

Table of Contents

Lab No.	Description (Title)	Signature
1	Overview of Networks and layered communications, understanding of Network equipment, wiring in details.	
2	CAT6 UTP EIA/TIA 568A/B straight and cross-over wiring, testing	
3	Basic Networking commands	
4	Overview of IP Addressing and sub-netting, static ip setting on machine, testing	
5	Introduction to Packet Tracer, creating of a LAN and connectivity test in the LAN.	
6	Implementation of Dynamic/Interior/Exterior routing (RIP, OSPF, BGP)	
7	Firewall Implementation, Router Access Control List (ACL)	
8	DNS, Web, FTP server configuration	

LAB 1

Overview of Networks and layered communication, understanding of networking equipment.

Objectives:

- To understand layered communications and protocols.
- To learn about networking equipment's like repeater, hub, switch, router, bridge, gateway.

Protocol:

A protocol is a collection of guidelines that controls how computers on a network communicate with one another. These rules include guidelines that regulate the following characteristics of a network:

- Access method
- Allowed physical topologies
- Types of cabling
- Speed of data transfer

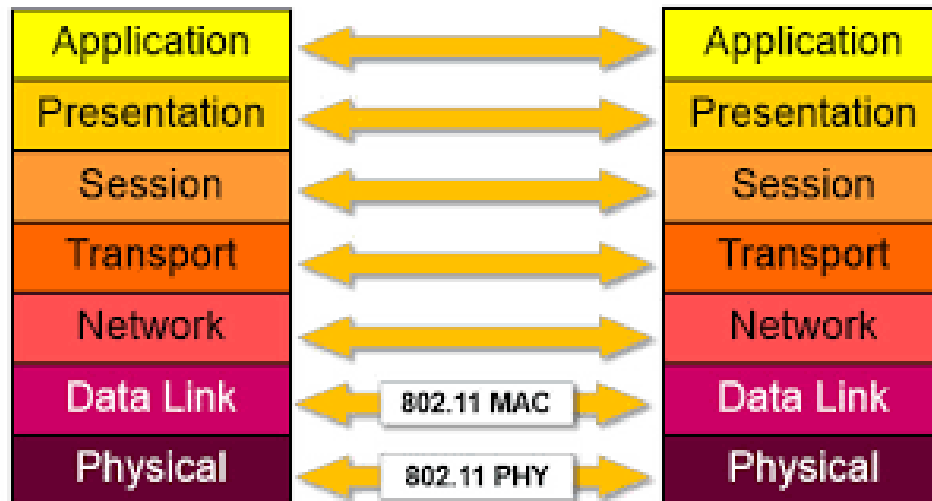
Layered Communication:

Computers use a complex system of protocols to communicate. Layers divide the work that a network performs. A hierarchy of protocol configurations is used in networks to segment the communication task into different layers. The OSI reference model is the primary illustration of layered communication.

OSI Layer:

A network is organized into seven layers (a protocol stack) according to the OSI reference model. These layers specify how data is handled and transferred across a network by networking hardware and software. When the protocol stack of one workstation or peripheral

device and that of another are compatible, interoperability—the goal of defining a standard protocol model—occurs. Communication between each layer and its equivalent layer on a receiving station is possible.



- **Physical Layer** – consists of rules for dealing with hardware, such as voltages, bit rates, frequencies, etc. The medium is below this and not given an actual layer assignment. For example: Network Interface Cards (NICs), Repeaters and Hubs.
- **Data-Link Layer** - this layer communicates using chunks of data called frames. The data-link layer can perform error checking and control the rate of flow of information. The data link layer is for a wire with just two ends, one sender and one receiver. For example: Bridges and Switches manipulate data in the Data-Link Layer.
- **Network Layer** - The network layer deals with addresses and provides message or **packet routing**. (Note: packets are like frames, but in the network layer.) Because not all devices are directly connected to each other, some packets may have to take several **hops** to get from source to destination. Finding a route for packets in a potentially large and changing network is the job of the network layer. **IP** is a network layer protocol, and **IP address** is what IP uses to determine where a packet should go. **Logical network addressing and routing occur in the Network Layer. Routers and Layer 3 switches are devices that operate at the Network layer.**
- **Transport Layer** - The transport layer provides reliable, transparent transfer of data between computers on a network. The transport layer is the lowest layer to provide and end-to-end view of the communication. The transport layer may have to break the

data into packets for the network layer. It is then the transport layer's job to make sure they are reassembled in the right order. The interaction between the end-to-end view of this layer and the machine-to-machine view of the network layer is probably the most critical one in the hierarchy. **TCP** is a transport protocol. Actually, both **TCP** and **IP** are part of the **TCP/IP model** instead of the OSI model. The TCP/IP model owes its success (and its name) to these two hardworking protocols, despite definitions in other layers in the TCP/IP model that are weaker than those in the OSI model. **TCP/IP and IPX/SPX Protocols are active at the Transport Layer.**

- **Session Layer** - The session layer provides remote logons and some other things. Many software developers have considered this layer fairly useless and simply absorb any needed functions into their application programs. Different network operating systems (Novell, WindowsNT) utilize this layer for different purposes.
- **Presentation Layer** - The presentation layer is also frequently bypassed, but it can provide translation of data transferred between applications. If data from a spreadsheet needs to be converted to data for a database, this happens at the presentation layer.
- **Application Layer** - The application layer contains communication services that include file transfer and message handling like Telnet, FTP, and email. These services then interact with other applications such as word processing, databases, and World Wide Web browsers.

Network Hardware:

Network hardware is a set of physical or network devices that are essential for interaction and communication between hardware units operational on a computer network. These are dedicated hardware components that connect to each other and enable a network to function effectively and efficiently.

Repeater:

Repeaters are simple devices that work at the physical layer of the OSI. It regenerates the signals.

Hub:

A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices. Network hubs are best suited for small, simple local area network (LAN) environments.



There are mainly two types of hubs:

1. **Passive:** The signal is forwarded as it is.
2. **Active:** The signal is amplified, so they work as repeaters.

Switch:

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s). It supports unicast, multicast as well as broadcast communications.



Most common switching methods are:

1. **Cut-through:** Directly forward what the switch gets.
2. **Store and forward:** receive the full frame before retransmitting it.

Normal Switches are on the data link layer (just above physical layer), that's why they deal with frames instead of bits and filter them based on MAC addresses. Switches are known to be used for their filtering capabilities. Intelligent switches work as a router.

Virtual LANs:

VLANs (Virtual LANs) and broadcast domains: Switches do not control broadcast domains by default, however, if a VLAN is configured in a switch it shall have its own broadcast domain.

VLAN is a logical group of network devices located on different LAN physical segments. However, they are logically treated as if they were located on a single segment.

Bridges:

Bridges are used to extend networks by maintaining signals and traffic. Bridges are on the data link layer so in principle they are capable to do what switches do like data filtering and separating the collision domain, but they are less advanced. They are known to be used to extend distance capabilities of networks.

In a comparison with switches, bridges are slower because they use software to perform switching. They do not control broadcast domains and usually come with a smaller number of ports. Multiport bridges are generally termed as switch.

Routers:

Routers are used to connect different LANs or a LAN with a WAN (e.g. the internet). Routers control both collision domains and broadcast domains. If the packet's destination is on a different network, a router is used to pass it the right way, so without routers, the internet could not function. Routers use NAT (Network Address Translation) in conjunction with IP Masquerading to provide the internet to multiple nodes in the LAN under a single IP address.

Routers work on the network layer so they can filter data based on IP addresses. They have routing tables to store network addresses and forward packets to the right port.



Gateway:

Gateways are very intelligent devices or else can be a computer running the appropriate software to connect and translate data between networks with different protocols or architecture, so their work is much more complex than a normal router. For instance, allowing communication between TCP/IP clients and IPX/SPX or AppleTalk. Gateways operate at the network layer and above, but most of them at the application layer.

LAB 2

CAT 6 UTP EIA/TIA 568A/B straight and crossover wiring and testing

Objectives:

- To understand the color-coding standard of UTP cable.
- To create straight and crossover cable and test its connectivity.

Apparatus:

- UTP CAT 6 Cable, RJ45, Crimper, LAN Tester.





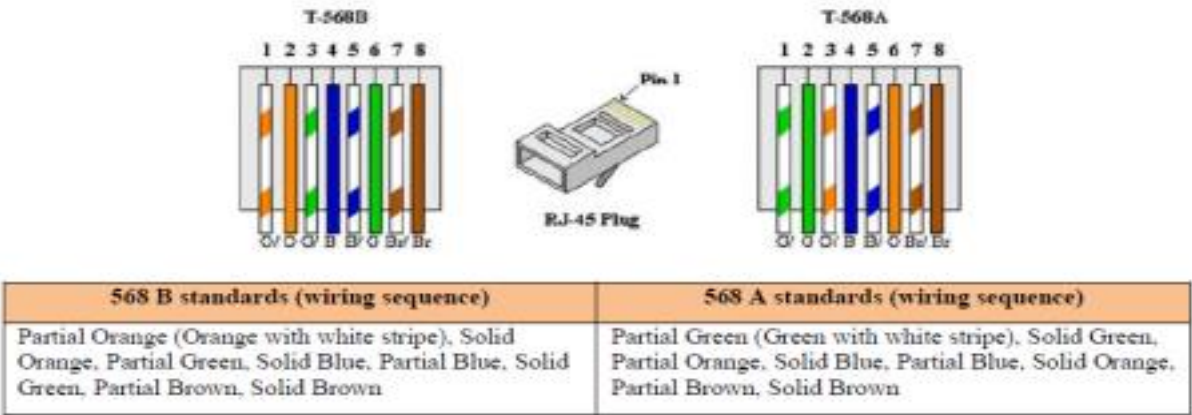
Steps:

1. Begin by stripping the outer covering from the end of cable.
2. Once you remove the outer covering, you need to untwist the twisted pair cables.
3. Once all the twisted pairs are untwisted pull them back and cut the exposed plastic core.
4. After that, straighten the wires.
5. Once all the wires have been straightened, arrange the wires in the order they need to be connected.
6. After arranging insert the wire into the RJ-45 connector and check if it is completely inserted.
7. After checking, clamp the wire in place using the clammer.
8. Repeat the above step for the next end.
9. Test for proper connectivity using LAN Tester.

Things to remember:

- Once the connector is clamped it cannot be reused.
- The order is followed from left to right.

- Odd number always holds partial color and even number contains solid color.
- The Standards are:



- The wire is said to be properly connected if the LAN Tester shows the proper sequence while testing.

LAB 3

Basic Networking commands

Objectives:

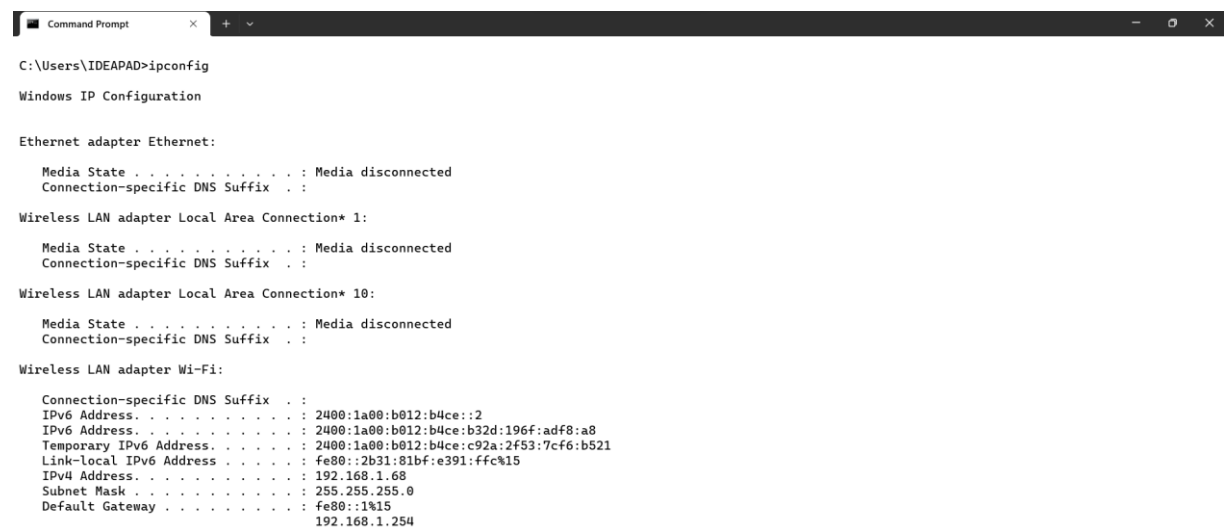
- To understand the basic Networking commands

Apparatus:

- Linux or Windows OS, terminal

Ipconfig:

ipconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed.



```
Command Prompt
C:\Users\IDEAPAD>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2400:1a00:b012:b4ce::2
    IPv6 Address. . . . . : 2400:1a00:b012:b4ce:b32d:196f:adf8:a8
    Temporary IPv6 Address. . . . . : 2400:1a00:b012:b4ce:c92a:2f53:7cf6:b521
    Link-local IPv6 Address . . . . . : fe80::2b31:81bf:e391:ffc%15
    IPv4 Address. . . . . : 192.168.1.68
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%15
                                192.168.1.254
```

Ipconfig /all:

Ipconfig /all is used to show all ip addresses and mac addresses of the computer.

```

Command Prompt

C:\Users\IDEAPAD>ipconfig/all

Windows IP Configuration

    Host Name . . . . . : DESKTOP-AVDJOCB
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Realtek PCIe GbE Family Controller
    Physical Address. . . . . : 7C-8A-E1-93-C7-A5
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Physical Address. . . . . : 92-0F-0C-E4-37-A3
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Physical Address. . . . . : 92-0F-0C-E4-37-B3
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . :
    Description . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
    Physical Address. . . . . : 98-0F-0C-E4-37-93
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv6 Address. . . . . : 2400:1a00:b012:b4ce::2(Preferred)
    Lease Obtained. . . . . : Saturday, July 8, 2023 1:40:28 PM
    Lease Expires . . . . . : Saturday, July 8, 2023 2:00:28 PM
    IPv6 Address. . . . . : 2400:1a00:b012:b4ce:b32d:196f:adf8:a8(Preferred)
    Temporary IPv6 Address. . . . . : 2400:1a00:b012:b4ce:c92a:2f53:7cf6:b521(Preferred)
    Link-local IPv6 Address . . . . : fe80::2b31:81bf:e391:ffc%15(Preferred)
    IPv4 Address. . . . . : 192.168.1.68(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Wednesday, July 5, 2023 5:50:13 PM
    Lease Expires . . . . . : Sunday, July 9, 2023 1:40:26 PM
    Default Gateway . . . . . : fe80::1%15
                                192.168.1.254
    DHCP Server . . . . . : 192.168.1.254
    DHCPv6 IAID . . . . . : 294653708
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-36-C1-25-7C-8A-E1-93-C7-A5
    DNS Servers . . . . . : 2400:1a00:0:32::165
                                2400:1a00:8000:4::73
                                192.168.1.254
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\IDEAPAD>

```

Ping:

Ping is used to send a packet to the ip address and wait for a response.

```

Command Prompt

C:\Users\IDEAPAD>ping youtube.com

Pinging youtube.com [2404:6800:4002:806::200e] with 32 bytes of data:
Reply from 2404:6800:4002:806::200e: time=20ms
Reply from 2404:6800:4002:806::200e: time=21ms
Reply from 2404:6800:4002:806::200e: time=21ms
Reply from 2404:6800:4002:806::200e: time=21ms

Ping statistics for 2404:6800:4002:806::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 21ms, Average = 20ms

C:\Users\IDEAPAD>

```

Traceroute:

tracert<ip> is used to trace route.

```
Command Prompt

C:\Users\IDEAPAD>tracert google.com

Tracing route to google.com [2404:6800:4002:823::200e]
over a maximum of 30 hops:

  1    1 ms    1 ms    1 ms    2400:1a00:b012:b4ce::1
  2    4 ms    6 ms    7 ms    2400:1a00:b1a7::1
  3    6 ms    3 ms    3 ms    2400:1a00:0:45::46
  4    *        *        *        Request timed out.
  5    4 ms    5 ms    6 ms    2400:1a00:0:41::136
  6   11 ms   11 ms    6 ms    2400:1a00:0:41::139
  7    6 ms    7 ms    7 ms    2400:1a00:dccc:1:72:9:128:66
  8   22 ms   21 ms   21 ms    2400:1a00:dccc:1:72:9:128:33
  9   20 ms   22 ms   21 ms    2001:4860:1:1::28d0
 10   23 ms   23 ms   25 ms    2404:6800:803d::1
 11   22 ms   24 ms   23 ms    2001:4860:0:1::1824
 12   22 ms   20 ms   22 ms    2001:4860:0:1::53a1
 13   23 ms   21 ms   22 ms    del12s06-in-x0e.1e100.net [2404:6800:4002:823::200e]

Trace complete.

C:\Users\IDEAPAD>
```

What is my IP?

It is used to get public IP of your gateway.

Arp -a:

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

```
Command Prompt

C:\Users\IDEAPAD>arp -a

Interface: 192.168.1.68 --- 0xf
 Internet Address      Physical Address      Type
 192.168.1.254         04-75-f9-a4-ca-a0    dynamic
 192.168.1.255         ff-ff-ff-ff-ff-ff    static
 224.0.0.2             01-00-5e-00-00-02    static
 224.0.0.22            01-00-5e-00-00-16    static
 224.0.0.251           01-00-5e-00-00-fb    static
 224.0.0.252           01-00-5e-00-00-fc    static
 239.255.255.250       01-00-5e-7f-ff-fa    static
 255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\IDEAPAD>
```

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.

```
Command Prompt
C:\Users\IDEAPAD>hostname
DESKTOP-AVDJOCB
C:\Users\IDEAPAD>
```

Nslookup:

nslookup is a network administration command-line tool available in 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".

```
Command Prompt - nslookup
C:\Users\IDEAPAD>nslookup
Default Server:  vip6-safenet-kmd01.wlink.com.np
Address:  2400:1a00:0:32::165
>
```

Netstat:

It is used to show all ip addresses and ports that are being used by the computer.

```
Command Prompt - netstat
C:\Users\IDEAPAD>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:53417          DESKTOP-AVDJOCB:53796  ESTABLISHED
TCP    127.0.0.1:53773          DESKTOP-AVDJOCB:65001  ESTABLISHED
TCP    127.0.0.1:53796          DESKTOP-AVDJOCB:53417  ESTABLISHED
TCP    127.0.0.1:65001          DESKTOP-AVDJOCB:53773  ESTABLISHED
TCP    192.168.1.68:53774       20.198.119.143:https   ESTABLISHED
TCP    192.168.1.68:53865       103.180.115.7:https    TIME_WAIT
TCP    192.168.1.68:53867       31:https               TIME_WAIT
TCP    192.168.1.68:53872       server-108-158-245-24:https TIME_WAIT
TCP    192.168.1.68:53873       239:https              TIME_WAIT
TCP    192.168.1.68:53885       server-18-164-188-105:https TIME_WAIT
TCP    192.168.1.68:53887       194:https              TIME_WAIT
TCP    192.168.1.68:53893       112:https              TIME_WAIT
TCP    192.168.1.68:53895       server-108-158-244-162:https TIME_WAIT
TCP    192.168.1.68:53896       server-18-164-246-12:https TIME_WAIT
TCP    192.168.1.68:53898       a12b7a488abeaa9e4:https TIME_WAIT
TCP    192.168.1.68:53900       192:https              TIME_WAIT
TCP    192.168.1.68:53901       server-18-164-246-77:https TIME_WAIT
TCP    192.168.1.68:53903       ec2-52-74-226-183:https TIME_WAIT
TCP    192.168.1.68:53904       113:https              TIME_WAIT
TCP    192.168.1.68:53906       139:https              TIME_WAIT
TCP    192.168.1.68:53907       50:https               TIME_WAIT
TCP    192.168.1.68:53910       50:https               TIME_WAIT
TCP    192.168.1.68:53913       ec2-18-143-106-89:https TIME_WAIT
TCP    192.168.1.68:53923       137:https              TIME_WAIT
TCP    192.168.1.68:53925       ec2-54-151-187-164:https TIME_WAIT
TCP    192.168.1.68:53926       ec2-18-141-29-20:https  TIME_WAIT
TCP    192.168.1.68:53934       server-108-158-236-179:https TIME_WAIT
TCP    192.168.1.68:53935       104.18.24.185:https    TIME_WAIT
```

Systeminfo:

It is used to show all information about the computer

```
Command Prompt
C:\Users\IDEAPAD>systeminfo

Host Name:                DESKTOP-AVDJOCB
OS Name:                  Microsoft Windows 11 Home
OS Version:               10.0.22621 N/A Build 22621
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         LENOVO
Registered Organization:
Product ID:                00325-82214-76215-AAOEM
Original Install Date:     1/25/2023, 10:10:49 PM
System Boot Time:          7/5/2023, 5:49:59 PM
System Manufacturer:       LENOVO
System Model:              82K2
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3301 Mhz
BIOS Version:              LENOVO H3CN30WW(V2.00), 6/28/2021
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:45) Mathmandu
Total Physical Memory:      7,532 MB
Available Physical Memory:  2,659 MB
Virtual Memory: Max Size:  15,212 MB
Virtual Memory: Available:  5,573 MB
Virtual Memory: In Use:     9,639 MB
Page File Location(s):     C:\pagefile.sys
Domain:                     WORKGROUP
Logon Server:               \\DESKTOP-AVDJOCB
Hotfix(s):                  4 Hotfix(s) Installed.
                           [01]: KB5027119
                           [02]: KB5012170
                           [03]: KB5027231
                           [04]: KB5026549
Network Card(s):           2 NIC(s) Installed.
                           [01]: Realtek PCIe GbE Family Controller
                           Connection Name: Ethernet
                           Status: Media disconnected
                           [02]: MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
                           Connection Name: Wi-Fi
                           DHCP Enabled: Yes
                           DHCP Server: 192.168.1.254
                           IP address(es)
                           [01]: 192.168.1.68
                           [02]: fe80::2b31:81bf:e391:ffc
                           [03]: 2400:1a00:b012:b4ce:c92a:2f53:7cf6:b521
                           [04]: 2400:1a00:b012:b4ce:b32d:196f:adf8:a8
                           [05]: 2400:1a00:b012:b4ce::2
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.

C:\Users\IDEAPAD>
```

Route print:

It is used to show all ip addresses and ports that are being used by the computer

```
Command Prompt

C:\Users\IDEAPAD>route print

=====
Interface List
16...7c 8a e1 93 c7 a5 .....Realtek PCIe GbE Family Controller
2...92 0f 0c e4 37 a3 .....Microsoft Wi-Fi Direct Virtual Adapter
7...92 0f 0c e4 37 b3 .....Microsoft Wi-Fi Direct Virtual Adapter #2
15...90 0f 0c e4 37 93 .....MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.254     192.168.1.68     35
127.0.0.0                  255.0.0.0        On-link           127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link           127.0.0.1        331
127.255.255.255            255.255.255.255  On-link           127.0.0.1        331
192.168.1.0                255.255.255.0    On-link           192.168.1.68     291
192.168.1.68               255.255.255.255  On-link           192.168.1.68     291
192.168.1.255              255.255.255.255  On-link           192.168.1.68     291
224.0.0.0                  240.0.0.0        On-link           127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link           192.168.1.68     291
255.255.255.255            255.255.255.255  On-link           127.0.0.1        331
255.255.255.255            255.255.255.255  On-link           192.168.1.68     291
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
15 4131 ::/0                  fe80::1
1 331 ::1/128                On-link
15 4131 2400:1a00:b012:b4ce::/64 On-link
15 51 2400:1a00:b012:b4ce::/64 fe80::1
15 291 2400:1a00:b012:b4ce::2/128
    On-link

15 291 2400:1a00:b012:b4ce:b32d:196f:adf8:a8/128
    On-link
15 291 2400:1a00:b012:b4ce:c92a:2f53:7cf6:b521/128
    On-link
15 291 fe80::/64                On-link
15 291 fe80::2b31:81bf:e391:ffc/128
    On-link
1 331 ff00::/8                 On-link
15 291 ff00::/8                 On-link
=====
Persistent Routes:
None

C:\Users\IDEAPAD>
```


LAB 4

Overview of IP Addressing and Sub-Netting.

Objective:

- To understand theoretical knowledge of IPv4 addressing and sub-netting

Overview:

Subnetting:

Subnetting is the practice of dividing a network into two or smaller networks. It increases routing efficiency, which helps to enhance the security of the network and reduces the size of the broadcast domain.

IP Subnetting designates high-order bits from the host as part of the network prefix. This method divides a network into smaller subnets.

IPv4 Classes:


Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 — 127	0XXXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24} - 2$	2^7
Class B	128 — 191	10XXXXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16} - 2$	2^{14}
Class C	192 — 223	110XXXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^8 - 2$	2^{21}
Class D [Multicast]	224 — 239	1110XXXXX	224.0.0.0-239.255.255.255			
Class E [Experimental]	240 — 255	1111XXXXX	240.0.0.0-255.255.255.255			

Subnet Mask:

A subnet mask is a 32 bits address used to distinguish between a network address and a host address in IP address. A subnet mask identifies which part of an IP address is the network address and the host address. They are not shown inside the data packets traversing the Internet. They carry the destination IP address, which a router will match with a subnet.



Subnet Value	Bit Value							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Two types of subnet masks are:

- The default Subnet Mask is the number of bits which is reserved by the address class. Using this default mask will accommodate a single network subnet in the relative class.
- A Custom Subnet Mask can be defined by an administrator to accommodate many Network

Class	Default subnet mask	No. of networks	No. of host per network
A	255.0.0.0	256	16,777,214
B	255.255.0.0	65,536	65,534
C	255.255.255.0	16,77,216	126

Example:

IP address: 192.100.10.66 / 25

Subnet Mask: 11111111.11111111.11111111.10000000

$$\text{Total Subnets} = 2^1 = 2$$

$$\text{Total Hosts} = 2^7 = 128$$

$$\text{Usable Hosts} = 2^7 - 2 = 128 - 2 = 126$$

$$\text{Valid Subnets} = 256 - 128 = 128$$

Subnet (Network IP)	Usable IP Pool		Broadcast IP
	First Host	Last Host	
192.100.10.0	192.100.10.1	192.100.10.126	192.100.10.127
192.100.10.128	192.100.10.129	192.100.10.254	192.100.10.255

LAB 5

Introduction to Packet Tracer, Creating of LAN and connectivity test in the LAN

Objective:

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

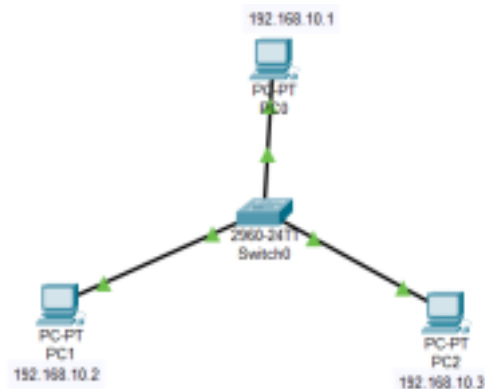
Overview:

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

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

Simple LAN Configuration:

To create a simple LAN 3 PCs are connected to a central switch as shown in the figure below:



Configuration:

1. Connect the PCs to the Switch using Fast Ethernet.
2. Click on PC 0 and go to Desktop then to IP Configuration.
3. Set the IPv4 Address as 192.168.10.1.
4. Close the window.
5. Repeat the same steps to configure the IP Address in PC 1 and PC 2. Set the IP as 192.168.10.2 and 192.168.10.3 for PC 1 and PC 2 respectively.



To test for proper configuration:

- Double click on any of the PC and go to desktop.
- Open Command prompt.
- Ping any other PC in the LAN. If the configuration is successful reply will be received else the request will be timed out.

```
Command Prompt X

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=0ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 3ms

C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

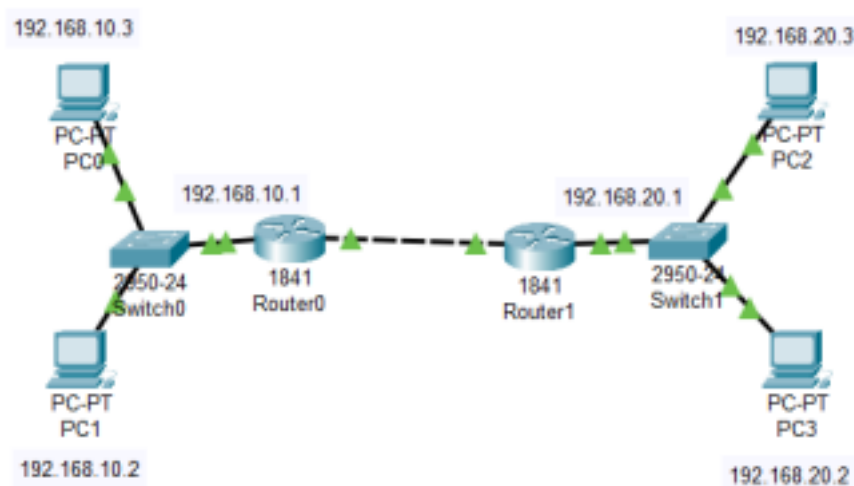
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Static Routing:

To create a static routing configuration two PCs are connected to a switch and the switch is connected to a Router this router is connected to another Router that is connected to a Switch that is connected to two PCs as shown in the figure below:



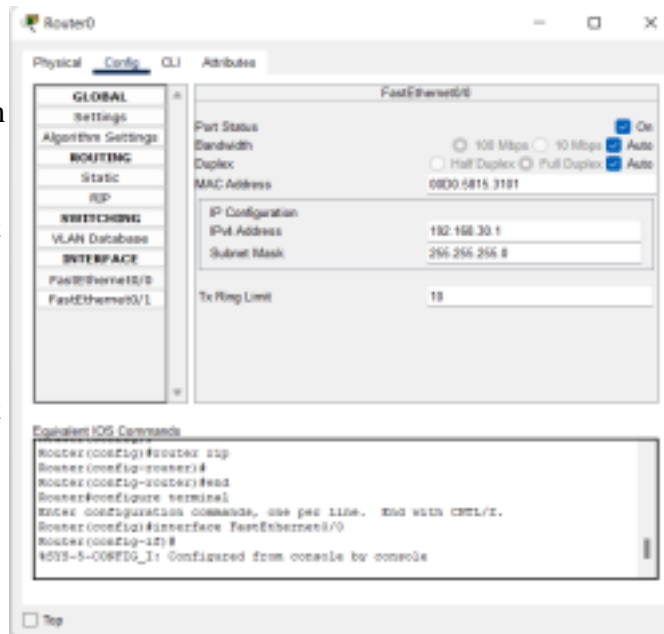
Configuration:

Connect the PCs to the Switch using Fast Ethernet then connect the Switch to a Router then mirror the connection.

For Routers:

In Router 0

- Double click on the router and go to config and then interface.
- In Fast Ethernet 0/0, Set the port status to on and set the IP Address as 192.168.30.1.
- In Fast Ethernet 0/1, Set the port status to on and set the IP Address as 192.168.10.1.
- Close the window.



In Router 1

- Double click on the router and go to config and then interface.
- In Fast Ethernet 0/0, Set the port status to on and set the IP Address as 192.168.30.2.
- In Fast Ethernet 0/1, Set the port status to on and set the IP Address as 192.168.20.1.
- Close the window.

For PCs:

PCs connected to Router 0

- Double click on the PC and go to desktop and then IP Configuration.
- Set the IP Address as 192.168.10.2 and The Default Gateway as 192.168.10.1.
- Close

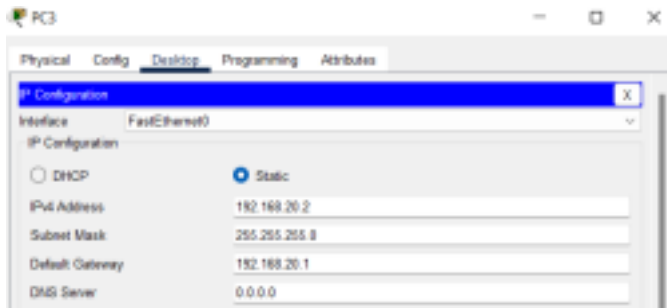
the window.

- Repeat the same step for the next PC and Set the IP Address as 192.168.10.3 and Gateway as 192.168.10.1.



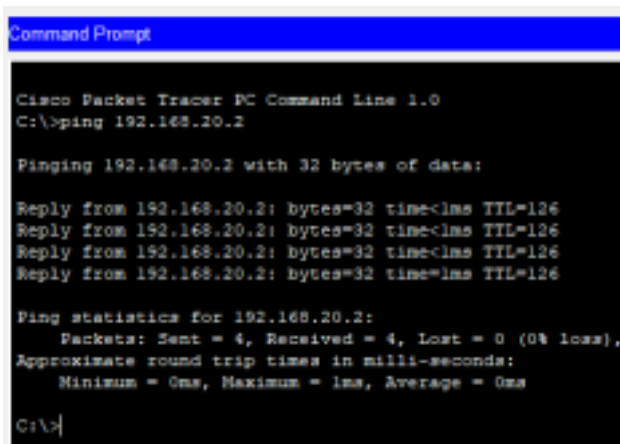
PCs connected to Router 1

- Double click on the PC and go to desktop and then IP Configuration. • Set the IP Address as 192.168.20.2 and The Default Gateway as 192.168.20.1. • Close the window.
- Repeat the same step for the next PC and Set the IP Address as 192.168.20.3 and Gateway as 192.168.20.1.



To test for proper configuration:

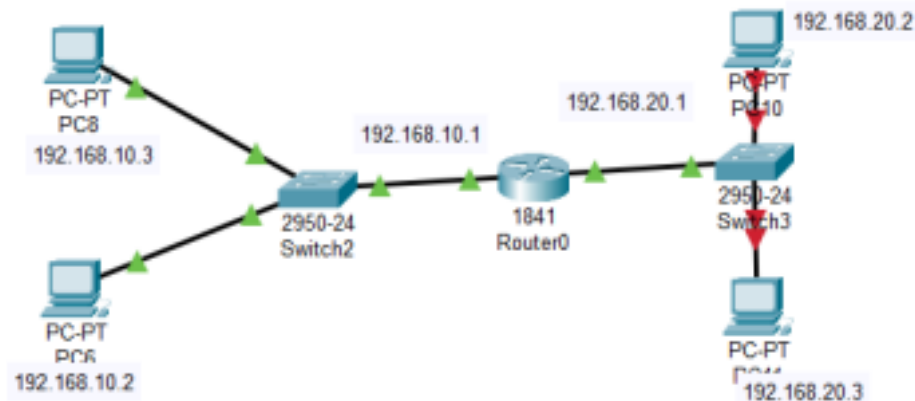
- Double click on any of the PC and go to desktop.
- Open Command prompt.



- Ping any other PC in the Network. If the configuration is successful reply will be received else the request will be timed out.

Basic Routing:

To create a static routing configuration two PCs are connected to a switch and the switch is connected to a Router this router is connected to a Switch that is connected to two PCs as shown in the figure below:

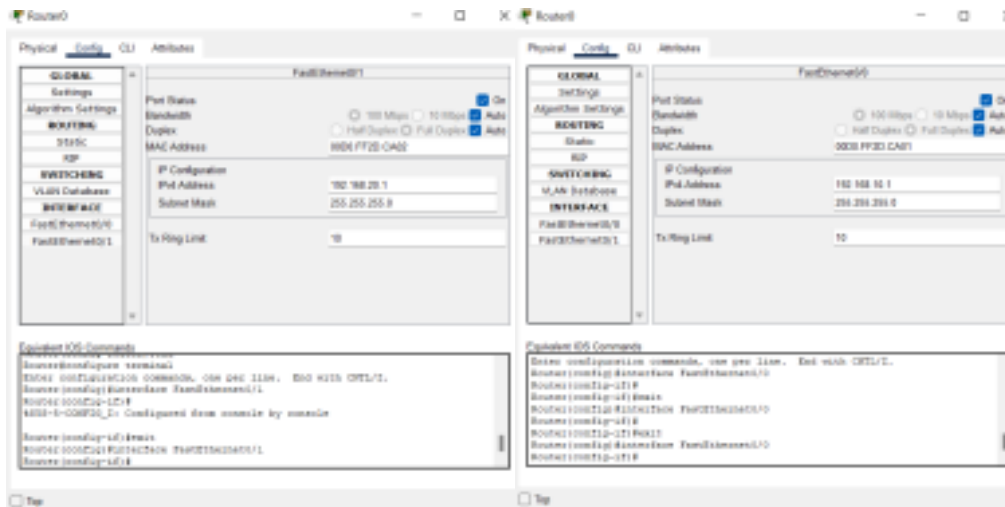


Configuration:

Connect the PCs to the Switch using Fast Ethernet then connect the Switch to a Router then mirror the connection.

For Routers:

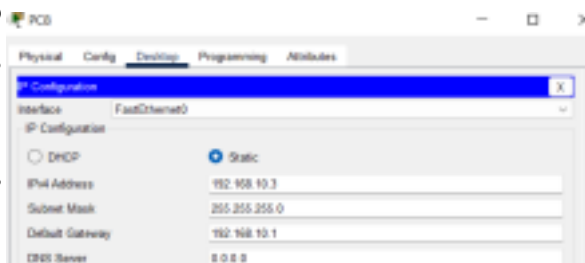
- Double click on the router and go to config and then interface.
 - In Fast Ethernet 0/0, Set the port status to on and set the IP Address as 192.168.10.1. •
 - In Fast Ethernet 0/1, Set the port status to on and set the IP Address as 192.168.20.1. •
- Close the window.



For PCs:

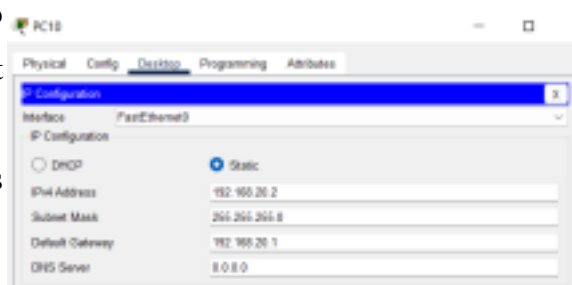
PCs connected to Router Fast Ethernet 0/0

- Double click on the PC and go to desktop and then IP Configuration. • Set the IP Address as 192.168.10.2 and The Default Gateway as 192.168.10.1.
- Close the window.
- Repeat the same step for the next PC and Set the IP Address as 192.168.10.3 and Gateway as 192.168.10.1.



PCs connected to Router Fast Ethernet 0/1

- Double click on the PC and go to desktop and then IP Configuration. • Set the IP Address as 192.168.20.2 and The Default Gateway as 192.168.20.1.
- Close the window.
- Repeat the same step for the next PC

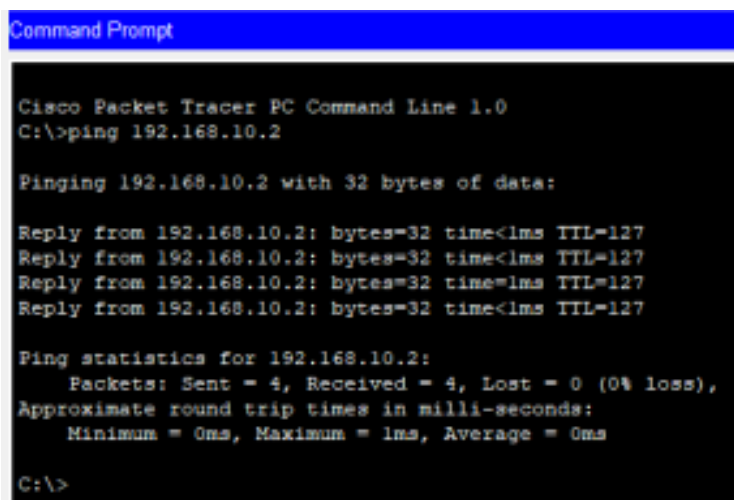


and Set the IP Address as 192.168.20.3

and Gateway as 192.168.20.1.

To test for proper configuration:

- Double click on any of the PC and go to desktop.
- Open Command prompt.
- Ping any other PC in the Network. If the configuration is successful reply will be received else the request will be timed out.



```
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

LAB 6

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

Objective:

- To understand the basic operations of dynamic interior and exterior routing protocols.

Overview:

Distance Vector Routing: Distance vector protocols (a vector contains both distance and direction), such as RIP, determine the path to remote networks using hop count as the metric. A hop count is defined as the number of times a packet needs to pass through a router to reach a remote destination. For IP RIP, the maximum hop is 15. A hop count of 16 indicates an unreachable network. Two versions of RIP exist: version 1 and version 2. IGRP is another example of a distance vector protocol with a higher hop count of 255 hops. A higher hop counts allows your network to scale larger. One of the drawbacks of protocols, such as RIP and IGRP, is convergence time, which is the time it takes for routing information changes to propagate through all your topology. Table 2-2 describes the characteristics of distance vector protocols.

The name distance vector is derived from the fact that routes are advertised as vectors of (distance, direction), where distance is defined in terms of a metric and direction is defined in terms of the next-hop router. For example,

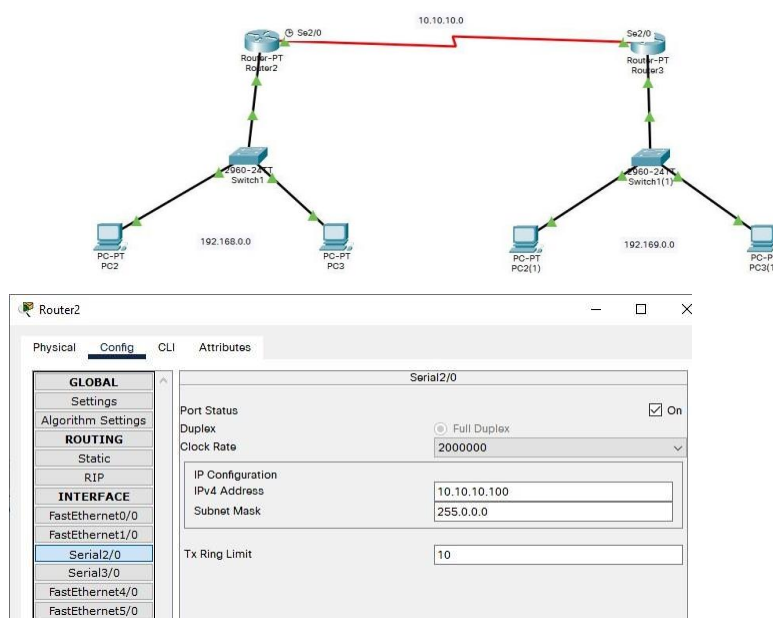
"Destination A is a distance of 5 hops away, in the direction of next-hop router X." As that statement implies, each router learns routes from its neighboring routers' perspectives and then advertises the routes from its own perspective. Because each router depends on its neighbors for information, which the neighbors in turn may have learned from their neighbors, and so on, distance vector routing is sometimes facetiously referred to as "routing by rumor."

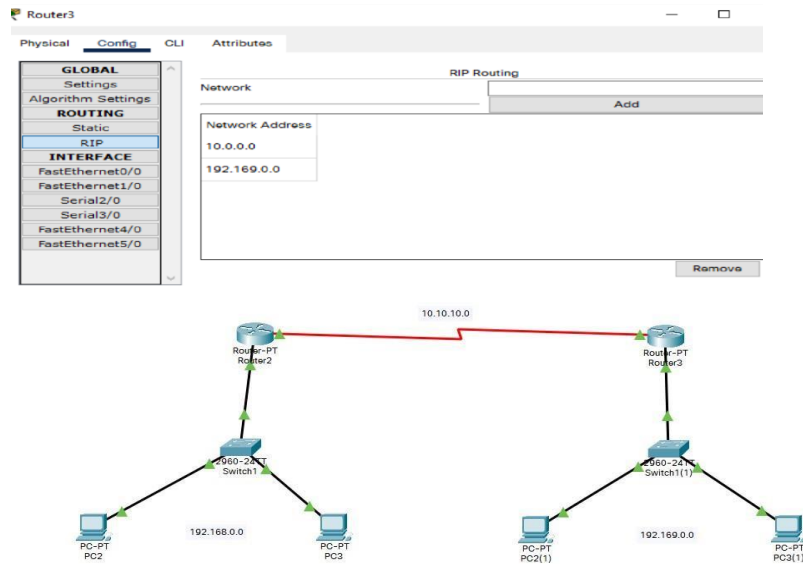
Dynamic Routing:

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:

- Create two networks with routers that have a serial port
- Assign IP to nodes and routers. Connect serial port of routers to same network.
- Go to RIP configuration and add all networks the router is connected to.
- The RIP configuration is now complete and can be checked by a PDU



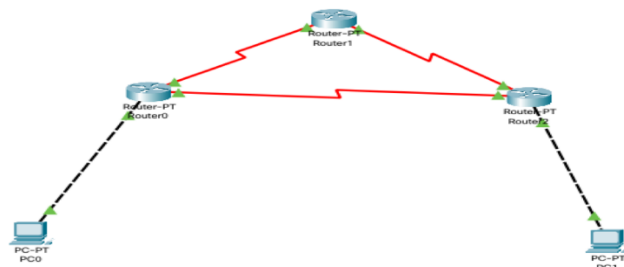


OSPF

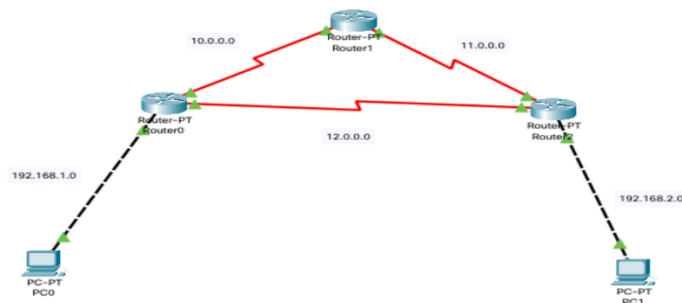
The Open Shortest Path First (OSPF) protocol is commonly used by network routers to dynamically identify the fastest and shortest available routes for sending packets to their destination.

To implement OSPF, we follow the steps below:

- Create a Network with 3 routers and connect them.



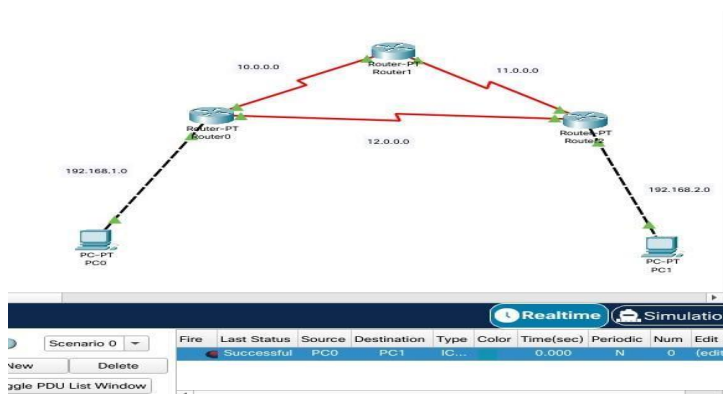
- Assign IP address to all systems and routers.



- 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 add] [subnet mask comp] area [area no] Save the config.

```
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 10.0.0.0 0.255.255.255 area 0
Router(config-router)#network 12.0.0.0 0.255.255.255 area 0
Router(config-router)#
Router(config-router)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

- 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.

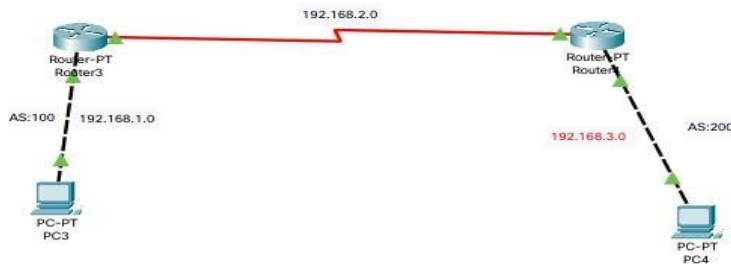
Implementation of BGP protocol:

To implement BGP protocol, we follow following steps:

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



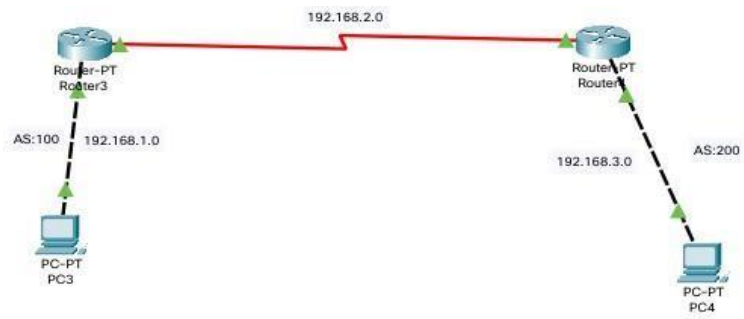
- Assign IP addresses to routers and end devices.



- 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.

```
Router(config-if)#exit
Router(config)#router bgp 100
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#neighbor 192.168.2.178
^
% Invalid input detected at '^' marker.
Router(config-router)#neighbor 192.168.2.178 remote-as 200
^
% Invalid input detected at '^' marker.
Router(config-router)#neighbor 192.168.2.178 remote-as 200
Router(config-router)#neighbor 192.168.3.200 remote-as 200
Router(config-router)#exit
Router(config)#
```

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



PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC4	PC3	ICMP		0.000	N	0	(edit)	

LAB 7

Firewall Implementation, Router Access Control List (ACL)

Objective:

- To understand the router firewall Access Control Lists (ACLs)

Overview:

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 permit 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.

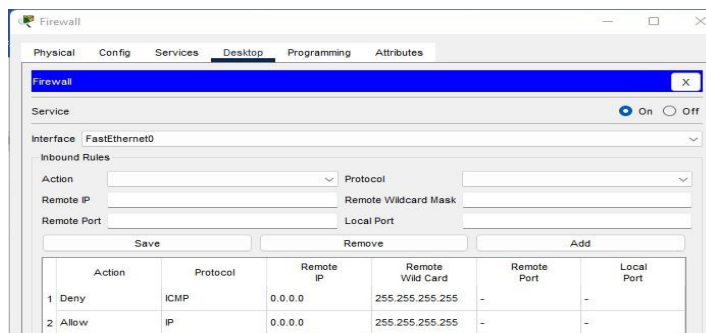
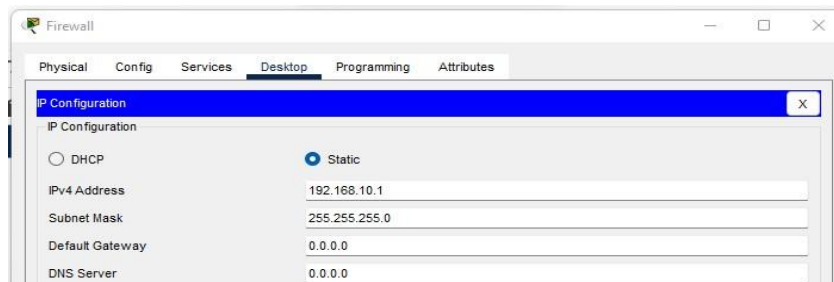
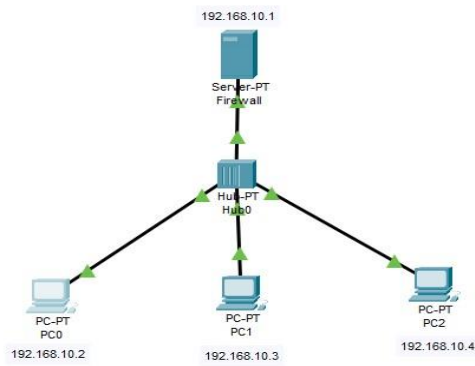
A standard ACL can be used for several purpose. In this lab we will see how it can be used in controlling the unwanted network traffic. With standard ACL, we can define certain conditions for the network traffic passing through the router. By default router does not filter any traffic unless we manually put an ACL.

Firewall Implementation:

To configure Firewall three PCs and a server is connected to a hub as shown in the figure below:

For server:

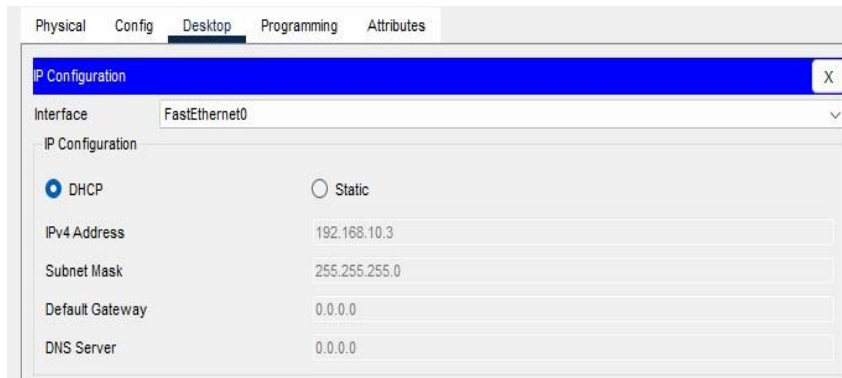
- Double click on the server and go to desktop.
- Then set 192.168.10.1 as the IP Address for the server.
- Go to services and turn on HTTP and HTTPS.
- Click on firewall in the desktop and turn it on and specify the rules.



For PCs:

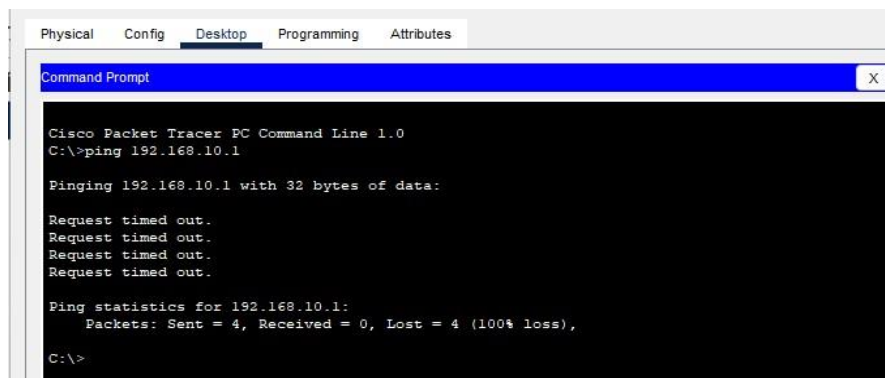
- Double Click and go to Desktop and then to IP Configuration.
- Set the IPv4 addresses as shown below.





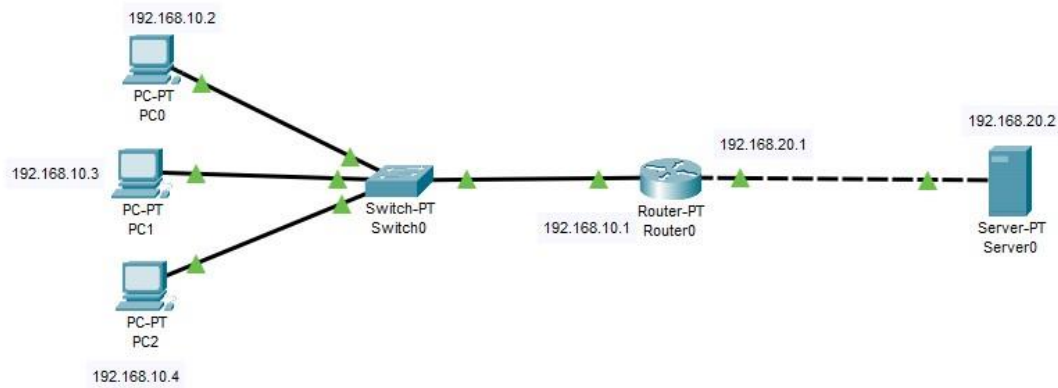
Testing:

- Here the ICMP is blocked but IP is allowed.



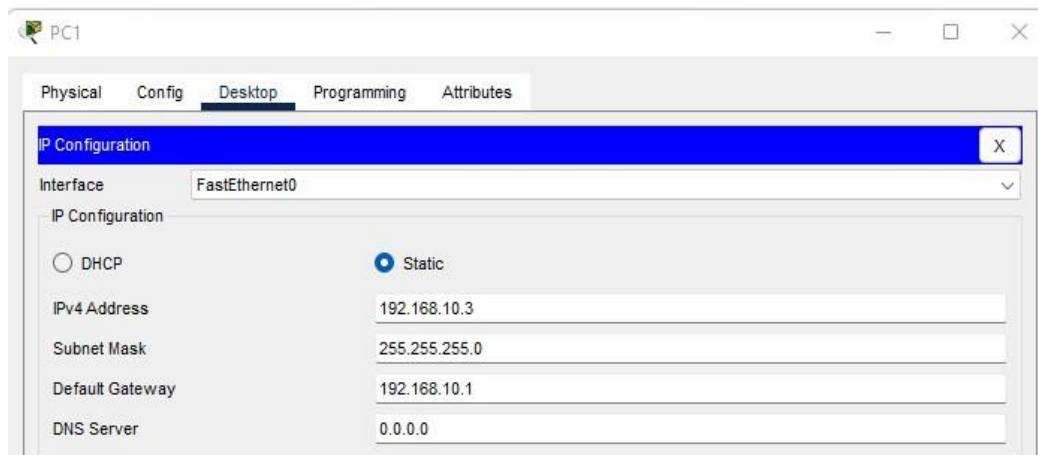
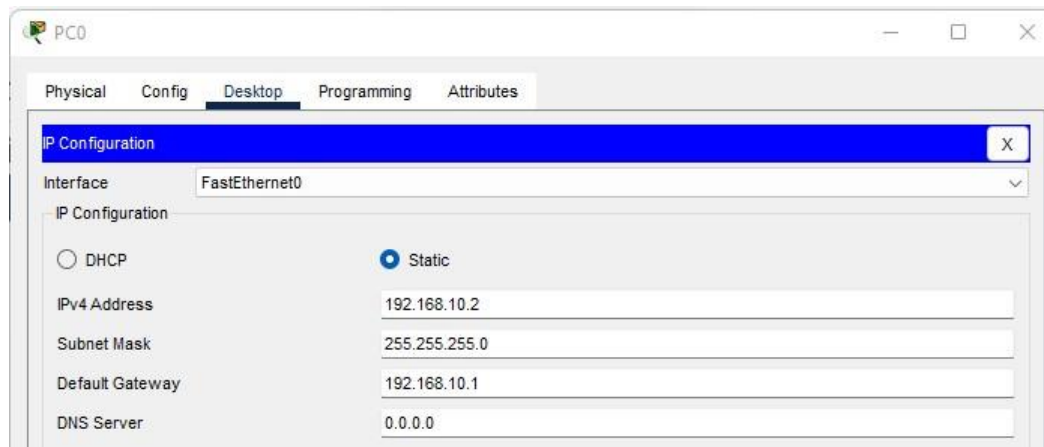
Router Access Control List (ACL):

Connect the PCs to the switch and then connect it with the router. Then the router is connected to the server.



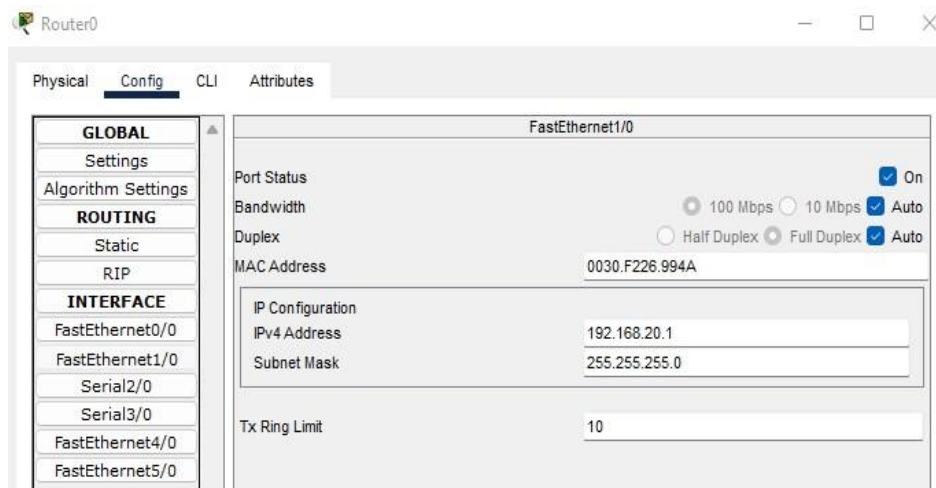
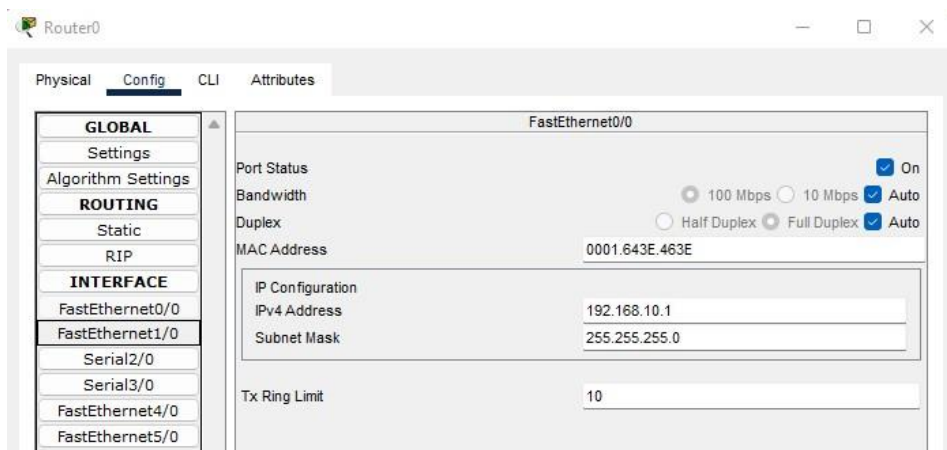
For PC:

- Double click on PC and go to Desktop.
- Go to IP Configuration and Set Up the IP addresses and Gateways as shown.



For Router0:

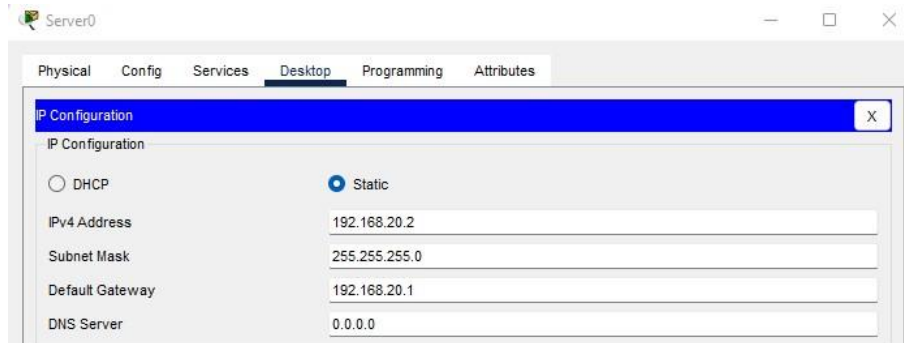
- Double click and go to config
- Set the FastEthernet 0/0 IPv4 as 192.168.10.1
- Set the FastEthernet 0/1 IPv4 as 192.168.20.1 • Type the commands in the CLI as given below.
- Close the window.



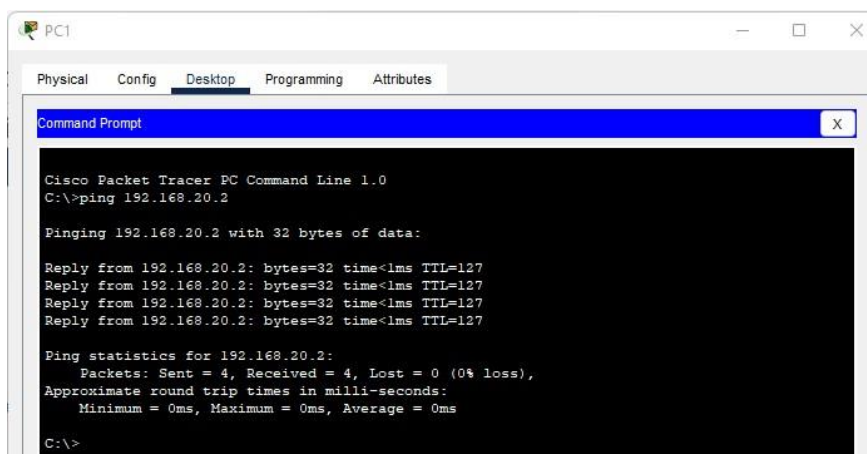
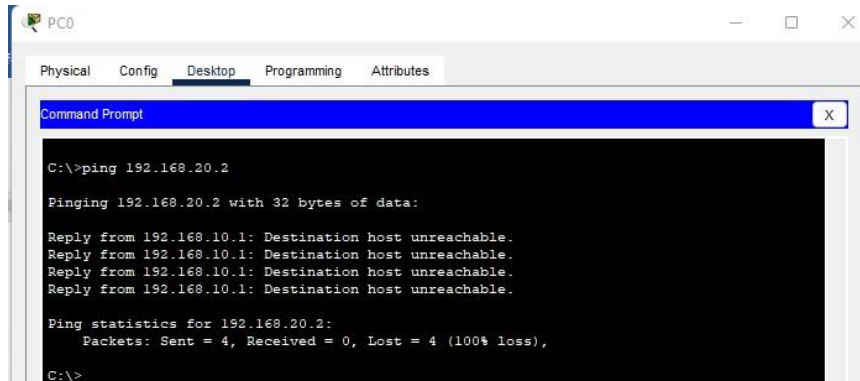
```
Router(config)#ip access-list standard 12
Router(config-std-nacl)#deny host 192.168.10.2
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#interface fast
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip access-group 12 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

For server:

- Double click on the server and go to desktop.
- Set the IP address as 192.168.20.2 and the Gateway as 192.168.20.1.



Test the configuration by pinging through different PCs.



LAB 8

DNS, Web, FTP server configuration

Objective:

- To understand the functions and importance of DNS, web, FTP services in a network environment.
- Configure a DNS server to manage domain name resolution.
- Setup a web server to host websites.
- Enable an FTP server to facilitate file transfers

Overview:

Server services such as DNS, web, DHCP, and FTP play critical roles in network infrastructure. This lab introduces students to the configuration of these server services, which are essential for efficient communication, website hosting, IP address management, and file transfers. Students will learn the necessary steps to set up and configure each service and gain practical experience in managing these vital components of network infrastructure.

Web server is a computer where the web content is stored. Basically, web server is used to host the web sites but there exist other web servers also such as gaming, storage, FTP, email etc.

Web Server Working

Web server respond to the client request in either of the following two ways:

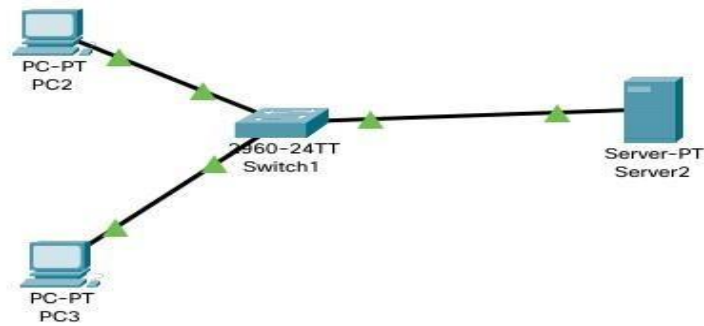
Sending the file to the client associated with the requested URL.

Generating response by invoking a script and communicating with database.

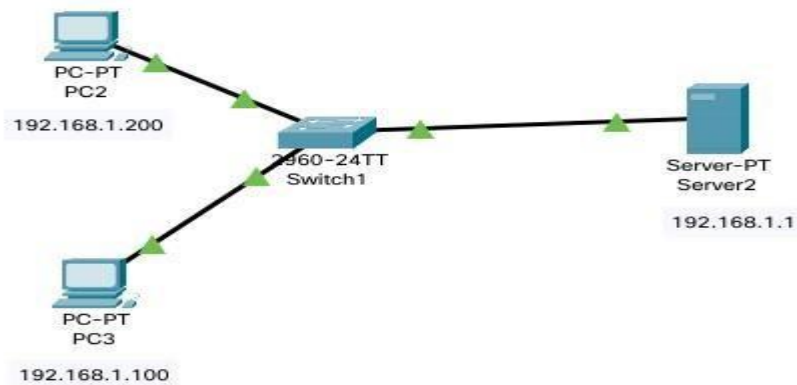
Configuring a web server

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

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



- Configure IP's of switch server and end devices.



- Open server. Go to services tab. Click https and turn http and https on.

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

HTTP

HTTP ☒ On ☐ Off

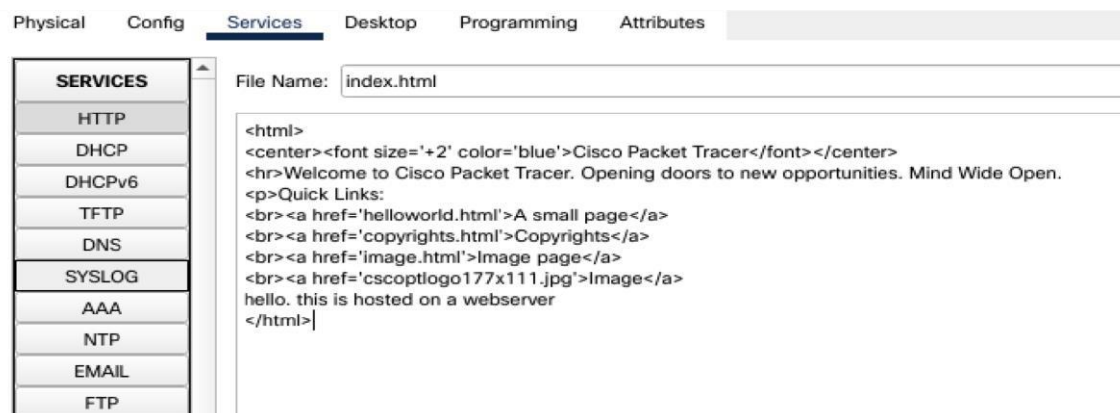
HTTPS

HTTPS ☐ On ☒ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

- Edit the index.html file and save.



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



DNS server

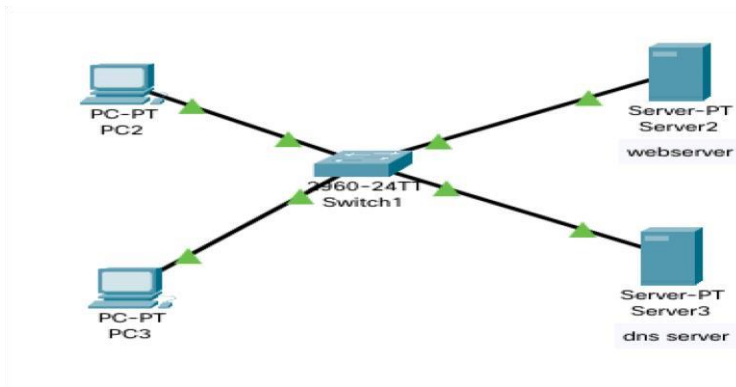
The purpose of a DNS server is to translate what a user types into their browser into something a computer can understand and use to locate a website. In other words, its purpose is to convert a domain name such as `www.example.com` into an IP address such as `71.232.101.120`.

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

Configuring a DNS server

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

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



- Configure the IP addresses to all devices and add the DNS server's ip to the 'DNS server' section of ip configuration menu.

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.200

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 192.168.1.233

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

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

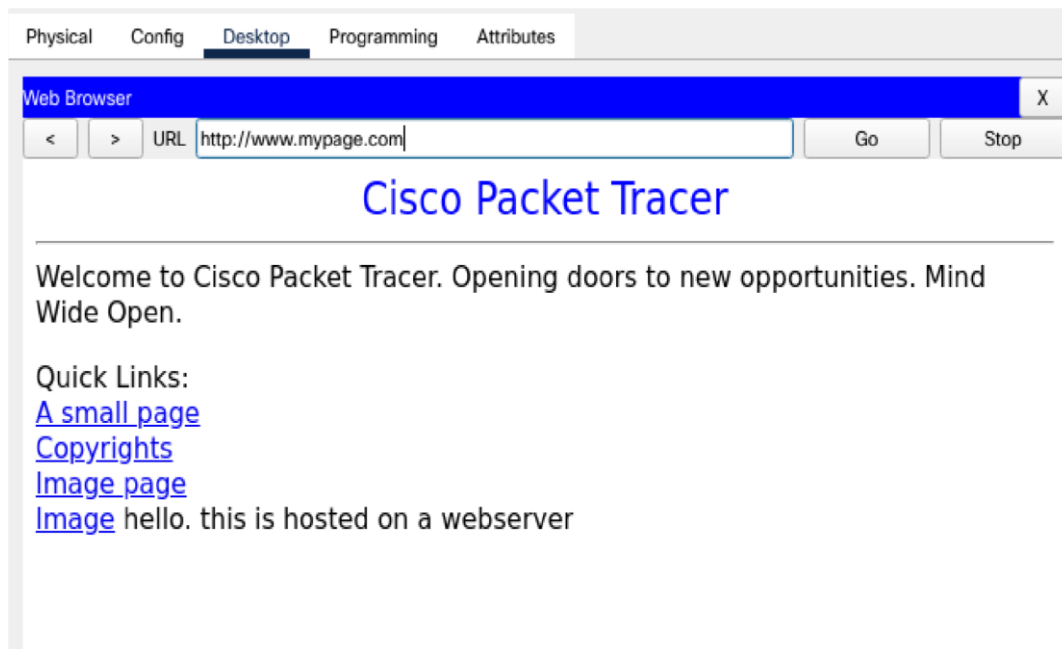
Name Type A Record

Address

Add Save Remove

No.	Name	Type	Detail
0	www.mypage.com	A Record	192.168.1.1

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



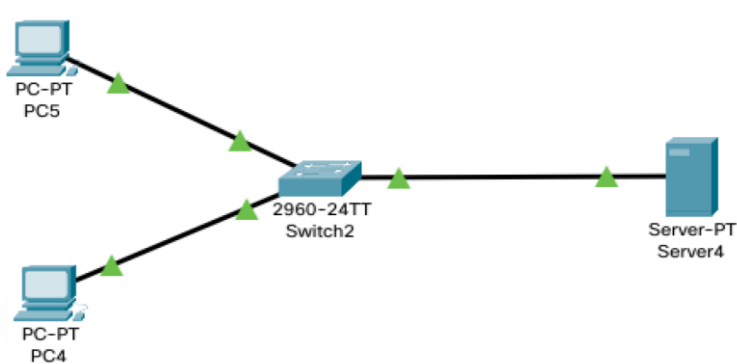
FTP

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

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



- Assign IP to all devices and server.

The IP Configuration window shows the following settings for the FastEthernet0 interface:

- Interface: FastEthernet0
- IP Configuration:
 - ☐ DHCP
 - ☒ Static
- IPv4 Address: 192.168.1.111
- Subnet Mask: 255.255.255.0
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0

- Open server and enable FTP service. Create a username and password and assign the r/w privileges and click add.

The Services configuration window shows the FTP service enabled. The User Setup section includes the following table:

	Username	Password	Permission
1	cisco	cisco	RWDNL
2	user	password	RWDNL

Buttons for Add, Save, and Remove are visible on the right side of the table.

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

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.1
Trying to connect...192.168.1.1
Connected to 192.168.1.1
220- Welcome to PT Ftp server
Username:user
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

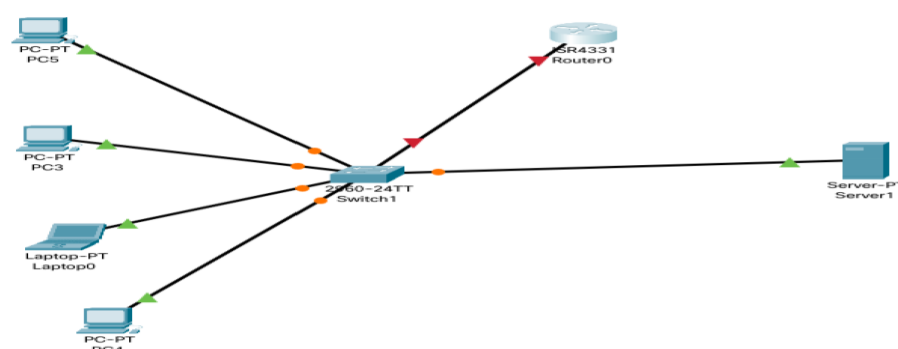
- We can now perform file operations on the ftp server using commands like delete, rename etc.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP. A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. DHCP is an enhancement of an older protocol called BOOTP. DHCP is an important part of the DDI solution (DNSDHCP-IPAM).

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

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



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

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0/0

GigabitEthernet0/0/1

GigabitEthernet0/0/2

GigabitEthernet0/0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0002.16AE.2E01

IP Configuration

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

- 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.

Physical Config **SERVICES** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

Interface FastEthernet0 Service ☒ On ☐ Off

Pool Name dhcp

Default Gateway 192.168.1.1

DNS Server 10.10.10.10

Start IP Address : 192 168 0 200

Subnet Mask: 255 255 255 0

Maximum Number of Users : 56

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
dhcp	192.168....	10.10.10...	192.168....	255.255....	56	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168....	255.255....	255	0.0.0.0	0.0.0.0

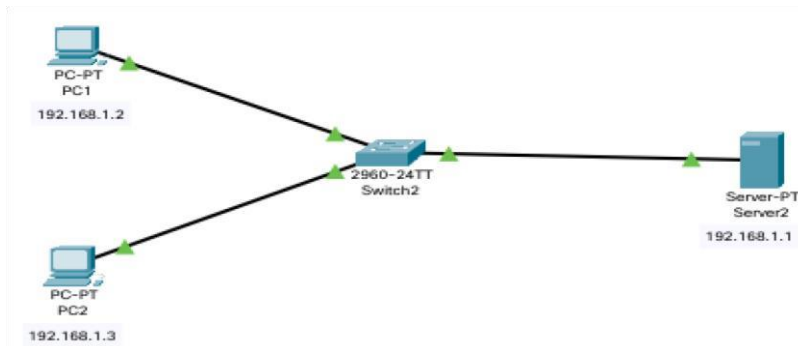
- DHCP configuration is now complete, now the end devices will be assigned an IP address through the DHCP server.

Email Server

An email server, or simply mail server, is an application or computer in a network whose sole purpose is to act as a virtual post office. The server stores incoming mail for distribution to local users and sends out outgoing messages. This uses a client-server application model to send and receive messages using Simple Mail Transfer Protocol (SMTP).

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

- Create a network with end devices, server and switch and assign IP.



- 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.

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL**
- FTP
- IoT
- VM Management
- Radius EAP

EMAIL

SMTP Service: ☒ ON ☐ OFF

POP3 Service: ☒ ON ☐ OFF

Domain Name: Set

User Setup

User: Password:

pc1
pc2

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

Physical Config Desktop **Programming** Attributes

Configure Mail X

User Information

Your Name:

Email Address:

Server Information

Incoming Mail Server:

Outgoing Mail Server:

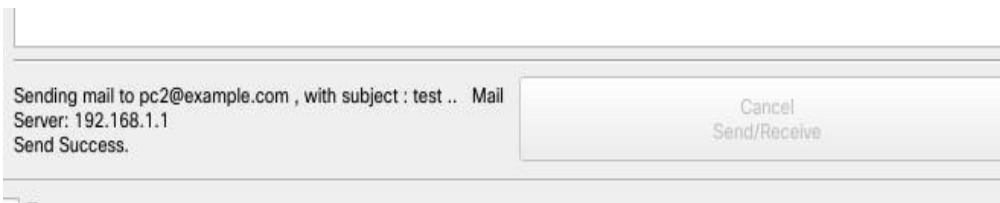
Logon Information

User Name:

Password:

Save Clear Reset

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



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

