**COMPUTER NETWORK**

**PRACTICAL SHEET**



August 27, 2022

rITIK lAL sHRESTHA

Prime College, CSIT 4th “B”

Contents

[1. Detail Understanding of basic Networking Devices and its workings 2](#_Toc112498498)

[ Hub 2](#_Toc112498499)

[ Switch 3](#_Toc112498500)

[ Bridge 3](#_Toc112498501)

[ Routers 3](#_Toc112498502)

[ Gateway 4](#_Toc112498503)

[ Repeaters 4](#_Toc112498504)

[2. Basic Networking Commands 7](#_Toc112498505)

[ Ipconfig 7](#_Toc112498506)

[ Ipconfig/all 7](#_Toc112498507)

[ Netstat 8](#_Toc112498508)

[ Tracert/Traceroute 9](#_Toc112498509)

[ Ping 10](#_Toc112498510)

[ Arp –a 11](#_Toc112498511)

[ Nslookup 11](#_Toc112498512)

[ Pathping 12](#_Toc112498513)

[ Hostname 12](#_Toc112498514)

[ Getmac 12](#_Toc112498515)

[3. Understanding IP Addressing and Sub-netting, Static IP Setting 13](#_Toc112498516)

[IPv4 Addressing 13](#_Toc112498517)

[Subnet Mask 13](#_Toc112498518)

[Network Classes 13](#_Toc112498519)

[Subnetting a Class C network 14](#_Toc112498520)

[Subnetting a Class B network 15](#_Toc112498521)

[Subnetting class A network 15](#_Toc112498522)

[4. Introduction to Packet Tracer, creating of a LAN and connectivity test in the LAN 16](#_Toc112498523)

[Introduction to Packet Tracer 16](#_Toc112498524)

[Creating a Local Area Network 16](#_Toc112498525)

[Connectivity test in LAN 19](#_Toc112498526)

[5. Basic Router Configuration and its Routing Implementation 21](#_Toc112498527)

[Basic Router Configuration 21](#_Toc112498528)

[Routing 23](#_Toc112498529)

[Static Routing 23](#_Toc112498530)

[Implementation of Static routing 23](#_Toc112498531)

[6. Implementation of Dynamic/interior/exterior routing (RIP, OSPF, BGP) 26](#_Toc112498532)

[Dynamic Routing 26](#_Toc112498533)

[Implementation of Dynamic Routing RIP 26](#_Toc112498534)

[OSPF 28](#_Toc112498535)

[BGP 31](#_Toc112498536)

[Implementation of BGP protocol 31](#_Toc112498537)

[7. Packet capture and header analysis by wire-shark (TCP, UDP, IP) 33](#_Toc112498538)

[Wireshark 33](#_Toc112498539)

[Packet Capture 33](#_Toc112498540)

[Packet Filtering 34](#_Toc112498541)

[Packet Analysis 34](#_Toc112498542)

[8. Basic concept of DNS, Web, FTP, DHCP 36](#_Toc112498543)

[Web Server 36](#_Toc112498544)

[Configuring a web server 36](#_Toc112498545)

[DNS server 40](#_Toc112498546)

[Configuring a DNS server 40](#_Toc112498547)

[FTP 43](#_Toc112498548)

[Implementation of FTP server 43](#_Toc112498549)

[DHCP 45](#_Toc112498550)

[Email Server 47](#_Toc112498551)

# Detail Understanding of basic Networking Devices and its workings

**Network Devices**

Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices. Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network. These devices transfer data in a fast, secure and correct way over same or different networks. Some of the networking devices are:

## Hub

A hub is a repeater with multiple ports, and can be thought of as being the center point of a star topology network. It is often known as a multi-port repeater (or as a concentrator in Ethernet).

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.



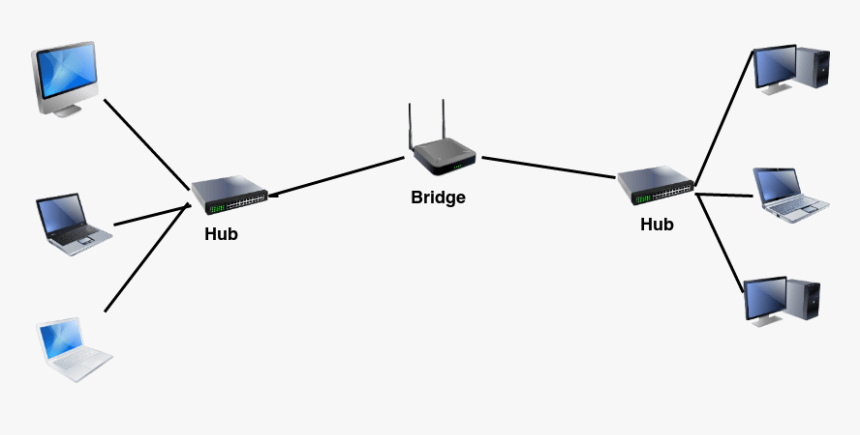
## Switch

A switch is an intelligence device and operates at Layer-2 of OSI layer. It 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.



## Bridge

A network bridge connects multiple network segments at the data link layer (Layer 2) of the OSI model. In other words, it is normally used to connect two networks at the data link layer. Useful when the networks have different data link layers but the same network layer. For ex. A connection between Ethernet and token bus would normally be a bridge. 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.

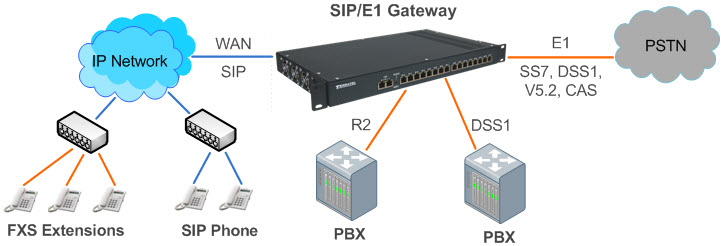


## Routers

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.

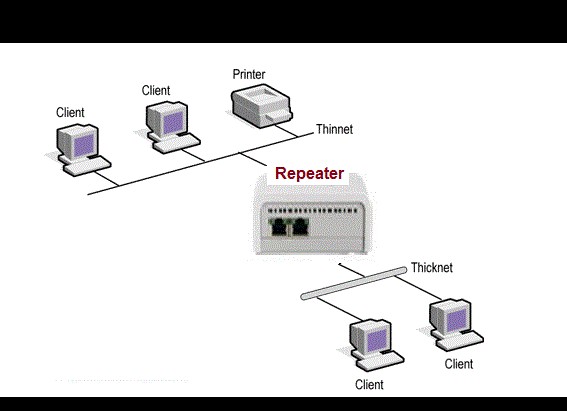


## Gateway

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. Gateway is also called a protocol converter.

## Repeaters

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.

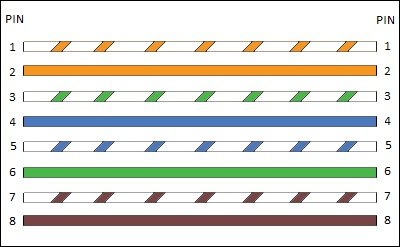


**Network Wiring**

An Ethernet cable 'hardwires' your computer to an internet connection. An Ethernet cable, sometimes referred to as a network cable, is a cord that runs from a router, modem, or network switch to your computer, giving your device access to the local area network (LAN) — in other words, giving it internet access.

The Ethernet cables are categorized as Cat 5, Cat 5e, Cat 6, and UTP cable. Cat 5 cable can support a 10/100 Mbps Ethernet network while Cat 5e and Cat 6 cable to support Ethernet network running at 10/100/1000 Mbps. Ethernet cables can be wired as straight through or crossover.

**Straight through**

Straight-through cable is a type of CAT5 with RJ-45 connectors at each end, and each has the same pin out. It is in accordance with either the T568A or T568B standards. It uses the same color code throughout the LAN for consistency. This type of twisted-pair cable is used in LAN to connect a computer or a network hub such as a router. It is one of the most common types of network cable.

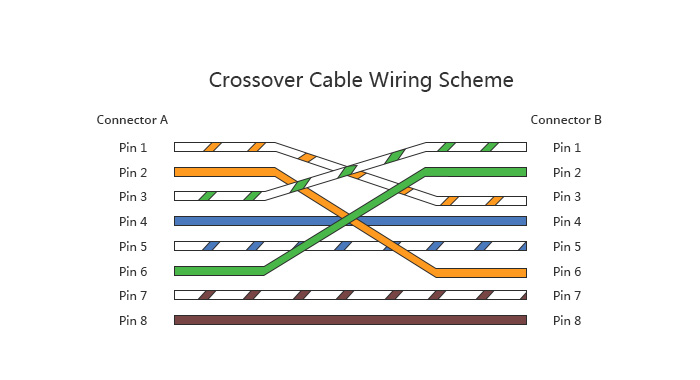
*Straight Through*

**Crossover**

A Crossover cable is a type of CAT 5 where one end isT568A configuration and the other end as T568BConfiguration. In this type of cable connection, Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6.

Crossover cable is used to connect two or more computing devices. The internal wiring of crossover cables reverses the transmission and receive signals. It is widely used to connect two devices of the same type: e.g., two computers or two switches to each other.

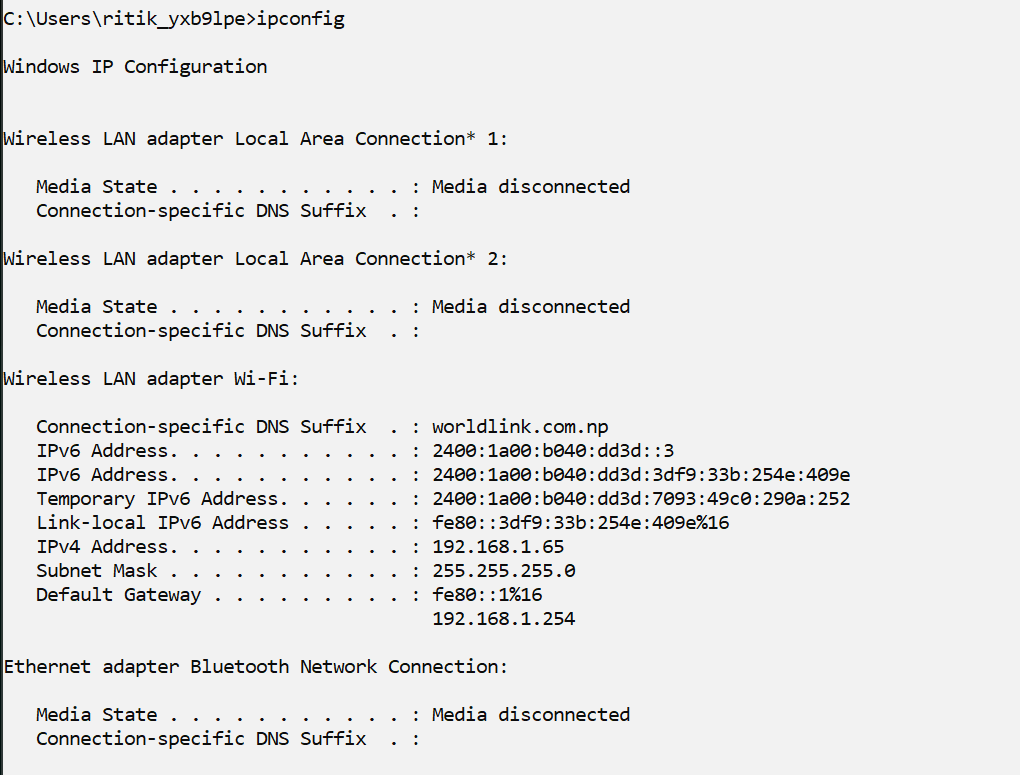
In regard to physical appearance, Crossover Ethernet cables are very much similar to regular Ethernet cables. Still, they are different with regard to the order with which the wires are arranged. This type of Ethernet cable is made to connect to network devices of the same kind over Ethernet directly.

Crossover cables are mostly used to connect two hosts directly.

*Crossover*

# Basic Networking Commands

## Ipconfig

Ipconfig command shows all of the network interfaces, Ethernet, Wi-Fi adapters, Bluetooth adapters etc. It also shows the v6 and v4 IP addresses of the system.

## Ipconfig/all

Retrieve all TCP/IP network information.

Table

Description automatically generated

## Netstat

Netstat is a command-line tool that we can use in Command Prompt to display statistics for all network connections. It allows us to understand open and connected ports to monitor and troubleshoot networking problems for system or applications. When using this tool, we can list

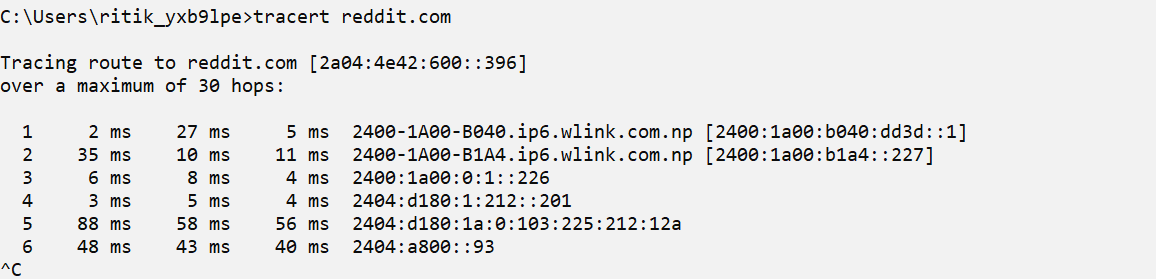
active networks (incoming and outgoing) connections and listening ports. We can view network adapter statistics as well as statistics for protocols (such as IPv4 and IPv6).

Table

Description automatically generated

## Tracert/Traceroute

A traceroute works by sending Internet Control Message Protocol (ICMP) packets, and every router involved in transferring the data gets these packets. The ICMP packets provide information about whether the routers used in the transmission are able to effectively transfer the data. An Internet Protocol (IP) tracer is helpful for figuring out the routing hops data has to go through, as well as response delays as it travels across nodes, which are what send the data toward its destination. Traceroute also enables us to locate where the data was unable to be sent along, known as points of failure. We can also perform a visual traceroute to get a visual representation of each hop.



## Ping

The [ping](https://www.lifewire.com/how-to-ping-computer-or-website-818405) command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. It's usually used as a simple way to verify that a computer can communicate over the network with another computer or network device. The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command provides.

Text

Description automatically generated

## Arp –a

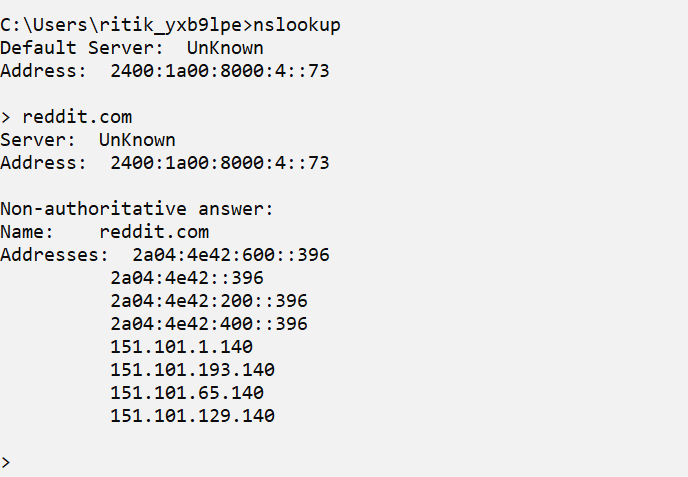
ARP stands for Address Resolution Protocol. This protocol is used by network nodes to match IP addresses to MAC addresses.

Text

Description automatically generated

## Nslookup

nslookup is a network administration command-line tool available in many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records. The name "nslookup" means "name server lookup".



## Pathping

Text

Description automatically generated with medium confidencePathping is a TCP/IP based utility (command-line tool) that provides useful information about Network latency and network loss at intermediate hops between a source address and a Destination address.

## Hostname

The hostname command is used to show or set a computer's host name and domain name. It is one of the most basic of the network administrative utilities.

A picture containing logo

Description automatically generated

## Getmac

Getmac is a Windows command used to display the Media Access Control (MAC) addresses for each network adapter in the computer.

Chart

Description automatically generated with medium confidence

# Understanding IP Addressing and Sub-netting, Static IP Setting

## IPv4 Addressing

An IP address is a 32-bit number that uniquely identifies a host (computer or another device, such as a printer or router) on a TCP/IP network. IP addresses are normally expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.123.132.

For a TCP/IP network to work efficiently as a collection of networks, the routers that pass packets of data between networks do not know the exact location of a host for which a packet of information is destined. Routers only know what network the host is a member of and use information stored in their route table to determine how to get the packet to the destination host’s network. After the packet is delivered to the destination’s network, the packet is delivered to the appropriate host.

For this process to work, an IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address. If we take the example 192.168.123.132 and divide it into these two parts we get 192.168.123.0 as network address and 0.0.0.132 as host address.

## Subnet Mask

The second item, which is required for TCP/IP to work, is the subnet mask. The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network. In TCP/IP, the parts of the IP address that are used as the network and host addresses are not fixed, so the network and host addresses above cannot be determined unless we have more information. This information is supplied in another 32-bit number called a subnet mask. In this IP 192.168.1.1 the subnet mask is 255.255.255.0.

## Network Classes

Internet addresses are allocated by the InterNIC, the organization that administers the Internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

* Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.
* Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.
* Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

**Subnetting**

The goal of subnetting is to create a fast, efficient, and resilient computer network. As networks become larger and more complex, the traffic traveling through them needs more efficient routes. If all network traffic was traveling across the system at the same time using the same route, bottlenecks and congestion would occur resulting in sluggish and inefficient backlogs.

Creating a subnet allows you to limit the number of routers that network traffic has to pass through. An engineer will effectively create smaller mini-routes within a larger network to allow traffic to travel the shortest distance possible.

There could be hundreds of thousands of devices that are connected within a network. This means that the corresponding IP addresses can create a complex route that traffic has to travel. Subnetting limits the IP address usage to within a few devices. This allows an engineer to use subnetting to create sub-networks, sorting data so that it can travel without touching every part of the more complex routers. In order to do this, an engineer needs to match each IP address class to a subnet mask.

A subnet mask echoes an IP address, but it can only be utilized within an internal network. This mask helps to identify which part of the IP address relates to the network and which part relates to the host. This means that specific data is sent on particular routes according to its destination. A subnet mask creates the tool which enables a router to match an IP address with a sub-network.

## Subnetting a Class C network

Let us consider a class C network 192.168.1.0. Now, dividing this network into 4 subnets. Since we need 4 subnets, we have 2^2=4

So the new subnet is 255.255.255.192 Also, the number of hosts is 2^6=64 So subnet range is: 0-63

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Network Address | Subnet Address Range | Broadcast Address |
| 1 | 192.168.1.0 | 192.168.1.1-192.168.1.62 | 192.168.1.63 |
| 2 | 192.168.1.64 | 192.168.1.65-192.168.1.126 | 192.168.1.127 |
| 3 | 192.168.1.128 | 192.168.1.129-192.168.1.190 | 192.168.1.191 |
| 4 | 192.168.1.192 | 192.168.1.62-192.168.1.254 | 192.168.1.255 |

## Subnetting a Class B network

Let consider a class B network 172.16.0.0. Now, dividing this network into 4 subnets. Since we need 4 subnets, we have 2^2=4

So new subnet is 255.255.192.0

Also, the number of host is 2^14=16,384 So, the subnet range is 0-16,383

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Network Address | Subnet Range | Broadcast Address |
| 1 | 172.16.0.0 | 172.16.0.1-172.16.63.254 | 172.16.63.255 |
| 2 | 172.16.64.0 | 172.16.64.1-172.16.127.254 | 172.16.127.255 |
| 3 | 172.16.128.0 | 172.16.128.1-172.16.191.254 | 172.16.191.255 |
| 4 | 172.16.192.0 | 172.16.192.1-172.16.255.254 | 172.16.255.255 |

## Subnetting class A network

Let consider a class B network 10.0.0.0. Now, dividing this network into 4 subnets. Since we need 4 subnets, we have 2^2=4

So new subnet is 255.192.0.0

Also, the number of host is 2^22=4194302 So, the subnet range is 0-4194301

|  |  |  |  |
| --- | --- | --- | --- |
| SN | Network Address | Subnet Range | Broadcast Address |
| 1 | 10.0.0.0 | 10.0.0.1-10.63.255.254 | 10.63.255.255 |
| 2. | 10.64.0.0 | 10.64.0.1-10.127.255.254 | 10.127.255.255 |
| 3. | 10.128.0.0 | 10.128.0.1-10.191.255.254 | 10.191.255.255 |
| 4. | 10.192.0.0 | 10.192.0.1-10.254.255.254 | 10.255.255.255 |

# Introduction to Packet Tracer, creating of a LAN and connectivity test in the LAN

## Introduction to Packet Tracer

**Cisco Packet Tracer** as the name suggests, is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks. The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

Using this tool is widely encouraged as it is part of the curriculum like CCNA, CCENT where Faculties use Packet Trace to demonstrate technical concepts and networking systems. Students complete assignments using this tool, working on their own or in teams.

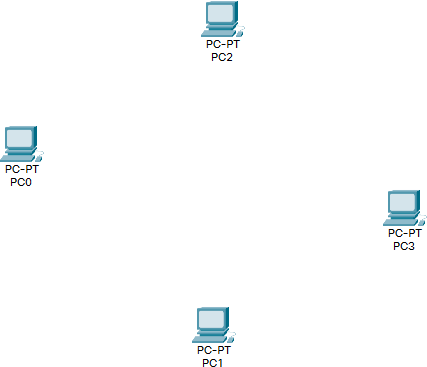
Engineers prefer to test any protocols on Cisco Packet Tracer before implementing them. Also, Engineers who would like to deploy any change in the production network prefer to use Cisco Packet Tracer to first test the required changes and proceed to deploy if and only if everything is working as expected.

This makes the job easier for Engineers allowing them to add or remove simulated network devices, with a Command line interface and a drag and drop user interface.

## Creating a Local Area Network

To create a LAN in Packet tracer, we follow the steps below:

1. ADD computers to from end devices tab.



1. Add a Central Networking Device form networking devices tab.

Diagram

Description automatically generated

1. Connect the Devices to the Switch using appropriate wires.

A picture containing text, device, traffic light, gauge

Description automatically generated

1. Use IP configuration on each computer to manually set IP address.

Graphical user interface, text, application, email

Description automatically generatedA picture containing text, device, screenshot, gauge

Description automatically generated

1. The Local Area Network is now created and ready to test and test can be done by simply sending packets from one pc to another pc. If the packets can be transferred successfully then LAN is successfully implemented.

## Connectivity test in LAN

To test the connectivity in Local Network, we can use following two methods.

1. **Ping**

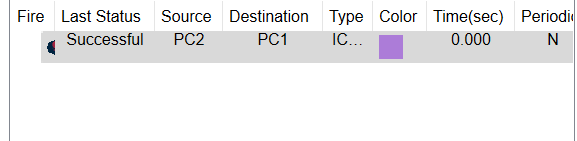
Ping uses ICMP protocol to check if a device is running or not. To ping a device, we type in ‘ping [destination ip]’ in terminal or command prompt.

A picture containing text

Description automatically generated

1. **PDU’s**

DU stands for "Protocol Data Unit." A PDU is a specific block of information transferred over a network. To use PDU, click the PDU icon, then click the sender , then click the receiver. The Transfer status will be shown below.



Diagram

Description automatically generated

# 5. Basic Router Configuration and its Routing Implementation

## Basic Router Configuration

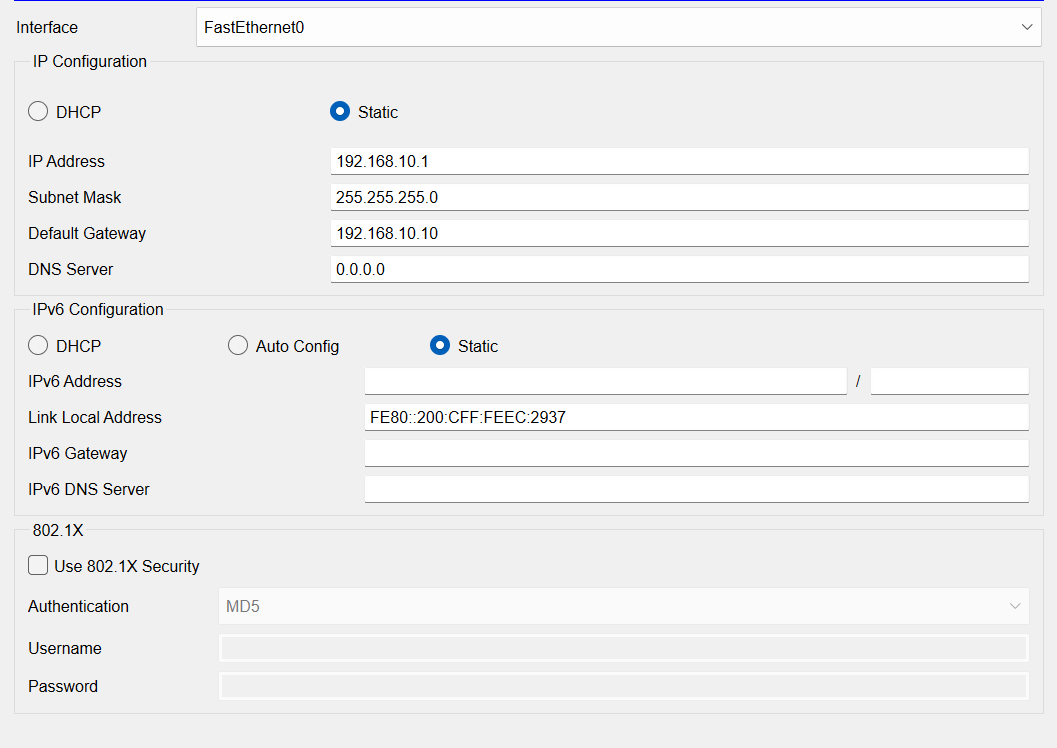
Routers are generally used to connect two different networks. To configure Routers let us consider two networks. Network A and Network B. now to connect the two, we use routers as follows.

1. Create two networks with different IP’s

A picture containing chart

Description automatically generated

1. Configure IP’s for both networks, also add router’s address to gateway address.



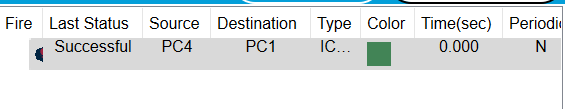
1. Diagram

   Description automatically generated with low confidenceConnect the two network’s switches to router’s ports, assign network gateway address to each of the port

Graphical user interface, text, application, email

Description automatically generated

1. The router is now configured. We can test it by sending packets from PC4 of one network to PC1 to another network.



## Routing

Routers refer to internal routing tables to make decisions about how to route packets along network paths. A routing table records the paths that packets should take to reach every destination that the router is responsible for. Routing tables can either be static or dynamic.

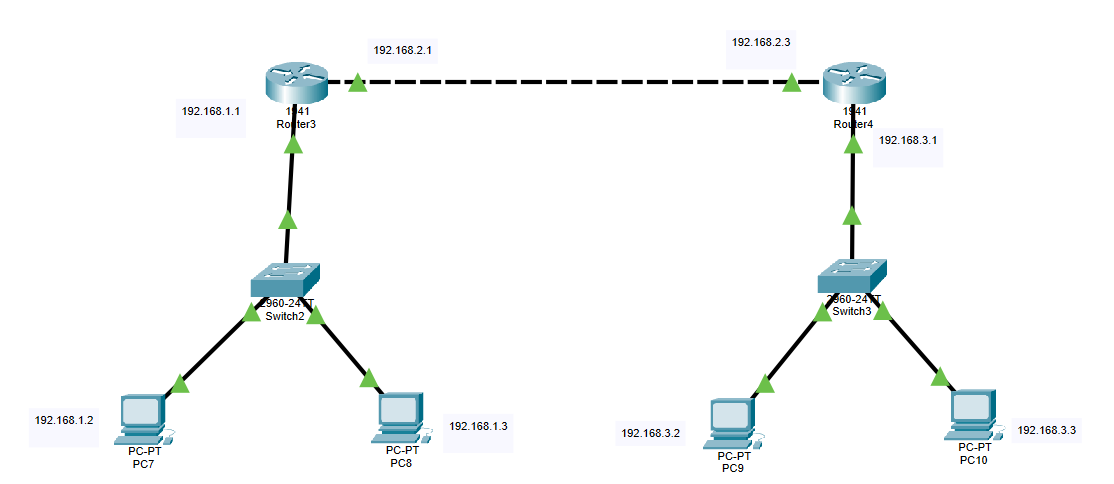
## Static Routing

Static routing tables do not change. A network administrator manually sets up static routing tables. This essentially sets in stone the routes data packets take across the network, unless the administrator manually updates the tables.

## Implementation of Static routing

To implement static routing, we follow the steps below

1. Firstly, create two networks with each of their own routers.

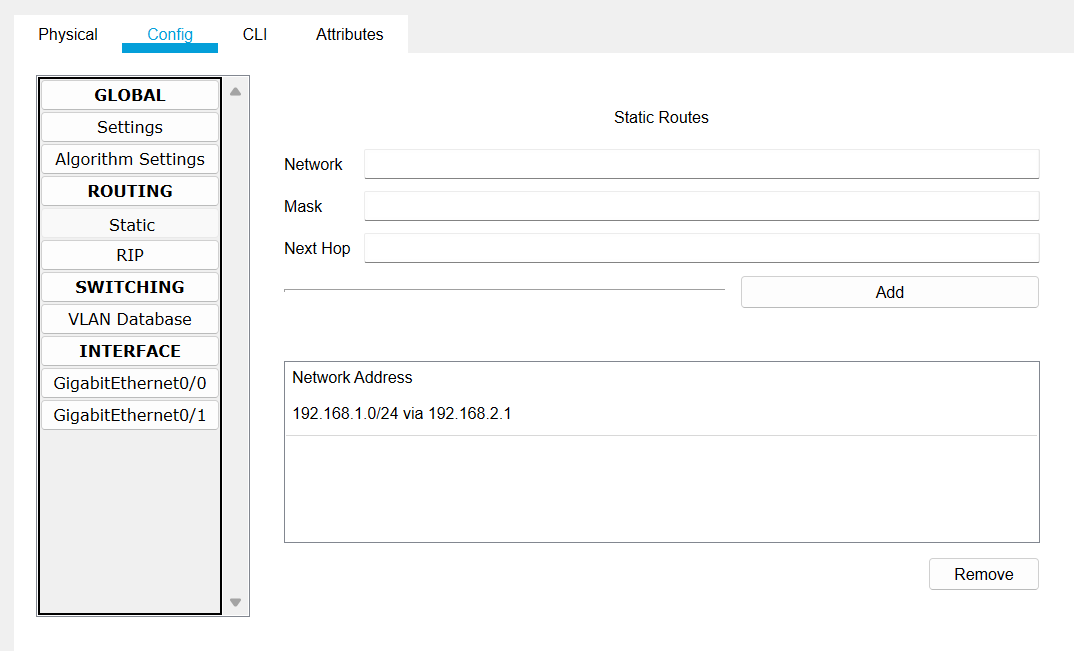


1. Assign IP’s to all nodes and Routers.

Graphical user interface, text, application, email

Description automatically generated

1. Configure the static routing table on both routers



1. Static routing is now complete and can be checked by a PDU.

Graphical user interface, application

Description automatically generatedDiagram

Description automatically generated with medium confidence

# 6. Implementation of Dynamic/interior/exterior routing (RIP, OSPF, BGP)

## Dynamic Routing

Dynamic routing tables update automatically. Dynamic routers use various routing protocols to determine the shortest and fastest paths. They also make this determination based on how long it takes packets to reach their destination — similar to the way Google Maps, Waze, and other GPS services determine the best driving routes based on past driving performance and current driving conditions.

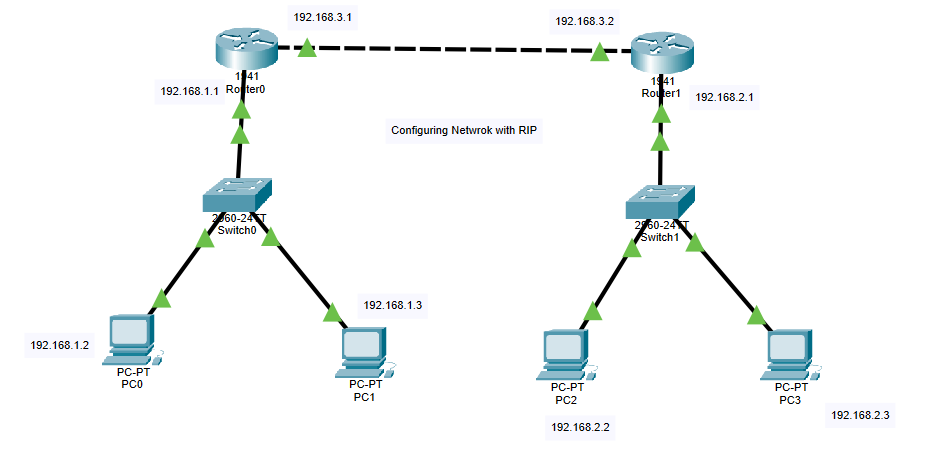
Dynamic routing requires more computing power, which is why smaller networks may rely on static routing. But for medium-sized and large networks, dynamic routing is much more efficient.

## Implementation of Dynamic Routing RIP

The Routing Information Protocol (RIP) uses "hop count" to find the shortest path from one network to another, where "hop count" means number of routers a packet must pass through on the way. (When a packet goes from one network to another, this is known as a "hop.")

To implement RIP, we follow the steps below.

1. Create two networks with routers as usual as we did with static routing.



1. Assign IP to nodes and routers. Connect with another router in another network with different IP address.

Graphical user interface, text, application, email

Description automatically generated

1. Go to RIP configuration and add all networks the router is connected to

Graphical user interface, application

Description automatically generated

1. The RIP configuration is now complete and can be checked by a PDU

Graphical user interface, application, Word

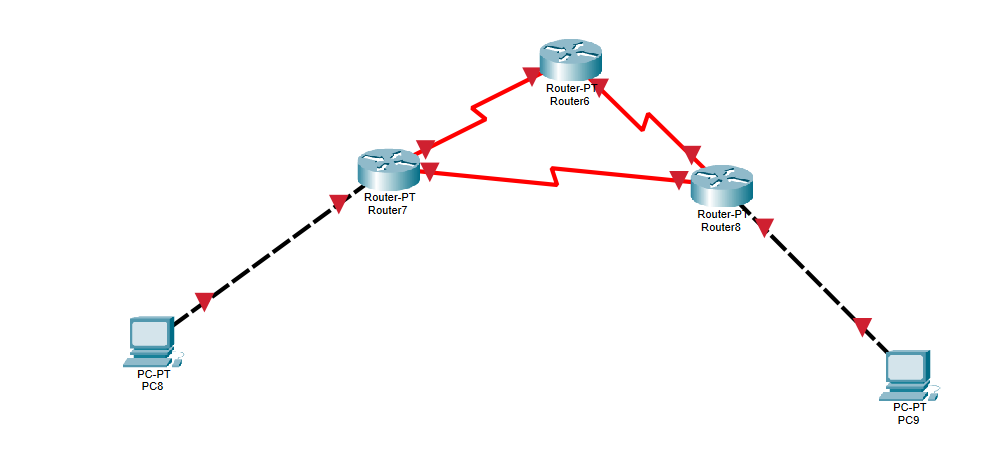
Description automatically generated

## OSPF

The Open Shortest Path First (OSPF) protocol is commonly used by network routers to dynamically identify the fastest and shortest available routes for sending packets to their destination.

To implement OSPF, we follow the steps below

1. Create a Network with 3 routers and connect them.



1. Assign IP address to all systems and routers

Chart

Description automatically generated1

1. Configure OSPF protocol for each router Go to CLI mode for each router

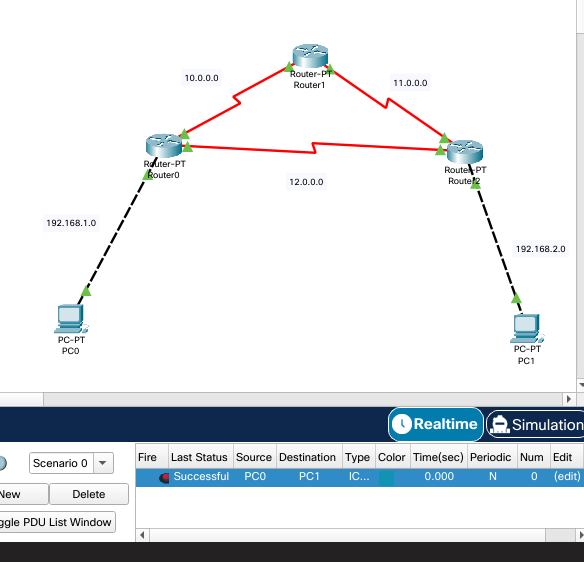
Go to config mode

Type in *router ospf [process id]*

Then add all networks connected to the router typing *network [network addd] [subnet mask comp] area [area no]*

Save the config

1. OSPF configuration is now complete. We can test this using a simple PDU



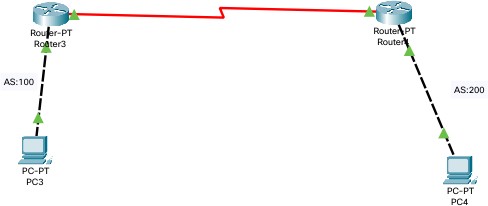
## BGP

The full form of BGP is the Border Gateway Protocol. This type of routing protocol sends updated router table data when changes are made. Therefore, there is no auto-discovery of topology changes, which means that the user needs to configure BGP manually.

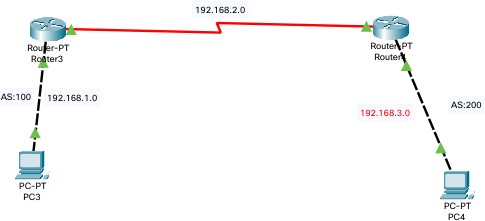
## Implementation of BGP protocol

To implement BGP protocol, we follow following steps.

1. Create a network with two routers and end devices. Name the networks as autonomous system and an integer value



1. Assign IP addresses to routers and end devices.

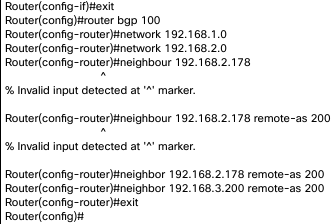


1. Now configure routers with BGP protocol Open router’s CLI and go to config mode. Type in router *bgp [AS number]*

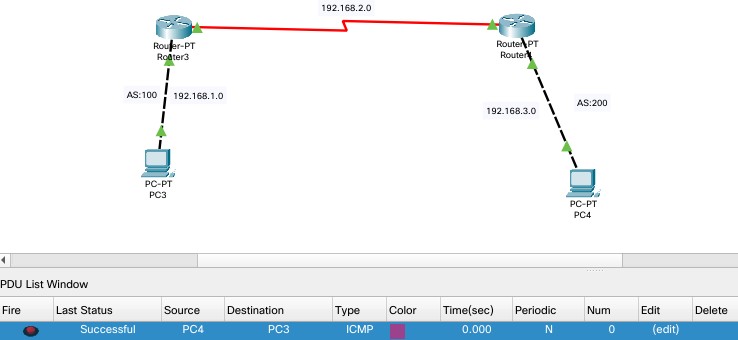
Add networks routers are connected to using *network [ip address]*

Add routers and devices not in network by *neighbor [ip address] remote-as [AS number]*

Save the configuration.



1. The BGP configuration is now complete and can be tested using a PDU



# Packet capture and header analysis by wire-shark (TCP, UDP, IP)

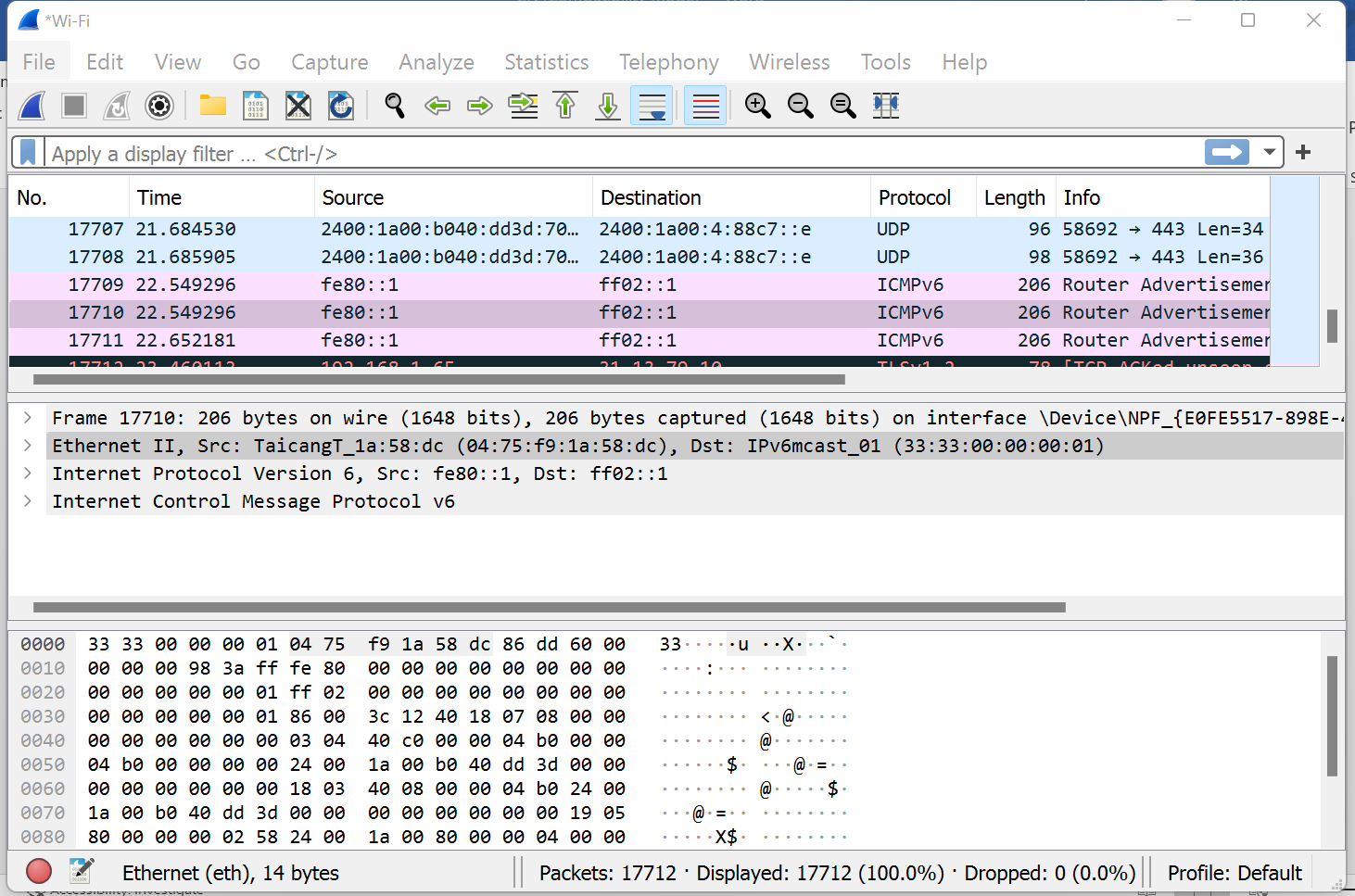
## Wireshark

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network.

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things: Packet Capture, Filtering and Visualization. Wireshark has many uses, including troubleshooting networks that have performance issues. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

## Packet Capture

Wireshark listens to a network connection in real time and then grabs entire streams of traffic. To capture Packets, open Wireshark, and select the interface to capture packets on.



## Packet Filtering

Table

Description automatically generatedWireshark can filter traffic based on the protocol. To filter packets based on Protocol of packet like TCP, UDP, DNS, etc. we apply display filter on the top bar.

## Packet Analysis

To analyze a packet, click on the packet and the information will be displayed below. The information is encrypted while transferring through the network. Let us consider a TCP packet.

Under the Transmission Control Protocol, we can see all the information on the TCP header.

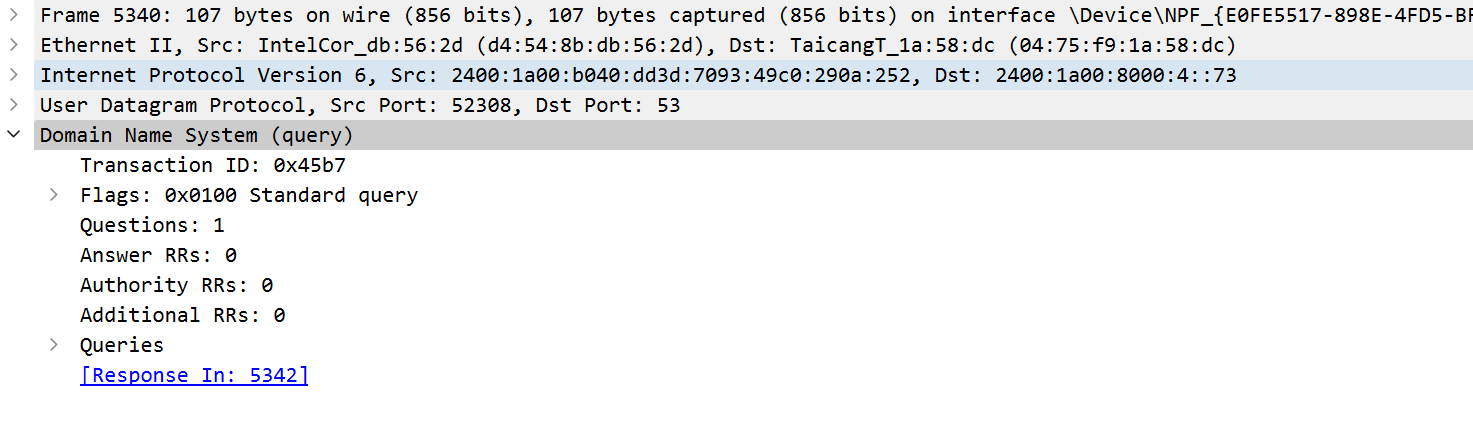
Graphical user interface, text, application

Description automatically generated

Also, we can check the IPv4 header from the internet protocol tab

Graphical user interface, text, application, email

Description automatically generated

Similarly, let us consider a DNS request packet. Here we can see the DNS request and the reply with the IP of the requested site.

# Basic concept of DNS, Web, FTP, DHCP

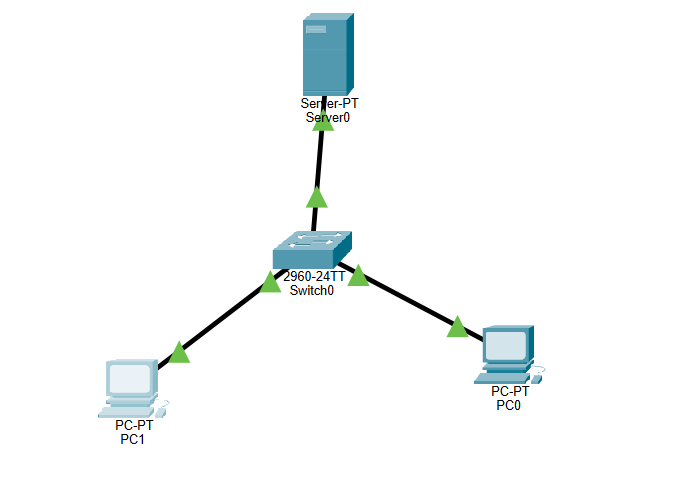
## Web Server

A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web. The main job of a web server is to display website content through storing, processing and delivering webpages to users. Besides HTTP, web servers also support SMTP (Simple Mail Transfer Protocol) and FTP (File Transfer Protocol), used for email, file transfer and storage.

## Configuring a web server

To configure a web server, we follow the steps below

* + 1. Create a network with a switch, a server and end devices.



* + 1. Configure IP’s of switch server and end devices.

A picture containing diagram

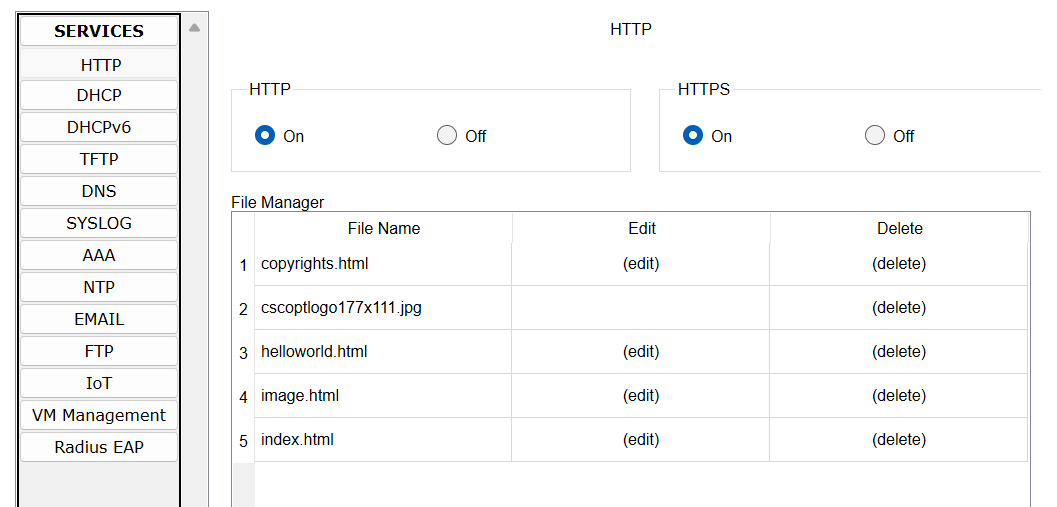
Description automatically generated

Setting up server IP address

Graphical user interface, text, application, email

Description automatically generated

* + 1. Open server. Go to services tab. Click https and turn http and https on.



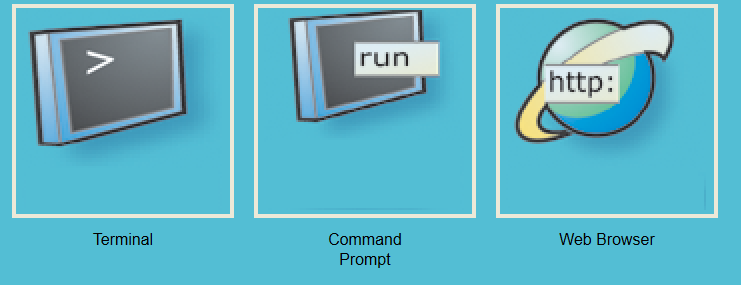
* + 1. Edit the index.html file and save.

I have edited the title of this file and inserted my name in header. And also change the text of the image.

Graphical user interface, text, application

Description automatically generated

* + 1. Open up browser from any one end devices and type in IP of the webserver and the website will openup.



Graphical user interface, text, application, email

Description automatically generated

## DNS server

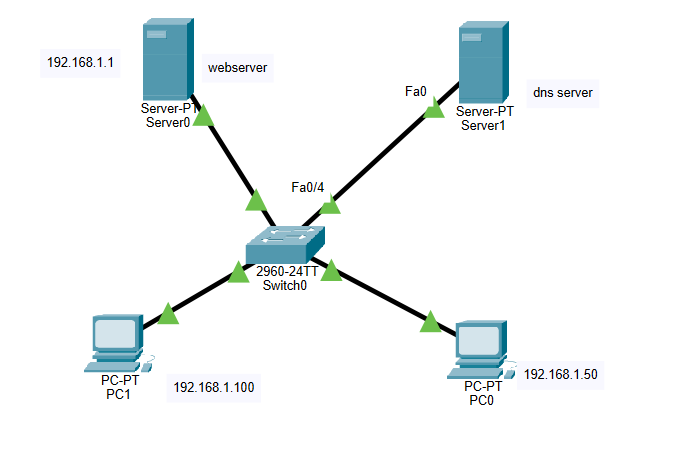
A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases serves to resolve, or translate, those names to IP addresses as requested. DNS servers run special software and communicate with each other using special protocols. It's easier to remember a domain or hostname like lifewire.com than it is to remember the site's IP address numbers 151.101.2.114. So when you access a website, like Facebook, all you have to type is the URL https://[www.facebook.com.](http://www.facebook.com/)

However, computers and network devices don't work well with domain names when trying to locate each other on the internet. It's far more efficient and precise to use an IP address, which is the numerical representation of what server in the network (internet) the website resides on.

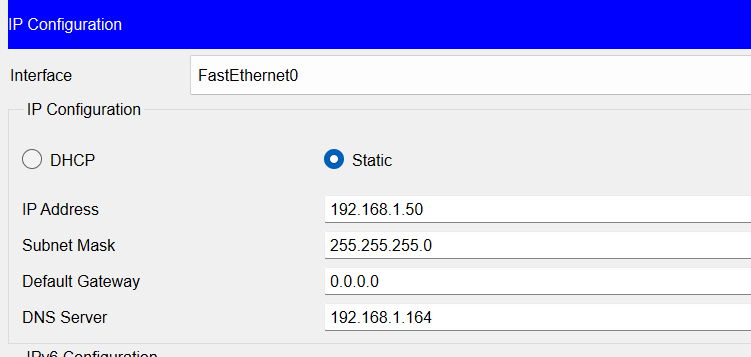
## Configuring a DNS server

To configure a DNS server. We follow the steps below.

1. Create a network with end devices, switch, a webserver and a dns server



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



1. Graphical user interface, text, application

   Description automatically generatedOpen DNS server, go to services and turn on DNS. add website address and IP of the webserver and click add.
2. Graphical user interface, text, application, email

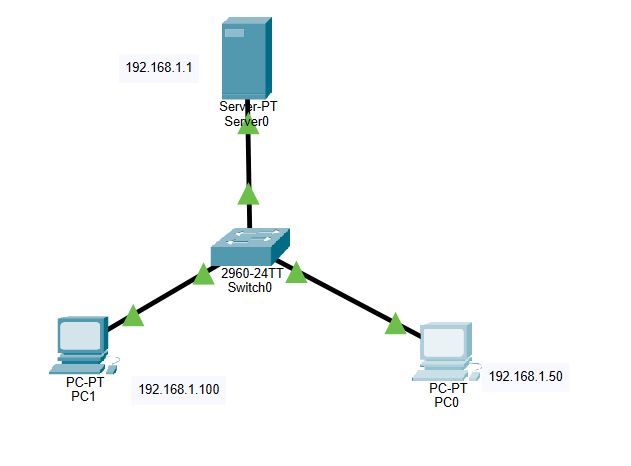
   Description automatically generatedOpen web browser on any end device and type in website address and the website should appear.

## FTP

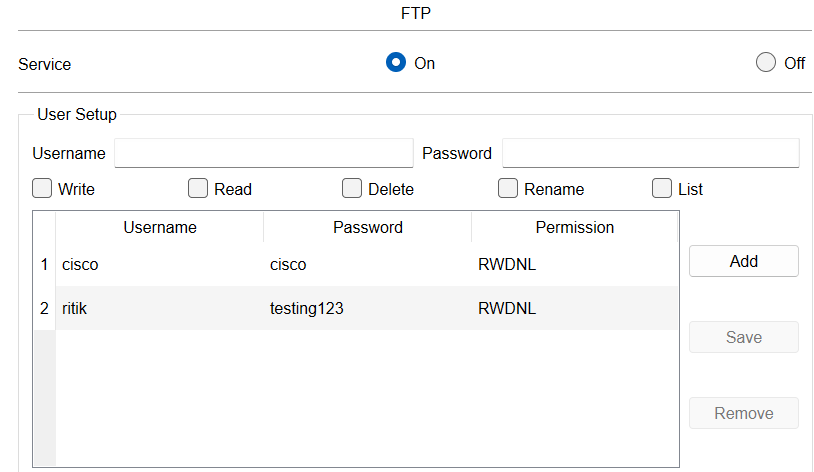
The File Transfer Protocol (FTP) is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).

## Implementation of FTP server

To implement FTP server, we follow the steps below

1. Create a network with a server, a switch and end devices and assign IP addresses to end devices and the server.
2. Open server and enable FTP service.

Create a username and password and assign all of the privileges and click add.



1. Text

   Description automatically generatedOpen end device and go to command prompt and type *ftp [server ip]*.use the previously created username and password and log in.
2. We can now perform file operations on the ftp server using commands like delete, rename etc.

A picture containing text

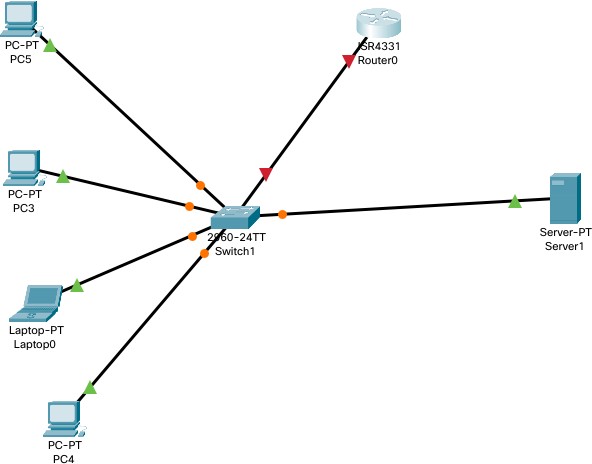
Description automatically generated

## DHCP

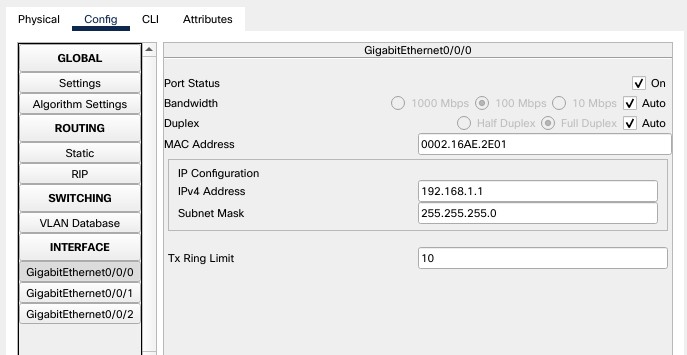
Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

To configure a DHCP server, we follow the steps below,

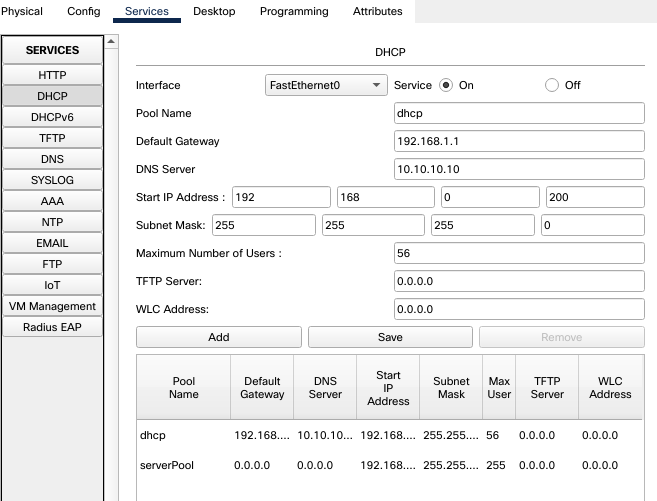
1. Create a network with a server, switch, router and end devices.



1. Open server settings and set an ip for the DHCP server and Router.



1. Open server and go to services then to DHCP. Turn it on and set the gateway address, starting address and DNS server info and click on add



1. DHCP configuration is now complete, now the end devices will be assigned an IP address through the DHCP server.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generatedRequesting IP address

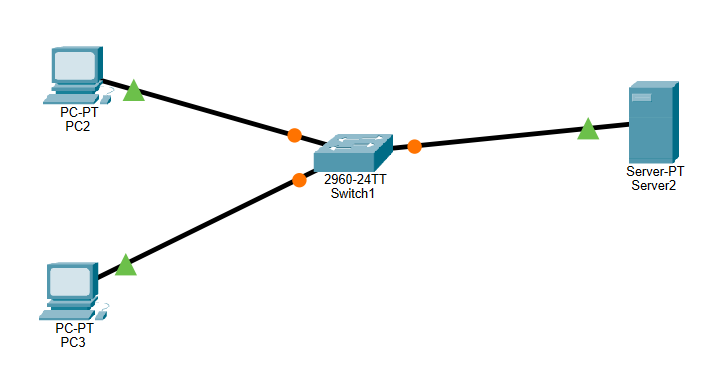
After requesting IP

## Email Server

A mail server (sometimes also referred to an e-mail server) is a server that handles and delivers e- mail over a network, usually over the Internet. A mail server can receive e-mails from client computers and deliver them to other mail servers. A mail server can also deliver e-mails to client computers.

To configure an email server, we follow the steps below.

1. Create a network with end devices, server and switch.

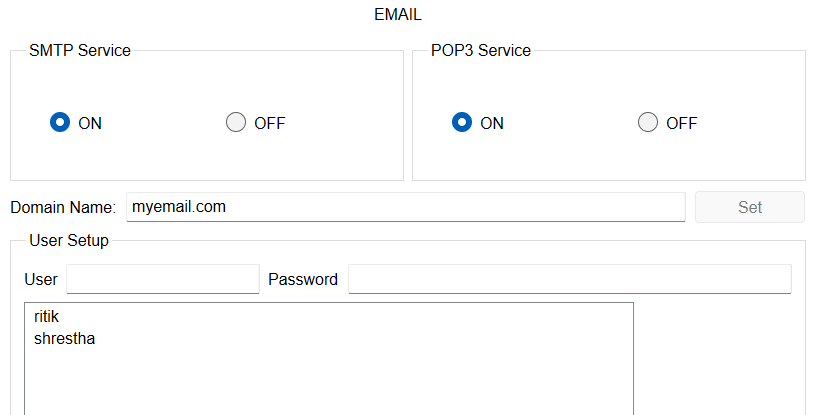


1. Assign IP to routers, end devices and server

Diagram

Description automatically generated

1. Open server and go to services. Then go to email and turn both email services on Create a domain name and create username and password.



1. Open the end devices, and open email tab. Then fill in username, passwords and mail server ip and press save.

Graphical user interface, application

Description automatically generated

1. Now open any end device and go to email. Click compose and fill in details of receiver and click send

Graphical user interface, text

Description automatically generated with medium confidence

1. To receive the email, go to the receiver, click on email and click receive.

Graphical user interface, text, application, email

Description automatically generated