Lab Manual Table of Contents

LAB # 1 : Networking Devices

Since, we are going to do a series of tutorials on packet tracer. In this manner, we need to have a familiarity of various networking components and devices. We are going to discuss some important devices which are going to be used in networking.

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers etc. These devices also need cables to connect them. In this tutorial, we are going to discuss these important devices.

Network interface cards

A 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. It allows users to connect to each other either by using cables or wirelessly.The NIC provides the transfer of data in megabytes.

NIC

Every device on a network that needs to transmit and receive data must have a network interface card (NIC) installed. They are sometimes called network adapters, and are usually installed into one of the computer's expansion slots in the same way as a sound or graphics card. The NIC includes a transceiver, (a transmitter and receiver combined). The transceiver allows a network device to transmit and receive data via the transmission medium. Each NIC has a unique 48-bit Media Access Control (MAC) address burned in to its ROM during manufacture. The first 24 bits make up a block code known as the Organisationally Unique Identifier (OUI) that is issued to manufacturers of NICs, and identify

the manufacturer. The issue of OUIs to organisations is administered by the Institute of Electrical and Electronics Engineers (IEEE). The last 24 bits constitute a sequential number issued by the manufacturer. The MAC address is sometimes called a hardware address or physical address, and uniquely identifies the network adapter. It is used by many data link layer communications protocols, including Ethernet, the 802.11 wireless protocol and Bluetooth. The use of a 48-bit adress allows for 248(281,474,976,710,656) unique addresses. A MAC address is usually shown in hexadecimal format, with each octet separated by a dash or colon,

For example: 00-60-55-93-R2-N7

Repeaters

A repeater is an electronic device that receives a signal and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair ethernet configurations, repeaters are required for cable runs longer than 100 meters away from the computer. As signals travel along a transmission medium there will be a loss of signal strength i.e. attenuation. A repeater is a non-intelligent network device that receives a signal on one of its ports, regenerates the signal, and then retransmits the signal on all of its remaining ports. Repeaters can extend the length of a network (but not the capacity) by connecting two network segments. Repeaters cannot be used to extend a network beyond the limitations of its underlying architecture, or to connect network segments that use different network access methods. They can, however, connect different media types, and may be able to link bridge segments with different data rates.

Repeater

Repeaters are used to boost signals in coaxial and twisted pair cable and in optical fibre lines. An electrical signal in a cable gets weaker the further it travels, due to energy dissipated in conductor resistance and dielectric losses. Similarly a light signal traveling through an optical fiber suffers attenuation due to scattering and absorption. In long cable runs, repeaters are used to periodically regenerate and strengthen the signal.

Hubs

A hub contains multiple ports. When a packet arrives at one port, it is copied to all the ports of the hub for transmission. In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Passing it along to every port ensures that it will reach its intended destination. This

places a lot of traffic on the network and can lead to poor network response times. Additionally, a 10/100Mbps hub must share its bandwidth with each and every one of its ports. So when only one PC is broadcasting, it will have access to the maximum available bandwidth. If, however, multiple PCs are broadcasting, then that bandwidth will need to be divided among all of those systems, which will degrade performance.

Network Hub

Bridges

A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do not copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.

Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Network Bridge

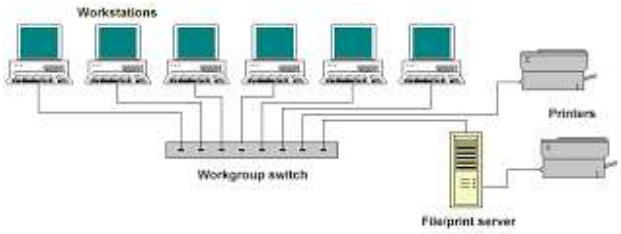
Bridges don't know anything about protocols, but just forward data depending on the destination address in the data packet. This address is not the IP address, but the MAC (Media Access Control) address that is unique to each network adapter card. The bridge is basically just to connect two local-area networks (LANs), or two segments of the same LAN that use the same protocol. Bridges can extend the length of a network, but unlike repeaters they can also extend the capacity of a network, since each port on a bridge

has its own MAC address. When bridges are powered on in an Ethernet network, they start to learn the network's topology by analysing the source addresses of incoming frames from all attached network segments (a process called backward learning). Over a period of time, they build up a routing table .

The bridge monitors all traffic on the segments it connects, and checks the source and destination address of each frame against its routing table. When the bridge first becomes operational, the routing table is blank, but as data is transmitted back and forth, the bridge adds the source MAC address of any incoming frame to the routing table and associates the address with the port on which the frame arrives. In this way, the bridge quickly builds up a complete picture of the network topology. If the bridge does not know the destination segment for an incoming frame, it will forward the frame to all attached segments except the segment on which the frame was transmitted. Bridges reduce the amount of traffic on individual segments by acting as a filter, isolating intra-segment traffic. This can greatly improve response times.

Switches

The switch is a relatively new network device that has replaced both hubs and bridges in LANs. A switch uses an internal address table to route incoming data frames via the port associated with their destination MAC address. Switches can be used to connect together a number of end-user devices such as workstations, or to interconnect multiple network segments. A switch that interconnects end-user devices is often called a workgroup switch. Switches provide dedicated full-duplex links for every possible pairing of ports, effectively giving each attached device its own network segment This significantly reduces the number of intra-segment and inter-segment collisions. Strictly speaking, a switch is not capable of routing traffic based on IP address (layer 3) which is necessary for communicating between network segments or within a large or complex LAN. Some switches are capable of routing based on IP addresses but are still called switches as a marketing term. A switch normally has numerous ports, with the intention being that most or all of the network is connected directly to the switch, or another switch that is in turn connected to a switch.



Network Switch

Routers

Routers are networking devices that forward data packets between networks using headers and forwarding tables to determine the best path to forward the packets. A network environment that consists of several interconnected networks employing different network protocols and architectures requires a

sophisticated device to manage the flow of traffic between these diverse networks. Such a device, sometimes referred to as an intermediate system, but more commonly called a router, must be able to determine how to get incoming packets (or datagrams) to the destination network by the most efficient route. Routers gather information about the networks to which they are connected, and can share this information with routers on other networks. The information gathered is stored in the router's internal routing table, and includes both the routing information itself and the current status of various network links. Routers exchange this routing information using special routing protocols.

A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect, and are the critical device that keeps data flowing between networks and keeps the networks connected to the Internet. When data is sent between locations on one network or from one network to a second network the data is always seen and directed to the correct location by the router. The router accomplishes this by using headers and forwarding tables to determine the best path for forwarding the data packets, and they also use protocols such as ICMP to communicate with each other and configure the best route between any two hosts. The Internet itself is a global network connecting millions of computers and smaller networks. There are various routing protocols which are helpful for various different environments and will be discussed later.

In order for the communication to take place, cables play important role. Cable is the medium through which

LAB # 2 : Networking Cables and Connections

information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. The type of cable chosen for a network is related to the network's topology, protocol, and size.

There are various types of cables used in networks as follows.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable

Twisted Pair Cables:

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs. In balanced pair operation, the two wires carry equal and opposite signals and the destination detects the difference between the two. This is known as differential mode transmission. Noise sources introduce signals into the wires by coupling of electric or magnetic fields and tend to couple to both wires equally. The noise thus produces a common-mode signal which is cancelled at the receiver when the difference signal is taken.

Categories Of UTP Cable:

It has been categorized into three categories based on the equipment that are being connected through these wires.

i. Straight Through Cable

ii. Cross Over Cable

iii. Roll Over Cable

Explanation:

Straight Through Cable:

Straight through cables are used to connect different devices like Switch to PC. Switch to Router. Router to Switch etc. Straight-through cables are used when each end of the communication transmits and receives on different pairs.

Cross Over Cable:

In a cross over the cable, the send and receive wires are "crossed over", meaning the wires are opposite on each end. This allows two PCs to talk to each other, has it connects the send of one computer to the receive of the other. Hence, the cross over cables are used to connect similar devices like PC to PC , Router to Router, Switch to Switch, Hub to Hub etc.

Roll Over Cable:

Roll over cables are used to connect to the console port of the device. It gets the name rollover because the pin outs on one end are reversed from the other, as if the wire had been rolled over and you were viewing it from the other side.

Transmission Pins:

Devices that transmit on 1,2 and receive on 3,6

1) PC

2)Router

3)Wireless Access Point AP

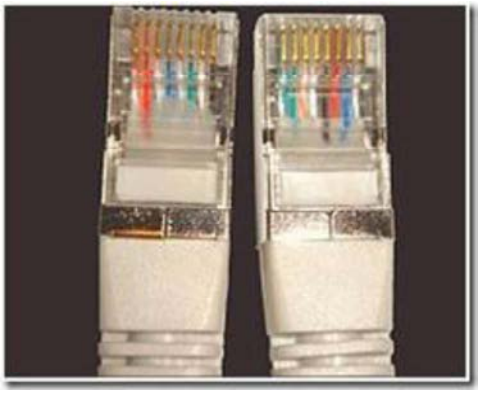
4) Networked printers

Devices that transmit on 3,6 and receive on 1,2

1)switch

2)bridge

3)hub



Required Equipment:

In order to make a network cable you need the following equipment.

i. Cat5, Cat5e cable.

CAT5 cable usually contains four pairs of copper wire, Fast Ethernet communications only utilize two pairs. A newer specification for CAT5 cable -CAT5 enhanced ("CAT5e" or "CAT 5e")- supports networking at Gigabit Ethernet[speeds (up to 1000 Mbps) over short distances by utilizing all four wire pairs, and it is backward-compatible with ordinary CAT5.

ii. A connector named RJ-45.

RJ45 connectors feature eight pins to which the wire strands of a cable interface electrically. Standard RJ-45 pin outs define the arrangement of the individual wires needed when attaching connectors to a cable.

iii. Crimping tool:

Use to crimp the cable inside RJ 45 connector.

iv. Wire stripper or Knife:

You can use a knife too to cut the wire open. In order to make different combinations of it. we will have to cut the upper protective coating and bring out the eight wires.

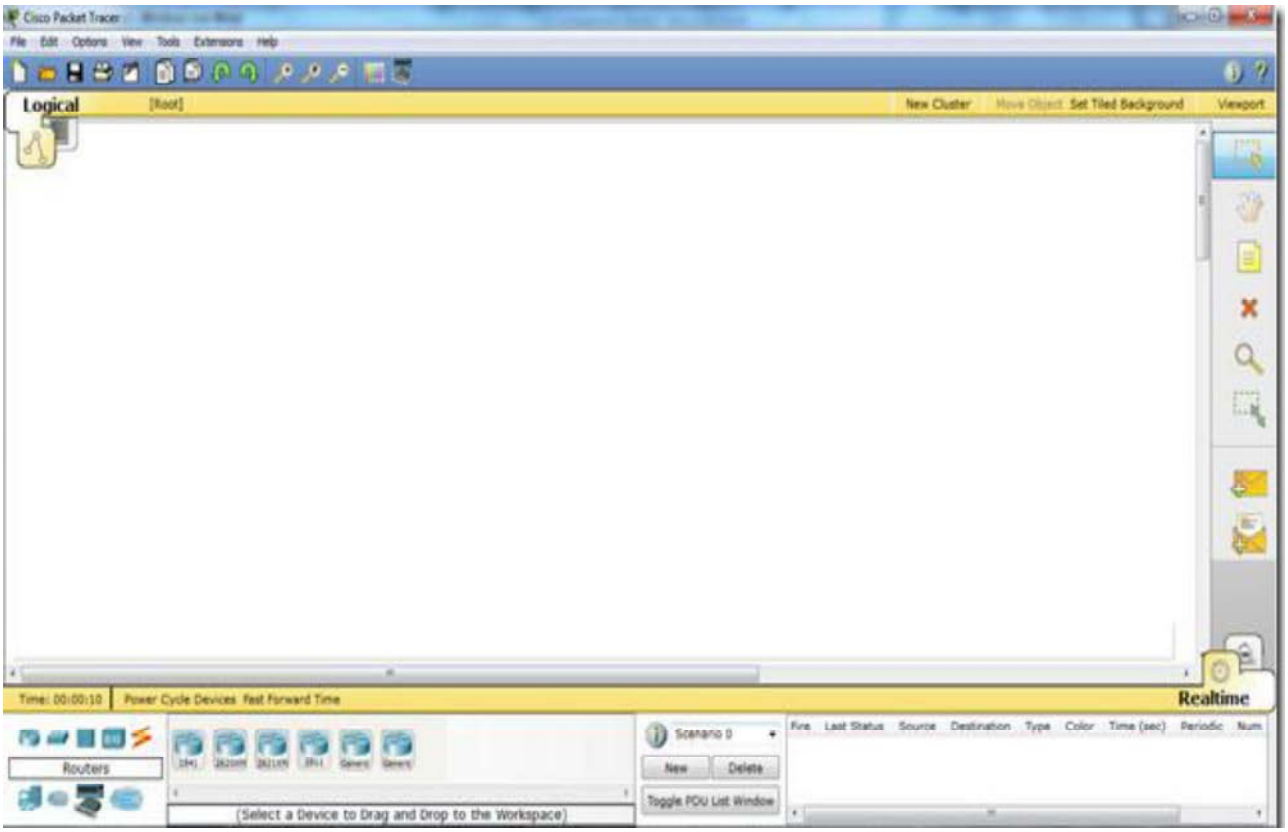
Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair)	100BaseT Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Auto-MDIX:

Auto-MDIX (automatic medium-dependent interface crossover) is a computer networking technology that automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately, thereby removing the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. When it is enabled, either type of cable can be used and the interface automatically corrects any incorrect cabling. For Auto-MDIX to operate correctly, the speed on the interface and duplex setting must be set to "auto".

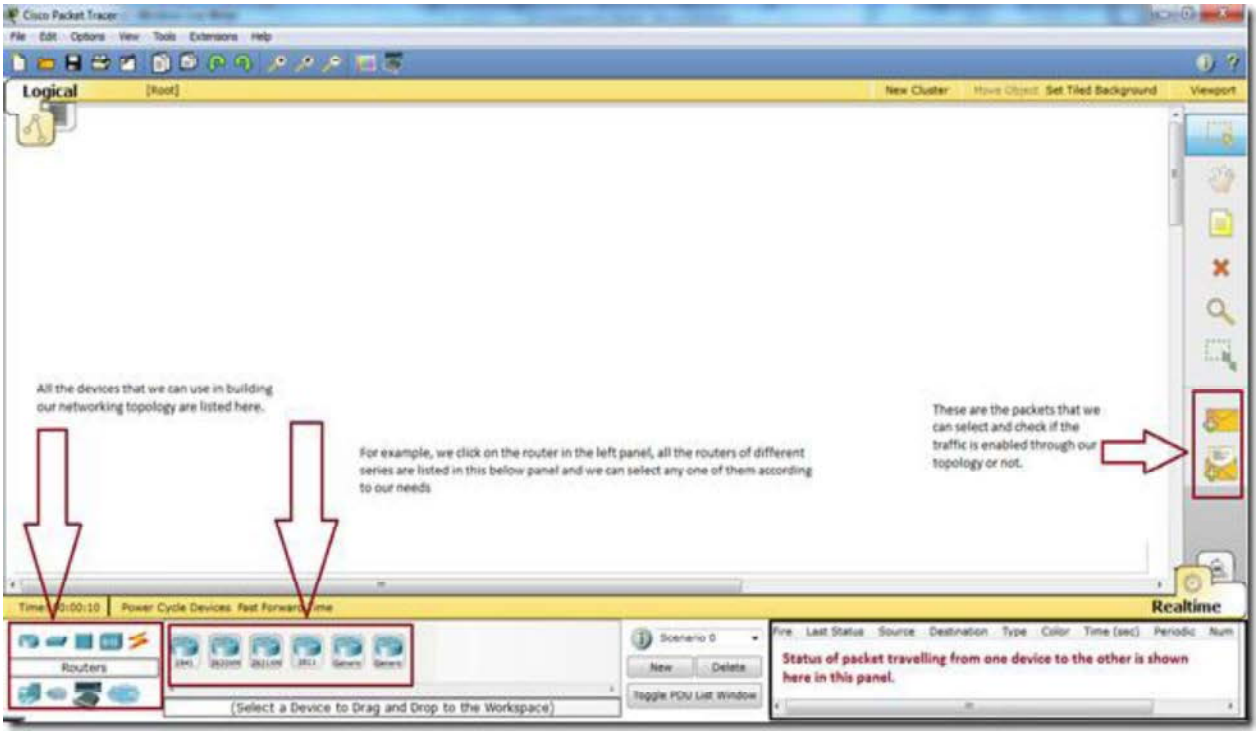
LAB # 3 : What is Packet Tracer

Packet Tracer is a powerful network simulator that can be utilized in training for CCNA and CCNP certification exam by allowing students to create networks with an almost unlimited number of devices and to experience troubleshooting without having to buy real Cisco routers or switches. The tool is created by Cisco Systems. The purpose of Packet Tracer is to offer students a tool to learn the principles of networking as well as develop Cisco technology specific skills. However, it is not be used as a replacement for Routers or Switches. Here how it looks like after we start it.

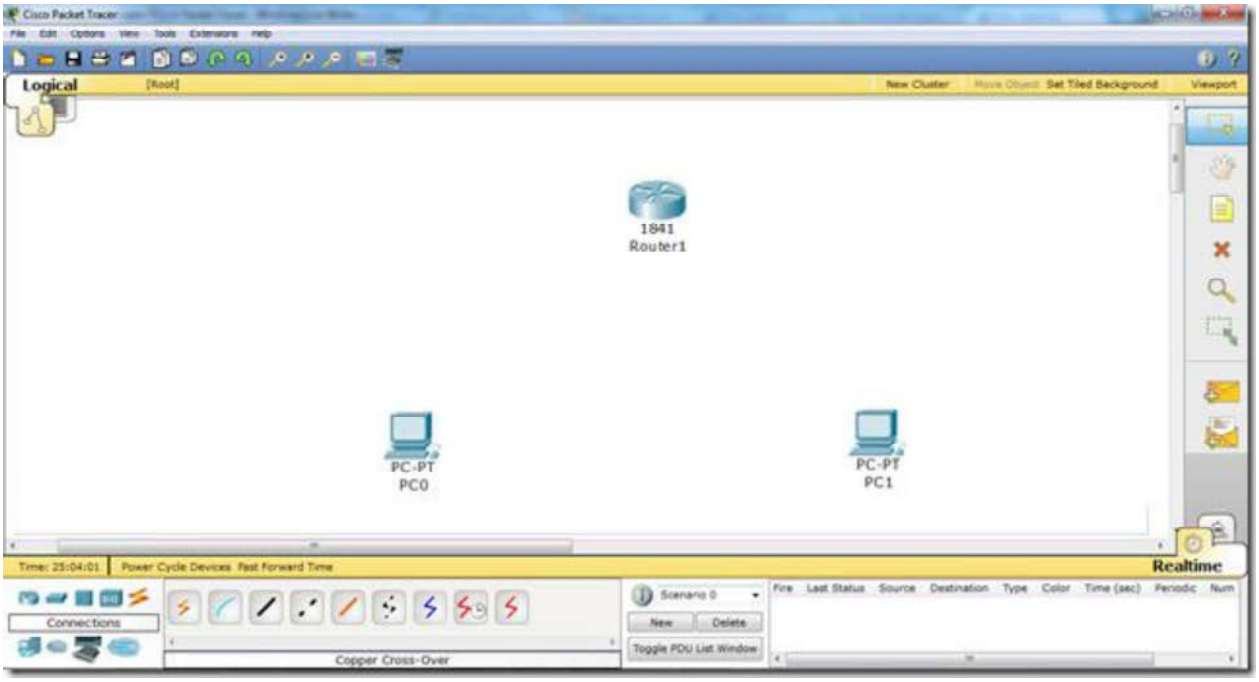


We are different modules and panels available in the packet tracer. Some important modules, which are important to

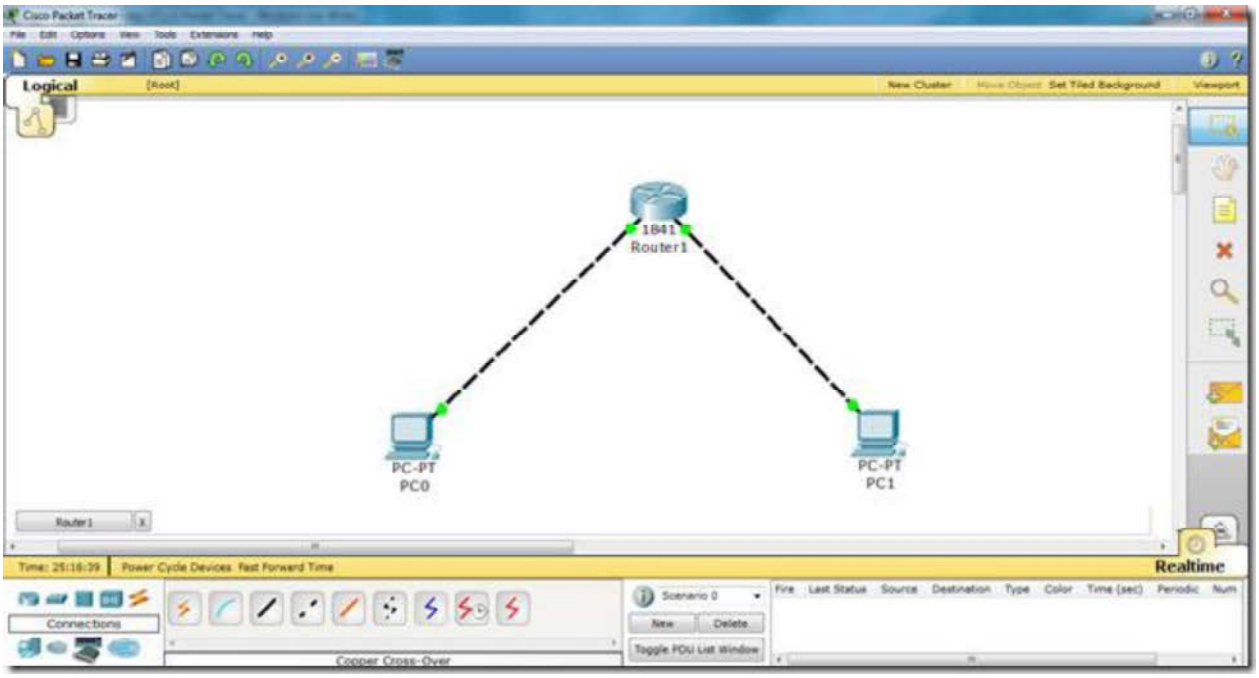
understand for the working in Packet Tracer, are mentioned in the following diagram.



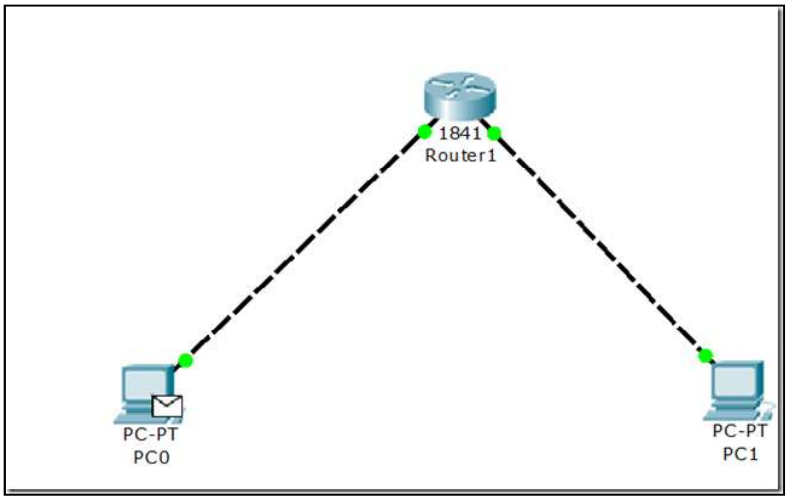
Now, in order to create a topology, we will have to select some of the devices and put them in our main window i.e. the white portion of packet tracer. and here how it looks after we add the devices.



Now, we will have to connect these devices and for that we use cables.



And after you successfully create the topology, you can check either the traffic is flowing or not by selecting the packet from right panel and putting it on both PCs as follows.



LAB # 4 :Packet Tracer CLI

There are various common commands that one needs to be familiar with. These commands will be used all the time. There are different modes. All modes have their own distinct commands.

Router>**enable** = Router>**enab** = Router>**en**	Entering a shortened form of a command is sufficient as long as there is no confusion about which command you are attempting to enter.
Router#**configure terminal** is the same as Router#**config t**	

All the configuration commands will be written in configuration mode.

Using the tab Key to Complete Commands

When you are entering a command, you can use the tab key to complete the command. Enter the first few characters of a command and press the tab key. If the characters are unique to the command, the rest of the command is entered in for you. This is helpful if you are unsure about the spelling of a command. For example, if we write in enable mode, "sh" and press tab button, "show" command will be written on the CLI mode.

Router#sh [Tab] = Router#**show**	

Router Modes

Router>	User mode
Router#	Privileged mode (also known as EXEC-level mode)
Router(config)#	Global configuration mode
Router(config-if)#	Interface mode

Router(config-subif)#	Subinterface mode
Router(config-line)#	Line mode
Router(config-router)#	Router configuration mode

TIP: There are other modes than these. Not all commands work in all modes. Be careful. If you type in a command that you know is correct—**show running-config**, for example—and you get an error, make sure that you are in the correct mode.

Entering Global Configuration Mode

Router>	Limited viewing of configuration. You cannot make changes in this mode.
Router#	You can see the configuration and move to make changes.
Router#**configure terminal** Router(config)#	Moves to global configuration mode. This prompt indicates that you can start making changes.

Configuring a Router Name

This command works on both routers and switches.

`Router(config)#hostname Cisco`	The name can be any word you choose.
`Cisco(config)#`	

Configuring Passwords

These commands work on both routers and switches.

`Router(config)#enable password cisco`	Sets enable password
`Router(config)#enable secret class`	Sets enable secret password

Here it is important to know that the enable secret password is encrypted by default. The enable password is not. For this reason, recommended practice is that you *never* use the enable password command. Use only the enable secret password command in a router or switch configuration. You cannot set both enable secret *password* and enable *password* to the same password. By doing so, it defeats the use of encryption.

Show Commands:

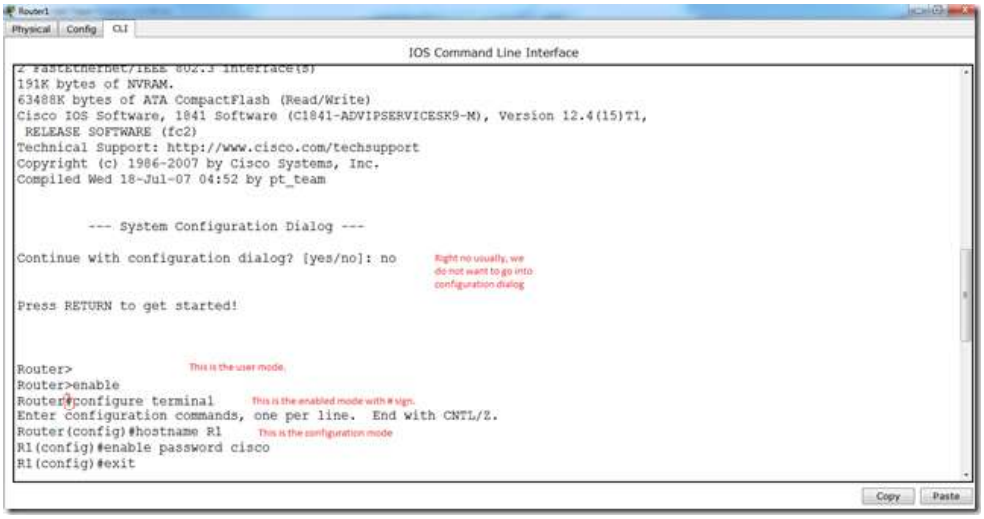
There are various show commands. in order to get familiar with these commands just write “show ?” in the enable mode.

Similarly, there are various commands that shows us the configurations that we have done on our router or any other device depending on the device we are working on. We will talk about later on.

Similarly, there are various commands in the configuration mode which we attain by entering the following command

Router# configure terminal.

Look at the following diagram.



Ok, so now lot of things are happening here. Red markers explain them, also we are setting the hostname of the router and we have successfully applied the password by the following command.

enable password cisco

Here, “cisco” is the password.

Similarly, the command

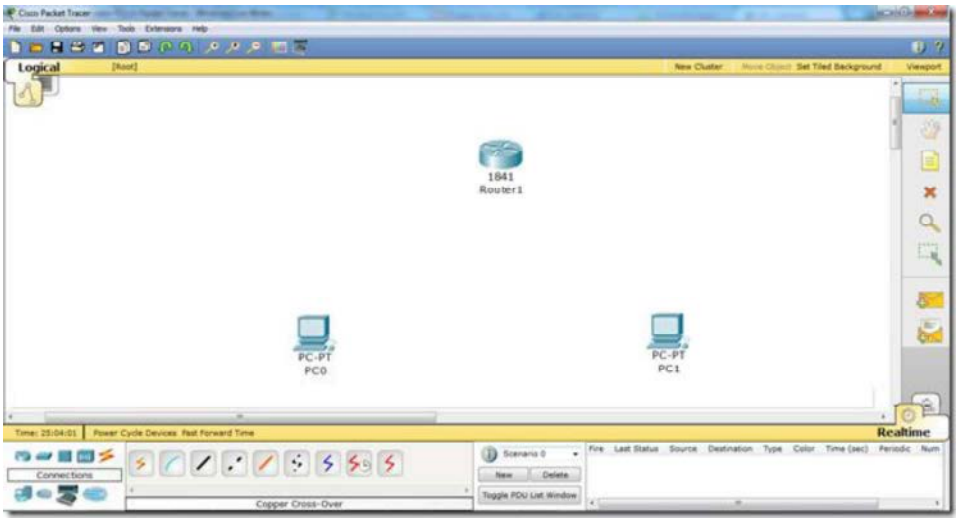
router#show ip interface brief

gives us the information about the interfaces of the router. Now, detail discussion on the interfaces will be done later

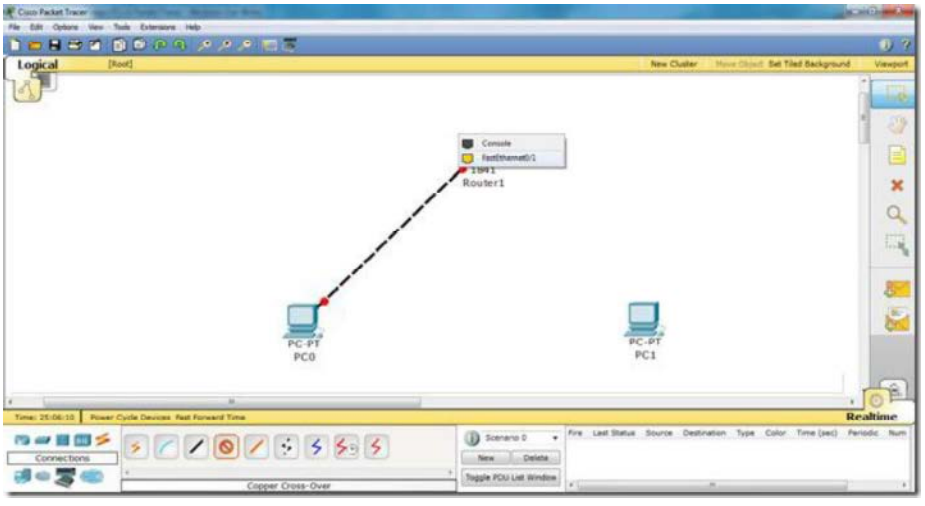
LAB # 5: Communication between PCs in Packet Tracer

Here, we will see communication enabled between PCs via Router in Packet Tracer. So, for this we need two PCs, a router ,and two cross over cables to connect them. Important point is that we use cross over cable to connect PC to a router because they both use the same pins for transmission and receiving of data.

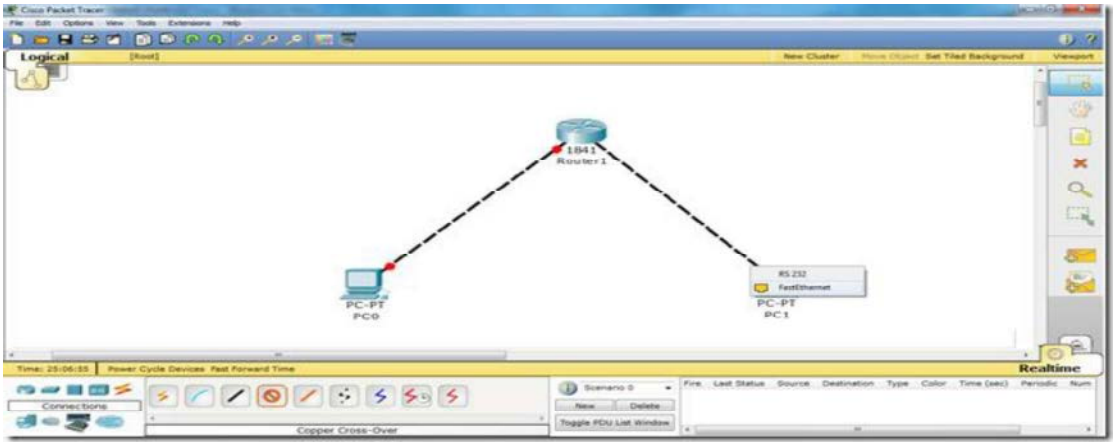
Here, we will see communication enabled between PCs via Router in Packet Tracer.
So, for this we need two PCs, a router ,and two cross over cables to connect them.
Important point is that we use cross over cable to connect PC to a router because they both use the same pins for transmissio n and receiving of data.



Now, we will connect them by selecting fast ethenet interfaces on both ends.



Similarly, on the PC side we will select fast Ethernet interface.



Now, we have connect the devices. Further, we will go to the router CLI mode and enter the following commands.

Step by step ,

we will have to do the following things.

i. Access the interfaces one by one

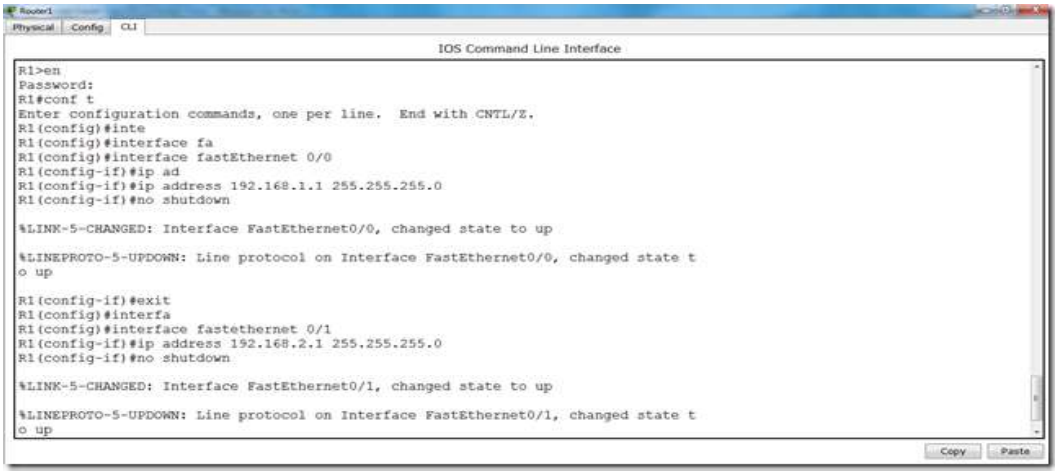
ii. Assign IP addresses to interfaces

iii. Change the status of the interfaces i.e. from Down to Up.

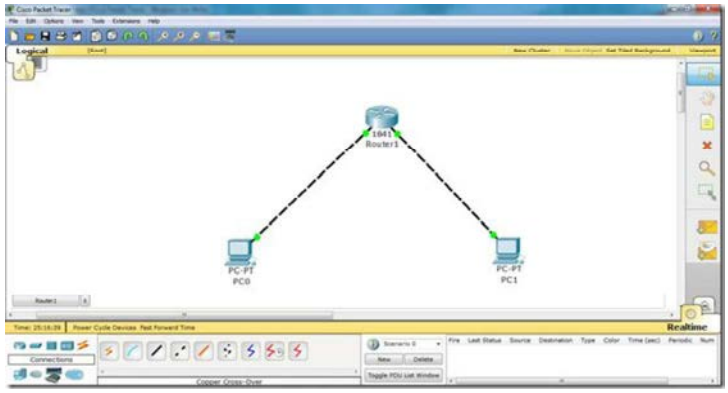
iv. Assign IP addresses to PCs.

v. Assign Default GateWay to PCs. FYI fast ethernet ip address is the gateway address to the PC.

Now, commands of the Router CLI mode are as follows.



Now, we have accessed both interfaces one by one and we have assigned IP addresses respectively.

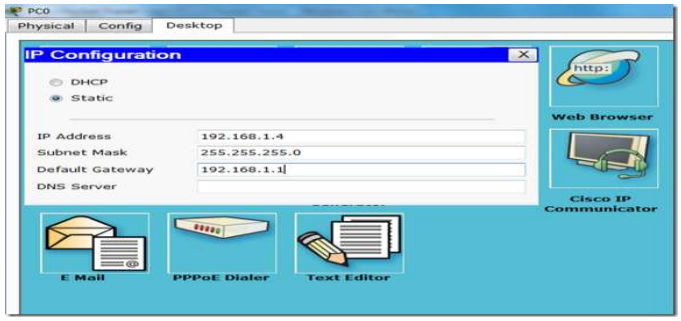


See the difference the lights have changed the color from Red to Green :)

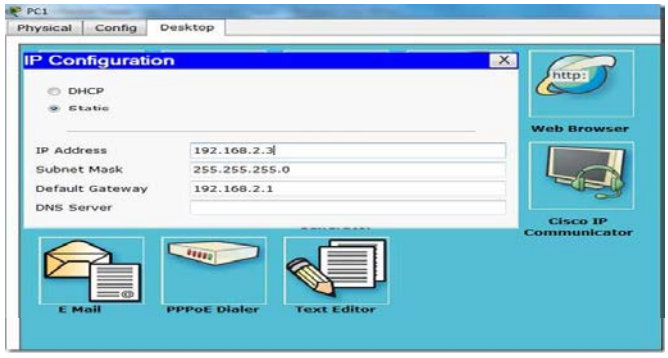
Now, lets assign IP addresses to the PCs.

Click on PC1, go to Desktop, then dick IP Configuration.

PC1:

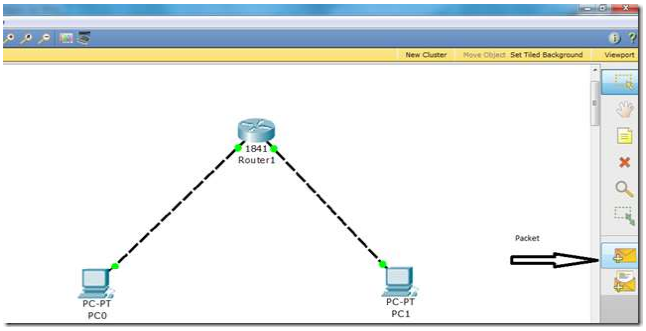


PC2:

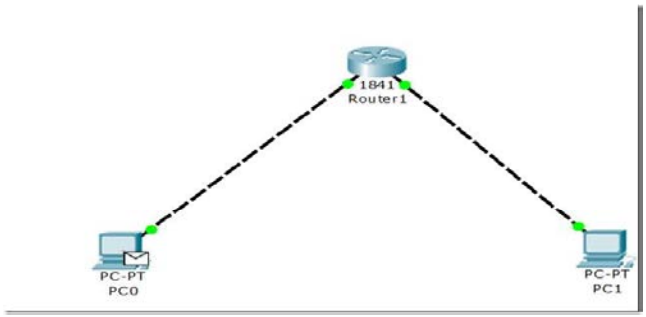


Now, our communication is enabled and we are able to communicate from PC1 to PC2 via Router.

Click on the packet in the right panel on the packet tracer, then click on PC1 and then click on PC2. You will see the successful packet tracer (status is shown in the bottom right corner)



Select it and dick on both PCs.



Bingo, your communication is successful.

LAB # 6: RIP on Packet Tracer

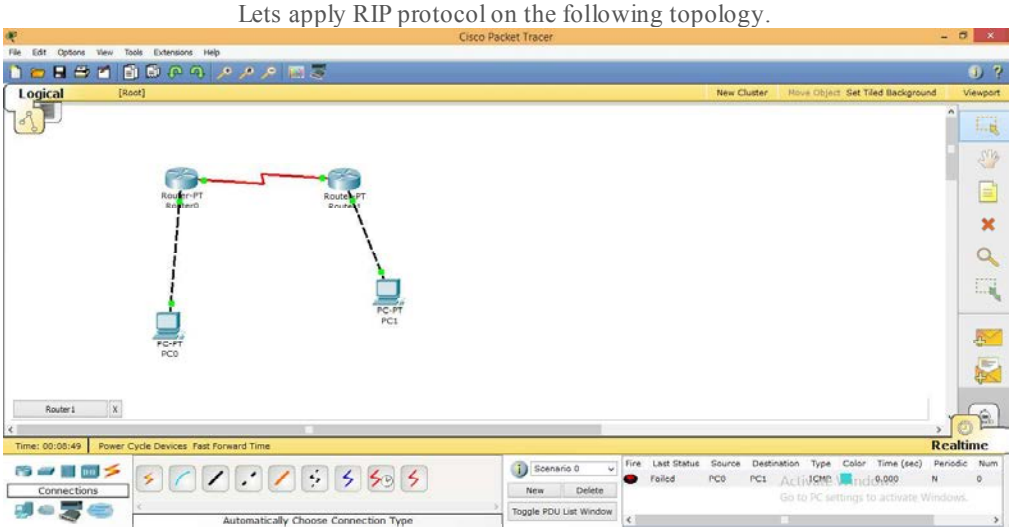
Main Commands

`Router(config)#router rip`	Enables RIP as a routing protocol.
`Router(config-router)#network w.x.y.z`	w.x.y.z is the network number of the *directly connected* network you want to advertise.

You need to advertise only the classful network number, not a subnet.

Explanation:

Lets apply RIP protocol on the following topology.



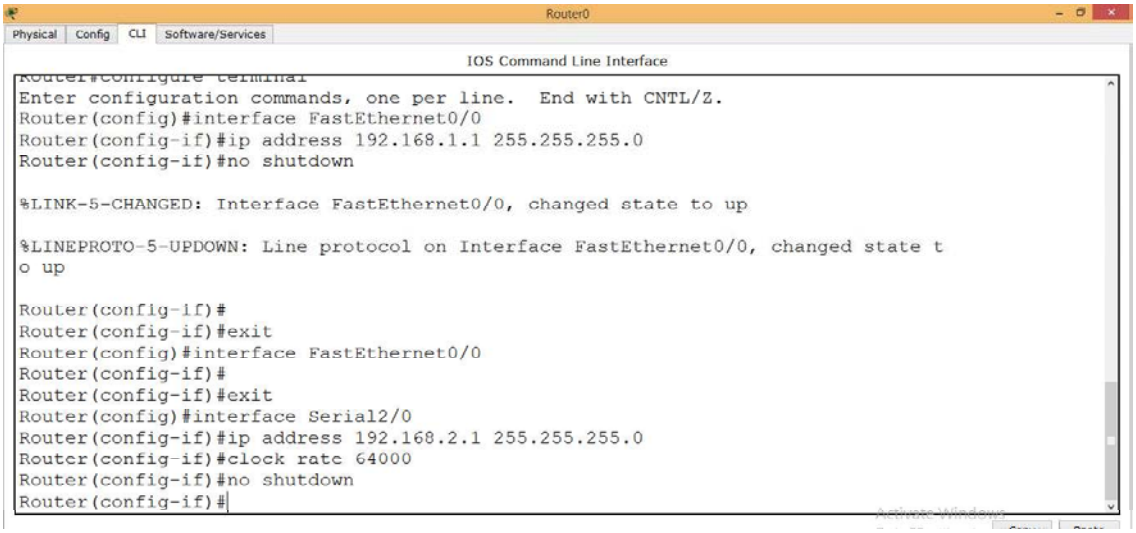
Now, we will follow the steps as mentioned in detail in the following article. i.e.

i. We will assign IP addresses to all the fast Ethernet and serial interfaces respectively.

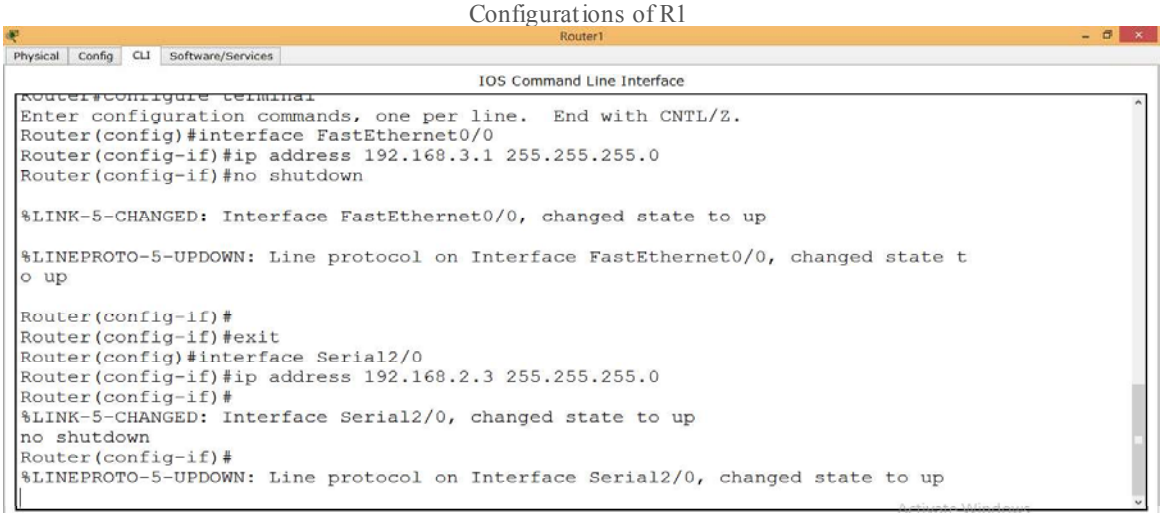
ii We will change the state of the interfaces from down to UP.

Then, after we are done with the basic step. We will apply RIP protocol commands on both routers.

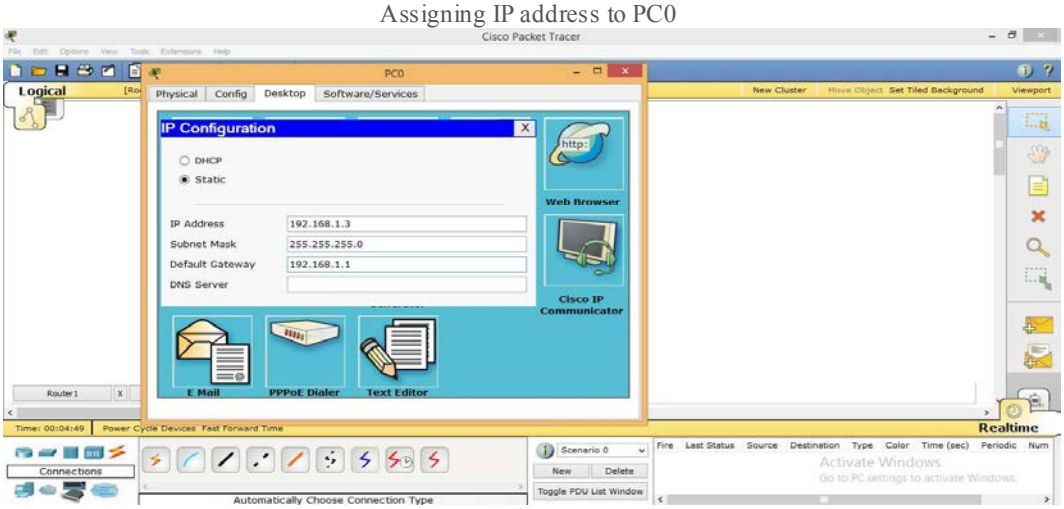
Configuration of Router 0 i.e. configuring both serial and fastethernet interfaces.



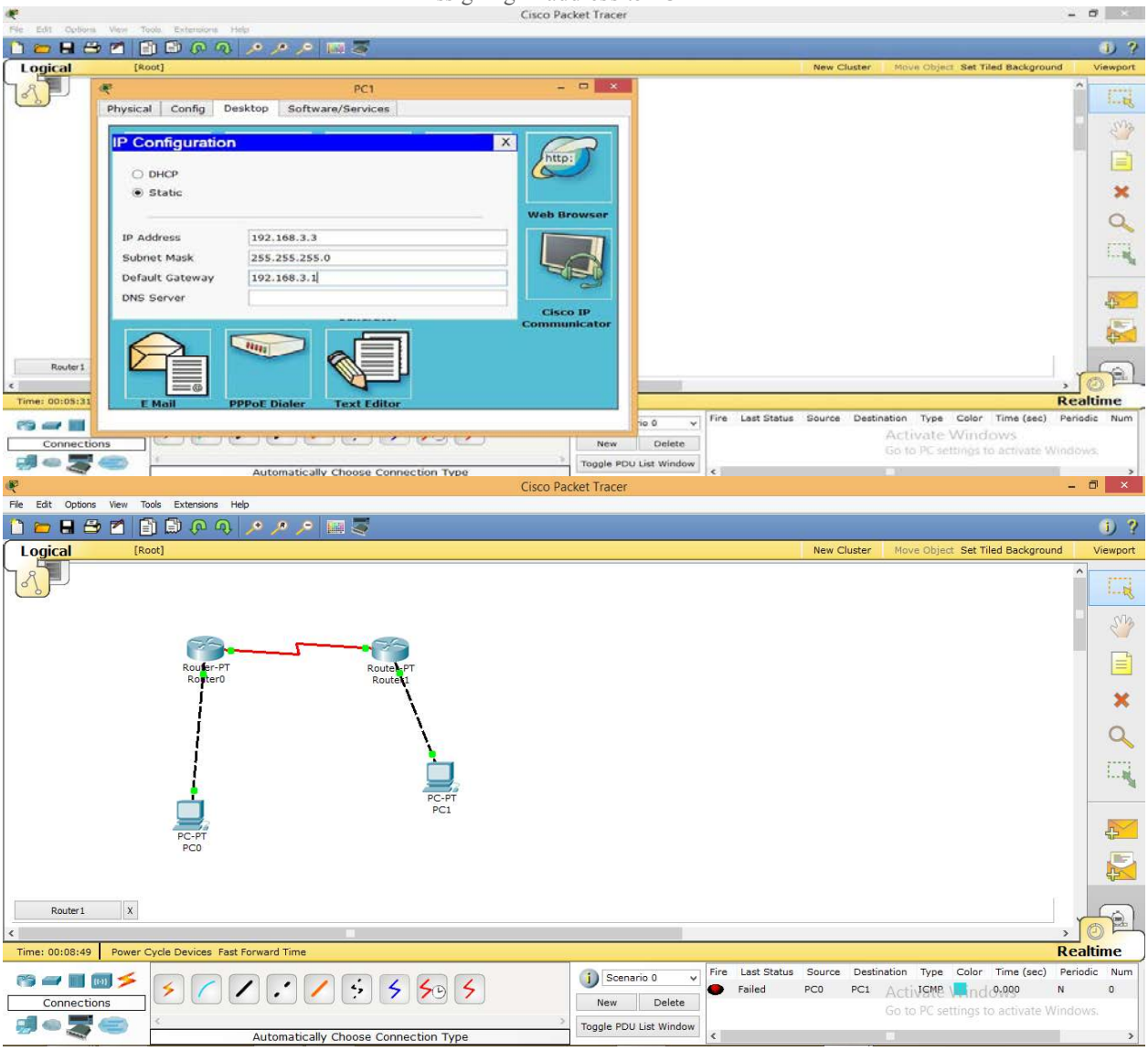
Configurations of R1



Assigning IP address to PC0



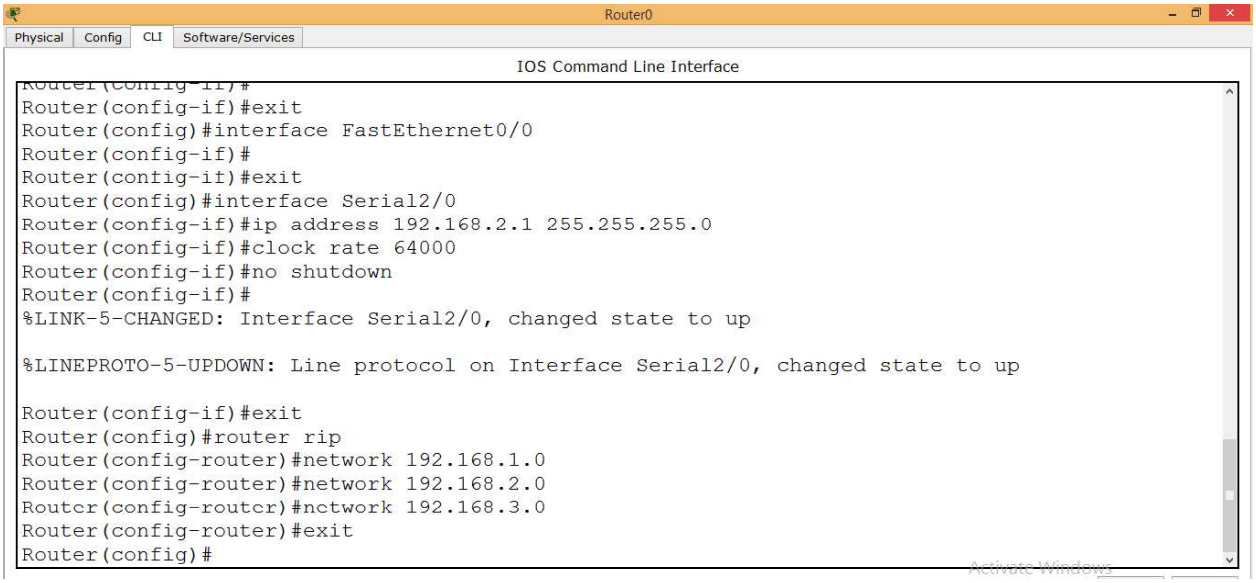
Assigning IP address to PC1



R1

In order to apply protocol RIP, we will write the following set of commands.

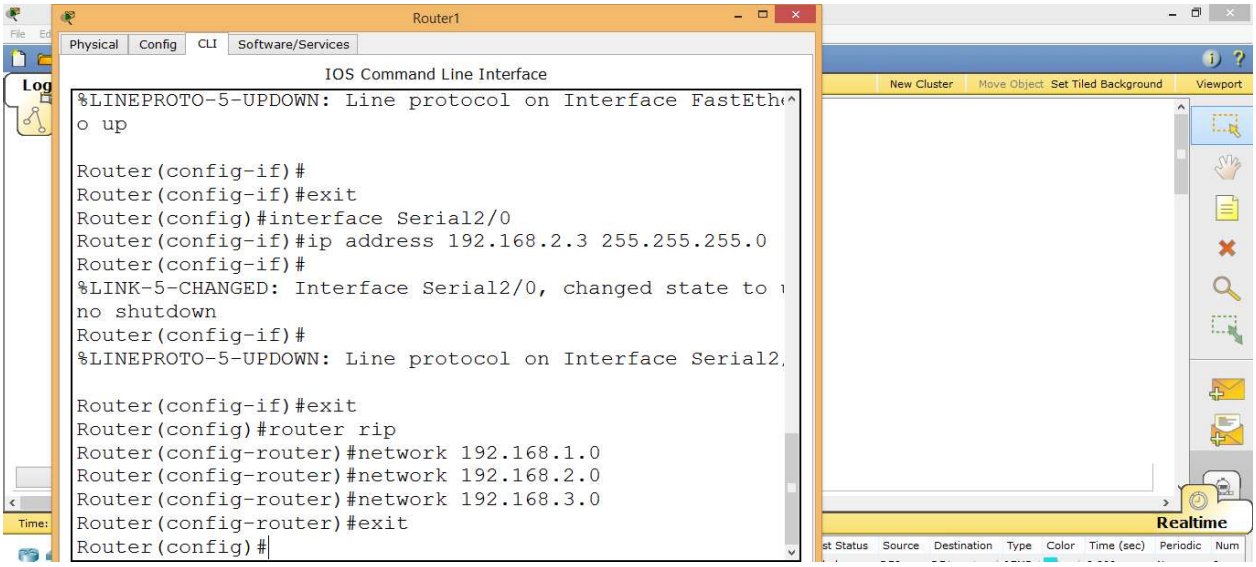
Router(config)# router rip
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
Router(config-router)# network 192.168.3.0
Router(config-router)#exit

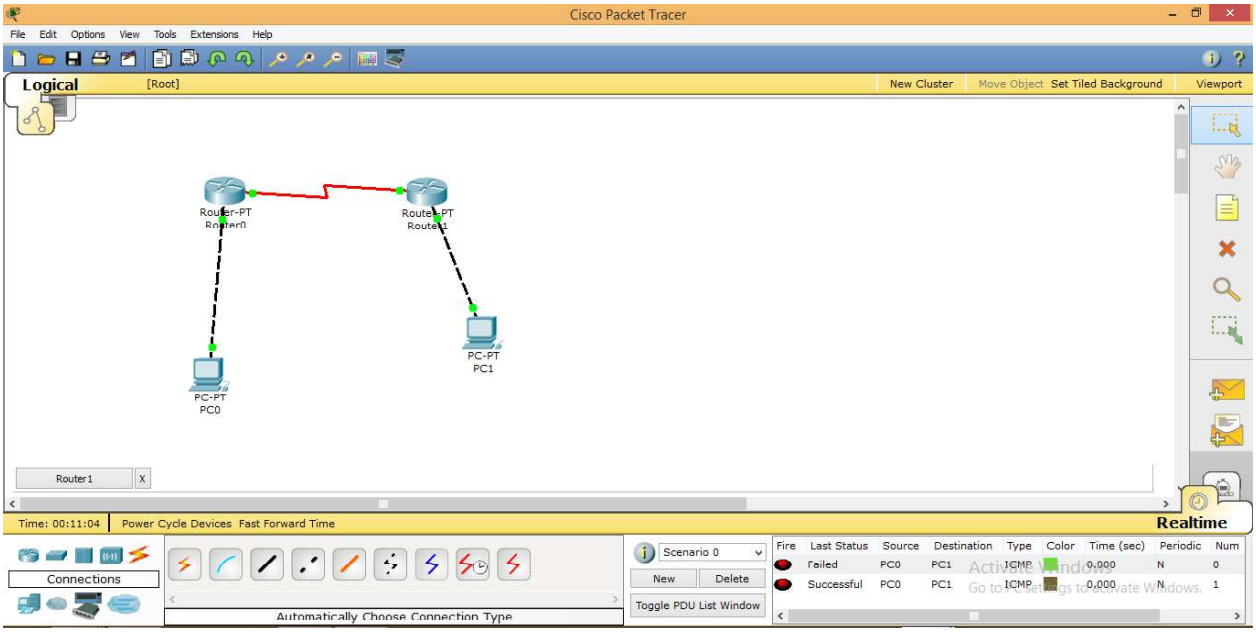


R2:

In order to apply protocol RIP, we will write the following set of commands on R2 as well.

Router(config)# router rip
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
Router(config-router)# network 192.168.3.0
Router(config-router)#exit



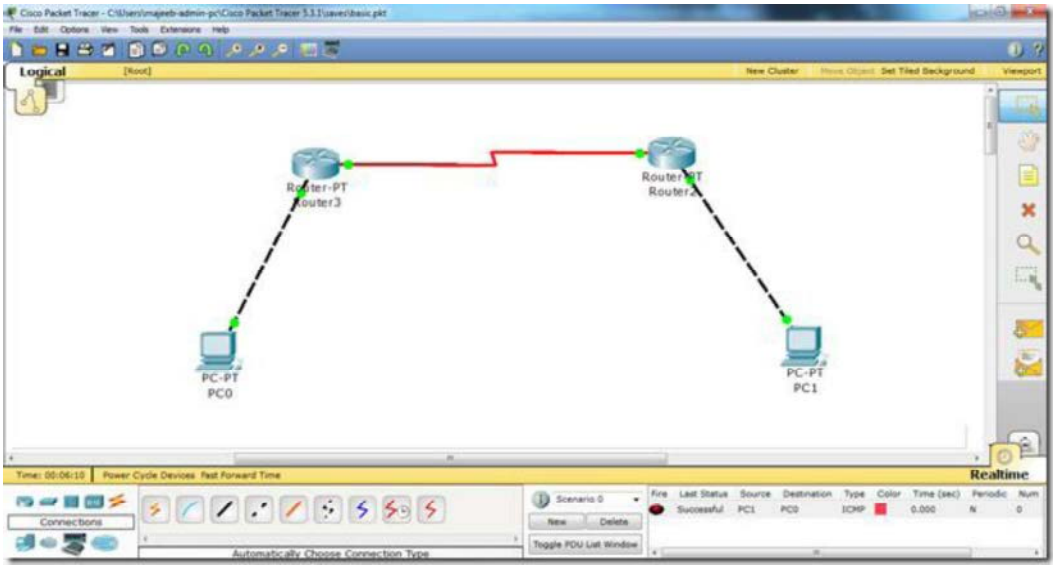


Write all the commands in the same fashion as in the above screen shots and voila, we are done with RIP protocol. Another important thing here is that we will add all the networks that we are using in our topology. Here in this particular example i am just using two networks x.x.1.0 and x.x.2.0 so thats why i have added these two network addresses to the RIP protocol.

Now, you can check it. Traffic is enabled and you can easily send data from PC0 to PC1.

LAB # 7: RIP Version 2 on Packet Tracer

There is no big difference between RIP version 1 and version 2 when we are applying them in packet tracer. In order to apply RIP version 2 on packet tracer. we will just have to add the following command. We will follow the same example that we used in RIP version 1.



Router(config)# router rip

Router(config-router)# network 192.168.1.0

Router(config-router)# network 192.168.2.0

Router(config-router)# version 2

Router(config-router)#exit

You see there is just the addition of one statement i.e. “version 2”. The rest is the same. We will apply the above set of commands on both routers i.e. Router 3 and Router 2 ,used in the topology above which is also used in this article, above and bingo, we have applied RIP V2 on packet tracer.

Just make sure that the protocol is applied as an additional step and cannot replace the basic steps i.e. we have to assign IP addresses to the router’s interfaces and PCs and also change the state of the interfaces from down to UP like in this article and then we will go ahead and apply Protocol.

LAB # 8: EIGRP on Packet Tracer

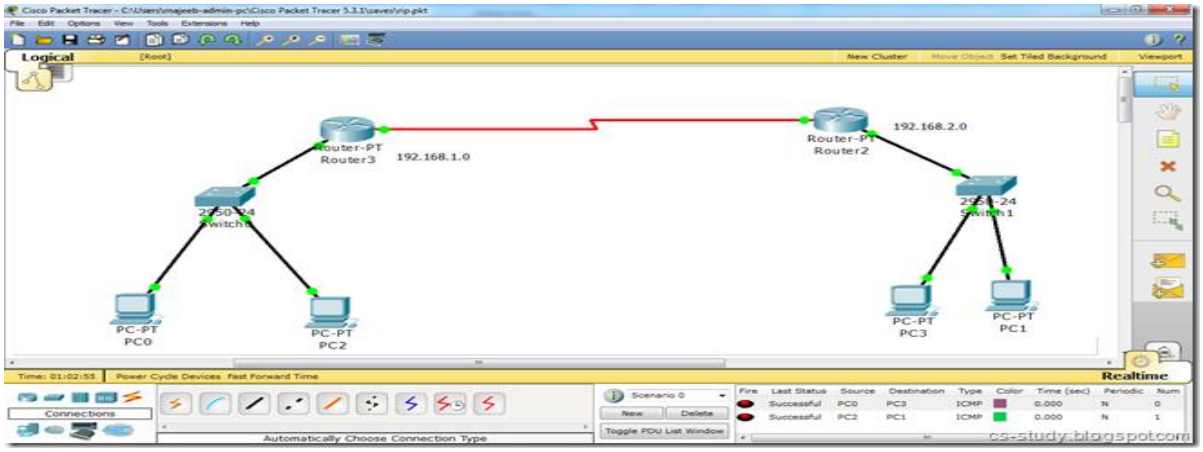
Hi everyone, today we are going to apply Enhanced Interior Gate Way Routing Protocol (EIGRP) on packet tracer. Here are the basic set of commands that we can apply on router CLI mode in order to apply EIGRP on router.

`Router(config)#router eigrp 100`	Turns on the EIGRP process. 100 is the autonomous system number, which can be a number between 1 and 65,535.
	All routers in the same autonomous system must use the same autonomous system number.
`Router(config-router)#network 10.0.0.0`	Specifies which network to advertise in EIGRP.
`Router(config-if)#bandwidth x`	Sets the bandwidth of this interface to *x* kilobits to allow EIGRP to make a better metric calculation.
	TIP: The **bandwidth** command is used for metric calculations only. It does not change interface performance.
`Router(config-router)#no network 10.0.0.0`	Removes the network from the EIGRP process.

Also, look at some additional commands.

`Router#show ip eigrp neighbors`	Displays the neighbor table.
`Router#show ip eigrp neighbors detail`	Displays a detailed neighbor table.
	TIP: The **show ip eigrp neighbors detail** command verifies whether a neighbor is configured as a stub router.
`Router#show ip eigrp interfaces`	Shows information for each interface.
`Router#show ip eigrp interfaces serial 0/0`	Shows information for a specific interface.
`Router#show ip eigrp interfaces 100`	Shows information for interfaces running process 100.
`Router#show ip eigrp topology`	Displays the topology table.
	TIP: The **show ip eigrp topology** command shows you where your feasible successors are.
`Router#show ip eigrp traffic`	Shows the number and type of packets sent and received.
`Router#show ip route eigrp`	Shows a routing table with only EIGRP entries.

Now, we are going to apply EIGRP on the following topology.



Now, after successfully applying IP addresses like in this topology, we will apply following commands.

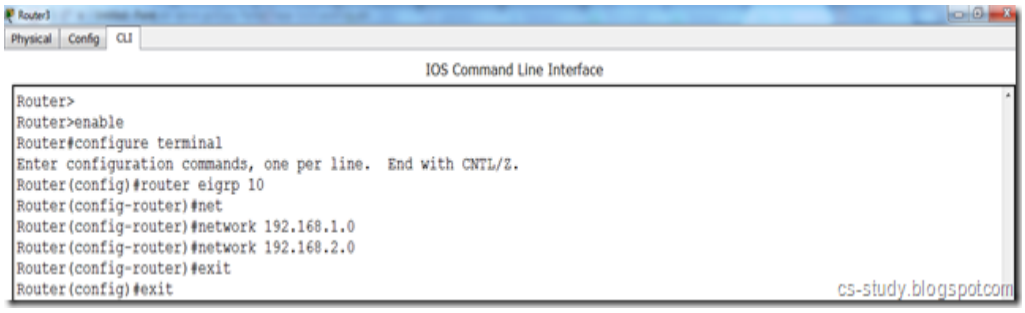
Router(config)#router eigrp 10

Router(config-router)#network 192.168.1.0

Router(config-router)#network 192.168.2.0

Router(config-router)#exit

Apply the above set of commands on both routers like this.



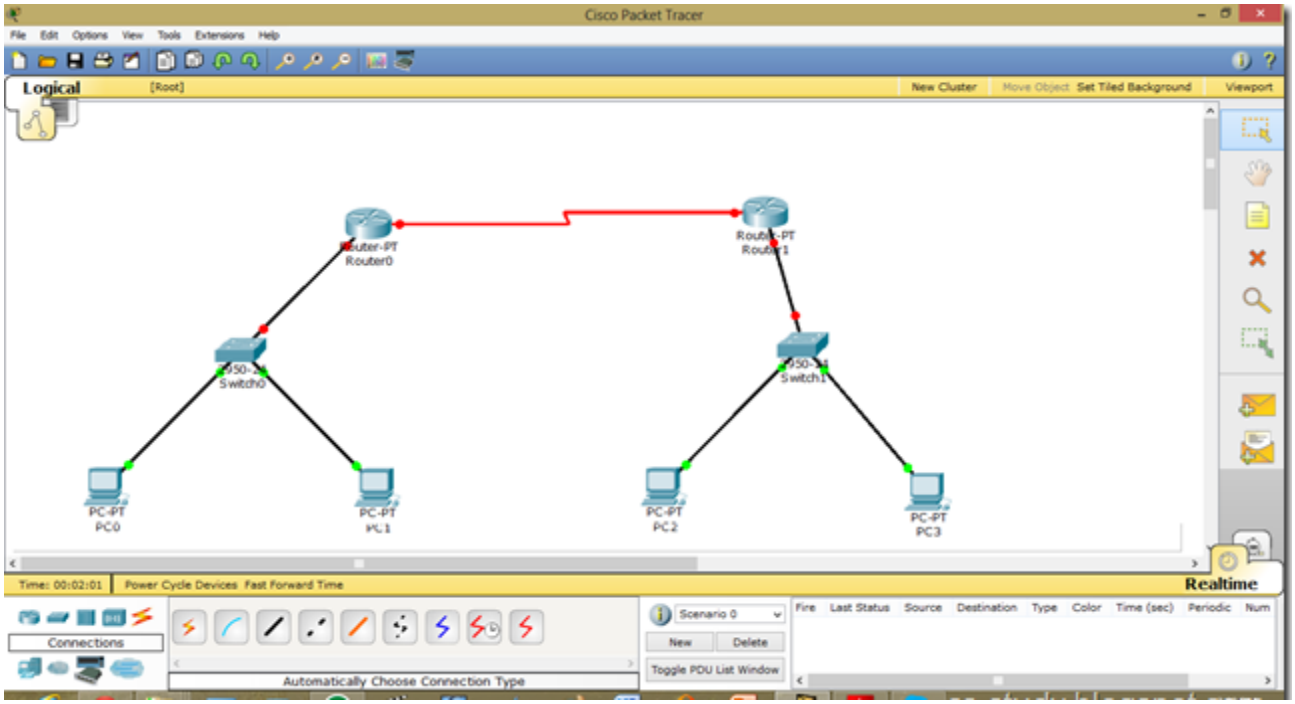
And eigrp protocol has been applied on this topology. Notice the following command.

router eigrp 10

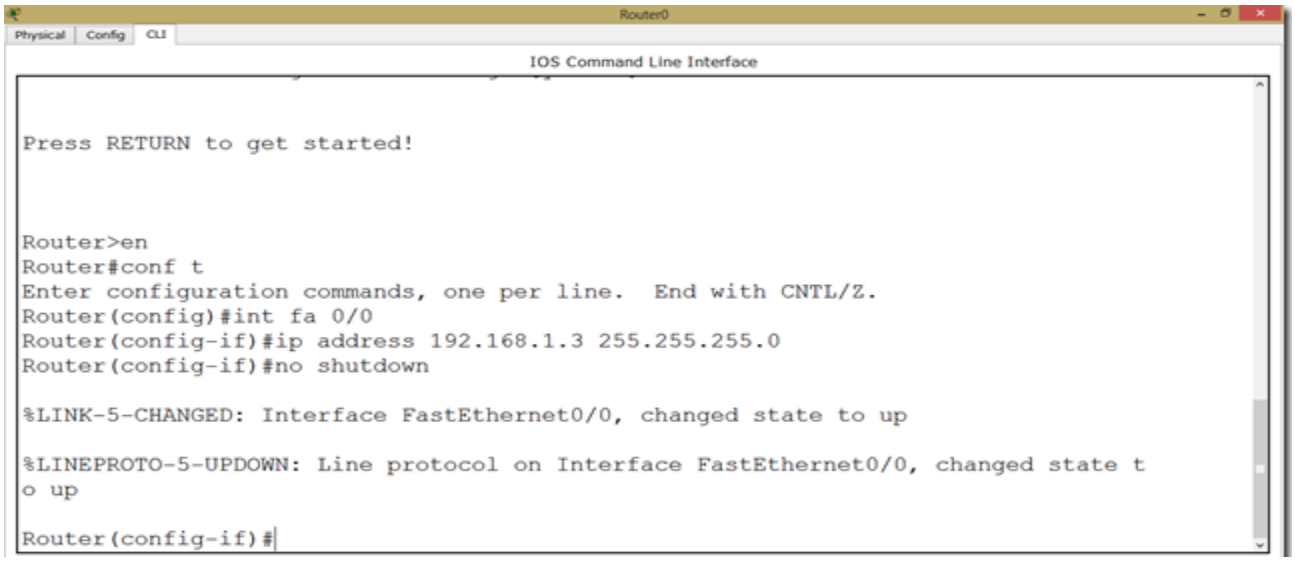
This number '10' is the process ID.

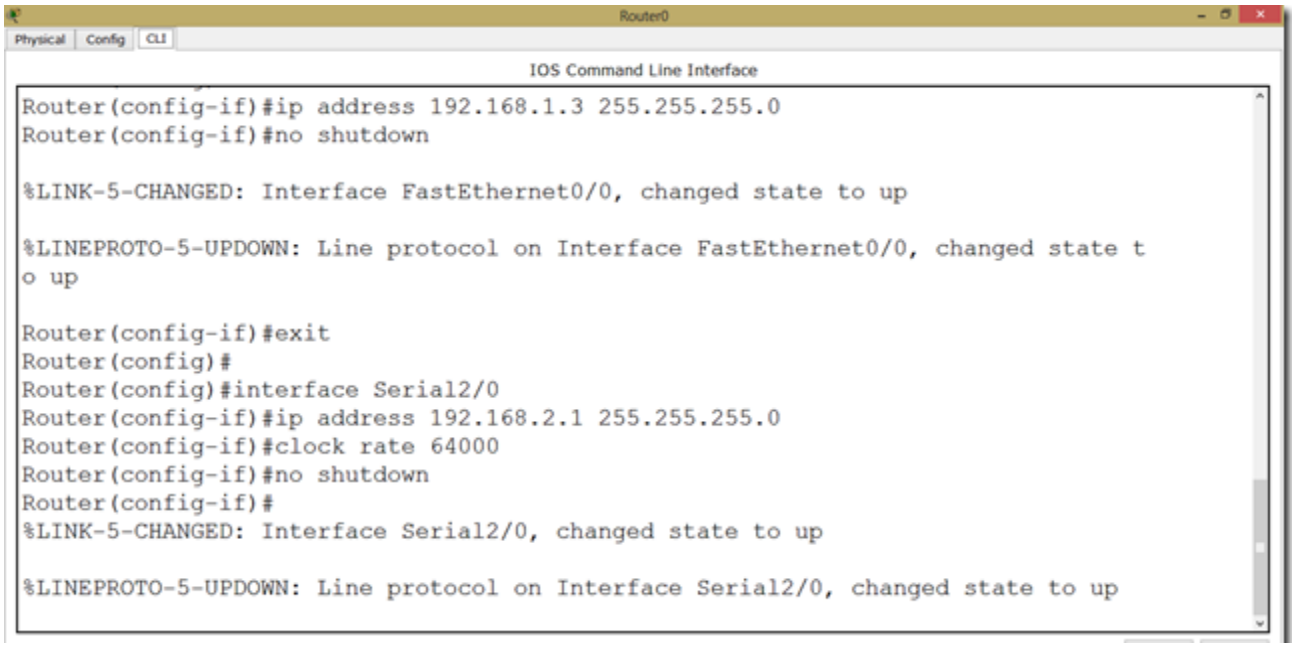
LAB # 9: OSPF on Packet Tracer

We are going to apply OSPF(open shortest path first) protocol on packet tracer. Let us take the following simple topology.

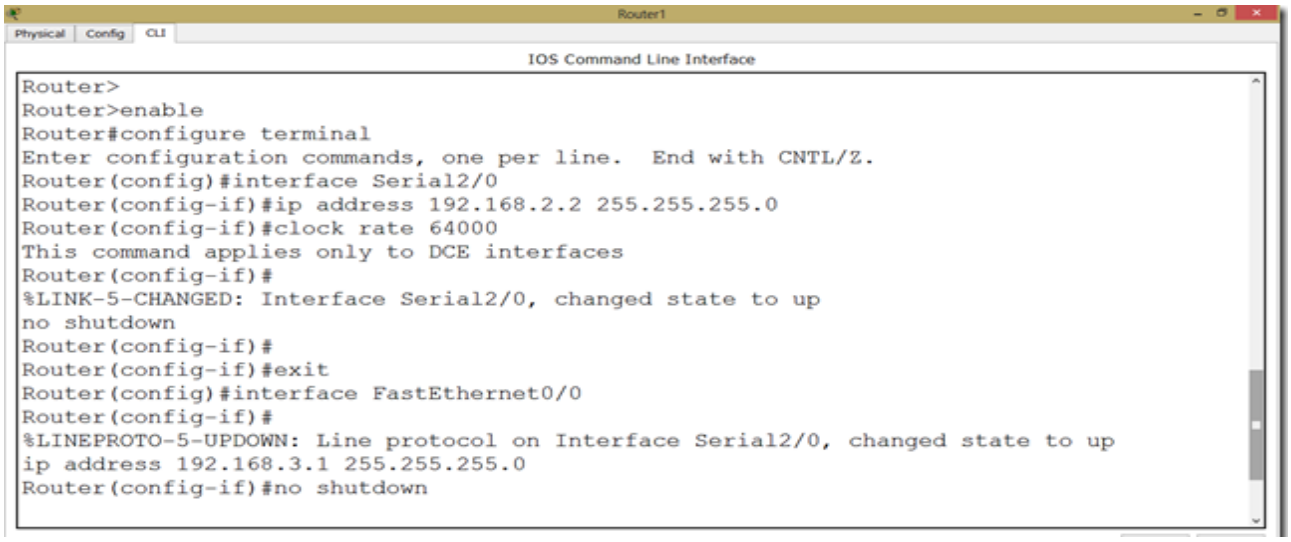


Now, let us apply the ospf on it. But before that, as usual :) , let us assign IP addresses and change the state of interfaces.

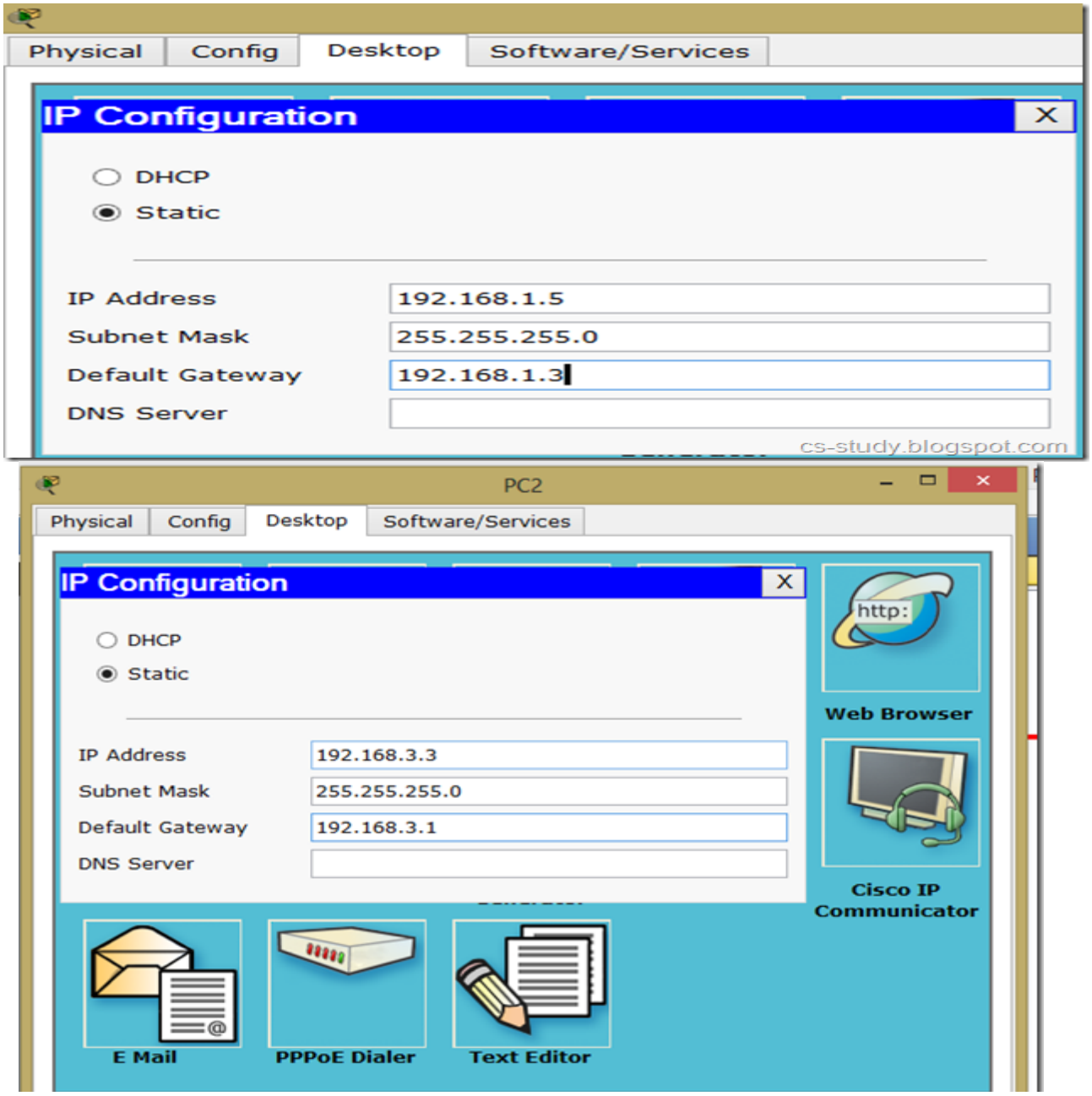




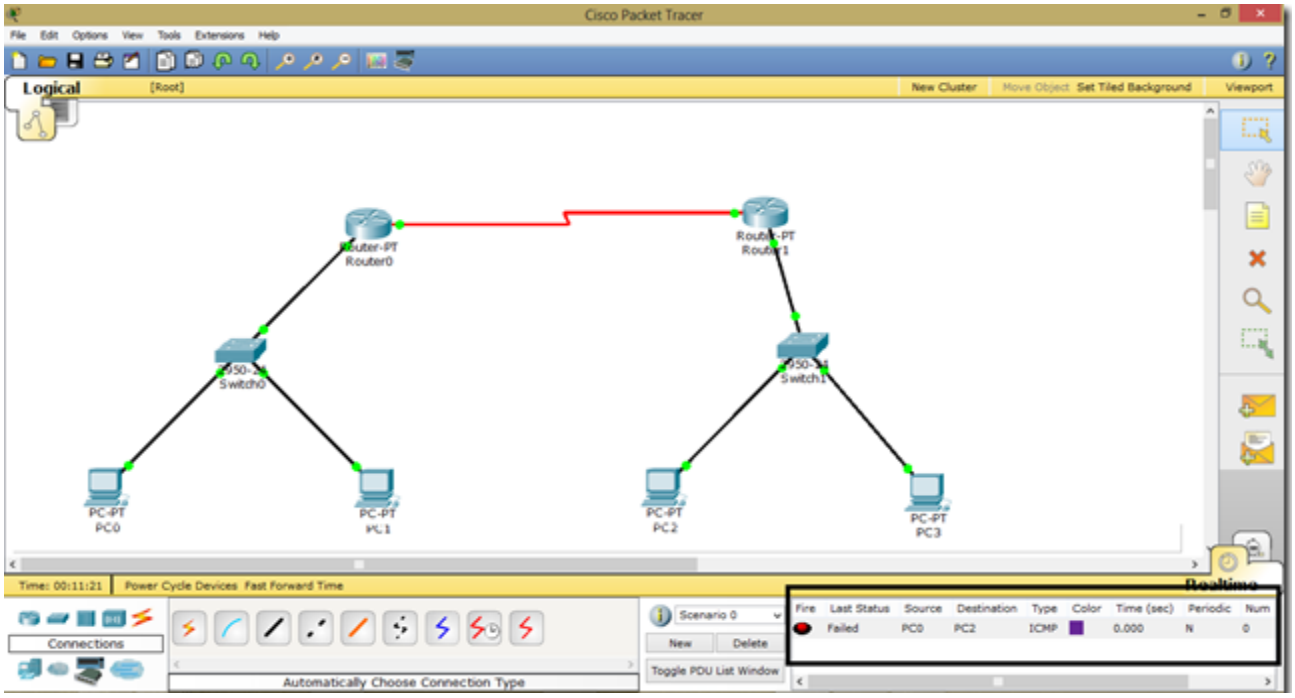
Similarly for the other router.



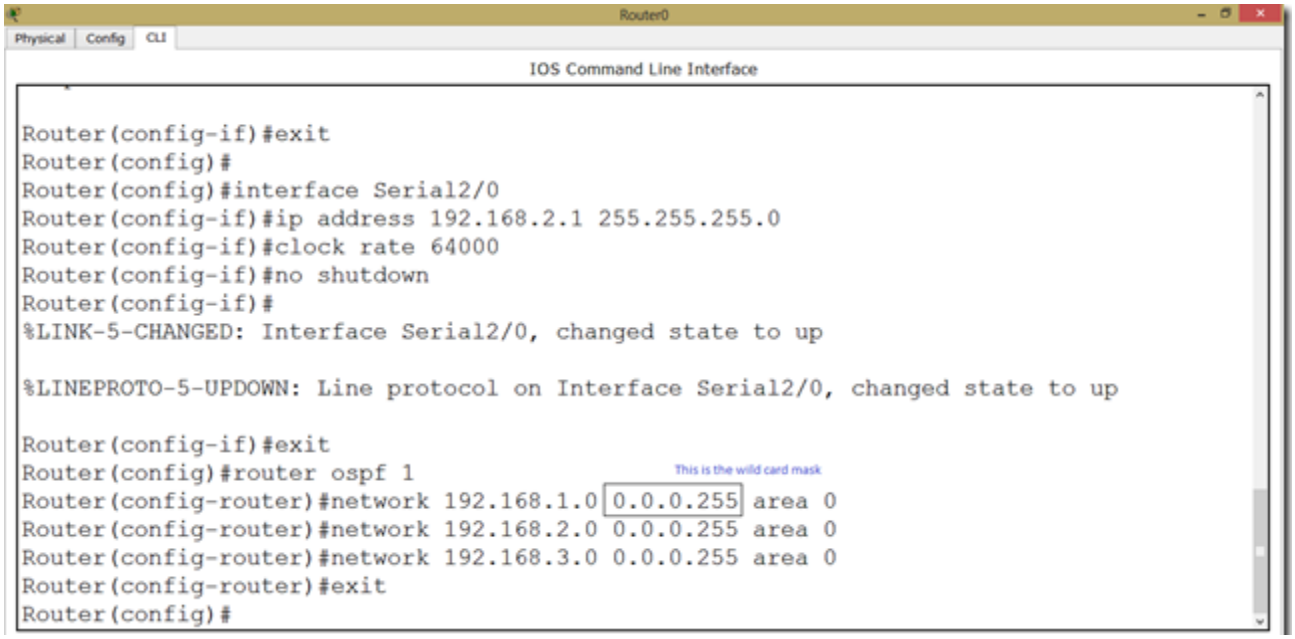
Assigning the IP addresses to PCs as follows.



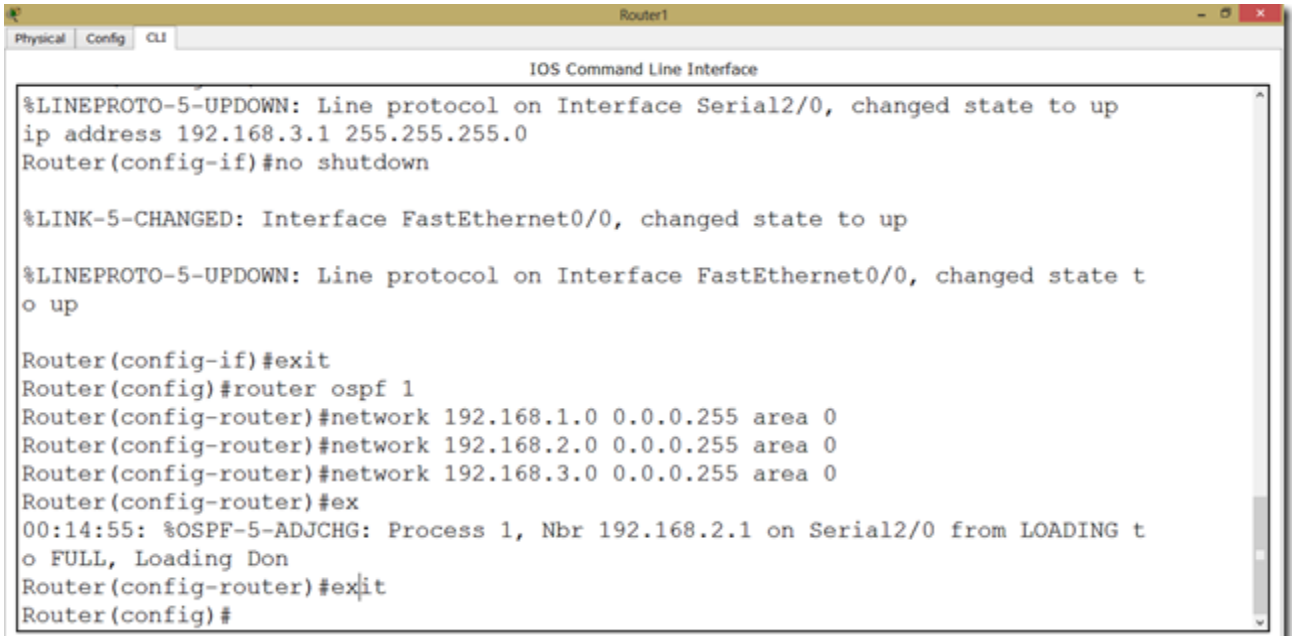
Now, as we can see, interfaces are up but the communication is not enabled because we have not applied the protocol yet.



Lets do it.



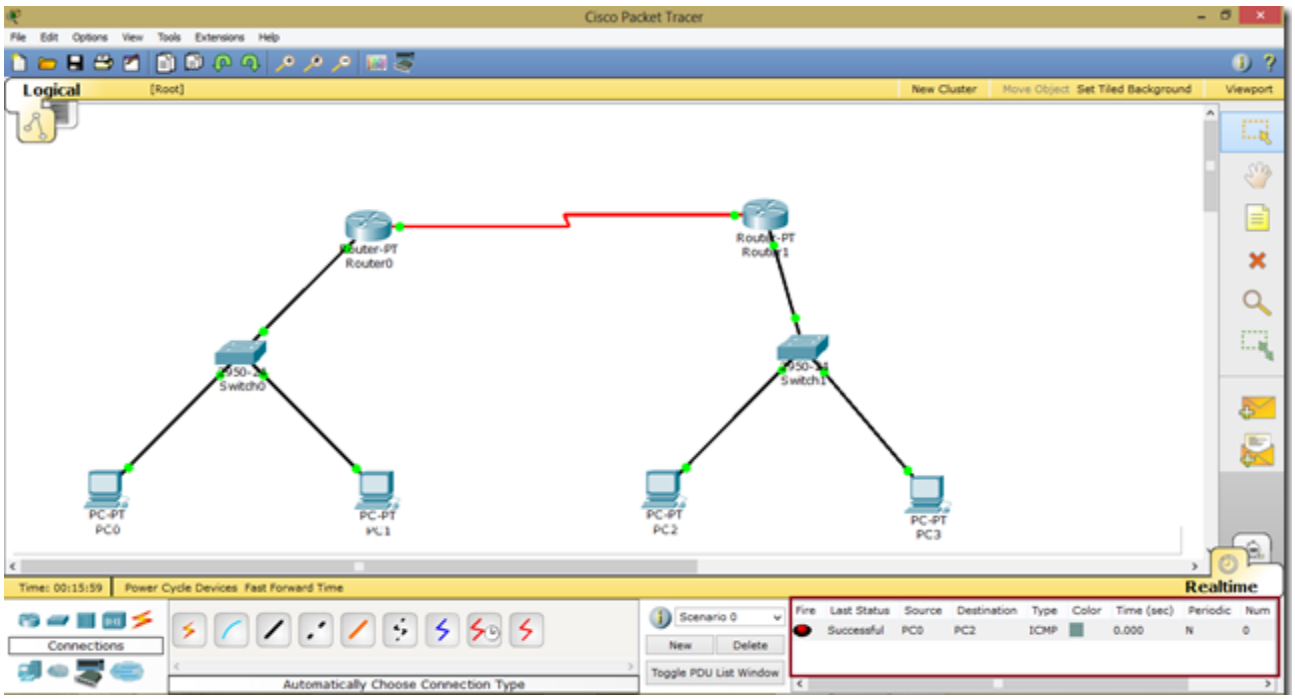
On router 1.



After applying protocol successfully , the traffic is flowing . Couple of things worth discussing

i. you will have to provide area id and process id on ospf protocol.

ii. you will have to provide wildcard mask on ospf.

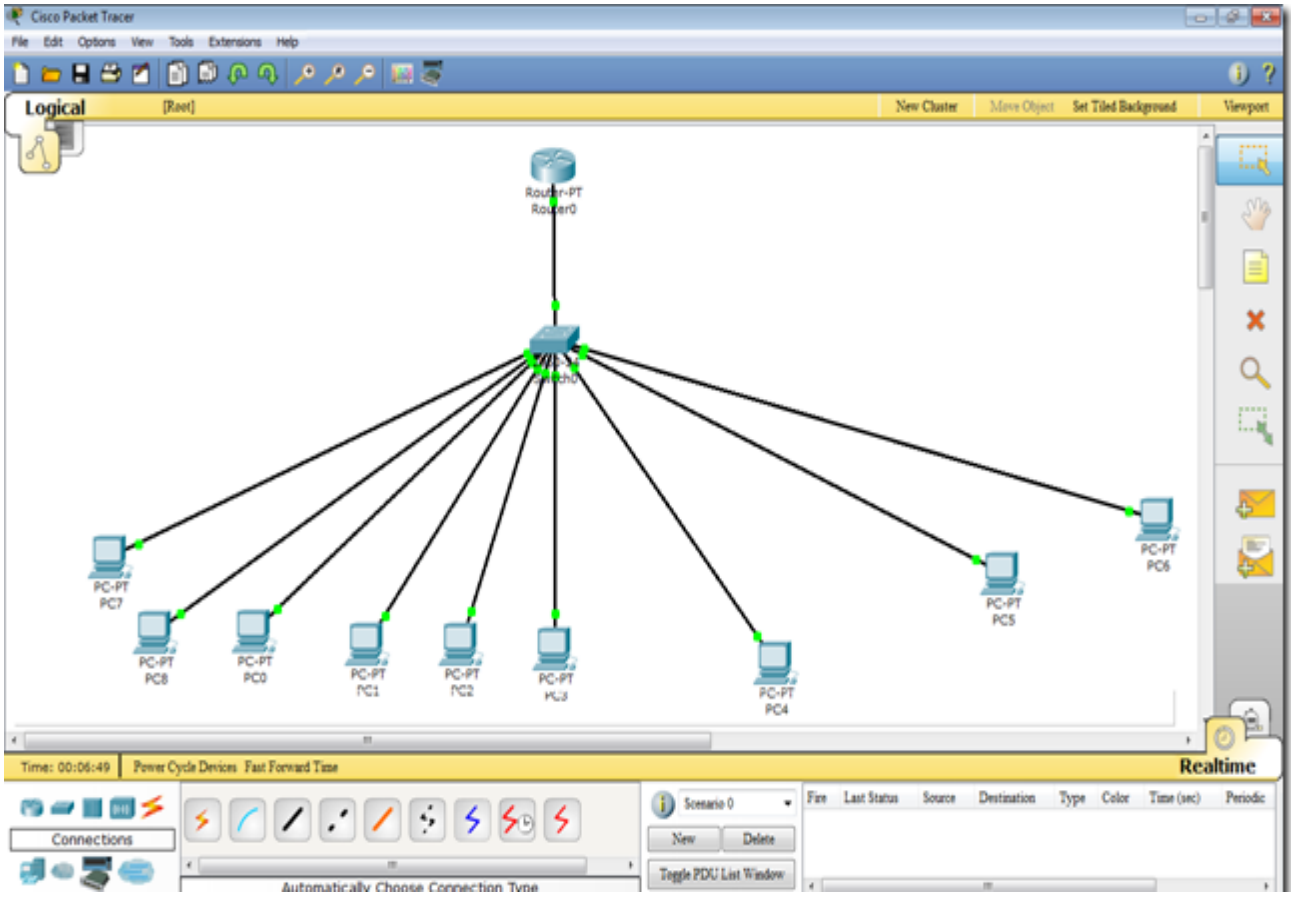


LAB # 10: DHCP on packet tracer

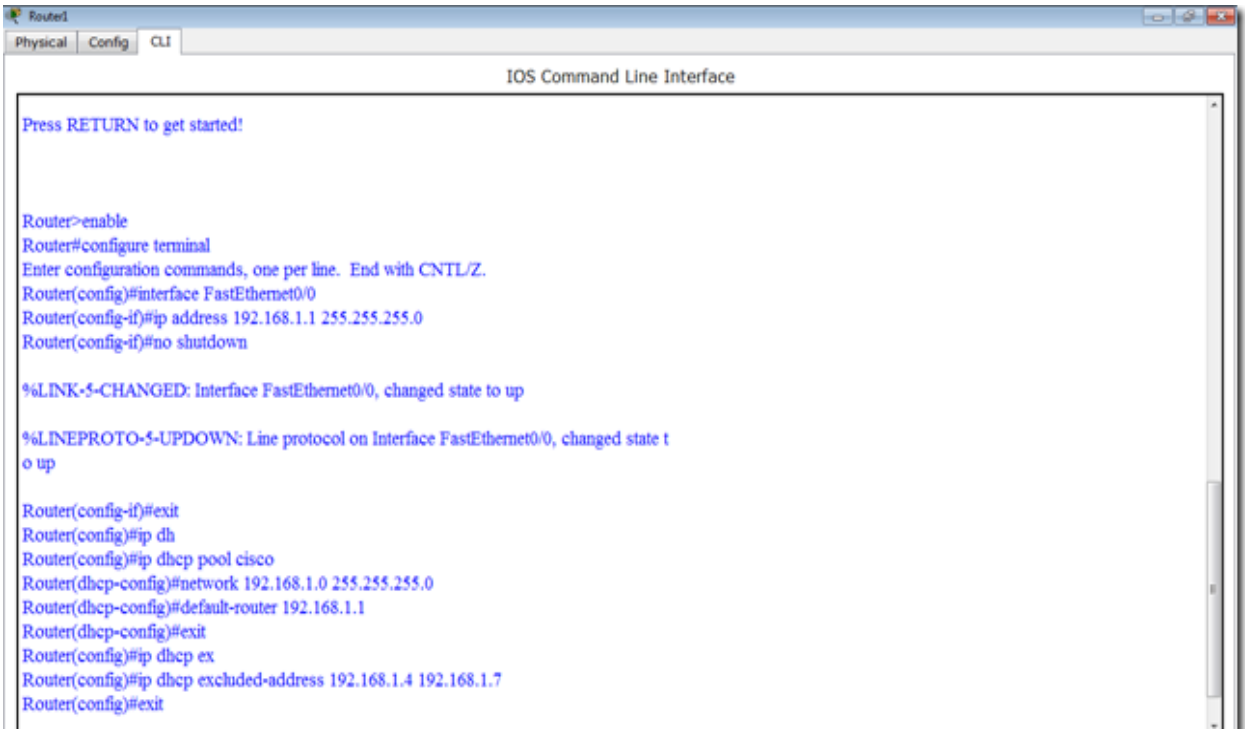
This tutorial is about how to configure dhcp on cisco router in packet tracer. The Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices. DHCP allows a computer to join an IP-based network without having a pre-configured IP address. DHCP is a protocol that assigns unique IP addresses to devices, then releases and renews these addresses as devices leave and re-join the network. Internet Service Providers (ISPs) usually use DHCP to allow customers to join the Internet with minimum effort. The DHCP server maintains a database of available IP addresses and configuration information. When it receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, and then allocates an IP address. DHCP servers typically grant IP addresses to clients only for a limited interval.

Lets apply DHCP on packet tracer.

First, let us make a topology with one router on which we will apply DHCP and several client PCs. More like this one,



Now, we will apply DHCP on the router.
The commands in sequence are as follows.



In the following command "ip dhcp pool cisco", we are creating a pool for DHCP called cisco. Cisco is the name here and we can name it whatever we want.

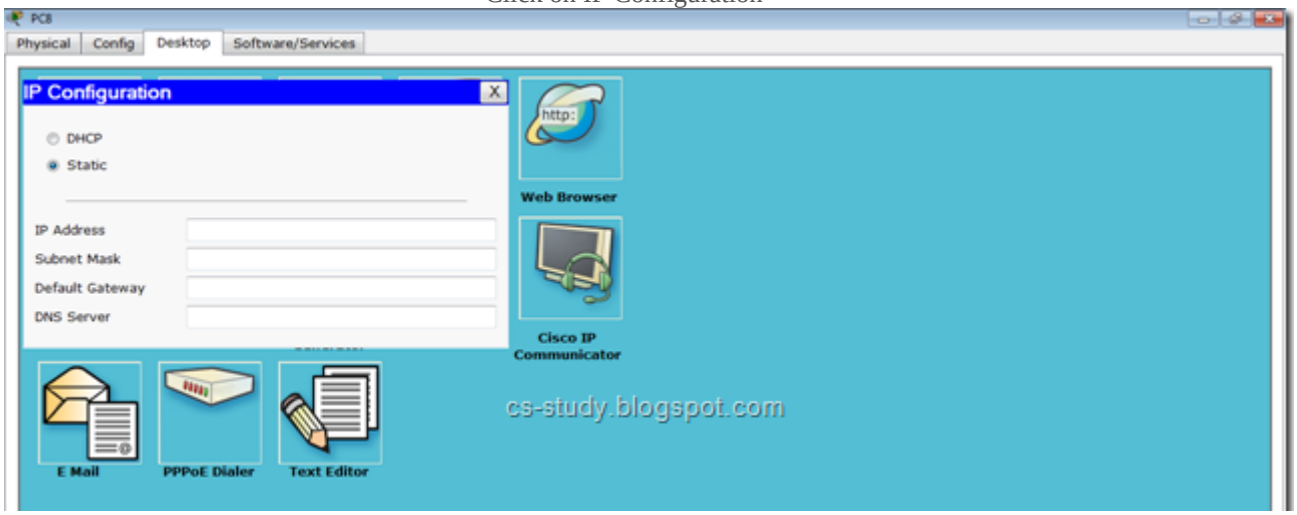
Similarly, in the command "default-router " we are telling the DHCP about the default route to follow.

Notice, after we exit from DHCP mode, we are excluding some IP addresses by applying this command "ip dhcp excluded-addresses x-x", where x is the starting and ending IP address respectively. We are basically reserving some Ips for our use. It can be used to attach printers, or assign it to some specific users for security purposes. You can also give dns address in dhcp by using the following command.

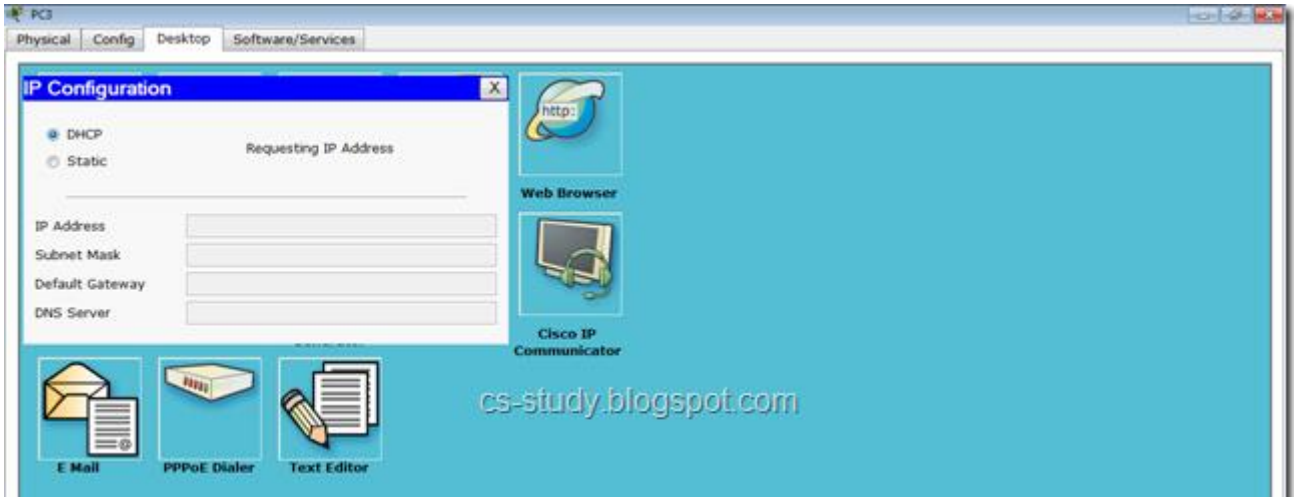
Dns-server 192.168.1.15.

Now, open the PC.

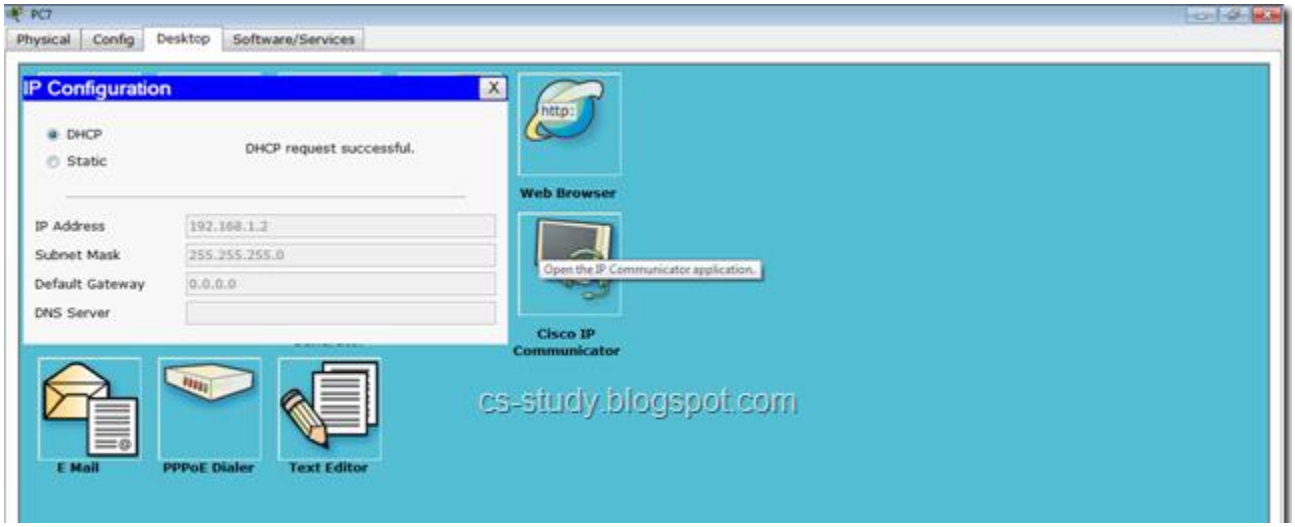
Click on IP Configuration



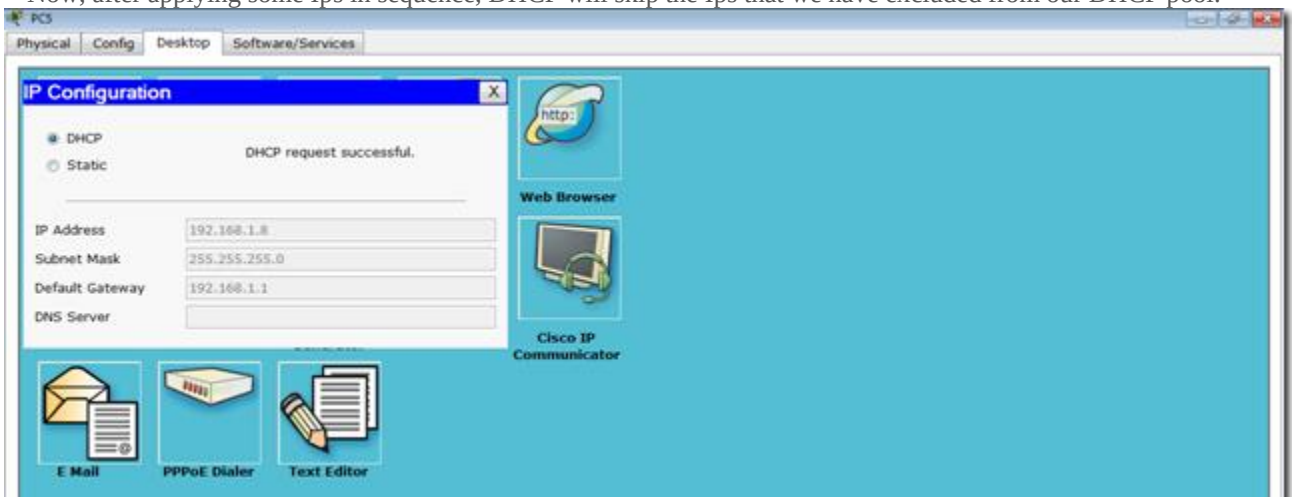
Select from Static to DHCP



And after DHCP request is completed you will see the following screen.



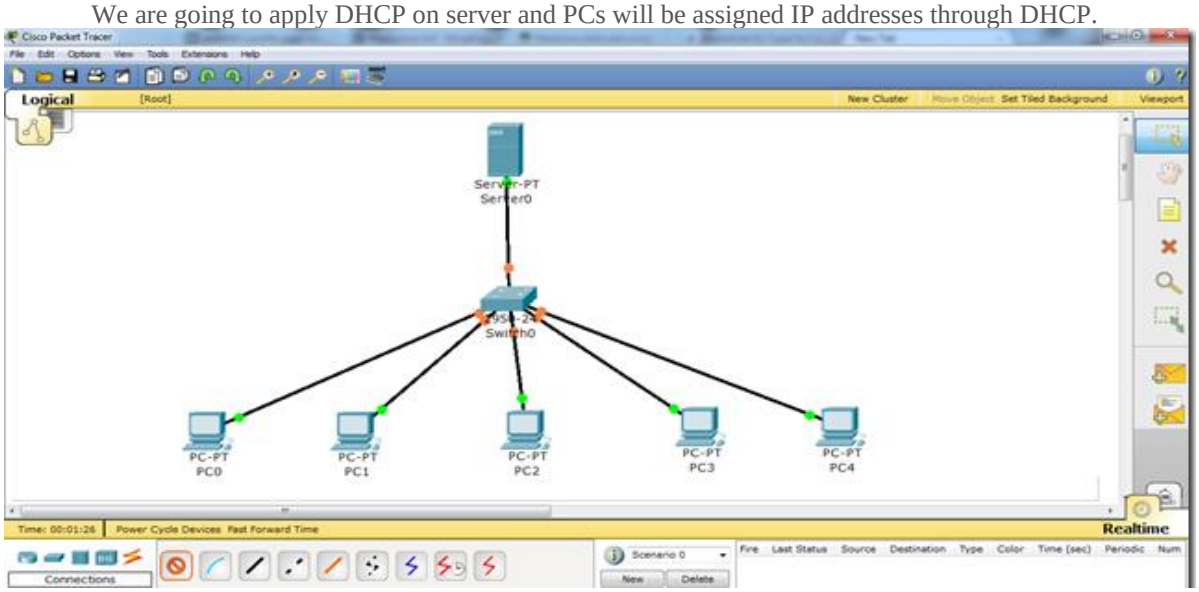
Now, after applying some Ips in sequence, DHCP will skip the Ips that we have excluded from our DHCP pool.



That is all, we have applied DHCP on packet tracer.

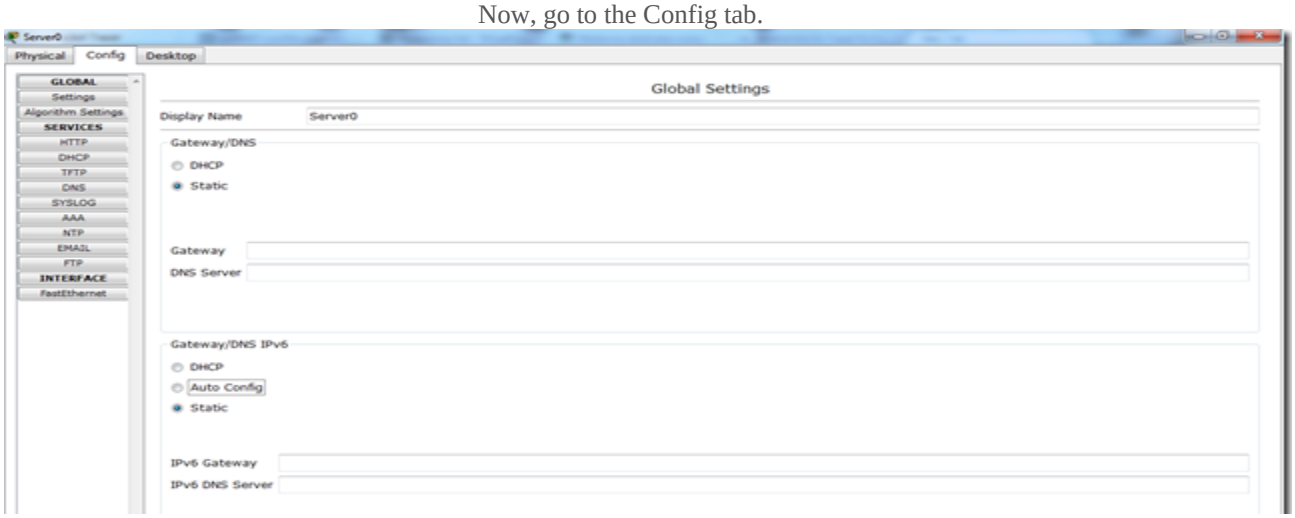
LAB # 11: DHCP on Packet tracer through Server

We are going to apply DHCP on server and PCs will be assigned IP addresses through DHCP.

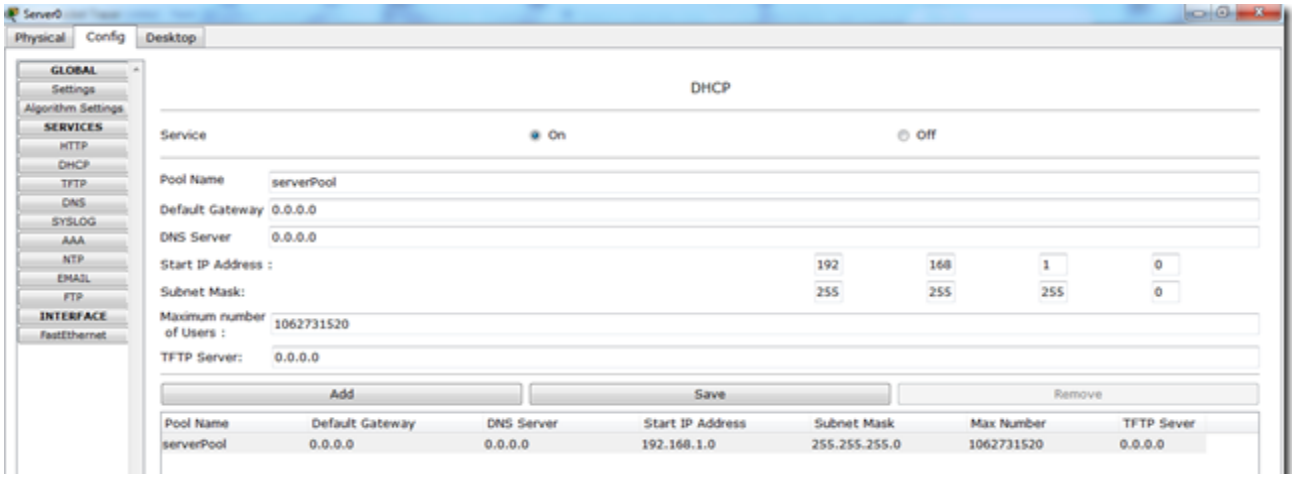


Open the server and go to the Desktop tab, click IP Configuration and enter the IP address.

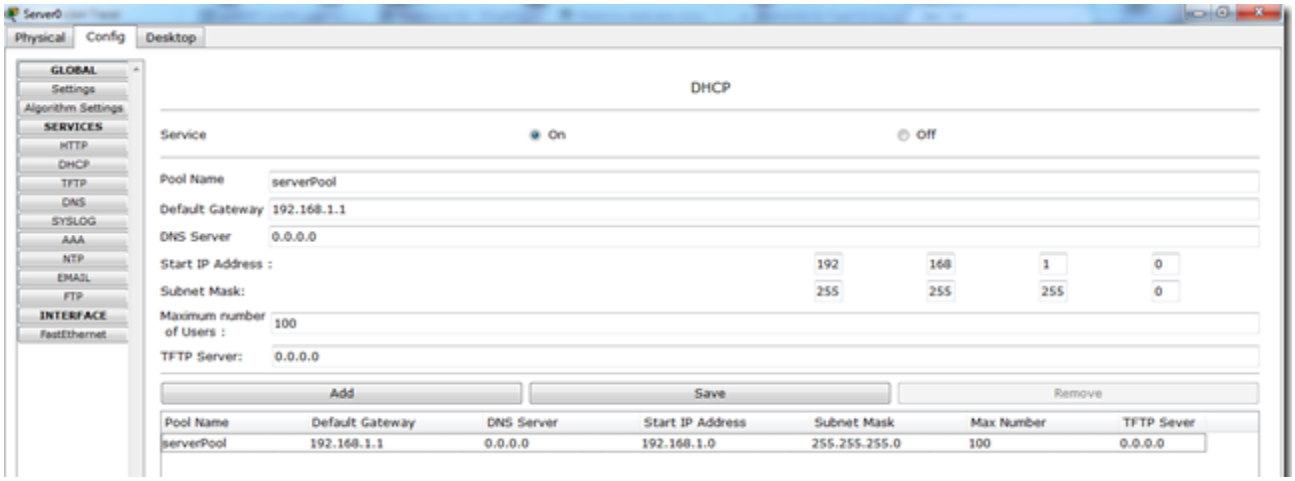
Now, go to the Config tab.



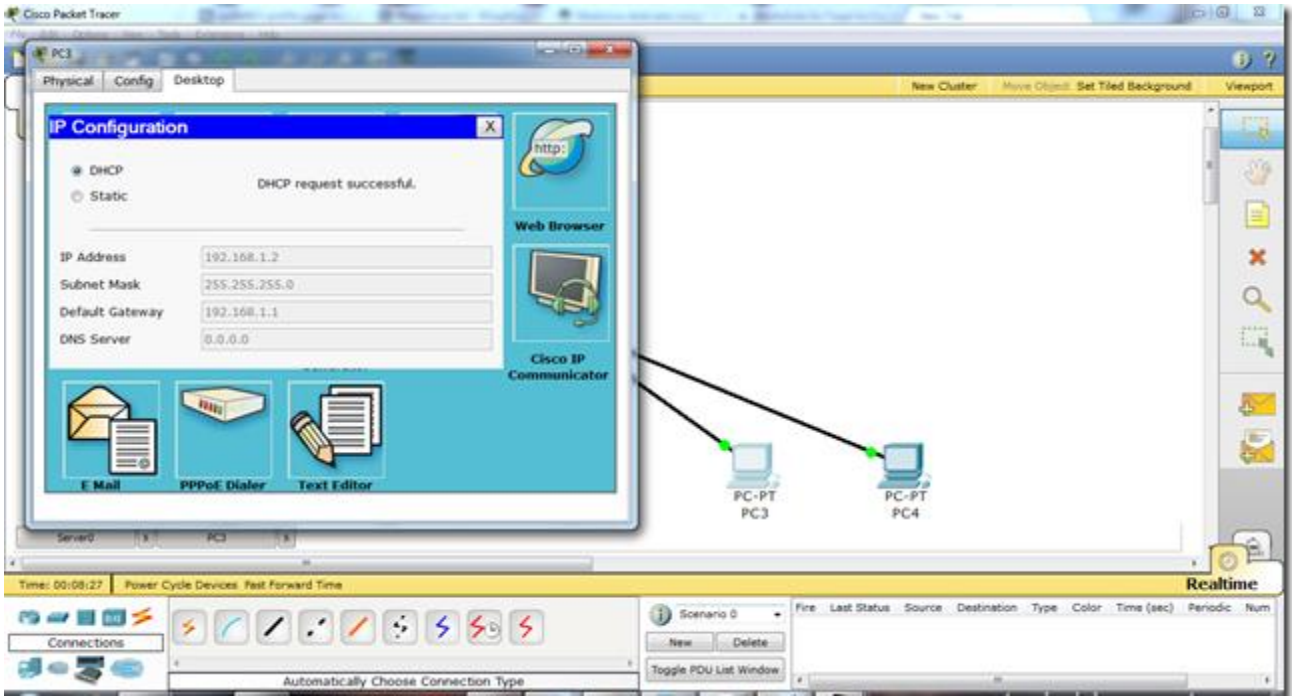
And go to the DHCP



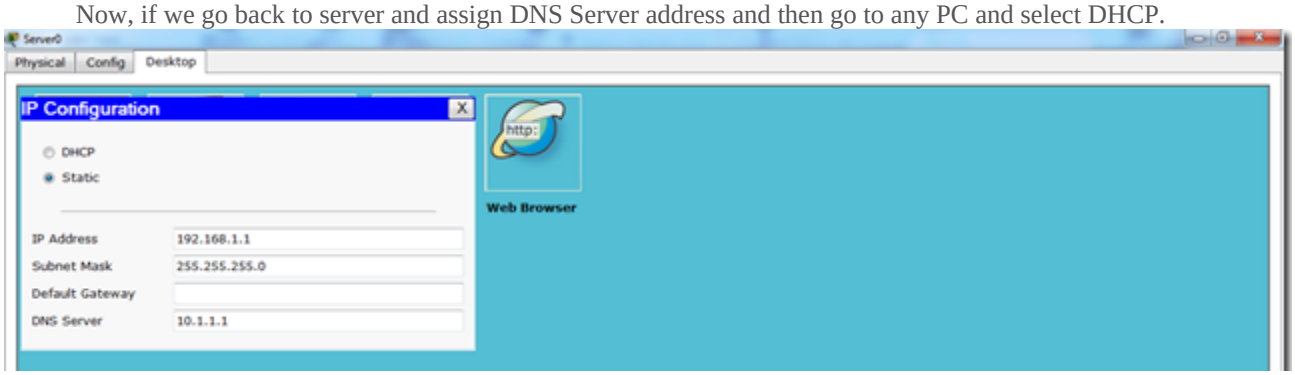
i. Enter IP for default Gateway.
ii. Start IP address
iii.. Maximum number of Users.
iv. Click Save.



Now, click on any PC that is attached to the server, go to IP configuration and select DHCP. You will see that DHCP will successfully assign IP address to the PC

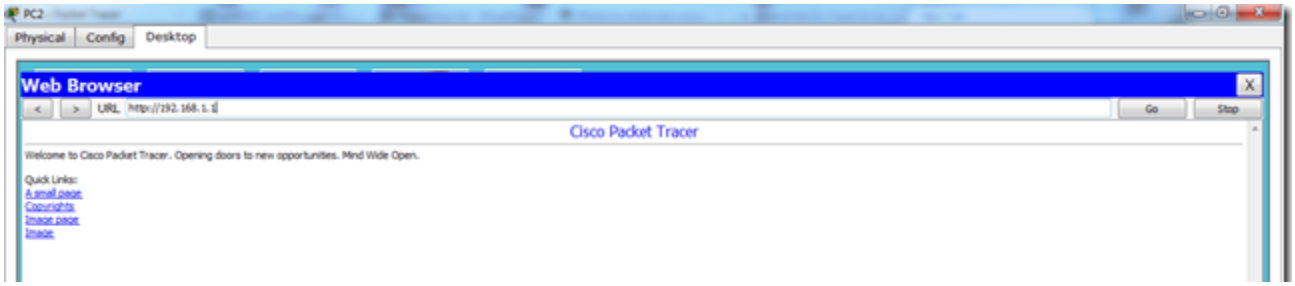


Now, if we go back to server and assign DNS Server address and then go to any PC and select DHCP.

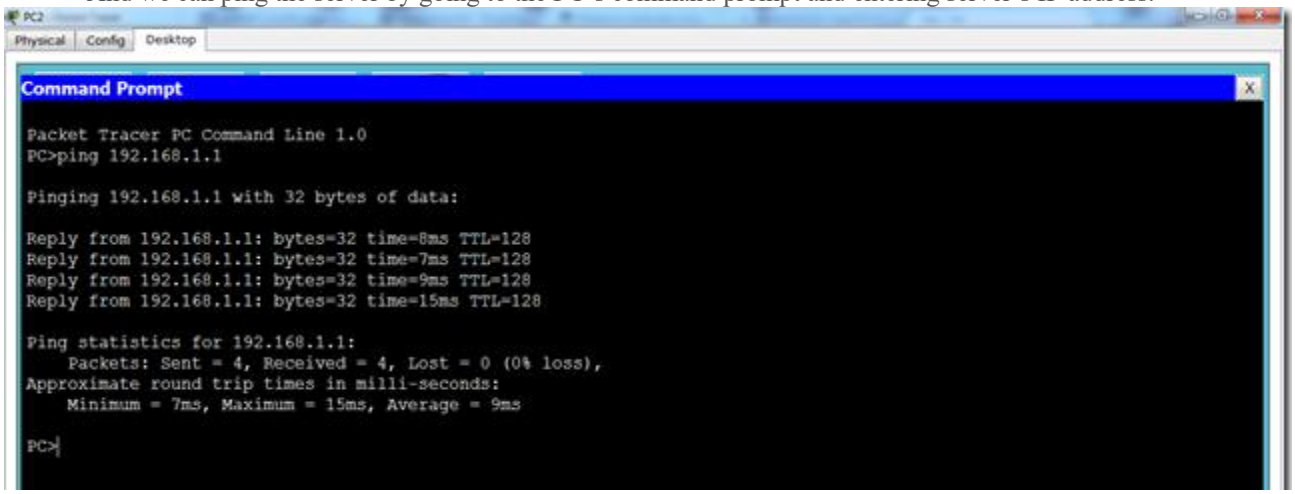


It will also assign DNS to the PC as well.

We can also open the website of the server through any PC by going to the Web Browser option and entering the IP address of the server.



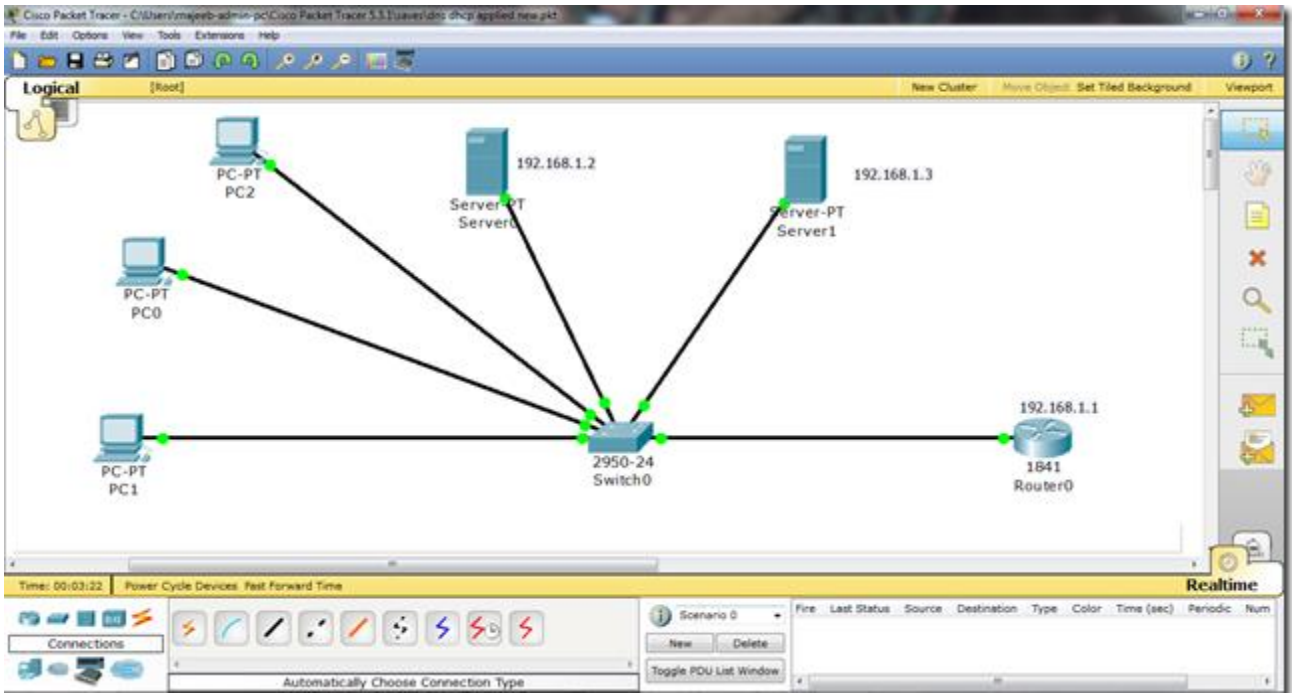
And we can ping the server by going to the PC's command prompt and entering server's IP address.



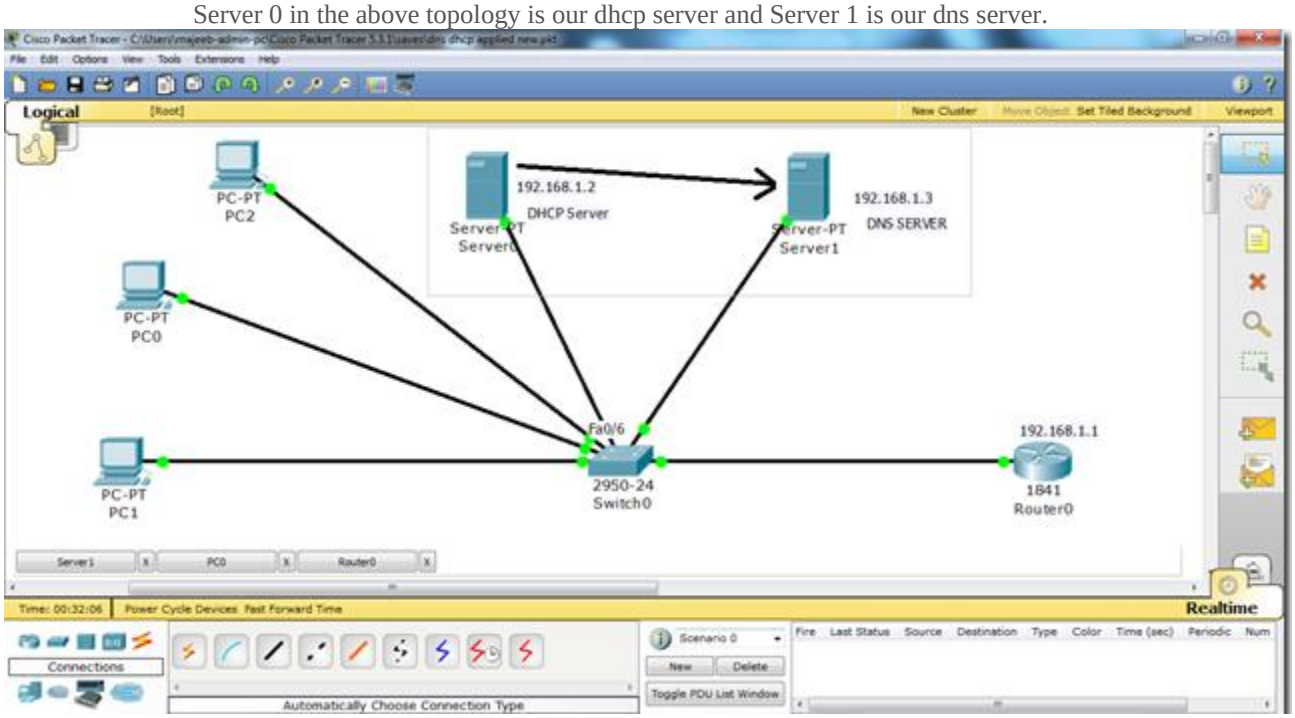
s

LAB # 12: DNS on packet tracer:

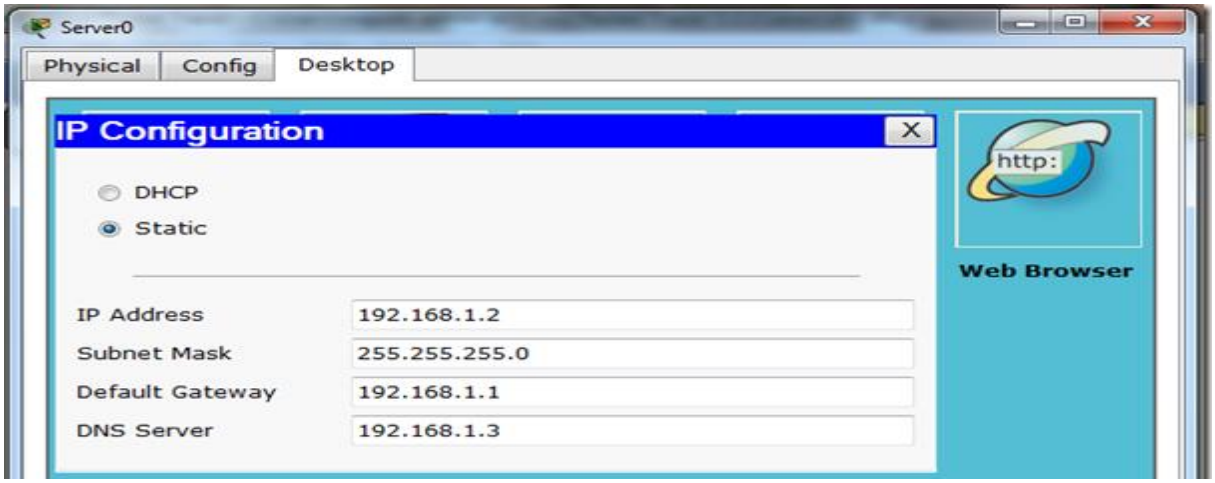
Here in this tutorial, we are going to set a dns (domain name system) server and a dhcp server. And then from our PC we will use dns service.



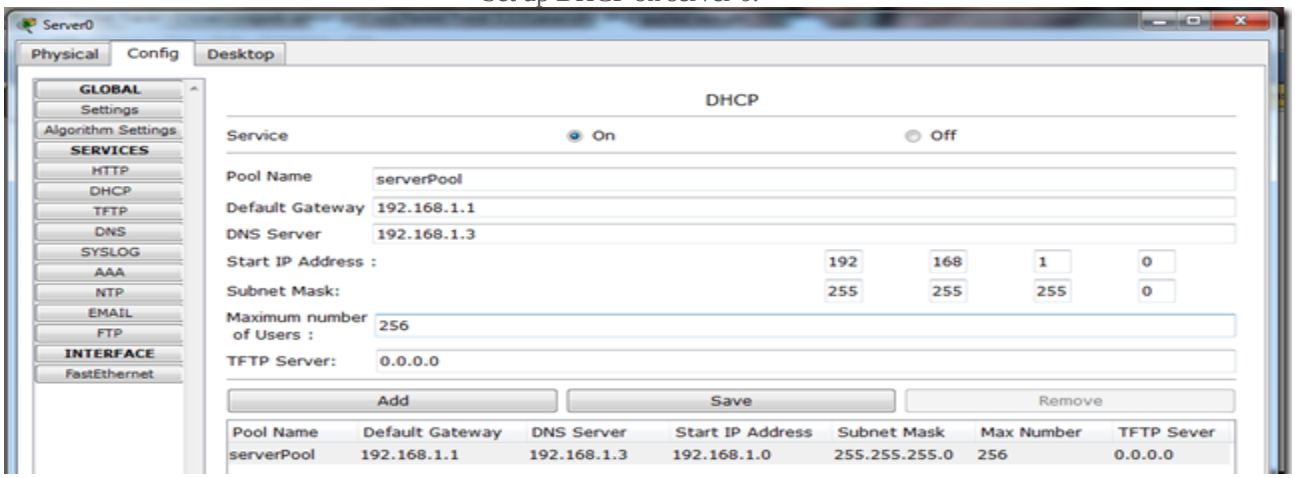
Server 0 in the above topology is our dhcp server and Server 1 is our dns server.



Set up IP on server 0.

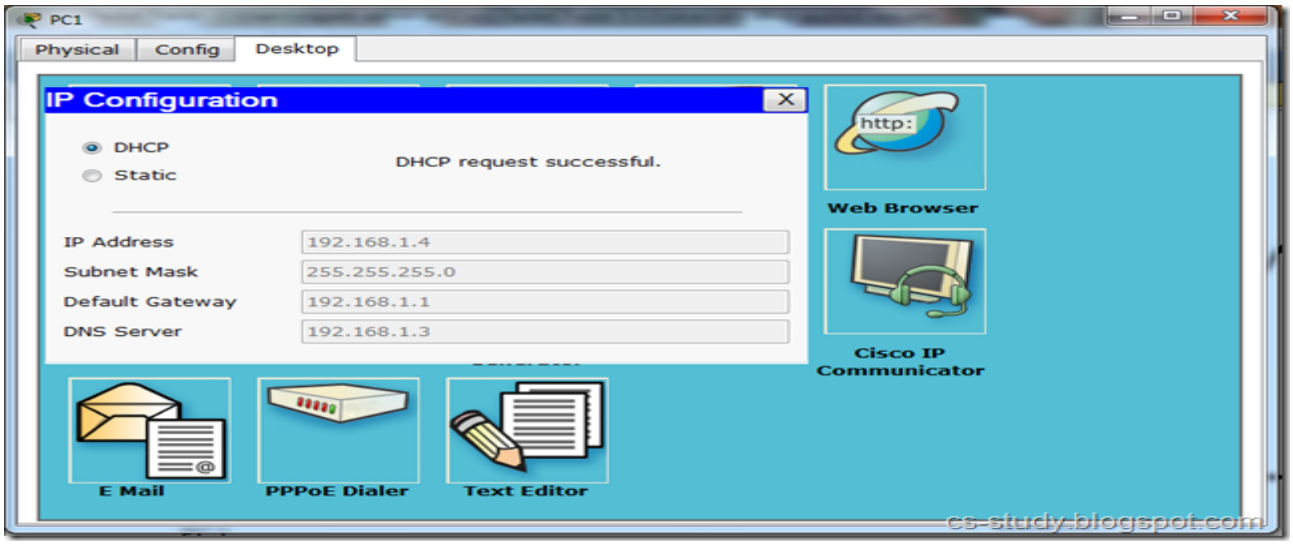


Set up DHCP on server 0.

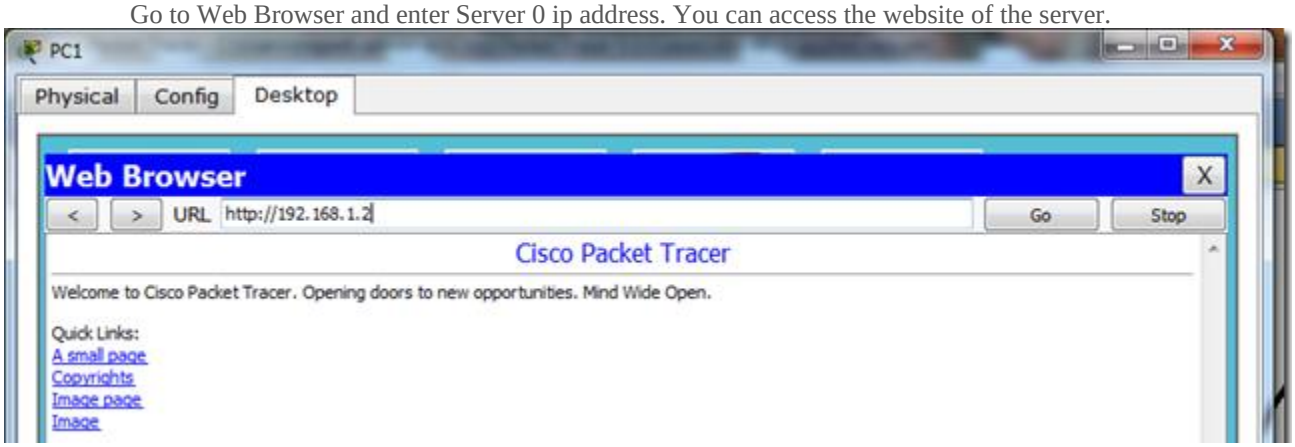


Set up IP on server 1.

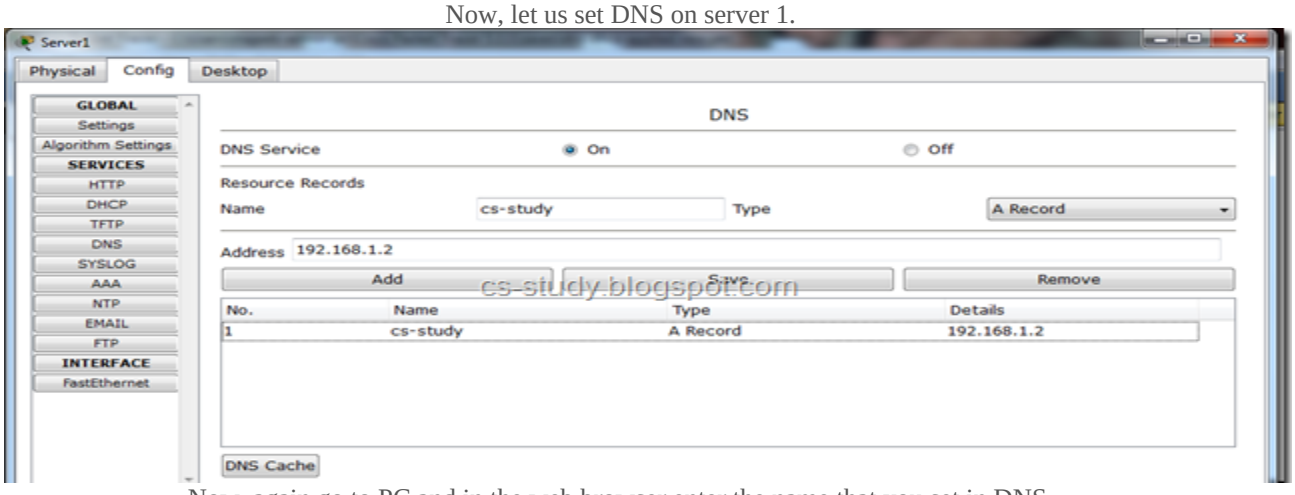
Now, go to PC and select DHCP.



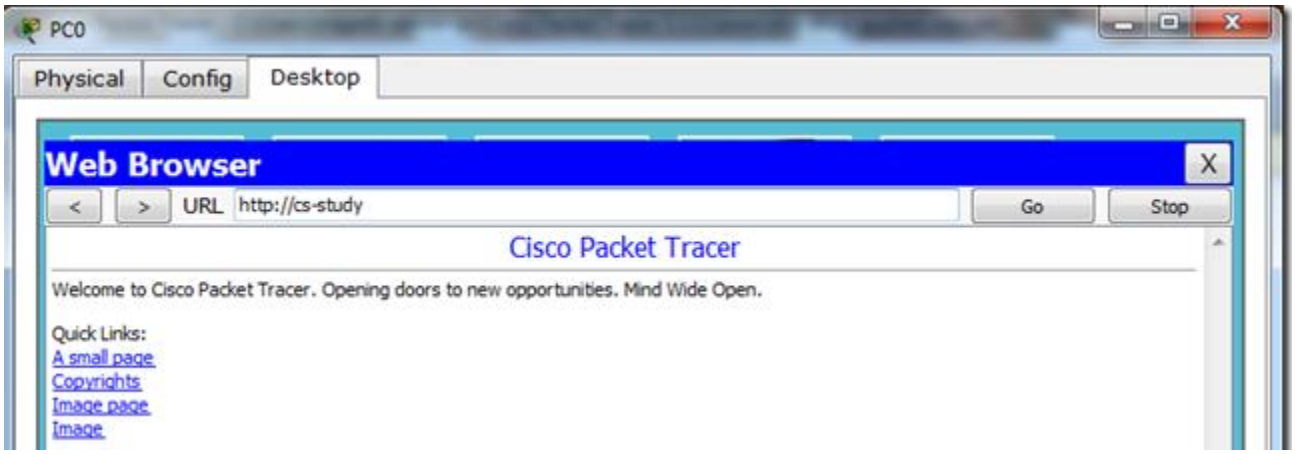
Go to Web Browser and enter Server 0 ip address. You can access the website of the server.



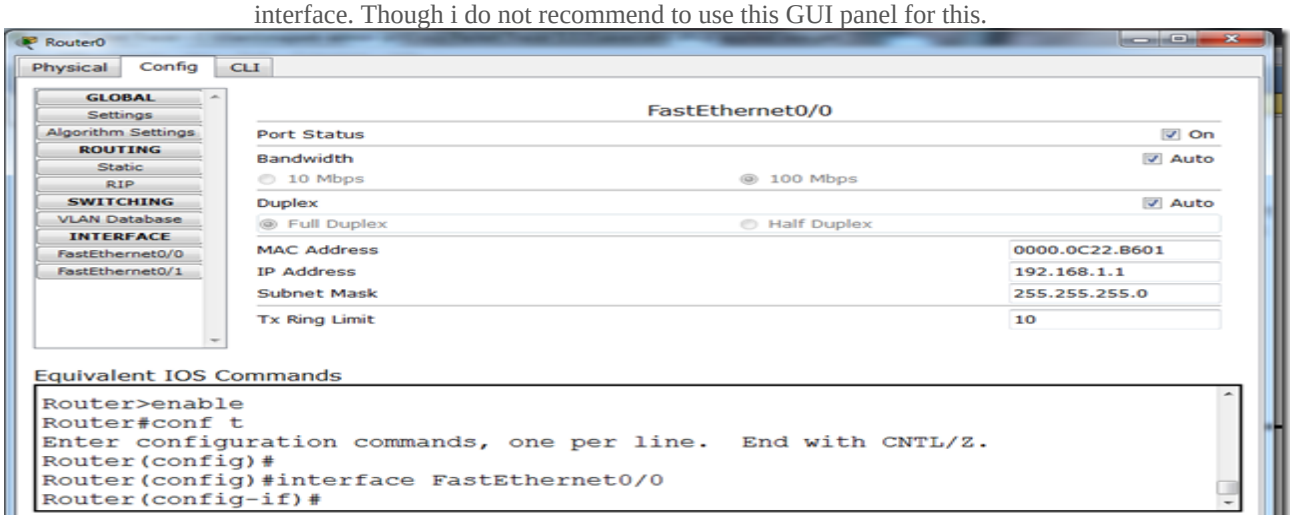
Now, let us set DNS on server 1.



Now, again go to PC and in the web browser enter the name that you set in DNS.

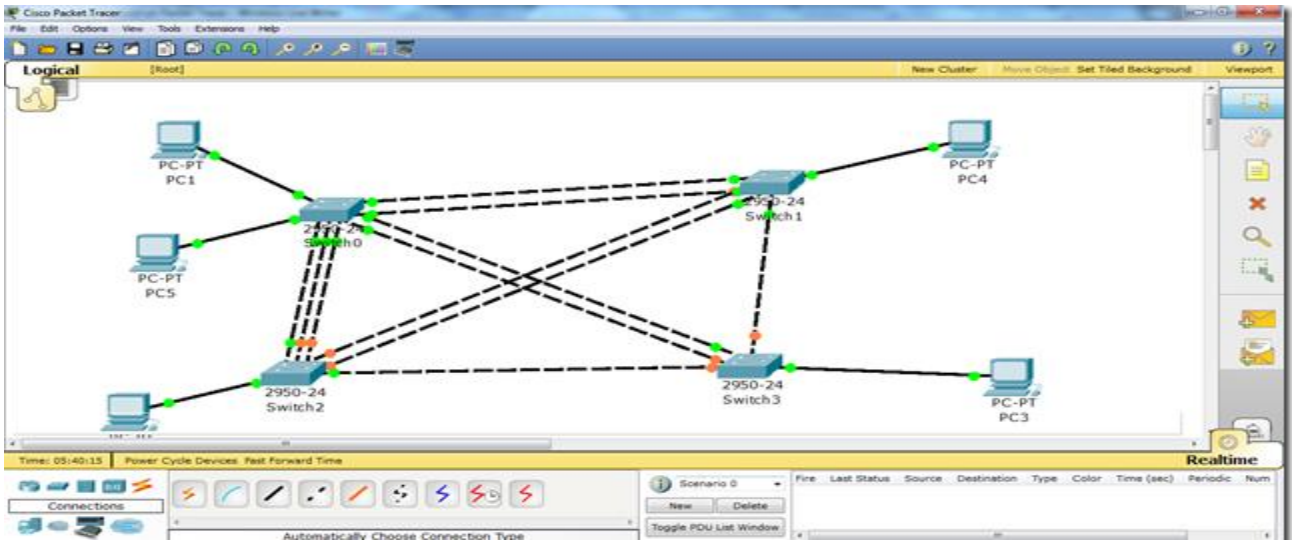


Voila, we have done it. Now, in this tutorial, router is additional and we can use it if required, Set the IP of the interface. Though i do not recommend to use this GUI panel for this.

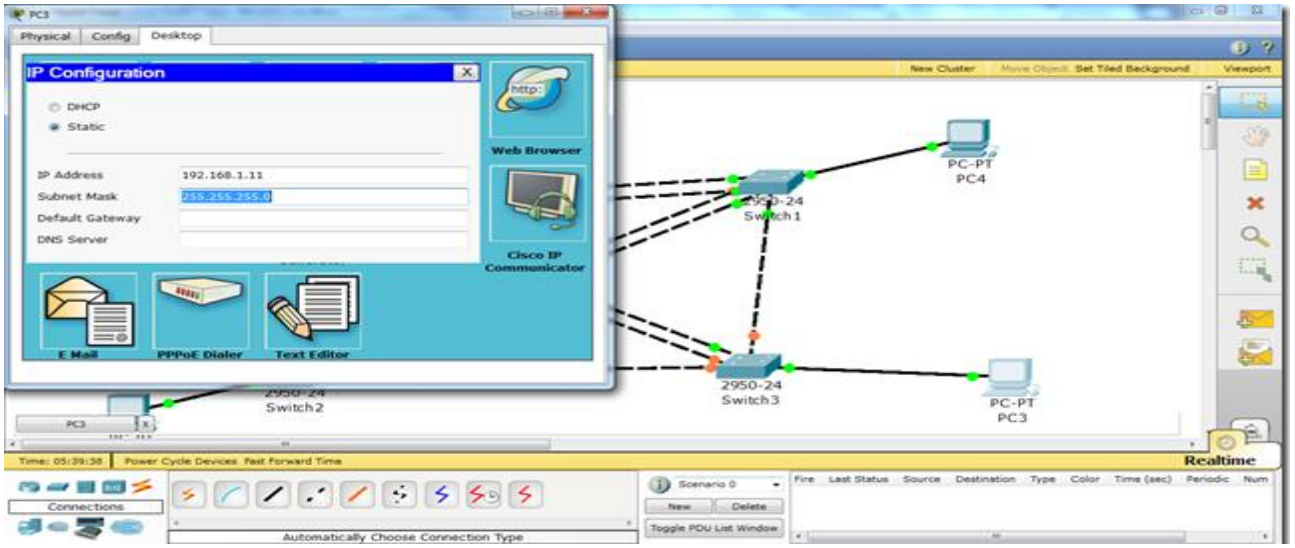


LAB # 15: Spanning Tree Protocol on Packet Tracer

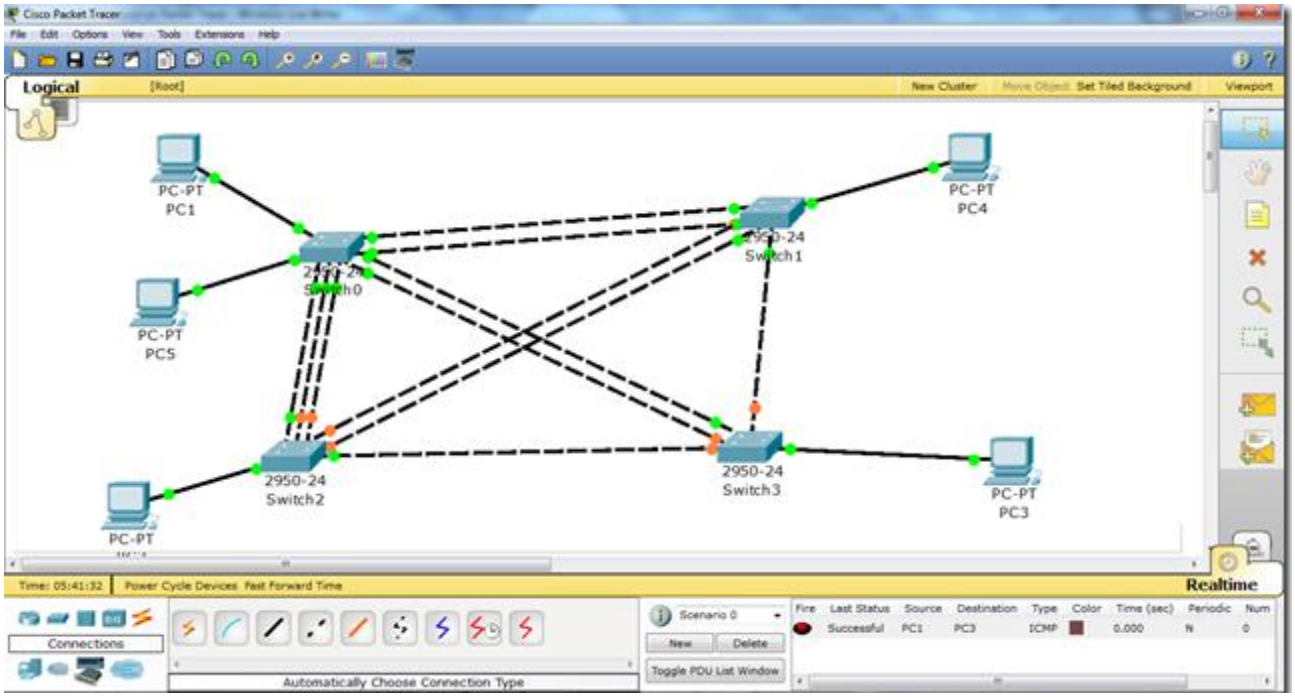
Let us apply STP on packet tracer. Let us develop a basic topology like the one in the following diagram.



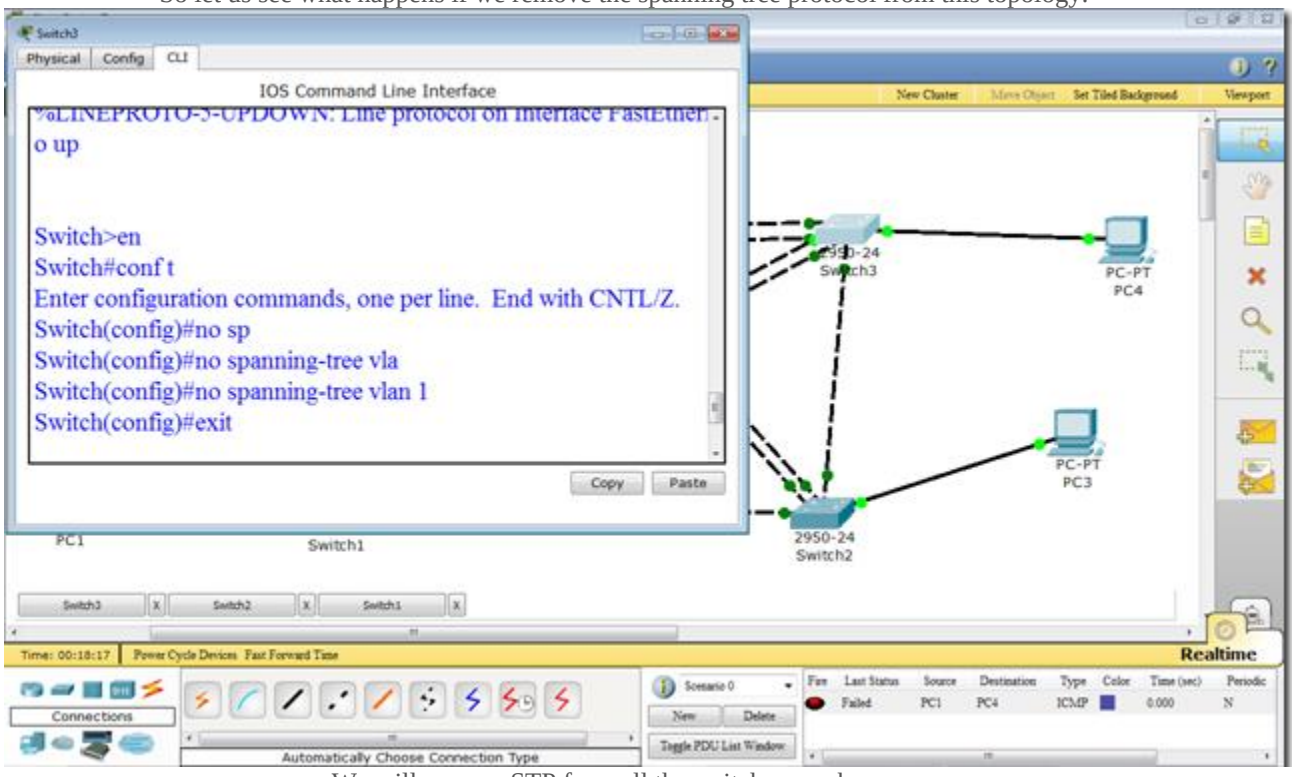
As we can see in the above diagram that some light are green while others are orange. Y is it so ? We will see that in a moment. Let us try to communicate between two Hosts. Assign IP addresses to all hosts



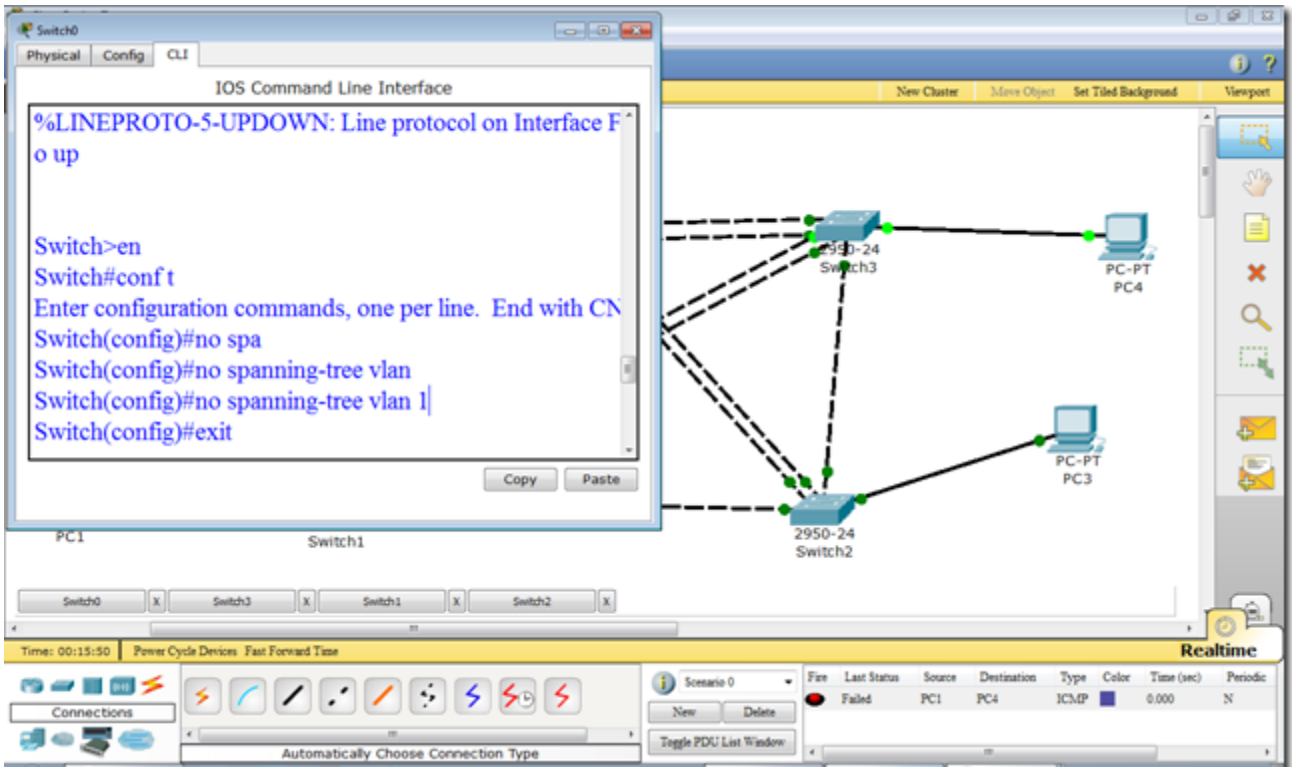
As we can see in the figure below, the communication is successful. It is due to the spanning tree protocol applied on the switch by default. It provides us with the loop free environment. It calculates the cost of each path and provides us with the one that has the minimum cost. That is the reason that some links are up while others are down with the orange light.

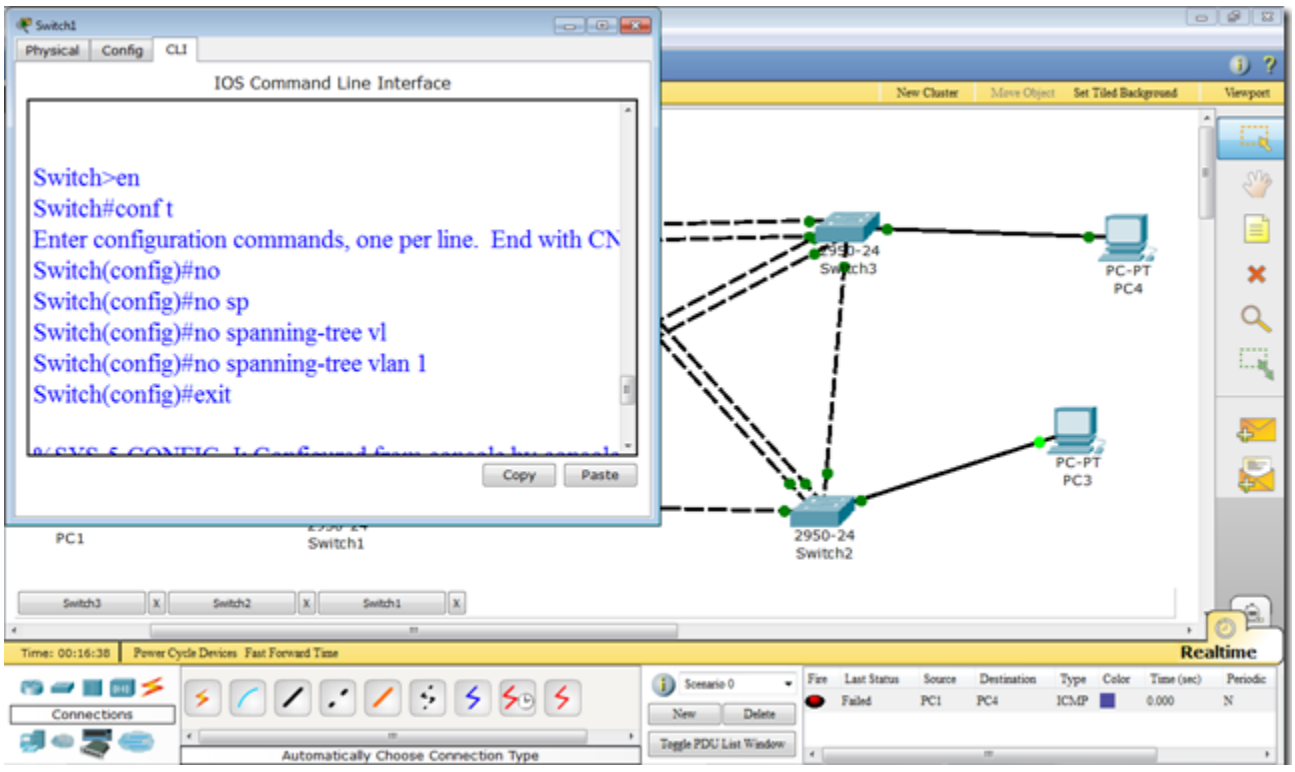


So let us see what happens if we remove the spanning tree protocol from this topology.



We will remove STP from all the switches one by one.


Switch0
Physical
Config
CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface F
o up
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CN
Switch(config)#no spa
Switch(config)#no spanning-tree vlan
Switch(config)#no spanning-tree vlan 1
Switch(config)#exit
Copy
Paste
PC1
Switch1
2950-24
Switch3
PC-PT
PC4
PC-PT
PC3
2950-24
Switch2
New Cluster
Move Object
Set Tiled Background
Viewport
Time: 00:15:50
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Failed
PC1
PC4
ICMP
0.000
N


Switch1
Physical
Config
CLI
IOS Command Line Interface
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CN
Switch(config)#no
Switch(config)#no sp
Switch(config)#no spanning-tree vl
Switch(config)#no spanning-tree vlan 1
Switch(config)#exit
Copy
Paste
PC1
Switch1
2950-24
Switch3
PC-PT
PC4
PC-PT
PC3
2950-24
Switch2
New Cluster
Move Object
Set Tiled Background
Viewport
Time: 00:16:38
Power Cycle Devices
Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Failed
PC1
PC4
ICMP
0.000
N

LAB # 20: Password Authentication Protocol on packet tracer (PAP)

The Point-to-Point Protocol (PPP) is a data link protocol commonly used in establishing a direct connection between two networking nodes. It can provide connection authentication, transmission encryption and compression. PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links etc. Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet, since IP packets cannot be transmitted over a modem line on their own, without some data link protocol. PPP is commonly used as a data link layer protocol for connection over synchronous and asynchronous circuits, where it has largely superseded the older Serial Line Internet Protocol (SLIP) and telephone company mandated standards (such as Link Access Protocol, Balanced (LAPB).
PPP was designed somewhat after the original HDLC specifications. The designers of PPP included many additional features that had been seen only in proprietary data-link protocols up to that time.

HDLC

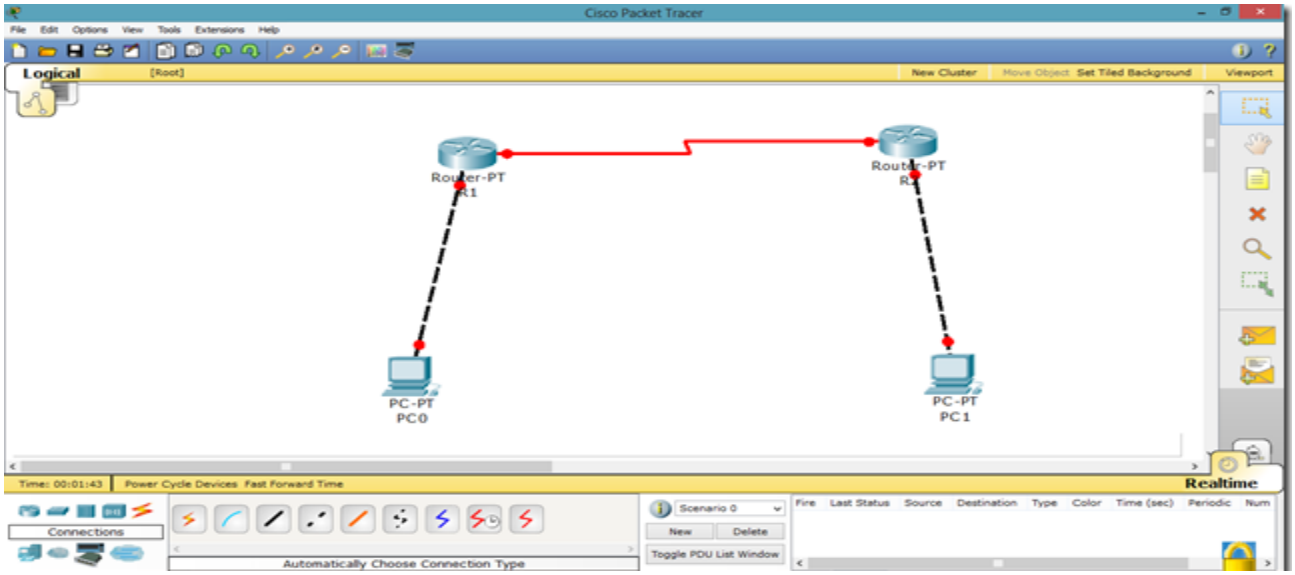
HDLC provides both connection-oriented and connectionless service. HDLC can be used for point to multipoint connections, but is now used almost exclusively to connect one device to another, using what is known as Asynchronous Balanced Mode (ABM).

PAP

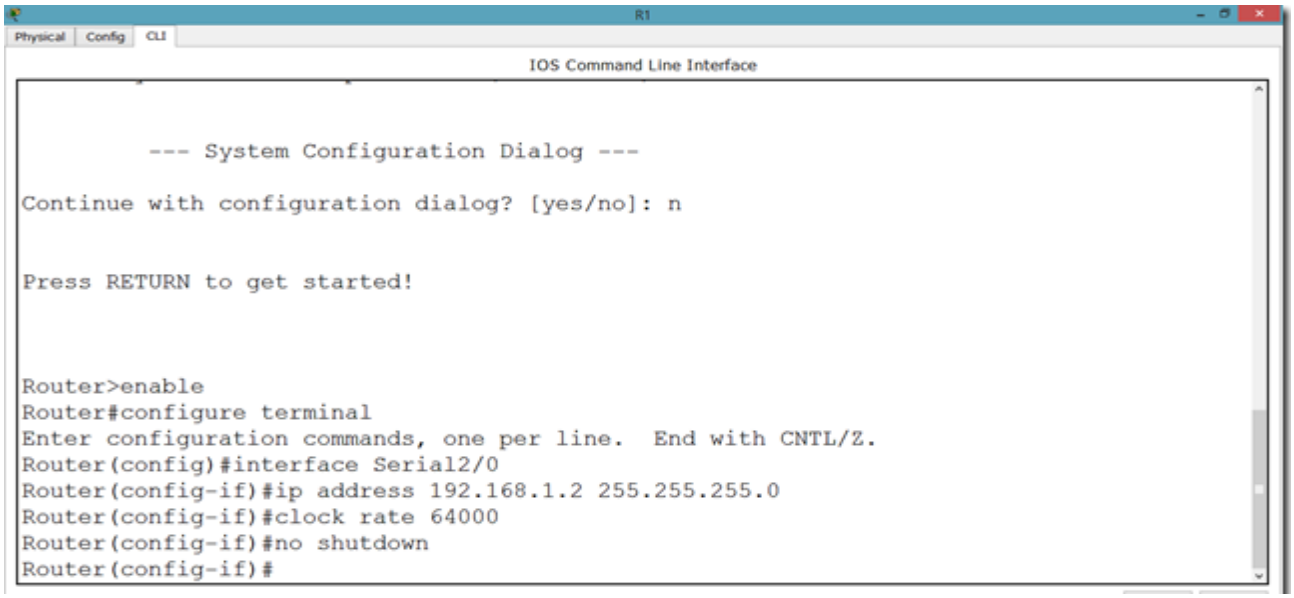
A **password authentication protocol** (**PAP**) is an authentication protocol that uses a password. PAP is used by Point to Point Protocol to validate users before allowing them access to server resources. Almost all network operating system remote servers support PAP.
PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure. It is used as a last resort when the remote server does not support a stronger authentication protocol, like CHAP or EAP (the latter is actually a framework).
Password-based authentication is the protocol that two entities share a password in advance and use the password as the basis of authentication. Existing password authentication schemes can be categorized into two types: weak-password authentication schemes and strong-password authentication schemes. In general, strong-password authentication protocols have the advantages over the weak-password authentication schemes in that their computational overhead are lighter, designs are simpler, and implementation are easier, and therefore are especially suitable for some constrained environments.

PAP works basically the same way as the normal login procedure. The client authenticates itself by sending a user name and an (optionally encrypted) password to the server, which the server compares to its secrets database. This technique is vulnerable to eavesdroppers who may try to obtain the password by listening in on the serial line, and to repeated trial and error attacks.

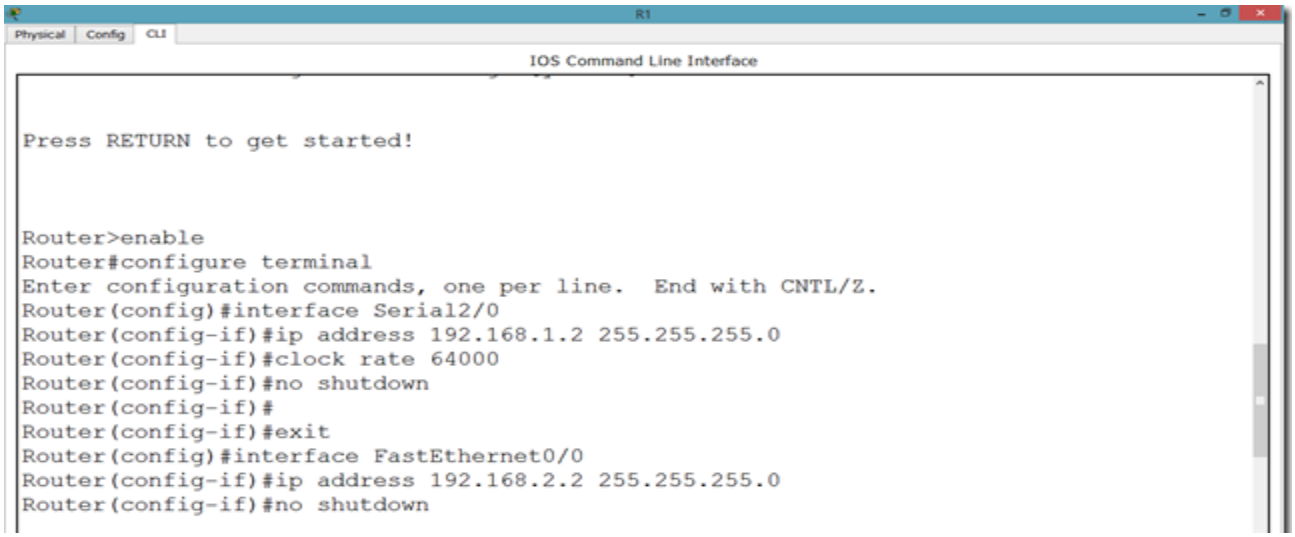
Let us apply PPP on packet tracer. Consider the following simpler topology.



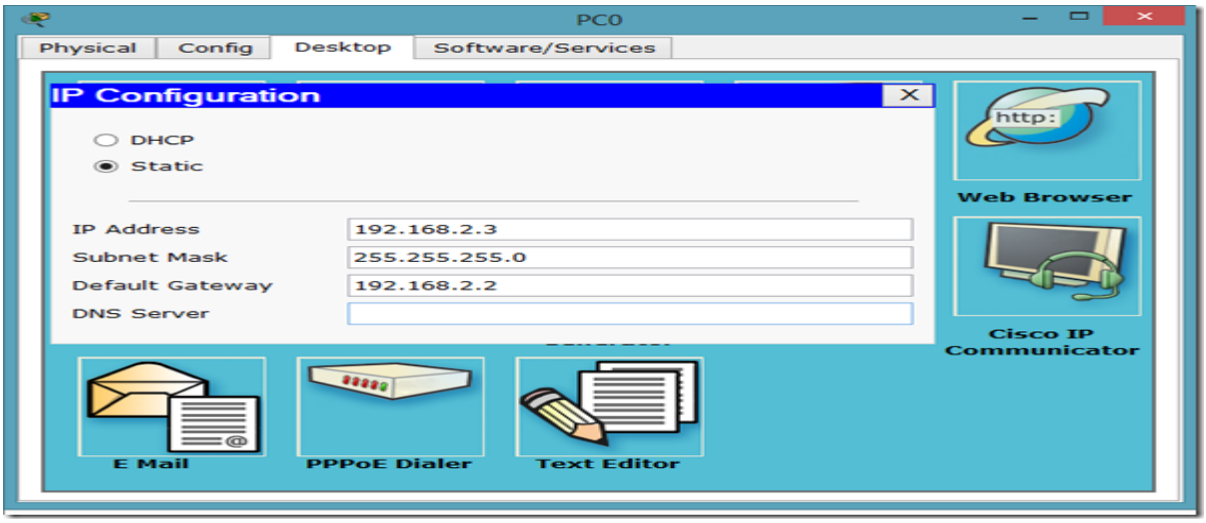
Let us apply IP addresses on the interfaces and change the state of the interface from down to UP. So that they can communicate.



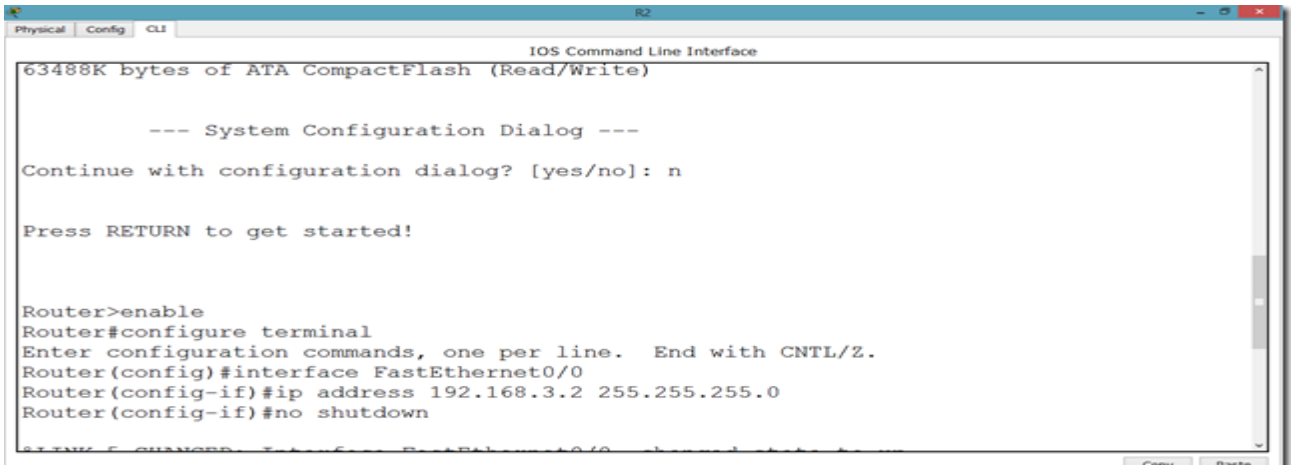
Similarly, for serial interface.



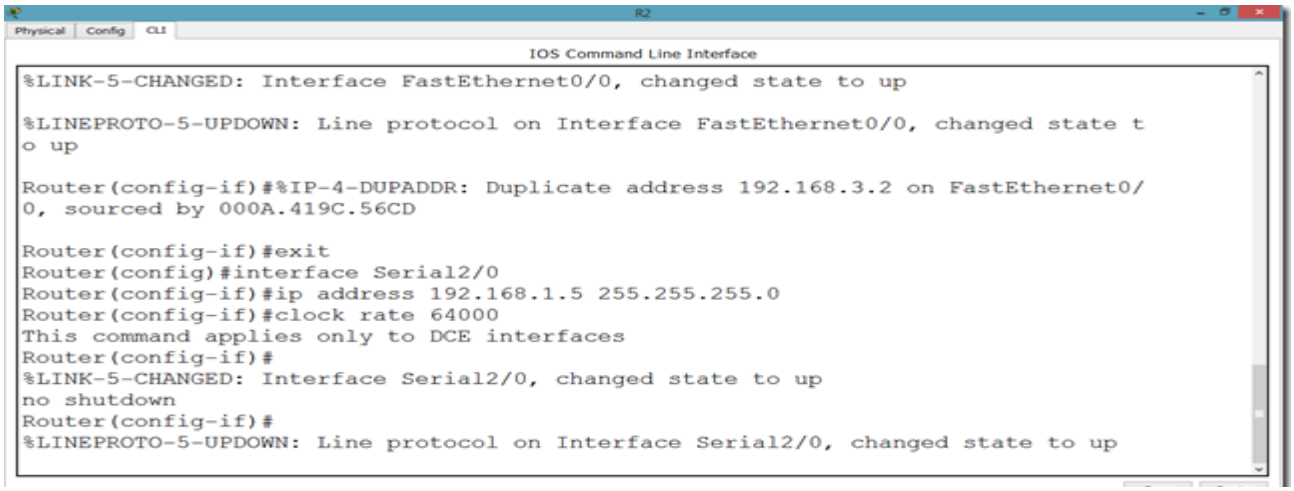
PC IP setup



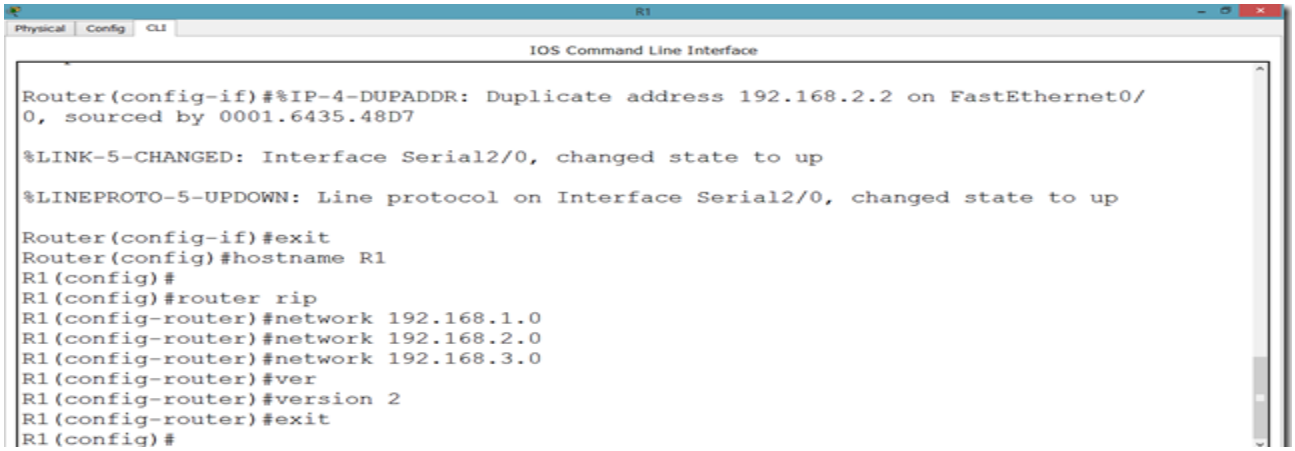
The IP configuration on other router.



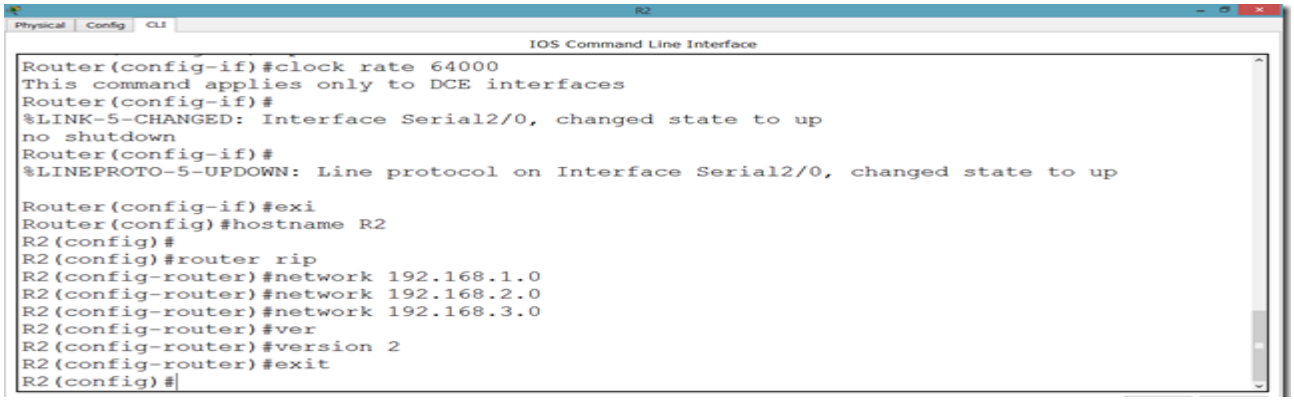
serial int setup.



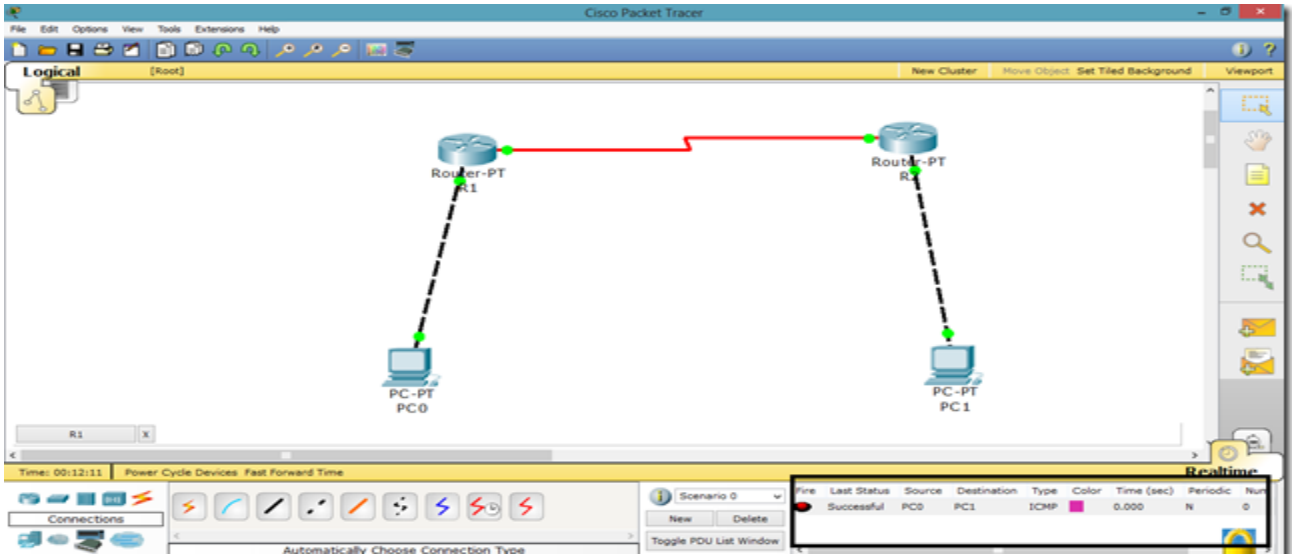
Now, we know that PCs that are attached cannot communicate until we apply a routing mechanism. In this case we are applying the RIP V2 protocol. Apply the following set of commands on both routers. We have also set the hostname of the router which will be useful to us later.



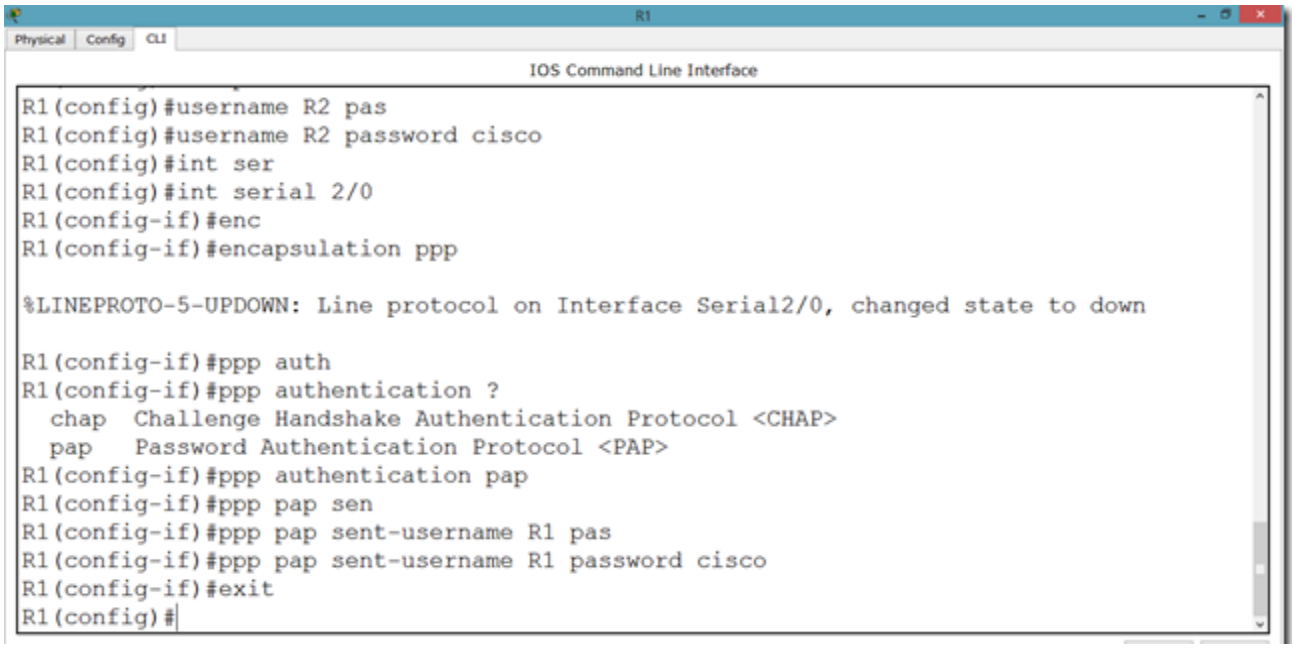
Now, let us set the commands on the second router as well.



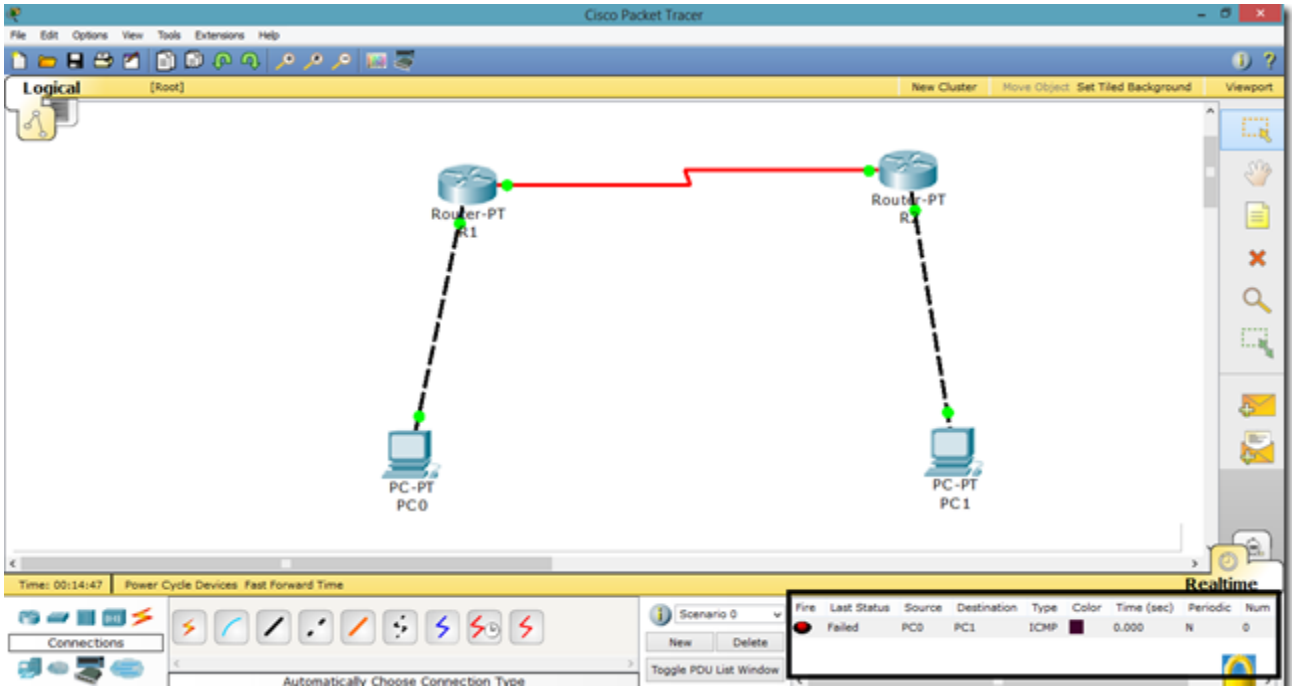
Now, both PCs can communicate.



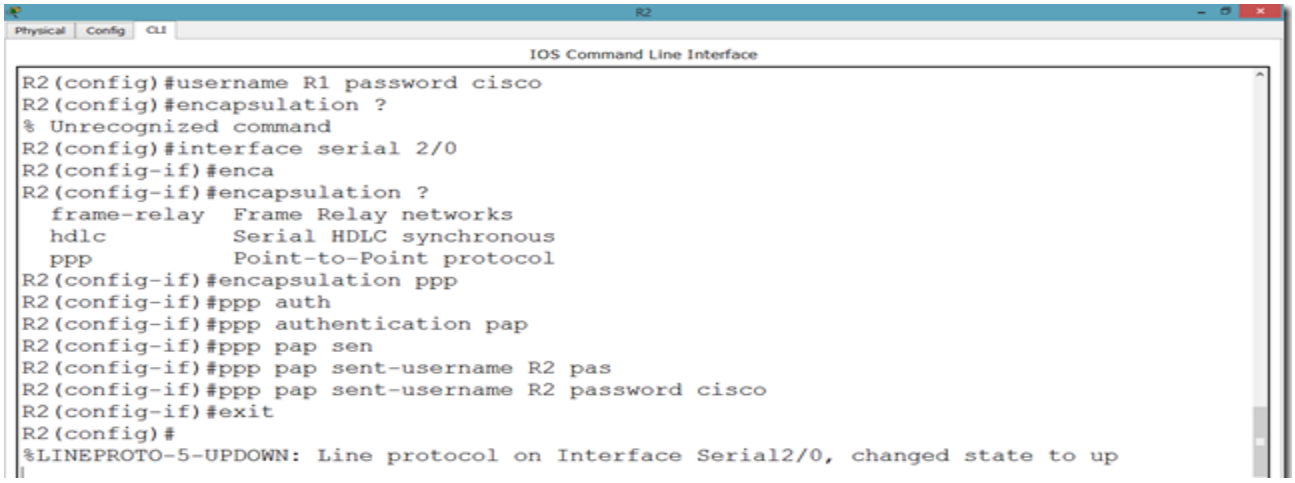
Now, we will set the authentication, In this tutorial we are going to apply PAP.



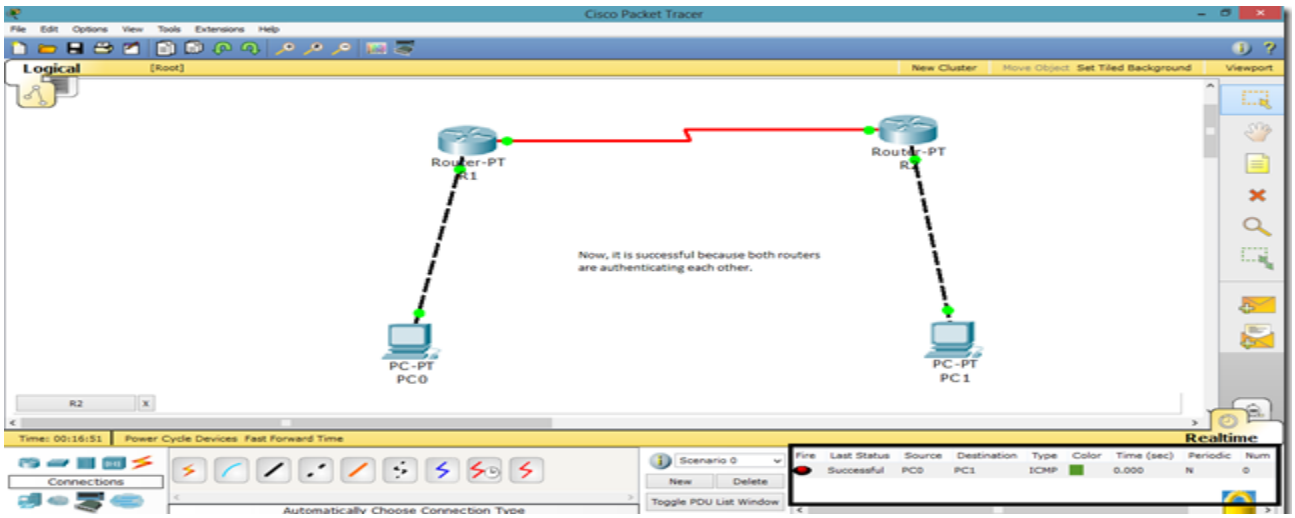
As we set the authentication on one router the communication is disabled.



Let us set it on other router as well.



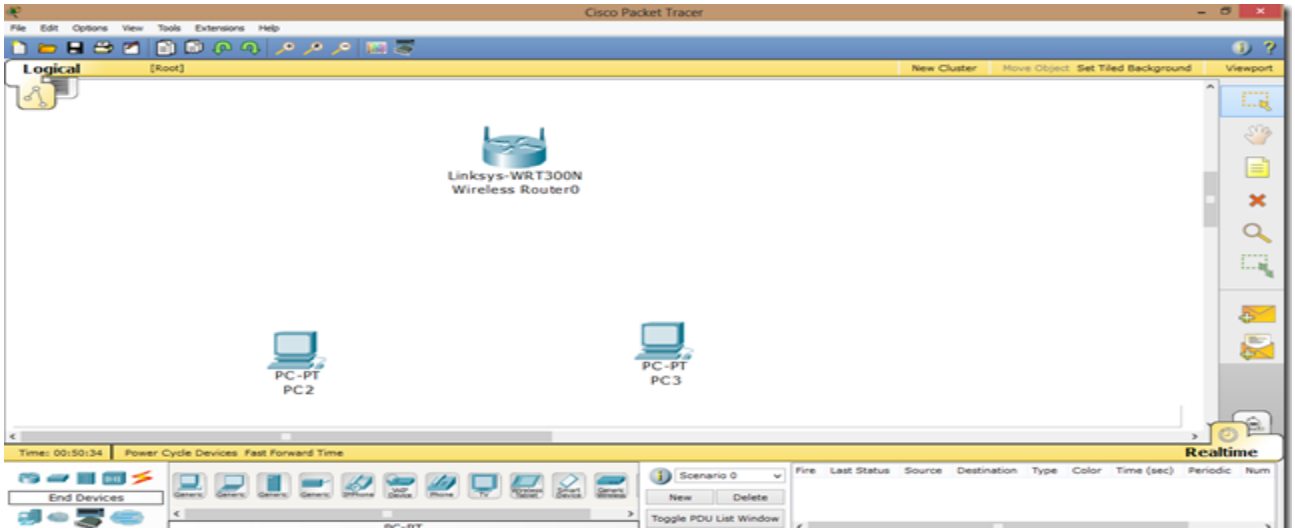
Now, they can communicate.



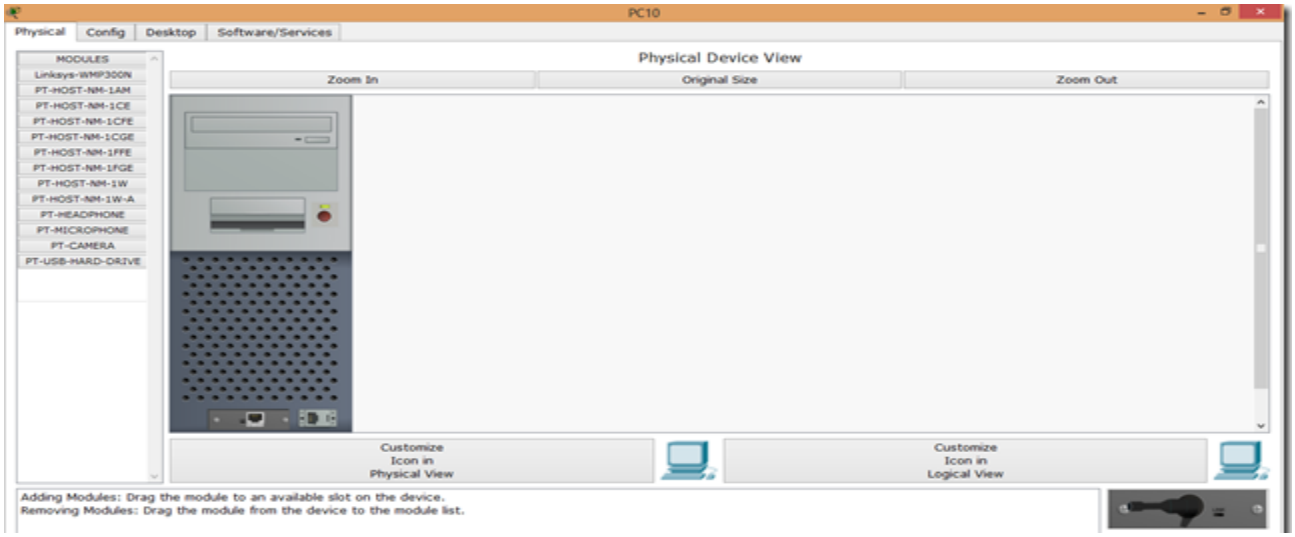
Now, if we run show run command in enable mode. We can see the

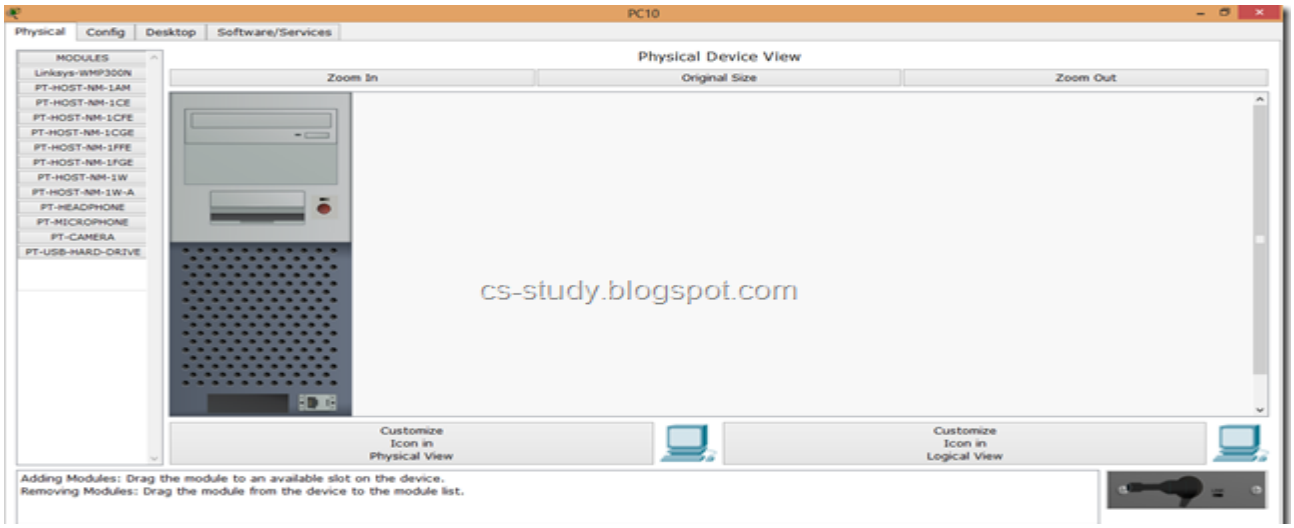
LAB # 23: Wireless Communication in Packet Tracer

Let us create wireless topology on packet tracer. For this go to the wireless devices and select linksys wireless router, take some PCs and provide them with wireless linksys module so that they can communicate through router wirelessly. For that go to the PC physical mode as shown in the figures below.

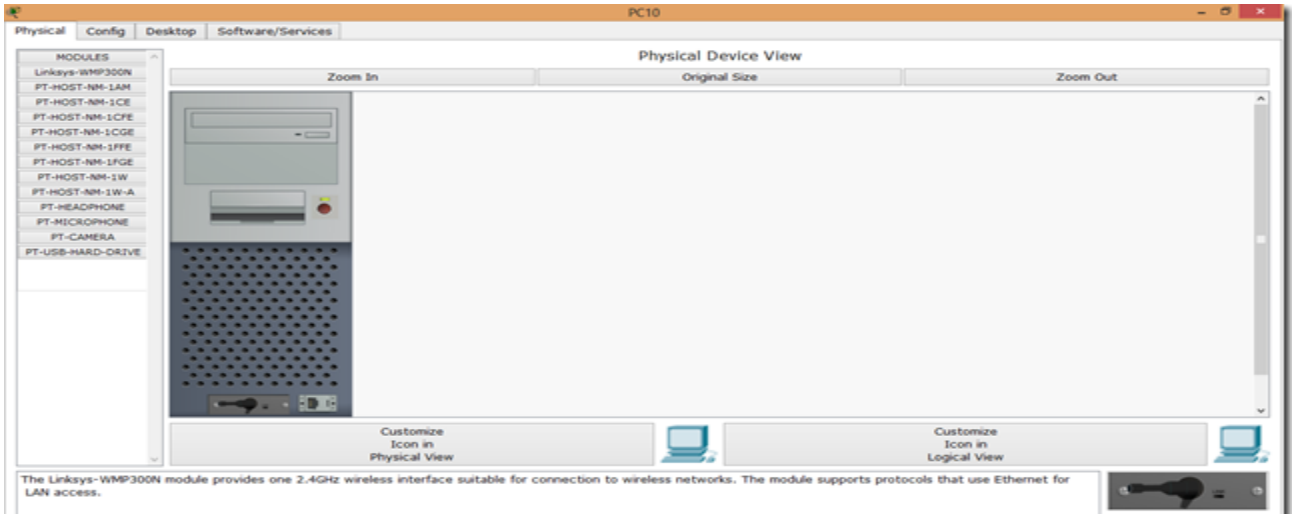


Go to PC, and remove wired LAN and install wireless LAN module.

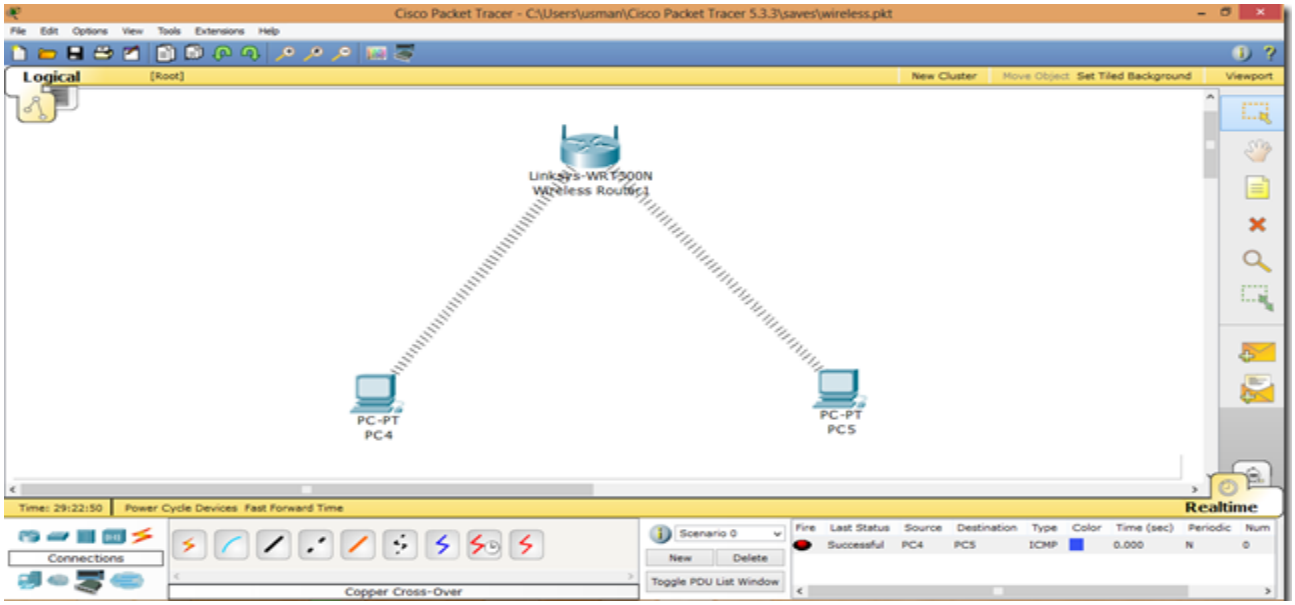




Now, its removed. Let us add wireless module.

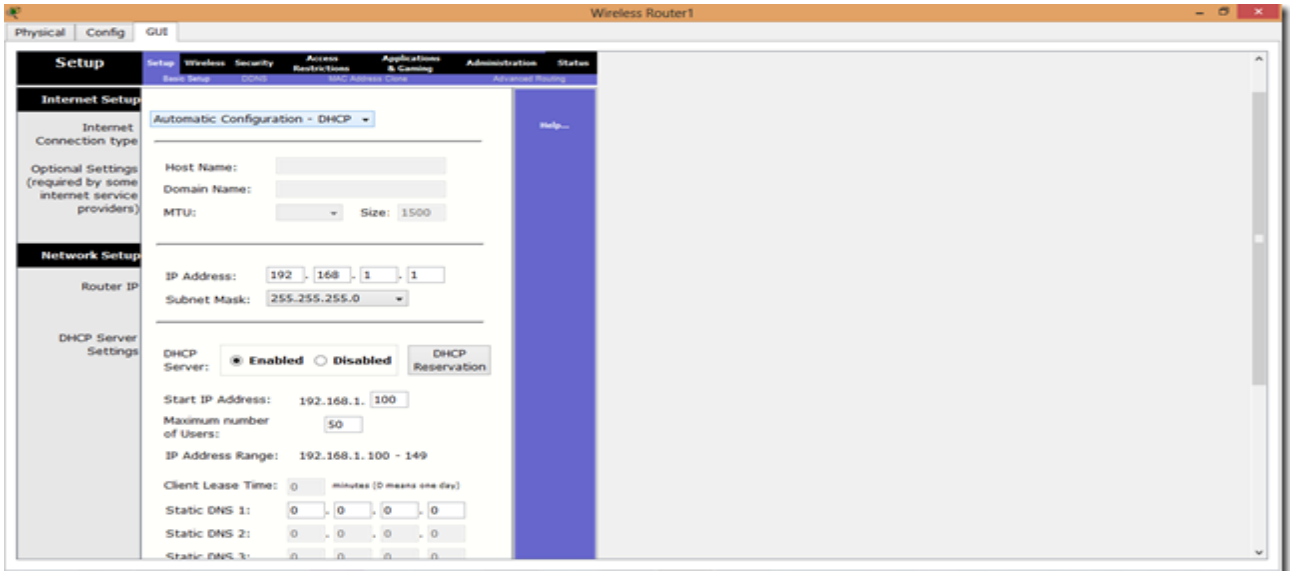


NOw, PCs are connected.

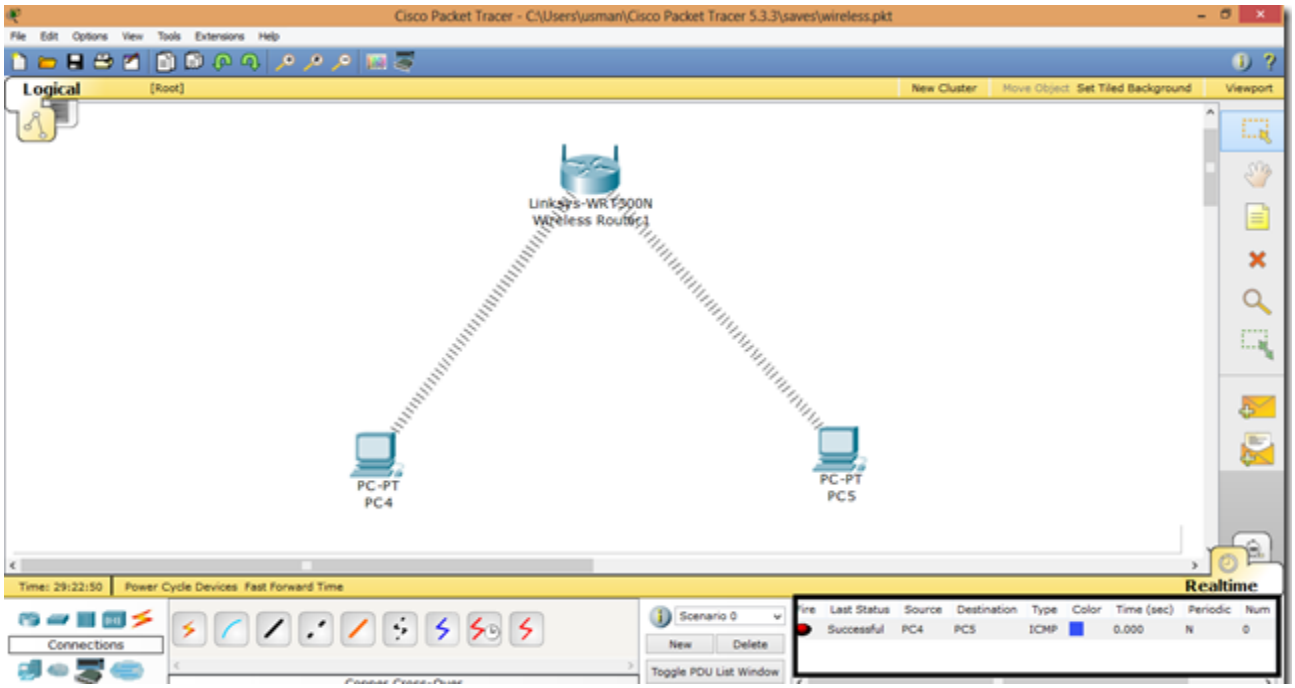


Set the IP address.

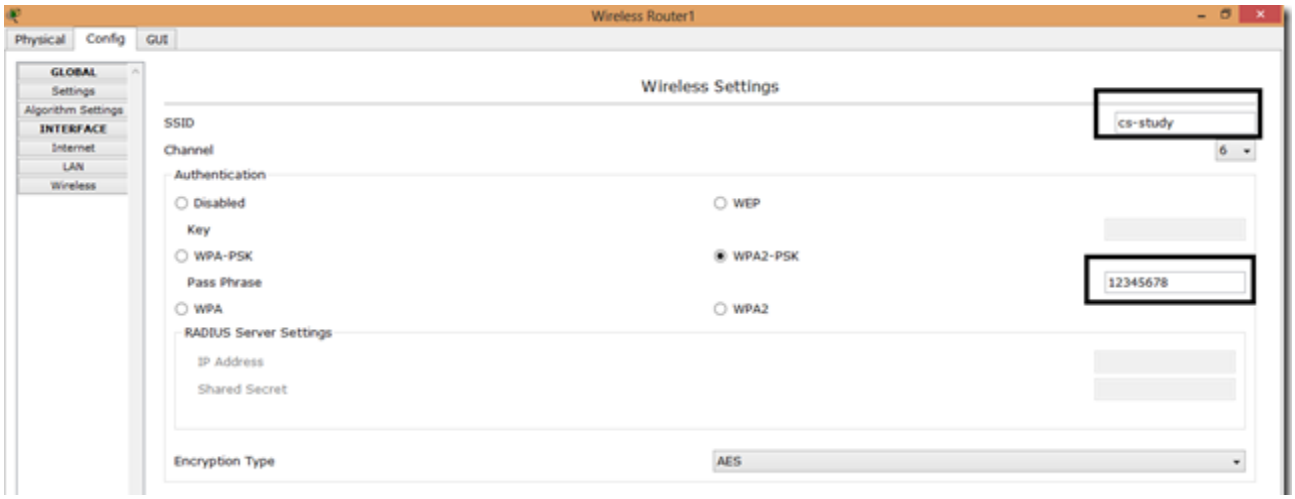
As this wireless router provides us with the DHCP service, so we can obtain IP automatically by using this service for our PCs.



So now our PCs can communicate.



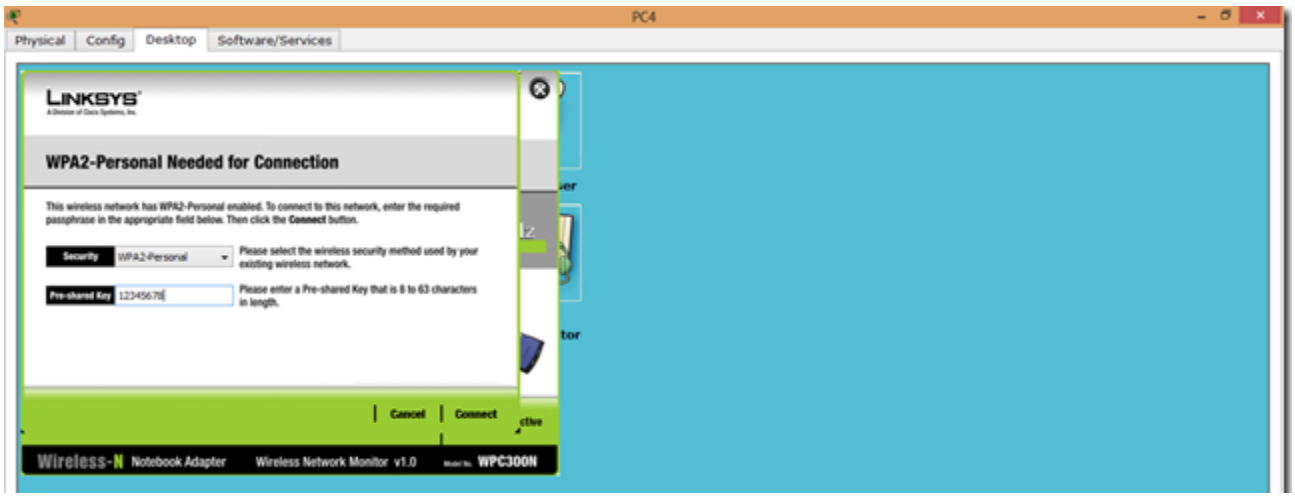
Now, let us apply authentication to our wireless router. For that, go to Config tab, click on Wireless. Provide it with the information as described below.



Go to PC desktop mode, Click on PC Wireless.

Click on connect. Select the device, you want to connect to, click connect.

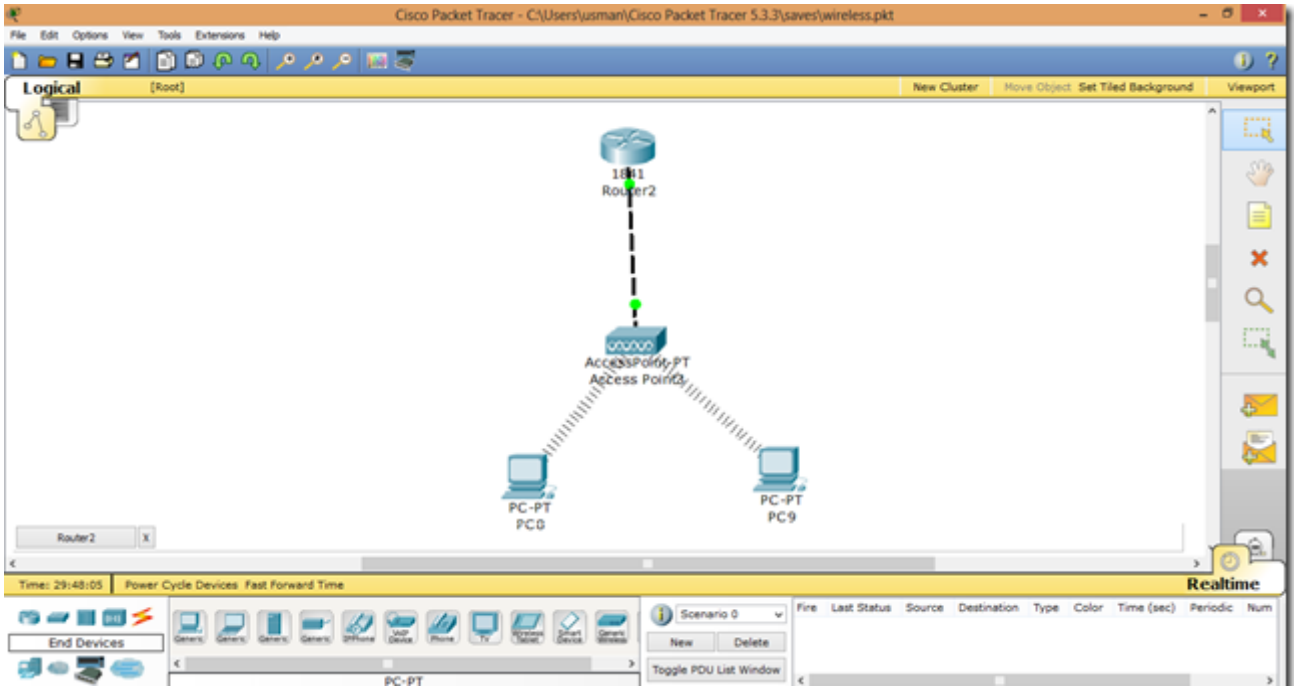
Give correct password.



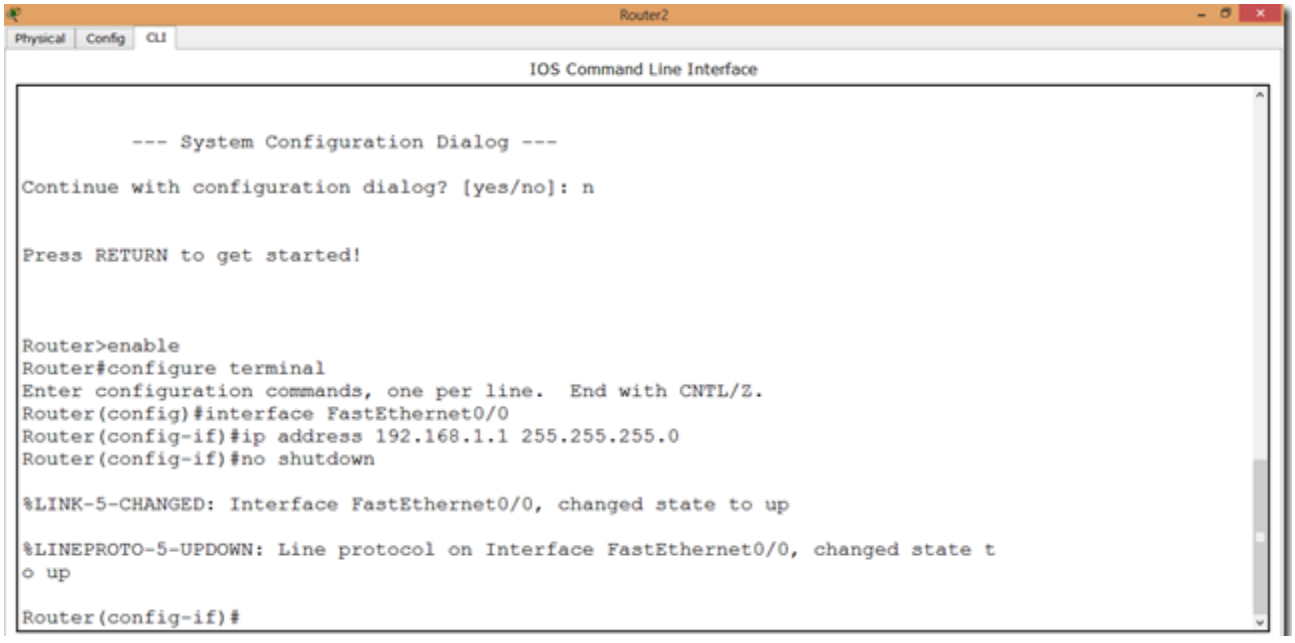
Now, we are done with it. We have successfully applied authentication.

Now, let us use Access point to connect to PCs wirelessly.

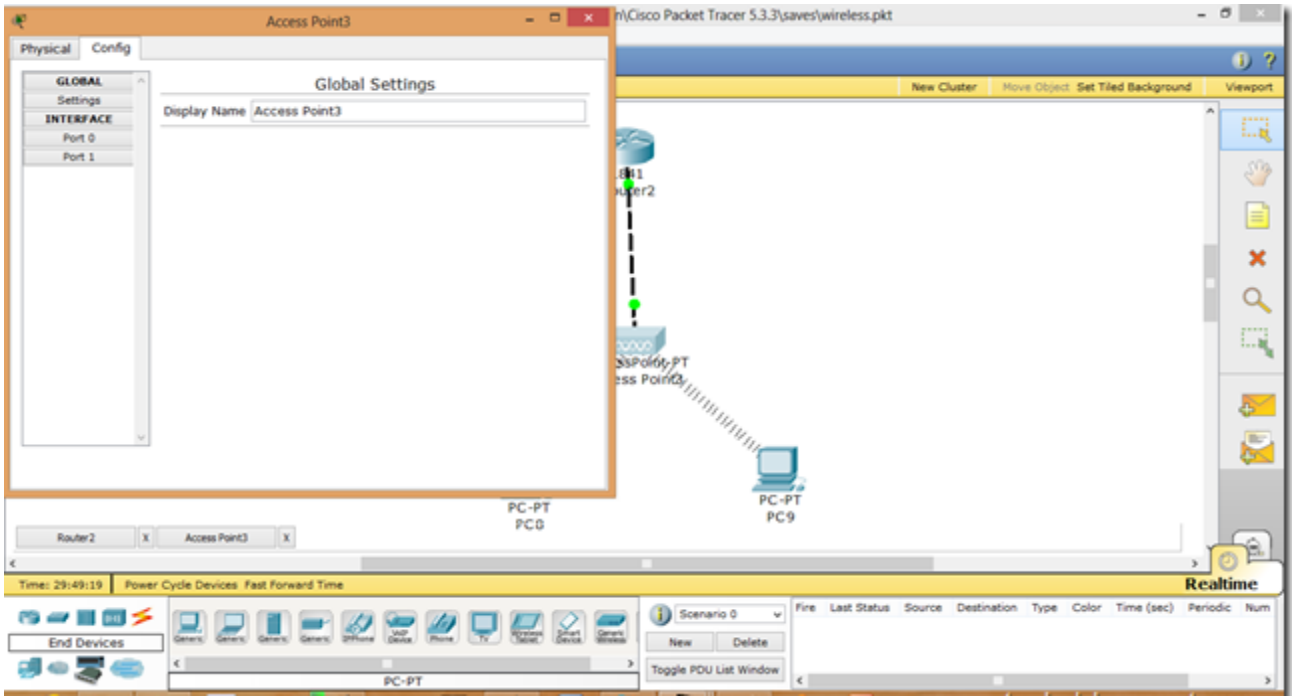
We can also connect wired router to access point in order to make our router wireless.



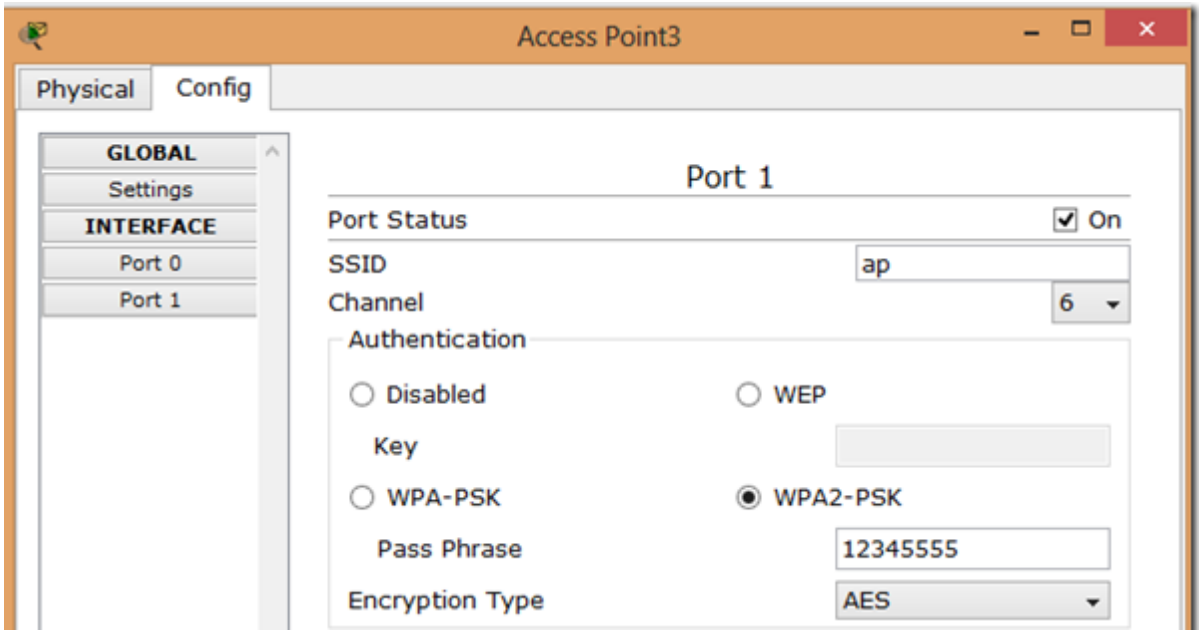
Apply IP addresses and put the status on.



We can also give authentication key to Access Point as well.



As in this figure below.



s