Lab Report of Computer Network
Batch 2080

Submitted by:
Mandip Shrestha
SID:20800625
Section: 'A'

Submited to:
Hiranya Bastakoti
Department of B.Sc. CSIT

INDEX

LAB 1: UNDERSTANDING OF NETWORK EQUIPMENT

Networking equipment refers to the physical and virtual devices used to facilitate communication and data transfer within a computer network. These devices play a crucial role in establishing and maintaining connections between computers, servers, and other networked devices. Here are some key pieces of networking equipment:

Repeater

A repeater is a simple device that operates at the physical layer (Layer 1) of the OSI model. Its primary function is to regenerate a signal before it becomes too weak or corrupted. This process extends the length to which the signal can be transmitted over the same network.

Hub

A hub is essentially a multi-port repeater that also operates at the physical layer of the OSI model. It connects multiple wires coming from different branches but cannot filter data, so it sends data packets to all connected devices. Hubs come in several types:

- **Active Hub**: Regenerates the signal before forwarding it.
- **Passive Hub**: Simply forwards the signal without regeneration.
- **Intelligent Hub**: Also known as manageable hubs, these provide additional features like remote management capability.

Bridge

A bridge is a networking device that operates at the data link layer (Layer 2) of the OSI model. It functions similarly to a repeater but with added functionality. A bridge filters content by reading the MAC addresses of the source and destination and is used for interconnecting two LANs that operate on the same protocol. There are two types of bridges:

- **Transparent Bridge**: Filters traffic between segments in a way that is invisible to network users.
- **Source Routing Bridge**: Uses source routing to determine the path to the destination

Switch

A switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (Layer 2) of the OSI model. Some switches also have the capability to forward data at the network layer (Layer 3) by adding routing functionality. Switches are more advanced than hubs and are designed to minimize network congestion.

Router

A router operates at the network layer (Layer 3) of the OSI model. It routes or forwards data packets based on their IP addresses and typically connects Local Area Networks (LANs) and Wide Area Networks (WANs). Routers use a dynamically updating routing table to make routing decisions for incoming packets.

Gateway

A gateway acts as a passage connecting two networks that may operate on different networking models. They perform the role of messenger agents, interpreting and transferring data between systems. In the OSI model, gateways operate at the application layer (Layer 7).

Network Interface Card (NIC)

A Network Interface Card (NIC) allows a networking device to communicate with other devices. It operates at both the physical layer and the data link layer of the OSI model. A NIC converts data packets between different data transmission technologies.

Modem

A modem operates at the physical layer of the OSI model. It converts digital signals generated by a computer into analog signals, which can then be transmitted over a cable line. It also transforms incoming analog signals into digital equivalents, allowing data to be processed by the receiving device.These devices are fundamental to building, maintaining, and optimizing a network, enabling seamless communication and data exchange.

LAB 2: CAT 6 UTP CABLE STRAIGHT & CROSSOVER WIRING AND TESTING

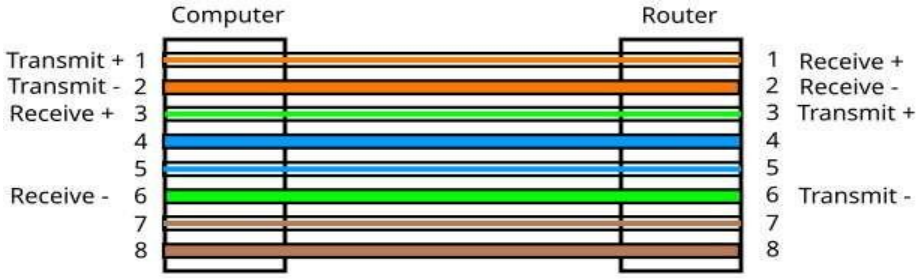
Ethernet cables are essential for setting up high-speed wired network connections between devices. These cables are made of four twisted pair conductors and use RJ45 connectors for data transmission at both ends. Ethernet cables come in various categories, like Cat 5, Cat 5e, and Cat 6.

Types of Ethernet Cables

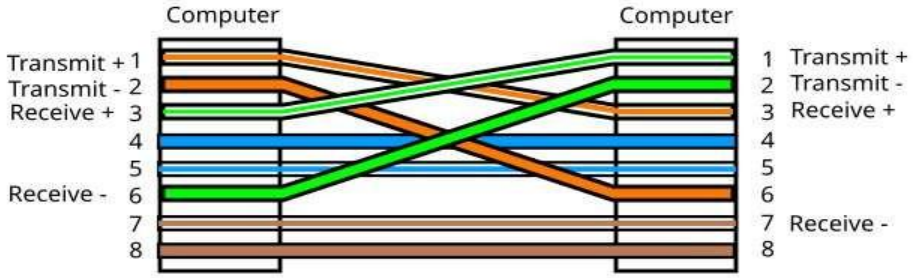
1. **Straight-Through Cable:**
    - Follows either T568A or T568B standards.
    - Has identical pin configurations on both ends.
    - Commonly used to connect computers or network hubs (like routers) within a LAN.
2. **Crossover Cable:**
    - One end follows T568A, and the other end follows T568B.
    - Internally, Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6.
    - Used to connect two devices of the same type (like two computers or two switches).

Wiring Standards

- **T568A Standard:**
    - Orange/White, Solid Orange, Green/White, Solid Blue, Blue/White, Solid Green, Brown/White, Solid Brown.
- **T568B Standard:**
    - Green/White, Solid Green, Orange/White, Solid Blue, Blue/White, Solid Orange, Brown/White, Solid Brown.



Straight Through Cable



Crossover Cable

Steps:

Cat 6 UTP cable wiring & testing can be done as:

1. Start by stripping the outer covering from the cable end.
2. Remove the outer covering, then untwist the paired cables.
3. After untwisting, pull back and trim the exposed plastic core.
4. Straighten the wires.
5. Arrange the wires in the required order for connection.
6. Insert the wires into the RJ-45 connector and check for complete insertion.
7. Clamp the wires in place.
8. Repeat the process for the opposite end.
9. Test connectivity using a LAN Tester.

Important considerations:

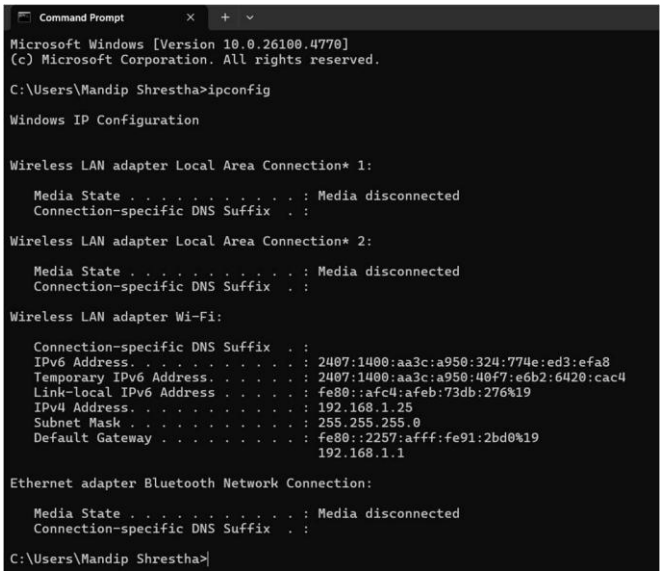
1. Once clamped, the connector is not reusable.
2. The wiring order follows a left-to-right sequence.
3. Odd-numbered positions always feature partial colors, while even-numbered positions contain solid colors.

LAB 3: BASIC NETWORKING COMMANDS

Networking commands are essential tools in computer networking that allow you to manage, diagnose, and troubleshoot network connections. By entering these commands into a command-line interface (CLI) or terminal window, you can interact directly with the operating system and network components. These commands give us the ability to view and adjust network settings, verify network connectivity, resolve issues, and collect detailed information about network devices and connections. In this lab, all the networking commands were executed using the Windows Command Prompt.

Some Basic Networking Commands are:

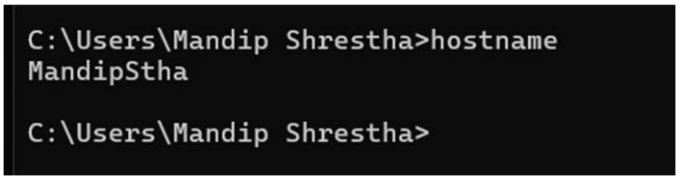
1. ipconfig:
This command is used to display the current network configuration settings for your system, including the IP address, subnet mask, and default gateway. It's often utilized for diagnosing and resolving network connectivity problems.



2. ipconfig /all:
An extended version of the ipconfig command that provides comprehensive details about all network interfaces on the system, both physical and virtual. It includes information on DHCP, DNS settings, MAC addresses, and more, making it useful for in-depth network troubleshooting.

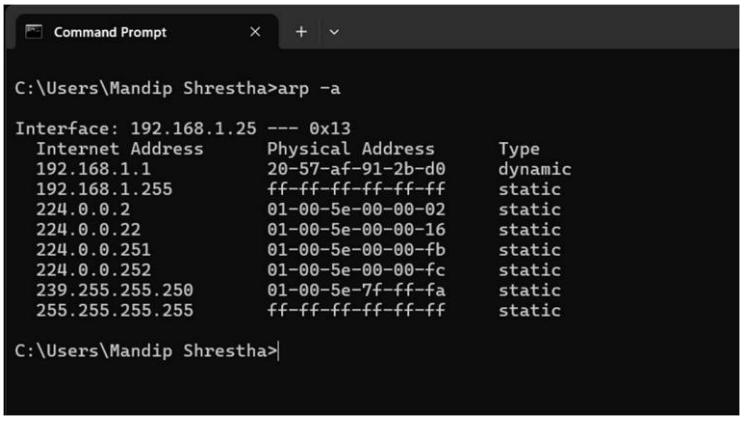
3. hostname:

Displays the name of the computer or device as recognized on the network. This is often used when configuring or troubleshooting network services that rely on the machine's hostname.



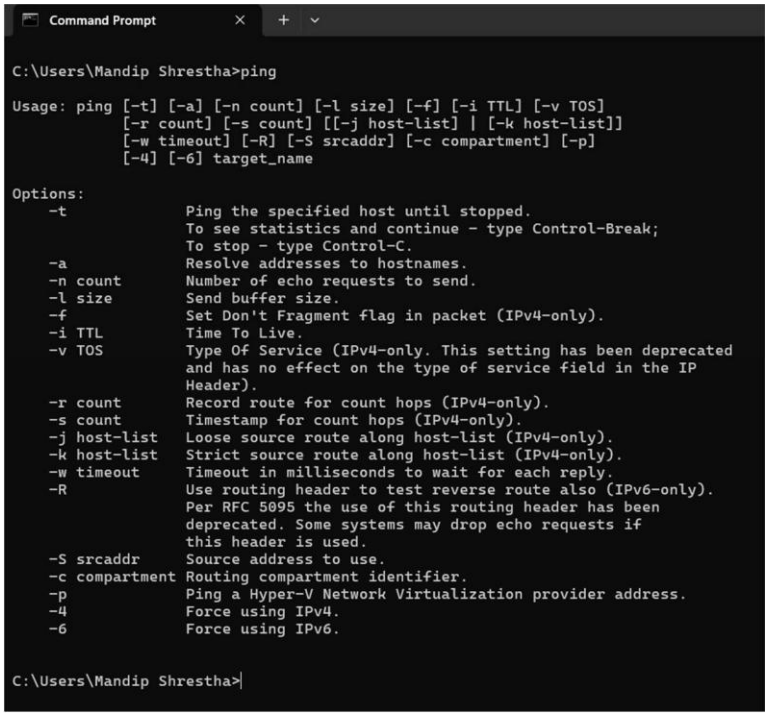
4. arp -a:

This command shows the Address Resolution Protocol (ARP) table, which maps IP addresses to their corresponding MAC addresses. It's useful for understanding the relationship between IP and hardware addresses on your local network.



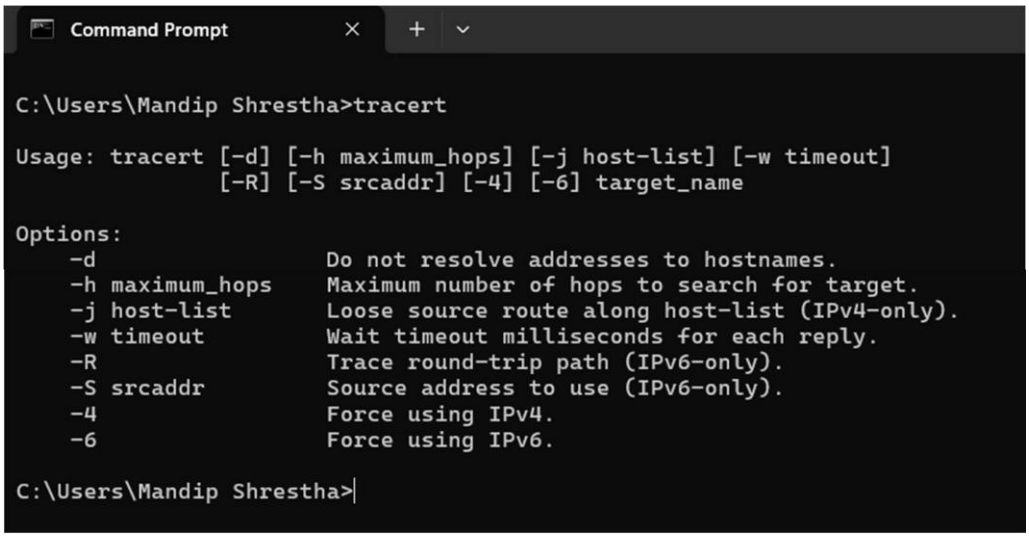
5. ping:

A basic command that sends a series of ICMP echo requests to a specified IP address or hostname to check network connectivity and measure the time it takes for a response. It's widely used to test if a device on the network is reachable.



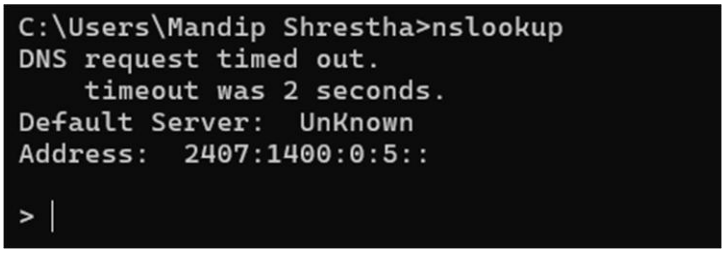
6. tracert:

Traces the path that packets take to reach a destination, showing each hop along the route and the time it takes to travel between them. It's useful for identifying where delays or failures occur in the network path.



7. nslookup:

Used to query DNS servers for domain name resolution, nslookup can retrieve information about IP addresses, domain names, and DNS records. It's an essential tool for diagnosing DNS-related issues.



8. systeminfo:

Displays detailed information about the system's hardware and software configuration, including the OS version, memory, processor, network interfaces, and more. It's often used for gathering system details for troubleshooting or documentation purposes.


Command Prompt
C:\Users\Mandip Shrestha>systeminfo
Host Name: MANDIPSTHA
OS Name: Microsoft Windows 11 Home
OS Version: 10.0.26100 N/A Build 26100
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: Mandip Shrestha
Registered Organization: N/A
Product ID: 00342-22274-30747-AAOEM
Original Install Date: 12/19/2024, 10:18:49 PM
System Boot Time: 7/30/2025, 5:30:30 PM
System Manufacturer: ASUSTeK COMPUTER INC.
System Model: Vivobook_ASUSLaptop K3604ZA_K3604ZA
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 154 Stepping 4 GenuineIntel ~1300 Mhz
BIOS Version: American Megatrends International, LLC. K3604ZA.300, 8/21/2023
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) Kathmandu
Total Physical Memory: 16,078 MB
Available Physical Memory: 9,184 MB
Virtual Memory: Max Size: 17,102 MB
Virtual Memory: Available: 9,785 MB
Virtual Memory: In Use: 7,317 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\MANDIPSTHA
Hotfix(s): 4 Hotfix(s) Installed.
[01]: KB5056579
[02]: KB5062660
[03]: KB5063666
[04]: KB5064485
Network Card(s): 2 NIC(s) Installed.
[01]: Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
Connection Name: Wi-Fi
DHCP Enabled: Yes
DHCP Server: 192.168.1.1
IP address(es)
[01]: 192.168.1.25
[02]: fe80::afc4:afeb:73db:276
[03]: 2407:1400:aa3c:a950:80c4:2288:c78b:cb25
[04]: 2407:1400:aa3c:a950:324:774e:ed3:efa8
[02]: Bluetooth Device (Personal Area Network)
Connection Name: Bluetooth Network Connection
Status: Media disconnected
Virtualization-based security: Status: Running
Required Security Properties:
Available Security Properties:
Base Virtualization Support
Secure Boot
DMA Protection
UEFI Code Readonly
Mode Based Execution Control
APIC Virtualization
Services Configured:
Hypervisor enforced Code Integrity
Services Running:
Hypervisor enforced Code Integrity
App Control for Business policy: Enforced
App Control for Business user mode policy: Off
Security Features Enabled:
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.
C:\Users\Mandip Shrestha>

LAB 4: OVERVIEW OF IP ADDRESSING & SUBNETTING

Internet Protocol (IP) Addressing

IP addressing is a critical component of any network, as it assigns a unique identifier to each device connected to the network. An IP address is a distinct sequence of numbers and/or letters that identifies a device within a network. It serves two primary purposes: identifying the host or network interface and indicating the location of the host within the network.

Types of IP Addresses

- **IPv4**:
  IPv4 is the most widely used format for IP addresses. It employs a 32-bit address system, which allows for a total of 2^32 possible addresses. An IPv4 address is typically divided into four segments, such as 192.168.0.2. Each segment represents an 8-bit number, ranging from 0 to 255.
- **IPv6**:
  IPv6 utilizes a 128-bit address system, enabling a significantly larger number of addresses than IPv4. An IPv6 address is represented as eight groups of four hexadecimal digits, with each group representing 16 bits. These groups are separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

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	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

Subnetting

Subnetting is the process of splitting a network into two or more smaller networks. It's used to optimize network efficiency and enhance security. Subnetting allows the creation of multiple networks within a single network, leading to better utilization of IP addresses.

Benefits of Subnetting

- **Improved Network Performance:**
  By breaking down a large network into smaller subnets, network traffic can be reduced, which enhances performance. Local traffic remains within the subnet, reducing congestion across the network.
- **Enhanced Security:**
  Subnetting helps isolate different parts of the network. If one subnet is compromised, the other subnets may remain secure because routers between subnets act as a firewall, blocking certain types of traffic.
- **Easier Administration:**
  Smaller networks are easier to manage. Network problems can be quickly identified and resolved within a subnet, without affecting the entire network.

Example:
IP address: 192.100.10.66 / 25
Subnet Mask: 11111111.11111111.11111111.10000000
Total Subnets = 2^1 = 2
Total Hosts = 27 = 128
Usable Hosts = 2^7-2 = 128-2 = 126
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 CISCO PACKET TRACER

Cisco Packet Tracer is a versatile network simulation tool that allows students and network administrators to explore network behavior and ask "what if" scenarios. It is designed to enhance learning and skill development in networking by providing simulation, visualization, authoring, assessment, and collaboration tools to simplify complex technology concepts.

Features

- **Network Simulation:**
  Simulate complex network topologies with various networking devices like routers, switches, wireless devices, and end devices.
- **Packet Capture and Analysis:**
  Capture and analyze network packets to troubleshoot and debug connectivity issues.
- **Protocols Support:**
  Supports a wide range of networking protocols such as TCP/IP, ICMP, DHCP, NAT, OSPF, EIGRP, RIP, VLAN, and more for practice in configuration and troubleshooting.
- **Multi-Platform Support:**
  Available on Windows, Linux, and macOS, making it accessible across different operating systems.
- **User-Friendly Interface:**
  Features an intuitive GUI for designing, configuring, and troubleshooting network topologies with ease.
- **Activity Wizard:**
  Provides pre-built networking scenarios and guided exercises for practicing network concepts and configurations.
- **Real-Time Visualization:**
  Visualize network activity and traffic flow in real-time to understand how data moves through the network.
- **Customization Option:**
  Customize network topologies, device configurations, and simulation parameters.

Usage

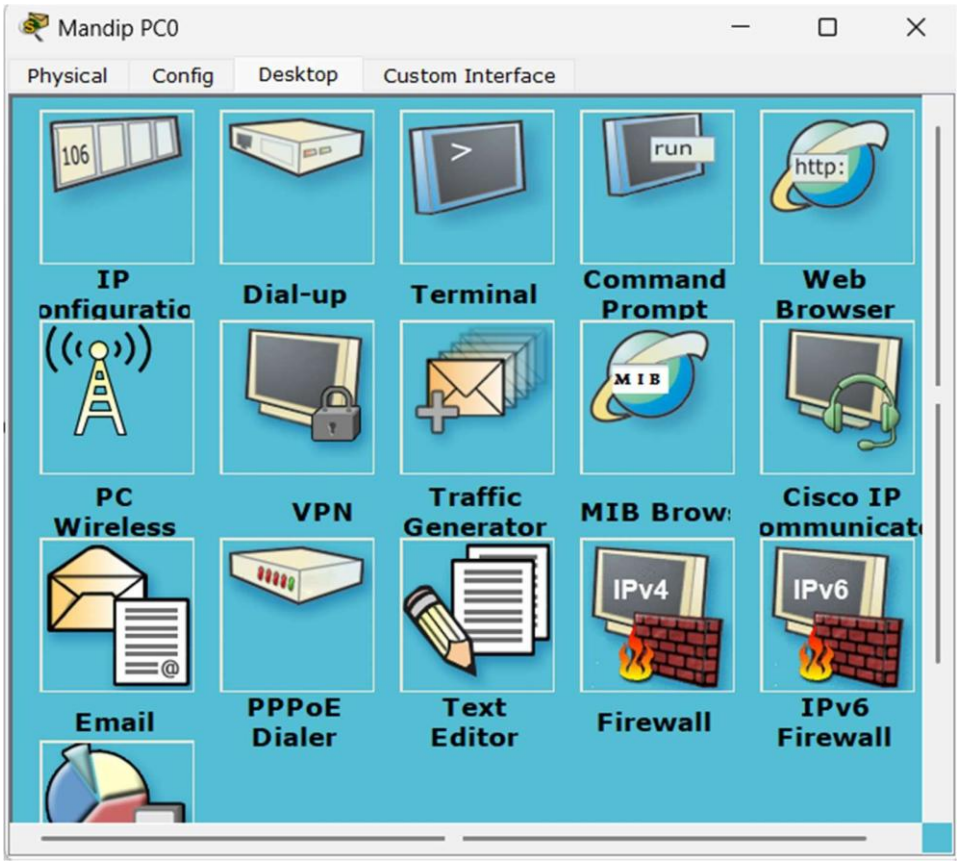
- **Educational Settings:**
  Widely used in educational environments to teach networking concepts, with instructors creating lab exercises and scenarios for students to practice in a simulated environment. It helps students design complex network topologies and understand network functionality.
- **Professional World:**
  Used by professionals as a virtual lab for training and testing network configurations before deployment. It supports continuous learning, troubleshooting practice, and fosters collaboration among professionals through file sharing and project collaboration.

LAB 6: CREATION OF BASIC LOCAL AREA NETWORK (LAN)

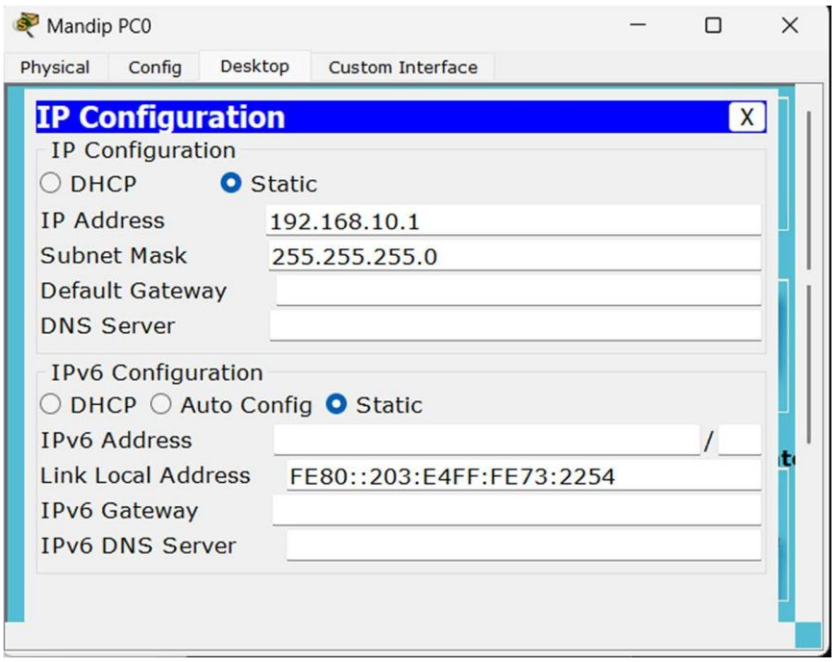
Local Area Network (LAN) is a network that consists of computers and other devices linked together to form a network within a circumscribed location. It connects devices within a limited geographic area typically exclusive to an organization, like a school, office, etc.

To create a basic Local Area Network (LAN) in **Cisco Packet Tracer**, follow these steps:

1. Place PCs (PC0, PC1, PC2) & a Switch (Switch1)
2. Connect them with Ethernet cable
3. Click on PC0
4. Goto Desktop > IP Configuration

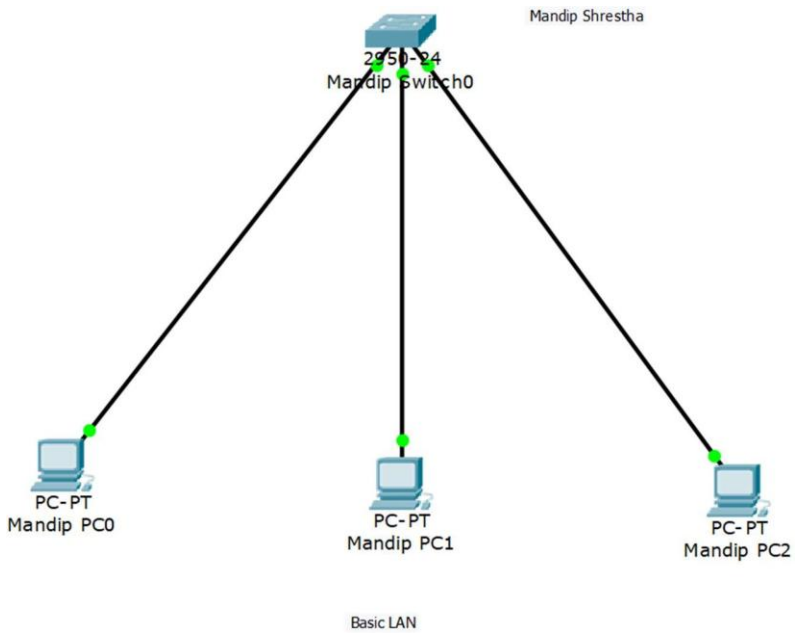


5. In IP Configuration, check on Static & Enter the IP address 192.68.10.1



6. Click on Subnet Mask, it will be set to 255.255.255.0 automatically
7. Leave other settings unchanged
8. Repeat Step 5, 6, 7 for Laptop0 & PC1. But set IP address 192.168.10.2 & 192.168.10.3 for Laptop0 & PC1 respectively.

Layout



Testing

The LAN can be tested in two ways:

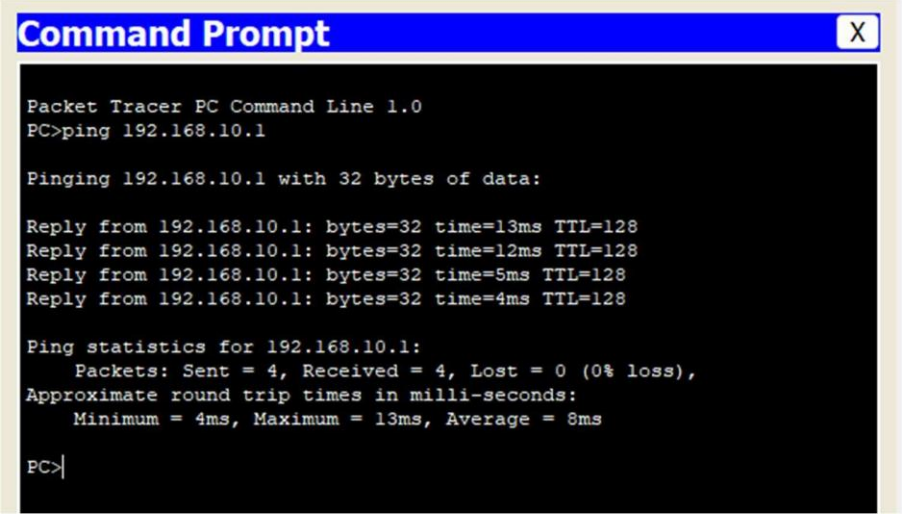
A. By sending packets from one PC to another

1. Click on packet (mail icon) & place on any two computers
2. If the status is Successful, the configuration is correct

Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit	Delete
	Successful	Mandi...	Mandip PC1	ICMP		0.000	N	0	(edit)	(delete)

B. By pinging target PC IP address from Command Prompt of one PC

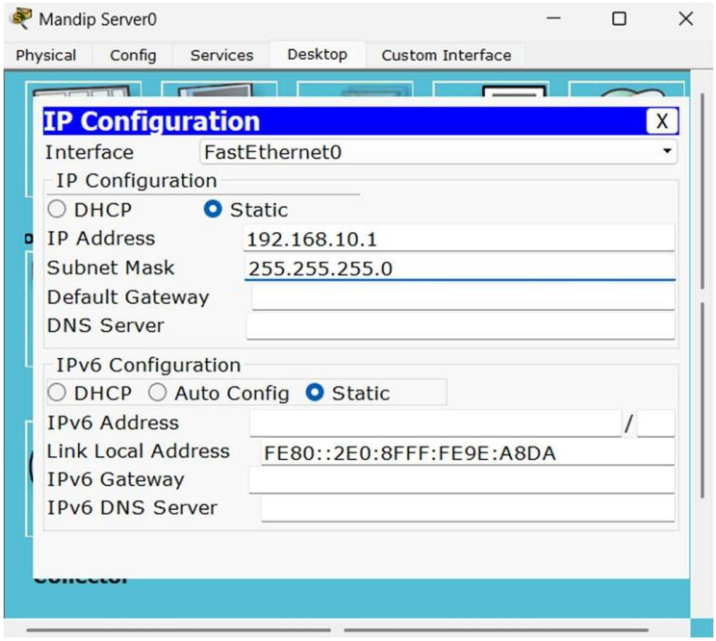
1. Goto Command Prompt of one PC (PC0)
2. Enter ping & IP of target PC (ping 192.168.10.3)
3. If the target PC replies, the configuration is successful.



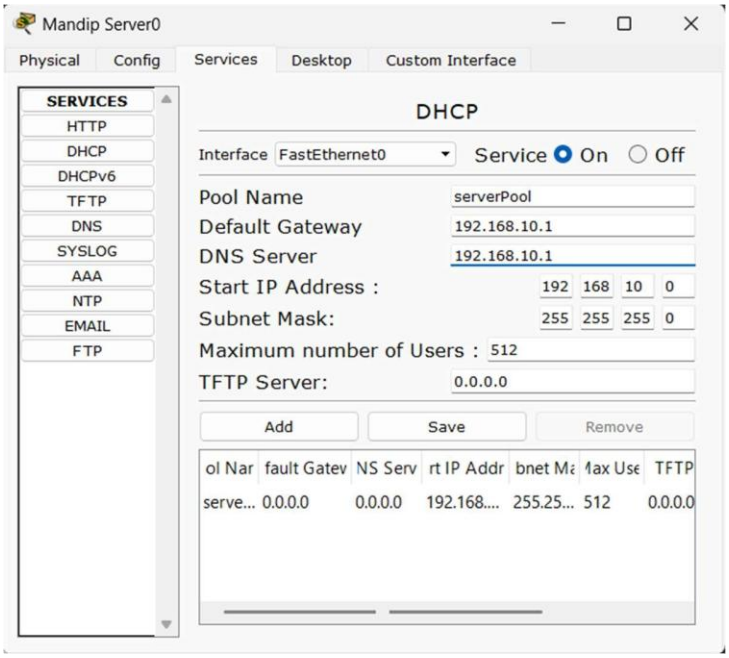
LAB 7: IMPLEMENTATION OF DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Dynamic Host Configuration Protocol (DHCP) serves as a network management protocol deployed on a network to automatically allocate IP addresses and various communication parameters to network-connected devices. This is accomplished through a client-server architecture. The technology eliminates the need for individually configuring network devices manually.
This technology comprises two essential network components: a centrally installed DHCP server within the network infrastructure and client instances of the protocol stack present on every computer or device connected to the network. Upon connecting to the network and periodically thereafter, a client initiates a request to the server, seeking a specific set of parameters via DHCP.

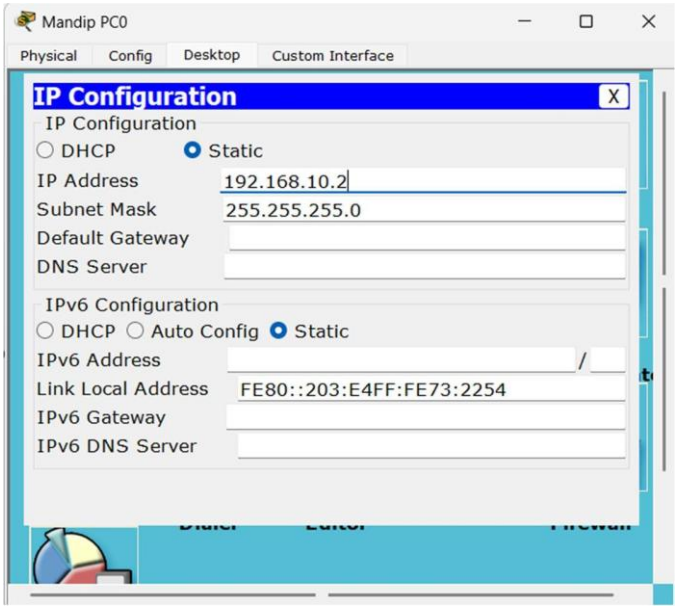
Configuration
In Cisco Packet Tracer, DHCP can be implemented as follows:
1. Place a Server (Server0)
2. Place PCs (PC0, PC1, PC2) & a Switch (Switch0)
3. Connect PCs to Switch using Ethernet
4. Connect Switch to Server
5. In Server,
 5.1. Goto Desktop > IP Configuration.
 5.2. Set IP address, Default Gateway & DNS server to 192.168.10.1 & Subnet Mask to 255.255.255.0



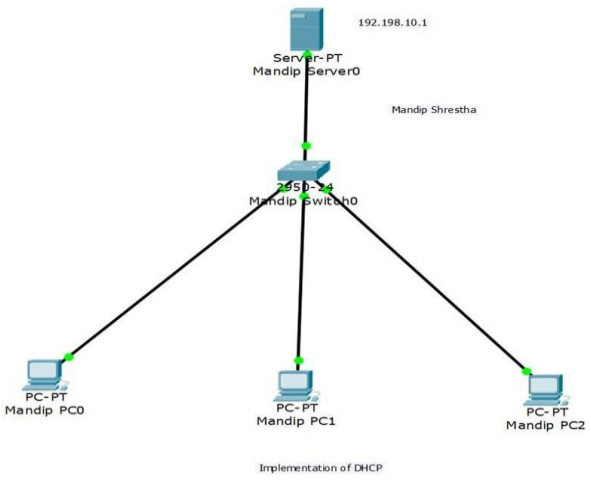
5.3. Goto Services > DHCP
5.4. Set Default Gateway & DNS Server to 192.168.10.1
5.5. Save the Configuration & Turn on DHCP service.



6. In PC (PC0),
   6.1. Goto Desktop > IP Configuration
   6.2. Switch the IP Configuration from Static to DHCP
   6.3. Review the new dynamically assigned IP address
   6.4. Repeat the process for other PCs.



Layout



Testing

The implementation can be tested in two ways:

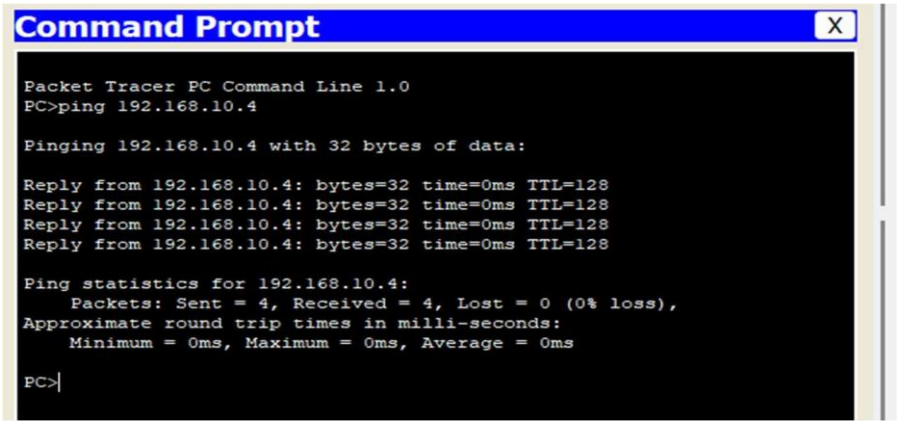
A. By sending packets from one PC to another

1. Click on packet (mail icon) & place on any two computers.
2. If the status is Successful, the configuration is correct.

Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit	Delete
	Successful	Mandip PC0	Mandip PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Mandip PC0	Mandip PC1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Mandip PC0	Mandip Server0	ICMP		0.000	N	2	(edit)	(delete)

B. By pinging target PC IP address from Command Prompt of one PC

1. Goto Command Prompt of one PC (PC1).
2. Enter ping & IP of target PC (ping 192.168.10.3).
3. If the target PC replies, the configuration is successful.



LAB 8: IMPLEMENTATION OF VIRTUAL LOCAL AREA NETWORK (VLAN)

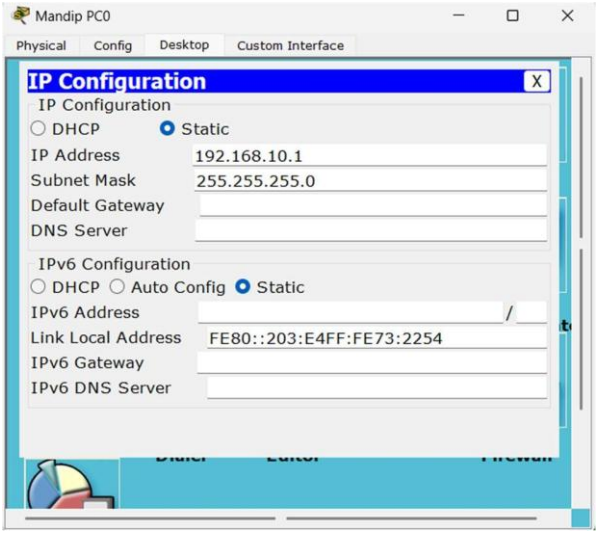
VLAN (Virtual Local Area Network) is a network technology that allows you to create logically segmented networks within a physical network infrastructure. It enables you to isolate traffic, even though segmented networks might share the same physical network infrastructure like switches or routers. Each VLAN behaves as if it is a separate physical network, even though devices within the VLAN might physically be connected to the same network infrastructure.

VLANs are typically used to improve network security, manage traffic more efficiently, and simplify network administration. By segmenting the network into VLANs, administrators can control which devices can communicate with each other, reducing the risk of unauthorized access or attacks. VLANs also allow for better management of network traffic by separating different types of traffic.

Configuration

In Cisco Packet Tracer, VLAN can be implemented as follows:

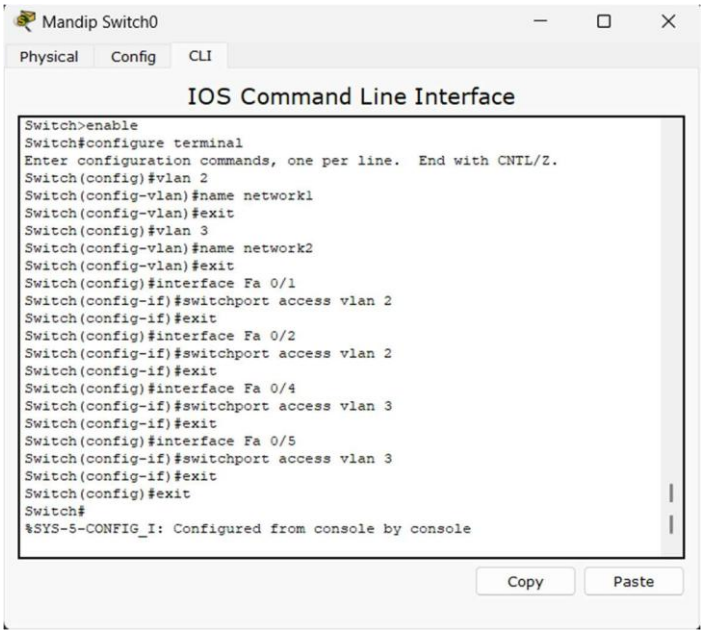
1. Place Switch (Switch0) & PCs (PC0, PC1, PC2, PC3)
2. Connect PCs to switch using Ethernet cable
3. In PC0,
    3.1. Goto Desktop > IP Configuration
    3.2. Enter IP address 192.168.10.1 & Default Gateway 255.255.255.0



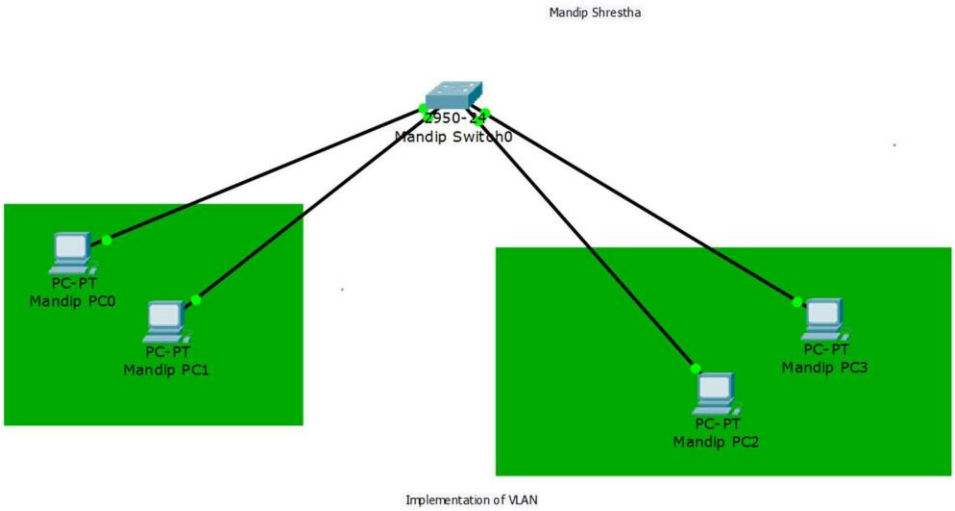
3.3. Repeat the steps for PC1, PC2, PC3. Set IP 192.168.10.2, 192.168.10.3 & 192.168.10.4 for PC1, PC2 & PC3 respectively. One PC should be successfully pinged from another.

4. In Switch (Switch0),
    4.1. Goto CLI (Command Line Interface) mode
    4.2. Enter the CLI commands line by line.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name network1
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name network2
Switch(config-vlan)#exit
Switch(config)#interface Fa 0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface Fa 0/2
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface Fa 0/4
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#interface Fa 0/5
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#exit
Switch#
```



Layout



Testing

1.Goto Command Prompt of one PC (PC0)

2Enter ping & IP address of target PC of another VLAN (ping 192.168.10.4)

2.1. The ping is successfully done at first

2.2. But after configuration of VLAN, the ping fails.

```
PC>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

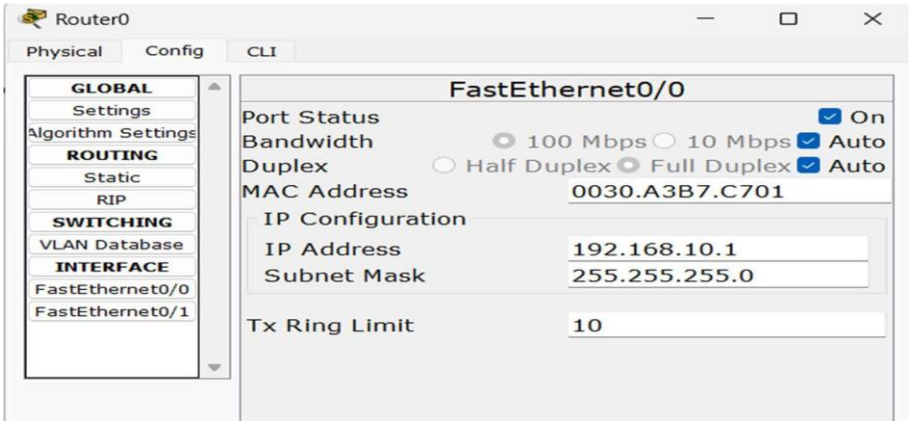
LAB 9: BASIC ROUTER CONFIGURATION

Basic router configuration typically involves setting up essential parameters to enable communication between networks.

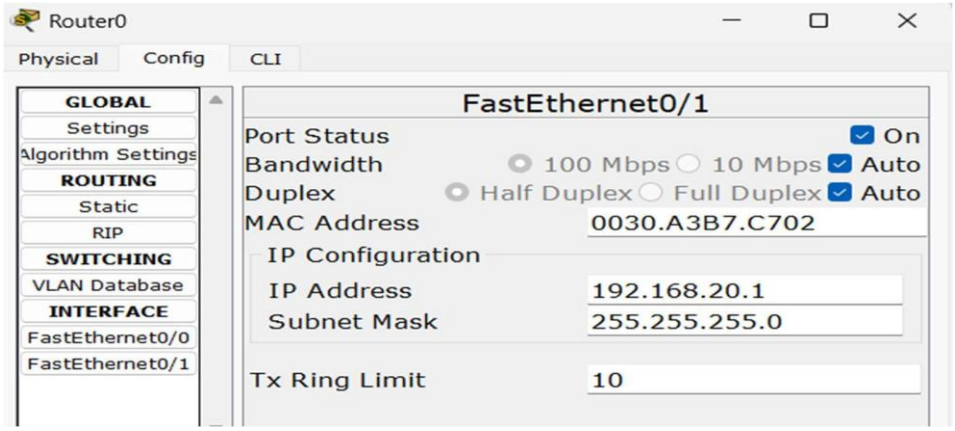
Configuration

In Cisco Packet Tracer, Basic Router Configuration can be done as follows:

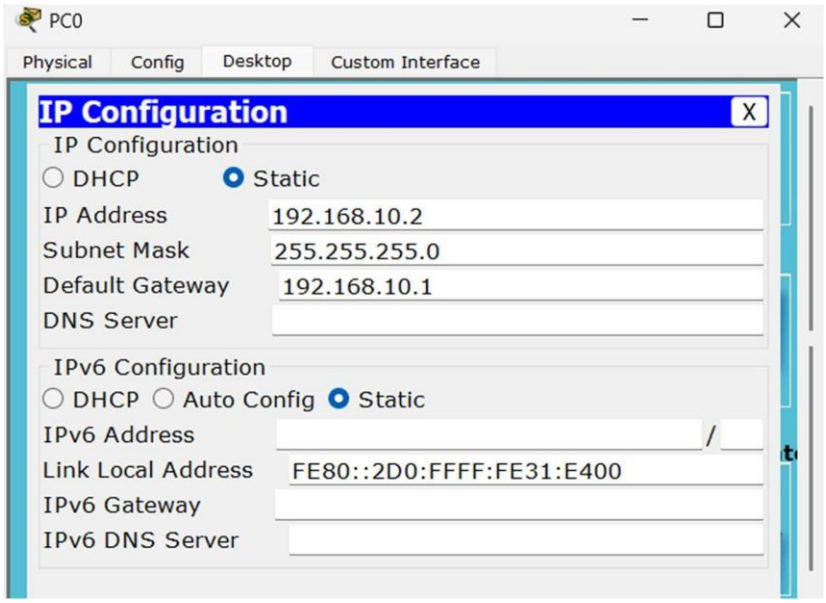
1. Place a router (Router0), two switches (Switch0 & Switch1) & four PCs (PC0, PC1, PC2 & PC3)
2. Connect PC0 & PC1 to Switch0 via ethernet
3. Connect PC2 & PC3 to Switch1 via ethernet
4. Connect Switch0 & Switch1 to Router0
5. In Router0,
    - 5.1. Goto Config > FastEthernet0/0
    - 5.2. Enter IP address 192.168.10.1 & Subnet Mask 255.255.255.0
    - 5.3. Turn on the port



5.4. Goto FastEthernet1/0
5.5. Enter IP address 192.168.20.1 & Subnet Mask 255.255.255.0
5.6. Turn on the port

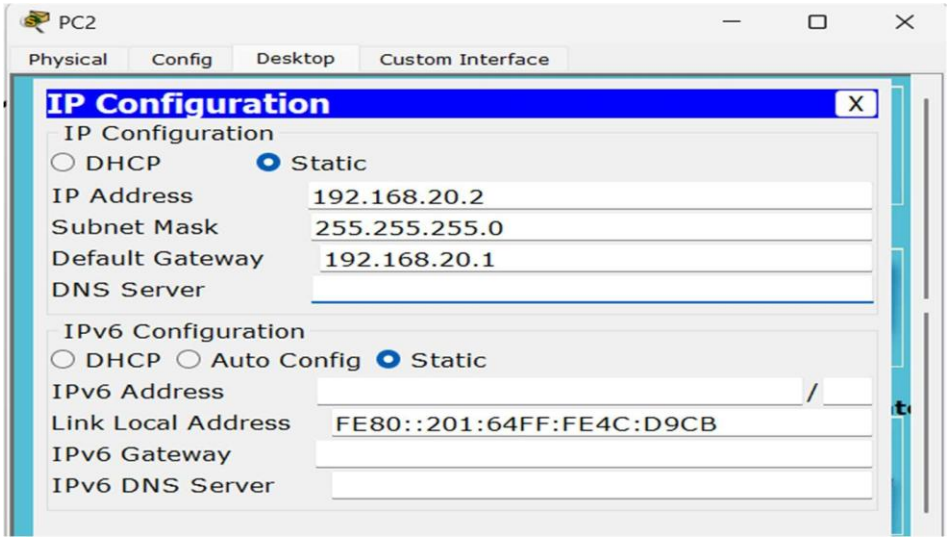


6. In PC0,
    6.1. Goto Desktop > IP Config
    6.2. Set IP address 192.168.10.2, Subnet Mask 255.255.255.0 & Default Gateway to IP address of router i.e 192.168.10.1



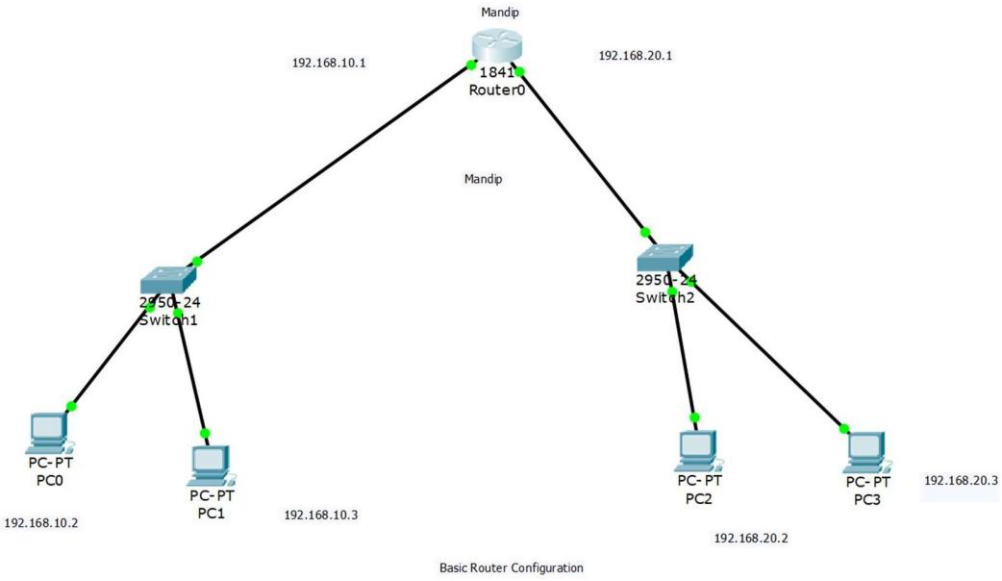
7. In PC1, Set IP address 192.168.10.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of router i.e 192.168.10.1

8. In PC2, Set IP address 192.168.20.2, Subnet Mask 255.255.255.0 & Default Gateway to IP address of router i.e 192.168.20.1



9. In PC3, Set IP address 192.168.20.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of router i.e 192.168.20.1

Layout



Testing

1. Goto Command Prompt of one PC (PC0)
2. Enter ping & IP of target PC (ping 192.168.20.3) & (ping 192.168.10.3)
3. If the target PC replies, the configuration is successful.

```
PC>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>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=0ms TTL=128
Reply from 192.168.10.3: bytes=32 time=0ms TTL=128
Reply from 192.168.10.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

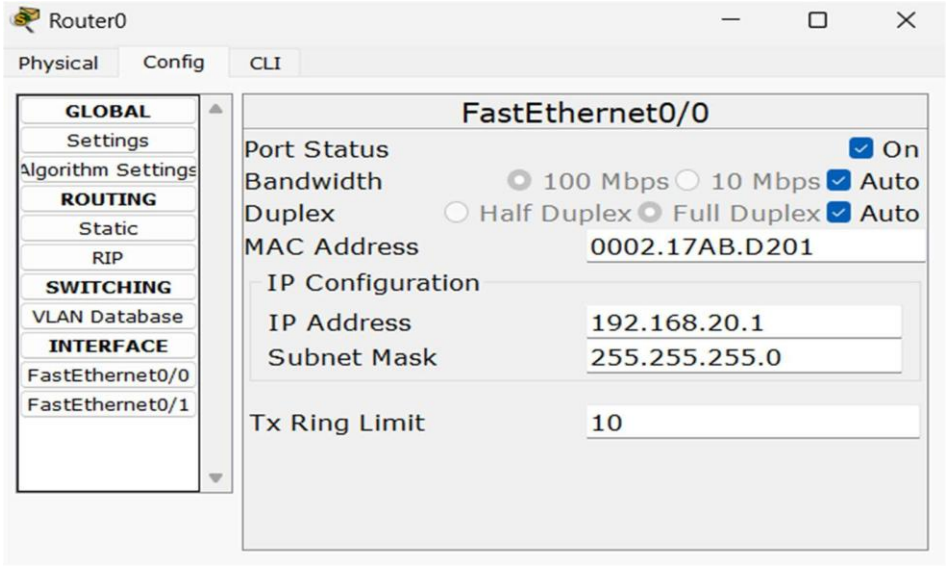
LAB 10: STATIC ROUTING CONFIGURATION

Static routing involves manually configuring the routing table on a router to specify the paths to reach specific destination networks.
It is a simple and efficient way to control routing in small networks with predictable traffic patterns. However, it requires manual configuration and does not adapt to changes in network topology automatically.

Configuration

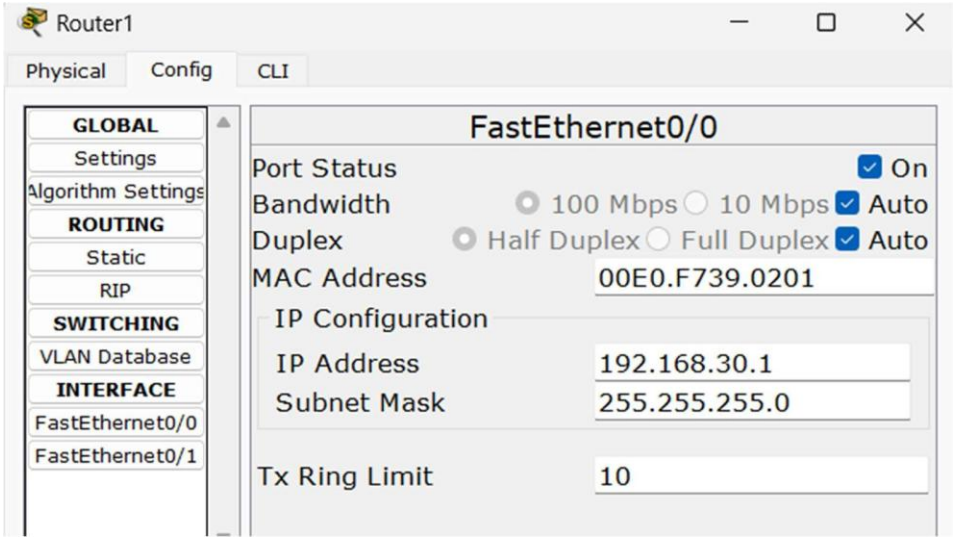
In Cisco Packet Tracer, Static Routing can be configured as follows:

1. Place two Routers (Router0 & Router1)
2. Place two Switches (Switch0 & Switch1)
3. Place four PCs (PC0, PC1, PC2 & PC3)
4. Connect PC0 & PC1 to Switch0
5. Connect PC2 & PC3 to Switch1
6. Connect Switch0 to Router0 & Switch1 to Router1
7. Connect Router0 & Router1
8. In Router0,
    8.1. Goto Config > FastEthernet0/0
    8.2. Enter IP address 192.168.20.1 & subnet mask 255.255.255.0
    8.3. Turn on the port



9. In Router1,
    9.1. Set IP address 192.168.30.1 & Subnet Mask 255.255.255.0 in FastEthernet0/0.

9.2. Set IP address 192.168.10.2 & Subnet Mask 255.255.255.0 in FastEthernet0/1

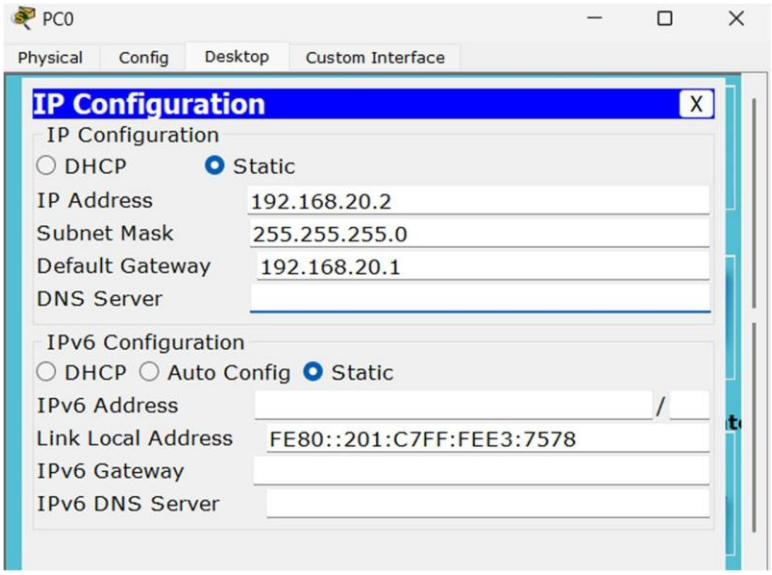


9.3. Turn on both ports

10. In PC0,

10.1 Goto Desktop > IP Config

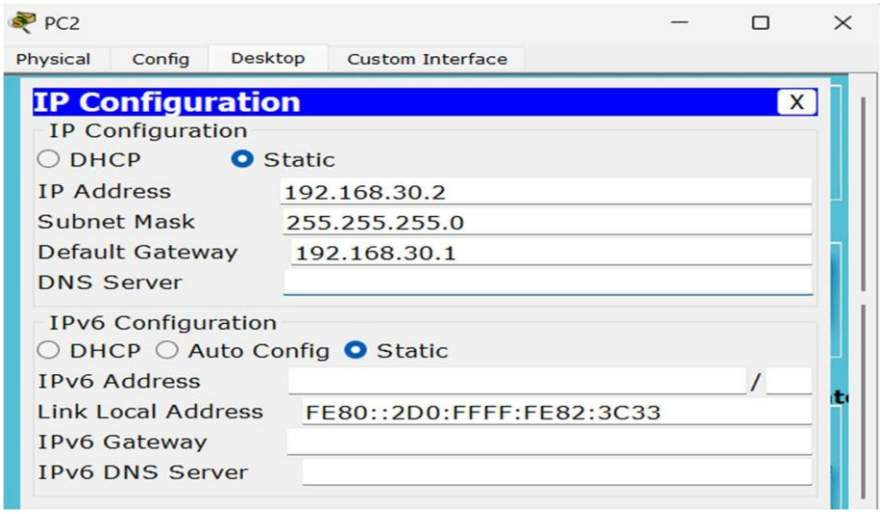
10.2. Set IP address 192.168.20.2, Subnet Mask 255.255.255.0 & Default Gateway same as IP address of Router0 i.e 192.168.20.1



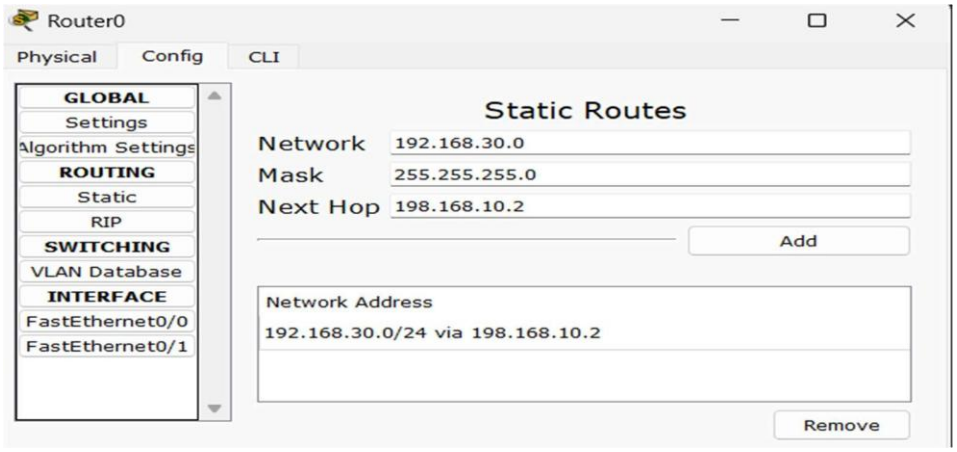
11. In PC1, Set IP address 192.168.20.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router0 i.e 192.168.20.1

12. In PC2, Set IP address 192.168.30.2, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router1 i.e 192.168.30.1

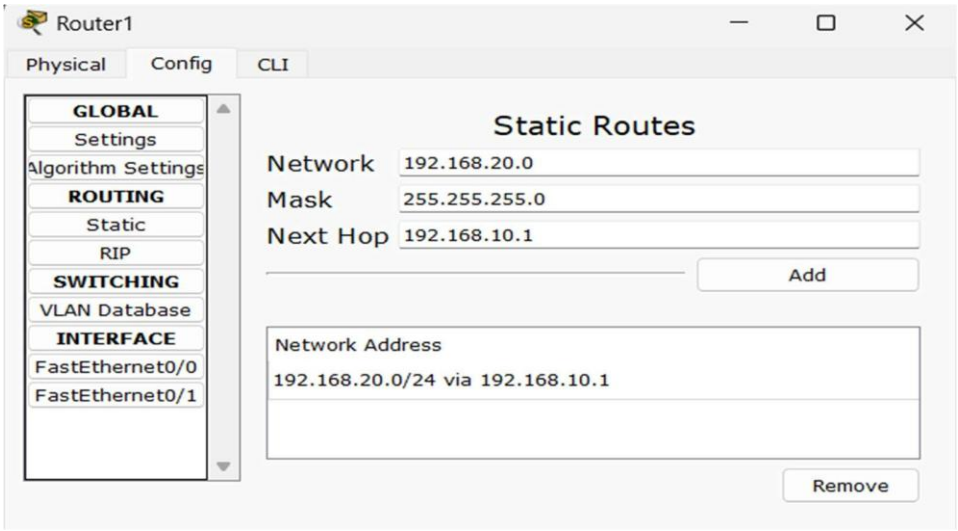
13. In PC3, Set IP address 192.168.30.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router1 i.e 192.168.30.1



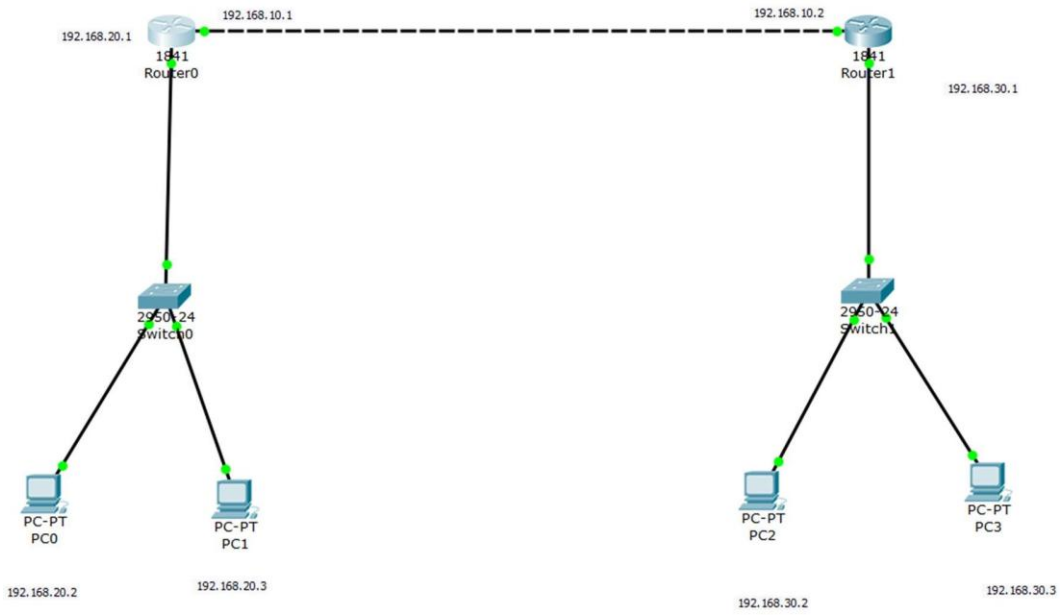
14. In Router0,
    14.1. Goto Config > Static
    14.2. Enter another router's network (192.168.30.0) in Network field
    14.3. Enter Subnet Mask 255.255.255.0 in Mask Field.
    14.4. Enter another router's IP address (192.168.10.2) in the Next Hop field.



15. In Router1,
    15.1. Goto Config > Static
    15.2. Enter another router's network (192.168.20.0) in Network field
    15.3. Enter Subnet Mask 255.255.255.0 in Mask Fields
    15.4. Enter another router's IP address (192.168.10.1) in Next Hop field.

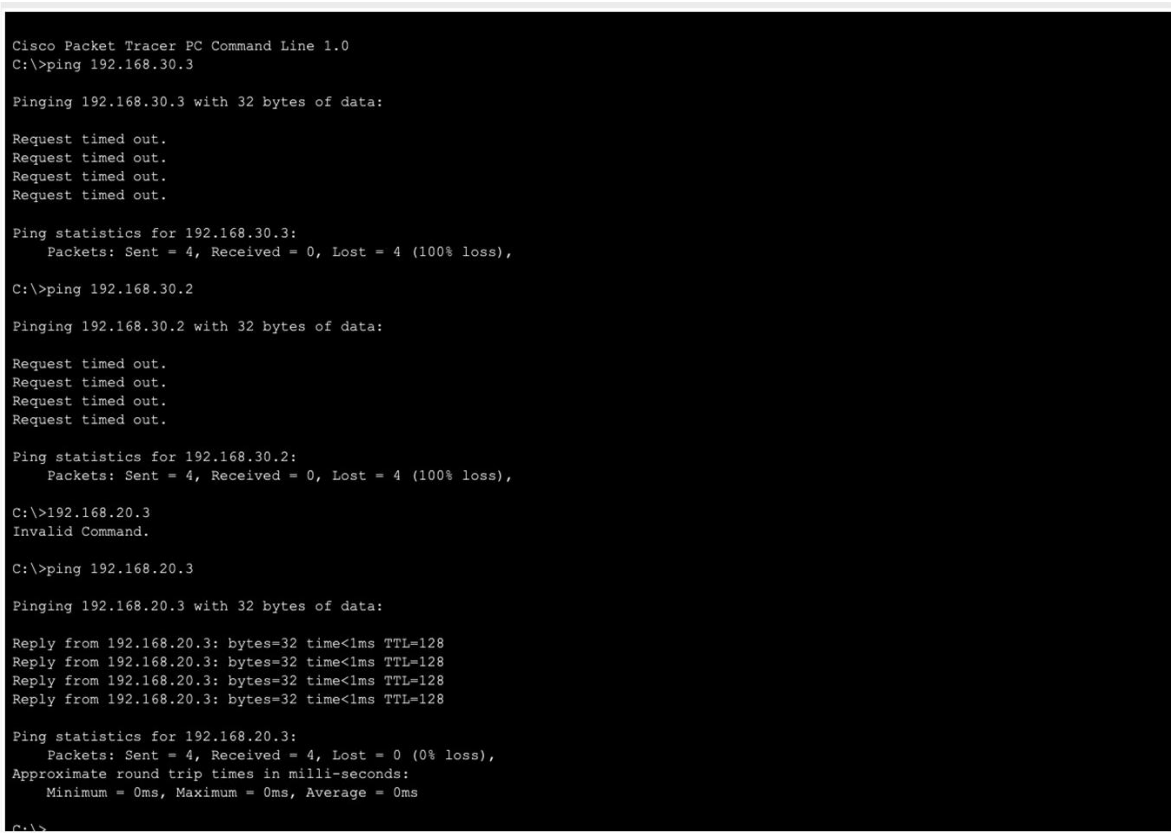

Router1
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Static Routes
Network 192.168.20.0
Mask 255.255.255.0
Next Hop 192.168.10.1
Add
Network Address
192.168.20.0/24 via 192.168.10.1
Remove

Layout


192.168.20.1
192.168.10.1
192.168.10.2
1841
Router0
1841
Router1
192.168.30.1
2950-24
Switch0
2950-24
Switch1
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
192.168.20.2
192.168.20.3
192.168.30.2
192.168.30.3

Testing

1. Goto Command Prompt of one PC (PC0).
2. Enter ping & IP of target PC (ping 192.168.30.3) & (ping 192.168.10.2).
3. If the target PC replies, the configuration is successful.



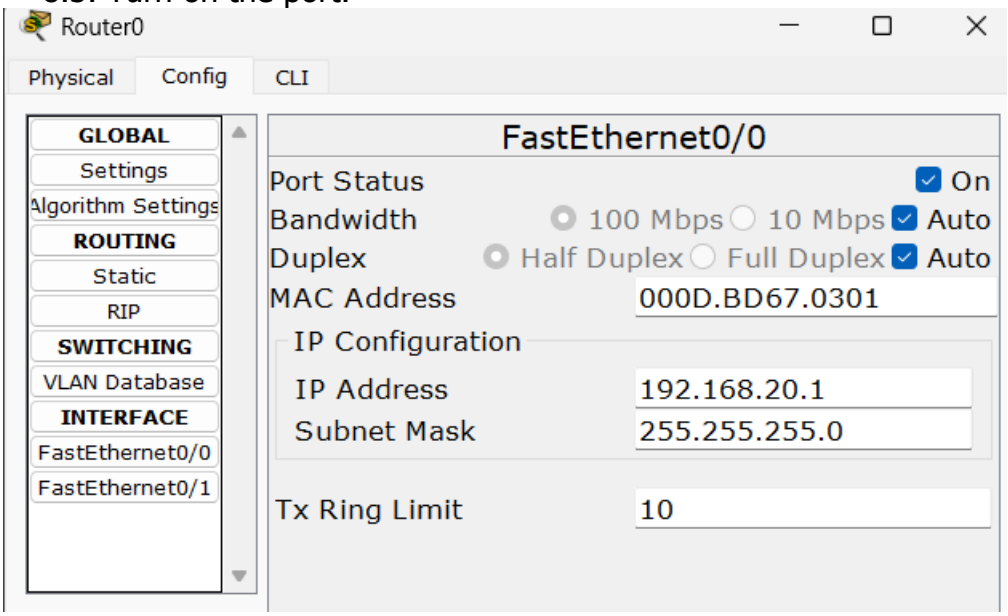
LAB 11: IMPLEMENTATION OF ROUTING INFORMATION PROTOCOL (RIP)

RIP or Routing Information Protocol is a distance-vector routing protocol used to dynamically exchange routing information between routers within a network. It operates based on hop count, where each router maintains a routing table containing the number of hops to reach each network.

Configuration

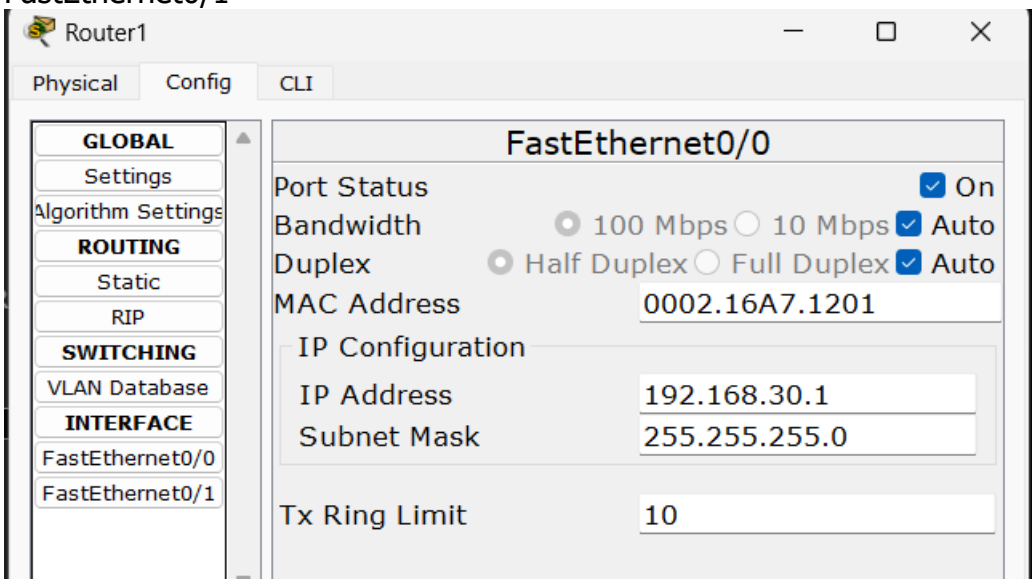
In Cisco Packet Tracer, RIP can be configured as follows:

1. Place two Routers (Router0 & Router1)
2. Place two Switches (Switch0 & Switch1)
3. Place four PCs (PC0, PC1, PC2 & PC3)
4. Connect PC0 & PC1 to Switch0
5. Connect PC2 & PC3 to Switch1
6. Connect Switch0 to Router0 & Switch1 to Router1
7. Connect Router0 & Router1
8. In Router0,
   8.1. Goto Config > FastEthernet0/0
   8.2. Enter IP address 192.168.20.1 & subnet mask 255.255.255.0
   8.3. Turn on the port.



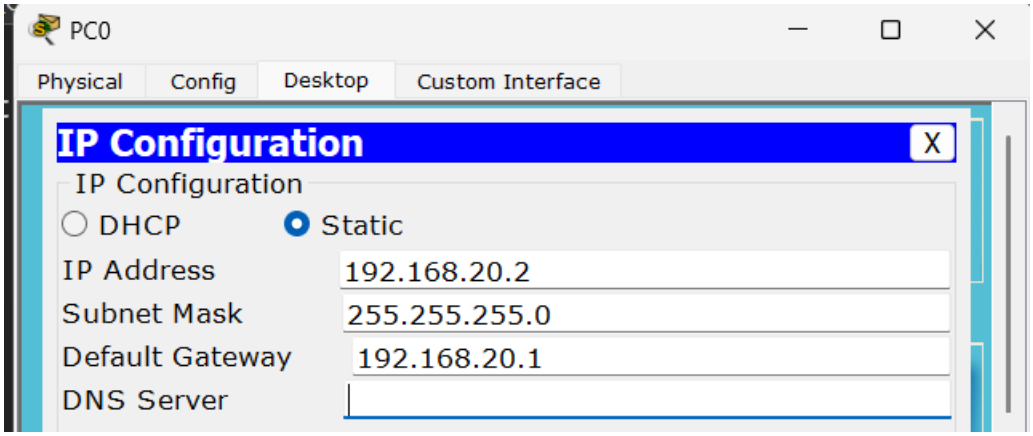
   8.4. Goto FastEthernet0/1
   8.5. Enter IP address 192.168.10.1 & Subnet Mask 255.255.255.0
   8.6. Turn on the port.

9. In Router1,
   9.1. Set IP address 192.168.30.1 & Subnet Mask 255.255.255.0 in FastEthernet0/0
   9.2. Set IP address 192.168.10.2 & Subnet Mask 255.255.255.0 in FastEthernet0/1

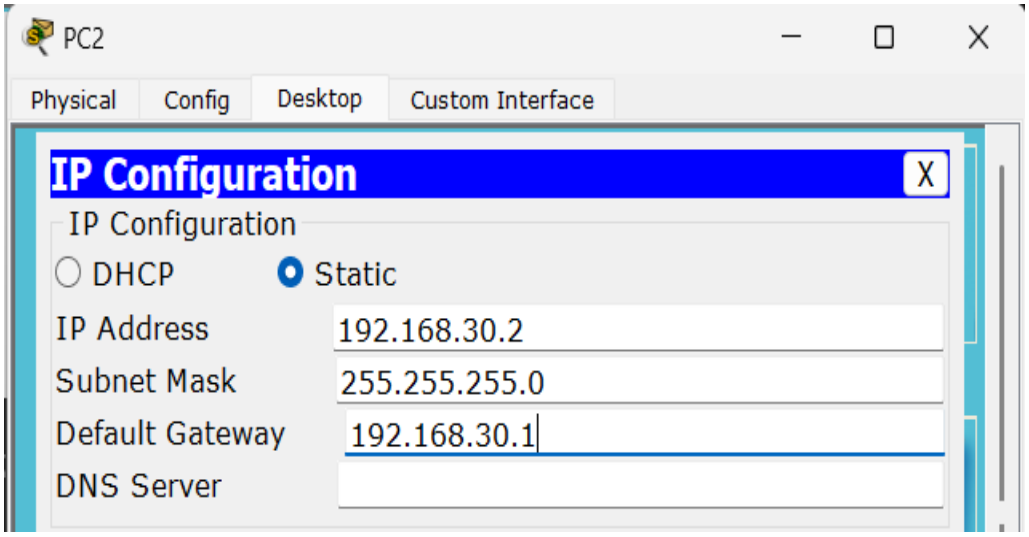


   9.3. Turn on both ports

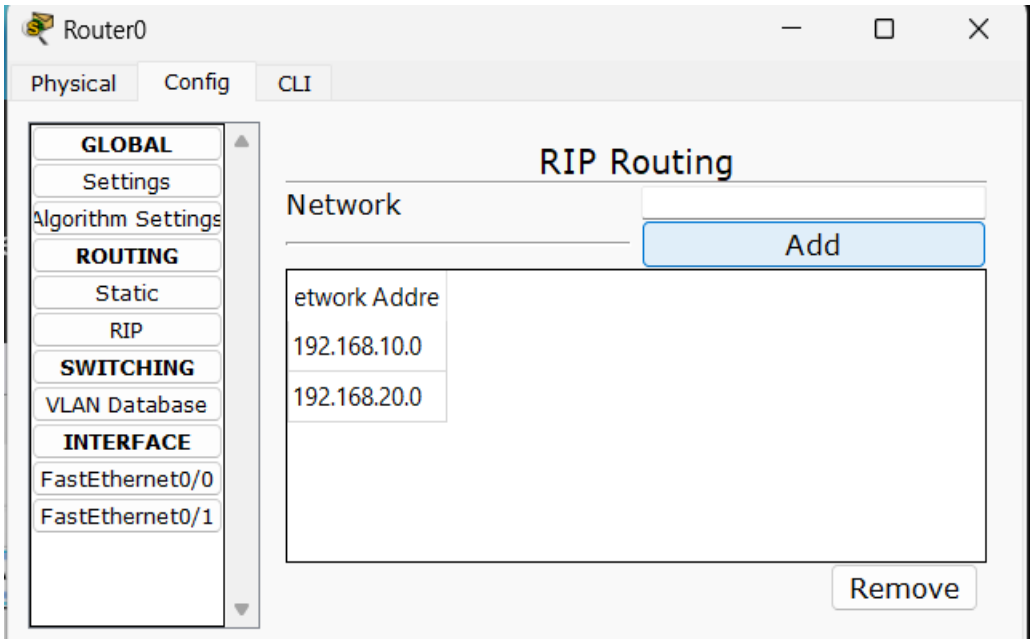
10. In PC0,
   10.1 Goto Desktop > IP Config
   10.2 Set IP address 192.168.20.2, Subnet Mask 255.255.255.0 & Default Gateway same as IP address of Router0 i.e 192.168.20.1



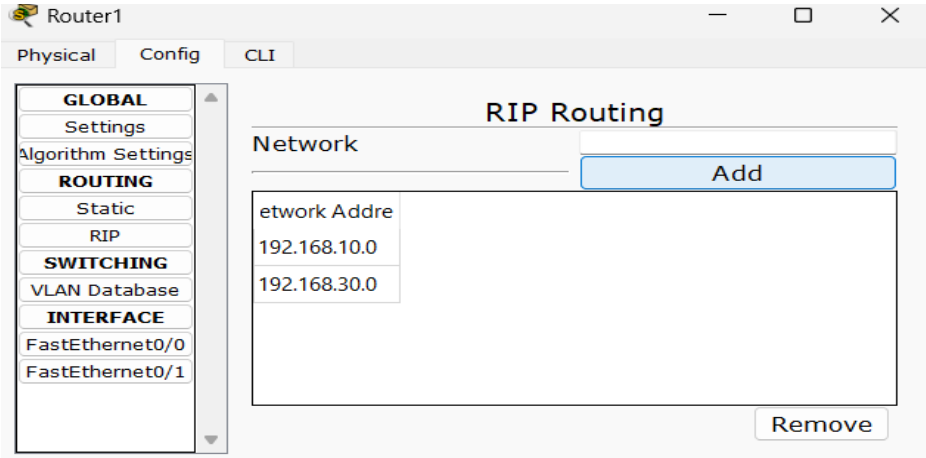
11. In PC1, Set IP address 192.168.20.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router0 i.e 192.168.20.1
12. In PC2, Set IP address 192.168.30.2, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router1 i.e 192.168.30.1
13. In PC3, Set IP address 192.168.30.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router1 i.e 192.168.30.1



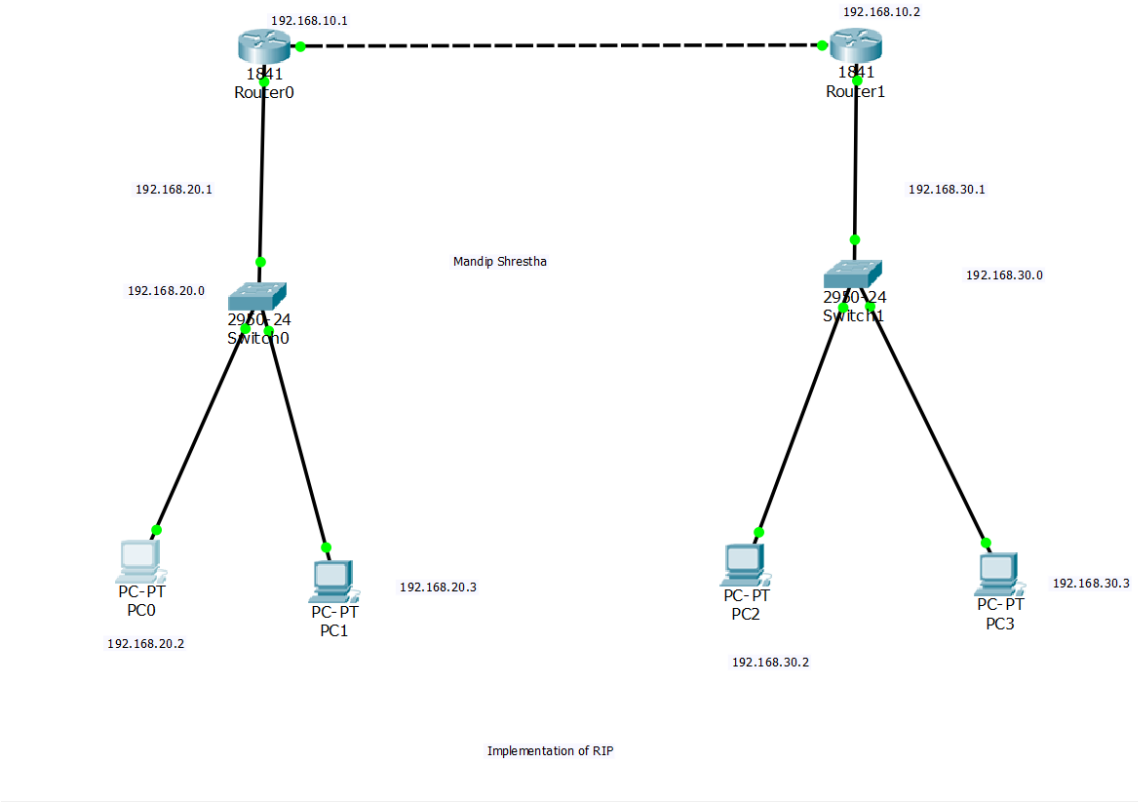
14. In Router0,
    14.1. Goto Config > RIP
    14.2. Enter two networks associated with Router0 in Network field i.e 192.168.10.0 &192.168.20.0



15. Repeat the process for Router1
    15.1. Enter IP addresses 192.168.10.0 & 192.168.30.0

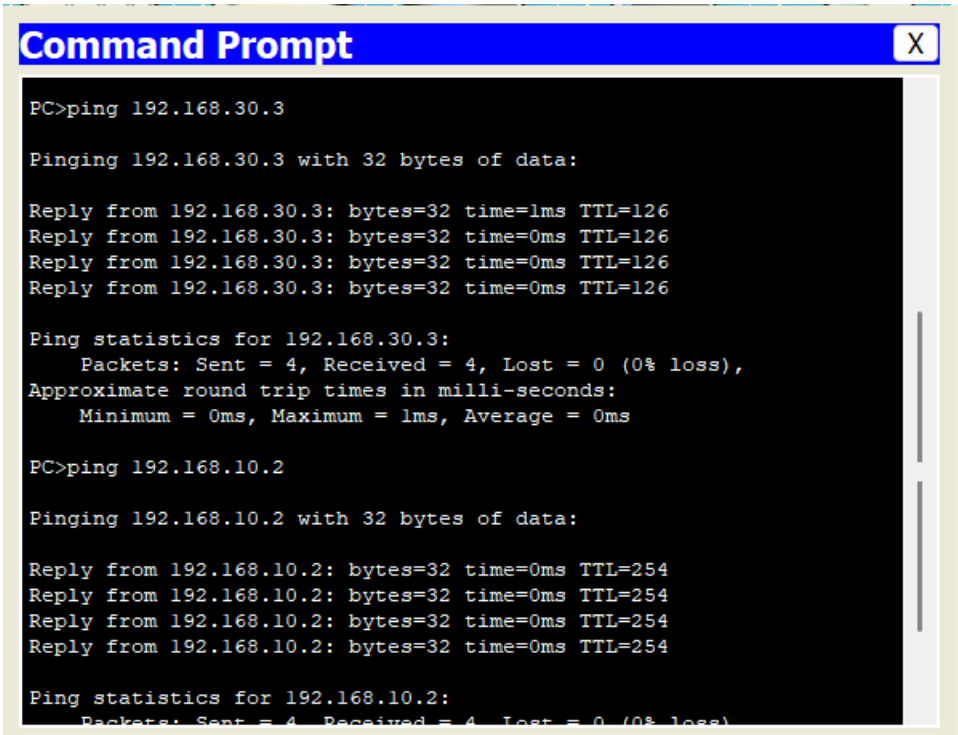


Layout



Testing

1. Goto Command Prompt of one PC (PC0)
2. Enter ping & IP of target PC (ping 192.168.30.3) & (ping 192.168.10.2)
3. If the target PC replies, the configuration is successful.



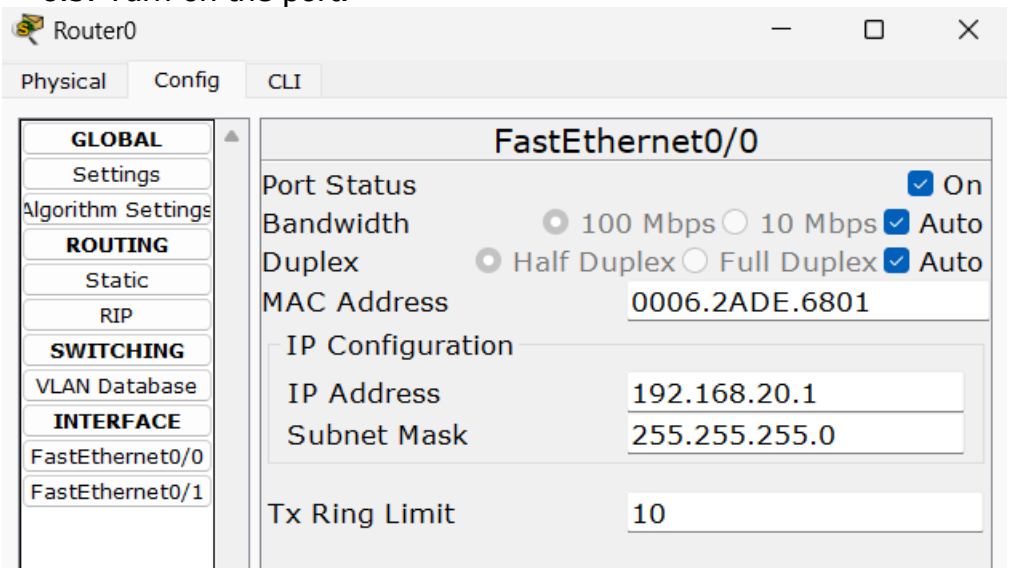
LAB 12: IMPLEMENTATION OF OPEN SHORTEST PATH FIRST PROTOCOL (OSPF)

OSPF, or Open Shortest Path First, is an Interior Gateway Protocol (IGP) primarily used within autonomous systems to facilitate intra-domain routing. It operates based on a link-state routing algorithm, where routers exchange information about their directly connected neighbors and the state of those links. OSPF calculates the shortest path to each destination network using a cost metric based on bandwidth.

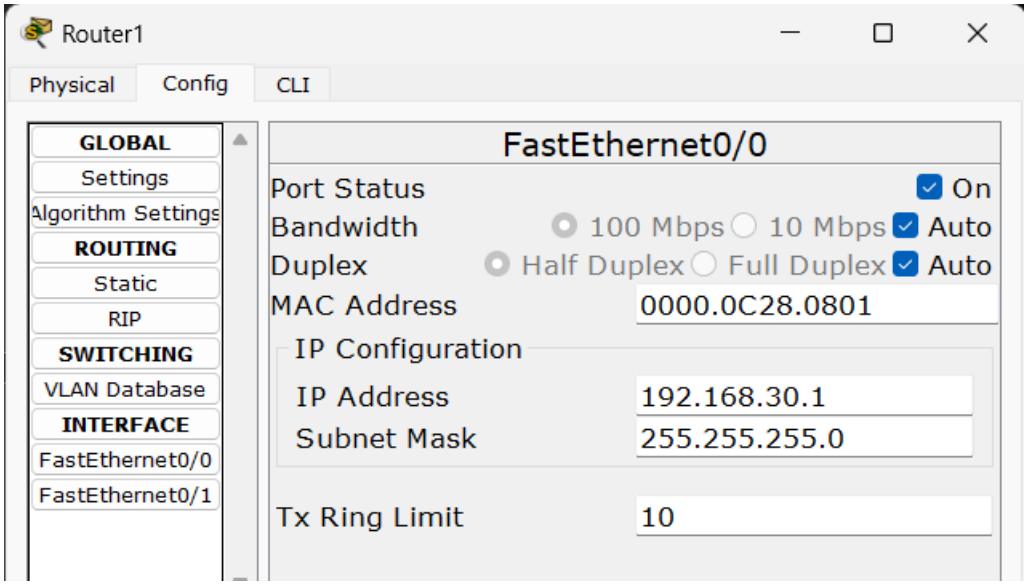
Configuration

In Cisco Packet Tracer, OSPF can be configured as follows:

1. Place two Routers (Router0 & Router1)
2. Place two Switches (Switch0 & Switch1)
3. Place four PCs (PC0, PC1, PC2 & PC3)
4. Connect PC0 & PC1 to Switch0
5. Connect PC2 & PC3 to Switch1
6. Connect Switch0 to Router0 & Switch1 to Router1
7. Connect Router0 & Router1
8. In Router0,
   8.1. Goto Config > FastEthernet0/0
   8.2. Enter IP address 192.168.20.1 & subnet mask 255.255.255.0
   8.3. Turn on the port.



   8.4. Goto FastEthernet0/1
   8.5. Enter IP address 192.168.10.1 & Subnet Mask 255.255.255.0
   8.6. Turn on the port.
9. In Router1,
   9.1. Set IP address 192.168.30.1 & Subnet Mask 255.255.255.0 in FastEthernet0/0



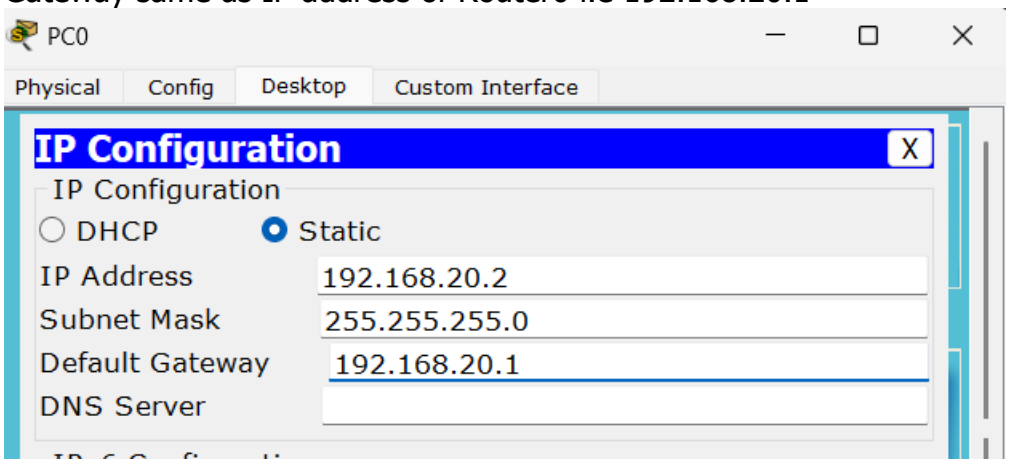
9.2. Set IP address 192.168.10.2 & Subnet Mask 255.255.255.0 in FastEthernet0/1

9.3. Turn on both ports.

10. In PC0,

10.1. 10.2. Goto Desktop > IP Config

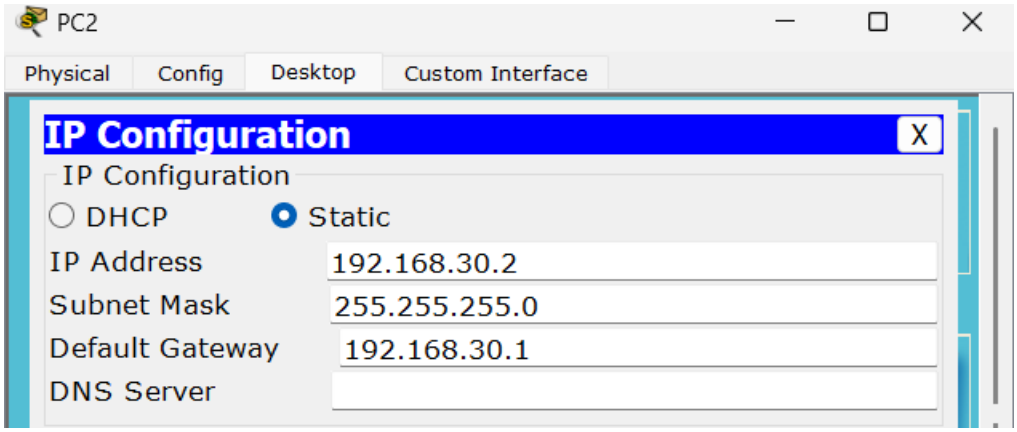
10.2 Set IP address 192.168.20.2, Subnet Mask 255.255.255.0 & Default Gateway same as IP address of Router0 i.e 192.168.20.1



11. In PC1, Set IP address 192.168.20.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router0 i.e 192.168.20.1

12. In PC2, Set IP address 192.168.30.2, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router1 i.e 192.168.30.1

13. In PC3, Set IP address 192.168.30.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router1 i.e 192.168.30.1

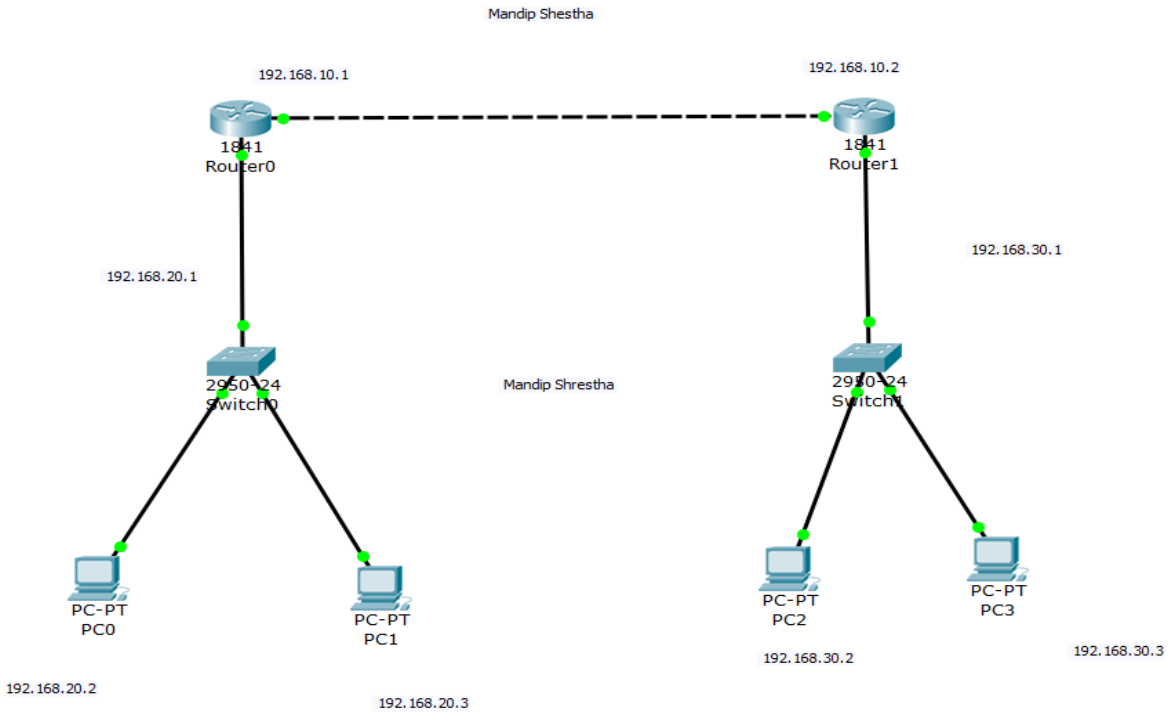


14. In Router0, Open CLI mode & enter following commands
Router>enable
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
```

15. In Router1, Open CLI mode & enter following commands
Router>enable
Router#configure terminal
Router(config)#router ospf 2
Router(config-router)#network 192.168.30.0 0.0.0.255 area 0
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#

Layout



Implementation of OSPF

Testing

1. Goto Command Prompt of one PC (PC0)
2. Enter ping & IP of target PC (ping 192.168.30.3) & (ping 192.168.10.2)
3. If the target PC replies, the configuration is successful.

```
PC>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=1ms TTL=126
Reply from 192.168.30.3: bytes=32 time=1ms TTL=126
Reply from 192.168.30.3: bytes=32 time=0ms TTL=126
Reply from 192.168.30.3: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>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=254
Reply from 192.168.10.2: bytes=32 time=0ms TTL=254
Reply from 192.168.10.2: bytes=32 time=0ms TTL=254
Reply from 192.168.10.2: bytes=32 time=0ms TTL=254

Ping statistics for 192.168.10.2:
```

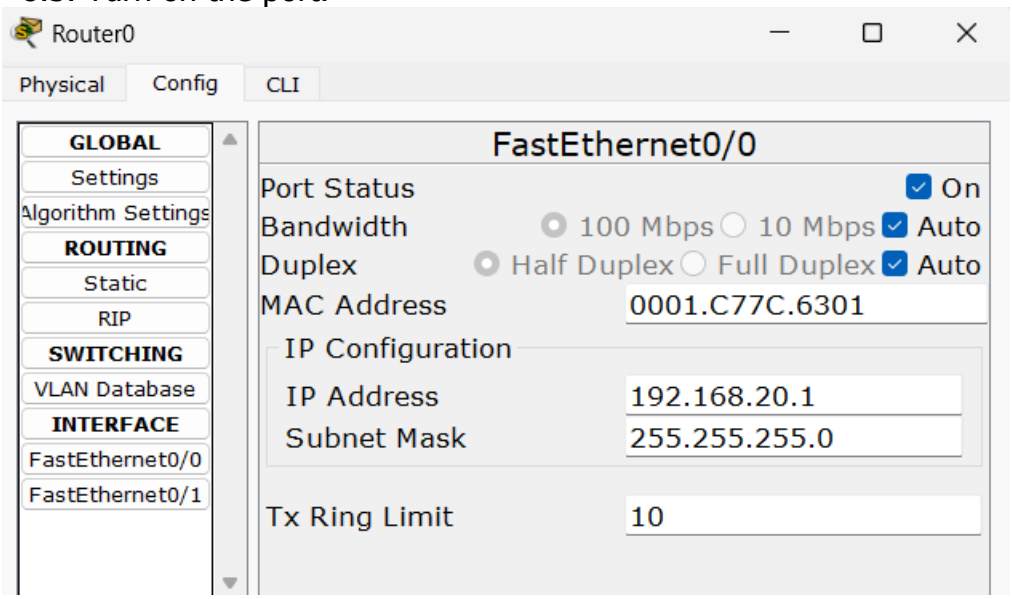
LAB 13: IMPLEMENTATION OF BORDER GATEWAY PROTOCOL (BGP)

BGP (Border Gateway Protocol) is an exterior gateway protocol designed for inter-domain routing between autonomous systems (AS) on the Internet. Unlike interior gateway protocols like OSPF, which operate within a single autonomous system, BGP is used to exchange routing and reachability information across AS boundaries. BGP utilizes path attributes such as autonomous system path length, route preference, and various policy-based attributes to determine the best path to a destination network. It operates on a path-vector algorithm and establishes TCP connections between BGP peers for reliable communication.

Configuration

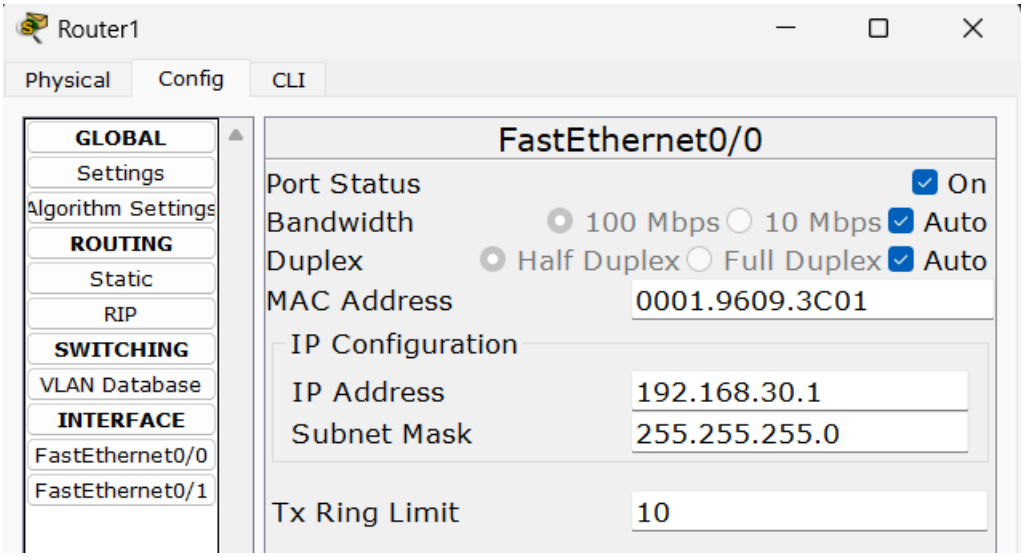
In Cisco Packet Tracer, BGP can be configured as:

1. Place two Routers (Router0 & Router1)
2. Place two Switches (Switch0 & Switch1)
3. Place four PCs (PC0, PC1, PC2 & PC3)
4. Connect PC0 & PC1 to Switch0
5. Connect PC2 & PC3 to Switch1
6. Connect Switch0 to Router0 & Switch1 to Router1
7. Connect Router0 & Router1
8. In Router0,
   8.1. Goto Config > FastEthernet0/0
   8.2. Enter IP address 192.168.20.1 & subnet mask 255.255.255.0
   8.3. Turn on the port.



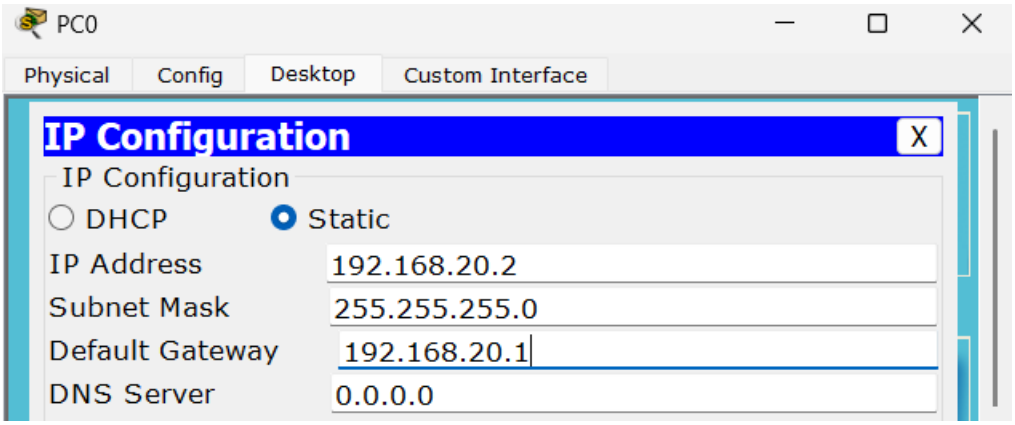
   8.4. Goto FastEthernet0/1
   8.5. Enter IP address 192.168.10.1 & Subnet Mask 255.255.255.0
   8.6. Turn on the port.

9. In Router1,
9.1. Set IP address 192.168.30.1 & Subnet Mask 255.255.255.0 in FastEthernet0/0



9.2. Set IP address 192.168.10.2 & Subnet Mask 255.255.255.0 in FastEthernet0/1
9.3. Turn on both ports.

10. In PC0,
10.1.Goto Desktop > IP Config
10.2.Set IP address 192.168.20.2, Subnet Mask 255.255.255.0 & Default Gateway same as IP address of Router0 i.e 192.168.20.1



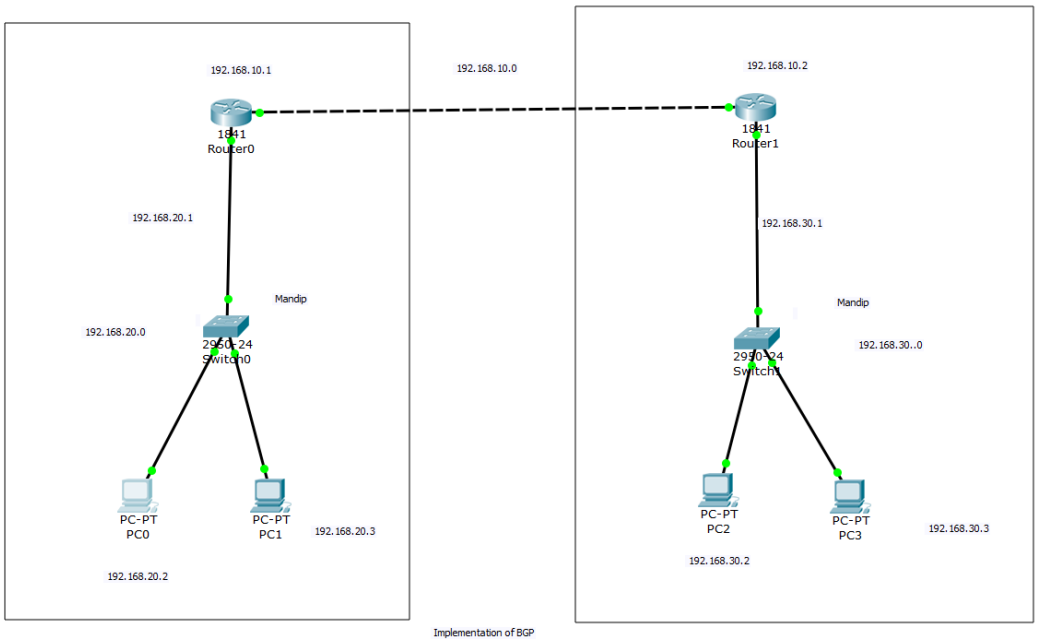
11. In PC1, Set IP address 192.168.20.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router0 i.e 192.168.20.1
12. In PC2, Set IP address 192.168.30.2, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router1 i.e 192.168.30.1
13. In PC3, Set IP address 192.168.30.3, Subnet Mask 255.255.255.0 & Default Gateway to IP address of Router1 i.e 192.168.30.1

14. In Router0, Open CLI mode & enter following commands
Router>enable
Router#configure terminal
Router(config)#router bgp 100
Router(config-router)#neighbor 192.168.10.2 remote-as 200
Router(config-router)#network 192.168.20.0 mask 255.255.255.0
Router(config-router)#exit
Router(config)#exit
Router#

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router bgp 100
Router(config-router)#neighbor 192.168.10.2  remote-as 200
Router(config-router)#network 192.168.20.0 mask 255.255.255.0
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

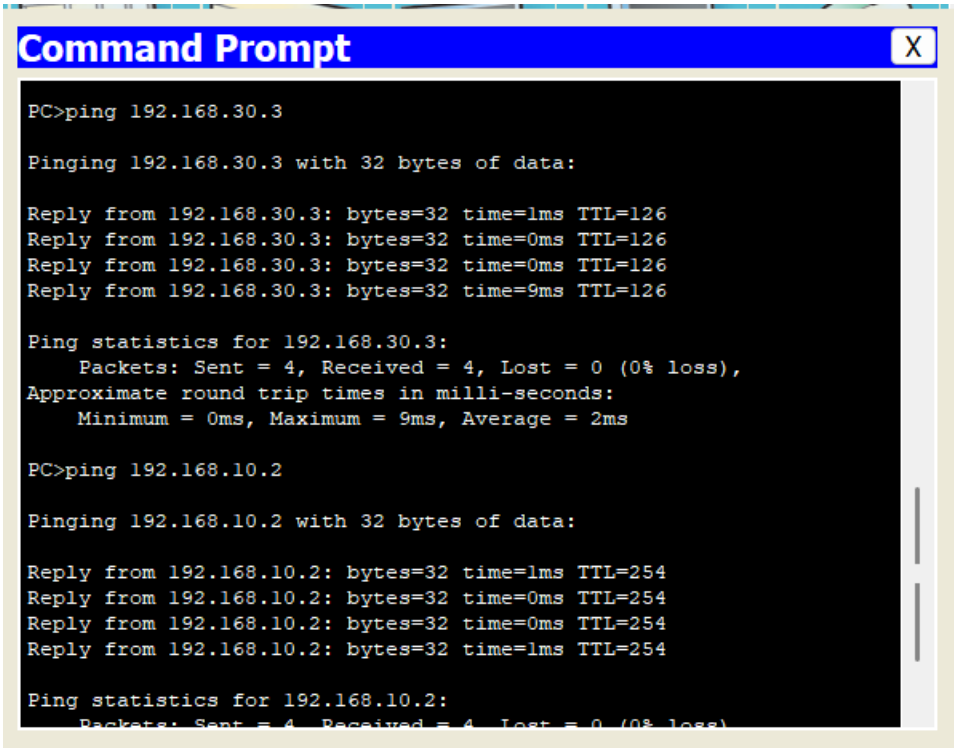
15. In Router1, Open CLI mode & enter following commands
Router>enable
Router#configure terminal
Router(config)#router bgp 200
Router(config-router)#neighbor 192.168.10.1 remote-as 100
Router(config-router)#network 192.168.30.0 mask 255.255.255.0
Router(config-router)#exit
Router(config)#

Layout



Testing

1. Goto Command Prompt of one PC (PC0)
2. Enter ping & IP of target PC (ping 192.168.30.3) & (ping 192.168.10.2)
3. If the target PC replies, the configuration is successful.



LAB 14: CONFIGURATION OF DOMAIN NAME SYSTEM (DNS) SERVER

The Domain Name System (DNS) is a distributed and hierarchical naming service that enables the identification of computers, services, and other resources connected to the Internet or private networks. It converts user-friendly domain names into numerical IP addresses, which are required to direct network traffic accurately.

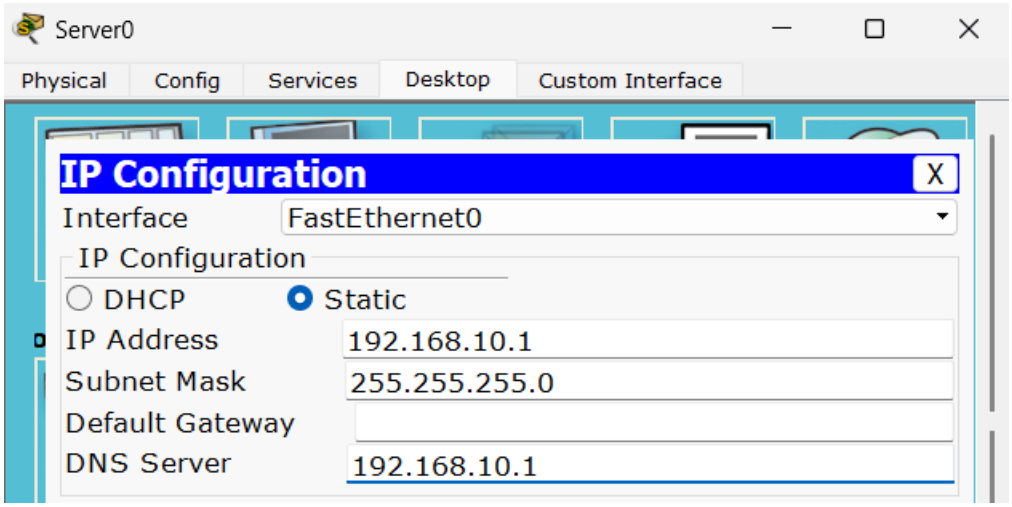
DNS servers are specialized computers that manage a database of public IP addresses linked to domain names. They play a key role in translating domain names into IP addresses and vice versa. When a user enters a domain name into a browser, the DNS server converts it into the associated IP address, allowing the browser to connect to the intended server.

These servers are essential for translating domain names into IP addresses, thus enabling seamless device communication on the Internet. Additionally, DNS servers provide vital services like load balancing, fault tolerance, and mail server configuration, supporting stable and efficient network functionality.

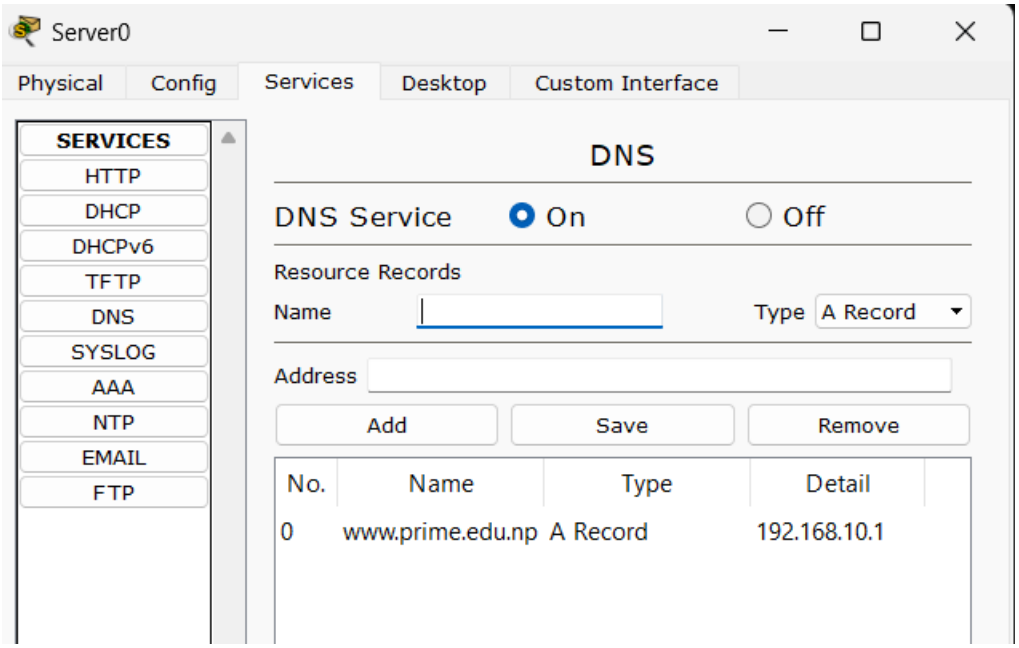
Configuration

In Cisco Packet Tracer, a DNS Server can be configured as follows:

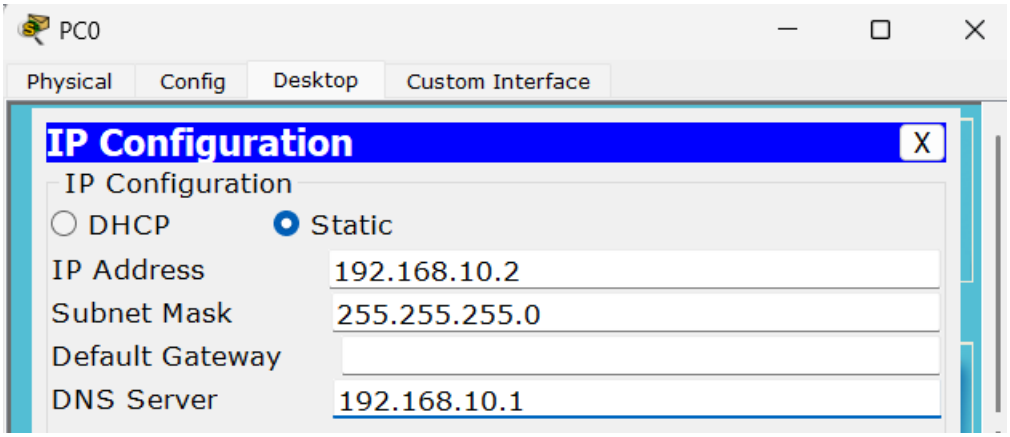
1. 2. Place a Server (Server0), a Switch (Switch0) & a PC (PC0)
Connect Server & PC to the Switch
3. In Server,
3.1. Goto Desktop > IP Configuration
3.2. Assign IP address 192.168.10.1, Subnet Mask 255.255.255.0 & DNS Server same as the IP address of server i.e 192.168.10.1



3.3. Goto Services > DNS
3.4. Enter domain name (www.prime.edu.np) in Name field
3.5. Enter DNS Server IP address (192.168.10.1) in Address field
3.6. Add & save
3.7. Turn on DNS service.

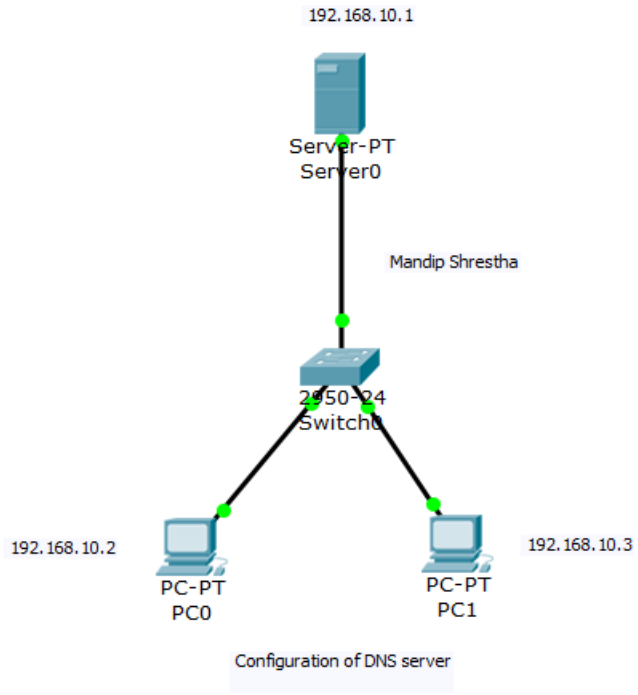


4. In PC0,
4.1. Goto Desktop > IP Configuration
4.2. Assign IP address 192.168.10.2, Subnet Mask 255.255.255.0 & DNS Server to IP address of DNS Server i.e 192.168.10.1



5. In PC1, Enter IP address 192.168.10.3, Subnet Mask 255.255.255.0 & DNS Server to IP address of DNS Server i.e 192.168.10.1

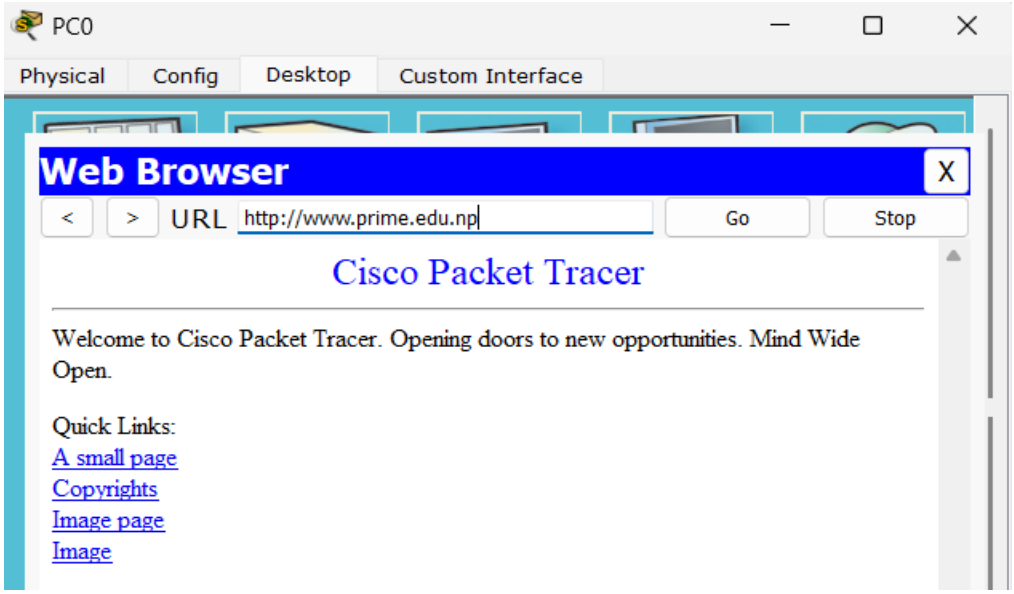
Layout



Testing

The configuration can be tested as follows:

1. In PC0, Goto Desktop > Web Browser
2. Enter www.prime.edu.np in URL field & Press Go. The webpage in DNS server will be displayed.



LAB 15: CONFIGURATION OF WEB SERVER

Web server is software or hardware that serves content, such as web pages, to clients over the internet. It processes incoming requests from clients, retrieves the requested resources, and sends them back to the clients, typically using HTTP or HTTPS protocols.

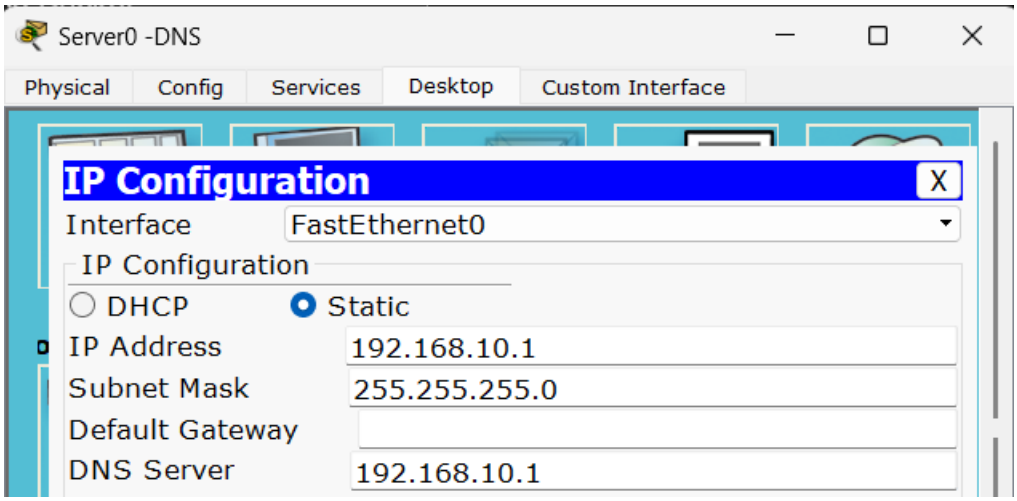
Configuration

In this lab, web server is configured along with a DNS server. In Cisco Packet Tracer, a Web Server
can be configured as follows:

1. Place two Servers (Server0 - DNS & Server1 - Web), a Switch (Switch0) & a PC (PC0)
2. Connect the Servers & PC to the Switch
3. In Server0 - DNS,

3.1. Goto Desktop > IP Configuration

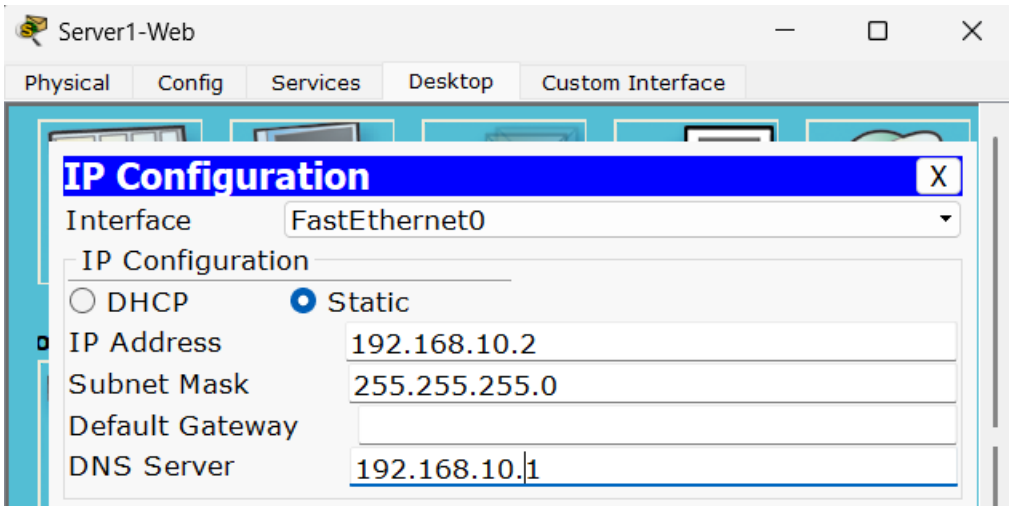
3.2. Assign IP address 192.168.10.1, Subnet Mask 255.255.255.0 & DNS Server same as the IP address of server i.e 192.168.10.1



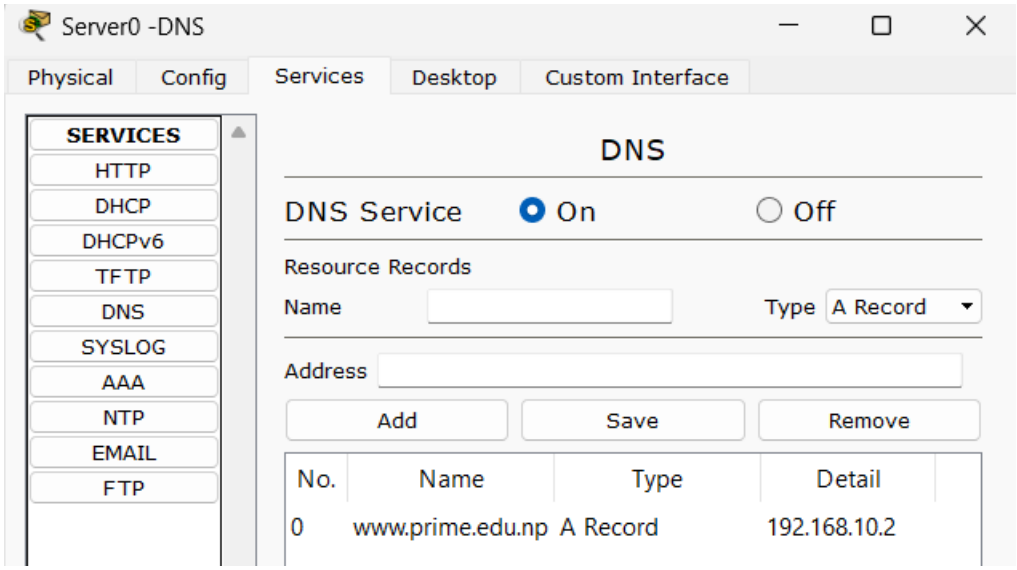
4. In Server1 – Web,

4.1. Goto Desktop > IP Configuration

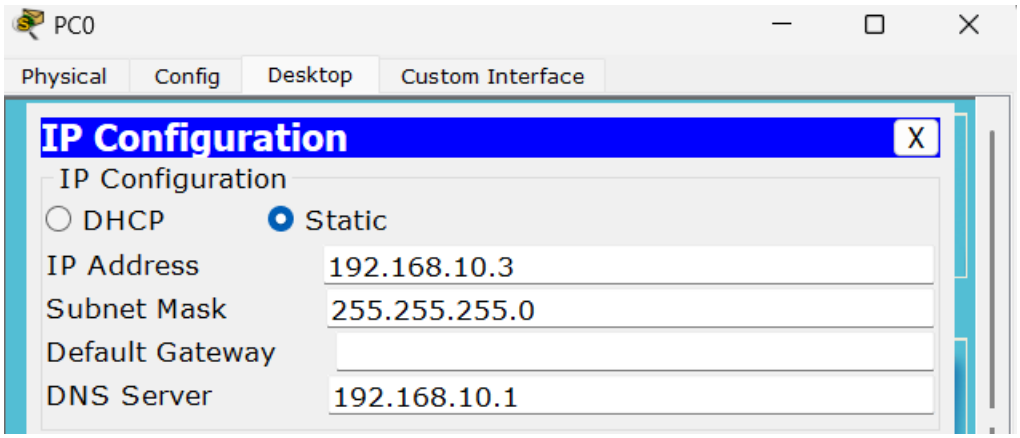
4.2. Assign IP address 192.168.10.2, Subnet Mask 255.255.255.0 & DNS Server same as the IP address of DNS server i.e 192.168.10.1



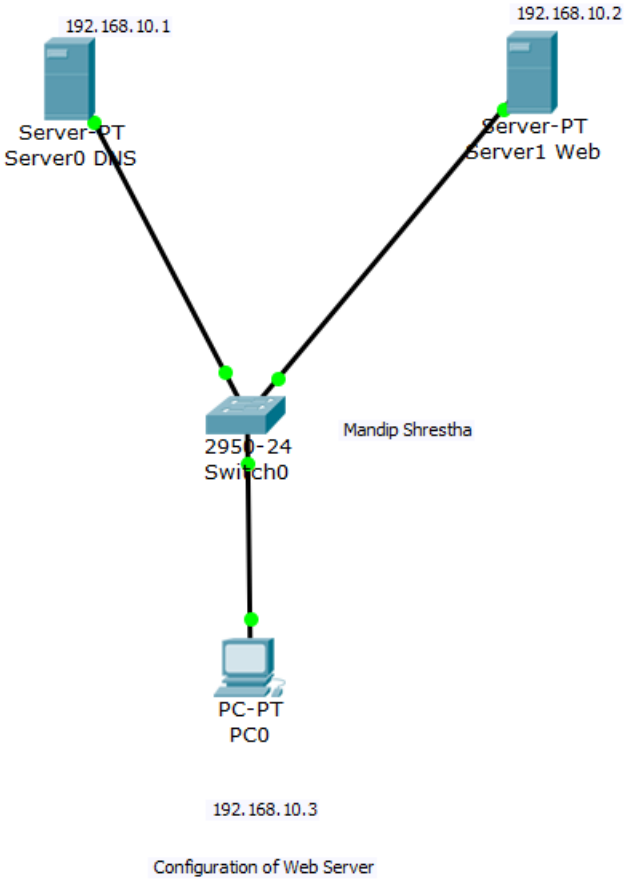
5. In Server 0 – DNS,
5.1. Goto Services > DNS
5.2. Enter domain name (www.prime.edu.np) in Name field
5.3. Enter Web Server IP address (192.168.10.2) in Address field
5.4. Add & save
5.5. Turn on DNS service.



6. In PC0,
6.1. Goto Desktop > IP Configuration
6.2. Assign IP address 192.168.10.3, Subnet Mask 255.255.255.0 & DNS Server to IP address of DNS Server i.e 192.168.10.1

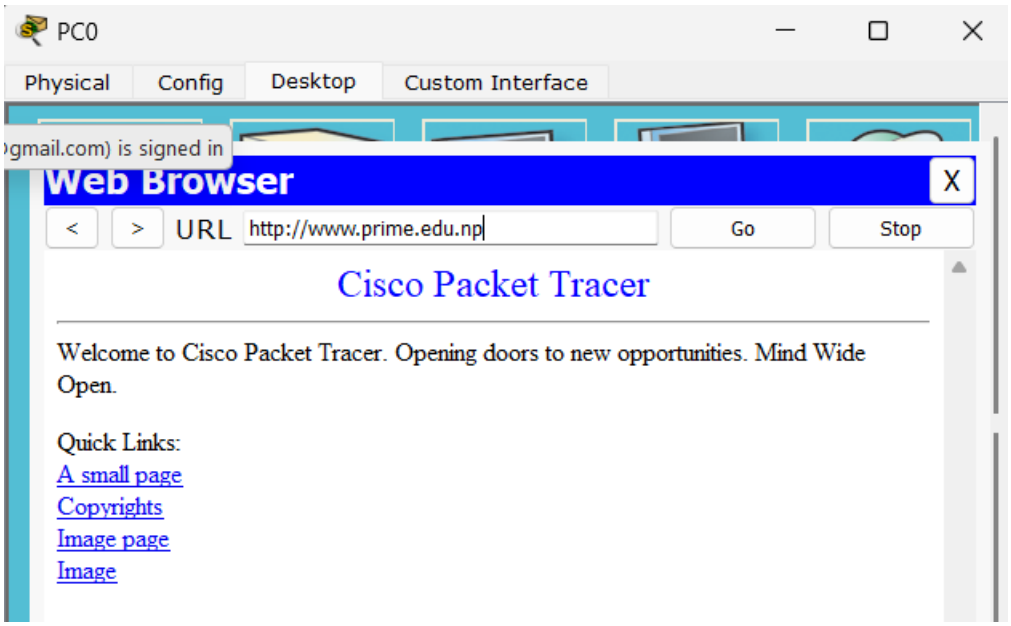

PC0
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.10.3
Subnet Mask
255.255.255.0
Default Gateway
DNS Server
192.168.10.1

Layout


192.168.10.1
192.168.10.2
Server-PT
Server0 DNS
Server-PT
Server1 Web
2950-24
Switch0
Mandip Shrestha
PC-PT
PC0
192.168.10.3
Configuration of Web Server

Testing

1. In PC0, Goto Desktop > Web Browser
2. Enter www.prime.edu.np in URL field & Press Go. The webpage in DNS server will be displayed.



LAB 16: CONFIGURATION OF FTP SERVER

FTP, or File Transfer Protocol, is a standard network protocol used for transferring files between a client and a server on a computer network. It allows users to upload, download, and manage files on remote servers securely and efficiently.

FTP server is a software application or hardware device that implements the FTP protocol and provides file transfer services to clients over a network. It is used to facilitate secure file transfer and sharing between clients and servers over a computer network, enabling efficient management of files and data storage.

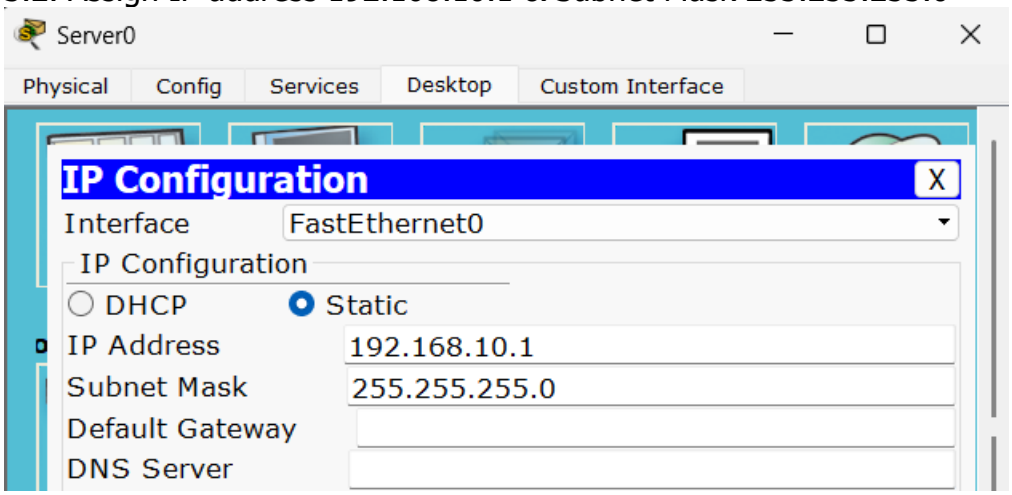
Configuration

In Cisco Packet Tracer, an FTP Server can be configured as follows:

1. Place a Server (Server0), a Switch (Switch0) & two PCs (PC0 & PC1)
2. Connect the Server & PCs to the Switch
3. In Server,

3.1. Goto Desktop > IP Configuration

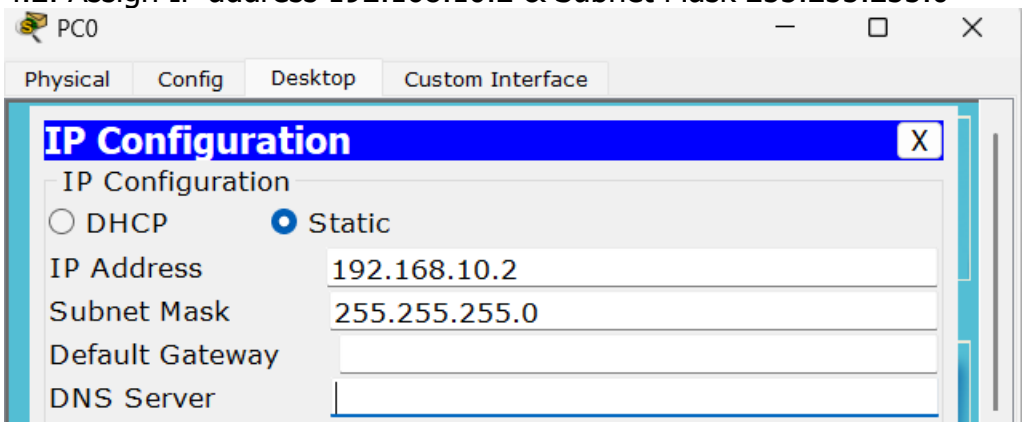
3.2. Assign IP address 192.168.10.1 & Subnet Mask 255.255.255.0



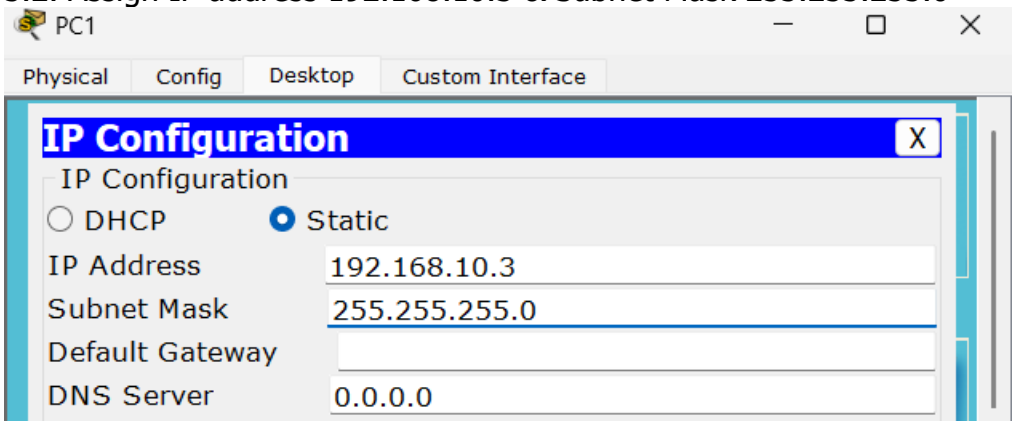
4. In PC0,

4.1. Goto Desktop > IP Configuration

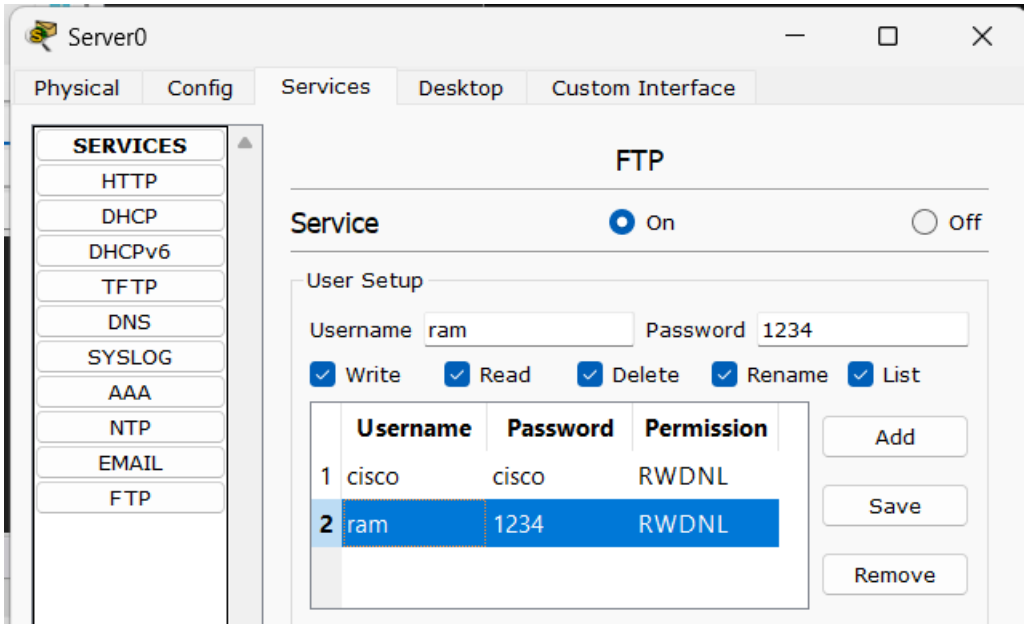
4.2. Assign IP address 192.168.10.2 & Subnet Mask 255.255.255.0



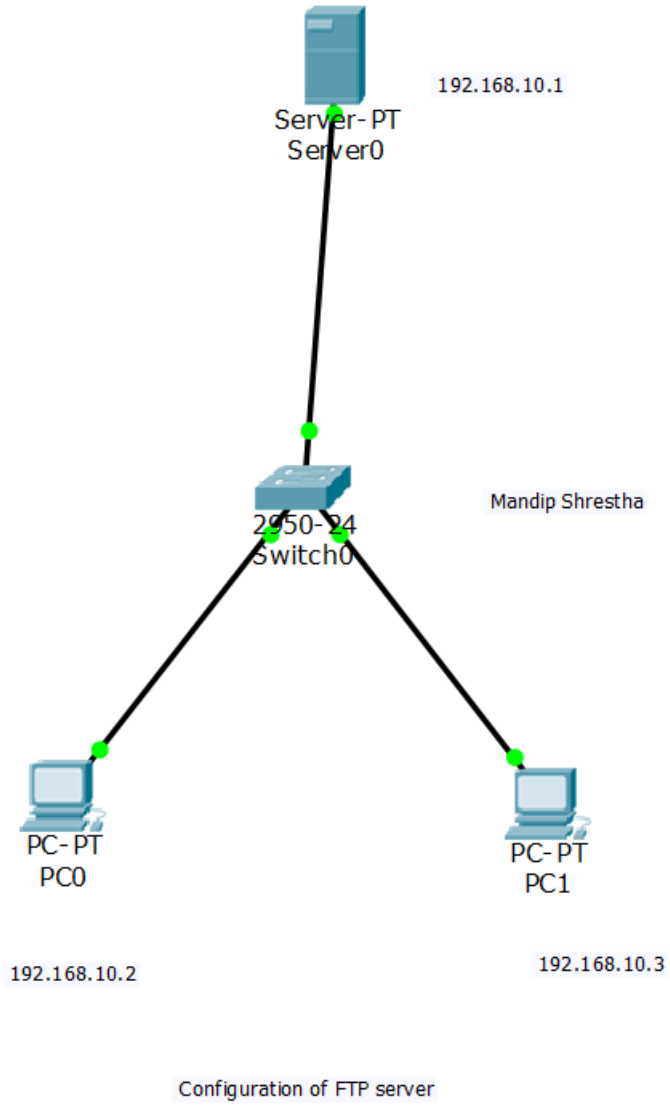
5. In PC1,
5.1. Goto Desktop > IP Configuration
5.2. Assign IP address 192.168.10.3 & Subnet Mask 255.255.255.0



6. In Server,
6.1. Goto Services > FTP
6.2. Enter Username & Password in respective fields
6.3. Check the boxes for required permissions
6.4. Add & save.



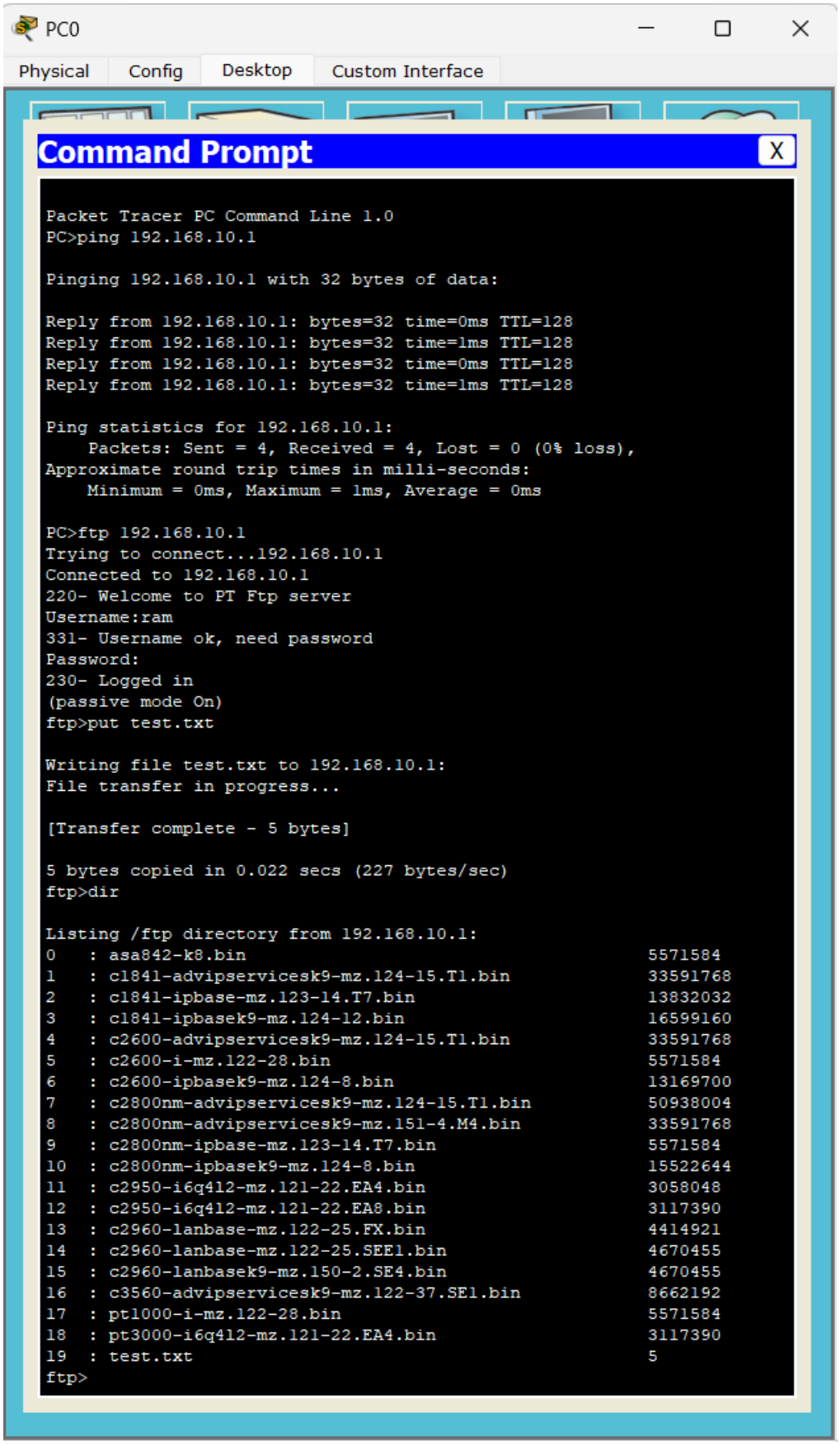
Layout



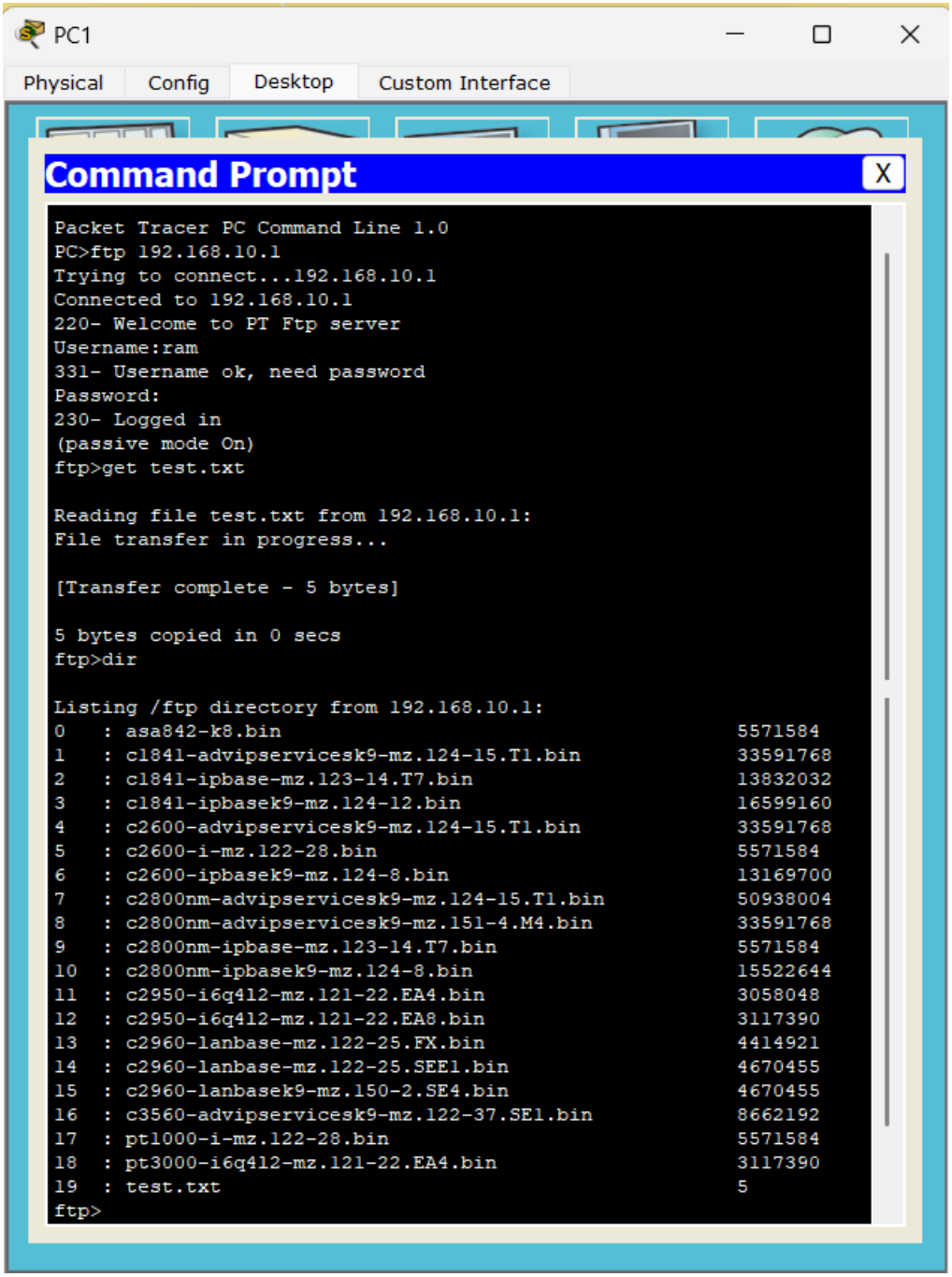
Testing

The configuration can be tested as follows:

1. In PC0,
1.1. Goto Desktop > Text Editor
1.2. Create & save one file (test.txt)
1.3. Goto Desktop > Command Prompt
1.4. Ping the server IP address to test connection
1.5. Enter ftp & IP address of server (ftp 192.168.10.1)
1.6. Enter username & password.
1.7. Once logged in, enter put & file name (put test.txt)
1.8. Once upload is complete, enter dir command to locate the file on server.


PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=0ms TTL=128
Reply from 192.168.10.1: bytes=32 time=1ms TTL=128
Reply from 192.168.10.1: bytes=32 time=0ms TTL=128
Reply from 192.168.10.1: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ftp 192.168.10.1
Trying to connect...192.168.10.1
Connected to 192.168.10.1
220- Welcome to PT Ftp server
Username:ram
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put test.txt
Writing file test.txt to 192.168.10.1:
File transfer in progress...
[Transfer complete - 5 bytes]
5 bytes copied in 0.022 secs (227 bytes/sec)
ftp>dir
Listing /ftp directory from 192.168.10.1:
0 : asa842-k8.bin 5571584
1 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
2 : c1841-ipbase-mz.123-14.T7.bin 13832032
3 : c1841-ipbasek9-mz.124-12.bin 16599160
4 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
5 : c2600-i-mz.122-28.bin 5571584
6 : c2600-ipbasek9-mz.124-8.bin 13169700
7 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
8 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
9 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
10 : c2800nm-ipbasek9-mz.124-8.bin 15522644
11 : c2950-i6q4l2-mz.121-22.EA4.bin 3058048
12 : c2950-i6q4l2-mz.121-22.EA8.bin 3117390
13 : c2960-lanbase-mz.122-25.FX.bin 4414921
14 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
15 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
16 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
17 : pt1000-i-mz.122-28.bin 5571584
18 : pt3000-i6q4l2-mz.121-22.EA4.bin 3117390
19 : test.txt 5
ftp>

2. In PC1,
2.1. Goto Desktop > Command Prompt
2.2. Enter ftp & IP address of server (ftp 192.168.10.1)
2.3. Enter username & password
2.4. Once logged in, enter get & file name (get test.txt)
2.5. Once downloaded, you can verify the file using dir command.



LAB 17: CONFIGURATION OF EMAIL SERVER

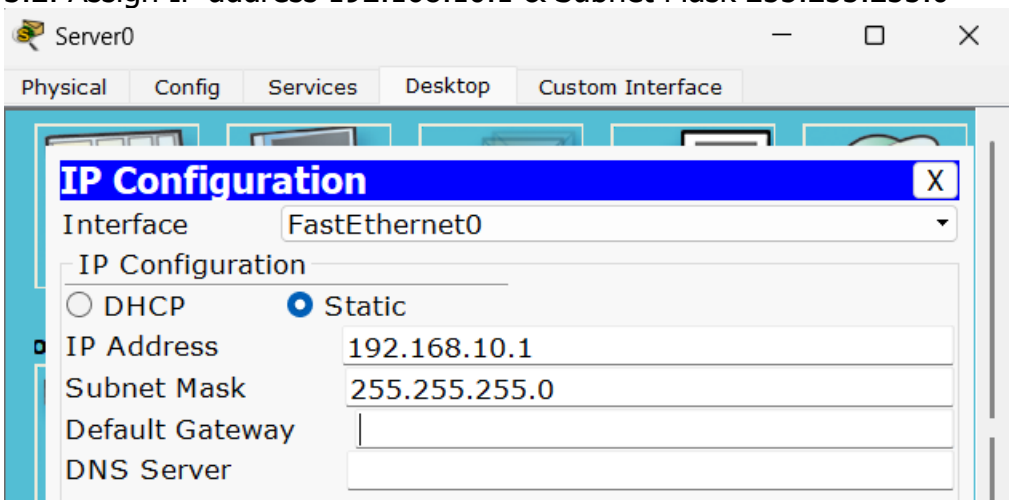
Email, or electronic mail, is a method of exchanging digital messages between individuals or groups using electronic devices and the internet. It allows users to send, receive, and manage messages, attachments, and other content electronically. An email server is a computer server responsible for sending, receiving, and storing email messages. It manages the storage and delivery of email messages between users within the same email domain or across different domains.

Protocols used in email

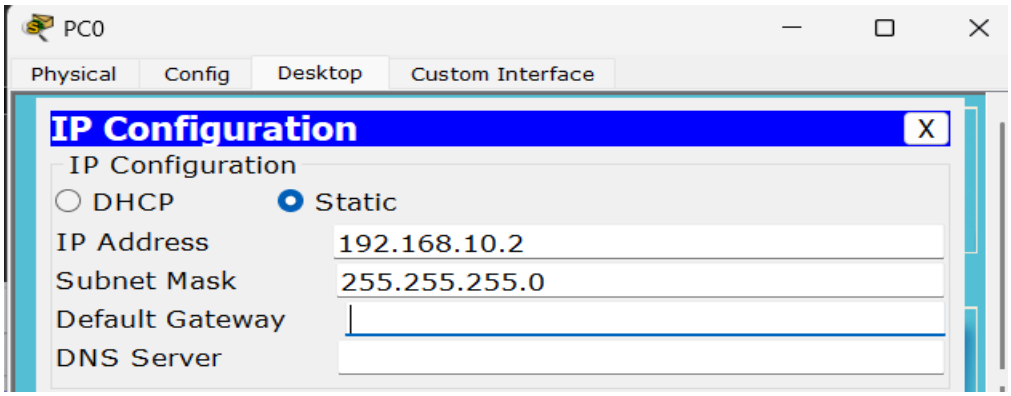
• SMTP (Simple Mail Transfer Protocol): Responsible for sending outgoing email messages from a client to a server or between mail servers over the internet.
• POP (Post Office Protocol): Allows email clients to retrieve incoming email messages from a remote mail server to the client's device, enabling users to download and store messages locally.
• IMAP (Internet Message Access Protocol): Provides an alternative to POP for retrieving incoming email messages from a remote mail server, allowing users to access and manage messages directly on the server without downloading them to the client's device. Email servers are essential for facilitating email communication by sending, receiving, and storing email messages, attachments, and other content. They also enable businesses to host email services, manage email accounts, and support collaboration and productivity among employees.

Configuration

In Cisco Packet Tracer, an Email Server can be configured as follows:
1. Place a Server (Server0), a Switch (Switch0) & two PCs (PC0 & PC1)
2. Connect the Server & PCs to the Switch
3. In Server,
3.1. Goto Desktop > IP Configuration
3.2. Assign IP address 192.168.10.1 & Subnet Mask 255.255.255.0

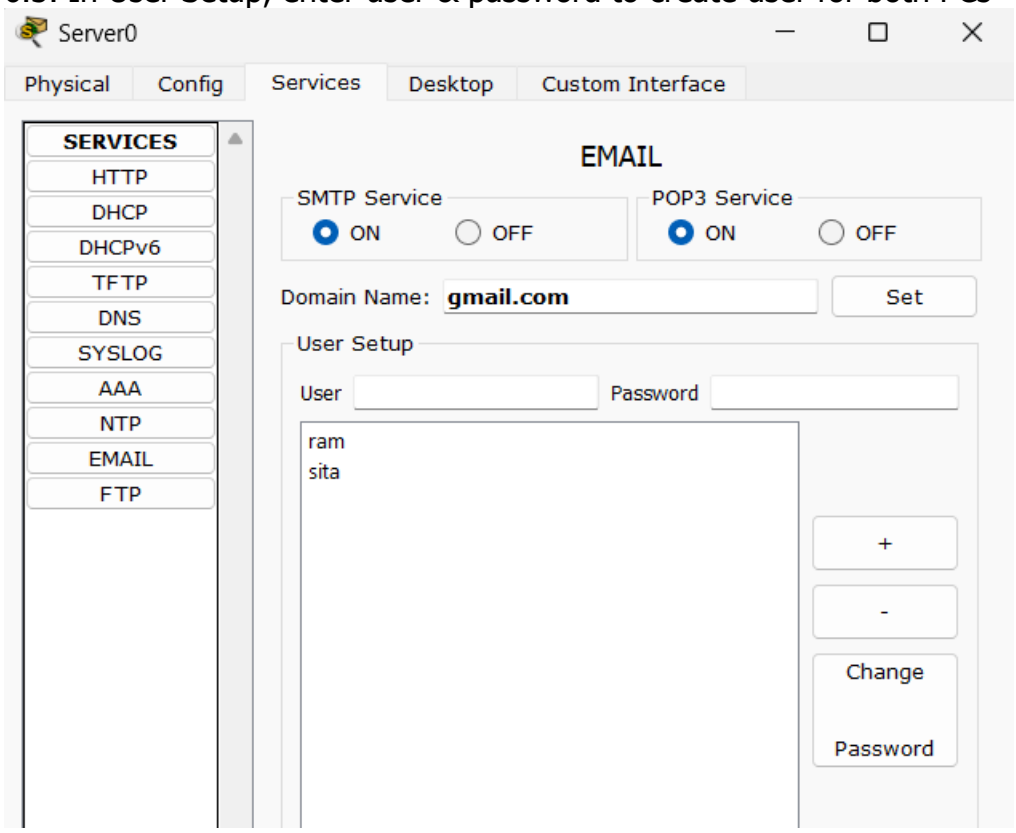


4. In PC0,
4.1. Goto Desktop > IP Configuration
4.2. Assign IP address 192.168.10.2 & Subnet Mask 255.255.255.0

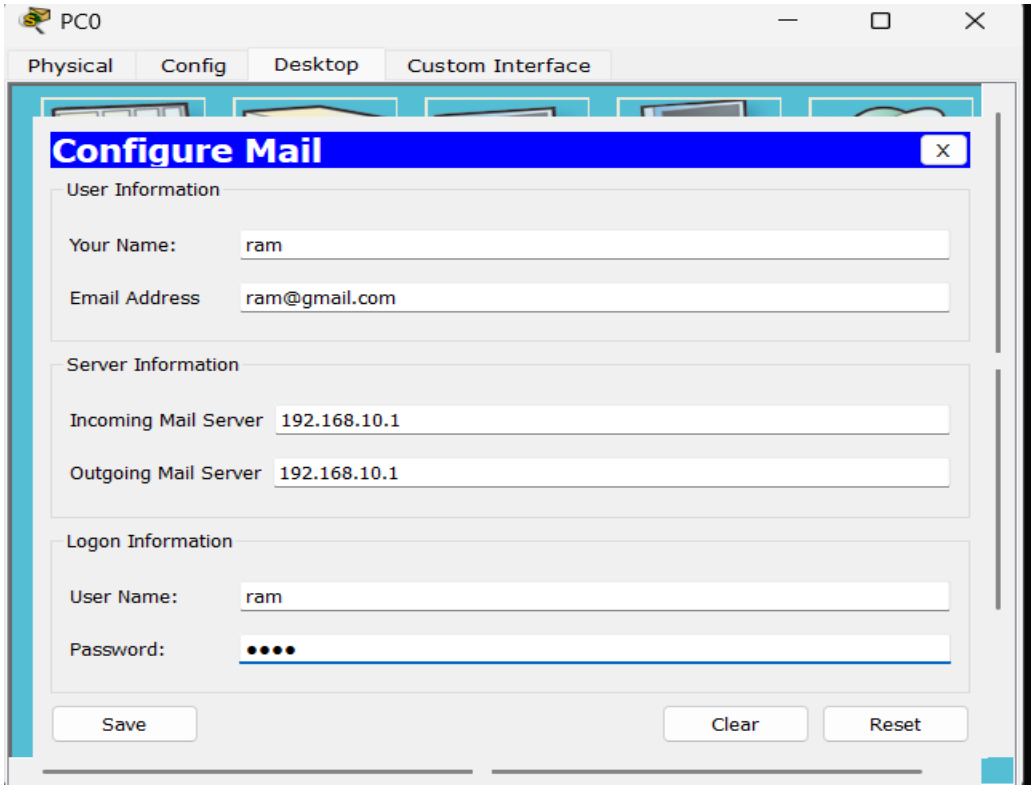


5. In PC1,
   5.1. Goto Desktop > IP Configuration
   5.2. Assign IP address 192.168.10.3 & Subnet Mask 255.255.255.0

6. In Server,
6.1. Goto Services > Email
6.2. Enter domain name
6.3. In User Setup, enter user & password to create user for both PCs



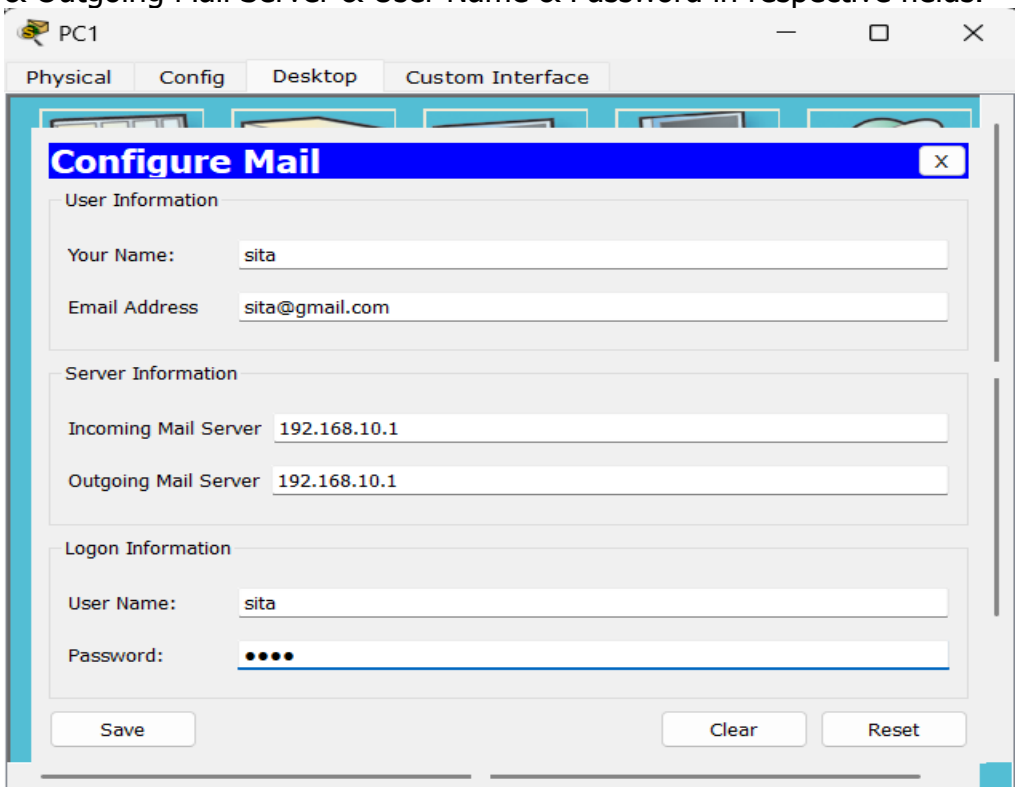
7. In PC0,
7.1. Goto Desktop > Email
7.2. Configure the email with appropriate information. Enter pc0 in Your Name, ram@gmail.com in Email Address, IP address of Mail Server (192.168.10.1) in Incoming
& Outgoing Mail Server & User Name & Password in respective fields.



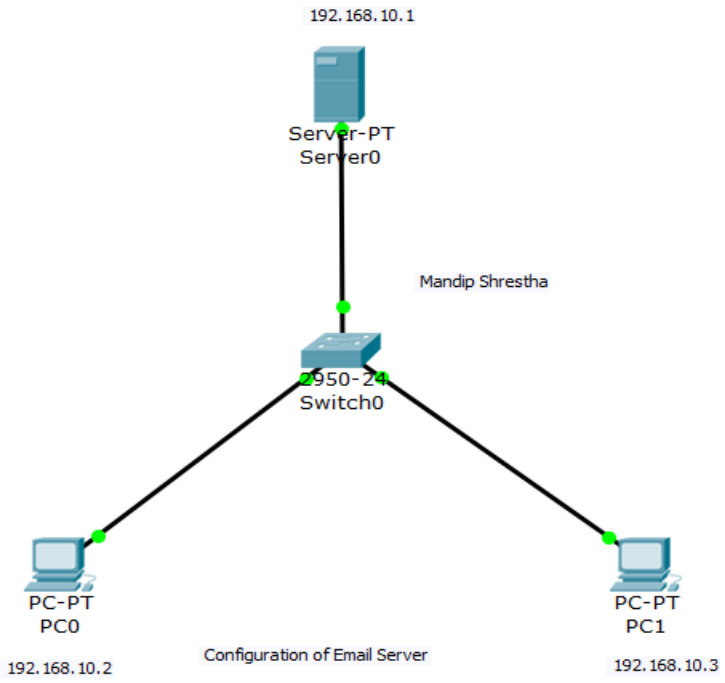
8. In PC1,

8.1. Goto Desktop > Email

8.2. Configure the email with appropriate information. Enter pc1 in Your Name, sita@gmail.com in Email Address, IP address of Mail Server (192.168.10.1) in Incoming
& Outgoing Mail Server & User Name & Password in respective fields.



Layout

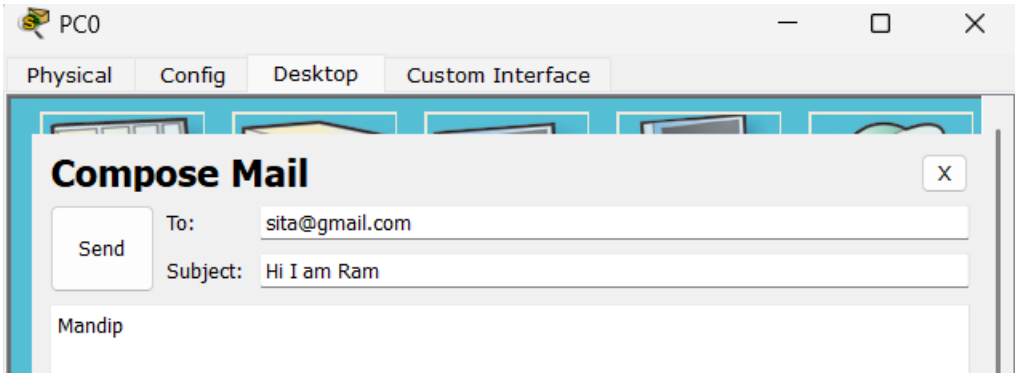


Testing

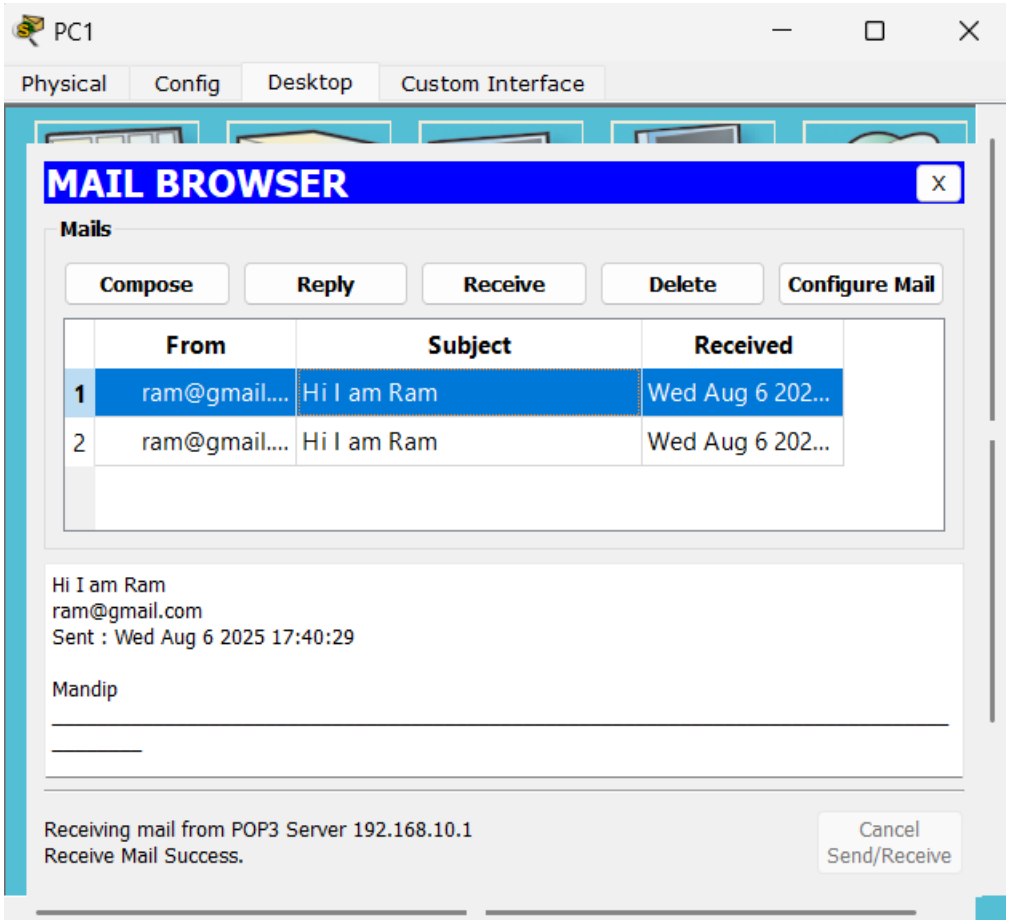
The configuration can be tested as follows:

A. Sending email from PC0

1. Goto Desktop > Email
2. Compose an email with Destination email address (ram@gmail.com), Subject & Body
3. Send



B. Receiving email from PC1
1. Goto Desktop > Email
2. Click Receive to receive any incoming emails.



LAB 18: IMPLEMENTATION OF FIREWALL (IPV4)

A firewall is a network security tool or software solution that monitors and manages inbound and outbound network traffic based on established security guidelines. Acting as a protective shield, it inspects each data packet passing through and decides whether to permit or block it according to specified security policies.

Uses of Firewalls

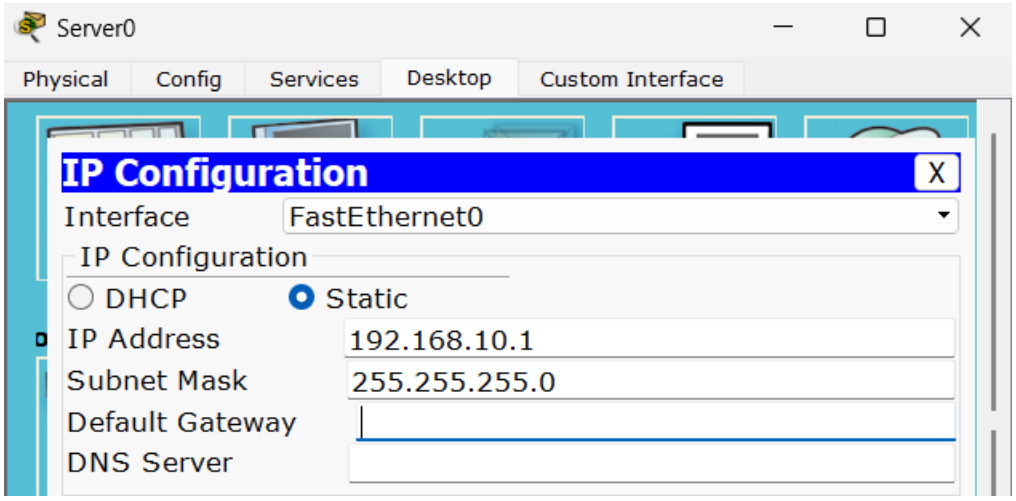
- Firewalls safeguard internal networks from unauthorized access and malicious attacks originating from external sources, such as cybercriminals and malware.
- Firewalls enforce access control policies to manage which users or systems are permitted to reach certain resources or services within the network.
- Firewalls can restrict access to certain websites, applications, or content categories to support acceptable use policies, helping to prevent employees from viewing inappropriate or potentially harmful content.

Advantages of Firewalls

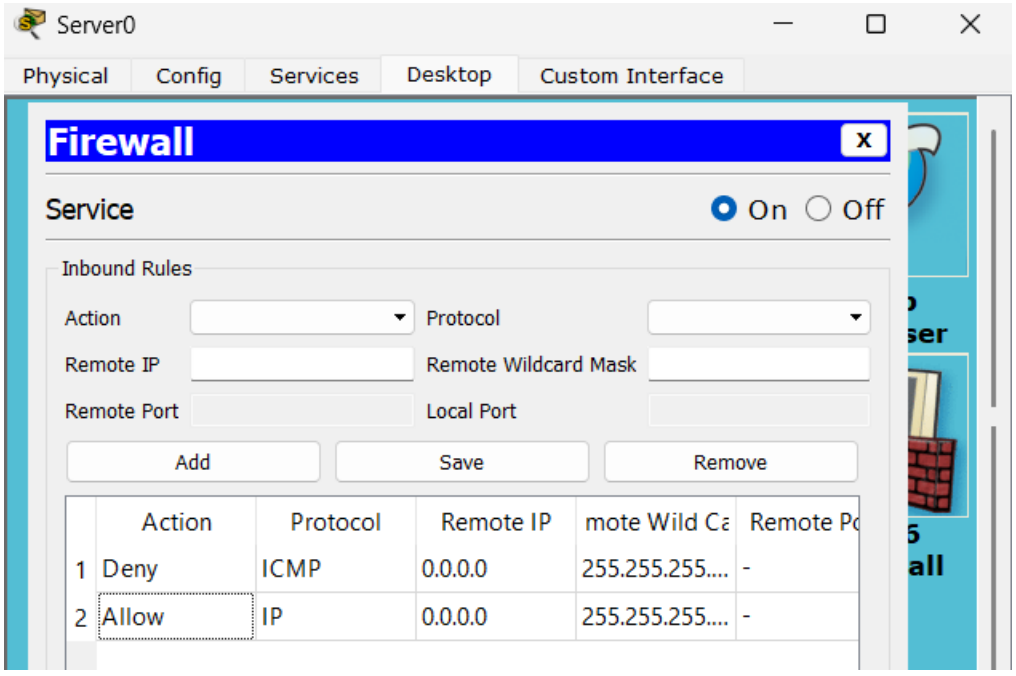
- Firewalls add an essential layer of security against external threats, minimizing the risk of unauthorized entry, data breaches, and network attacks.
- Firewalls allow organizations to monitor and regulate network traffic, enforcing security policies and controlling access to sensitive information.

Configuration

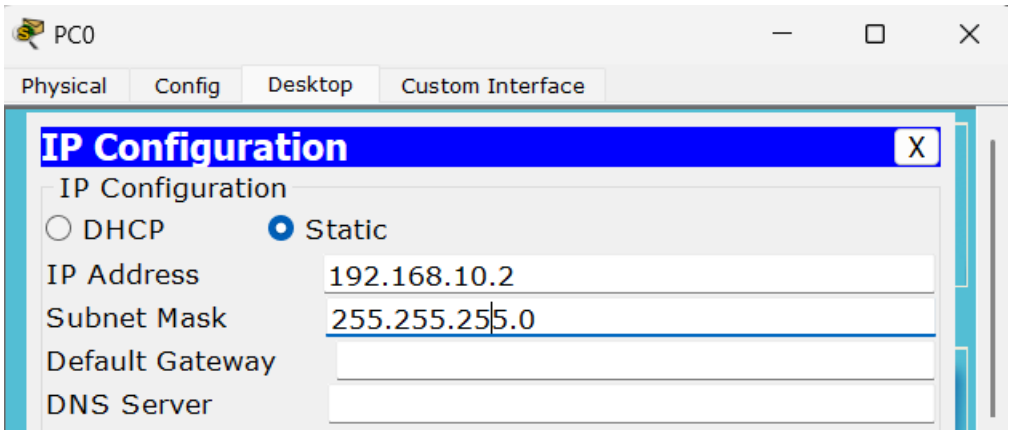
In this lab, we are denying the ICMP interaction but allowing the IP interaction of PCs in LAN to the
server. PCs in LAN can interact with each other but cannot interact with server. This configuration
can be achieved in Cisco Packet Tracer as follows:
1. Place a Server (Server0), a Switch (Switch0) & two PCs (PC0 & PC1)
2. Connect PCs & Server to the Switch
3. In Server,
  3.1. Goto Desktop > IP Configuration
  3.2. Set IP address 192.168.10.1 & Subnet Mask 255.255.255.0



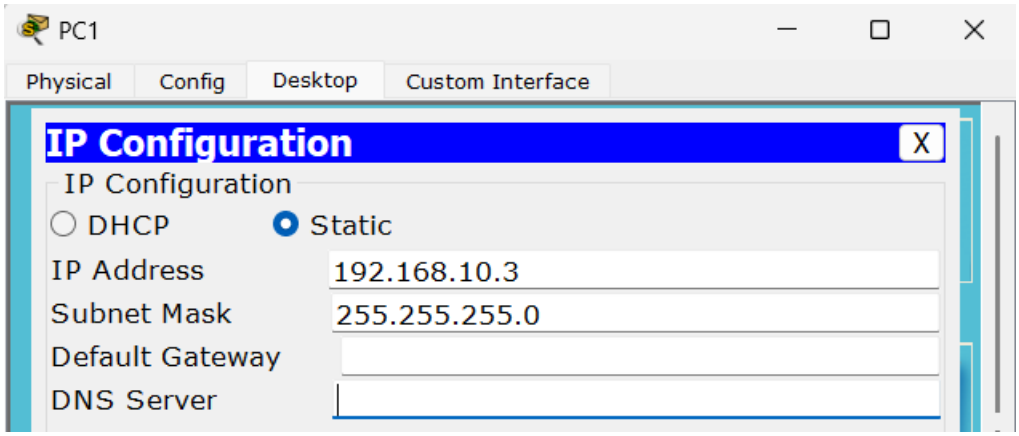
3.3. Goto Desktop > Firewall (IPV4)
3.4. Under Inbound Rules, Set Action to Deny, Protocol to ICMP, Remote IP to 0.0.0.0 &
Remote Wildcard Mask to 255.255.255.255
3.5. Add & save
3.6. Again, Under Inbound Rules, Set Action to Allow, Protocol to IP, Remote IP to 0.0.0.0 &
Remote Wildcard Mask to 255.255.255.255
3.7. Add & save
3.8. Turn on the service.



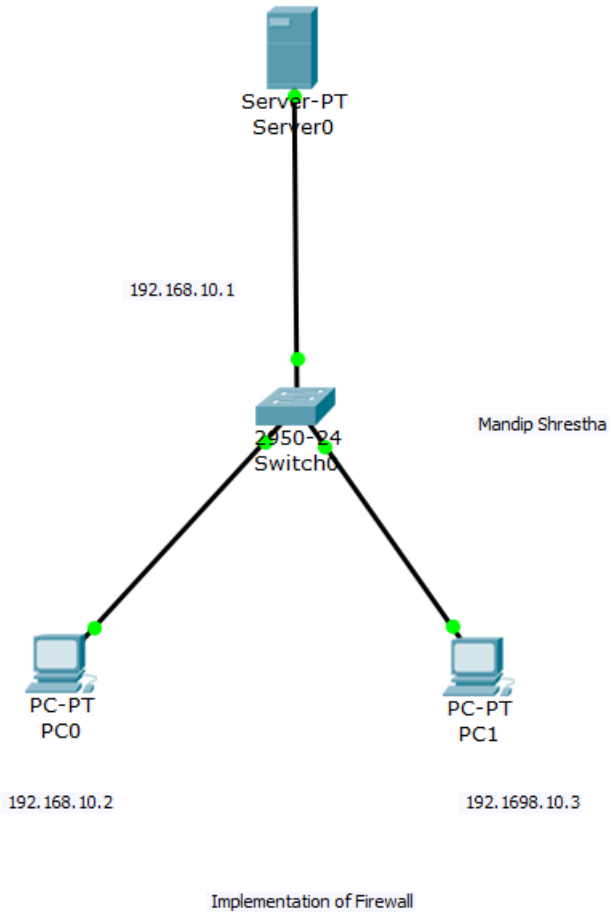
4. In PC0, Goto IP Configuration & set IP address 192.168.10.2 & Subnet Mask 255.255.255.0



5. In PC1, Goto IP Configuration & set IP address 192.168.10.3 & Subnet Mask 255.255.255.0



Layout



Testing

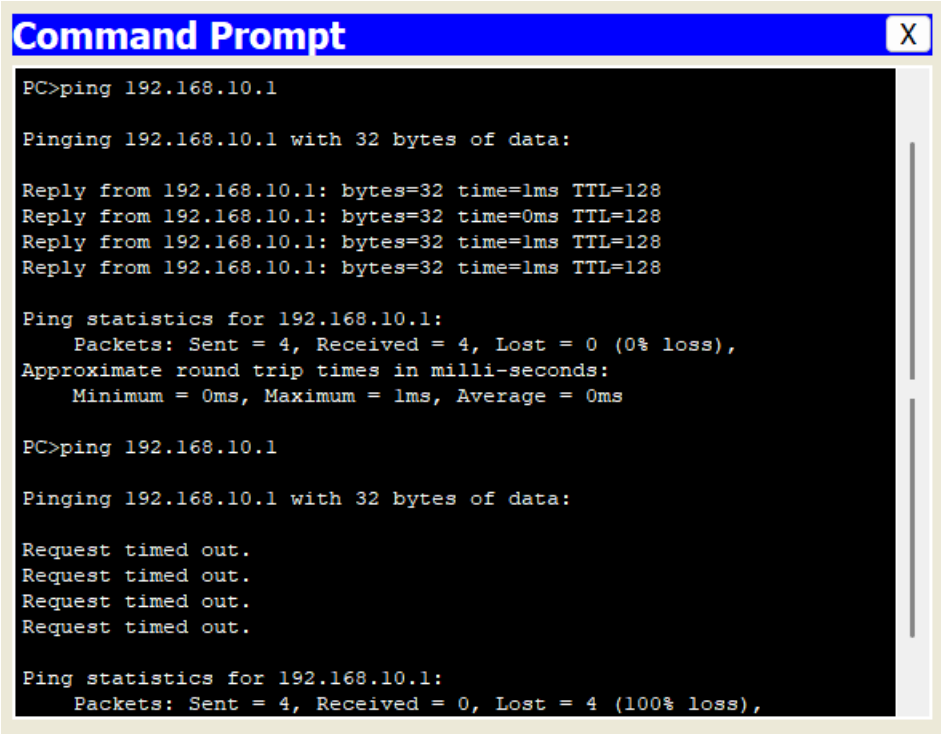
The implementation can be tested in the given ways.

A. By pinging target Server IP address from Command Prompt of one PC

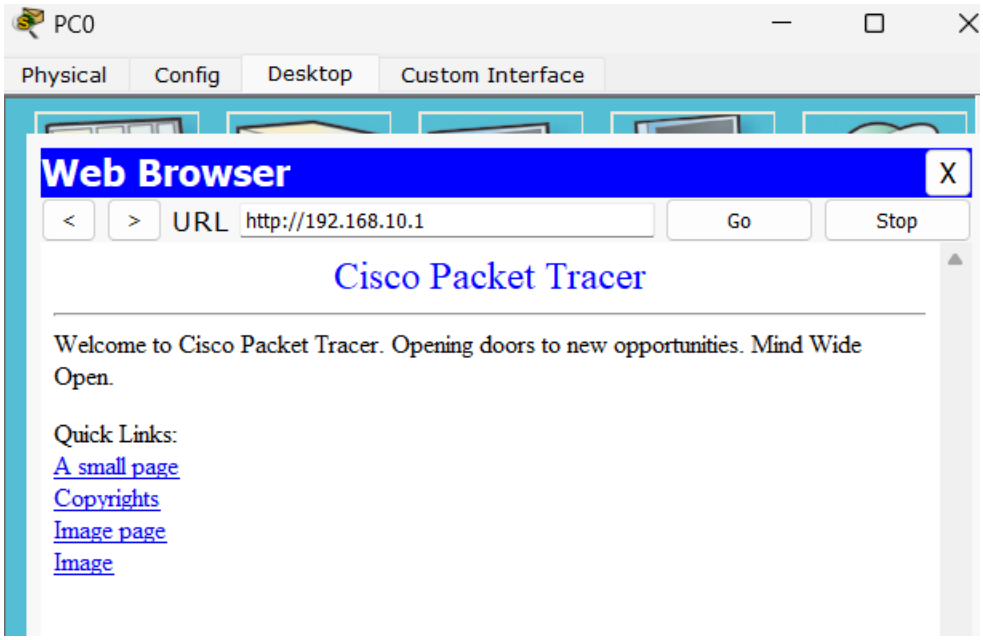
1. Goto Command Prompt of one PC (PC0).
2. Enter ping & IP of Server (ping 192.168.10.1).

2.1. The ping is successfully done before configuring the firewall.

2.2. But after configuration of the firewall, the ping fails.



B. By accessing IP address of Server through browser of PCs.
1.Goto Desktop > Web Browser
2.Enter IP address of Server (192.168.10.1)
3.The web page on server will be displayed. But server cannot be pinged from any PC.



LAB 19: IMPLEMENTATION OF ROUTER ACCESS CONTROL LIST (ACL)

Access Control Lists (ACLs) are sets of rules that define permissions for network traffic. These rules are applied to router interfaces to permit or deny traffic based on various criteria such as source IP address, destination IP address, protocol type, port numbers, and more. The primary purpose of implementing ACLs is to enhance network security by controlling the flow of traffic within the network. ACLs allow network administrators to define and enforce policies regarding which traffic is allowed to enter or exit specific network segments.

Configuration

In this lab, we are denying the access to server from one PC in the network by using ACL. In Cisco Packet Tracer, this configuration can be implemented as follows:

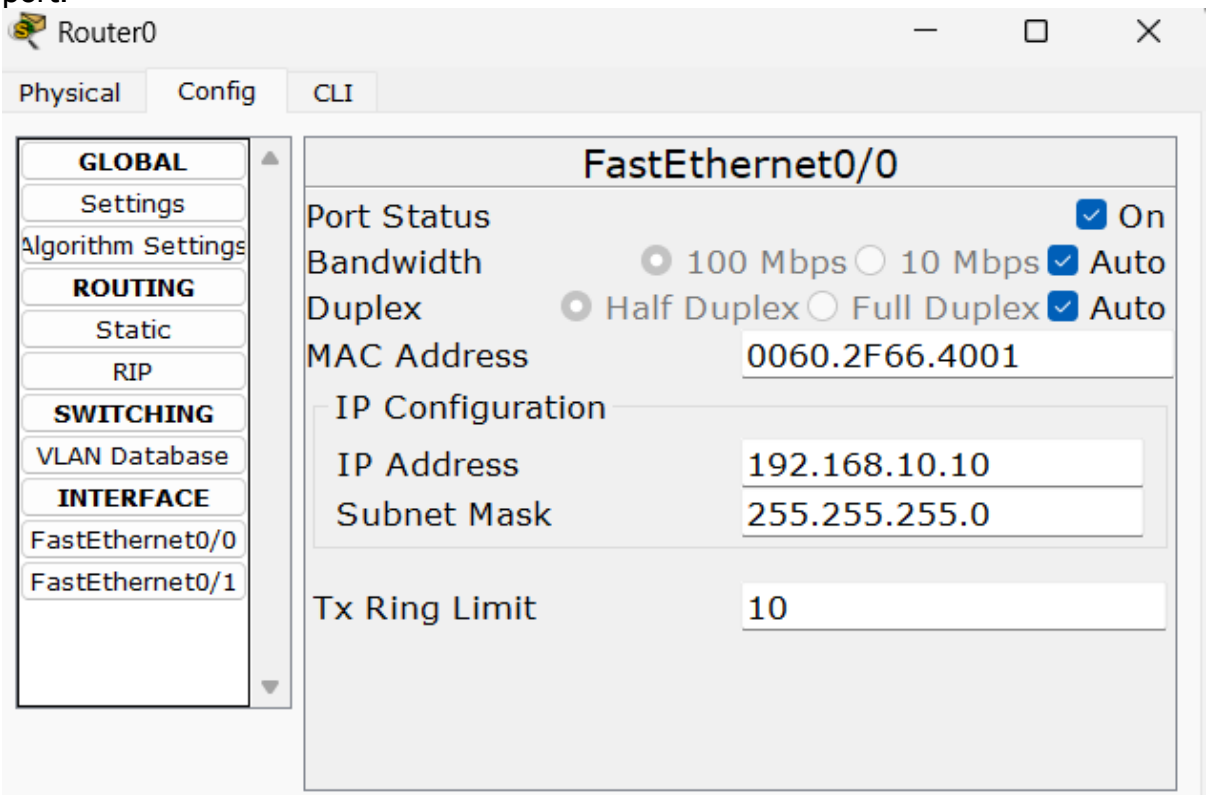
1.Place a Server (Server0), a Router (Router0), a Switch (Switch0) & two PCs (PC0 & PC1)

2. Connect the PCs to Switch, Switch to Router & Router to Server

3. In Router,

3.1. Goto Config > FastEthernet0/0

3.2. Enter IP address 192.168.10.10, Subnet Mask 255.255.255.0 & turn on the port.



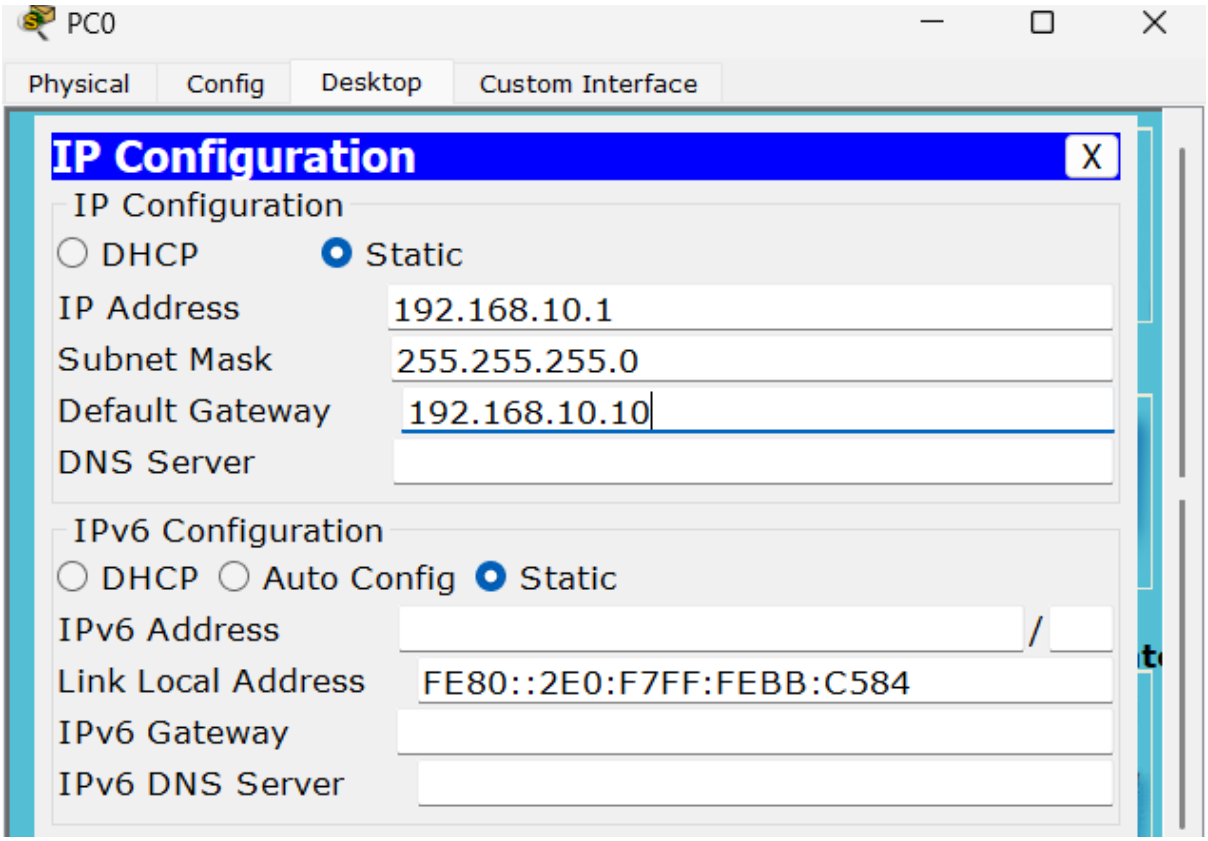
3.3. Goto FastEthernet0/1

3.4. Enter IP address 10.10.10.10, Subnet Mask 255.0.0.0 & turn on the port.

4. In PC0,

4.1. Goto Desktop > IP Configuration

4.2. Enter IP address 192.168.10.1, Subnet Mask 255.255.255.0 & Default Gateway 192.168.10.10

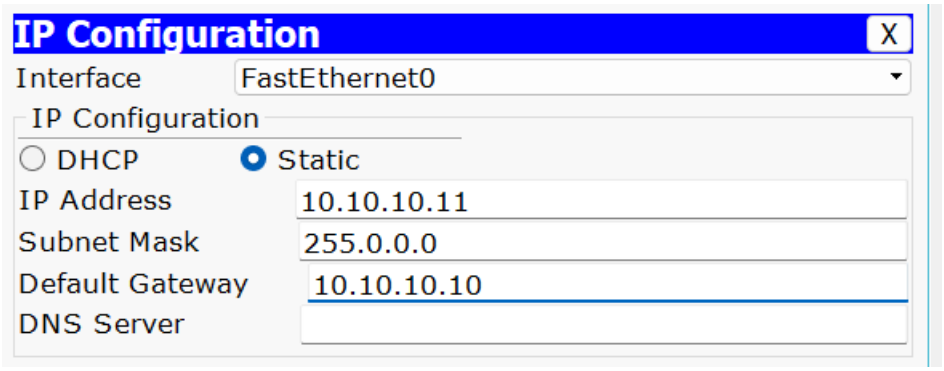


5. In PC1, Enter IP address 192.168.10.2, Subnet Mask 255.255.255.0 & Default Gateway
192.168.10.10

6. In Server,

6.1. Goto Desktop > IP Configuration

6.2. Enter IP address 10.10.10.11, Subnet Mask 255.0.0.0 & Default Gateway 10.10.10.10

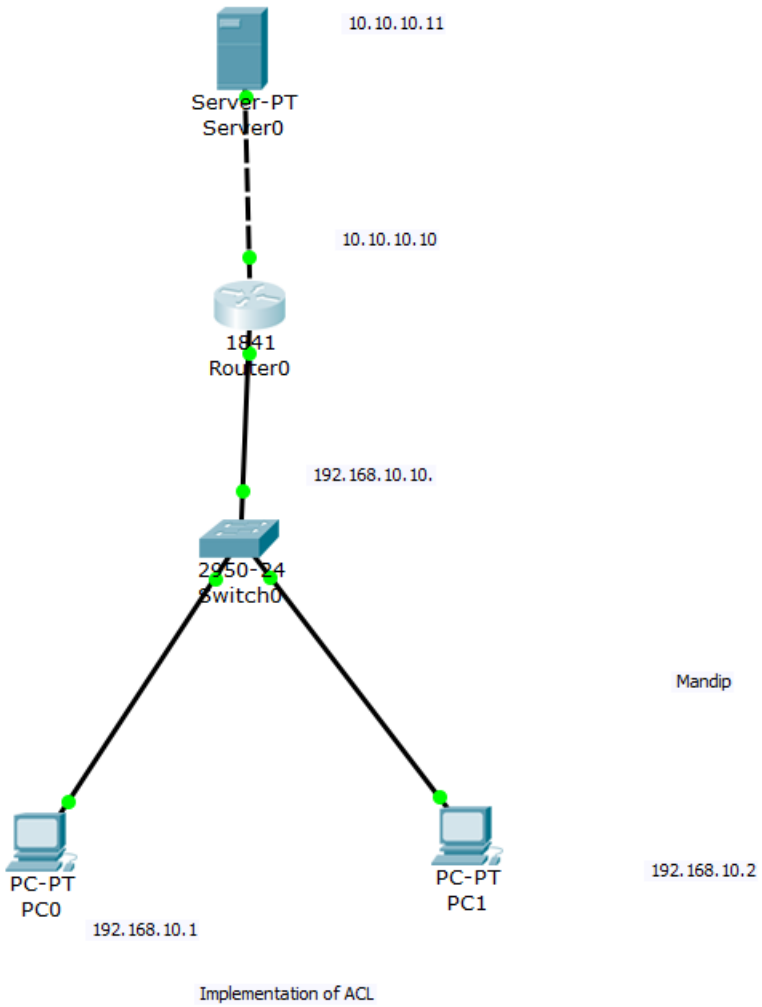


7. In Router, Open CLI mode & enter the following commands:

```
Router>enable
Router#configure terminal
Router(config)#ip access-list standard 11
Router(config-std-nacl)#deny host 192.168.10.1
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip access-group 11 in
Router(config-if)#exit
Router(config)#exit
Router#
```

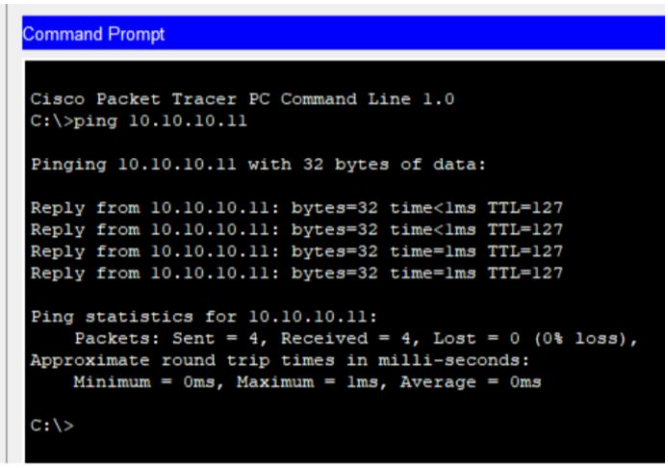
```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list standard 11
Router(config-std-nacl)#deny host 192.168.10.1
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#innterface fastEthernet 0/0
                  ^
% Invalid input detected at '^' marker.

Router(config)#interface fastEthernet 0/0
Router(config-if)#ip access-group 11 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Layout

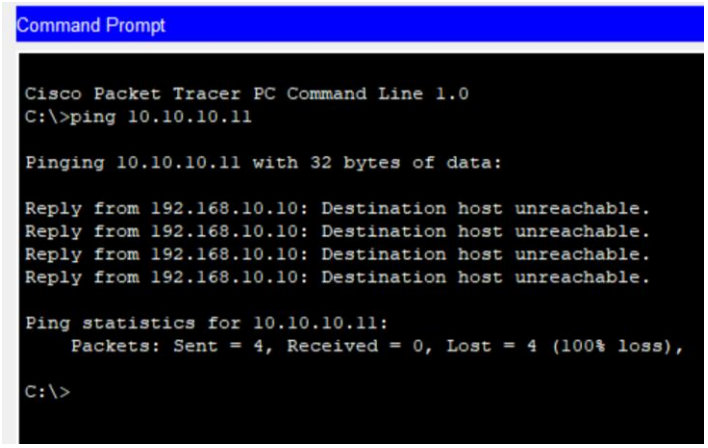


Testing

1. Goto Command Prompt of one PC (PC0)
2. Enter ping & IP of Server (ping 10.10.10.11)
   2.1. The ping is successfully done before configuring ACL
   2.2. But after configuration of ACL, the ping fails
3. Goto Command Prompt of PC1
4. Enter ping & IP address of Server (ping 10.10.10.11). The ping is successful from here as this IP address is not denied in ACL.



Before Configuring ACL



After Configuring ACL

LAB 20: OVERVIEW OF WIRESHARK

Wireshark is a popular open-source network protocol analyzer that enables network professionals to capture and examine network traffic. It provides an in-depth look at the data exchanged between devices on a network, aiding administrators in troubleshooting network problems, analyzing security events, and studying the behavior of network applications. Wireshark captures packets by setting network interface cards (NICs) to promiscuous mode, which allows them to capture all packets on the network, not just those specifically directed to the device.

Steps:

To capture packets using Wireshark:

1. Open Wireshark and choose the network interface you wish to capture traffic on.
2. Click the "Start" button to begin capturing packets.
3. Wireshark allows you to apply filters to capture specific traffic types, such as filtering by IP address, protocol, or port number. It also provides detailed analysis of packet headers.
4. Once you've gathered the necessary data, click the "Stop" button to end the capture.