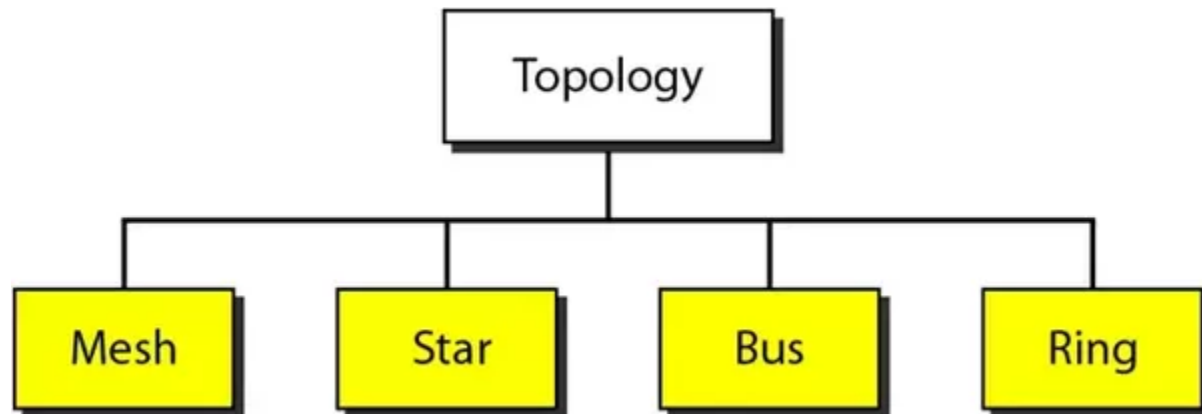


Practical No-1

Aim- To study various LAN topologies and their creation using network devices, cables and computers

Theory- The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as network topology.



Mesh technology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula:

Number of cables = $(n*(n-1))/2$; Where n is the number of nodes that represents the network.

Star topology

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

Bus topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a "**single lane**" through which the message is broadcast to all the stations.

Ring topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.

Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied above. It is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above.

Practical No-2

Aim- To connect the computers in Local Area Network.

Theory- A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

Creating LAN

Step 1 - Open Cisco packet tracer

Step 2- access your network and identify the components of your network, for example; Servers, Routers, End Devices, etc.

Step 3- Complete the cabling. Access the cables section and connect completely and correctly the cables between the network in order to ensure connectivity between the devices in the network using the connections .

Step 4- Configure the IP addresses on the end devices, correctly and completely configure the IP addresses on all end devices

Step 5- Test connectivity. test connectivity by opening a command prompt window on the end devices and try pinging the address which the network operates on. If it gives you a reply, it means your network was configured correctly.

Result- thus we have created a LAN Successfully.

Practical No-3

Aim- Familiarization with Networking Components and devices: LAN Adapters, Hubs, Switches, Routers etc.

Theory-

1. **Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. **Hub** – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub:-** These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without

cleaning and boosting them and can't be used to extend the distance between nodes.

- **Intelligent Hub :-** It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

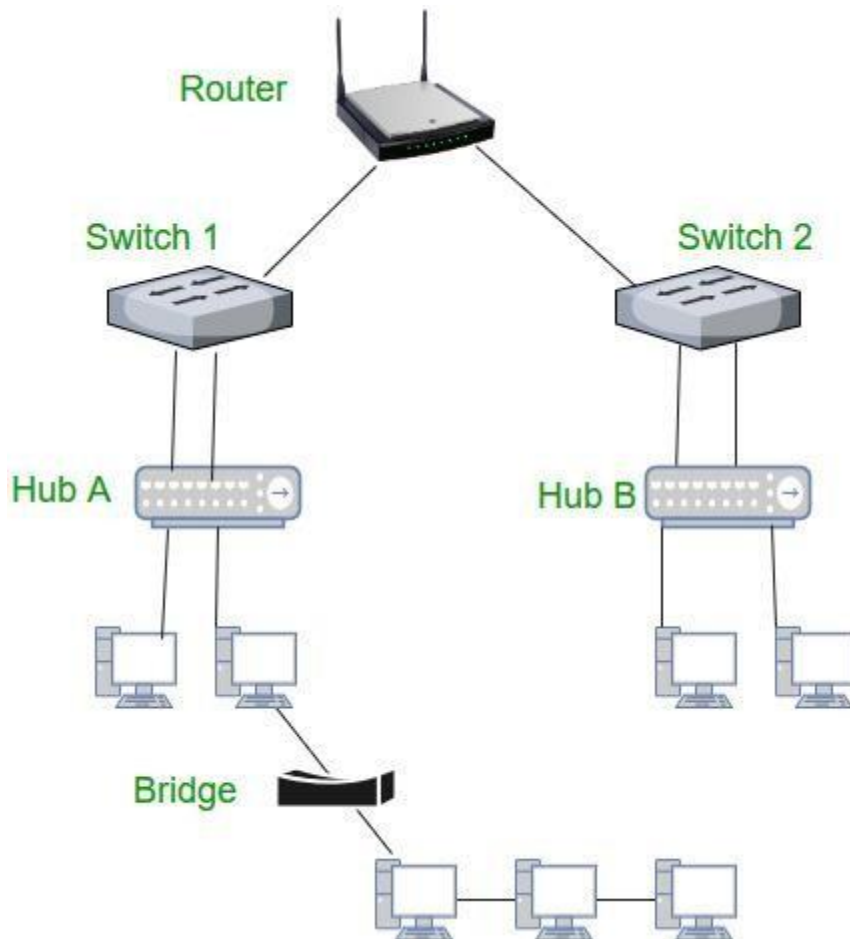
3. **Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

4. **Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same

5. **Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



Result- Thus we have studied networking Devices Successfully

Practical No-4

Aim- Write a program of bit stuffing used by Data Link Layer.

Theory-

Bit stuffing refers to the insertion of one or more bits into a data transmission as a way to provide signaling information to a receiver. The receiver knows how to detect, remove or disregard the stuffed bits.

In the data link layer of the Open Systems Interconnection model, a stream of bits is divided into more manageable units, or frames. Each frame contains the sending and receiving information to facilitate transmission.

To separate the frames, an 8-bit flag byte is injected at the beginning and end of the sequence. This keeps the receiver from interpreting the flag as part of the transmitted information.

In the **OSI model**, the size of the data frames in variable-length frames may vary. In such cases, it's very difficult to detect the end and beginning of a frame. Hence, bit stuffing is used to mark the end and beginning of the frames during variable-length data frame transfer.

Program-

Bit stuffing is a process of inserting an extra bit as 0, once the frame sequence encountered 5 consecutive 1's.

```
#include<stdio.h>
#include<string.h>
int main()
{
    int a[20],b[30],i,j,k,count,n;
    printf("Enter frame size (Example: 8):");
    scanf("%d",&n);
    printf("Enter the frame in the form of 0 and 1 :");
    for(i=0; i<n; i++)
        scanf("%d",&a[i]);
    i=0;
    count=1;
    j=0;
    while(i<n)
    {
        if(a[i]==1)
        {
            b[j]=a[i];
            for(k=i+1; a[k]==1 && k<n && count<5; k++)
            {
                j++;
                b[j]=a[k];
                count++;
                if(count==5)
                {
                    j++;
                    b[j]=0;
                }
                i=k;
            }
        }
    }
}
```

```
    }  
    else  
    {  
        b[j]=a[i];  
    }  
    i++;  
    j++;  
}  
printf("After Bit Stuffing :");  
for(i=0; i<j; i++)  
    printf("%d",b[i]);  
return 0;  
}
```

Result-

Practical No-5

Aim- Configuring the DHCP server in network.

Theory-

Dynamic Host Configuration Protocol (DHCP) is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts; only those hosts that are connected to the network consume IP addresses. The DHCP server assigns IP addresses from specified address pools on a router or router to DHCP clients and manages them.

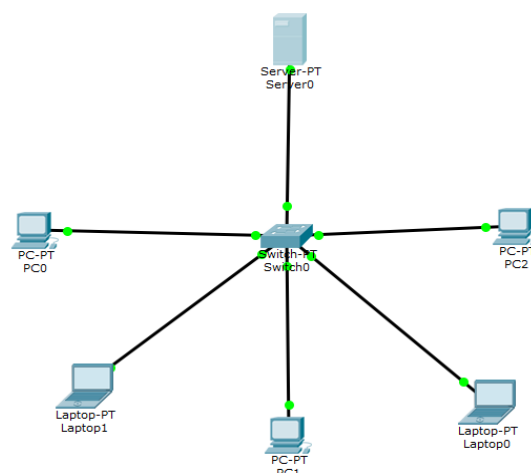
DHCP is a network management protocol used in networks to dynamically assign IP addresses and other network configuration information like default gateway, mask, DNS server address, etc. It is an application layer protocol.

Steps to Configure and Verify DHCP Server in Cisco Packet Tracer:

Step 1: First, open the cisco packet tracer desktop and select the devices given below:

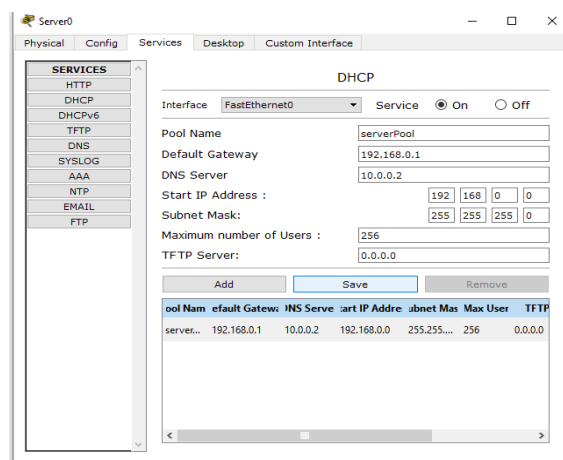
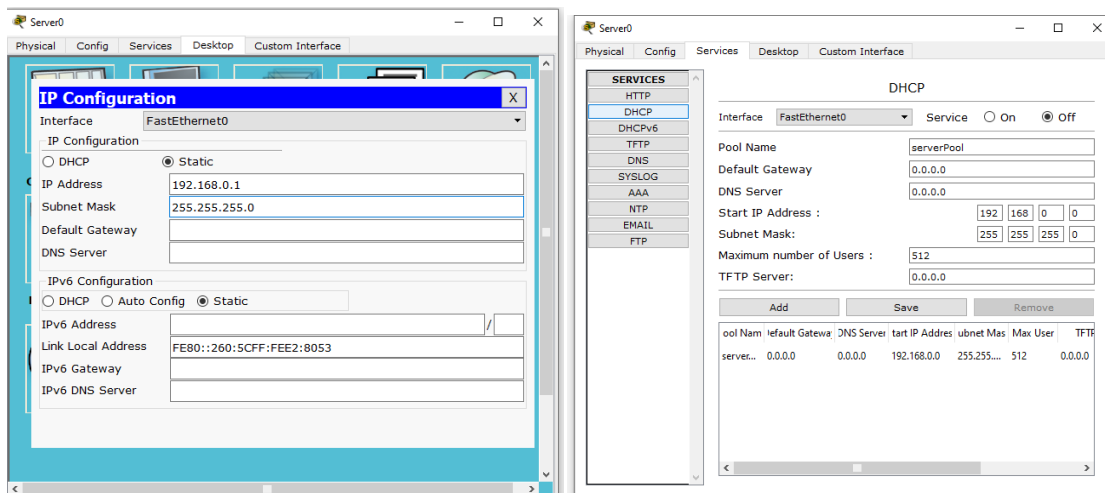
Sr.No	Device	Model-Name	Unit
1	PC	PC-PT	3
2	Laptop	Laptop-PT	2
3	Switch	Switch-PT	1
4	Server	Server-PT	1

- Now create a network topology as shown below the image.
- Use an Copper Straight-Through cable to connect the devices with others.



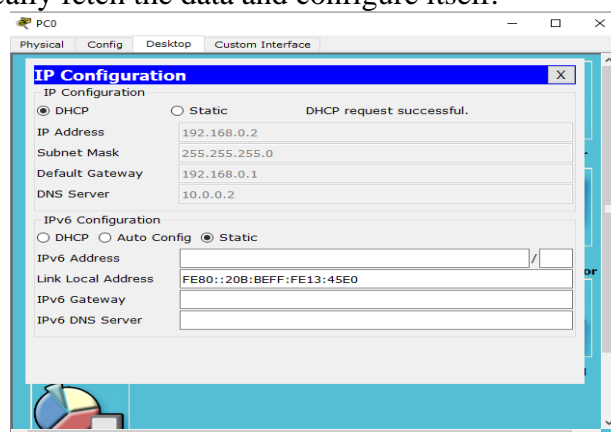
Step 2: Configure the Server with IPv4 address and Subnet Mask.

- To assign an IP address in Server, click on Server-PT.
- Then, go to desktop and IP configuration and there you will find IPv4 configuration.
- Select Static and add IPv4 address, subnet mask.



Step 3: Configuring the PCs and Laptops changing the IP configuration.

- To assign an IP address in PC0, click on PC0.
- Then, go to desktop and IP configuration and there you will find IPv4 configuration.
- Change its state from static to DHCP.
- It will automatically fetch the data and configure itself.



- Repeat the same procedure with other PCs and Laptops to configure them thoroughly.

Result-

Practical No-6

Aim- Configure Internet connection and use IP-Config, PING / Tracert and Net stat utilities to debug the network issues.

Theory- Windows IP Commands – ipconfig, ping, tracert, netstat etc.

Windows IP Commands

Let's now examine the most popular Windows CMD commands (from the DOS prompt) that are related to networking etc:

ipconfig command

This is one of the most useful IP commands on Windows. It displays tons of useful information about the current network settings on the machine such as IPv4 and IPv6 address of all network interface cards (Ethernet adapters, WiFi adapters, virtual network adapters etc), MAC address, default gateway, subnet mask, DNS server, DHCP information etc. If you want to find the local IP address assigned to your computer or the MAC address of your Ethernet Adapter this is the quickest way to find this information.

Here are some different options of this command:

ipconfig /? : Displays all available options.

ipconfig /all : This will display output as shown on the screenshot above but for ALL network connection adapters of the computer (Wired Ethernet, WiFi, VMware adapters etc).

ping command

Now let's examine one of the most popular utilities related to network connectivity.

Probably the first command that every computer user runs on the command line when having connectivity problems is the “ping” command.

This will quickly show you if can send and receive packets (**icmp** packets to be exact) from your computer and hence shows whether you have network connectivity or not.

Note also that “ping” is useful for testing connectivity for both the local computer from where you execute the command and also for a remote computer or server which you try to reach.

If for example you try to “ping” your local default gateway IP address and you get replies back (icmp echo replies), this means your local computer is properly connected to the network.

Now, if you “ping” a remote server on the Internet and you get replies back, it means that the remote server is properly connected to its network as well.

ping /? : Displays all available options as shown below:

ping [IP Address] : By default it will send 4 ICMP packets to the stated IP address.

ping [hostname or domain] : When “pinging” a hostname or domain name, the command will resolve first the name to IP address and then send the icmp packets to that IP.

tracert command

“tracert” in Windows stands for “Trace Route”. In Linux, the same command is “traceroute”.

The command traces the path that a TCP/IP packet takes towards a destination target and shows some information (if available) of the routing nodes within this path.

Just like the “ping” command, “tracert” sends also ICMP echo packets to the destination with varying Time-to-Live (TTL) values.

tracert [domain or IP] : Traces the TCP/IP path to the specified destination target IP or domain.

When troubleshooting connection problems in a large network, you can use tracert to see where the packets stop before reaching the target and focus your efforts to find the problem on the node which does not route packets.

netstat command

Another important command is the Network Statistics (“netstat”) utility found in both Windows and Linux OS.

It shows the established network TCP/IP connections of the local computer with remote hosts, open ports on the machine, the process ID (PID) of each connection etc.

Personally I use this command mostly for security forensic purposes to identify if there are backdoors running on the computer, malicious connections to external Command-and-Control servers etc.

netstat : Displays all connections.

netstat -ano : Displays all connections and listening ports (-a), addresses and ports in numerical form (-n) and also the process ID of each connection (-o).

Result:

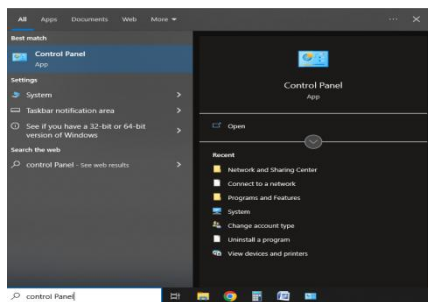
Practical No-7

Aim- Configuration of TCP/IP Protocols in Windows and Linux.

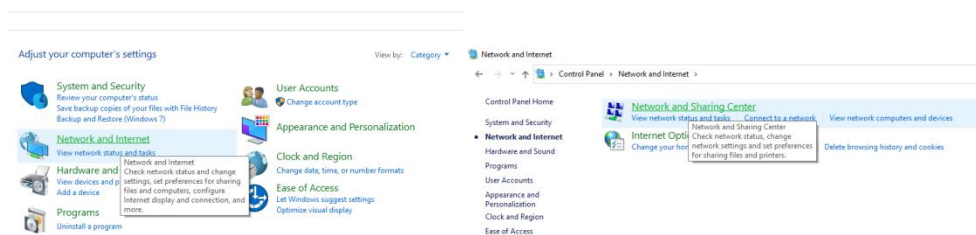
Theory-

The following instructions are based on the Configuring TCP/IP function of Windows XP.

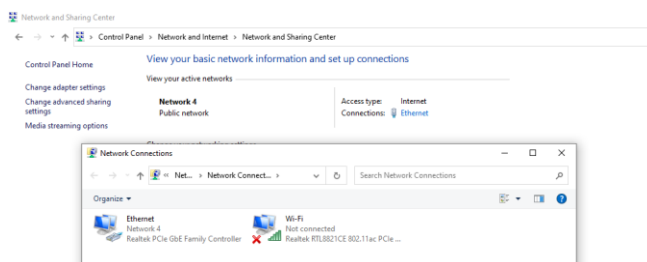
1. Search **Control Panel** using search box.



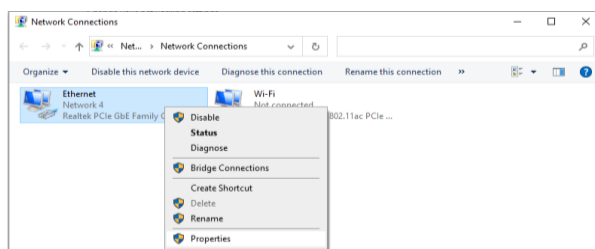
2. On the control panel, double-click **Network and Internet** > double-click **Network and Sharing Center**.



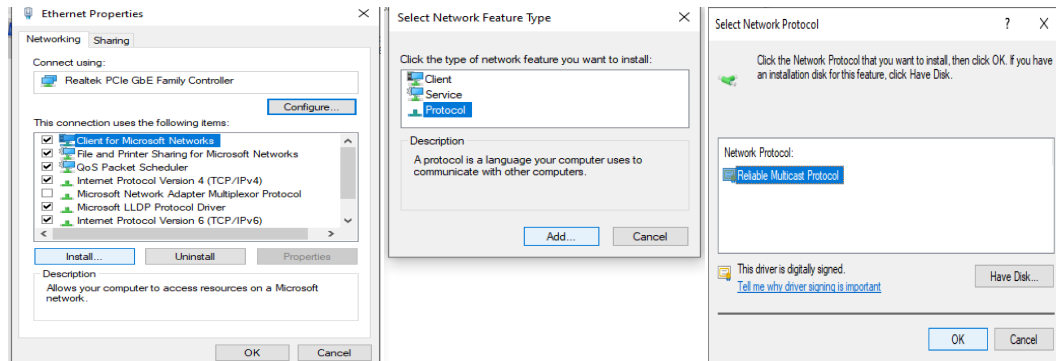
3. Click on **Change adapter settings** on left side of our screen.



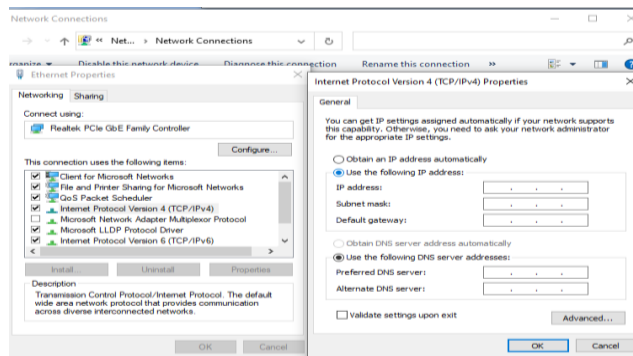
4. Right Click **Ethernet** > Click **Properties**.



5. Click **Properties**. If **Internet Protocol (TCP/IP)** does not appear in the list, do the following:
 - a. Click **Install**.
 - b. Select **Protocol**, and then click **Add**.
 - c. Select **Internet Protocol (TCP/IP)**.
 - d. Click **OK**. This returns you to the Local Area Connection Properties window.



6. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click on **Properties**. Or double-click **Internet Protocol Version 4 (TCP/IPv4)**



7. Select **Use the Following IP Address (2nd Option)**. Check with your network administrator to determine the correct settings for this tab. If your PC does not automatically obtain IP and DNS addresses, do the following:

Press  +  write **cmd > enter > open command prompt > use ipconfig /all** command to check ip address.

```
Wireless LAN adapter Local Area Connection* 12:

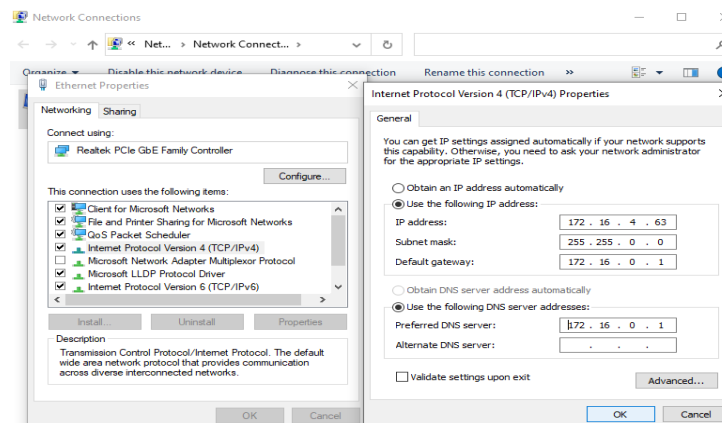
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Physical Address. . . . . : D2-32-4B-0C-3D-31
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : uniboxlogin.wifi-soft.com
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : B4-B6-86-D5-2C-25
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1379:1bc3:a8f3:9119%10(Preferred)
IPv4 Address. . . . . : 172.16.4.63(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : Friday, April 28, 2023 10:30:34 AM
Lease Expires . . . . . : Friday, April 28, 2023 11:12:12 AM
Default Gateway . . . . . : 172.16.0.1
DHCP Server . . . . . : 192.0.2.2
DHCPv6 IAID . . . . . : 179615366
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-80-F7-B8-B4-B6-86-D5-2C-25
DNS Servers . . . . . : 172.16.0.1
                        172.16.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

- a. Enter the IP address of your PC (for example, 172.16.4.63).
- b. Enter the subnet mask (for example, 255.255.0.0).
- c. Enter the default gateway (for example, 172.16.0.1).
- d. Enter the preferred DNS server (for example, 172.16.0.1).
- e. **Enter the alternate DNS server (for example, 172.16.0.1) // optional**

Click **OK**



Result: Hence, in this way we have successfully configured TCP/IP Protocol in windows.

Practical No-9

Aim- Transfer files between systems in LAN using FTP Configuration.

Theory-

FTP employs a **client-server** architecture whereby the client machine has an **FTP client** installed and establishes a connection to an **FTP server** running on a remote machine. After the connection has been established and the user is successfully authenticated, the data transfer phase can begin.

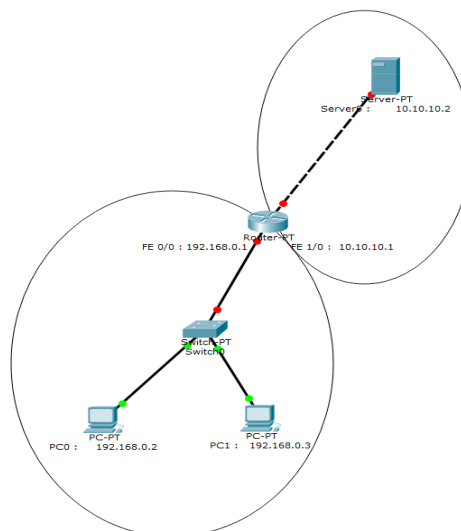
Let's now do FTP configuration in Packet Tracer:

1. Build the network topology.

Step 1: First, open the cisco packet tracer desktop and select the devices given below:

Sr.No	Device	Model-Name	Unit
1	PC	PC-PT	2
2	Switch	Switch-PT	1
3	Router	Router-PT	1
4	Server	Server-PT	1

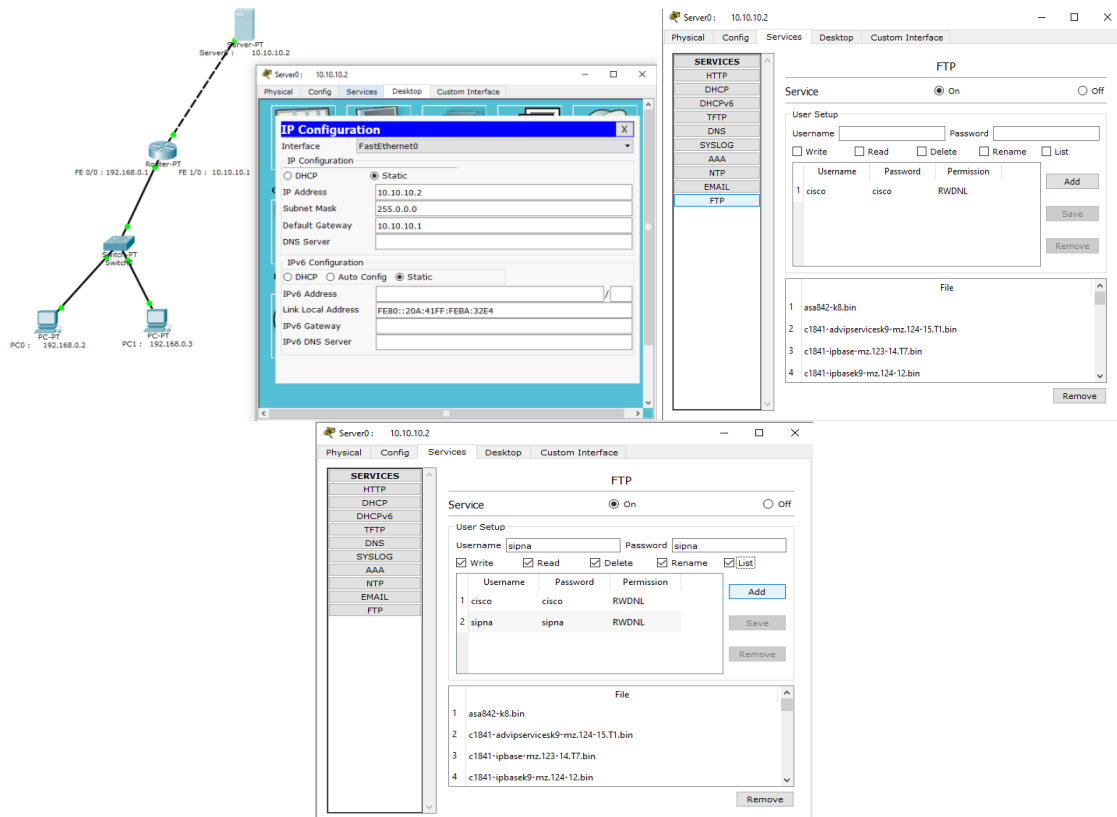
- Now create two different network topologies as shown below the image.
- Use an Automatically Choose Connection Type cable to connect the devices with others from bottom to up .
- Configure Router by assigning 2 IP addresses for Fast Ethernet 0/0 and Fast Ethernet 1/0 as shown in below image.
- Configure PC's by assigning an IP address and Default Gateway (**Default Gateway for PC's: IP address of Router Fast Ethernet 0/0 i.e 192.168.0.1**) as shown in below image.



Step 2: Configure the Server with IPv4 address and Subnet Mask, Default Gateway.

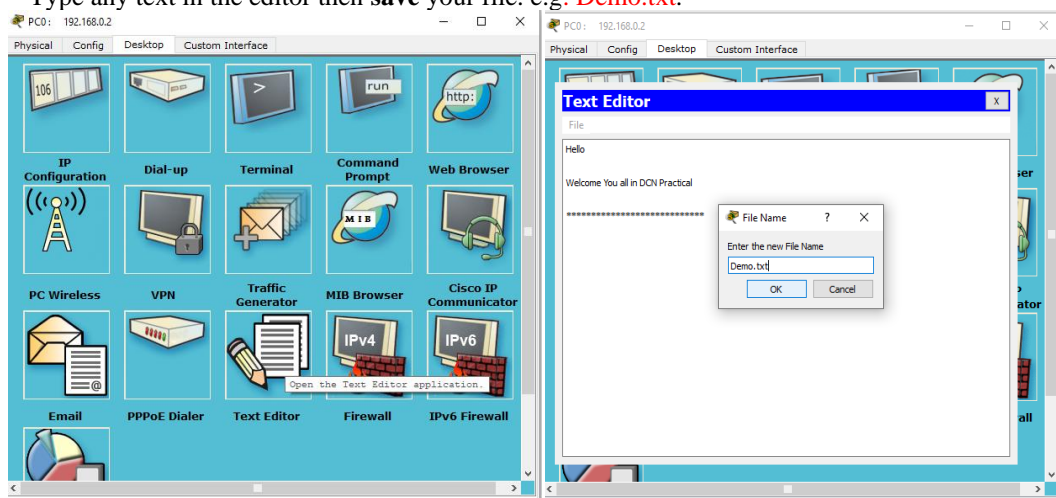
- To assign an IP address in Server, click on Server-PT.

- Then, go to desktop and IP configuration and there you will find IPv4 configuration.
- Select Static and add IPv4 address, Subnet mask and Default Gateway.
- Then, go to **Services** > Select **FTP**.
- Click Service as **On**
- Enter **Username** and **Password**.
- Tick on Write, Read, Delete, Rename, List (As per your choice).
- Click **Add**.



Step 3: Create a file in the PC0 then upload it to the server using FTP.

- To do this, open the **Text Editor** in the PC0, create a file and give it your name of choice.
- Type any text in the editor then **save** your file. e.g. **Demo.txt**.



- Open the PC0's Cisco command prompt and type following commands:
- Ping : to check server is connected with network or not.
>ping Server-IPaddress

```

PC>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time=32ms TTL=127
Reply from 10.10.10.2: bytes=32 time=0ms TTL=127
Reply from 10.10.10.2: bytes=32 time=0ms TTL=127
Reply from 10.10.10.2: bytes=32 time=1ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 32ms, Average = 8ms

PC>

```

- FTP the server using the server IP address by typing:

>ftp 10.10.10.2

Provide the **username** and **password** for ftp login.

```

PC>ftp 10.10.10.2
Trying to connect...10.10.10.2
Connected to 10.10.10.2
220- Welcome to PT Ftp server
Username:sipna
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put Demo.txt

Writing file Demo.txt to 10.10.10.2:
File transfer in progress...

[Transfer complete - 67 bytes]

67 bytes copied in 0.038 secs (1763 bytes/sec)
ftp>

```

You are now in the FTP prompt.

- Upload the file from the PC0 to the server using FTP.
So to do an FTP upload, we'll type:

>put Demo.txt

```

ftp>put Demo.txt

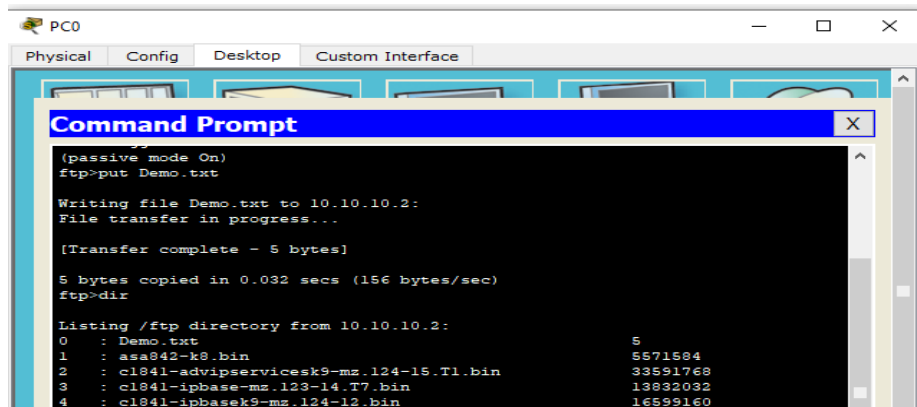
Writing file Demo.txt to 10.10.10.2:
File transfer in progress...

[Transfer complete - 5 bytes]

5 bytes copied in 0.032 secs (156 bytes/sec)
ftp>

```

- To check whether File is uploading successfully we type following command
>dir



```
PC0
Physical Config Desktop Custom Interface

Command Prompt
(passive mode On)
ftp>put Demo.txt

Writing file Demo.txt to 10.10.10.2:
File transfer in progress...

[Transfer complete - 5 bytes]

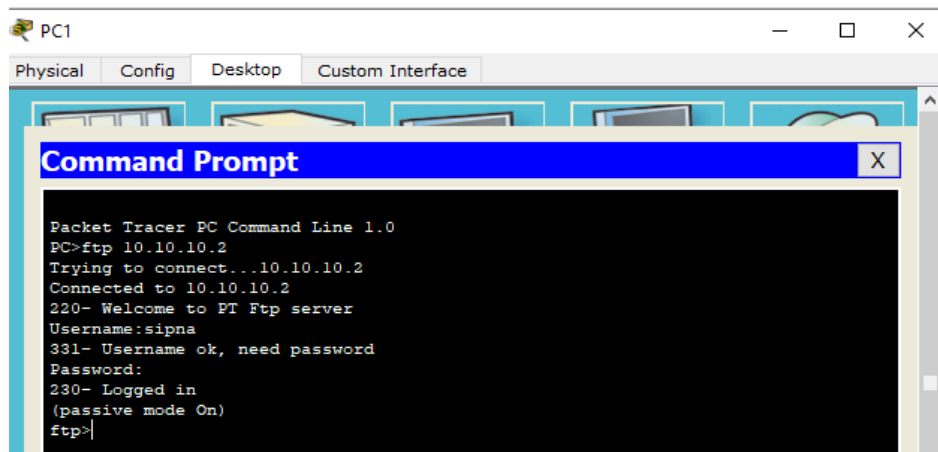
5 bytes copied in 0.032 secs (156 bytes/sec)
ftp>dir

Listing /ftp directory from 10.10.10.2:
 0 : Demo.txt                               5
 1 : asa842-k8.bin                         5571584
 2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
 3 : c1841-ipbase-mz.123-14.T7.bin          13832032
 4 : c1841-ipbasek9-mz.124-12.bin           16599160
```

- Open the **PC1**'s Cisco command prompt and type following commands FTP the server using the server IP address by typing:

>ftp 10.10.10.2

Provide the **username** and **password** for ftp login.

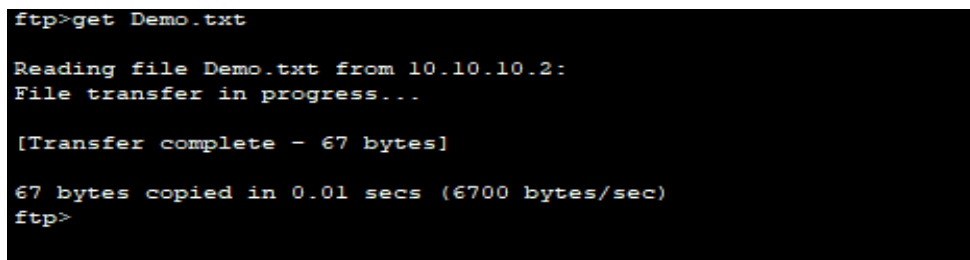


```
PC1
Physical Config Desktop Custom Interface

Command Prompt
Packet Tracer PC Command Line 1.0
PC>ftp 10.10.10.2
Trying to connect...10.10.10.2
Connected to 10.10.10.2
220- Welcome to FT Ftp server
Username:sipna
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

You are now in the FTP prompt.

- Download the file from server using FTP services from PC1.
So to do an FTP Download, we'll type:
>get Demo.txt
get- used to get(download) a file from the server.



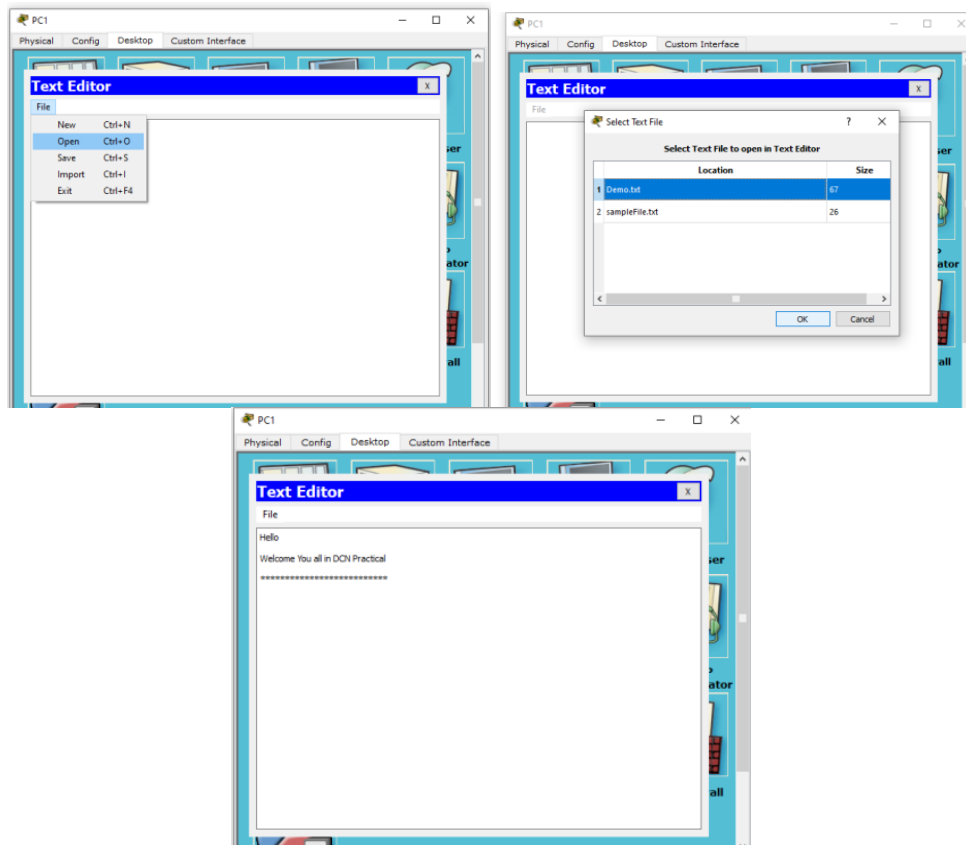
```
ftp>get Demo.txt

Reading file Demo.txt from 10.10.10.2:
File transfer in progress...

[Transfer complete - 67 bytes]

67 bytes copied in 0.01 secs (6700 bytes/sec)
ftp>
```

- To check File is downloading successfully from PC1 open Text Editor of PC1.
- Click File> Open>Select file>Ok.



Result: Hence, in this way we have successfully transfer files between systems in LAN using FTP Configuration.

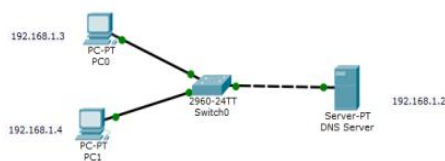
Practical No-10

Aim- Configuration of DNS Service in network.

Theory-

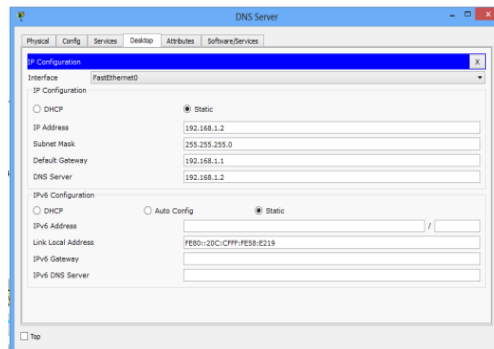
A Domain Name System (**DNS**) server resolves host names into IP addresses. Although we can access a network host using its IP address, DNS makes it easier by allowing us use domain names which are easier to remember.

1. Build the network topology.

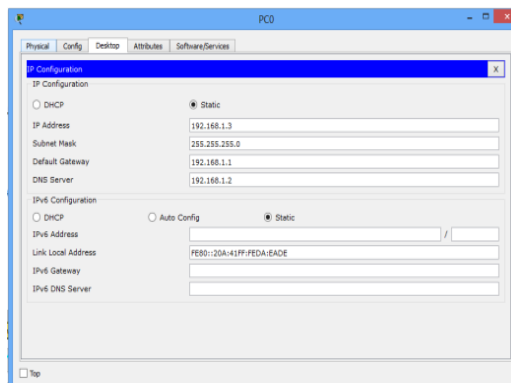


2. Configure static IP addresses on the PCs and the server.

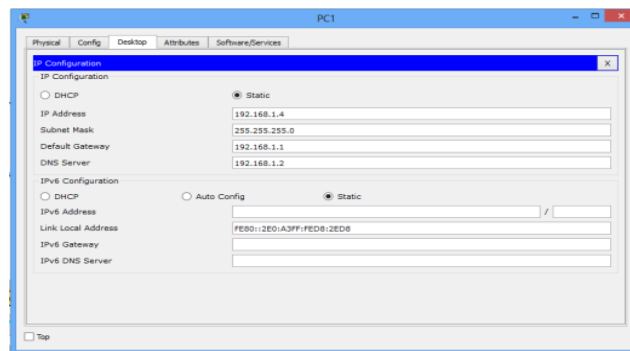
Server :- IP address: 192.168.1.2 **Subnet mask:** 255.255.255.0 **Default gateway:** 192.168.1.1 **DNS Server:** 192.168.1.2



PC0 :- IP add: 192.168.1.3 **Subnet mask:** 255.255.255.0 **Default gateway:** 192.168.1.1 **DNS server:** 192.168.1.2



PC1 :- IP address: 192.168.1.4 Subnet mask: 255.255.255.0 Default gateway: 192.168.1.1 DNS Server: 192.168.1.2



3. Configure DNS service on the generic server.

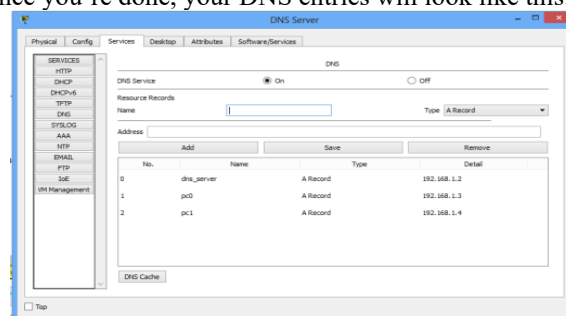
To do this, click on the server, then Click on **Services** tab. Click on **DNS** server from the menu. First turn **ON** the DNS service, then define **names** of the hosts and their corresponding **IP addresses**.

For example, to specify the DNS entry for PC0: In the **name** and **address** fields, type:

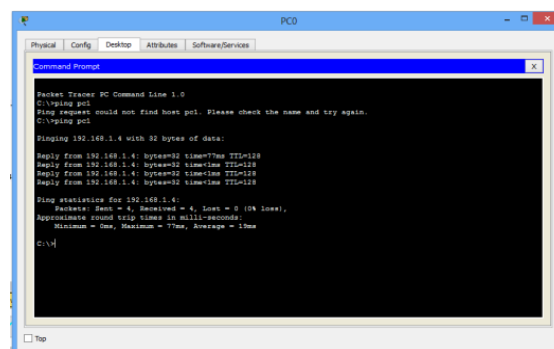
Name: PC0 **Address:** 192.168.1.3

- Click on **add** then **save**. Repeat this for the PC1 and the server.

Once you're done, your DNS entries will look like this:



4. Test **domain name – IP resolution**. Ping the hosts from one another using their names instead of their IP addresses. If the DNS service is turned on and all IP configurations are okay, then ping should work. For example, ping PC1 from PC0. Ping should be successful.



Result: Hence, in this way we have successfully Configured DNS Service in network.