Computer Engineering Department
Program: Sem VI

PART A
(PART A: TO BE REFFERED BY STUDENTS)

Experiment No.10

A.1 Aim:

Perform File Transfer and Access using FTP

A.2 Prerequisite:

- Knowledge about LAN, MAN and WAN and NW Elements.
- Linux NW Commands
- HW and IP Address concepts.
- Concept of Port, Socket, Localhost, Client and Server,
- Client and Server
- Application Layer protocols and application servers
- NW libraries.

A.3 Objective:

a) Configure FTP Services on Servers
b) Upload a File to the FTP Server
c) Download a File from the FTP Server

A.4 Outcome:

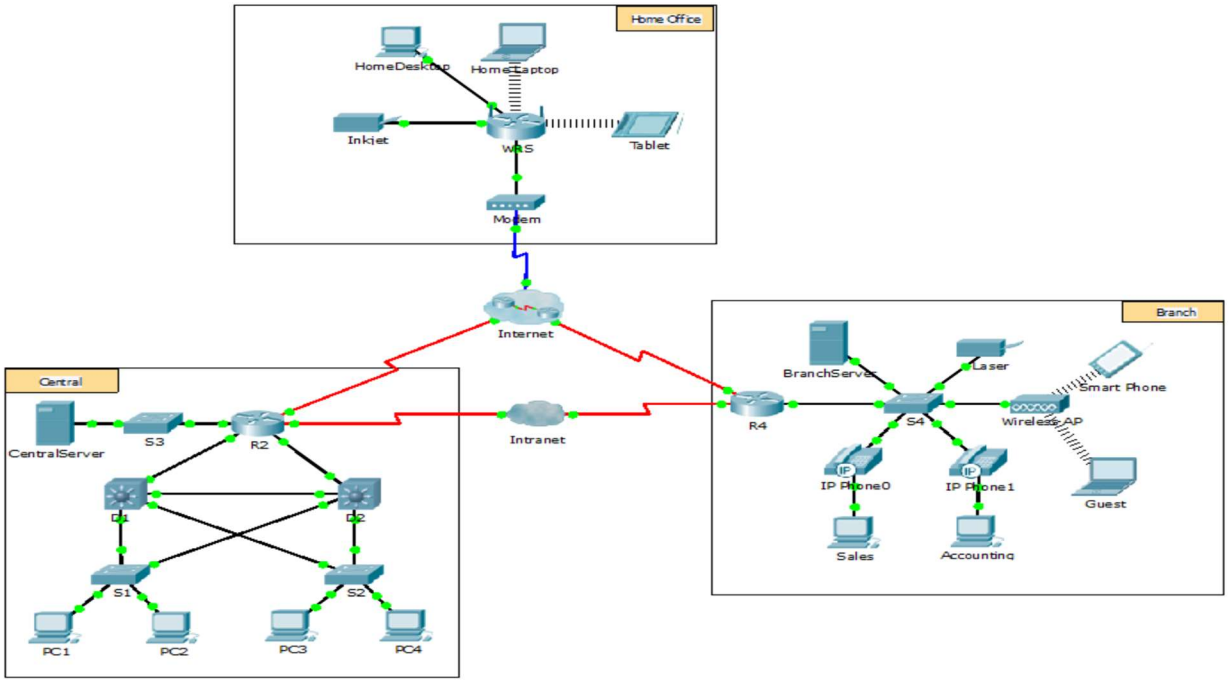
After successful completion of this experiment students will be able to

- Ability to configure FTP server
- Ability to establish connection with server
- Ability to upload a file on the FTP server
- Ability to Download the File from FTP server

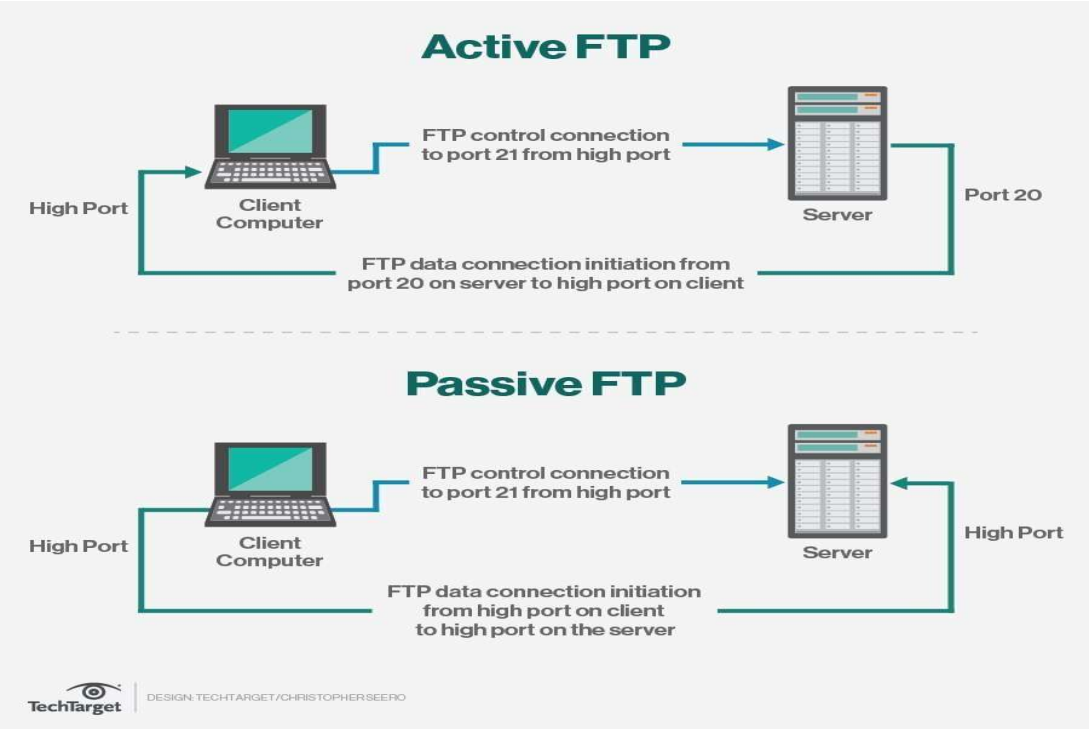
A.4 Theory/Tutorial:

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP.



FTP sessions work in passive or active modes. In active mode, after a client initiates a session via a command channel request, the server initiates a data connection back to the client and begins



transferring data. In passive mode, the server instead uses the command channel to send the client the information it needs to open a data channel. Because passive mode has the client initiating all connections, it works well across firewalls and Network Address Translation (NAT) gateways.

Part 1: Configure FTP Services on Servers

Step 1: Configure the FTP service on CentralServer.

a. Click **CentralServer** > **Services** tab > **FTP**.

b. Click **On** to enable FTP service.

c. In **User Setup**, create the following user accounts. Click **Add** to add the account:

Username	Password	Permissions
anonymous	anonymous	limited to **Read** and **List**
administrator	cisco	full permission

d. Click the default **cisco** user account and click **Remove** to delete it. Close the CentralServer configuration window.

Step 2: Configure the FTP service on BranchServer.

Repeat Step 1 on **BranchServer**.

Part 2: Upload a File to the FTP Server

Step 1: Transfer the README.txt file from the home laptop to CentralServer.

As network administrator, you must place a notice on the FTP servers. The document has been created on the home laptop and must be uploaded to the FTP servers.

a. Click **Home Laptop** and click the **Desktop** tab > **Text Editor**.

b. Open the **README.txt** file and review it. Close the **Text Editor** when done.

Note: Do not change the file because this affects scoring.

c. In the **Desktop** tab, open the Command Prompt window and perform the following steps:

1) Type **ftp centralserver.pt.pka**. Wait several seconds while the client connects.

Note: Because Packet Tracer is a simulation, it can take up to 30 seconds for FTP to connect the first time.

2) The server prompts for a username and password. Use the credentials for the **administrator** account.

3) The prompt changes to `ftp>`. List the contents of the directory by typing **dir**. The file directory on **CentralServer** displays.

4) Transfer the README.txt file: at the `ftp>` prompt, type **put README.txt**. The README.txt file is transferred from the home laptop to **CentralServer**.

5) Verify the transfer of the file by typing **dir**. The README.txt file is now listed in the file directory.

6) Close the FTP client by typing **quit**. The prompt will return to `PC>`.

Step 2: Transfer the README.txt file from the home laptop to BranchServer.

a. Repeat Step 1c to transfer the README.txt file to **branchserver.pt.pka**.

b. Close the Command Prompt and Home Laptop windows, respectively.

Part 3: Download a File from the FTP Server

Step 1: Transfer README.txt from CentralServer to PC2.

a. Click **PC2** and click the **Desktop** tab > **Command Prompt**.

1) Type **ftp centralserver.pt.pka**.

2) The server prompts for a username and password. Use the credentials for the **anonymous** account.

3) The prompt changes to `ftp>`. List the contents of the directory by typing **dir**. The README.txt file is listed at the top of the directory list.

4) Download the README.txt file: at the ftp> prompt, type **get README.txt**. The README.txt file is transferred to **PC2**.

5) Verify that the **anonymous** account does not have the permission to write files to **CentralServer** by typing **put sampleFile.txt**. The following error message displays:

```
Writing file sampleFile.txt to centralserver.pt.pka:
File transfer in progress...

%Error ftp://centralserver.pt.pka/sampleFile.txt (No such file or directory Or
Permission denied)
550-Requested action not taken. permission denied).
```

6) Close the FTP client by typing **quit**. The prompt returns to the `PC>` prompt.

7) Verify the transfer of the file to PC2 by typing **dir**. README.txt is listed in the directory.

8) Close the command line window.

b. In the **Desktop** tab, open the **Text Editor** and then the **README.txt** file to verify the integrity of the file.

c. Close the **Text Editor** and then the PC2 configuration window.

Step 2: Transfer the README.txt file from BranchServer to the Smart Phone.

Repeat Step 1 for **Smart Phone**, except download the README.txt file from **branchserver.pt.pka**.

References:

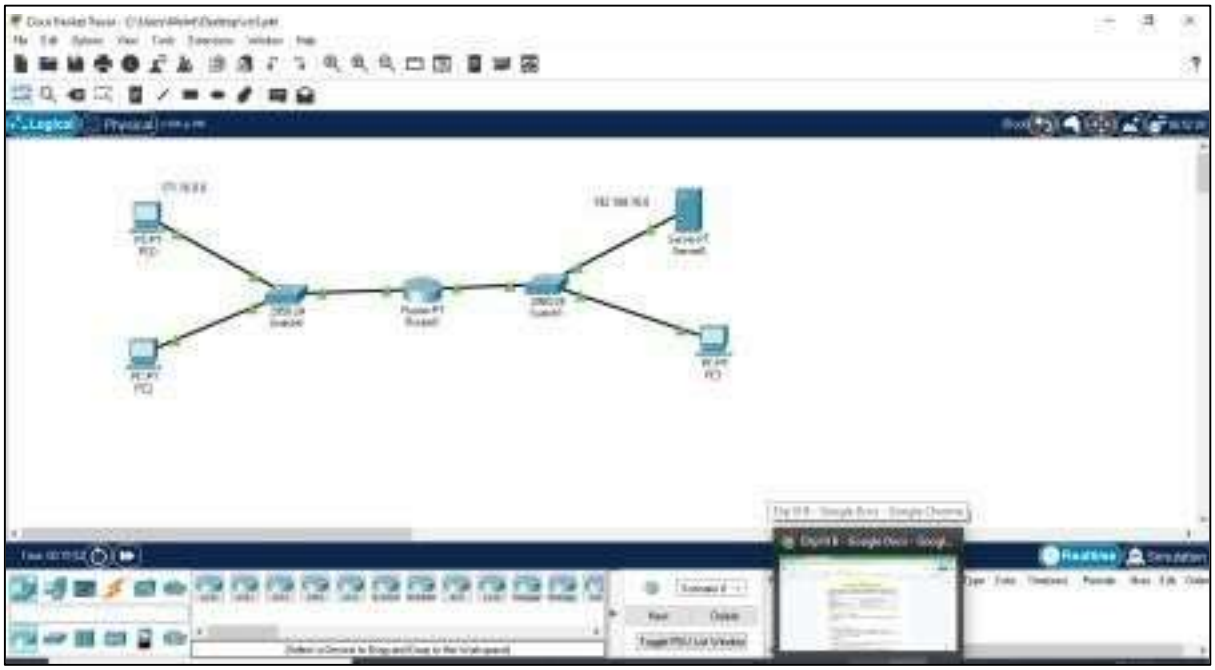
1. https://static-course-assets.s3.amazonaws.com/IntroNet50ENU/files/10.2.3.2%20Packet%20Tracer%20-%20FTP%20Instructions.pdf
2. https://www.youtube.com/watch?v=6R7EnoWrw0o
3. https://youtu.be/m8_IP74PEm8

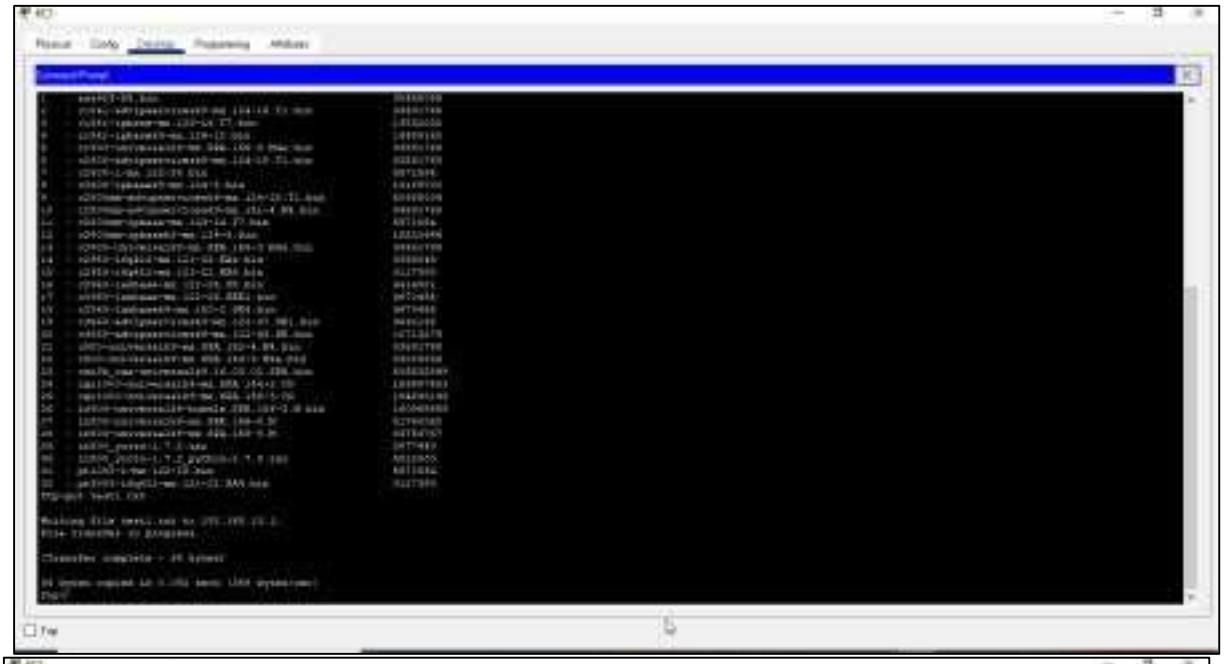
PART B

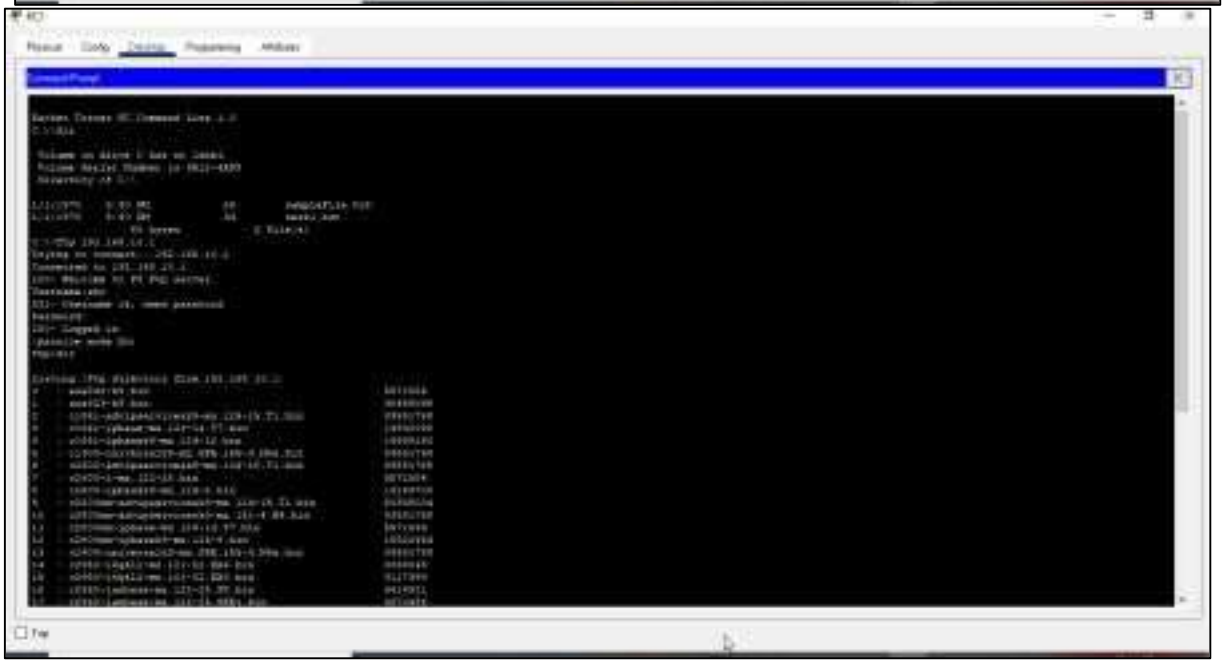
(PART B : TO BE COMPLETED BY STUDENTS)

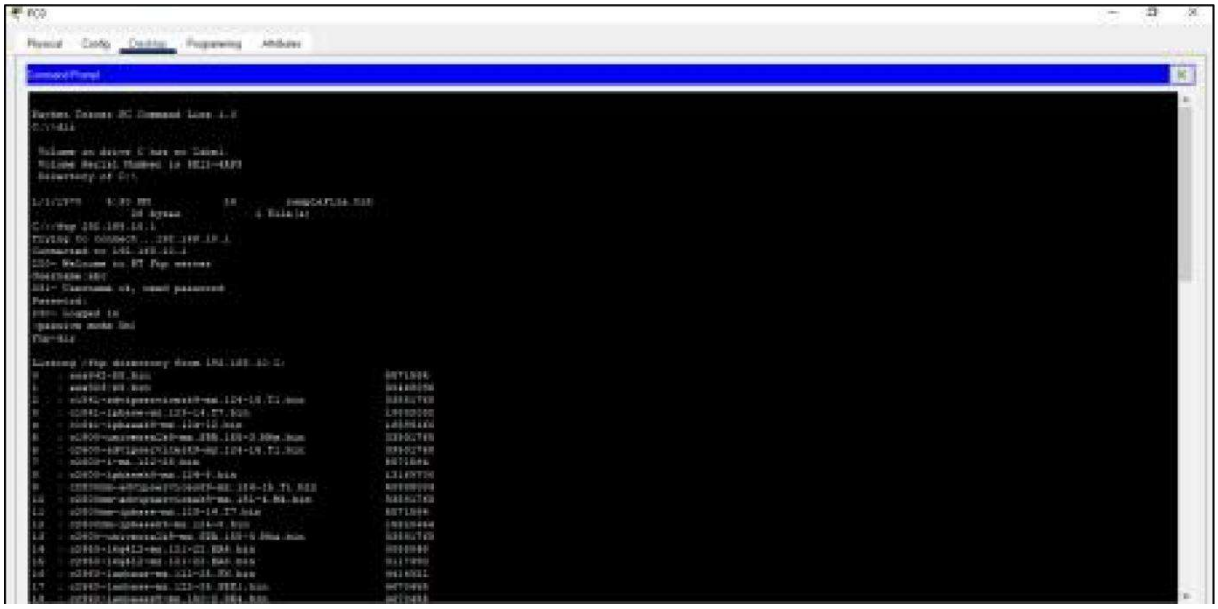
Roll No. A11	Name: Khan Mohammad TAQI Karrar Husain
Class : T.E A	Batch : A1
Date of Experiment:	Date of Submission
Grade :	

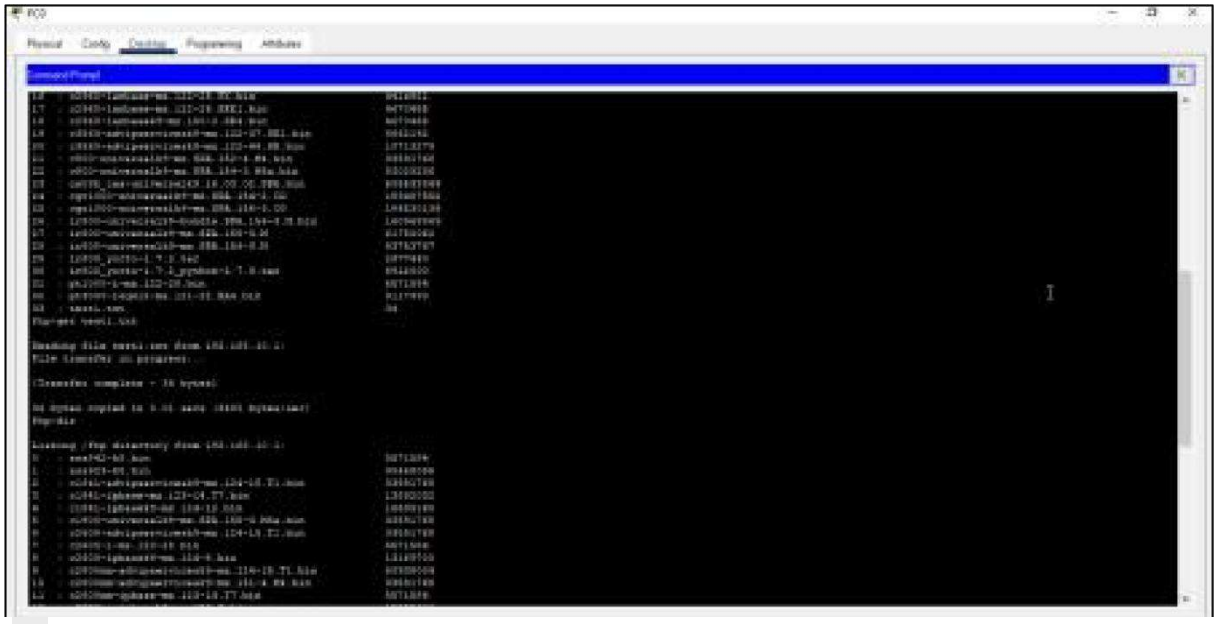
B.1 Document created by the student:

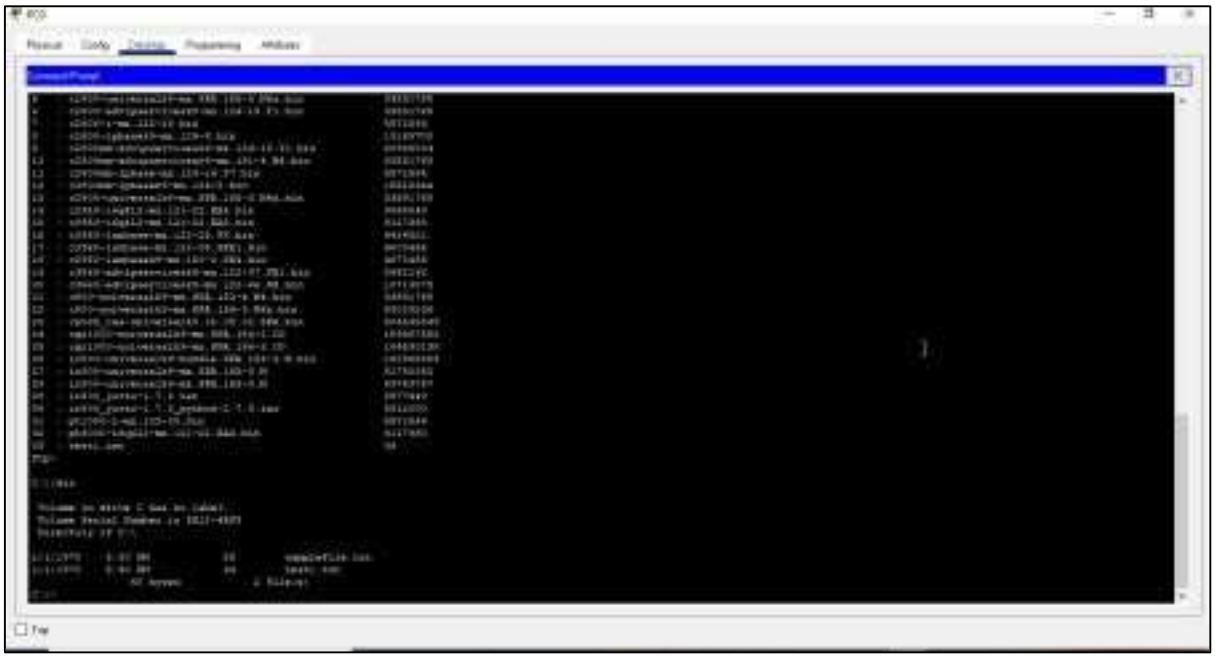












B.3 Observations and learning:

We created a network in packet tracer and implemented FTP. We created a file test1.txt in PC1 and then put it into the server. Then we fetched it in PC0 by using the get command.

B.4 Conclusion:

In this experiment we created a network in Packet Tracer and implemented.

B.5 Question of Curiosity

1. Write the different protocols used in Application layer.

Ans.

Application Layer:-

The application layer is present at the top of the OSI model. It is the layer through which users interact. It provides services to the user.

Application Layer protocol:-

1. TELNET:

Telnet stands for the TELecommunications NETwork. It helps in terminal emulation. It allows Telnet client to access the resources of the Telnet server. It is used for managing the files on the internet. It is used for initial set up of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

Command: telnet [\\RemoteServer]

\\RemoteServer : Specifies the name of the server to which you want to connect

2. FTP:

FTP stands for file transfer protocol. It is the protocol that actually lets us transfer files.It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP promotes sharing of files via remote computers with reliable and efficient data transfer. Port number for FTP is 20 for data and 21 for control.

Command: ftp machinename

3. TFTP:

The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it's the protocol of choice if you know exactly what you want and where to find it. It's a technology for transferring files between network devices and is a simplified version of FTP. Port number for TFTP is 69.

Command: tftp [options...] [host [port]] [-c command]

4. NFS:

It stands for network file system.It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network. Port number for NFS is 2049.

Command: service nfs start

5. SMTP:

It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called

"store and forward," SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. Port number for SMTP is 25.

Command: MAIL FROM:<mail@abc.com?

6. LPD:

It stands for Line Printer Daemon.It is designed for printer sharing.It is the part that receives and processes the request. A “daemon” is a server or agent. Port number for LPD is 515.

Command: lpd [-d] [-l] [-D DebugOutputFile]

7. X window:

It defines a protocol for the writing of graphical user interface–based client/server applications. The idea is to allow a program, called a client, to run on one computer. It is primarily used in networks of interconnected mainframes. Port number for X window start from 6000 and increases by 1 for each server.

Command: Run xdm in runlevel 5

8. SNMP:

It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information. It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defined values. Port number of SNMP is 161(TCP) and 162(UDP).

Command: snmpget -mALL -v1 -cpublic snmp_agent_Ip_address sysName.0

9. DNS:

It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.abc.com might translate to 198.105.232.4. Port number for DNS is 53.

Command: ipconfig /flushdns

10. DHCP:

It stands for Dynamic Host Configuration Protocol (DHCP).It gives IP addresses to hosts.There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68. Command: clear ip dhcp binding {address | * }

2. What are the ports used for FTP?

Ans.

FTP is an unusual service in that it utilizes two ports, a 'data' port and a 'command' port (also known as the control port). Traditionally these are port 21 for the command port and port 20 for the data port.

3. Examples of FTP applications?

Ans.

Examples of FTP clients that are free to download include FileZilla Client, FTP Voyager, WinSCP, CoffeeCup Free FTP, and Core FTP.

4. Which transport layer protocol is used by FTP? Give reason.

Ans.

As with many Internet protocols, the File Transfer Protocol (FTP) uses the Transmission Control Protocol (TCP) to provide guaranteed delivery on top of the Internet Protocol (IP).

When an FTP client requests to connect to an FTP server, a TCP connection is being established using the application layer within TCP and ports 20 and 21. FTP uses and relies on TCP to ensure all the packets of data are sent correctly and to the proper destination.

5. What are DNS, TELNET, DHCP and HTTP protocols?

Ans.

DNS:

It stands for Domain Name System. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.abc.com might translate to 198.105.232.4. Port number for DNS is 53.
Command: ipconfig

/flushdns DHCP:

It stands for Dynamic Host Configuration Protocol (DHCP).It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.
Command: clear ip dhcp binding

{address | * } TELNET:

Telnet stands for the TELecommunications NETwork. It helps in terminal emulation. It allows Telnet client to access the resources of the Telnet server. It is used for managing the files on the internet. It is used for initial set up of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

Command : telnet [\\RemoteServer]

\\RemoteServer : Specifies the name of the server to which you want to

connect HTTP

HTTP is a protocol which allows the fetching of resources, such as HTML documents. It is the foundation of any data exchange on the Web and it is a client-server protocol, which means requests are initiated by the recipient, usually the Web browser. A complete document is reconstructed from the different sub-documents fetched, for instance text, layout description, images, videos, scripts, and more.

6. What is SMTP? Where this protocol is used.?

Ans.

SMTP stands for Simple Mail Transfer Protocol.

SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.

It is a program used for sending messages to other computer users based on e-mail addresses.

It provides a mail exchange between users on the same or different computers, and it also supports:

a. It can send a single message to one or more recipients.
b. Sending message can include text, voice, video or graphics.
c. It can also send the messages on networks outside the internet.

The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.