FACULTY OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Computer Networks Laboratory - ENCS4130

Experiment. 6 Report

DHCP, DNS, Email, and Web Server Configuration

Prepared by: Layan Salem 1221026

Instructor: Dr. Sameh Awad

T.A: Eng. Tariq Odeh

Section: 3

Date: 1-May-2025

Place: Computer Network Lab

1 Abstract

In this experiment, we set up and tested several important network services using Cisco Packet Tracer, including DHCP, DNS, Web, and Email servers. The goal was to understand how these services work together in a typical network and how to configure them correctly. By the end of the lab, we expected each service to function properly providing dynamic IP addresses, resolving domain names, hosting a webpage, and allowing email communication. Through hands-on setup and testing, we learned how to manage server configurations and observed how data flows across the network.

2 Table of Content

3 Table of Figures

4 Table of tables

5 Introduction

In today’s world, computer networks depend on a few key services to keep everything running smoothly. This experiment looks at how to set up four of the most important ones: DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), a web server, and an email server. These services help automate network configurations, translate website names into IP addresses, serve web pages, and handle email between users.

We used Cisco Packet Tracer, a popular network simulation tool to build and test a virtual network. With it, we were able to set up and troubleshoot each service in a realistic, hands-on way. The goal was to create a working network where devices automatically get IP addresses, users can visit internal websites, and send emails within the system.

Through this experiment, we aimed to:

- ❖ Understand how DHCP automatically assigns IP addresses and other settings.
- ❖ Learn how DNS links website names to the right IP addresses.
- ❖ Set up a web server that hosts a basic HTML page.
- ❖ Configure an email server so users can send and receive messages on the network.

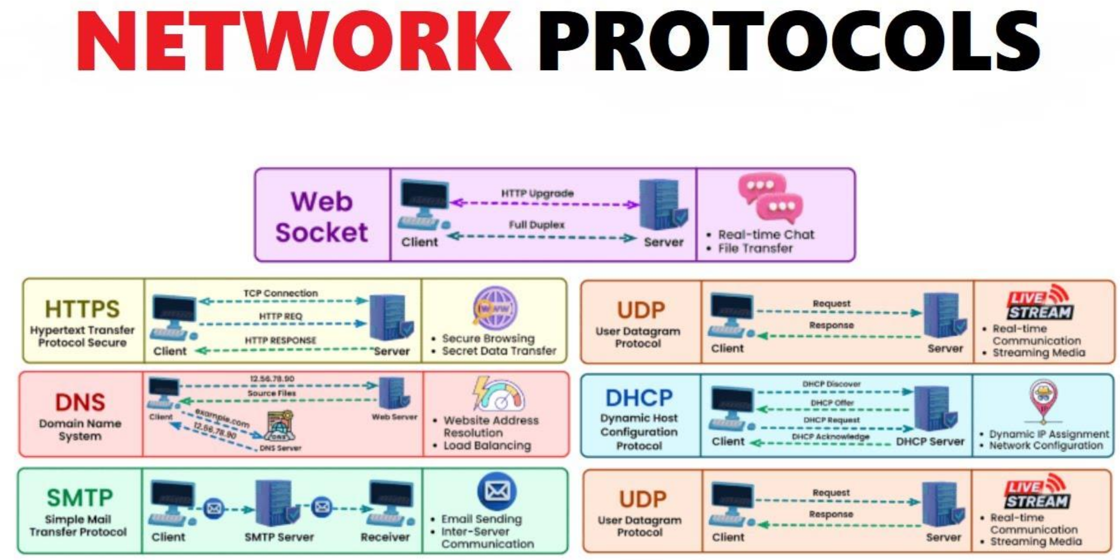


Figure 1 networks protocols [1]

5.1 Dynamic Host Configuration Protocol (DHCP)

is a system used to automatically assign IP addresses and other network settings (like DNS servers, subnet masks, and default gateways) to devices on a network. Instead of manually configuring each device, DHCP makes the process faster and easier, especially in larger networks with many devices.

5.1.1 How it works

When a device connects to the network, DHCP sends it the necessary configuration details so it can communicate with other devices and access the internet. This automation saves time and reduces errors compared to manual setup.

5.1.2 Key Components:

- DHCP Server: Assigns IP addresses and network settings from a pool of available options.
- *DHCP Client:* Any device (like a phone or computer) that connects to the network and receives info from the server.
- *DHCP Relay:* Helps pass messages between the server and clients, especially useful when the network is divided into multiple subnets. [2]

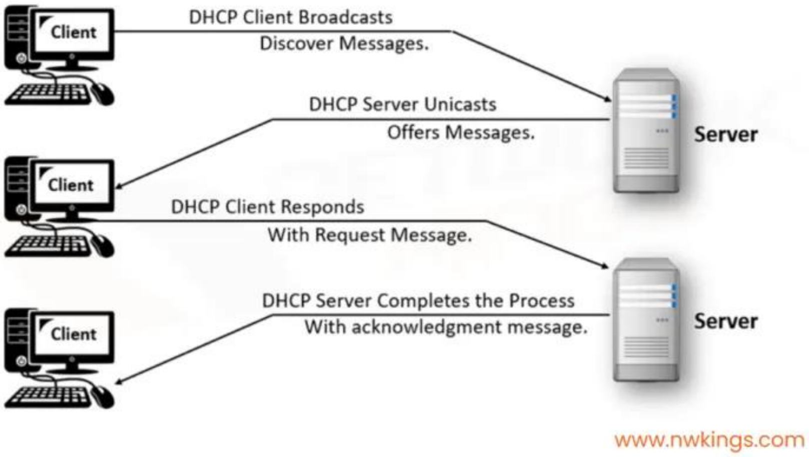


Figure 2 DHCP Client-Server Interaction [3]

5.2 Domain Name System (DNS)

The Domain Name System (DNS) works like the internet’s phonebook. Instead of remembering a bunch of IP addresses (like 192.168.1.1 or longer ones in IPv6), we use easy to remember names like google.com. DNS takes those domain names and translates them into the actual IP addresses computers need to find websites and other online resources.

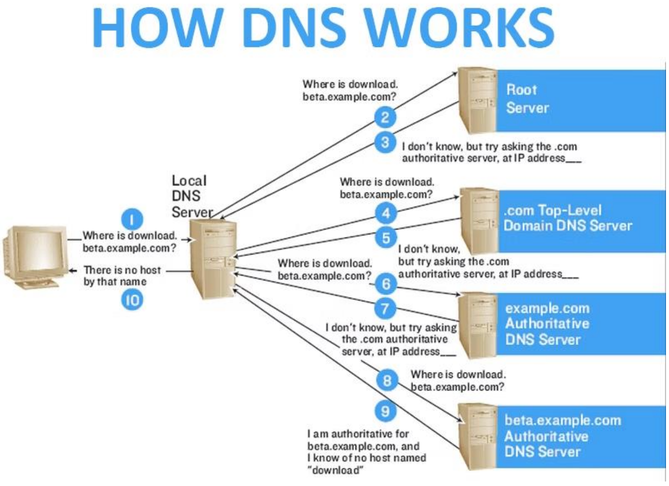

HOW DNS WORKS
Root Server
.com Top-Level Domain DNS Server
example.com Authoritative DNS Server
beta.example.com Authoritative DNS Server
Local DNS Server
1 Where is download. beta.example.com?
2 Where is download. beta.example.com?
3 I don't know, but try asking the .com authoritative server, at IP address___
4 Where is download. beta.example.com?
5 I don't know, but try asking the .com authoritative server, at IP address___
6 Where is download. beta.example.com?
7 I don't know, but try asking the .com authoritative server, at IP address___
8 Where is download. beta.example.com?
9 I am authoritative for beta.example.com, and I know of no host named "download"
10 There is no host by that name

Figure 3 DNS [5]

5.2.1 How does DNS work?

When a user enters a domain name into a web browser, a process known as DNS resolution is initiated. This process takes place behind the scenes and involves several steps to retrieve the correct IP address associated with the requested domain. The resolution process includes the participation of four main types of DNS servers:

- **DNS Recursor** → This server acts as an intermediary between the client (such as a browser) and the rest of the DNS hierarchy. It receives the query and begins the process of finding the correct IP address.
- **Root Nameserver** → The root server is the first step in directing the query. It does not contain the IP address itself but points to the correct Top-Level Domain (TLD) server (e.g., .com, .org).
- **TLD Nameserver** → This server manages the last part of the domain name (such as .com in example.com) and directs the query to the authoritative nameserver for the specific domain.
- **Authoritative Nameserver** The final destination in the query chain, this server holds the DNS records for the domain and responds with the correct IP address. Once received, the browser uses this IP to connect to the desired web server.

5.2.2 Recursive vs. Authoritative DNS Servers:

DNS servers play different roles in the resolution process:

- A **Recursive DNS** Resolver is the starting point of the DNS lookup. It accepts a client’s request and performs the necessary steps to find the final answer. This may involve multiple queries to different servers unless the requested information is already stored in its cache, which can speed up the process significantly.

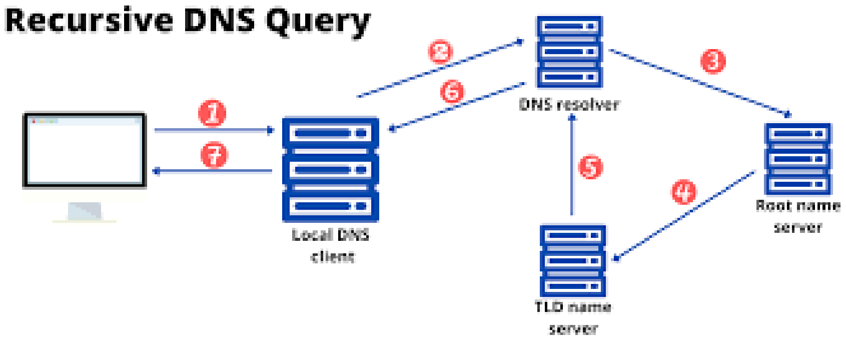


Figure 4 recursive DNS [6]

- An **Iterative DNS** Server does not provide the final answer but instead responds with a referral to another DNS server that is closer to the desired information. For example, a root DNS server may refer the recursive resolver to a TLD server, which may then refer it to an authoritative server. Iterative servers guide the recursive resolver through each step of the DNS resolution process until the final answer is found.

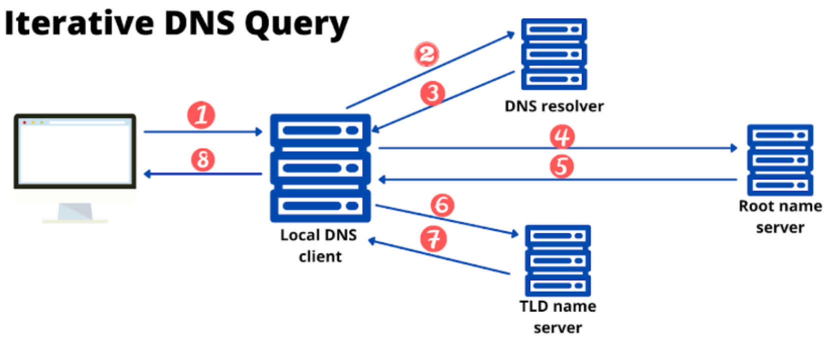


Figure 5: iterative DNS [6]

Overall, DNS plays a critical role in making the internet user-friendly and efficient by hiding the complexity of IP addressing behind simple, memorable domain names.[4]

5.3 Web server

A web server is a combination of hardware and software that stores, processes, and delivers web content like text, images, and videos to users over the internet. The hardware component is a computer that stores files and connects to the internet, while the software controls how these files are served to client devices.

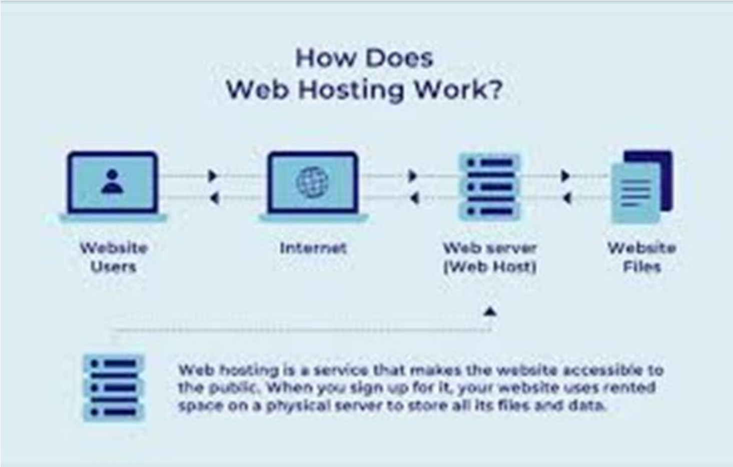

How Does
Web Hosting Work?
Website Users
Internet
Web server (Web Host)
Website Files
Web hosting is a service that makes the website accessible to the public. When you sign up for it, your website uses rented space on a physical server to store all its files and data.

Figure 6 web server

5.3.1 How It Works

When a user enters a URL in a browser, the browser uses DNS to find the server's IP address and establishes a TCP connection. Then, the browser sends an HTTP request for the desired webpage. The server processes this request and sends back an HTTP response containing the requested content, which the browser then displays.

5.3.2 Protocols and Error Handling

Web servers use HTTP/HTTPS for transferring content. Additional protocols like SMTP for email and FTP for file transfer may also be supported. If the requested content is unavailable, the server returns an error message (e.g., 404 Not Found).

5.4 Email Server

An email server is the backbone of email communication, ensuring that messages are properly sent, received, and managed across networks. Although this process happens in the background and is often invisible to users, it involves a structured sequence of operations carried out using specific communication protocols.

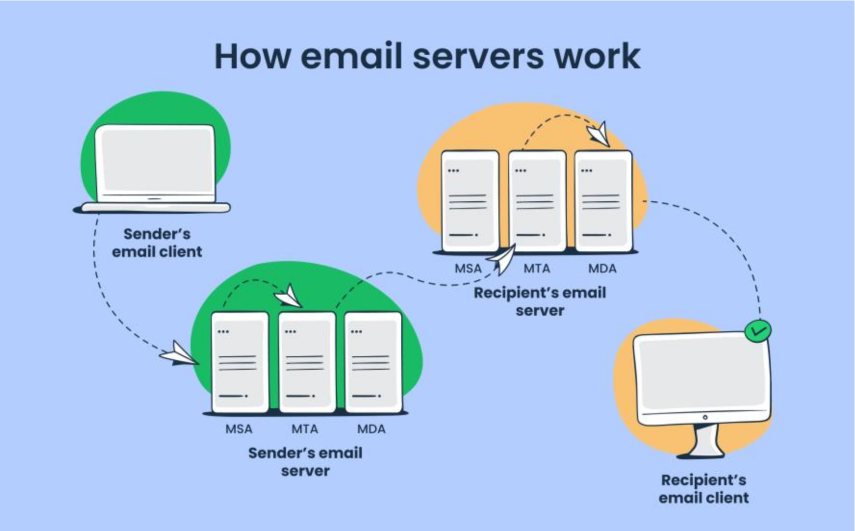


Figure 7: email server

The two main protocols involved are:

- **SMTP (Simple Mail Transfer Protocol):** This protocol handles outgoing emails. When a user sends an email, SMTP takes care of delivering the message from their device to their mail server and then forwards it to the recipient's server.

- **IMAP (Internet Message Access Protocol):** This protocol is responsible for retrieving incoming emails. It allows users to access their emails from multiple devices without needing to download them, keeping messages synchronized across platforms.

In some cases, POP3 (Post Office Protocol version 3) may be used instead of IMAP. POP3 downloads the message to a device and then deletes it from the server, offering a more secure but less flexible alternative.

To properly route emails between servers, the system relies on DNS (Domain Name System) and MX (Mail Exchange) records. These records help identify the correct server associated with a given domain name, ensuring messages are delivered to the right destination.

5.4.1 How the Email Process Works

1. When a user sends an email, the message is first handled by the SMTP server.
2. The SMTP server identifies the recipient's domain and uses DNS to find the correct IP address.
3. Once located, the message is forwarded to the recipient's server.
4. The recipient accesses their email via an IMAP server, which allows them to read, respond to, or delete the message as needed.

This entire process, while happening within seconds, relies on several components working together behind the scenes to ensure email communication is smooth, reliable, and secure.[7]

6 Procedure and Discussion

6.1 Topology

The topology after built in Cisco packet tracer, see fig 8.

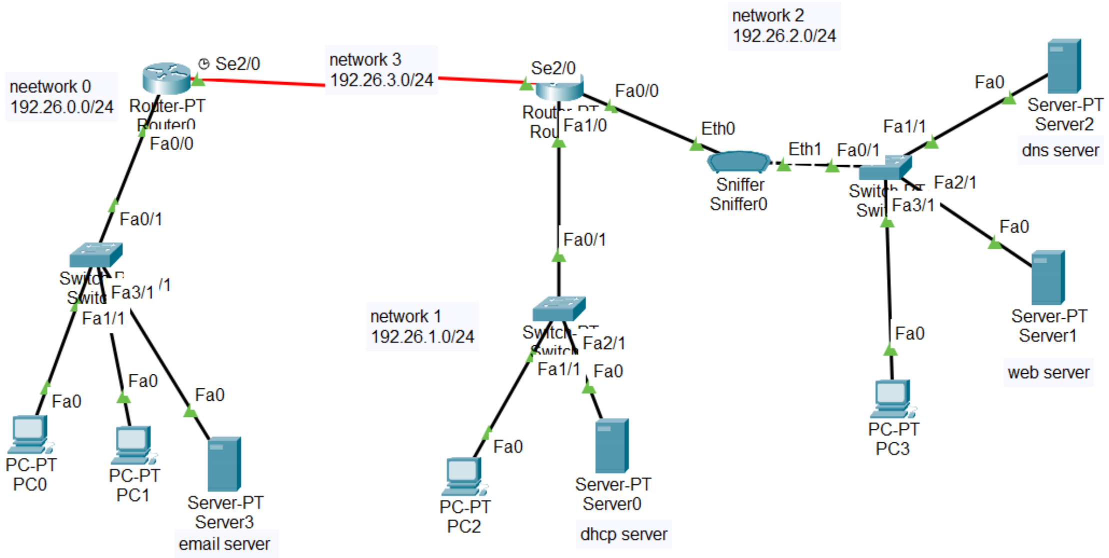
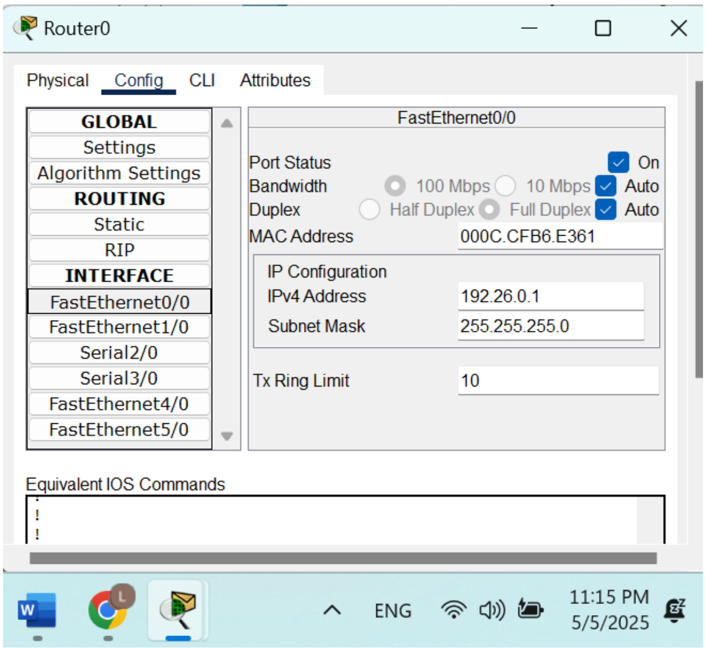


Figure 8 topology.

6.2 Network Setup and Configuration

6.2.1 Configuring Static IPs for Routers Interfaces

First, I assigned static IP addresses to the router interfaces as shown in Figure 9:



FastEthernet0/0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 000C.CFB6.E361

IP Configuration

IPv4 Address 192.26.0.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
!
!
```

Figure 9 static IP for router0

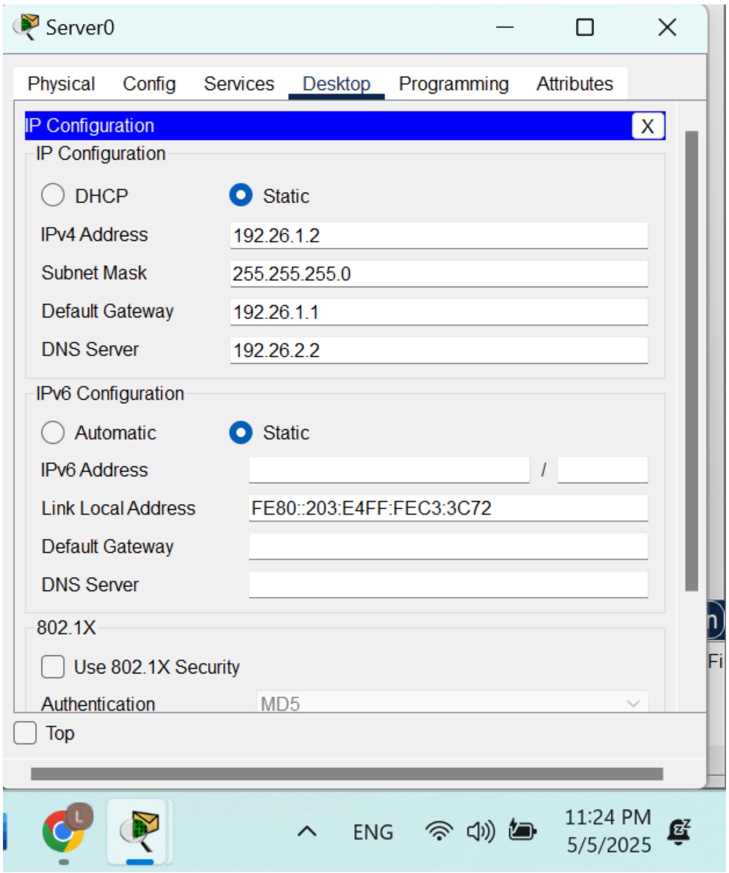
The table below summarizes each router interface along with its assigned IP address.

Table 1 routers Ips

Area	Network	Device	Interface	IP address	Subnet Mask	Wildcard Mask
Area 0	Network 0 192.26.0.0/24	Router 0	Fa0/0	192.26.0.1	255.255.255.0	0.0.0.255
Area 0	Network 1 192.26.1.0/24	Router 1	Fa0/1	192.26.1.1	255.255.255.0	0.0.0.255
Area 0	Network 2 192.26.2.0/24	Router 1	Fa0/0	192.26.2.1	255.255.255.0	0.0.0.255
Area 0	Network 3 192.26.3.0/24	Router 0	Se2/0	192.26.3.1	255.255.255.0	0.0.0.255
Area 0		Router 1	Se2/0	192.26.3.2	255.255.255.0	0.0.0.255

6.2.2 IP Configuration for the Servers

Figures 10 to 13 illustrate the IP configurations for the DNS, DHCP, web, and email servers. Each configuration includes the assigned static IP address, subnet mask, default gateway, and DNS settings.



Server0

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.26.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.26.1.1

DNS Server: 192.26.2.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::203:E4FF:FEC3:3C72

Default Gateway:

DNS Server:

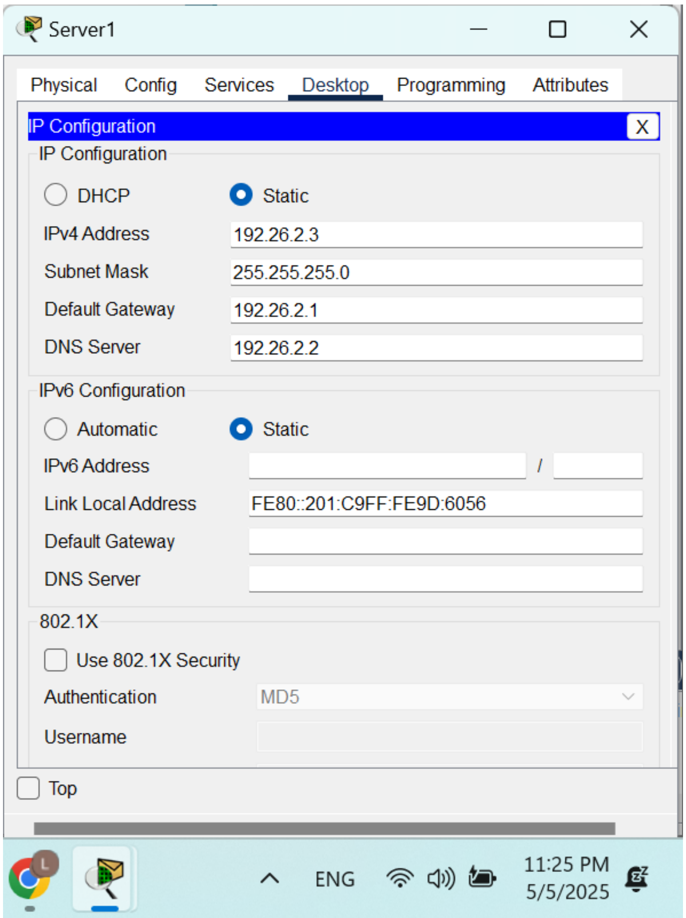
802.1X

□ Use 802.1X Security

Authentication: MD5

□ Top

Figure 10 IP configuration for dhcp server.



IP Configuration

○ DHCP ● Static

IPv4 Address 192.26.2.3

Subnet Mask 255.255.255.0

Default Gateway 192.26.2.1

DNS Server 192.26.2.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::201:C9FF:FE9D:6056

Default Gateway

DNS Server

802.1X

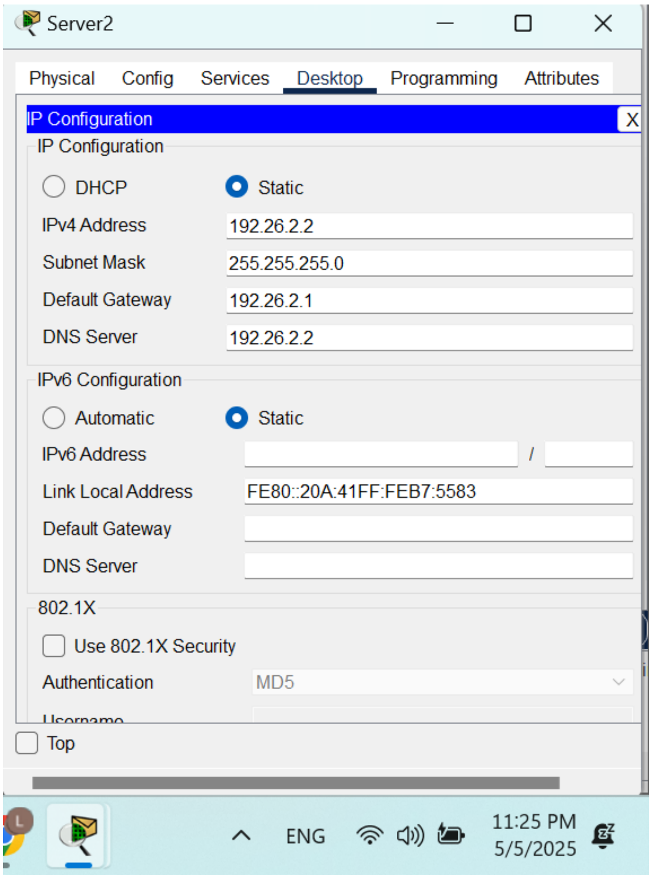
□ Use 802.1X Security

Authentication MD5

Username

□ Top

Figure 11 IP configuration for Web server.



IP Configuration

○ DHCP ● Static

IPv4 Address 192.26.2.2

Subnet Mask 255.255.255.0

Default Gateway 192.26.2.1

DNS Server 192.26.2.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::20A:41FF:FEB7:5583

Default Gateway

DNS Server

802.1X

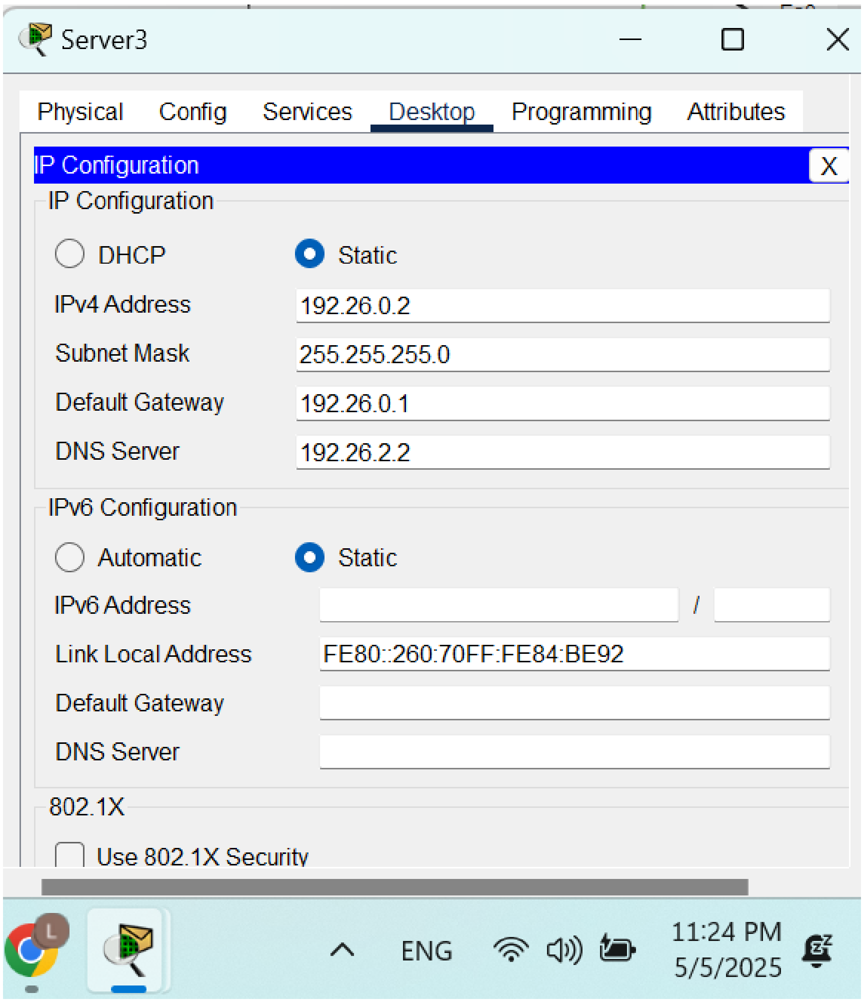
□ Use 802.1X Security

Authentication MD5

Username

□ Top

Figure 12 IP configuration for DNS server.



IP Configuration

○ DHCP ● Static

IPv4 Address 192.26.0.2

Subnet Mask 255.255.255.0

Default Gateway 192.26.0.1

DNS Server 192.26.2.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::260:70FF:FE84:BE92

Default Gateway

DNS Server

802.1X

□ Use 802.1X Security

Figure 13 IP configuration for email server.

6.2.3 Enabling OSPF Routing

OSPF routing was enabled on both Router0 and Router1. The configuration involved specifying the OSPF process and defining the networks to be advertised through OSPF on each router.

1. on Router0, i use the following commands:
    - router ospf 1
    - network 192.26.0.0 0.0.0.255 area 0
    - network 192.26.3.0 0.0.0.255 area 0

2. on Router1, i use the following commands:
    - router ospf 1
    - network 192.26.1.0 0.0.0.255 area 0
    - network 192.26.2.0 0.0.0.255 area 0
    - network 192.26.3.0 0.0.0.255 area 0

6.2.4 Configuring DHCP on a Router

DHCP was configured on Router1 to provide dynamic IP address assignment for two subnets: 192.26.1.0/24 (LAN1) and 192.26.2.0/24 (LAN0). Reserved IP address ranges were excluded from each subnet to prevent conflicts with statically assigned addresses. For the 192.26.1.0/24 network, the range 192.26.1.1 to 192.26.1.10 was excluded using the following command:

- ip dhcp excluded-address 192.26.1.1 192.26.1.10

A DHCP pool named LAN1 was then created with the corresponding network details:

- ip dhcp pool LAN1
- network 192.26.1.0 255.255.255.0
- default-router 192.26.1.1
- dns-server 192.26.2.2

Similarly, the address range 192.26.2.1 to 192.26.2.10 was excluded for the 192.26.2.0/24 subnet:

- ip dhcp excluded-address 192.26.2.1 192.26.2.10

A second DHCP pool, LAN0, was created with the following configuration:

- ip dhcp pool LAN0
- network 192.26.2.0 255.255.255.0
- default-router 192.26.2.1
- dns-server 192.26.2.2

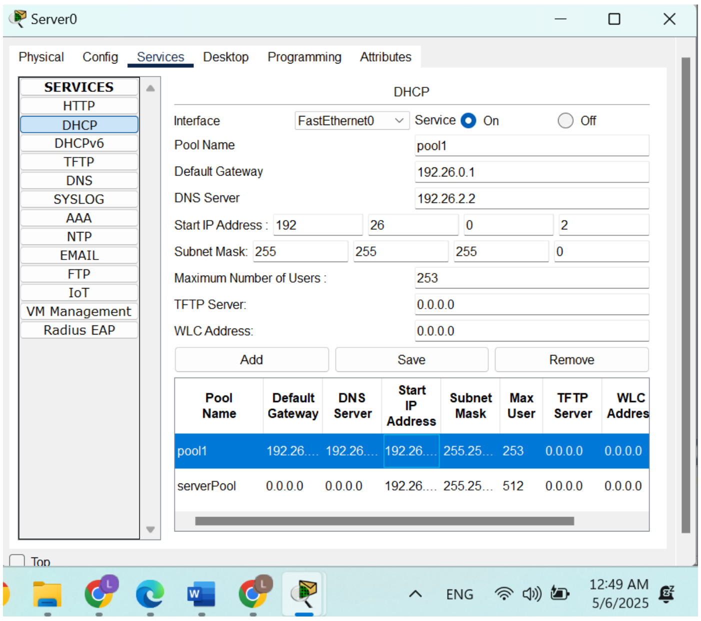
Finally, the DHCP service was enabled using:

- service dhcp

As a result, all DHCP-enabled devices in LAN1 and LAN0 automatically received their IP configuration from Router1, based on their respective subnet settings.

6.2.5 Configuring DHCP Server

Server0 was configured to act as a DHCP server for the 192.26.0.0/24 network, as shown in Figures 11 and 12. The configuration was done through the Services tab by enabling the DHCP service on the FastEthernet0 interface. A DHCP pool named Pool1 was created with the following:



Interface: FastEthernet0 Service ● On ○ Off

Pool Name: pool1

Default Gateway: 192.26.0.1

DNS Server: 192.26.2.2

Start IP Address : 192 26 0 2

Subnet Mask: 255 255 255 0

Maximum Number of Users : 253

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Addres
pool1	192.26....	192.26....	192.26....	255.25...	253	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.26....	255.25...	512	0.0.0.0	0.0.0.0

Figure 14 Assigning IP addresses dynamically using the DHCP server.

After adding and saving the configuration, DHCP clients within the 192.26.0.0/24 subnet such as connected PCs began receiving IP addresses dynamically from the server, along with the correct gateway and DNS settings. This setup ensures centralized IP address management and simplifies network administration for the subnet.

6.2.6 Configuring DHCP Relay on Router0

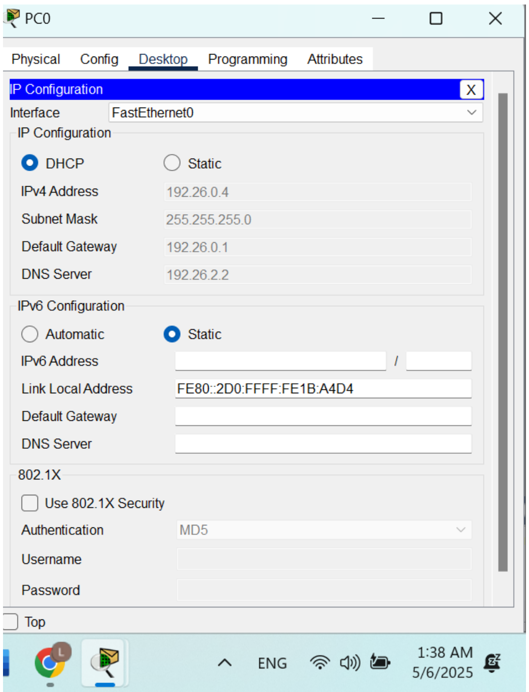
Since Server0, which functions as the DHCP server, is not directly connected to the 192.26.0.0/24 network, Router0 was configured to act as a DHCP relay. This allows DHCP broadcast requests from clients in the 192.26.0.0/24 subnet to be forwarded to the DHCP server. The configuration was applied on the FastEthernet0/0 interface (the gateway for this subnet) using the ip helper-address command, as shown below:

- interface FastEthernet0/0
- ip address 192.26.0.1 255.255.255.0
- ip helper-address 192.26.1.2

This setup enables DHCP clients on the 192.X.0.0/24 network to successfully receive IP configurations from Server0, even though the server resides on a different subnet.

6.2.7 Assigning Dynamic IP Addresses

To enable dynamic IP addressing, all PCs were configured to obtain their network settings via DHCP. This was done by accessing the IP Configuration settings under the Desktop tab on each PC and selecting the DHCP option.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.26.0.4

Subnet Mask: 255.255.255.0

Default Gateway: 192.26.0.1

DNS Server: 192.26.2.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2D0:FFFF:FE1B:A4D4

Default Gateway:

DNS Server:

802.1X

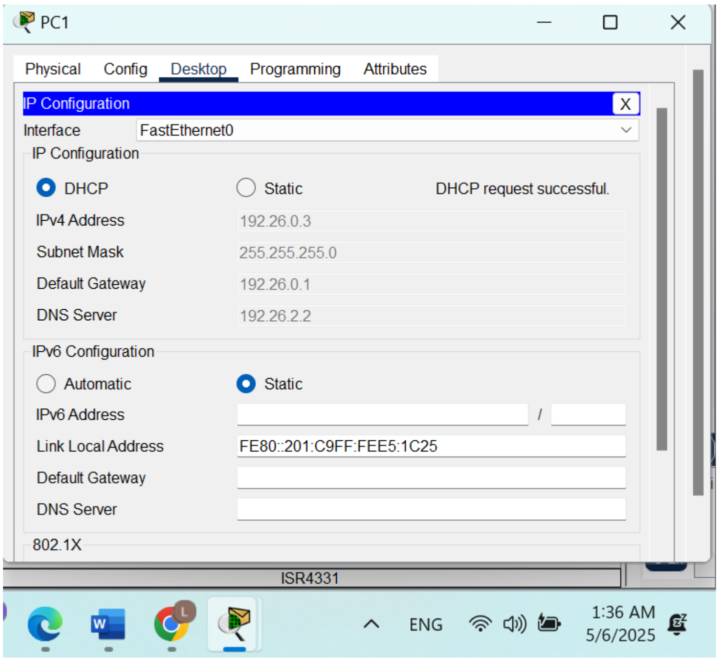
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Figure 15 IP configuration for PC0.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.26.0.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.26.0.1

DNS Server: 192.26.2.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

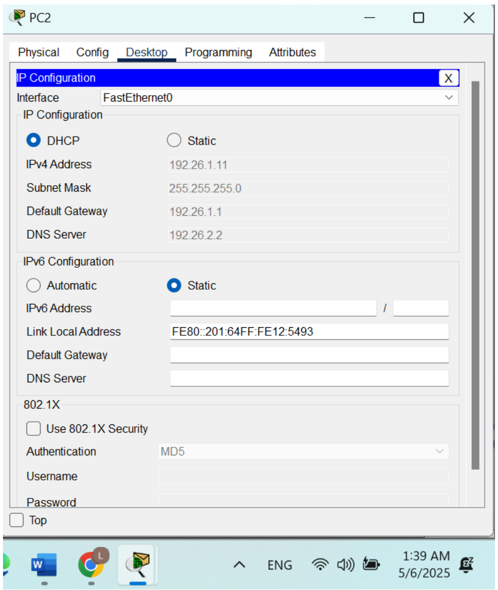
Link Local Address: FE80::201:C9FF:FEE5:1C25

Default Gateway:

DNS Server:

802.1X

Figure 16 IP configuration for PC1.



PC2

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.26.1.11

Subnet Mask: 255.255.255.0

Default Gateway: 192.26.1.1

DNS Server: 192.26.2.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:64FF:FE12:5493

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

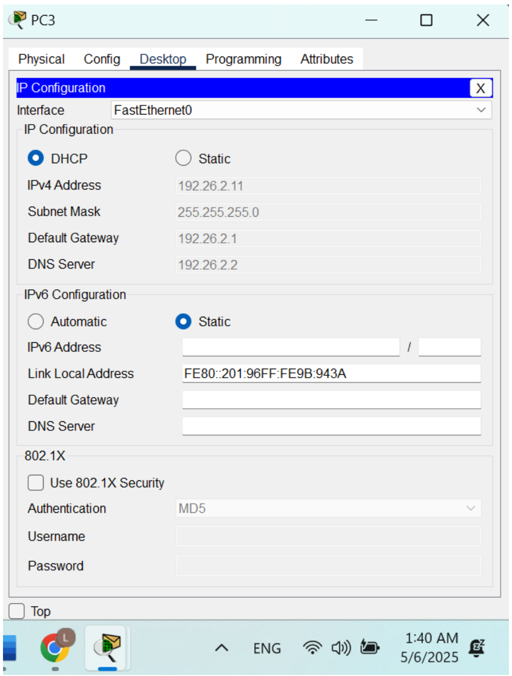
Username:

Password:

□ Top

ENG 1:39 AM 5/6/2025

Figure 17 IP configuration for PC2.



PC3

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.26.2.11

Subnet Mask: 255.255.255.0

Default Gateway: 192.26.2.1

DNS Server: 192.26.2.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:96FF:FE9B:943A

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top

ENG 1:40 AM 5/6/2025

Figure 18 IP configuration for PC3.

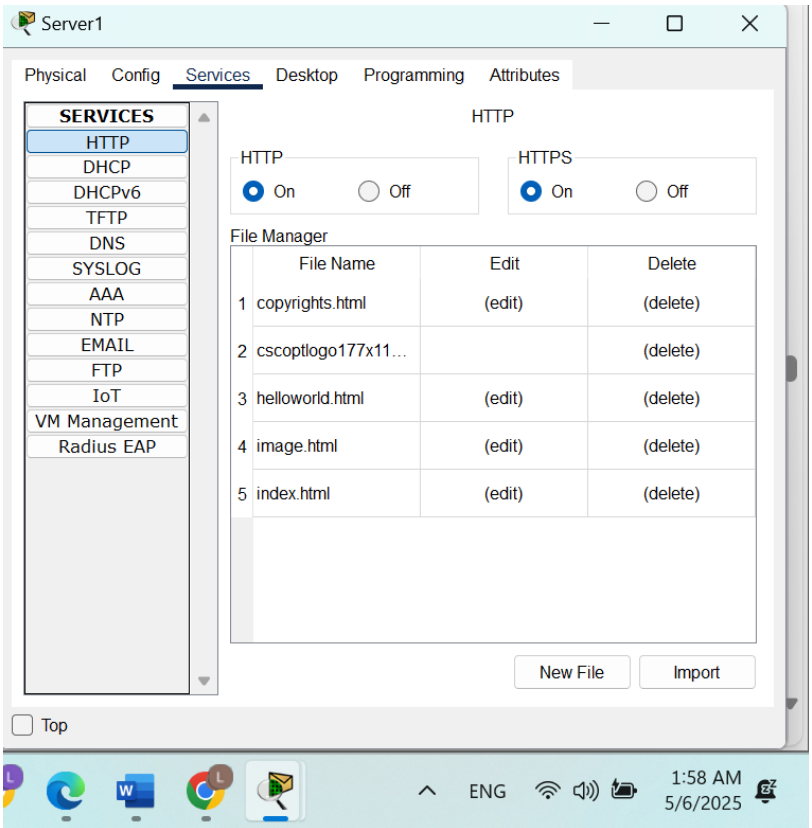
PC0 and PC1, which are part of the 192.26.0.0/24 network, successfully received their IP configurations including IP address, subnet mask, default gateway, and DNS server from the DHCP server (Server0), as illustrated in Figure 13 for PC0.

Similarly, PC2 and PC3, located in different subnets, obtained their IP settings from Router1's DHCP service. Figure 18 displays the DHCP-assigned configuration for PC3.

This verified that DHCP services were functioning correctly across the network, providing automated and accurate IP configuration to all client devices.

6.2.8 Configuring Web Server

Server1 was configured to function as a web server by enabling its HTTP service. This was done through the Services tab under the HTTP section, where the HTTP service was turned ON.



HTTP

HTTP: ● On ○ Off

HTTPS: ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x11...		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Figure 19 Enabling HTTP service.

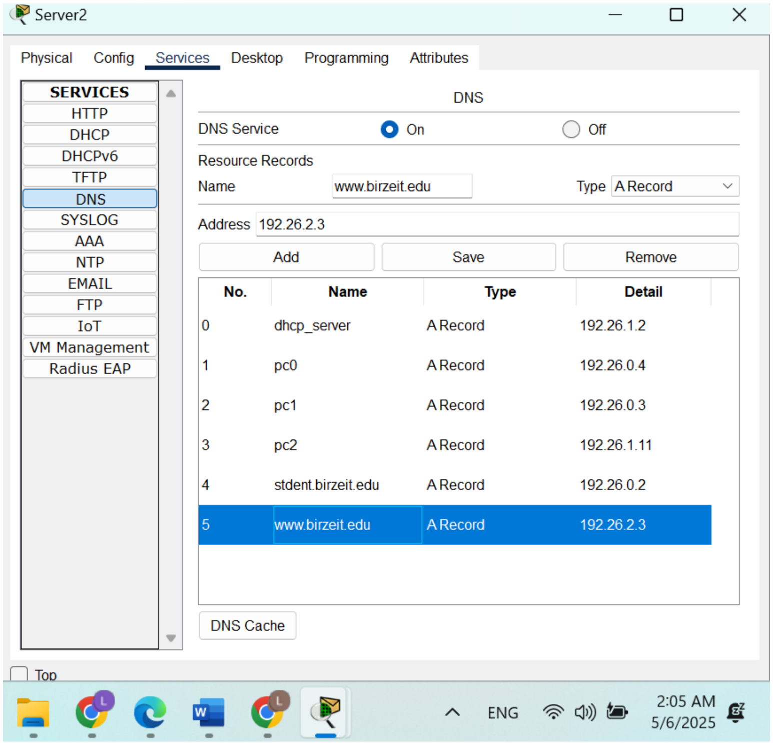
As a result, clients accessing Server1 via its IP address or through a configured domain. Figure 19 illustrates the HTTP service configuration on Server1.

6.2.9 Configuring DNS Server

Server2 was configured as the DNS server to enable domain name resolution within the network. This process began by accessing the Services tab on Server2, selecting the DNS service, and turning it ON.

Domain name entries were then added to the DNS table. Each entry included a domain name (e.g., www.birzeit.edu) and its corresponding IP address. These records were saved and stored with details such as record number, name, type, and address.

To enable name based communication across the network, DNS entries were added for all relevant devices including PCs and servers allowing them to be reached by their hostnames instead of IP addresses. This setup is shown in Figure 20 and ensures ease of access and improved network management.



DNS

DNS Service ● On ○ Off

Resource Records

Name www.birzeit.edu Type A Record

Address 192.26.2.3

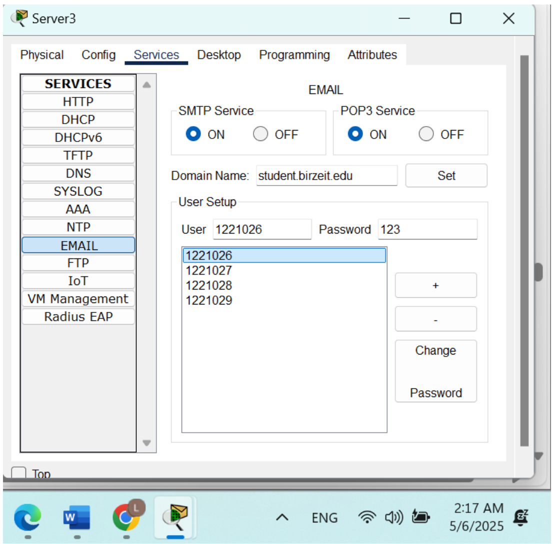
No.	Name	Type	Detail
0	dhcp_server	A Record	192.26.1.2
1	pc0	A Record	192.26.0.4
2	pc1	A Record	192.26.0.3
3	pc2	A Record	192.26.1.11
4	stdent.birzeit.edu	A Record	192.26.0.2
5	www.birzeit.edu	A Record	192.26.2.3

Figure 20 Adding records to all PCs to the DNS table.

6.2.10 Configuring Email Server

To enable internal email communication within the network, Server3 was configured as the Email Server, as demonstrated in Figures 21. The SMTP and POP3 services were activated by navigating to the Services tab, selecting the Email service, and turning both protocols ON.

The domain name for the email service was set to student.birzeit.edu, and user accounts were created for each PC in the network. Each account included a username and password, resulting in email addresses such as: 1221026@student.birzeit.edu.



EMAIL

SMTP Service ● ON ○ OFF

POP3 Service ● ON ○ OFF

Domain Name: student.birzeit.edu

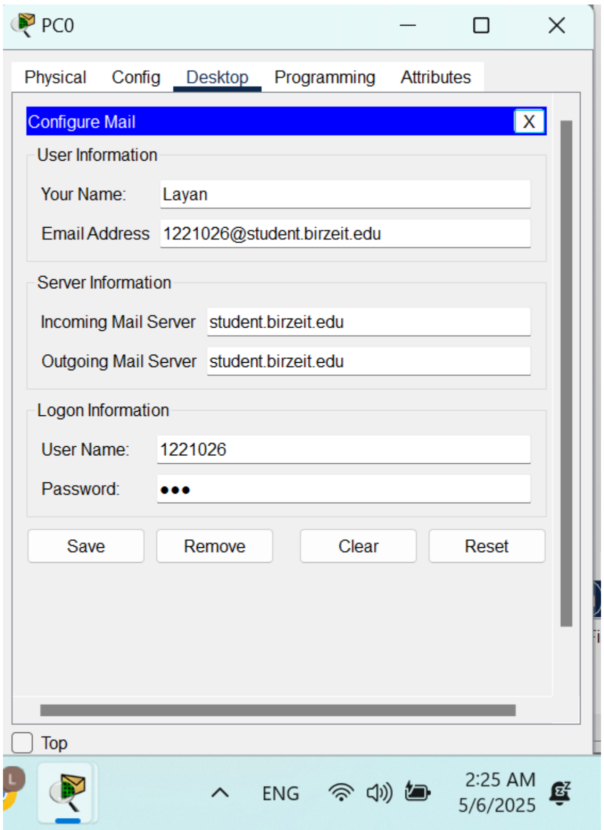
User Setup

User 1221026 Password 123

1221026
1221027
1221028
1221029

Figure 21 creating user account

Figures 22 and 23 illustrate the configuration process for PC0 and PC1. After configuring all clients, internal email exchange was tested. A message was sent from the user "Layan" (1221026@student.birzeit.edu) to "Sadeel" (1221027@student.birzeit.edu), as shown in Figures 24 and 25.



User Information

Your Name: Layan

Email Address 1221026@student.birzeit.edu

Server Information

Incoming Mail Server student.birzeit.edu

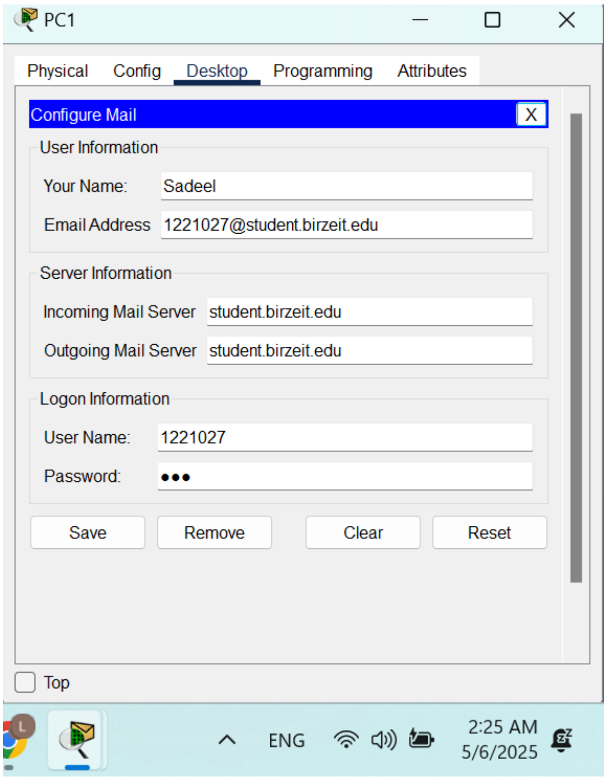
Outgoing Mail Server student.birzeit.edu

Logon Information

User Name: 1221026

Password: ●●●

Figure 22 Configuring Email Clients on PC0.



User Information

Your Name: Sadeel

Email Address 1221027@student.birzeit.edu

Server Information

Incoming Mail Server student.birzeit.edu

Outgoing Mail Server student.birzeit.edu

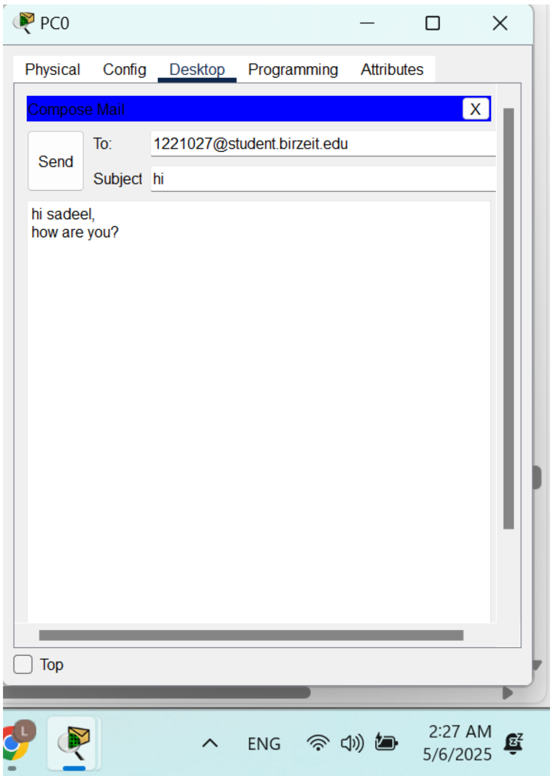
Logon Information

User Name: 1221027

Password: ●●●

Figure 23 Configuring Email Clients on PC1.

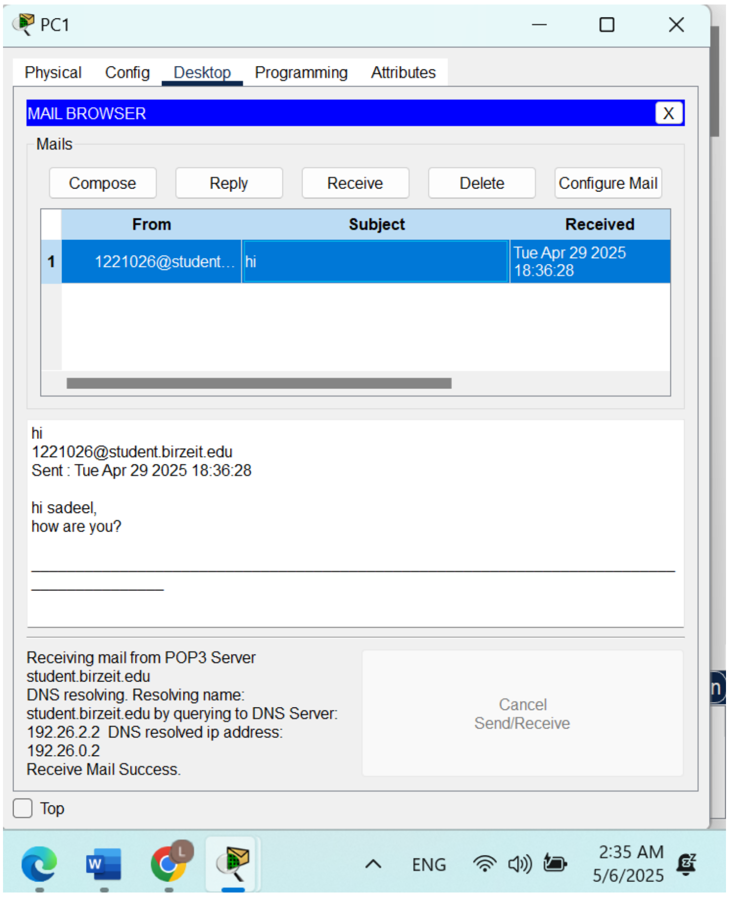
Sadeel received the email using the "Receive" function and successfully replied to it. Layan was then able to view the reply upon checking for new messages, as illustrated in Figures 24 through 26.



To: 1221027@student.birzeit.edu
Subject hi

hi sadeel,
how are you?

Figure 24 Sending an Email. From Layan to Sadeel



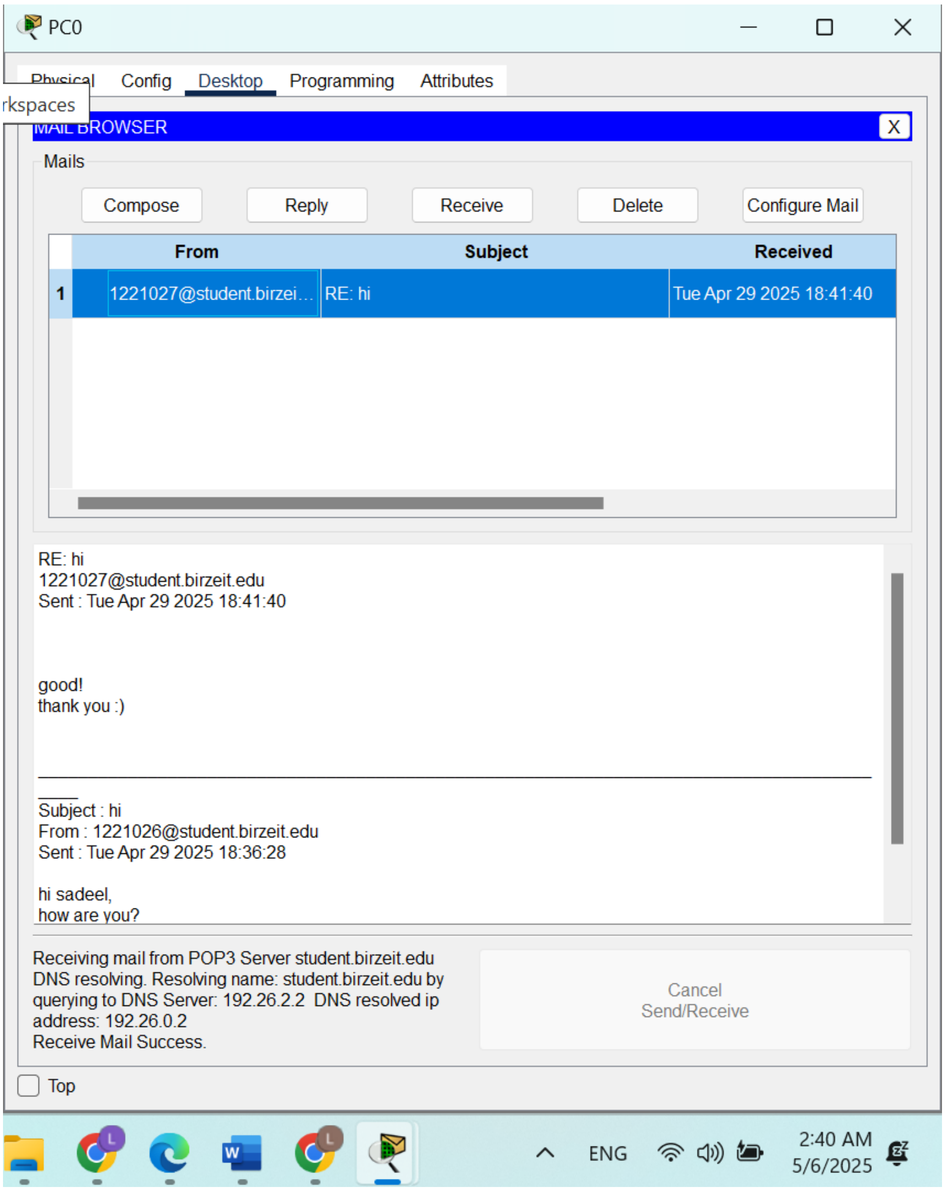
	From	Subject	Received
1	1221026@student...	hi	Tue Apr 29 2025 18:36:28

hi
1221026@student.birzeit.edu
Sent : Tue Apr 29 2025 18:36:28

hi sadeel,
how are you?

```
Receiving mail from POP3 Server
student.birzeit.edu
DNS resolving. Resolving name:
student.birzeit.edu by querying to DNS Server:
192.26.2.2  DNS resolved ip address:
192.26.0.2
Receive Mail Success.
```

Figure 25 Show received Emails.



	From	Subject	Received
1	1221027@student.birzei...	RE: hi	Tue Apr 29 2025 18:41:40

RE: hi
1221027@student.birzeit.edu
Sent : Tue Apr 29 2025 18:41:40

good!
thank you :)

Subject : hi
From : 1221026@student.birzeit.edu
Sent : Tue Apr 29 2025 18:36:28

hi sadeel,
how are you?

```
Receiving mail from POP3 Server student.birzeit.edu
DNS resolving. Resolving name: student.birzeit.edu by
querying to DNS Server: 192.26.2.2  DNS resolved ip
address: 192.26.0.2
Receive Mail Success.
```

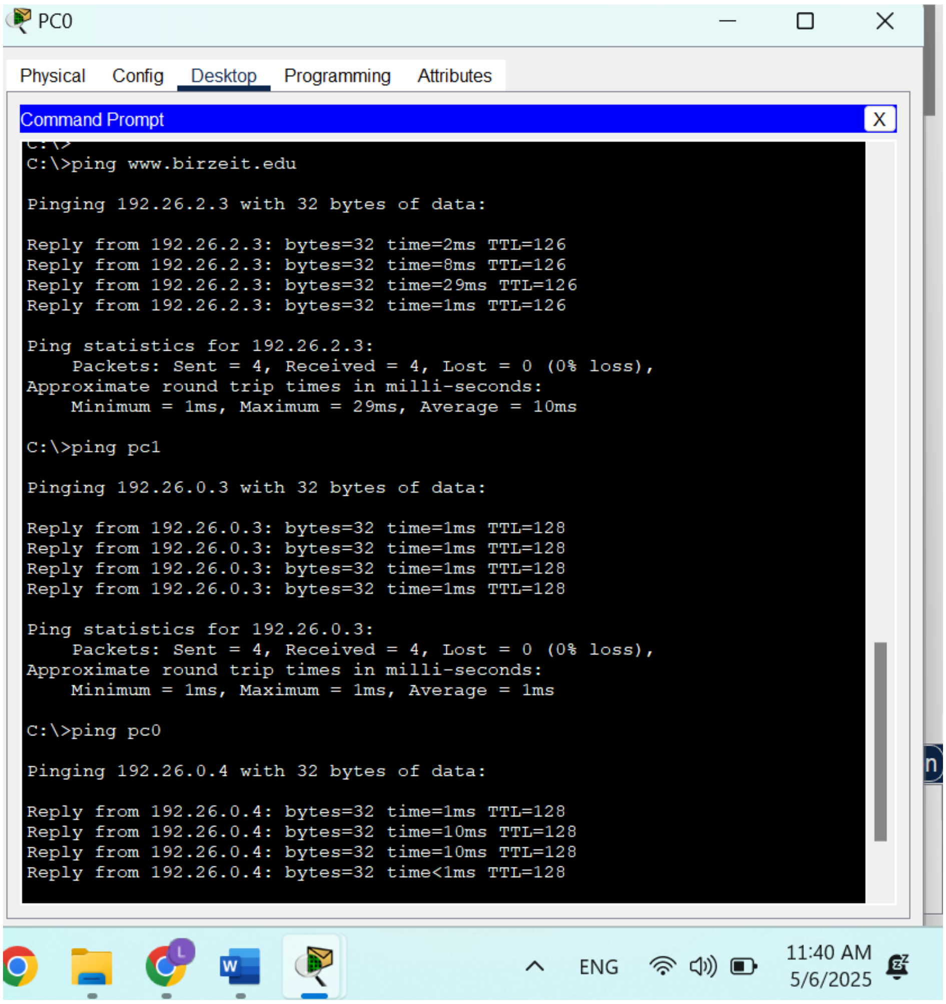
Figure 26 received Replying to Email

This verified the successful operation of the internal mail server, allowing bidirectional email communication between users in the network.

7 Testing and Verification

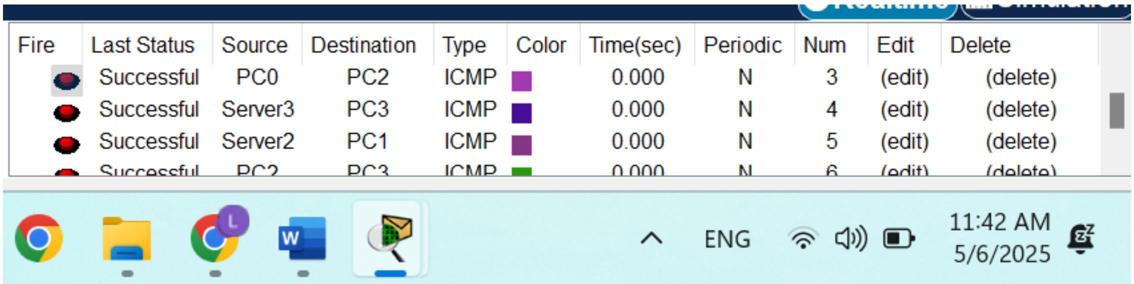
7.1 DNS Testing

To verify the functionality of the DNS server, the ping command was executed from multiple PCs using domain names instead of IP addresses. For example, the command ping www.birzeit.edu was used to check if the domain name correctly resolved to the IP address of the corresponding server. A successful resolution and response confirmed that the DNS server was functioning as expected. This process is illustrated in Figure 27.



```
C:\>
C:\>ping www.birzeit.edu

Pinging 192.26.2.3 with 32 bytes of data:

Reply from 192.26.2.3: bytes=32 time=2ms TTL=126
Reply from 192.26.2.3: bytes=32 time=8ms TTL=126
Reply from 192.26.2.3: bytes=32 time=29ms TTL=126
Reply from 192.26.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.26.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 29ms, Average = 10ms

C:\>ping pc1

Pinging 192.26.0.3 with 32 bytes of data:

Reply from 192.26.0.3: bytes=32 time=1ms TTL=128
Reply from 192.26.0.3: bytes=32 time=1ms TTL=128
Reply from 192.26.0.3: bytes=32 time=1ms TTL=128
Reply from 192.26.0.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.26.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping pc0

Pinging 192.26.0.4 with 32 bytes of data:

Reply from 192.26.0.4: bytes=32 time=1ms TTL=128
Reply from 192.26.0.4: bytes=32 time=10ms TTL=128
Reply from 192.26.0.4: bytes=32 time=10ms TTL=128
Reply from 192.26.0.4: bytes=32 time<1ms TTL=128
```

Figure 27 testing (ping)

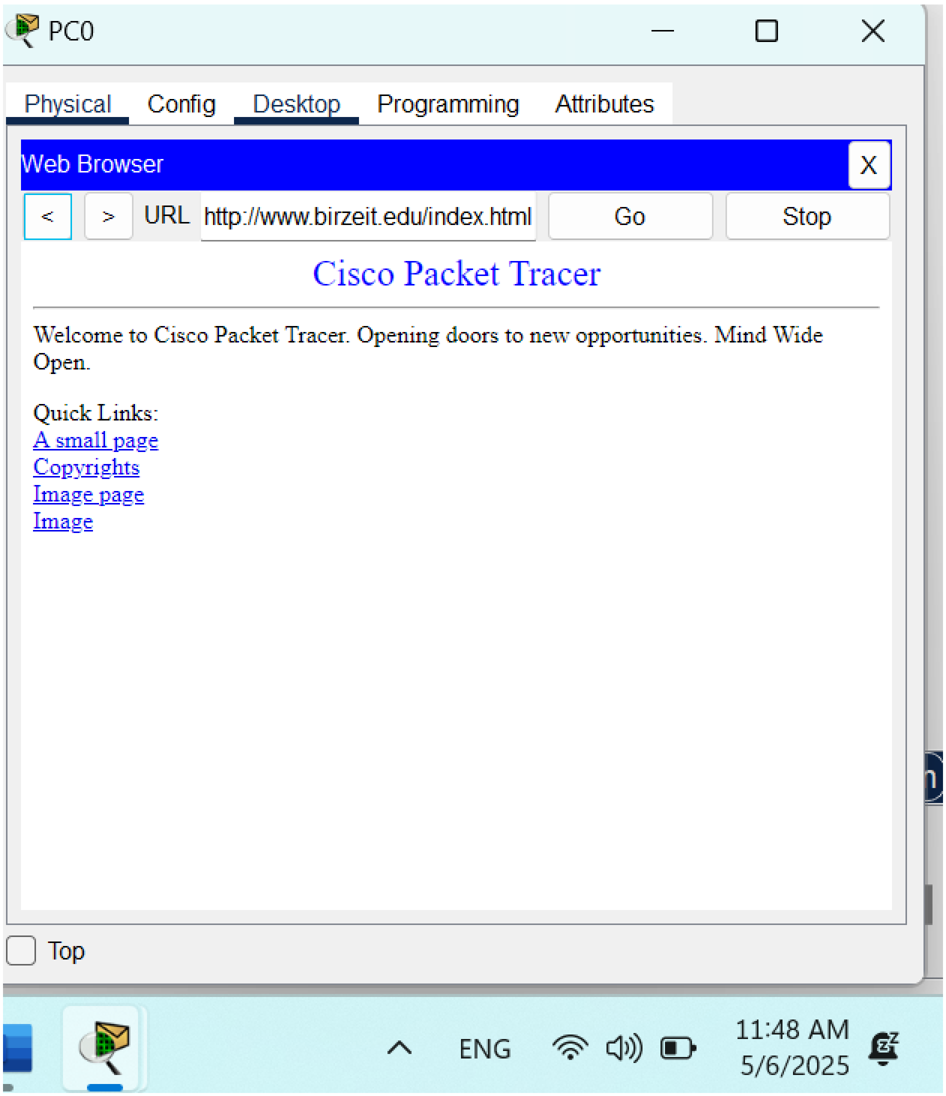


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC2	ICMP	🟪	0.000	N	3	(edit)	(delete)
●	Successful	Server3	PC3	ICMP	🟦	0.000	N	4	(edit)	(delete)
●	Successful	Server2	PC1	ICMP	🟪	0.000	N	5	(edit)	(delete)
●	Successful	PC2	PC3	ICMP	🟩	0.000	N	6	(edit)	(delete)

Figure 28 testing 2

7.2 Web Server Testing

The web server configuration was tested by accessing the hosted webpage from client PCs. This was done by opening a web browser and entering either the server’s IP address (e.g., http://192.26.2.3) or the domain name (e.g., http://www.birzeit.edu). The successful loading of the webpage confirmed that the HTTP service on Server1 was active and that DNS resolution (if the domain name was used) was functioning properly. Figure 29 demonstrates this testing.



URL http://www.birzeit.edu/index.html

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Figure 29 web server testing

8 Packet Sniffing

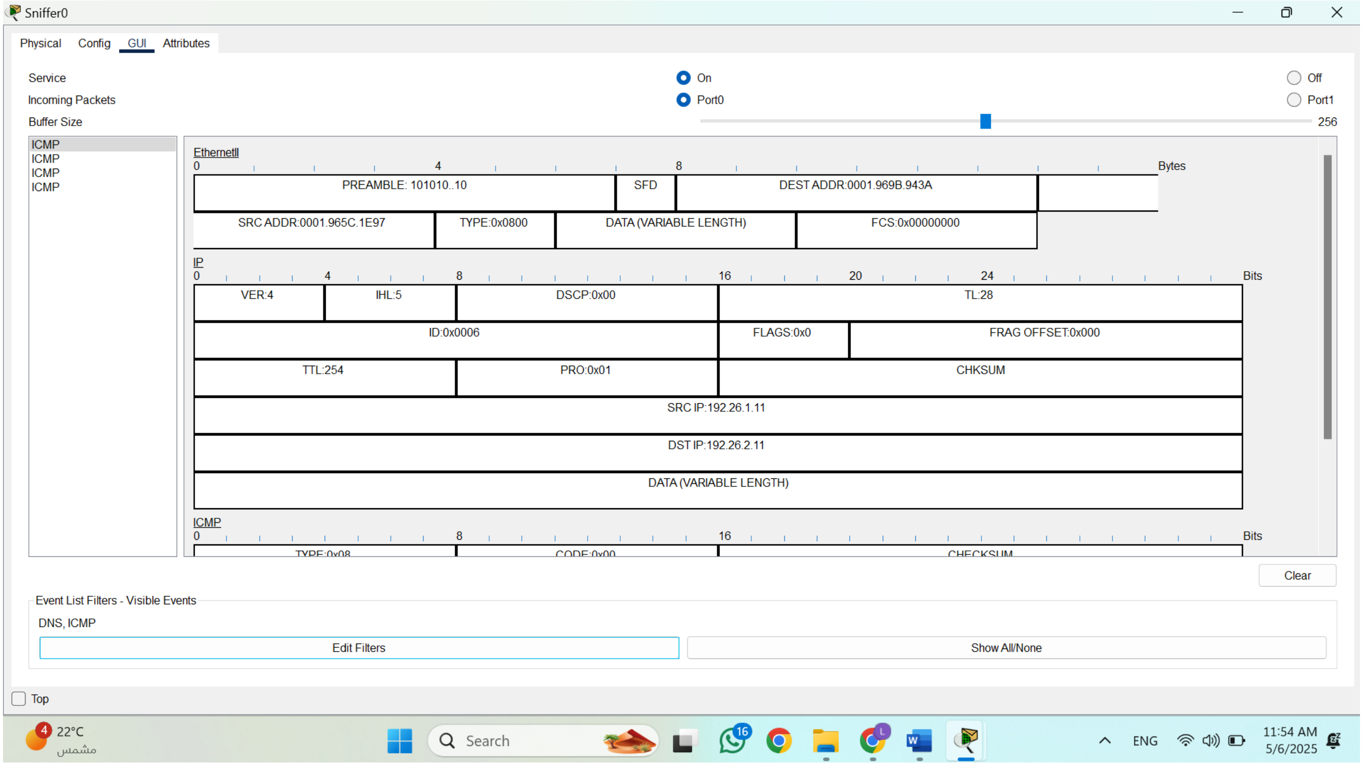
In this step, the Sniffer device was used to monitor and analyze network traffic to better understand data flow within the network. The sniffer tool was accessed by navigating to Sniffer → GUI → Service, and enabling packet capture by toggling the Check On option. Port 0 was selected to capture incoming packets on the designated interface.

By default, the sniffer captures all protocol types. To narrow the analysis to relevant traffic, filters were applied using the Edit Filters option, with only DNS and ICMP protocols enabled.

A test was conducted by performing a ping from PC1 to PC3 using the domain name pc3. This triggered a DNS query to resolve the domain name to an IP address, followed by ICMP packets for the actual ping operation.

- DNS packets captured during this process demonstrated the domain name resolution carried out by the DNS server.
- ICMP packets confirmed the successful connectivity between PC1 and PC3 after resolution.

Figures 30 illustrate the ping operation, filter application, and captured packet details for ICMP protocols. The analysis validated that ICMP services were functioning correctly within the configured network.


Sniffer0

Physical Config GUI Attributes

Service ● On ○ Off
Incoming Packets ● Port0 ○ Port1
Buffer Size 256

ICMP
ICMP
ICMP
ICMP

EthernetII (Bytes)
PREAMBLE: 101010..10 | SFD | DEST ADDR:0001.969B.943A
SRC ADDR:0001.965C.1E97 | TYPE:0x0800 | DATA (VARIABLE LENGTH) | FCS:0x00000000

IP (Bits)
VER:4 | IHL:5 | DSCP:0x00 | TL:28
ID:0x0006 | FLAGS:0x0 | FRAG OFFSET:0x000
TTL:254 | PRO:0x01 | CHKSUM
SRC IP:192.26.1.11
DST IP:192.26.2.11
DATA (VARIABLE LENGTH)

ICMP (Bits)
TYPE:0x08 | CODE:0x00 | CHECKSUM

Event List Filters - Visible Events
DNS, ICMP

Figure 30 Packet Details for ICMP Protocol.

9 Conclusion

This lab helped us gain practical experience with configuring core network services. We successfully set up the DHCP server to assign IP addresses automatically, configured DNS to resolve names to IP addresses, created a functioning web server, and set up email accounts for communication. We also used packet sniffing to observe how data moves through the network, especially DNS and ICMP packets during domain resolution and ping tests. Overall, the experiment gave us a clearer understanding of how different services support network functionality and how to troubleshoot and verify their operation.

10 Feedback

I found this experiment both helpful and engaging. It gave us the chance to apply what we’ve learned in class to real-world scenarios using Packet Tracer. Working through the configurations and tests helped reinforce key networking concepts. The steps were clear, and the time provided was enough to complete everything without feeling rushed. It was especially interesting to see how all the different servers worked together within the network. Overall, it was a great learning experience.

11 References

[1] **https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D7pBZg-E0Lyw&psig=AOvVaw2tmHilEI7rjHqMPLdJg_Kk&ust=1746304334228000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCOCsi9_QhY0DFQAAAAAdAAAAABAE** [Accessed on 1st May at 3:50 PM]]

[2] **https://www.fortinet.com/resources/cyberglossary/dynamic-host-configuration-protocol-dhcp#:~:text=Dynamic%20Host%20Configuration%20Protocol%20(DHCP)%20is%20used%20to%20dynamically%20assign,enables%20access%20to%20a%20network.** [Accessed on 1st May at 4:30 PM]]

[3] **https://www.nwkings.com/dora-process-in-dhcp** [Accessed on 1st May at 6:00 PM]]

[4] **https://www.cloudflare.com/learning/dns/what-is-dns/** [Accessed on 2nd May at 2:10 PM]]

[5] **https://www.hackers-arise.com/post/2019/05/20/network-basics-for-hackers-domain-name-service-dns-and-bind-theory-vulnerabilities-and-im** [Accessed on 2nd May at 2:50 PM]]

[6] https://threat.media/definition/what-is-an-iterative-dns-query/ [Accessed on 2nd May at 3:25 PM]]

[7] **https://www.one.com/en/email/what-is-an-email-server#:~:text=An%20email%20server%20is%20a,information%20across%20to%20one%20another.** [Accessed on 2nd May at 4:05 PM]]