COE344 Computer Networks– Lab Manual

By

Dr. Fazal Noor

Updated by

Yazeed Almalaq

Computer Science and Software Engineering Department University of Hail

Table of Contents

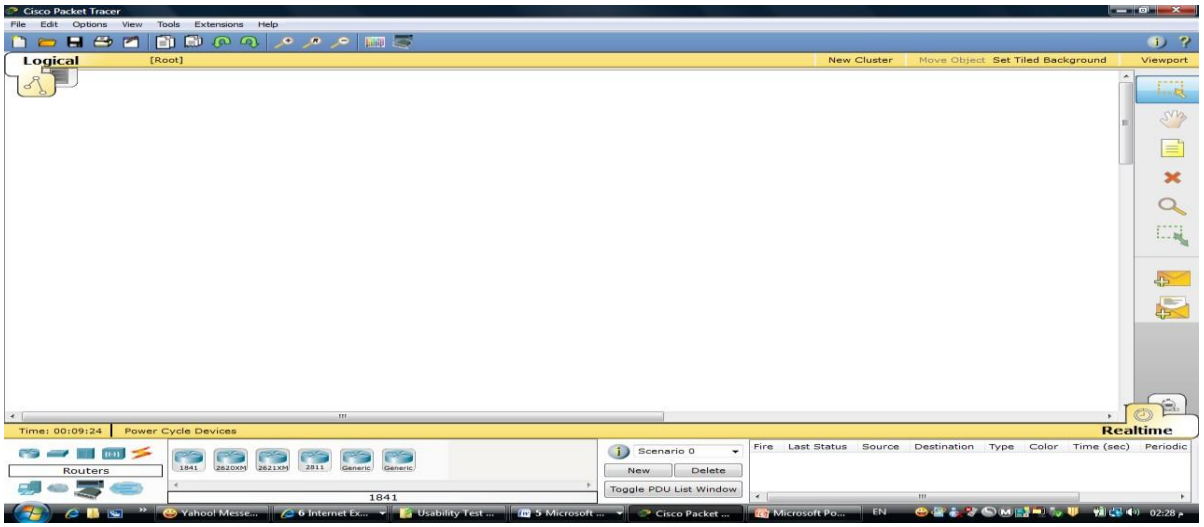
LAB 1: Introduction to Packet Tracer and Simple 2 PC network.

Objectives:

- Learn Packet Tracer to design and simulate networks.
- Learn to create a simple LAN with two PCs using an Ethernet hub and two straight-through cables to connect the workstations.
- Learn to configure and verify the network connectivity.
- Learn about various network related commands.

1.) Click on Packet Tracer Icon on the desktop of your computer screen.

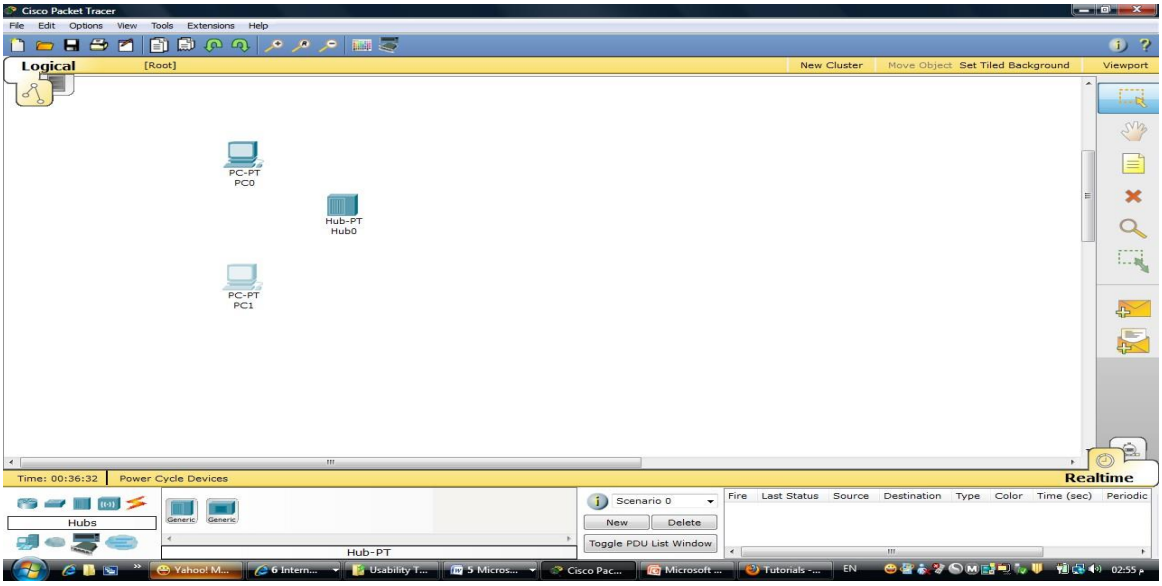
2.) You will see a window appear as below.



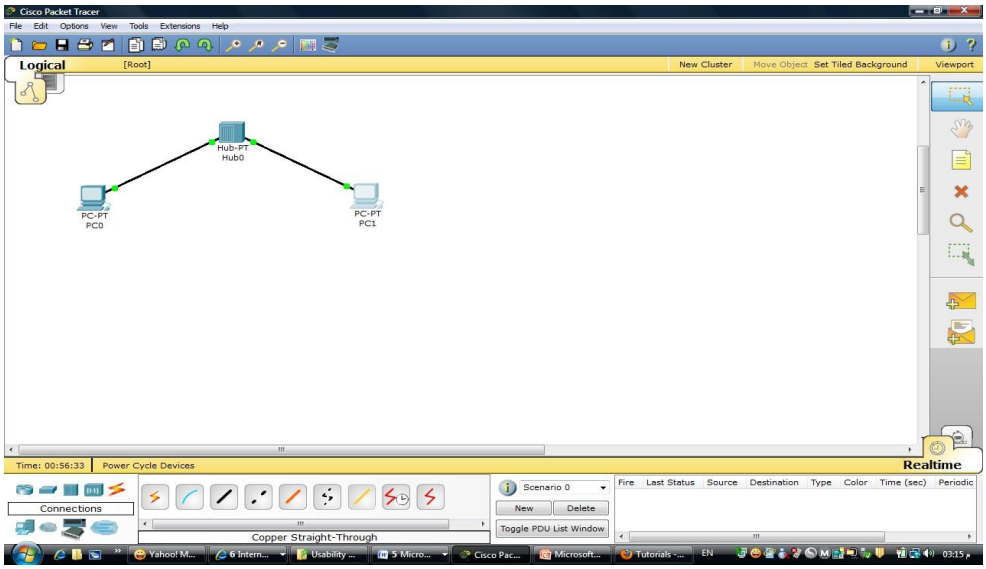
3. Click on Help then click on Tutorials. Under Tutorials → Click on Interface Overview. An automated tutorial will begin. Try to understand it as much as possible. When finished with the tutorial start the next tutorial. Under Logical Workspace → click on Creating a Network Topology. Again an automated tutorial will begin and go through it. After finishing, you will now design a simple network next.

4. By now you should have a basic understanding of Packet Tracer. Now let us make a simple network with 2 PC and a hub or a switch. Move your mouse cursor to lower left corner over the PC icon. Now click on PC icon. On the window right, you will see Generic under a PC icon. Click on it and drag the mouse to main window and drop it. You will see a picture of PCO. Again click on PC icon and drag the mouse to the main window and let it go. You will see another PC1 appearing. That is you have 2 computers on the main window.

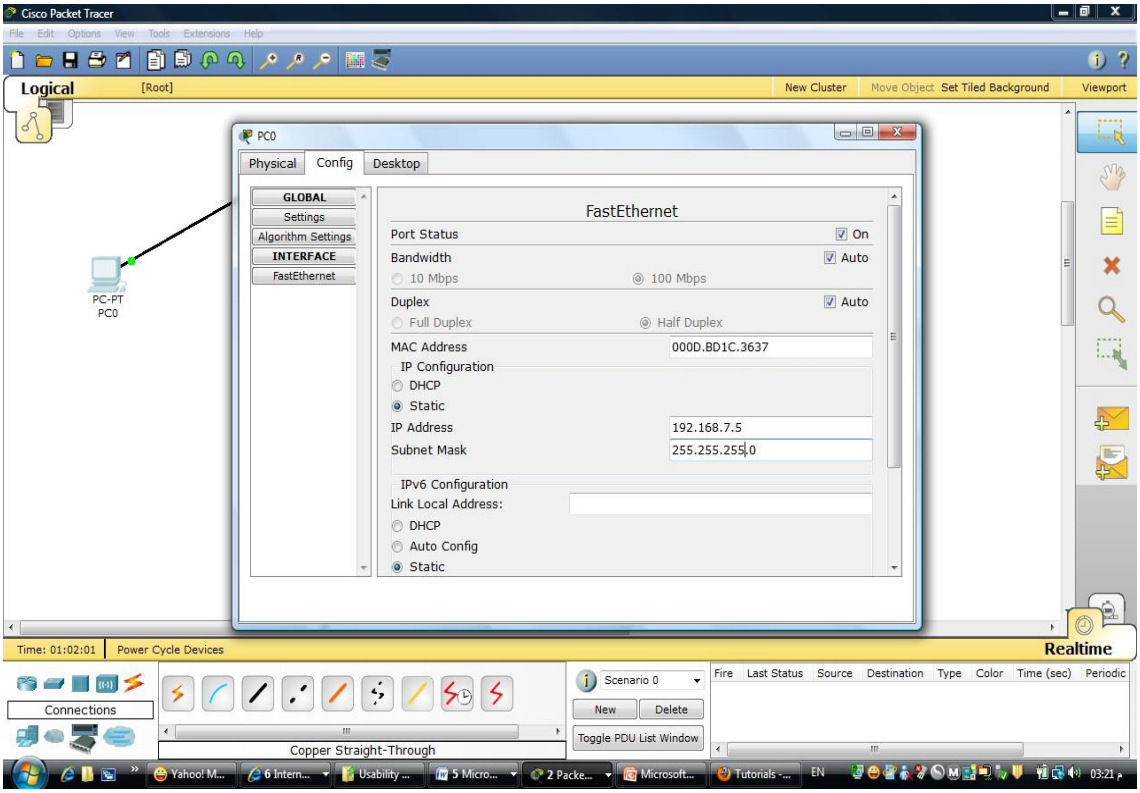
5. Now choose a hub. You do this by going to the lower corner and choosing the third icon, note in the box the word Hubs will appear. On the right window next to it, you will see 2 generic devices. Click on it and drag the mouse to main window and let go. This is what you should have by now, 2 PCs and 1 Hub.



6. Now we want to connect the cables. Again lower left corner the 5th icon (zig-zag orange in color) click on it and in box the word connections will appear. Now on the window on right you will see different types of cables appearing. Choose the third on “Copper Straight-Through”. Click on this cable and drag it to the PCO and to the Hub. You will see ports with numbers you may connect to anyone. Again repeat between PC1 and the Hub. This is what you should have by now.

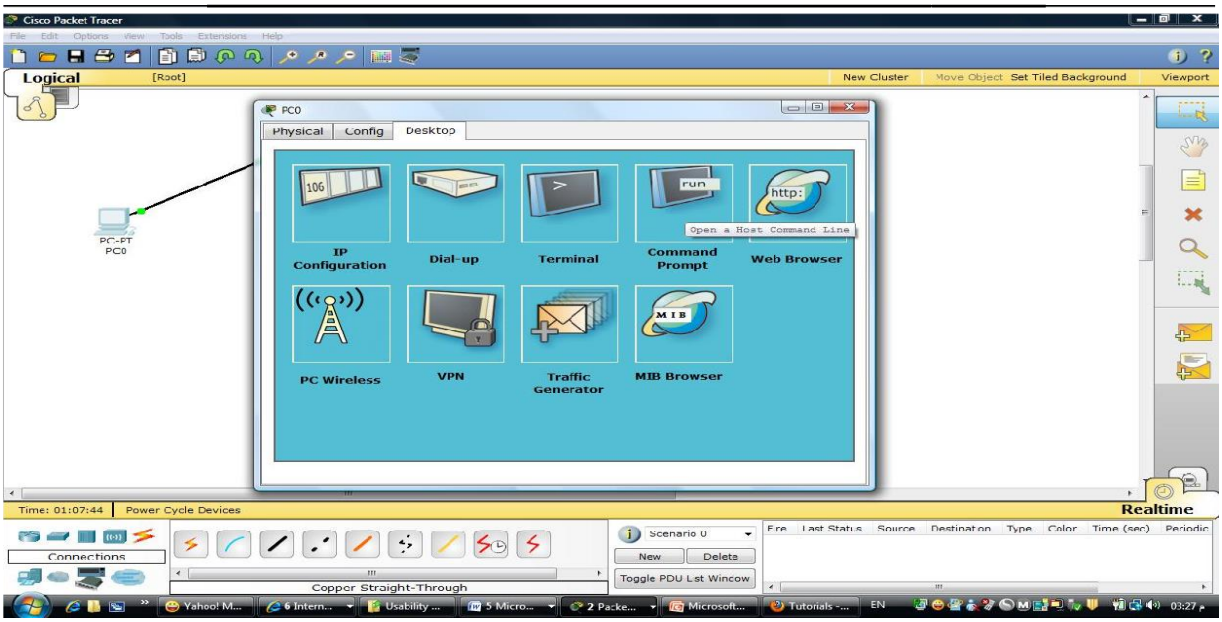


Now that we have the simple network, we need to assign IP addresses to the 2 PCs. Fast double click on PC0. You will get pop-up window of PCO and click on “Config” menu to get the window below. Click on Fastethernet. In the IP Address type in **192.168.7.5** and for subnet mask type **255.255.255.0**. Click on X to close this box afterwards.

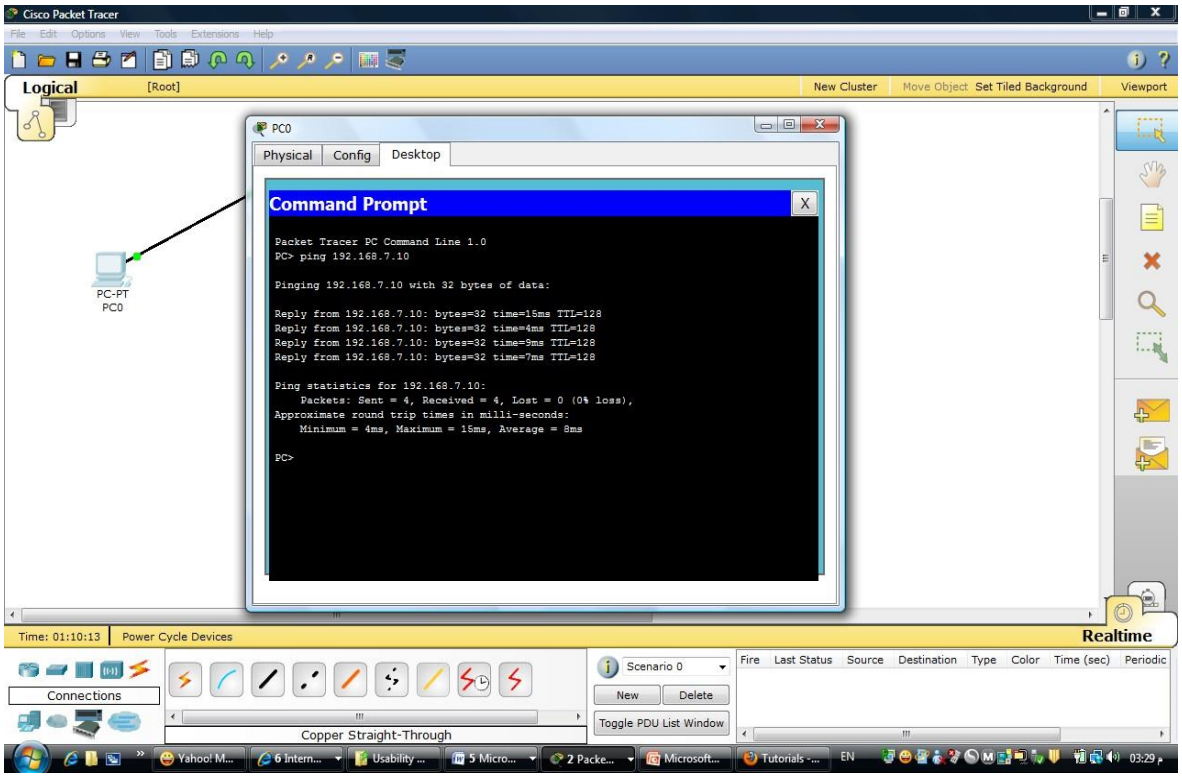


7. Similarly do with PC1 but assign the following IP address **192.168.7.10** and subnet mask **255.255.255.0** Click on X to close the sub window.

8. To test the ping command. Fast double click on PCO to get the following. Under desktop click on “COMMAND PROMPT” window.



9. You will get the following and in the window type: **ping 192.168.7.10** < press enter >



You will see that 4 packets are sent to PC1 and get a reply back. If you do not get a reply then something is wrong with your network. The ping utility shows if the connection between source pc and destination pc is working or not.

11.) After testing out the "**ping**" command. Do the following excerises.

12.) In the Command Prompt as above instead of typing ping. Now type **ipconfig** < press enter >. Write down what you get:

Ip address	
Subnet mask	
Default gateway:	

13.) Next type **tracert 192.168.7.10** < press enter >. What do you see ?

14.) Next type **arp –a** <press enter>. What do you see ?

15.) Practice by adding more PCs to your network and assigning IP addresses.

16.) If you assign one PC an ip address of 192.168.7.15 and another PC with ip address of 192.168.8.20. Can you ping each other ? Yes or No.

\

LAB 2: Dynamic Host Control Protocol (DHCP) and Domain Name System (DNS)

Objectives:

- Learn Packet Tracer to design and simulate networks.
- Learn to configure DHCP server and a DNS server

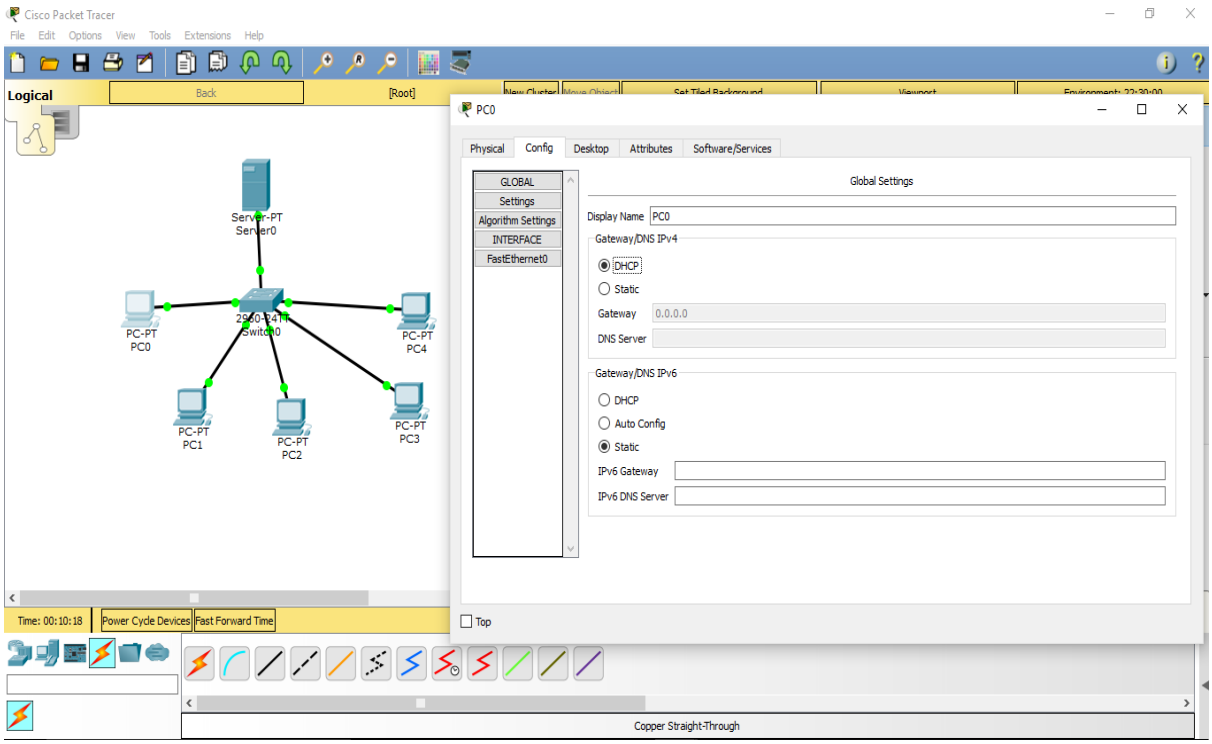
Introduction: Dynamic Host Control Protocol (DHCP) server is used to assign IP addresses to the clients automatically. Suppose you have 100 PCs then it would be easier to use DHCP to assign IPs instead of assigning each PC an IP address manually (static IP address). Domain Name System (DNS) server is used to translate between a name and an ip address.

Part I: Configuring DHCP server:

1.) Click on Packet Tracer Icon on the desktop of your computer screen.

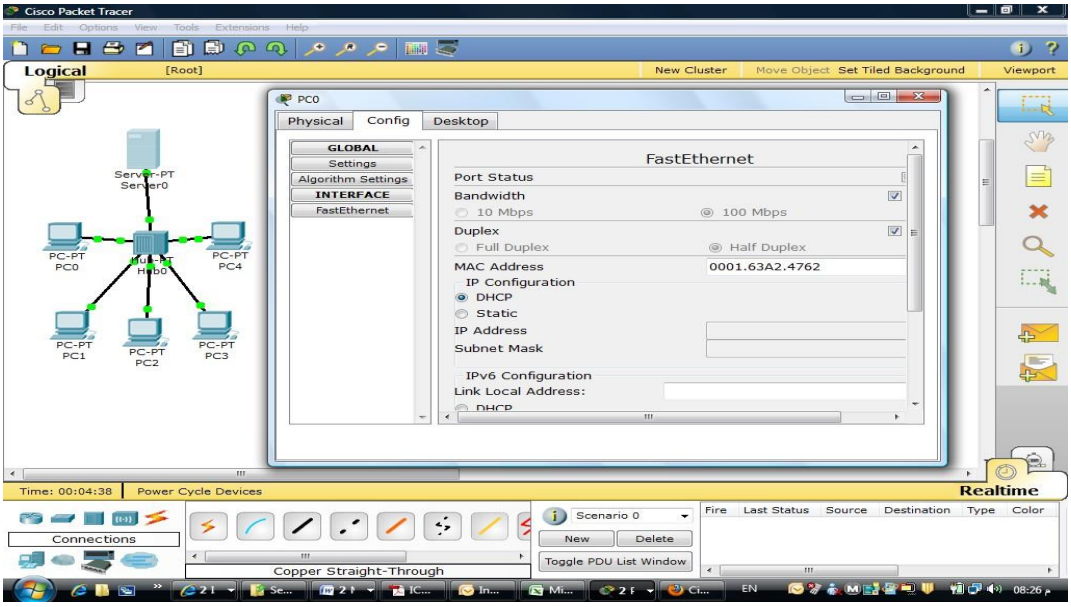
2.) Design a network with 5 PCs, 1 Server, and 1 Hub as shown in the diagram below. **Note** do ***not*** assign any IP addresses to the 5 PCs. We will configure server0 to ***automatically*** assign IP addresses from a pool of IP address range. First we will configure the client PCs to use DHCP. Click on PC0 to bring up the setup screen as below. From Global Settings click on DHCP button as shown below.

\

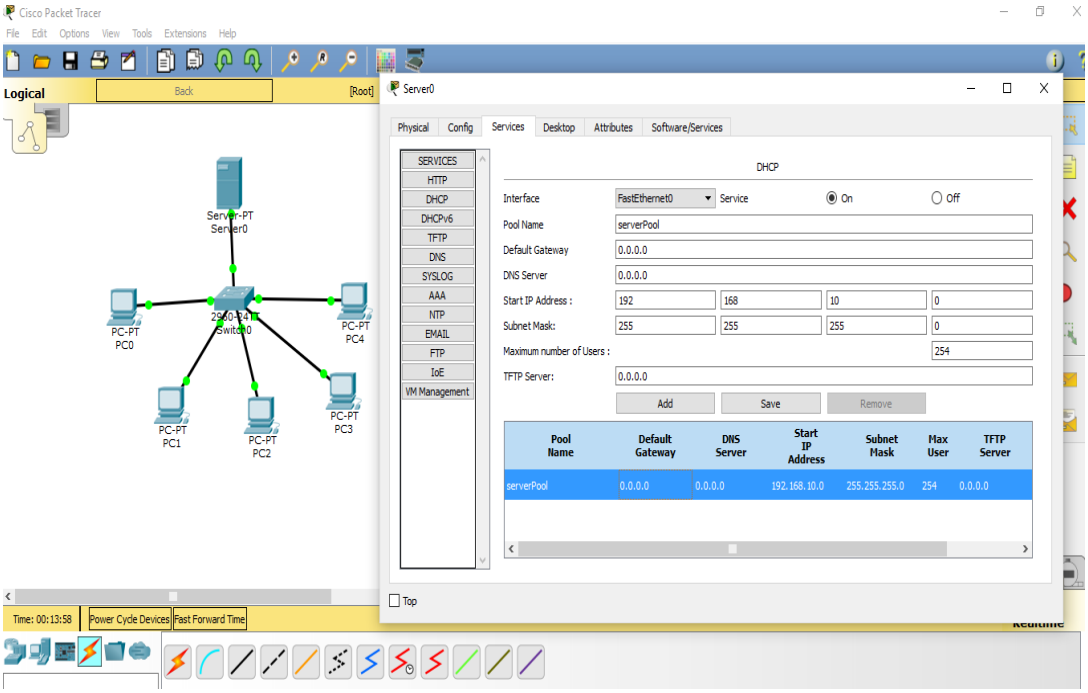


3.) Click on FastEthernet and under IP configuration click on DHCP. Once done with PCO, repeat for all other client PCs, namely, PC1, PC2, PC3, PC4. Each client PC is now configured for

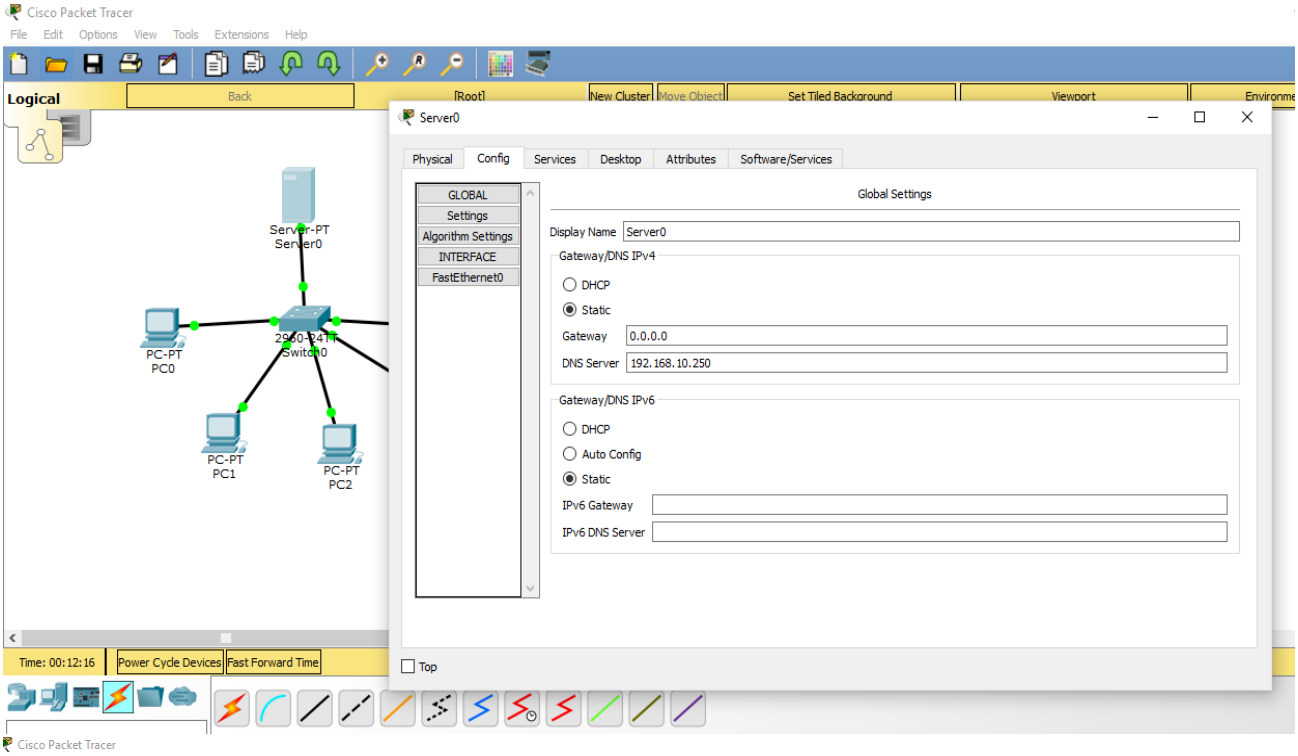
DHCP, that is whenever the client PC is powered on it will request an IP address from the DCHP server. ***NOTE: You can power ON or OFF a device by clicking on the device and then under Physical photo of the device you can switch ON by clicking 1 (on the switch) power button led will light up and clicking on 0 to switch OFF device (led will turn off). Make sure your devices are turned ON.***

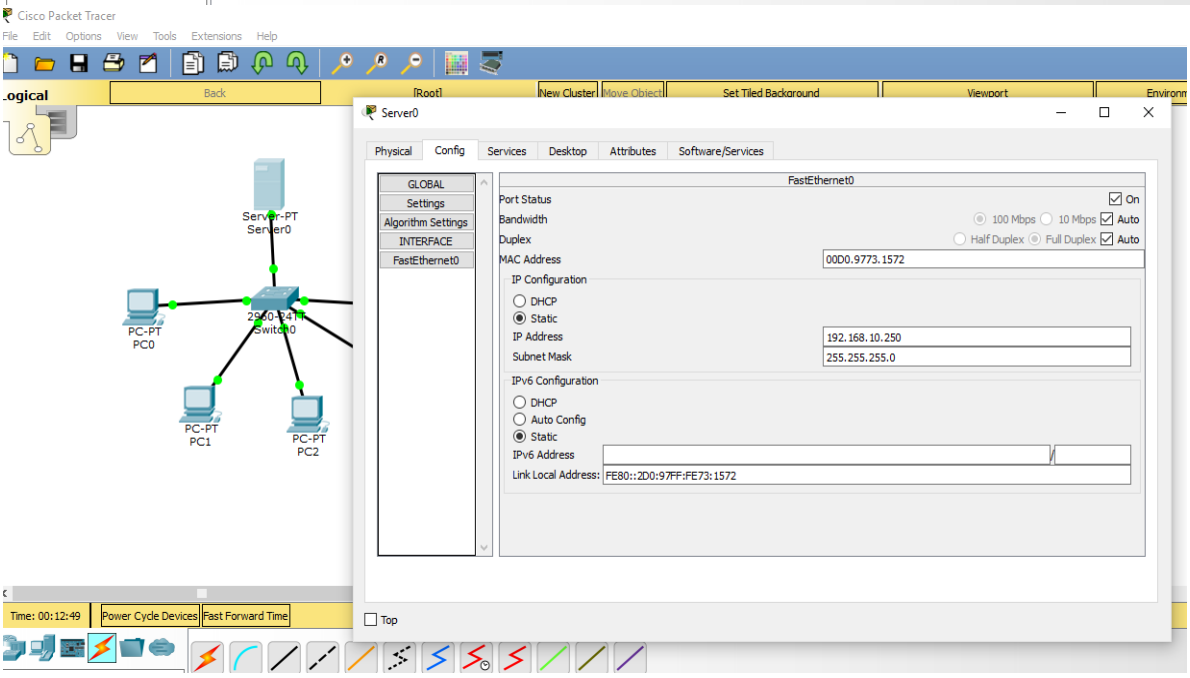


4.) Next we will configure the server0 as a DHCP server. Click on the server0 → Config → DHCP as shown below. In the DNS server box type in 192.168.10.250 for ip address. Next, in the Start IP address add 192.168.10.0 and in the Maximum number of users add 254. Then click on SAVE button.



5.) Assign a static IP address to server0 DHCP server. Click FastEthernet and assign 192.168.10.250 and 255.255.255.0 as the subnet mask. This is done only on the server0 and not the PCs. See below.

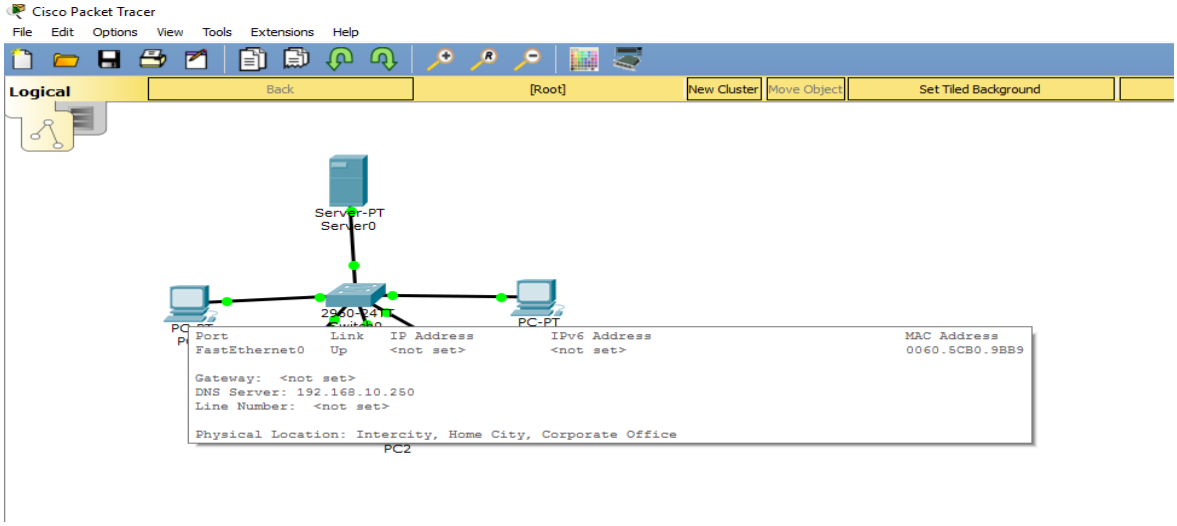




6.) Test your DHCP server is working by checking if client PCs are being assigned an IP

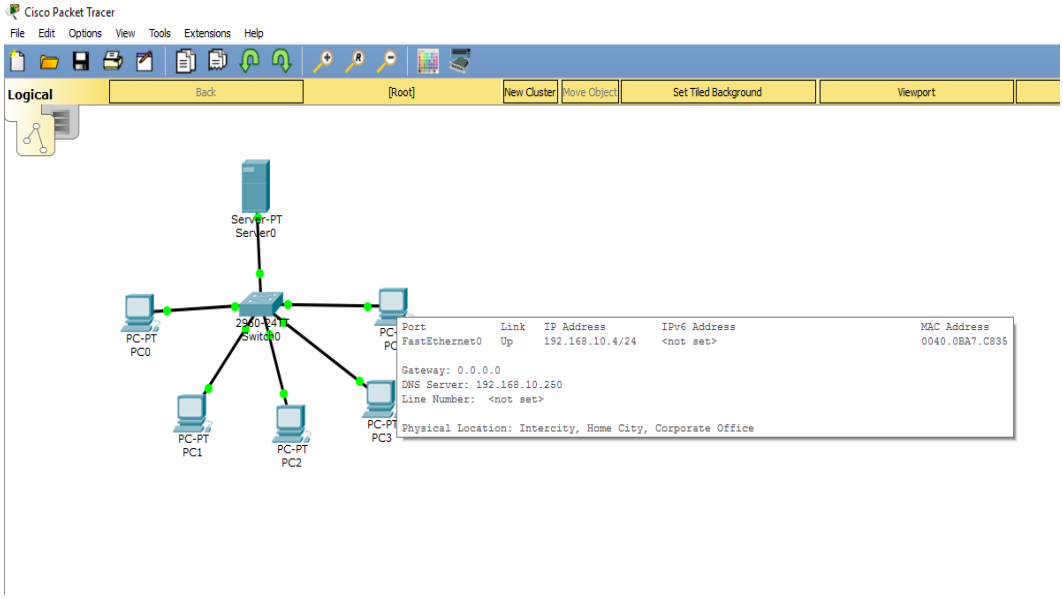
address automatically. Note: Move the mouse cursor over one of the PCs, in the Before figure below the IP address is not set.

Before Figure:



After figure: Note each PC will have an ip address assigned automatically by the DHCP server. Check by moving the mouse cursor over each PC and should see an IP address assigned from the DHCP server.

After Figure:

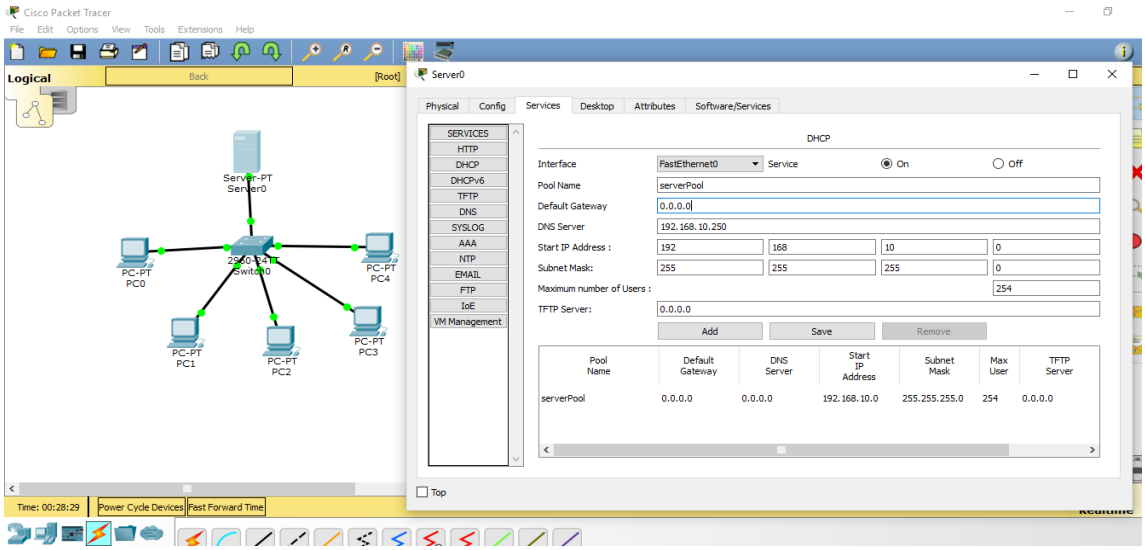


Excerises: Fill in the table below.

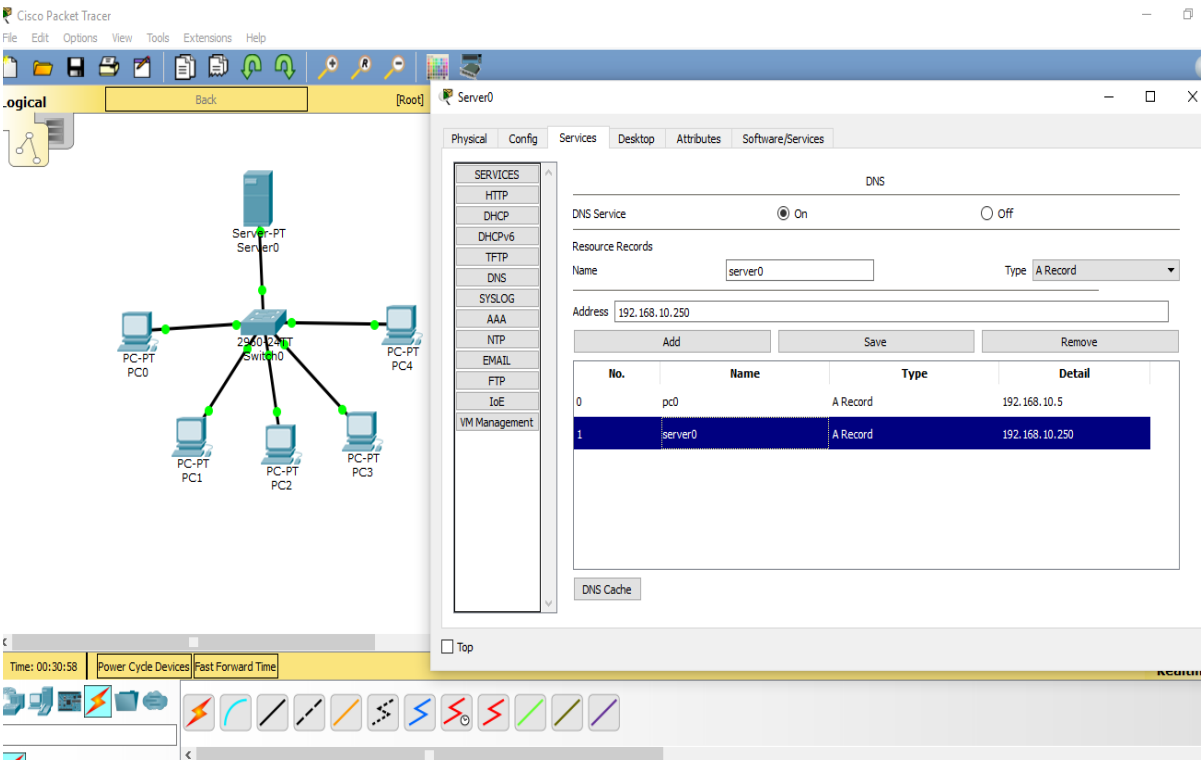
	Device	IP address	Subnet Mask	MAC Address
1	Server0	192.168.10.250	255.255.255.0	
2	PC0			
3	PC1			
4	PC2			
5	PC3			
6	PC4			

Part II. Configuring DNS server.

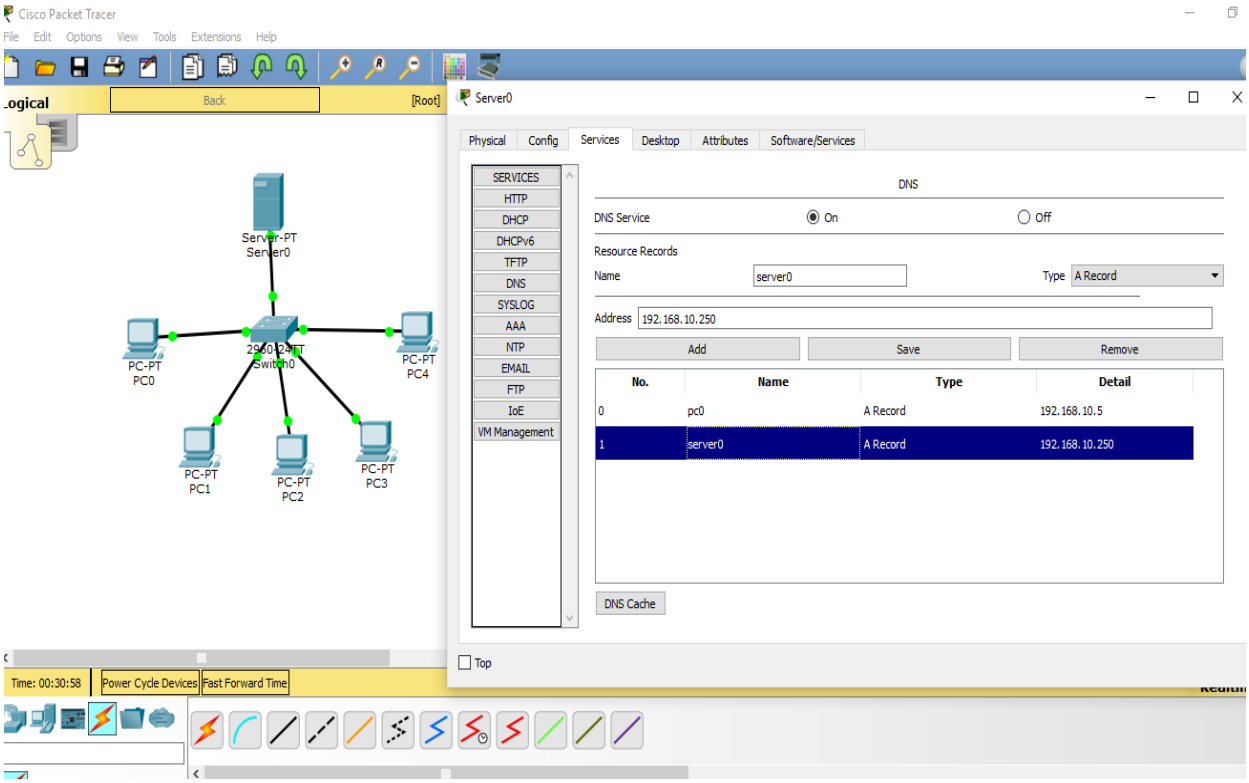
1.) Click on Server0 → Config → DHCP. In the DNS Server box type in 192.168.10.250. This will be DNS server ip address same as DHCP server ip address. Click on SAVE button.



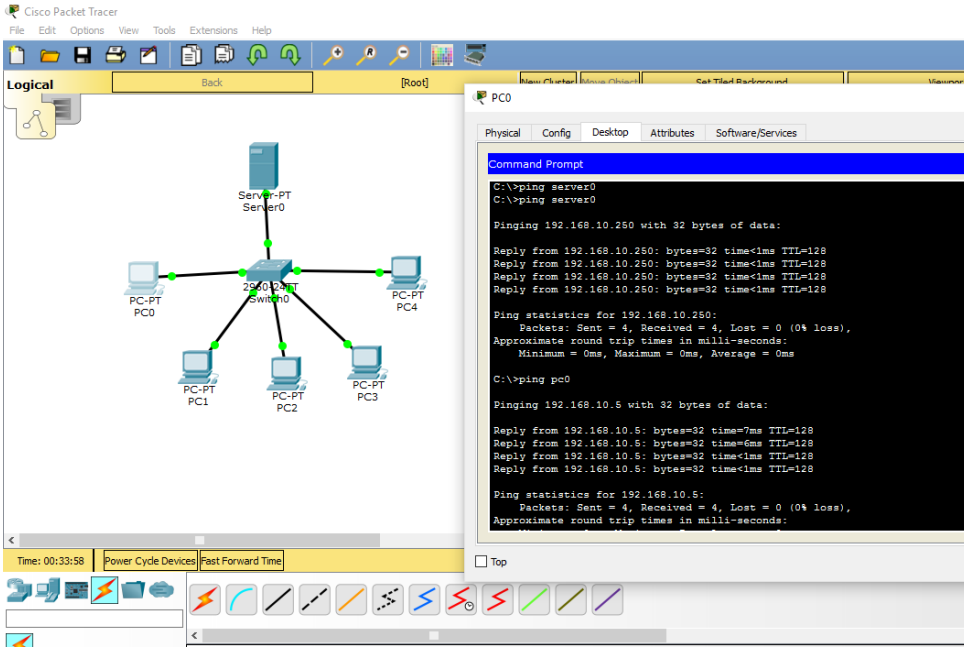
2.) Click on Server0 → Config → DNS and for Name enter server0 and for address enter 192.168.10.250 then click on Add and Save as in figure below.



3.) Next under Resource Records add name PC0 and type in the corresponding address (***DO NOT USE THE SAME IP ADDRESS SHOWN IN THE FIGURE BELOW AS YOUR PC0 IP ADDRESS WILL DEPEND ON WHAT DHCP SERVER HAS ASSIGNED TO IT***). Click Add and SAVE.



4.) Next test your DNS server is working. Click on PC0 → Desktop → Command Prompt. In the Command window type **ping server0**. Then **ping pc1**. You should get as shown below.



5.) **Note** that we are now using **ping *<u>name</u>***, where ***name*** is server0 or pc0 or pc1 etc. We do **<u>not</u>** have to use **ping *<u>ip address</u>***, because DNS is doing the translation for the name. Note in the above figure when **ping pc1** is used we get an error. Why ? Because there is no entry in the record see step 3 above. Add the information for other PCs, follow step 3 above for DNS.

6.) Use simulation mode to send PDU, follow steps of Lab # 2. Power cycle the devices and then note how different protocols are being utilized by observing the window on the right.

<u>Exercise:</u>

1 Why is DNS useful ?

2 Why is DHCP useful ?

Lab 3: IP Addressing Overview Part 1.

Objectives:

This Lab will focus on your ability to accomplish the following tasks:

- Name the five different classes of IP addresses
- Describe the characteristics and use of the different IP address classes
- Identify the Class of an IP address based on the network number
- Determine which part (octets) of an IP address is the network ID and which part is the host ID
- Identify valid and invalid IP host addresses based on the rules of IP addressing
- Define the range of addresses and default subnet mask for each class

Background:

This lab will help you develop an understanding of IP addresses and how TCP/IP networks operate. IP addresses are used to uniquely identify individual TCP/IP networks and hosts (computers and printers) on those network in order for devices to communicate. Workstations and servers on a TCP/IP network are called "HOSTS" and each will have a unique IP address which is referred to as its "HOST" address. TCP/IP is the most widely used protocol in the world. The Internet or World Wide Web uses only IP addressing. In order for a host to access the Internet, it must have an IP address.

In its basic form, the IP address has two parts; a Network Address and a Host Address. The network portion of the IP address is assigned to a company or organization by the Internet Network Information Center (InterNIC). Routers use the IP address to move data packets between networks. IP Addresses are 32 bits long (with current version IPv4) and are divided into 4 octets of 8 bits each. They operate at the network layer, Layer 3 of the OSI model, (the Internetwork Layer of the TCP/IP model) and are assigned statically (manually) by a network administrator or dynamically (automatically) by a Dynamic Host Configuration Protocol (DHCP) Server. The IP address of a workstation (host) is a "logical address" meaning it can be changed. The MAC address of the workstation is a 48-bit "physical address" which is burned into the NIC and cannot change unless the NIC is replaced. The combination of the logical IP address and the physical MAC address help route packets to their proper destination.

There are 5 different classes of IP addresses and depending on the class, the network and host part of the address will use a different number of bits. In this lab you will work with the different classes of IP addresses and become familiar with the characteristics of each. The understanding of IP addresses is critical to your understanding of TCP/IP and Internetworks in general.

Tools / Preparation:

Use Cisco Packet Tracer to design your networks.

Step 1 – Review IP Address classes and Their Characteristics.

Explanation: There are 5 classes of IP addresses (A thru E). Only the first 3 classes are used commercially. We will discuss a class A network address in the table to get started. The first column is the class of IP address. The second column is the first octet which must fall within the range shown for a given class of address. The class A address must start with a number between 1 and 126. The first bit of a class "A" address is always a zero meaning the High Order Bit (HOB) or the 128 bit cannot be used. 127 is reserved

for loop back testing. The first octet alone defines the network ID for a class A network address. The default subnet mask uses all binary ones (decimal 255) to mask the first 8 bits of the class A address. The default subnet mask helps routers and hosts determine if the destination host is on this network or another one. Since there are only 126 class A networks, the remaining 24 bits (3 octets) can be used for hosts. Each class A network can have 2^24 power (2 to the 24th power) or over 16 million hosts. It is common to subdivide the network into smaller groupings called subnets using a custom subnet mask which will be discussed in the next lab.
The network or host or host portion of the address can not be all ones or all zeros. As an example, the class A address of 118.0.0.5 is a valid IP address since the network portion (first eight bits equal to 118) is not all zeros and the host portion (the last 24 bits) is not all zeros or all ones. If the host portion were all zeros it would be the network address itself. If the host portion were all 1's it would be a broadcast for the network address. The value of any octet can never be greater than decimal 255 or binary 11111111.

Cls	**1st Octet Decimal Range**	**1st Octet High Order Bits**	**Network / Host ID (N=Network, H=Host)**	**Default Subnet Mask**	**Number of Networks**	**Hosts per Network** (usable addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 (2^7 – 2)	16,777,214 (2^{24} – 2)
B	128 – 191	1 0	N.N.H.H	255.255.0.0	16,382 (2^{14} - 2)	65,534 (2^{16} – 2)
C	192 – 223	1 1 0	N.N.N.H	255.255.255.0	2,097,150 (2^{21} – 2)	254 (2^8 – 2)
D	224 – 239	1 1 1 0	Reserved for Multicasting			
E	240 – 254	1 1 1 1 0	Experimental, used for research			

* Class A address 127 cannot be used and is reserved for loopback and diagnostic functions

Step 2 - Basic IP Addressing.

Task: Use the IP address chart and your knowledge of IP address classes to answer the following questions.

1. What is the decimal and binary range of the first octet of all possible class "B" IP addresses?
   Decimal: From:_____To: _____
   Binary: From:_____To: _____
2. Which octet(s) represent the network portion of a class C IP address? _____
3. Which octet(s) represent the host portion of a class "A" IP address?

4. Which is the maximum number of hosts you can have with a class C network address? _____
5. How many class B networks are there? _____
6. How many hosts can each class B network have? _____
7. How many octets are there in an IP address?_____How many bits per octet? _____

Step 3 – Determine the host and network portion of the IP address.

Task: With the following IP host addresses, indicate the Class of each address, the Network Address or ID, the Host portion, the Broadcast Address for this network and the default Subnet Mask.

Explanation: The host portion will be all zeros for the network ID. Enter just the octets that make up the host. The host portion will be all ones for a broadcast. The network portion of the address will be all ones for the subnet mask.

Host IP Address	Addr.Class	Network Address	Host Address	Network Broadcast Address	Default Subnet Mask
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

8. Fill in the following table:
9. Given an IP address of **142.226.0.15**
   - What is the binary equivalent of the second octet? _____
   - What is the Class of the address? _____
   - What is the network address of this IP address? _____
   - Is this a valid IP host address (Y/N) ? _____
   - Why or why not? _____
     _____
     _____
     _____

Step 4 – Determine which IP host addresses are valid for commercial networks.

Task: For the following IP host addresses determine which are valid for commercial networks. Why or why not?.

Explanation: Valid means it could be assigned to a workstation, server, printer, router interface etc.

1. Fill in the following table.

IP Address	**Valid Address? (Yes/No)**	**Why or why not?**
150.100.255.255		
175.100.255.18		
195.234.253.0		
100.0.0.23		
188.258.221.176		
127.34.25.189		
224.156.217.73		

Step 5 – Design a network using a hub or a switch with 5 PCs. You are given a Class A network address of 2.0.0.0 and subnet mask of 255.0.0.0 Assign IP addresses and subnet masks accordingly.

Lab 4: IP Addressing Part 2.

Objectives:

This Lab will focus on Class C subnet masks and your ability to accomplish the following tasks:

- Cite some reasons why a subnet mask would be needed
- Distinguish between a ***Default Subnet Mask*** and a ***Custom Subnet Mask***
- Determine the ***subnets*** available with a particular IP network address and Subnet mask
- Given a network address and requirements for how many subnets and hosts, be able to determine what subnet mask should be used
- Given a network address and a subnet mask, be able to determine the number of subnets and host per subnet that can be created as well as useable subnets and useable number of hosts
- Use the "ANDing" process to determine if a destination IP address is Local or Remote
- Identify valid and invalid IP host address based on a given a Network number and subnet mask

Background:

This lab will help you understand the basics of IP subnet masks and their use with TCP/IP networks. The subnet mask can be used to split up an existing network into "subnetworks" or "subnets". This may be done to 1) reduce the size of the broadcast domains (create smaller networks with less traffic), 2) to allow LANs in different geographical locations to communicate or 3) for security reason to separate one LAN from another. Routers separate subnets and the router determines when a packet can go from one subnet to another. Each router a packet goes through is considered a "hop". Subnet masks help workstations, servers and routers in an IP network determine if the destination host for the packet they the want to send is on their own network or another network. Default subnet masks were discussed in a prior lab. This Lab will review the Default Subnet Mask and then focus on Custom Subnet Masks which will use more bits than the default subnet mask by "borrowing" these bits from the host portion of the IP address. This creates a three-part address; 1) The original network address assigned, 2) The subnet address made up of the bits borrowed and 3) the host address made up of the bits left after borrowing some for subnets.

Tools / Preparation:

You may use Cisco Packet Tracer and/or Cisco Configmaker.

Step 1 – IP Address Basics.

Explanation: IP network addresses are assigned by the Internet Network Information Center (InterNIC). If your organization has a class "A" IP network address, the first octet (8 bits) is assigned be InterNIC and your organization can use the remaining 24 bits to define up to 16,777,214 hosts on your network. This is a lot of hosts! It is not possible to put all of these hosts on one physical network without separating them with routers and subnets. A workstation may be on one network or subnet and a server may be on another network or subnet. When the workstation needs to retrieve a file from the server it will need to use its subnet mask to determine the network or subnet that the server is on. The purpose of a subnet mask is to help hosts and routers determine the network location where a destination host can be found. Refer to the following table to review IP address classes, default subnet masks and the number of networks and hosts that can be created with each class of network address.

Cls	**1st Octet Decimal Range**	**1st Octet High Order Bits**	**Network / Host ID (N=Network, H=Host)**	**Default Subnet Mask**	**Number of Networks**	**Hosts per Network** (usable addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 (2^7 – 2)	16,777,214 (2^{24} – 2)
B	128 – 191	1 0	N.N.H.H	255.255.0.0	16,382 (2^{14} - 2)	65,534 (2^{16} – 2)
C	192 – 223	1 1 0	N.N.N.H	255.255.255.0	2,097,150 (2^{21} – 2)	254 (2^{8} – 2)
D	224 – 239	1 1 1 0	Reserved for Multicasting			
E	240 – 254	1 1 1 1 0	Experimental, used for research			

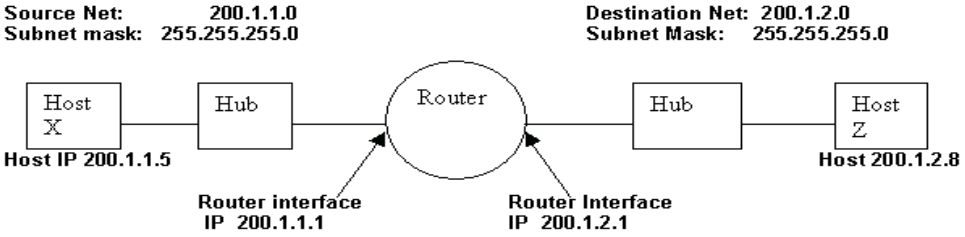
Step 2 – The "ANDing" process.

Explanation: Hosts and routers use the "ANDing" process to determine if a destination host is on the same network or not. The ANDing process is done each time a host wants to send a packet to another host on an IP network. If you want to connect to a server, you may know the IP address of the server you want to connect to or you may just enter the host name (e.g. www.cisco.com) and a Domain Name Server (DNS) will convert the host name to an IP address. First the source host will compare (AND) its own IP address to its own subnet mask. The result of the ANDing is to identify the network where the source host resides. It will then compare the destination IP address to its own subnet mask. The result of the 2nd ANDing will be the network that the destination host is on. If the source network address and the destination network address are the same they can communicate directly. If the results are different then they are on different networks or subnets and will need to communicate through routers or may not be able to communicate at all.

ANDing depends on the subnet mask. A default subnet mask for a Class C network is 255.255.255.0 or 11111111.111111111.111111111.00000000. This is compared to the source IP address bit for bit. The first bit of the IP address is compared to the first bit of the subnet mask and the second bit to the second etc. If the two bits are both ones, then the **ANDing result is a ONE**. If the two bits are a zero and a one or two zeros then the **ANDing result is a ZERO**. Basically this means that a combination of 2 ones results in a ONE, anything else is a zero. The result of the ANDing process is the network or subnet number that the source or destination address is on.

Step 3 – Two Class C networks using the default subnet mask.

Explanation: This example will show how a Class C default subnet mask can be used to determine which network a host is on. A default subnet mask does not break an address into subnets. If the default subnet mask is used then the network is not being "subnetted". Host X (source) on network 200.1.1.0 has an IP address of 200.1.1.5 and wants to send a packet to host Z (destination) on network 200.1.2.0 and has an IP address of 200.1.2.8. All hosts on each network are connected to hubs or switches and then to a router. Remember that with a Class C network address ARIN assigns the first 3 octets (24 bits) as the network address so these are two different class C networks. This leaves one octet (8 bits) for hosts so each class C network could have up to 254 hosts (2^8 power = 256 – 2 = 254).



The ANDing process will help the packet get from host 200.1.1.5 on network 200.1.1.0 to host 200.1.2.8 on network 200.1.2.0 using the following steps.

a. **Host X compares its own IP address to its own subnet mask using the ANDing process**

Host X IP address 200.1.1.5	11001000.00000001.00000001.00000101
Subnet Mask 255.255.255.0	11111111.11111111.11111111.00000000
ANDing Result (200.1.1.0)	11001000.00000001.00000001.00000000

NOTE: The result of step 3a of the ANDing process is the network address of host X which is 200.1.1.0

b. **Next host X compares the IP address of the Host Z destination to its own subnet mask using the ANDing process.**

Host Z IP address 200.1.2.8	11001000.00000001.00000010.00001000
Subnet Mask 255.255.255.0	11111111.11111111.11111111.00000000
ANDing Result (200.1.2.0)	11001000.00000001.00000010.00000000

NOTE: The result of step3b ANDing process is the network address of host Z which is 200.1.2.0.
Host X compares the ANDing results from step A and the ANDing result from step B and they are different. Host X now knows that host Z is not in its Local Area Network (LAN) and it must send the packet to its "Default Gateway" which is the IP address of the router interface of 200.1.1.1 on network 200.1.1.0. The router will then repeat the ANDing process to determine which router interface to send the packet out.

Step 4 – One Class C network using a Custom subnet mask.

Explanation: This example uses a single Class C network address (200.1.1.0) and will show how a class C custom subnet mask can be used to determine which subnetwork (or subnet) a host is on and to route packets from one subnetwork to another. Remember that with a class C network address ARIN assigns the first 3 octets (24 bits) as the network address. This leaves 8 bits (one octet) for hosts so each class C network could have up to 254 hosts (2^8 power = 256 – 2 = 254).
Perhaps you want less than 254 host (workstations and servers) all on one network and you want to create 2 sub-networks and separate them with a router for security reason or to reduce traffic. This will create smaller independent broadcast domains and can improve network performance and increase security since these subnetworks will be separated by a router. Assume you will need at least 2 subnetworks and at least 50 hosts per subnetwork. Since you only have one Class C network address you have only 8 bits in the fourth octet available for a total of 254 possible hosts, you must create a Custom Subnet mask. You will use the custom subnet mask to "BORROW" bits from the host portion of the address. The following steps will help accomplish this:

a. The first step to "subnetting" is to determine how many subnets are needed. In this case you will need 2 subnetworks. To see how many bits you should borrow from the host portion of the network address, add the bit values from right to left until the total is equal to or greater than the number of subnets you will need. Since we need 2 subnets, add the one bit and the two bit which equals three. This is over the number of subnets we need, so we will need to borrow at least two bits from the host address starting from the left side of the octet that contains the host address.

Network address: 200.1.1.0

4th octet Host address bits:	1	1	1	1	1	1	1	1
Host address bit values (from right)	128	64	32	16	8	4	**2**	**1**

(Add bits starting from the right side (the 1 and the 2) until you get more than the number of subnets needed)

b. Once we know how many bits to borrow we take them from the left side of the first octet of the host address. Every bit we borrow from the host leaves fewer bits for the hosts. Even though we increase the number of subnets, we decrease the number of hosts per subnet. Since we need to borrow 2 bits from the left side, we must show that new value in our subnet mask. Our existing default subnet mask was 255.255.255.0 and our new "Custom" subnet mask is 255.255.255.192. The 192 comes from the value of the first two bits from the left (128 + 64 = 192). These bits now become 1s and are part of the overall subnet mask. This leaves 6 bits for host IP addresses or 2^6 = 64 hosts per subnet.

4th Octet borrowed bits for subnet:	**1**	**1**	1	1	1	1	1	1
Subnet bit values: (from left side)	128	64	32	16	8	4	2	1

With this information you can build the following table. The first two bits are the Subnet binary value. The last 6 bits are the host bits. By borrowing 2 bits from the 8 bits of the host address you can create 4 subnets with 64 hosts each. The 4 networks created are the "0" net, the "64" net, the "128" net and the "192" net. The "0" net and the "192" net are considered unusable. This is because the "0" net has all zeros in the subnet portion of the address and the 192 net has all ones in the subnet portion of the address.

Subnet No.	Subnet bits borrowed Binary value	Subnet bits Decimal Value	Host bits possible binary values (range) (6 bits)	Subnet / Host Decimal range	Useable?
Subnet #0	00	0	000000 – 111111	0 – 63	NO
Subnet #1	01		64 000000 – 111111	64 – 127	YES
Subnet #2	10		128 000000 – 111111	128 – 191	YES
Subnet #3	11		192 000000 – 111111	192 – 254	NO

Notice that the first subnet always starts at 0 and, in this case, increases by 64 which is the number of hosts on each subnet. One way to determine the number of hosts on each subnet or the start of each subnet is to take the remaining host bits to the power of 2. Since we borrowed two of the 8 bits for subnets and have six bits left, the number of hosts per subnet is 2^6 or 64. Another way to figure the number of host per subnet or the "increment" from one subnet to the next is to subtract the subnet mask value in decimal (192 in the fourth octet) from 256 (which is maximum number of possible combinations of 8 bits) which equals 64. This means you start at 0 for the first network and add 64 for each additional subnetwork. If we take the second subnet (the 64 net) as an example the IP address of 200.1.1.64 cannot be used for a host ID because it is the "network ID" of the "64" subnet (host portion is all zeros) and the IP address of 200.1.1.127 cannot be used because it is the broadcast address for the 64 net (host portion is all ones).

Step 5 – One Class C network using a Custom Subnet Mask.

Task: Use the following information and the previous examples to answer the following subnet related questions.

Explanation: Your company has applied for and received a Class C network address of 197.15.22.0. You want to subdivide your physical network into 4 subnets, which will be interconnected by routers. You will need at least 25 hosts per subnet. You will need to use a Class C custom subnet mask and will have a router between the subnets to route packet from one subnet to another. Determine the number of bits you will need to borrow from the host portion of the network address and then the number of bits left for host addresses. (Hint: There will be 8 subnets)

Fill in the table below and answer the following questions:

Subnet No.	Subnet bits borrowed Binary value	Subnet bits Decimal & Subnet No.	Host bits possible binary values (range) (6 bits)	Subnet / Host Decimal range	Use?
Subnet #0					
Subnet #1					
Subnet #2					
Subnet #3					
Subnet #4					
Subnet #5					
Subnet #6					
Subnet #7					

QUESTIONS: Use the table you just developed above to help answer the following questions:

1. Which octet(s) represent the network portion of a Class C IP address? _____
2. Which octet(s) represent the host portion of a Class C IP address? _____
3. What is the binary equivalent of the Class C network address in the scenario (**197.15.22.0** Binary Network address: _____._____._____._____
4. How many high-order bits were borrowed from the host bits in the fourth octet? _____
5. What subnet mask must you use (show the subnet mask in decimal and binary)? Decimal Subnet mask:_____._____._____._____ Binary subnet mask._____
6. What is the maximum number of subnets that can be created with this subnet mask? _____
7. What is the maximum number of useable subnets that can be created with this mask? _____
8. How many bits were left in the 4 the octet for host IDs? _____
9. How many hosts per subnet can be defined with this subnet mask? _____
10. What is the maximum number of hosts that can be defined for all subnets with this scenario (assuming you cannot use the lowest and highest subnet numbers and cannot use the lowest and highest host ID on each subnet) ? _
11. Is **197.15.22.63** a valid host IP address with this scenario? _____
12. Why or why not ? _____
13. Is **197.15.22.160** a valid host IP address with this scenario? _____
14. Why or why not ? _____

Host "A" has an IP address of **197.15.22.126**. Host "B" has an IP address of **197.15.22.129**. Are these hosts on the same subnet? _____Why?

Lab 5: Routers Part 1.

Objectives:

- *Login to a router in both user and privileged modes.*
- *Use several basic router commands to configure router interfaces.*
- *Use ping command to check connectivity between different networks.*
- *To learn the purpose and use of routers.*

Background:

This lab will introduce the Cisco Internetwork Operating System (IOS) command line user interface. You will login to the router and use different levels of access to enter commands in "User Mode" and "Privileged Mode". You will become familiar with the commands available in each mode (User or Privileged). The IOS command interface is the most common method of configuring a Cisco router. You will see many commands available, especially in privileged mode. Do not be overwhelmed. As with many things, the 80/20 rule applies. You can do 80% of what you need to do on a daily basis with 20% of the commands available.

Tools / Preparation:

You will need to become familiar with these commands:

1. *Enable*
2. *Config terminal*
3. *Interface*
4. *Ip address*
5. *No shutdown*
6. *Pressing the keys Cntrl-Z on the keyboard.*
7. *Copy running start-up*

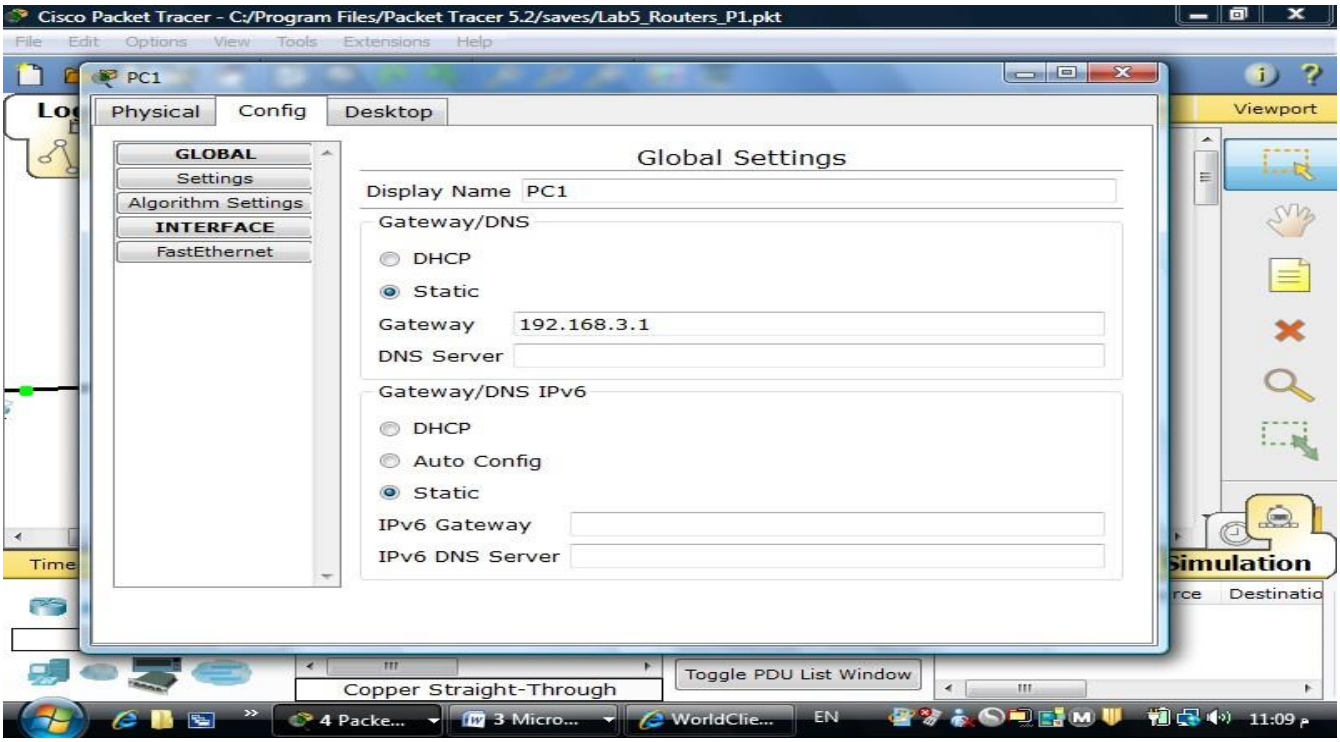
Resources Required in the Packet tracer:

- *4 PCs with 2 switches and 1 Cisco 2811 router.*

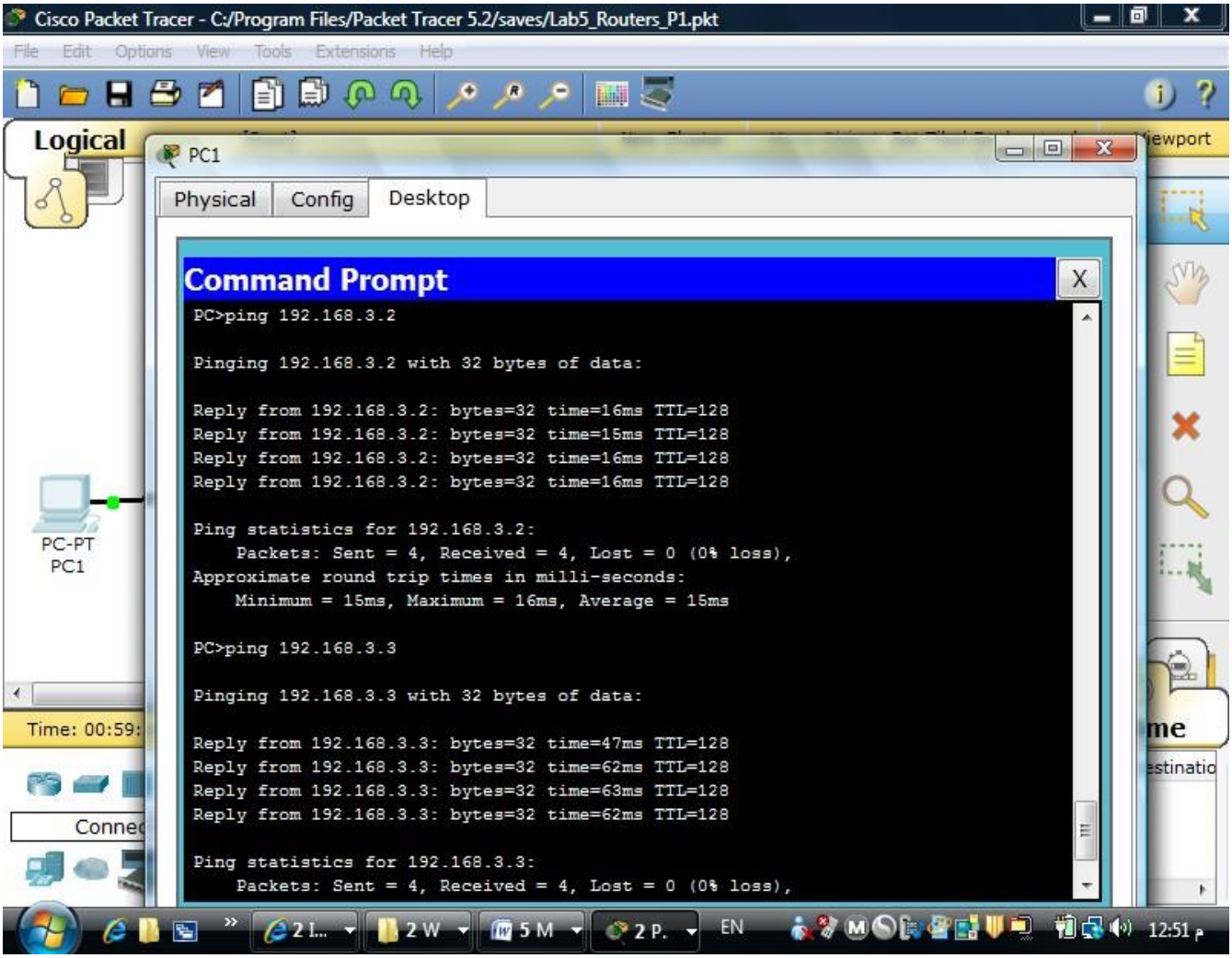
Step 1: *Open Packet tracer and design a network as shown in figure below. Use the same type of devices as shown in the figure, for router choose Cisco 2811, for switches choose 2960. In this step only assign IP addresses to the PCs and also assign gateway addresses on the PCs. In the following steps you will assign IP addresses to the Router interfaces. Assign IP addresses as follows:*

Device	IP address	Gateway Address
PC1	192.168.3.2	192.168.3.1
PC2	192.168.3.3	192.168.3.1
PC3	192.168.4.2	192.168.4.1
PC4	192.168.4.3	192.168.4.1
Router fastethernet0/0	192.168.3.1	
Router fastethernet0/1	192.168.4.1	

Note: *It is extremely important you assign the gateway addresses on the PCs under config menu → global → settings.*


Cisco Packet Tracer - C:/Program Files/Packet Tracer 5.2/saves/Lab5_Routers_P1.pkt
File Edit Options View Tools Extensions Help
PC1
Physical
Config
Desktop
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet
Global Settings
Display Name PC1
Gateway/DNS
DHCP
Static
Gateway 192.168.3.1
DNS Server
Gateway/DNS IPv6
DHCP
Auto Config
Static
IPv6 Gateway
IPv6 DNS Server
Viewport
Simulation
Time
Destinatio
Toggle PDU List Window
Copper Straight-Through
4 Packe...
3 Micro...
WorldClie...
EN
11:09

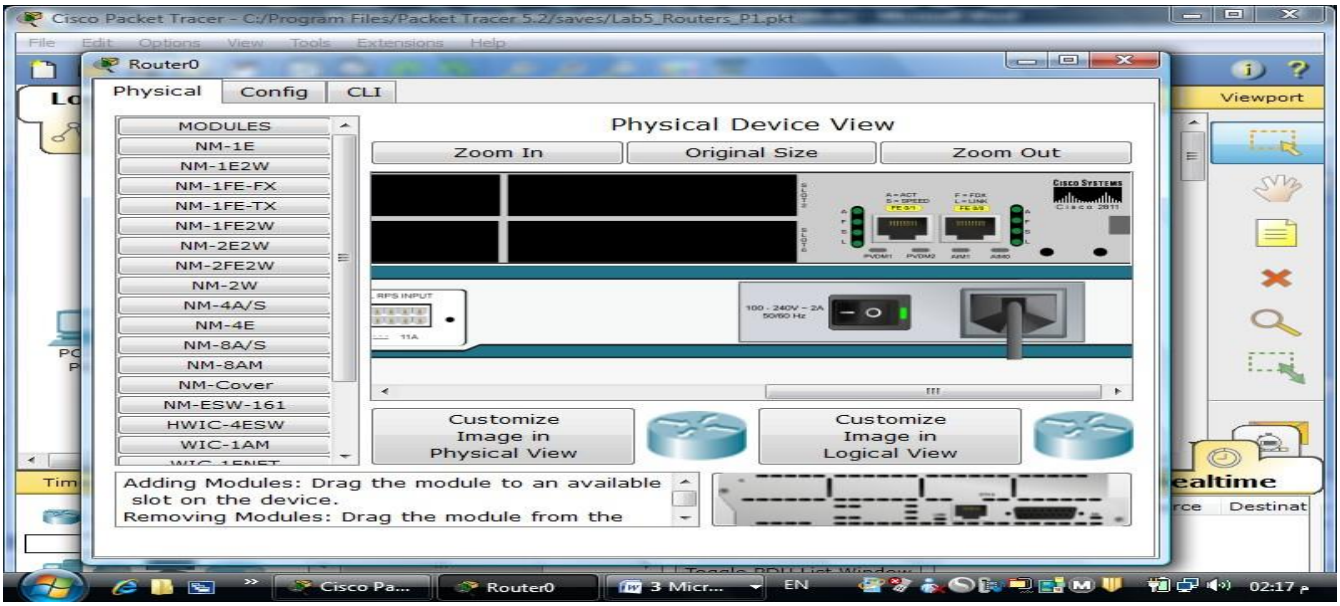
Step 2: Click on PC1 and from the Command Prompt use the ping command and ping the PCs on the same switch. For example, ***ping 192.168.3.2*** and ***ping 192.168.3.3***. See figure below.



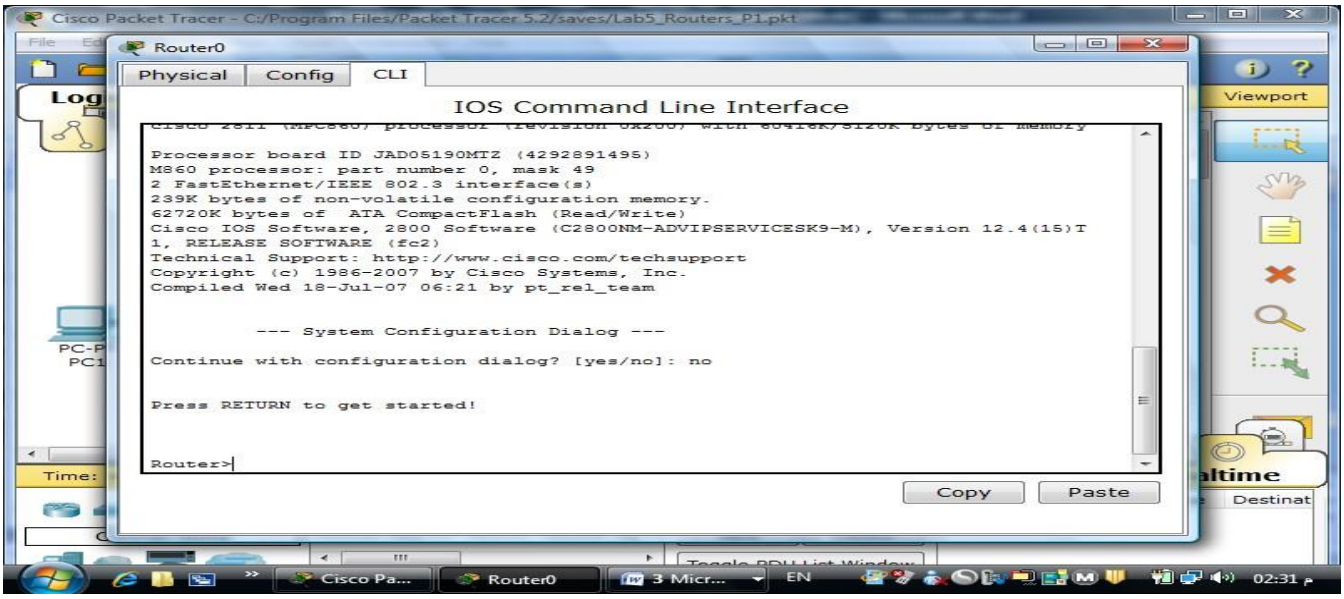
Step 3: From PC1 **ping 192.168.4.2**. What do you get ? Request timed out, because router is not configured yet.

Step 4*. Click on PC3 and from Command prompt use Ping command.* ***Ping 192.168.4.3*** *what do you observe ? There will be a reply, because PC3 and PC4 are on the same network.*

Step 5*. In order for pinging to work from one network to another network we need to configure the router to perform routing. First of all click on router and let us see the physical device. Below is a figure of router's physical look, note if you click on the button 0/1 (green light), you will either turn on (green light) or turn off (green light off) the router. Turning on the router will boot the router. So make sure the router is turned on to do the configuration.*



***Step 6**: Next click on CLI from Router0. You should see as in figure below.*

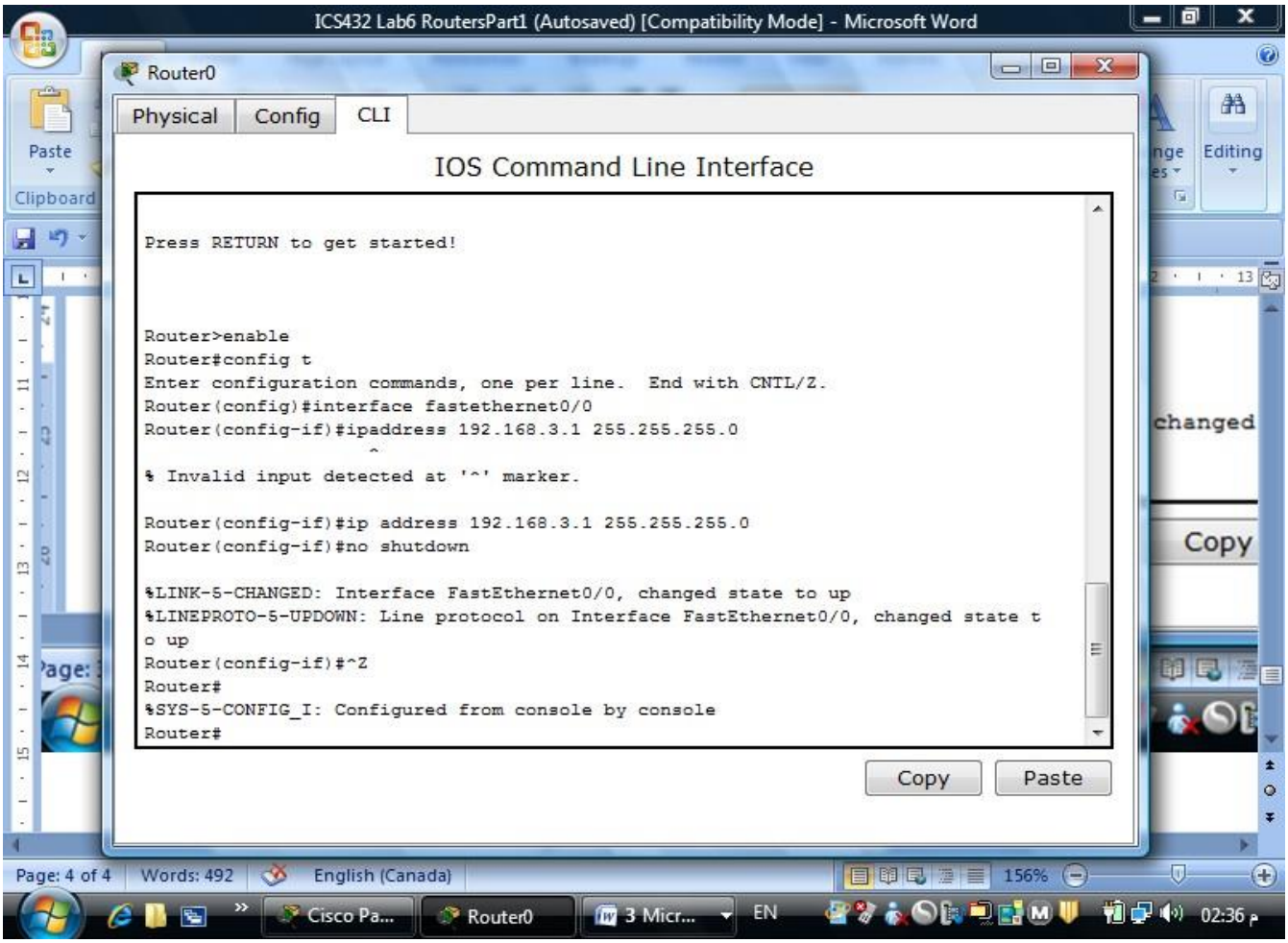


To configure the fastethernet0/0 port on router0, type the following:

- *enable*
- *config t*
- *interface fastethernet0/0*
- *ip address 192.168.3.1 255.255.255.0*
- *no shutdown*
- *press CNTRL-Z*

Note: at the start you see in the interface: router > this means the router is in user mode, when you type "enable" at the prompt you will see router# note the # indicates router is in privilege mode. In this mode you can do the

configuring . The interface command is used to specify which interface to configure, the ip address command is used to specify an address and subnet mask to assign the interface chosen in 2. No shutdown is used to bring the interface up into operation. Last cntrl-z is pressed to exit from the mode and go back.



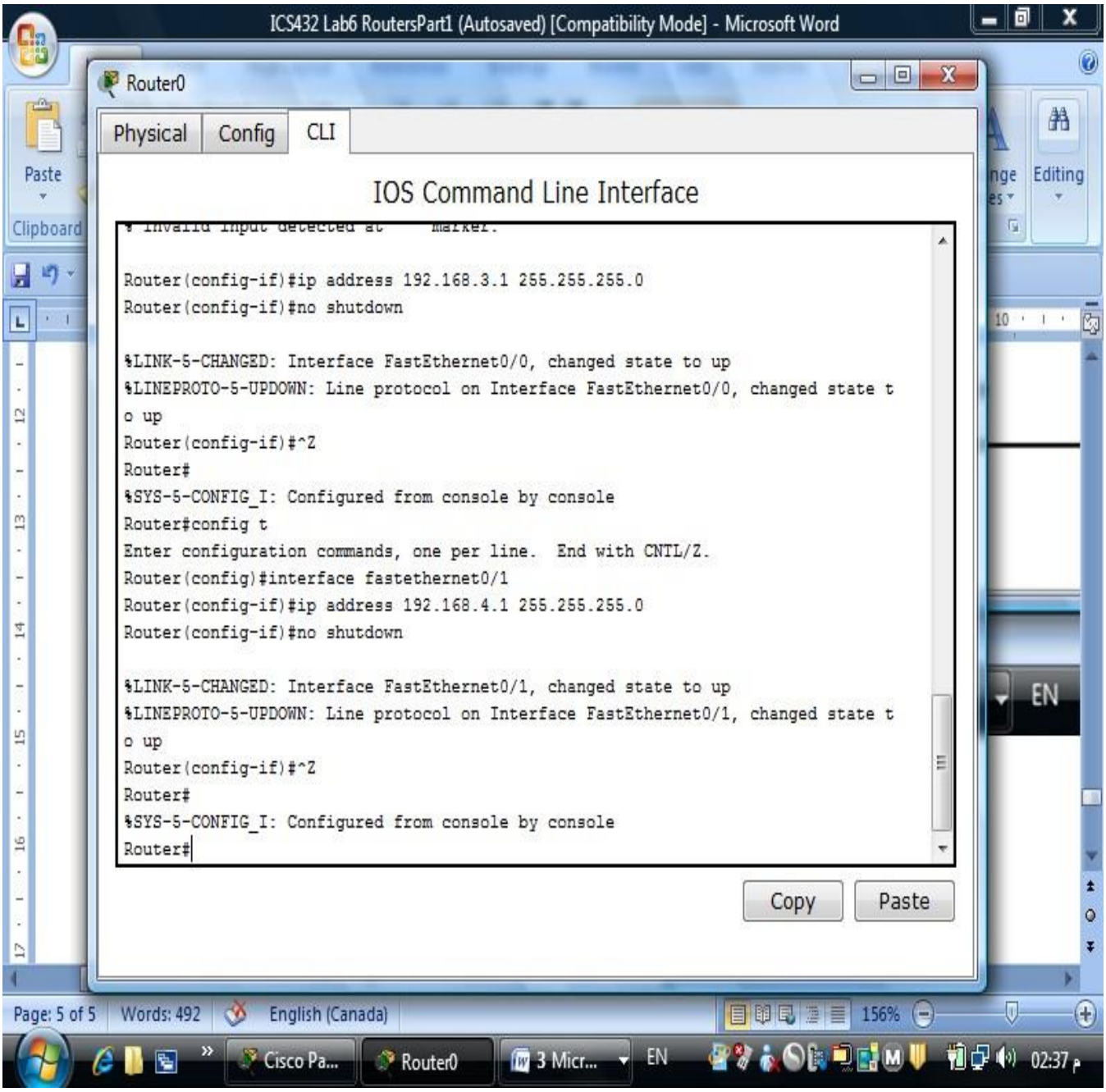
Similarly do the configuration for the 2nd port fastethernet0/1 on the router0. Type in the following commands.

1. *config t*
2. *interface fastethernet0/1*

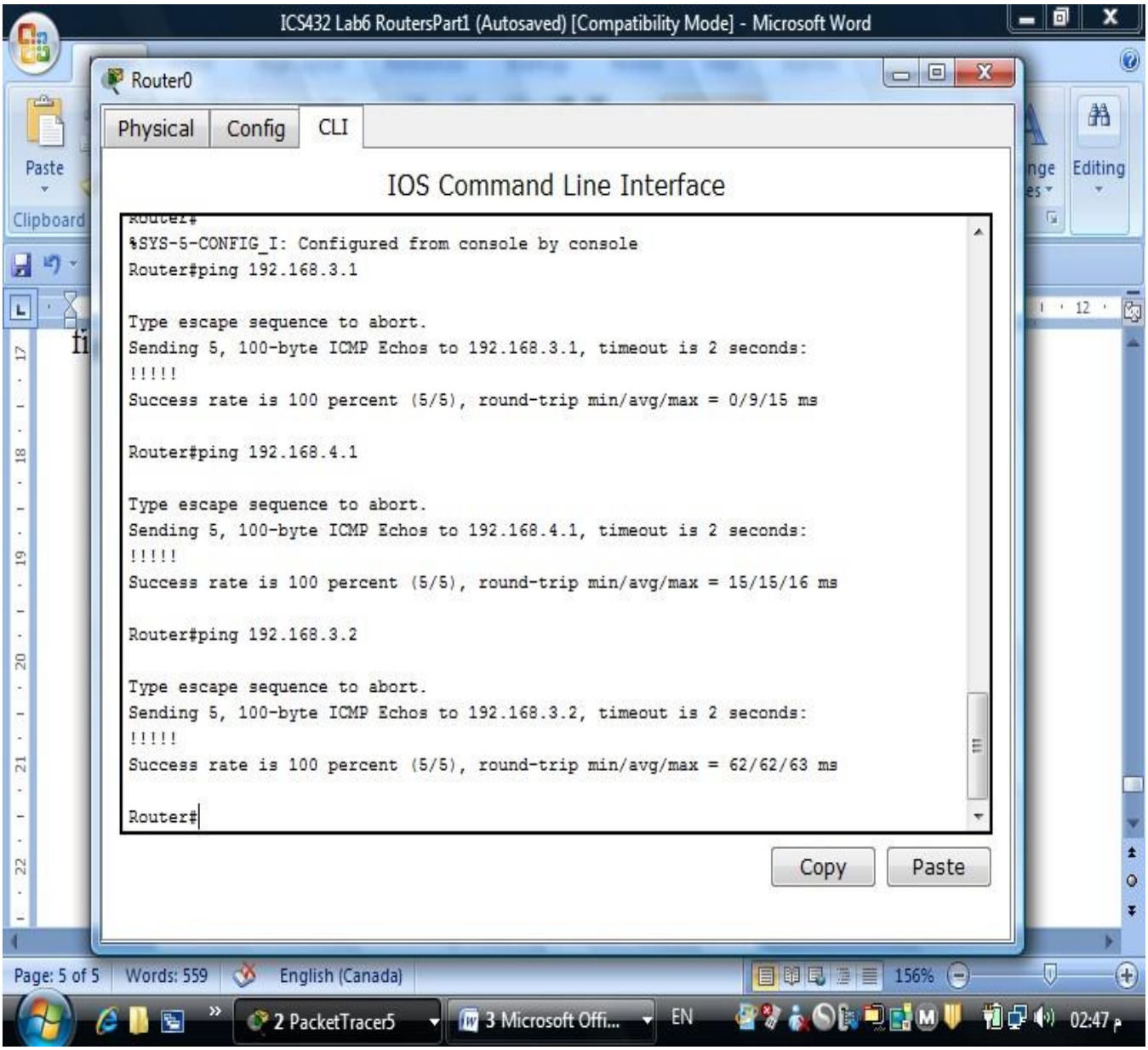
3. *ip address 192.168.4.1 255.255.255.0*
4. *no shutdown*
5. *cntrl-z*

You must type the following command to save whatever configuration you have done on the router otherwise you will lose the current configuration.

Router > **copy running start** see one of the figures below.

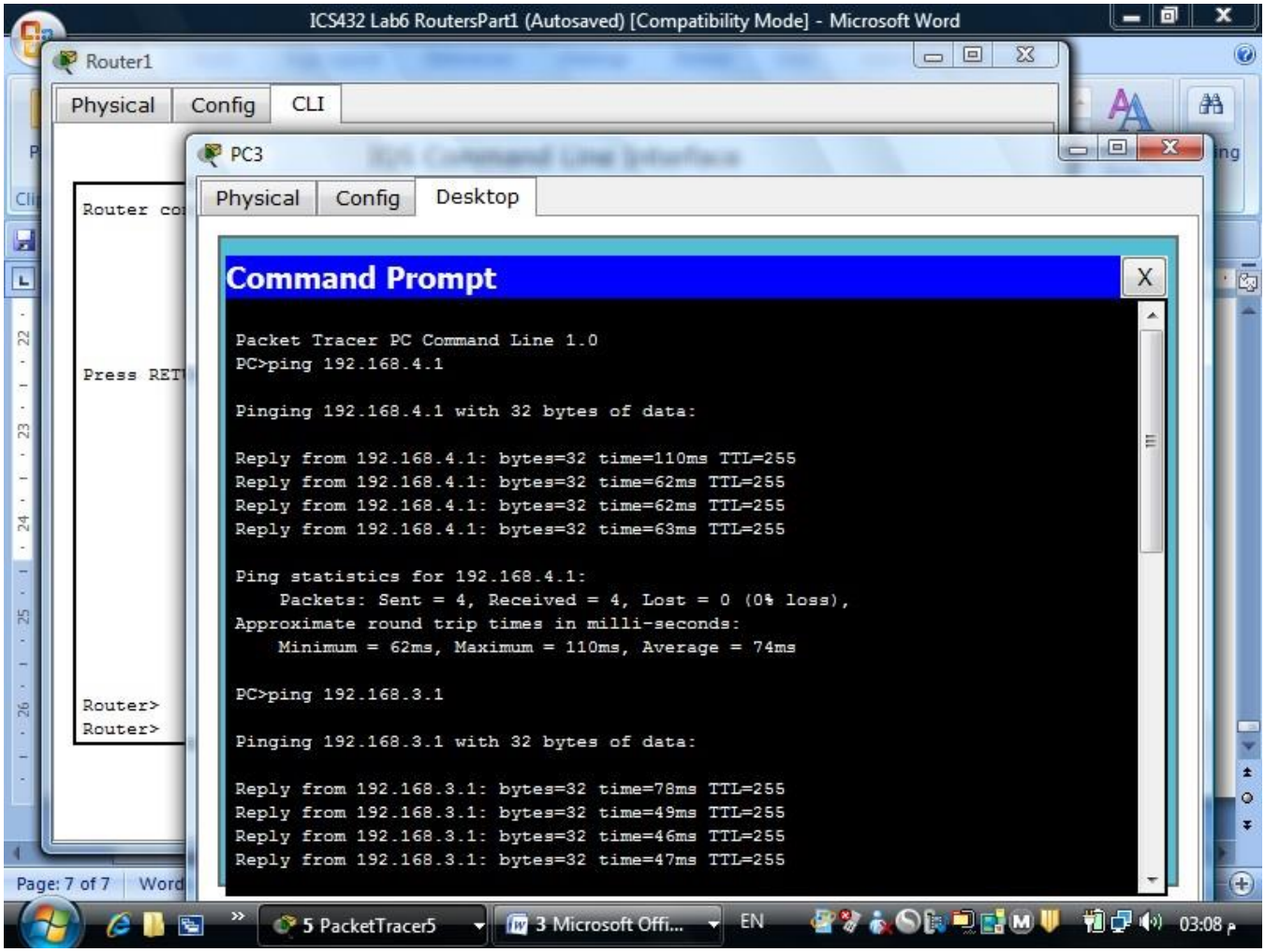


From the router interface you should be able to ping the router interfaces and the PCs on either switches. Do as shown in the figure below.



From any PC click on Command Prompt and do as below, ping 192.168.3.1 , ping 192.168.3.2, ping 192.168.3.3, ping 192.168.4.1, ping 192.168.4.2, ping 192.168.4.3, ping 192.168.4.9 . What do you observe ?

There will be reply from each indicating there is connection except 192.168.4.9 which does not exist on the network



Questions:

1. *Given 192.168.3.1 and subnet mask 255.255.255.0 what is the network address?*
2. *Given 192.168.4.57 and subnet mask 255.255.255.0 what is the network address?*
3. *Why do we use switches ?*
4. *Why do we use routers ?*
5. *What is a gateway address ?*
6. *What happens if you forget to assign a gateway address on a PC ?*
7. *When you type **?** at the router prompt, what do you see ?.*
8. When you type **show interfaces**, observe what you see.
9. When you type **show ip route**, observe what you see.
10. When you type **show protocols**, observe what you see.

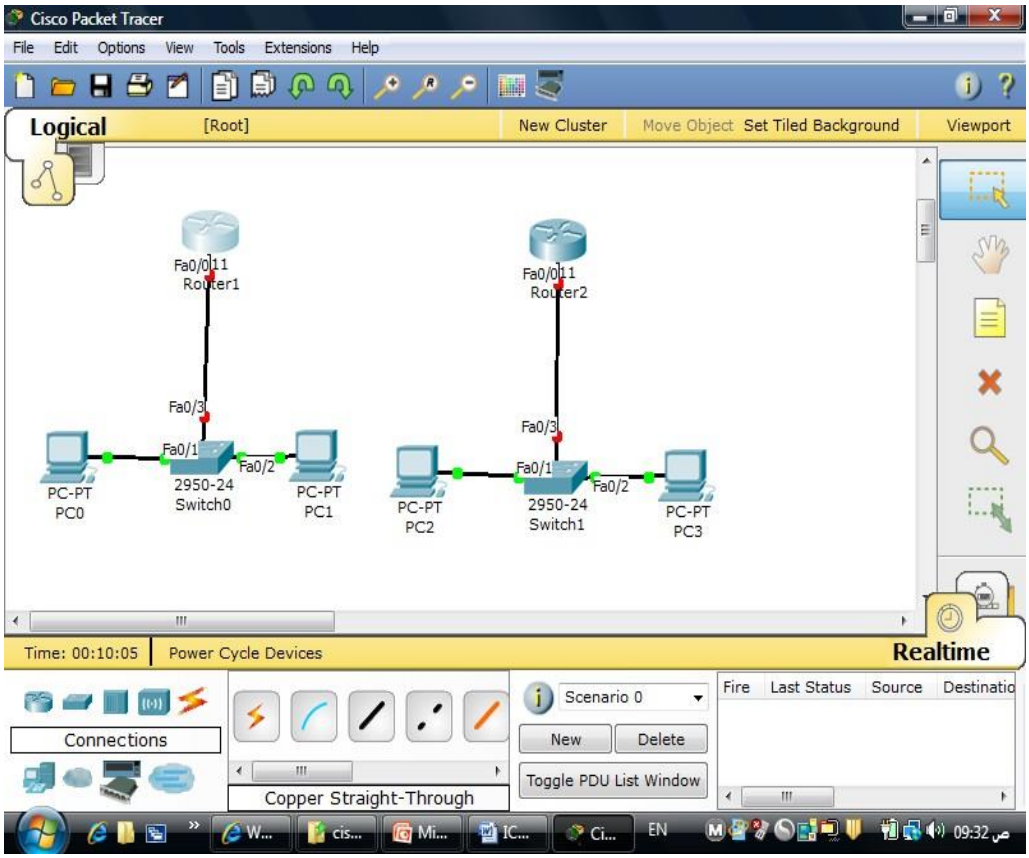
Lab 6: Two Router Serial Connection

Objectives:

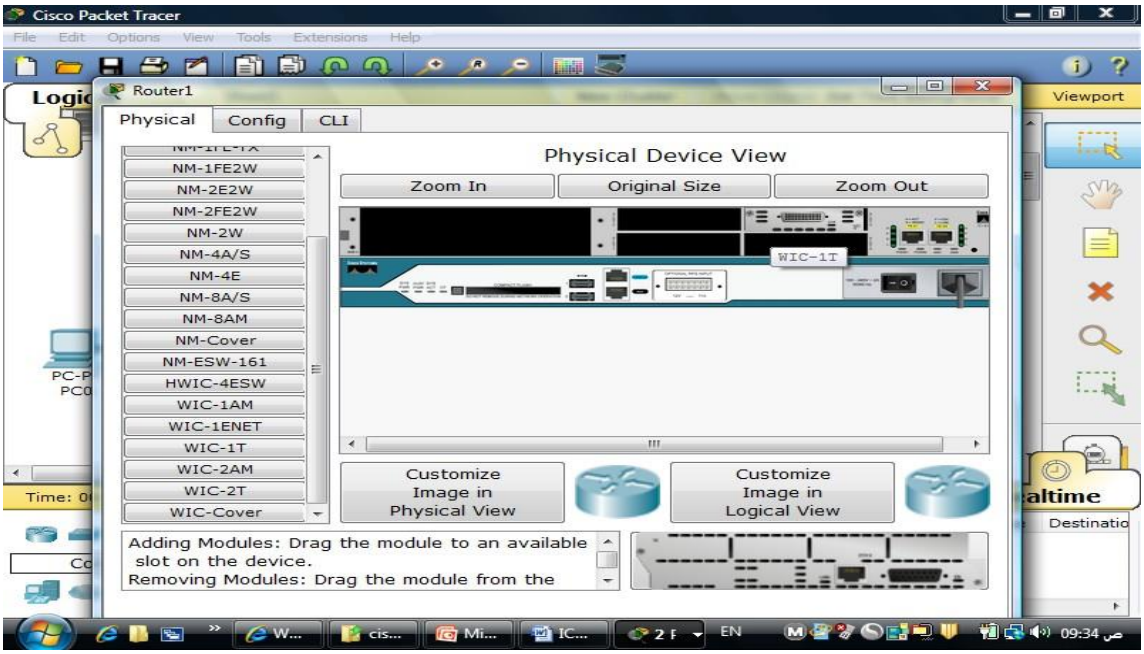
- *To configure serial interfaces between 2 routers*
- *To know what is DTE and DCE and configuring each side*
- *To review some common commands*

Step 1: Setup a network with 2 routers (2811), 2 switches, 4 PCs as shown below. Assign IP addresses as follows:

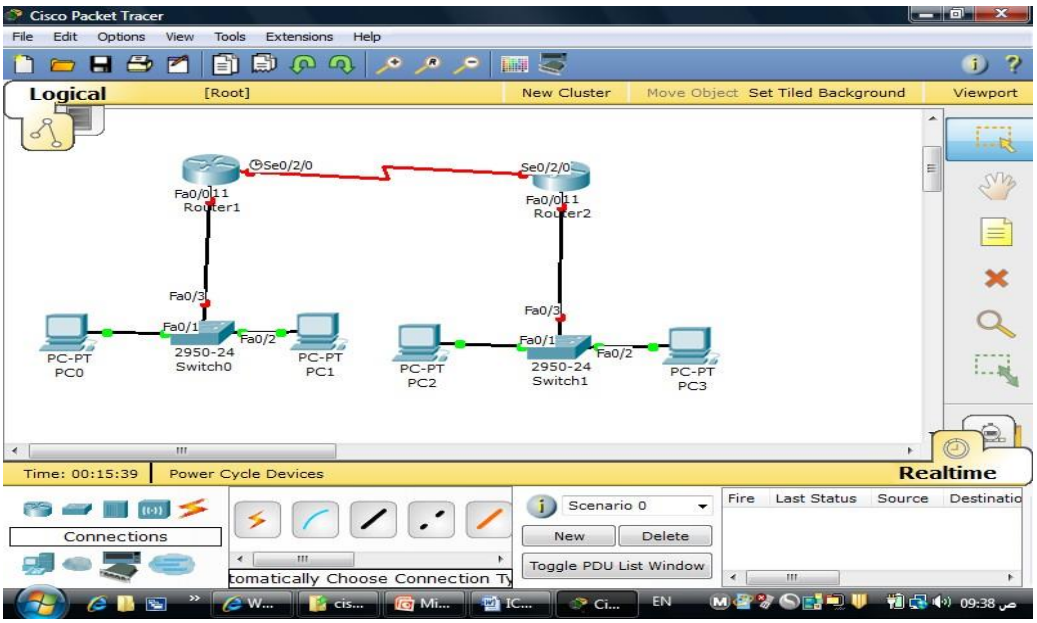
	Interface	IP address	Subnet Mask
Router 1	Fastethernet	192.168.1.1	255.255.255.0
Router 2	Fastethernet	192.168.2.1	255.255.255.0
Router 1	Serial Interface	193.100.200.1	255.255.255.0
Router 2	Serial interface	193.100.200.2	255.255.255.0
PC0		192.168.1.2	255.255.255.0
PC1		192.168.1.3	255.255.255.0
PC2		192.168.2.2	255.255.255.0
PC3		192.168.2.3	255.255.255.0


Cisco Packet Tracer
File Edit Options View Tools Extensions Help
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Fa0/0
Router1
Fa0/0
Router2
Fa0/3
Fa0/1
Fa0/2
2950-24
Switch0
PC-PT
PC0
PC-PT
PC1
Fa0/3
Fa0/1
Fa0/2
2950-24
Switch1
PC-PT
PC2
PC-PT
PC3
Time: 00:10:05
Power Cycle Devices
Realtime
Connections
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destinatio
EN
09:32 ص

Click on router 1, turn off the router by clicking on the on/off switch on the router. From Physical menu insert a module named wic-1T in the slot as shown in figure below. This is done by dragging the module from left and placing it in the slot in the physical device view. Similarly do for the other router 2, add a module wic-1T.



Next from the cable selection, choose the first cable (automatically choose connection). Drag it from router 1 to router 2. Note: the clock icon appears on the left router 1 side (see figure). This serial connection (serial0/2) is called the DCE (Data Communication Equipment). On router 2 side the serial interface (serial0/2) is called the DTE (Data terminal equipment).



Next we need to configure the serial interfaces. From the CLI mode of router 1. Type the following commands.

Router> enable

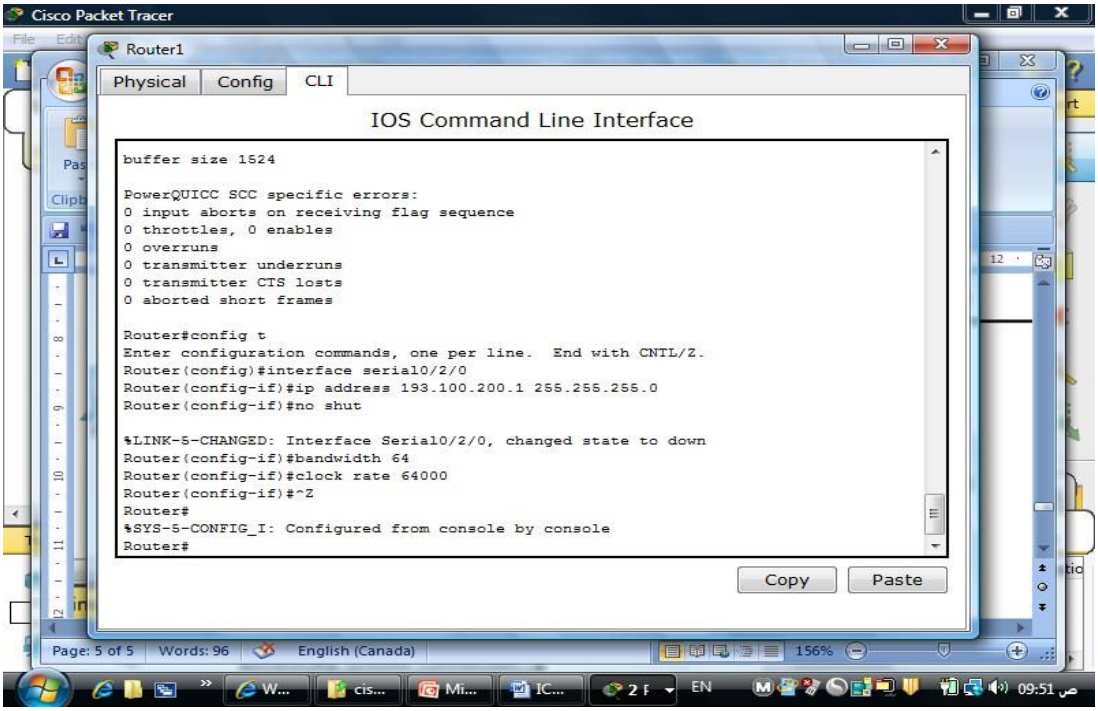
Router# config t

interface serial/0/2/0

ip address 193.100.200.1 255.255.255.0

no shutdown
bandwidth 64

clock rate 64000 (Note: this command only on DCE side) cntrl-z



copy running startup

Similarly, configure the serial interface (serial0/2/0) on router 2. From the CLI mode of router 2. Type the following commands.

Router> enable

Router# config t
interface serial/0/2/0

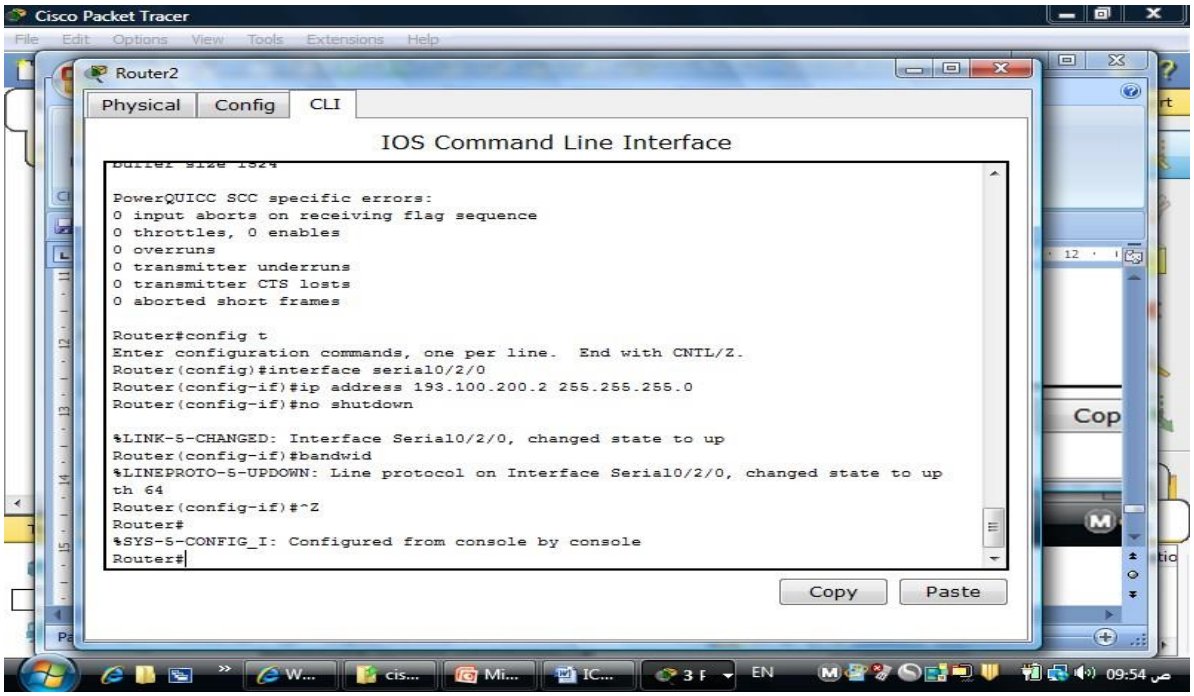
ip address 193.100.200.2 255.255.255.0

no shutdown
bandwidth 64

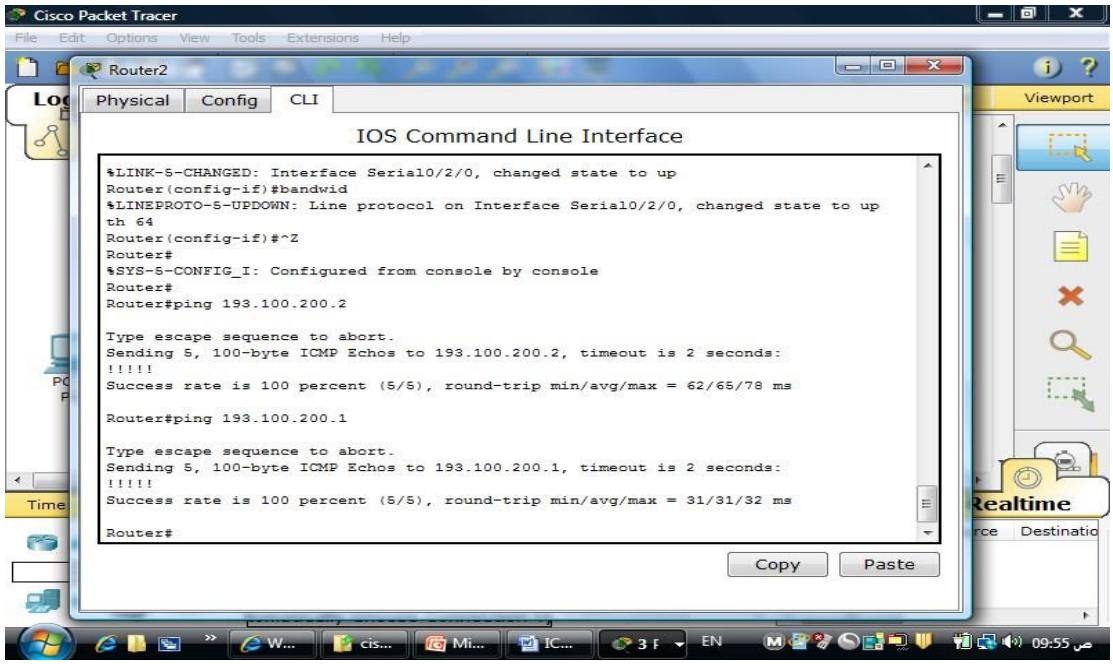
cntrl-z

copy running startup

Note:on DTE side we do not enter the clock rate command.

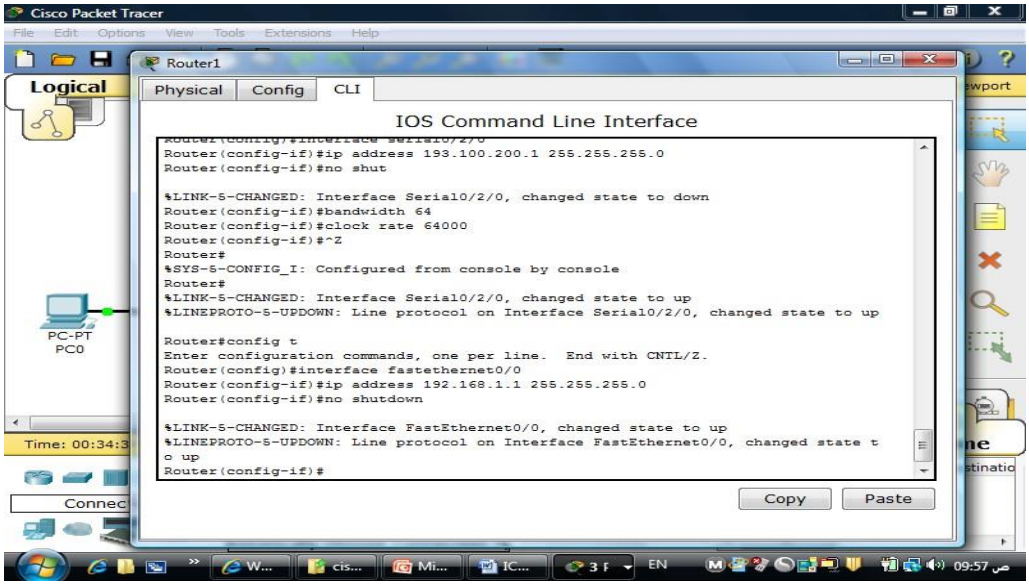


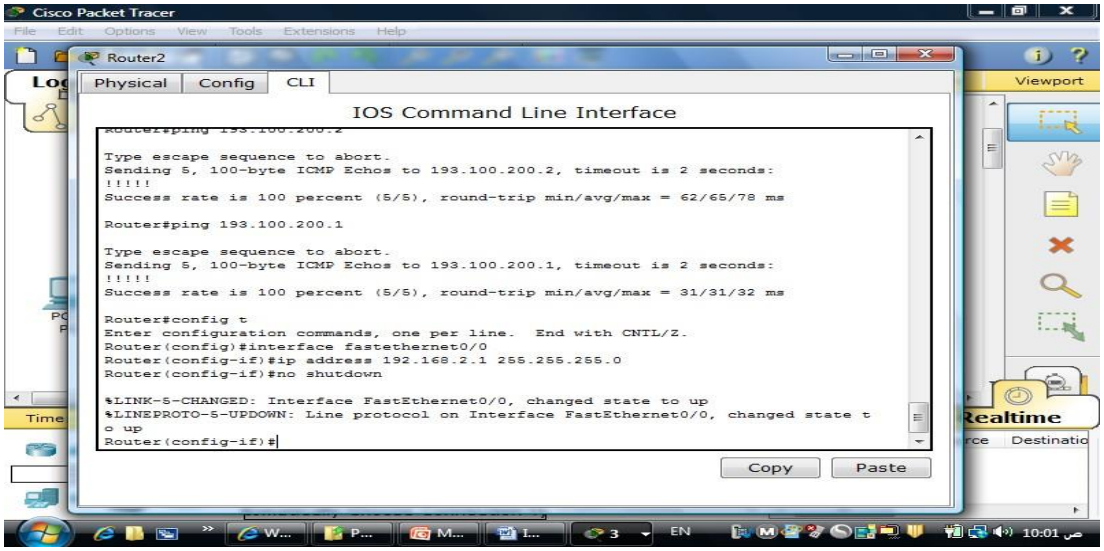
At this stage you should be able to ping the 2 interfaces on the 2 routers. So from say router 2 ping 193.100.200.1 and ping 193.100.200.2. You should get results as in figure below.



- *Next configure the fastethernet0/0 interfaces of router 1 and router 2 as done in Lab 6. See the next 2 figures.*
- *Assign ip address to PCs as given in the table above. Also assign the gateway on each PC. From any PC, ping other*

PCs on the 2 different networks.





Questions:

How many networks are there in this lab ?

What are the network addresses in this lab ?

What happens if you do not assign a gateway ?

What are serial ports on the routers used for ?

What are fastethernet ports on the routers used for?

LAB 7: Dynamic Host Control Protocol (DHCP) on Routers.

Objective:

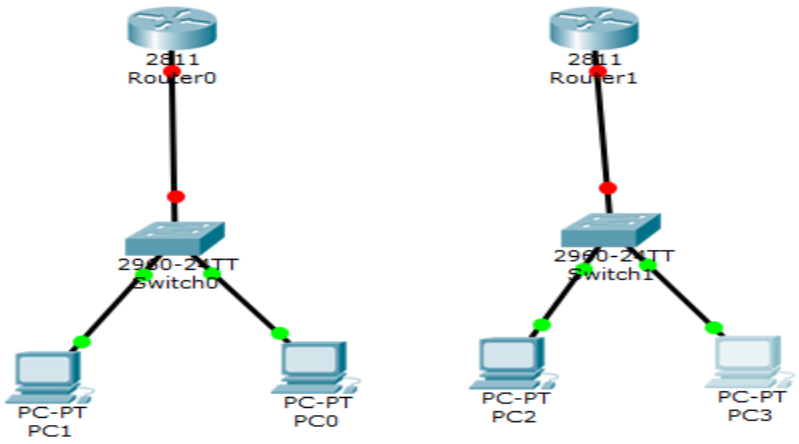
This lab is about how to configure DHCP on cisco router in packet tracer. The Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices. DHCP allows a computer to join an IP-based network without having a pre-configured IP address. DHCP is a protocol that assigns unique IP addresses to devices, then releases and renews these addresses as devices leave and re-join the network.

Internet Service Providers (ISPs) usually use DHCP to allow customers to join the Internet with minimum effort. The DHCP server maintains a database of available IP addresses and configuration information. When it receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, and then allocates an IP address. DHCP servers typically grant IP addresses to clients only for a limited interval.

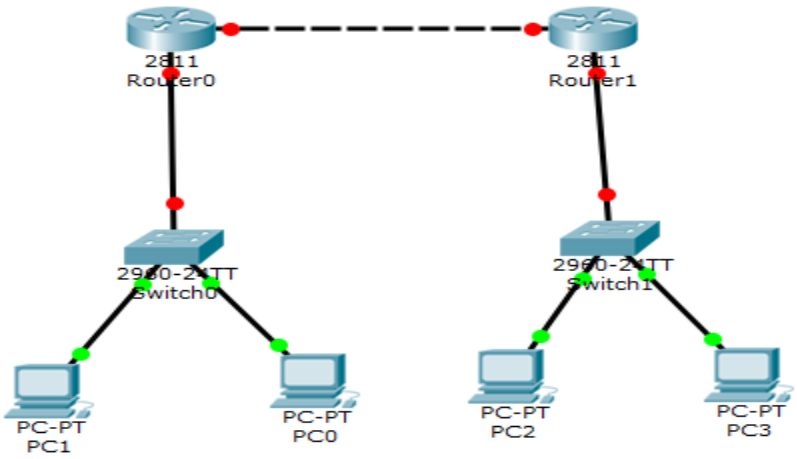
Let's apply DHCP on packet tracer.
First, let us make a topology with one router on which we will apply DHCP and several client PCs. More like this one,

Step 1: Setup a network with 2 routers (2811), 2 switches, 4 PCs as shown below. Assign IP addresses as follows:

	Interface	IP address	Subnet Mask
Router 1	Fastethernet	10.0.0.1	255.0.0.0
Router 2	Fastethernet	20.0.0.1	255.0.0.0
Router 1	Fastethernet	30.0.0.1	255.0.0.0
Router 2	Fastethernet	30.0.0.2	255.0.0.0

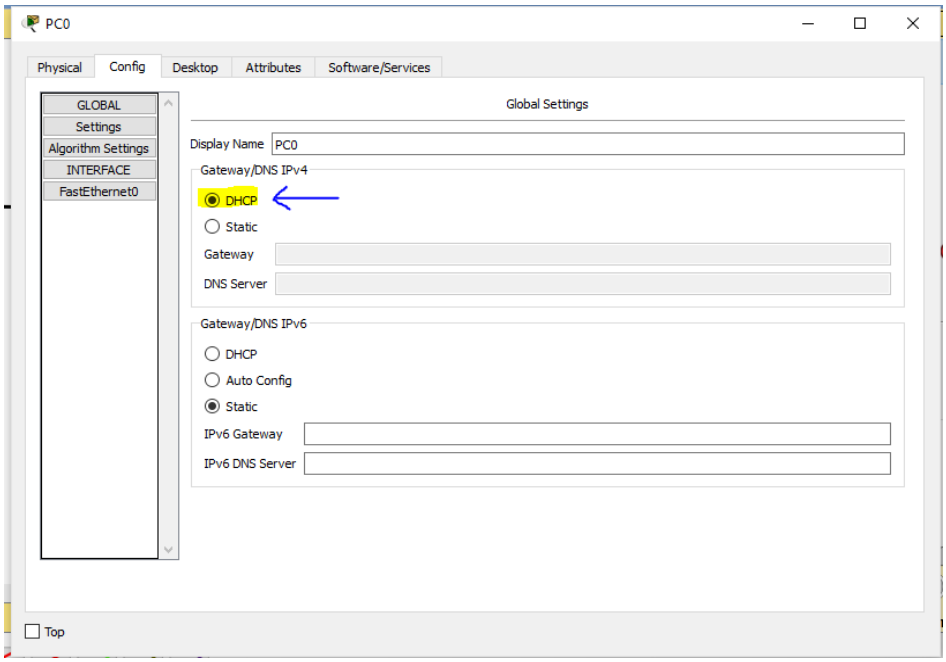


Use cross-over cable to connect between Router0 and Router1

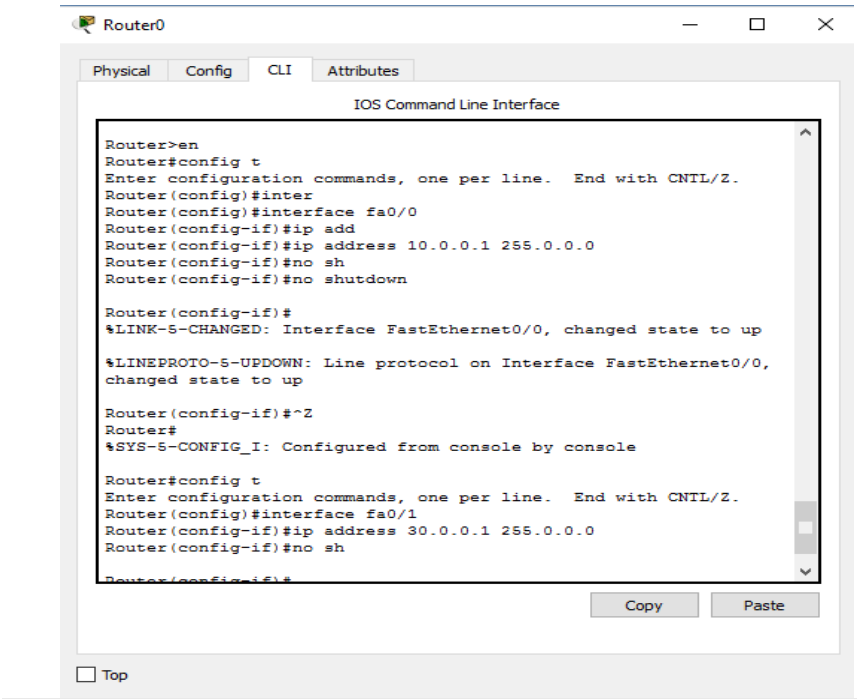


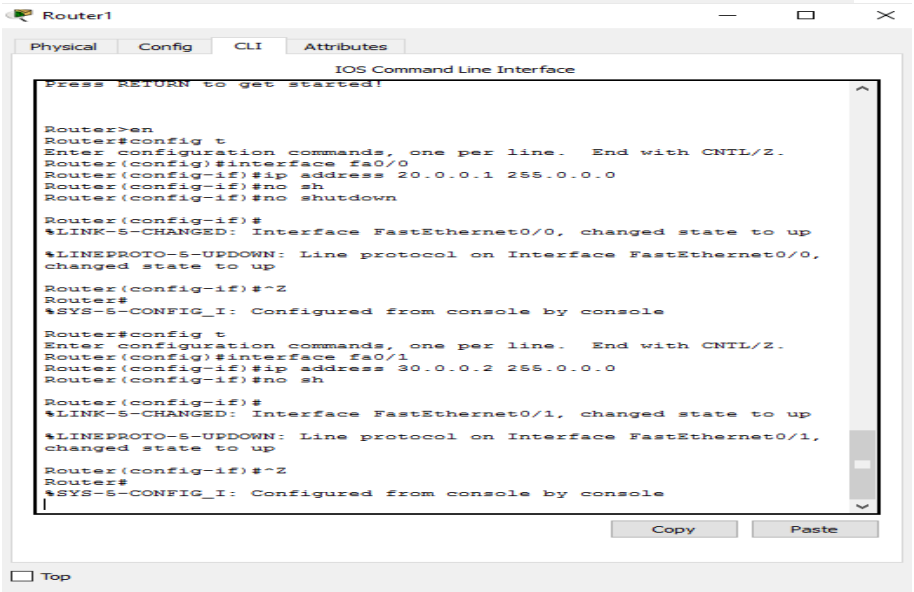
Step 2: .Click on PC0 to bring up the setup screen as below. From Global Settings click on DHCP button as shown below.

Do the same for PC1, PC2 and PC3

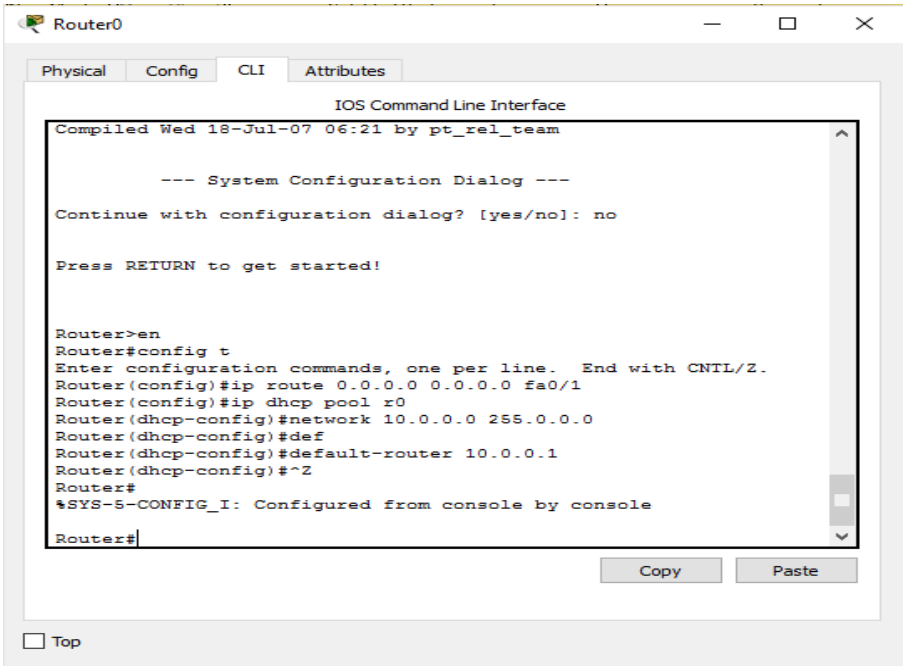


Step 3: configure the interfaces for Router0 and Router1 same as shown in figure below

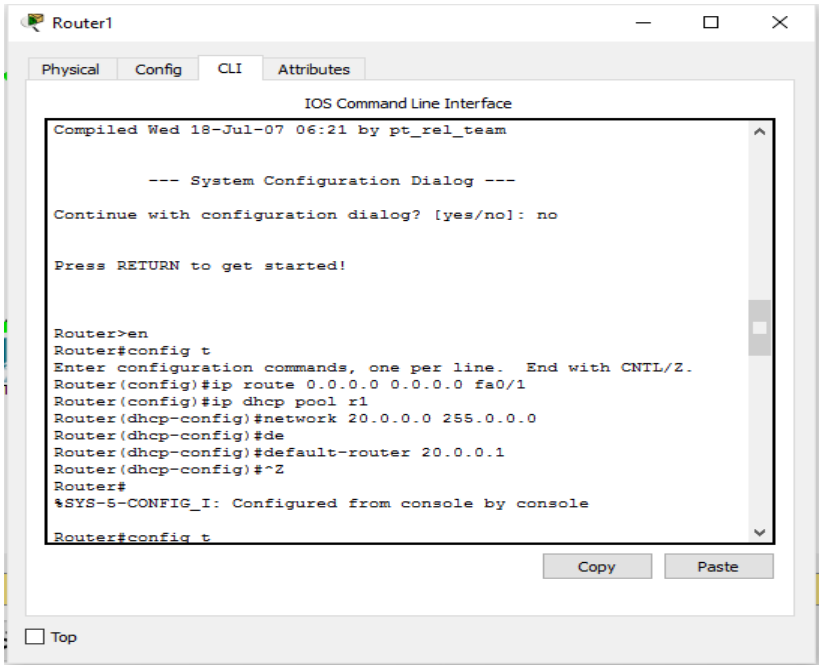




Step 4: Type the following commands to configure DHCP
On Router0 :
config t
()# ip route 0.0.0.0 0.0.0.0 fa0/1
()# ip dhcp pool r0
()# Network 10.0.0.0 255.0.0.0
()# default-route 10.0.0.1



On Rotuer1:
config t
()# ip route 0.0.0.0 0.0.0.0 fa0/1
()# ip dhcp pool r1
()# Network 20.0.0.0 255.0.0.0
()# default-route 20.0.0.1



Questions:
What is the deference between DHCP on lab2 and this lab?
What is the IP address and network address for PC0?
What is the IP address and network address for PC1?
What is the IP address and network address for PC2?
What is the IP address and network address for PC3?