LAB Manual

King Khalid University

College of computer Sciences

Department of computer sciences

2020-2021

Data Communication &

Computer Networks-371CCS3

Course Syllabus

SYLLABUS AND SCHEDULE FOR PRACTICAL COURSE		
Week	***Experiment***	***Contact hours***
Week 1-2	Introduction to Computer Networks Comparison of Layers in OSI Model	2 hours
Week 3	Network Fundamentals Ethernet Cables, Create a LAN	2 hours
Week 4	IP Addressing Classes of IP Address, Subnetting, Super netting	2 hours
Week 5	Introduction to Cisco Packet Tracer	2 hours
Week 6	Connecting client and a server Test connectivity with PING command, running HTTP and FTP services.	2 hours
Week 7		2 hours
Week 8		2 hours
Week 9		2 hours
Week 10		2 hours
Week 11 & 12		4 hours
Week 13		2 hours
Week 14		2 hours
Week 15		2 hours

- **Course Description (As per course Specification)**

- This course is a detailed introduction to the basic hardware and software, architectural components for computer communications in local area networks. The components that are focused upon include understanding the basics of computer networks, switching, routing, protocols and security.

Hardware / Software Requirements

- Windows Operating System
- CISCO Packet Tracer

Marks Distribution with assessment criteria

S. No	Assessment	Week Due	Marks
1	Quiz-1	**5**	**4**
2	Assignment 1	**4**	**3**
3	Assignment 2	**8**	**3**
4	Lab exam	**15**	**10**
Total Marks			**20**

Instructions for assessment methods:

1. quizzes, assignments, exam

Lab Session 1 / Exercise # (Week 1)

Configure Network Interface Cards

Step 1: Start > Control Panel > Network and Sharing Center > Manage Network Connections…
Right Click > Properties > "Highlight TCP/IP V4" > Properties
ipaddress --- 192.168.1.100
subnet mask --- 255.255.255.0
gateway --- 192.168.1.1
DNS 1 --- 192.168.1.1
DNS 2 --- ?

Basic Network Testing Tools
ipconfig
ipconfig /all
ping <ip address or domain name> : ICMP. Sends echo request and receives echo reply.
ping 192.168.4.1
ping yahoo.com
tracert <ip address or domain name>
tracert yahoo.com
nslookup (Name Server Look Up) <domain name or ip address> : Resolve name to an ip address
nslookup
nslookup yahoo.com
netstat : To look for open ports.
netstat –a
netstat -an
cls

Comparison of Network Layers

OSI Model	TCP/IP Model	PDU	Protocols	Network Devices
7. Application	Application	Data	HTTP, FTP, SMTP, Telnet, SSH, DNS, DHCP, POP, IRC	
6. Presentation			.jpg, .zip, ACSII, .mp3	
5. Session				
4. Transport	Transport	Segments	TCP, UDP, Port Numbers	Layer 4 Switches
3. Network	Internet	Packets	IP Addresses, Logical Addressing	Routers
2. Data Link	Network Access	Frames	MAC Addresses, Physical Addressing	NICs, Bridges, Switches
1. Physical		Bits	Media, Medium	NICs, Hubs, Cables, Wires, Radio waves

Keywords by Layer

Application Layer: network applications, services, peer-to-peer programs, programs
Presentation Layer: File – compression, format and security
Transport Layer: Reliable (tcp), connection oriented (tcp), end-to-end delivery, flow control
Network Layer: Logical Addressing, IP Addresses, Best Path, Path Determination
Data Link Layer: Physical Address, Media Access, Network Access, Network Access Control, Media Access Control, MAC Frame
Physical Layer: Bits, Media, Medium

Encapsulation and Decapsulation

The data is broken up into segments. With each segment there is a header added to the data.
Each segment header contains source and destination port numbers.
Each packet header contains source and destination IP addresses.
Each frame header contains source and destination MAC addresses.
Each completed piece which is popularly nicknamed "Packet" is encoded in binary.

LAB 2 – NETWORK FUNDAMENTALS

2.1 Ethernet Cables

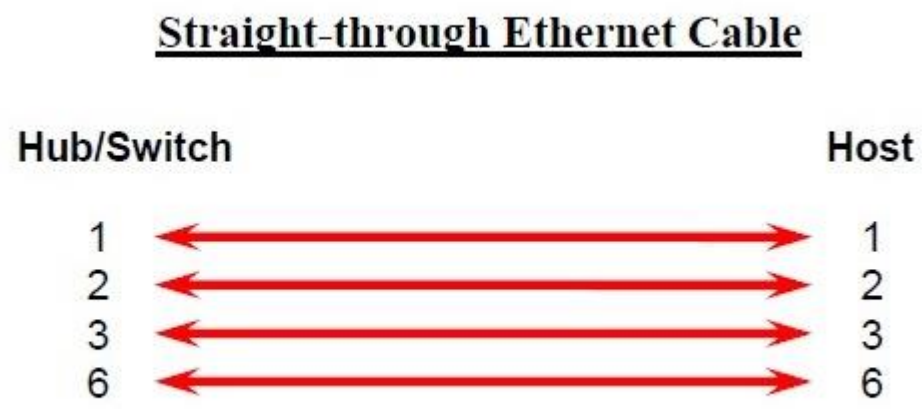
Objective

This lab demonstrates how to make an Ethernet Cables.
The types of Ethernet cables are:
1) Straight-through cable
2) Crossover cable
3) Rolled cable

Straight-Through Cable

The straight-through cable is used to connect
1) Host to switch or hub
2) Router to switch or hub
Four wires are used in straight-through cable to connect Ethernet devices. It is relatively simple to create; Figure shows the four wires used in a straight-through Ethernet cable.

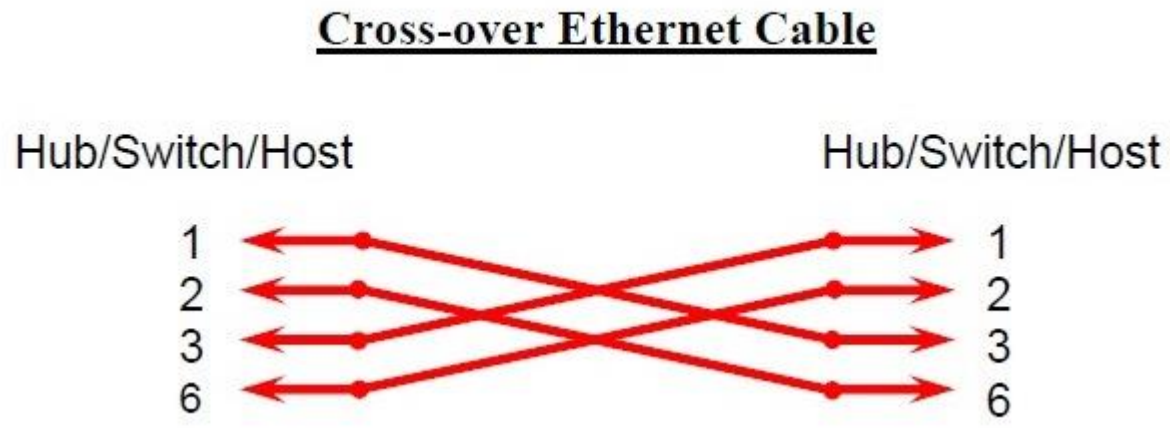
Diagram



Crossover Cable

The crossover cable can be used to connect
1) Switch to switch
2) Hub to hub
3) Host to host
4) Hub to switch
5) Router direct to host
The same four wires are used in this cable as in the straight-through cable; we just connect different pins together. Figure shows how the four wires are used in a crossover Ethernet cable.
Notice that instead of connecting 1 to 1, etc., here we connect pins 1 to 3 and 2 to 6 on each side of the cable.

Diagram

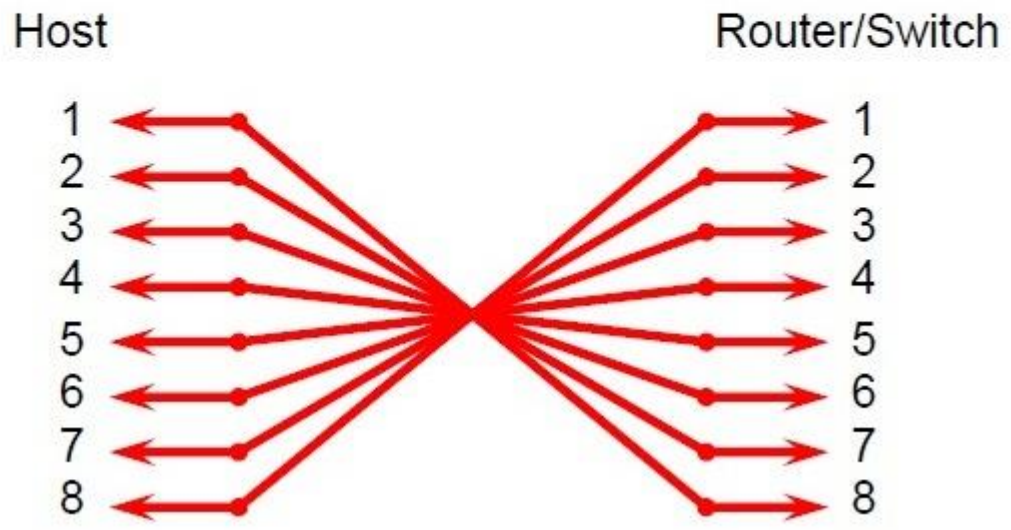


Rolled Cable

Although rolled cable isn't used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a host to a router console serial communication (com) port.
Eight wires are used in this cable to connect serial devices, although not all eight are used to send information, just as in Ethernet networks. Figure shows the eight wires used in a rolled cable.

Diagram

Rolled Ethernet Cable



To make, just cut the one side like a straight-through cable and reverse the other end.
Once you connect the cable from your PC to the Cisco router or switch, you can start HyperTerminal to create a console connection and configure the device.

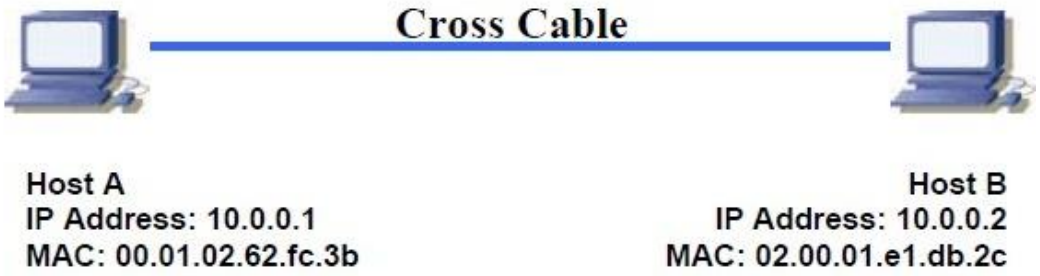
2.2 How to Create a LAN

Objective

This lab demonstrates how to make a LAN Network.
The demonstration includes :
1. To connect 2 PC's with a cross cable.
2. To connect 2 PC's with a switch using a straight cable.

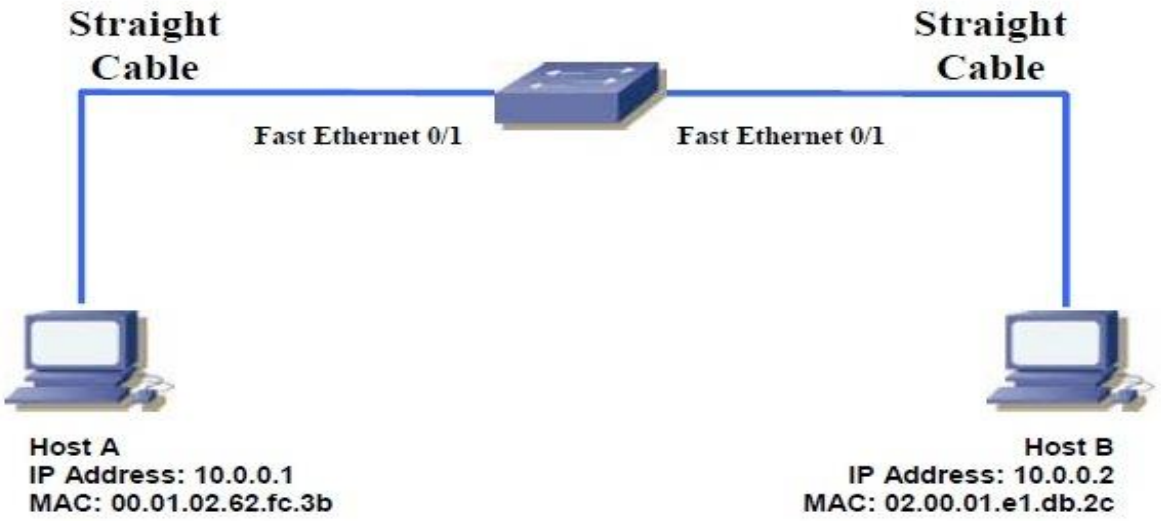
i. Connecting 2 PC's via Cross Cable

Diagram



ii. Connecting 2 PC's via Straight Cable

Diagram



Procedure

1. Make sure that both NICs are installed onto your PC's.
2. Assign IP address to your LAN (NIC) card on both PC's.
3. Check their connectivity by PING command & DATA sharing.

LAB 3 – IP Addressing

3.1 Classful Addressing

IPv4 Address Classes

The IPv4 address space can be subdivided into 5 classes - Class A, B, C, D and E. Each class consists of a contiguous subset of the overall IPv4 address range.

With a few special exceptions explained further below, the values of the leftmost four bits of an IPv4 address determine its class as follows:

Class	Leftmost bits	Start address	Finish address
A	0xxx	0.0.0.0	127.255.255.255
B	10xx	128.0.0.0	191.255.255.255
C	110x	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

Address Classes:

The Internet community originally defined five *address classes* to accommodate networks of varying sizes.

Class A

Class A addresses are assigned to networks with a very large number of hosts.

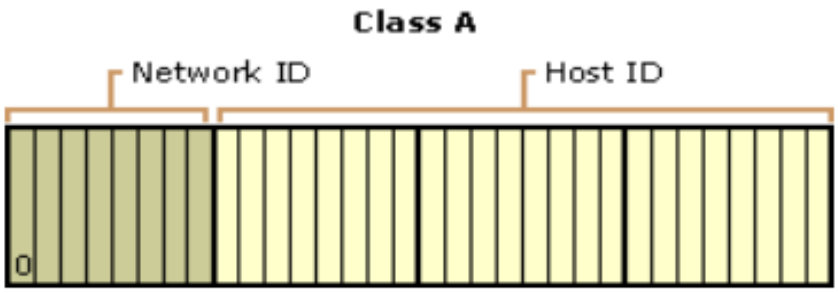


Figure 1.4 Class A IP Addresses

Class B

Class B addresses are assigned to medium-sized to large-sized networks.

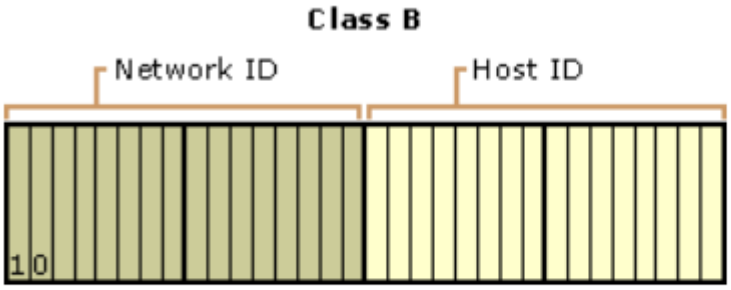


Figure 1.5 Class B IP Addresses

Class C

Class C addresses are used for small networks.

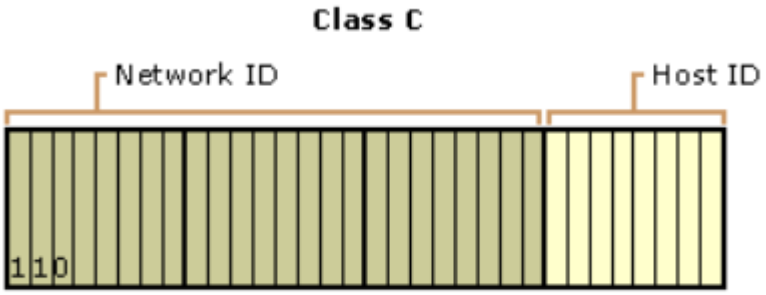


Figure 1.6 Class C IP Addresses

Class D and E

Class D and E are reserved for multicast purposes.

Table 1.11 IP Address Class Summary

Class	Range of classes
A	1–126
B	128–191
C	192–223

Table 1.12 Class Ranges of Network IDs

Address Class	First Network ID	Last Network ID
Class A	1.0.0.0	126.0.0.0
Class B	128.0.0.0	191.255.0.0
Class C	192.0.0.0	223.255.255.0

IPv4 address syntax

An IP address consists of 32 bits. Instead of expressing IPv4 addresses 32 bits at a time using binary notation (Base2), it is standard practice to segment the 32 bits of an IPv4 address into four 8-bit fields called octets. Each octet is converted to a decimal number (base 10) from 0–255 and separated by a period (a dot). This format is called dotted decimal notation. The following table provides an example of an IP address in binary and dotted decimal formats.

IP address in binary and dotted decimal formats

Binary Format	Dotted Decimal Notation
11000000 10101000 00000011 00011000	192.168.3.24

the For example, the IPv4 address of 11000000101010000000001100011000 is:

- Segmented into 8-bit blocks: 11000000 10101000 00000011 00011000
- Each block is converted to decimal: 192 168 3 24
- The adjacent octets are separated by a period: 192.168.3.24

All Class C addresses, for example, have the leftmost three bits set to '110', but each of the remaining 29 bits may be set to either '0' or '1' independently (as represented by an x in these bit positions):
110xxxxx xxxxxxxx xxxxxxxx xxxxxxxx
Converting the above to dotted decimal notation, it follows that all Class C addresses fall in the range from 192.0.0.0 through 223.255.255.255.

IP Address Class E and Limited Broadcast

The IPv4 networking standard defines Class E addresses as reserved, meaning that they should not be used on IP networks. Some research organizations use Class E addresses for experimental purposes. However, nodes that try to use these addresses on the Internet will be unable to communicate properly.
A special type of IP address is the limited broadcast address 255.255.255.255. A broadcast involves delivering a message from one sender to many recipients. Senders direct an IP broadcast to 255.255.255.255 to indicate all other nodes on the local network (LAN) should pick up that message. This broadcast is 'limited' in that it does not reach every node on the Internet, only nodes on the LAN.
Technically, IP reserves the entire range of addresses from 255.0.0.0 through 255.255.255.255 for broadcast, and this range should not be considered part of the normal Class E range.

IP Address Class D and Multicast

The IPv4 networking standard defines Class D addresses as reserved for multicast. Multicast is a mechanism for defining groups of nodes and sending IP messages to that group rather than to every node on the LAN (broadcast) or just one other node (unicast).
Multicast is mainly used on research networks. As with Class E, Class D addresses should not be used by ordinary nodes on the Internet.

IP Address Class A, Class B, and Class C

Class A, Class B, and Class C are the three classes of addresses used on IP networks in common practice, with three exceptions as explained next.

IP Loopback Address

127.0.0.1 is the loopback address in IP. Loopback is a test mechanism of network adapters. Messages sent to 127.0.0.1 do not get delivered to the network. Instead, the adapter intercepts all loopback messages and returns them to the sending application. IP applications often use this feature to test the behavior of their network interface.

As with broadcast, IP officially reserves the entire range from 127.0.0.0 through 127.255.255.255 for loopback purposes. Nodes should not use this range on the Internet, and it should not be considered part of the normal Class A range.

Zero Addresses

As with the loopback range, the address range from 0.0.0.0 through 0.255.255.255 should not be considered part of the normal Class A range.

Private Addresses

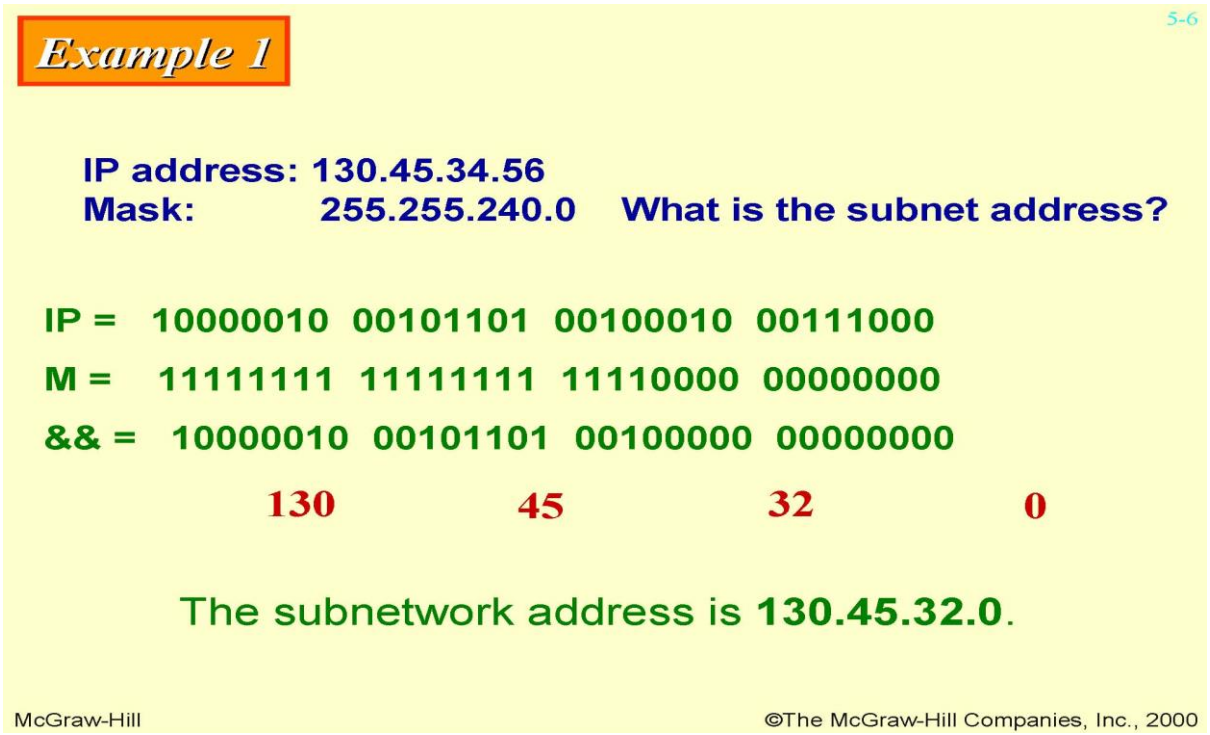
The IP standard defines specific address ranges within Class A, Class B, and Class C reserved for use by private networks (intranets). The table below lists these reserved ranges of the IP address space.

Class	Private start address	Private finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

3.2 Subnetting

Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets). An IP address includes a network segment and a host segment. Subnets are designed by accepting bits from the IP address's host part and using these bits to assign a number of smaller sub-networks inside the original network. Subnetting allows an organization to add sub-networks without the need to acquire a new network number via the Internet service provider (ISP). Subnetting helps to reduce the network traffic and conceals network complexity. Subnetting is essential when a single network number has to be allocated over numerous segments of a local area network (LAN).

Subnets were initially designed for solving the shortage of IP addresses over the Internet.

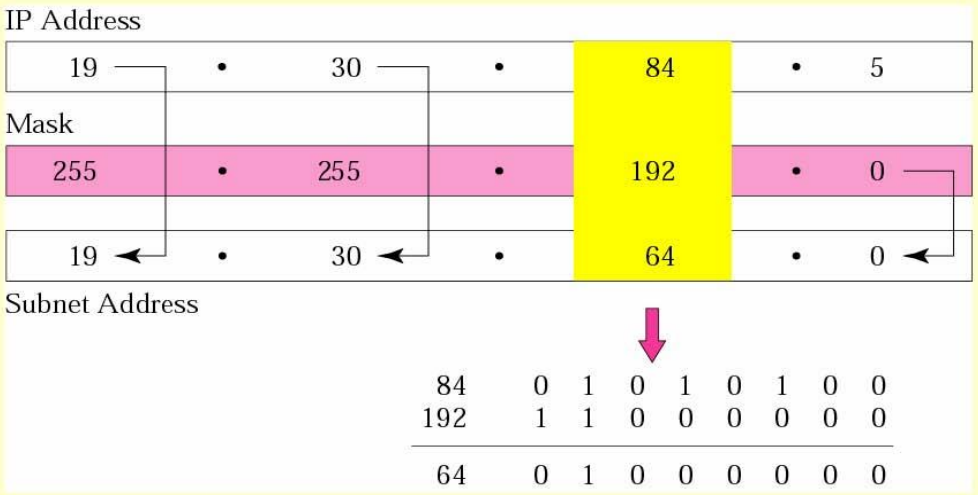


5-9

Example 2

IP = 19.30.80.5

M = 255.255.192.0 **What is the subnet address?**

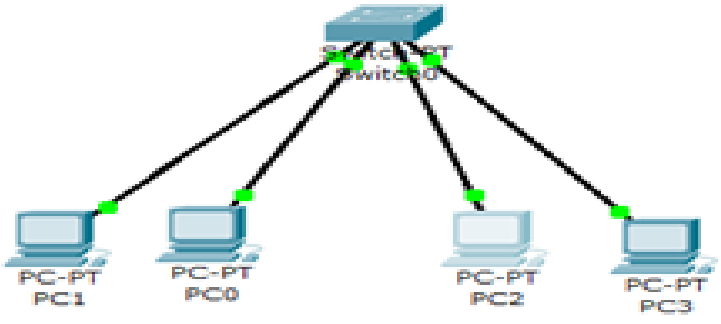


McGraw-Hill ©The McGraw-Hill Companies, Inc., 2000

LAB-4

Introduction to Cisco Packet Tracer

Task 1: Create a LAN using a switch and 4 PC's



Step1: Use four PC & One Generic Switch

Step2: Connect them all with copper straight cable

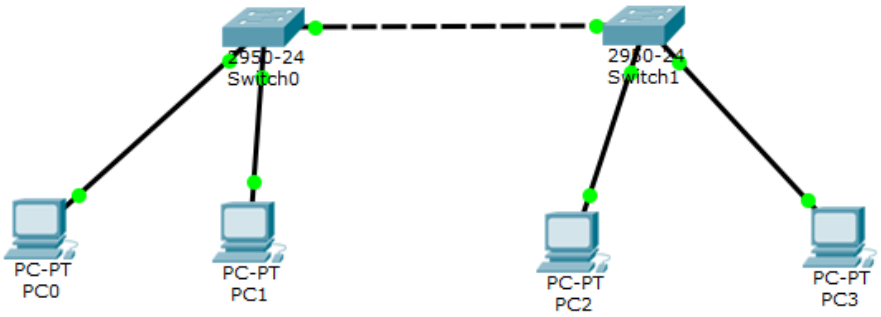
Step3: Set following IP & Mask

PC Name	IP Address	Subnet Mask
PC0	192.168.0.1	255.255.255.0

PC1	192.168.0.2	255.255.255.0
PC2	192.168.0.3	255.255.255.0
PC3	192.168.0.4	255.255.255.0

Write your observation, whether communication is ok with help of ping command.

Task 2: Create a LAN using 2 switches and 4 PC's and create two networks



Step1: Use four PC & two Switches
PC0 & PC1 for Network 1
PC2 & PC3 for Network 2

Step2: Connect them all with copper straight cable

Step3: Set following IP & Mask

PC Name	IP Address	Subnet Mask
PC0	192.168.0.1	255.255.255.0
PC1	192.168.0.2	255.255.255.0
PC2	162.68.0.1	255.255.0.0
PC3	162.68.0.2	255.255.0.0

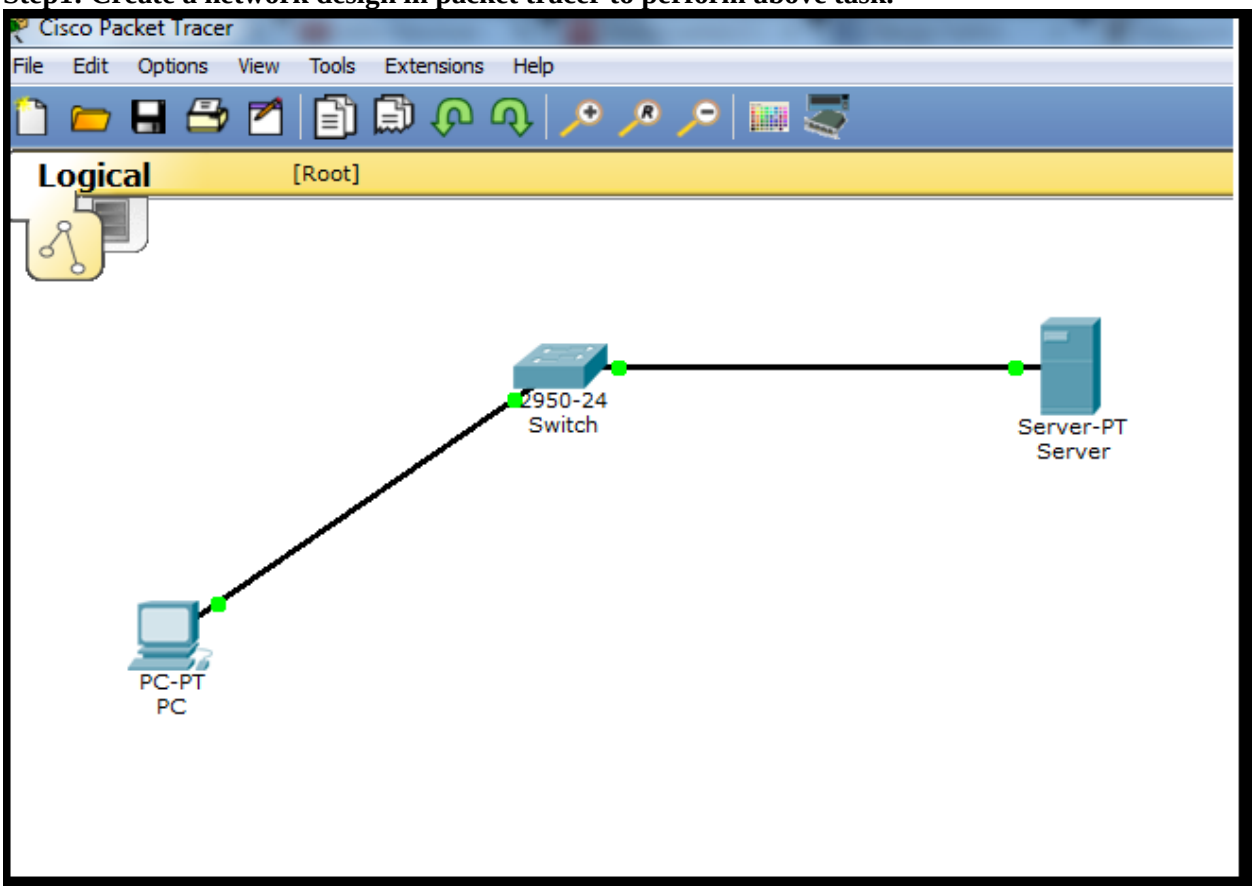
Task 3: Create a LAN with 3 switches and 6 computing devices.

Create 3 networks.

LAB 5

Connecting client and a server
Test connectivity with PING command, running HTTP and FTP services.

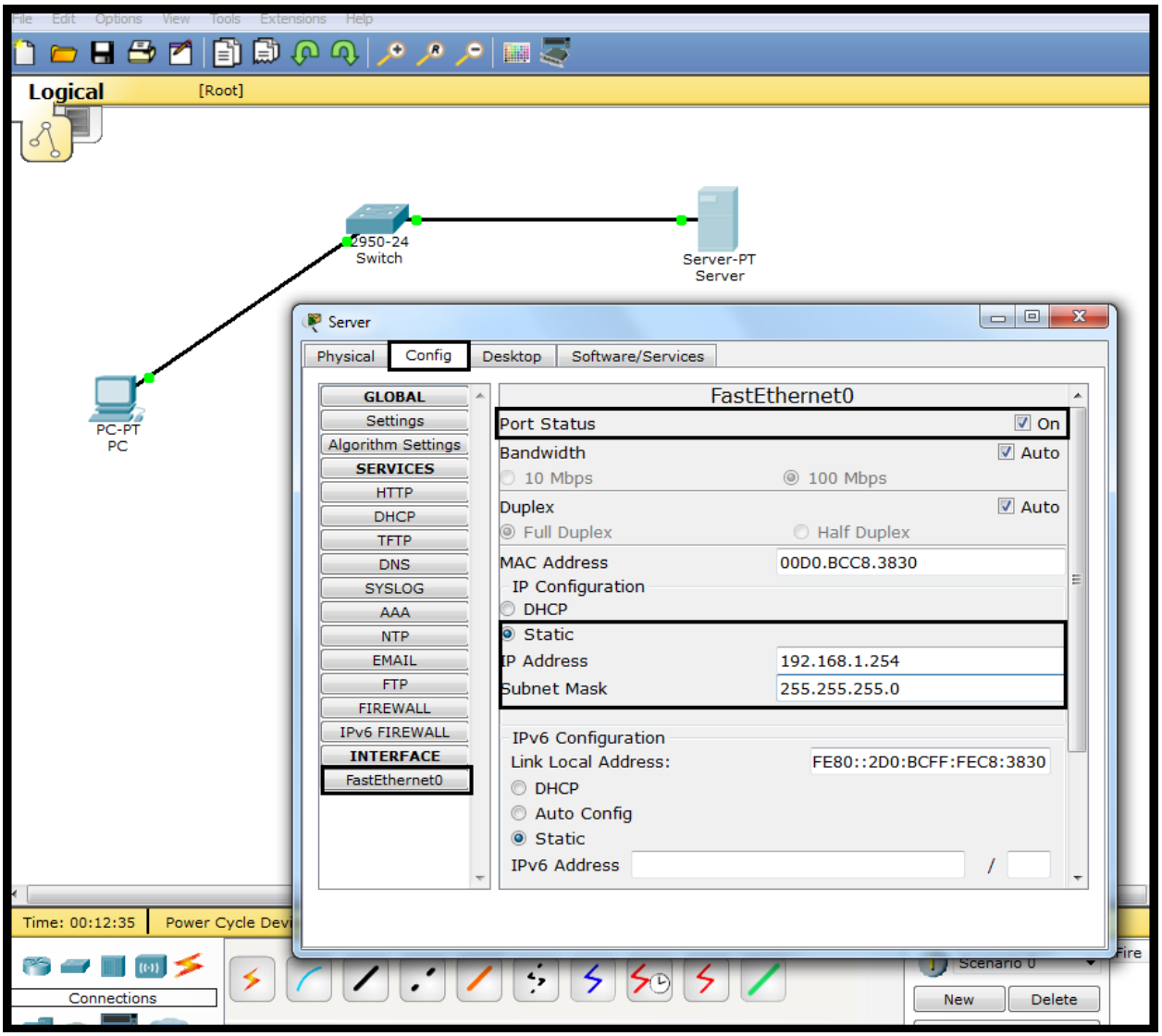
Step1: Create a network design in packet tracer to perform above task.



Here in above network design we have connected one machine with the switch. Also a server is connected to a switch. We need to configure IP addresses for the PC and the server first to carry out further tasks.

Step2: On Server::
Go to following tabs step by step to configure server IP address

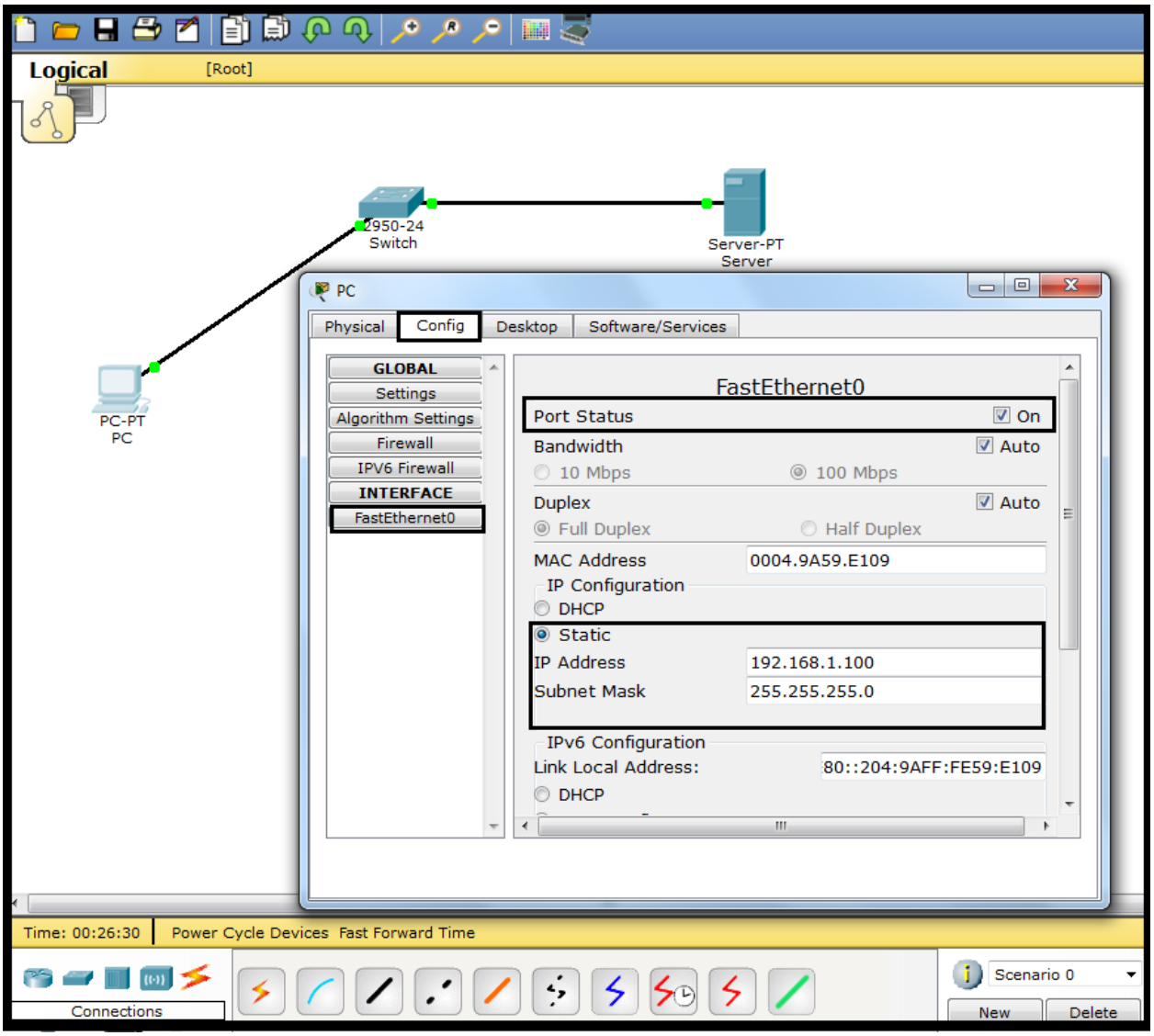
- **Config**
- **FastEthernet0**
- **Check Port Status (It should be ON)**
- **Check Static IP Address**
- **Fill IP Address (192.168.1.254)**
- **Check Subnet Mask (Autofill)**



Step3: On PC::
Go to following tabs step by step to configure server IP address

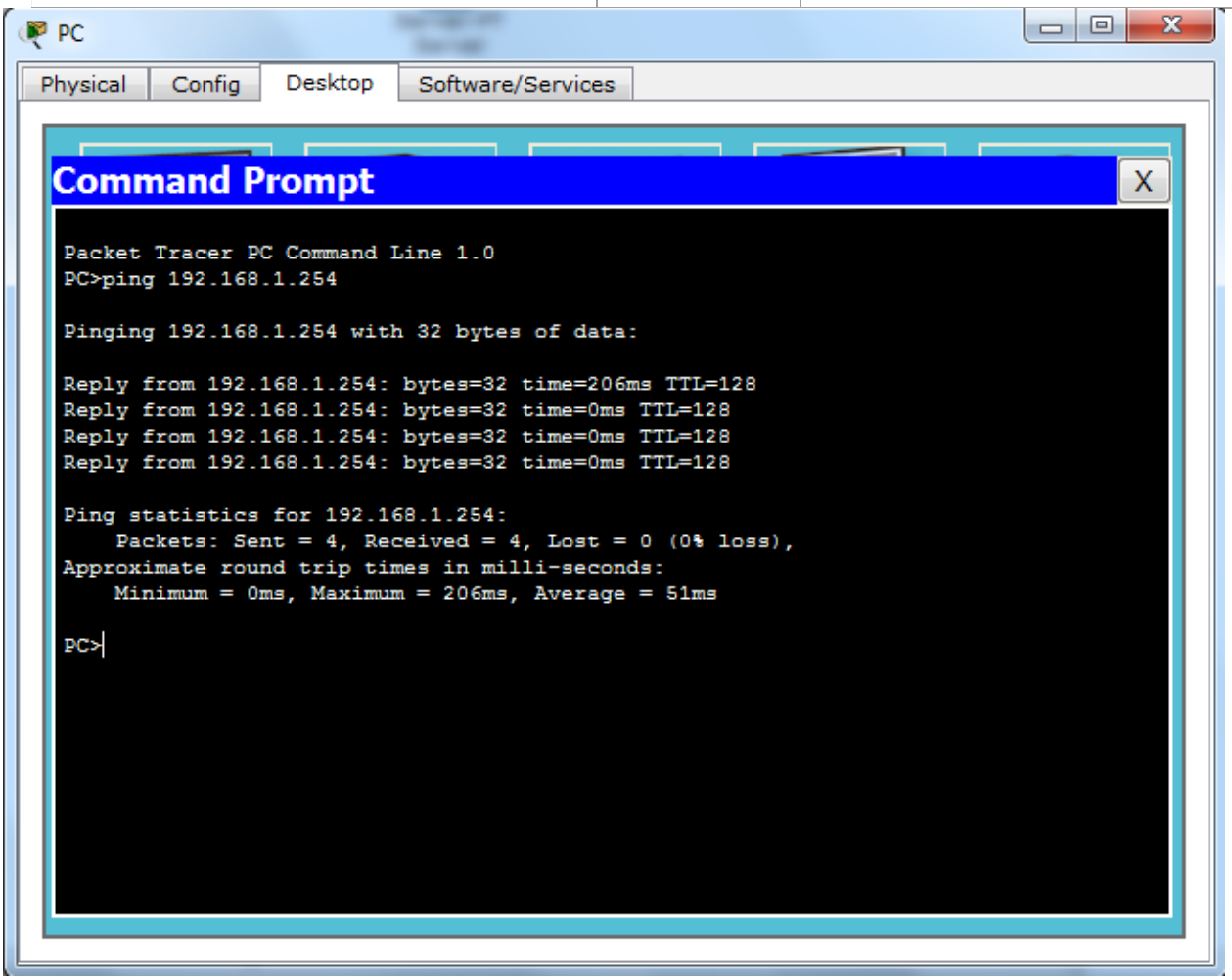
- **Config**
- **FastEthernet0**
- **Check Port Status (It should be ON)**
- **Check Static IP Address**

- **Fill IP Address (192.168.1.100)**
- **Check Subnet Mask (Autofill)**



Task1: Check if you are able to connect to Server. So PING Server assigned IP from PC.
Go to PC and perform following steps.

- **Desktop**
- **Command Prompt**
- **PING 192.168.1.254**



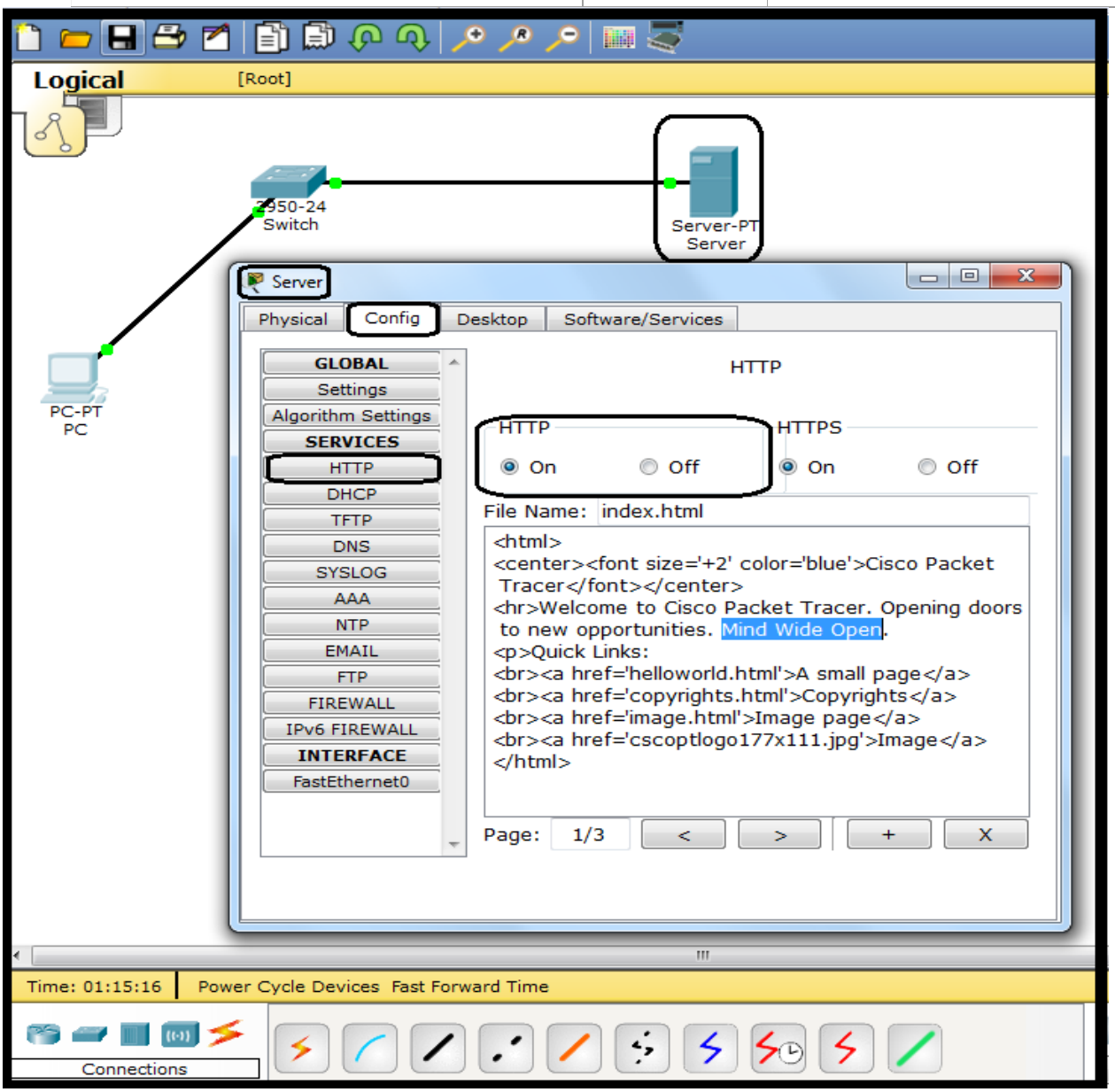
Conclusion: PC is able to ping server from its end. So PC and Server are connected successfully.

Task2: Go to server and configure HTTP and FTP services. Run them from PC to see if you are able to use both the services.

On Server:

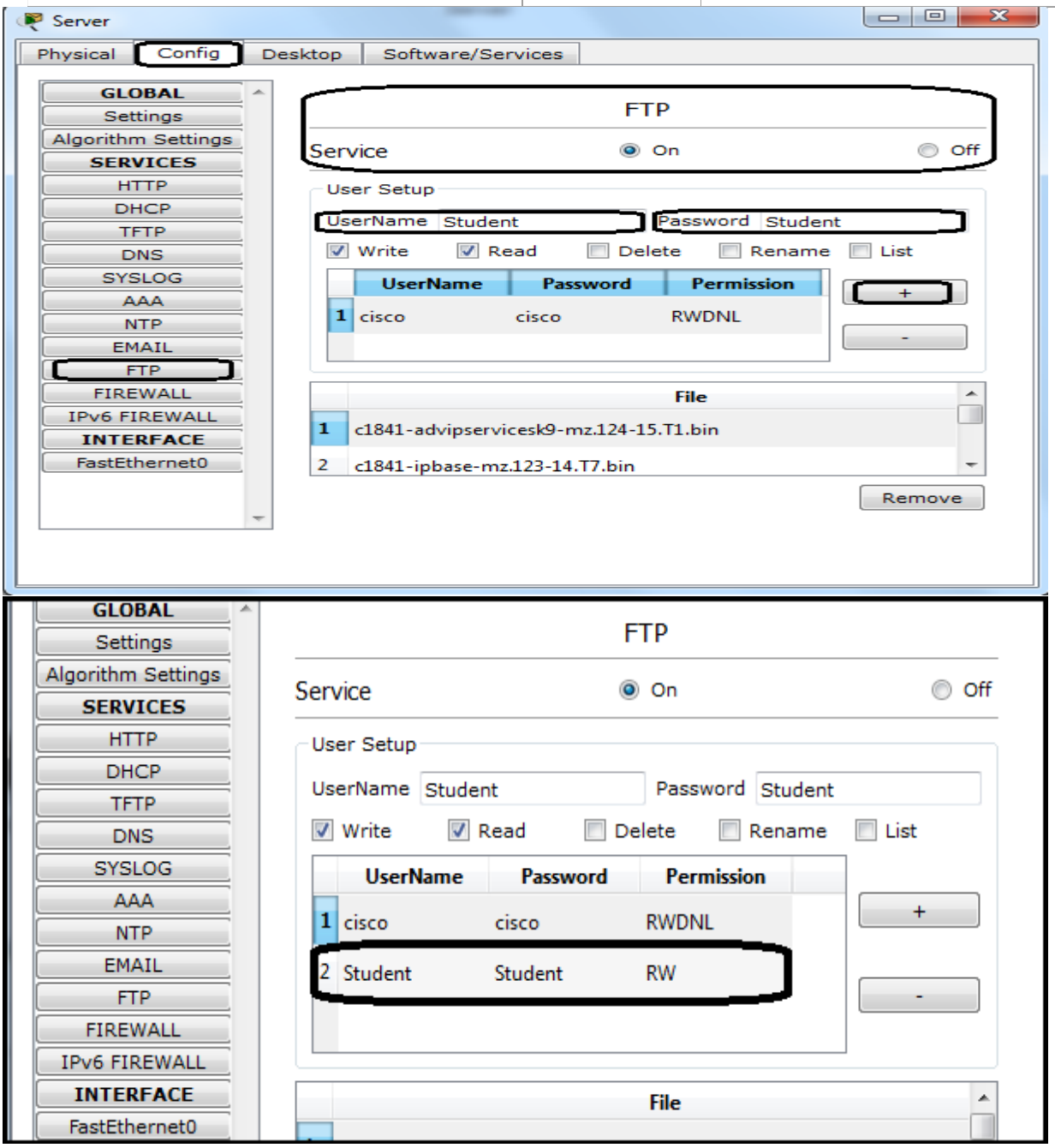
Step1: Go to following tabs step by step to configure services on the server.

- **Config**
- **Services- HTTP**
- **HTTP should be ON**



Step2:

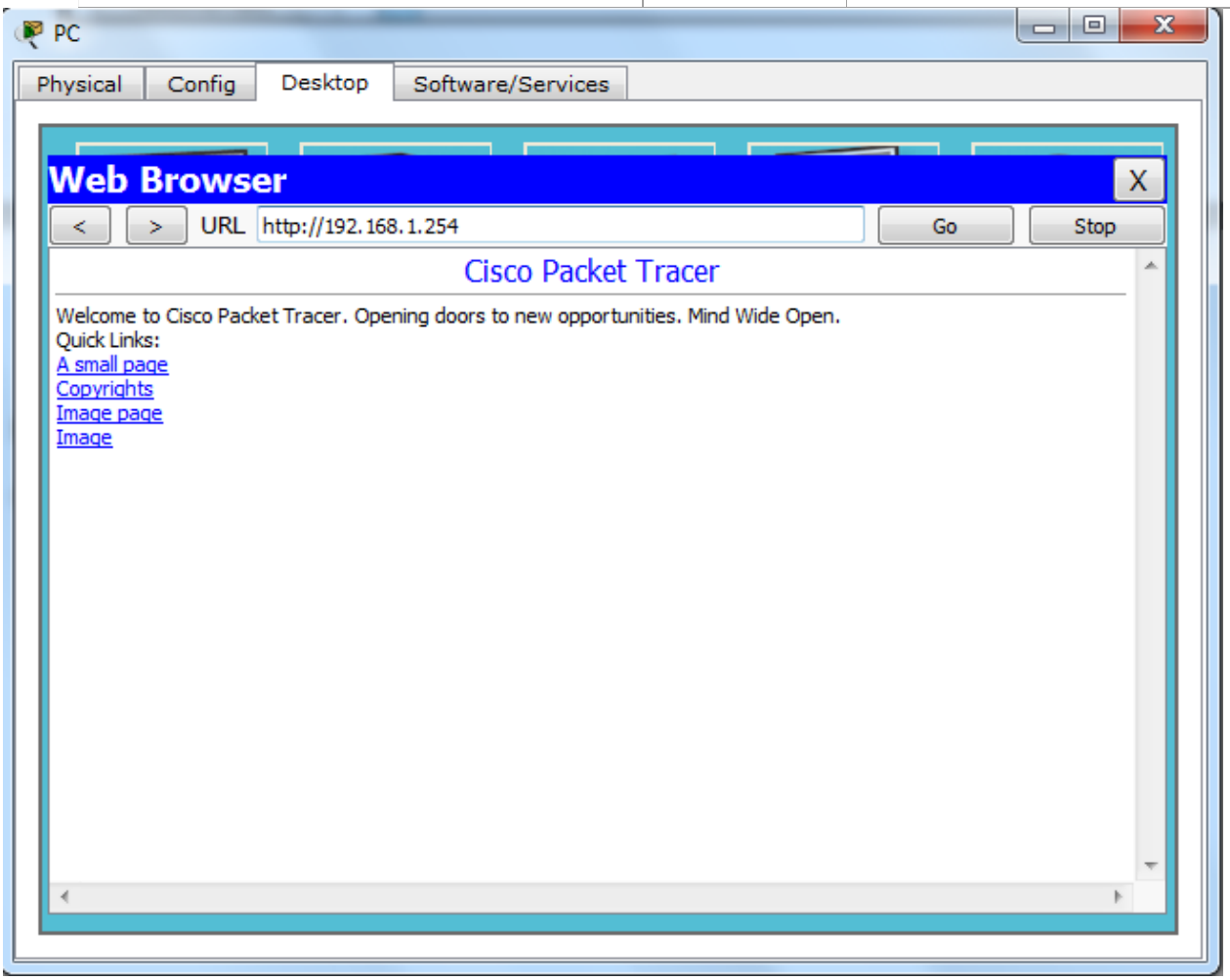
- **Go to FTP**
- **Check status of FTP (It should be ON)**
- **Create a User (Username: Student; Password: Student)**
- **Give READ and WRITE permissions. ADD (+) the new User.**



Step3: Perform the task now

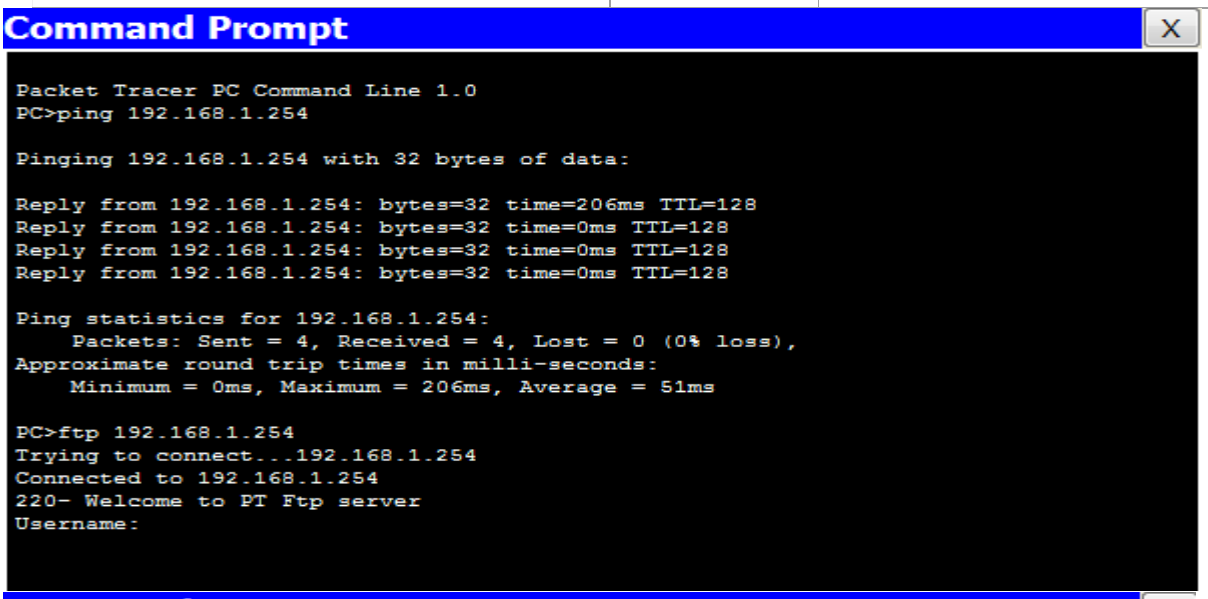
Go to PC and perform following steps.

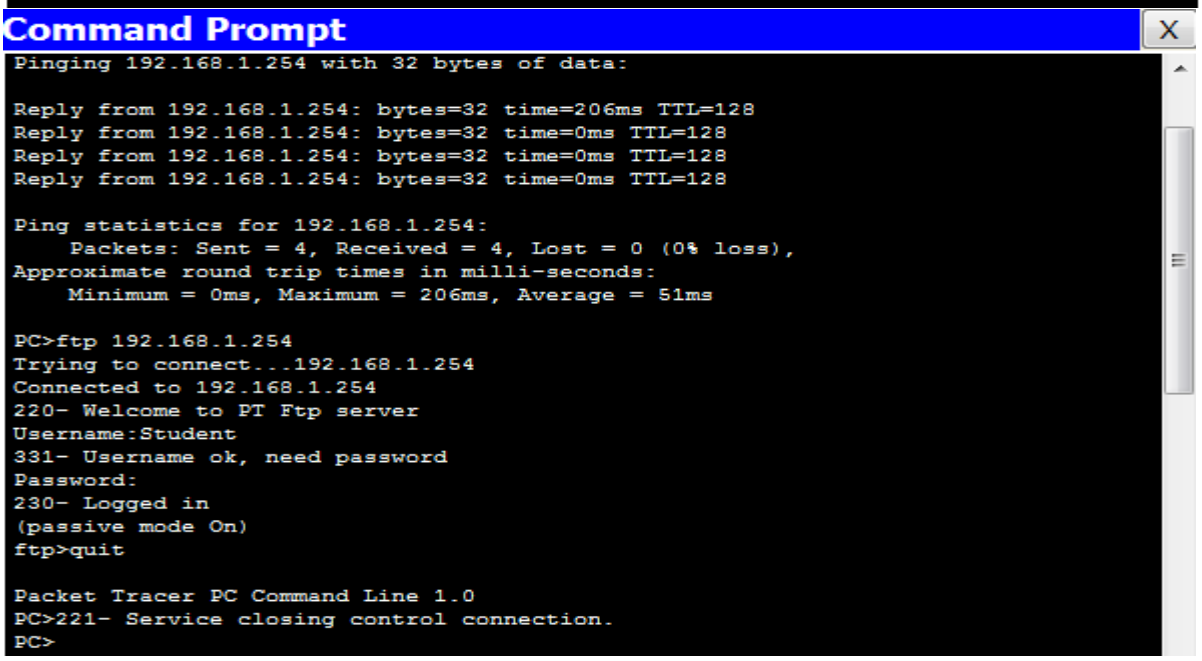
- **Go to desktop tab**
- **Click on Web Browser tab**
- **Type Server IP (192.168.1.254) in URL address bar.**



Conclusion: It opens up the Cisco Packet tracer Web Page.

- **Go to desktop tab and click on command promt.**
- **Type this command, PC>ftp "Server IP address" (Server IP: 192.168.1.254)**





Conclusion: A new User (Student) is created using FTP service. Above results shows how to login with created username and password.