Federal State Autonomous Educational Institution of Higher Education

"NATIONAL RESEARCH UNIVERSITY

HIGHER SCHOOL OF ECONOMICS

Tikhonov Moscow Institute of Electronics and Mathematics

Department of Electronic Engineering

Report / Laboratory No: 11.5.5, 2.5.5, 2.7.6, 4.6.5, 4.6.6

on the course "Protection of Computer Networks and Systems"

MS Information Security & Artificial Intelligence Technologies

Performed by: Khanzada Mubashir Hassan

Teacher:

Ilyukhin R.V

Senior Venerable. Ilyukhin R.V.

Moscow, 2025

Contents

Task 11.5.5 - Subnet an IPv4 Network

Introduction

This lab focuses on subnetting the IPv4 network 192.168.0.0/24 into smaller networks that meet client requirements. The goal was to create two LANs with at least 50 and 40 hosts each, plus two additional subnets for future expansion. Tasks included subnet design, device configuration, and connectivity verification.

Addressing Table

Table 1

Device	Interface	IP Address	Subnet Mask	Default Gateway
CustomerRouter	G0/0	**192.168.0.1**	**255.255.255.192**	N/A
	G0/1	**192.168.0.65**	**255.255.255.192**	
	S0/1/0	209.165.201.2	255.255.255.252	
LAN-A Switch	VLAN1	**192.168.0.2**	**255.255.255.192**	**192.168.0.1**
LAN-B Switch	VLAN1	**192.168.0.66**	**255.255.255.192**	**192.168.0.65**
PC-A	NOTHING	**192.168.0.62**	**255.255.255.192**	**192.168.0.1**
PC-B	NOTHING	**192.168.0.126**	**255.255.255.192**	**192.168.0.65**
ISPRouter	G0/0	209.165.200.225	255.255.255.224	N/A
	S0/1/0	209.165.201.1	255.255.255.252	
ISPSwitch	VLAN1	209.165.200.226	255.255.255.224	209.165.200.225
ISP Workstation	NOTHING	209.165.200.235	255.255.255.224	209.165.200.225
ISP Server	NOTHING	209.165.200.240	255.255.255.224	209.165.200.225

3. Subnet Design Summary

To meet the customer’s requirements, the base network 192.168.0.0/24 must be divided into multiple subnets. Requirements:

- LAN-A: minimum **50 hosts**

- LAN-B: minimum **40 hosts**
- **2 additional subnets** reserved for future expansion
- A **single subnet mask** for all subnets (no VLSM)

Subnetting Analysis

Table 2

Question	**Answer**
Largest subnet requires how many hosts?	50
Minimum number of subnets required?	4
Original mask in binary (/24)	11111111.11111111.11111111.00000000
“1” bits represent	Network portion
“0” bits represent	Host portion

To create at least 4 subnets, we borrow **2 bits** from the host portion of /24, resulting in a **/26 mask** (255.255.255.192).

Prefix	**Decimal Mask**	**Subnets**	**Hosts per Subnet**
/25	255.255.255.128	2	126
/26	**255.255.255.192**	**4**	**62**
/27	255.255.255.224	8	30
/28	255.255.255.240	16	14

Chosen mask: /26 — gives **4 subnets** and **62 usable hosts** per subnet (enough for all requirements).

Derived Subnets

Subnet	Prefix	Subnet Mask
192.168.0.0	/26	255.255.255.192
192.168.0.64	/26	255.255.255.192
192.168.0.128	/26	255.255.255.192
192.168.0.192	/26	255.255.255.192

- **LAN-A:** Uses the first subnet (192.168.0.0/26)
- **LAN-B:** Uses the second subnet (192.168.0.64/26)
- Remaining subnets reserved for future networks.

4. Device Configuration Overview

Router Configuration

- Hostname: CustomerRouter
- Enable secret: Class123
- Console password: Cisco123
- Configured interfaces G0/0 and G0/1 with respective IP addresses and subnet masks.
- Saved configuration to NVRAM.

Switch Configuration

- Assigned management IP addresses on VLAN1.
- Configured default gateways to communicate with the router.

PC Configuration

- Manually configured IP addresses, subnet masks, and gateways according to the Addressing Table.

5. Network Testing and Verification

Connectivity tests were conducted using the ping command:

Table 3

Test	**Result**
PC-A ↔ Default Gateway	Successful
PC-B ↔ Default Gateway	Successful
PC-A ↔ PC-B	Successful

All devices communicated successfully, confirming correct subnetting and configuration.

6. Conclusion

This activity demonstrated IPv4 subnetting and device configuration in Packet Tracer. Using a /26 subnet mask effectively divided the 192.168.0.0/24 network into four functional subnets supporting up to 62 hosts each. Proper configuration and testing verified full connectivity across LANs. The exercise reinforced key concepts of subnetting, addressing, and network design.

Task 2.5.5 – Configure Initial Switch Settings

1. Introduction

This activity focuses on performing initial switch configuration in Cisco Packet Tracer. It includes verifying the default switch setup, securing access using passwords, configuring a Message of the Day (MOTD) banner, encrypting passwords, and saving configurations to NVRAM. These are essential tasks for protecting switch access and ensuring persistence of settings after reboot.

2. Objectives

- **Part 1:** Verify the Default Switch Configuration
- **Part 2:** Configure Basic Switch Settings
- **Part 3:** Configure a MOTD Banner
- **Part 4:** Save Configuration Files to NVRAM
- **Part 5:** Configure a Second Switch (S2)

3. Background

Network switches must be properly configured before deployment to ensure secure and efficient operation. This lab demonstrates:

- Access control through console and enable passwords.
- Use of the enable secret command for encrypted privileged access.
- Implementation of warning banners to deter unauthorized access.
- Saving configurations permanently to NVRAM.

4. Part 1 – Verify Default Configuration

Commands and Results

Table 4

Command	Output / Observation
show running-config	Displays current switch configuration.
FastEthernet Interfaces	24
Gigabit Ethernet Interfaces	2
VTY Line Range	0–15

Command to view NVRAM	show startup-config
Why “startup-config is not present”?	The configuration has not yet been saved to NVRAM; it exists only in RAM.

Purpose:
Understanding the switch’s default setup before making changes ensures configurations are applied intentionally and correctly.

5. Part 2 – Basic Switch Configuration

Step 1: Assign a Hostname

Switch# configure terminal

Switch(config)# hostname S1

Step 2: Secure Console Access

S1(config)# line console 0

S1(config-line)# password letmein

S1(config-line)# login

Why is the login command required?
It enables password verification on the console port.

Step 3: Secure Privileged Mode Access

S1(config)# enable password c1$c0

S1(config)# enable secret itsasecret

- enable password → plain text
- enable secret → encrypted (preferred)

Why use enable secret?
It stores the password in encrypted form, preventing visibility to unauthorized users.

Step 4: Encrypt All Passwords

S1(config)# service password-encryption

Effect:
All existing and future passwords are stored in encrypted form within the configuration.

6. Part 3 – Configure a MOTD Banner

S1(config)# banner motd "This is a secure system. Authorized Access Only!"

Table 5

Question	Answer
When is the banner displayed?	When anyone logs into the switch.
Why configure a banner?	To warn unauthorized users and provide messages for network administrators.

7. Part 4 – Save Configuration Files to NVRAM

Verification and Saving:

S1# show run

S1# copy running-config startup-config

Table 6

Question	Answer
Command to view saved configuration	show startup-config
Are changes saved?	Yes, they match the running configuration.

Purpose:
Ensures the configuration is retained after power loss or reboot.

8. Part 5 – Configure Switch S2

Repeat the process for S2 using the following settings:

Table 7

Parameter	Configuration
Hostname	S2
Console Password	letmein
Enable Password	c1$c0
Enable Secret	itsasecret
MOTD Banner	“Authorized access only. Unauthorized access is prohibited and violators will be prosecuted.”
Encryption	service password-encryption
Save Configuration	copy running-config startup-config

Example Command Summary:

enable

configure terminal

hostname S2

line console 0

password letmein

Login

enable password c1$c0

enable secret itsasecret

service password-encryption

banner motd #Authorized access only. Unauthorized access is prohibited. #

end

copy running-config startup-config

9. Conclusion

In this lab, the initial switch configurations were successfully implemented. Both switches (S1 and S2) were assigned hostnames, secured with console and enable passwords, and configured with encrypted secrets. MOTD banners were applied to display security warnings to users. Finally, configurations were saved to NVRAM to ensure persistence.

This activity reinforced essential security practices for Cisco switch management, highlighting the importance of password protection, encryption, and documentation in real-world network administration.

Task 2.7.6 - Implement Basic Connectivity

Introduction

In this activity, you will first create a basic switch configuration. Then, you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use various **show** commands to verify the configuration and use the **ping** command to verify basic connectivity between devices.

Instructions

Part 1: Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

Step 1: Configure S1 with a hostname.

a. Click S1 and then click the CLI tab.

b. Enter the correct command to configure the hostname as S1.

Step 2: Configure the console and encrypted privileged EXEC mode passwords.

a. Use **cisco** for the console password.

b. Use **class** for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

Question:

How can you verify that both passwords were configured correctly?

Answer: Upon exiting user EXEC mode, the switch requires password authentication for console access and will request credentials again when entering privileged EXEC mode. Additionally, the show running-config command can be utilized to display the configured passwords in the system.

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Step 4: Save the configuration file to NVRAM.

Question:

Which command do you issue to accomplish this step?

Step 5: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

Step 1: Configure both PCs with IP addresses.

a. Click PC1 and then click the Desktop tab.

b. Click IP Configuration. In the Addressing Table above, you can see that the IP address for PC1 is 192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the IP Configuration window.

c. Repeat steps 1a and 1b for PC2.

Step 2: Test connectivity to switches.

a. Click PC1. Close the IP Configuration window if it is still open. In the Desktop tab, click Command Prompt.

b. Type the **ping** command and the IP address for S1 and press Enter.

Packet Tracer PC Command Line 1.0

PC> **ping 192.168.1.253**

Question:

Were you successful? Explain.

Answer: The ping failed because the IP address had not yet been assigned to the switch's management interface

Part 3: Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 1: Configure S1 with an IP address.

Switches can be used as plug-and-play devices. This means that they do not need to be configured for them to work. Switches forward information from one port to another based on MAC addresses.

Question:

If this is the case, why would we configure it with an IP address?

Answer: To enable remote management, a switch requires an IP address assigned to its management interface, which by default is VLAN 1.

Use the following commands to configure S1 with an IP address.

S1# **configure terminal**

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

S1(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.253 255.255.255.0**

S1(config-if)# **no shutdown**

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#

S1(config-if)# **exit**

S1#

Question:

Why do you enter the **no shutdown** command?

Answer: The **no shutdown** command administratively places the interface in an active state.

Step 2: Configure S2 with an IP address.

Use the information in the Addressing Table to configure S2 with an IP address.

Step 3: Verify the IP address configuration on S1 and S2.

Use the **show ip interface brief** command to display the IP address and status of all the switch ports and interfaces. You can also use the **show running-config** command.

Step 4: Save configurations for S1 and S2 to NVRAM.

Question: Which command is used to save the configuration file in RAM to NVRAM?

Answer: copy running-config startup-config

Step 5: Verify network connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1 and S2 from PC1 and PC2.

a. Click PC1 and then click the Desktop tab.

b. Click Command Prompt.

c. Ping the IP address for PC2.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

Note: You can also use the **ping** command on the switch CLI and on PC2.

All pings should be successful. If your first ping result is 80%, try again. It should now be 100%. You will learn why a ping may sometimes fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

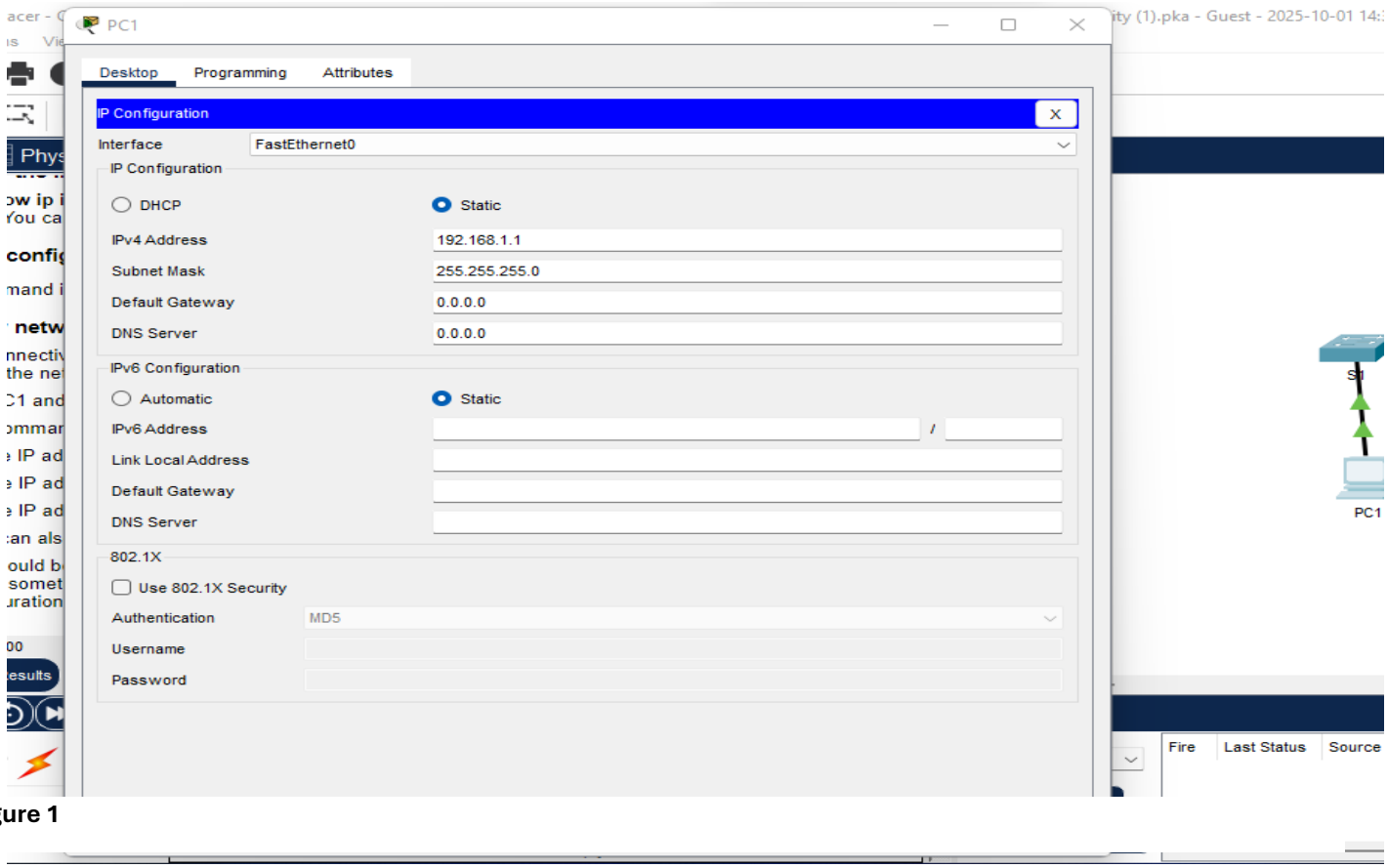

Figure 1

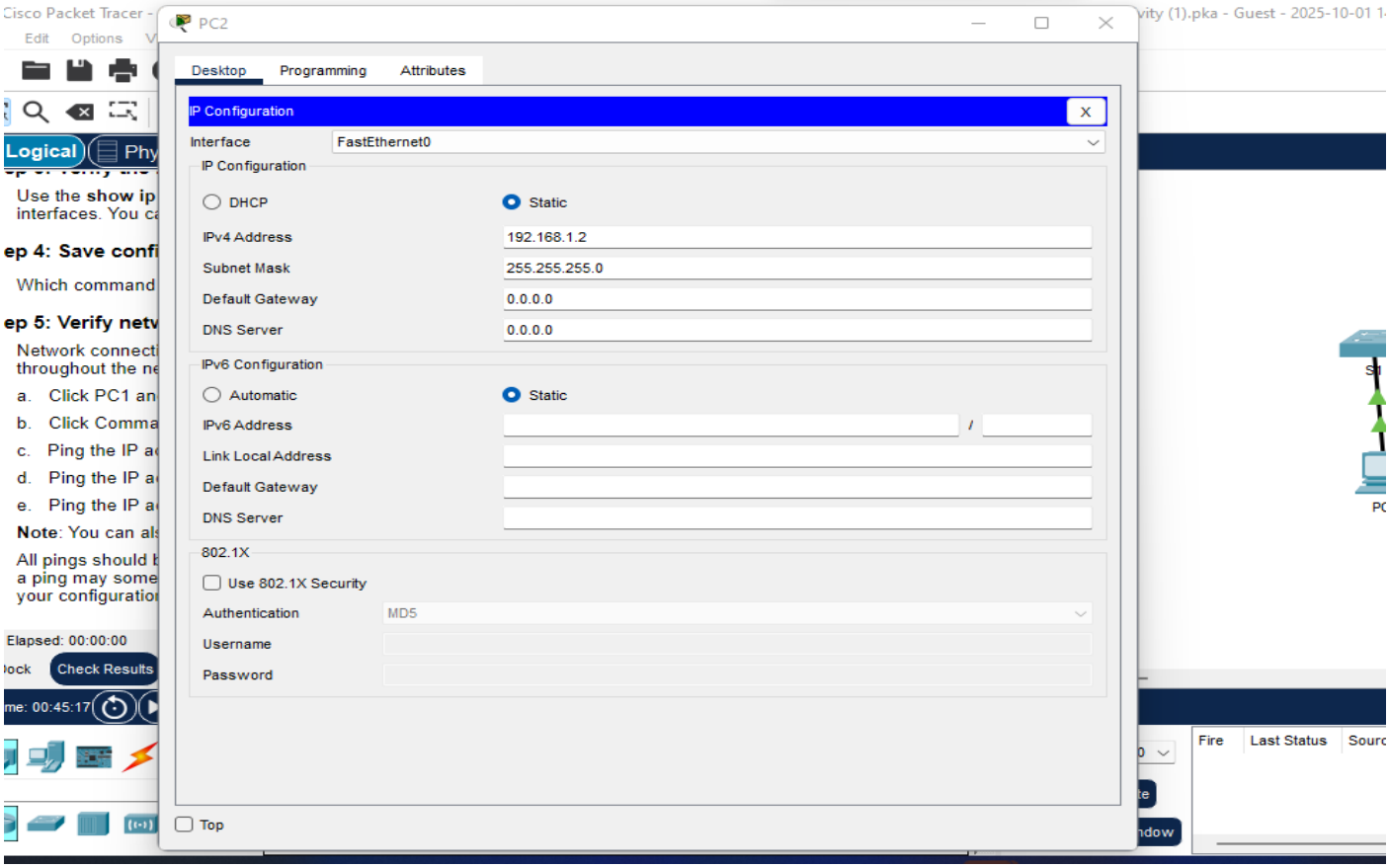

Figure 2

Conclusion:

This activity successfully demonstrated the complete process of implementing basic network connectivity from initial configuration to final verification. By methodically configuring S1 and S2 switches with hostnames, security passwords, MOTD banners, and management IP addresses, then assigning appropriate IP addresses to PC1 and PC2, a functional network infrastructure was established. The verification process using ping commands confirmed successful connectivity between all devices, validating that the configuration was applied correctly. This exercise reinforced several critical networking concepts: the importance of proper IP addressing schemes, the necessity of saving configurations to NVRAM for persistence, the role of switch management interfaces for remote access, and the use of diagnostic tools like ping for troubleshooting. The successful completion of this lab provides essential foundational skills for more advanced network configuration and management tasks.

Task 4.6.5 – Connect a Wired and Wireless LAN

Introduction

This lab demonstrates connecting and verifying both wired and wireless LANs using Cisco Packet Tracer. The objective is to properly connect devices, configure IP addresses, and verify end-to-end communication. The lab also explores physical and logical topologies to reinforce network design understanding.

Objectives

- Connect routers, switches, and wireless devices using correct cables.
- Configure connections between wired and wireless networks.
- Verify communication using ping and web access.

Addressing Table

Table 8

Device	Interface	IP Address	Connects To
Cloud	Eth6	N/A	F0/0
Cloud	Coax7	N/A	Port0
Cable Modem	Port0	N/A	Coax7
Cable Modem	Port1	N/A	Internet
Router0	Console	N/A	RS232
Router0	F0/0	192.168.2.1/24	Eth6
Router0	F0/1	10.0.0.1/24	F0
Router0	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
Router1	F1/0	172.16.0.1/24	F0/1
WirelessRouter	Internet	192.168.2.2/24	Port 1
WirelessRouter	Eth1	192.168.1.1	F0
Family PC	F0	192.168.1.102	Eth1
Switch	F0/1	172.16.0.2	F1/0
Netacad.pka	F0	10.0.0.254	F0/1

Device	Interface	IP Address	Connects To
Configuration Terminal	RS232	N/A	Console

Step-by-Step Implementation

1. Connect Cloud and Modem

- Router0 Fa0/0 → Cloud Eth6 (Straight-Through)
- Cloud Coax7 → Cable Modem Port0 (Coaxial)Link lights green.

2. Connect Routers

- Router0Ser0/0/0 → Router1Ser0/0 (Serial DCE)
- Router0 F0/1 → netacad.pka F0 (Crossover)
- Router0 Console → Configuration Terminal RS232 (Console cable)

3. Connect Remaining Devices

- Router1 F1/0 → Switch F0/1 (Straight-Through)
- Modem Port1 → Wireless Router Internet
- Wireless Router Eth1 → Family PC F0

4. Verify Connectivity

- **Family PC → netacad.pka:** Ping and web browser successful.
- **Home PC → Switch:** Ping successful.
- **Router0:** show ip interface brief confirms interface status.

5. Physical Topology Observations

- Cloud has 2 cables connected.
- Fiber cables use pairs for transmit and receive.
- Home network shows wireless coverage mesh; no rack required.

Conclusion

The wired and wireless LANs were successfully connected and verified. All devices communicated correctly, and ping tests confirmed connectivity. The lab provided practical experience in selecting cables, connecting devices, and understanding physical/logical network topologies. This foundational knowledge is critical for managing real-world networks.

4.6.6 – Viewing Wired and Wireless NIC Information

Objective

The purpose of this lab is to explore, identify, and manage the network interface cards (NICs) — both wired and wireless — installed on a Windows PC. The lab demonstrates how to view NIC details, activate or deactivate interfaces, connect to networks, and use system tray network controls.

Required Resources

1 PC running Windows OS

At least two NICs: one wired (Ethernet) and one wireless (Wi-Fi)

A functional wired and wireless network connection.

Part 1: Identify and Work with PC NICs

1. Viewing NICs via Network and Sharing Center

Access Control Panel > Network and Internet > View network status and tasks.

Click Change adapter settings to view all NICs, including wired, wireless, VPN, and virtual adapters.

2. Managing the Wireless NIC

Enabling and Connecting

Right-click the Wi-Fi adapter to enable it if disabled.

Use Connect/Disconnect to connect to an authorized SSID.

Status and Connection Details

SSID: HSE. Guest

Connection Speed: 200.0 Mbps

MAC Address: 74-40-BB-31-F3-39

DNS Servers

Primary: 8.8.8.8, Secondary: 8.8.4.4

Reason for Multiple DNS Servers: A secondary DNS ensures network continuity if the primary DNS is unavailable.

Command-Line Verification

Using ipconfig /all confirms the same NIC details shown in the Network Connection Details window.

Security and Network Properties.

Wireless Properties > Security Tab displays the network security type and key.

Connecting to new SSIDs requires entering the security key.

3. Managing the Wired NIC

Status and Configuration

Enable the Ethernet adapter and check its Status.

Detailed adapter info shows the physical address, DHCP status, and IP configuration.

Example Ethernet Adapter Output (Summary):

Description: Realtek PCIe GbE Family Controller

Physical Address: 10-62-E5-C3-44-65

Media State: Disconnected

DHCP Enabled: Yes

Other Notable NICs:

Hyper-V Virtual Ethernet Adapters – Used for virtualization and internal networks.

Wi-Fi Direct Virtual Adapters – Enable peer-to-peer wireless connections.

Part 2: Identify and Use the System Tray Network Icons

1. Network Icon Usage

Clicking the network icon displays available SSIDs.

Disabling Wi-Fi hides all wireless networks from the list.

Ethernet can also be disabled similarly.

2. Network Problem Indicators

Network Disabled Icon: Appears when all NICs are disabled.

Network Problem Icon: Appears when a NIC is enabled but cannot connect.

Troubleshooting can be accessed via Network & Internet settings > Troubleshoot.

Key Findings and Observations

Both wired and wireless NICs can coexist on the same machine. If both are active, the system assigns two different IP addresses, and wireless takes precedence.

Multiple DNS servers ensure network reliability.

Virtual adapters (e.g., Hyper-V) are automatically created for virtualization environments.

System tray icons provide quick insights into network status and allow basic NIC management.

Reflection: Why Enable Multiple NICs?

Activating more than one NIC allows a PC to handle multiple network connections simultaneously.

Examples include:

Proxy server setup: Where one NIC connects to the internet and the other to an internal LAN.

Load balancing or redundancy: Ensuring continuous connectivity if one network path fails.

Network segmentation: Accessing different networks securely and efficiently.

Conclusion

This lab successfully demonstrated how to identify, configure, and troubleshoot both wired and wireless NICs in a Windows environment. Understanding NIC functionality is essential for managing network connectivity, optimizing performance, and maintaining reliable access in multi-network environments.