**TABLE OF CONTENTS**

[Lab 1: Basic Network Equipment 1](#_bookmark0)

[Lab 2: Network Cables 3](#_bookmark1)

[Lab 3: Basic Networking Commands (Dos Commands) 5](#_bookmark2)

[Lap 4: IPv4 Addressing and Subnetting 11](#_bookmark3)

[Lap 5: Overview of Packet Tracer and its features 13](#_bookmark4)

[Lab 6: Implementation of LAN 15](#_bookmark5)

[Lab 7: Implementation of DHCP 17](#_bookmark6)

[Lap 8: Implementation of DNS 19](#_bookmark7)

[Lab 9: Implementation of HTTP 22](#_bookmark8)

## Objectives

# Lab 1: Basic Network Equipment

* To understand Basic Network Equipment

## Theory

1. **Hub:** A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmission to specific devices. Network hubs are best suited for small, simple local area network (LAN) environments. Hubs cannot provide routing capabilities or other advanced network service.



#### Fig: Hub

1. **Switch:** A network switch connects devices (such as computers, printers, wireless access points) in a network to each other, and allows them to “talk” by exchanging data packets. Switches can be hardware devices that manage physical networks, as well as software-based virtual devices.



#### Fig: Switch

1. **Router:** A router is a device that connects two or, more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by

forwarding data packets to their intended IP Addresses and allowing multiple devices to use the same internet connection.



#### Fig: Router

1. **Bridge:** A network bridge is a computer networking device that creates a single, aggregate network from multiple communication networks or network segments. This function is called network bridging. Bridging connects two separate networks as if they were a single network.



#### Fig: Bridge

1. **Repeater:** A repeater is a network device that retransmits a received single with more power and to an extended geographical or topological network boundary than what would be capable or topological network boundary than what would be capable with the original signal. Repeaters amplify the received/input signal to a higher frequency domain so that it is reusable, scalable, and available.



#### Fig: Repeater

**Conclusion:** Hence, we understood about the different networking devices.

## Objective

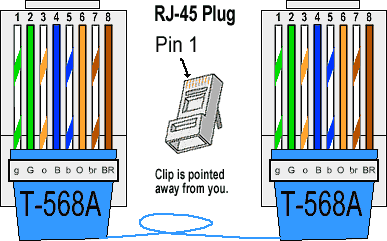
# Lab 2: Network Cables

### To construct straight and crossover cable

## Theory

#### Standard (Straight Cabling):

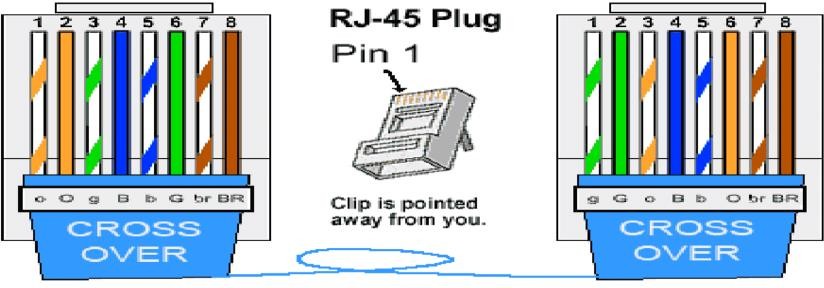
A straight cable is used to connect dissimilar devices such as a computer to a hub, TVs to a router, and so on. Straight cabling has the same pinout at both ends. This types of twisted-pair cable are used in LAN to connect a computer or a network hub such as a router. It follows either the T568A (outdated) or T568B standards. The most common types of cabling are used today.



#### Fig: Straight cabling

#### Crossover Cabling:

A cross cable is used to connect two similar devices, only by using the cable itself. The connection between PC–to–PC, Router ––Router, Hub–to–Hub, etc. can be done using crossover cabling. Crossover cabling has different pins out at both ends, specifically T8566A at one end and T856B at the other end. It is widely used to connect two devices of the same type: e.g., two computers or two switches to each other.

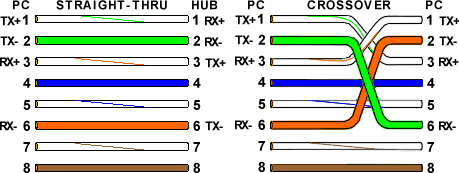


#### Fig: Crossover cabling

#### Procedure:

For the implementation of the straight and cross-cabling standards in networking. The UTP cable must be crimped using the procedure described below:

* 1. Remove the outmost vinyl shield for 12mm at one end of the cable (Say A side)
  2. Cut the inner transparent plastic thread.
  3. Arrange the wires according to the desired standard.
  4. Insert the metal wires into the RJ45 connector keeping the arrangement of wire the same.
  5. Also make the other side of the cable (Say B side)
  6. The crimping is complete.



Testing the crimped cable using the cable tester:

1. Connect one end of the crimped cable to the master port and another node to the remake port of the cable tester
2. Press the start button and ensure that all the lights blink synchronously in both the master and slave.
3. If any light does not blink or multiple lights blink at once, there is an error in the cable.
4. Re-crimp the cable and test again.

## Conclusion:

Hence, both straight and crossover cables were constructed and tested successfully**.**

# Lab 3: Basic Networking Commands (Dos Commands)

## Objective

* To understand networking commands in DOS

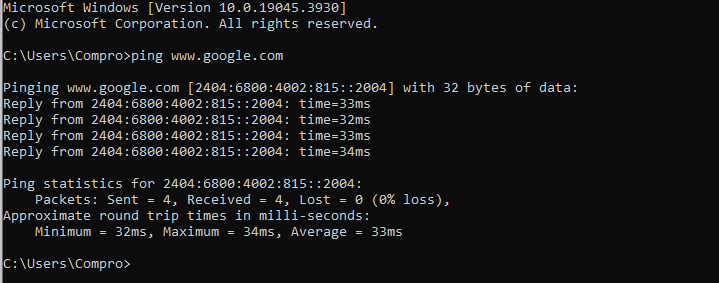
#### Theory:

Networking Commands in DOS

#### Ping

The ping command is one of the most often used networking utilities for detecting devices on a network and for troubleshooting network problems. When you ping a device you send that devices a short message, which it then sends back (the echo).

The general format is ping hostname or ping IP address. Example: Ping [www.google.com](http://www.google.com/) or Ping: 192.168.10.10



#### Ipconfig:

Another indispensable and frequently used utility is used for finding network information about your local machine-like IP addresses. DNS addresses etc.

Basic Use: Finding Your IP Address and Default Gateway Ipconfig has several switches the most common are:

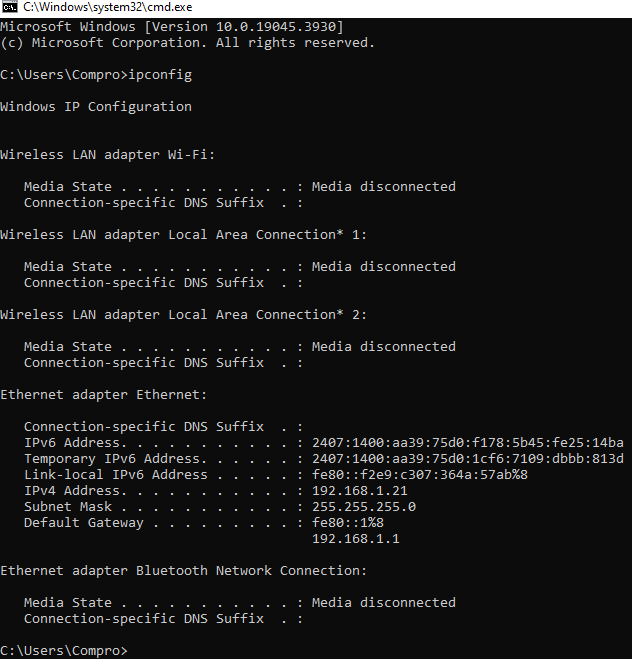
*Ipconfig/all*- display more information about the network setup on your systems including the MAC address.

*ipconfig/release* --release the current IP address

*ipconfig/renew* – renew IP address

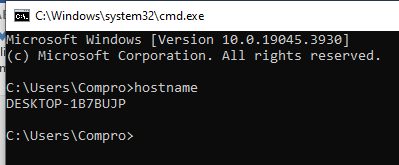
*ipconfig/?* – shows help

*ipconfig/flushdns* - flush the DNS caches



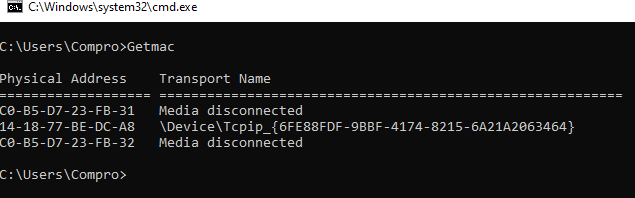
#### Hostname:

A very simple command that displays the hostname of your machine. This is much quicker than going to the control panel >system route.



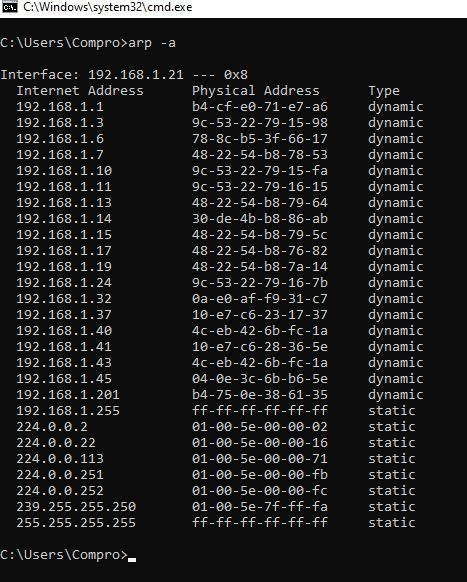
#### getmac:

Another very simple command that shows the MAC address of your network interfaces**.**



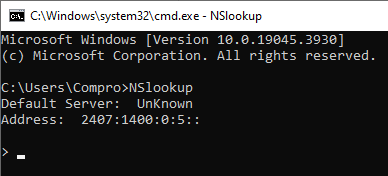
#### arp -a

This is used for showing the address resolution cache. This command must be used with a command line switch arp –a is the most common.



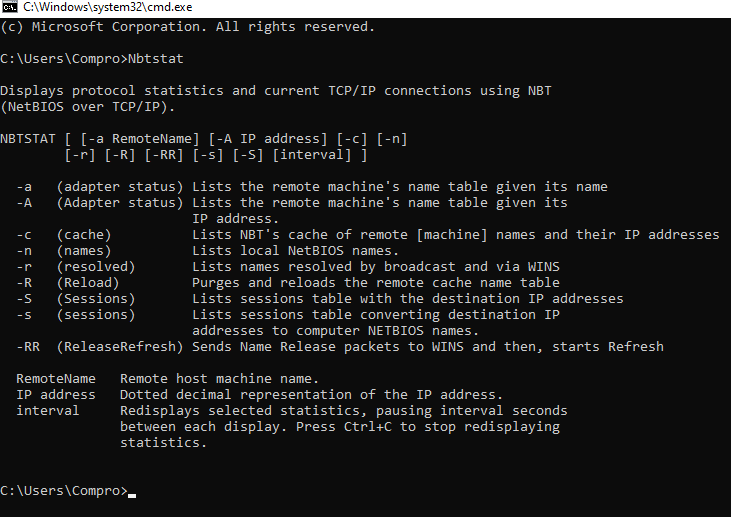
#### NSlookup:

Used for checking DNS record entries.



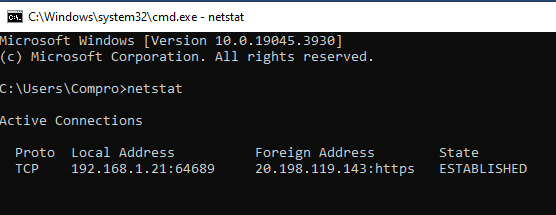
#### Nbtstat:

Diagnostic tool for troubleshooting NetBIOS problems.



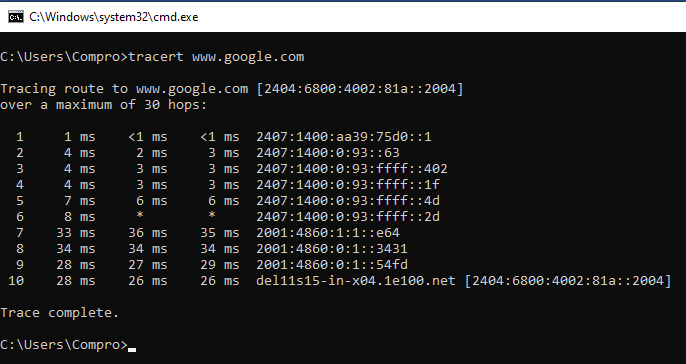
#### Netstat:

Used for displaying information about TCP and UPD connections and ports.

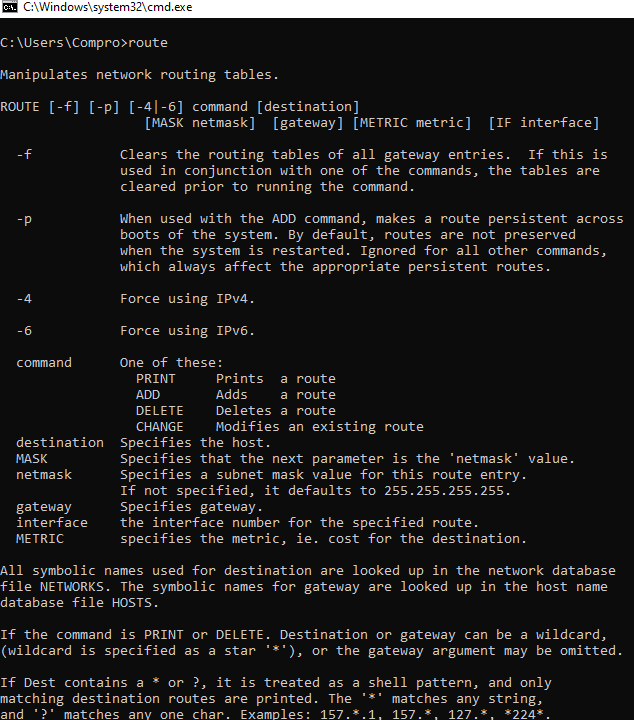


#### Tracert:

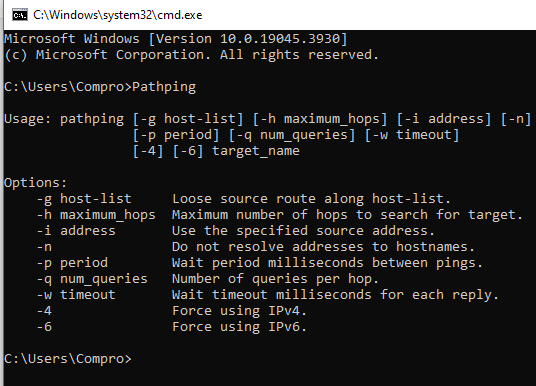
The tracert command is a command Prompt command that is used to get the network packet being sent and received and the number of hops for that packet to reach to target.

Example: target [www.google.com](http://www.google.com/)

#### Route:

In IP networks, routing tables are used to direct packets from one subnet to another. The Route command provides the device’s routing tables. To get this result, just type route print. The Route command results in the routing table, and the user can make changes by Commands such as Route Add, Route Delete, and Route Change, which allows modifying the routing table as a requirement.

#### Path Ping:

The pathing command provides a combination of the best aspects of Tracert and Ping.

**Conclusion:** Hence, all networking commands were executed successfully in command prompts.

## Objective

# Lap 4: IPv4 Addressing and Subnetting

* + To understand theoretical knowledge of IPV4 Addressing and subnetting

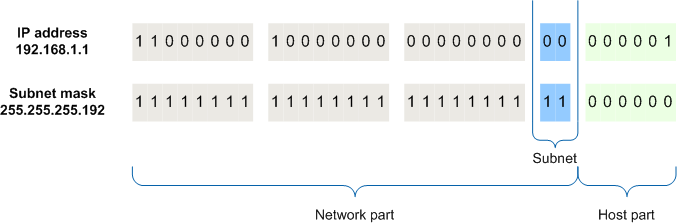
## Theory:

#### IPV4 Address:

An IP address is an address used to uniquely identify a device on an IP network. The IPV4 address is made up of 32 binary bits which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet 8 bits). Each octet is converted to decimal and separated by a period(dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 0000000011111111 binaries.

#### Subnetting:

Subnetting is the practice of dividing a network into two or smaller networks. Subnets often work as a subnet mask, which acts as a sort of filter for internet traffic. The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use a Subnet Mask, which is as long as the size of the network address in the IP address. The Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mark, the result yields the Network address. For example, say the IP address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then



This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

## Conclusion:

Hence, we understood IP Addressing and Subnetting**.**

## Objective

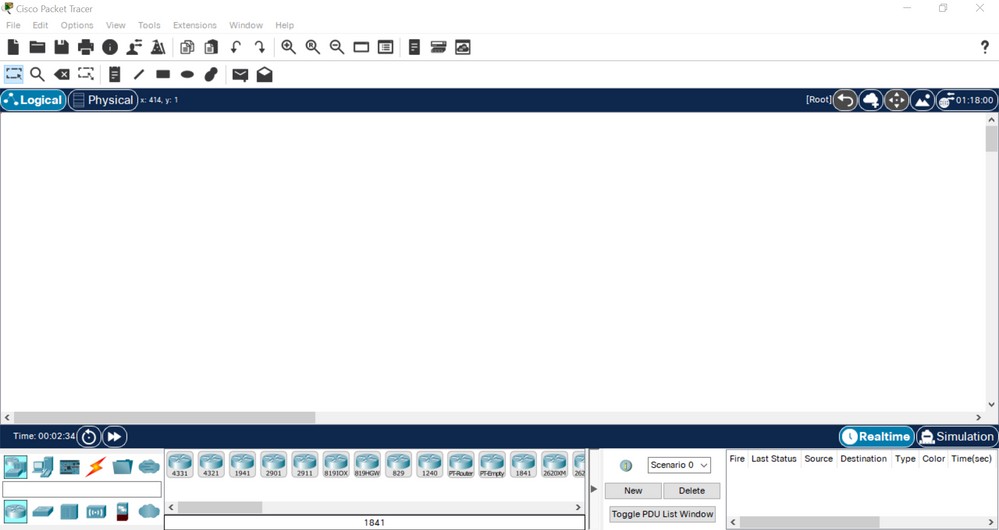
# Lap 5: Overview of Packet Tracer and its features

* To understand the network simulator tools.
* To understand LAN networking, creation of VLAN, and IP addressing in the VLAN and VLAN Trunk.

## Theory

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag-and-drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused on Cisco Networking Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches, and various other types of network devices. A physical connection between devices is represented by a 'cable' item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, and BGP, to the extent required by the current CCNA curriculum. As of version 5.3, Packet Tracer also supports the Border Gateway Protocol.



#### Fig: Interface of Cisco packet Tracer

#### Feature of Cisco packet Tracer

1. Network Simulation
2. Device Emulation
3. Multiuser Collaboration
4. Packet Capture and Analysis
5. Built-in Protocols and Applications
6. Interactive Learning Activities

## Conclusion:

This lab aims to familiar with the Cisco Packet Tracer.

# Lab 6: Implementation of LAN

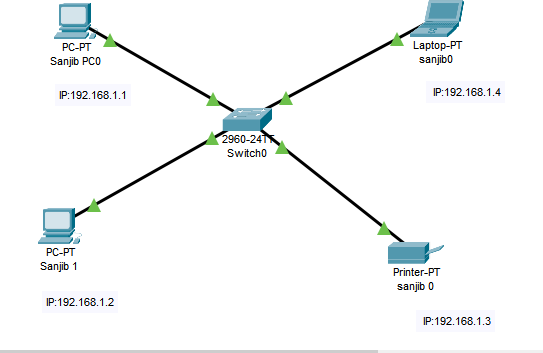
### **Objective:** To know the implementation of the Local Area Network

## Theory:

A local area network (LAN) is a collection of devices connected to one physical location, such as a building, office, or home. A LAN can be smaller or larger, ranging from a home network with thousands of users to an enterprise network with thousands of users and devices in an office or school. A LAN comprises cables, access points switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANS via wide area networks.

## Implementation:

In the packet tracer, computers are connected to a switch and the switch is connected to a router through wires. IP Address is assigned to the router and the computers. The computer must use the IP Address of the router as its default gateway. After assigning IP addresses and gateways the computer should be able to communicate with the router and also with each other. Each computer must be assigned a unique IP Address.



#### Fig: LAN

Switch and client as required

* Configure gateway and local IP for –client
* Configure the switch under the LAN database give the LAN no and LAN name check the port no of the router on which the switch is connected and change that to trunk. Make sure all clients are configured to LAN checking their port.

## Conclusion:

Hence, LAN configurations are implemented using a Cisco packet tracer.

## Objective:

# Lab 7: Implementation of DHCP

* To know about the implementation of the Dynamic Host Configuration Protocol

## Theory:

DHCP is a network protocol used on an IP network where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints. In addition to the IP address, DHCP also assigns the subnet mask, default gateway address, domain name server (DNS) address, and other pertinent configuration parameters.

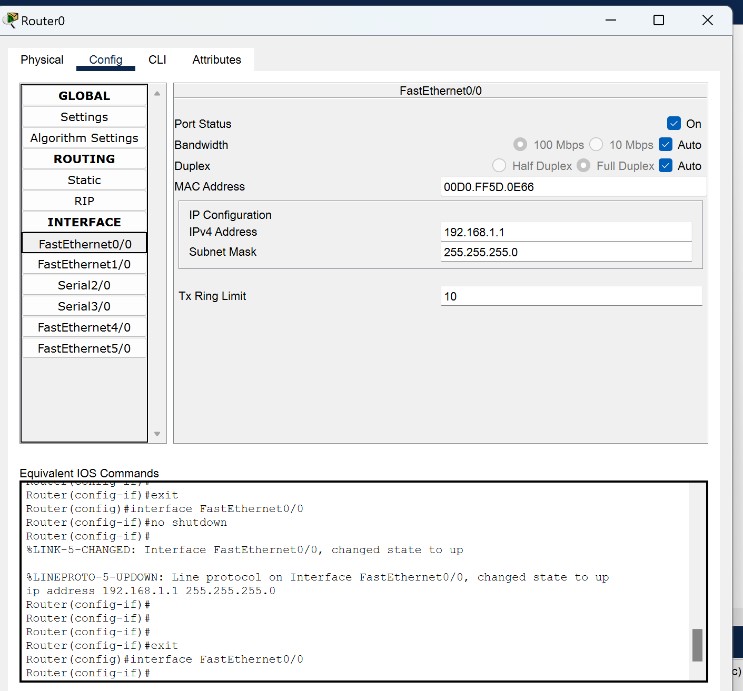
## Implementation:

Step 1: Set a router with one server and set a desktop as required.

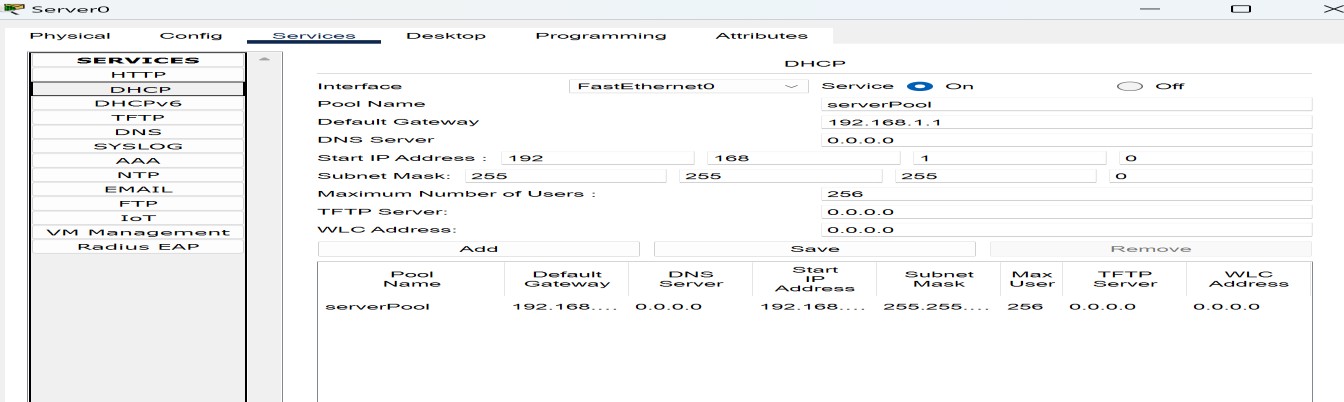
Step 2: Enable the ports of the router and set an IP address for both server and router.

Step 3: Go to services on the server and the services assign the IP address of the router in the server and set the start IP address.

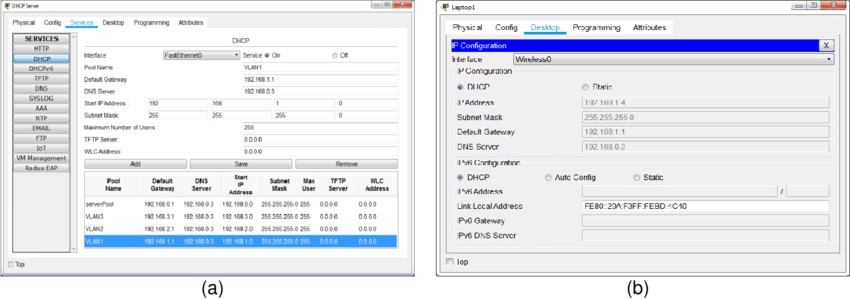
Step 4: Enable the DHCP in the IP configuration section of the desktop.



#### Fig: Router Configuration (DHCP)

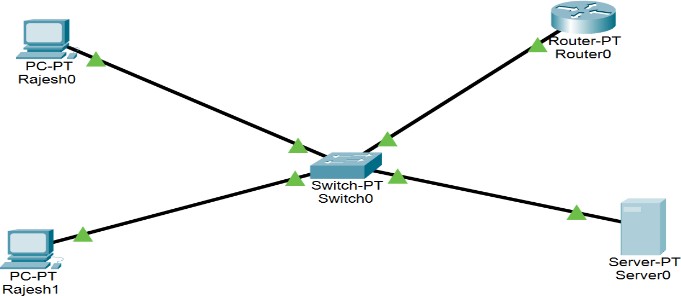


#### Fig: Server Configuration (DHCP)



#### Fig: IP Assignment Dynamically (DHCP)

* DHCP server IP assignment



## Conclusion:

Hence, DHCP Configuration is implemented using a packet tracer.

## Objective:

# Lap 8: Implementation of DNS

* To understand the function and importance of DNS service in a network environment.
* Configuration of a DNS server to manage domain name resolution

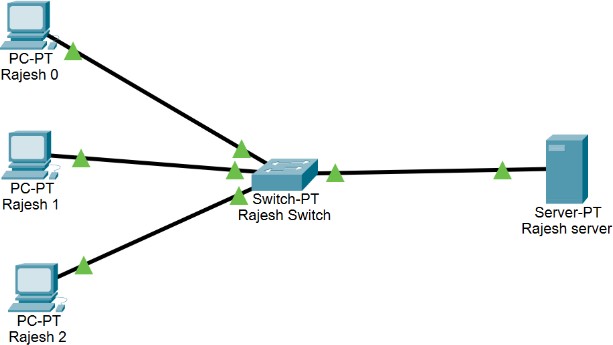
## DNS server

The purpose of a DNS server is to translate what a user types into their browser into something a computer can understand and use to locate a website. In other words, its purpose is to convert a domain name such as [www.example.com](http://www.example.com/) into an IP address such as 71.232.101.120.

Thanks to DNS servers, people don’t have to memorize complex IP addresses like 216.58.217.206, which is Google’s IP address. They just have to memorize [www.google.com.This](http://www.google.com.This/) translation process — formally known as DNS resolution — requires multiple hardware components. The most important is known as the primary DNS server.

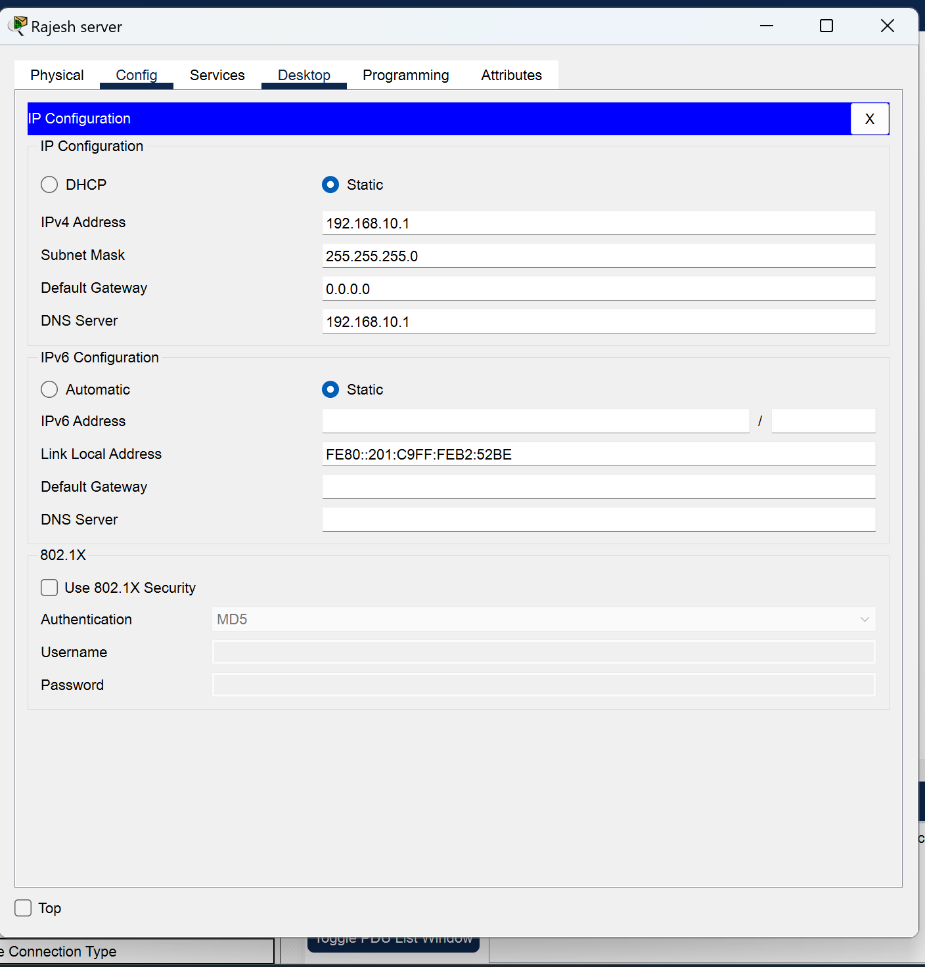
#### Configuring a DNS server

* + Create a network with end devices, switch, and DNS server.

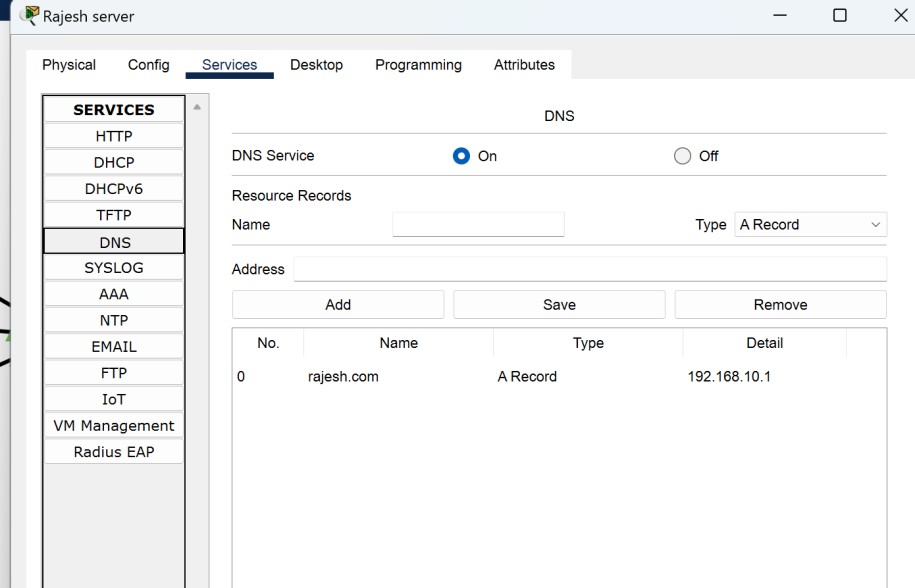


#### Fig: ip configuration

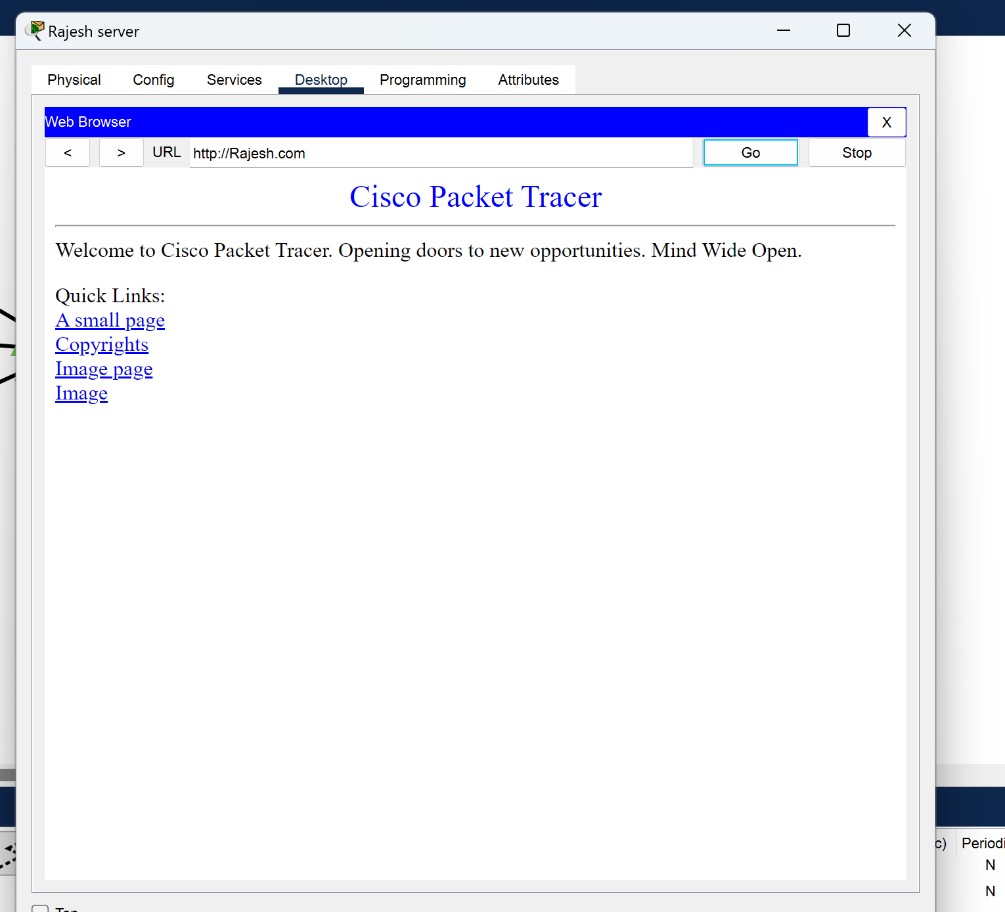
* + Configure the IP addresses to all devices and add the DNS server’s IP to the ‘DNS server’ section of the IP configuration menu.



* + Open the DNS server, go to services, and turn on DNS. add a website address and add.



* Open the web browser on any end device and type in a website address and the website should appear.



## Conclusion:

The lab aims to become familiar with DNS Servers.

## Objective

# Lab 9: Implementation of HTTP

* To know about the HTTP
* To know about the web server, and perform the HTTP operation

## Overview

The implementation of HTTP, or Hypertext Transfer Protocol, involves the creation of software systems that enable communication between clients, such as web browsers, and servers, such as web servers. HTTP operates on a request-response model, where clients send requests to servers, and servers respond with the requested resources or information. The implementation process typically includes developing HTTP servers capable of handling incoming requests, parsing request headers, processing data, and generating appropriate responses. Additionally, HTTP clients are designed to send requests, interpret responses, and handle various status codes. Implementation efforts focus on adhering to HTTP specifications, optimizing performance, ensuring reliability, and incorporating security measures to create robust and efficient systems for web communication.

## HTTP Working

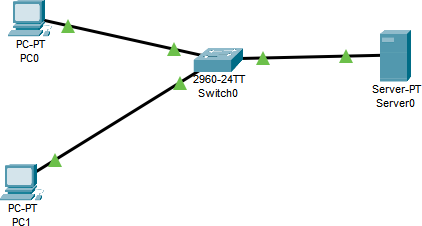
Http responds to the client's request in either of the following two ways:

* Sending the file to the client associated with the requested URL.
* Generating response by invoking a script and communicating with the database.

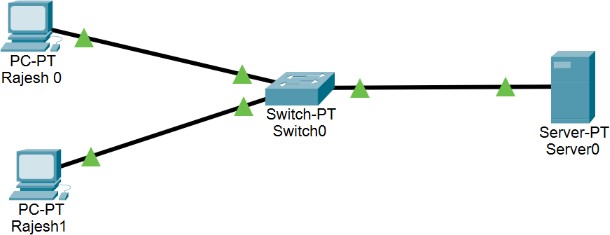
## Configuring an HTTP

To configure a web server, we follow the steps below:

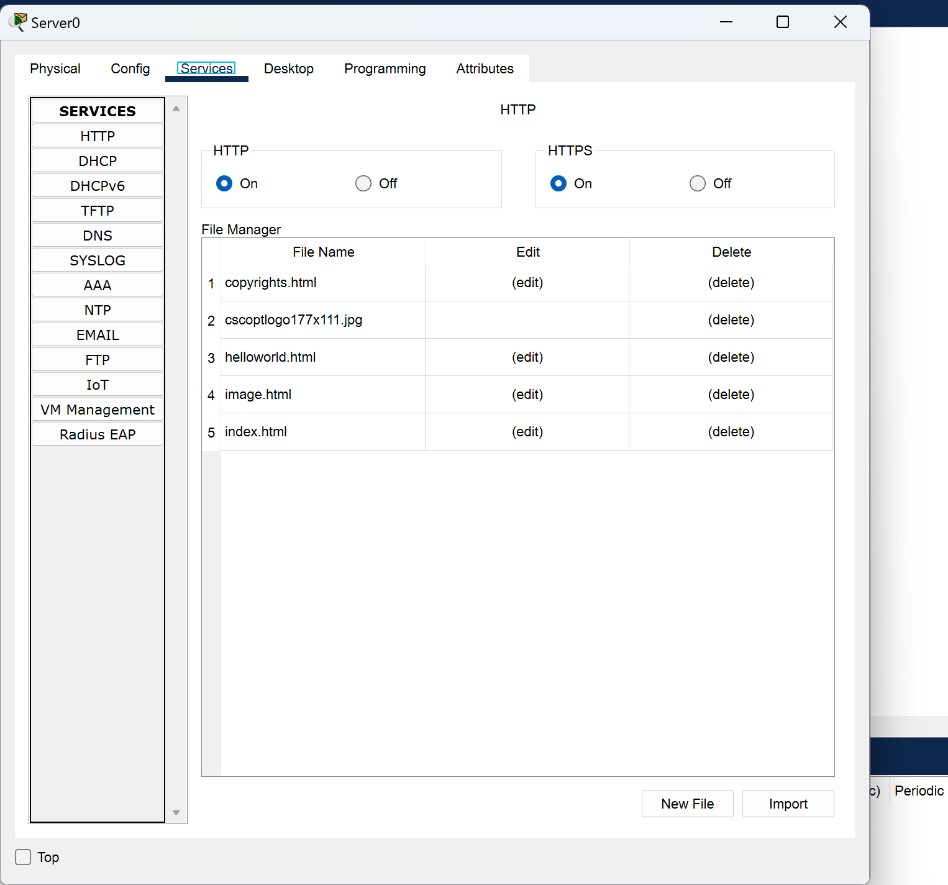
* + Create a network with a switch, a server, and end devices.



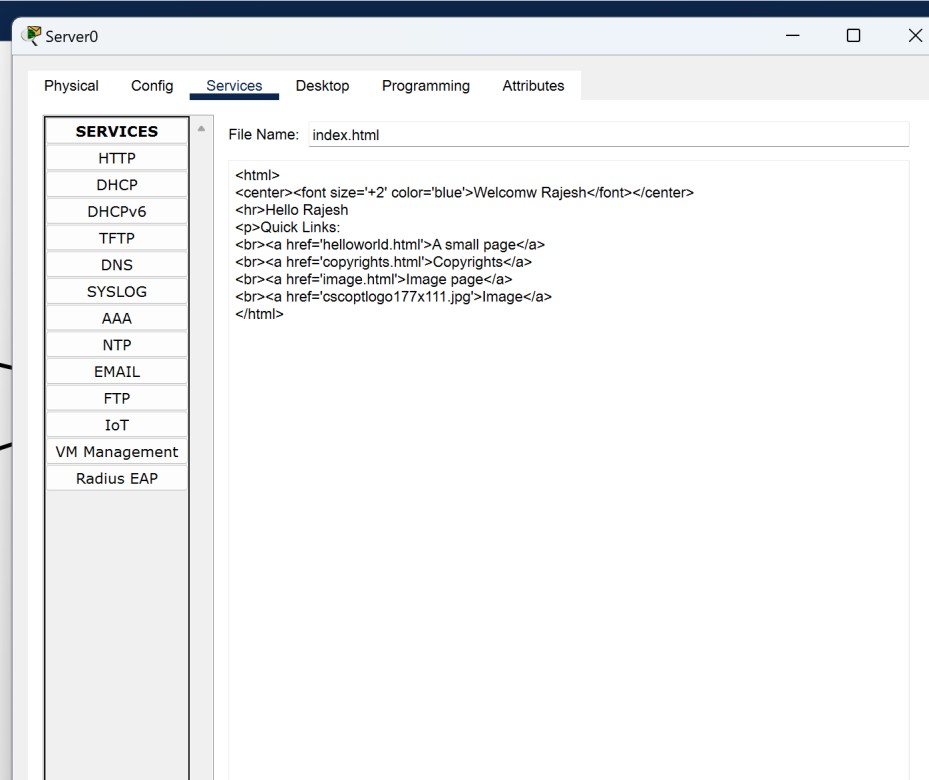
* + Configure IPs of switch server and end devices.



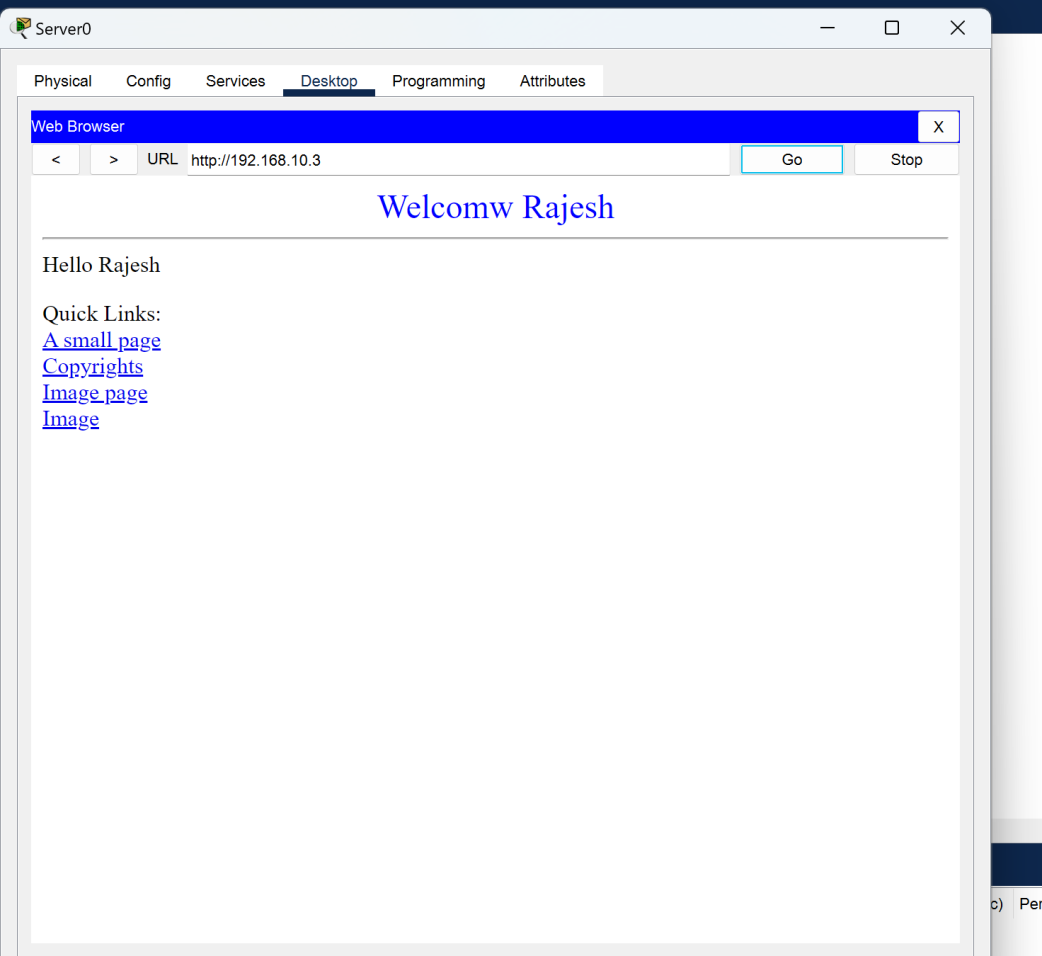
* + Open server. Go to the services tab. Click https and turn http and https on.



* + Edit the index.html file and save



* + Open up the browser and type in the IP of the webserver and the website will open up.



## Conclusion:

The lab aims to become familiar with HTTP.