Premier University

Department of Computer Science and Engineering

CSE 368 - Computer Networks Laboratory

LABORATORY MANUAL

July 2024

CONTENTS

1. Introduction to different types of networking cables

Title: Fabrication and Testing of LAN Cable.

Objective:

1. Learn about cables, different types of cable and equipment.
2. Learn about when which types of cables are needed.
3. Fabricate a LAN cable for internet connection.
4. Test if the cable is correctly working.

Prerequisite: None

Theory:

Figure 1.1: LAN Cable

LAN Cable:
A LAN cable is a conductor that connects devices in a Local Area Network (LAN) with a network connector**.**

CAT 4, 5, 6:
Cat 4, Cat 5, and Cat 6 are different categories of Ethernet cables used for networking purposes. The main difference lies in their performance capabilities and the level of data transmission they can support.

- Cat 4 cables were commonly used in the past but are now considered outdated. They can support data transmission speeds of up to 16 Mbps.
- Cat 5 cables can handle higher data transmission speeds of up to 100 Mbps.
- Cat 6 cables are the most advanced among the three. They can support data transmission speeds of up to 10 GB p/s over short distances. Cat 6 cables have better shielding and reduced crosstalk, resulting in improved performance and less interference.

RJ-45 Connector:
A registered jack (RJ) is a standardized physical network interface for connecting telecommunications or data equipment. The most common twisted-pair connector is an 8-position, 8-contact (8P8C) modular plug and jack commonly referred to as an RJ45 connector.

Figure 1.2: RJ-45 Connector

Straight Through Cable:

A straight-through cable is a type of Ethernet cable used to connect different types of devices within a network.

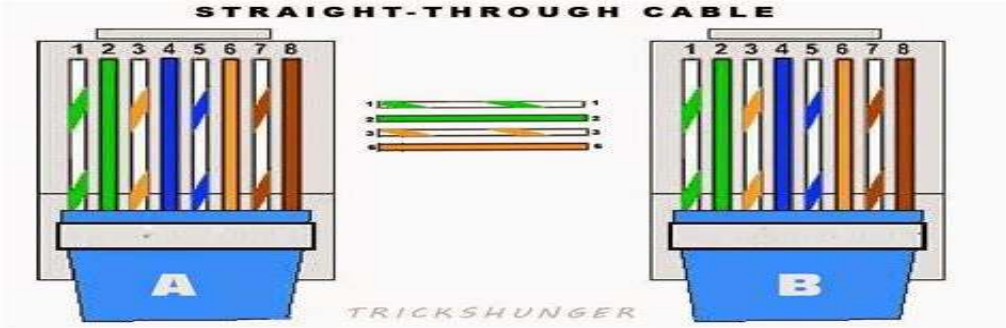


Figure 1.3: Straight-Through Cable Order Diagram

Crossover Cable:

A crossover cable is a type of Ethernet cable used to connect similar devices directly to each other without needing an intermediate network device like a switch or hub.

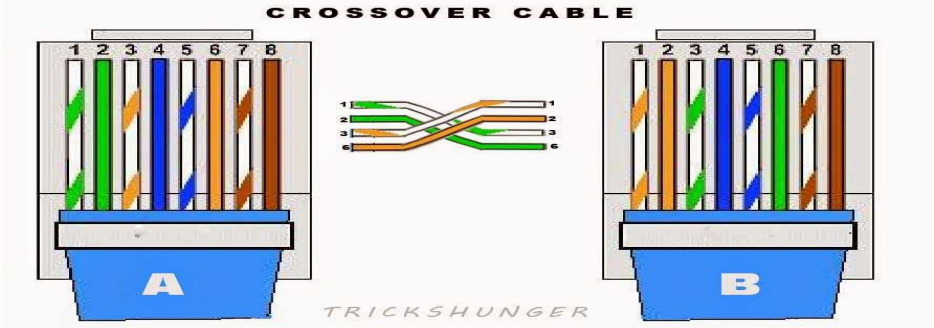


Figure 1.4: Crossover Cable Order Diagram

Methodology:

1. Cut into the plastic sheath about **one inch** from the end of the cut cable.

2. Pinch the wires between fingers and straighten them out as needed (Straight through/ Crossover) the color order is important to get correct.

3. Make a straight cut across the eight wires to shorten them to **half an inch** from the cut sleeve to the end of the wires.

4. Push all eight unstripped colored wires into the connector.

5. Carefully place the connector into the Ethernet crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There's also a locking tab that holds the blue plastic sleeve in place for a tight compression fit.

6. Test the cable using the cable tester.

Equipment:

1. CAT5e or CAT6 cable
2. RJ45 connectors
3. Crimping tool
4. Cutter/stripper
5. Cable tester

Procedure:

- Unwind the cable.

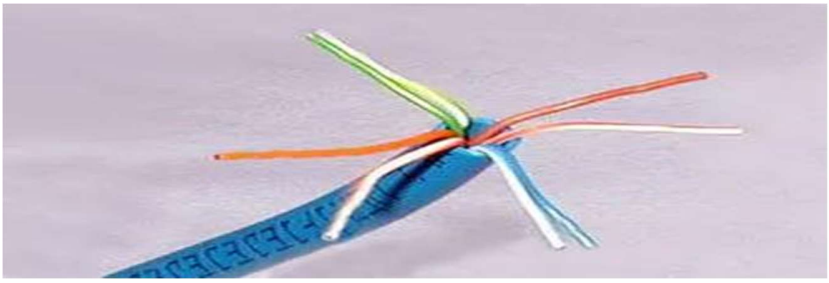


Figure 1.5: Unwind cable.

- Cut into same length while following the color scheme of straight through/ crossover.

Figure 1.6: Cable cut into same length

- Insert cable into the RJ-45 connector. And check if all 8 wire's end are visible in the connector's front side.

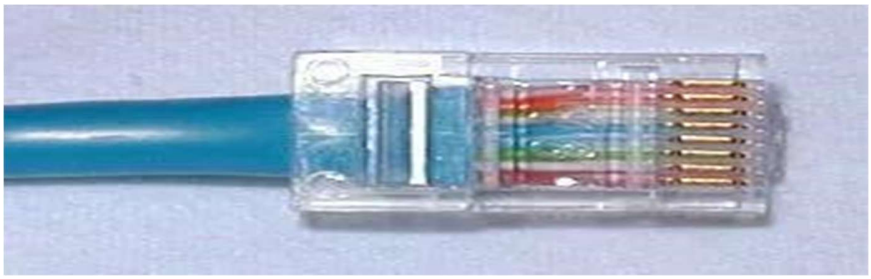


Figure 1.7: Cable inside the RJ-45 connector.

- Put the RJ-45 connector inside the clamper and carefully put pressure in the clamper. This will lock the cable with the connector permanently.

Figure 1.8: Clamping the cable.

- Now put each end of the wire into the 2 ports of the cable tester. The tester will blink lights that resembles the pattern shown in the diagram of **Figure 3, 4**. Check if the pattern matches according to the diagram.

Figure 1.9: Testing the cable.

Observation and Result:

The cable tester as shown in **Figure 9** will blink lights according to the diagram of the straight through/ crossover cable order/pattern.

Additional reading materials/ online tutorial/ References:

1. Video Tutorial: https://www.youtube.com/watch?v=Uw8FSXx4dnU
2. Article: https://www.wikihow.com/Create-an-Ethernet-Cable

2. Introduction to Cisco Packet Tracer.

Title: Introduction to CISCO Packet Tracer.

Objective:

1. Familiarize with CISCO Packet Tracer.
2. Learn basic functionality of CISCO Packet Tracer.
3. Use CISCO Packet Tracer for building and configuring a basic network.
4. Check connectivity of the network.

Prerequisite:

1. Knows basic equipment/ devices (i.e. End devices, Switch and different types of cable) and their functionality.
2. Understanding of networking, networking structure and terminology.

Theory:

IP Address:

An Internet Protocol address is a numerical label such as 192.0.2.1 that is assigned to a device connected to a computer network that uses the Internet Protocol for communication. IP addresses serve two main functions: network interface identification, and location addressing.

Gateway:

A gateway is a network node or device that connects two networks that use different transmission protocols. Gateways play an important role in connecting two networks. It works as the entry-exit point for a network because all traffic that passes across the networks must pass through the gateway.

Methodology:

1. Learn about menus, sub-menus.
2. Make a basic network.
3. Configure the network
4. Check connectivity.

Equipment:

1. PC
2. Switch (2960-24TT)
3. Wire

Procedure:

Step 1: Familiarize with CISCO Packet Tracer

- This illustrates Cisco Packet Tracer. Cisco Packet Tracer's graphical interface makes it easy to visualize network connections and understand how data flows between devices.

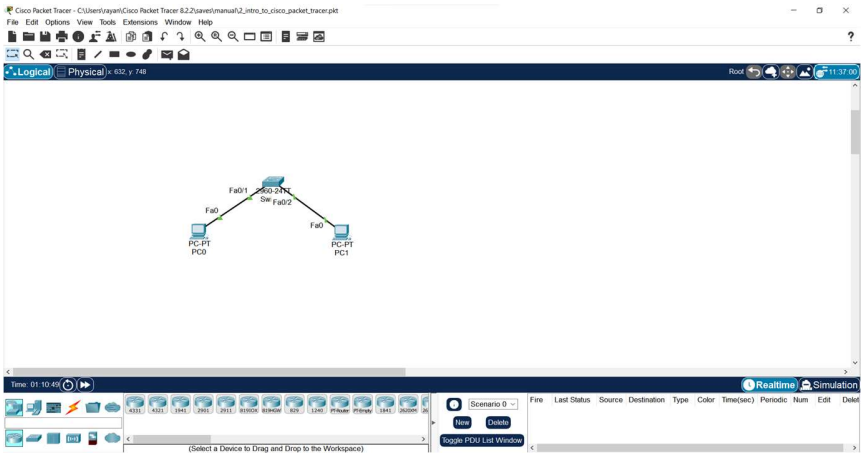


Figure 2.1: Cisco Packet Tracer Interface.

- Here in top there is the toolbar that provides quick access to various menus related to file and customization. Also there is PDU (Packet), drawing and note option available.

Figure 2.2: Cisco Packet Tracer Interface - Main Toolbar.

- Here in bottom there is the bottom toolbar that provides quick access to various tools and options for network design and simulation.

Figure 2.3: Cisco Packet Tracer Interface: Bottom Toolbar.

- In this menu every kind of components/equipment that are needed for building a network is available. Here different types of networking devices such as computer/communication devices, IOT devices, wire, miscellaneous and multiuser connection are available.

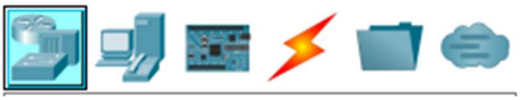


Figure 2.4: Types of component available in Cisco Packet Tracer.

- While selecting the submenus there will be component of verity model available.

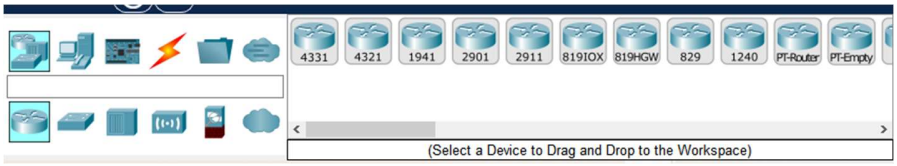


Figure 2.5: Different type of Router.

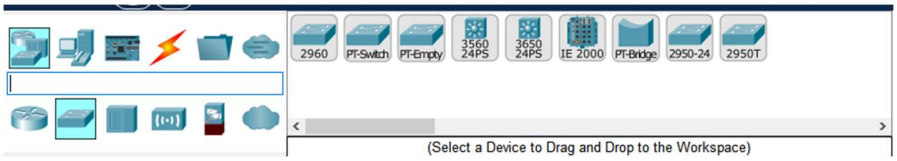


Figure 2.6: Different types of Switch.

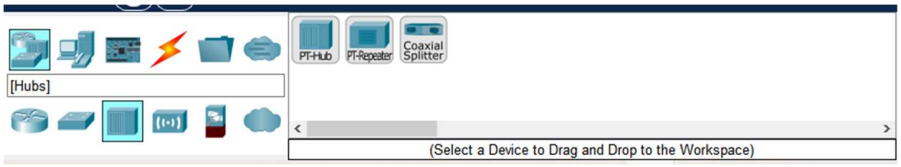


Figure 2.7: Different types of Hub.

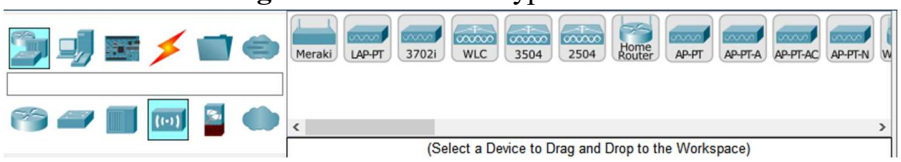


Figure 2.8: Different types of Wireless Devices.

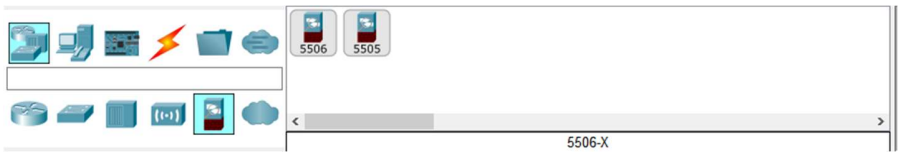


Figure 2.9: Different types of security components.

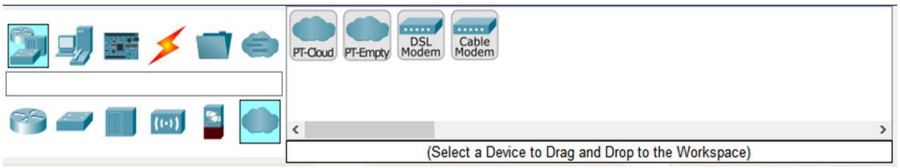


Figure 2.10: Different types of WAN Emulation.

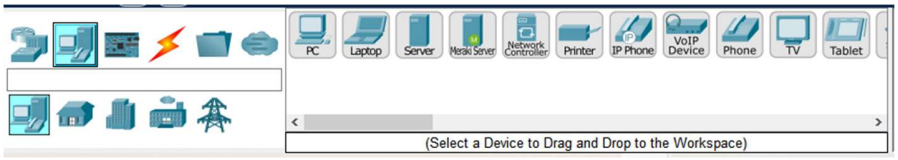


Figure 2.11: Different types of End Devices.

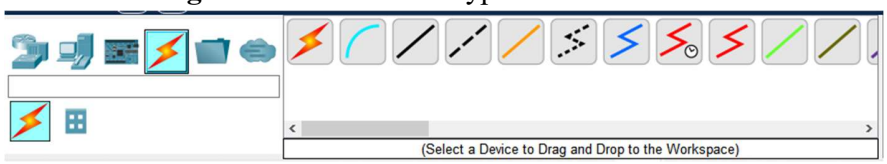


Figure 2.12: Different types of cable.

This option from the cable menu helps to connect any devices with the type of wire those devices needed automatically.

User Have to select the required components (By left mouse click) if user need more of that component then instead of selecting every times user can just (ctrl + left mouse click) to avoid this problem. When done press ESC from keyboard to dis-select the component.

[N.B: Live demonstrated should be presented in-order to help users understanding how to work with Packet Tracer software.**]**

- Double click on any component will pop open a screen where there will be menus/options for configure the component.

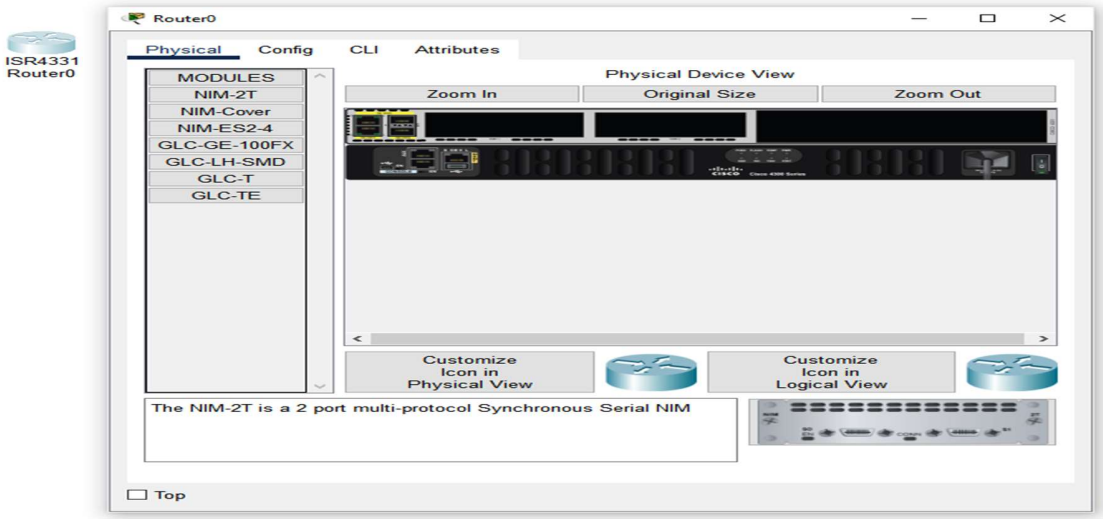


Figure 2.13: View of configuration screen of a component.

Step 2: Make and configure a basic network

- Drag and drop 1 PC,1 Laptop, 1 Switch (2960-24TT) from the bottom toolbar

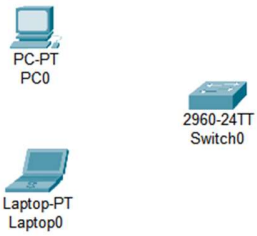


Figure 2.13: PC, Laptop, and Switch in the main window.

- Use the "Automatically Choose Connection Type" as shown in **figure 2.12** from the cable menu from the bottom toolbar. Then Select on 2 of the one by one for connection.

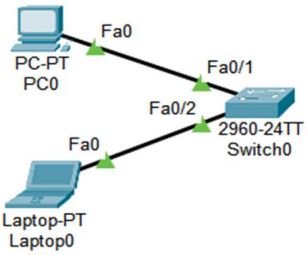


Figure 2.14: Both end devices are connected to the switch via cable.

Step 3: Configure the network

- Double click on end devices (PC, Laptop) will show a pop up screen from there go to desktop

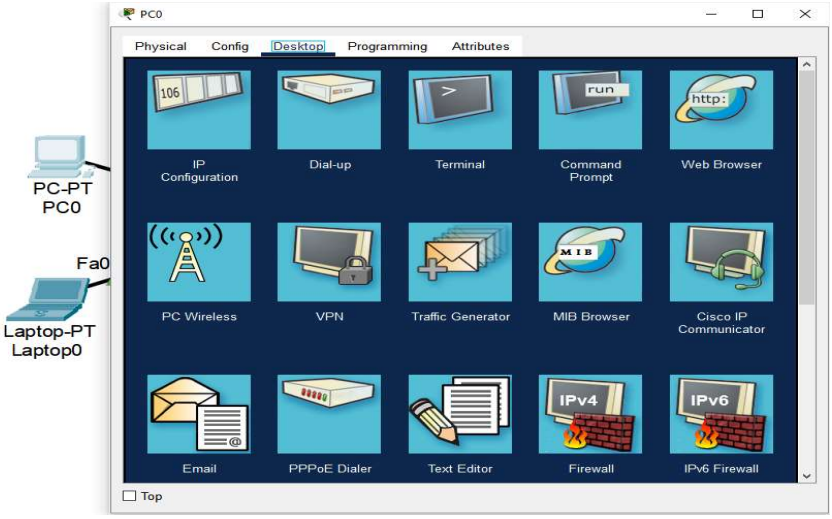


Figure 2.15: End Device configuration menus.

- Select IP Configuration from there.

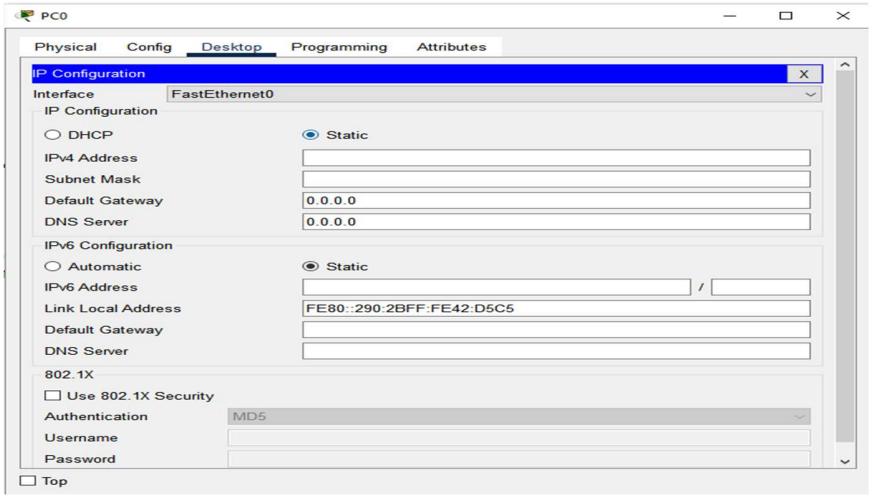


Figure 2.16: IP Configuration menu for PC0

- Set IP and Gateway for the devices.

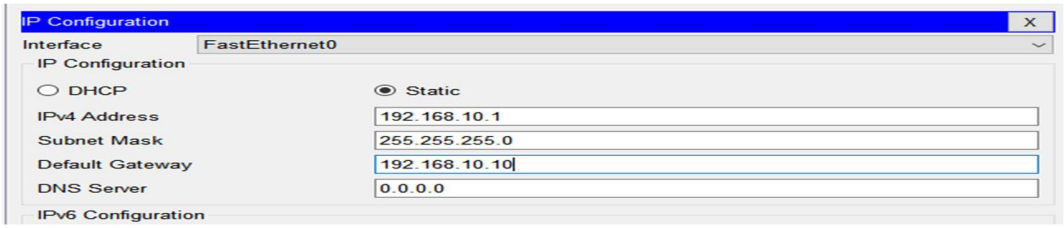


Figure 2.17: IP and Gateway for PC0

- Repeat This process for another End Device (Laptop)

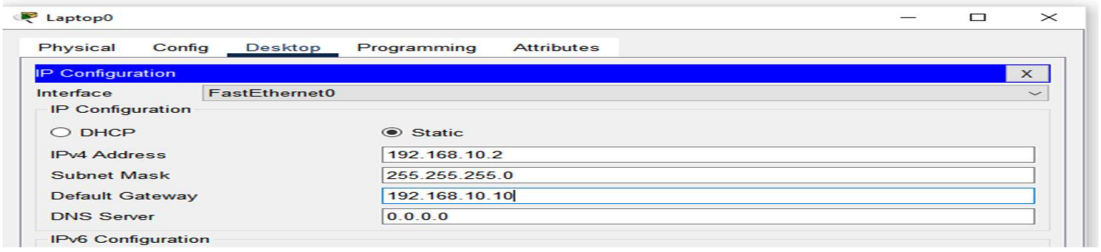


Figure 2.18: IP and Gateway for Laptop0

Step 4: Check Connectivity.

- From the top menu **Figure 2.2** select this icon and click on both 2 End Devices (PC0, Laptop0) source and destination.

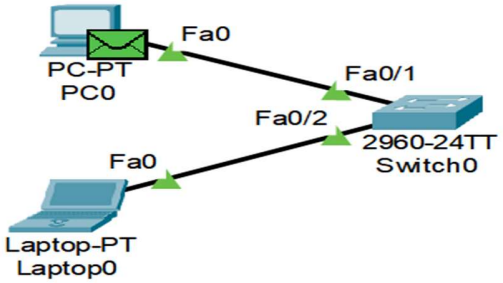


Figure 2.19: Adding simple PPU

- Click Simulation from the bottom toolbar

Figure 2.20: Simulation menu in bottom toolbar

- This will show the Simulation menu in the right side of screen. Where there will be a play button. Click that play button, the packet will transfer/travel from source to destination and every step/action will be visible.

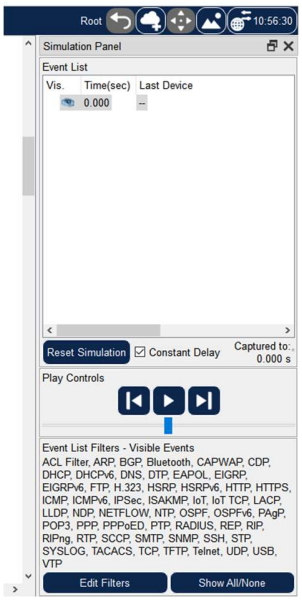


Figure 2.21: Right sidebar for simulation menus.

- If the packet is successfully transferred and received the result will be shown in the right side of the bottom toolbar.

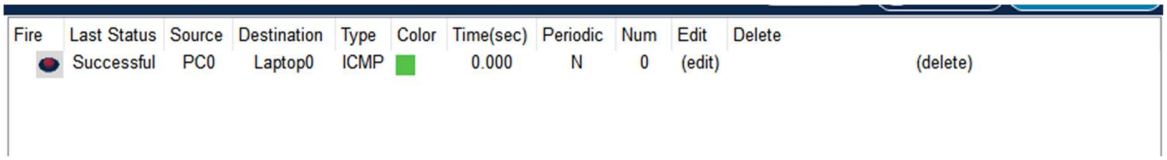


Figure 2.22: Result of successful packet transmit and receive.

This verifies that the network is properly configured and working correctly.

Observation and Result:

Here are the mostly used components that will be needed for future work. User can find, get the component, show the configuration window and connect devices using "Automatic Console Connection Type" from the cable menu. Configured the component use the simulation and successfully send and receive a packet.

Additional reading materials/ online tutorial/ References:

1. Video Tutorial: https://www.youtube.com/watch?v=frUQMHXhnvs
2. Article: https://learningnetwork.cisco.com/s/article/Using-Packet-Tracer-for-CCNA-Studys

3. Basic Router Configuration.

Title: Basic Router Configuration.

Objectives

1. Learn how to access and configure a router.
2. Understand basic commands for initial device setup.
3. Assigning name to the router and setting up domain.
4. Disabling DNS lookup.
5. Assigning console and vty password and creating a banner.
6. Configuring 3 interfaces (g0/0, g0/1 and loopback) of the router.
7. Verify network connectivity.
8. Saving the running configuration file.
9. Accessing the router form another computer using telnet.

Prerequisites

1. Knowledge of how to build network topology, configure the components.
2. Familiarity with command-line interfaces.

Theory

Router

Figure 3.1: Router

A router is a device that connects two or more packet-switched networks or subnetworks.

It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

Switch

Figure 3.2: Switch

The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments.

Switches have many ports, and when data arrives at any port, the destination address is examined first and some checks are also done and then it is processed to the devices.

VTY (Virtual Teletype)

“VTY" stands for Virtual Teletype. VTY is a virtual port used for Telnet or SSH access to the device, allowing network administrators to connect to and manage Cisco devices remotely.

Telnet (Teletype Network)

Telnet is a client/server application protocol that provides access to virtual terminals of remote systems on local area networks or the Internet.

Methodology

1. Set Up the Topology and Initialize End Devices.
2. Assigning name to the router and setting up domain.
3. Disabling DNS lookup.
4. Assigning console and vty password and creating a banner.
5. Configuring 3 interfaces (g0/0, g0/1 and loopback) of the router.
6. Verify network connectivity.
7. Saving the running configuration file.
8. Accessing the router form another computer using telnet.

Equipment

1. 2 Router (2911)
2. 1 Switch (2960-24TT)
3. 3 End Devices (2 PC, 1 Laptop)

Procedure

Step 1: Creating a network and configure the End Devices.

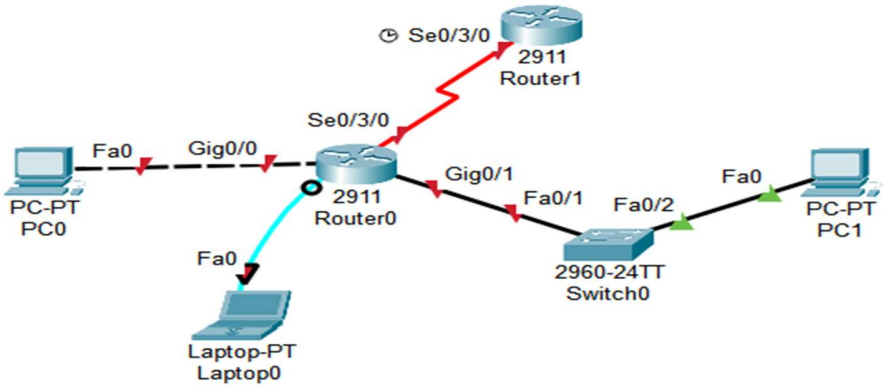


Figure 3.3: Topology of established network.

- Configure PC0 ip 192.168.10.2, subnet mask 255.255.255.0 and default gateway 192.168.10.1
- Configure PC1 ip 192.168.11.2, subnet mask 255.255.255.0 and default gateway 192.168.11.1
- Configure Laptop0 ip 192.168.12.2, subnet mask 255.255.255.0 and default gateway 192.168.12.1
- Turn on the routers interface.

Step 2: Assigning name to the router and setting up domain.

a. Console into the router and enable privileged EXEC mode.

router> enable

b. Enter configuration mode.

router# config terminal

c. Assign a device name to the router.

router(config)# hostname R1

Step 3: Disabling DNS lookup.

a. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

R1(config)# no ip domain lookup

Step 4: Assigning console and vty password and Creating a banner.

a. Assign the console password to "ciscoConsole"

R1(config)# line console 0
R1(config-line)# password ciscoConsole
R1(config-line)# login

b. Assign the privilege mode (Exec mode) password to "ciscoEnable"

R1(config)# enable password ciscoEnable

c. Assign "ciscoVty" as the vty password and enable login.

R1(config)# line vty 0 4
R1(config-line)# password ciscoVty
R1(config-line)# login

d. Create a banner that warns anyone accessing the device.

R1(config)# banner motd @
****
Authorized Access Only.
****
@

Step 5: Configuring 3 interfaces (g0/0, g0/1 and loopback) of the router.

a. Configure all three interfaces on the router with the IPv4 address and add description.

R1(config)# interface g0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description Connection to PC-0
R1(config-if)# no shutdown
R1(config-if)# exit

R1(config)# interface g0/1
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# description Connection to Switch-1
R1(config-if)# no shutdown
R1(config-if)# exit

R1(config)# interface loopback0
R1(config-if)# ip address 192.168.12.1 255.255.255.0
R1(config-if)# description loopback adapter
R1(config-if)# no shutdown
R1(config-if)# exit

(**N.B.** The loopback interface acts as a placeholder for the static IP address and provides default routing information.)

Step 6: Verify network connectivity.

a. Check console login

b. Check network's packet transfer to verify successful connection.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	

Figure 3.5: Packet transfer from PC0 to PC1 successful.

Figure 3.6: Console login and privileged EXEC mode login.

Step 7: Saving the running configuration file.

a. Save the running configuration to the startup configuration file.

R1# copy running-config startup-config

Step 8: Accessing the router form another computer using telnet.

a. From PC-A's Command Prompt

C:\>telnet 192.168.10.1

b. Enter password (ciscoVty) to check if it's working.

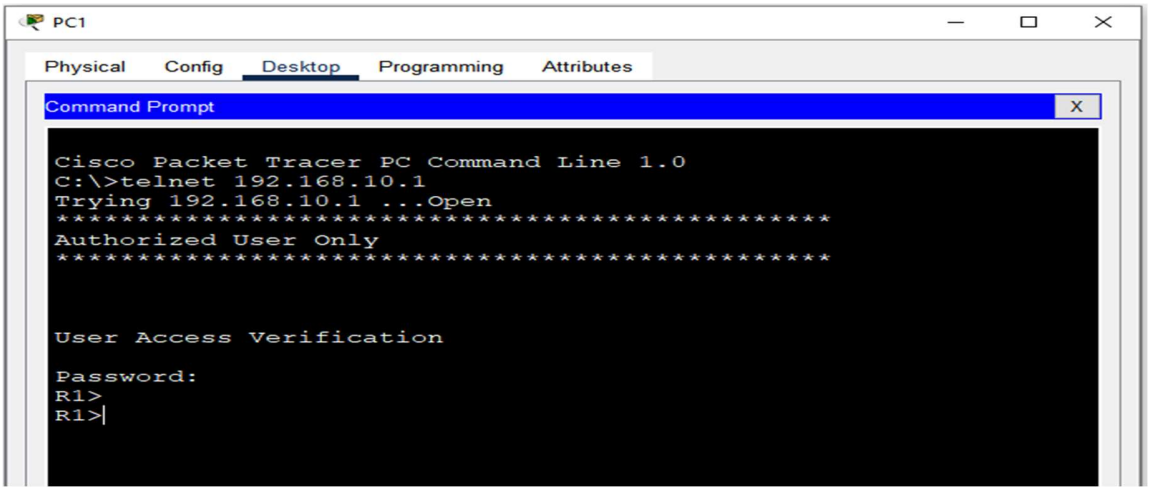


Figure 3.7: Login from PC0 to PC1 using Telnet.

Observation and Result

The telnet is working so does the user verification system.

Additional reading materials/ online tutorial/ References.

4. Application Layer Services (Server).

Title: Application Layer Services (Server)

Objectives

1. Learn how to setup and configure DHCP servers.
2. Learn how to setup and configure DNS servers.
3. Learn how to setup and configure HTTP servers.
4. Learn how to setup and configure Email (SMTP) servers.

Prerequisites

1. Knowledge of how to build network topology, configure the components.

Theory

Application layer Services

An application layer is an abstraction layer that specifies the shared communication protocols and interface methods used by hosts in a communications network. An application layer abstraction is specified in both the Internet Protocol Suite and the OSI model. Although both models use the same term for their respective highest-level layer.

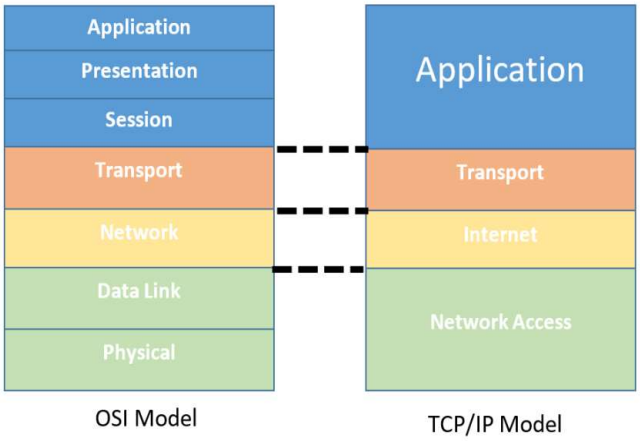


Figure 4.1: OSI and TCP/IP model

HTTP (Hypertext Transfer Protocol)

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

HTTP Server
HTTP server is a combination of hardware and software. Through this software and hardware, we translate and browse all the data and information. The webpages or websites that we visit while browsing, is stored within this server.

DHCP (Dynamic Host Configuration Protocol)
DHCP (Dynamic Host Configure Protocol) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network.

DNS (Domain Name System)
The Domain Name System (DNS) is the phonebook of the Internet. When user type domain names such as 'google.com' or 'nytimes.com' into web browsers, DNS is responsible for finding the correct IP address for those sites. Browsers then use those addresses to communicate with origin / main servers or to access website information.

SMTP (Simple Mail Transfer Protocol)
Simple Mail Transfer mechanism (SMTP) is a mechanism for exchanging email messages between servers. It is an essential component of the email communication process and operates at the application layer of the TCP/IP protocol stack. SMTP is a protocol for transmitting and receiving email messages. In this article, we are going to discuss every point about SMTP.

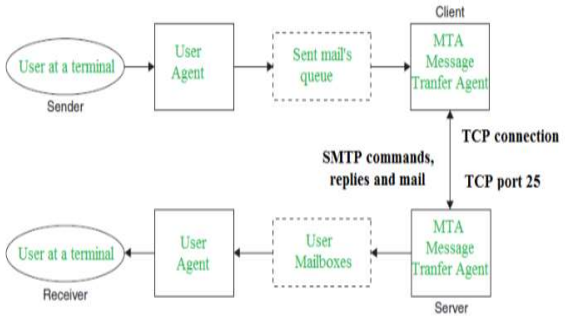


Figure 4.2: SMTP Model

Methodology

1. Set up the topology.
2. Configure IP addresses for the servers.
3. Configure DHCP server.
4. Configure IP address and default gateway automatically by DHCP.
5. Configure DNS server and verify it's working.
6. Configure HTTP server and verify it's working.
7. Configure Email (SMTP) server and verify it's working.

Equipment

1. 2 Server-PT
2. 4 Switch (2960-24TT)
3. 4 End Devices (2 PC, 1 Laptop)

Procedure

Step 1: Creating a network and configure the End Devices.

Here the IP of the PC's will not be configured manually because the DHCP server will automatically provide and configure IP for the PCs.

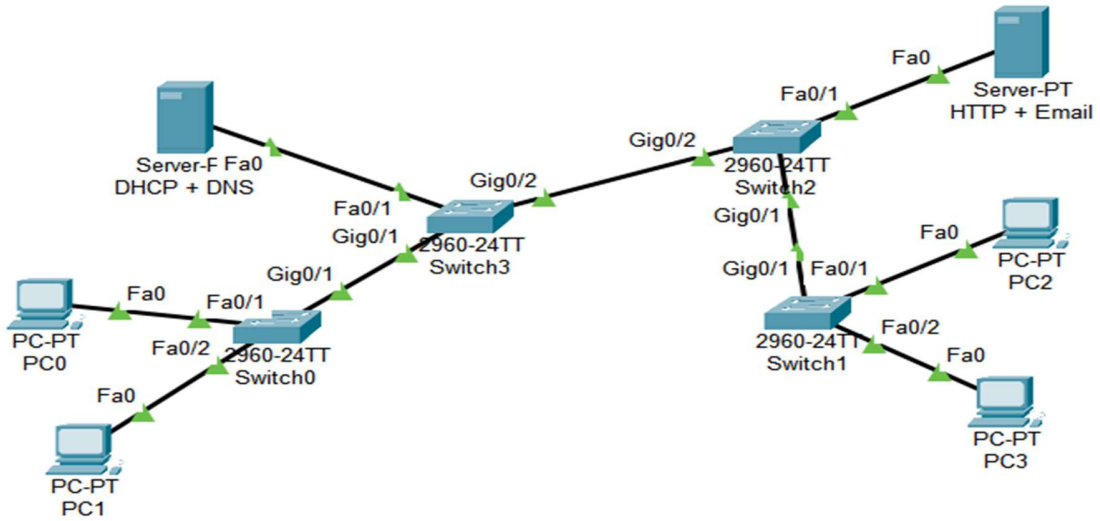


Figure 4.3: Topology of established network.

Step 2: Configure IP Addresses for the servers.

- Set 192.168.100.10 as IP address and 192.168.100.1 as default gateway for the DHCP + DNS server.

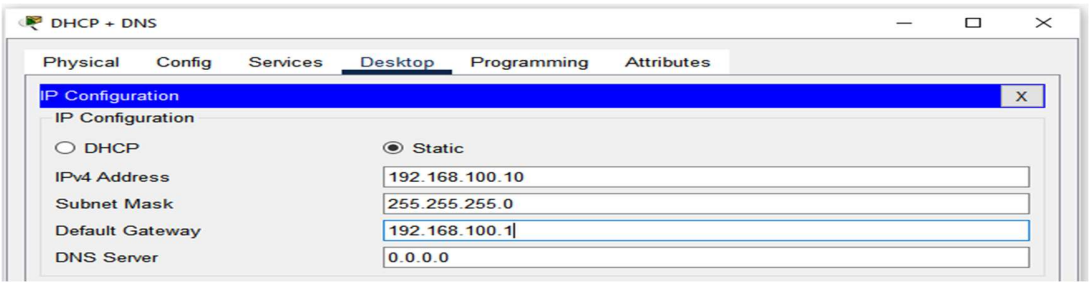


Figure 4.4: IP address and default gateway for DHCP+DNS server.

- Set 192.168.100.10 as IP address and 192.168.100.1 as default gateway for the HTTP + Email server.

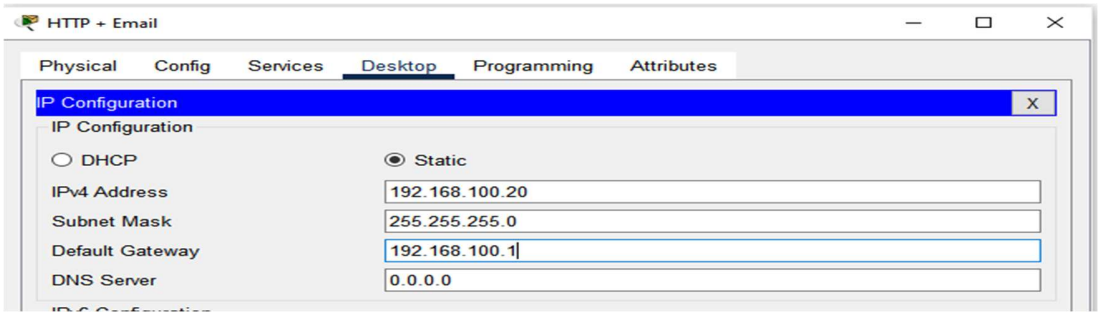


Figure 4.5: IP address and default gateway for HTTP + Email server.

Step 3: Configure DHCP Server

- Click on the DHCP + DNS server, from service tab select DHCP from the right menu.
- Turn on the server.
- Put 192.168.100.1 as default gateway.
- For DNS server put 192.168.100.10 (DHCP + DS Server's IP)
- Set start IP address 192.168.100.50
- And Define maximum user number (Which will get IP from this server automatically).
- Click Save Button

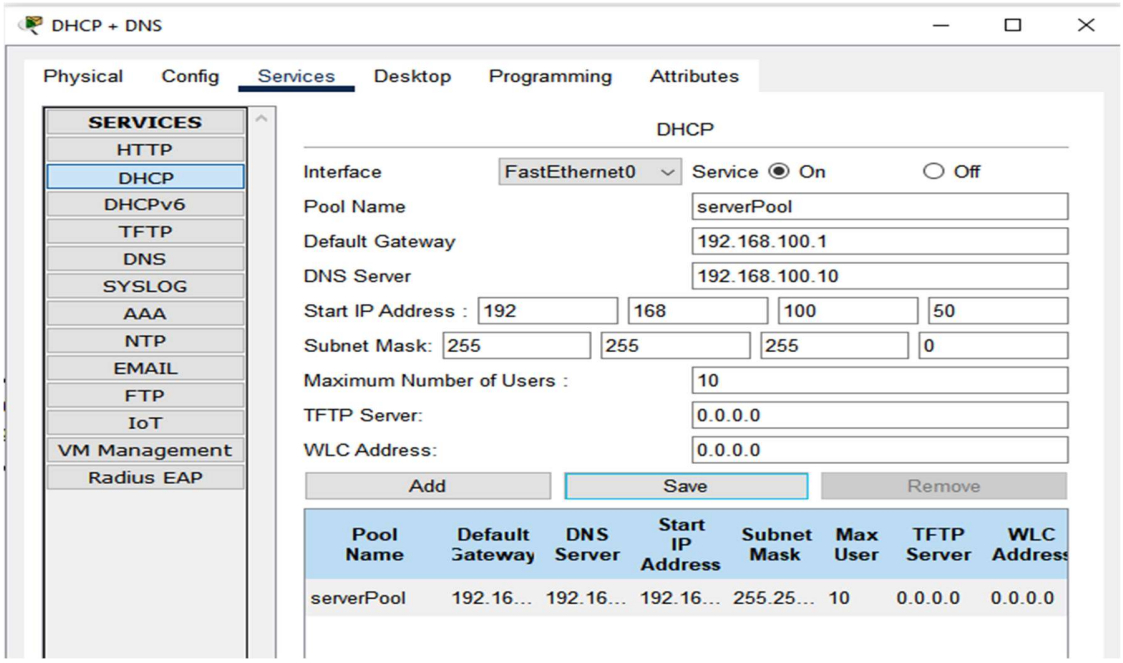


Figure 4.6: DHCP server configuration.

Step 4: Configure IP address and default gateway automatically by DHCP

- In every PC on desktop's IP configuration menu click DHCP it will request for IP address, Default gateway and when the request is successful the IP address, Subnet mask and Default gateway will automatically and dynamically initialized.

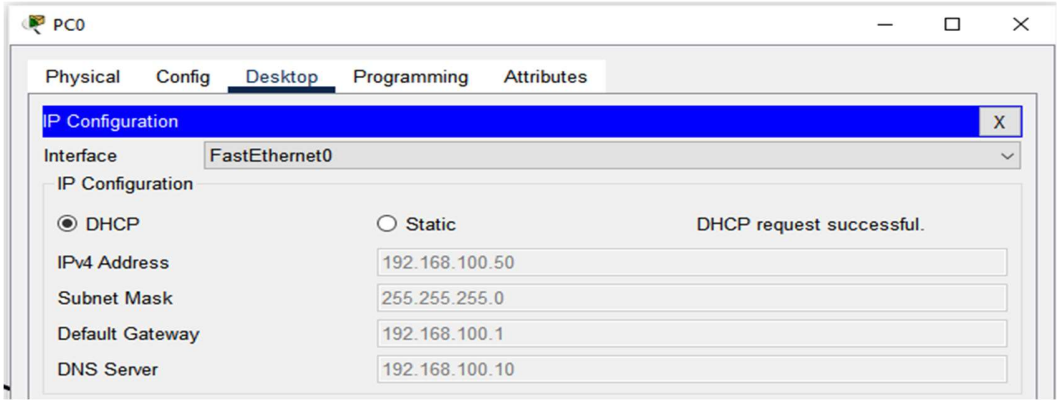


Figure 4.7: IP address, subnet mask and default gateway automatically configured on PC0.

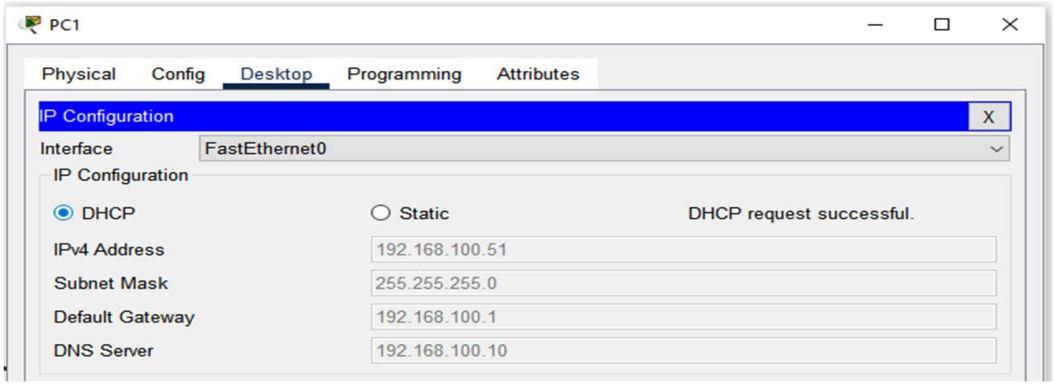


Figure 4.8: IP address, subnet mask and default gateway automatically configured on PC1.

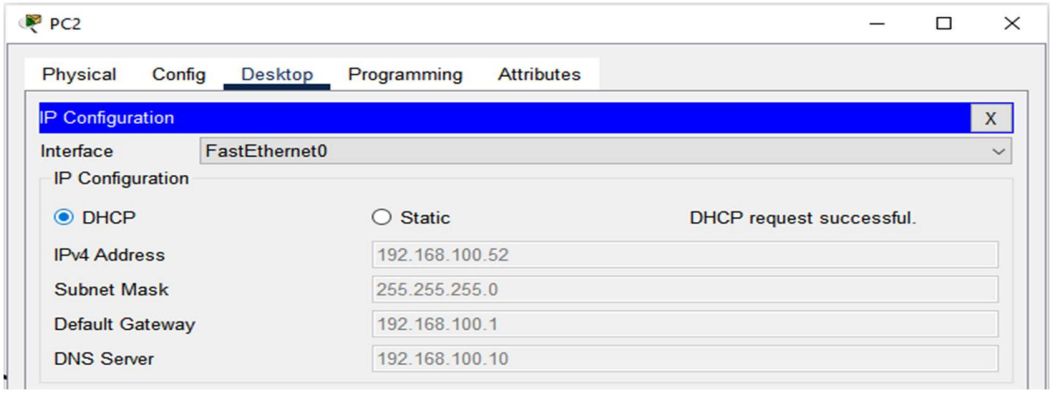


Figure 4.9: IP address, subnet mask and default gateway automatically configured on PC2.

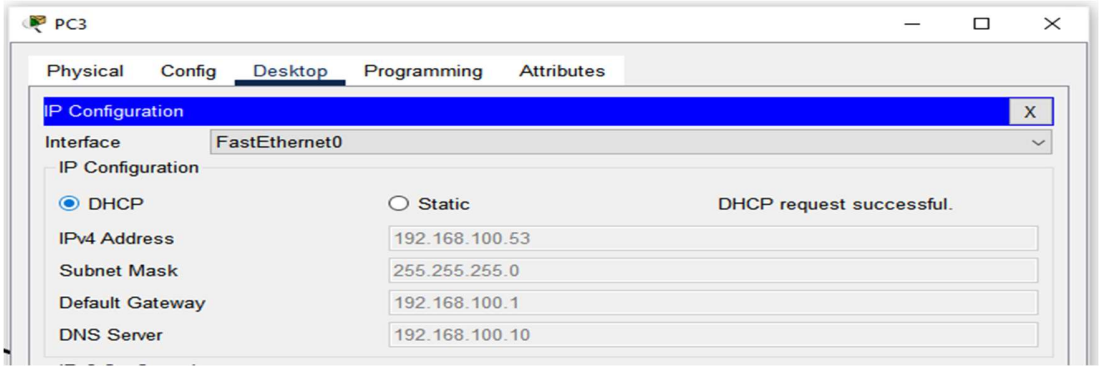


Figure 4.10: IP address, subnet mask and default gateway automatically configured on PC3.

Step 5: Configure DNS server.

- In DHCP + DNS server click DNS option from Services menu.
- Turn on the DNS service
- Put a name for an IP address
- Put the IP address
- Click save

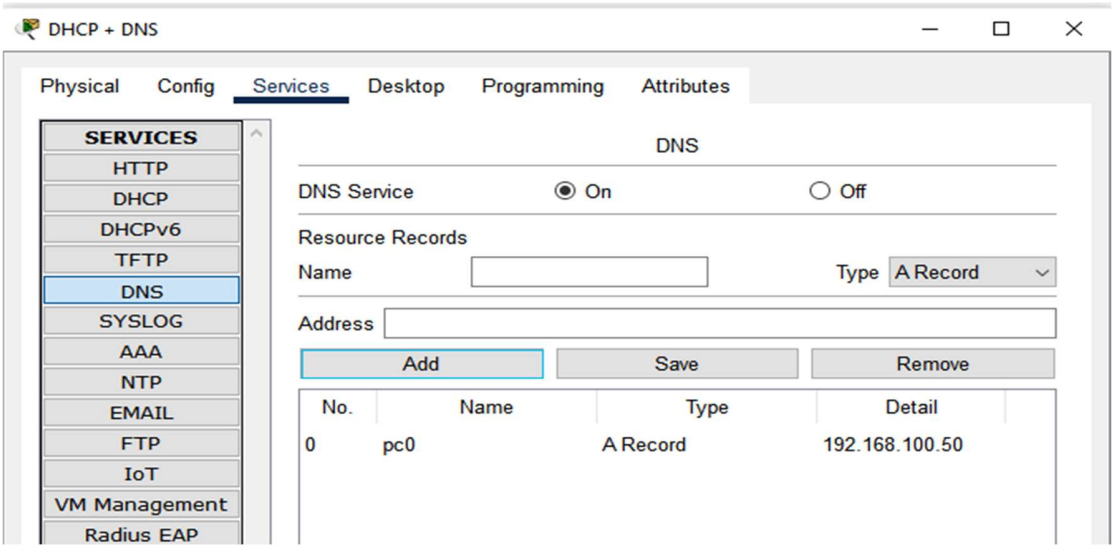


Figure 4.11: Adding record in the DNS server.

- To verify if its working, here in DNS server 192.168.100.50 (which is the IP address for PC0) is recorded as “pc0”. Open any other PC (for this case PC1) click PC1’s command prompt and write **ping pc0**. Which will send and receive 4 packets from pc0 (192.168.100.50 or PC0). If the 4 packets are received then the DNS server is working correctly.

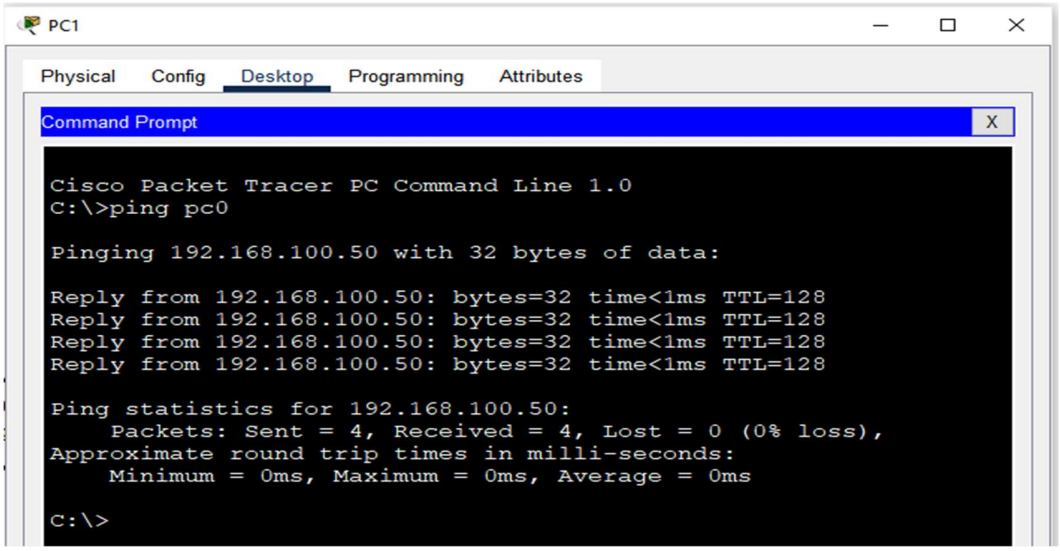


Figure 4.12: All packet are successfully send and received from PC0.

Step 6: Configure HTTP server and verify it's working.

- IN HTTP + Email server turn on HTTP and click on New File.

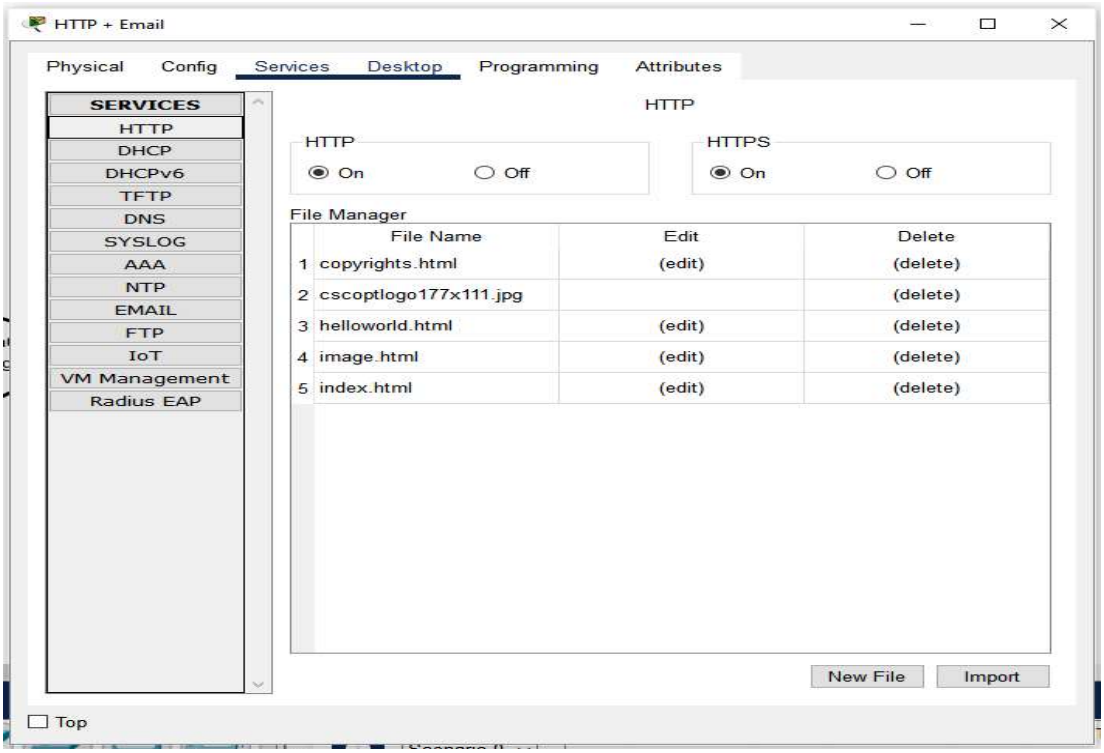


Figure 4.13: HTTP server menu.

- Put a file name and a html text for verification.

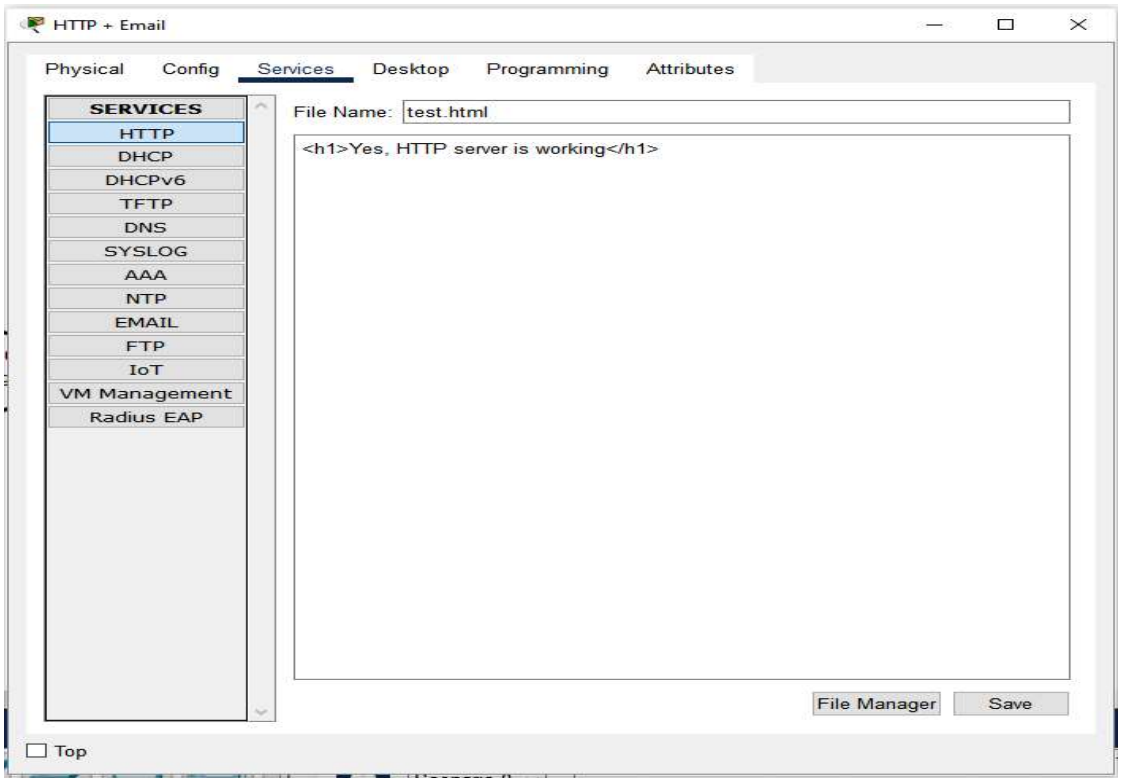


Figure 4.14: Creating a html document.

- To verify its working from any PC (in this case PC1) open its browser and type the IP address or the domain name (IF its been added into the DNS server's record) then the html document name that has been created now. In this case the link will be IP address/test.html or http://192.168.100.20/test.html in the URL field. It will show the contents from the test.html that is created above.

Figure 4.15: Contents from test.html document which is stored in HTTP server.

Step 7: Configure Email (SMTP) server and verify it's working.

- In HTTP + Email server form services select Email. Here in user field fill user name and password and add by clicking + option on right.

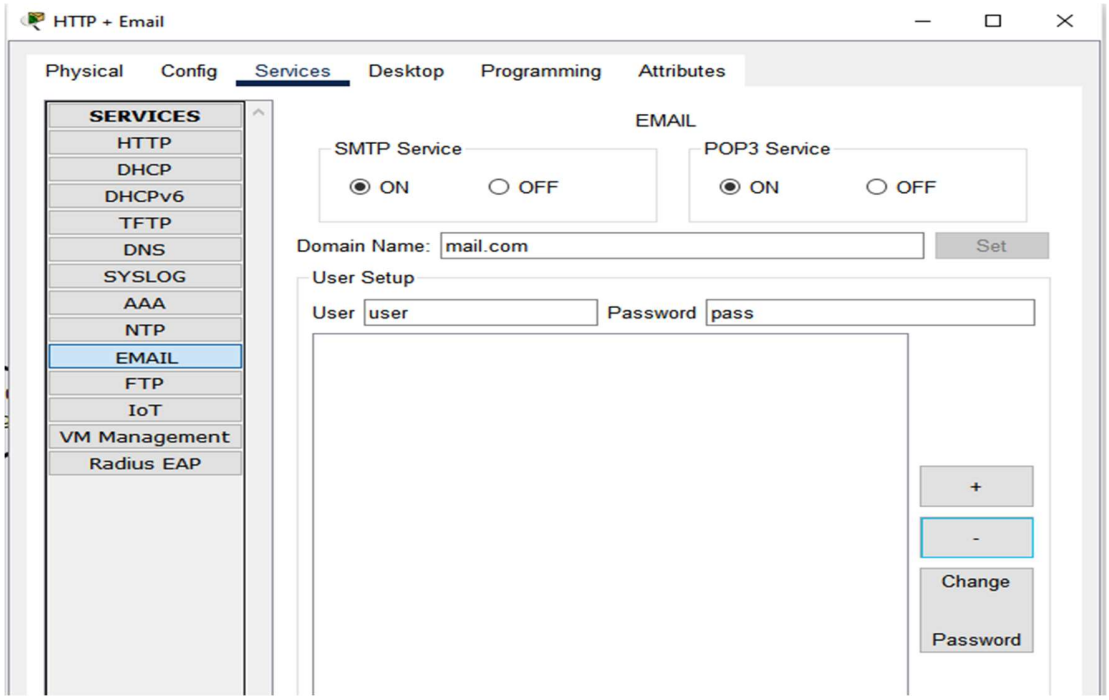


Figure 4.16: Adding users in SMTP services.

- From any PC's (in this case PC1 and PC3) select browser and fill the credential. Remember these credential should match with the added user's credential from Email services. In incoming and outgoing server put HTTP + Email server's IP address.

Figure 4.17: User 1's credential added.

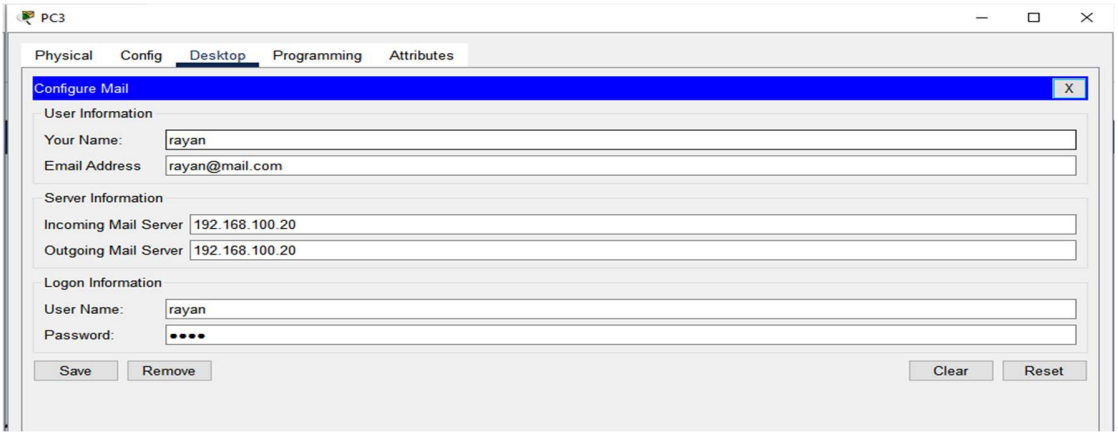


Figure 4.18: User 1's credential added.

- To test if its working compose a mail and send the mail. On the other pc if the mail is available from the receive menu then the Email/SMTP server is working correctly.

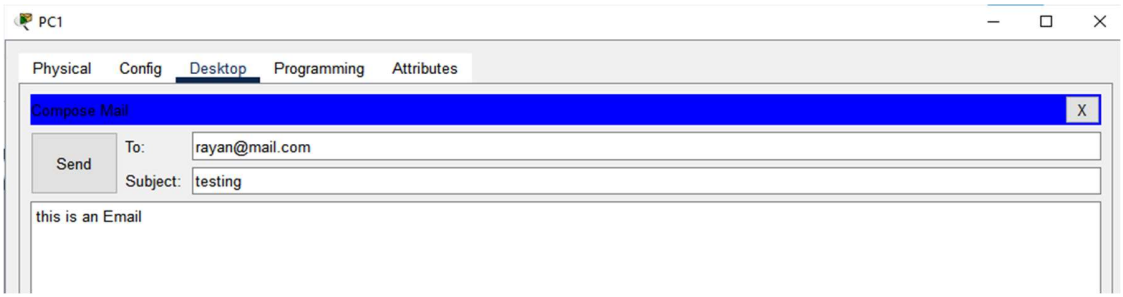


Figure 4.19: Composing an Email.

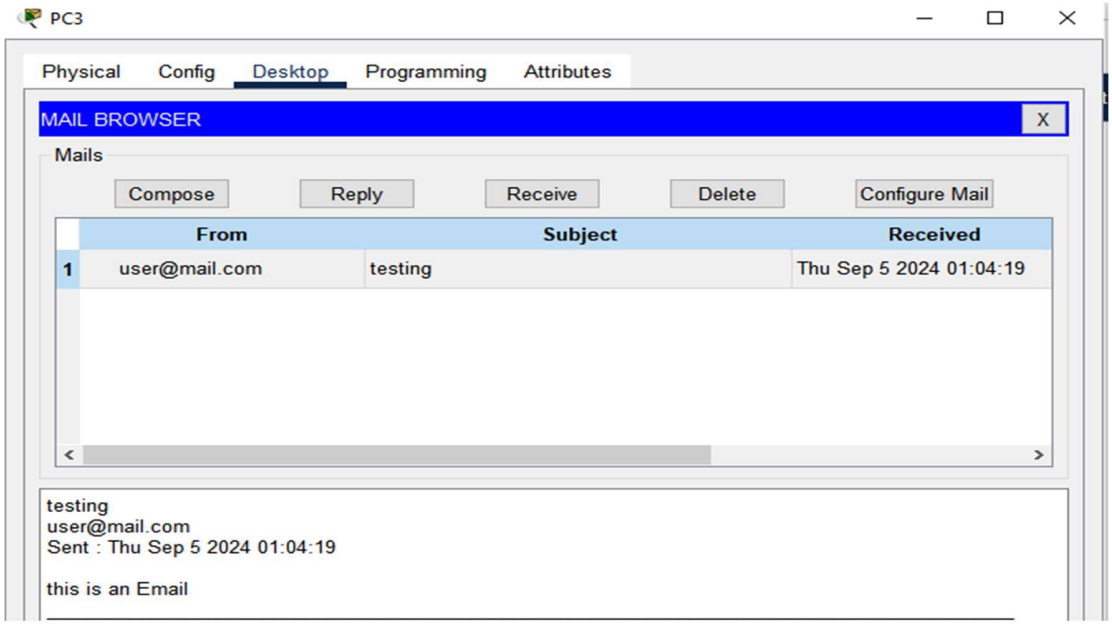


Figure 4.20: Email successfully received.

Observation and Result

All of the servers i.e. DHCP, DNS, HTTP, Email are working properly.

Additional reading materials/ online tutorial/ References.

1. DHCP server setup article: https://www.packettracerlab.com/setting-up-a-dhcp-server/
2. DNS server setup article: https://www.packettracerlab.com/dns-in-cisco-packet-tracer/
3. HTTP server setup article: https://ccnapracticallabs.com/set-up-http-server-packet-tracer/
4. Email server setup article: https://computernetworking747640215.wordpress.com/2018/07/05/configuring-a-mail-server-in-packet-tracer/

5. Sub-netting and VLSM

Title: Routing Protocol Configuration.

Objectives

1. Implement Sub-netting and VLSM

Prerequisites

1. Knowledge of how to build network topology, configure the components.
2. **Theoretical knowledge on Sub-netting, VLSM, and IP address and subnet mask calculation based on VLSM.**
3. Different class of IP,

Theory

Sub-netting

When a bigger network is divided into smaller networks, to maintain security, then that is known as Sub-netting.

Subnets make networks more efficient. Through sub-netting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.

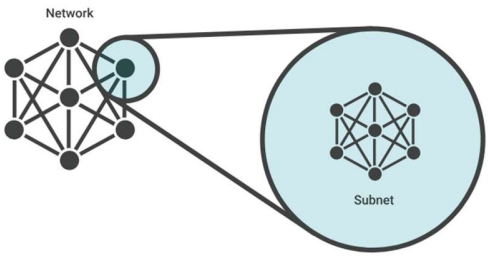


Figure 5.1: Sub-net

Approaches to sub-netting:

There are two approaches to subnetting an IP address for a network: Fixed length subnet mask (FLSM) and variable-length subnet mask (VLSM).

In FLSM subnetting, all subnets are of equal size with an equal number of host identifiers. It use the same subnet mask for each subnet, and all the subnets have the same number of addresses in them. It tends to be the most wasteful because it uses more IP addresses than are necessary.

VLSM is a subnet design strategy that allows all subnet masks to have variable sizes. In VLSM subnetting, network administrators can divide an IP address space into subnets of different sizes,

and allocate it according to the individual need on a network. This type of subnetting makes more efficient use of a given IP address range.

Subnet mask

Subnet masks are used by a computer to determine if any computer is on the same network or on a different network. An IPv4 subnet mask is a 32-bit sequence of ones (1) followed by a block of zeros (0). The ones designate the network prefix, while the trailing block of zeros designates the host identifier. In shorthand, we use /24, which simply means that a subnet mask has 24 ones, and the rest are zeros.

Methodology

1. Set up the topology.
2. Configure IP addresses for the PCs and routers.
3. Implementing OSPF in routers.
4. Check connectivity.

Equipment

1. 2 Server-PT
2. 4 Switch (2960-24TT)
3. 4 End Devices (2 PC, 1 Laptop)

Procedure:

Step 1: Setup the network Topology.

- Connect all component as shown in this figure.

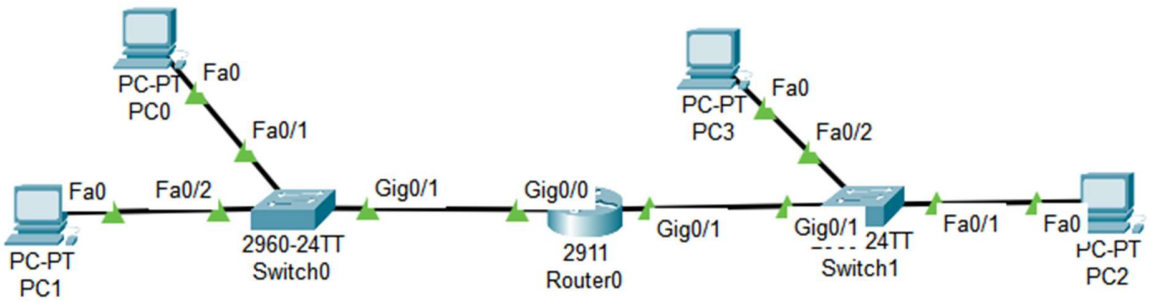


Figure 5.2: Topology of established network.

Here assume that on left side the network need 10 IP address valid/usable and on the right side it needs 2 valid/usable IP address. For this requirement do the calculation of IP address range and subnet mask for the range for IP address 192.168.10.0/24 which will be needed for configuration.

Step 2: Configure IP addresses for the PCs and routers.

- For left side of network: (PC0, PC1)
  IP address range: 192.168.10.0 – 192.168.10.15
  Subnet mask: 255.255.255.240
  Default gateway: 192.168.10.1

  Network address: 192.168.10.0
  Broadcast address: 192.168.10.15

- For right side of network: (PC2, PC3)
  IP address range: 192.168.10.16 – 192.168.10.23
  Subnet mask: 255.255.255.248
  Default gateway: 192.168.10.17

  Network address: 192.168.10.16
  Broadcast address: 192.168.10.23

- Configure IP address, subnet mask and default gateway on the PC and routers according to the calculation.

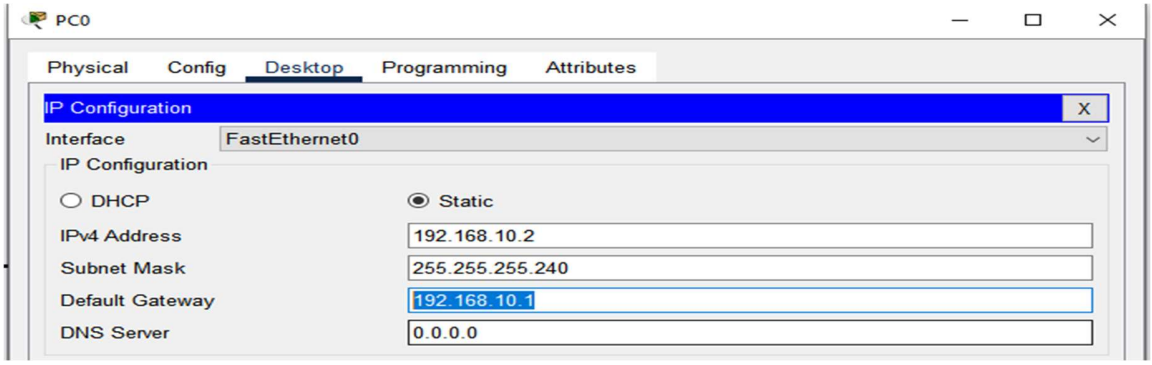


Figure 5.3: IP address, subnet mask and default gateway configured on PC0

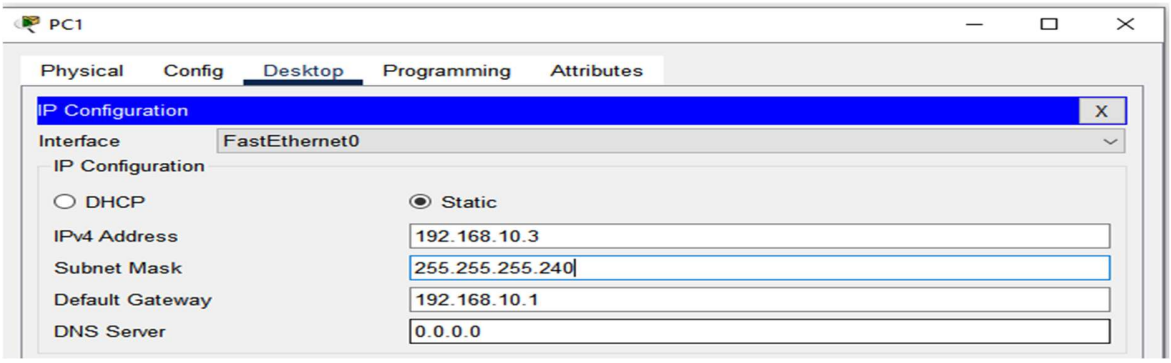


Figure 5.4: IP address, subnet mask and default gateway configured on PC1

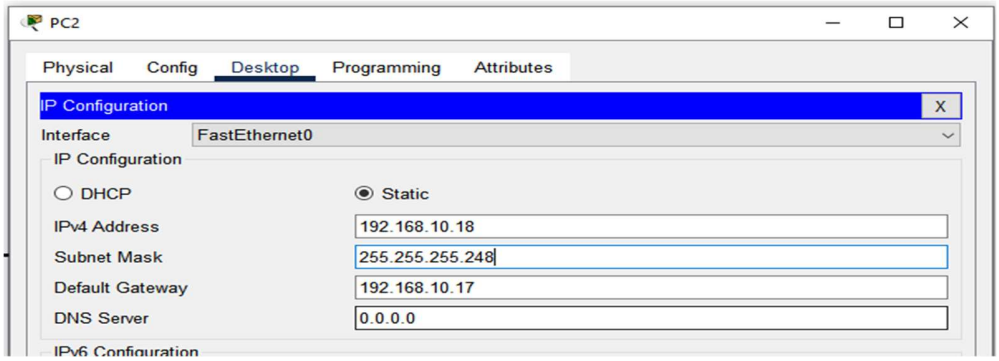


Figure 5.5: IP address, subnet mask and default gateway configured on PC2

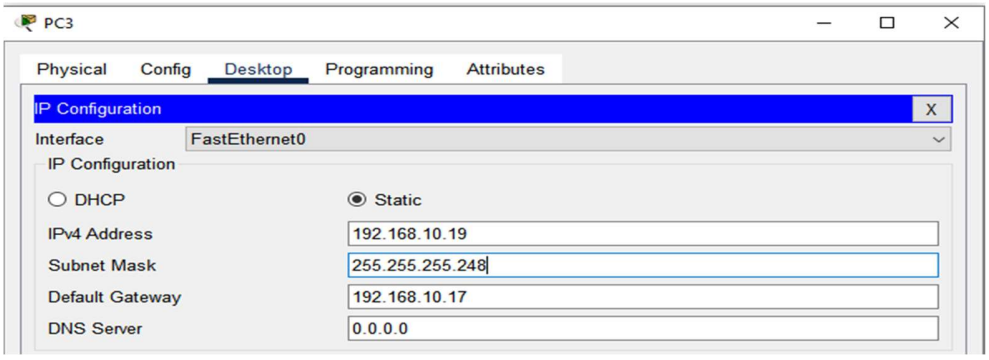


Figure 5.6: IP address, subnet mask and default gateway configured on PC3

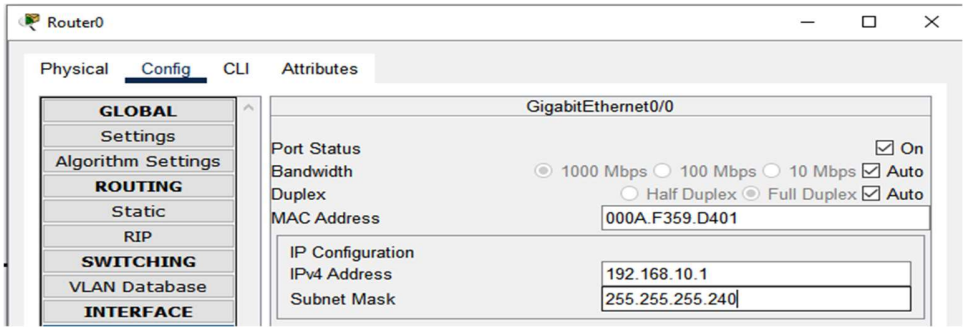


Figure 5.7: IP address, subnet mask for interface gig0/0 configured on Router

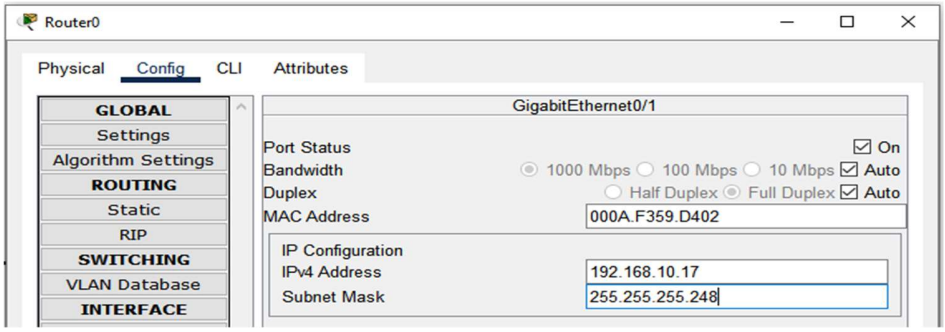
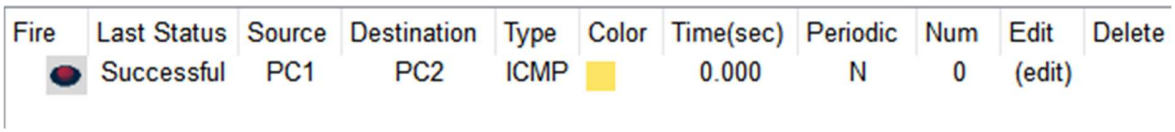


Figure 5.8: IP address, subnet mask for interface gig0/0 configured on Router

Step 3: Check connectivity

- For confirming if VLSM is working correctly transmit and receive a packet from any PC from left side sub network to the right side sub network to opposite side network PC. If its successful then the VLSM is correctly implemented.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC2	ICMP		0.000	N	0	(edit)	

Figure 5.9: Packet transmission and received successfully.

Observation and Result

Packet from one sub network to another sub network's end device is successfully transmitted and received, meaning VLSM is working proporly.

Additional reading materials/ online tutorial/ References.

6. Routing Protocol Configuration

Title: Routing Protocol Configuration.

Objectives

1. Configure OSPF routing protocol.

Prerequisites

1. Knowledge of how to build network topology, configure the components.
2. Knowledge of VLSM for IP address and subnet mask assigning.

Theory

OSPF

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First. It is a network layer protocol which works on protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router (DR)/Backup Designated Router (BDR).

OSPF working

1. Neighbor Discovery:
    - OSPF routers use Hello packets to discover and establish neighbor relationships with directly connected routers.
    - Routers must agree on certain parameters (like Hello and Dead intervals) to become neighbors.
2. Link-State Advertisements (LSAs):
    - Once neighbors are established, routers exchange Link-State Advertisements (LSAs). Which contains information about the router's links and their state.
3. Link-State Database (LSDB):
    - Each router maintains an LSDB, a database of all received LSAs.
    - The LSDB is identical on all routers within the same OSPF area.
4. Shortest Path First (SPF) Algorithm:
    - Routers use the SPF algorithm (Dijkstra's algorithm) to calculate the shortest path to each destination and The result is installed in the router's routing table.

5. Areas:
    - Area 0, the backbone area, is the central area to which all other areas connect.
6. Route Calculation:
    - OSPF calculates the best path based on the cost (metric), which is typically determined by the bandwidth of the links.

Methodology

1. Set up the topology.
2. Configure IP addresses for the PCs and routers.
3. Implementing OSPF in routers.
4. Check connectivity.

Equipment

1. 4 Routers (2911)
2. 6 Switch (2960-24TT)
3. 6 End Devices

Procedure:

Step 1: Setup the network Topology.

- Connect all component as shown in this figure and for connecting routers with routers use serial cable for that use HWIC-2T module.

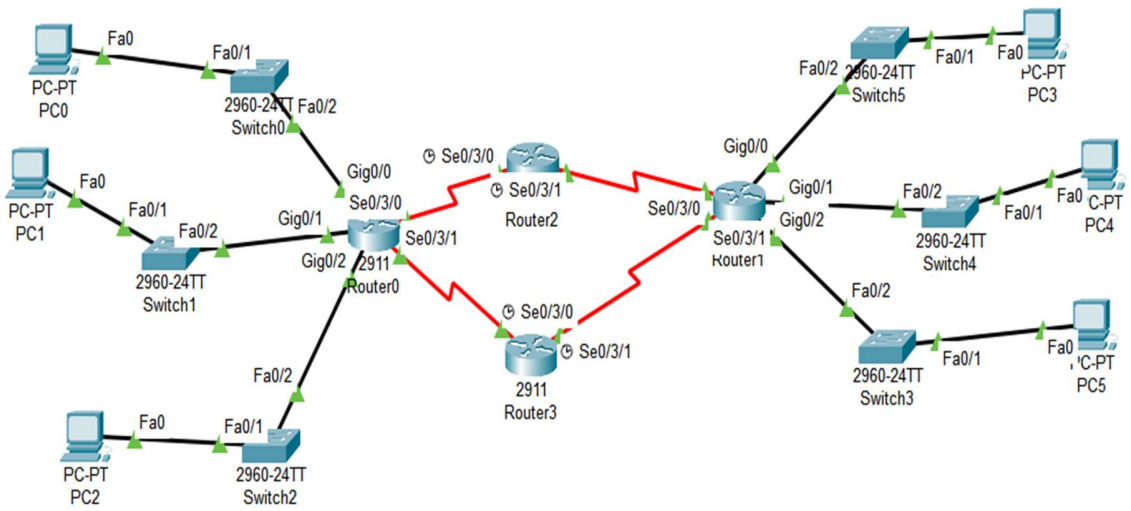


Figure 6.1: Topology of established network.

- Configure IP address, subnet mask and default gateway for the PC.

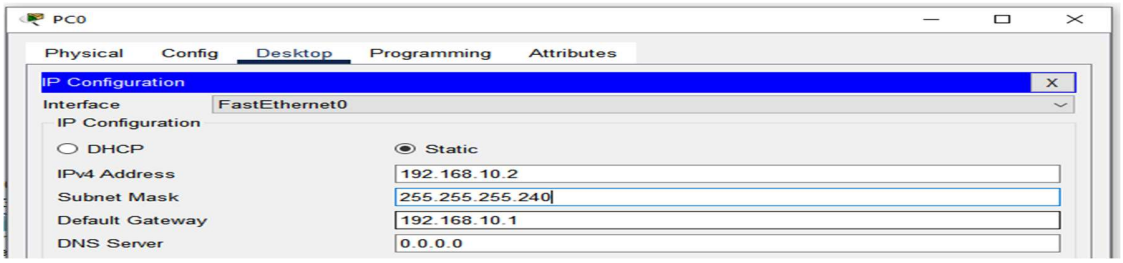


Figure 6.2: IP address, subnet mask and default gateway configured on PC0.

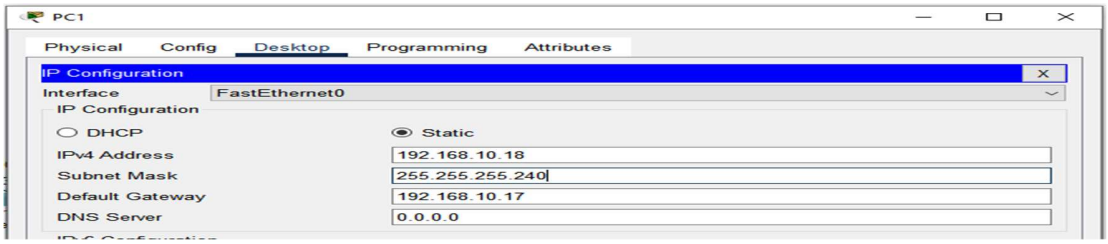


Figure 6.3: IP address, subnet mask and default gateway configured on PC1.

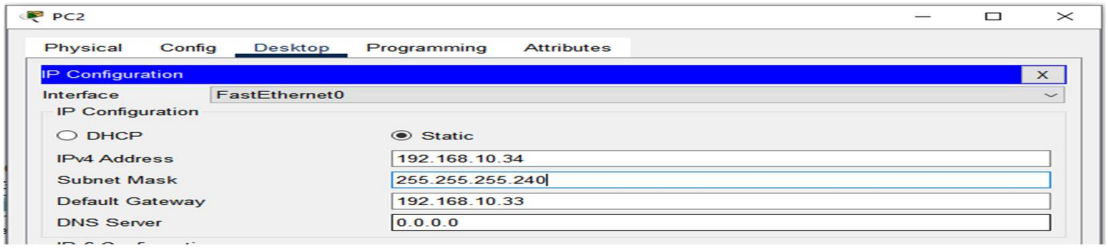


Figure 6.4: IP address, subnet mask and default gateway configured on PC2.

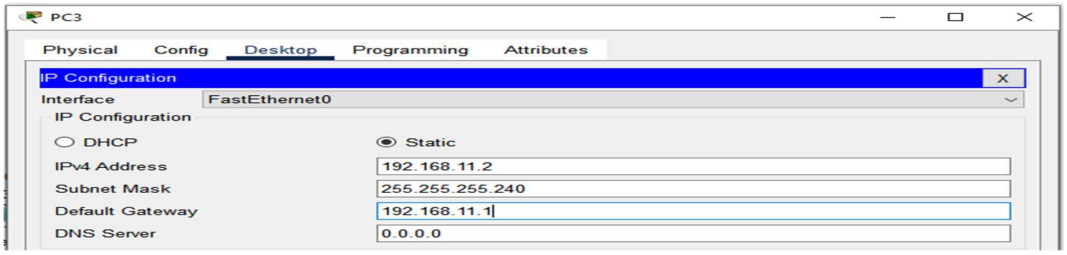


Figure 6.5: IP address, subnet mask and default gateway configured on PC3.

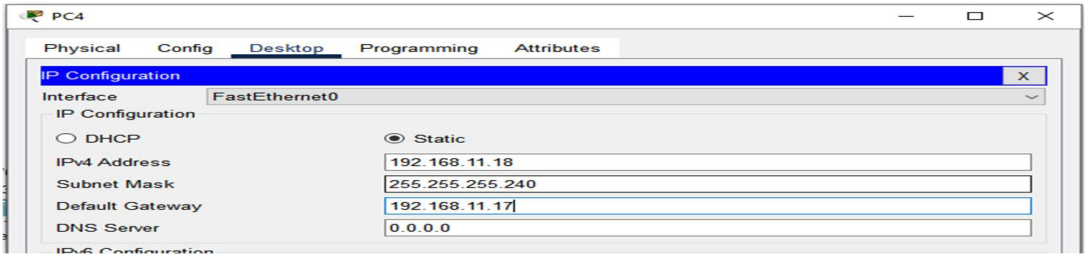


Figure 6.6: IP address, subnet mask and default gateway configured on PC4.

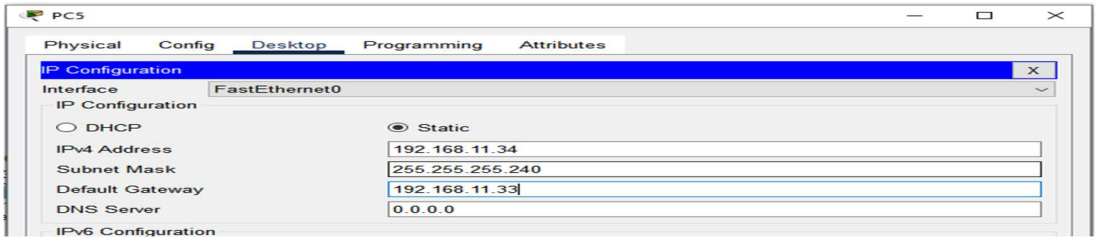


Figure 6.7: IP address, subnet mask and default gateway configured on PC5.

- Turn on every router interface that is connected and configure IP address and subnet mask for all of the interfaces that are being used.

Router 0:

- IP address & subnet mask for Gig0/0 (GigabitEtherrnet0/0) which connects the Switch0, PC0 with Router0.

Figure 6.8: IP address and subnet mask configured for Gig0/0 (GigabitEthernet0/0)

- IP address & subnet mask for Gig0/1 (GigabitEtherrnet0/1) which connects the Switch1, PC1 with Router0.

Figure 6.9: IP address and subnet mask configured for Gig0/1 (GigabitEthernet0/1)

- IP address & subnet mask for Gig0/2 (GigabitEtherrnet0/2) which connects the Switch2, PC2 with Router0

Figure 6.10: IP address and subnet mask configured for Gig0/2 (GigabitEthernet0/2)

- IP address & subnet mask for Se0/3/0 (Serail0/3/0) which connects Router2 with Router0

Figure 6.11: IP address and subnet mask configured for Se0/3/0 (Serail0/3/0)

- IP address & subnet mask for Se0/3/1 (Serail0/3/1) which connects Router3 with Router0

Figure 6.12: IP address and subnet mask configured for Se0/3/1 (Serail0/3/1)

Router 2:

- IP address & subnet mask for Se0/3/0 (Serail0/3/0) which connects Router0 with Router2

Figure 6.13: IP address and subnet mask configured for Se0/3/0 (Serail0/3/0)

- IP address & subnet mask for Se0/3/1 (Serail0/3/1) which connects Router1 with Router2

Figure 6.14: IP address and subnet mask configured for Se0/3/1 (Serail0/3/1)

Router 1:

- IP address & subnet mask for Gig0/0 (GigabitEtherrnet0/0) which connects the Switch5, PC3 with Router1.

Figure 6.15: IP address and subnet mask configured for Gig0/0 (GigabitEthernet0/0)

- IP address & subnet mask for Gig0/1 (GigabitEtherrnet0/1) which connects the Switch4, PC4 with Router1.

Figure 6.16: IP address and subnet mask configured for Gig0/1 (GigabitEthernet0/1)

- IP address & subnet mask for Gig0/2 (GigabitEtherrnet0/2) which connects the Switch3, PC5 with Router1.

Figure 6.17: IP address and subnet mask configured for Gig0/0 (GigabitEthernet0/0)

- IP address & subnet mask for Se0/3/0 (Serail0/3/0) which connects Router2 with Router1

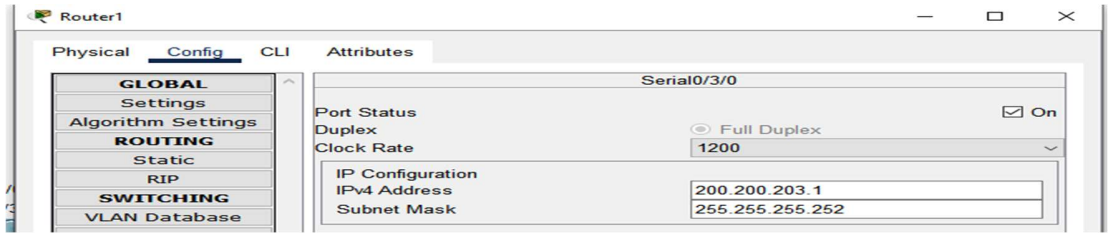


Figure 6.18: IP address and subnet mask configured for Se0/3/0 (Serail0/3/0)

- IP address & subnet mask for Se0/3/1 (Serail0/3/1) which connects Router3 with Router1

Figure 6.19: IP address and subnet mask configured for Se0/3/1 (Serail0/3/1)

Router 3:

- IP address & subnet mask for Se0/3/0 (Serail0/3/0) which connects Router0 with Router3

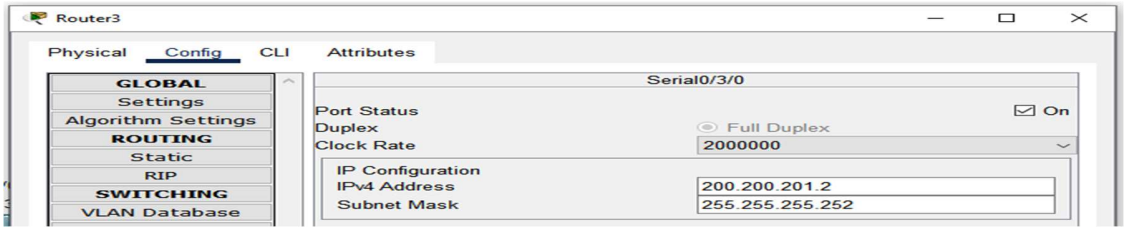


Figure 6.20: IP address and subnet mask configured for Se0/3/0 (Serail0/3/0)

- IP address & subnet mask for Se0/3/1 (Serail0/3/1) which connects Router1 with Router1

Figure 6.21: IP address and subnet mask configured for Se0/3/1 (Serail0/3/1)

In this network setup, devices connected to Switches 0, 1, and 2 are under Router 0 and can communicate with each other without needing a routing protocol because they are part of the same router's routing table. However, devices connected to Router 0 cannot communicate with devices connected to Router 1 (Switches 3, 4, and 5) without configuring a routing protocol. To enable communication between devices on different routers, OSPF (Open Shortest Path First) will be demonstrated in this experiment. OSPF will allow the routers to dynamically share and update their routing tables, ensuring that all networks can communicate with each other across the routers.

Step 3: Implementing OSPF in routers.

For Router 0:

- Console into the router and enable privileged EXEC mode.
  Router> enable
- Enter configuration mode.
  Router# config terminal
- Enable OSPF.
  Router (config)# router ospf 1
- Assign Router IDs.
  Router (config-router)# router-id 1.1.1.1

(Assign a router ID to each router. This ID should be a unique IP address-like identifier for OSPF to use. It does not need to be an actual IP address from the network but should be unique)

- Define OSPF Network Statements
  Router (config-router)# network 192.168.10.0 0.0.0.15 area 0
  Router (config-router)# network 192.168.10.16 0.0.0.15 area 0
  Router (config-router)# network 192.168.10.32 0.0.0.15 area 0
  Router (config-router)# network 200.200.200.0 0.0.0.3 area 0
  Router (config-router)# network 200.200.201.0 0.0.0.3 area 0

(Define the networks that OSPF should advertise and the associated wildcard mask. The wildcard mask is the inverse of the subnet mask. Specify the area as `0` (for a simple setup with one OSPF area).)

- Exit configuration mode and return to privileged EXEC mode.
  Router (config-router)# end
- Save configuration
  Router# write memory

For Router 1:

- Console into the router and enable privileged EXEC mode.
  Router> enable
- Enter configuration mode.
  Router# config terminal
- Enable OSPF.
  Router (config)# router ospf 1
- Assign Router IDs.
  Router (config-router)# router-id 2.2.2.2

- Define OSPF Network Statements
  Router (config-router)# network 192.168.11.0 0.0.0.15 area 0
  Router (config-router)# network 192.168.11.16 0.0.0.15 area 0
  Router (config-router)# network 192.168.11.32 0.0.0.15 area 0
  Router (config-router)# network 200.200.202.0 0.0.0.3 area 0
  Router (config-router)# network 200.200.203.0 0.0.0.3 area 0
- Exit configuration mode and return to privileged EXEC mode.
  Router (config-router)# end
- Save configuration
  Router# write memory

For Router 2:

- Console into the router and enable privileged EXEC mode.
  Router> enable
- Enter configuration mode.
  Router# config terminal
- Enable OSPF.
  Router (config)# router ospf 1
- Assign Router IDs.
  Router (config-router)# router-id 3.3.3.3
- Define OSPF Network Statements
  Router (config-router)# network 200.200.200.0 0.0.0.3 area 0
  Router (config-router)# network 200.200.203.0 0.0.0.3 area 0
- Exit configuration mode and return to privileged EXEC mode.
  Router (config-router)# end
- Save configuration
  Router# write memory

For Router 3:

- Console into the router and enable privileged EXEC mode.
  Router> enable
- Enter configuration mode.
  Router# config terminal
- Enable OSPF.
  Router (config)# router ospf 1
- Assign Router IDs.
  Router (config-router)# router-id 4.4.4.4
- Define OSPF Network Statements

Router (config-router)# network 200.200.201.0 0.0.0.3 area 0

Router (config-router)# network 200.200.202.0 0.0.0.3 area 0

- Exit configuration mode and return to privileged EXEC mode.

  Router (config-router)# end

- Save configuration

  Router# write memory

Verify OSPF Configuration:

Verify that OSPF is running and that neighbors have been discovered in every routers.

Router# show ip ospf neighbor

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
3.3.3.3           0   FULL/  -        00:00:38
200.200.200.2   Serial0/3/0
4.4.4.4           0   FULL/  -        00:00:38
200.200.201.2   Serial0/3/1
Router#
```

Figure 6.22: All connected routers with Router 0

```
Neighbor ID     Pri   State           Dead Time   Address
Interface
3.3.3.3           0   FULL/  -        00:00:38
200.200.203.2   Serial0/3/0
4.4.4.4           0   EXSTART/  -     00:00:37
200.200.202.1   Serial0/3/1
Router#
```

Figure 6.23: All connected routers with Router 1

```
Neighbor ID     Pri   State           Dead Time   Address
Interface
1.1.1.1           0   FULL/  -        00:00:34
200.200.200.1   Serial0/3/0
4.4.4.4           0   FULL/  -        00:00:34
200.200.203.1   Serial0/3/1
Router>
```

Figure 6.23: All connected routers with Router 2

```
Neighbor ID     Pri   State           Dead Time   Address
Interface
1.1.1.1           0   FULL/  -        00:00:33
200.200.201.1   Serial0/3/0
4.4.4.4           0   EXSTART/  -     00:00:30
200.200.202.2   Serial0/3/1
Router#
```

Figure 6.23: All connected routers with Router 2

Step 4: Check connectivity

- Transmit a packet form any network of Router 0 to Router 1 and vice versa, if the packet transmission and receive is successful that means the OSPF protocol is working and because of that packets can be sent to different routers.

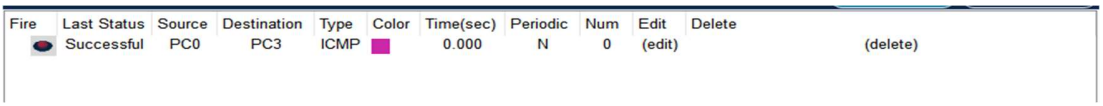


Figure 6.24: Packet transmission and received from PC0 to PC3 successful.

Observation and Result

Packet from one router's end device to another routers end device is successfully transmitted and received, meaning OSPF is working as routing protocol here.

Additional reading materials/ online tutorial/ References.