Project report on CCNA Course

Submittted by kodakandla srikar
Sri chandrasekhendra Saraswathi viswa maha Vidyalaya (SCSVMV)
Email:kodakandlasrikar99@gmail.com
Mobile number:9176462946

Project 1

Configuring Application Layer Services of the OSI Model

The application layer is a layer in the Open Systems Interconnection (OSI) seven-layer model and in the TCP/IP protocol suite. It consists of protocols that focus on process-to-process communication across an IP network and provides a firm communication interface and end-user services.

The application layer is the seventh layer of the OSI model and the only one that directly interacts with the end user.

The application layer provides many services, including:

- Simple Mail Transfer Protocol
- File transfer
- Web surfing
- Web chat
- Email clients
- Network data sharing
- Virtual terminals
- Various file and data operations

The application layer provides full end-user access to a variety of shared network services for efficient OSI model data flow. This layer has many responsibilities, including error handling and recovery, data flow over a network and full network flow. It is also used to develop network-based applications.

More than 15 protocols are used in the application layer, including File Transfer Protocol, Telnet, Trivial File Transfer Protocol and Simple Network Management Protocol.

Its major network device or component is the gateway.

We always remember the name of a website, not their IP address because IP addresses are very hard to remember. It’s more or less like not remembering the mobile number of a person instead saving that number by a name.

The domain name service protocol working at the application layer translates the domain names IP addresses for us

Hypertext Transfer Protocol (HTTP):

HTTP protocol defines how messages are formatted and transmitted over the internet. HTTP has different status codes that tell what actions needs to be taken by the web servers and browsers in response to various commands.

For example, HTTP 404 is used when the resource in not found.

Simple Mail Transfer Protocol (SMTP)

SMTP stands for Simple Mail Transfer Protocol. This protocol is used in delivering an email from an email client, such as Outlook Express, to an email server or when email is delivered from one email server to another. SMTP uses port 25.

Telnet

Telnet protocol is used to login to a remote server and it provides a bidirectional interactive text-oriented communication facility using a virtual terminal connection.

Telnet is one of the best examples of the client-server protocol. This protocol is based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23, where a Telnet server application (telnetd) is listening. Telnet, however, predates TCP/IP and was originally run over Network Control Program (NCP) protocols.

Simple Network Management Protocol (SNMP)

A network admin uses many devices to run a network. Simple Network Management Protocol (SNMP) is an Internet-standard protocol for network management. SNMP is used by network admins mostly for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include most of the networking devices such as routers, switches, servers, workstations, printers, modem racks and more.

BOOTP

When a network device or a computer is powered up the first thing it does is the booting up its operating system. BOOTP protocol is used for the same for the devices connected over to a network. When a computer that is connected to a network is powered up, the system software broadcasts BOOTP messages onto the network to request an IP address assignment and it also notifies other devices that a particular device has woken up. A BOOTP configuration server assigns an IP address based on the request from a pool of addresses configured by an administrator.

Some of the famous protocols which run on the Application layer are:

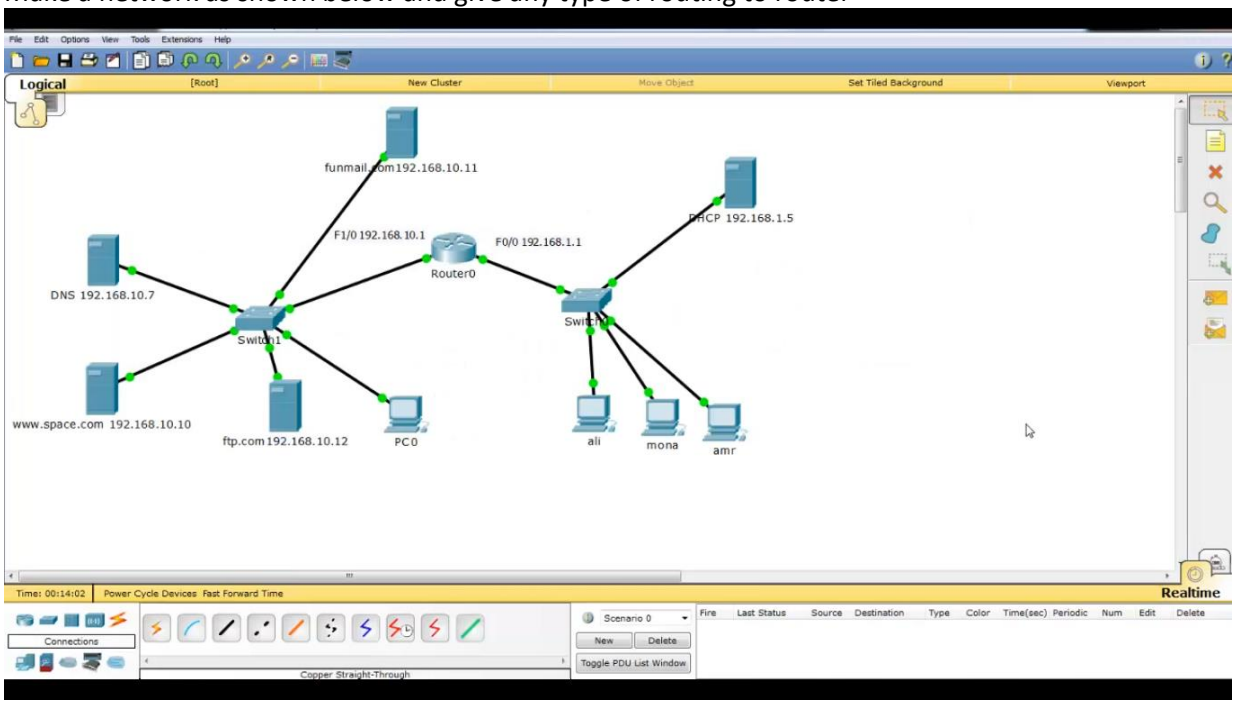
- BitCoin
- BitTorrent
- Finger
- FreeNet
- Gopher
- HTTP
- Telnet

- SNMP
- SMTP
- MIME
- NFS
- SIP
- SDP
- XMPP etc.

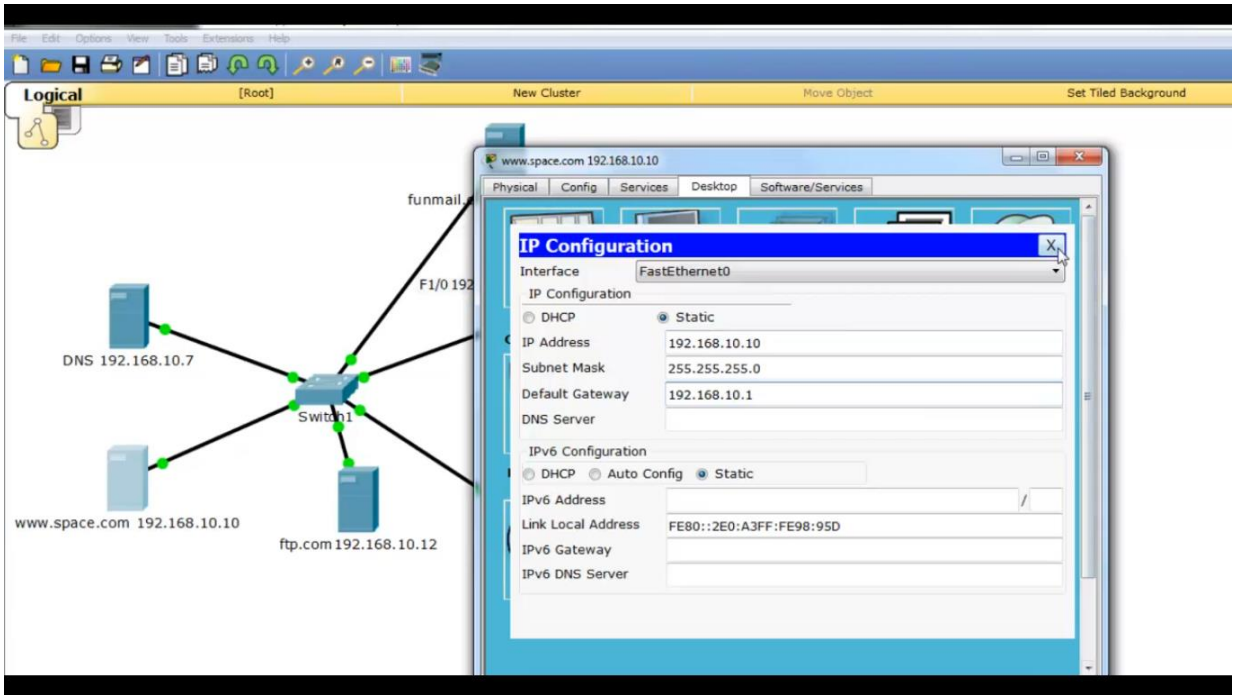
  Software used: Cisco packet tracer

  Procedure:

Make a network as shown below and give any type of routing to router

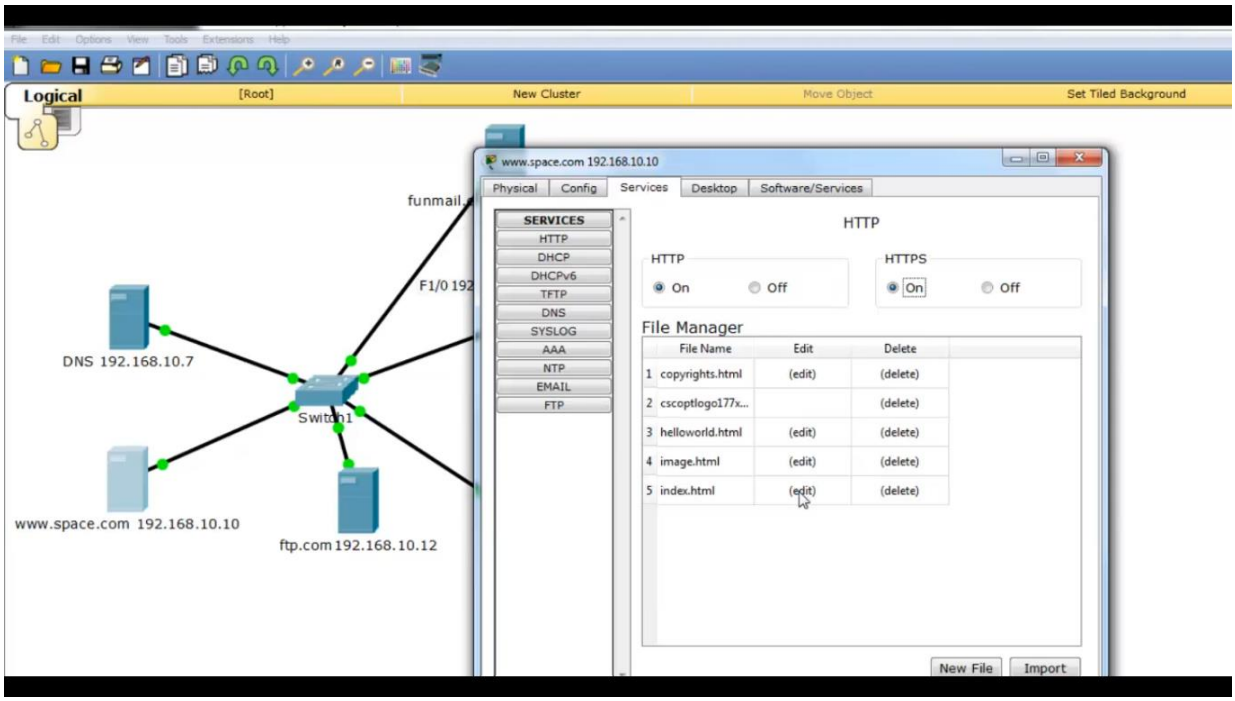


Now give ip addresses to server as shown below

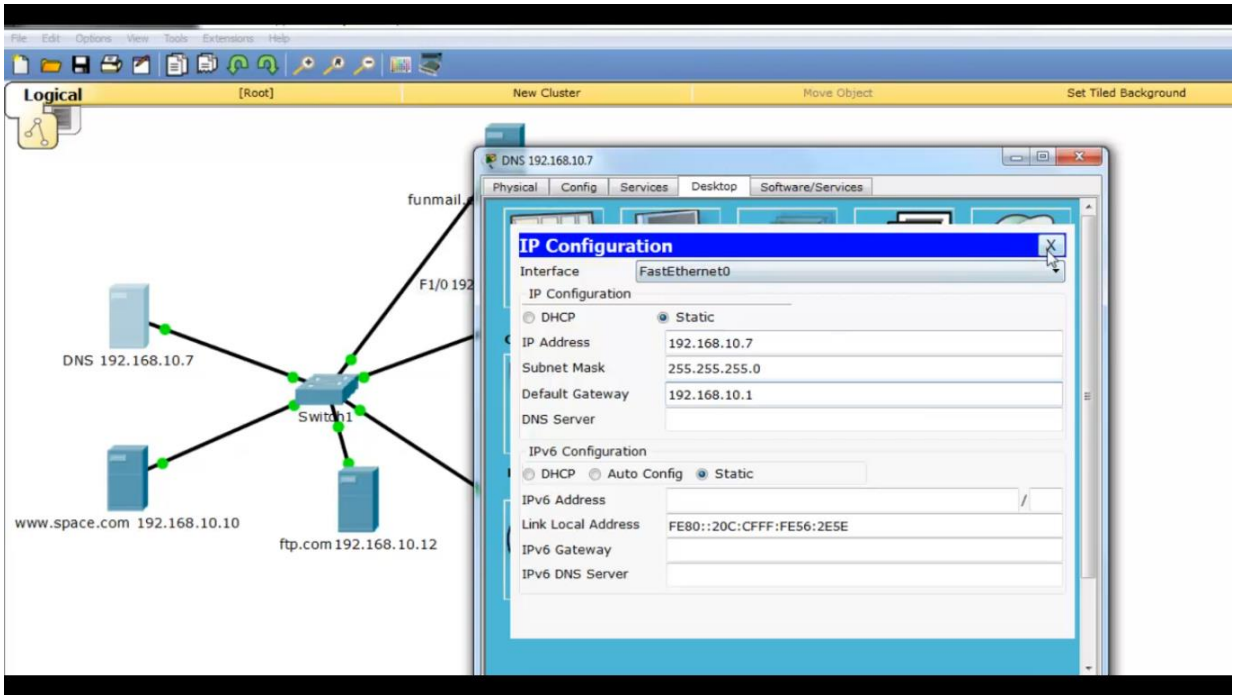


Now go to servers as shown below

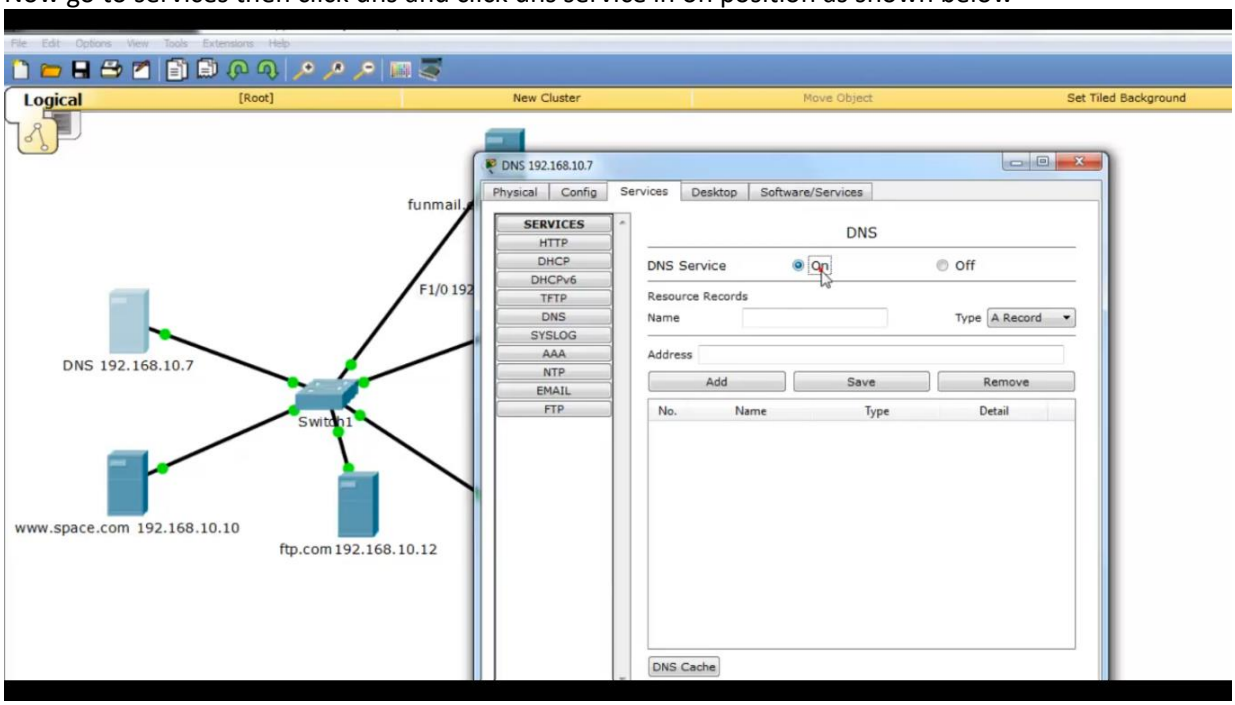
Now click on in http and https if you want them



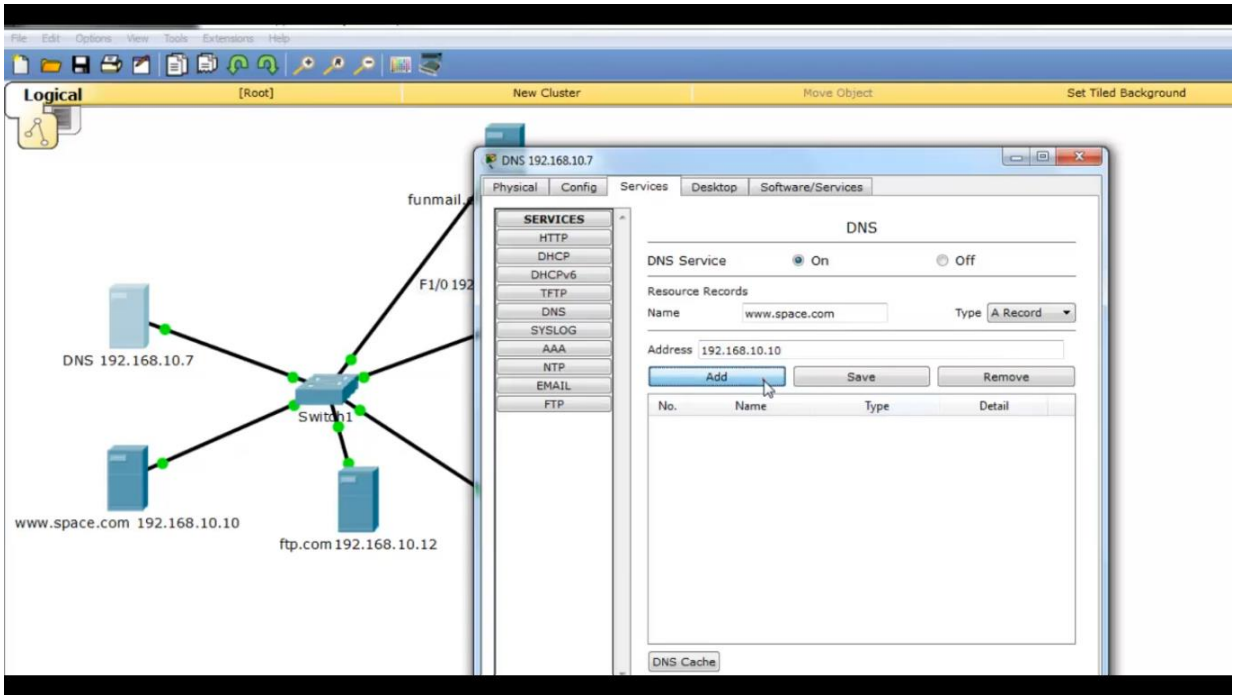
Now configure DNS server as shown below



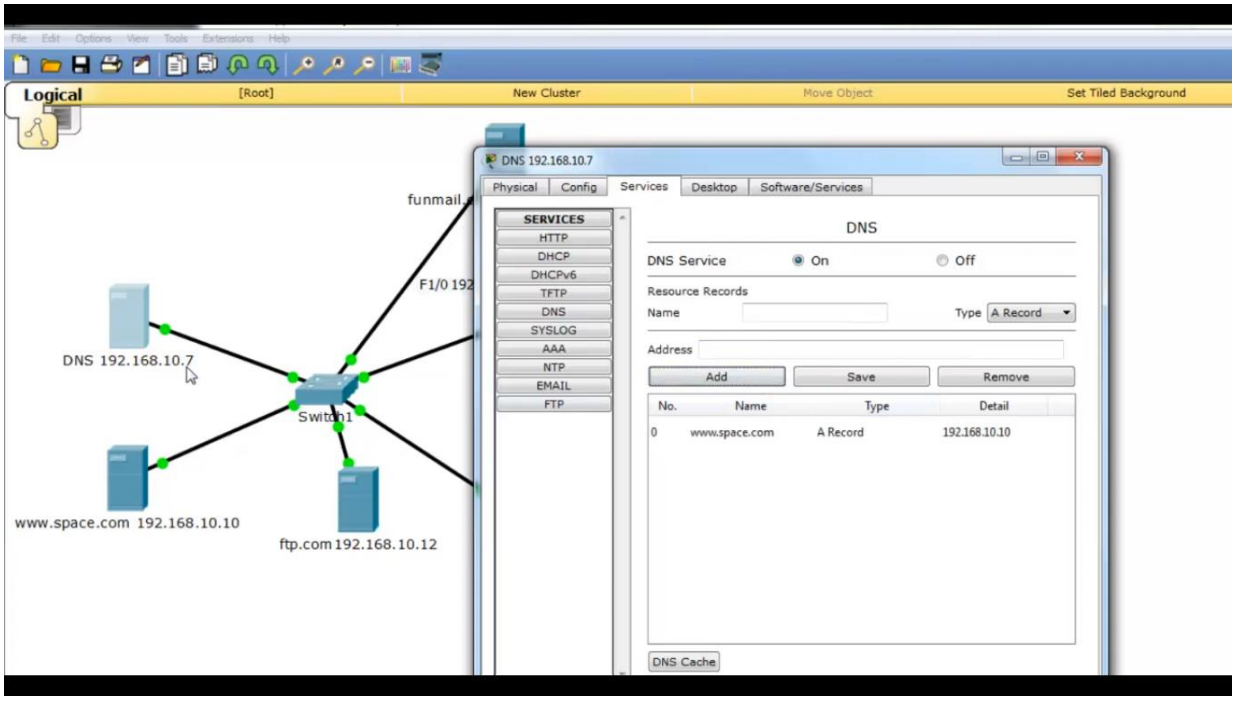
Now go to services then click dns and click dns service in on position as shown below



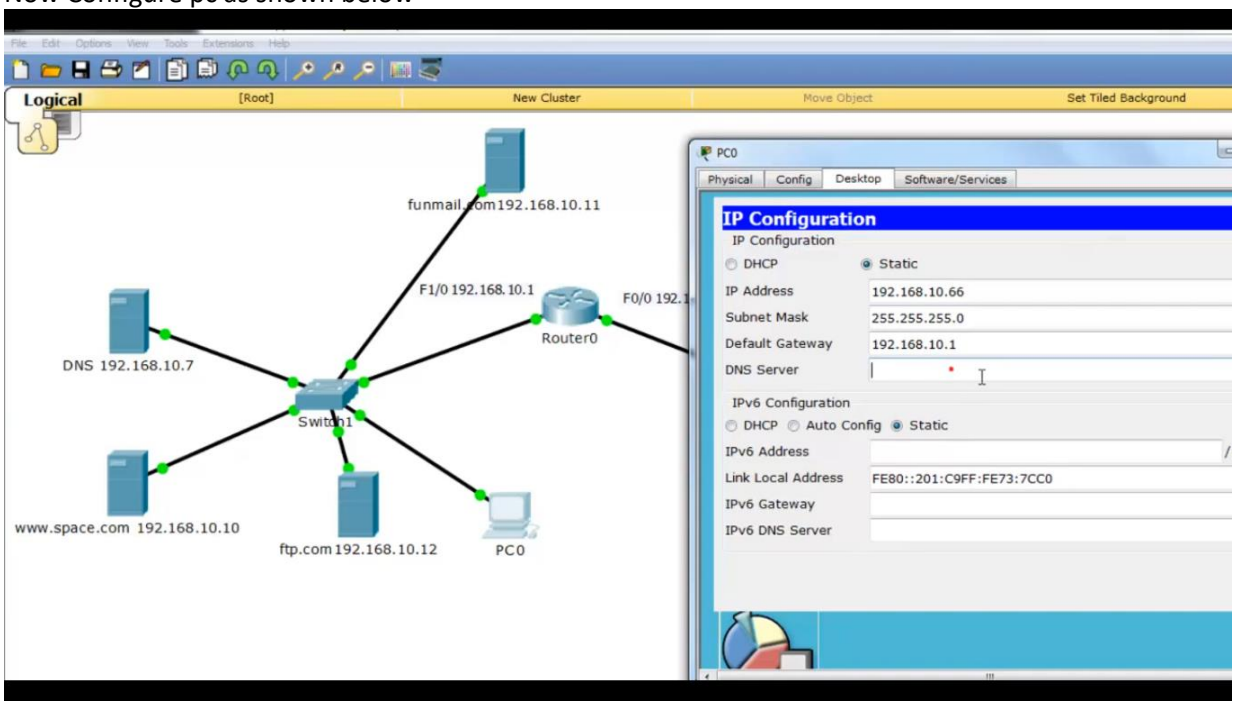
Now give webpage ip address and domain name and click “add this” as shown below



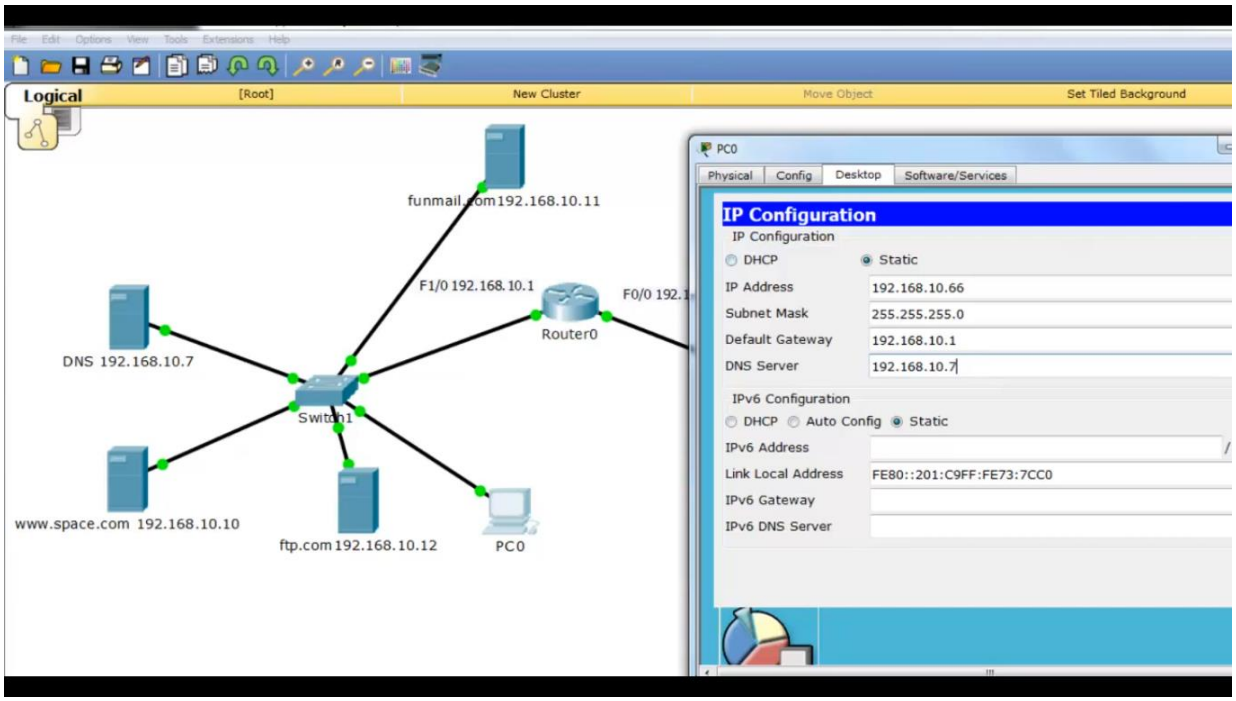
Like this add all server’s ip addresses and domain names



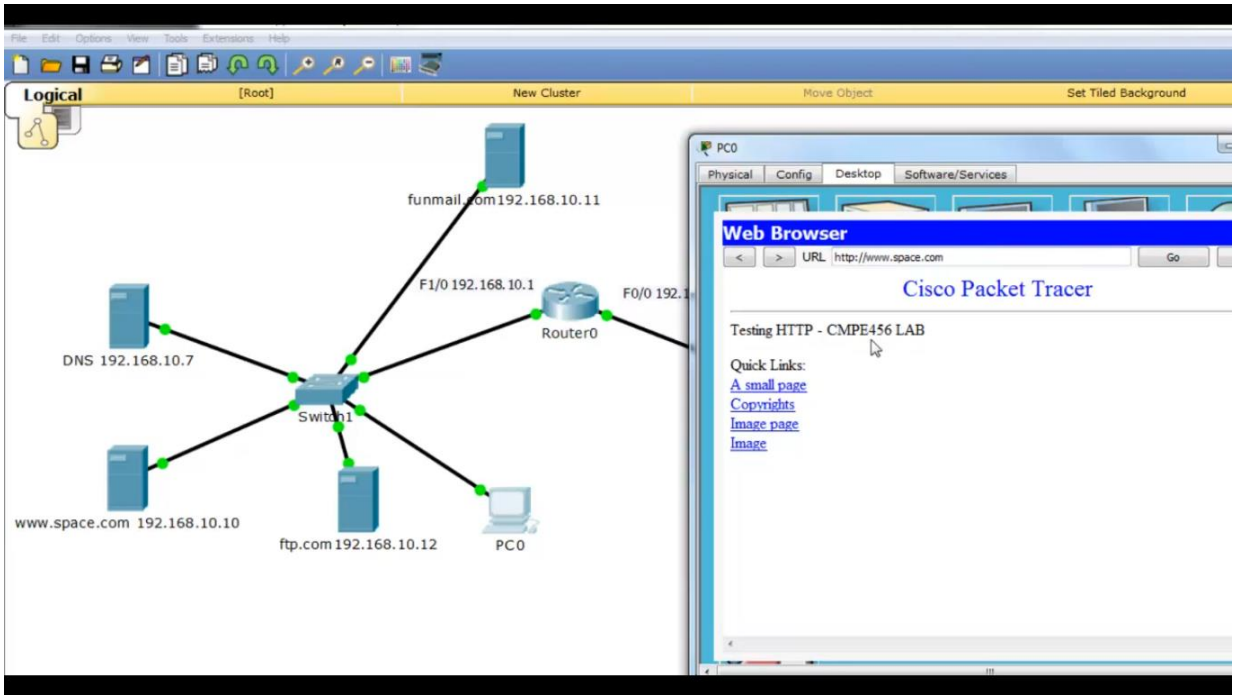
Now Configure pc as shown below



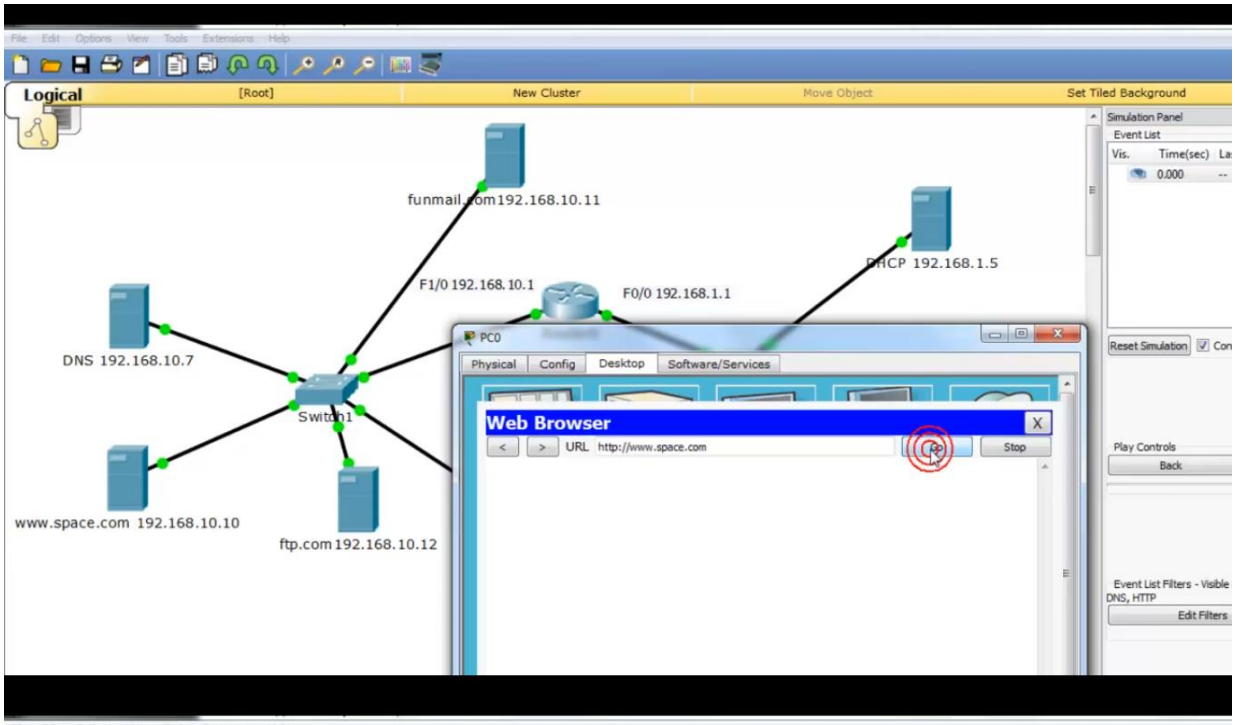
Do the same for other computers also
Give dns server address to pc as shown below

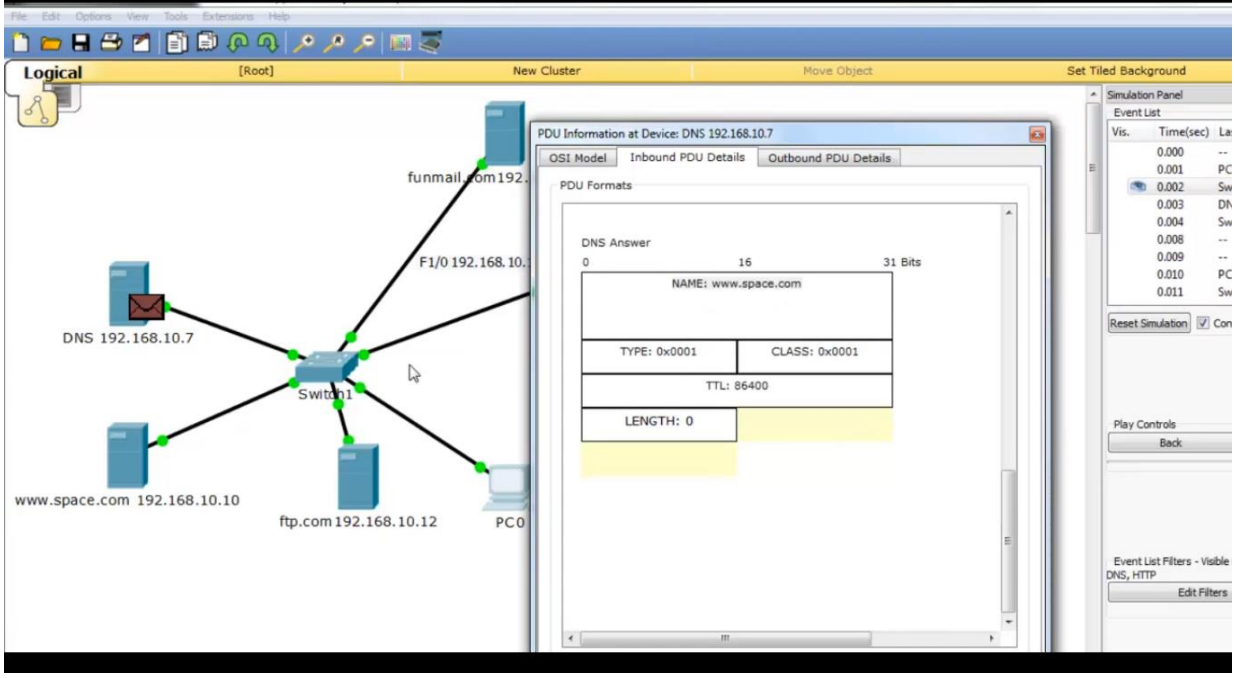


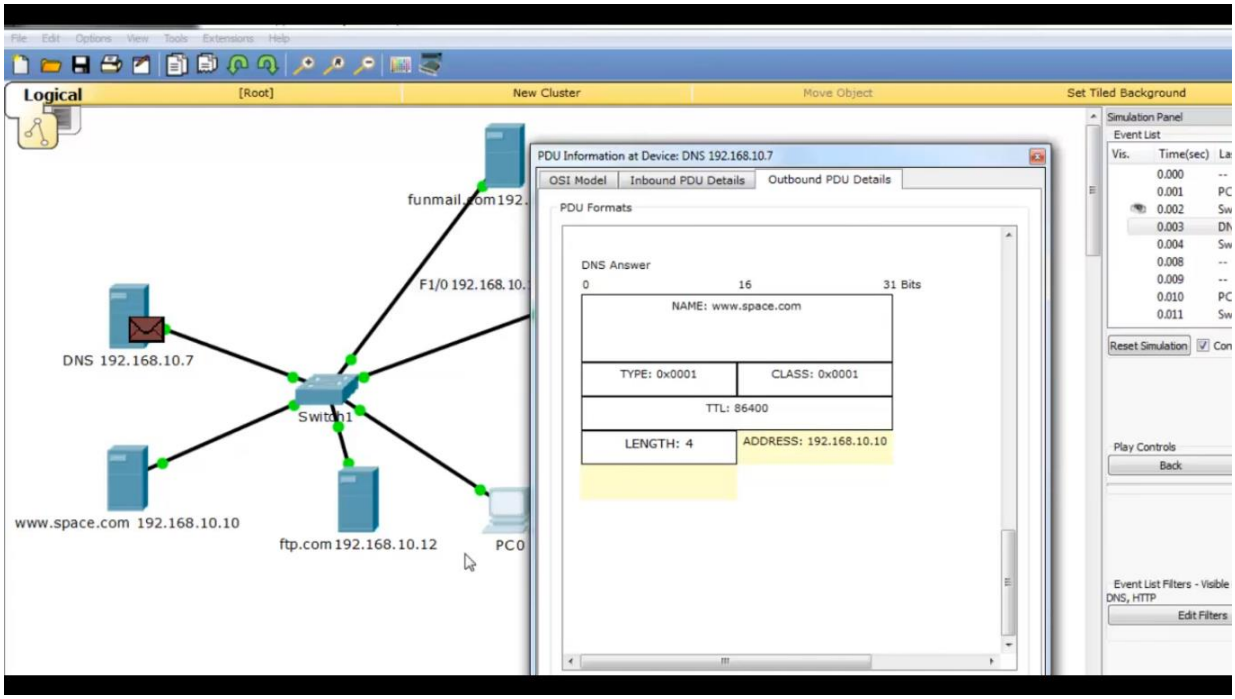
Now just test it



It worked!!!
Now check with Domain name as shown below


Logical
[Root]
New Cluster
Move Object
Set Tiled Background
funmail.com 192.168.10.11
DHCP 192.168.1.5
F1/0 192.168.10.1
F0/0 192.168.1.1
DNS 192.168.10.7
Switch1
www.space.com 192.168.10.10
ftp.com 192.168.10.12
PC0
Physical
Config
Desktop
Software/Services
Web Browser
URL http://www.space.com
Stop
Simulation Panel
Event List
Vis.
Time(sec)
Reset Simulation
Play Controls
Back
Event List Filters - Visible
DNS, HTTP
Edit Filters


Logical
[Root]
New Cluster
Move Object
Set Tiled Background
funmail.com 192.
F1/0 192.168.10.
DNS 192.168.10.7
Switch1
www.space.com 192.168.10.10
ftp.com 192.168.10.12
PC0
PDU Information at Device: DNS 192.168.10.7
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
DNS Answer
0
16
31 Bits
NAME: www.space.com
TYPE: 0x0001
CLASS: 0x0001
TTL: 86400
LENGTH: 0
Simulation Panel
Event List
Vis.
Time(sec)
Reset Simulation
Play Controls
Back
Event List Filters - Visible
DNS, HTTP
Edit Filters



Now also works!!!

So we have successfully configured Application Layer Service of the OSI Model

---END---

Project 2

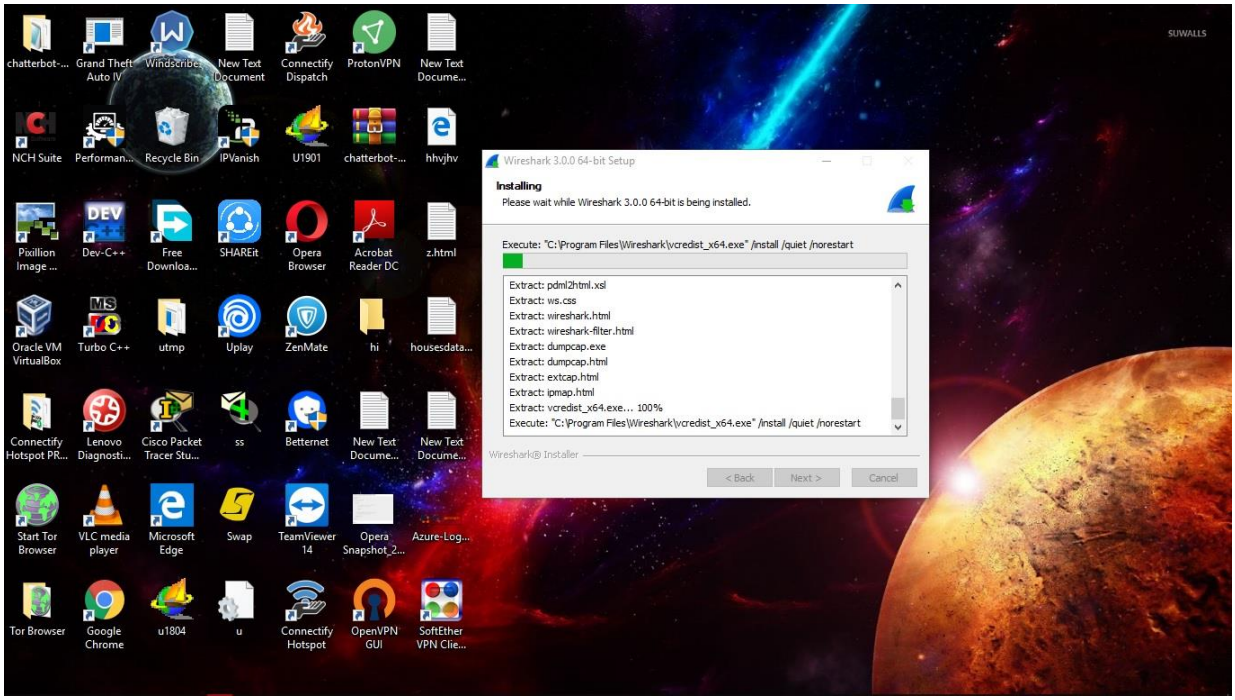
IP Packet Analysis using WIRESHARK

Software Used:

WIRESHARK

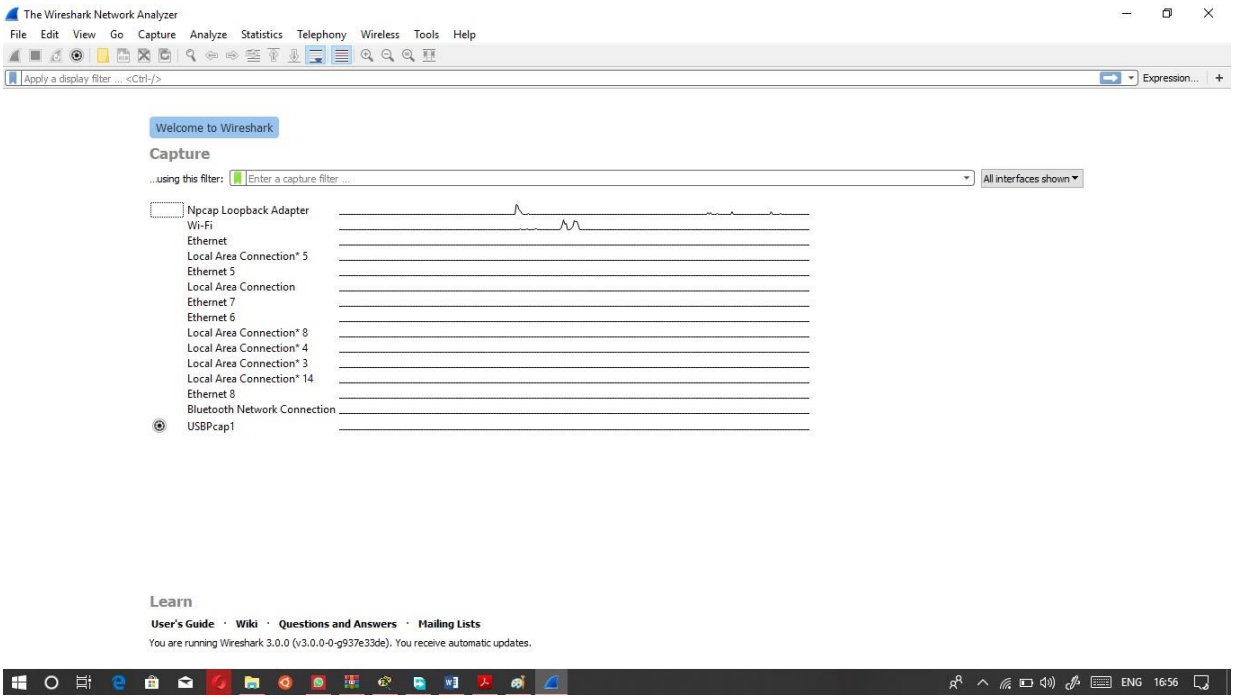
Procedure:

*First install wireshark software



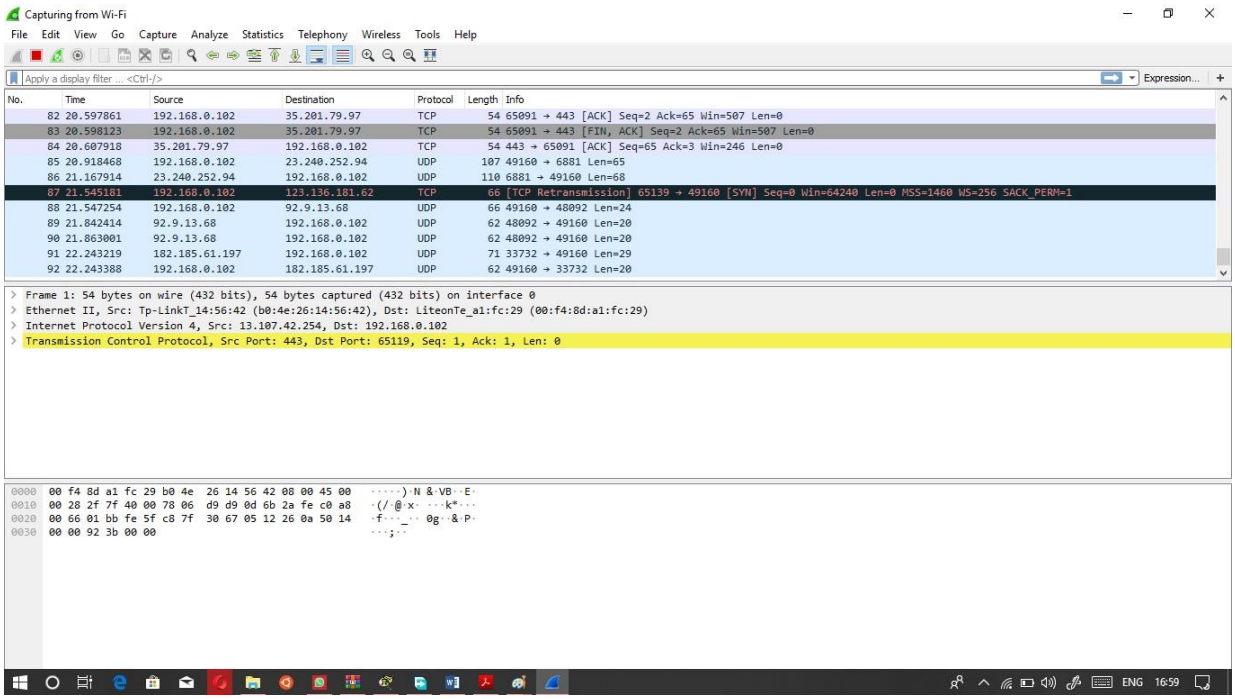
Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options.



As soon as you click the interface’s name, you’ll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

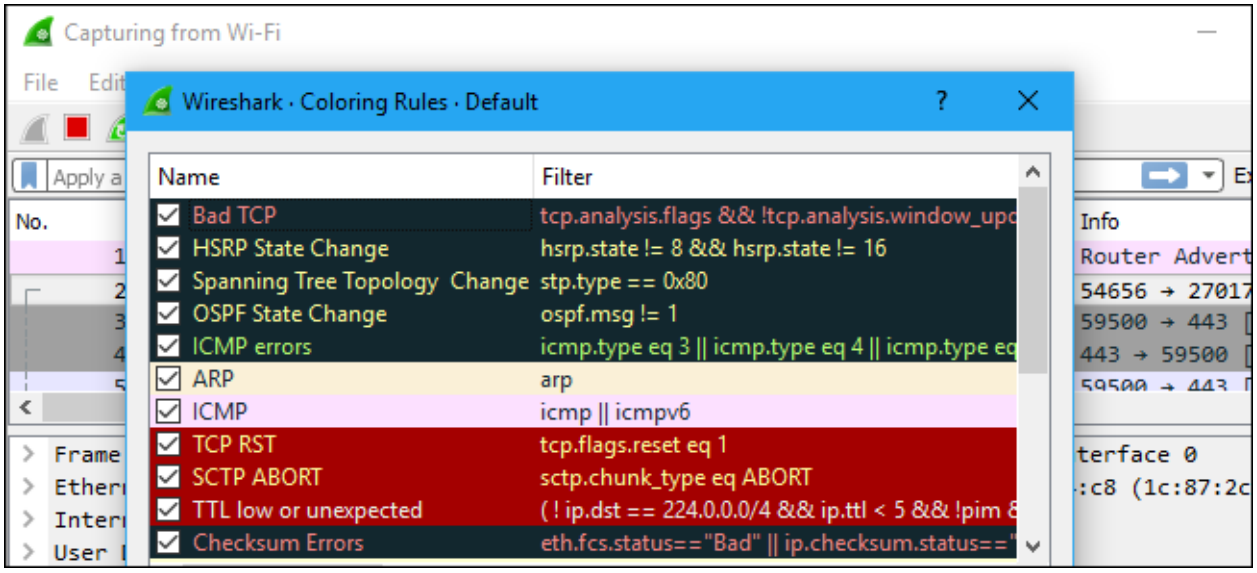
If you have promiscuous mode enabled—it’s enabled by default—you’ll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the “Enable promiscuous mode on all interfaces” checkbox is activated at the bottom of this window.



Color Coding

You'll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

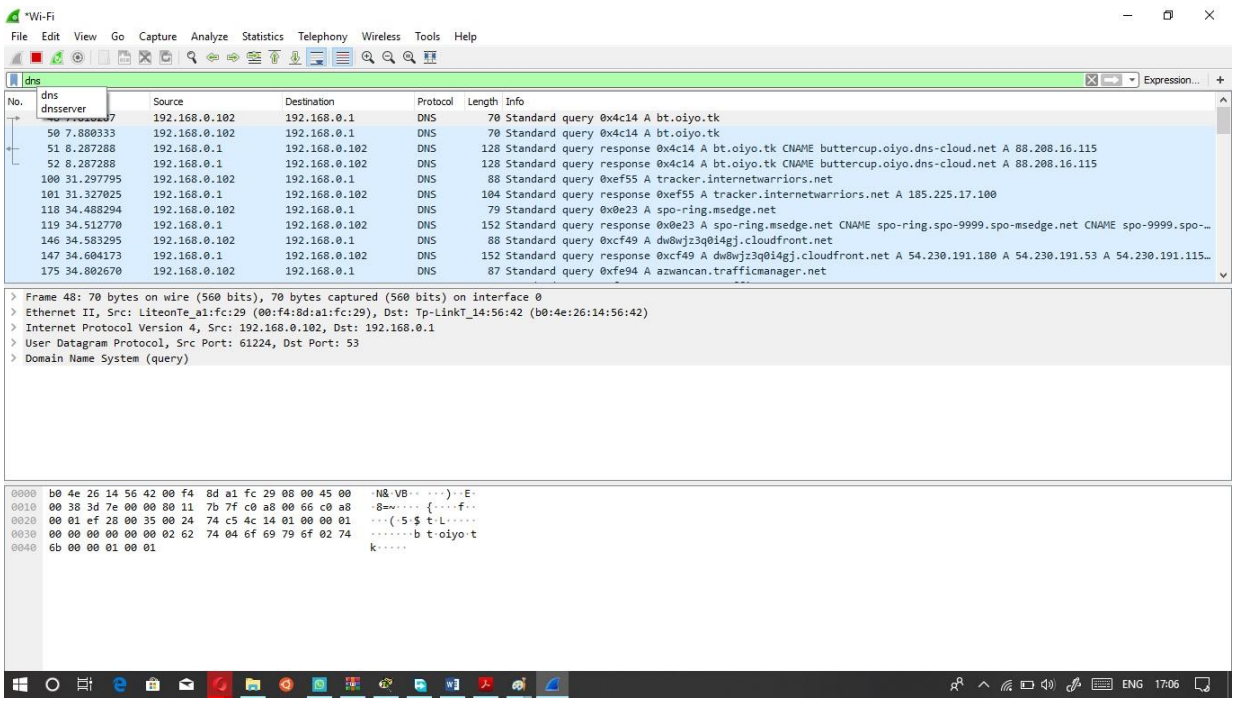
If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.

Filtering Packets

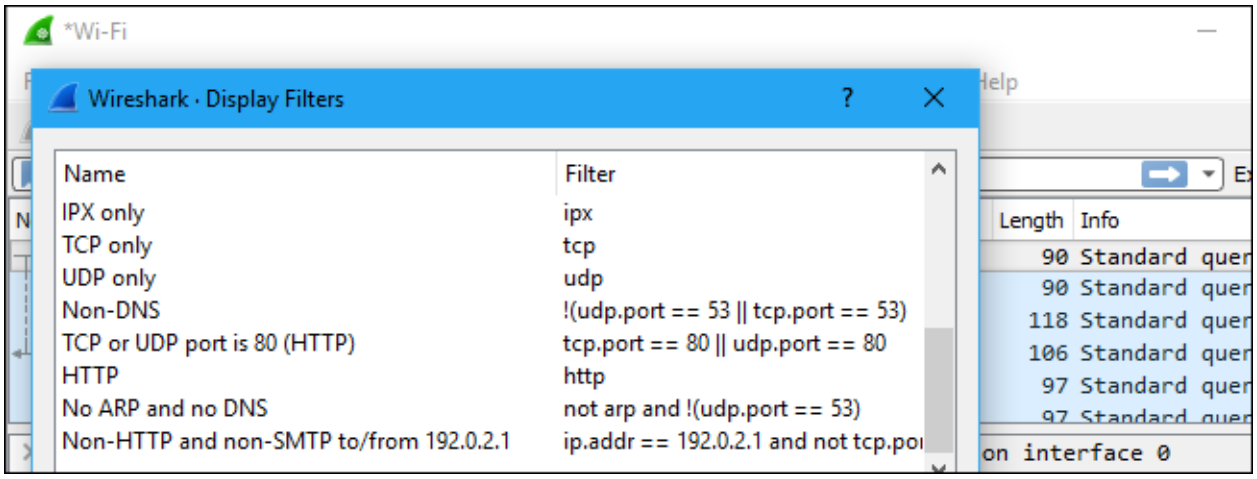
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

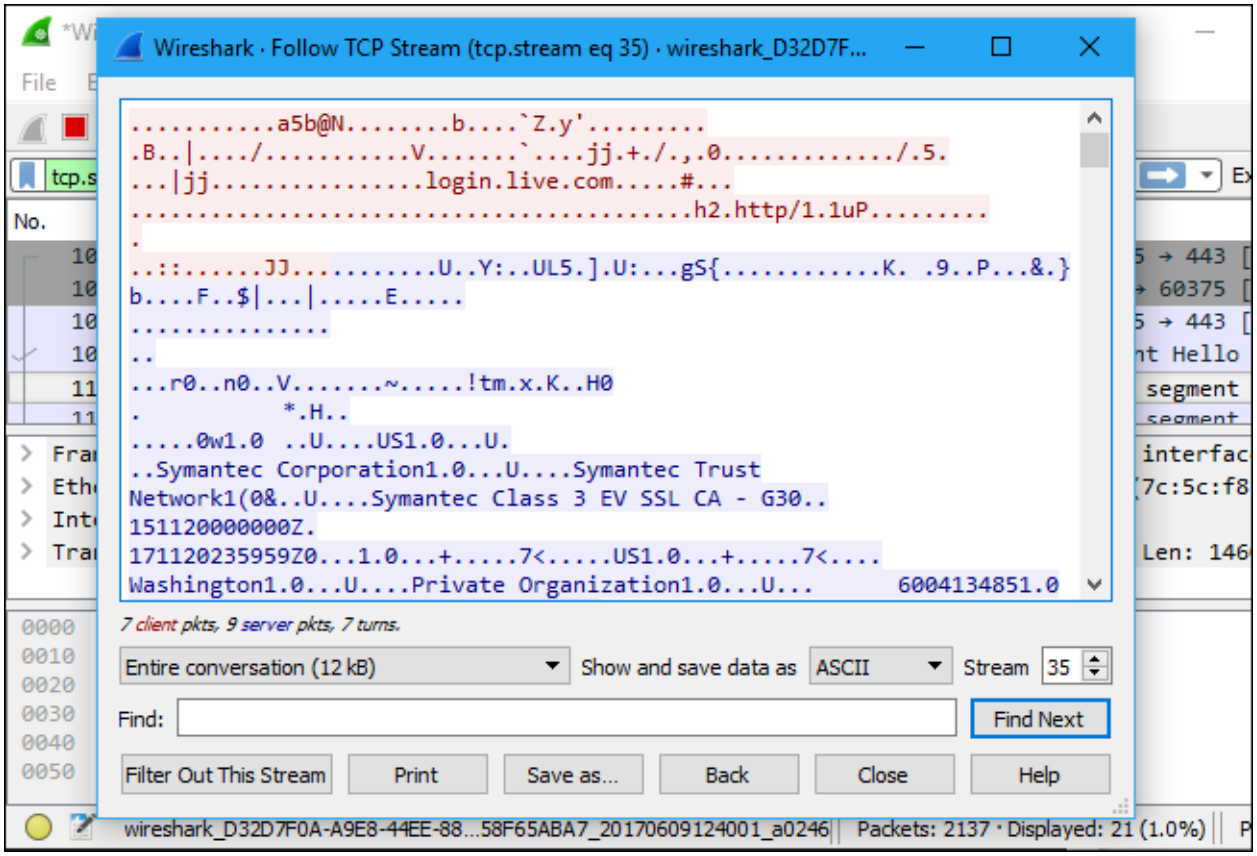
For more information on Wireshark's display filtering language, read the Building display filter expressions page in the official Wireshark documentation.



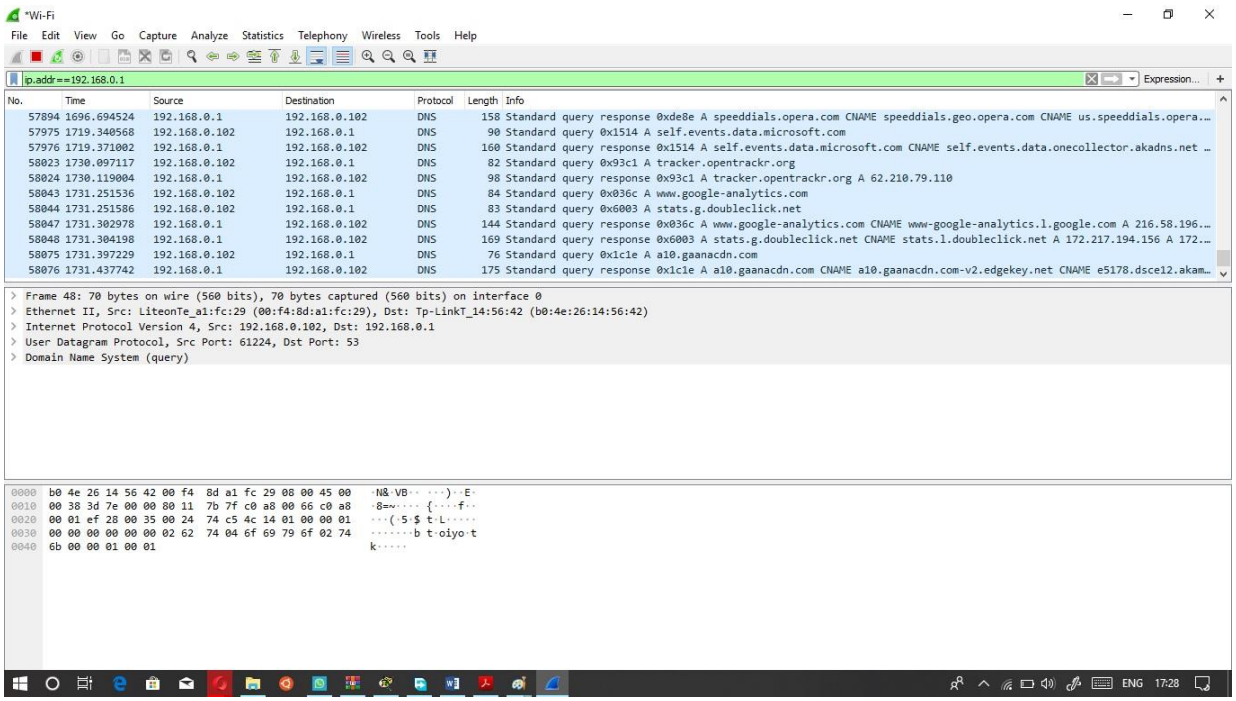
Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.

Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.



- To filter traffic from any specific IP address type: `ip.addr == 'xxx.xx.xx.xx'` in the **Apply a display filter** field.
- To filter traffic for specific protocol say `TCP`, `UDP`, `SMTP`, `ARP`, `DNS` Requests etc just type the protocol name in the Apply a display filter field.



---END---

Project 3

Intra-department Lab Network using RIP Routing

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

Hop Count :

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

Features of RIP :

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbor routers. This is also known as *Routing on rumours*.

RIP versions :

There are three vesions of routing information protocol – **RIP Version1**, **RIP Version2**and **RIPng**.

RIP v1 is known as *Classful* Routing Protocol because it doesn't send information of subnet mask in its routing update.

RIP v2 is known as *Classless* Routing Protocol because it sends information of subnet mask in its routing update.

To configure RIP

Configure RIP for Router:

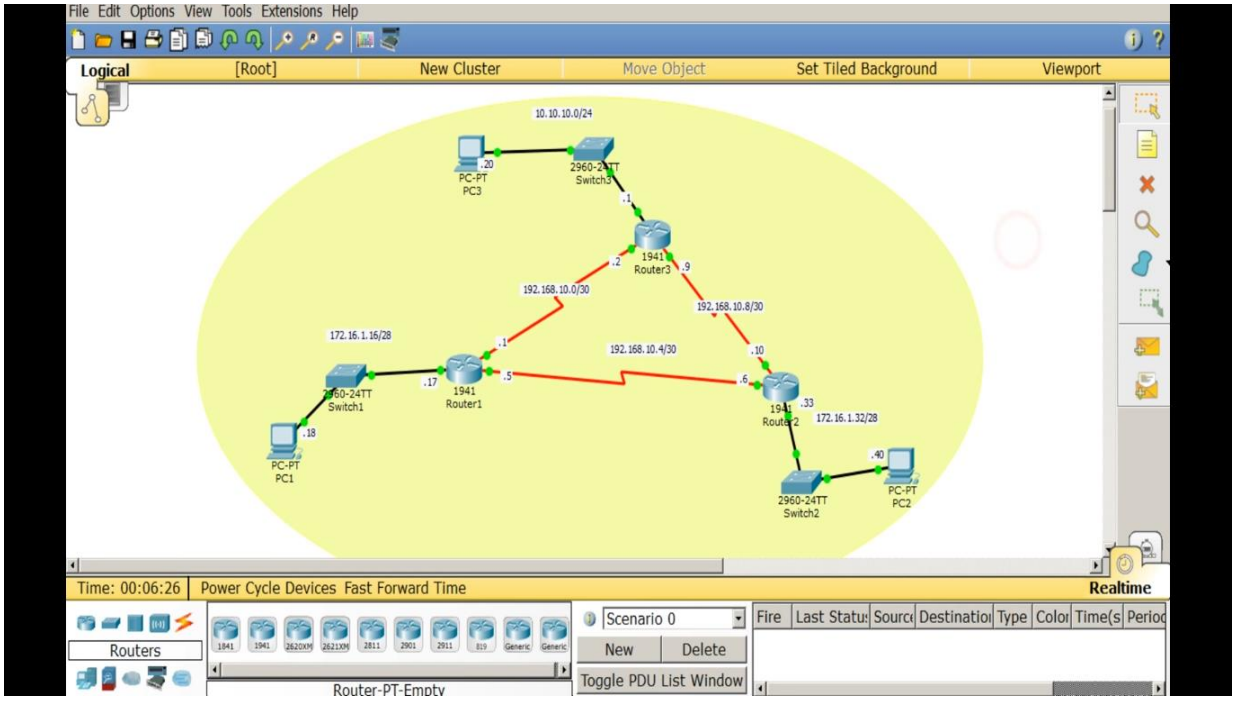
```
R1(config)# router rip
R1(config-router)# network <I.p address>
R1(config-router)# network <I.p address>
R1(config-router)# version 2 (OR) version 1
R1(config-router)# no auto-summary
```

RIP timers :

- **Update timer :** The default timing for routing information being exchanged by the routers operating RIP is 30 seconds. Using Update timer, the routers exchange their routing table periodically.

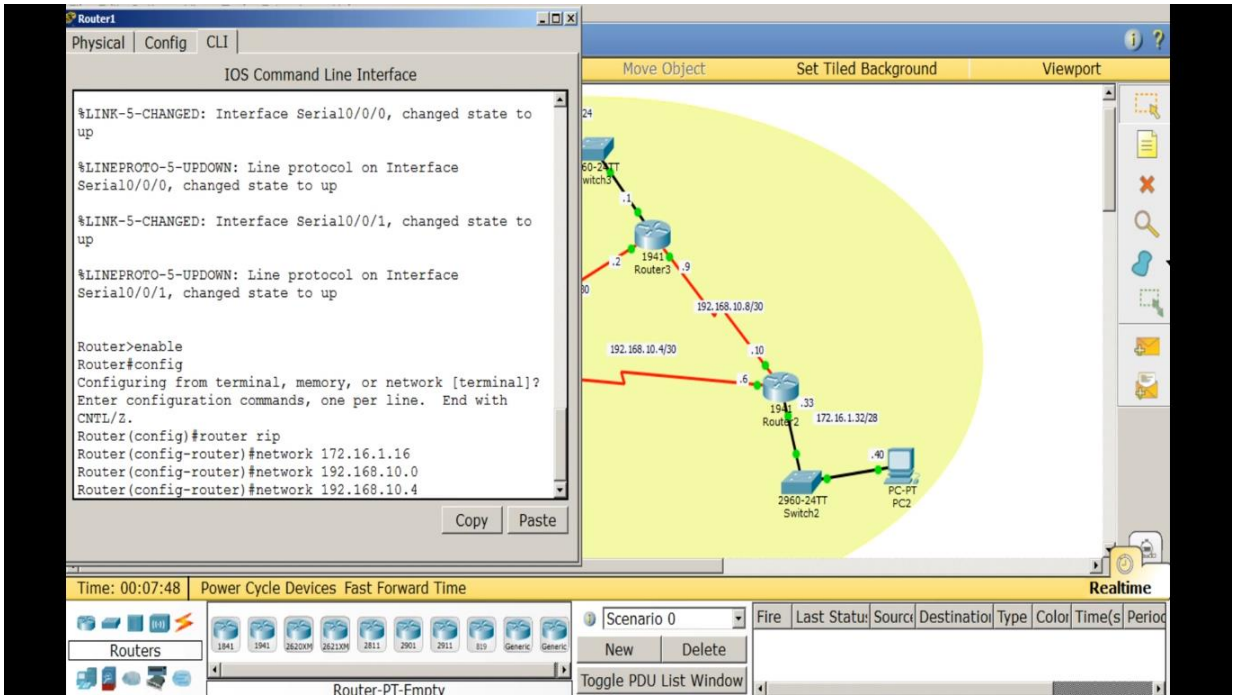
- **Invalid timer:** If no update comes until 180 seconds, then the destination router consider it as invalid. In this scenario, the destination router mark hop count as 16 for that router.
- **Hold down timer :** This is the time for which the router waits for neighbour router to respond. If the router isn't able to respond within a given time then it is declared dead. It is 180 seconds by default.
- **Flush time :** It is the time after which the entry of the route will be flushed if it doesn't respond within the flush time. It is 60 seconds by default. This timer starts after the route has been declared invalid and after 60 seconds i.e time will be 180 + 60 = 240 seconds.
  Software used:
  Cisco packet tracer

Procedure:
Connect computers and routers as shown below



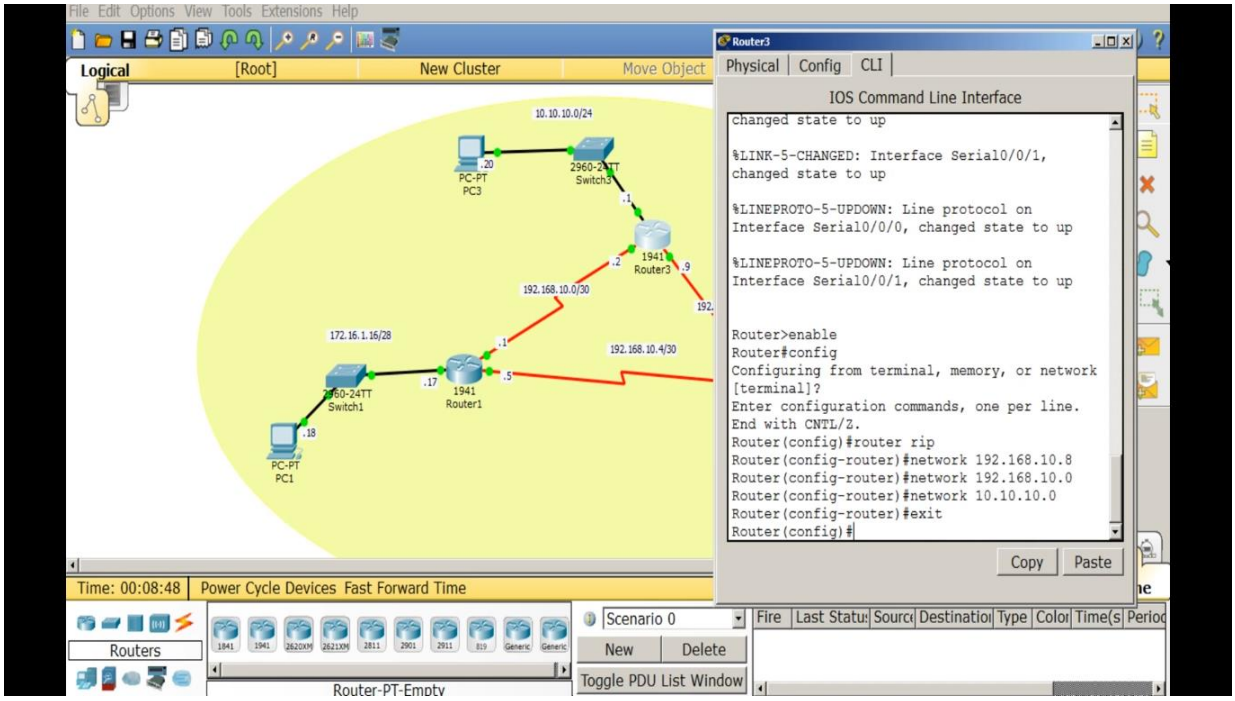
Now give ip's and subnets to routers in Rip version 1 or Rip version 2

Now we are configuring router 1

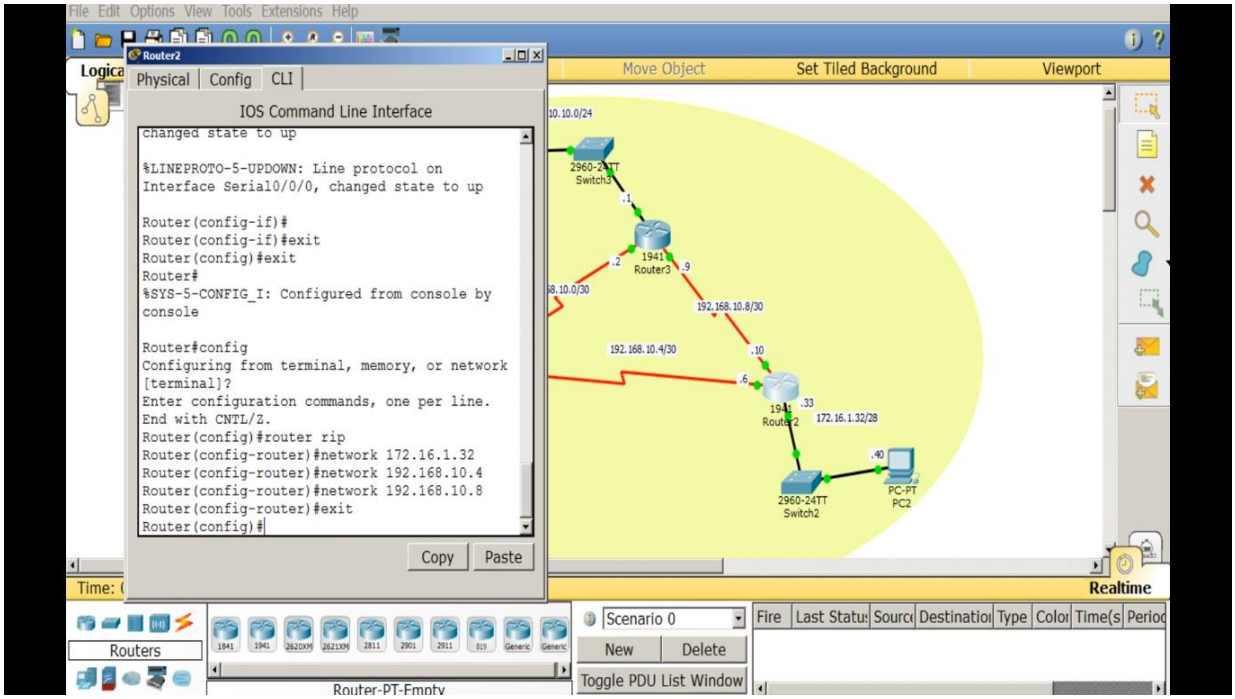


Now configure other routers as shown below

Router 3



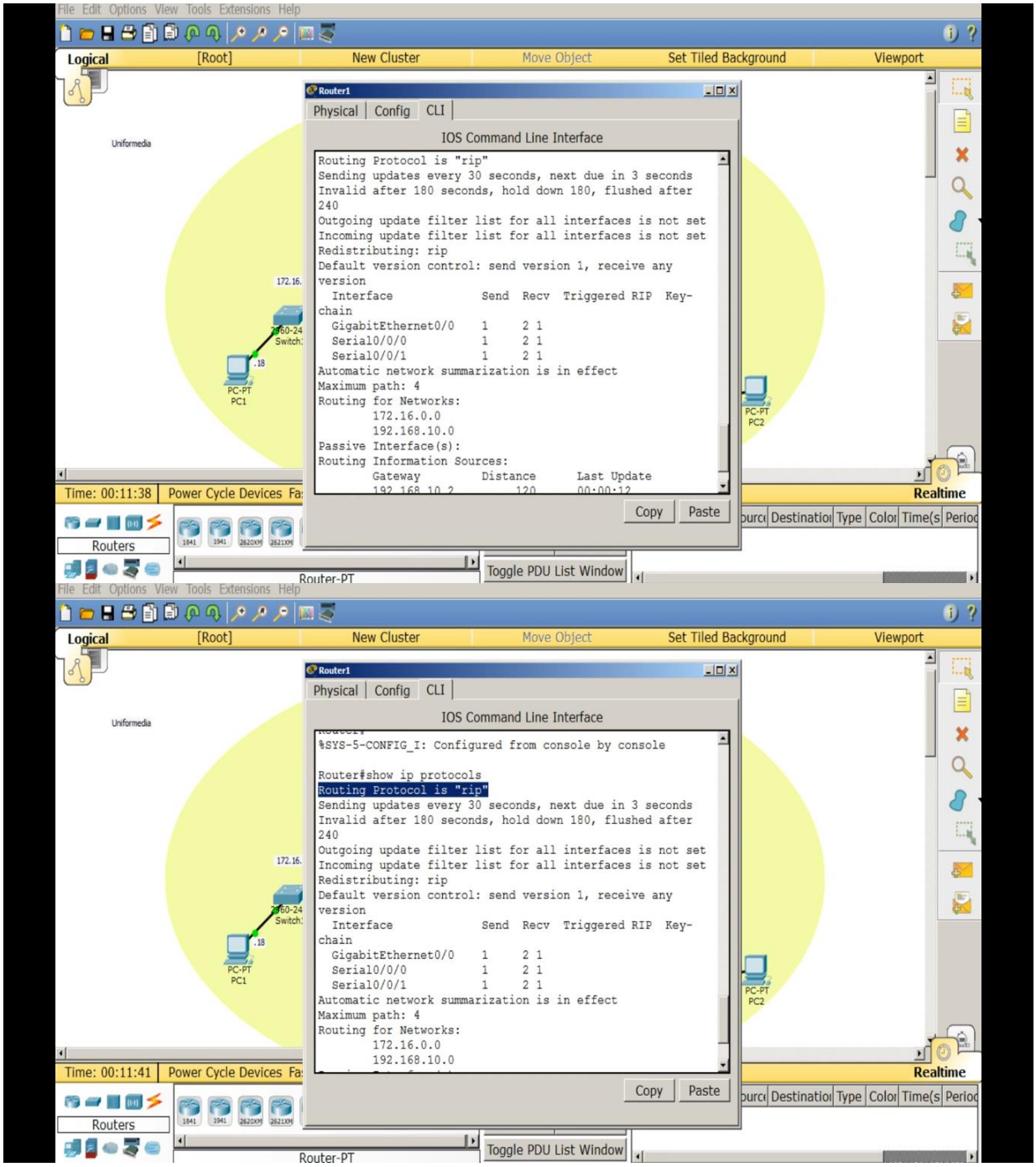
Router 2

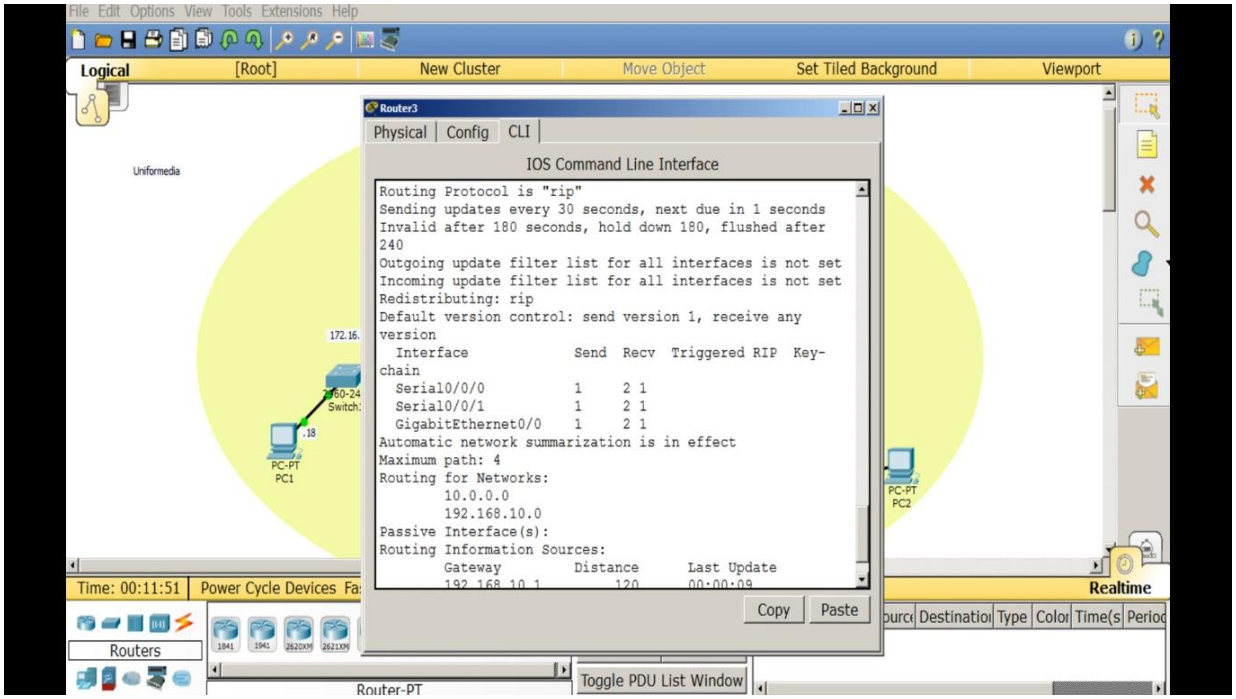


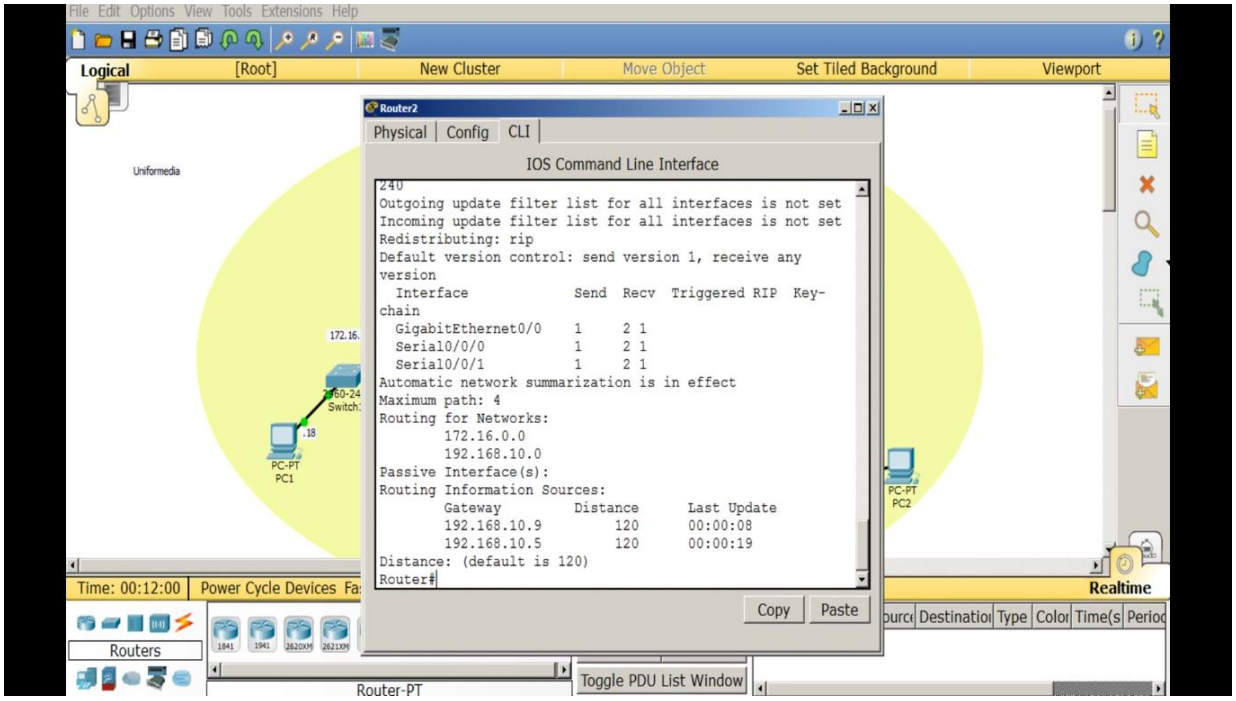
Now we have completed configuring routers

Now to show ip route protocols type ip route protocal
If you have configured correctly then you can see this screen shot in your computer

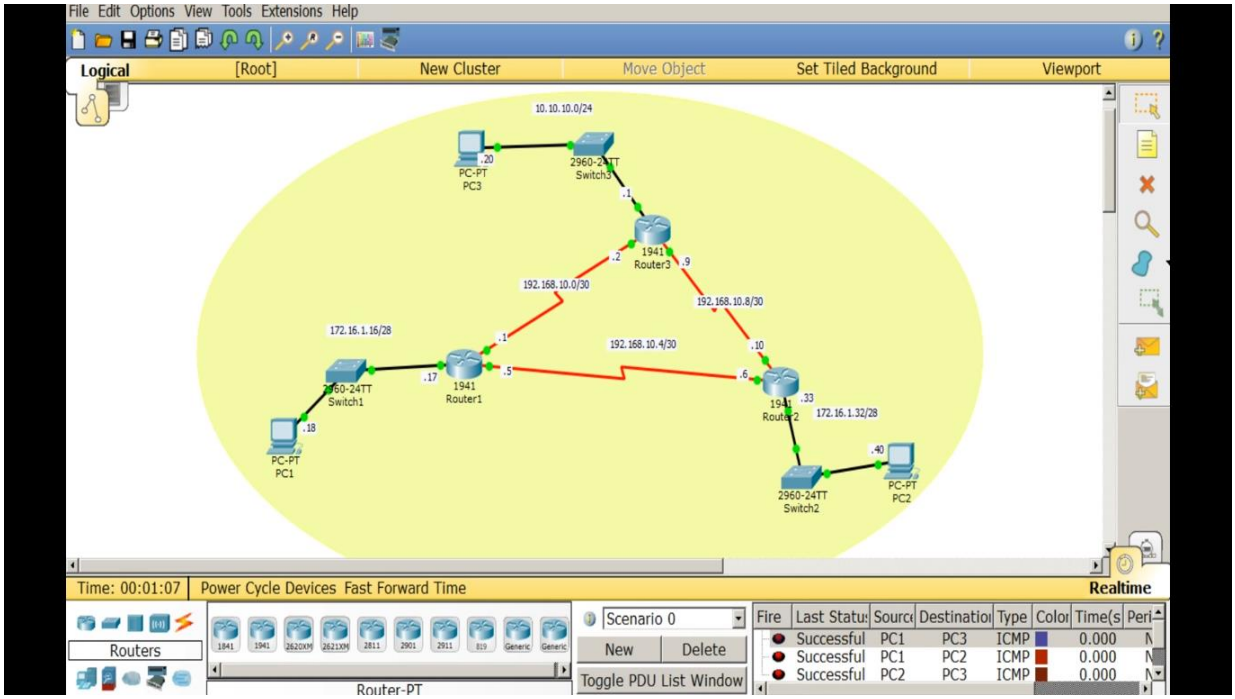
Now give ip address, subnet masks, default gateway to the computers.


File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Router1
Physical
Config
CLI
IOS Command Line Interface
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 3 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
Interface Send Recv Triggered RIP Key-chain
GigabitEthernet0/0 1 2 1
Serial0/0/0 1 2 1
Serial0/0/1 1 2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
172.16.0.0
192.168.10.0
Passive Interface(s):
Routing Information Sources:
Gateway Distance Last Update
Copy
Paste
Uniformedia
PC-PT PC1
PC-PT PC2
Time: 00:11:38
Power Cycle Devices
Realtime
Routers
Toggle PDU List Window
Router-PT
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip protocols
Routing Protocol is "rip"
Time: 00:11:41





Now check whether packet travels from one pc to other pc to check connectivity



So, It is showing successful

The above picture is Intra-department Lab Network using RIP Routing as there is no connection to external internet
I took ratio, if there are 100 pc's then I took 1 pc for convinence
This is called as RIP Routing

---END---

Project 4
Office Area Network using Static Routing

Advantage of static routing

- It is easy to implement.
- It is most secure way of routing, since no information is shared with other routers.
- It puts no overhead on resources such as CPU or memory.

Disadvantage of static routing

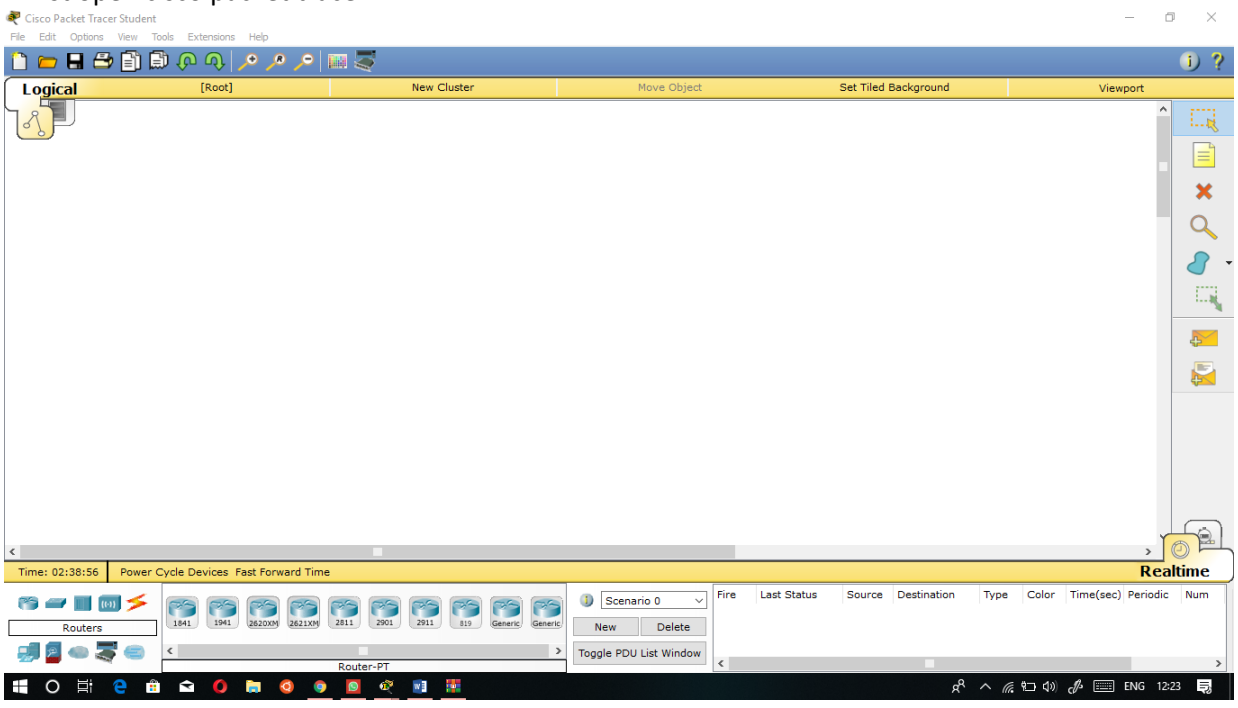
- It is suitable only for small network.
- If a link fails it cannot reroute the traffic.

To explain static routing, I will use packet tracer network simulator software

Software used: Cisco packet tracer

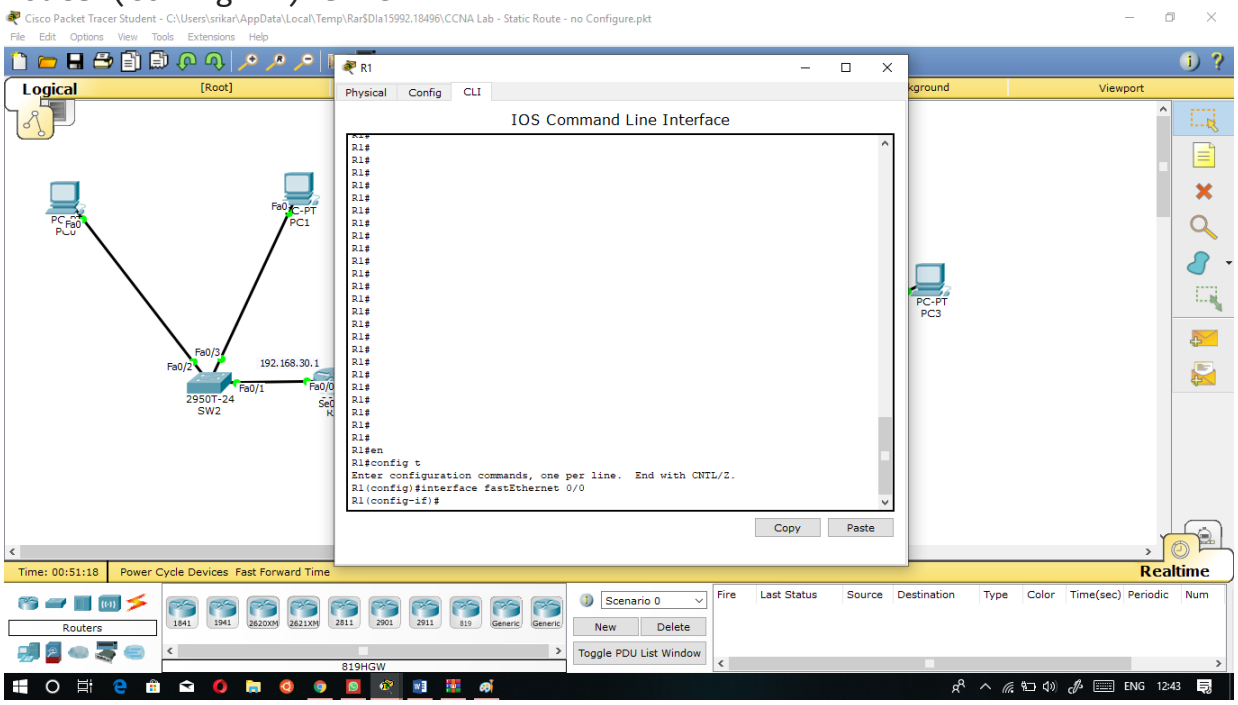
Procedure:

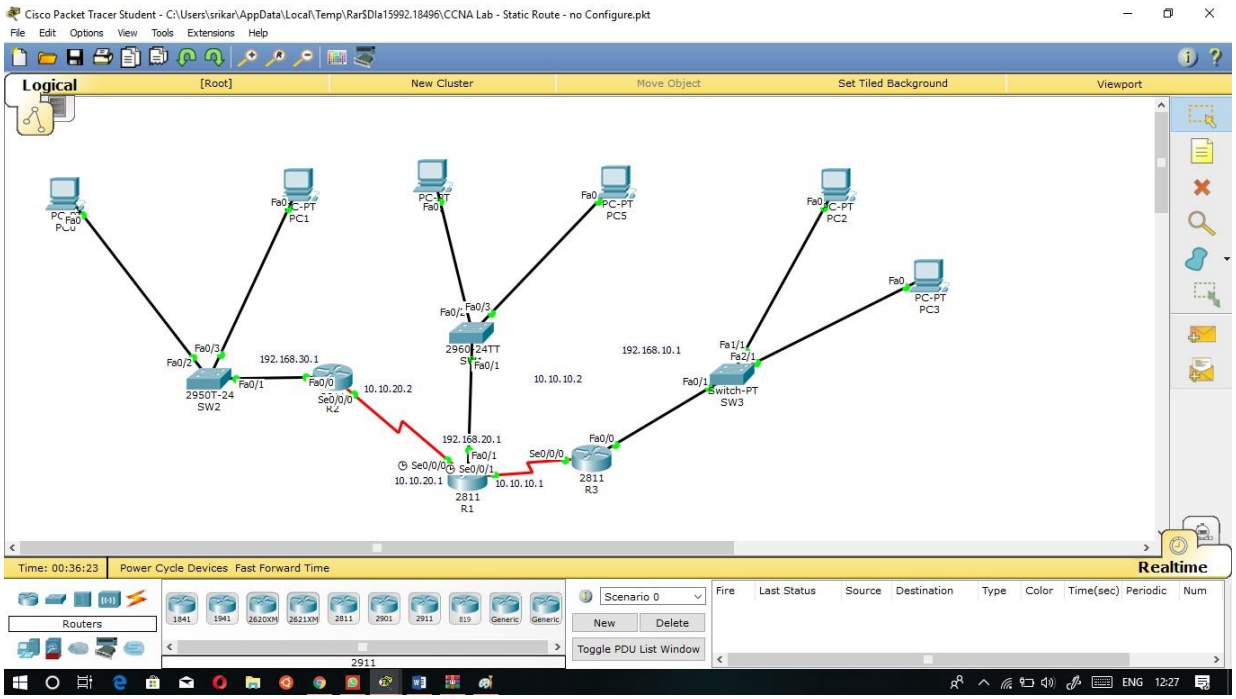
*First open cisco packet tracer



*Create a practice lab as shown in following figure or download this pre-created practice lab and load in packet tracer
*Type these commands on every routers with their respective ip addresses and subnet masks

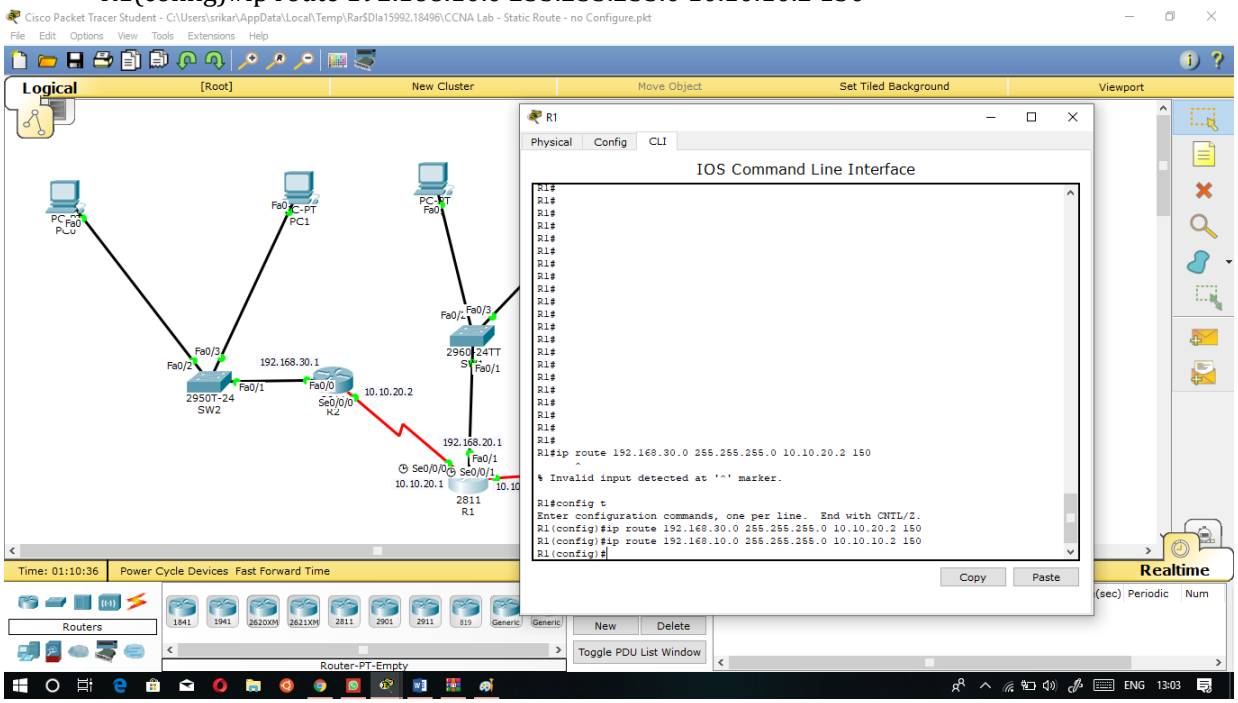
```
Router>enable
Router#configure terminal

Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 10.10.20.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#no auto-summary
Router(config-if)#exit
```





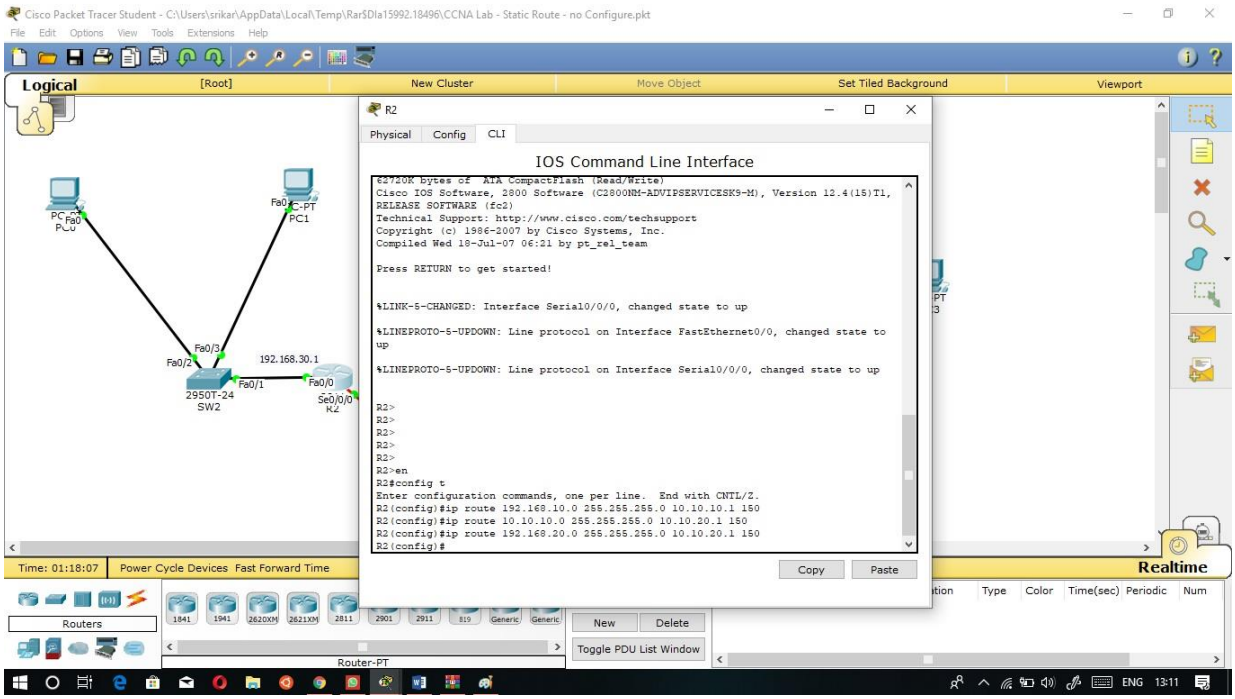
1. In the **R1** type the following commands to introduce two LANs 192.168.10.0/24 and 192.168.30.0/24 for Router 1.

- R1(config)#ip route 192.168.30.0 255.255.255.0 10.10.20.2 150
- R1(config)#ip route 192.168.10.0 255.255.255.0 10.10.10.2 150



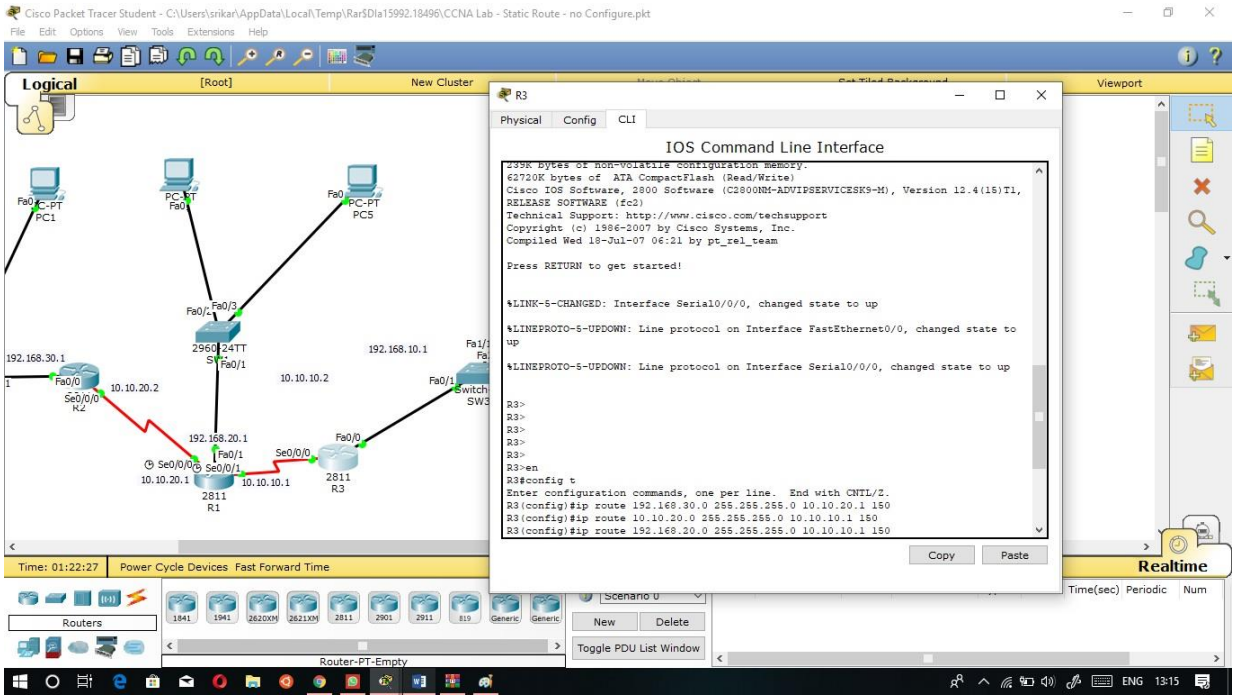
2. Router2: Add three networks for router 2 and be sure that do not configure it with wrong IP address.

R2(config)#ip route 192.168.10.0 255.255.255.0 10.10.10.1 150
R2(config)#ip route 10.10.10.0 255.255.255.0 10.10.20.1 150
R2(config)#ip route 192.168.20.0 255.255.255.0 10.10.20.1 150



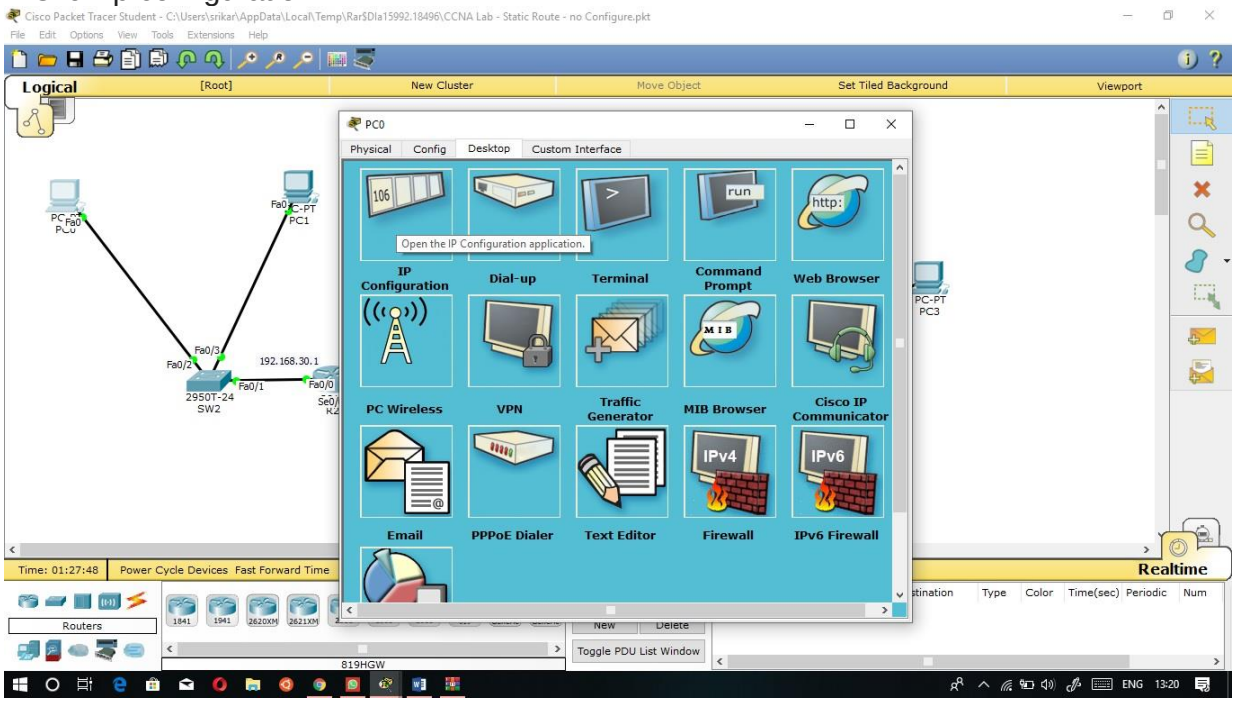
3. Router3: Do the same as router 2 but with different destination and exit interface address.

R3(config)#ip route 192.168.30.0 255.255.255.0 10.10.20.1 150
R3(config)#ip route 10.10.20.0 255.255.255.0 10.10.10.1 150
R3(config)#ip route 192.168.20.0 255.255.255.0 10.10.10.1 150

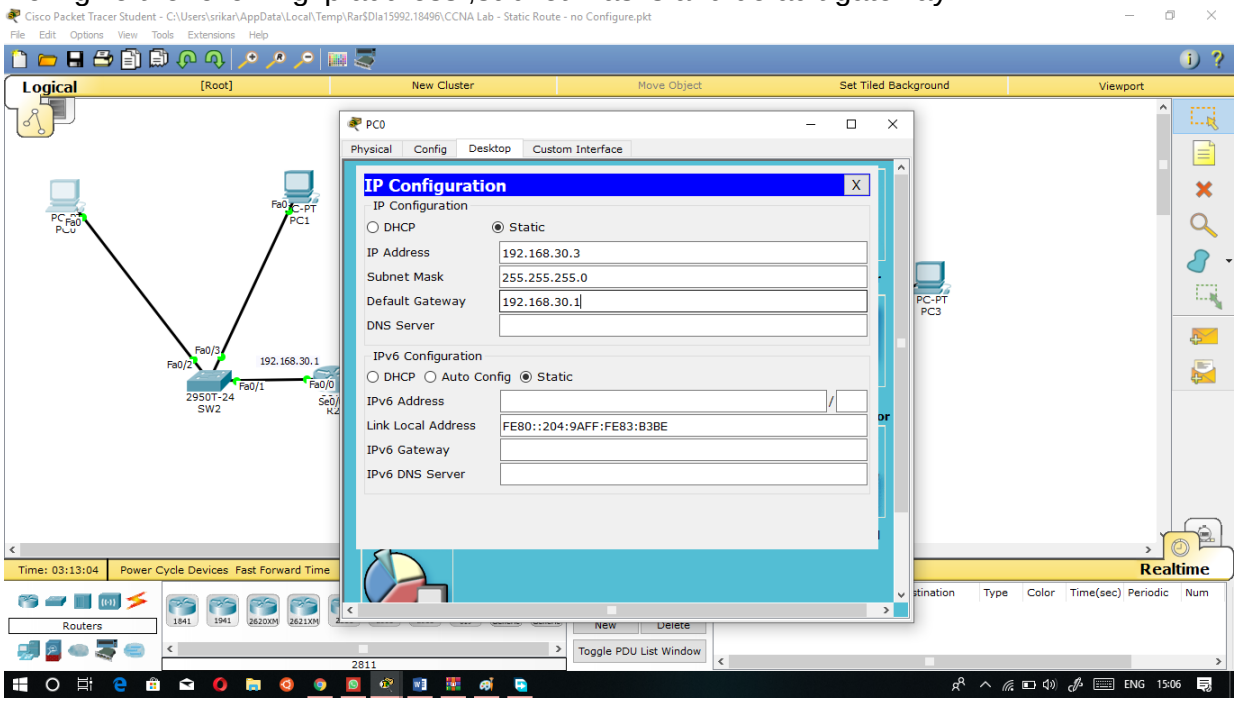


* with '**show ip route** or **show run**' commands we can see the routing tables

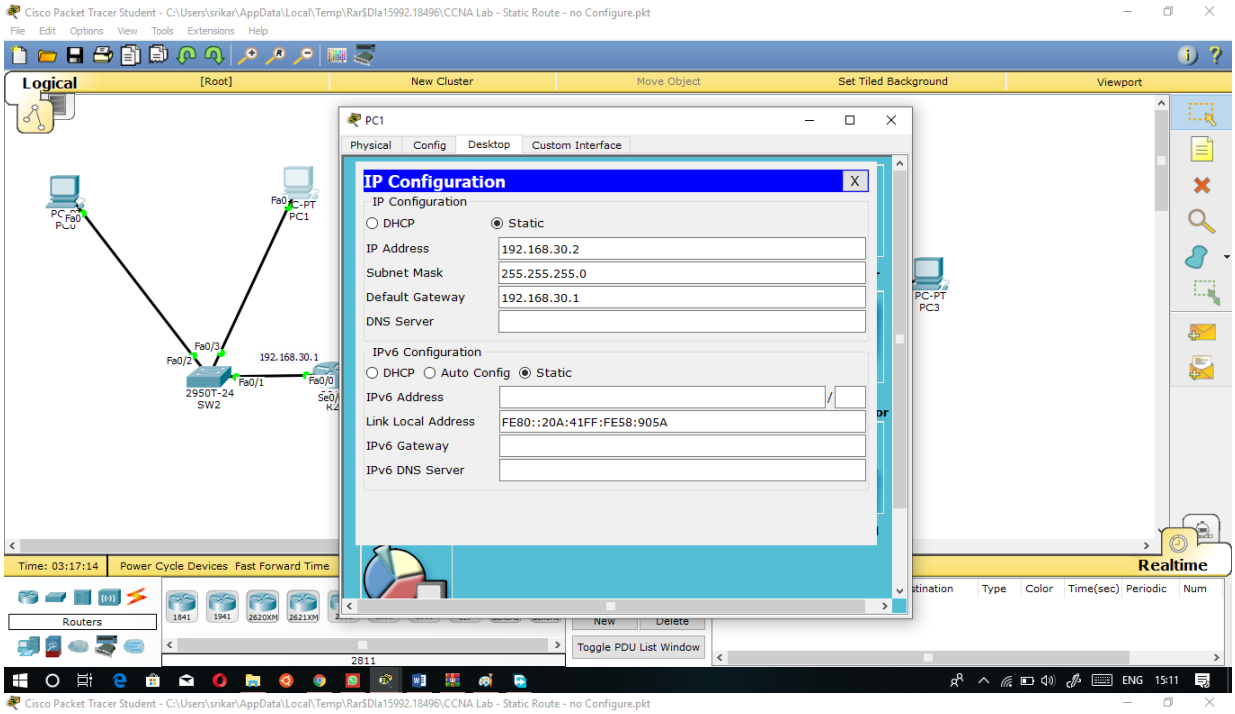
Now we have successfully completed our routing
Now we should give ip,subnet,default gateway to pc or laptop
*Click ip configuration

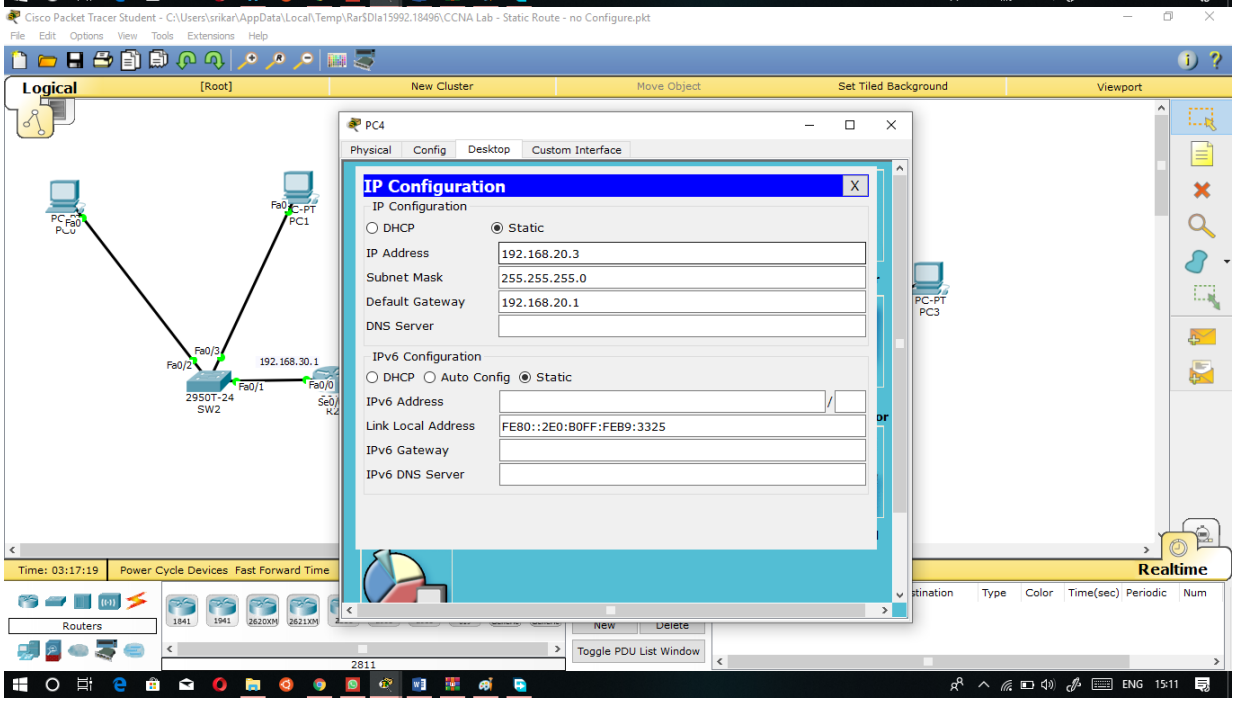


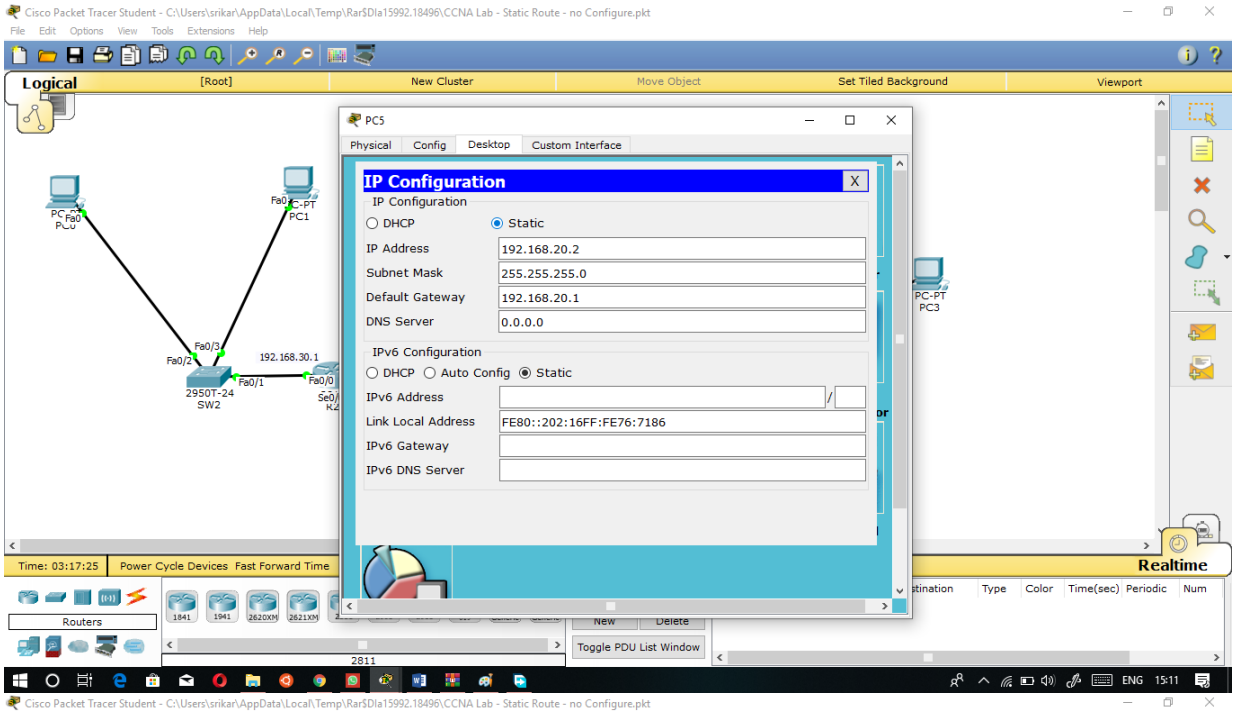
Now give the following ip address ,subnet masks and default gateway

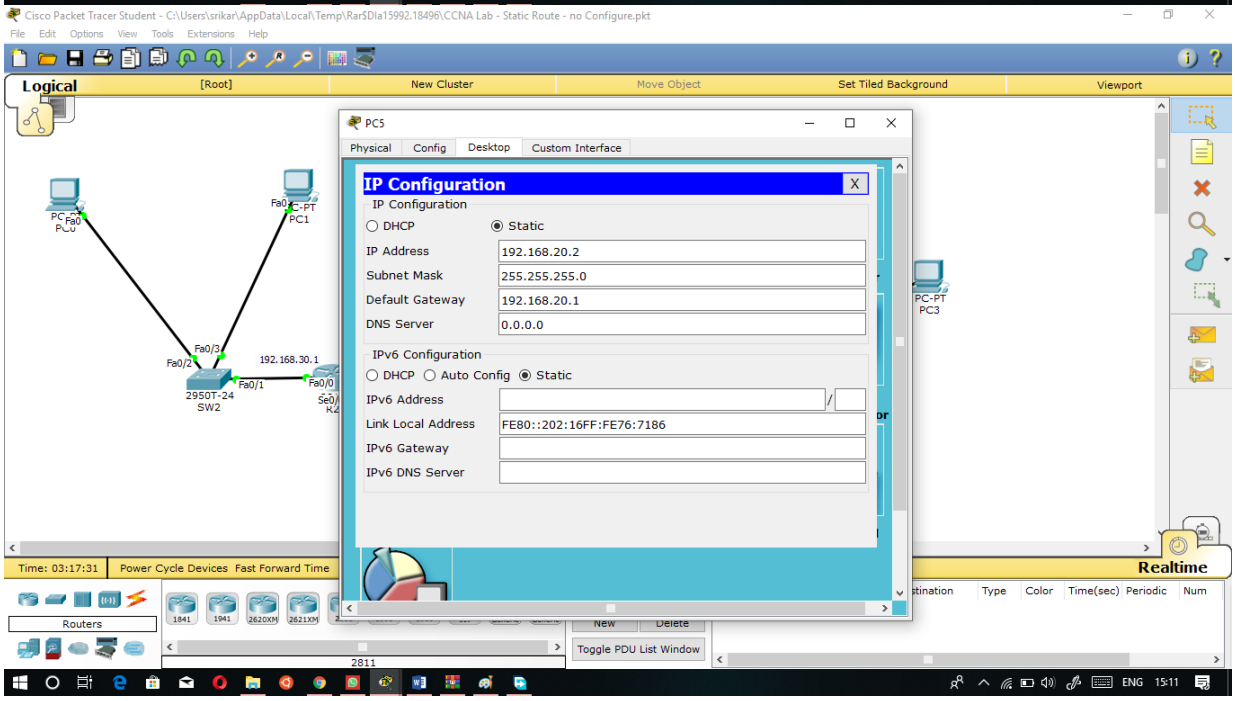


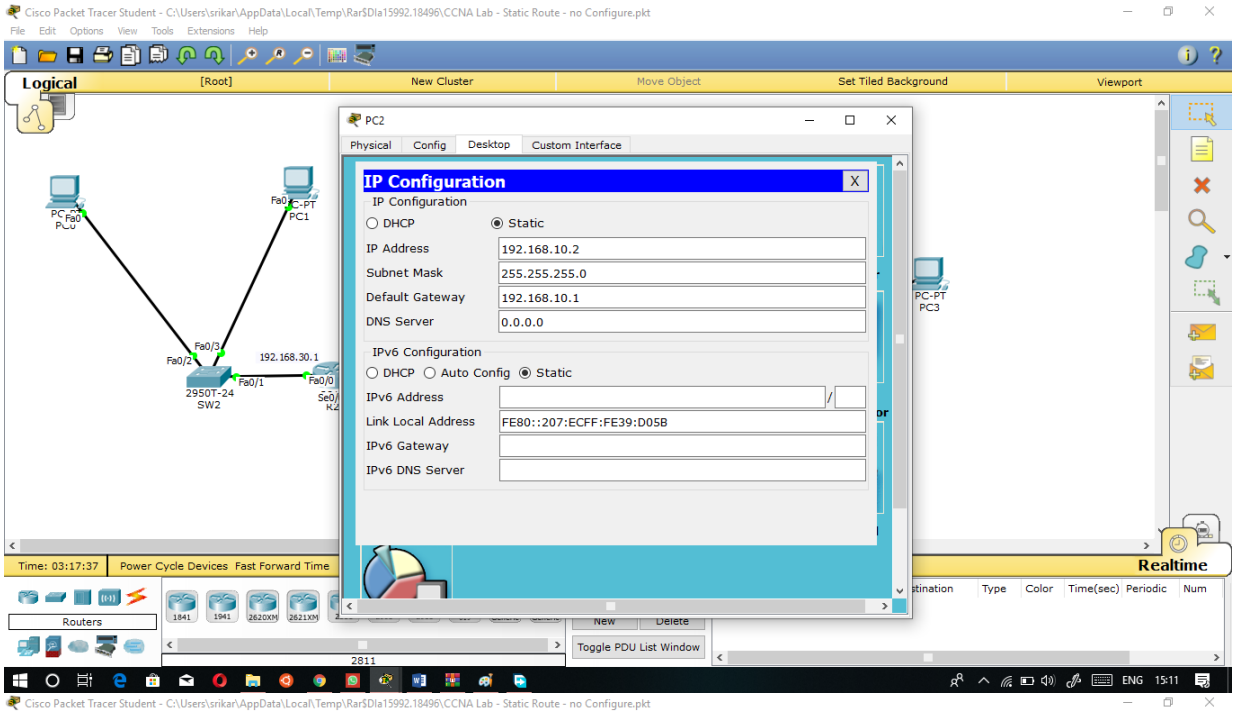
Now give ip's,default gateway and subnet masks to other computers as shown in the below screenshots

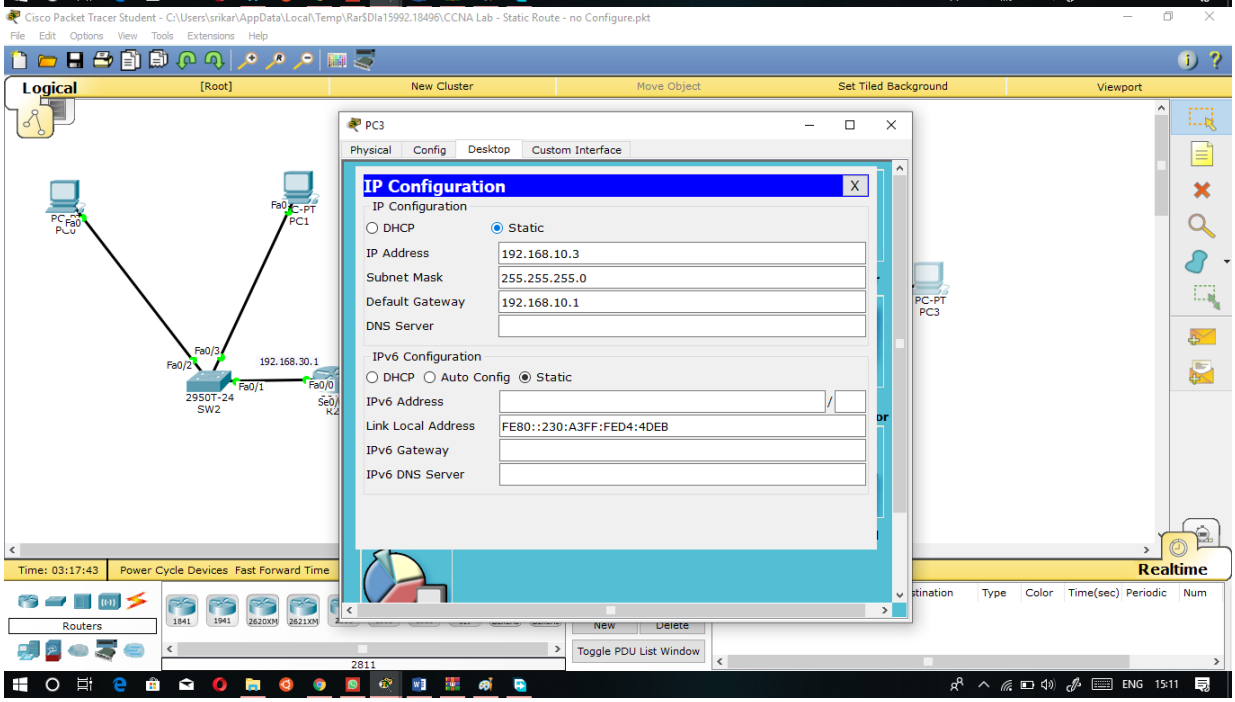

Cisco Packet Tracer Student - C:\Users\srikar\AppData\Local\Temp\Rar$DIa15992.18496\CCNA Lab - Static Route - no Configure.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC1
Physical Config Desktop Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address 192.168.30.2
Subnet Mask 255.255.255.0
Default Gateway 192.168.30.1
DNS Server
IPv6 Configuration
DHCP Auto Config Static
IPv6 Address
Link Local Address FE80::20A:41FF:FE58:905A
IPv6 Gateway
IPv6 DNS Server
PC-PT PC1
PC-PT PC3
2950T-24 SW2
192.168.30.1
Fa0/1
Fa0/2
Fa0/3
Time: 03:17:14
Power Cycle Devices Fast Forward Time
Realtime
Routers
Toggle PDU List Window
ENG 15:11


Cisco Packet Tracer Student - C:\Users\srikar\AppData\Local\Temp\Rar$DIa15992.18496\CCNA Lab - Static Route - no Configure.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC4
Physical Config Desktop Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address 192.168.20.3
Subnet Mask 255.255.255.0
Default Gateway 192.168.20.1
DNS Server
IPv6 Configuration
DHCP Auto Config Static
IPv6 Address
Link Local Address FE80::2E0:B0FF:FEB9:3325
IPv6 Gateway
IPv6 DNS Server
PC-PT PC1
PC-PT PC3
2950T-24 SW2
192.168.30.1
Fa0/1
Fa0/2
Fa0/3
Time: 03:17:19
Power Cycle Devices Fast Forward Time
Realtime
Routers
Toggle PDU List Window
ENG 15:11

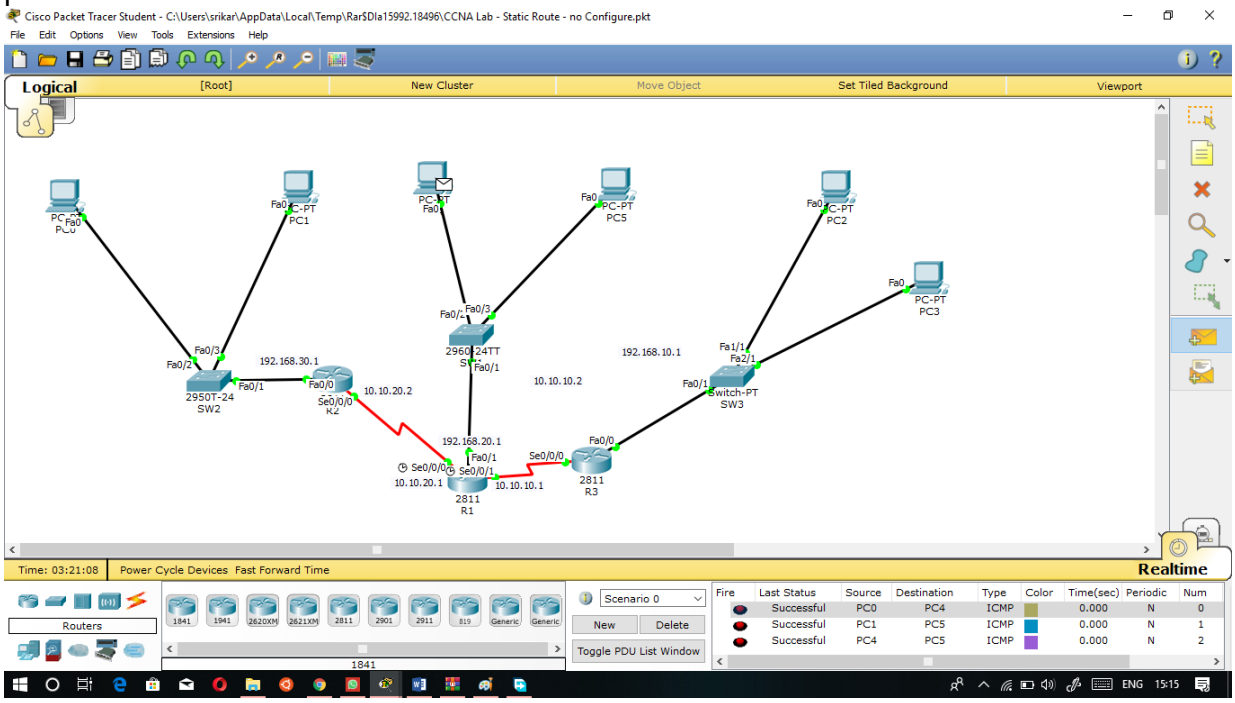

Cisco Packet Tracer Student - C:\Users\srikar\AppData\Local\Temp\Rar$DIa15992.18496\CCNA Lab - Static Route - no Configure.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC5
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address 192.168.20.2
Subnet Mask 255.255.255.0
Default Gateway 192.168.20.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::202:16FF:FE76:7186
IPv6 Gateway
IPv6 DNS Server
PC-PT PC1
PC-PT PC3
2950T-24 SW2
192.168.30.1
Fa0/1
Fa0/2
Fa0/3
Time: 03:17:25
Power Cycle Devices
Fast Forward Time
Realtime
Routers
2811
Toggle PDU List Window
Type
Color
Time(sec)
Periodic
Num
ENG 15:11


Cisco Packet Tracer Student - C:\Users\srikar\AppData\Local\Temp\Rar$DIa15992.18496\CCNA Lab - Static Route - no Configure.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC5
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address 192.168.20.2
Subnet Mask 255.255.255.0
Default Gateway 192.168.20.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::202:16FF:FE76:7186
IPv6 Gateway
IPv6 DNS Server
PC-PT PC1
PC-PT PC3
2950T-24 SW2
192.168.30.1
Fa0/1
Fa0/2
Fa0/3
Time: 03:17:31
Power Cycle Devices
Fast Forward Time
Realtime
Routers
2811
Toggle PDU List Window
Type
Color
Time(sec)
Periodic
Num
ENG 15:11


Cisco Packet Tracer Student - C:\Users\srikar\AppData\Local\Temp\Rar$DIa15992.18496\CCNA Lab - Static Route - no Configure.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address 192.168.10.2
Subnet Mask 255.255.255.0
Default Gateway 192.168.10.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::207:ECFF:FE39:D05B
IPv6 Gateway
IPv6 DNS Server
PC-PT PC1
PC-PT PC3
2950T-24 SW2
192.168.30.1
Fa0/1
Fa0/2
Fa0/3
Time: 03:17:37
Power Cycle Devices
Fast Forward Time
Realtime
Routers
2811
Toggle PDU List Window
Type
Color
Time(sec)
Periodic
Num
ENG 15:11


Cisco Packet Tracer Student - C:\Users\srikar\AppData\Local\Temp\Rar$DIa15992.18496\CCNA Lab - Static Route - no Configure.pkt
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
IP Configuration
DHCP
Static
IP Address 192.168.10.3
Subnet Mask 255.255.255.0
Default Gateway 192.168.10.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address FE80::230:A3FF:FED4:4DEB
IPv6 Gateway
IPv6 DNS Server
PC-PT PC1
PC-PT PC3
2950T-24 SW2
192.168.30.1
Fa0/1
Fa0/2
Fa0/3
Time: 03:17:43
Power Cycle Devices
Fast Forward Time
Realtime
Routers
2811
Toggle PDU List Window
Type
Color
Time(sec)
Periodic
Num
ENG 15:11

Now we have completed given ip's, subnet masks and default gateway to all the pc's



Now check whether packets can transfer between pc's
First packet always fails, so try for second time
I have took ratio, so In real life, switch 2 is connected to 20 pc's(1st floor),switch 1 is connected to 2nd floor which contains 20 pc's, and switch 3 is connected to 3rd floor which contains 20 pc's. Each floor is working in different sectors in the same offfice.

---END---

Project 5

College Network using EIGRP

EIGRP Overview

EIGRP is a Cisco proprietary routing protocol loosely based on their original IGRP (Interior Routing Protocol). EIGRP is an advanced distance-vector routing protocol, it can only use it in an all-Cisco network, but EIGRP more than makes up for this deficiency by being easy to configure, fast, and reliable.

Like RIP, EIGRP is based on a distance vector algorithm that determines the best path to a destination. But EIGRP uses a more complex metric than RIP's simple hop count. The EIGRP metric is based on the minimum bandwidth and net delay along each possible path, which means that EIGRP can accommodate larger networks than RIP.

Cisco included so many useful features such as automatic two-way redistribution that make the migration from IGRP to EIGRP relatively straightforward.

EIGRP operates very efficiently over large networks. It achieves this efficiency in part by sending non-periodic updates. This means that, unlike RIP, EIGRP only distributes information about routes that have changed, and only when there is a change to report. The rest of the time, routers only exchange small "Hello" packets to verify that routing peers are still available. So, in a relatively stable network, EIGRP uses very little bandwidth. This is especially useful in WAN configurations.

It is also extremely efficient over LAN portions of a network. On each network segment, routers exchange routing information using multicast packets, which helps to limit bandwidth usage on segments that hold many routers.

Every router in an EIGRP network includes a topology table, which is a central feature of the DUAL algorithm. Every time a router receives a new piece of routing information from one of its neighbors, it updates the topology table. This helps to give it a reliable and up-to-date image of all of the connections in the network that are currently in use. Every destination subnet known to EIGRP appears in the topology table.

EIGRP includes many of the features such as Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Masks (VLSM) that are needed in larger networks.

Features of EIGRP

EIGRP is an advanced distance vector or hybrid routing protocol that includes the following features:

Rapid convergence: EIGRP uses the Diffusing Update Algorithm (DUAL) to achieve rapid convergence. A router that uses EIGRP stores all available backup routes for destinations so that it can quickly adapt to alternate routes. If no appropriate route or

backup route exists in the local routing table, EIGRP queries its neighbors to discover an alternate route.

Reduced bandwidth usage: EIGRP does not make periodic updates. Instead, it sends partial updates when the path or the metric changes for that route. When path information changes, DUAL sends an update about only that link rather than about the entire table.

Classless routing: Because EIGRP is a classless routing protocol, it advertises a routing mask for each destination network. The routing mask feature enables EIGRP to support discontiguous subnetworks and variable-length subnet masks (VLSM).

Multiple network layer support: EIGRP supports AppleTalk, IP version 4 (IPv4), IP version 6 (IPv6), and Novell Internetwork Packet Exchange (IPX), which use protocol-dependent modules (PDM). PDMs are responsible for protocol requirements that are specific to the network layer.

Less overhead: EIGRP uses multicast and unicast rather than broadcast. As a result, end stations are unaffected by routing updates and requests for topology information.

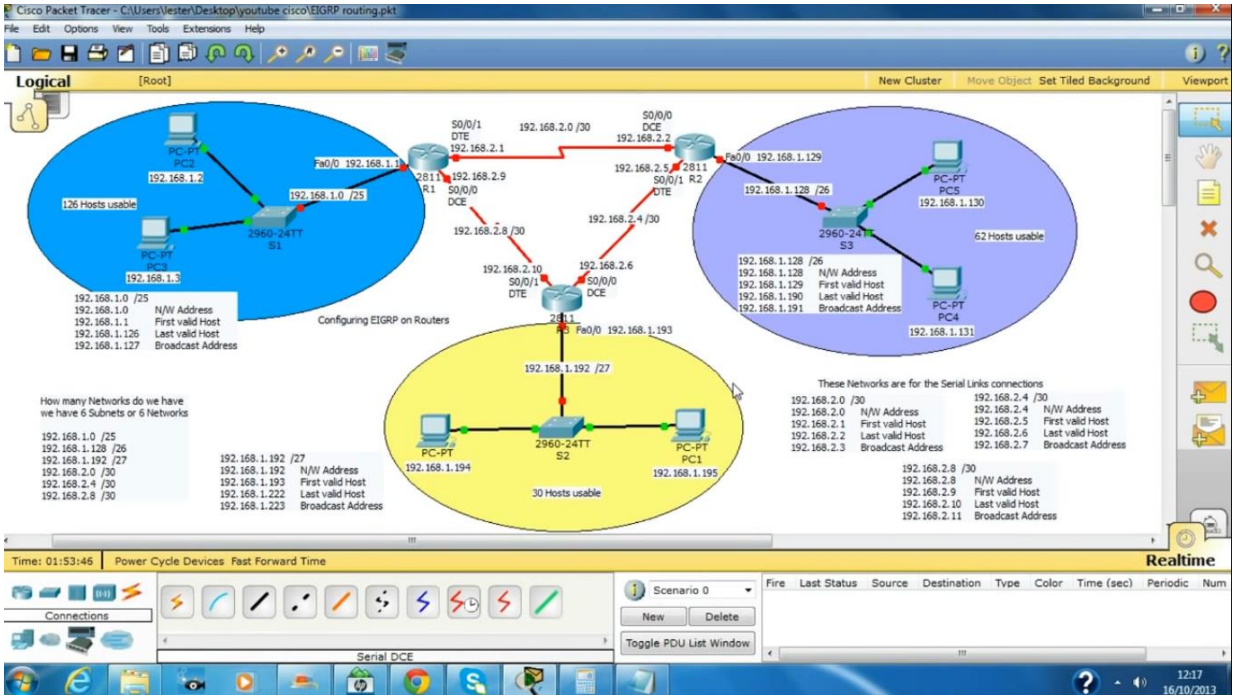
Load balancing: EIGRP supports unequal metric load balancing, which allows administrators to better distribute traffic flow in their networks.

Easy summarization: EIGRP enables administrators to create summary routes anywhere within the network rather than rely on the traditional distance vector approach of performing classful route summarization only at major network boundaries.

Software used: cisco packet tracer

Procedure :

First create a network as shown in the below screenshot



To configure EIGRP on a network use the following command

Configuration:-

For class full addresses:-

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router eigrp 1
R1(config-router)#network <I.P address>
R1(config-router)#network <I.P address>
R1(config-router)#network <I.P address>
R1(config-router)#
R1(config-router)#exit
R1(config)#
R1#

R1#copy running-config startup-config
```

For class-less address:-

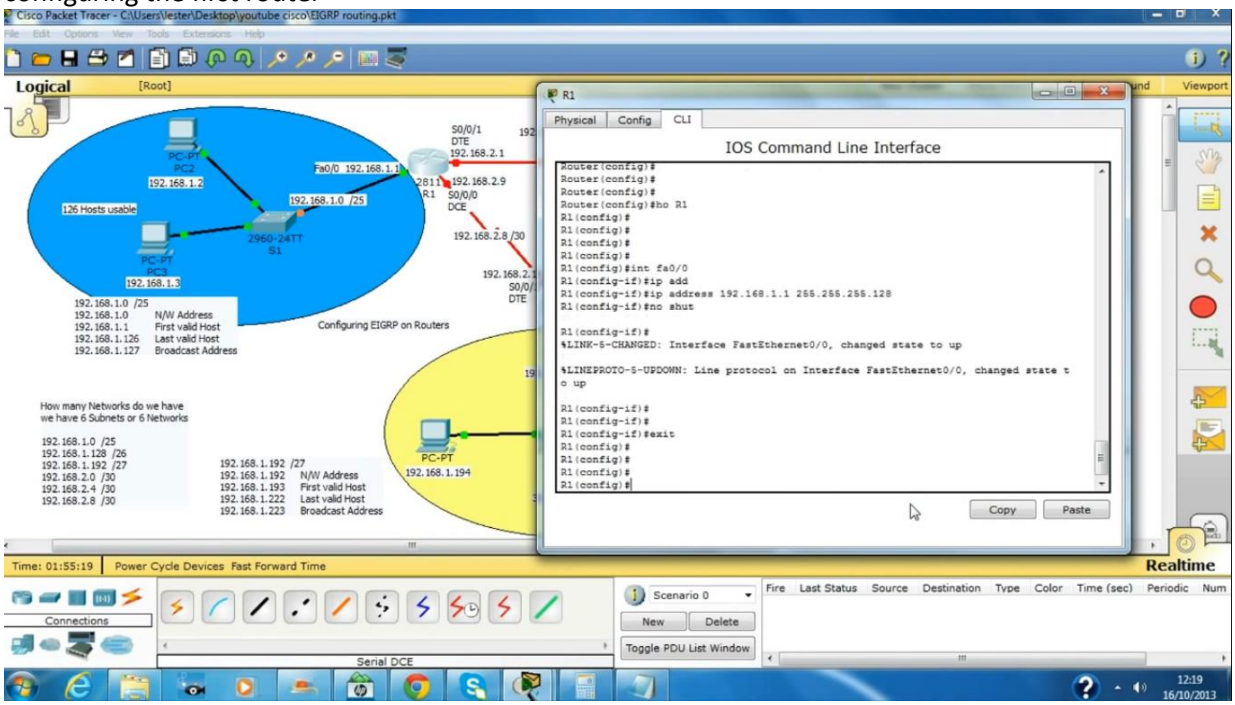
```
R1(config)#router eigrp 1
R1(config-router)#network <I.P address> <Wildcard mask>
R1(config-router)#network <I.P address> <Wildcard mask>
R1(config-router)#network <I.P address> <Wildcard mask>
R1(config-router)#no auto-summary
R1(config-router)#exit
R1(config)#
```

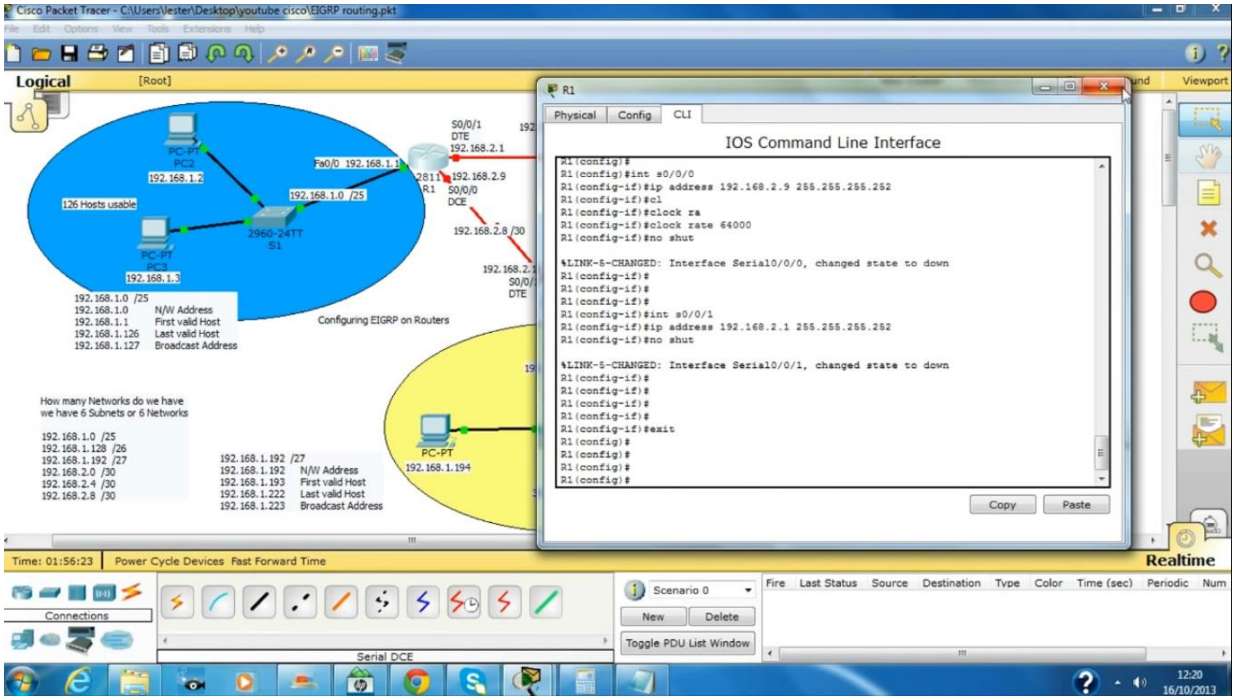
```
show ip eigrp neighbors : to ckeck neighbor table
show ip eigrp topology  : to check topology table
show ip route           : to check routing table
```

`debug eigrp packets : to check hello events`

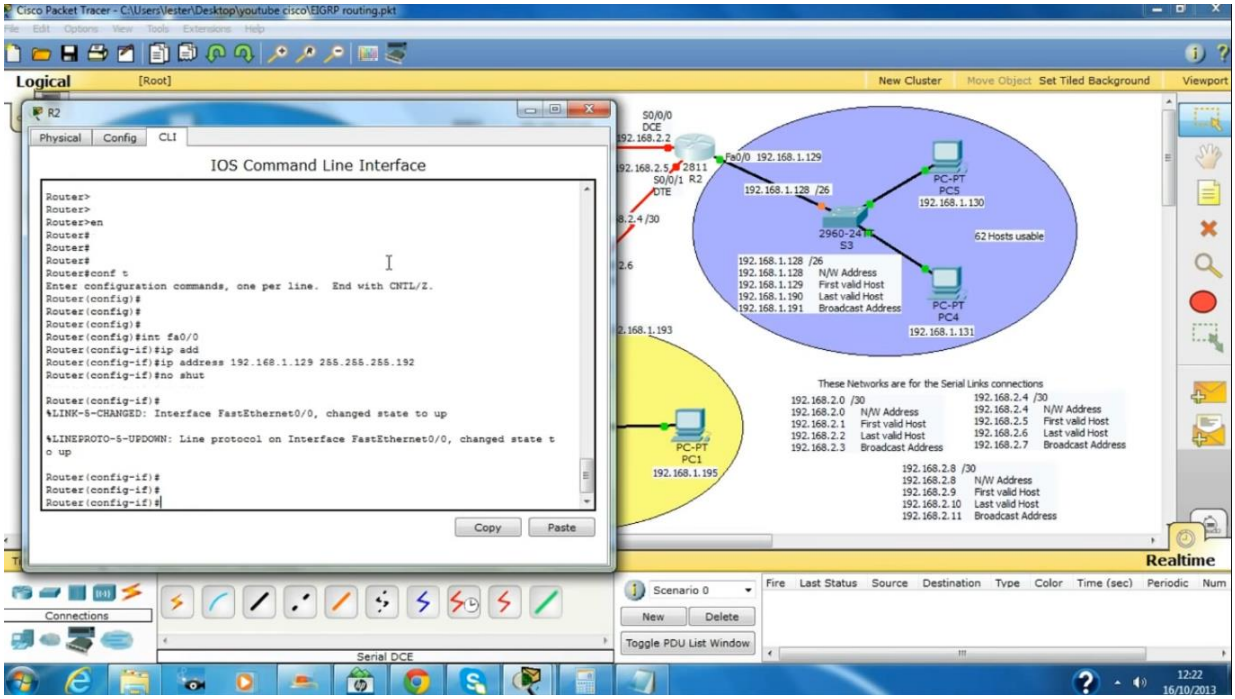
debug ip rip : hello events in RIP

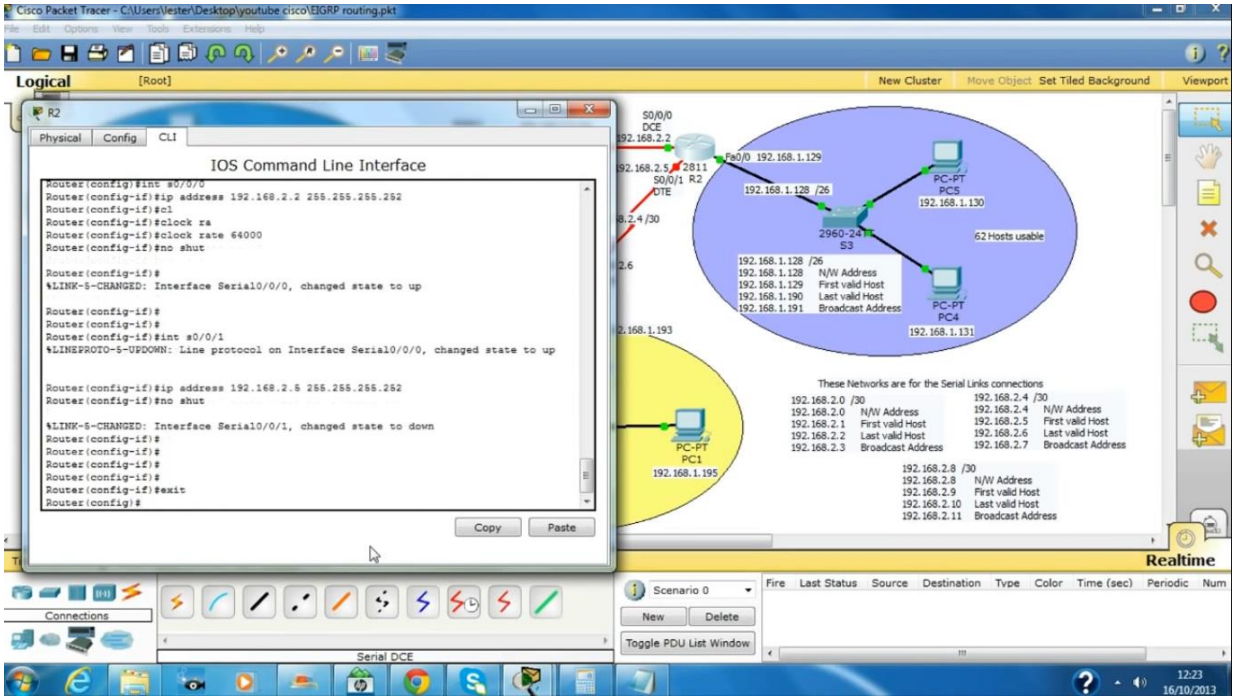
as shown in the above commands I have done the same in the below screen shots
configuring the first router

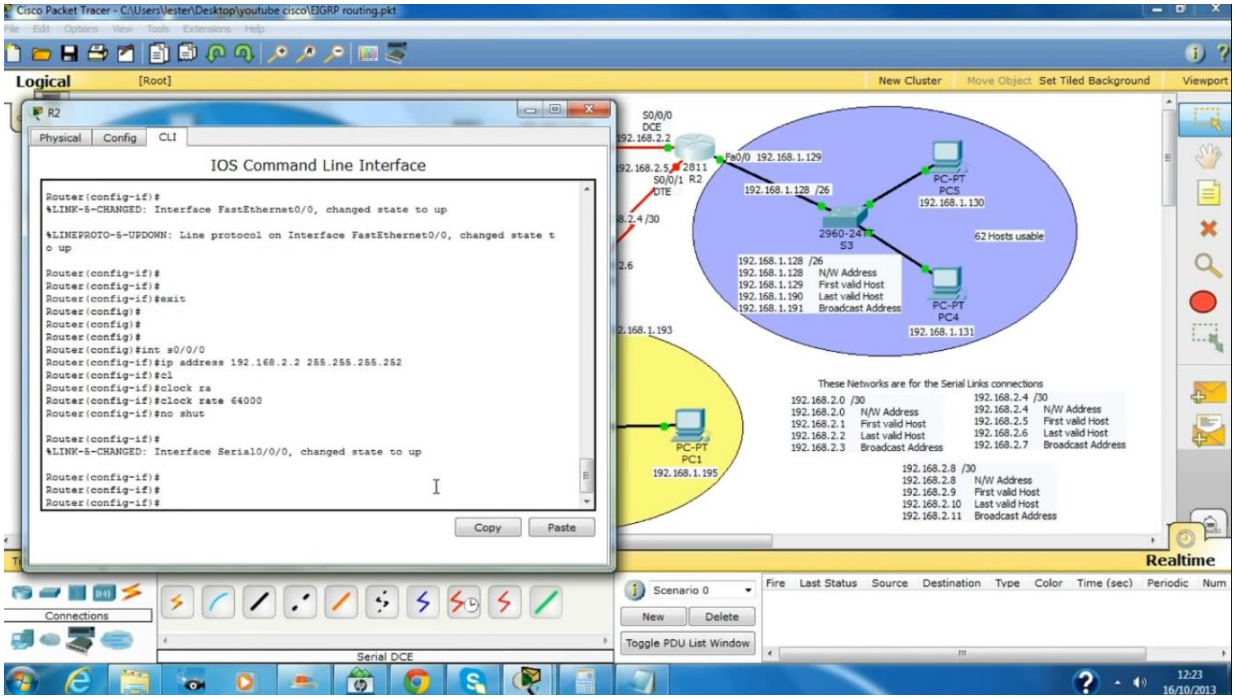




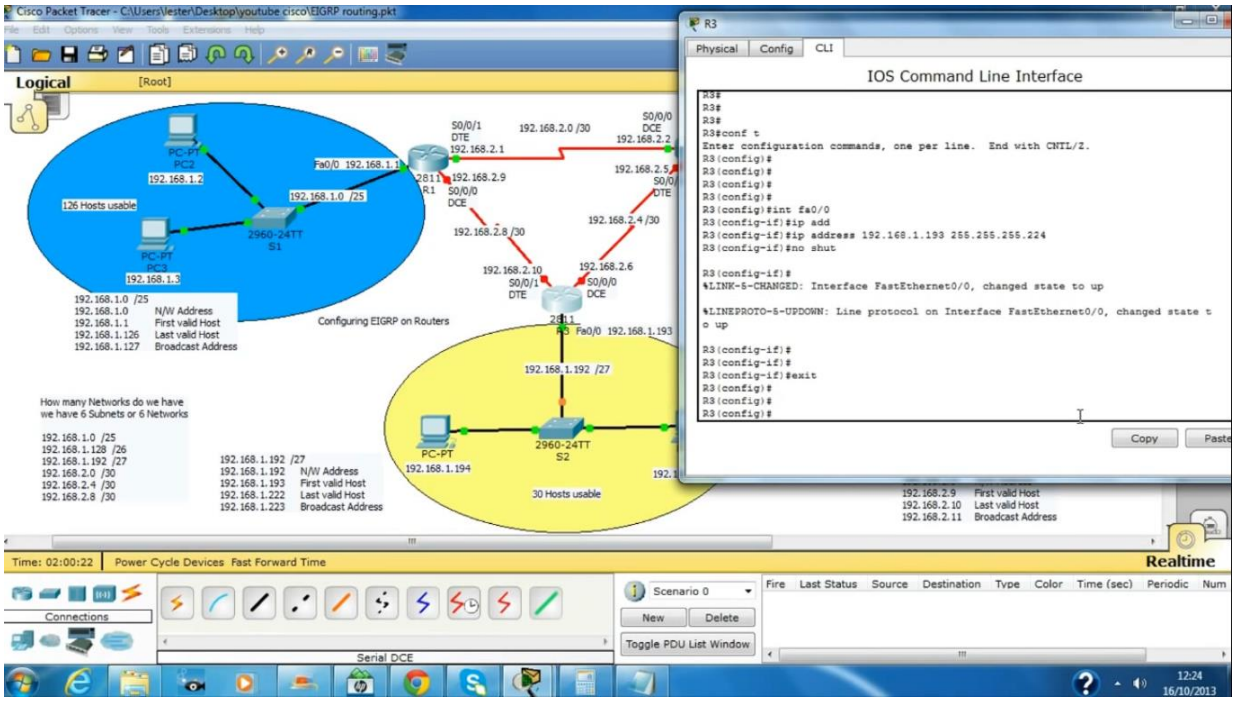
Now configuring second router as followes

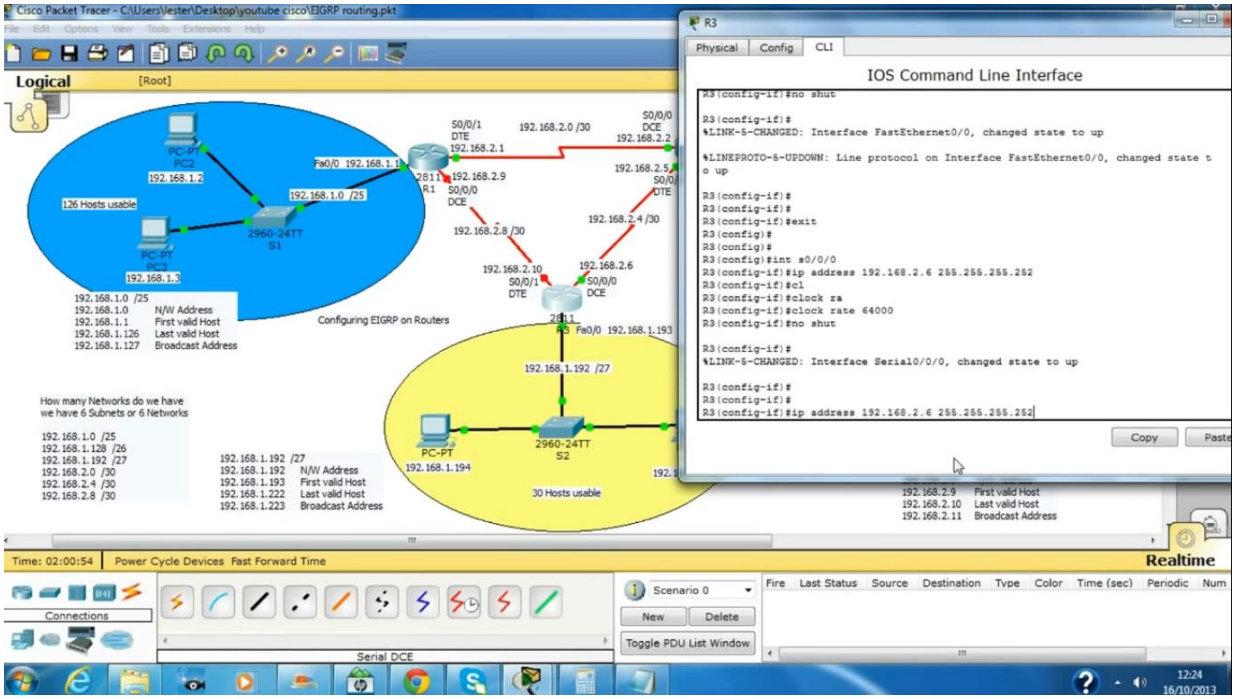

Cisco Packet Tracer - C:\Users\lester\Desktop\youtube cisco\EIGRP routing.pkt
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
R2
Physical
Config
CLI
IOS Command Line Interface
Router>
Router>
Router>en
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip add
Router(config-if)#ip address 192.168.1.129 255.255.255.192
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
Router(config-if)#
Router(config-if)#
Router(config-if)#
Copy
Paste
S0/0/0
DCE
192.168.2.2
192.168.2.5
2811
S0/0/1 R2
DTE
Fa0/0 192.168.1.129
192.168.1.128 /26
PC-PT
PC5
192.168.1.130
2960-24TT
S3
62 Hosts usable
192.168.1.128 /26
192.168.1.128 N/W Address
192.168.1.129 First valid Host
192.168.1.190 Last valid Host
192.168.1.191 Broadcast Address
PC-PT
PC4
192.168.1.131
192.168.1.193
PC-PT
PC1
192.168.1.195
These Networks are for the Serial Links connections
192.168.2.0 /30
192.168.2.0 N/W Address
192.168.2.1 First valid Host
192.168.2.2 Last valid Host
192.168.2.3 Broadcast Address
192.168.2.4 /30
192.168.2.4 N/W Address
192.168.2.5 First valid Host
192.168.2.6 Last valid Host
192.168.2.7 Broadcast Address
192.168.2.8 /30
192.168.2.8 N/W Address
192.168.2.9 First valid Host
192.168.2.10 Last valid Host
192.168.2.11 Broadcast Address
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
Connections
Serial DCE
12:22
16/10/2013

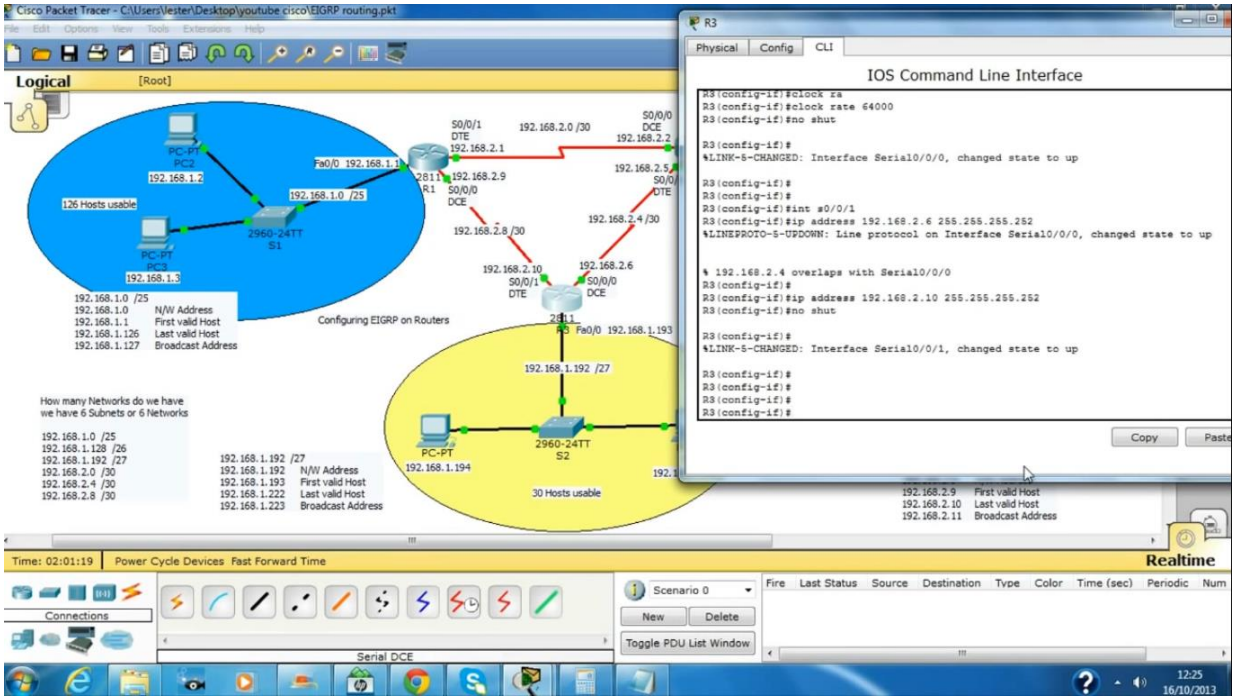

Cisco Packet Tracer - C:\Users\lester\Desktop\youtube cisco\EIGRP routing.pkt
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
R2
Physical
Config
CLI
IOS Command Line Interface
Router(config)#int s0/0/0
Router(config-if)#ip address 192.168.2.2 255.255.255.252
Router(config-if)#cl
Router(config-if)#clock ra
Router(config-if)#clock rate 64000
Router(config-if)#no shut
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#
Router(config-if)#
Router(config-if)#int s0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Router(config-if)#ip address 192.168.2.5 255.255.255.252
Router(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
Copy
Paste
S0/0/0
DCE
192.168.2.2
192.168.2.5
2811
S0/0/1 R2
DTE
Fa0/0 192.168.1.129
192.168.1.128 /26
PC-PT
PC5
192.168.1.130
2960-24TT
S3
62 Hosts usable
192.168.1.128 /26
192.168.1.128 N/W Address
192.168.1.129 First valid Host
192.168.1.190 Last valid Host
192.168.1.191 Broadcast Address
PC-PT
PC4
192.168.1.131
192.168.1.193
PC-PT
PC1
192.168.1.195
These Networks are for the Serial Links connections
192.168.2.0 /30
192.168.2.0 N/W Address
192.168.2.1 First valid Host
192.168.2.2 Last valid Host
192.168.2.3 Broadcast Address
192.168.2.4 /30
192.168.2.4 N/W Address
192.168.2.5 First valid Host
192.168.2.6 Last valid Host
192.168.2.7 Broadcast Address
192.168.2.8 /30
192.168.2.8 N/W Address
192.168.2.9 First valid Host
192.168.2.10 Last valid Host
192.168.2.11 Broadcast Address
Realtime
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
Connections
Serial DCE
12:23
16/10/2013



Now we are configuring the last router (R3)
It is also shown below

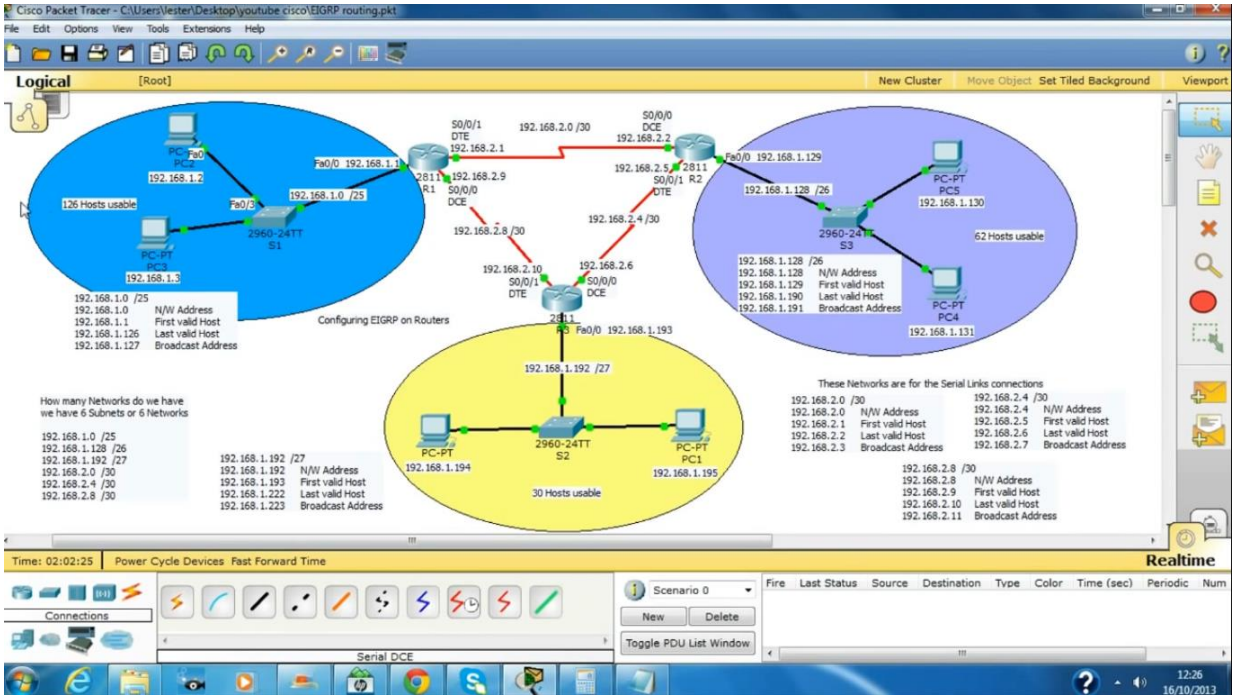




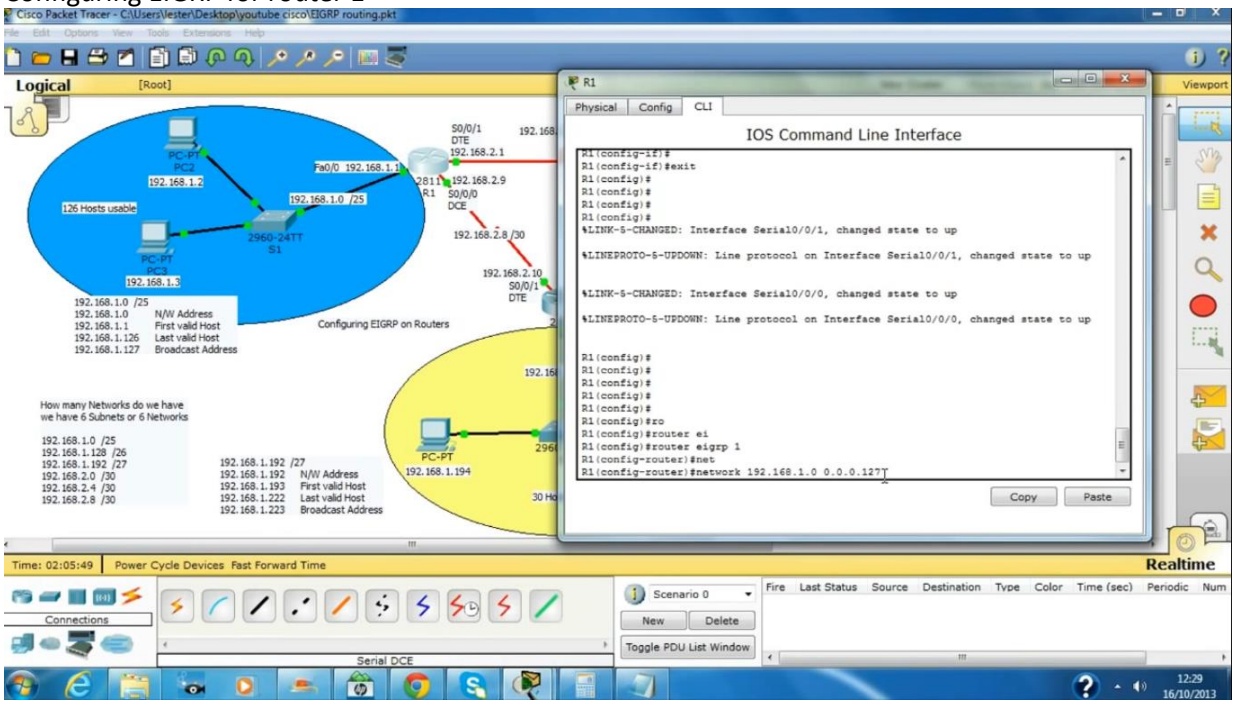


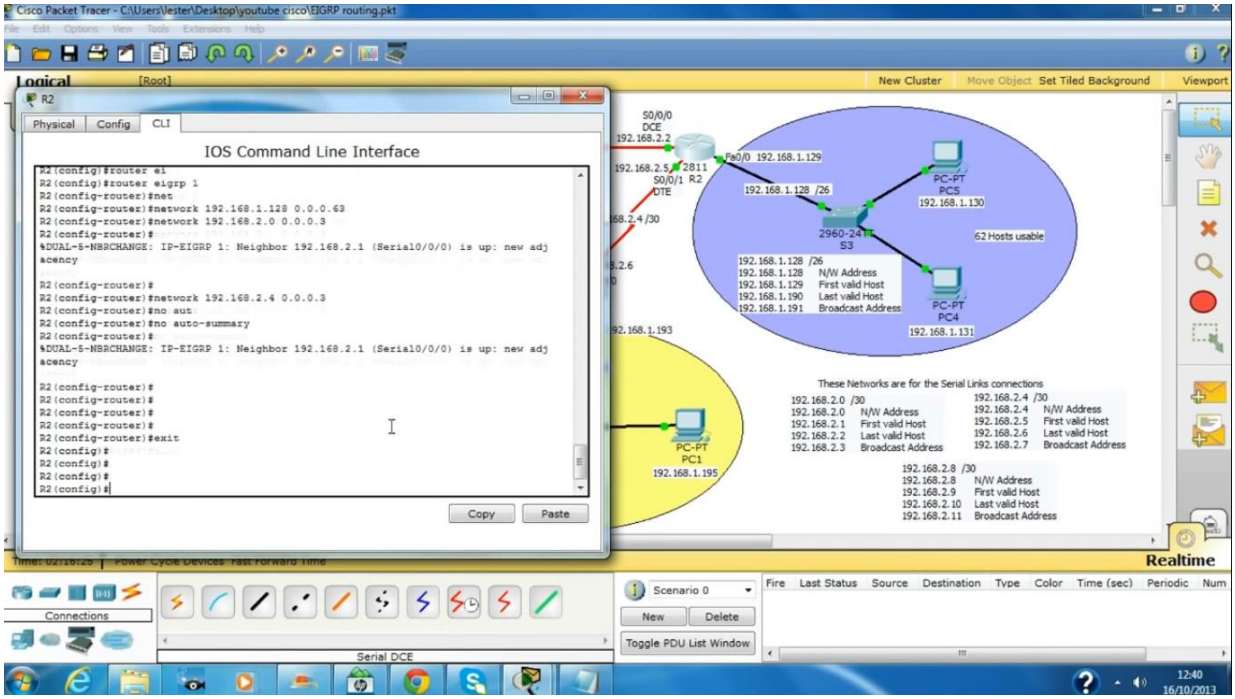
Now as you can see that all the connections are in green colour and we have successfully done

But the last step is we have to do EIGRP protocol

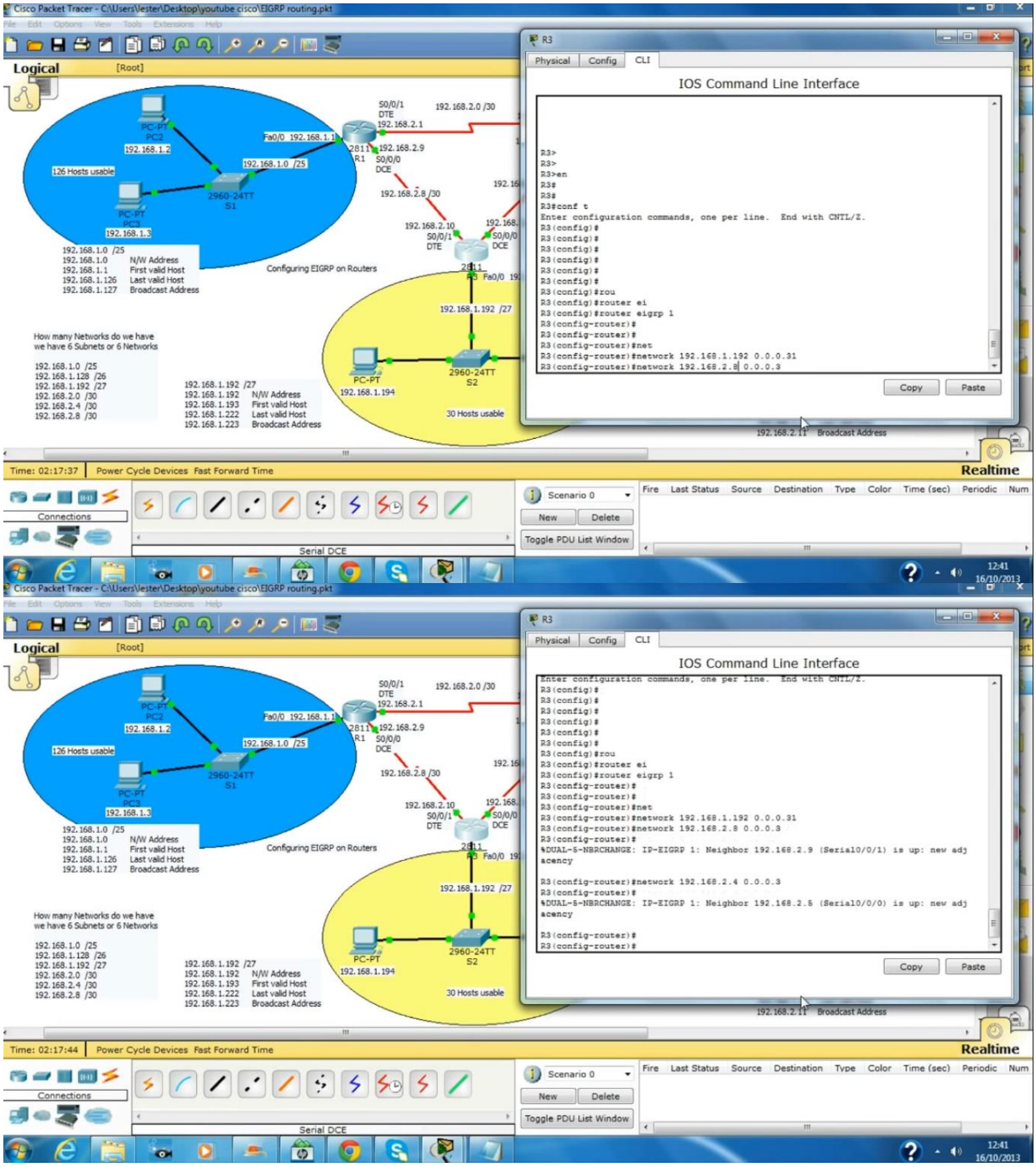


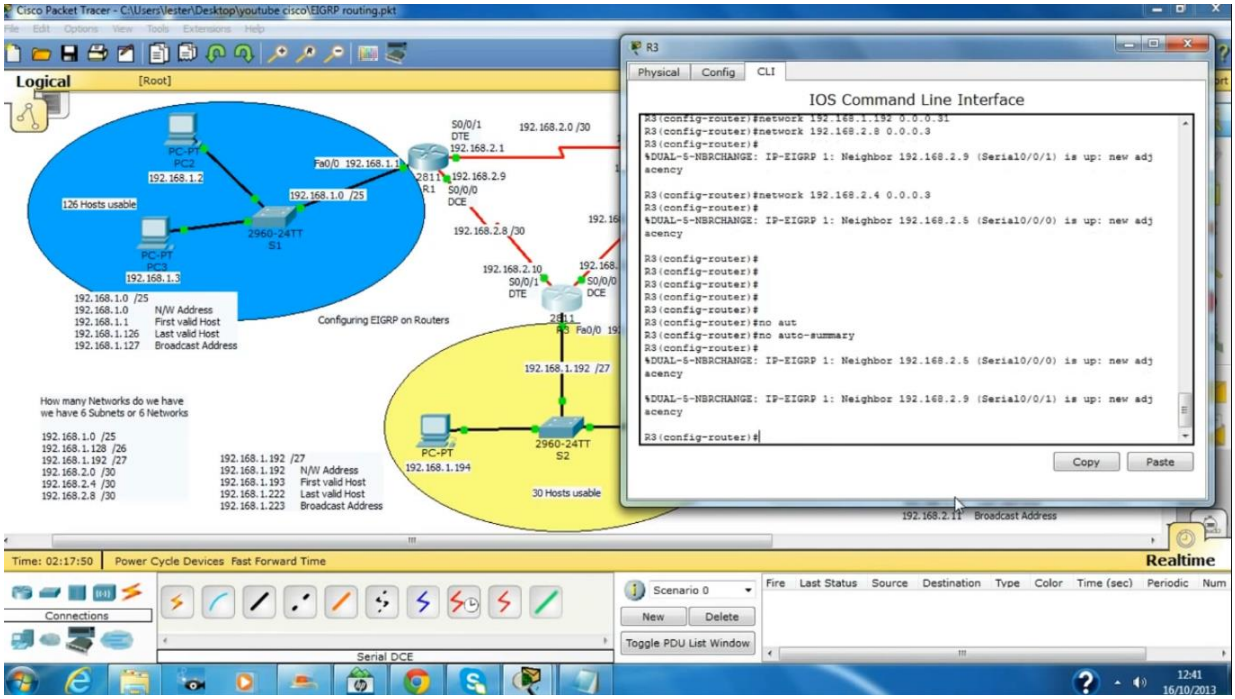
Configuring EIGRP for router 1



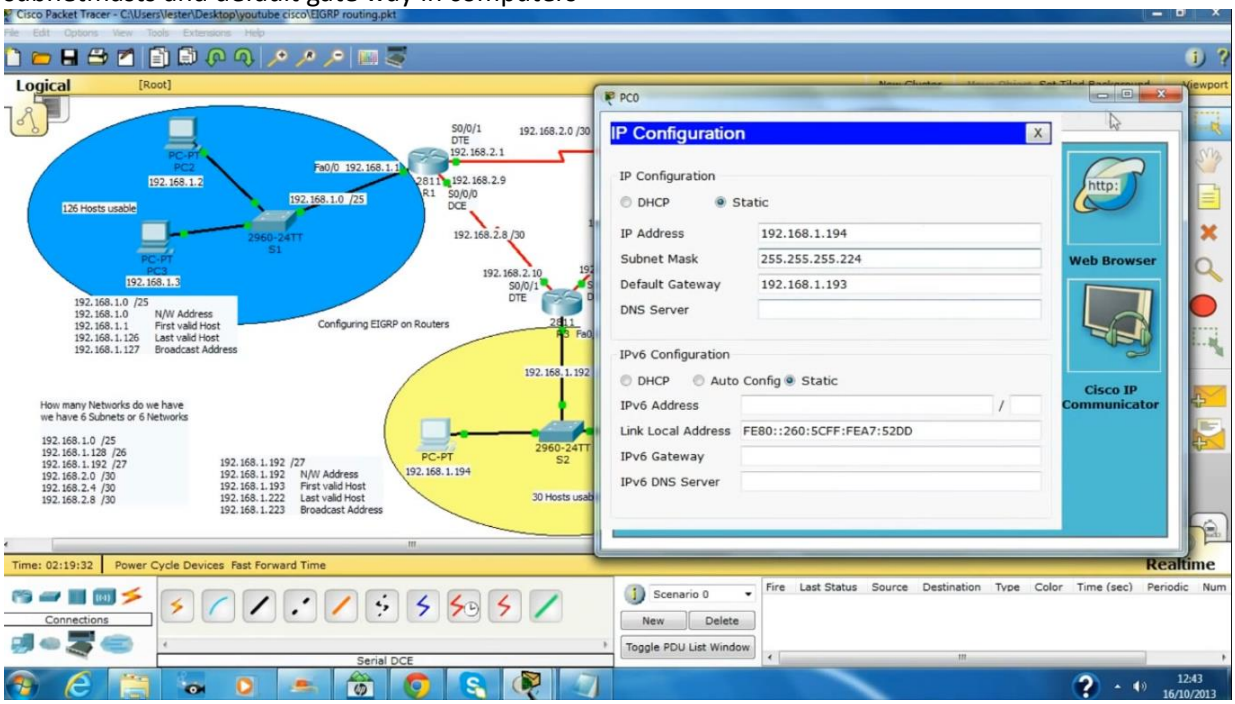


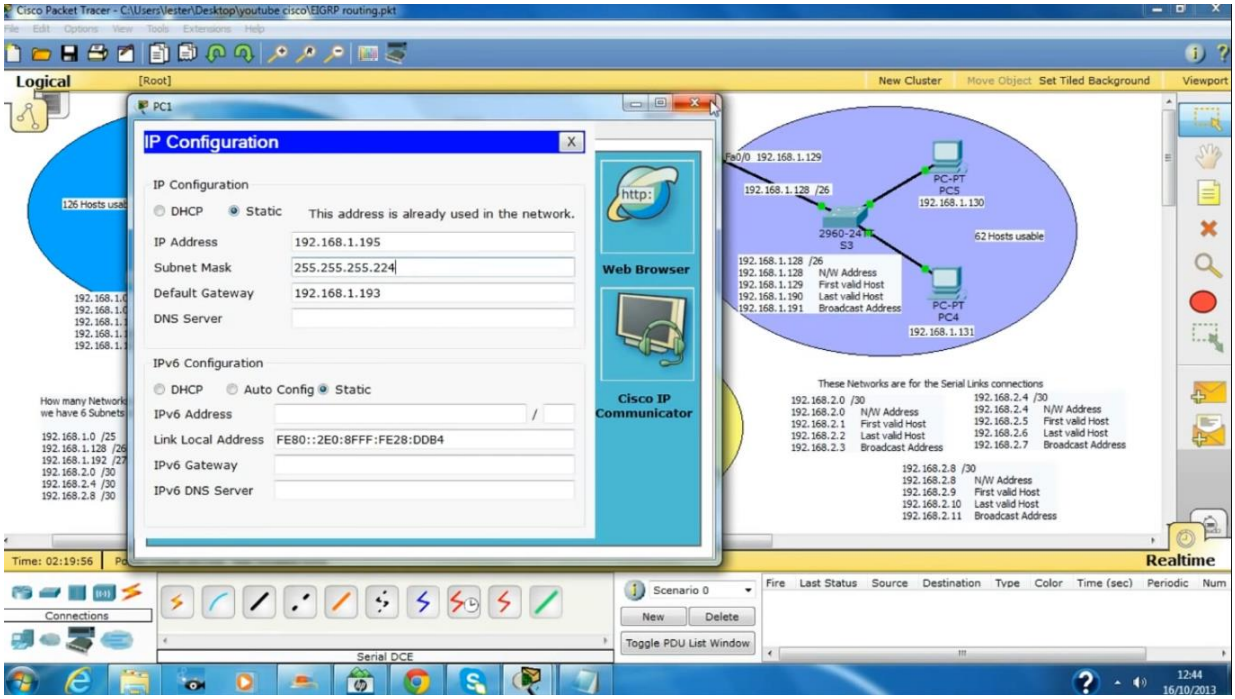
Configuring router 2 in EIGRP

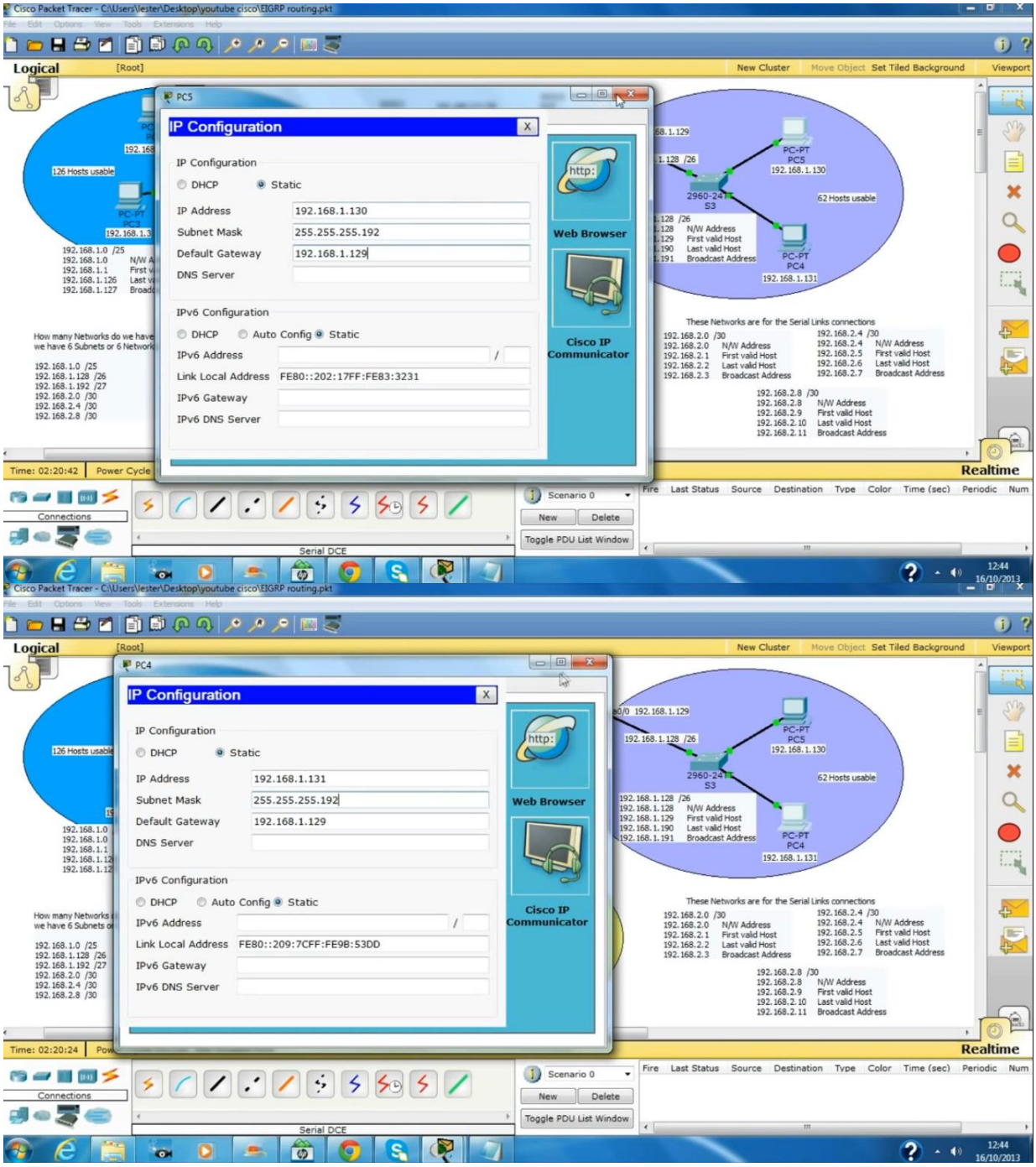

Cisco Packet Tracer - C:\Users\lester\Desktop\youtube cisco\EIGRP routing.pkt
Logical
[Root]
R3
Physical
Config
CLI
IOS Command Line Interface
R3>
R3>
R3>en
R3#
R3#
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#
R3(config)#
R3(config)#
R3(config)#
R3(config)#
R3(config)#rou
R3(config)#router ei
R3(config)#router eigrp 1
R3(config-router)#
R3(config-router)#
R3(config-router)#net
R3(config-router)#network 192.168.1.192 0.0.0.31
R3(config-router)#network 192.168.2.8 0.0.0.3
Copy
Paste
PC-PT
PC2
192.168.1.2
Fa0/0 192.168.1.1
2811
R1
S0/0/1
DTE
192.168.2.1
192.168.2.0 /30
192.168.2.9
S0/0/0
DCE
126 Hosts usable
192.168.1.0 /25
2960-24TT
S1
PC-PT
PC3
192.168.1.3
192.168.2.8 /30
192.168.2.10
S0/0/1
DTE
S0/0/0
DCE
2811
R3
Fa0/0
192.168.1.192 /27
192.168.1.0 /25
N/W Address
First valid Host
Last valid Host
Broadcast Address
192.168.1.1
192.168.1.126
192.168.1.127
Configuring EIGRP on Routers
How many Networks do we have
we have 6 Subnets or 6 Networks
192.168.1.0 /25
192.168.1.128 /26
192.168.1.192 /27
192.168.2.0 /30
192.168.2.4 /30
192.168.2.8 /30
192.168.1.192 /27
192.168.1.192
192.168.1.193
192.168.1.222
192.168.1.223
PC-PT
192.168.1.194
2960-24TT
S2
30 Hosts usable
192.168.2.11
Broadcast Address
Time: 02:17:37
Power Cycle Devices Fast Forward Time
Realtime
Connections
Serial DCE
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
12:41
16/10/2013
Cisco Packet Tracer - C:\Users\lester\Desktop\youtube cisco\EIGRP routing.pkt
Logical
[Root]
R3
Physical
Config
CLI
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#
R3(config)#
R3(config)#
R3(config)#
R3(config)#
R3(config)#rou
R3(config)#router ei
R3(config)#router eigrp 1
R3(config-router)#
R3(config-router)#
R3(config-router)#net
R3(config-router)#network 192.168.1.192 0.0.0.31
R3(config-router)#network 192.168.2.8 0.0.0.3
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.9 (Serial0/0/1) is up: new adj
acency
R3(config-router)#network 192.168.2.4 0.0.0.3
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.5 (Serial0/0/0) is up: new adj
acency
R3(config-router)#
R3(config-router)#
Copy
Paste
PC-PT
PC2
192.168.1.2
Fa0/0 192.168.1.1
2811
R1
S0/0/1
DTE
192.168.2.1
192.168.2.0 /30
192.168.2.9
S0/0/0
DCE
126 Hosts usable
192.168.1.0 /25
2960-24TT
S1
PC-PT
PC3
192.168.1.3
192.168.2.8 /30
192.168.2.10
S0/0/1
DTE
S0/0/0
DCE
2811
R3
Fa0/0
192.168.1.192 /27
192.168.1.0 /25
N/W Address
First valid Host
Last valid Host
Broadcast Address
192.168.1.1
192.168.1.126
192.168.1.127
Configuring EIGRP on Routers
How many Networks do we have
we have 6 Subnets or 6 Networks
192.168.1.0 /25
192.168.1.128 /26
192.168.1.192 /27
192.168.2.0 /30
192.168.2.4 /30
192.168.2.8 /30
192.168.1.192 /27
192.168.1.192
192.168.1.193
192.168.1.222
192.168.1.223
PC-PT
192.168.1.194
2960-24TT
S2
30 Hosts usable
192.168.2.11
Broadcast Address
Time: 02:17:44
Power Cycle Devices Fast Forward Time
Realtime
Connections
Serial DCE
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
12:41
16/10/2013



And do the same for other routers
If you want this in EIGRP version 2, Then simply write 2 in place of in above commands
Now we have successfully done with the routers, So now we have to configure ip addresses, subnetmasts and default gate way in computers



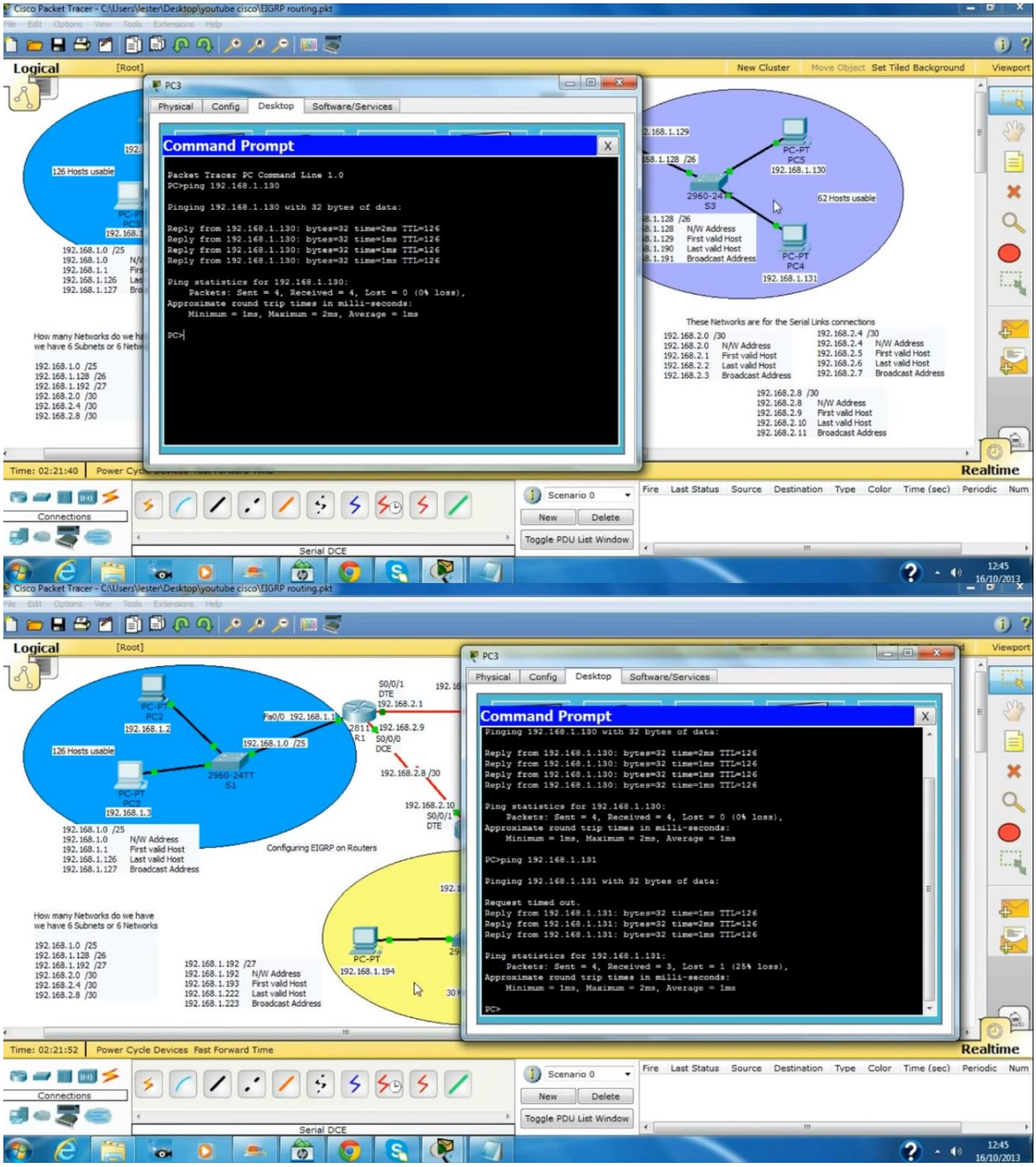

Cisco Packet Tracer - C:\Users\lester\Desktop\youtube cisco\EIGRP routing.pkt
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
PC1
IP Configuration
IP Configuration
DHCP
Static
This address is already used in the network.
IP Address
192.168.1.195
Subnet Mask
255.255.255.224
Default Gateway
192.168.1.193
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::2E0:8FFF:FE28:DDB4
IPv6 Gateway
IPv6 DNS Server
Web Browser
Cisco IP Communicator
Fa0/0 192.168.1.129
192.168.1.128 /26
PC-PT PC5
192.168.1.130
2960-24TT S3
62 Hosts usable
192.168.1.128 /26
192.168.1.128 N/W Address
192.168.1.129 First valid Host
192.168.1.190 Last valid Host
192.168.1.191 Broadcast Address
PC-PT PC4
192.168.1.131
These Networks are for the Serial Links connections
192.168.2.0 /30
192.168.2.0 N/W Address
192.168.2.1 First valid Host
192.168.2.2 Last valid Host
192.168.2.3 Broadcast Address
192.168.2.4 /30
192.168.2.4 N/W Address
192.168.2.5 First valid Host
192.168.2.6 Last valid Host
192.168.2.7 Broadcast Address
192.168.2.8 /30
192.168.2.8 N/W Address
192.168.2.9 First valid Host
192.168.2.10 Last valid Host
192.168.2.11 Broadcast Address
How many Networks we have 6 Subnets
192.168.1.0 /25
192.168.1.128 /26
192.168.1.192 /27
192.168.2.0 /30
192.168.2.4 /30
192.168.2.8 /30
Time: 02:19:56
Realtime
Connections
Serial DCE
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time (sec)
Periodic
Num
12:44
16/10/2013

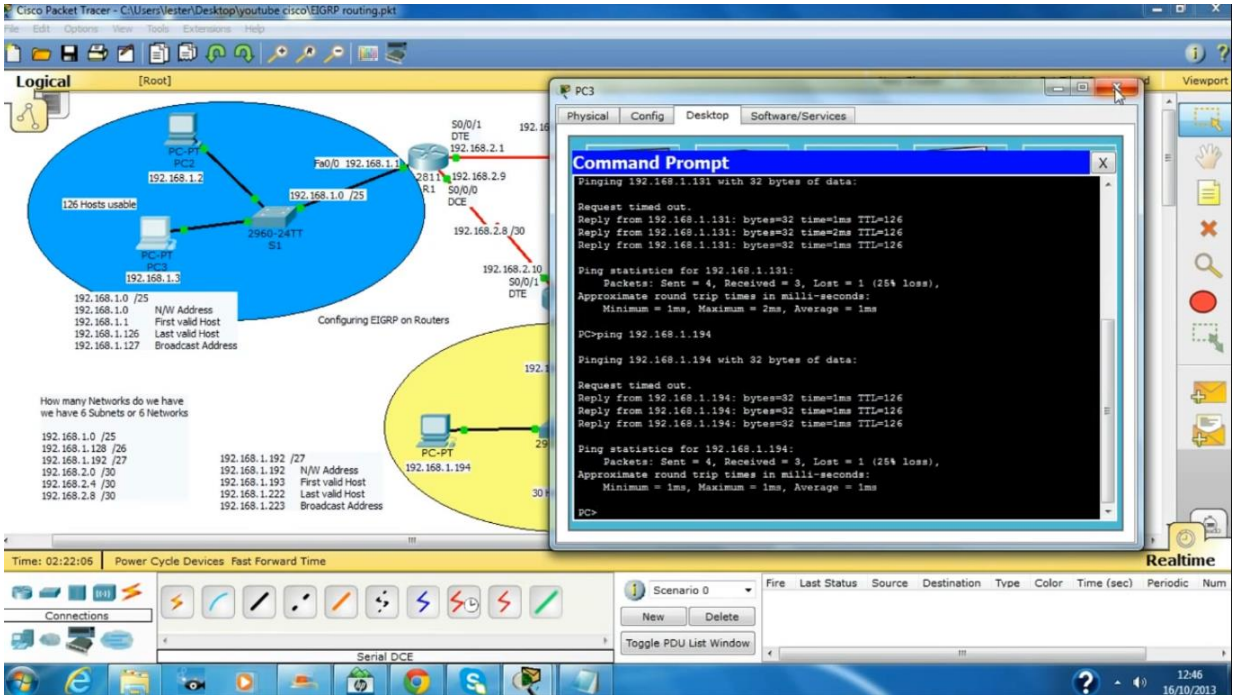


Now we have successfully completed.

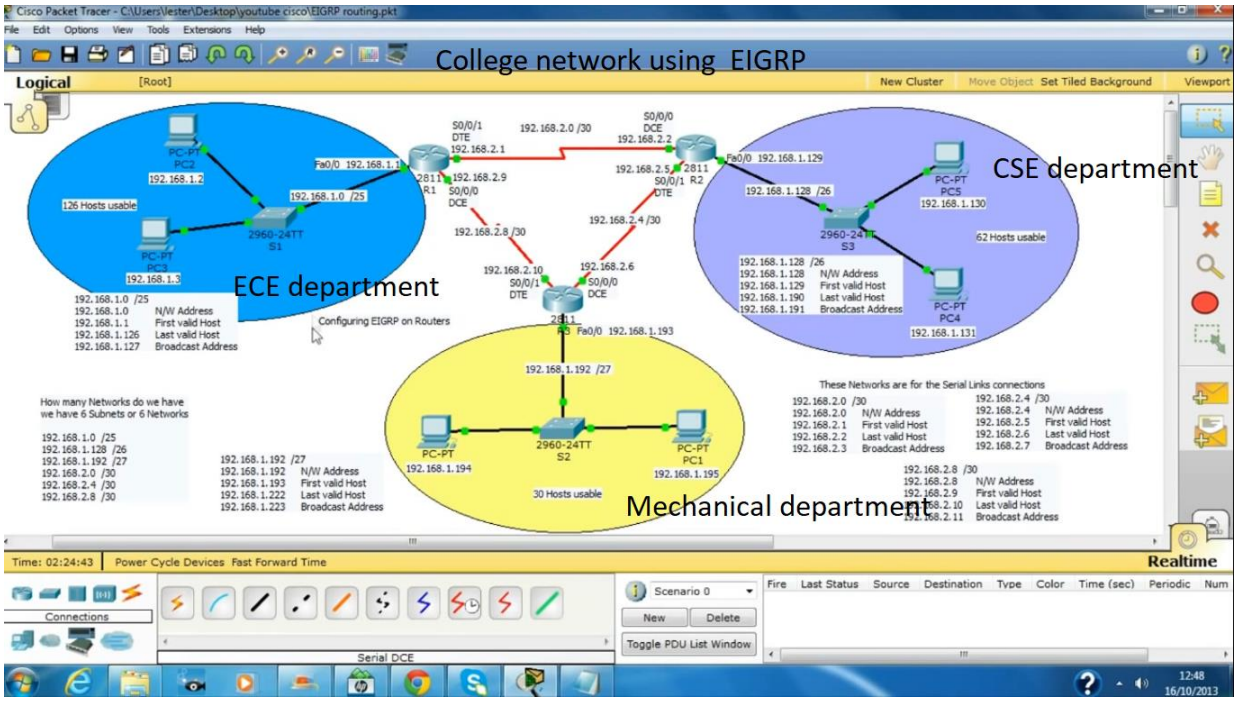
Now check wheather every thing were fine

So that I use ping to check connectivity between the computers


Cisco Packet Tracer - C:\Users\lester\Desktop\youtube cisco\EIGRP routing.pkt
Logical
[Root]
PC3
Physical
Config
Desktop
Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.130
Pinging 192.168.1.130 with 32 bytes of data:
Reply from 192.168.1.130: bytes=32 time=2ms TTL=126
Reply from 192.168.1.130: bytes=32 time=1ms TTL=126
Reply from 192.168.1.130: bytes=32 time=1ms TTL=126
Reply from 192.168.1.130: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.130:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>
126 Hosts usable
62 Hosts usable
2960-24TT
S3
PC-PT
PC5
192.168.1.130
PC-PT
PC4
192.168.1.131
These Networks are for the Serial Links connections
Time: 02:21:40
Realtime
Connections
Serial DCE
Scenario 0
New
Delete
Toggle PDU List Window
12:45
16/10/2013
Cisco Packet Tracer - C:\Users\lester\Desktop\youtube cisco\EIGRP routing.pkt
Logical
[Root]
PC3
Physical
Config
Desktop
Software/Services
Command Prompt
Pinging 192.168.1.130 with 32 bytes of data:
Reply from 192.168.1.130: bytes=32 time=2ms TTL=126
Reply from 192.168.1.130: bytes=32 time=1ms TTL=126
Reply from 192.168.1.130: bytes=32 time=1ms TTL=126
Reply from 192.168.1.130: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.130:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>ping 192.168.1.131
Pinging 192.168.1.131 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.131: bytes=32 time=1ms TTL=126
Reply from 192.168.1.131: bytes=32 time=2ms TTL=126
Reply from 192.168.1.131: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.131:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
PC>
126 Hosts usable
2960-24TT
S1
2811
R1
PC-PT
PC2
192.168.1.2
PC-PT
PC3
192.168.1.3
PC-PT
192.168.1.194
192.168.1.0 /25
192.168.1.0 N/W Address
192.168.1.1 First valid Host
192.168.1.126 Last valid Host
192.168.1.127 Broadcast Address
192.168.1.192 /27
192.168.1.192 N/W Address
192.168.1.193 First valid Host
192.168.1.222 Last valid Host
192.168.1.223 Broadcast Address
Configuring EIGRP on Routers
How many Networks do we have
we have 6 Subnets or 6 Networks
192.168.1.0 /25
192.168.1.128 /26
192.168.1.192 /27
192.168.2.0 /30
192.168.2.4 /30
192.168.2.8 /30
Time: 02:21:52
Power Cycle Devices Fast Forward Time
Realtime
Connections
Serial DCE
Scenario 0
New
Delete
Toggle PDU List Window
12:45
16/10/2013



So we get success!!!



As we cannot take every computer In a college network I took 2 computers in each department as our college has about 200 computers in every department I took 1/100th ratio of it and I have tried it in a cisco packet tracer

---END---

Project 6

Creating Virtual Local-Area Network

A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.

Higher-end switches allow the functionality and implementation of VLANs. The purpose of implementing a VLAN is to improve the performance of a network or apply appropriate security feature

Configuration –

We can simply create VLANs by simply assigning the vlan-id and Vlan name.

```
#switch1(config)#vlan 2

#switch1(config-vlan)#vlan accounts
```

Here, 2 is the Vlan I'd and accounts is the Vlan name. Now, we assign Vlan to the switch ports.e.g-

```
Switch(config)#int <Interphase name>

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access Vlan 2
```

Also, switchport range can be assigned to required vlans.

```
Switch(config)#int range <Interphase name>

Switch(config-if)#switchport mode access

Switch(config-if) #switchport access Vlan 2
```

Assigning IP address to the PC's. Now, we will create Vlan 2 and 3 or etc.. on switch.

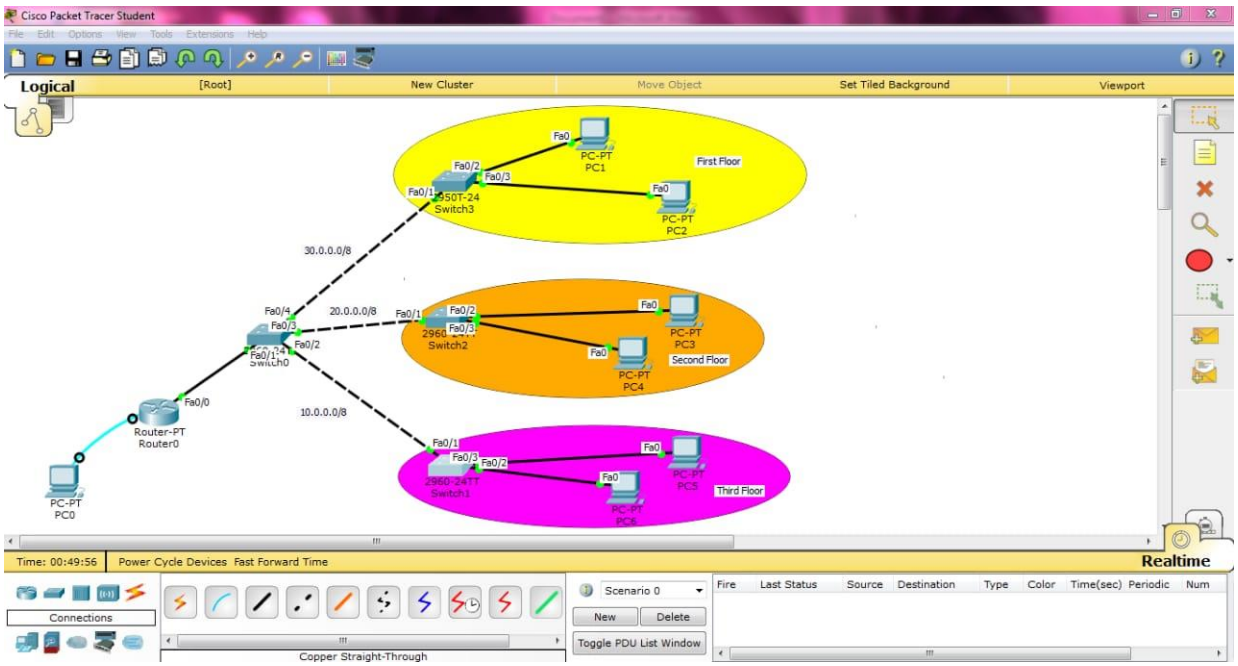
```
Switch(config)#vlan 2

Switch(config)#vlan 3
```

We have made VLANs but the most important part is to assign switch ports to the VLANs .

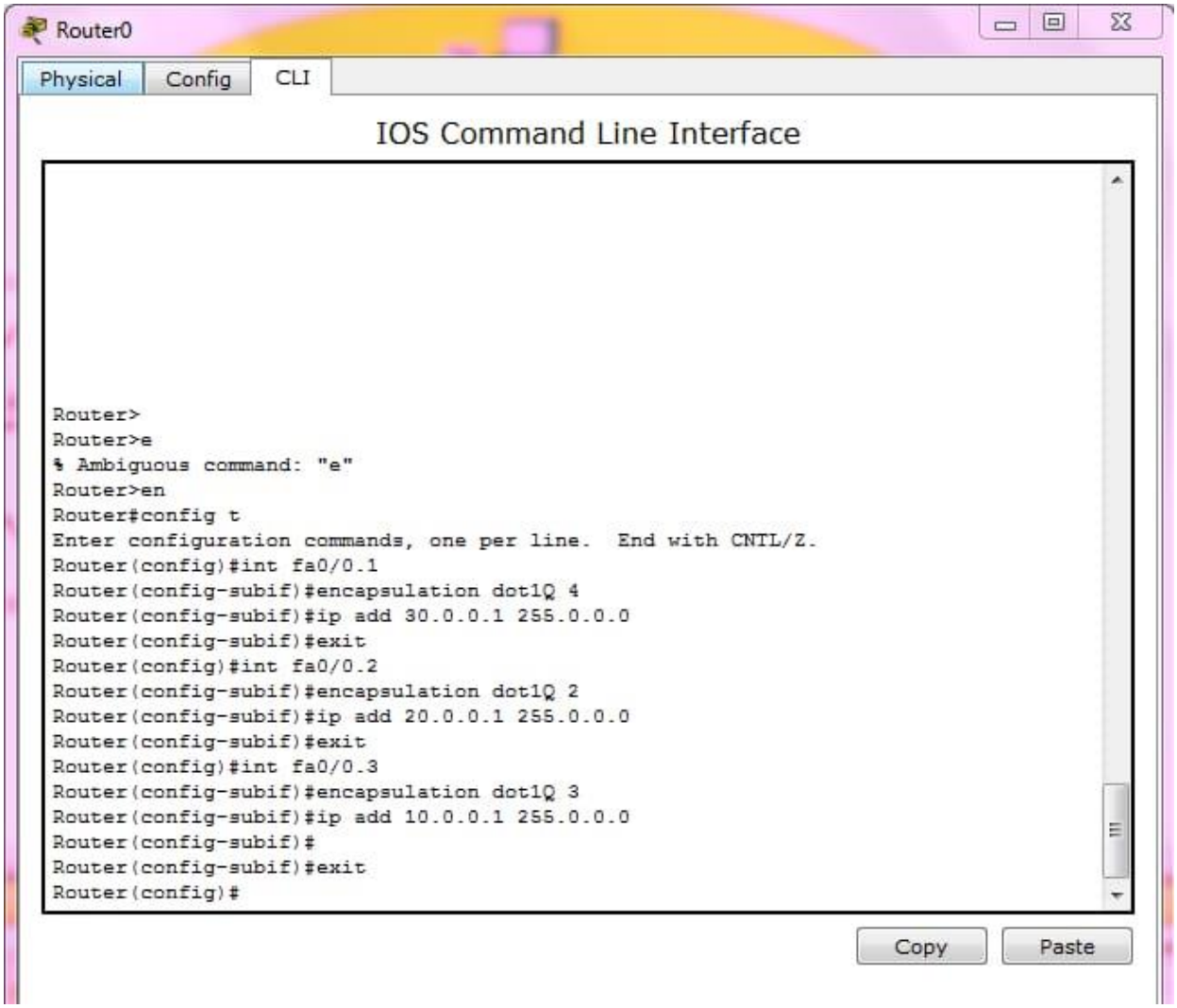
```
Switch(config)#int <Interphase name>
Switch(config-if)#switchport mode access
Switch(config-if) #switchport access Vlan 2

Switch(config)# <Interphase name>
Switch(config-if)#switchport mode access
Switch(config-if) #switchport access Vlan 3

Switch(config)#int <Interphase name>
Switch(config-if)#switchport mode access
Switch(config-if) #switchport access Vlan 2
```

Software used: Cisco packet tracer

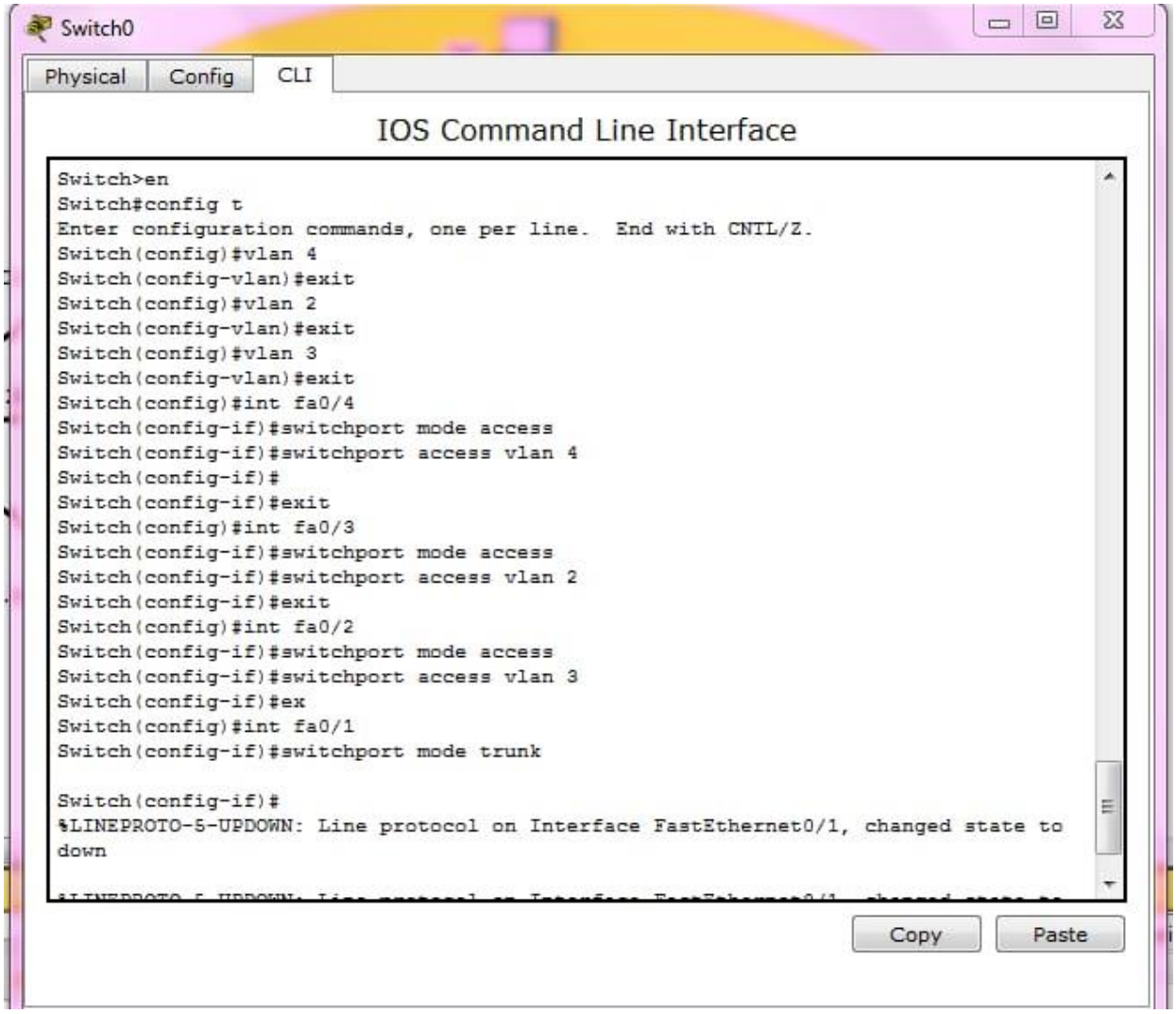
Procedure:
Now create a network as shown below



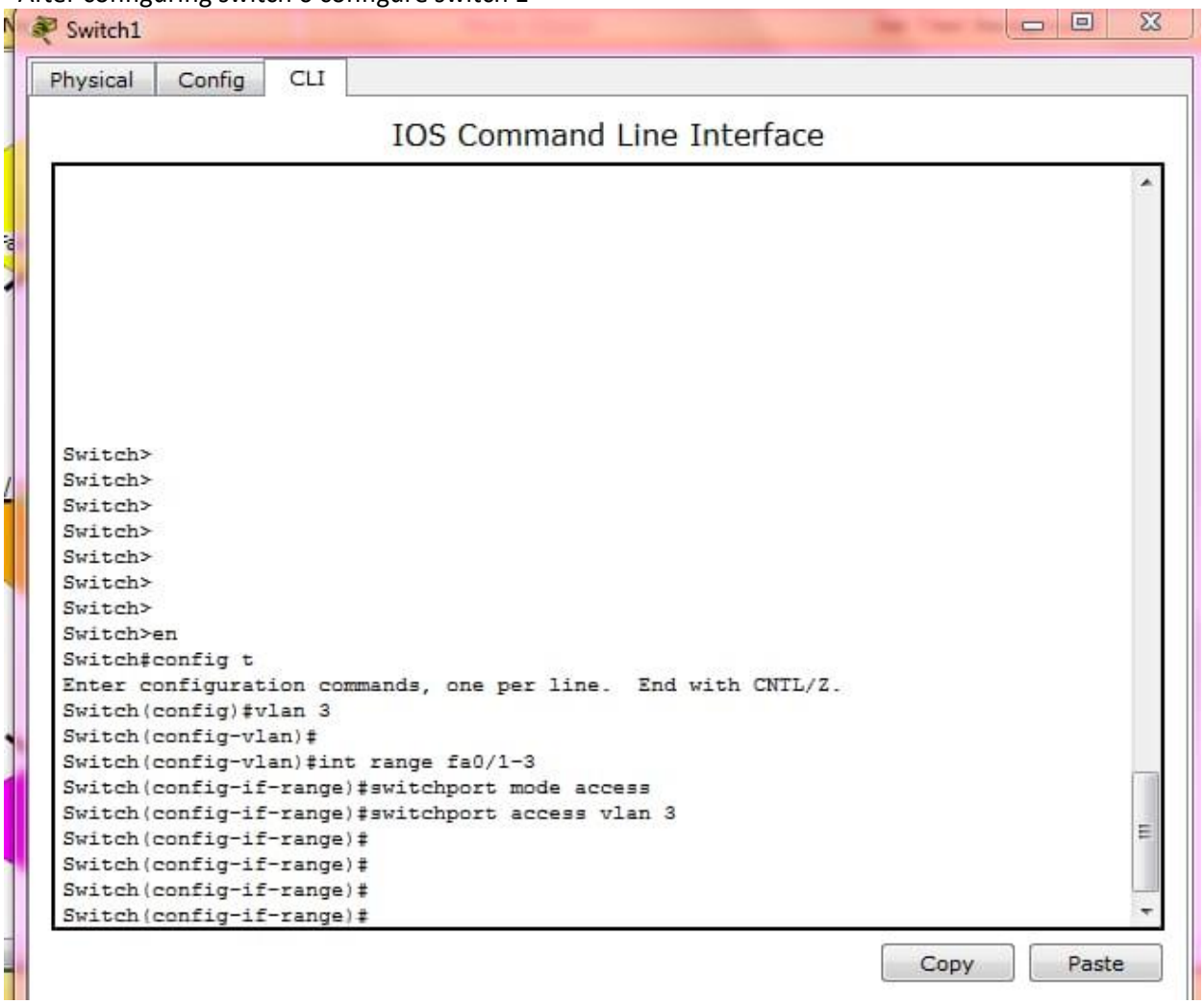
Configure routers as shown below
Configuring router 0



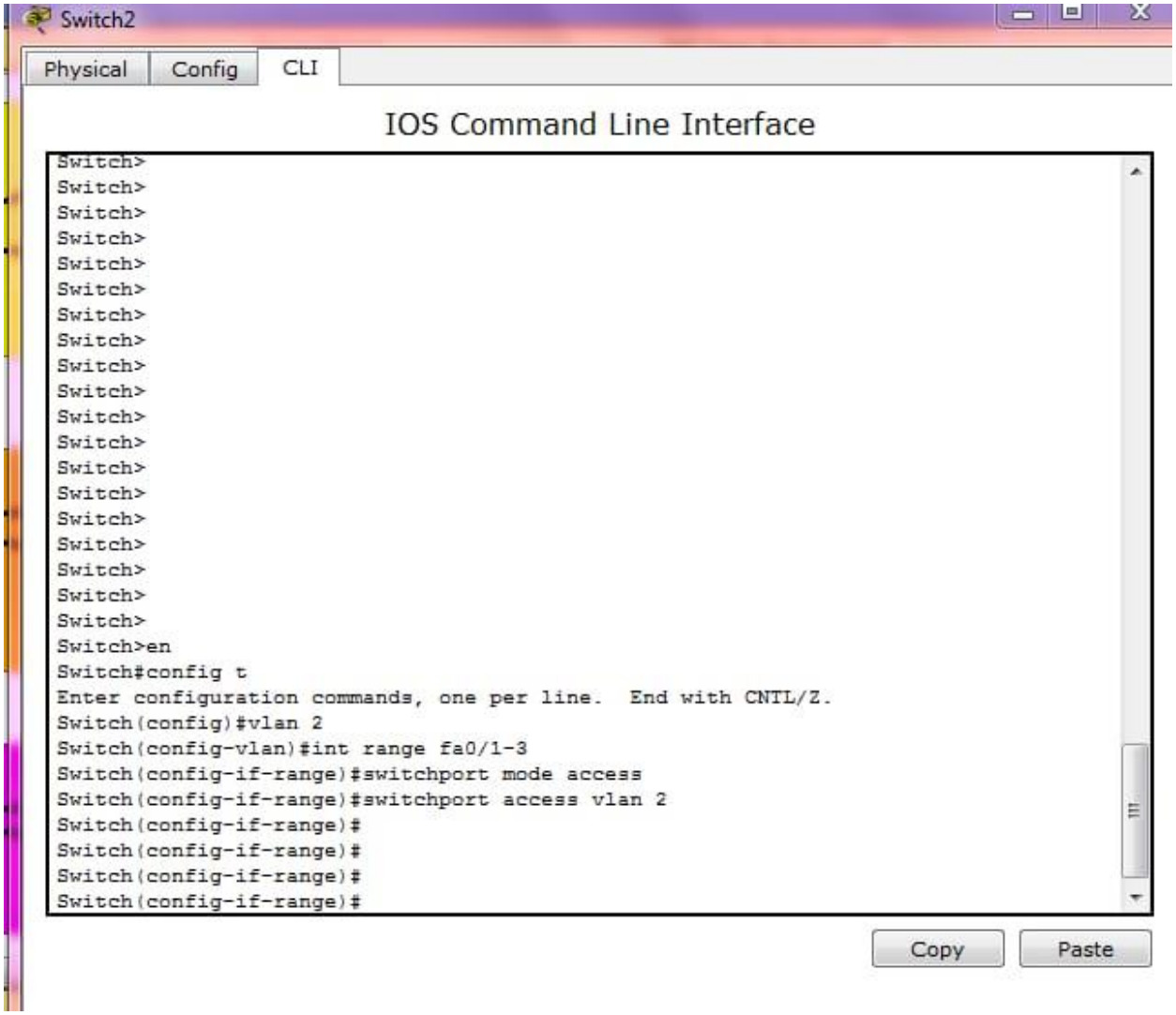
Now after configuring routers we have to configure switches
As shown below
Now we are configuring switch 0


Switch0
Physical
Config
CLI
IOS Command Line Interface
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 4
Switch(config-vlan)#exit
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#ex
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Copy
Paste

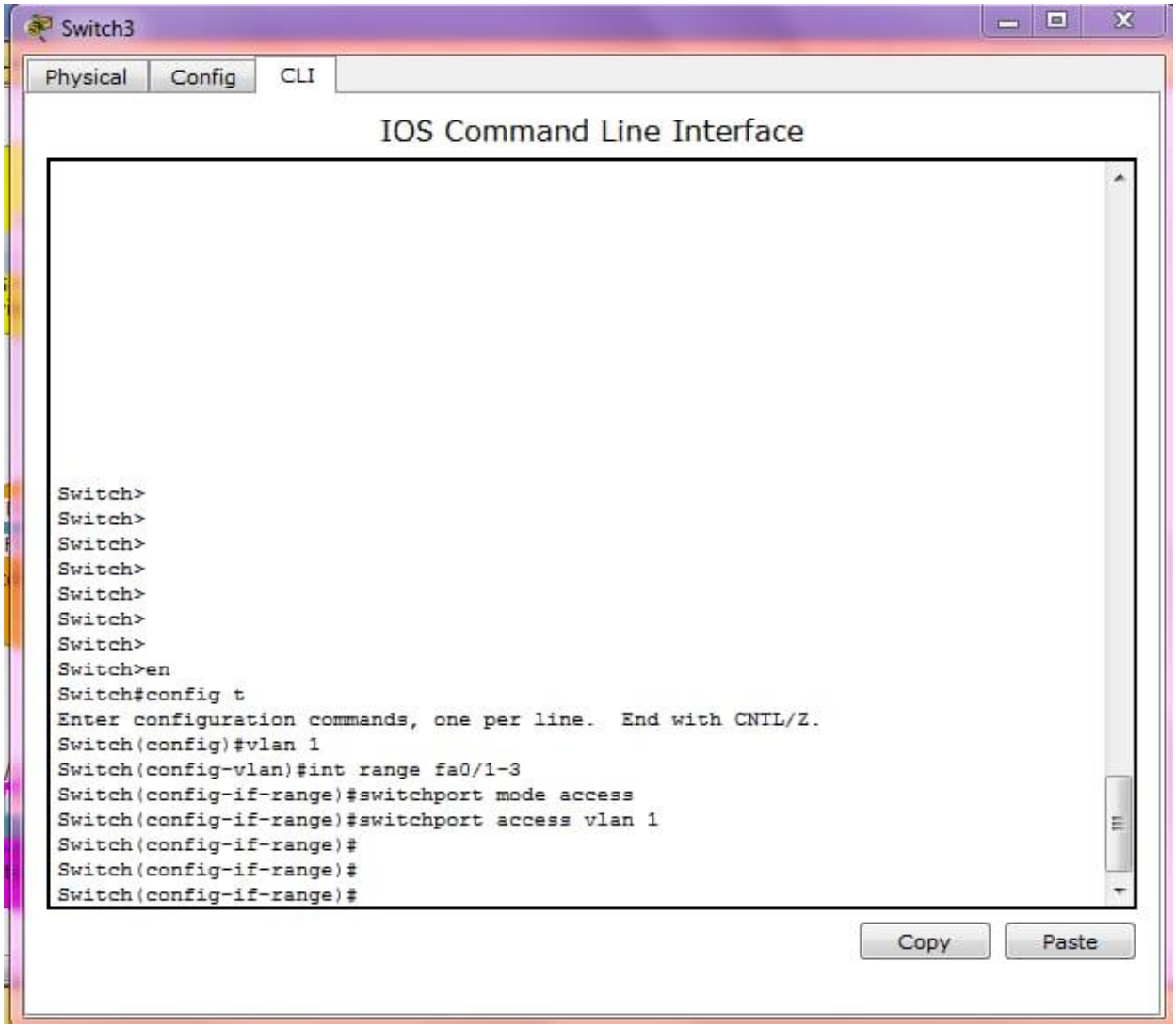
After configuring switch 0 configure switch 1



Now configure switch 2

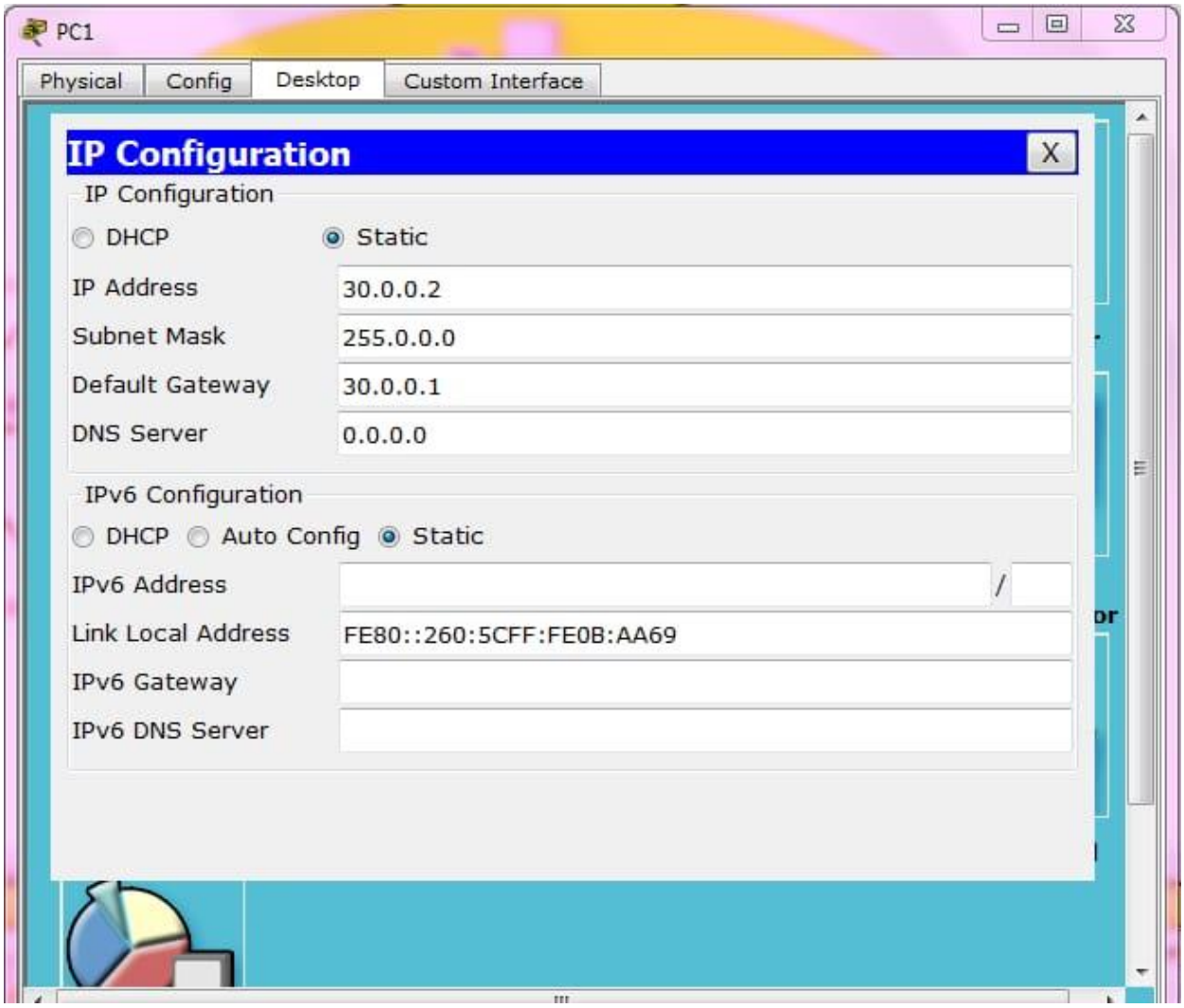


Now configure switch 3 as shown below

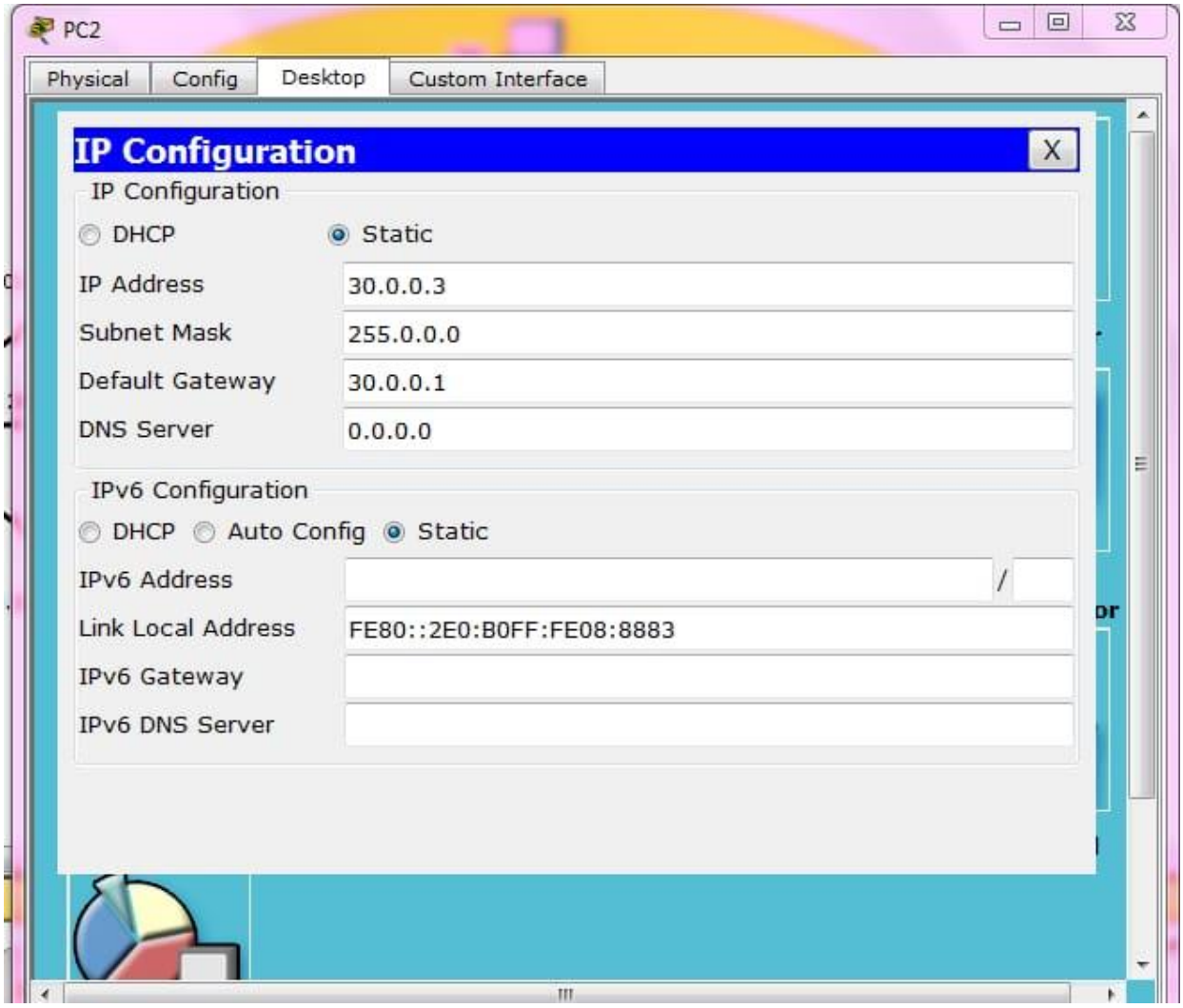


Now we have successfully completed routers and switches
So, we have to give ip addresses, subnet masks, dns and default gateway to computers as shown below

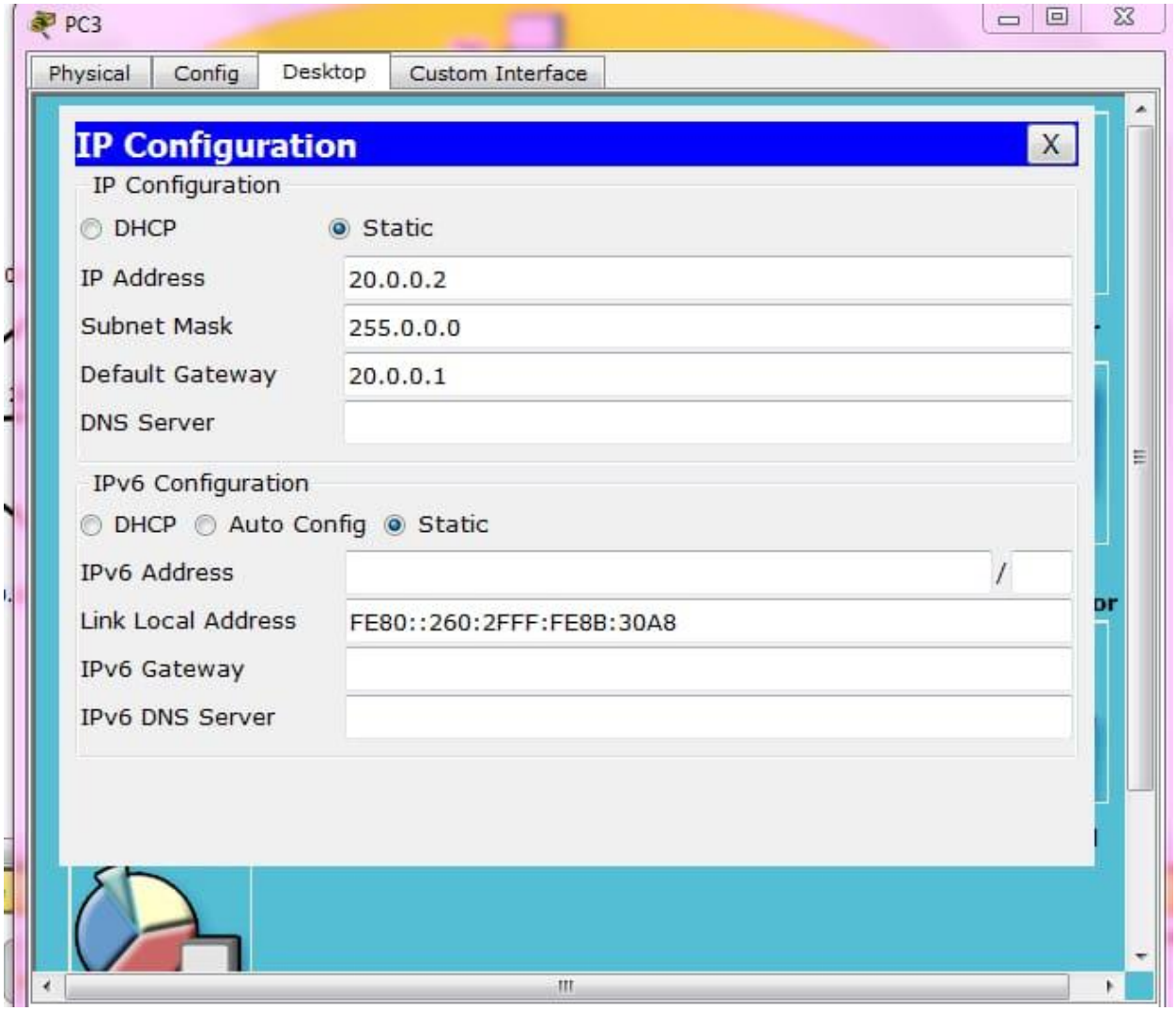
Now configuring pc 1



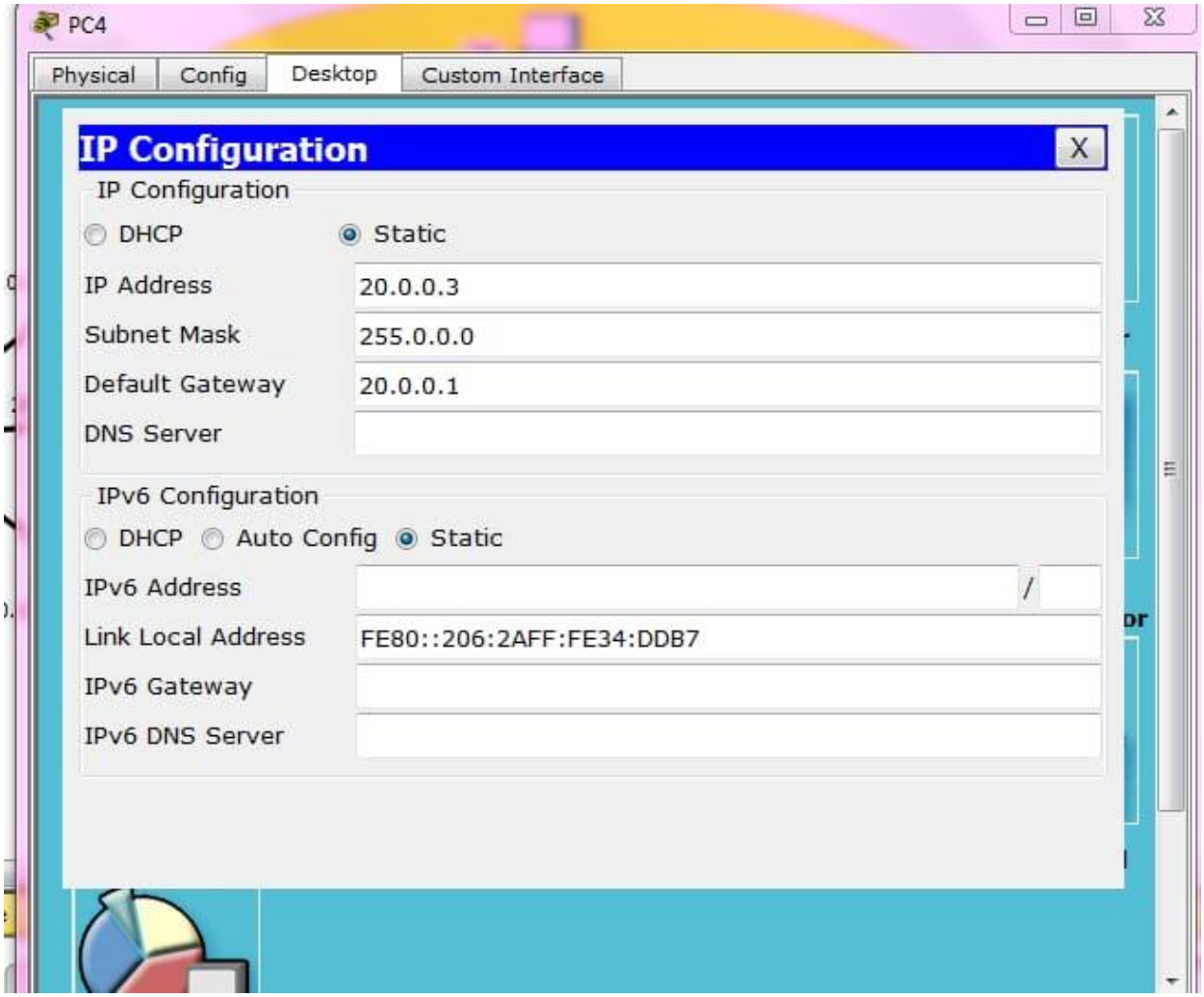
Now configure pc 2



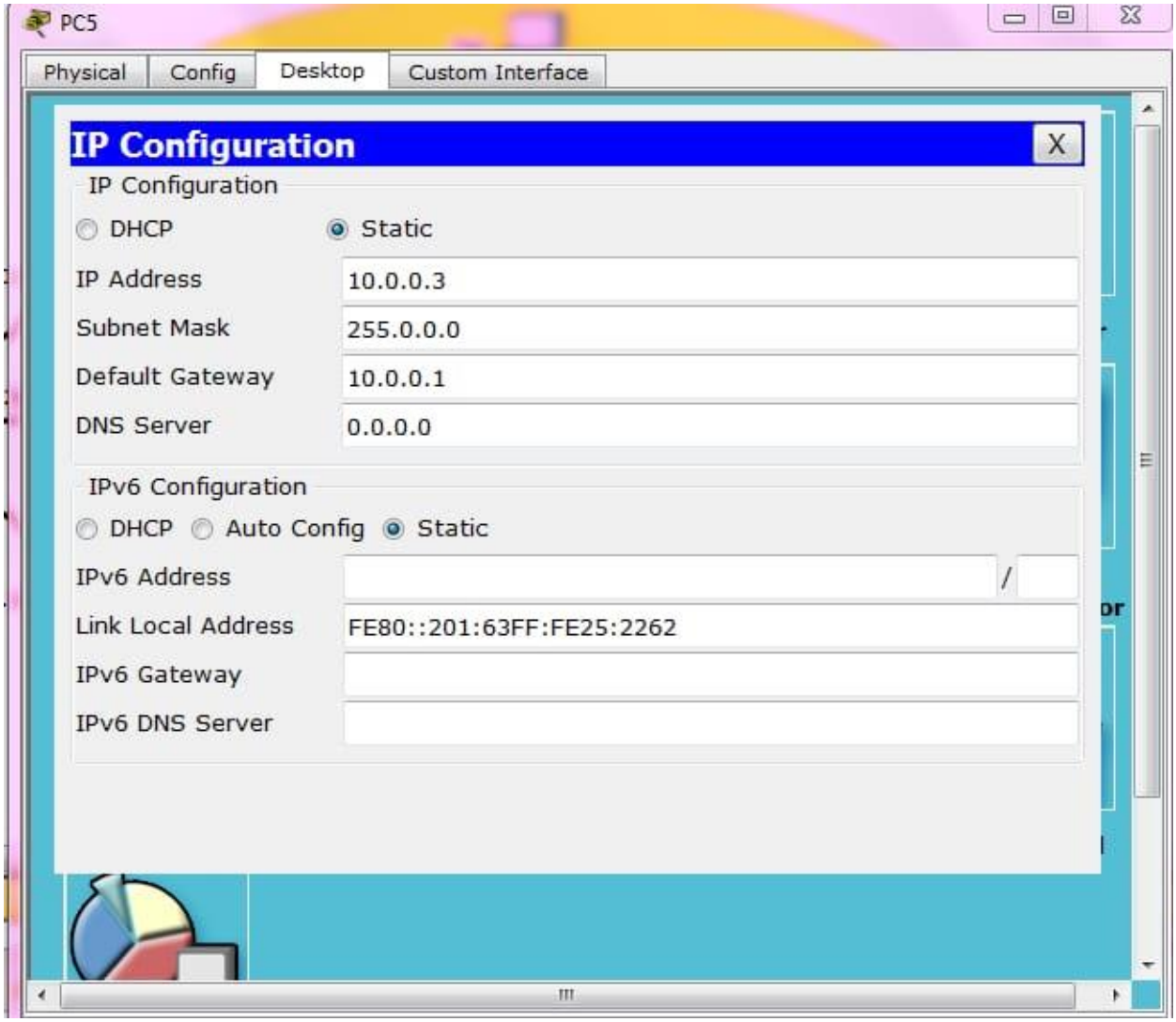
Now configure pc 3



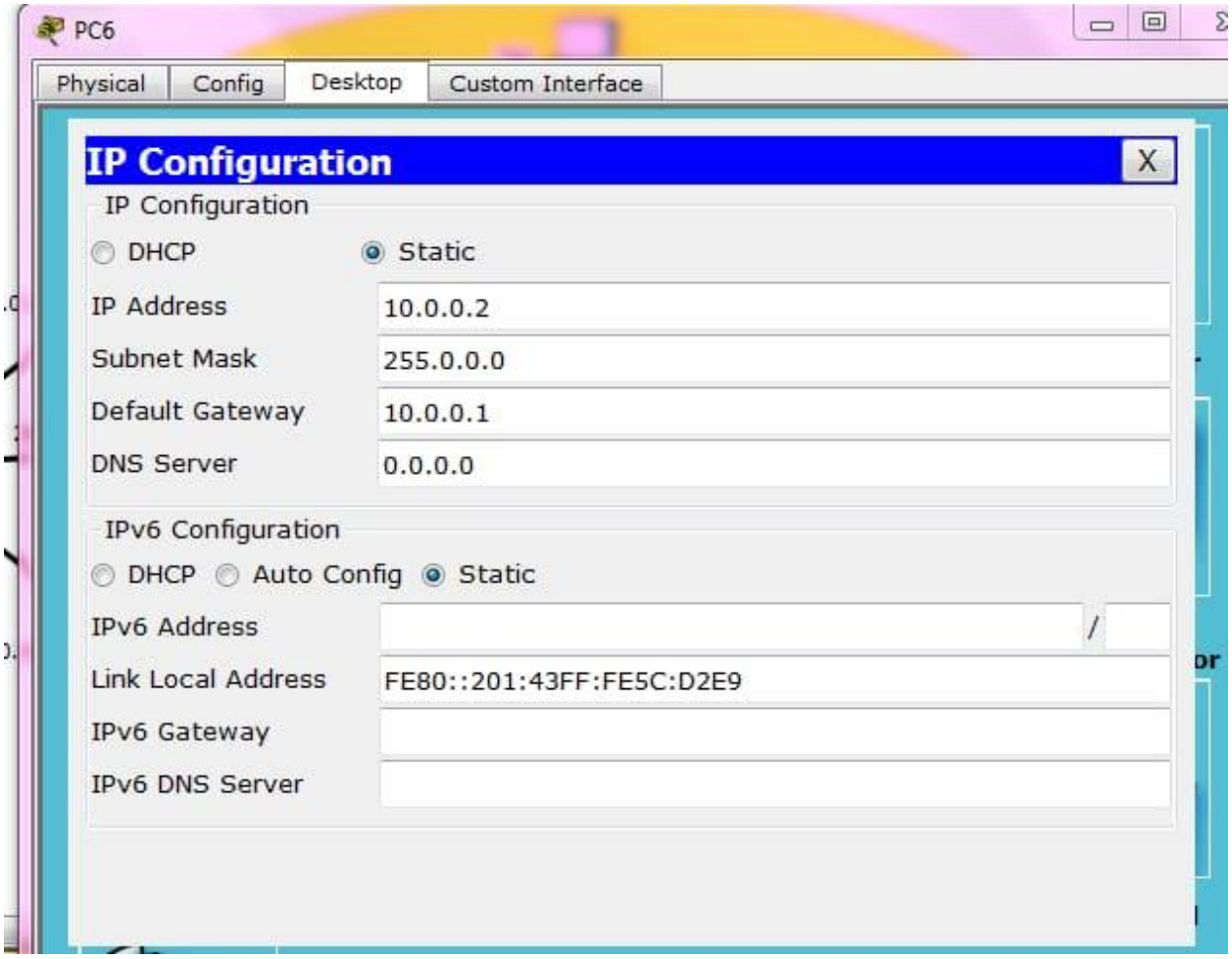
Now configure pc 4



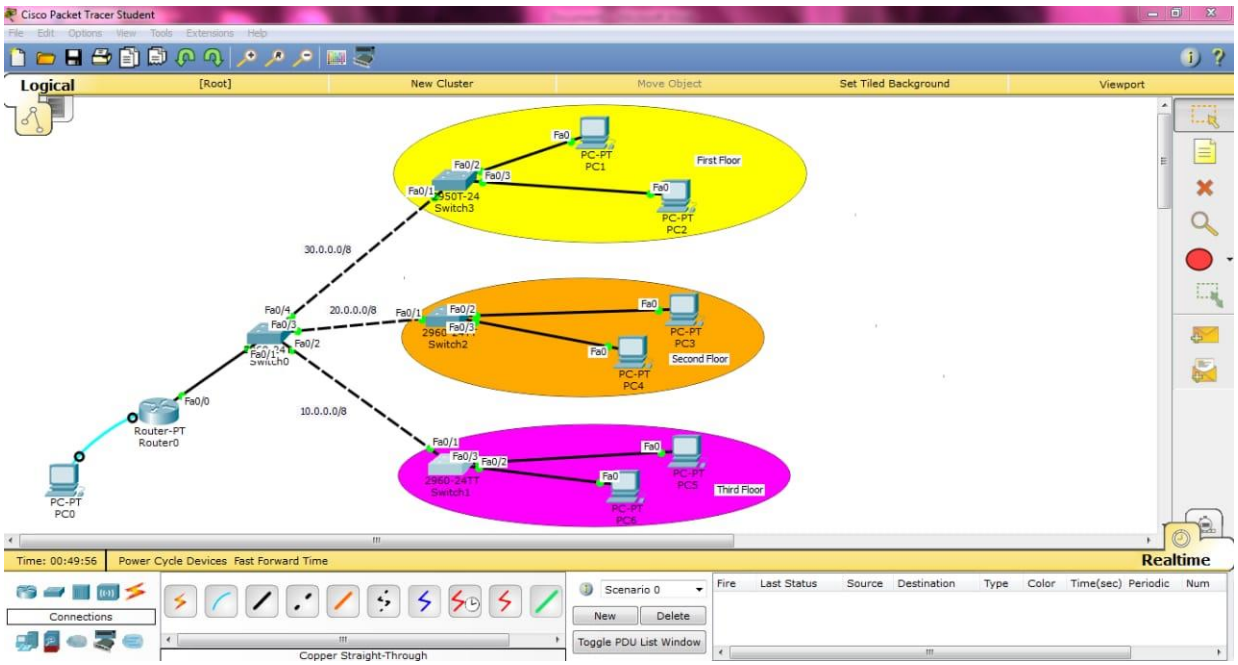
Now configure pc 5



Now configure pc 6



Now we have successfully completed configuring pc, routers and switches



Creating Virtual Local-Area Network was successfully done!!!

---END---

Project 7

Controlling Traffic using Access Control List

There are **three types Access Lists** in common. Thse access list types are :

– **Standard Access List**
– **Extended Access List**
– **Named Access List**

Standard Access-Lists are the simplest one. With Standard Access-List you can check only the source of the IP packets. On the other hand, with **Extended Access-Lists**, you can check source, destination, specific port and protocols. Lastly, with **Named Access-Lists**, you can use names instead of the numbers used in standard and extended ACLs. It do not have too much difference, but it is different with its named style.

Standard Access-List Configuration

Let's start to write Standard Access-List. We will configure the Standard Access-List on router .

```
Router # configure terminal

Router (config)# ip access-list standard 1

Router (config-std-nacl)# permit  <I.p address>  <wildcard mask>

Router (config-std-nacl)# permit  <I.p address>  <wildcard mask>
```

With this ACL configuration that we have written, we permit PC0 and PC1 to access the server. At the end of ACLs, there is an "**Implicit Deny**". These Implicit Deny, prohibits the other IP addresses. Because of the fact that we did not, allow PC2's IP address, it is autoamtically denied and can not access the server.

Here, there is no need to write but to show how to write deny, I will write the deny command also. As Is aid before, for this scenario, it is not necesary. But, you can write.

```
Router (config-std-nacl)# deny  <I.p address>  <wildcard mask>
```

```
Router (config-std-nacl)# end

Router #  copy run start
```

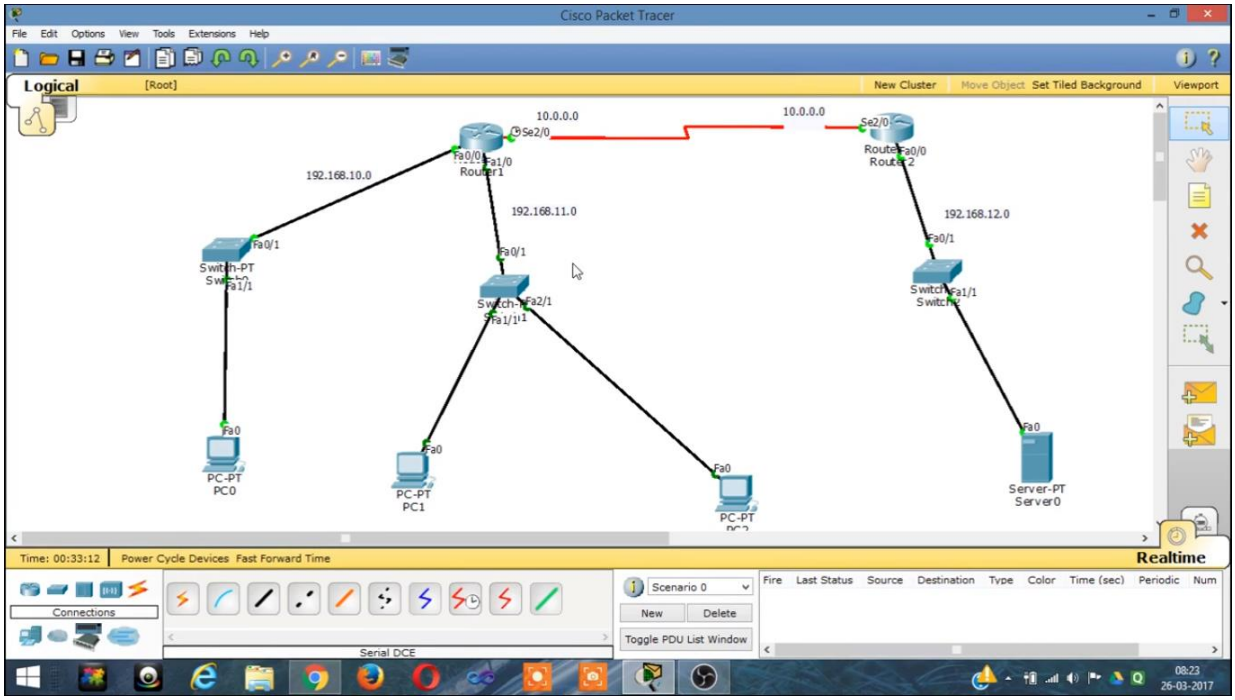
Applyin Standard Access-List to the Interface

After creating ACLs, we need to apply this ACL to the **interface**. For Standard Access-List, it is better to apply this ACL, close to the destination. So, for this configuration, we will apply our standard acceess list to the fastethernet 0/1 interface of the router.In other words, we will add ACL to the server face of the router.

Software used : cisco packet tracer

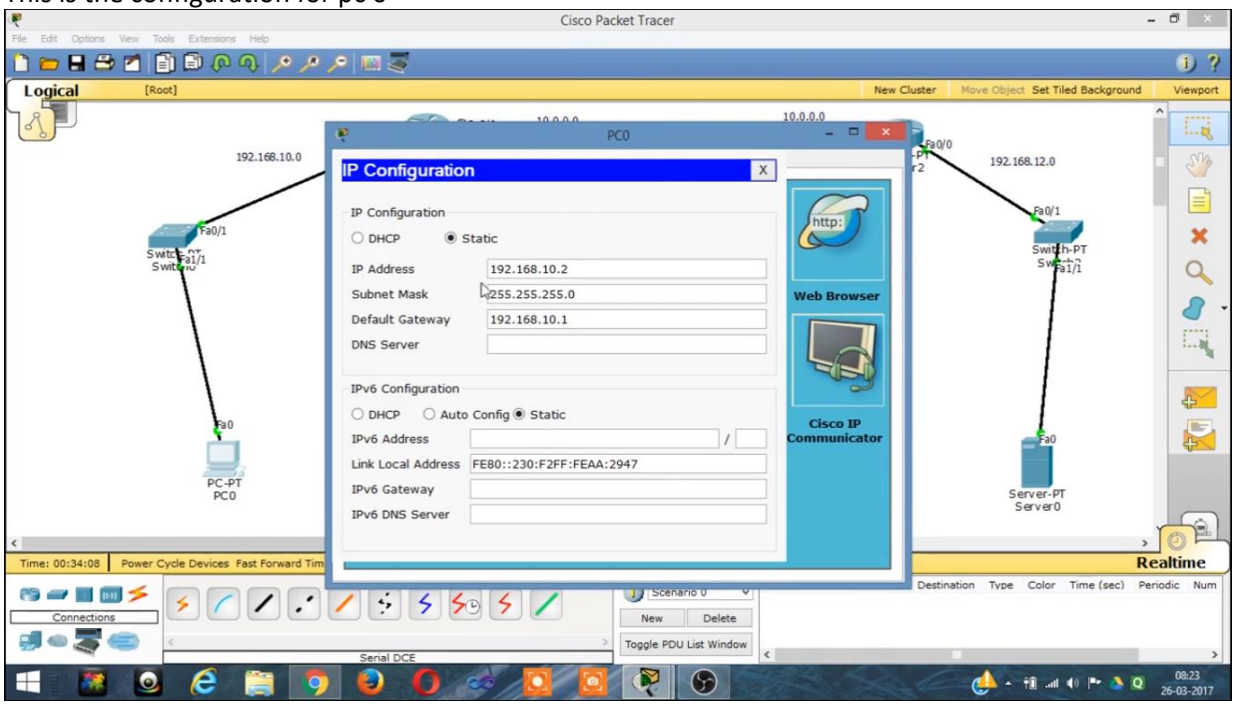
Procedure:

Create the network as shown below and configure routers using any routing protocols as rip is easier I had chosen RIP protocol. You can any routing protocols as your wish

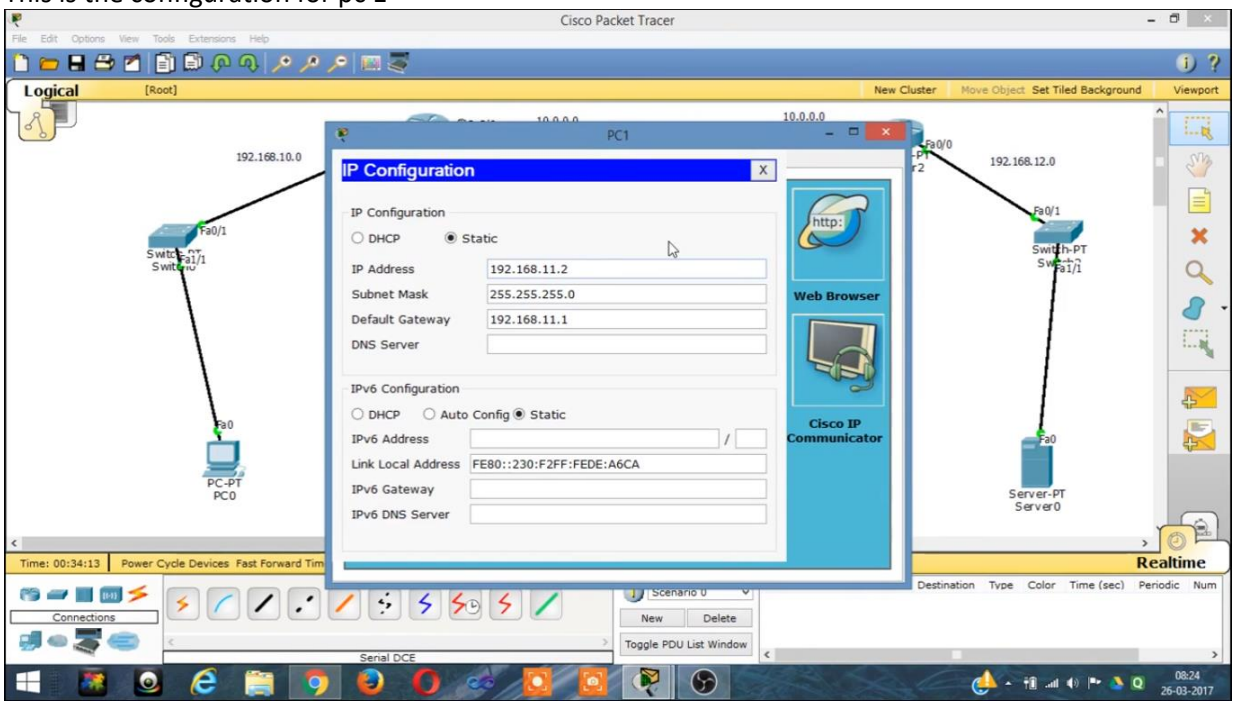


Now configure computers as shown below

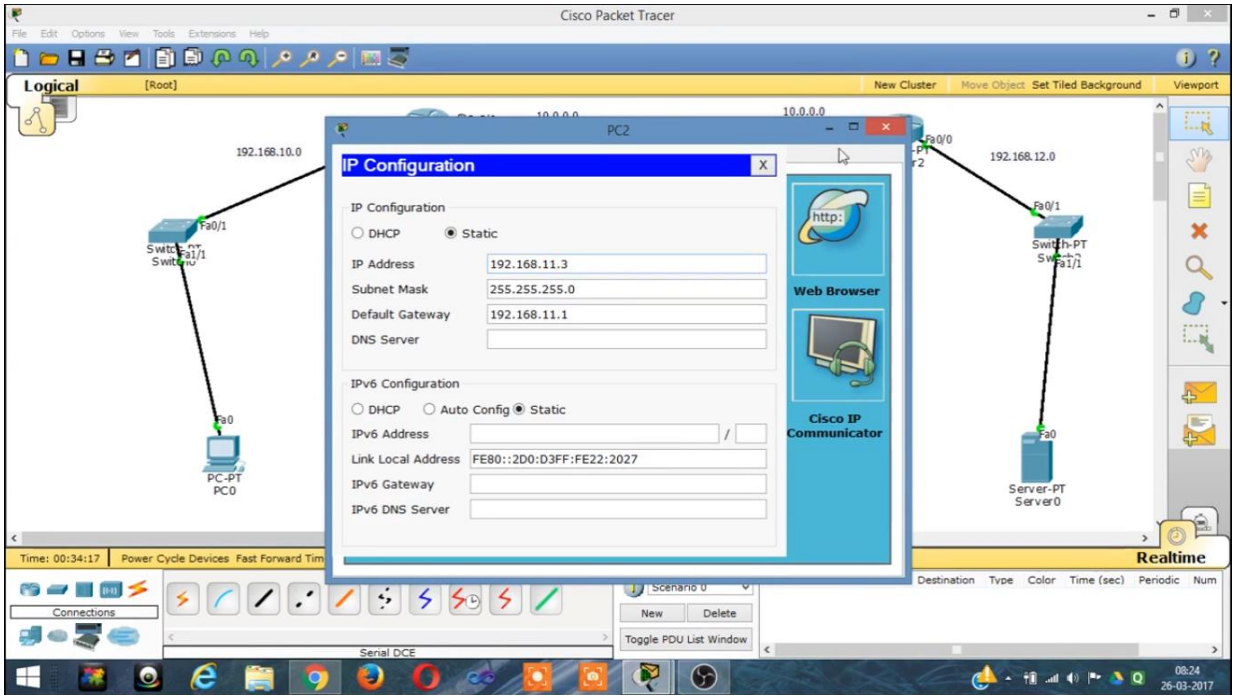
This is the configuration for pc 0



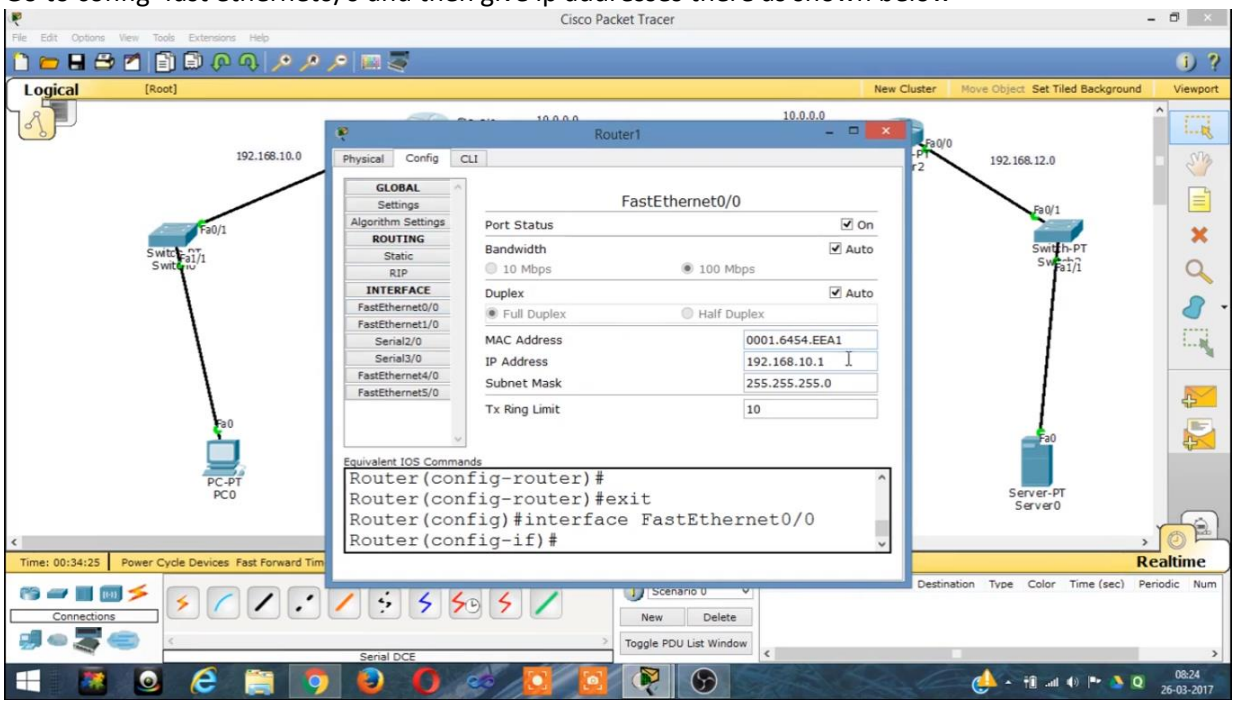
This is the configuration for pc 1



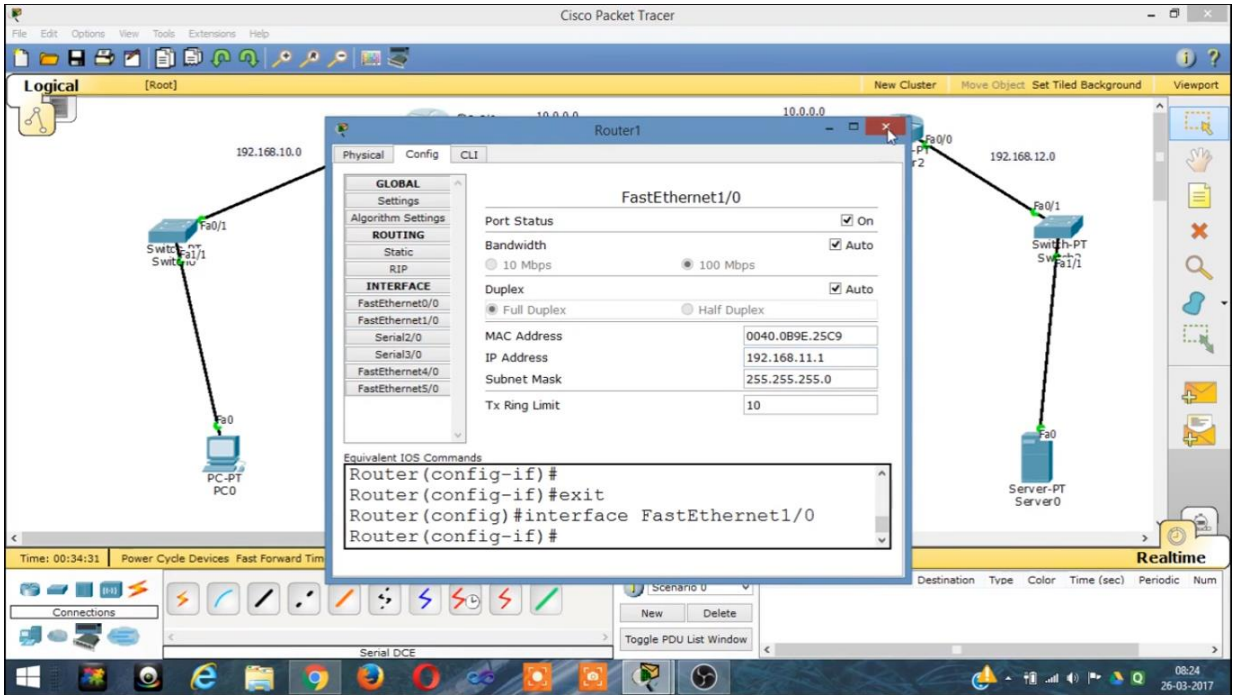
This is the configuration for pc 2



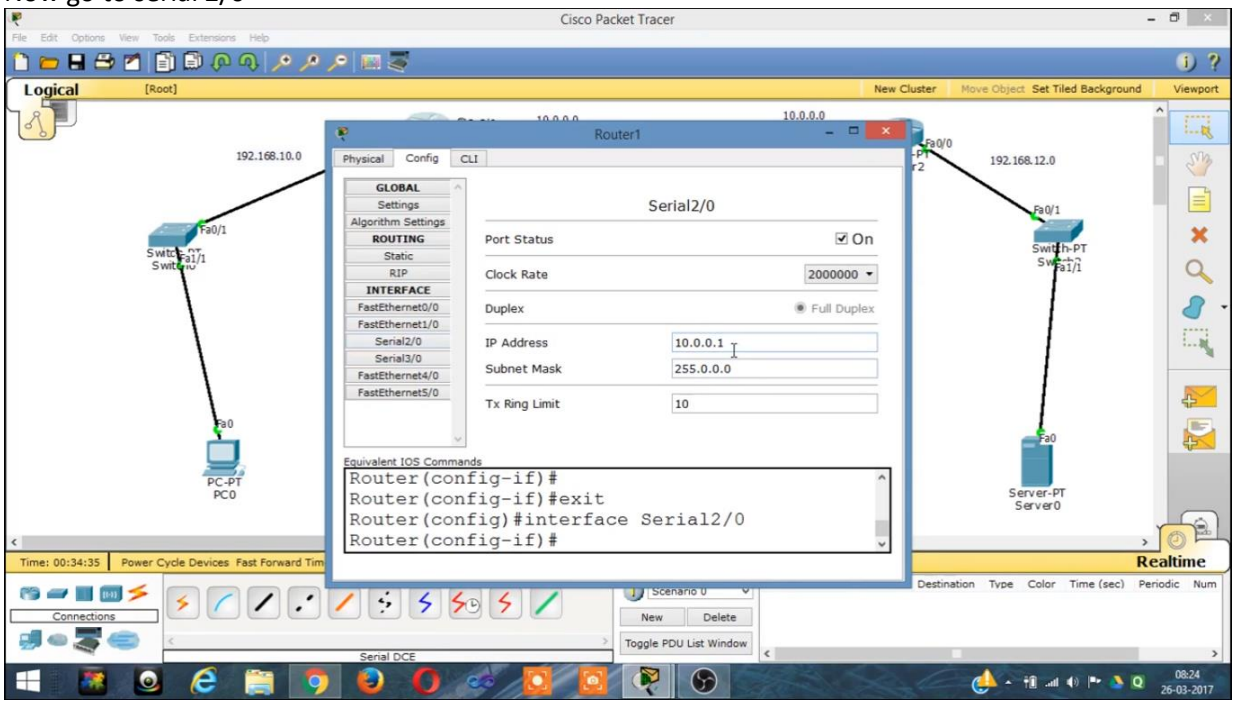
Now we have successfully completed configuration for routers and pc's
Now go to router 1 and do the following changes
Go to config>fast ethernet0/0 and then give ip addresses there as shown below



Now go to fastethernet 1/0 and do the changes specified in the below screenshot

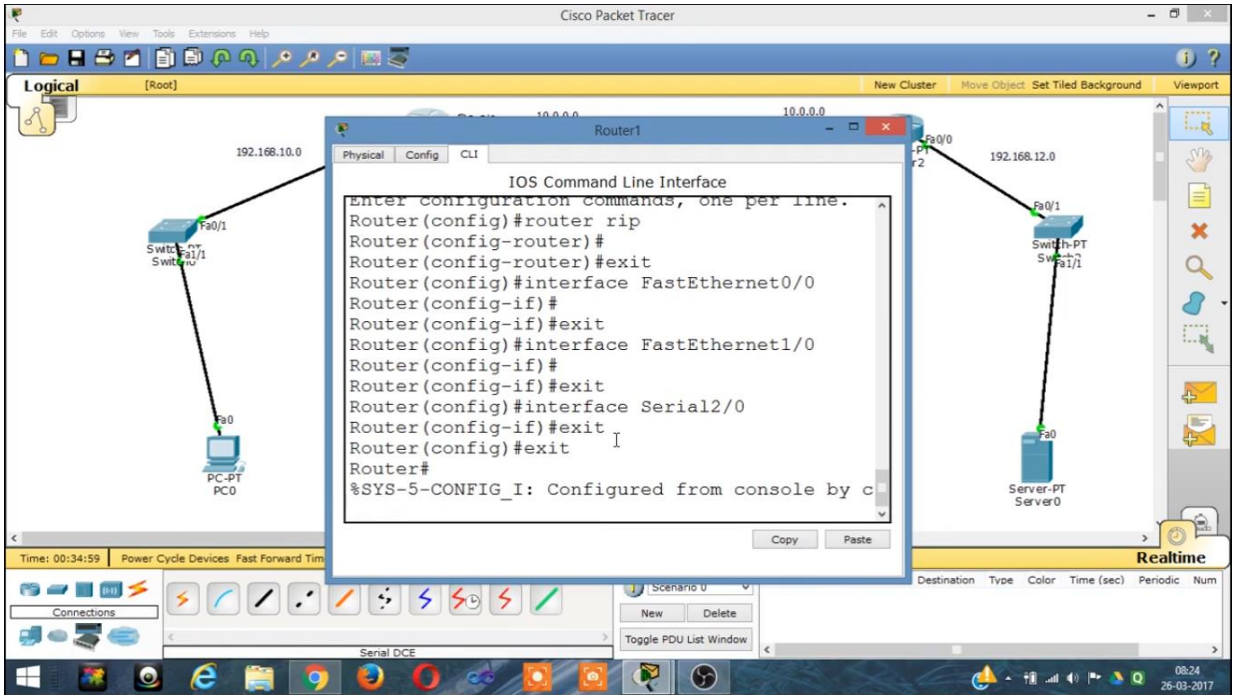


Now go to serial 2/0



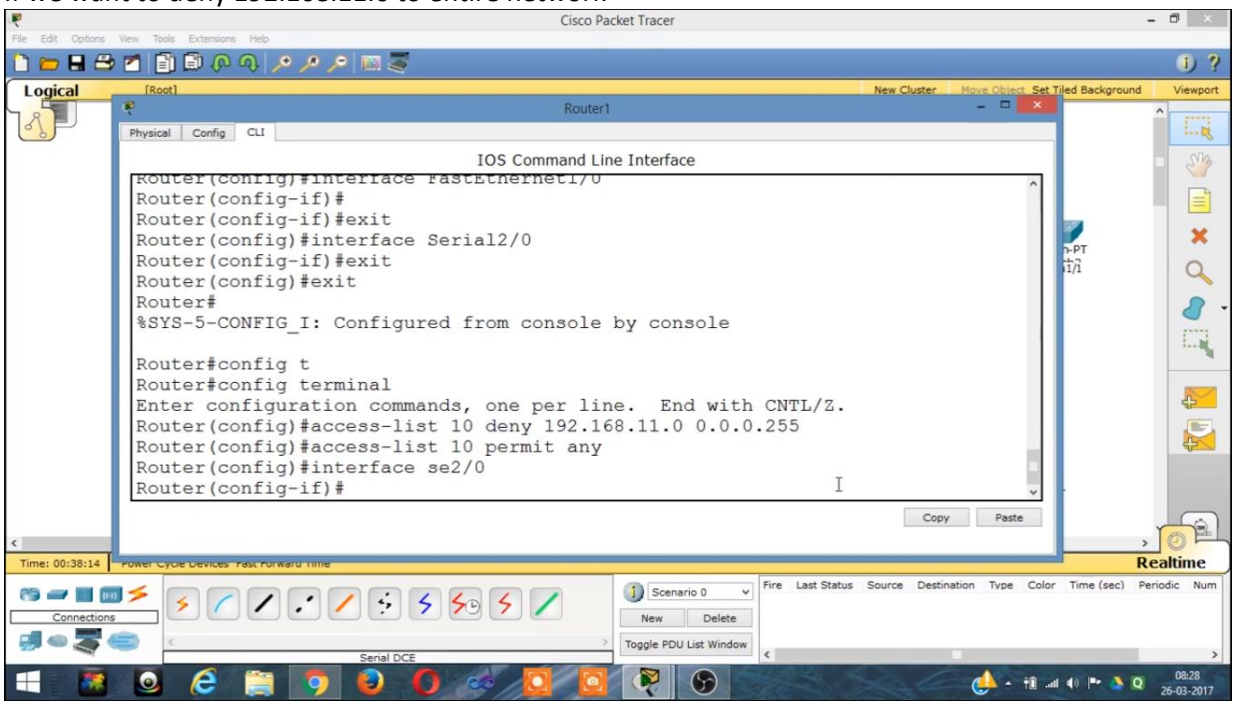
Now do the same for the other router also

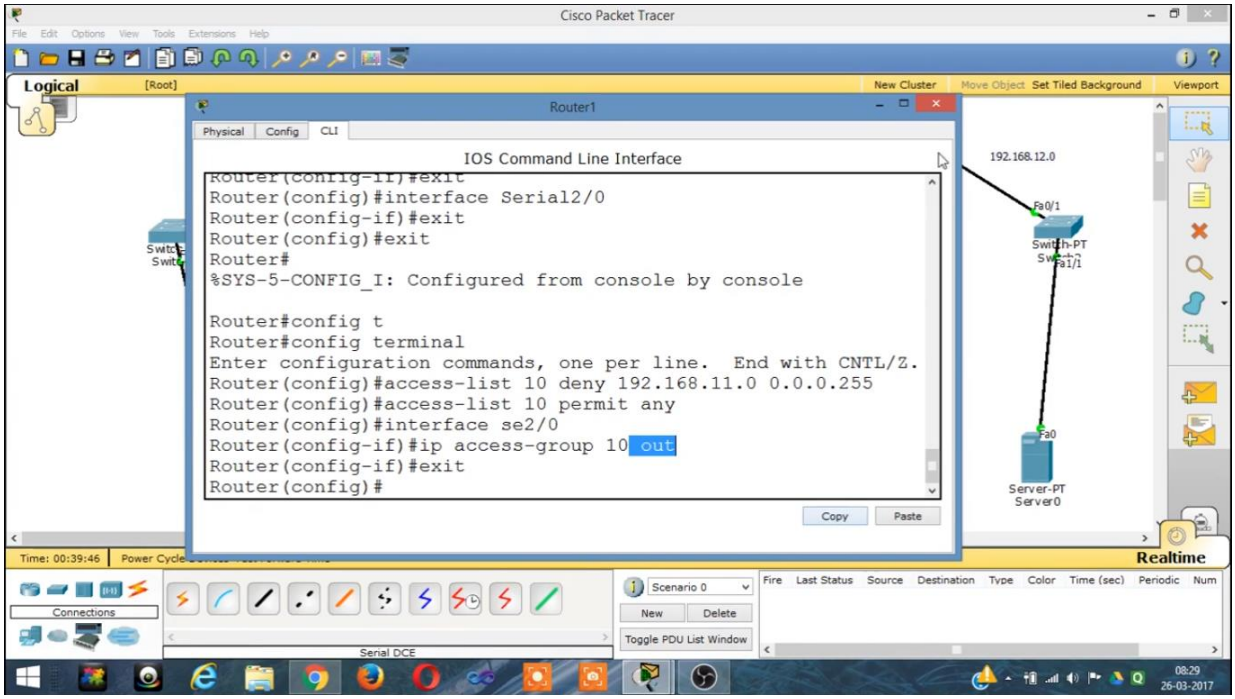
Now we have successfully created the entire network
Now let us try to send packets between pc's to check the connectivity
It will definetly tells failure because we didn't configure routing yet
Now configure router 1 as shown below



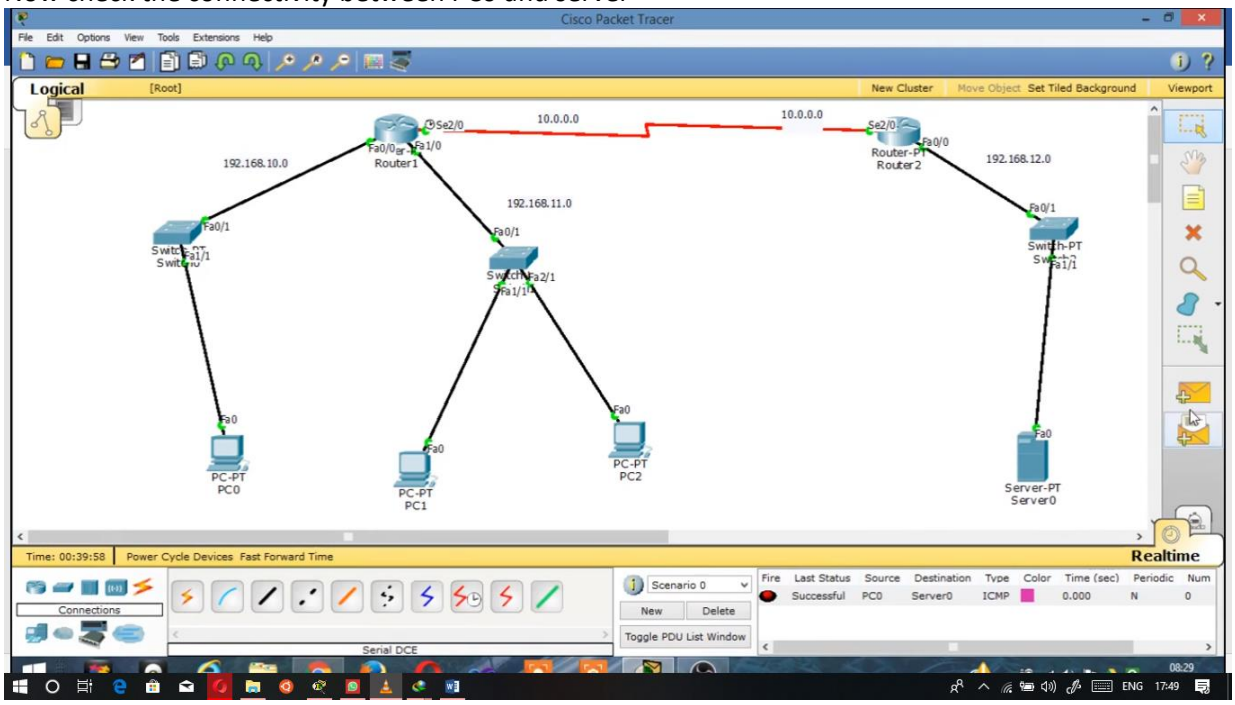
And do the routing for other routers also

Now configure ACL for the same router
If we want to deny 192.168.11.0 to entire network



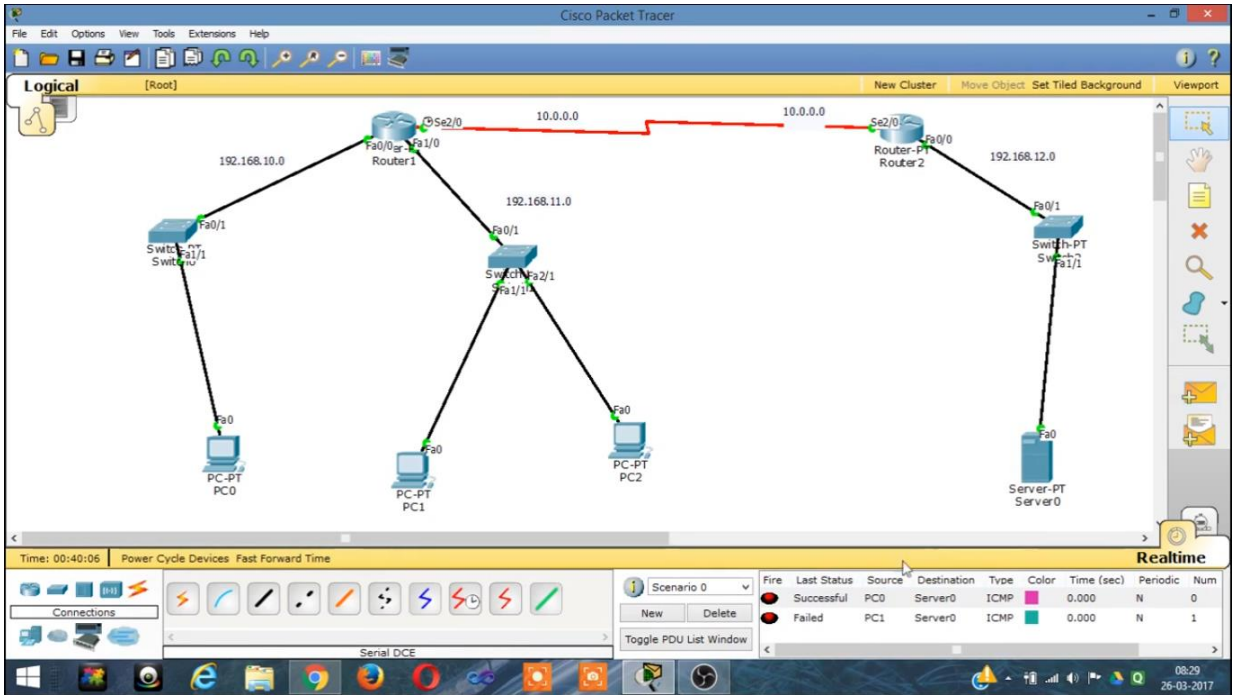


Now check the connectivity between PC0 and server

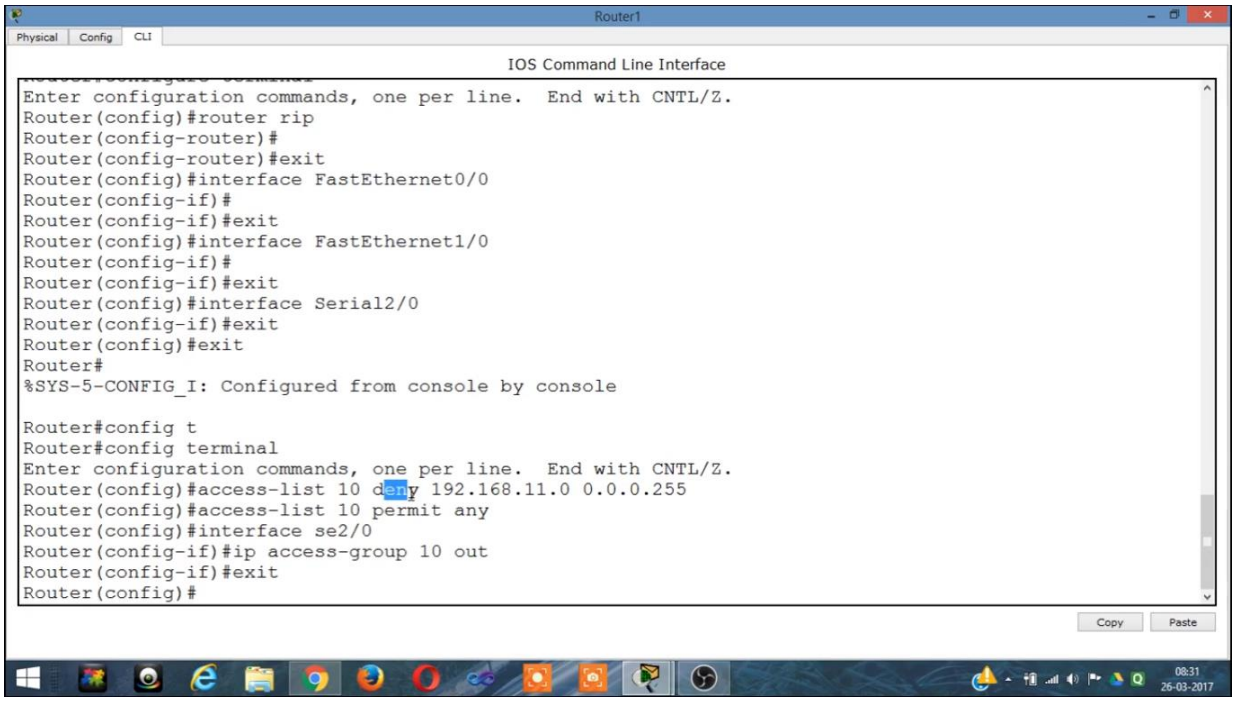


Now it is successful!!!

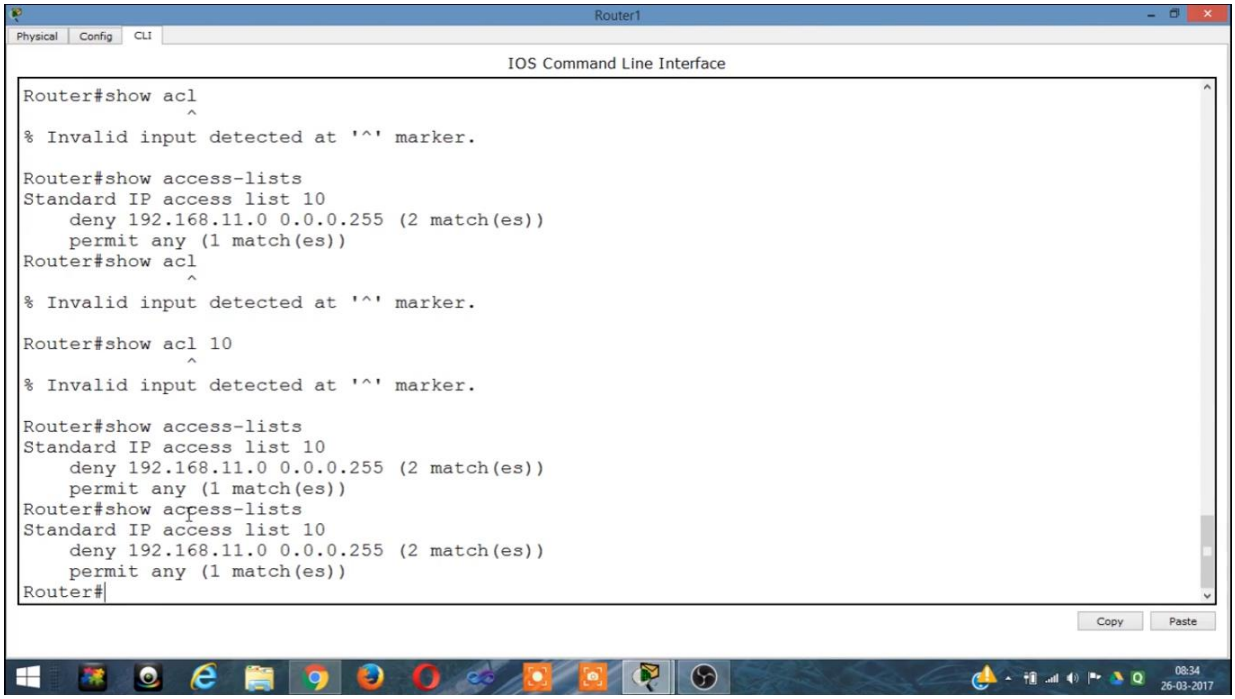
Now try to send packet from pc1 to the server



Now it fails because we had restricted 192.168.11.0 to access 10.0.0.0and 192.168.10.0 as shown in figure



Now type show access lists as shown in below screenshot



Now we have successfully Controlled Traffic using Access Control List

---END---