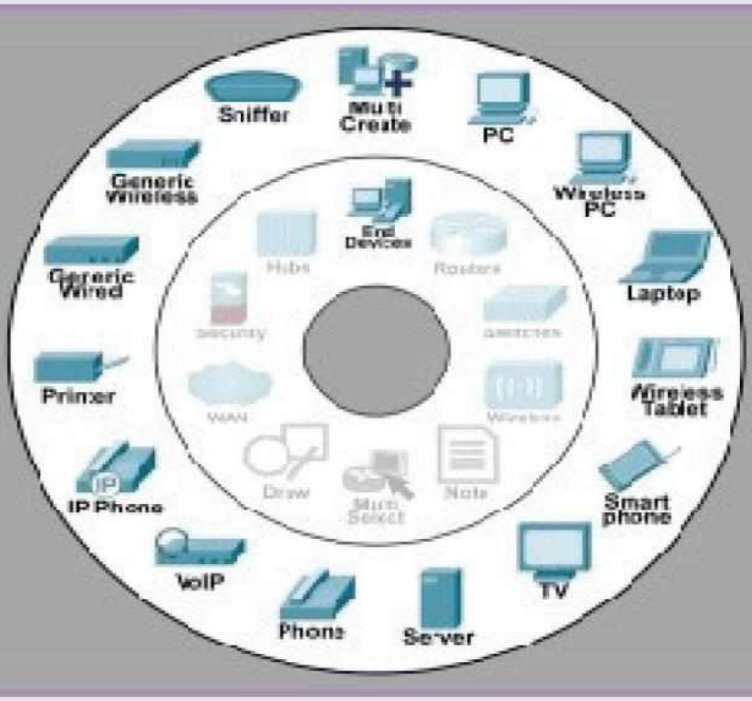
Learn Packet Tracer by Examples



Technical manual on configuring routers, switches and other networking devices

Learn Packet Tracer by Examples

Technical manual on configuring routers, switches and other networking devices

Blerton Abazi

ISBN: 1545240523
ISBN-13: 1545240523

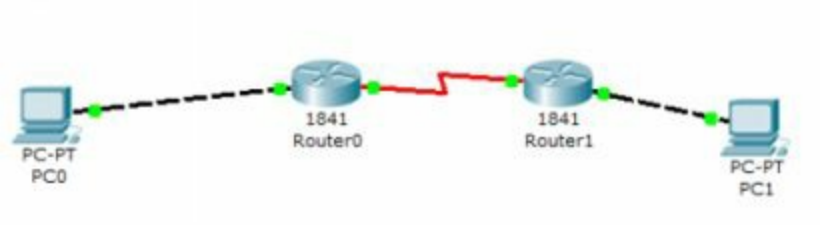
DEDICATION

I would like to thank all my colleagues and family for support.

Cisco Routing Basics

The intructions are intended to assist students who are just starting to learn about configuring Cisco routers and explore some simple networks using static, RIP and RIPv2 routing configurations.

Create the simple network



Simple Packet Tracer Router Network

Configure the PCs and Routers

The commands which are typed in to the left router are also shown here and will appear something like the following when typed (I've only included the lines in which the user typed something).

```
Router>enable
Router#configure terminal

Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface serial 0/1/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

The configuration of the router on the right hand side will be very similar. However, the IP addresses will be different and dependant on which end of the serial connection (between the routers) has the DCE end the "clock rate" command should not be required. Rather than typing the commands in it is possible to past a series of confiugaration commands in and to have them executed one after the other. While I don't recommend you do this while you are learning showing the configurations in this format is a short hand way of making the configuaration of the routers clear. As such the following shows the configuarion of both the left and right hand side router from the previous image.

```
!
! Configuration for the left hand router
!
```

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Serial0/1/0
ip address 192.168.2.1 255.255.255.0
clock rate 64000
no shutdown
!
! Configuration for the right hand router
!
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
no shutdown
!
interface Serial0/1/0
ip address 192.168.2.2 255.255.255.0
no shutdown
```

Adding Static Routes

Once all the interfaces are configured to allow all devices to communicate the routes need to be communicated. To do this in this instance we add static routes.

The actual route commands required on the routers are as follows

```
! route for left hand router
ip route 192.168.3.0 255.255.255.0 Serial0/1/0
```

```
! route for right hand router
ip route 192.168.1.0 255.255.255.0 Serial0/1/0
```

Using RIP instead of static routes

Instead of adding static routes to get the network to operate correctly it is possible to use a routing protocol. In this lesson we use the same network as originally created but without the static routes from the previous step. Instead we shows how to setup RIP to communicate routing information between routers.

The necessary RIP commands for both the routers are as follows.

```
! commands for the left hand router
router rip
network 192.168.1.0
network 192.168.2.0
```

```
! commands for the right hand router
router rip
network 192.168.3.0
network 192.168.2.0
```

RIP version 2 and why

RIP version 1 is a classful routing protocols. This means that it doesn't provide a subnet mask in routing updates to other routers and as such it doesn't support certain network and subnet arrangements. I will not go into too much detail here as you can find out more from the CCNA course material. However, I provide a simple example here of a network in which RIP version 1 would not work to advise the neighboring router of known routes correctly.

Using the same network topology as initially shown use the following three subnets to provide IP addresses. The subnets are 10.1.1.0/24, 192.168.2.0/24, and 10.1.3.0/24. The configuration of the routers is as follows.

```
! configuration for left hand router
interface FastEthernet0/0
ip address 10.1.1.1 255.255.255.0
no shutdown
!
interface Serial0/1/0
ip address 192.168.2.1 255.255.255.0
clock rate 64000
no shutdown
!
router rip
network 10.0.0.0
network 192.168.2.0
```

```
! configuration for right hand router
interface FastEthernet0/0
ip address 10.1.3.1 255.255.255.0
no shutdown
!
interface Serial0/1/0
ip address 192.168.2.2 255.255.255.0
no shutdown
!
router rip
network 10.0.0.0
```

network 192.168.2.0

This configuration requires the LHS PC has an IP address of 10.1.1.2 and the RHS PC has an address of 10.1.3.2.

When this network is setup with these configurations you will find that the PCs will not able to ping each other. The reason being that a class C network address (192.168.2.0) is between two subnetted class A addresses (10.0.0.0). There are several commands which will assist to verify this. The first command is "show ip route". This command will show the routes in the route table. Another command is "debug ip rip", which can be reversed with "no debug ip rip", but while it's on you get an idea what routing information passes between the routers.

To get this network to work and for each router to be aware of all routes all that is required is to add the "version 2" into the RIP configuration. This changes the RIP protocol from version 1 to version 2 and turns it from a classful protocol to a classless protocol. In effect it allows for the subnet mask to be transferred with a network and therefore, in this instance, the routers can now learn about the networks the other rotuers have attached. Below I show the complete configuration with the "version 2" and "no auto-summary" settings added in. I suggest you initially just add the version 2 setting by going into the configuration mode and first typing "router rip" and then at the prompt typing "version 2 – it should look somehting like this: Router(config-router)#version 2. Once done on both routers the network should work and you can check with "show ip route" command. You can then add the "no auto-summary" setting to see what happens, to do that you'll need to use the "show ip route" command again. Anyway the complete RIP version 2 configuration for the network is as follows.

```
! configuration for left hand router
interface FastEthernet0/0
ip address 10.1.1.1 255.255.255.0
no shutdown
!
interface Serial0/1/0
ip address 192.168.2.1 255.255.255.0
clock rate 64000
no shutdown
!
router rip
version 2
network 10.0.0.0
network 192.168.2.0
no auto-summary
```

```
! configuration for right hand router
interface FastEthernet0/0
ip address 10.1.3.1 255.255.255.0
no shutdown
!
interface Serial0/1/0
ip address 192.168.2.2 255.255.255.0
no shutdown
!
router rip
version 2
network 10.0.0.0
network 192.168.2.0
no auto-summary
```

The IP addresses on the computers are the same as set previously (i.e. LHS PC has an IP address of 10.1.1.2 and the RHS PC has an address of 10.1.3.2).

Configure a DHCP server in multiple VLAN's

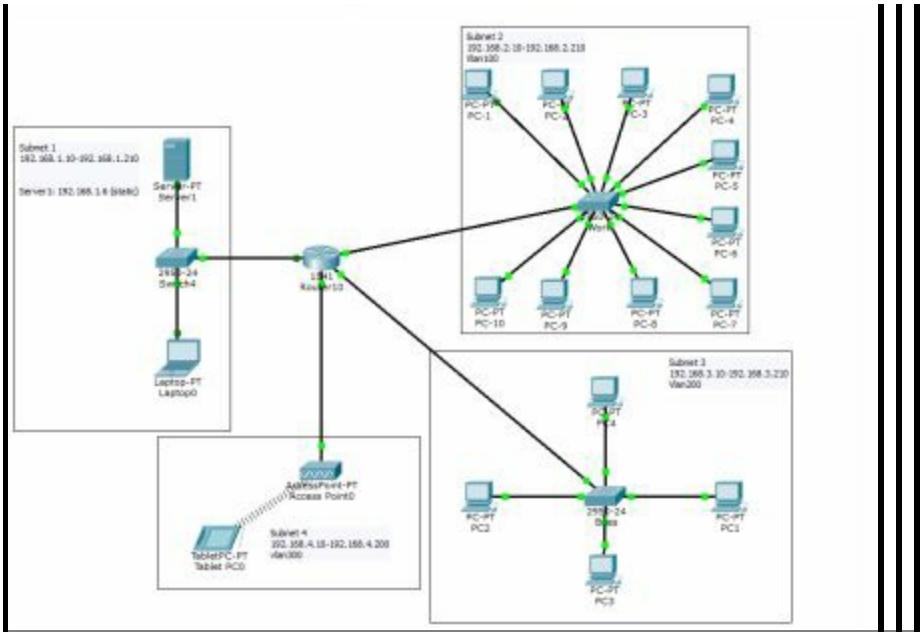
Information

For my school project we had to make a network for our fictive business. Because we cannot build the network physical we made it in Packet Tracer. The requirements for our network are:

- Multiple VLAN's
- Physical DHCP server

This is a very small network with basic subnetting. This tutorial is just to show you how you can have 1 DHCP server for multiple VLAN's.

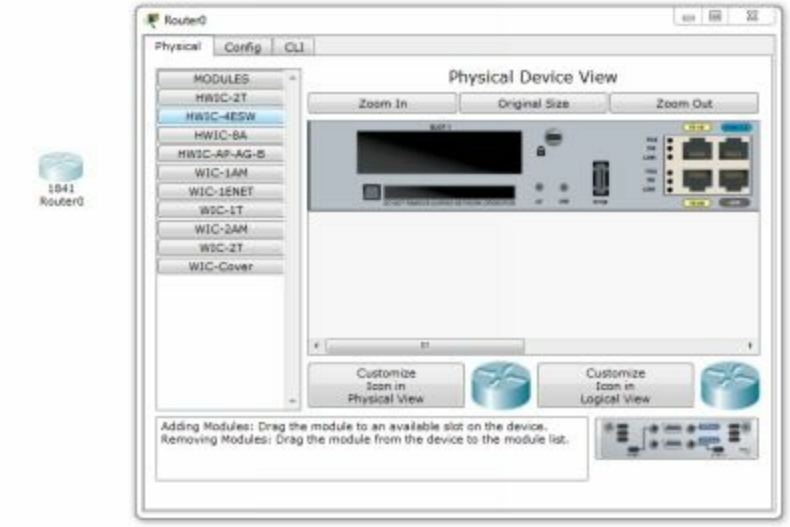
Result



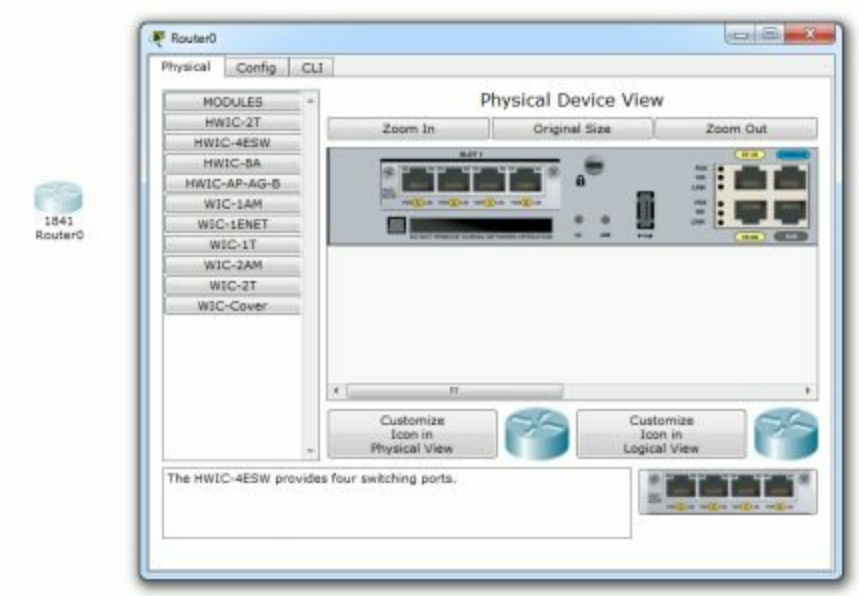
Network with multiple VLAN's and a DHCP server.

Tutorial

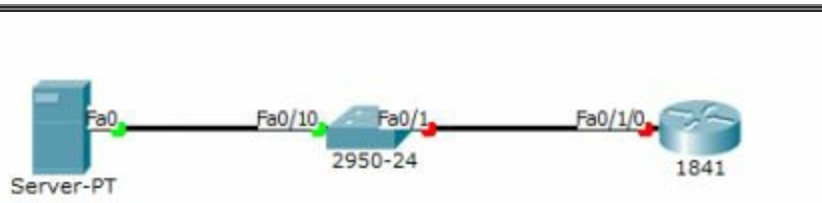
So, how do you build this network. In the following steps I will try to explain step by step. I made a screenshot of every step. But if you just want the commands just scroll down to the running config of the router.



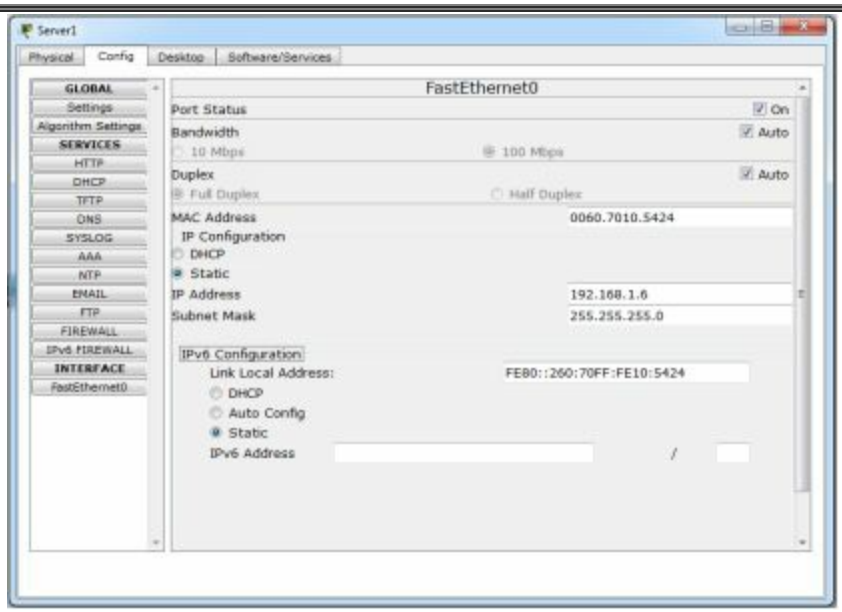
Step 1: First add a router, in this case I took the standard one: "1841". But this router does not have enough ports so we add the "HWIC-4ESW" module. This module contains 4x FastEthernet ports. Do not forget to power off the device before you add the module.



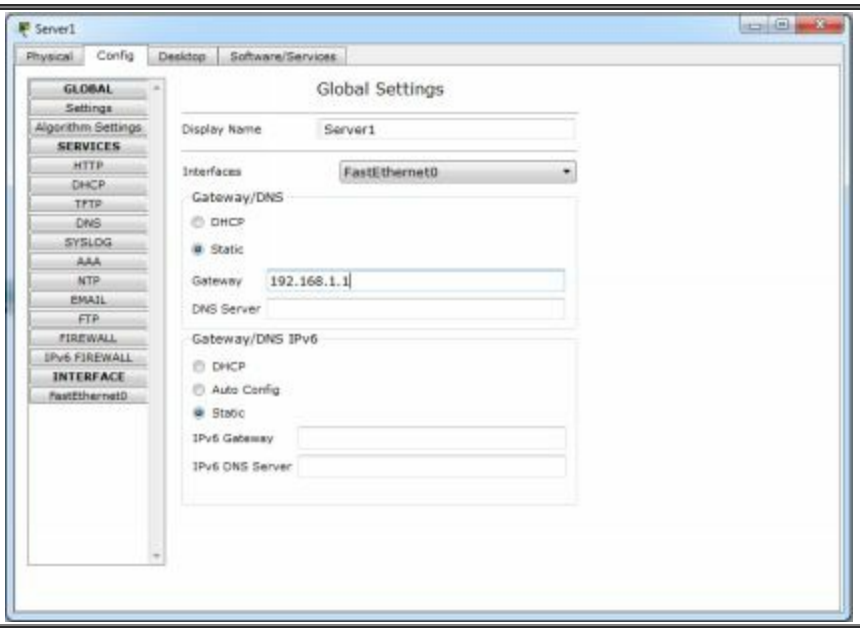
Step 2: When you have added the "HWIC-4ESW" module you can power on the device again.



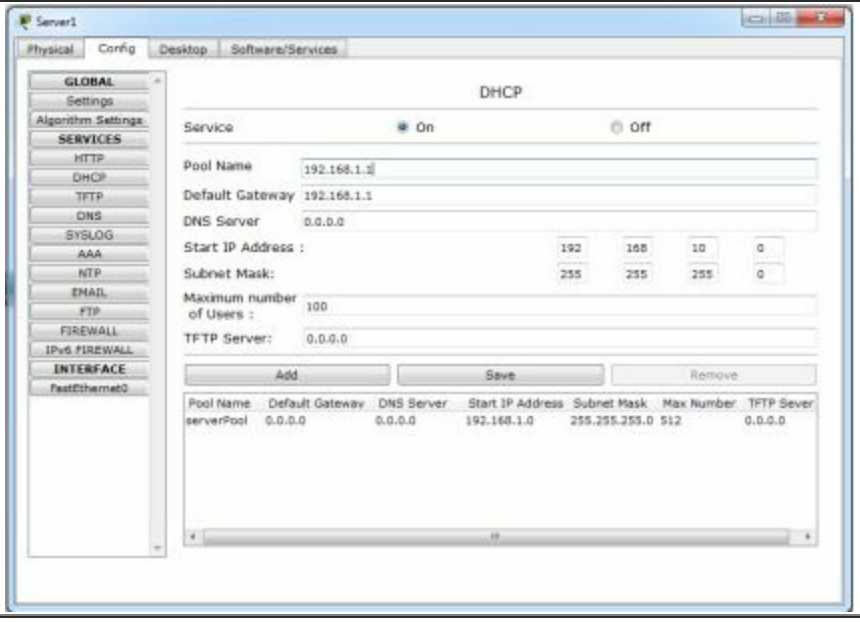
Step 3: Now add your server and a switch. Connect them with a straight-through cable. For the switch you can choose but I have chosen the "2950-24". The server you can find in "End Devices".



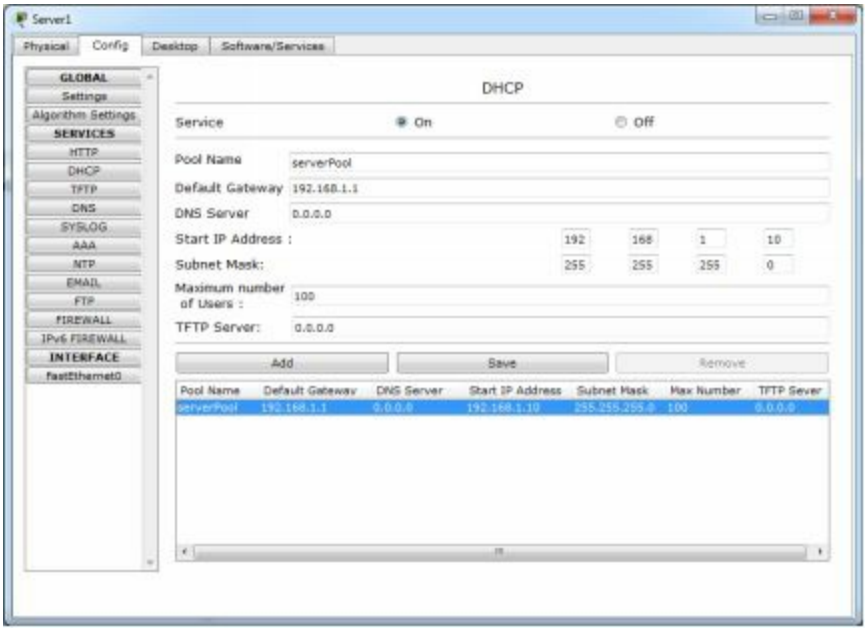
Step 4: When you have added the server it's time to configure it. First we give the server a static ip address. For this server I used 192.168.1.6 and 255.255.255.0 as subnet mask.This is a personal choice, if you want to use a other ip address, you can.



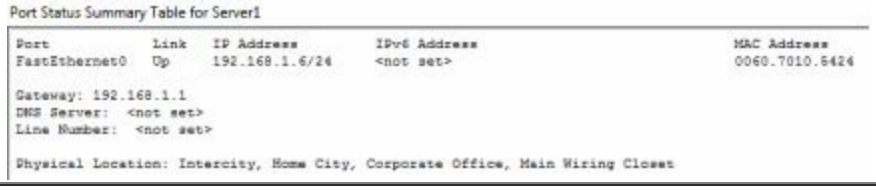
Step 5: Next we have to configure the default gateway. Since our ip address is 192.168.1.6 we have to choose one in the same local network. I always choose the first ip address available in the local network. So here our default gateway is 192.168.1.1.



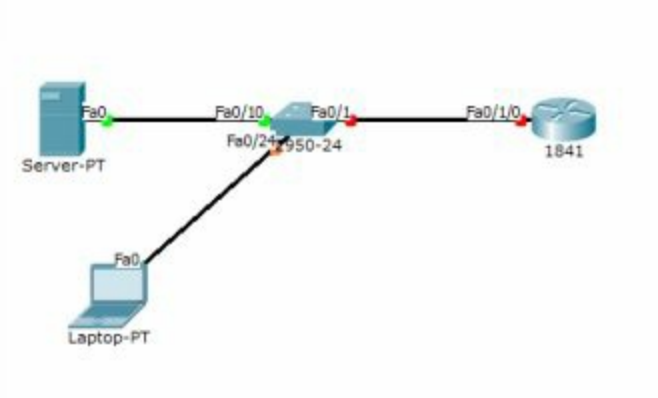
Step 6: Now we can configure the DHCP server. The first pool is for our local network 192.168.1.0.



Step 7: The start ip is 192.168.1.10 with a subnet mask 255.255.255.0. With a maximum of 100 users. So the ip addresses available for the DHCP clients are 192.168.1.10-192.168.110.

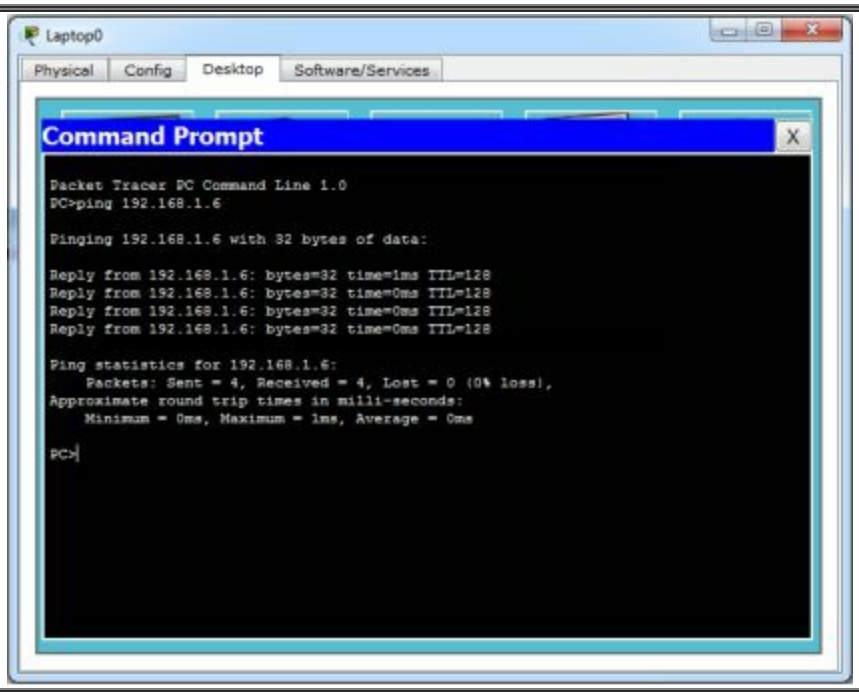


Step 8: When our DHCP server is configured the port status summary should look like this.

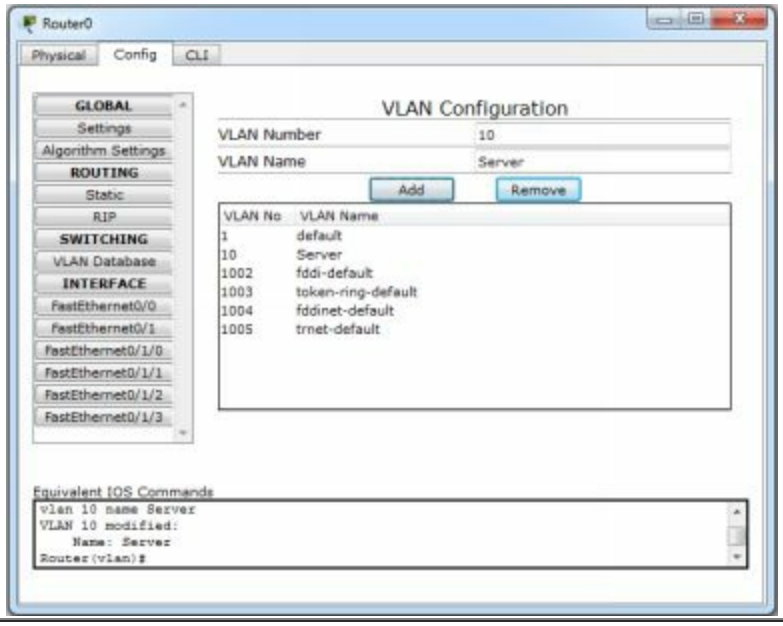


Step 9: Now we add a computer in the same local network. For example a laptop and connect it to the switch.

Step 10: Now change the ip configuration to DHCP. Now our laptop has a ip address provided by the DHCP server.

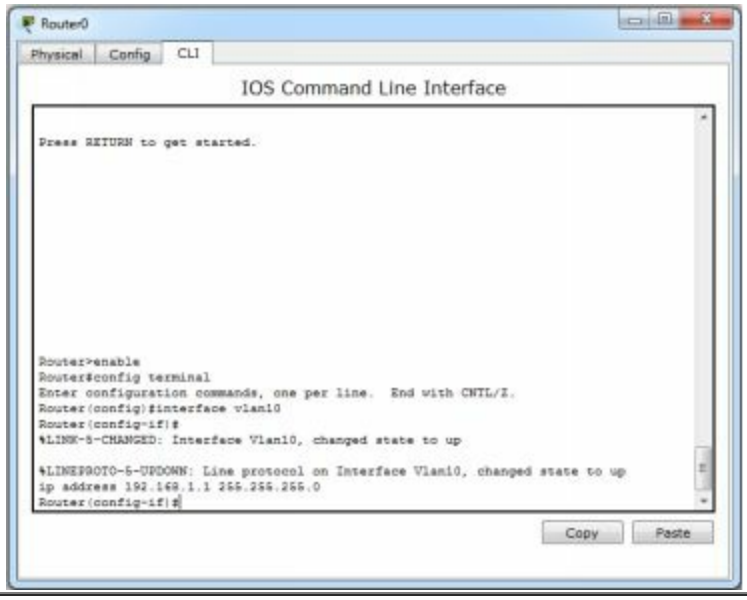


Step 11: To verify our network works you can ping from the laptop to the server.

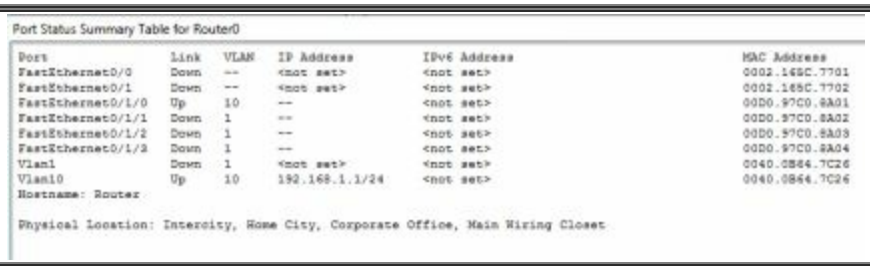


Step 12: We have to create VLAN's on our router. We do this step by step so now we only add our VLAN for the subnet where our server is located.

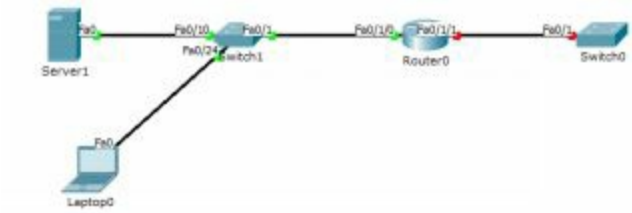
Step 13: We have made our VLAN, but we still have to assign it to the right FastEthernet port. I have plugged this particular network to "FastEthernet0/1/0". Here we change the VLAN to 10. **Also do not forget to change the port status to on!**



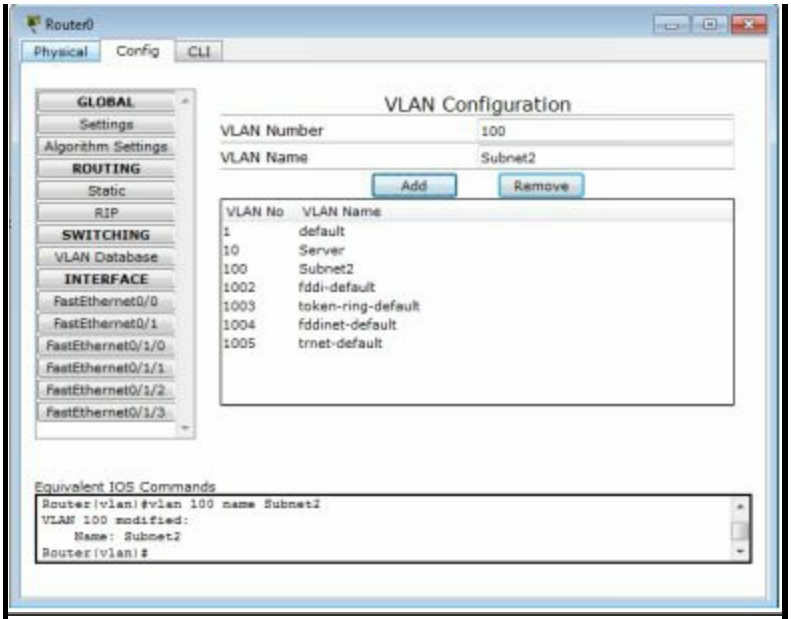
Step 14: We also have to give the VLAN an ip address. You can easily do this in the CLI. The commands you can see in the screenshot.



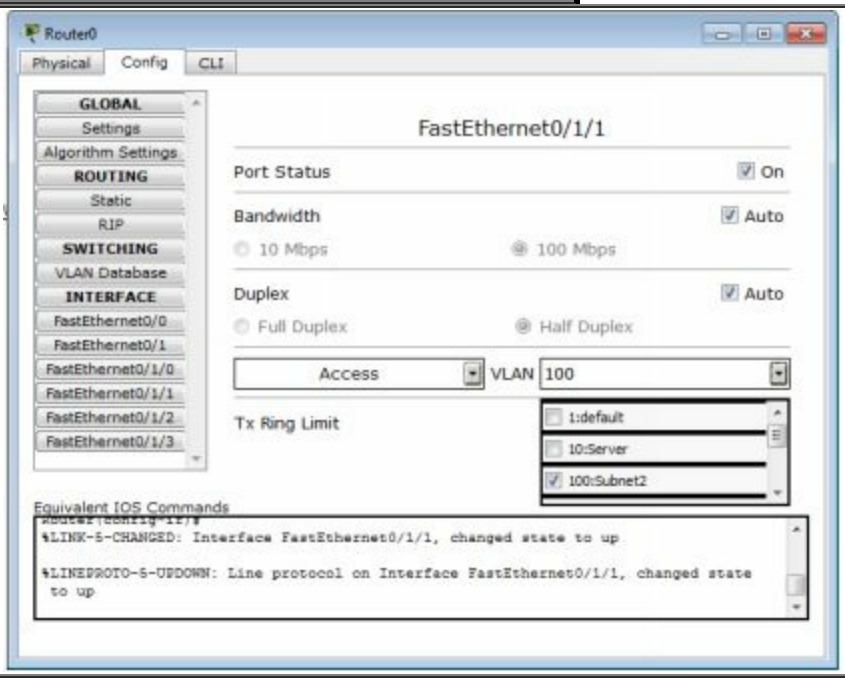
Step 15: After these steps the port status summary should look like this.



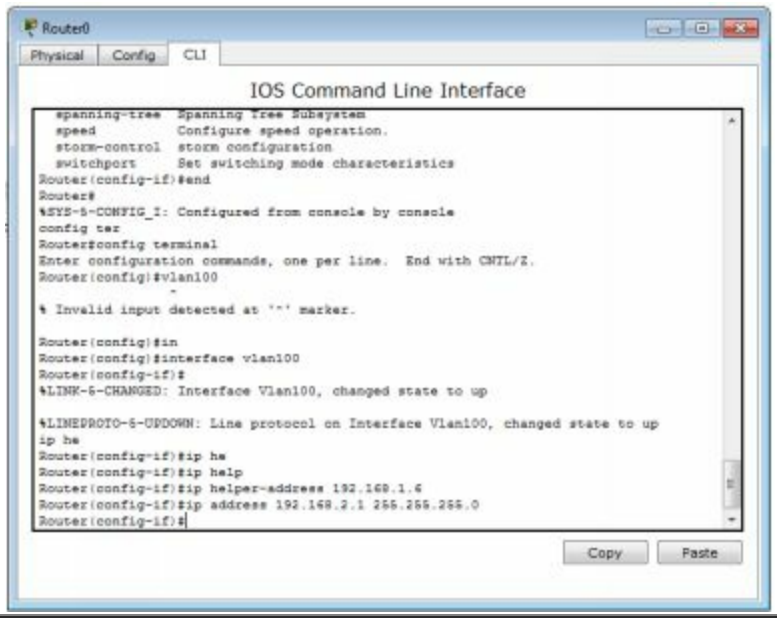
Step 16: Now we can start building our second subnet, starting by adding a new switch.



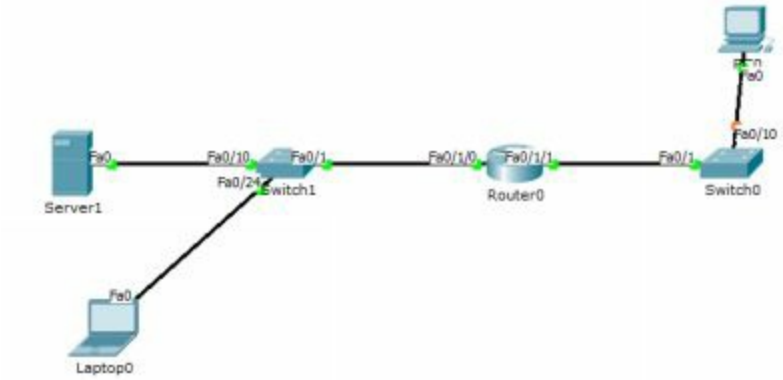
Step 17: Adding the second subnet to the router.



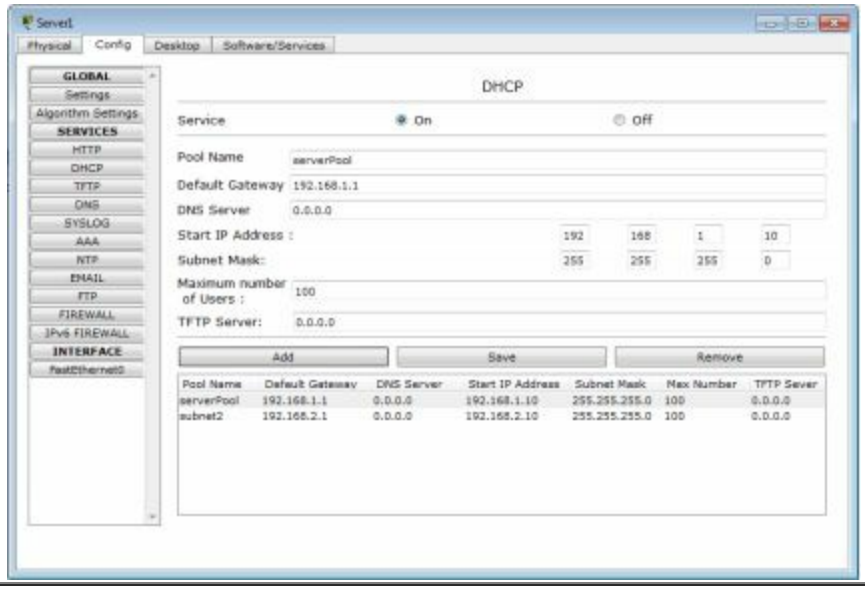
Step 18: Change the port status to on, and the VLAN to the one we just created.



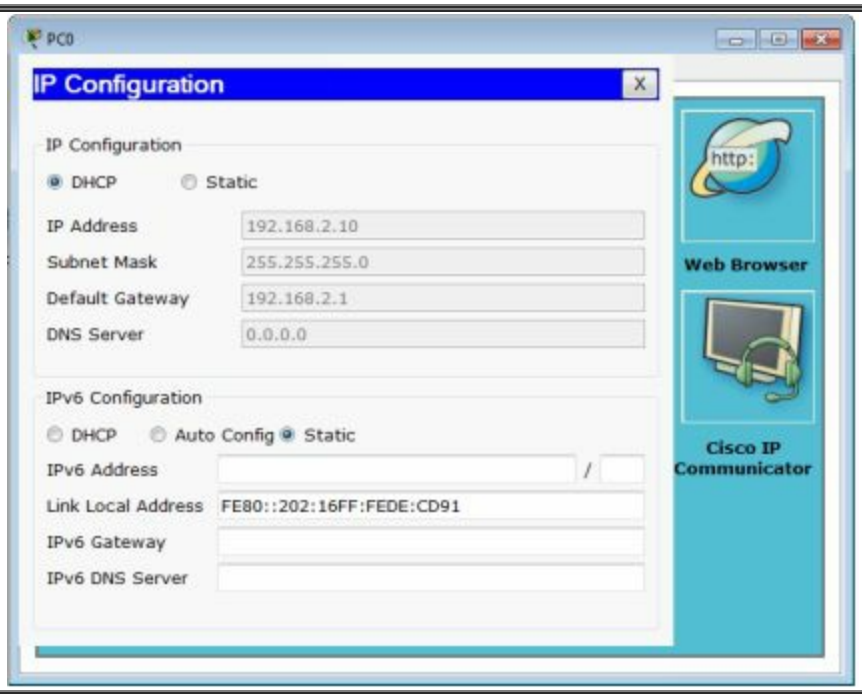
Step 19: Also we have to configure an ip address for VLAN 100. Because our DHCP server is located in a other subnet we have to use the ip helper-address command. This will enable our DHCP packets to flow to 192.168.1.6.



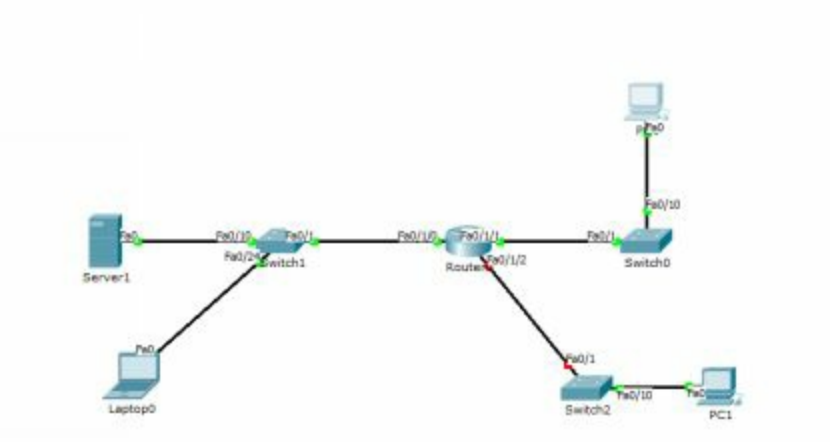
Step 20: The basic network is made. By adding a new end device to the new switch we can test our DHCP server.



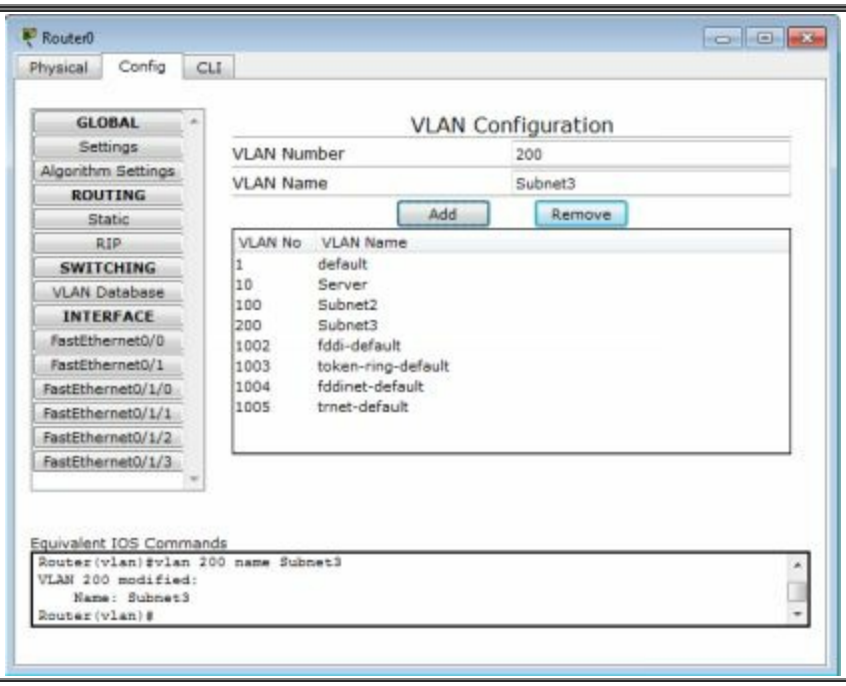
Step 21: But first we need to add an other pool to our DHCP server. This time we need to add the 192.168.2.0 network.



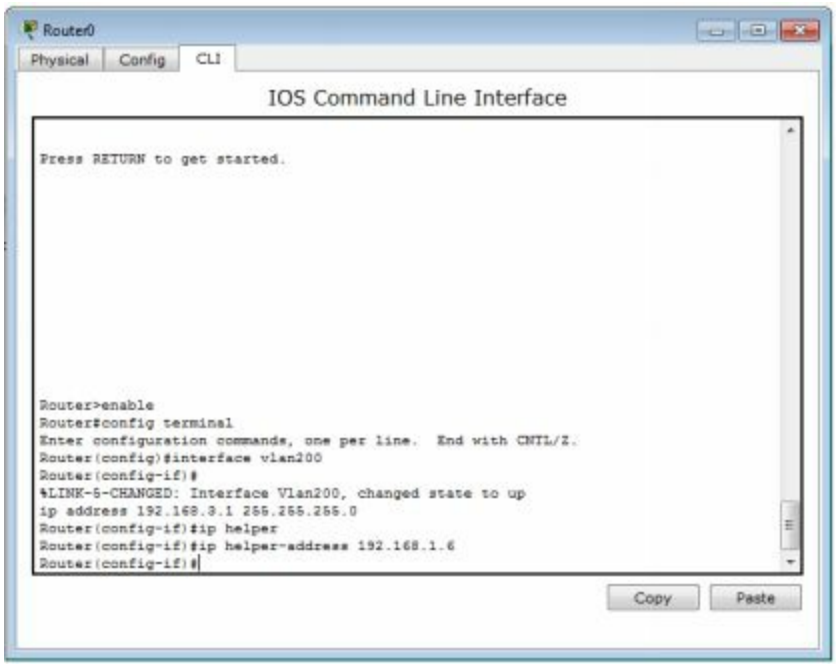
Step 22: When the pool is added we can test the configuration. Go to your pc on the second subnet and change the ip configuration to DHCP. After some seconds your pc should have a ip address provided by the DHCP server.



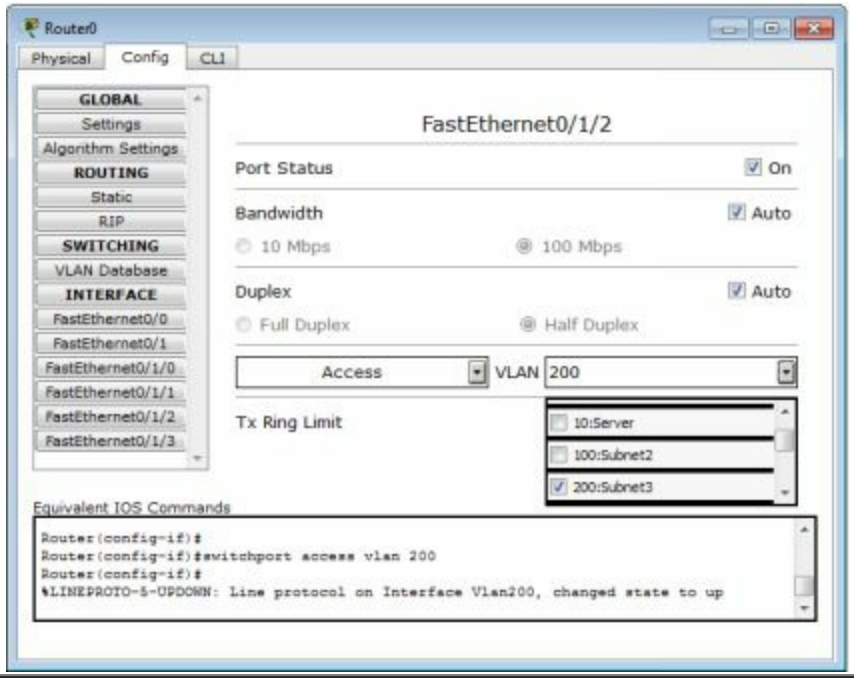
Step 23: Now add a third switch and a pc for our third subnet.



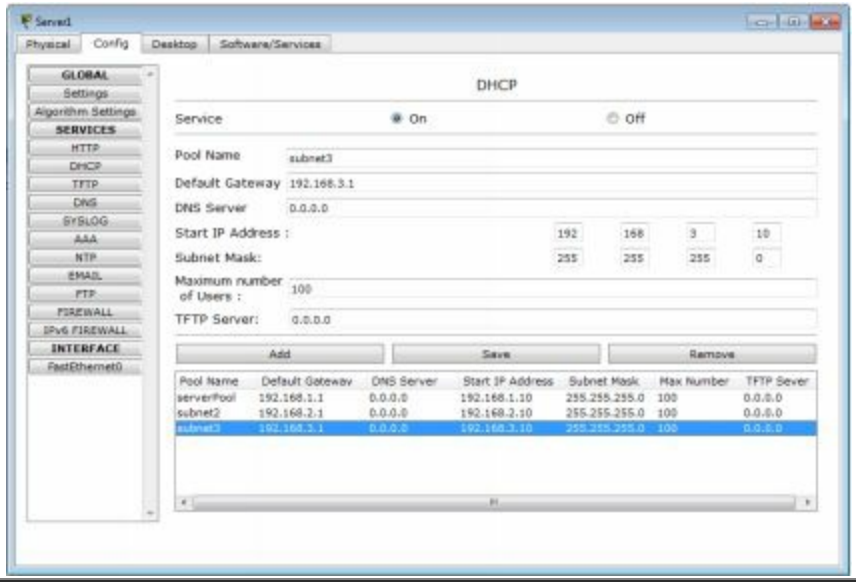
Step 24: Again we have to add a new subnet in our router.



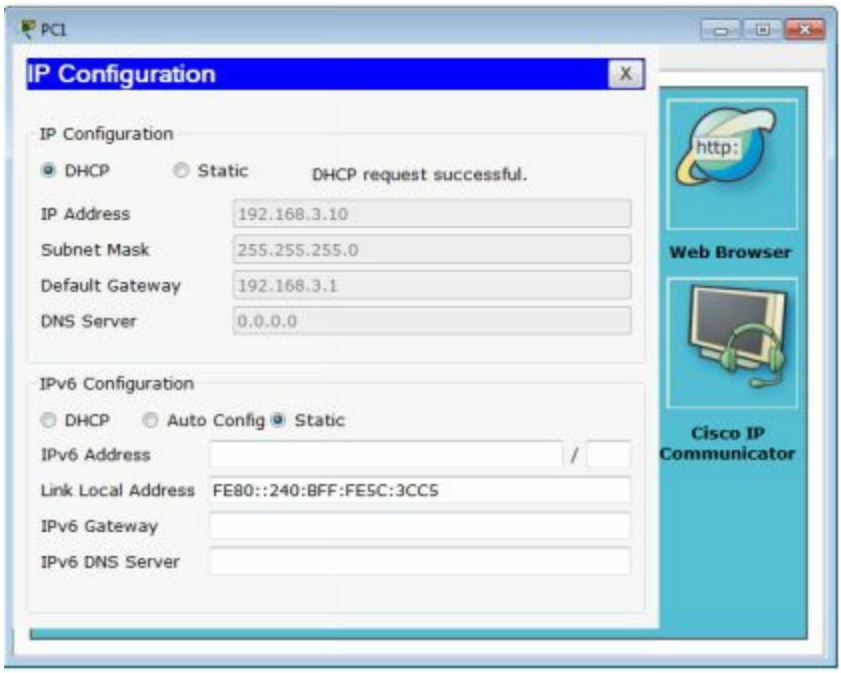
Step 25: Also again configure the ip address and ip helper address.



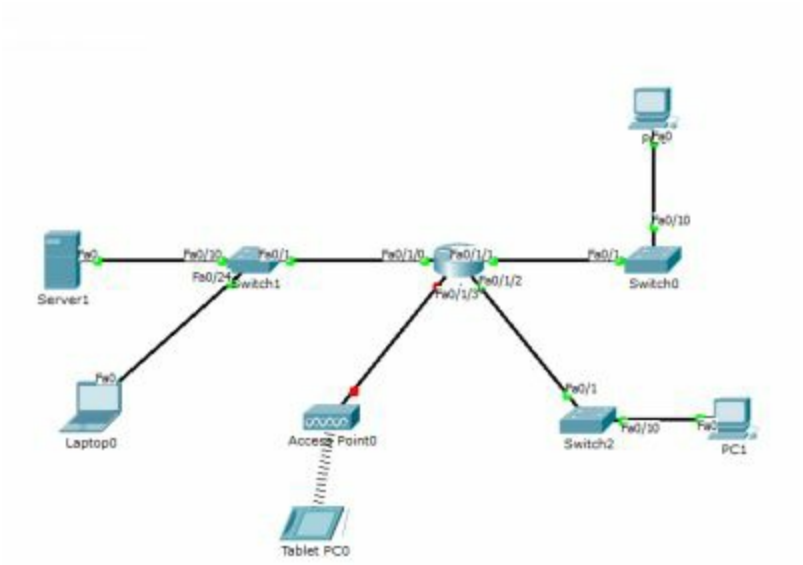
Step 26: Change the "FastEthernet0/1/2" to VLAN200. Again switch the port to on.



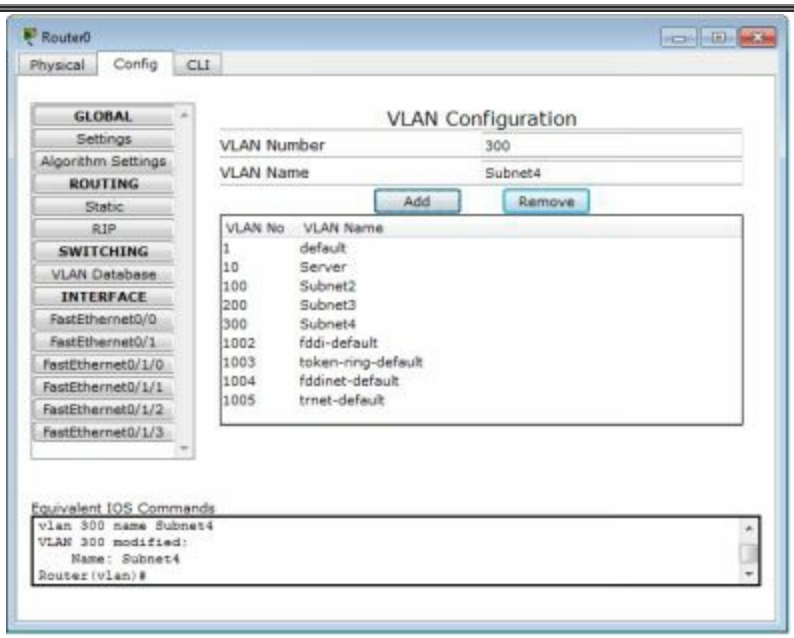
Step 27: Now add the third subnet to the pool. This time it's network 192.168.3.0.



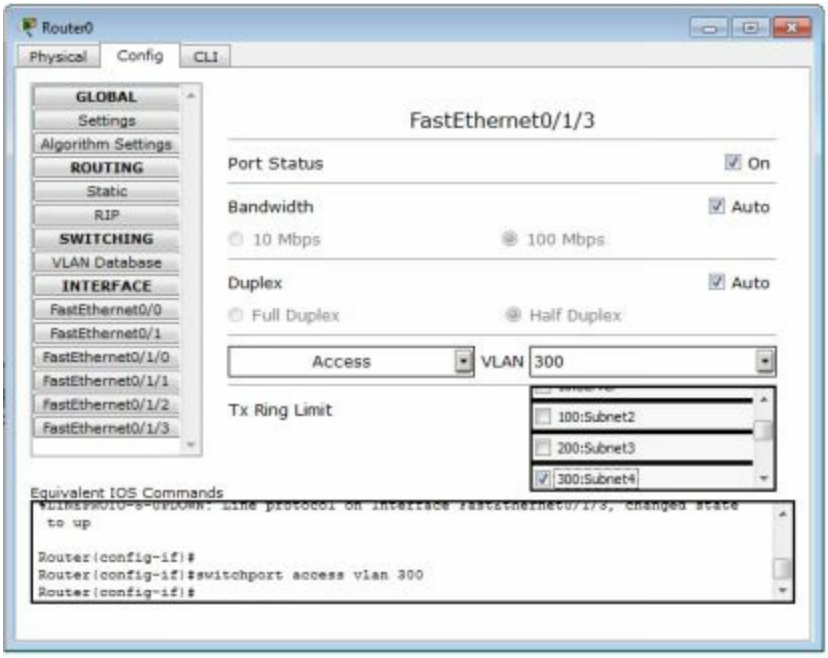
Step 28: Again change the ip configuration to DHCP. Normally your pc will receive an ip address.



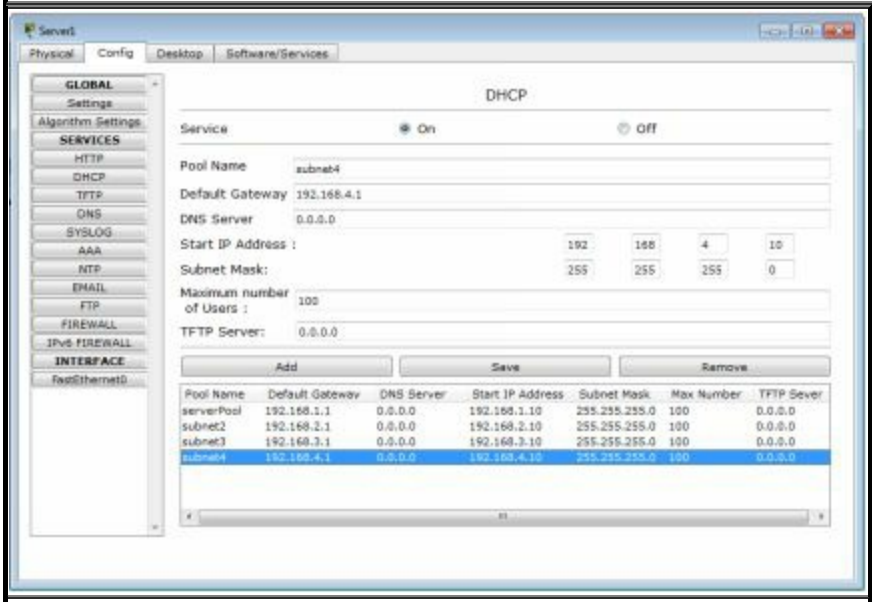
Step 29: The last subnet is connected with an access point. Add the access point and a wireless device to your network.



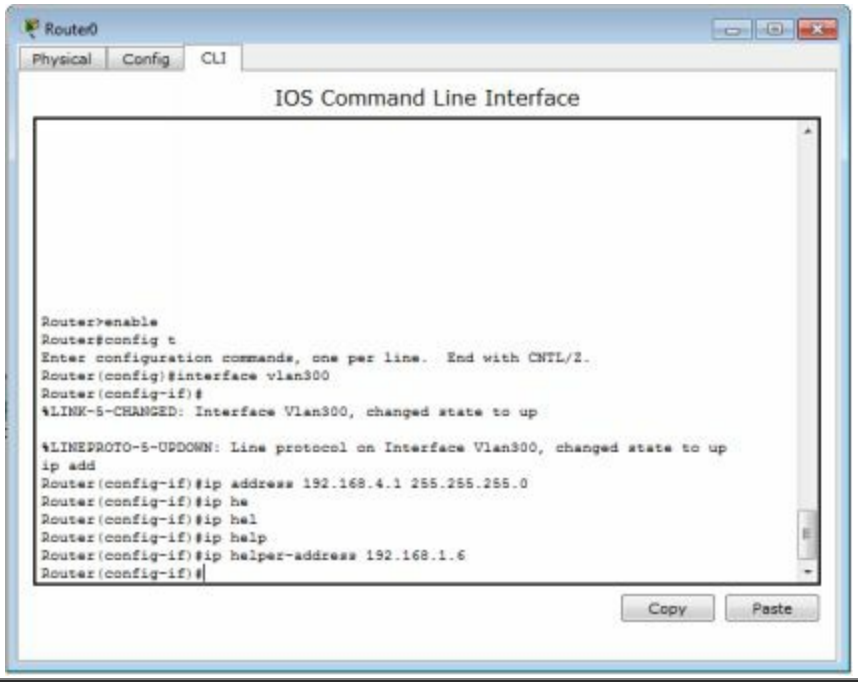
Step 30: Next we add the last subnet: Subnet4 with number 300.



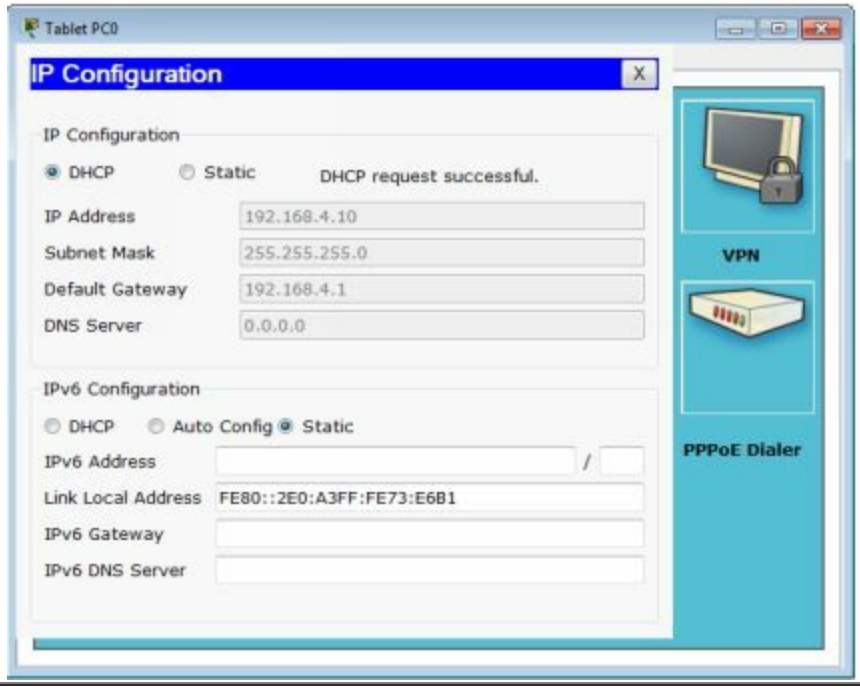
Step 31: Again change the VLAN of "FastEthernet0/1/3". **Do not forget to switch the port on!**



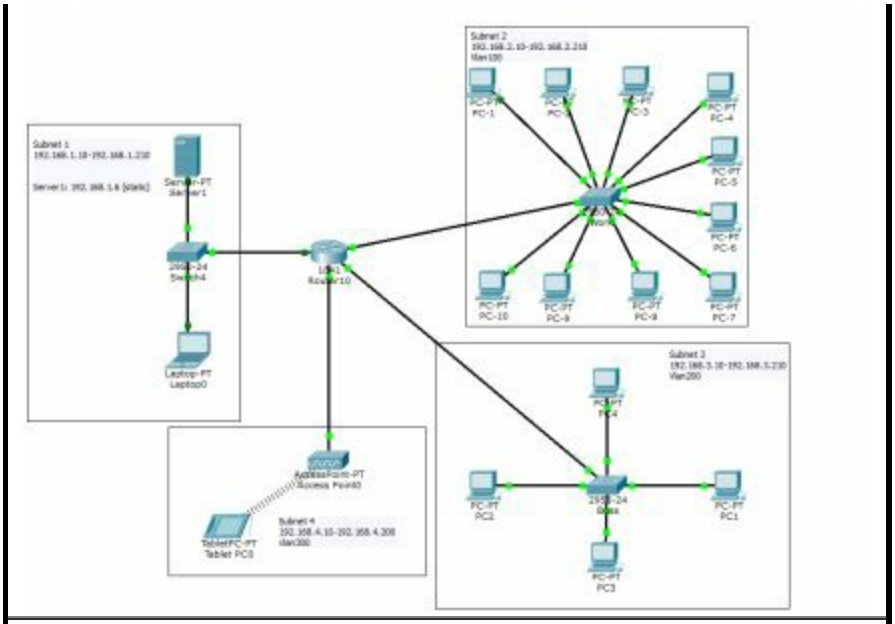
Step 32: Add the network to the DHCP.



Step 33: Give the VLAN the ip address 192.168.4.1 with ip helper address 192.168.1.6.



Step 34: The tablet should get a ip address from the DHCP server.



Step 35: Now simply add more clients to your network.

Running Config

Over here is the running config of the router:

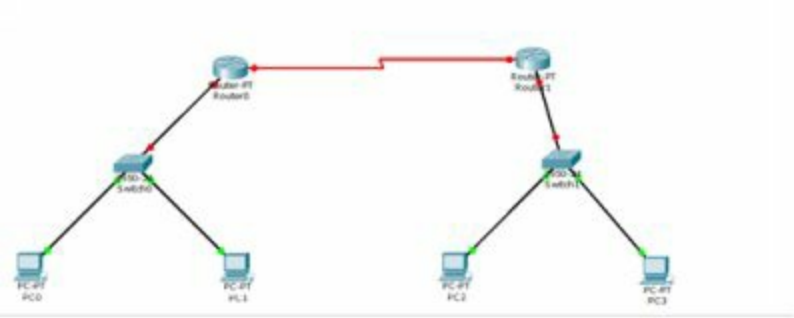
```
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
spanning-tree mode pvst
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
```

```
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/1/1
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/1/2
 switchport access vlan 200
 switchport mode access
!
interface FastEthernet0/1/3
 switchport access vlan 300
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan100
 ip address 192.168.2.1 255.255.255.0
 ip helper-address 192.168.1.6
!
interface Vlan200
 ip address 192.168.3.1 255.255.255.0
 ip helper-address 192.168.1.6
!
interface Vlan300
 ip address 192.168.4.1 255.255.255.0
 ip helper-address 192.168.1.6
!
```

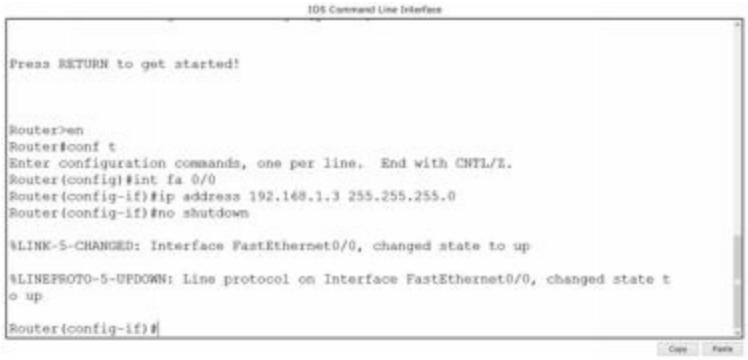
```
router rip
!
ip classless
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

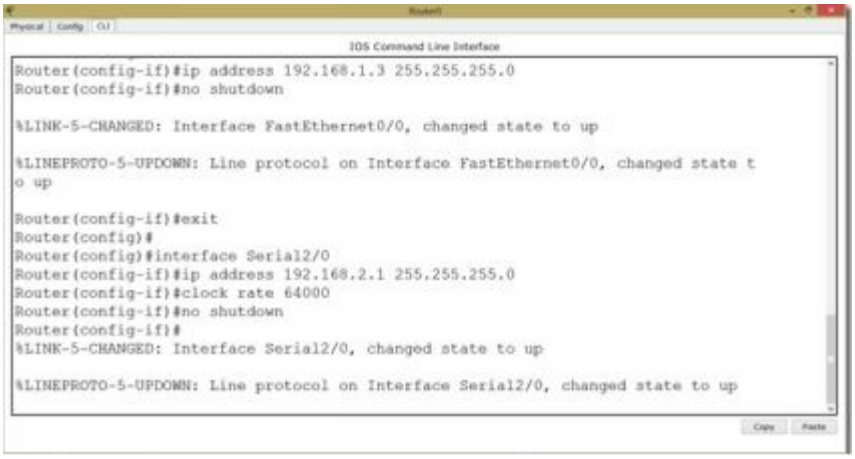
OSPF on packet tracer

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

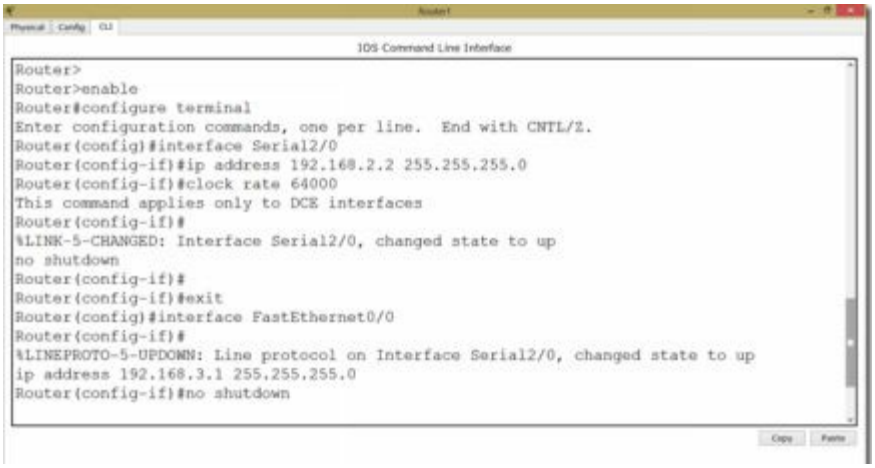


Now, let us apply the ospf on it. But before that, as usual, let us assign IP addresses and change the state of interfaces.

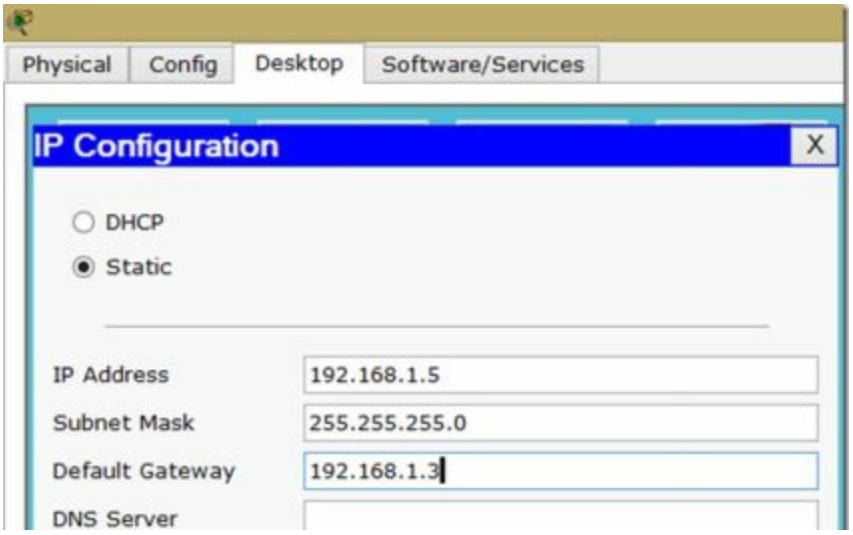


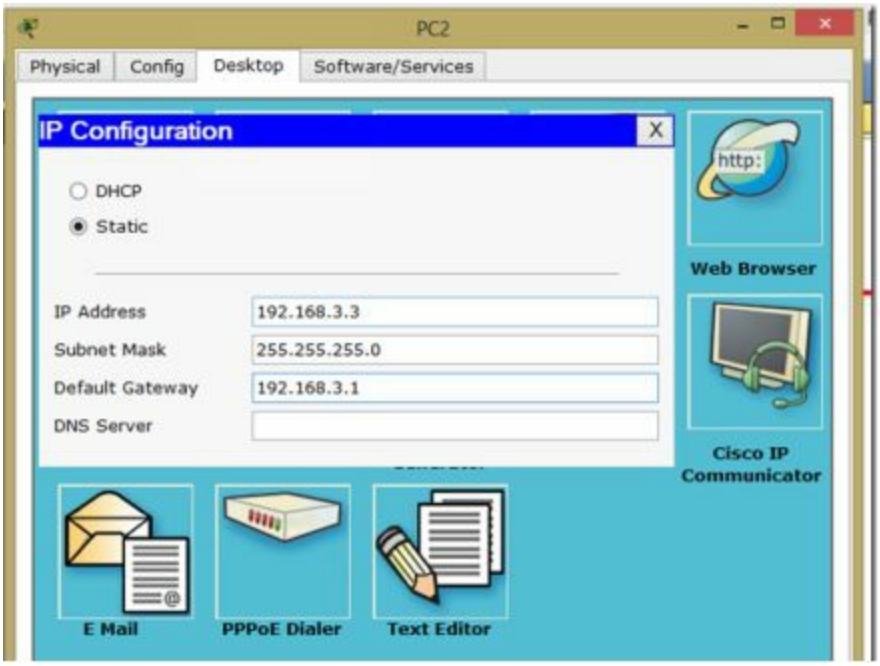


Similarly for the other router.

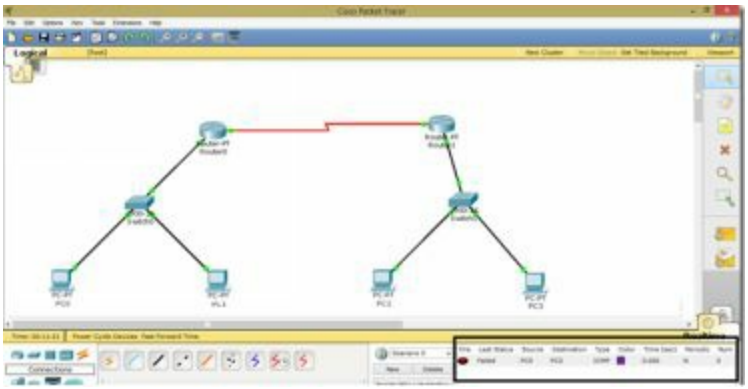


Assigning the IP addresses to PCs as follows.

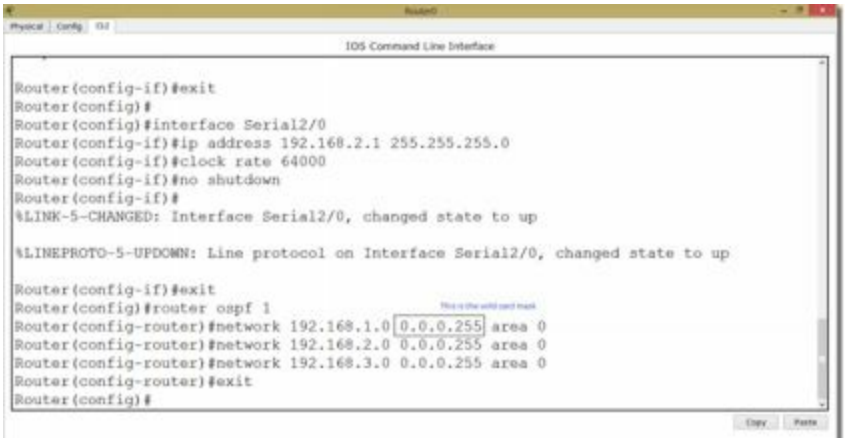




Now, as we can see, interfaces are up but the communication is not enabled because we have not applied the protocol yet.

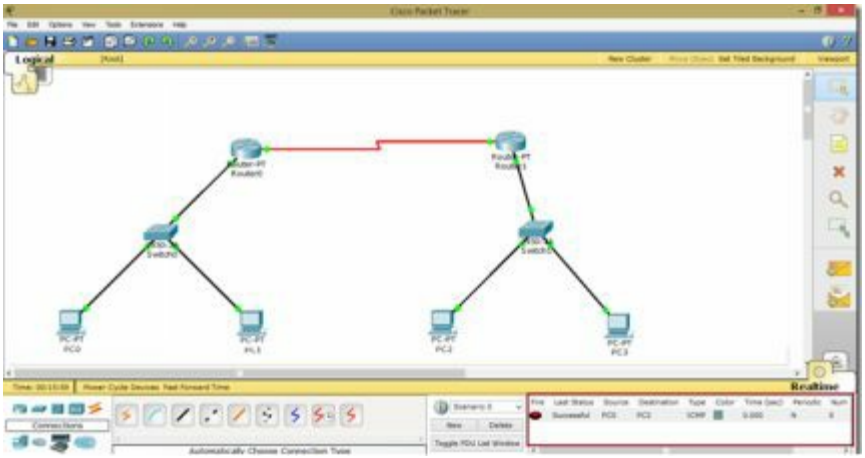


Lets do it.



On router 1.

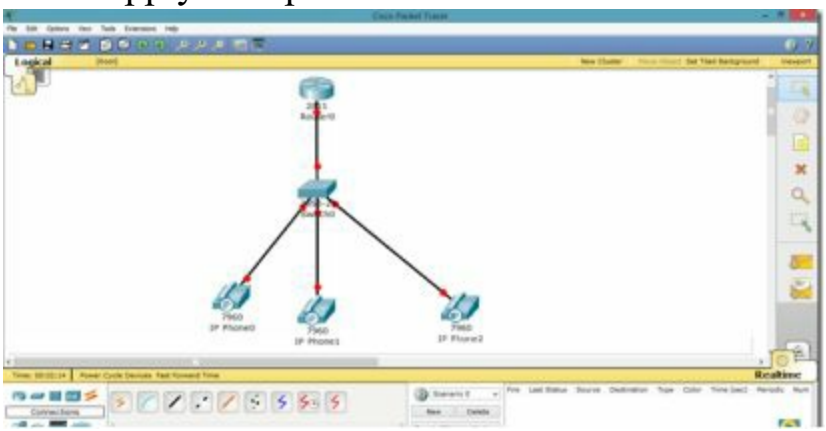
After applying protocol successfully , the traffic is flowing . Couple of things worth discussing
i. you will have to provide area id and process id on ospf protocol.
ii. you will have to provide wildcard mask on ospf.



VOICE OVER IP (VOIP) ON PACKET TRACER

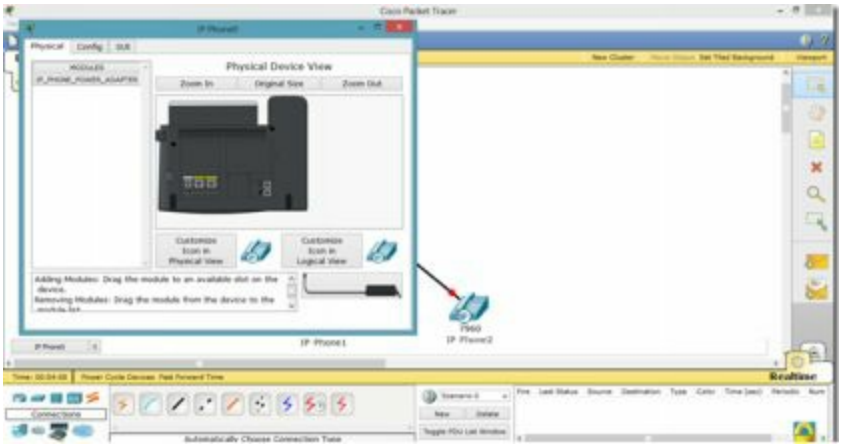
Voice over IP (VoIP, or voice over Internet Protocol) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet

Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony,Internet telephony, voice over broadband (VoBB), broadband telephony, IP communications, and broadband phone.
Internet telephony refers to communications services —voice, fax, SMS, and/or voice-messaging applications— that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP telephony and VoIP are used interchangeably, IP telephony refers to all use of IP protocols for voice communication by digital telephony systems, while VoIP is one technology used by IP telephony to transport phone calls
Let us apply it on packet tracer.



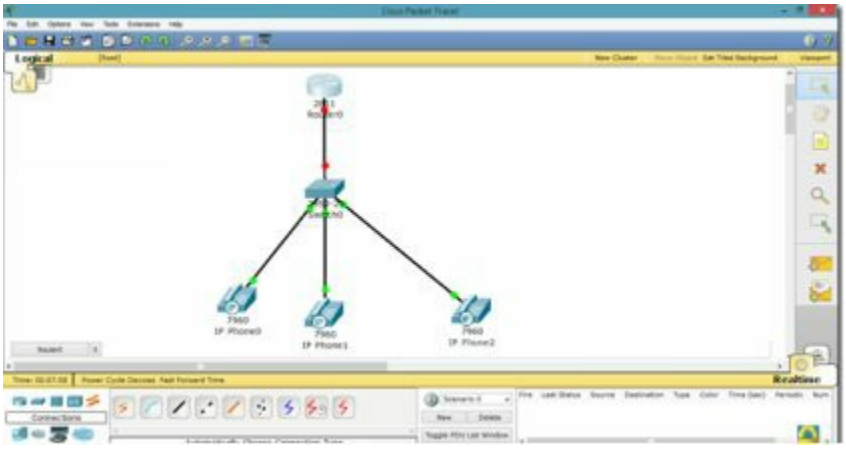
This IP Phone is displayed below. And when we try to go to any other mode its give us error and ask us to switch it on first.

For that, go to Physical mode and put the power adapter (in the bottom right corner) into the phone as shown in figure.



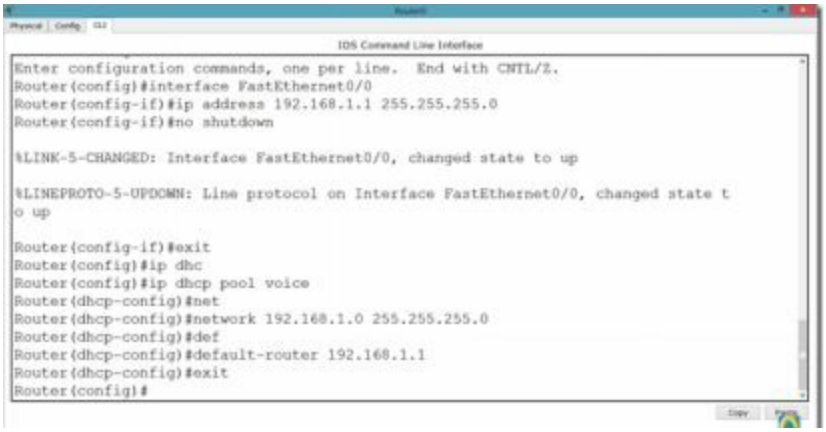
Now, we have inserted the antenna into IP phone. Repeat it for other phones as well.

Now, we see that interface of IP phone is UP.

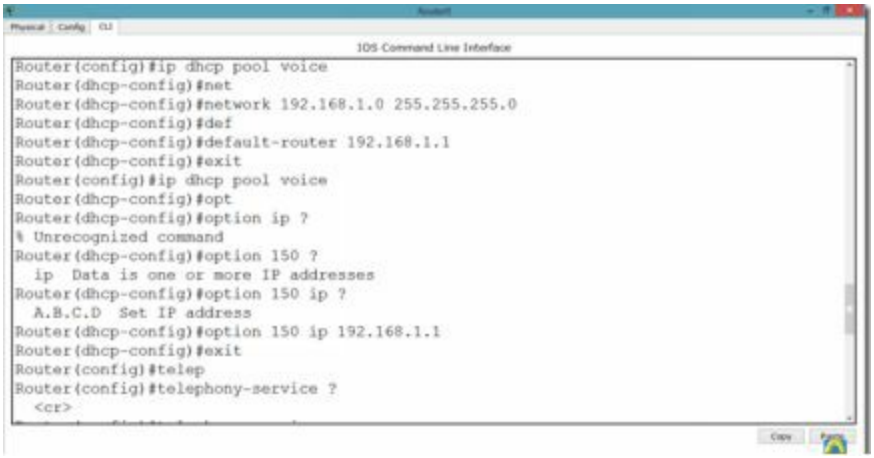


Now, go to router and assign IP address.

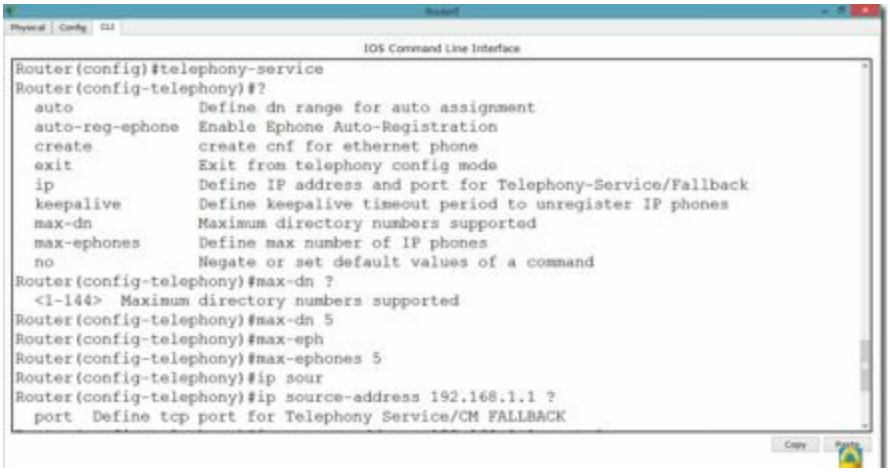
We will have to set DHCP server on router to assign IP addresses to IP phones.



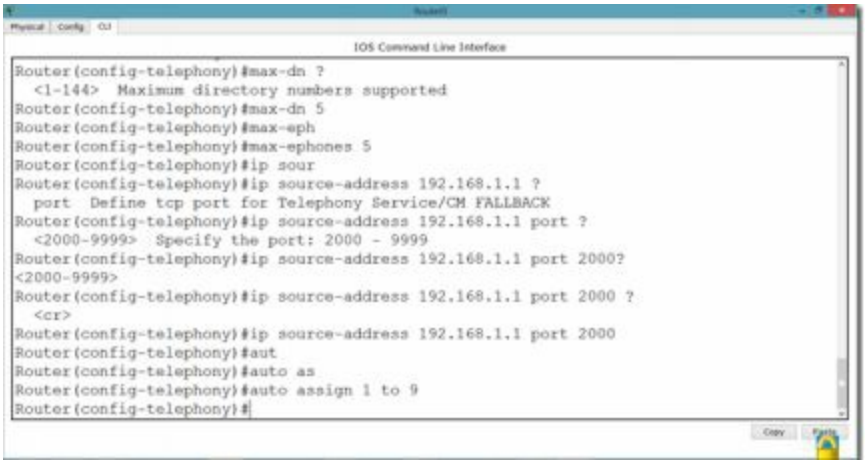
We will have to give an additional command for voip.
Router(dhcp-config)#option 150 ip 192.168.1.1



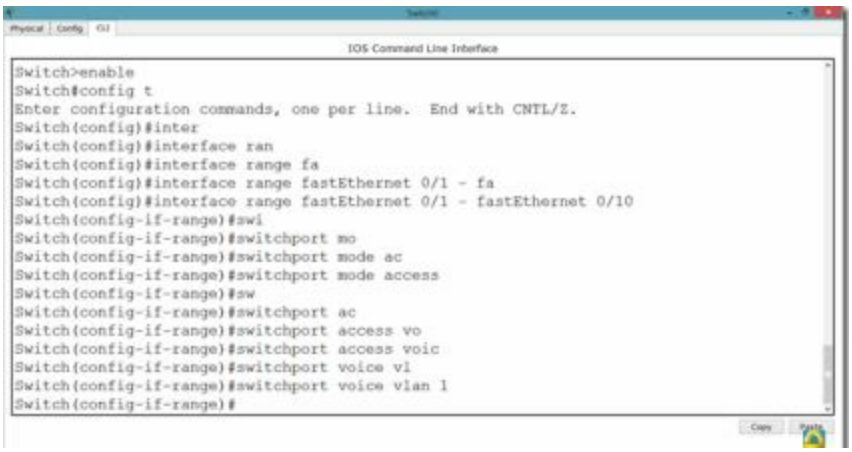
Now, let us apply commands to the router for voip. You might have noticed we took 2811 series router because it facilitates the following commands.



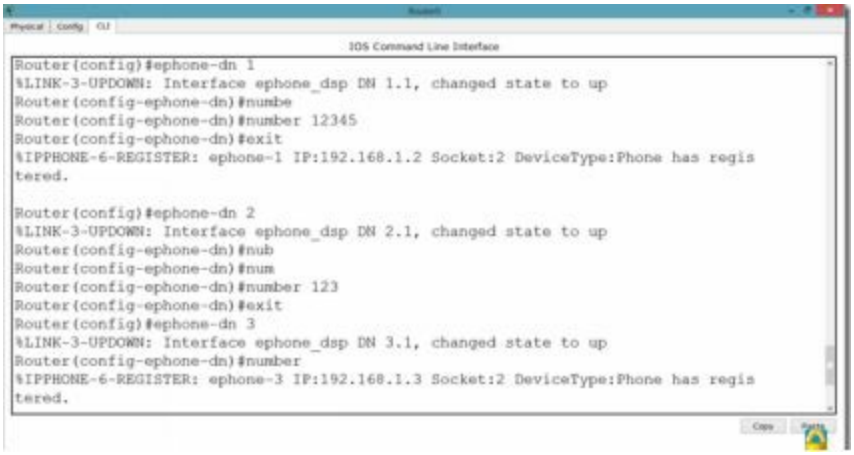
Continued.



Now, we will go to the switch and make the interfaces support voip as follows.



After that, we will have to assign phone number to our IP phone by applying following commands.



Continued…

Now, we can see that in GUI mode of Phone, we have a phone number available.

This means that we can call from one phone to the other. Lets do that.

And when we pick up the reciever, it says that we are connected :) .

Commands on Router for VOIP

Router(config)#ip dhcp pool voice

Router(dhcp-config)#option 150 ip 192.168.1.1
Router(dhcp-config)#exit

Router(config)#telephony-service

Router(config-telephony)#max-dn 5

Router(config-telephony)#max-ephones 5

Router(config-telephony)#ip source-address 192.168.1.1 port 2000

Router(config-telephony)#auto assign 1 to 9
Router(config-telephony)#exit

Router(config)#ephone-dn 1
%LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

Router(config-ephone-dn)#number 12345
Router(config-ephone-dn)#exit

%IPPHONE-6-REGISTER: ephone-1 IP:192.168.1.2 Socket:2 DeviceType:Phone has

registered.
Router(config)#ephone-dn 2

%LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up

Router(config-ephone-dn)#number 123
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 3
%LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up

Router(config-ephone-dn)#number 11111
Router(config-ephone-dn)#exit

Commands on Switch for VOIP
Switch(config)#interface range fastEthernet 0/1 - fastEthernet 0/10
Switch(config-if-range)#switchport mode access

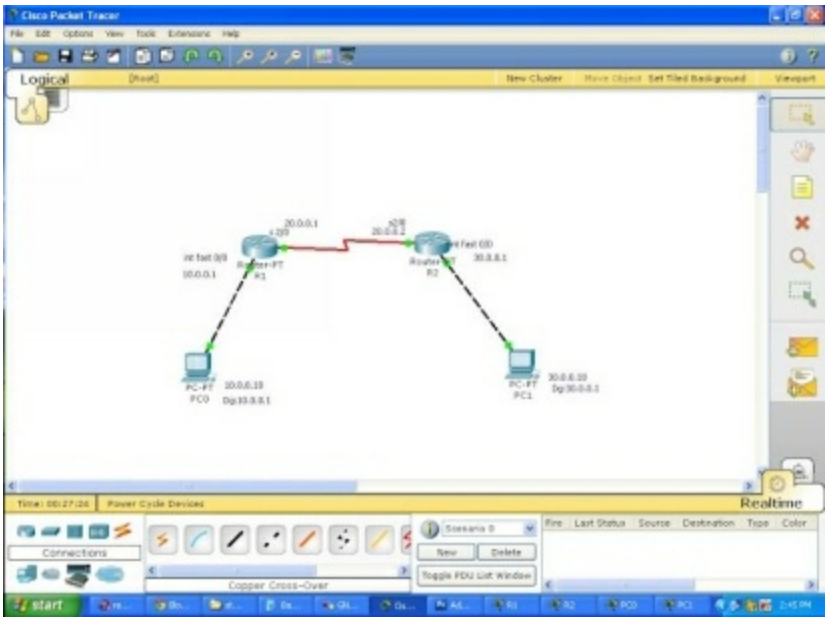
Switch(config-if-range)#switchport voice vlan 1

How to Configure a Simple Static Routing in Packet Tracer

How to configure a simple static routing in packet tracer using a simple topology with two routers
here we go

Steps:

Step 1:First Create a topology like this



you will get a red light first this is configured topology

Step 2: Configure ip address to routers go to global configuration mode in R1 and R2 configure connected interfaces

In Router 1

Interface Fastethernet0/0 in global configuration mode

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 10.0.0.1 255.0.0.0
```

```
R1(config-if)#no shutdown
R1(config-if)#exit
```

Interface Serial 2/0

```
R1(config)#interface serial 2/0
R1(config-if)#ip address 20.0.0.1 255.0.0.0
R1(config-if)#clock rate 64000
R1(config-if)#encapsulation ppp
R1(config-if)#no shutdown
R1(config-if)#exit
```

In Router 2

Interface Fastethernet 0/0

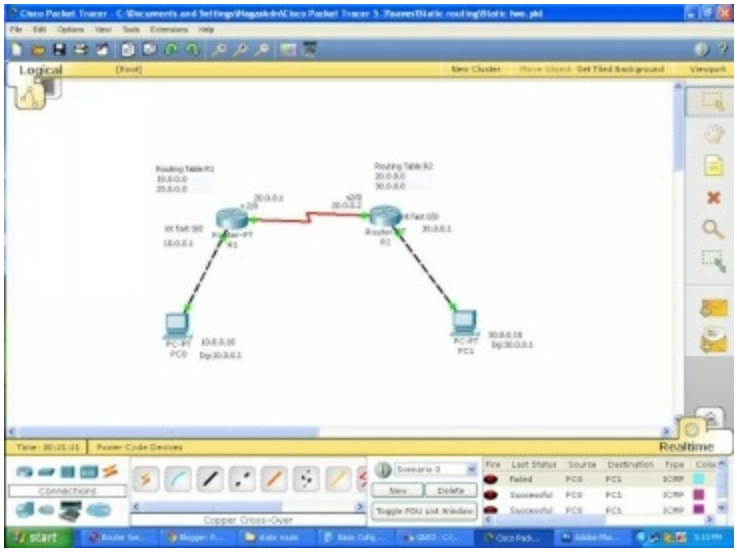
```
R2(config)#interface fastethernet 0/0
R2(config-if)#ip address 30.0.0.1 255.0.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

Interface Serial 2/0

```
R2(config)#interface serial 2/0
R2(config-if)#ip address 20.0.0.2 255.0.0.0
R2(config-if)#encapsulation ppp
R2(config-if)#no shutdown
R2(config-if)#exit
```

Step 3 : Assign ip address for both Pc's with appropriate ip and subnetmask and default gateway How ?

Step 4: Now configure both router with static route



By default, Routers Know only directed connected networks here Router 1 know only 10.0.0.0 and 20.0.0.0 it doesn't know the 30.0.0.0 like this R2 doesn't know about 10.0.0.0.So We are going to add Static route to this both router

R1(config)#ip route Destination Network| Destination N/W SubnetMask |Next Hop Address

In Router R1,Just give this command,In this case Destination is 30.0.0.0 and its subnet mask is 255.0.0.0 next hop address is 20.0.0.2

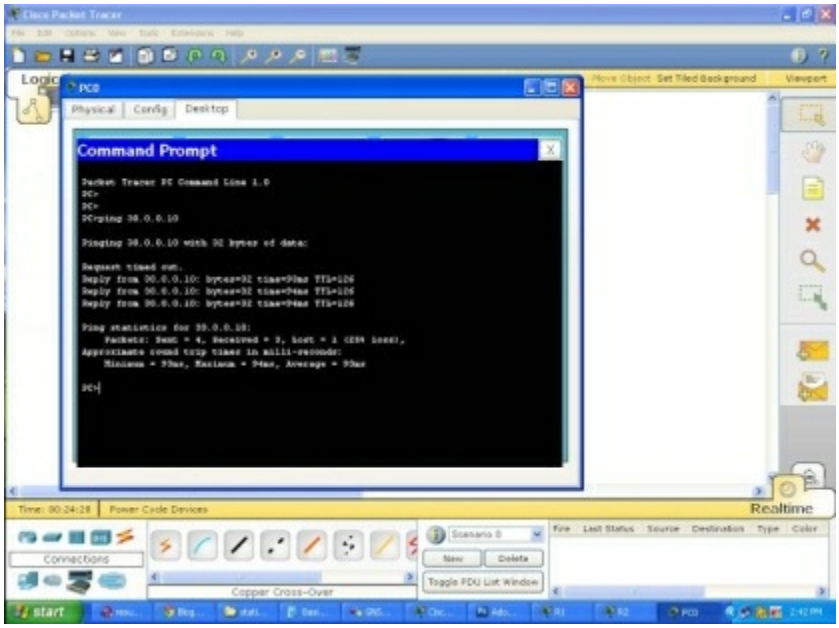
R1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2

In Router R2

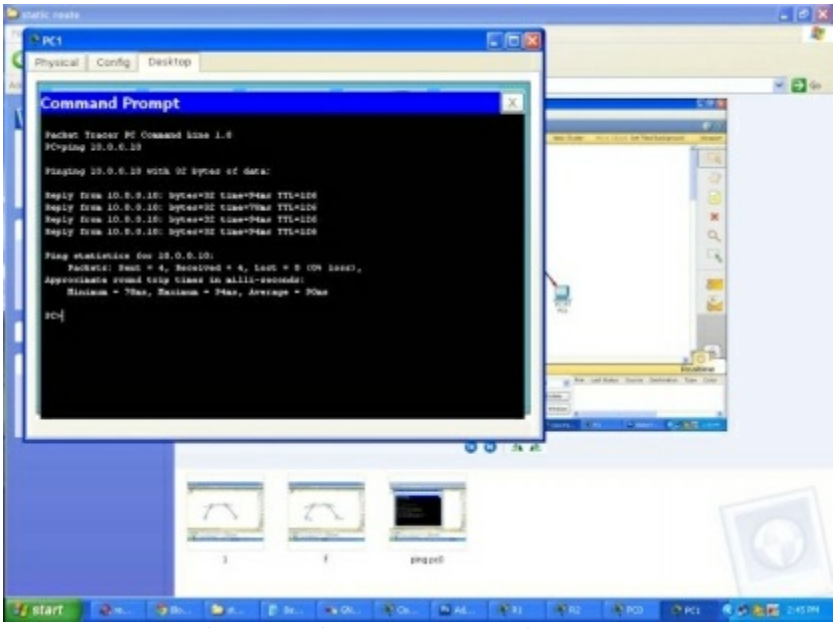
R2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1

Thats it!!..Now both routers know all networks,check by ping ip address of host

Step 5:Double click PC move to desktop then command prompt give the command ping 30.0.0.10 in PC 0 you will get reply from 30.0.0.10 like this



From PC1



Telnet and SSH on packet tracer

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers. To telnet means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface.

SSH

Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client (running SSH server and SSH client programs, respectively). It was designed as a replacement for Telnet and other insecure remote shell protocols such as the Berkeley rsh and rexec protocols, which send information, notably passwords, in plaintext, rendering them susceptible to interception and disclosure using packet analysis. The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet.

a network protocol that ensures a high-level encryption, allowing for the data transmitted over insecure networks, such as the Internet, to be kept intact and integrate. SSH and SSH Telnet, in particular, work for establishing a secure communication between two network-connected computers as an alternative to remote shells, such as TELNET, that send sensitive information in an insecure environment.

In contrast to other remote access protocols, such as FTP, SSH Telnet ensures higher level of connection security between distant machines but at the same time represents a potential threat to the server stability. Thus, SSH access is considered a special privilege by hosting providers and is often assigned to users only per request.

Let us apply Telnet and SSH on packet tracer.

1
Take the topology as in the above diagram. Set IPs on the PCs. As, by default, all PCs are in vlan 1. We will create a virtual interface on switch with vlan 1 as follows.

2

Now, we can ping to switch by our hosts because hosts are in vlan 1 and switch also has a vlan 1 interface.
3

Now, try to telnet the switch from our PC, it refuses because we have not applied authentication on the switch yet.
4
So, lets apply line authentication on the switch. The system supports 20 virtual tty (vty) lines for Telnet, Secure Shell Server (SSH) and FTP services. Each Telnet, SSH, or FTP session requires one vty line. You can add security to your system by configuring the software to validate login requests.

4.5
Now, we can easily telnet. But it does not let us go in the switch enabled mode because we have not set the password on the switch yet.

5

Lets apply password on the switch enabled mode.

6
Now, we can go inside Switch configuration mode from our pc.

7

So, now let us apply SSH on the switch.

9

Commands continued.

11

Now, we try to telnet it but it is refused because ssh has over ruled telnet. So, we will use SSH protocol on it. By default username is admin.

12

And we can apply any sort of configuration on our switch from out pc.

13

Now, if we want to change the username from admin to something else, we will do it as follows.

14

and from our pc as follows.

15

The SSH commands are as follows.

Switch(config)#ip domain name ?

WORD Default domain nameSwitch(config)#ip domain name
abc.comSwitch(config)#crypto key generate rsa
% Please define a hostname other than Switch.

Switch(config)#hostname s1

s1(config)#ip domain name cs-studys1

s1(config)#crypto key generate rsa

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

s1(config)#line vty 0 15

s1(config-line)#transport input ssh

The name for the keys will be: s1.cs-study
How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

s1(config)#ip ssh version 2

s1(config-line)#

Challenge Hand Shake Authentication Protocol on Packet Tracer (CHAP)

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).

CHAP

CHAP provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. The MS-CHAP variant does not require either peer to know the plaintext, but has been broken. Thus, CHAP provides better security as compared to Password Authentication Protocol (PAP).

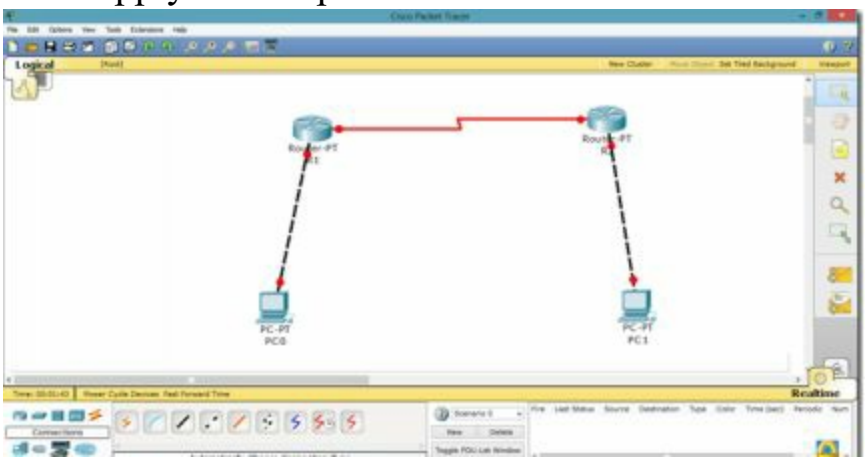
CHAP Working

CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).

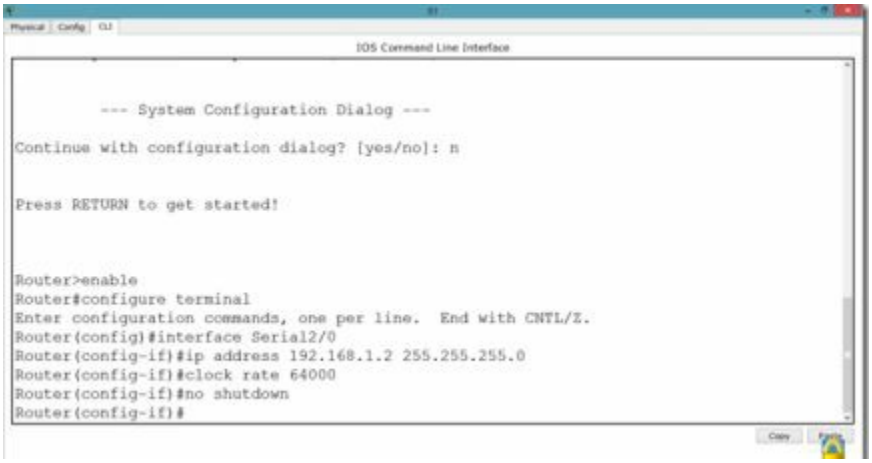
1. After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
2. The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
4. At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.

   Another feature of CHAP is that it doesn't only require the client to authenticate itself at startup time, but sends challenges at regular intervals to make sure the client hasn't been replaced by an intruder, for instance by just switching phone lines.

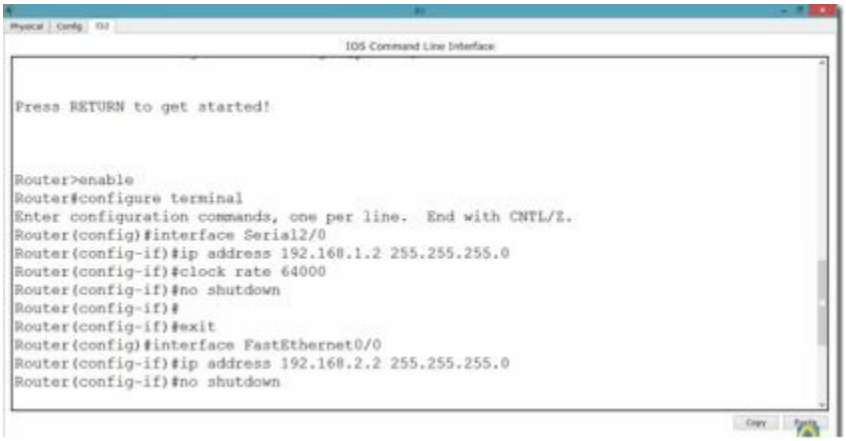
Let us apply PPP on packet tracer. Consider the following simpler topology.



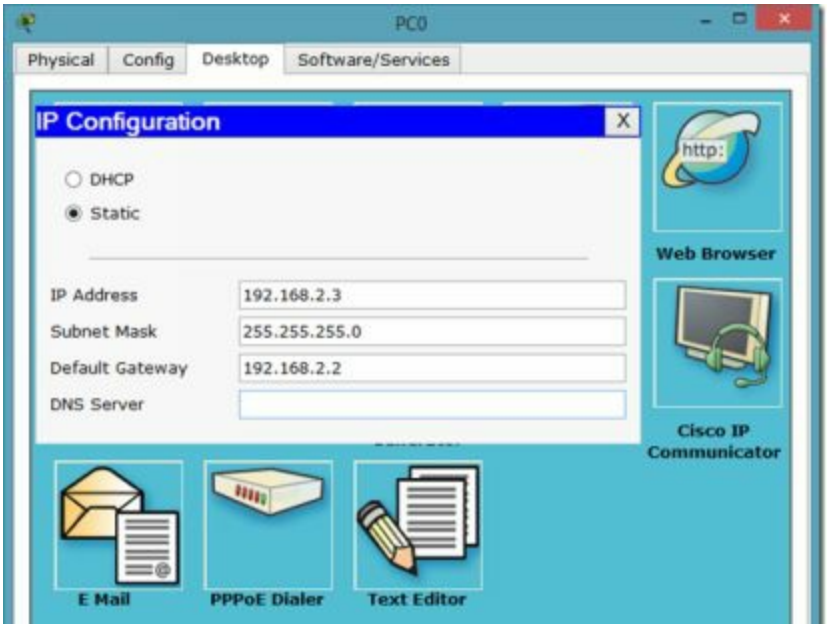
Let us apply IP addresses on the interfaces and change the state of the interface from down to UP. So that they can communicate.



Similarly, for serial interface.

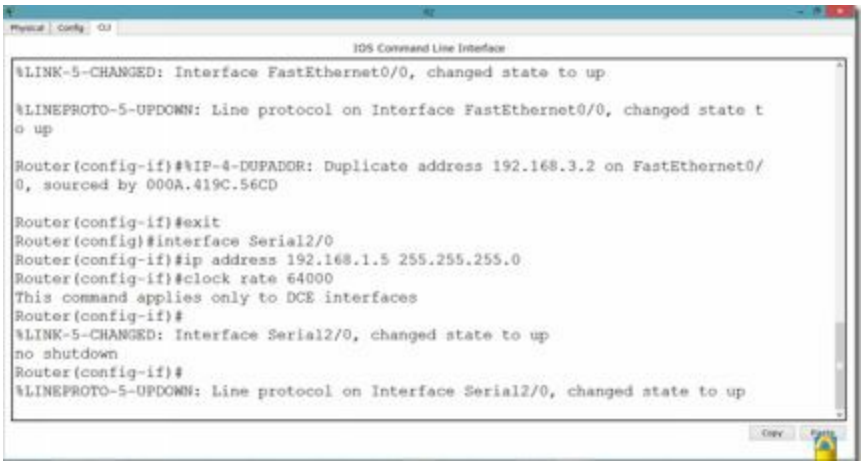


And IP configuration on PC.



The IP configuration on other router.

Serial Interface setting.

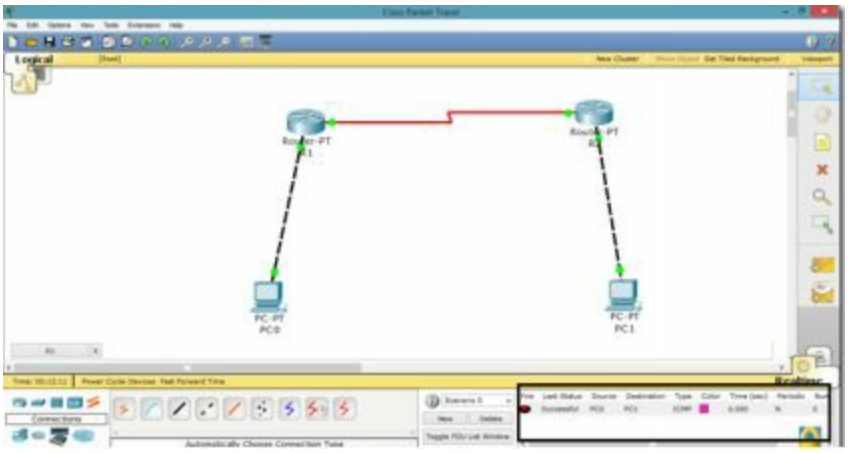


Now, we know that PCs that are attached cannot communicate until we apply a routing mechanism. In this case we are applying the RIP V2 protocol. Apply the following set of

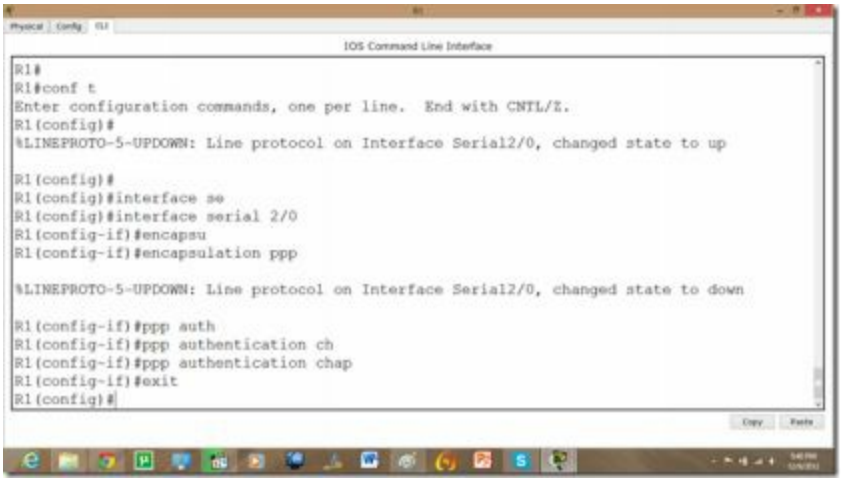
commands on both routers. We have also set the hostname of the router which will be useful to us later.

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

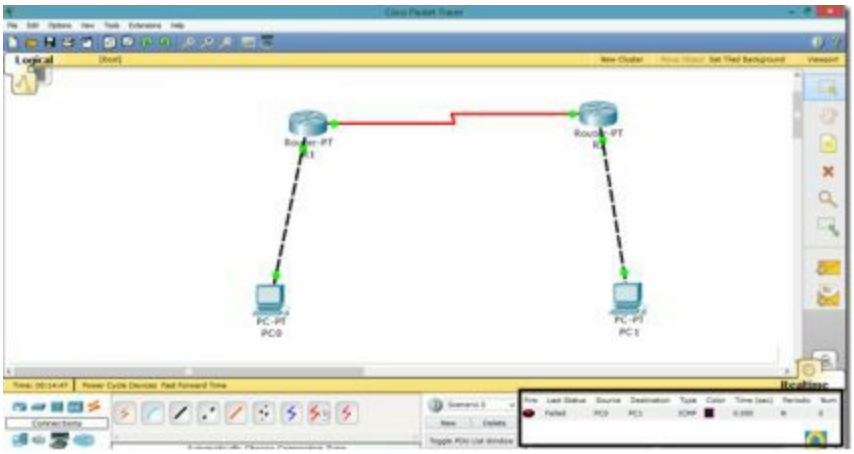
Now, both PCs can communicate.



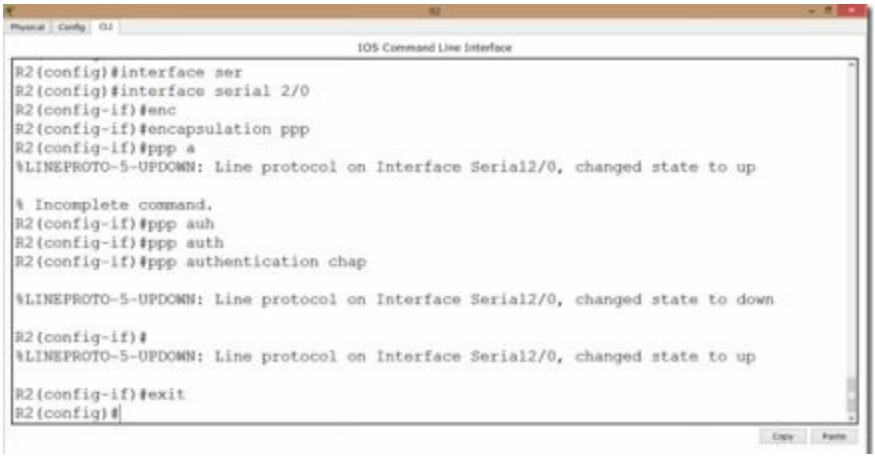
Now, we will set the authentication, In this tutorial we are going to apply CHAP(Challenge Handshake Authentication Protocol).



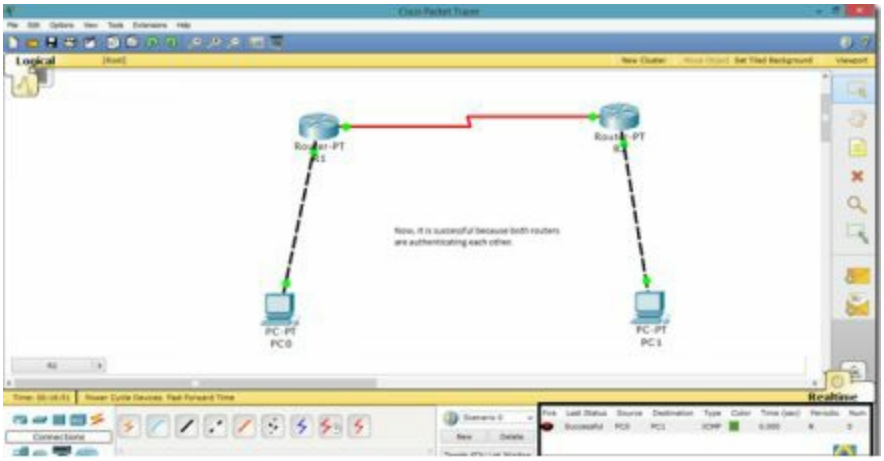
As we set the authentication on one router the communication is disabled.



Let us set it on other router as well.



Now, the communication is enabled.


Logical
Router-PT
Router-PT
Now, it is successful because both routers are authenticating each other.
PC-PT
PC0
PC-PT
PC1
Realtime

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.

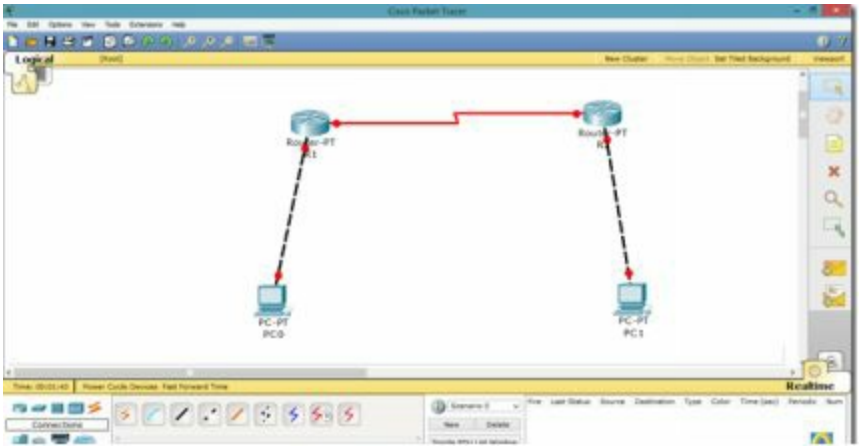
PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure. It is used as a last resort when the remote server does not support a stronger authentication protocol, like CHAP or EAP (the latter is actually a framework).

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

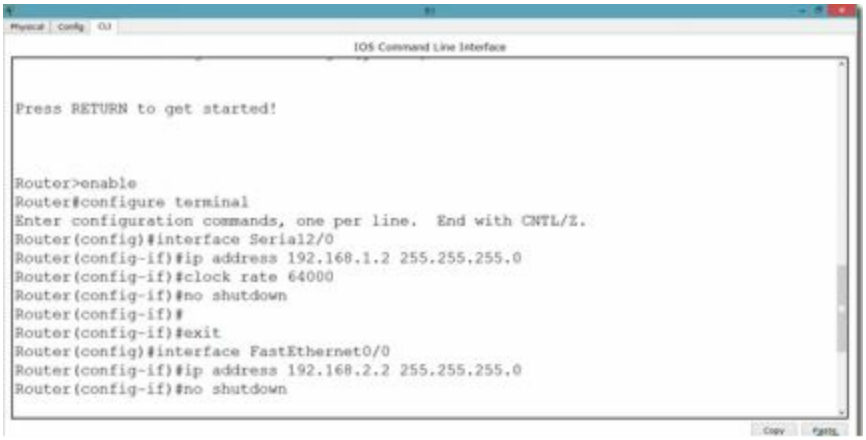
authenticates itself by sending a user name and an (optionally encrypted) password to the server, which the server compares to its secrets database. This technique is vulnerable to eavesdroppers who may try to obtain the password by listening in on the serial line, and to repeated trial and error attacks.

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



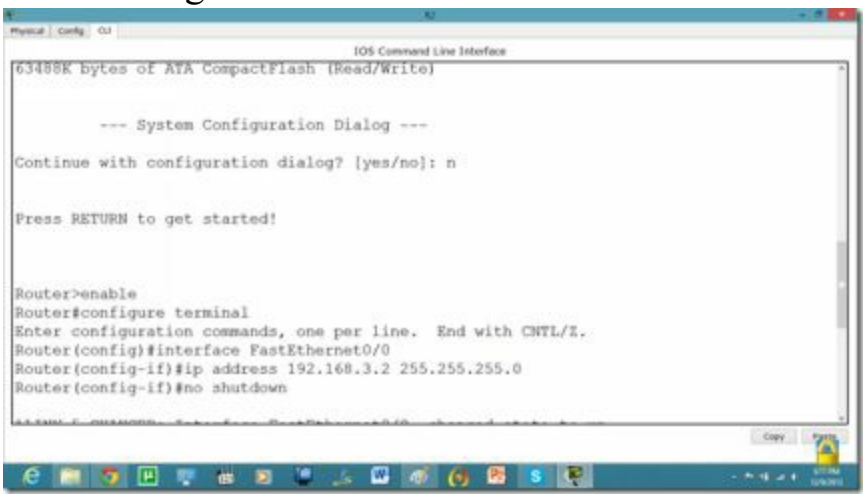
Let us apply IP addresses on the interfaces and change the state of the interface from down to UP. So that they can communicate.

Similarly, for serial interface.

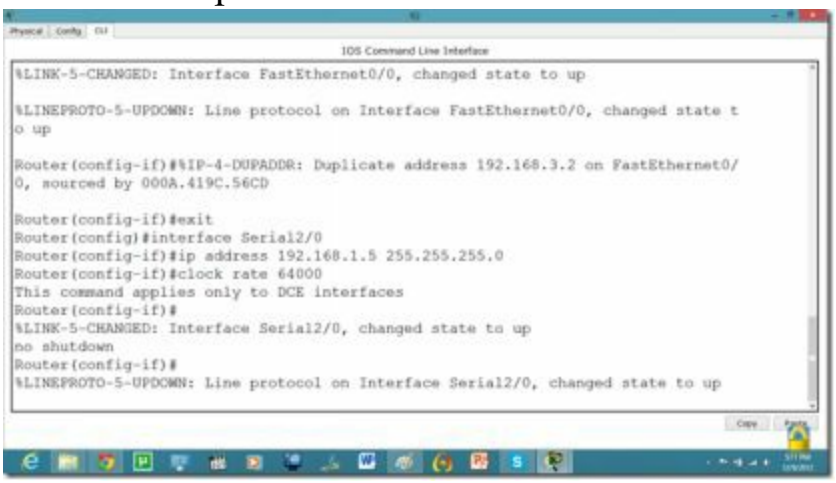


PC IP setup

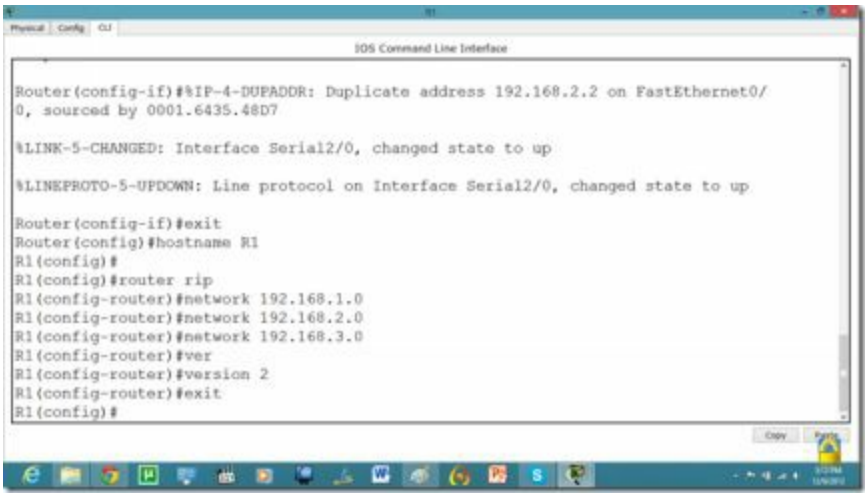
The IP configuration on other router.



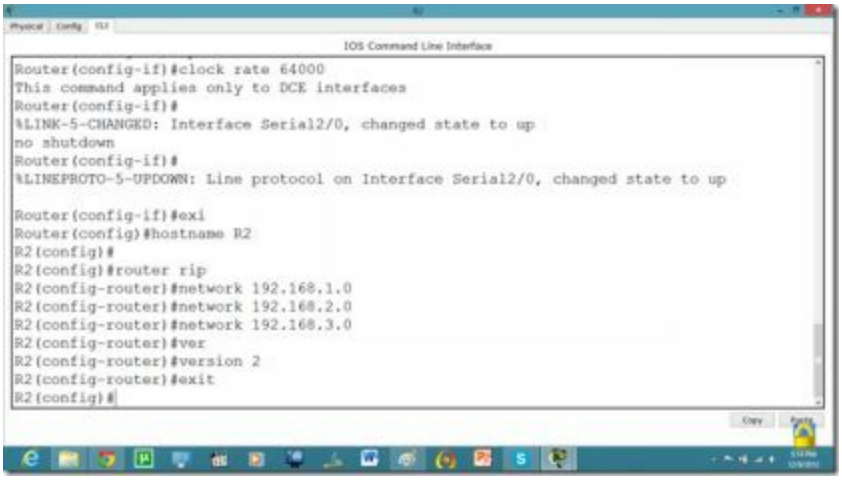
serial int setup.



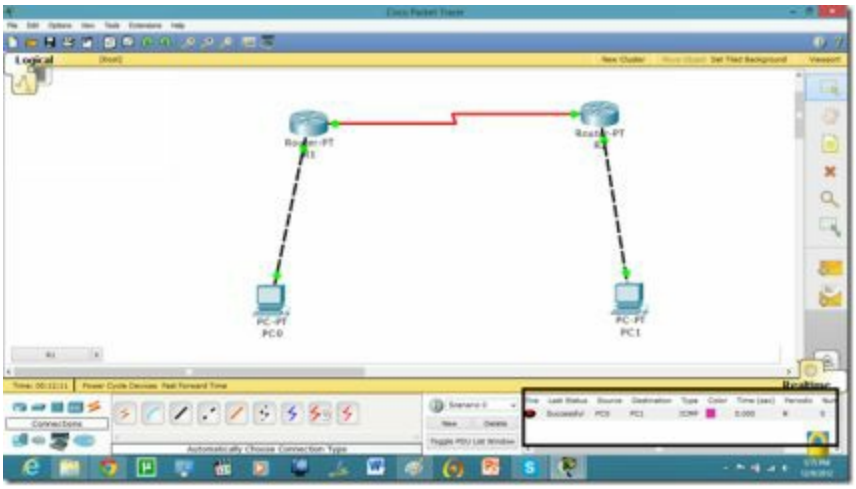
Now, we know that PCs that are attached cannot communicate until we apply a routing mechanism. In this case we are applying the RIP V2 protocol. Apply the following set of commands on both routers. We have also set the hostname of the router which will be useful to us later.



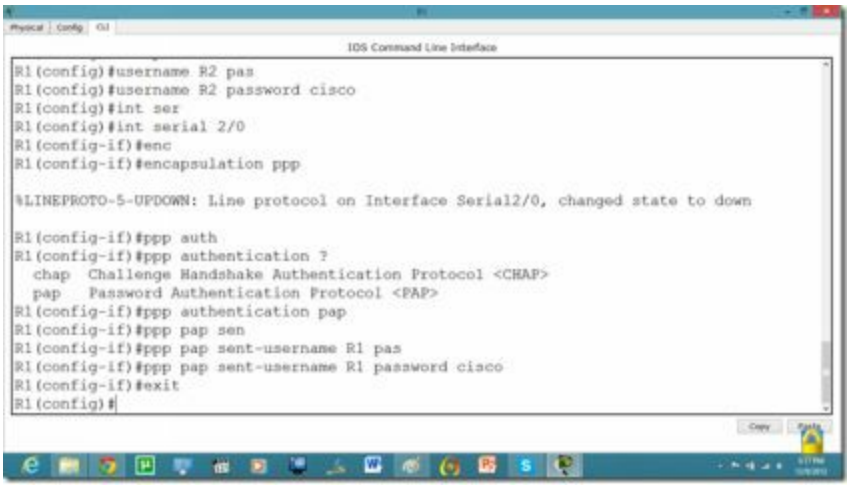
Now, let us set the commands on the second router as well.



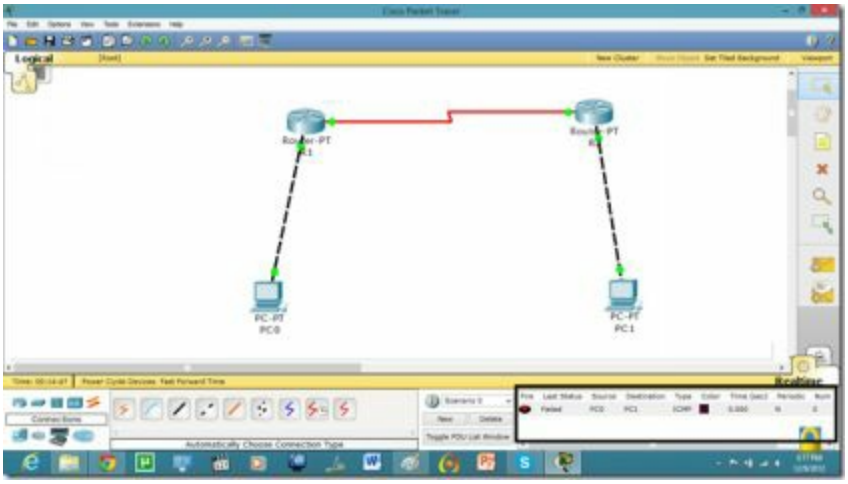
Now, both PCs can communicate.



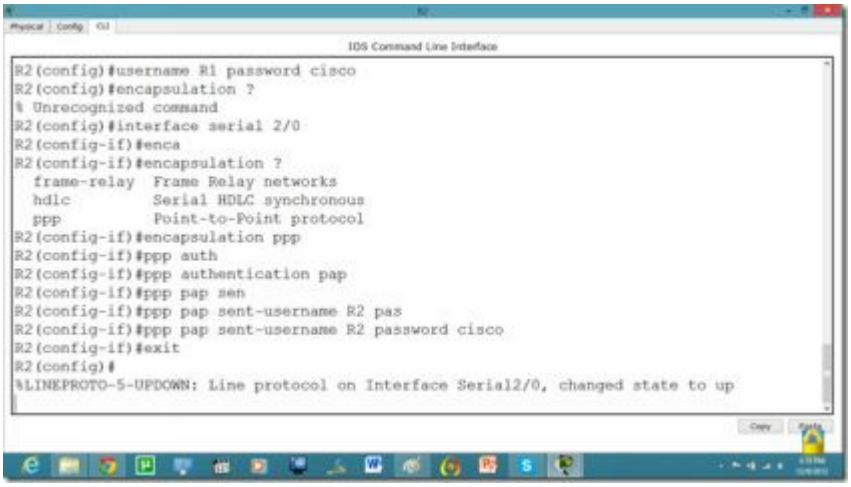
Now, we will set the authentication, In this tutorial we are going to apply PAP.



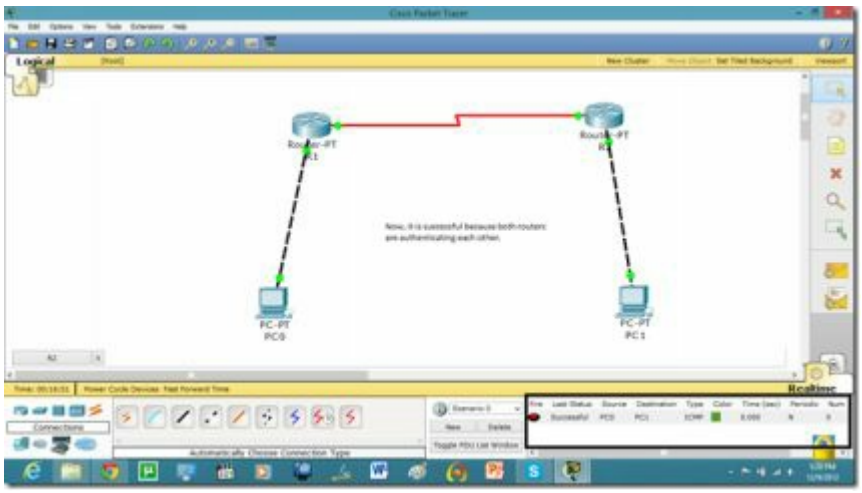
As we set the authentication on one router the communication is disabled.



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 authentication enabled in router.


Physical
Config
CLI
IOS Command Line Interface
!
!
interface FastEthernet0/0
ip address 192.168.2.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial2/0
ip address 192.168.1.2 255.255.255.0
encapsulation ppp
ppp authentication pap
ppp pap sent-username R1 password 0 cisco
clock rate 64000
Copy
Paste