# Understanding of Network Devices and Wiring in details

**Network Devices**

## Network devices are physical hardware components that link computers, printers, fax machines, and other electronic devices to a network. Networking gear, often known as network devices, is the actual hardware needed for communication and interaction on a computer network. These devices quickly, securely, and accurately transfer data over the same or separate networks. Network equipment can be either intra- or inter-networked. Several networking devices include:

## Hub

The central node in a network with a star topology is a hub, which is a repeater with several ports. It's frequently called a multi-port repeater (or as a concentrator in Ethernet).

A hub joins several wires that come from several branches, like the connector in a star topology that joins various stations. Data packets are delivered to all connected devices since hubs are unable to filter data. In other words, all hosts connected by Hub continue to share a single collision domain. Additionally, they lack the intelligence to choose the best route for data packets, which results in waste and inefficiency.

**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.

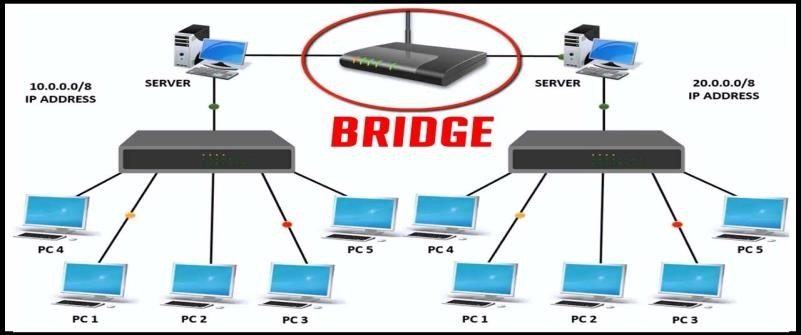


## Switch

* At Layer 2 of the OSI layer, switches function as intelligent devices. It is a multiport bridge with a buffer and a design that can increase its efficiency (a large number of ports indicate less traffic) and performance. Data link layer equipment includes switches. The switch can perform error checking before forwarding data, which makes it incredibly efficient because it only forwards good packets to the right port and does not transmit packets that include mistakes. In other words, while the broadcast domain stays the same, the switch separates the collision domain of the hosts.



## Bridge

* At the data connection layer (Layer 2) of the OSI architecture, a network bridge connects various network segments. To join two networks at the data connection layer, in other words, is how it is typically utilized. Useful when networks have the same network layer but separate data link layers. An example would be a bridge connecting Ethernet and the token bus. A bridge is a repeater with the additional capability of content filtering via source and destination MAC address reading. Additionally, it is utilized to connect two LANs that use the same protocol. It is a 2-port device because it has a single input and output port.

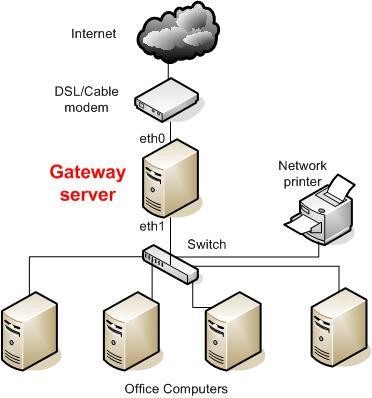
## Routers

Similar to a switch, a router directs data packets depending on their IP addresses. Mainly a Network Layer device, the router. LAN and WAN connections are typically made via routers, which also decide how to route data packets based on a dynamically updated routing table. The broadcast domains of hosts connected by a router are divided.



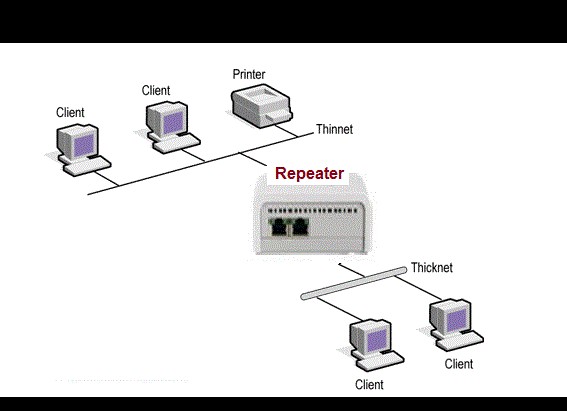
## Gateway

* A gateway, as its name suggests, is a passageway that connects two networks—which may use various networking models—together. They essentially serve as the messengers who interpret and transport data from one system to another. Protocol converters are another name for gateways, which can work at any network layer. In general, gateways are more complicated than switches or routers. Another name for a gateway is a protocol converter.



## Repeaters

Operating at the physical layer is a repeater. Its task is to increase the length to which the signal can be broadcast over the same network by regenerating the signal over the same network before the signal becomes too weak or garbled. The fact that repeaters do not enhance the signal is a crucial aspect to keep in mind. When the signal deteriorates, they incrementally replicate it to restore it to its original strength. It is a two port gadget.



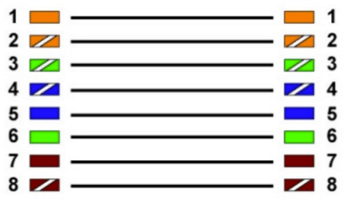
**Network Wiring**

A network cable called an Ethernet cable is used for wired, high-speed communications between two devices. This network cable is constructed of twisted pair conductors in a four-pair cable. The RJ45 connector, which is utilized for data transfer at both ends of the cable, is employed.

Cat 5, Cat 5e, Cat 6, and UTP cable are the different types of Ethernet cables. A 10/100 Mbps Ethernet network can be supported by Cat 5 cable, while 10/100/1000 Mbps Ethernet networks can be supported by Cat 5e and Cat 6 cables. Ethernet wires can either be crossed over or run straight through.

**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*

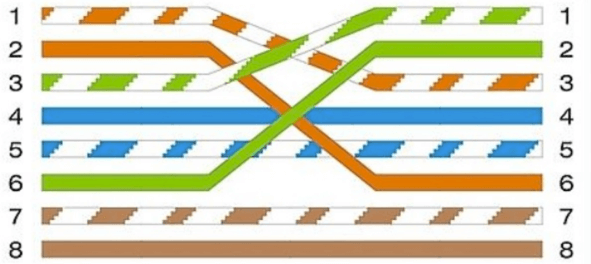
**Crossover**

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.

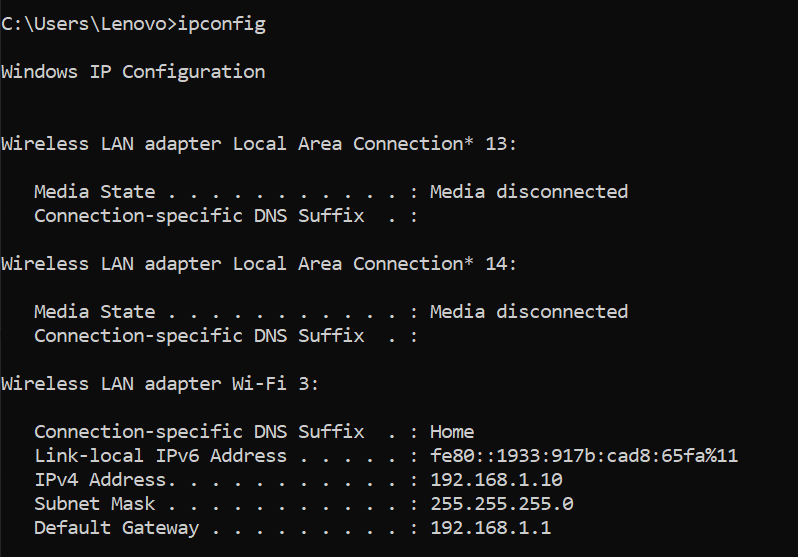


*Crossover*

# Basic Networking Commands

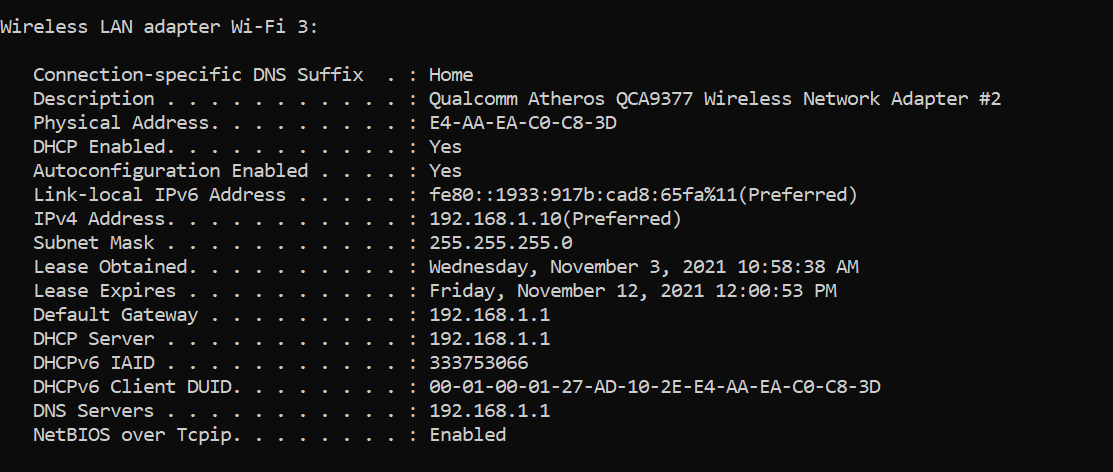
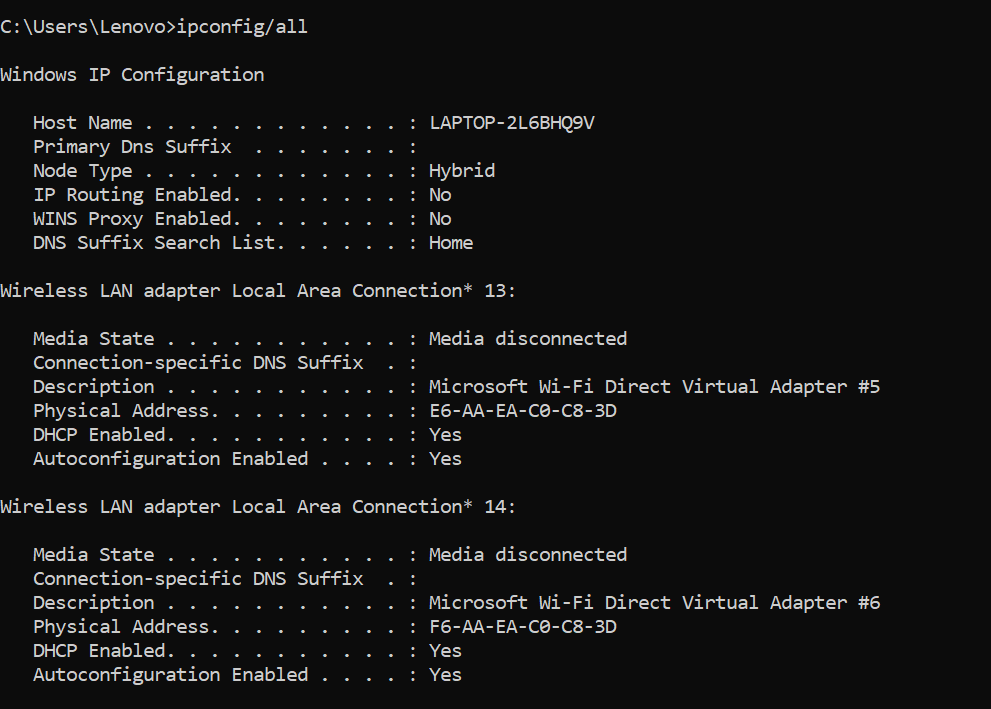
## Ipconfig

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

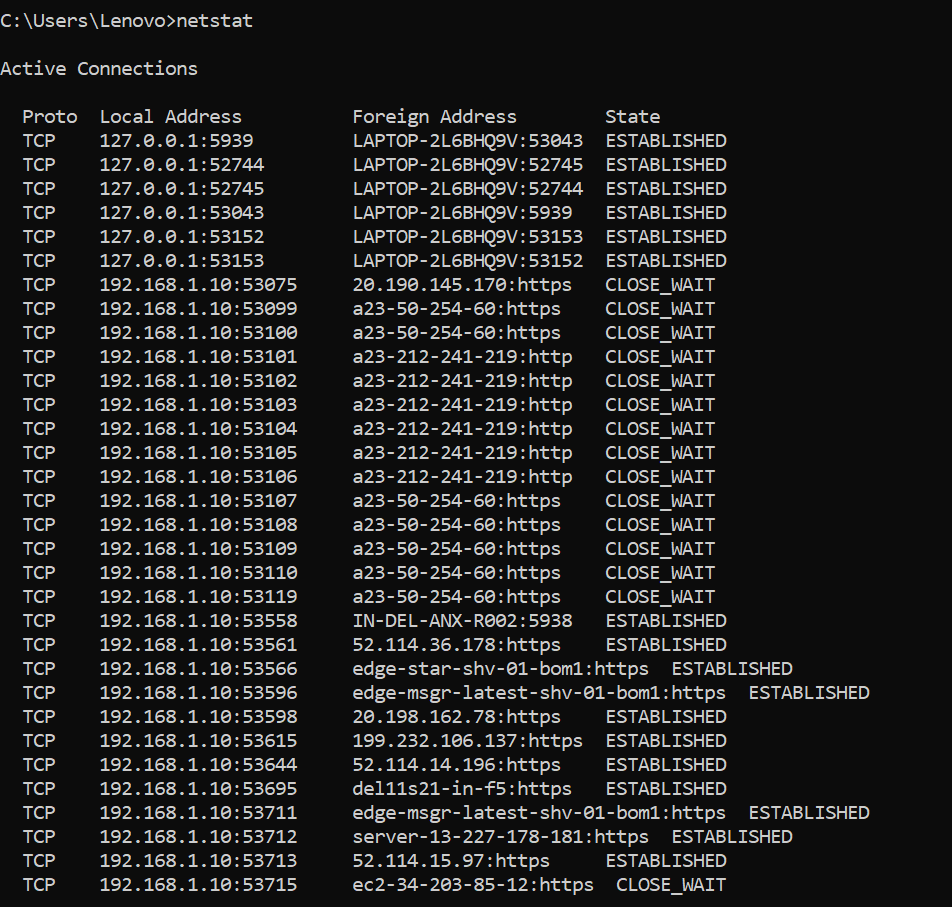
Retrieve all TCP/IP network information.



## Netstat

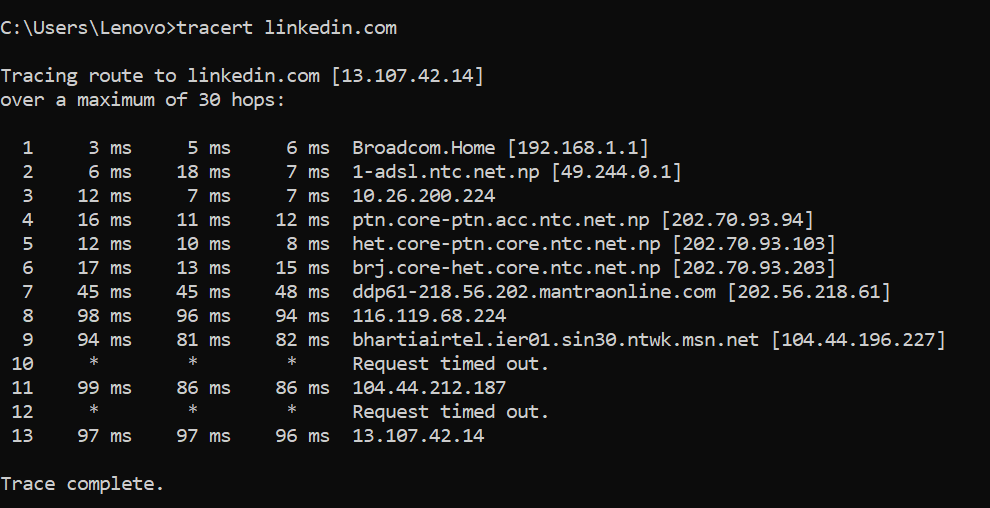
Netstat is a command-line tool that we can use in Command Prompt to display statistics for all network connections. It allows us to understand open and connected ports to monitor and troubleshoot networking problems for system or applications. When using this tool, we can list

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).



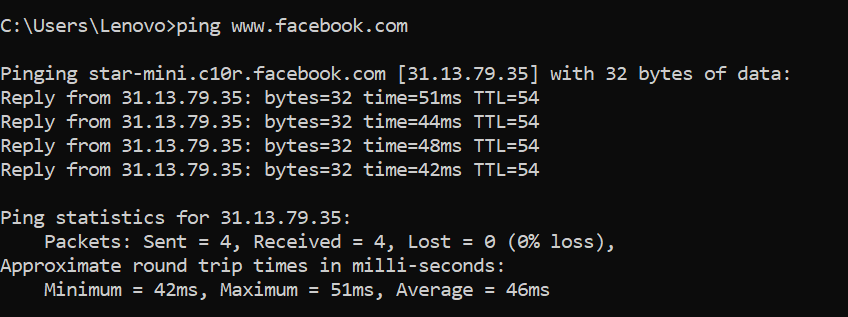
## Tracert/Traceroute

Every router involved in the data transport receives the Internet Control Message Protocol (ICMP) packets that are sent by a traceroute. The ICMP packets reveal whether or not the routers involved in the transmission can successfully transfer the data. An IP tracer is useful for determining the routing hops and response times that data must experience as it moves across nodes, which are what send the data to its destination. We can identify the points of failure, or places where the data was unable to be transmitted, using Traceroute. In order to see a visual representation of each hop, we may also run a visual traceroute.



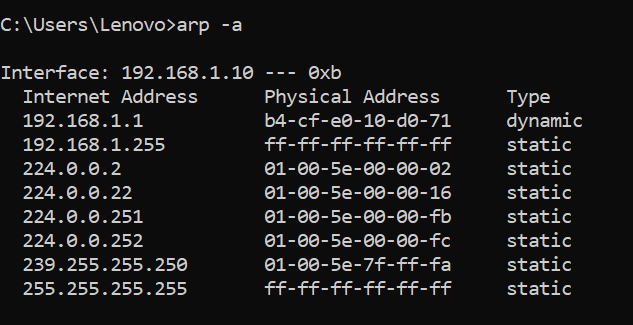
## Ping

The ping command can be used in Command Prompt to check whether the source computer can connect to a particular destination machine. It's typically used as a quick and easy way to check whether a computer can communicate with another computer or network device via a network. The Internet Control Message Protocol (ICMP) Echo Request messages are sent to the target computer as part of the ping command, which then waits for a response. The ping command gives two main pieces of information: how many of those responses are received and how long it takes for them to return.



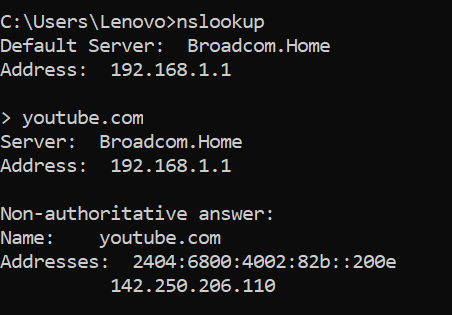
## Arp –a

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



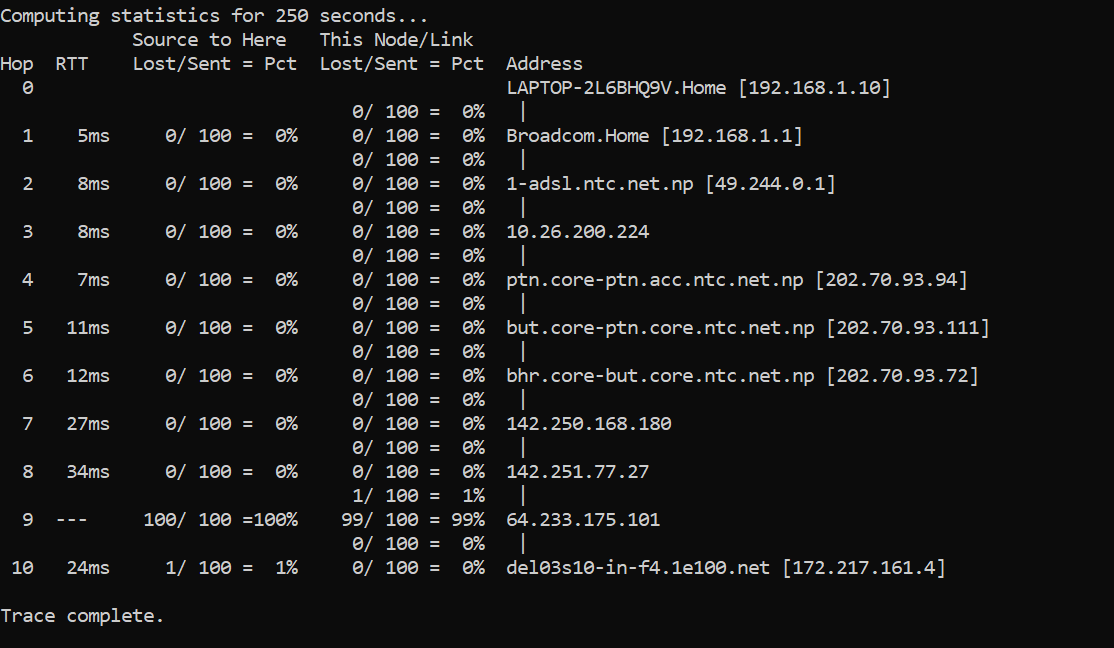
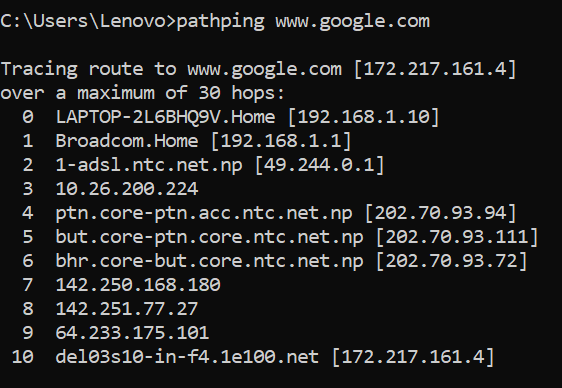
## Nslookup

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".



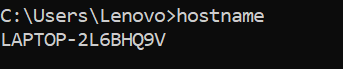
## Pathping

Pathping 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.



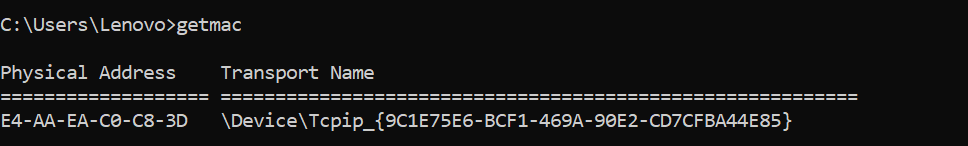
## Hostname

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.



## Getmac

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



# Overview of IP Addressing and Sub-netting, Static IP Setting

## IPv4 Addressing

On a TCP/IP network, a host (a computer or other device, such as a printer or router) is uniquely identified by its 32-bit IP address. Four integers separated by periods make up an IP address, which is typically written as 192.168.123.132.

The routers that transfer data packets between networks must not be aware of the precise location of a host for whom a packet of information is meant in order for a TCP/IP network to function effectively as a collection of networks. Only the network the host is a part of is known to routers, and they use the data in their route table to work out how to get the packet to the destination host's network.

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 subnet mask is the second component needed for TCP/IP to function. The TCP/IP protocol uses the subnet mask to identify whether a host is on a local subnet or a faraway network. The network and host addresses listed above cannot be identified without additional information because in TCP/IP, the components of the IP address that are used as the network and host addresses are not fixed. A subnet mask, another 32-bit value, is used to provide this data. The subnet mask for this IP address is 255.255.255.0.

## Network Classes

The InterNIC, the company in charge of running the Internet, assigns Internet addresses. Classes have been created for these IP addresses. Classes A, B, and C are the most prevalent among these. Although classes D and E exist, end users rarely use them. The default subnet mask differs for every address class. An IP address's first octet can be used to determine its class. The Class A, B, and C Internet address ranges are listed below, 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 purpose of subnetting is to build a computer network that is quick, effective, and dependable. More effective pathways are required to carry the traffic through networks as they grow bigger and more complicated. All network traffic would experience bottlenecks and congestion if it all took the same path at the same time, leading to slow and ineffective backlogs.

You can reduce the number of routers that network traffic must transit through by setting up a subnet. To enable traffic to go the shortest distance possible, an engineer will effectively designate smaller mini-routes within a larger network.

A network may have hundreds of thousands of interconnected devices. This implies that a convoluted path for traffic can be created by the associated IP addresses. Subnetting restricts the use of IP addresses to a small number of devices. In order to organize the data so that it can transit without touching every component of the more complicated routers, an engineer can utilize subnetting to establish sub-networks. An engineer must match each IP address class to a subnet mask in order to accomplish this.

Although a subnet mask is similar to an IP address, it can only be used on internal networks. This mask makes it easier to distinguish between the IP address's host and network components.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

As the name suggests, Cisco produced the tool known as Cisco Packet Tracer. With the help of this program, you may simulate both simple and complicated networks. Cisco Packet Tracer's major goal is to assist students in gaining practical networking experience and developing skills particular to Cisco technology. This program cannot replace hardware routers or switches because the protocols are implemented solely in software. It's interesting to note that this tool includes many more networking devices in addition to Cisco models.

The use of this program is strongly advised because it is covered in courses like CCNA and CCENT where professors utilize Packet Trace to illustrate networking systems and technical ideas. Using this application, students finish their projects while working individually or in groups.

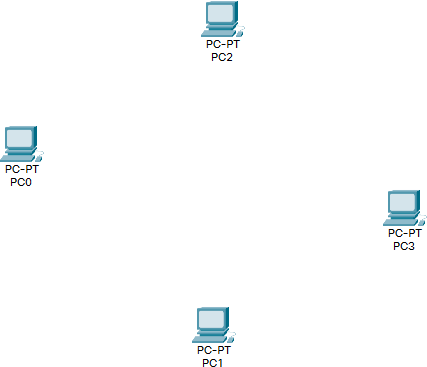
Before installing any protocols, engineers want to test them on Cisco Packet Tracer. Additionally, engineers prefer to use Cisco Packet Tracer before deploying any modifications to the production network to ensure that everything is operating as intended. Only then do they move forward with the deployment.

Engineers can now add or remove virtual network devices using a drag and drop user interface or a command line interface, simplifying their work.

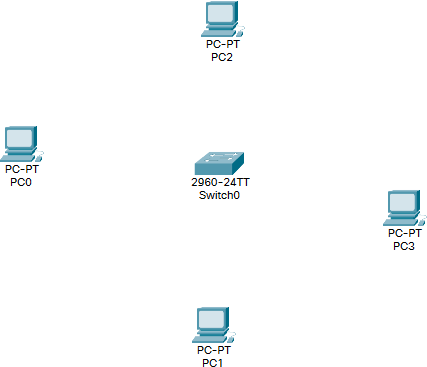
## Creating a Local Area Network

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

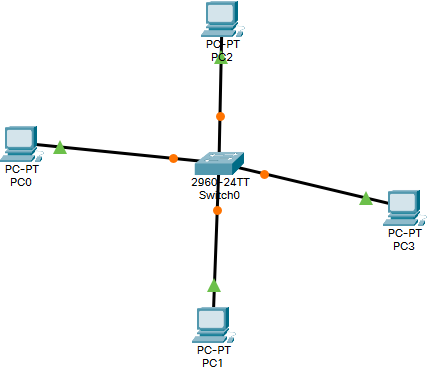
1. ADD computers to from end devices tab.

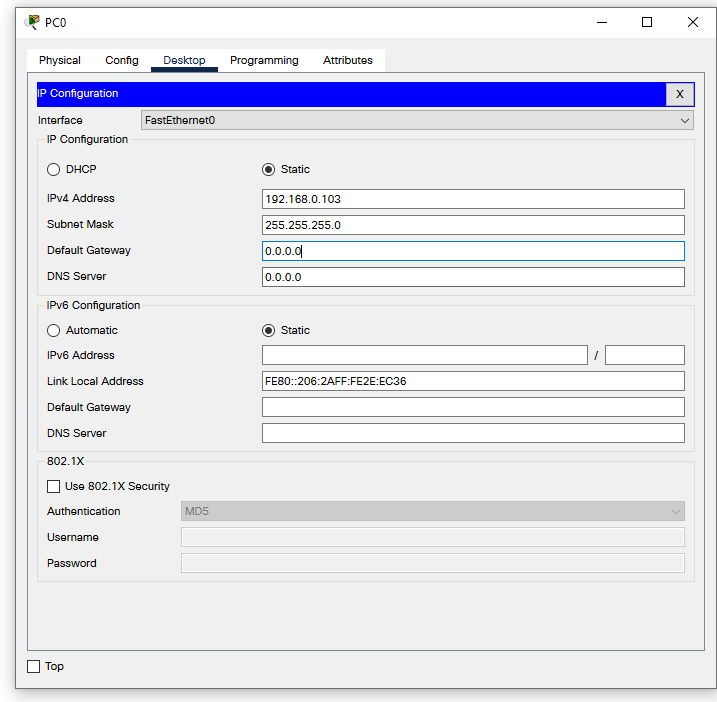


1. Add a Central Networking Device form networking devices tab.



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



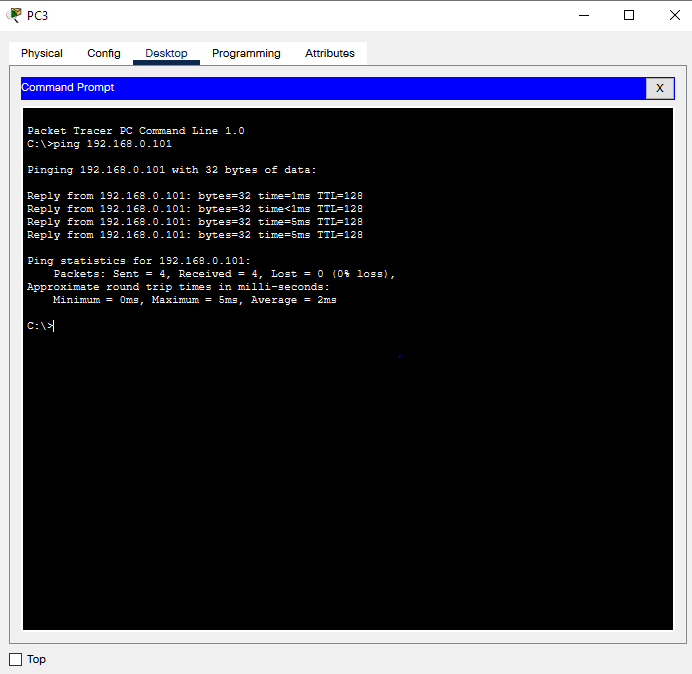
1. Use IP configuration on each computer to manually set IP address.
2. The Local Area Network is now created and ready to test.

## Connectivity test in LAN

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

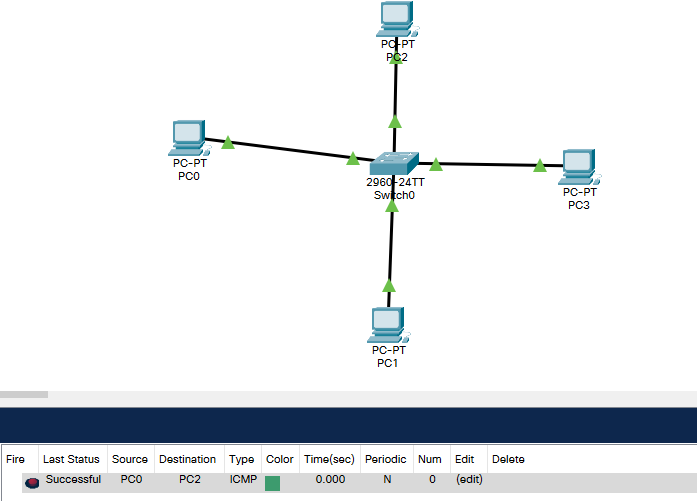
1. Ping

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.



1. PDU’s

PDU 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.



# 5. Basic Router Configuration, Static Routing Implementation

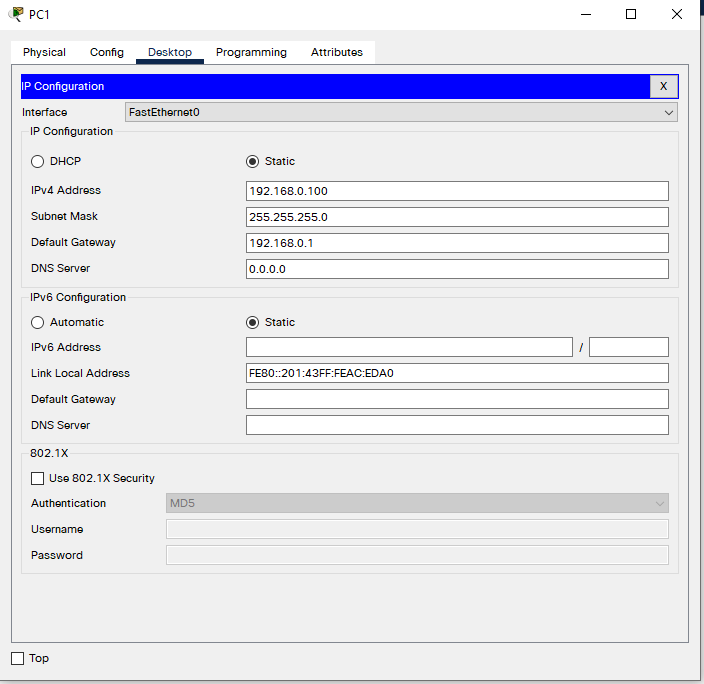
## Basic Router Configuration

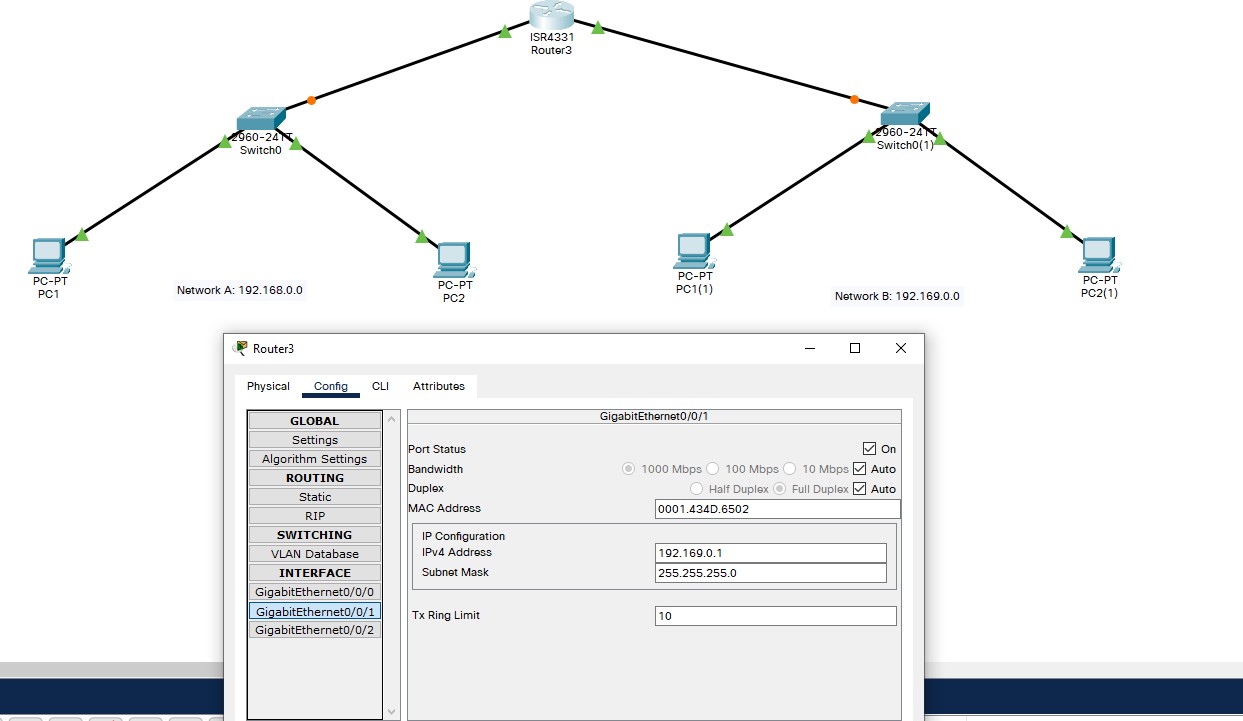
Routers are generally used to connect two different networks. To configure Routers let us consider two networks. Network A and Network B. now to connect the two, we use routers as follows.

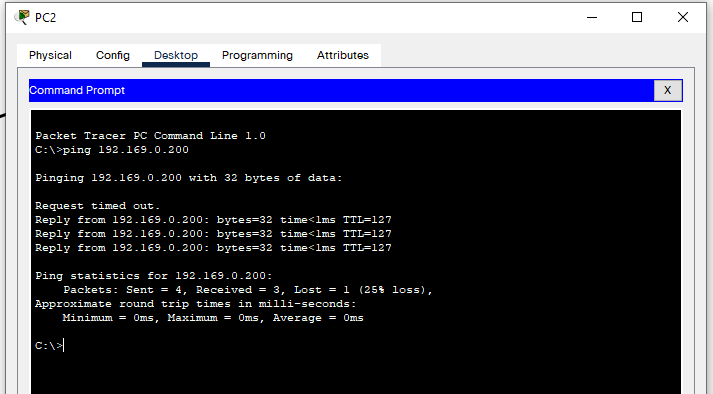
1. Create two networks with different IP’s



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



1. Connect the two network’s switches to router’s ports, assign network gateway address to each of the port
2. The router is now configured. We can test it by pinging a system outside the home 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.

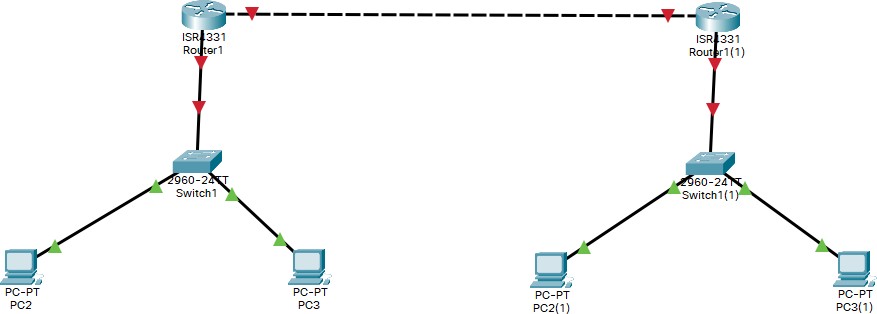
## Static Routing

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.

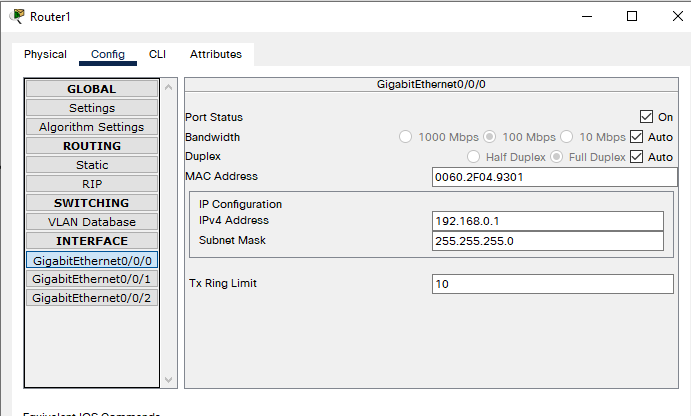
## Implementation of Static routing

To implement static routing, we follow the steps below

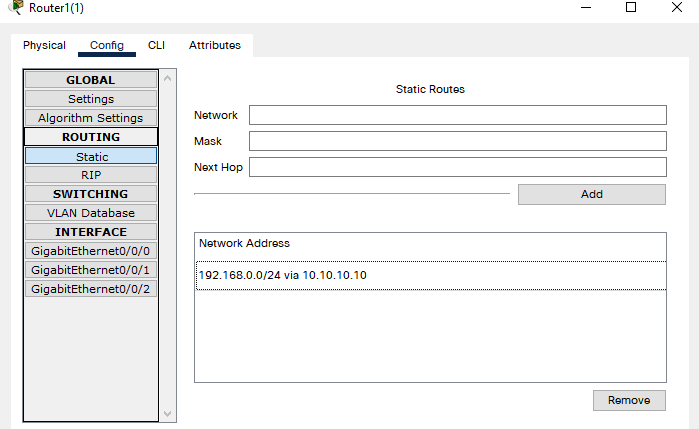
1. Firstly, create two networks with each of their own routers.



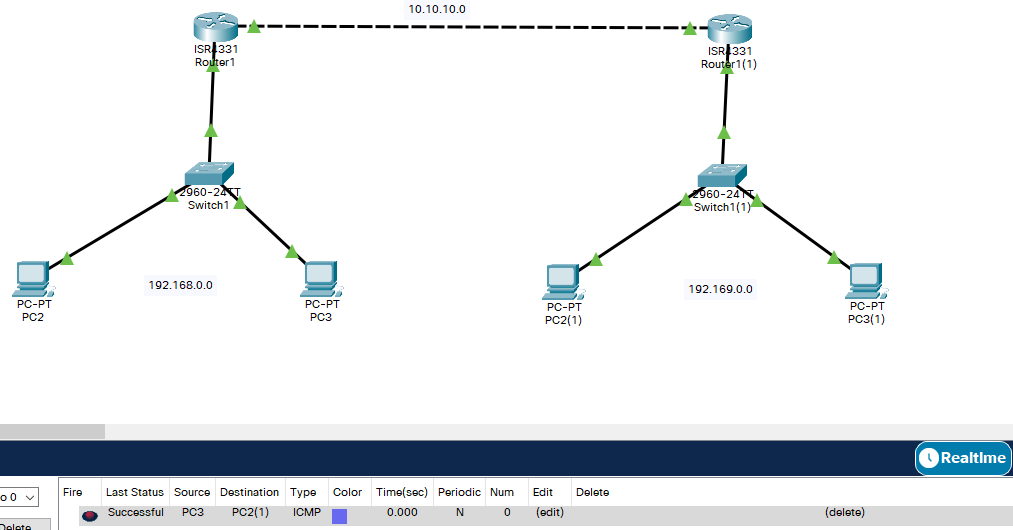
1. Assign IP’s to all nodes and Routers.



1. Configure the static routing table on both routers



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



# 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.

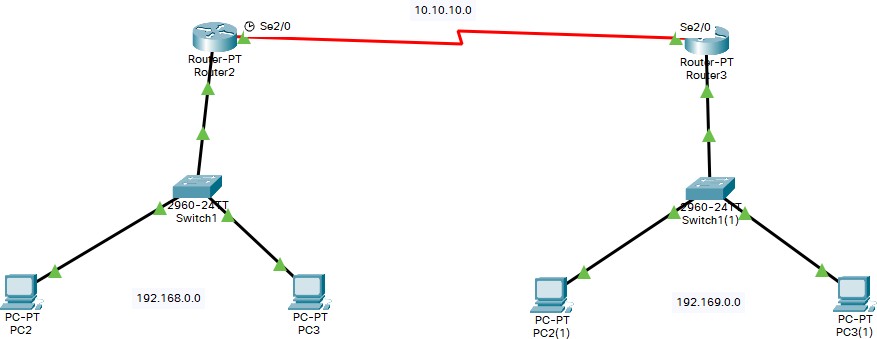
Dynamic routing requires more computing power, which is why smaller networks may rely on static routing. But for medium-sized and large networks, dynamic routing is much more efficient.

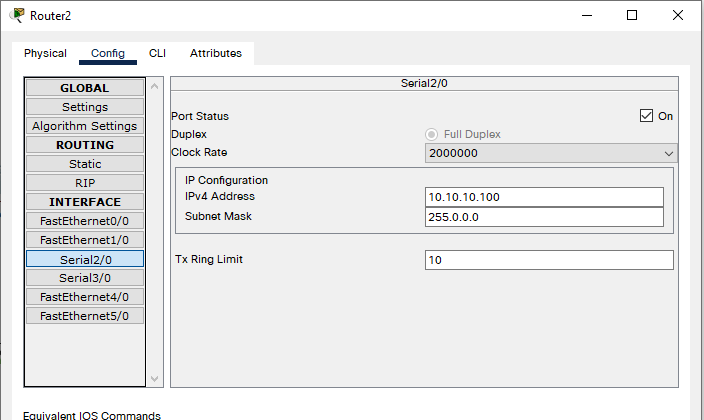
## Implementation of Dynamic Routing RIP

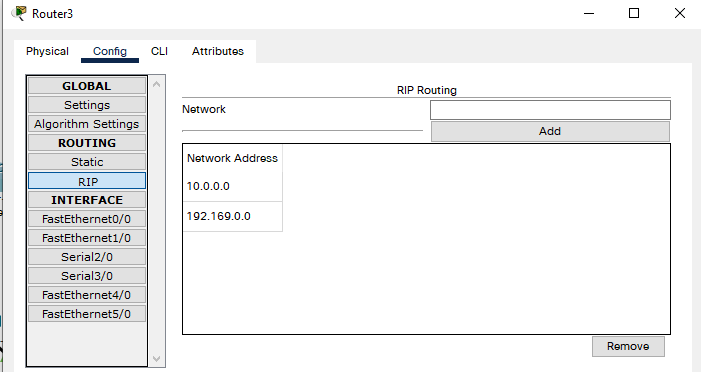
The Routing Information Protocol (RIP) uses "hop count" to find the shortest path from one network to another, where "hop count" means number of routers a packet must pass through on the way. (When a packet goes from one network to another, this is known as a "hop.")

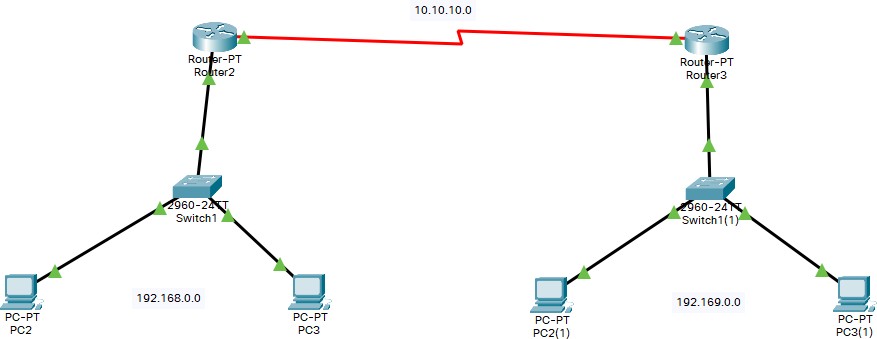
To implement RIP, we follow the steps below.

1. Create two networks with routers that have a serial port



1. Assign IP to nodes and routers. Connect serial port of routers to same network.
2. Go to RIP configuration and add all networks the router is connected to



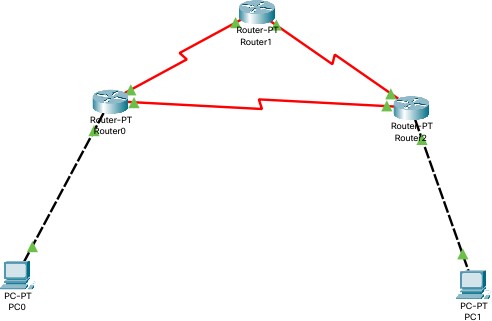
1. The RIP configuration is now complete and can be checked by a PDU

## OSPF

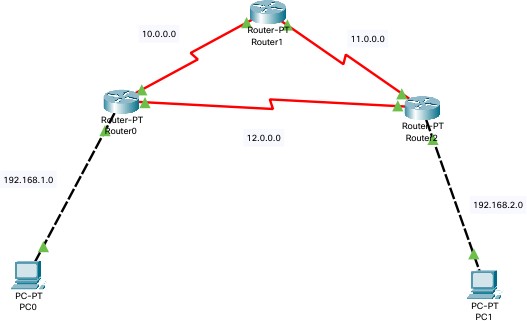
The Open Shortest Path First (OSPF) protocol is commonly used by network routers to dynamically identify the fastest and shortest available routes for sending packets to their destination.

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



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

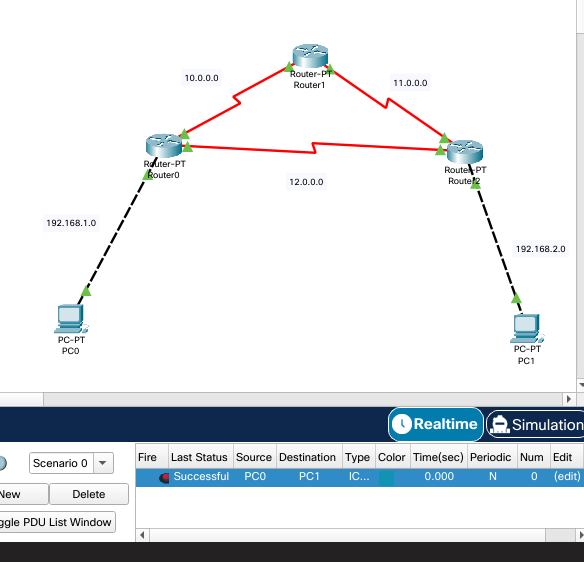
Go to config mode

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



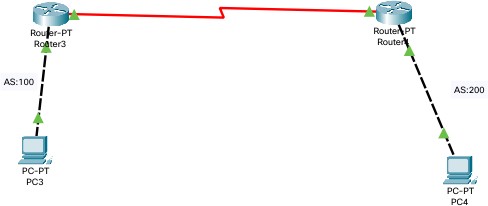
## BGP

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.

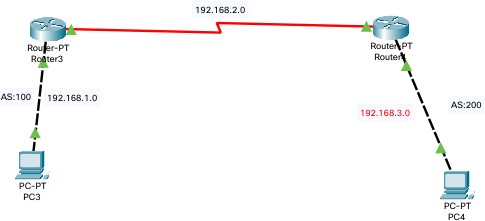
## Implementation of BGP protocol

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.

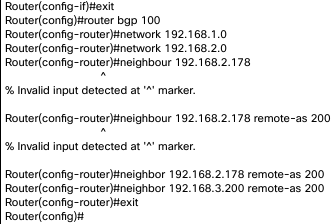


1. Now configure routers with BGP protocol Open router’s CLI and go to config mode. Type in router *bgp [AS number]*

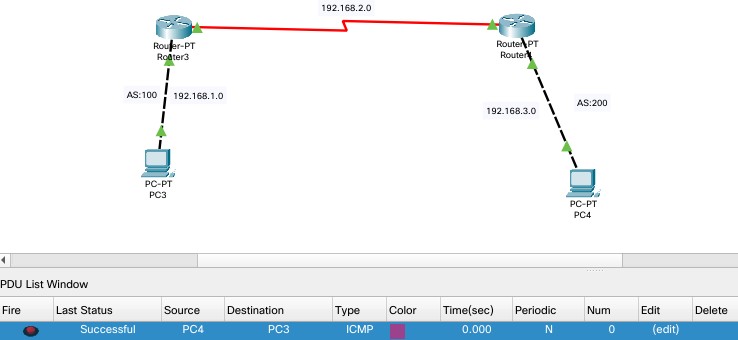
Add networks routers are connected to using *network [ip address]*

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)

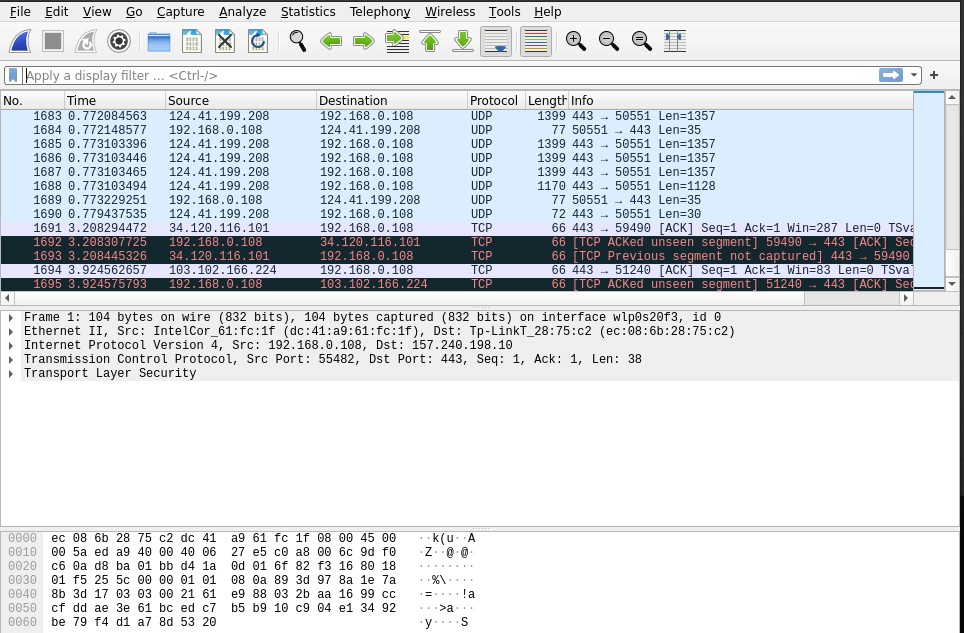
## Wireshark

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.

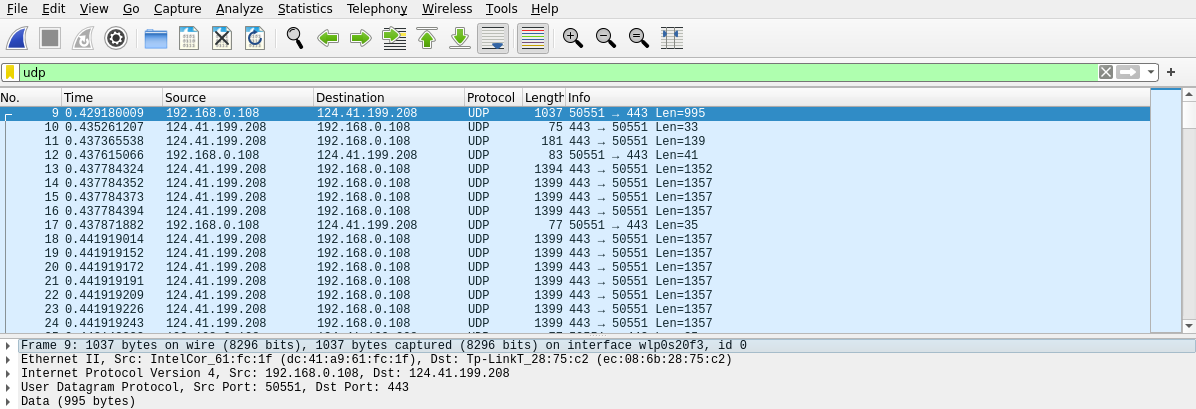
## Packet Capture

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

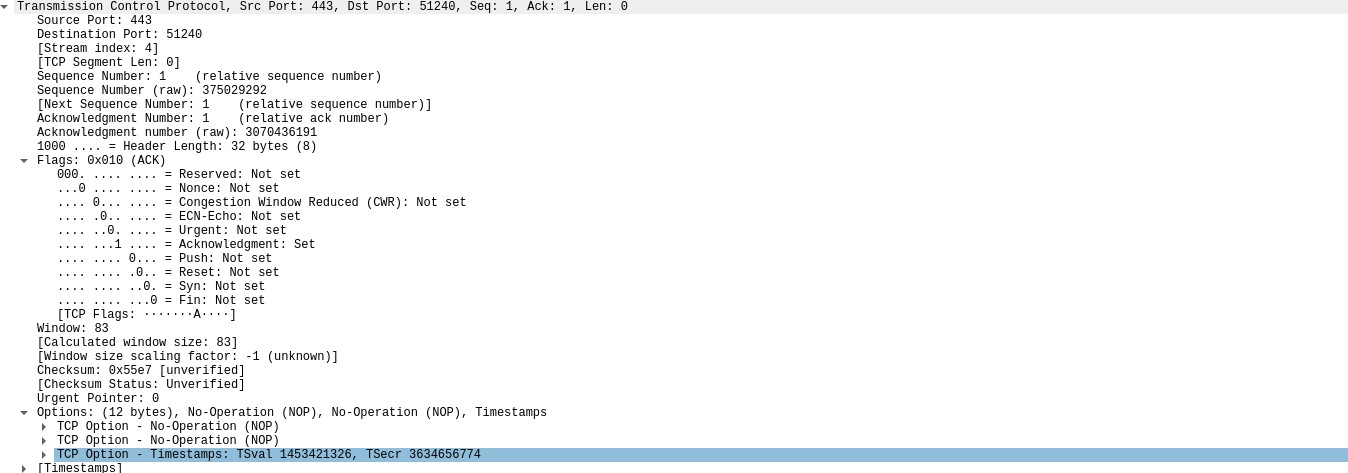
Wireshark can filter traffic based on the protocol. To filter packets based on Protocol of packet like TCP, UDP, DNS, etc. we apply display filter on the top bar.



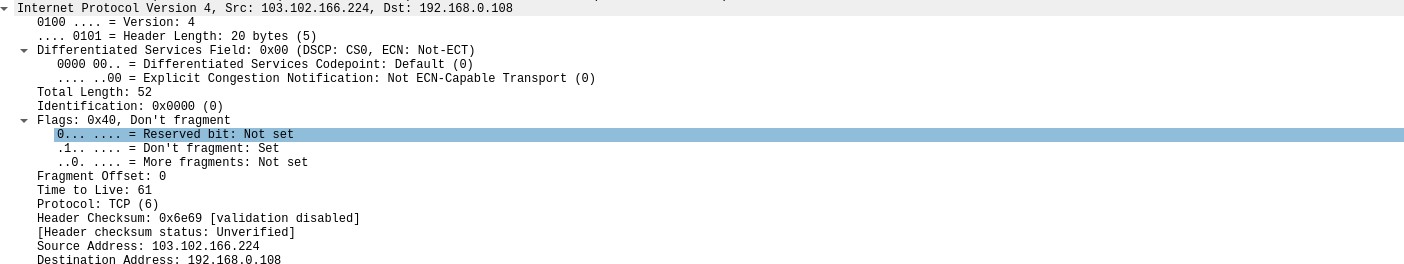
## Packet Analysis

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.

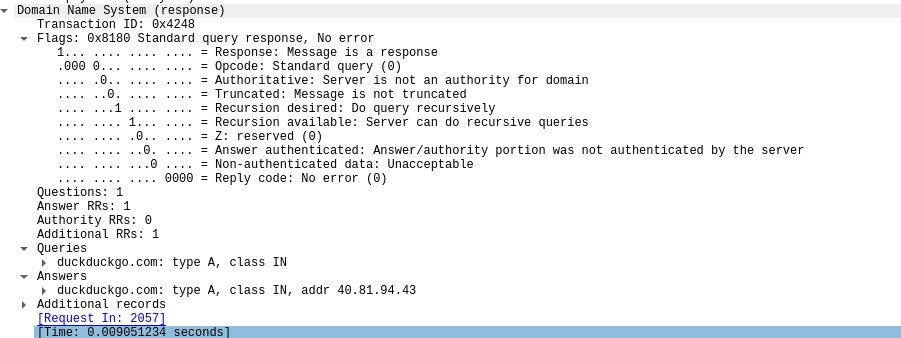
Under the Transmission Control Protocol, we can see all the information on the TCP header.



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



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

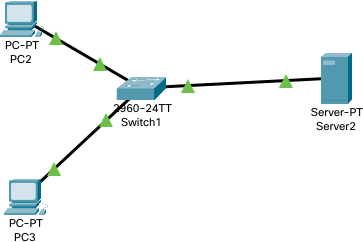
## Web Server

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.

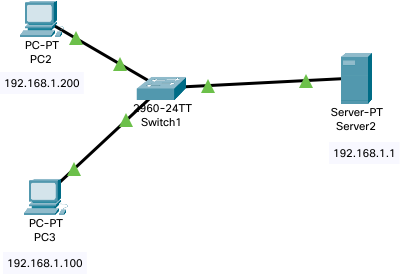
## Configuring a web server

To configure a web server, we follow the steps below

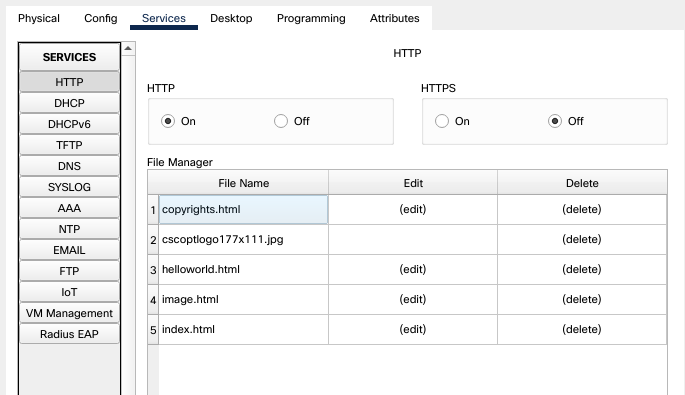
* + 1. Create a network with a switch, a server and end devices.



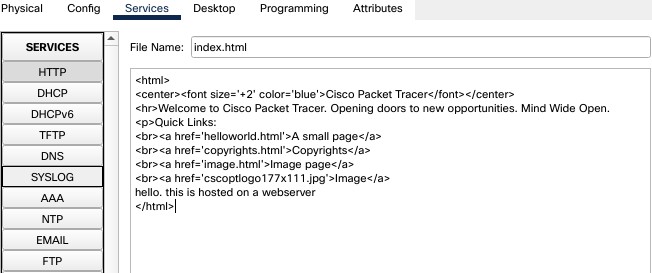
* + 1. Configure IP’s of switch server and end devices.



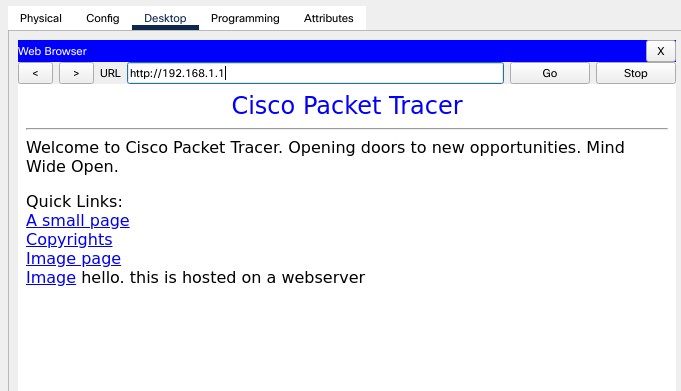
* + 1. Open server. Go to services tab. Click https and turn http and https on.



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



* + 1. Open up browser and type in IP of the webserver and the website will openup.



## DNS server

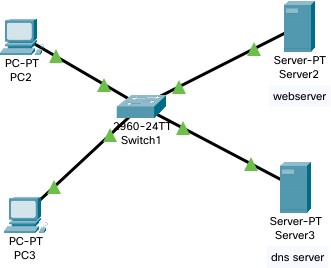
A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases serves to resolve, or translate, those names to IP addresses as requested. DNS servers run special software and communicate with each other using special protocols. It's 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.

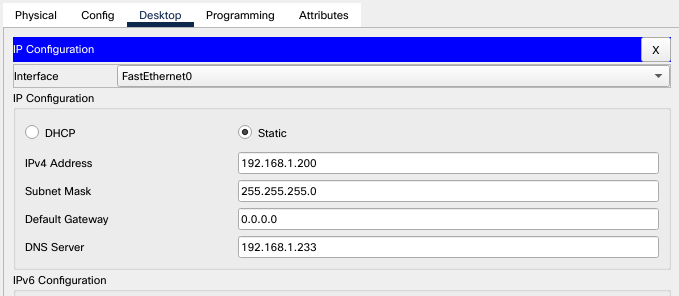
## Configuring a DNS server

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

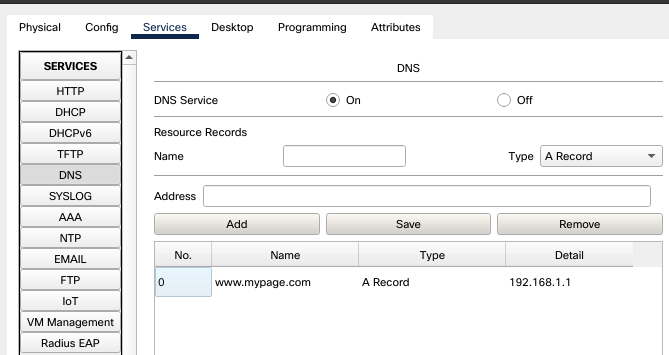
1. Create a network with end devices, switch, a webserver and a dns server



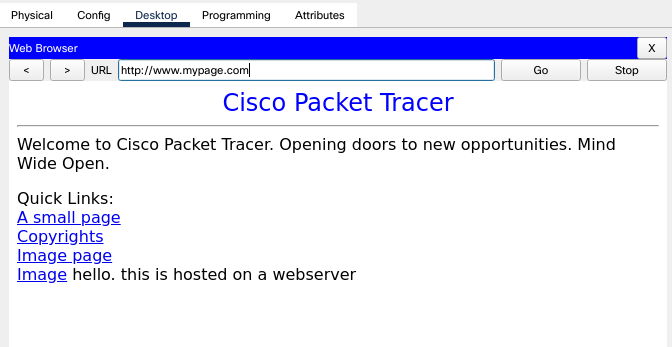
1. Configure the IP addresses to all devices and add the DNS server’s ip to the ‘DNS server’ section of ip configuration menu



1. Open DNS server, go to services and turn on DNS. add website address and IP of the webserver and click add.



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



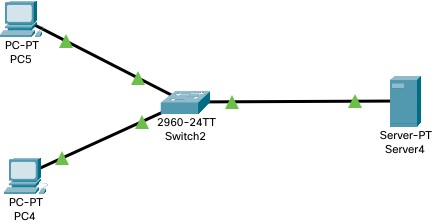
## FTP

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).

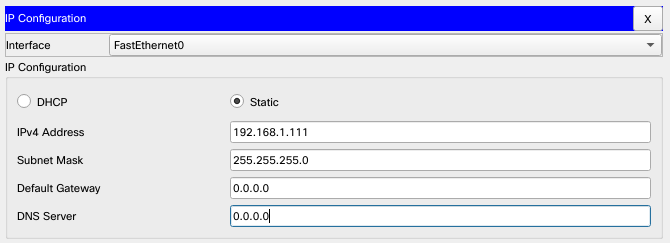
## Implementation of FTP server

To implement FTP server, we follow the steps below

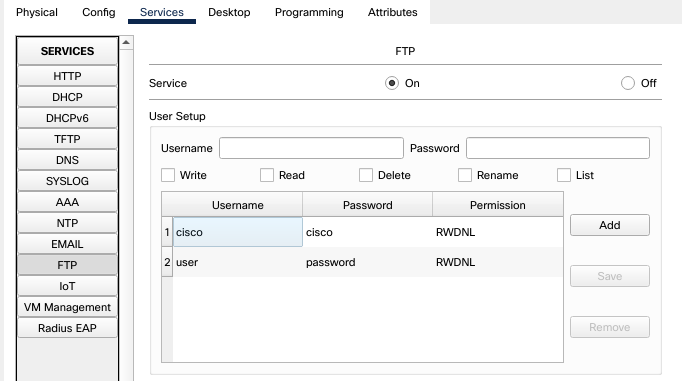
1. Create a network with a server, a switch and end devices.



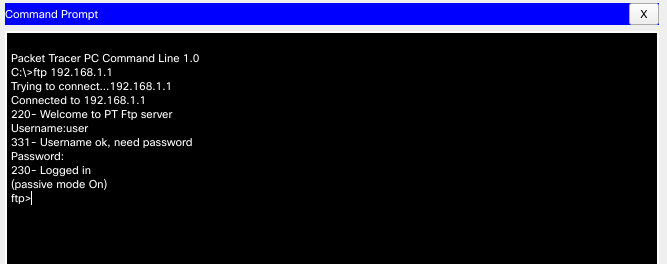
1. Assign IP to all devices and server



1. Open server and enable FTP service.

Create a username and password and assign the r/w privileges and click add.

1. Open end device and go to command prompt and type *ftp [server ip]*.use the previously created username and password and log in.



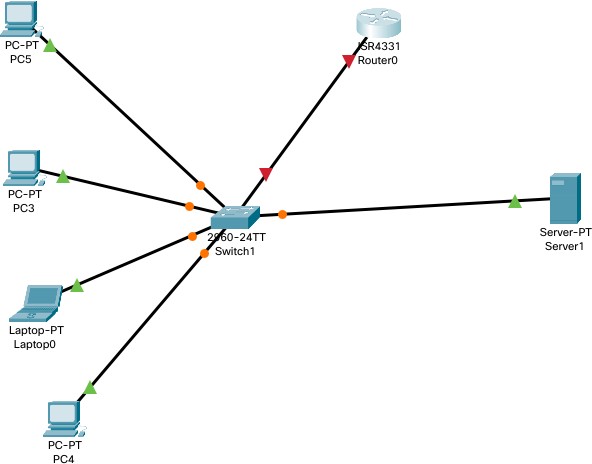
1. We can now perform file operations on the ftp server using commands like delete, rename etc.

## DHCP

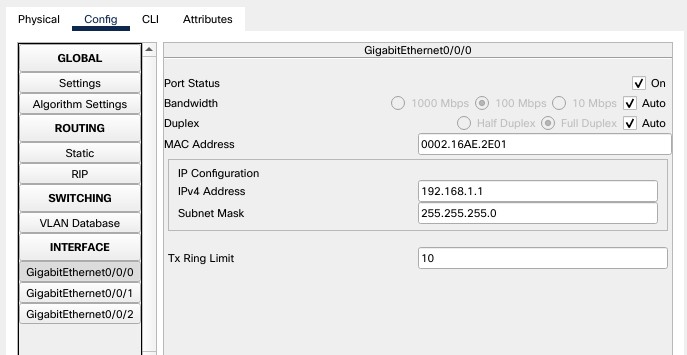
Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

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

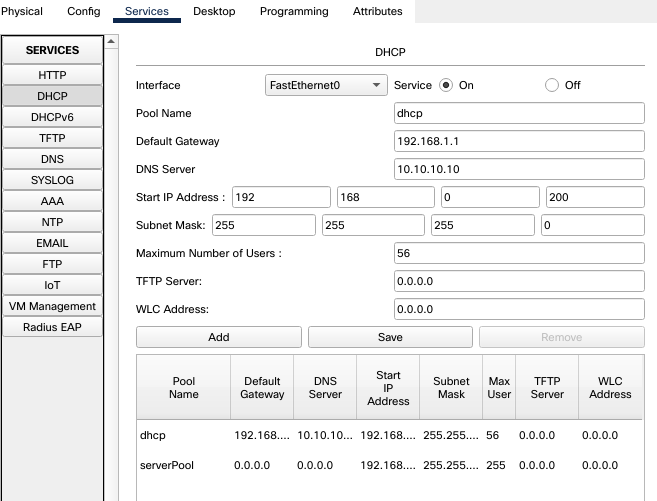
1. Create a network with a server, switch,router and end devices.



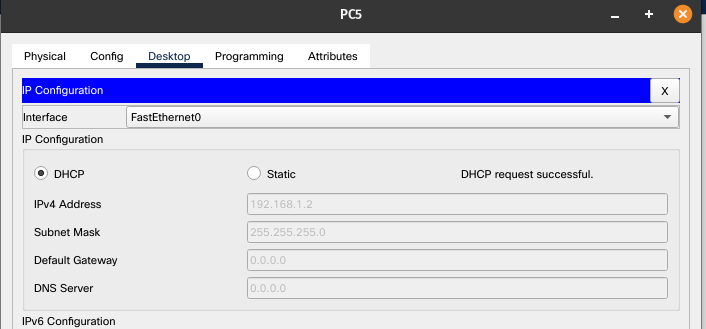
1. Open server settings and set an ip for the DHCP server and Router.



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.

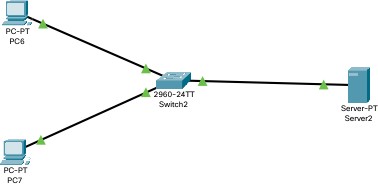


## Email Server

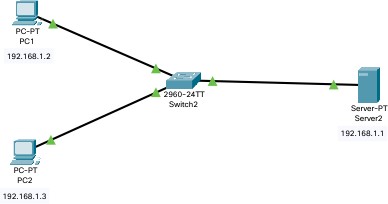
A mail server (sometimes also referred to an e-mail server) is a server that handles and delivers e- mail over a network, usually over the Internet. A mail server can receive e-mails from client computers and deliver them to other mail servers. A mail server can also deliver e-mails to client computers.

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

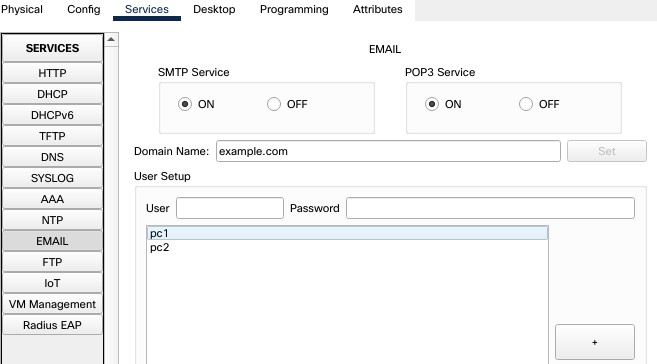
1. Create a network with end devices, server and switch.



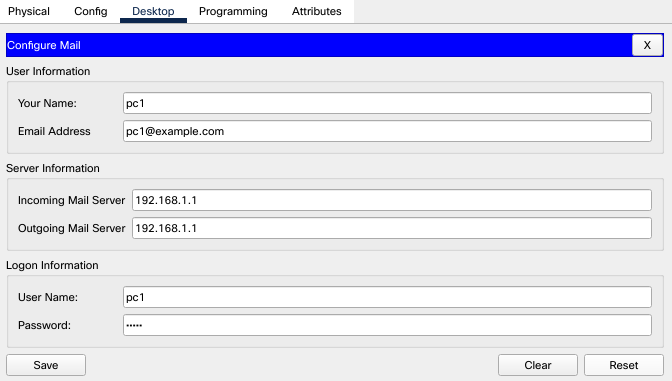
1. Assign IP to routers, end devices and server



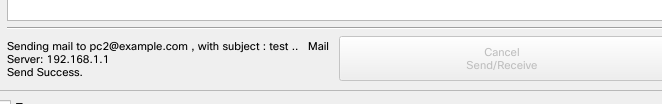
1. Open server and go to services. Then go to email and turn both email services on Create a domain name and create username and password.



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



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



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

