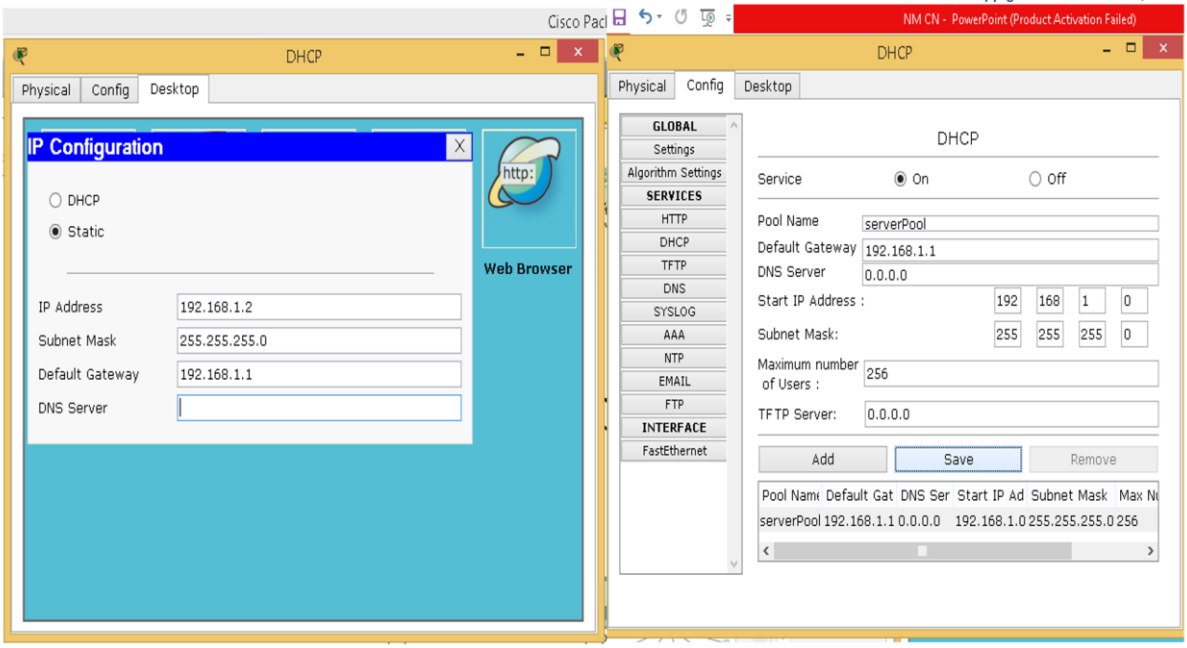
DNS (Domain Name System): The Internet's DNS system works much like a phone book by managing the mapping between names and numbers. DNS servers translate requests for names into IP addresses, controlling which server an end user will reach when they type a domain name into their web browser. These requests are called queries.

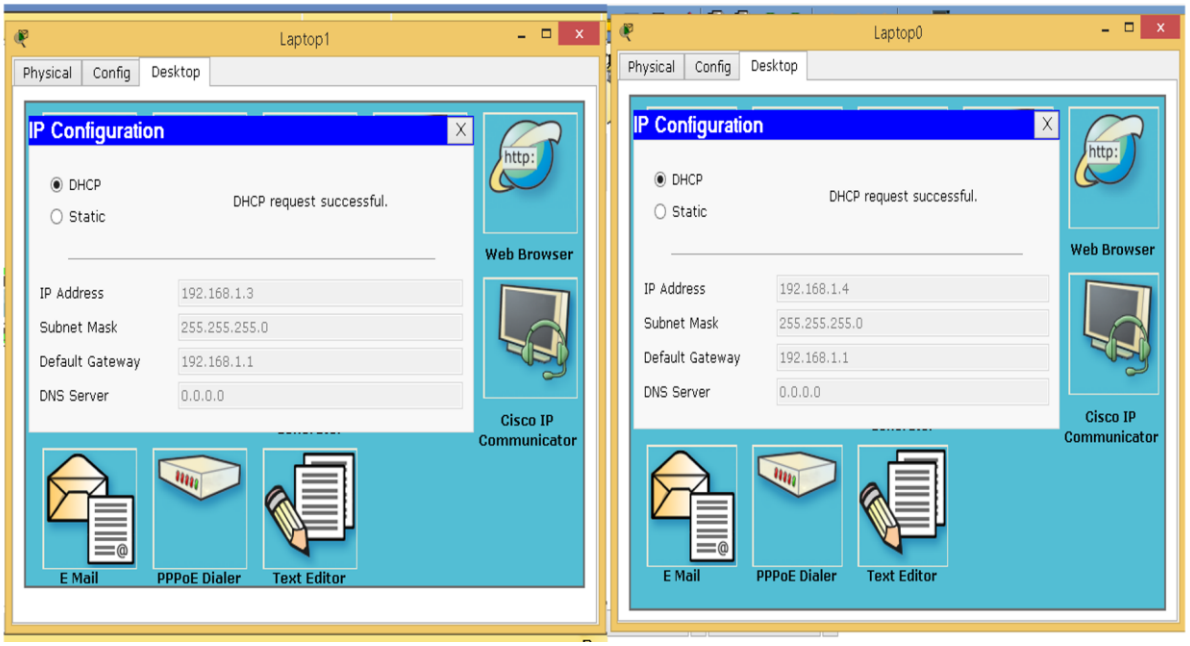
Practical 7a
AIM: To Configure DHCP Server & Client











Copyright © PROF. GUFRAN QURESHI

Practical 7b
AIM: To Configure DNS Server & Client