**PRACTICAL NO.: 01**

**Title:**

Determine the Network Equipment in Network

**Objective:**

To identify different equipment used in networking

**Theory:**

Networking equipment refers to the hardware devices utilized in computer networks to facilitate communication and data transfer between different devices within the network. These devices include routers, switches, hubs, modems, access points, network interface cards (NICs), and various types of cables and connectors. Each networking equipment serves a specific function and plays a crucial role in the operation and efficiency of the network.

Here's a brief overview of some common networking equipment:

1. **Router**:

A router is a crucial networking device responsible for directing data packets between computer networks. It operates at the network layer of the OSI model and uses routing tables to determine the best path for data transmission based on IP addresses. Routers connect multiple networks, such as LANs and WANs, and enable communication between devices across different networks.

1. **Switch**:

Switches are fundamental networking devices that connect multiple devices within a LAN (Local Area Network) and facilitate communication by forwarding data packets to their intended destinations. Unlike hubs, switches operate at the data link layer of the OSI model and use MAC addresses to determine the correct port for data delivery. They offer improved performance and efficiency by creating dedicated communication paths between devices, reducing network congestion, and supporting full-duplex communication.

1. **Firewall**:

A firewall is a network security device designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between an internal network and external networks, such as the internet, to prevent unauthorized access and protect against cyber threats. They are essential for safeguarding sensitive data, preventing unauthorized access to network resources, and ensuring the integrity and confidentiality of network communications.

1. **Modem**:

A modem (modulator-demodulator) is a networking device that converts digital data from a computer into analog signals for transmission over communication channels such as telephone lines or cable systems. It enables devices to access the internet and communicate with other devices over long distances using various transmission mediums. Modems are essential for connecting to internet service providers (ISPs) and establishing reliable internet connectivity for residential and business users.

1. **Hub**:

A hub is a basic networking device that operates at the physical layer (Layer 1) of the OSI model. It serves as a central connection point for multiple Ethernet devices within a LAN (Local Area Network), allowing them to communicate with each other. Hubs are primarily used in small networks or as network extenders, but they have largely been replaced by switches in modern network deployments due to their limitations.

1. **Network Interface Card (NIC):**

A network interface card, commonly referred to as NIC or network adapter, is a hardware component that enables a computer or other device to connect to a network. It is typically installed inside a computer and provides the necessary interface for connecting to Ethernet, Wi-Fi, or other types of networks. NICs play a crucial role in enabling network connectivity and facilitating data transmission between devices on a network.

**Conclusion**:

Hence, we studied about the different equipment used in networking.

**Practical No.: 02**

**Title:**

Identify the networking wire and cable

**Objective:**

To know about networking cable standards

**Theory:**

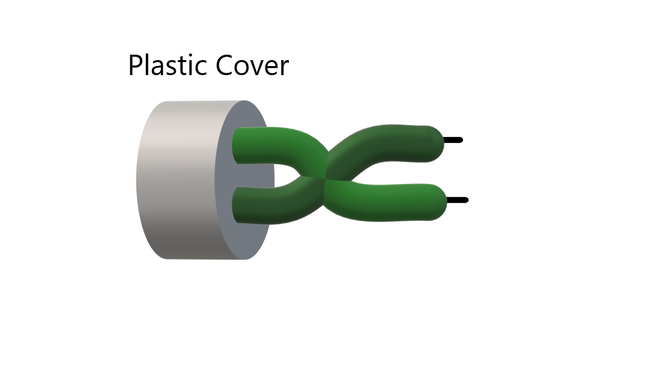
In computer networks, several types of cables are used to establish connections and transmit data between devices. Here are some common types of cables used in computer networks:

1. **Twisted Pair Cable:**

Twisted pair cables are one of the most common types of cables used in networking.

They consist of pairs of insulated copper wires twisted together to reduce electromagnetic interference (EMI) and crosstalk. They are flexible, easy to install, and cost-effective, making them suitable for both residential and commercial applications. It is categorized inti two types:

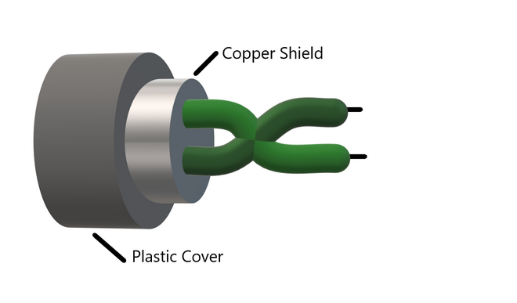
1. Unshielded Twisted Pair Cables (UTP) :

These are a pair of two insulated copper wires twisted together without any other insulation or shielding and hence are called unshielded twisted pair cables. They reduce the external interference due to the presence of insulation. Unshielded twisted pair cables are arranged in pairs so that we can add a new connection whenever required.

*Unshielded Twisted Pair cable*

1. Shielded Twisted Pair Cables (STP) :

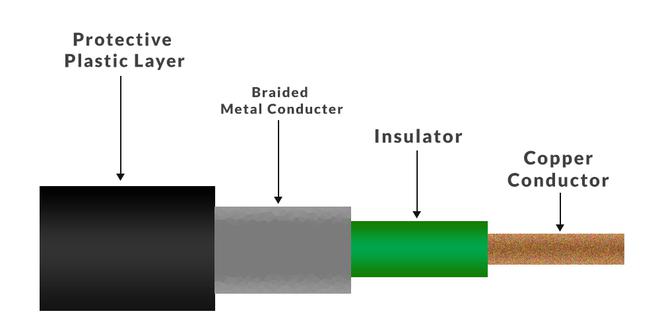
These types of cables have extra insulation or protective covering over the conductors in the form of a copper braid covering. This covering provides strength to the overall structure of the cable. It also reduces noise and signal interference in the cable. The shielding ensures that the induced signal can be returned to the source via ground and only circulate around the shield without affecting the main propagating signal.



*Shielded Twisted Pair cable*

1. **Coaxial Cable:**

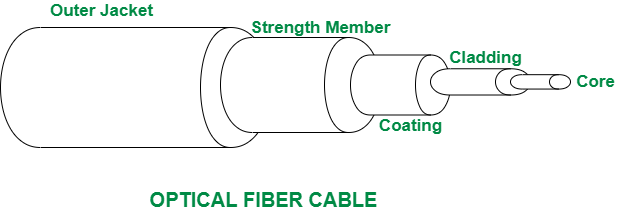
Coaxial cables consist of a central conductor surrounded by a dielectric insulator, a metallic shield, and an outer insulating layer. They offer excellent noise immunity, high bandwidth, and low signal loss, making them suitable for carrying high-frequency signals over long distances. Coaxial cables are commonly used for cable television (CATV), broadband internet connections, CCTV systems, and high-speed data networks. They come in different varieties such as RG-6 and RG-59, with RG-6 offering higher bandwidth and better performance compared to RG-59. Coaxial cables are widely used in both residential and commercial applications due to their reliability, durability, and versatility.



*Coaxial Cable*

1. **Fiber Optic Cable:**

Fiber optic cables use strands of glass or plastic fibers to transmit data using light signals. They offer high bandwidth, low signal loss, and immunity to electromagnetic interference, making them ideal for long-distance and high-speed data transmission. Fiber optic cables are classified into single-mode fiber (SMF) and multi-mode fiber (MMF) based on the number of light paths they support and the distance they can transmit data. SMF cables are used for long-distance telecommunications and high-speed internet connections, while MMF cables are suitable for shorter distances in LANs, data centers, and campus networks. Fiber optic cables are commonly used in high-performance networks, telecommunications systems, cable television (CATV), and internet backbone infrastructure.



*Fiber Optic Cable*

**Conclusion:**

Hence, we studied in details about the different cables used in networking.

**PRACTICAL NO.: 03**

**Title:**

Packet Tracer Practical

**Objective:**

To create and test LAN and VLAN using Packet Tracer

**Theory:**

Packet tracer is a standalone, medium-fedility, simulation-based learning environment for networking devices to design, configure, and troubleshoot computer networks at a CCNA-level complexity.

AN (Local Area Network) is a data communication network that locally connects network devices such as workstations, servers, routers, etc. to share the resources within a small area such as a building or campus. Physical or wireless connections are set up between workstations to share the resources. Ethernet and Wi-fi are the most important technologies of LAN. Personal networks at home, school, office, etc. are examples of LAN. These are generally privately-owned networks.

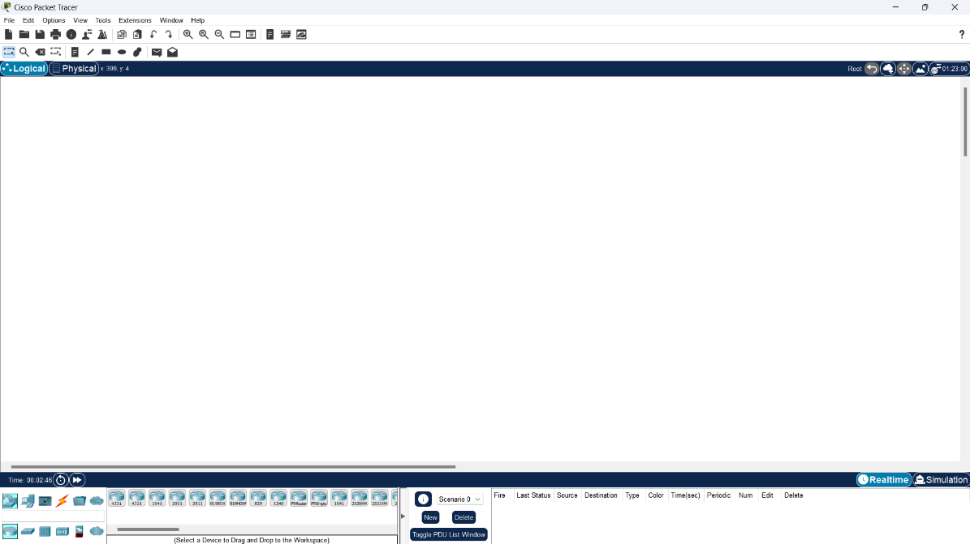
A Virtual LAN (VLAN) is simply a logical LAN, just as its name suggests. VLANs have similar characteristics to those of physical LANs, only that with VLANs, you can logically group hosts even if they are physically located on separate LAN segments. We treat each VLAN as a separate subnet or broadcast domain.

**Workspace**:

Packet Tracer uses following two representation schemas for network:

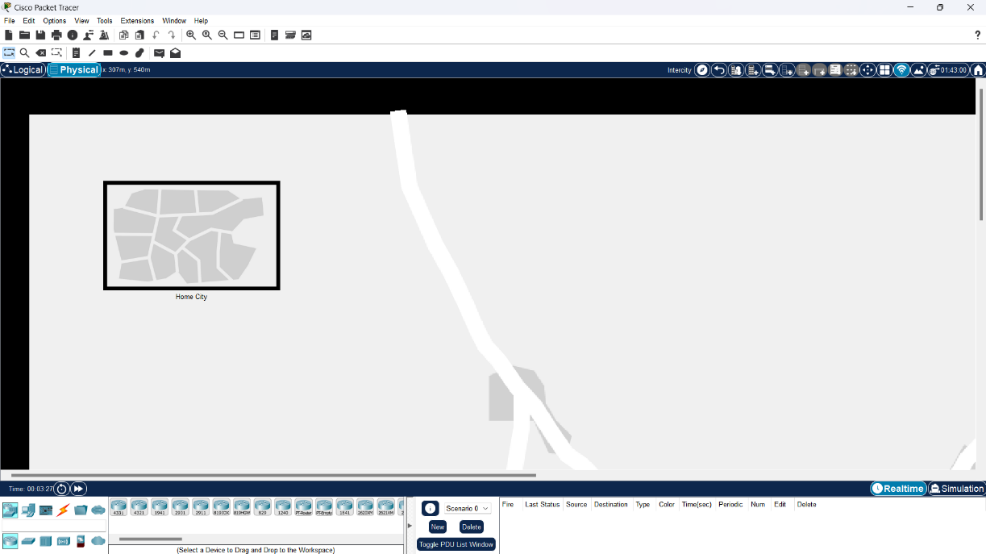
* **The Logical Workspace**

The Logical workspace allows you to build a logical network topology, without regard to its physical scale and arrangement.



* **The Physical Workspace**

The It allow you to arrange devices physically in cities, buildings, and wiring closets. Distances and other physical measures will affect network performance and other characteristics if wireless connections are used.



**Procedure:**

1. Configuring IP Addresses on PCs:

* Select a PC:

Click on the PC you want to configure to select it.

* Access Configuration Tab:

Click on the “Config” tab at the bottom of the screen to access the configuration options for the selected PC.

* Assign IP Address:

Manually assign an IP address to the PC, such as:

PC1: IP – 192.168.1.2

PC2: IP – 192.168.1.3

Set the subnet mask, e.g., 255.255.255.0.

* Repeat for Other PCs:

Repeat the process for each PC, ensuring that each has a unique IP address within the same subnet.

1. Configuring the Switch:

* Select the Switch:

Click on the switch to select it.

* Access Command Line Interface (CLI):

Click on the “CLI” tab at the bottom of the screen to access the Command Line Interface (CLI) of the switch.

* Enter Configuration Mode:

Enter the command to configure the switch.

1. Testing Connectivity:

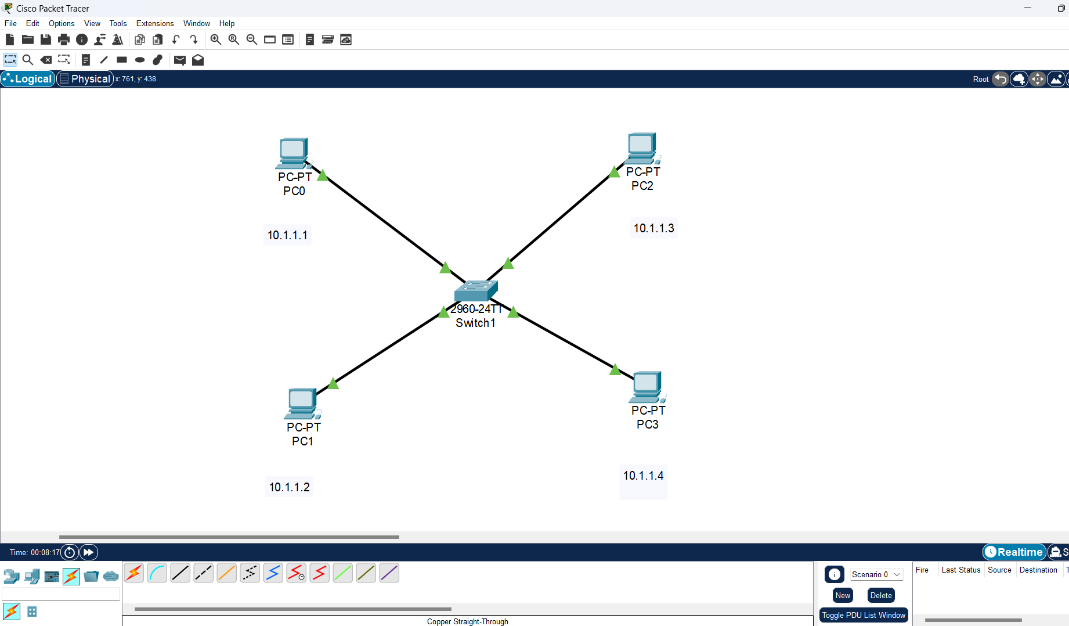
* Open Command Prompt:

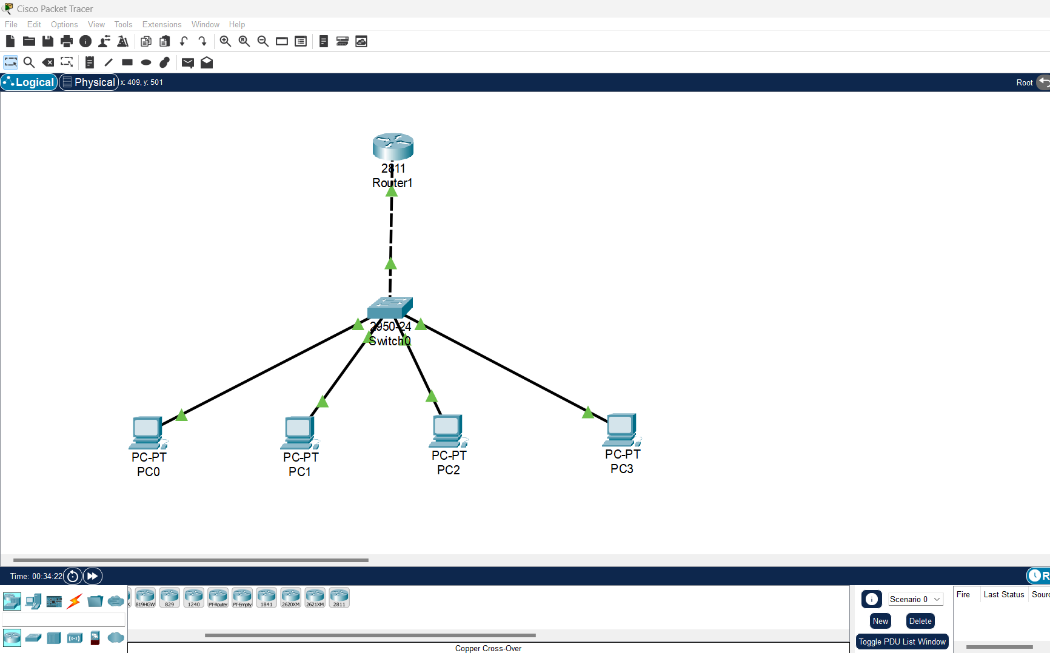
Open the command prompt on one of the PCs.

* Ping Another PC:

Use the “ping” command to test connectivity to another PC, e.g., ping 192.168.1.3.

This command sends packets to the specified IP address and checks for a response, verifying LAN communication.

**LAN setup:**

**VLAN setup:**

**Conclusion:**

Hence, we studies and tested the LAN and VLAN configuration successfully using packet tracer in lab.

**PRACTICAL NO.: 04**

**Title:**

Determine the Network Equipment in Network

**Objective:**

To understand theoretical knowledge of IPv4 Addressing and Subnetting.

**Theory:**

An IP address (*internet protocol address*) is a numerical representation that uniquely identifies a specific interface on the network. Addresses in IPv4 are **32**-bits long. This allows for a maximum of 4,294,967,296 (232) unique addresses. Addresses in IPv6 are **128**-bits, which allows for 3.4 x 1038 (2128) unique addresses. IP addresses are binary numbers but are typically expressed in decimal form (IPv4) or hexadecimal form (IPv6) to make reading and using them easier for humans.

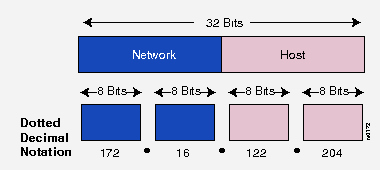
# Terminologies

* **IPv4 address:** a 32-bit number, usually written in dotted decimal form, that uniquely identifies an interface of some computer
* **Host Address:** another term for IP address of the end device
* **Network:** a group of hosts, all of which have an identical beginning position of their ip addresses.
* **Broadcast Address:** a 32-bit number that is used to address all hosts in the network. It can't be assigned as an ip address of a host.
* **Subnet:** a group of hosts, all of which have an identical portion of their ip addresses, a subnet differs from a network in that a subnet is a further subdivision of a network.
* **Sub-netting:** the process of subdividing networks into smaller subnets.
* **Subnet mask:** A 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host.

# IPv4 Address representations

IPv4 addresses are actually 32-bit binary numbers, consisting of the two identifiers which, identify the network and the host to the network. It is generally represented as 4 octets of numbers from 0-255 represented in decimal form instead of binary form.

The IP address is divided into two main parts; the Network Number and the Host Number. The host number identifies a host in the network and is assigned by the local network administrator.



# Subnet Masks

A single IP address identifies both a network, and a unique interface on that network. A subnet mask can also be written in dotted decimal notation and determines where the network part of an IP address ends, and the host portion of the address begins.

When expressed in binary, any bit set to one means the corresponding bit in the IP address is part of the network address. All the bits set to zero mark the corresponding bits in the IP address as part of the host address. The bits marking the subnet mask must be consecutive ones. Most subnet masks start with 255. and continue on until the network mask ends.

A Class A network mask is defined as 255.0.0.0.

A Class B network mask is defined as 255.255.0.0. A Class C network mask would be 255.255.255.0

# IP Address Classes

Before variable length subnet masks allowed networks of any size to be configured, the IPv4 address space was broken into five classes.

# Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127. The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (27-2) and 16,777,214 hosts (224-2).

(Note: 0 Octet is forbidden in RFC and 127 is reserved for loopback testing.)

# Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to

10. The default subnet mask for Class B is 255.255.0.0. Class B has 16384 (214) Network addresses and 65534 (216-2) Host addresses.

# Class C Address

The first octet of Class C IP address has its first 3 bits set to 110. The default subnet mask for Class C is 255.255.255.0. Class C gives 2097152 (221) Network addresses and 254 (28-2) Host addresses.

# Class D Address

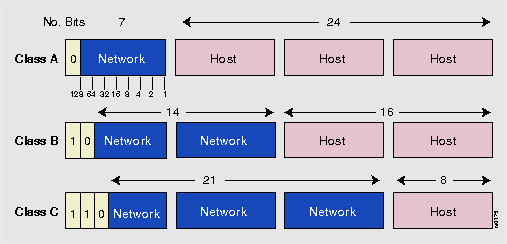
The first four bits of the first octet in Class D IP addresses are set to 1110. Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

# Class E Address

The first four bits of the first octet in Class D IP addresses are set to 1111. This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

# Network and Host Portion:

A Class A address has the first octet as the network portion and the remaining 3 octets as the host portion. A Class B address has the first and second octets as the network portion and the third and fourth octets as the host portion. A Class C address has the first, second, and third octet as the network portion and the last octet as the host portion.



# Overview: IP Address Classes and Bit-Wise representations Class A

0. 0. 0. 0 = 00000000.00000000.00000000.00000000

|  |  |  |
| --- | --- | --- |
| 127.255.255.255 | = | 01111111.11111111.11111111.11111111  0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH |
| **Class B** |  |  |
| 128. 0. 0. 0 | = | 10000000.00000000.00000000.00000000 |
| 191.255.255.255 | = | 10111111.11111111.11111111.11111111 |
|  |  | 10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH |

# Class C

192. 0. 0. 0 = 11000000.00000000.00000000.00000000

223.255.255.255 = 11011111.11111111.11111111.11111111

110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH

# Class D

224. 0. 0. 0 = 11100000.00000000.00000000.00000000

239.255.255.255 = 11101111.11111111.11111111.11111111

1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

# Class E

240. 0. 0. 0 = 11110000.00000000.00000000.00000000

255.255.255.255 = 11111111.11111111.11111111.11111111

1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

# Private addresses

Within the address space, certain networks are reserved for private networks. Packets from these networks are not routed across the public internet. This provides a way for private networks to use internal IP addresses without interfering with other networks. The private networks are

* Class A Private Range: 10.0.0.0 to 10.255.255.255
* Class B Private APIPA Range: 169.254.0.0 to 169.254.255.255
  + *Automatic Private IP Addressing* (APIPA) is a feature on *Microsoft Windows*-based computers to automatically assign itself an IP address within this range if a *Dynamic Host Configuration Protocol* (DHCP) server is not available. A DHCP server is a device on a network that is responsible for assigning IP address to devices on the network.
* Class B Private Range: 172.16.0.0 to 172.31.255.255
* Class C Private Range: 192.168.0.0 to 192.168.255.255

# Special addresses

Certain IPv4 addresses are set aside for specific uses:

|  |  |
| --- | --- |
| 127.0.0.0 | Loopback address (the host’s own interface) |
| 224.0.0.0 | IP Multicast |
| 255.255.255.255 | Broadcast (sent to all interfaces on network) |

# IPV4 Subnetting

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

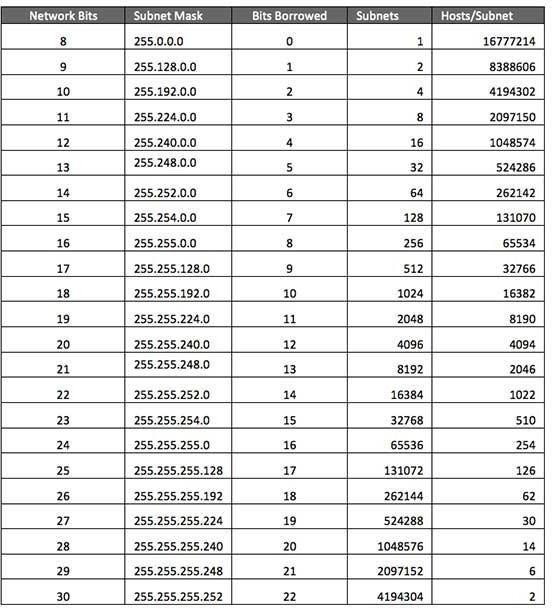
# Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (21=2) with (223-2) 8388606 Hosts per Subnet.

The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets −

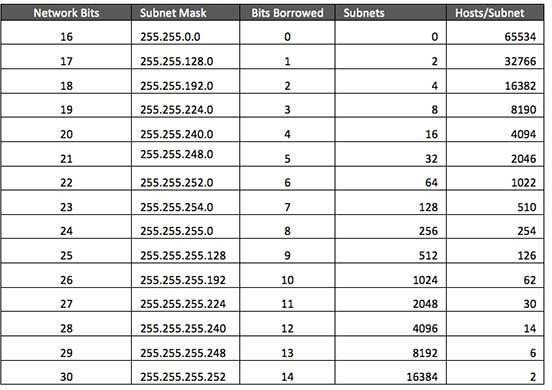
In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.



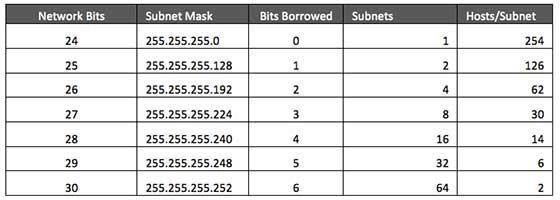
# Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits providing

(214) 16384 Networks and (216-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting −



# Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address –

**Exercise Address Class** 10.250.1.1- Class A

150.10.15.0- ClassB

192.14.2.0-Class C

148.17.9.1- Class B

193.42.1.1- Class C

126.8.156.0- ClassA

220.200.23.1- Class C

230.230.45.58- Class D

177.100.18.4- Class B

119.18.45.0-Class A

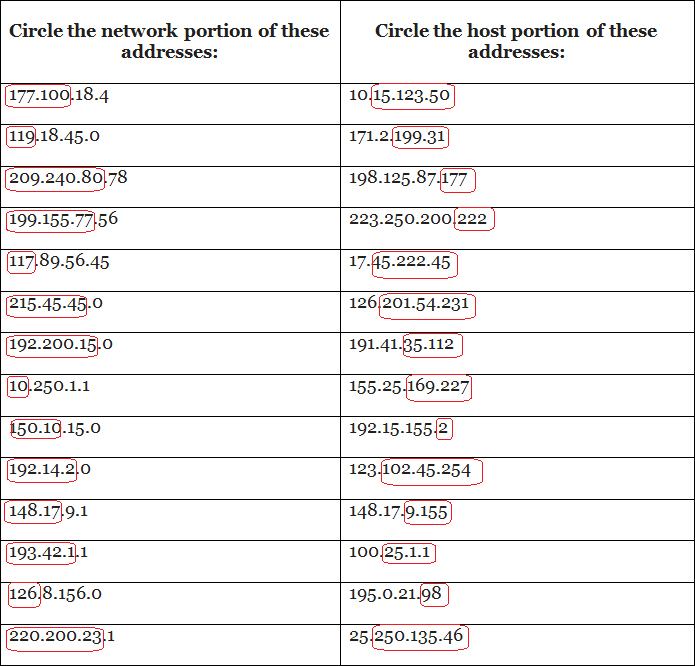
249.240.80.78- Class E

199.155.77.56- Class C

117.89.56.45- Class A

215.45.45.0- Class C

199.200.15.0- Class C

**Network & Host Identification**

# Default Subnet Masks

Write the correct default subnet mask, network address and broadcast address for each of the following addresses:

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Address** | **Default Subnet**  **Mask** | **Network**  **Address** | **Broadcast**  **Address** |
| 177.100.18.4 | 255.255.0.0 | 177.100.0.0 | 177.100.255.255 |
| 119.18.45.0 | 255.0.0.0 | 119.0.0.0 | 119.255.255.255 |
| 191.249.234.191 | 255.255.0.0 | 191.249.0.0 | 191.249.255.255 |
| 223.23.223.109 | 255.255.255.0 | 223.23.223.0 | 223.23.223.255 |
| 10.10.250.1 | 255.0.0.0 | 10.0.0.0 | 10.255.255.255 |
| 126.123.23.1 | 255.255.0.0 | 126.123.0.0 | 126.123.255.255 |
| 223.69.230.250 | 255.255.255.0 | 223.69.230.0 | 223.69.230.255 |
| 192.12.35.105 | 255.255.255.0 | 192.12.35.0 | 192.12.35.255 |
| 77.251.200.51 | 255.0.0.0 | 77.0.0.0 | 77.255.255.255 |
| 189.210.50.1 | 255.255.0.0 | 189.210.0.0 | 189.210.255.255 |
| 88.45.65.35 | 255.0.0.0 | 88.0.0.0 | 88.255.255.255 |
| 193.100.77.8 | 255.255.255.0 | 193.100.77.0 | 193.100.77.255 |
| 125.125.250.1 | 255.0.0.0 | 125.0.0.0 | 125.255.255.255 |
| 220.90.130.45 | 255.255.255.0 | 220.90.130.0 | 220.90.130.255 |
| 134.125.34.9 | 255.255.0.0 | 134.125.0.0 | 134.125.255.255 |

**PRACTICAL NO.: 05**

**Title:**

Determine the Static Routing Implementation

**Objective:**

To understand the Static Routing ,ist Advantages and Drawbacks

**Theory:**

Static routing is useful in small network where numbers of routes are limited. In

static routing we need to add route manually with IP route command. Like other routing methods static routing also has its pros and cons.

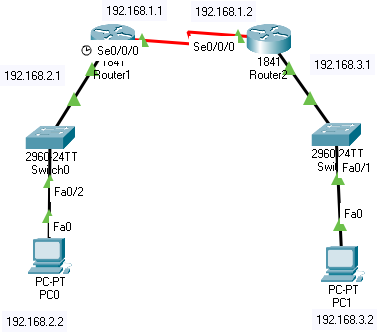
# Advantage of static routing

* It is easy to implement.
* It is most secure way of routing, since no information is shared with other routers.
* It puts no overhead on resources such as CPU or memory.

# Disadvantage of static routing

* It is suitable only for small network.
* If a link fails static route cannot reroute the traffic.

# Configuration



1. **Router Basic Configuration Router 1**

Router>enable Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname r1 r1(config)#enable password cisco r1(config)#enable secret class

r1(config)#line console 0 r1(config-line)#password cisco r1(config-line)#login

r1(config-line)#

r1(config-line)#line vty 0 15 r1(config-line)#password cisco r1(config-line)#login

r1(config-line)#

r1(config-line)#line aux 0 r1(config-line)#password cisco r1(config-line)#login

r1(config-line)# r1(config-line)#exit

r1(config)#service password-encryption

# Router 2

Router#

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname r2 r2(config)#enable password cisco r2(config)#enable secret class

r2(config)#line console 0 r2(config-line)#password cisco r2(config-line)#login

r2(config-line)#

r2(config-line)#line vty 0 15 r2(config-line)#password cisco r2(config-line)#login

r2(config-line)#

r2(config-line)#line aux 0 r2(config-line)#password cisco r2(config-line)#login

r2(config-line)#

r2(config-line)#exit

r2(config)#service password-encryption

# Router Interface Configuration Router 1

**Serial Link**

r1(config)#interface serial 0/0/0 r1(config-if)#description Link to R2

r1(config-if)#ip address 192.168.1.1 255.255.255.0

r1(config-if)#clock rate 64000 r1(config-if)#no shutdown r1(config-if)#

# Fast Ethernet

r1(config-if)#

r1(config)#interface fastethernet 0/0

r1(config-if)#ip address 192.168.2.1 255.255.255.0 r1(config-if)#no shutdown

r1(config-if)#exit

# Router 2 Serial Link

r2(config)#interface serial 0/0/0

r2(config-if)#des link from LAN to internet r2(config-if)#ip address 192.168.1.2 255.255.255.0 r2(config-if)#no shutdown

r2(config-if)#exit

# Fast Ethernet

r2(config-if)#interface fastethernet 0/0

r2(config-if)#ip address 192.168.3.1 255.255.255.0 r2(config-if)#no shutdown

r2(config-if)#exit

# Routes Configuration

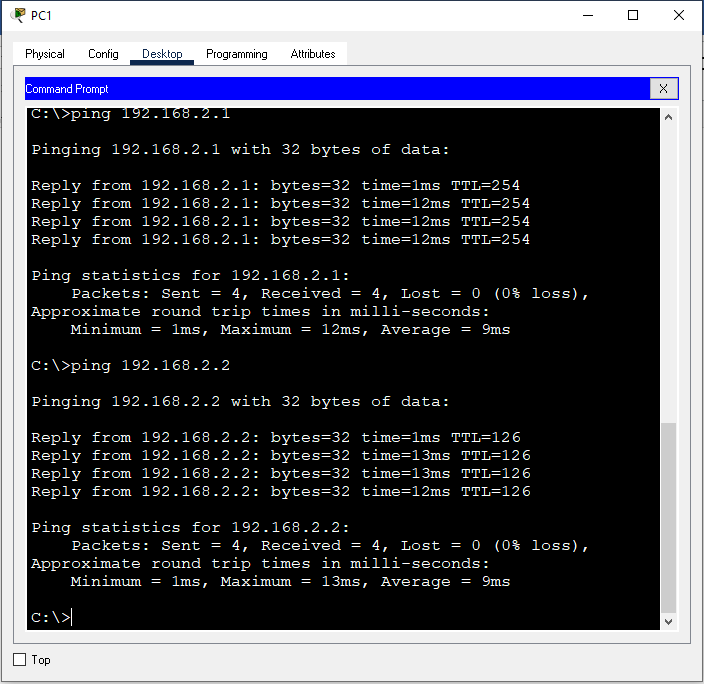
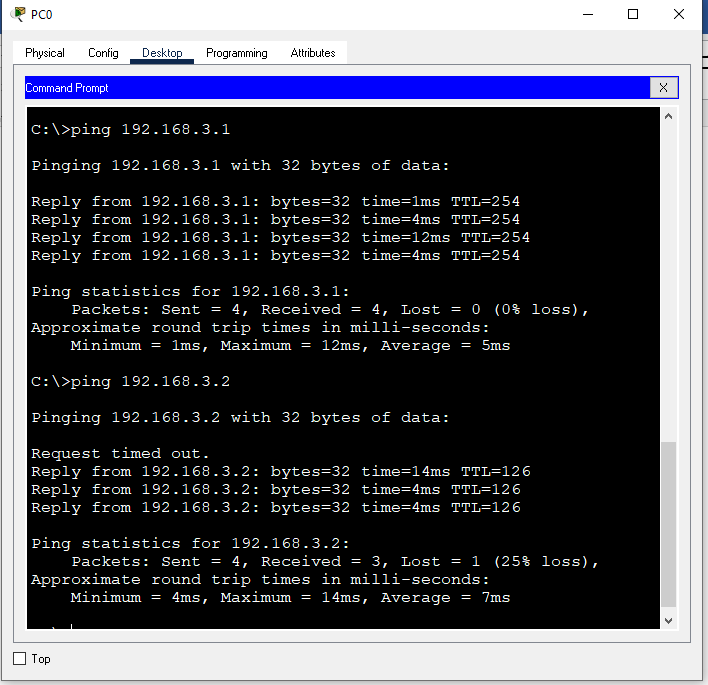
**Router 1**

r1(config)#ip route 192.168.3.0 255.255.255.0 192.168.1.2

# Router 2

r2(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1

1. **Result**



**PRACTICAL NO.: 06**

**Title:**

Packet Firewall Implementation, Router Access Control List (ALC)

**Objective:**

To understand the router Firewall: Access Control List

**Theory:**

Packet filtering at the network level can be achieved by applying the Access Control Lists (ACLs) at the router called router firewall. ACLs at the router filter the inbound traffic while it permits or deny packets based on source IP/network and destination IP/network, IP, TCP, UDP protocol information. Generally, we use the ACLs to provide a basic level of security for accessing our network. Access lists can allow one host to access a part of network and prevent another host from accessing the same area.

A standard ACL can be used for several purpose. In this lab we will see how it can be used in controlling the unwanted network traffic. With standard ACL, we can define certain conditions for the network traffic passing through the router.

By default, router does not filter any traffic unless we manually configure an ACL. There are two types of ACLs:

1. **Standard ACL:** permits or denies packets based on source IP address.
   * Valid ACL ID range is: 1 - 99.
   * Applied closest to the destination.
   * Denies or permits

# Source IP Address

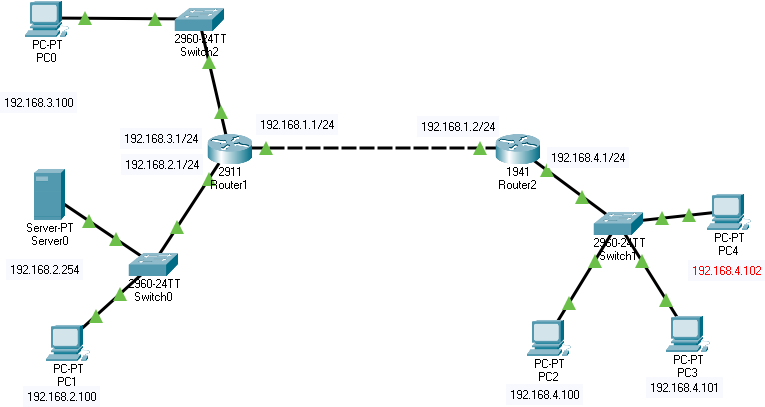
1. **Extended ACL:** it permits or denies packets based on source and destination IP address and also based on IP protocol information.
   * Valid Extended ACL ID range is: 100 - 199
   * Applied closest to the Source.
   * Denies or permits

# Source IP Address

* + - **Destination IP Address**

# Port or Service

Access lists of some protocols must be identified by a name, and access lists of other protocols must be identified by a number. Some protocols can be identified by either a name or a number. When a number is used to identify an access list, the number must be within the specific range of numbers that is valid for the protocol. Cisco Access Control Lists are the set of conditions grouped together by name or number. These conditions are used in filtering the traffic passing from router. Through these conditions we can filter the traffic; either when it enters in router or when it exits from router.

When creating an access list, we define criteria that are applied to each packet that is processed by the router; the router decides whether to forward or block each packet on the basis of whether or not the packet matches the criteria.

# Configurations

**Router 1 Configuration**

Router>enable Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Router(config)#interface gigabitEthernet 0/0 Router(config-if)#ip address 192.168.1.1 255.255.255.0 Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#interface gigabitEthernet 0/1 Router(config-if)#ip address 192.168.2.1 255.255.255.0 Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#interface gigabitEthernet 0/2 Router(config-if)#ip address 192.168.3.1 255.255.255.0 Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

Router(config-if)#exit Router(config)#

Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.1.2 Router(config)#

Router#

# Router 2 Configuration

Router> Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z. Router(config)#interface gigabitethernet 0/0

Router(config-if)#ip address 192.168.1.2 255.255.255.0 Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#interface gigabitEthernet 0/1 Router(config-if)#ip address 192.168.4.1 255.255.255.0 Router(config-if)#no shut down

Router(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)# Router(config-if)#exit Router(config)#

Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1

Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.1.1 Router(config)#

# Standard ACL Implementation

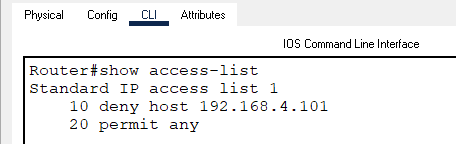
* 1. **Blocking a host (192.168.4.101) in the network 192.168.2.0**
     1. Create the access list (standard: 1-99)
        1. Specify more specific statements on the top
        2. Specify more general statements at the bottom
        3. Note that at the end of every access-list there is an implicit deny (eg. Access-list 1 deny any)
     2. Apply the access list to an interface (0utbound)

# Router 1 Configuration

* Deny (source ip address)
* Permit (any ipaddress)
* There is implicit deny (any address) at the end as the default which is not seen.

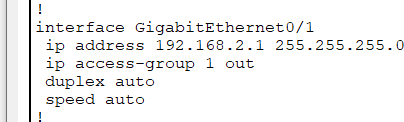
Router(config)#access-list 1 deny 192.168.4.100 0.0.0.0 Router(config)#access-list 1 permit any Router(config)#exit

Router#show access-list

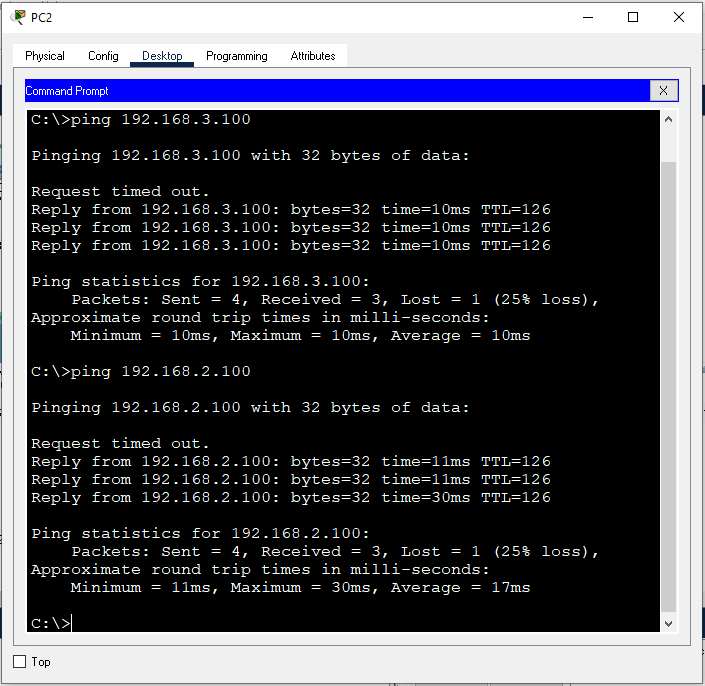
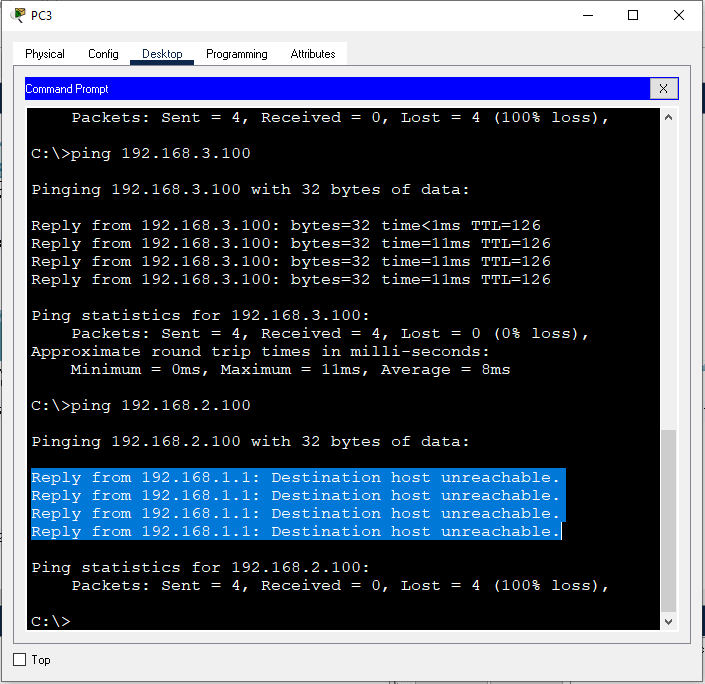


Router(config)#interface gigabitethernet 0/1 Router(config-if)#ip access-group 1 out Router(config-if)#exit

Router(config)#exit Router#

%SYS-5-CONFIG\_I: Configured from console by console Router#show run

# Verify the Connectivity



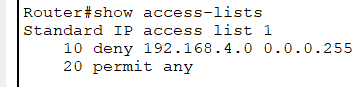
* 1. **Blocking a Network ( E.g 192.168.4.0)**

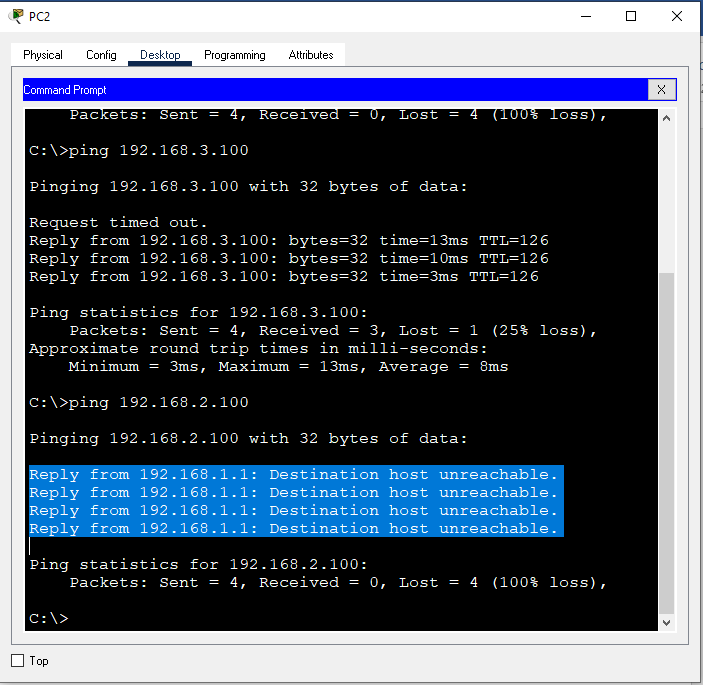
We should use wild mask (0.0.0.255) for the Class C network when we need to block the whole network e.g 192.168.4.0.

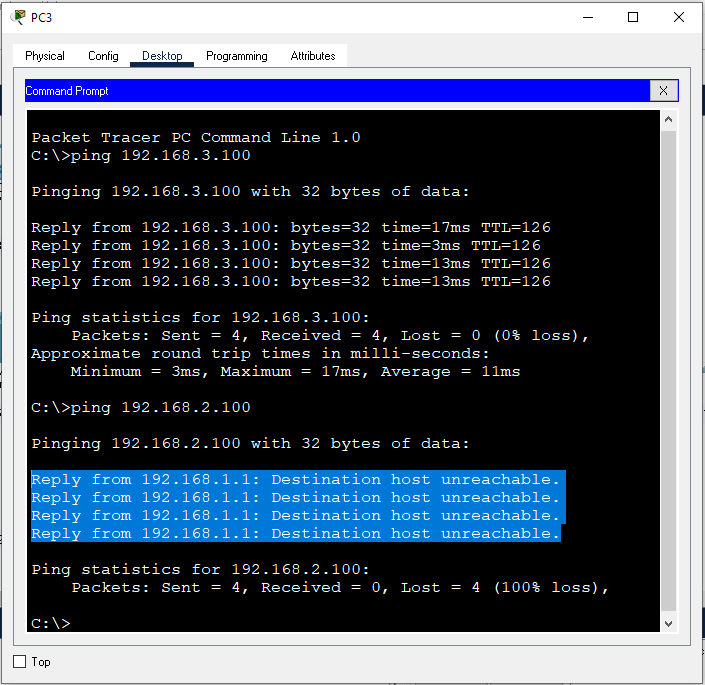
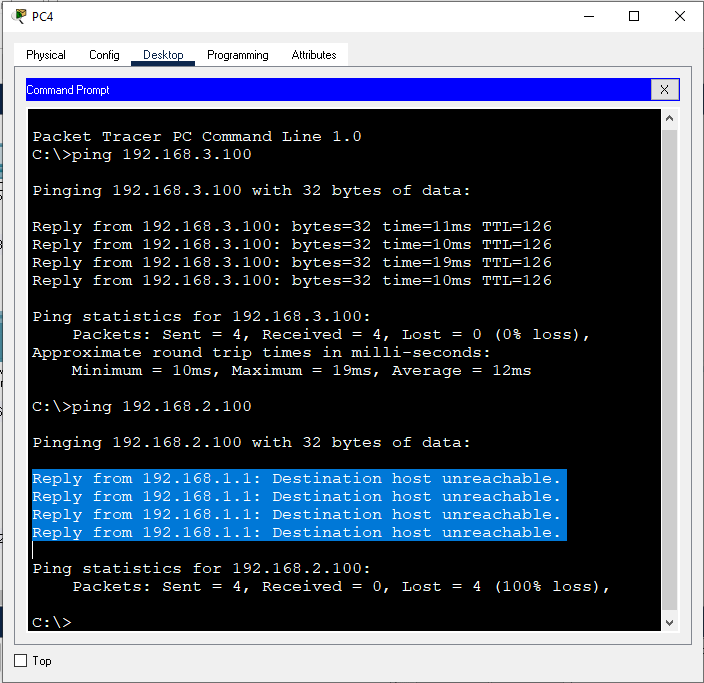
Router(config)#no access-list 1

Router(config)#access-list 1 deny 192.168.4.0 0.0.0.255 Router(config)#access-list 1 permit any Router(config)#exit

Router#show access-lists







# Extended ACL

* 1. Create an access-list (100-199)
* denies or permits port (service)
* denies or permits source IP Address
* denies or permits Destination IP Address
  1. Apply the access-list to an interface (inbound)

# Remove the Standard ACL from Router 1 Router 1

Router(config)#no access-list 1 Router(config)#interface gigabitEthernet 0/1 Router(config-if)#no ip access-group 1 out Router(config-if)#exit

Router(config)#exit

# Configure Extended ACL in Router 2 Router 2

* Deny (protocol-source-destination)
* Permit (protocol-any-any)
* There is implicit deny (protocol-any-any) at the end as the default which is not seen.

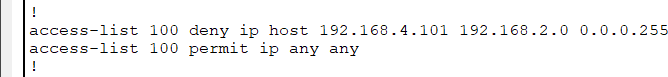
Router(config)#access-list 100 deny ip 192.168.4.101 0.0.0.0

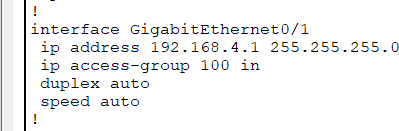
192.168.4.0 0.0.0.255

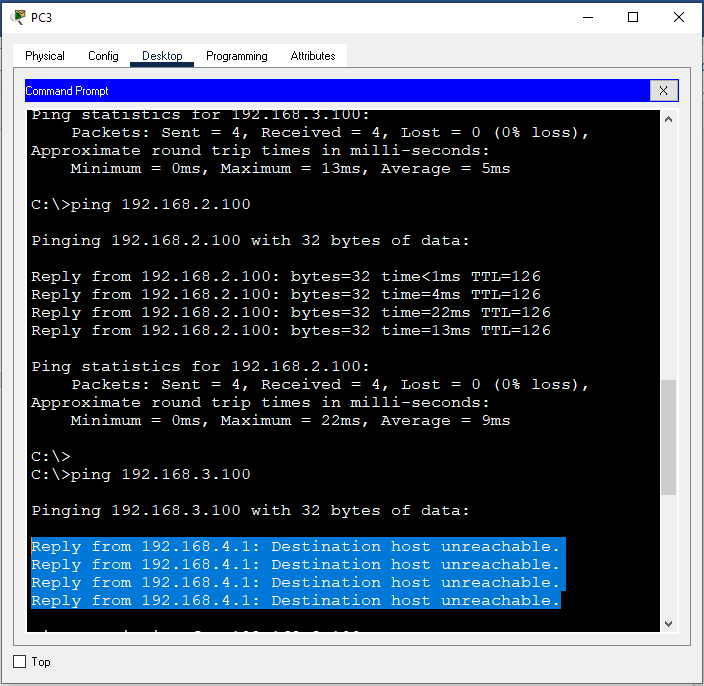
Router(config)#access-list 100 permit ip any any Router(config)#exit

Router#

Router(config)#interface gigabitEthernet 0/1 Router(config-if)#ip access-group 100 in Router(config-if)#exit







# Allow HTTP traffic but block ICMP (ping)

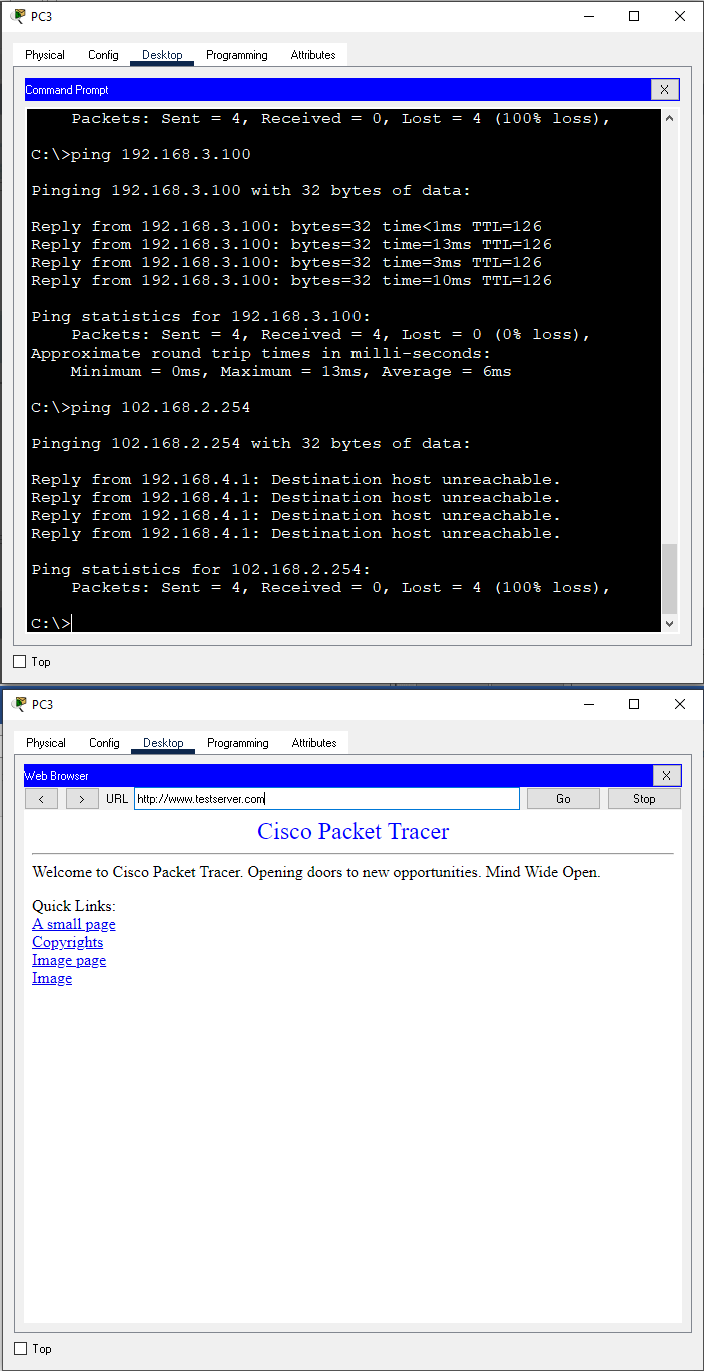
Router(config)#no access-list 100

Router(config)#access-list 100 deny icmp 192.168.4.101 0.0.0.0

192.168.2.254 0.0.0.0

Router(config)#access-list 100 permit ip any any Router(config)#

# Verify ACLs



**PRACTICAL NO.: 07**

**Title:**

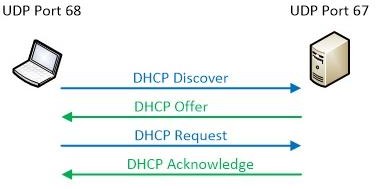
DHCP, WEB, DNS, EMSIL, FTP Server Confguration

**Objective:**

To understand the working principle of DHCP, WEB, DNS, EMSIL, FTP Server.

**Theory:**

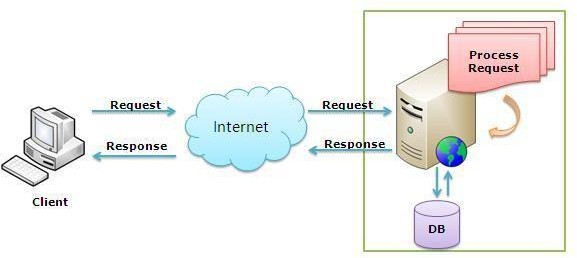
**DHCP:** Dynamic Host Configuration Protocol is a network management protocol that is used to dynamically assign the IP address and other information to each host on the network so that they can communicate efficiently. DHCP automates and centrally manages the assignment of IP address easing the work of network administrator. The DHCP also assigns the subnet masks, default gateway and domain name server (DNS) address and other configurations to the host and by doing so, it makes the task of network administrator easier. The DHCP client uses port 68 where as the server uses port 67 to connect to the DHCP client.



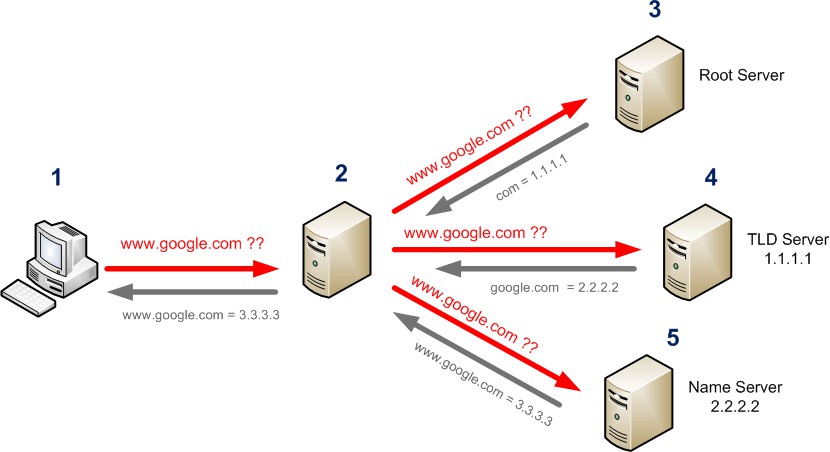
# Components of DHCP

1. **DHCP Server:** It is typically a server or a router that holds the network configuration information.
2. **DHCP Client:** It is the endpoint that gets the configuration information from the server like any computer or mobile.
3. **DHCP Relay Agent:** If you have only one DHCP Server for multiple LAN’s then the DHCP relay agent present in every network will forward the DHCP request to the servers. This because the DHCP packets cannot travel across the router. Hence, the relay agent is required so that DHCP servers can handle the request from all the networks.
4. **IP address pool:** It contains the list of IP address which are available for assignment to the client.
5. **Subnet Mask:** It tells the host that in which network it is currently present.
6. **Lease Time:** It is the amount of time for which the IP address is available to the client. After this time the client must renew the IP address.
7. **Gateway Address:** The gateway address lets the host know where the gateway is to connect to the internet.

**Web Server:** Web server generally refers to a website server, which refers to a program that resides on a certain type of computer on the Internet. It can provide documents to Web clients such as browsers, and can also place website files for the world to browse; data files can be placed for all World download. The three most popular Web servers are Apache and Microsoft's Internet Information Services (Internet Information Services, IIS). HTTP uses port 80 for connection where as HTTPS uses port 443.



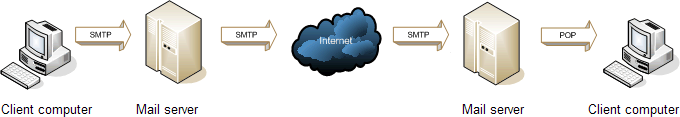
**DNS:** DNS is an essential part of the Internet which manages to translate all the inquiries into IP addresses and can identify different devices that are connected to the network. Apart from translating hostnames to IP addresses (A and AAAA DNS records), DNS also has many different functions like defining port in use, connecting services to domains, authentication of emails.



# Components of DNS

1. **Domain Namespace**: It is a tree-like hierarchy structure that divides hostnames into smaller pieces called domains. They are further divided into more categories: top-level domains, second-level domains, and subdomains.
2. **Authoritative DNS servers**: Such a server has the main information – the zone file. It has all the DNS records, and all the changes to the records happen inside it. It has the most accurate information for a hostname.
3. **Recursive DNS servers:** Those servers will have a temporary memory where they store DNS records. They have a mechanism for synchronizing with the authoritative nameserver and updating the information. The advantage is that they can be many, located in different regions, and provide redundancy and speed.
4. **DNS Query:** Each request comes from a device that demands a DNS record. It is a question that runs from one recursive server to another in search of the answer.
5. **DNS Records:** Domain name system keeps information in so-called DNS records. They are text documents with various purposes like A Record, SPF record, CNAME record, etc.

**Mail 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.

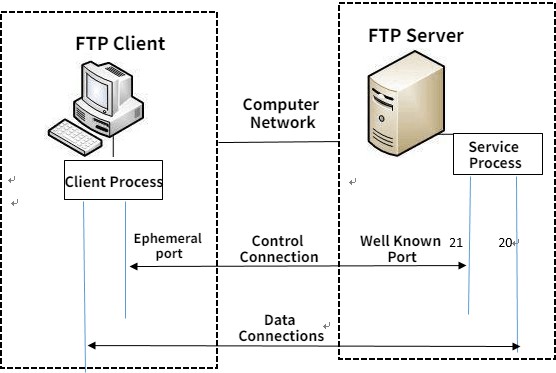


# SMTP, POP3 and IMAP4

* 1. **SMTP (Simple Mail Transfer Protocol)** is a protocol that is used when e-mails are delivered from clients to servers and from servers to other servers. It uses port 25, 2525 and 465.
  2. **POP3 (Post Office Protocol version 3)** is used to retrieve email from the servers. It uses port 110 and 995.
  3. **IMAP4 (Internet Message Access Protocol Version 4)** is a further development of the POP3 protocol and is used to read e-mail from mail servers. IMAP4 is not used as much as POP3, but many modern mail servers have support for IMAP4. It uses por 143 and 993

**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.

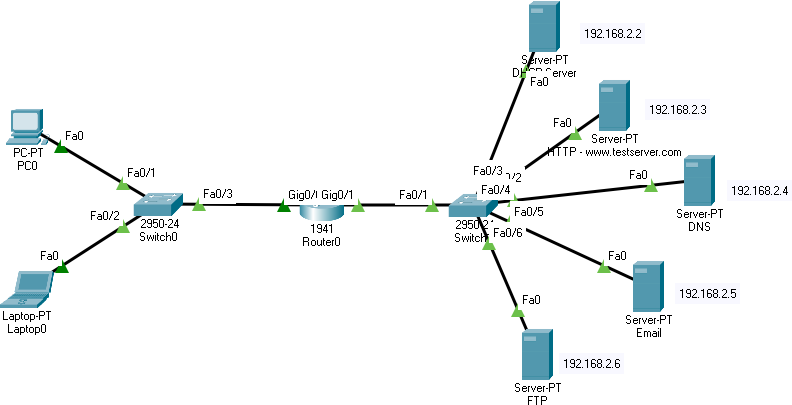
FTP Uses:

1. TCP port 20 for data connection
2. TCP port 21 for command connection

# Modes

* 1. **Active Mode**—The client issues a PORT command to the server signaling that it will

“actively” provide an IP and port number to open the Data Connection back to the client.

* 1. **Passive Mode**—The client issues a PASV command to indicate that it will wait “passively” for the server to supply an IP and port number, after which the client will create a Data Connection to the server.

# Configurations

**Steps to Follow**

* Make the LAN
* Connect All Cables
* Make sure to remember all ports you connect cable to

# Router Interface Configuration

* Go to router and assign static ip addresses

Router>enable Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z. Router(config)#int g0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0 Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#int g0/1

Router(config-if)#ip address 192.168.2.1 255.255.255.0 Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

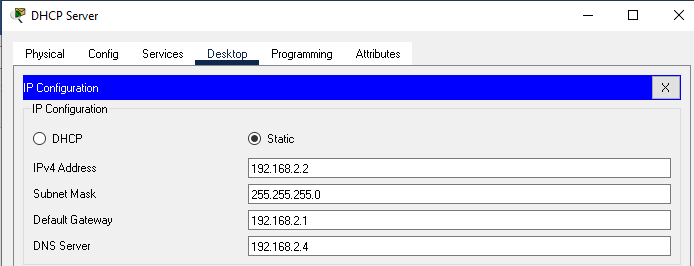
# DHCP helper configuration in the Router

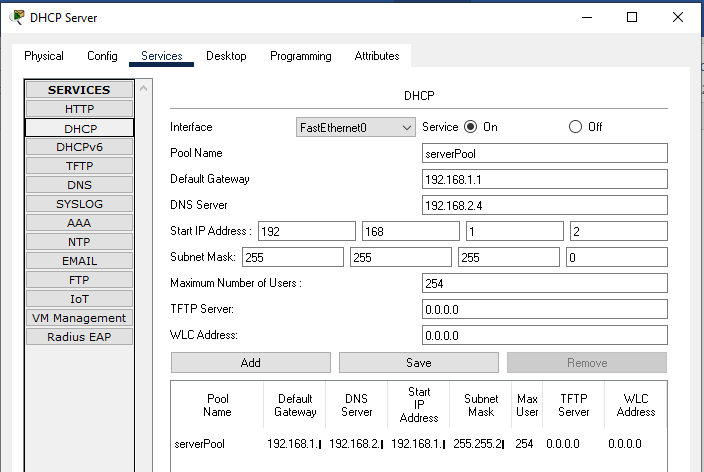
* Enable ip helper-address in the router for DHCP

Router(config-if)#int g0/0

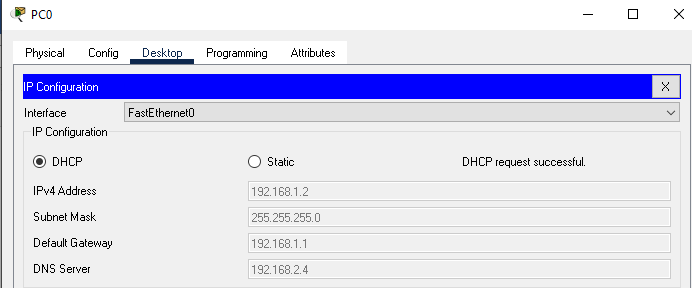
Router(config-if)#ip helper-address 192.168.2.2 Router(config-if)#

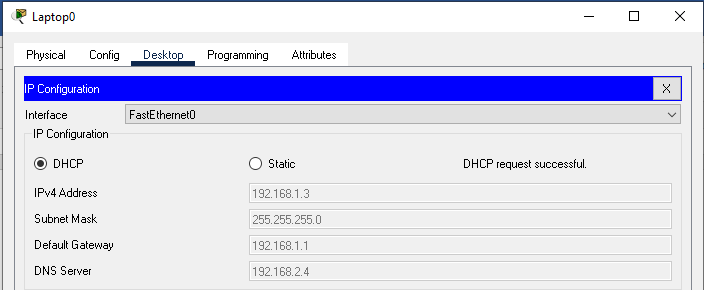
# DHCP Server Configuration

* Assign the static ip address to the server
* Turn ON the DHCP service and create the server pool as follows

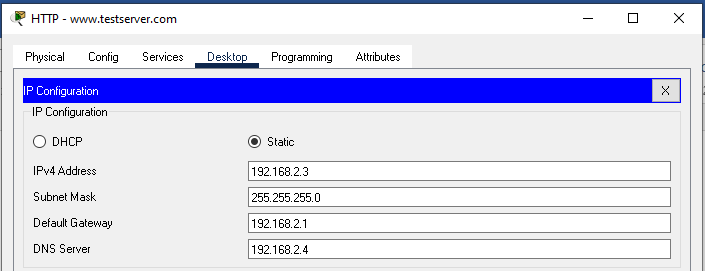


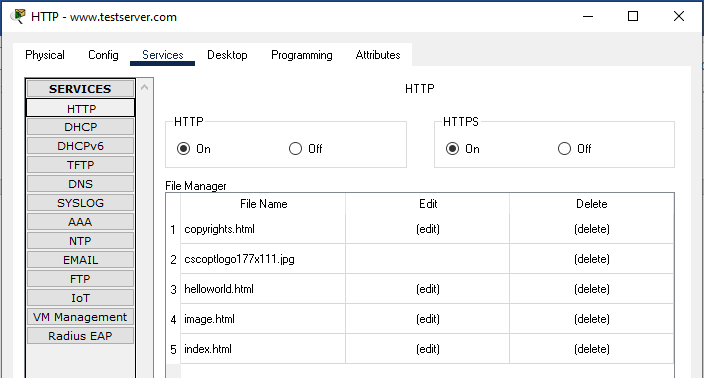
# Assign Dynamic IP Configuration to PC0 and Laptop0

* Go to PC0>Desktop>IP Configuration then select DHCP
* Go to Laptop0>Desktop>IP Configuration then select DHCP

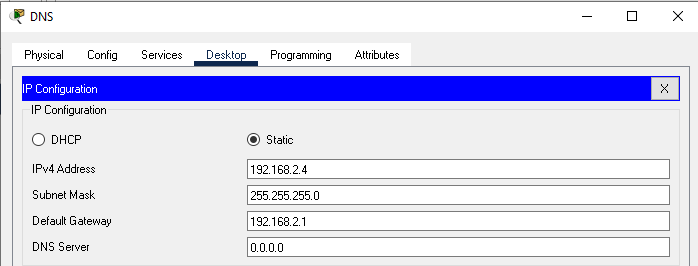


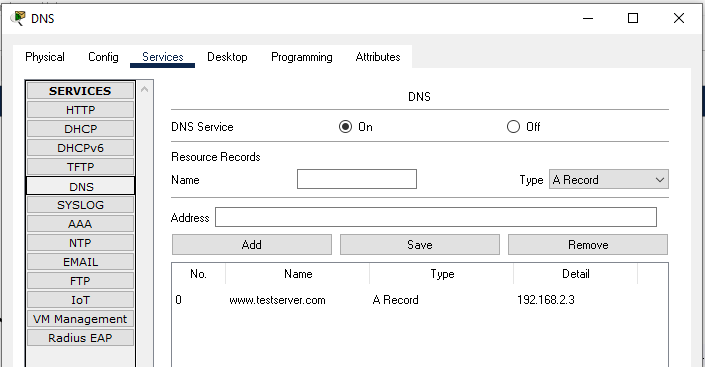
# HTTP Server

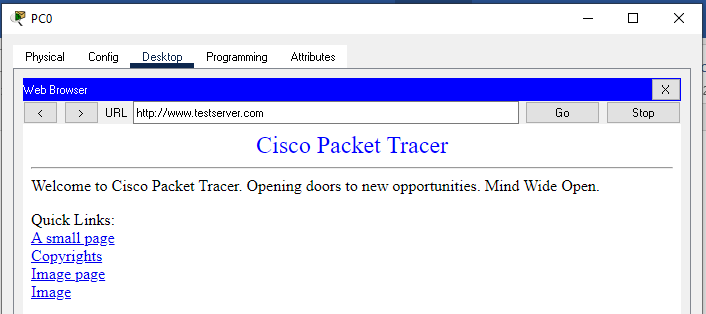
* Assign static ip address to the HTTP server
* Make sure to turn ON the HTTP Service



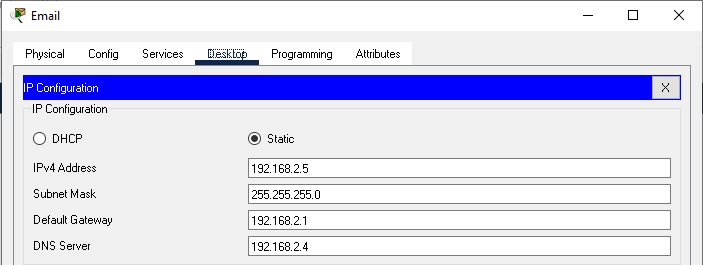
# DNS Server Configuration

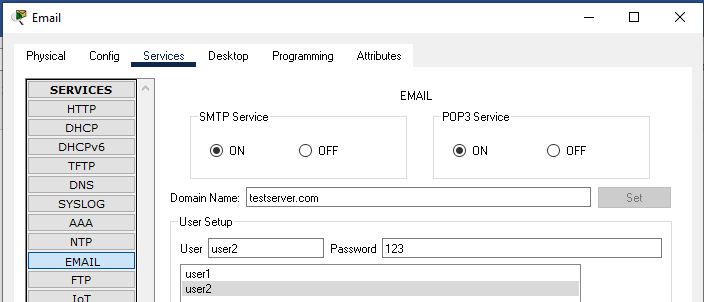
* Assign the static ip address to the DNS server
* Add DNS Records of the domain name (eg. www.testserver.com)

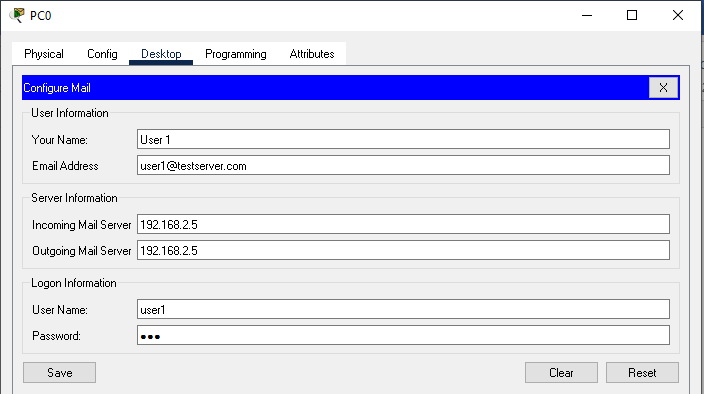
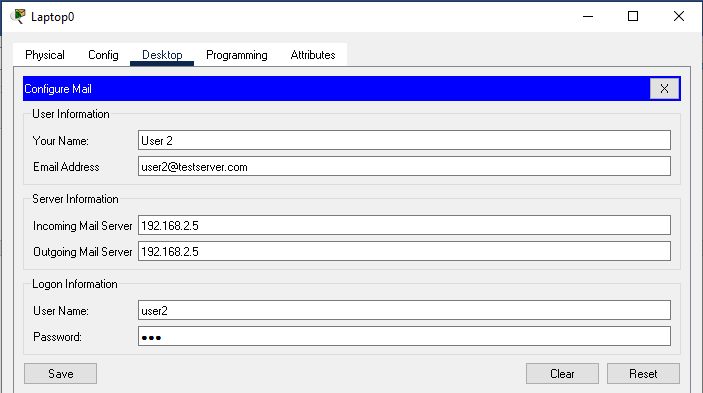


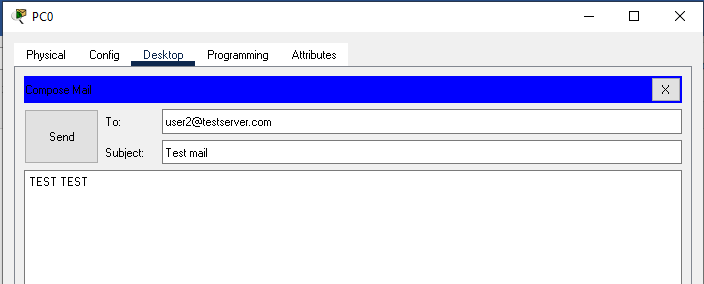
* Go to PC0>Desktop>Web browser and open the url

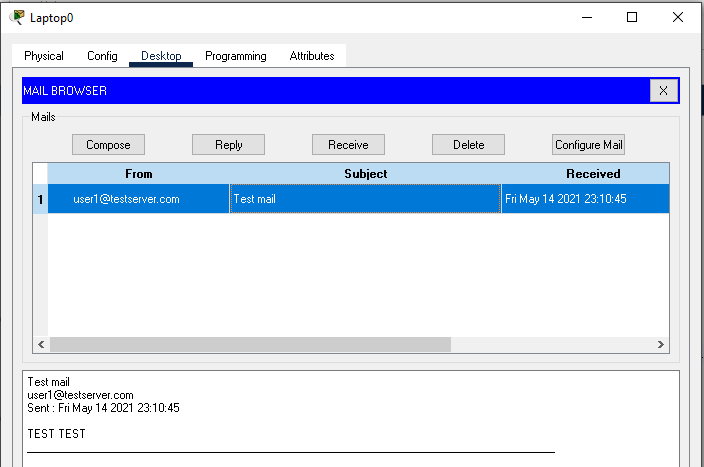
# EMAIL Server Configuration

* Assign the static ip address to the EMAIL server
* Turn ON the SMTP and POP3 services and create two users

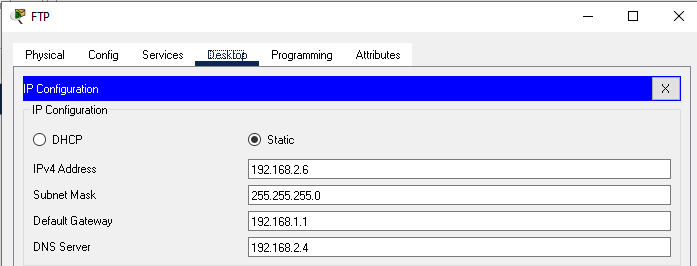


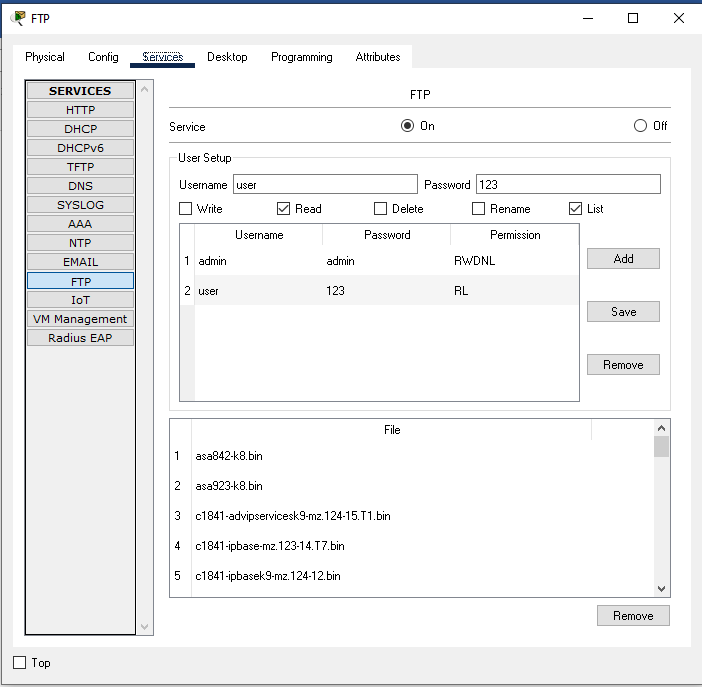
* Go to PC0>Email>Configure user as follows
* Go to Laptop0>Email and create user account as follows
* Go to PC0>Desktop>Email and compose the email as follows

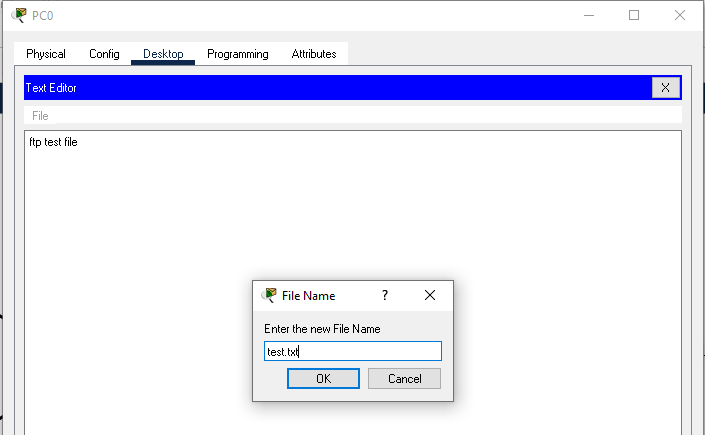


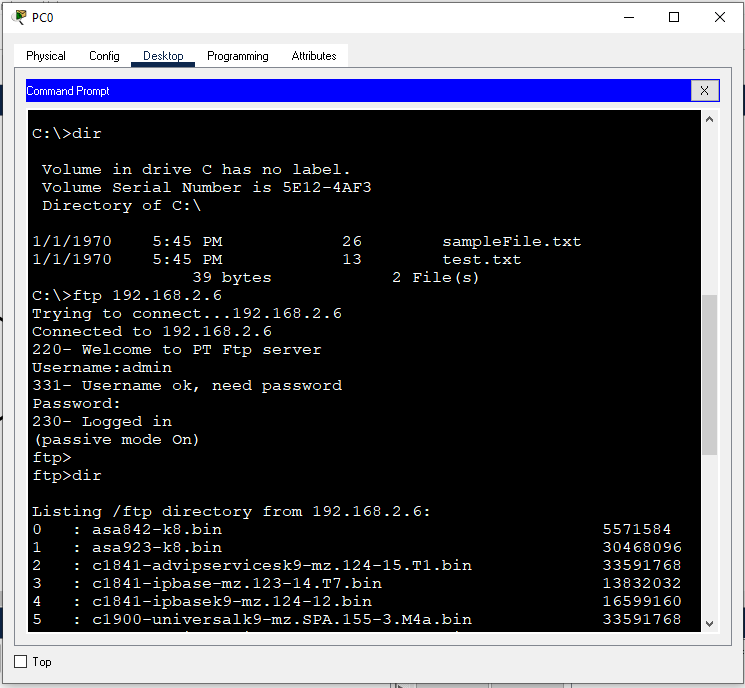
* Go to Laptop0>Desktop>Email and check (receive) email as follows

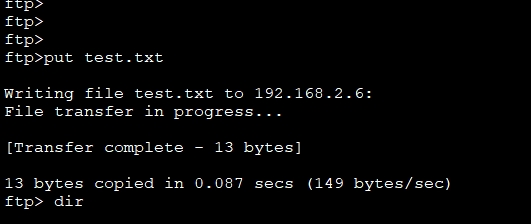
# FTP Server Configuration

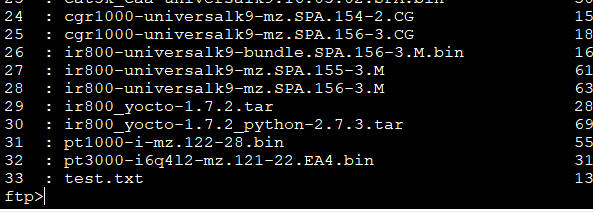
* Assign static ip address to the FTP server as follows
* Enable the FTP service and create two users: admin (with write ,read, delete, rename, list options) and user (with read and list only)



* Go to PC0>Desktop>Text Editor, create a file **test.txt** and save it on the desktop
* Go to Desktop>Command Prompt and verify the created file using **dir** command then login into the ftp server as follows using admin user and password



* Use **PUT** command to upload **test.txt** into the FTP Server as follows:
* Verify the uploaded file using the command **dir**



* Go to Laptop0>Desktop>Command Prompt, connect to the FTP server using user account and password and use **GET** command to download file **test.txt** into the desktop. After the transfer type **dir** command to verify it.

