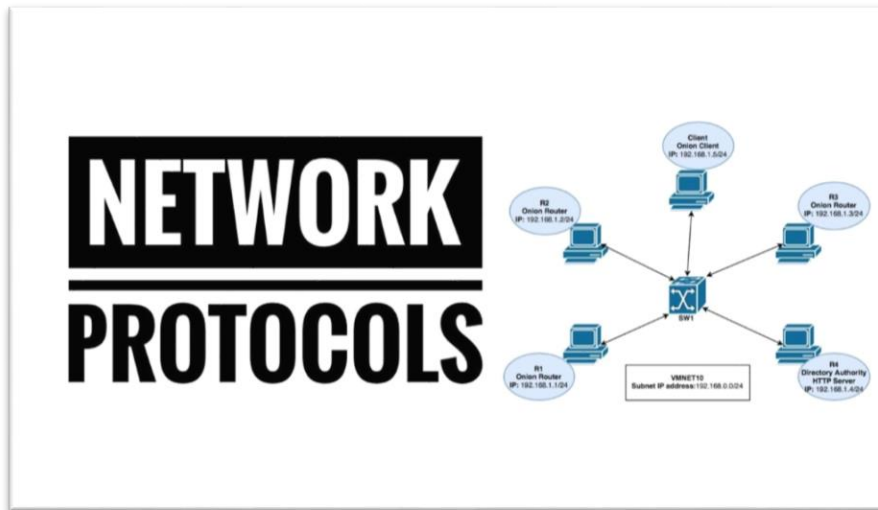


# HARDWARE AND NETWORKING

## SERVICE LEVEL- III

Based on November, 2023 Version-II



**MODULE TITLE: - Installing and managing Network Protocols**

**MODULE CODE: EIS HNS3 M03 1123**

**NOMINAL DURATION: 40 Hours**

**Prepared by: - Ministry of Labor and Skill**

## Table of Contents

Table of Contents .....	i
<b>Unit One: Network protocols</b> .....	<b>1</b>
1. Introduction to network protocols .....	2
1.1. Network protocol .....	3
1.2. Manage appropriate network protocol service .....	5
1.2.1. Select network protocol service .....	5
1.2.2. Test network protocol service .....	7
1.2.3. Validate network protocol service .....	9
1.3. Design a network address system.....	11
1.3.1. IP address .....	13
1.4. Configuring and testing IP address.....	15
1.4.1. Configuring an IP Address (Windows): .....	15
Self-check Questions .....	17
Operation sheet 1.1 .....	19
LAP Test .....	31
<b>Unit Two: Network protocols application</b> .....	<b>32</b>
2 . Introduction to network protocol applications .....	33
2.1 Common network protocol applications .....	33
2.2 Evaluating user requirement and recommend network-protocol services.....	35
2.3 Applying IP addressing scheme .....	36
2.4 . Network layers .....	38
Self-check questions.....	41
Developer profile .....	<b>Error! Bookmark not defined.</b>
Reference.....	<b>Error! Bookmark not defined.</b>



## Unit One: Network protocols

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Overview of network protocols services
- Selecting, testing and validating network protocol services
- Designing a network addressing system
- Configuring and testing IP address

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Understand of network protocols services
- Select, teste and validate appropriate network protocol services
- Design a network address system
- Configure and test IP address

## 1. Introduction to network protocols

A **network** is like a digital community where computers and other devices are connected to each other, allowing them to communicate and share information. Imagine it as a way for computers to talk to each other, just like people do in a community. The main need of networks are:

- **Sharing of resource:** - Networks allow us to share things like files, printers, and internet connections. It is like sharing toys or books with friends.
- **Communication:** - Computers on a network can send messages to each other. It is similar to sending notes or messages to friends in your school.
- **Collaboration:** - People can work together on projects even if they are not in the same place. It is like doing a group project with friends from different classrooms.

A **protocol** is like a set of rules or instructions that everyone follows to make sure things work smoothly. Think of it as a recipe or a game with specific steps that everyone needs to understand and follow.

**Network protocols** are a set of rules and conventions that govern how data is transmitted, received, and processed in a computer network. These protocols enable communication between devices by defining the format and sequencing of data exchanged between them. The use of standardized protocols ensures interoperability and seamless communication across diverse hardware and software platforms. Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way. In order for two computers to talk to each other, they must be speaking the same language.

Here is an introduction to some key aspects of network protocols:

- Communication standard

Network protocols serve as communication standards, establishing a common language for devices to exchange information. These standards define how data is formatted, transmitted, and interpreted by devices in a network.

- Protocol stack

Network protocols are often organized into a layered structure known as a protocol stack. The most well-known reference model for this is the OSI (Open Systems Interconnection) model, which consists of seven layers, each addressing specific aspects of network communication.

## 1.1. Network protocol

A network protocol is a standardized set of rules that allows devices on a network to communicate efficiently. These rules cover how data is formatted, transmitted, received, and how devices identify and address each other. Think of the internet as a massive global conversation. For everyone to understand and respond appropriately there must be a common language. Network protocols ensure that devices worldwide can understand and interpret data consistently. Each protocol serves a specific purpose, and understanding their applications can help in designing and troubleshooting network systems. Here are some common network protocols and their applications:

### 1. Transmission Control Protocol (TCP):

- Application: Web browsing, email, file transfer.
- Description: Ensures reliable, ordered, and error-checked delivery of data. Used for applications where accurate and complete data transmission is crucial.

### 2. Internet Protocol (IP):

- Application: Routing and addressing data packets on the internet.
- Description: Responsible for addressing and routing data packets between devices on a network. IP is fundamental for internet communication.

### 3. Hypertext Transfer Protocol (HTTP):

- Application: Web browsing.
- Description: Facilitates the transfer of hypertext (web pages) between a web server and a web browser. The foundation of data communication on the World Wide Web.

### 4. File Transfer Protocol (FTP):

- Application: File transfer between computers.
- Description: Enables the transfer of files between a local and remote computer. Commonly used for website maintenance and data sharing.

### 5. Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP3)/Internet Message Access Protocol (IMAP):

- Application: Email communication.
- Description: SMTP is used for sending emails, while POP3 and IMAP are used for receiving emails. These protocols work together to manage email communication.

### 6. Domain Name System (DNS):

- Application: Resolving domain names to IP addresses.
  - Description: Translates human-readable domain names (e.g., www.example.com) into IP addresses that computers use to identify each other on the internet.
7. Dynamic Host Configuration Protocol (DHCP):
- Application: Automatic IP address assignment.
  - Description: Dynamically assigns IP addresses to devices on a network, making it easier to manage and configure large networks.
8. Secure Shell (SSH) and Telnet:
- Application: Remote command-line access to servers.
  - Description: SSH provides secure, encrypted communication for accessing and managing remote servers, while Telnet is an older protocol without encryption.
9. Simple Network Management Protocol (SNMP):
- Application: Network management and monitoring.
  - Description: Facilitates the exchange of management information between network devices, allowing administrators to monitor and manage network performance.
10. Hyper Text Transfer Protocol Secure (HTTPS):
- Application: Secure web browsing.
  - Description: An extension of HTTP with added security features using SSL/TLS encryption, ensuring secure communication for online transactions and sensitive data.

TCP/IP	OSI Model	Protocols
Application Layer	Application Layer	DNS - DHCP - FTP - HTTPS - LDAP - NTP - POP3 - RTP - RTSP - SSH - SIP - SMTP - Telnet - TFTP
	Presentation Layer	JPEG - MIDI - MPEG - PICT - TIFF
	Session Layer	NetBIOS - NFS - PAP - SCP - SQL - ZIP
Transport Layer	Transport Layer	TCP - UDP
Internet Layer	Network Layer	ICMP - IGMP - IPsec - IPv4 - IPv6 - IPX - RIP
Link Layer	Data Link Layer	ARP - ATM - CDP - FDDI - Frame Relay - HDLC - MPLS - PPP - STP - Token Ring
	Physical Layer	Bluetooth - Ethernet - DSL - ISDN - 802.11 - WiFi

Figure 1. 1 Network protocol

Understanding these protocols and their applications is crucial for network administrators, developers, and anyone involved in managing or troubleshooting computer networks. Each protocol plays a specific role in enabling the diverse range of services we use in our interconnected digital world.

## 1.2. Manage appropriate network protocol service

Managing network protocol services involves overseeing the configuration, monitoring, and maintenance of the protocols that enable communication and data transfer within a network. To manage the service of network protocol we use select, test and validate appropriate network protocol service.

### 1.2.1. Select network protocol service

Selecting an appropriate network protocol service depends on the specific requirements and goals of your network. Here are some common scenarios along with corresponding network protocol services:

#### 1. Web Browsing:

Appropriate Protocol: Hypertext Transfer Protocol (HTTP) or its secure counterpart HTTPS.

Description: HTTP is used for standard web browsing, while HTTPS adds a layer of security with encrypted communication.

#### 2. Secure Remote Access:

Appropriate Protocol: Secure Shell (SSH) or Virtual Private Network (VPN) protocols.

Description: SSH provides secure command-line access, while VPNs enable secure access to a private network over the internet.

#### 3. File Transfer:

Appropriate Protocol: File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP).

Description: FTP is suitable for basic file transfers, while SFTP adds encryption for enhanced security.

#### 4. Email Communication:

Appropriate Protocol: Simple Mail Transfer Protocol (SMTP) for sending emails, and Post Office Protocol (POP3) or Internet Message Access Protocol (IMAP) for receiving emails.

Description: SMTP is used to send emails, while POP3 and IMAP retrieve emails from a server.

#### 5. Network Management:

Page 5 of 46	Ministry of Labor and Skills Author/Copyright	Install and Manage Network Protocols Level - III	Version -1
			November, 2023



Appropriate Protocol: Simple Network Management Protocol (SNMP).

Description: SNMP facilitates the exchange of management information between network devices, allowing for monitoring and control.

#### **6. Dynamic IP Address Assignment:**

Appropriate Protocol: Dynamic Host Configuration Protocol (DHCP).

Description: DHCP automatically assigns IP addresses to devices on a network, simplifying network configuration.

#### **7. Web Security:**

Appropriate Protocol: HTTPS (SSL/TLS).

Description: HTTPS ensures secure communication between a web browser and a server, crucial for online transactions and sensitive data.

#### **8. Real-Time Communication:**

Appropriate Protocol: Real-Time Transport Protocol (RTP) for audio and video streaming.

Description: RTP is commonly used for real-time communication, such as VoIP (Voice over Internet Protocol) and video conferencing.

#### **9. Domain Name Resolution:**

Appropriate Protocol: Domain Name System (DNS).

Description: DNS translates human-readable domain names into IP addresses, facilitating internet navigation.

#### **10. Remote System Management:**

- Appropriate Protocol: Intelligent Platform Management Interface (IPMI) or Remote Desktop Protocol (RDP).
- Description: IPMI provides remote management capabilities for servers, while RDP allows remote access to desktop environments.

#### **11. Database Connectivity:**

- Appropriate Protocol: Structured Query Language (SQL) protocols like MySQL, PostgreSQL, or Microsoft SQL Server protocols.
- Description: Each database system often has its own protocol for communication between client applications and database servers.

#### **12. Collaboration and Messaging:**

- Appropriate Protocol: Extensible Messaging and Presence Protocol (XMPP) for instant messaging.
- Description: XMPP is commonly used for real-time communication and collaboration in messaging applications.

When selecting a network protocol service, consider the specific needs, security requirements, and compatibility with your network infrastructure and devices. It's often a good practice to use secure versions of protocols (e.g., HTTPS instead of HTTP) when dealing with sensitive data or communication. Additionally, stay informed about updates and advancements in protocols to ensure the continued security and efficiency of your network.

### 1.2.2. Test network protocol service

Testing network protocol services is a crucial step to ensure that they operate as intended, meet performance expectations, and are secure. Below are key steps and considerations for testing an appropriate network protocol service:

#### 1. Functionality Testing:

- Objective: Verify that the protocol service performs its intended functions.
- Activities:- Perform basic operations and transactions using the protocol. Test different features and functionalities provided by the protocol.

#### 2. Performance Testing:

- Objective: Assess the speed, responsiveness, and efficiency of the protocol service.
- Activities:-Measure data transfer rates under varying network conditions. Test the protocol's performance under heavy loads and high traffic.

#### 3. Security Testing:

- Objective: Identify and address potential security vulnerabilities in the protocol service.
- Activities:-Conduct penetration testing to uncover potential weaknesses. Verify that encryption mechanisms (e.g., SSL/TLS) are implemented correctly.

#### 4. Compatibility Testing:

- Objective: Ensure that the protocol service is compatible with different devices, platforms, and software applications.
- Activities:-Test the protocol across various operating systems and devices. Verify interoperability with different versions of the protocol.

### 5. Reliability and Stability Testing:

- Objective: Assess the reliability and stability of the protocol service under normal and stressful conditions.
- Activities:-Conduct stress testing to simulate heavy usage and monitor the protocol's behavior. Evaluate how the protocol handles unexpected events or errors.

### 6. Scalability Testing:

- Objective: Evaluate the ability of the protocol service to scale with the growth of the network.
- Activities:-Test the protocol's performance as the number of users or devices increases. Assess how well the protocol handles additional network nodes.

### 7. Usability Testing:

- Objective: Assess the user-friendliness and ease of use of the protocol service.
- Activities:- Gather feedback from end-users regarding their experience with the protocol. Identify and address any usability issues or user interface concerns.

### 8. Error Handling and Recovery Testing:

- Objective: Verify how well the protocol service handles errors and recovers from failures.
- Activities:- Intentionally induce errors and observe the protocol's response. Test the recovery mechanisms to ensure minimal disruption.

### 9. Interoperability Testing:

- Objective: Confirm that the protocol service works seamlessly with other protocols and network devices.
- Activities:- Test the protocol's compatibility with devices from different vendors. Verify integration with other network services.

### 10. Documentation Verification:

- Objective: Confirm that the documentation accurately reflects the protocol service's features and configurations.
- Activities:-Review the official documentation for completeness and accuracy. Ensure that configuration steps align with the actual behavior of the protocol.

By following these testing activities, you can ensure that the network protocol service is thoroughly evaluated for functionality, performance, security, and usability. Regular testing and monitoring are essential to maintain the reliability and effectiveness of the protocol service over time.

### 1.2.3. Validate network protocol service

Validating an appropriate network protocol service involves ensuring that the service meets the intended requirements, operates effectively, and complies with relevant standards. Here's a step-by-step guide for validating a network protocol service:

#### 1. Review Requirements:

- **Objective:** Confirm that the network protocol service aligns with the specified requirements.
- **Activities:** - Refer to the initial project or network requirements documentation.

Verify that the chosen protocol addresses the identified needs.

#### 2. Check Standards Compliance:

- **Objective:** Ensure that the network protocol service complies with industry standards and specifications.
- **Activities:** - Refer to relevant standards documents.

Confirm that the protocol adheres to protocols and conventions outlined in industry specifications.

#### 3. Functional Validation:

- **Objective:** Confirm that the protocol service performs its intended functions.
- **Activities:-** Execute test cases based on functional requirements. Verify that the protocol service meets expectations for data transfer, addressing, and other functionalities.

#### 4. Performance Validation:

- **Objective:** Assess the performance of the protocol service under various conditions.
- **Activities:-** Measure data transfer rates, latency, and throughput. Evaluate performance under both normal and peak load scenarios.

#### 5. Security Validation:

- **Objective:** Confirm that the protocol service implements necessary security measures.
- **Activities:-** Verify the use of encryption mechanisms (e.g., SSL/TLS). Conduct security testing to identify and address potential vulnerabilities.

#### 6. Compatibility and Interoperability Testing:

- **Objective:** Ensure that the protocol service works seamlessly with other protocols and devices.

- **Activities:**-Test interoperability with devices from different vendors. Verify compatibility with various operating systems and network environments.

#### 7. Error Handling Validation:

- **Objective:** Confirm that the protocol service effectively handles errors and failures.
- **Activities:**- Intentionally induce errors and assess the protocol's response. Verify the effectiveness of error recovery mechanisms.

#### 8. Scalability Validation:

- **Objective:** Assess the protocol service's ability to scale with network growth.
- **Activities:**- Test performance as the number of users or devices increases. Evaluate scalability under different network conditions.

#### 9. Usability Validation:

- **Objective:** Assess the user-friendliness and ease of use of the protocol service.
- **Activities:**- Gather feedback from end-users. Evaluate the protocol service's user interface and overall user experience.

#### 10. Documentation Verification:

- **Objective:** Confirm that documentation accurately reflects the protocol service's features and configurations.
- **Activities:**- Review official documentation for completeness and accuracy.

Ensure that configuration steps align with the actual behavior of the protocol.

#### 11. Compliance Validation:

- **Objective:** Verify that the protocol service complies with industry standards and regulatory requirements.
- **Activities:**- Conduct audits to ensure adherence to relevant standards. Confirm compliance with any legal or regulatory requirements.

#### 12. Feedback and Improvement:

- **Objective:** Gather feedback from stakeholders and end-users to identify areas for improvement.
- **Activities:** - Encourage open communication and feedback. Use feedback to make necessary adjustments and improvements.

By following these validation activities, you can ensure that the network protocol service is thoroughly assessed, meets requirements, and operates effectively in the intended network

environment. Regular validation, monitoring, and feedback mechanisms contribute to the continuous improvement of the protocol service.

### 1.3. Design a network address system

Designing a network address system involves planning how devices on a network will be identified and communicated with. This includes defining IP addressing schemes, sub-netting, and addressing assignments. Below are the steps to design a network address system:

#### 1. Define Network Requirements:

Clearly understand the requirements of your network. Consider the number of devices, scalability, security needs, and any specific constraints or regulations.

#### 2. Choose IP Addressing Scheme:

Decide whether you will use IPv4 or IPv6. IPv4 is the most widely used, but IPv6 is becoming increasingly important due to the exhaustion of IPv4 addresses.

#### 3. Address Space Planning:

Determine the size of your network and allocate address space accordingly. Plan for growth to ensure that your addressing scheme can accommodate future expansion.

#### 4. sub netting:

Divide your network into subnets to improve efficiency, security, and manageability. Sub netting allows you to group devices logically and control traffic flow.

#### 5. Select Private IP Address Range:

If you are using IPv4, choose a private IP address range for your internal network. Common private IP address ranges include 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255.

#### 6. Assign Subnet Addresses:

Assign specific subnets to different departments, functions, or physical locations based on your organization's structure and needs. Document the purpose of each subnet.

#### 7. Plan for VLANs (Virtual LANs):

If your network includes VLANs, plan how they will be integrated into your addressing scheme. VLANs allow you to logically segment a network regardless of physical location.

#### 8. Consider DHCP (Dynamic Host Configuration Protocol):

Decide whether to use static or dynamic IP addressing. DHCP can simplify IP address management by automatically assigning addresses to devices on the network.

### **9. Document Addressing Plan:**

Create a detailed document outlining the entire addressing plan. Include information about the address ranges, subnets, VLANs, and any other relevant details. This document will be valuable for troubleshooting and future network administrators.

### **10. Implement IPv6 (if applicable):**

If you are designing a new network or upgrading an existing one, consider implementing IPv6 alongside IPv4. IPv6 provides a larger address space and is essential for the long-term sustainability of your network.

### **11. Consider Network Security:**

Implement security measures in your addressing plan, such as using firewalls, access control lists (ACLs), and private addressing for internal resources.

### **12. Plan for Remote Access:**

If your network supports remote access, plan how devices will be addressed and secured. This may involve using VPNs (Virtual Private Networks) and addressing schemes for remote networks.

### **13. Validate and Test:**

Before deploying the addressing scheme, validate it in a test environment. This helps identify any issues and ensures that the design meets the requirements.

### **14. Document Network Changes:**

Keep the addressing plan documentation updated whenever there are changes to the network. This includes additions of new subnets, modifications to existing ones, and changes to device addressing.

### **15. Monitor and Adjust:**

Regularly monitor the network for performance, security, and growth. Adjust the addressing plan as needed to accommodate changes in requirements or network topology.

By following these steps, you can design a network address system that meets the requirements of your organization, provides scalability, and ensures efficient and secure communication among devices on the network.

Designing a network addressing system involves allocating IP addresses with consideration for subnets and host IDs. When designing a network-addressing scheme, sub netting involves dividing an IP address space into smaller, more manageable sub-networks. Each subnet has its own unique subnet ID, and devices within the subnet are assigned host IDs.

### 1.3.1. IP address

IP addresses are classified into two main types based on version: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). These types differ in their format and the number of bits used to represent addresses.

#### 1. IPv4 (Internet Protocol version 4):

- **Format:** IPv4 addresses are 32-bit numerical labels, typically represented in dotted-decimal format (e.g., 192.168.0.1).
- **Address Space:** Provides approximately 4.3 billion unique addresses.
- **Notation:** Consists of four octets separated by periods (e.g., 192.168.0.1).
- **Common Usage:** Still widely used in most networks today.
- **Example:** 192.168.1.1

#### 2. IPv6 (Internet Protocol version 6):

- **Format:** IPv6 addresses are 128-bit hexadecimal numbers, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- **Address Space:** Offers an immensely larger address space than IPv4, allowing for virtually unlimited unique addresses.
- **Notation:** Consists of eight groups of four hexadecimal digits, separated by colons.
- **Common Usage:** Becoming increasingly adopted as IPv4 addresses are exhausted.
- **Example:** 2001:0db8::1

#### Additional Types:

1. Public IP Address:- is globally unique and routable on the Internet. The Internet Assigned Numbers Authority (IANA) to organizations and individuals assigns it.

- **Example:** The IP address assigned to your home router by your Internet Service Provider (ISP).

2. Private IP Address:- are reserved for use within private networks and are not routable on the public Internet. They are defined in RFC 1918.

- **Example:** Addresses from ranges like 192.168.0.0 to 192.168.255.255, 172.16.0.0 to 172.31.255.255, and 10.0.0.0 to 10.255.255.255.

3. Static IP Address:- is manually assigned to a device and does not change over time. It is often used for servers and network devices.

- **Example:** Configuring a printer with a fixed IP address of 192.168.1.100.



4. Dynamic IP Address: is assigned automatically by a DHCP (Dynamic Host Configuration Protocol) server. It may change periodically.

- **Example:** Computers and smartphones in a home network obtaining IP addresses from a router's DHCP server.

Understanding these types of IP addresses is essential for effective network management and communication on the Internet.

## IP address class

IP address classes are a way to categorize IP addresses based on their initial bits, and they were a part of the original design of the Internet Protocol (IPv4). IP addresses are divided into five different classes, designated as Class A, Class B, Class C, Class D, and Class E. Each class has a specific range of IP addresses that can be assigned to networks.

### 1. Class A:

- Range: 1.0.0.0 to 126.0.0.0
- Network ID: The first octet represents the network ID, and the remaining three octets are used for host addresses.
- Example: 10.0.0.1

### 2. Class B:

- Range: 128.0.0.0 to 191.255.0.0
- Network ID: The first two octets represent the network ID, and the remaining two octets are used for host addresses.
- Example: 172.16.0.1

### 3. Class C:

- Range: 192.0.0.0 to 223.255.255.0
- Network ID: The first three octets represent the network ID, and the last octet is used for host addresses.
- Example: 192.168.0.1

### 4. Class D:

- Range: 224.0.0.0 to 239.255.255.255
- Purpose: Class D addresses are reserved for multicast groups, which are used for one-to-many communication.

### 5. Class E:

- Range: 240.0.0.0 to 255.255.255.254
- Purpose: Class E addresses are reserved for experimental or future use and are not used in general networking.

## 1.4. Configuring and testing IP address

Configuring and testing an IP address involves setting up the IP address on a device, such as a computer or network device, and ensuring that it can communicate with other devices on the network. Below are step-by-step instructions for configuring and testing an IP address on a typical computer running a Windows operating system. Keep in mind that the exact steps may vary slightly depending on the operating system in use.

### 1.4.1. Configuring an IP Address (Windows):

#### 1. Open Network Settings:

- Open the "Settings" menu on your computer and go to "Network & Internet."

#### 2. Access Network Connections:

- Click on "Change adapter options" to access your network connections.

#### 3. Select Network Adapter:

- Right-click on the network adapter you want to configure (e.g., Ethernet or Wi-Fi) and choose "Properties."

#### 4. Choose Internet Protocol Version 4 (TCP/IPv4):

- In the properties window, find and select "Internet Protocol Version 4 (TCP/IPv4)" from the list.

#### 5. Specify IP Address:

- Choose the option to "Use the following IP address" and enter the desired IP address, subnet mask, default gateway, and DNS server addresses. These values should be provided by your network administrator or determined based on your network configuration.

#### 6. Save Changes:

- Click "OK" to save the changes and close the properties window.

#### Testing the IP Address (Windows):

##### 1. Open Command Prompt:

- Open the Command Prompt by searching for "cmd" in the Start menu.

## 2. Check IP Configuration:

- Use the command **ipconfig** to display the current IP configuration of the device. Verify that the configured IP address, subnet mask, default gateway, and DNS server information match the values you set. Use the following commands on CMD

```
Bash  
Ipconfig
```

## 3. Ping the Default Gateway:

- Use the command **ping** to test communication with the default gateway. Replace "gateway\_ip" with the actual IP address of your default gateway.

```
bash  
ping gateway_ip
```

## 4. Ping a Remote Device:

- Test communication with a remote device on the network by using the **ping** command with the remote device's IP address.

```
Bash  
ping remote_device_ip
```

Replace "remote\_device\_ip" with the actual IP address of the remote device.

## 5. Verify Internet Connectivity:

- Test internet connectivity by pinging a well-known external IP address, such as a public DNS server.

```
Bash  
ping 8.8.8.8
```

## 6. Test DNS Resolution:

- Check if DNS resolution is working by pinging a domain name.

```
bash  
ping www.example.com
```

If the ping is successful, DNS resolution is working correctly.

**Note:** - If you encounter issues, double-check the IP configuration settings and ensure they are correct. Ensure that the configured IP address is within the correct subnet range. If using DHCP, ensure that the DHCP server is reachable and configured correctly.



- C. To route traffic between different networks
- D. To assign IP addresses dynamically

- \_\_\_\_\_6. How can you test the connectivity between two devices on a network using their IP addresses?
- A. By pinging the destination IP address
  - B. By performing a DNS lookup
  - C. By establishing an FTP connection
  - D. By sending an email

**Part III: - Give short answer**

1. List and explain with each of IP address class?
2. Demonstrate steps to design a network address system?
3. List and explain network protocols and their applications?

## Operation sheet 1.1

**Operation title:** Configure and test IP address

**Purpose:** - Assign static and dynamic IP address for computer

**Instruction:** Use the figure below, given equipment and task. You have given 1 Hr. for the task and you are expected to complete tasks.

**Tools and requirement:** Computes, Network, Network driver

Task 1:- Assign static IP address for computer

To perform this task you use:


- IP: - 192.168.0.10
- Subnet mask: - 255.255.255.0
- Default IP address: - 192.168.0.254

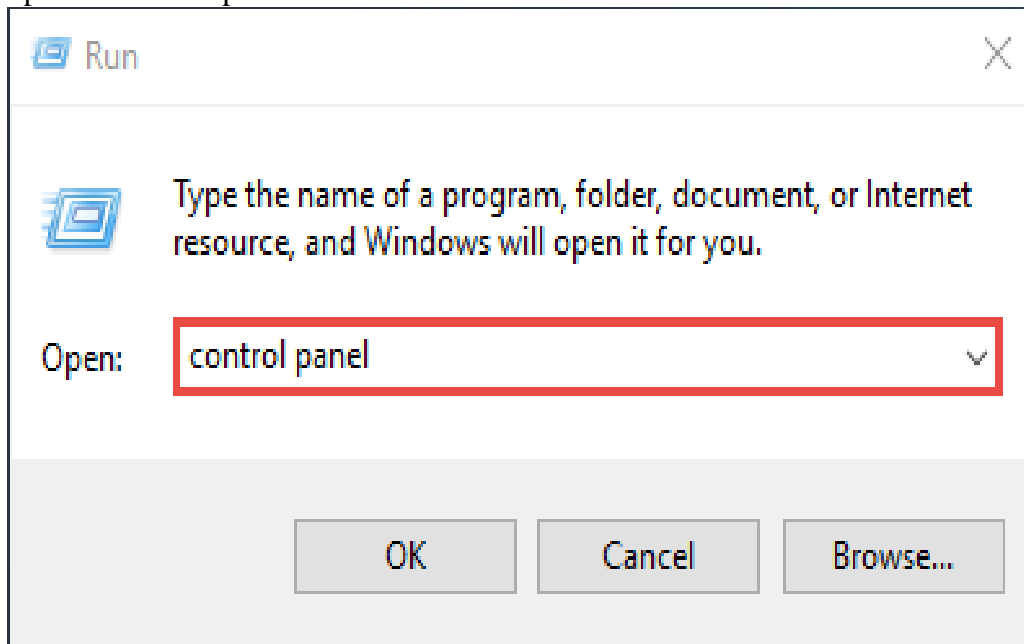
Task 2:- Assign dynamic IP address for computer

Task 3:- Test the configuration of IP address

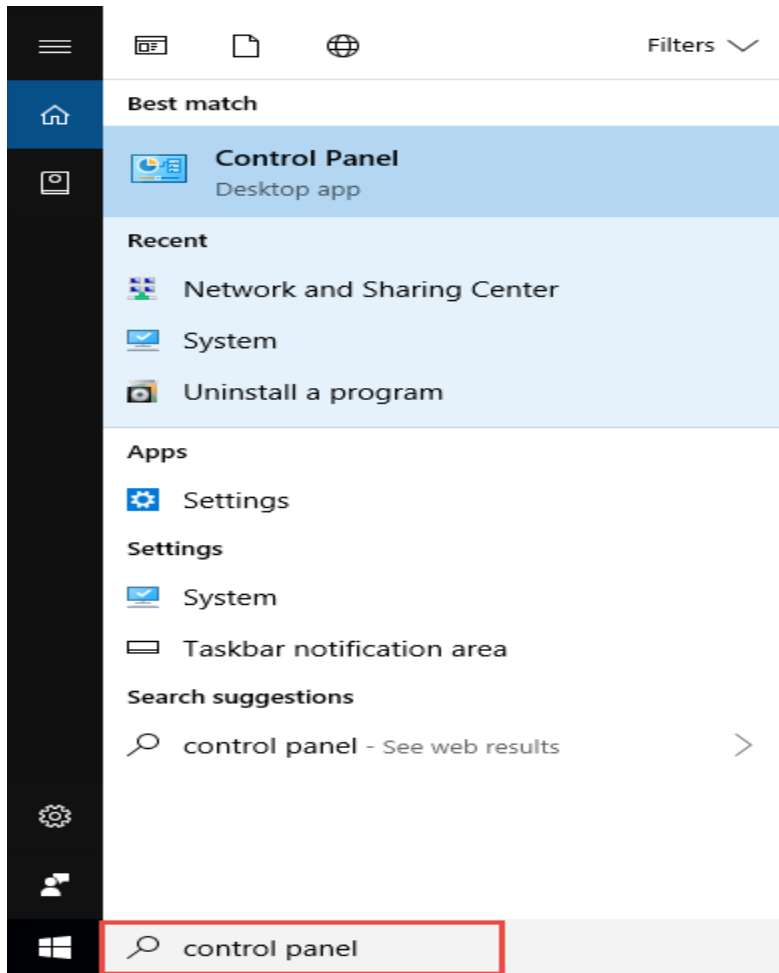
### Task 1:- Assign static IP address for computer

#### Step 1:- Open the Control Panel

Press “Windows  + R”, then a Run box comes out. Input control panel and press Enter to open the control panel.

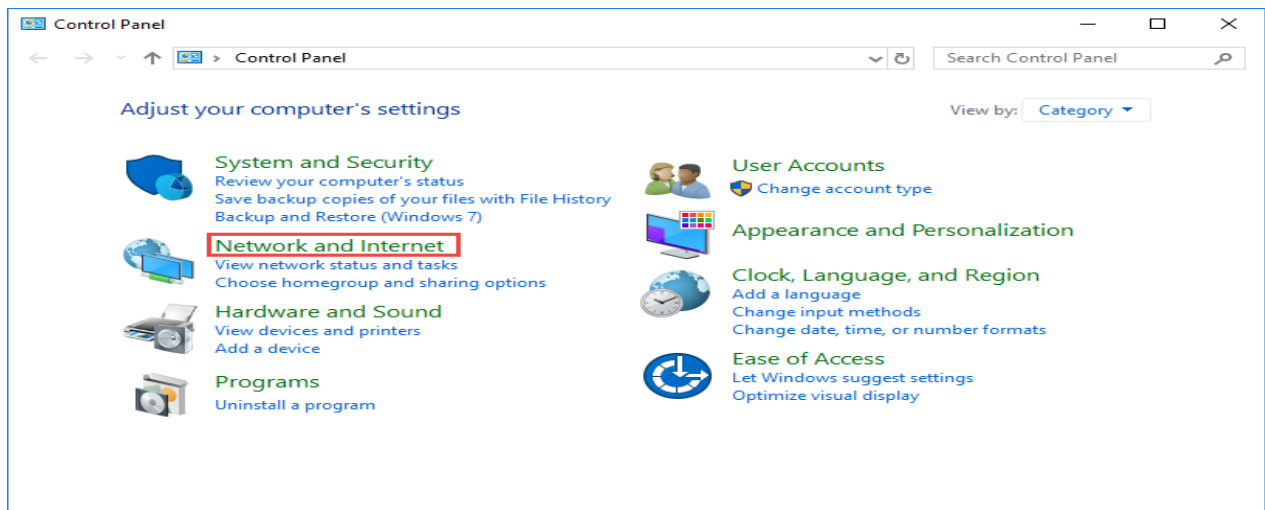


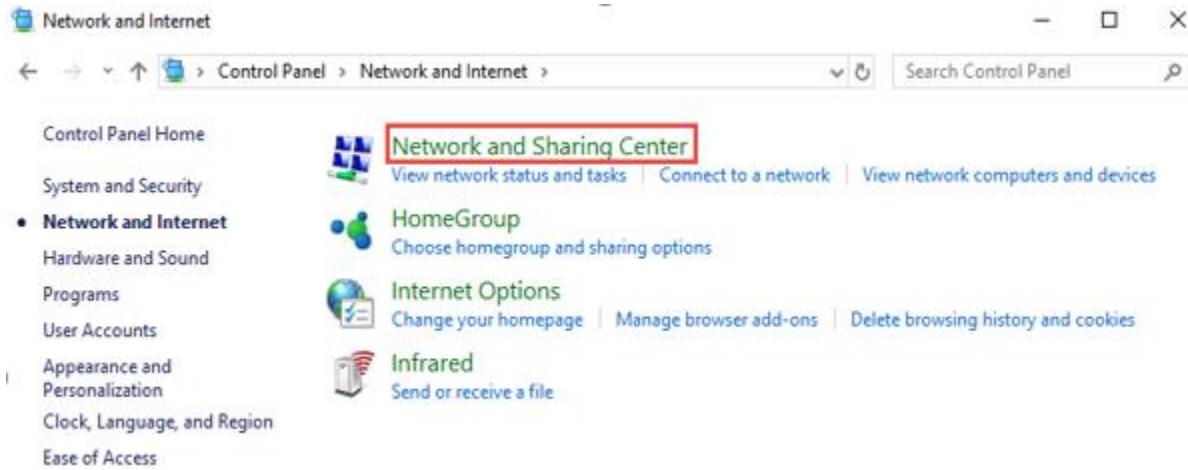
You can also type control panel in the search bar at the lower left of the screen and press Enter to open the control panel.



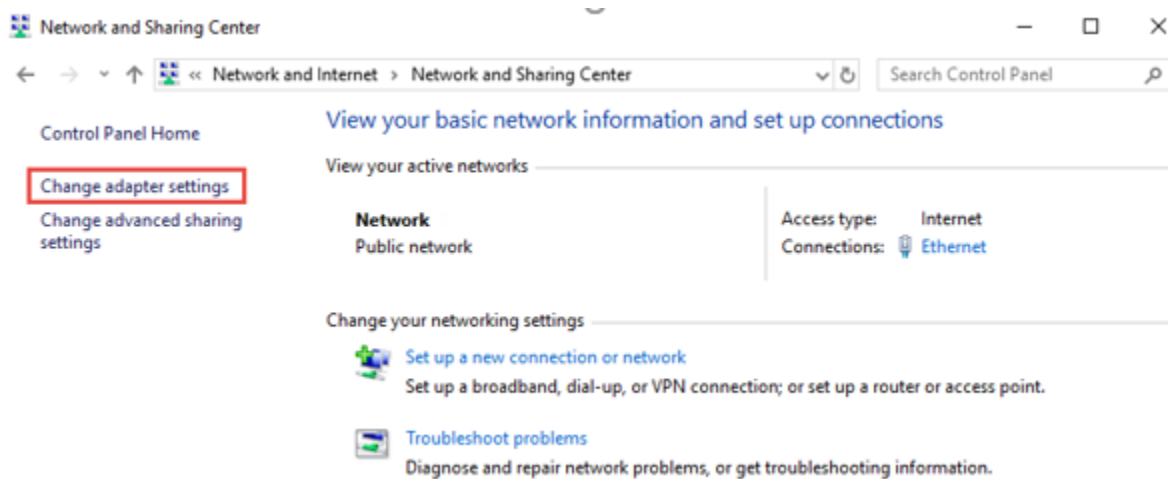
Step 2: Go to Network Connections

Go to Network and Internet → Network and Sharing Center.



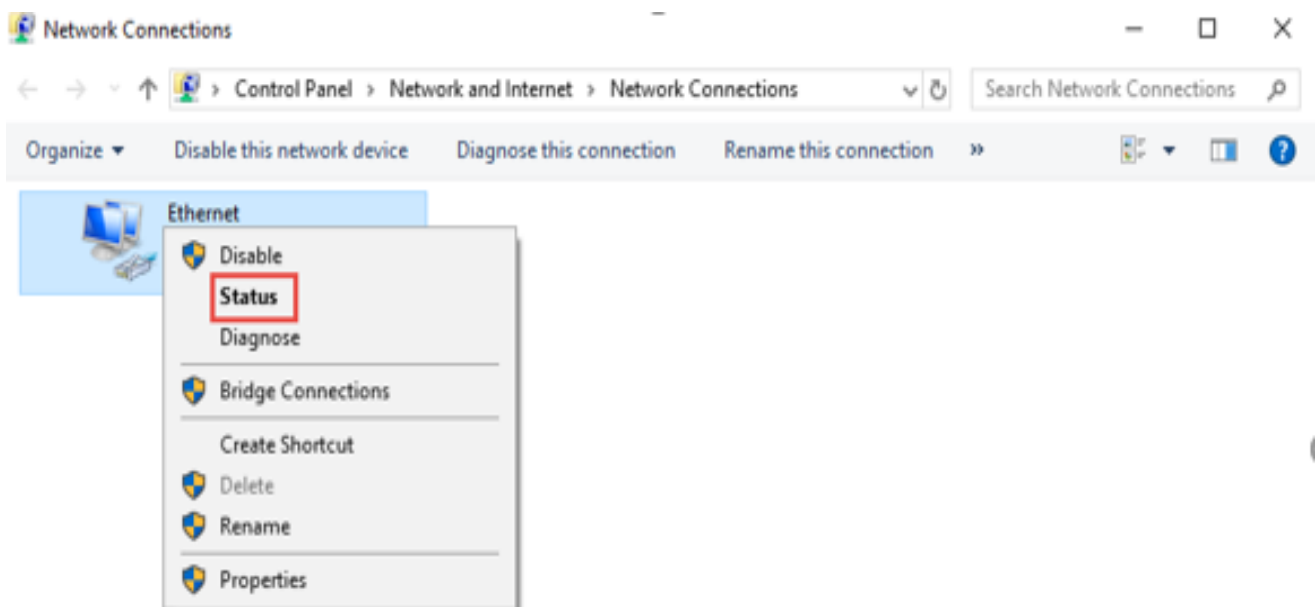


Select Change adapter settings on the left.



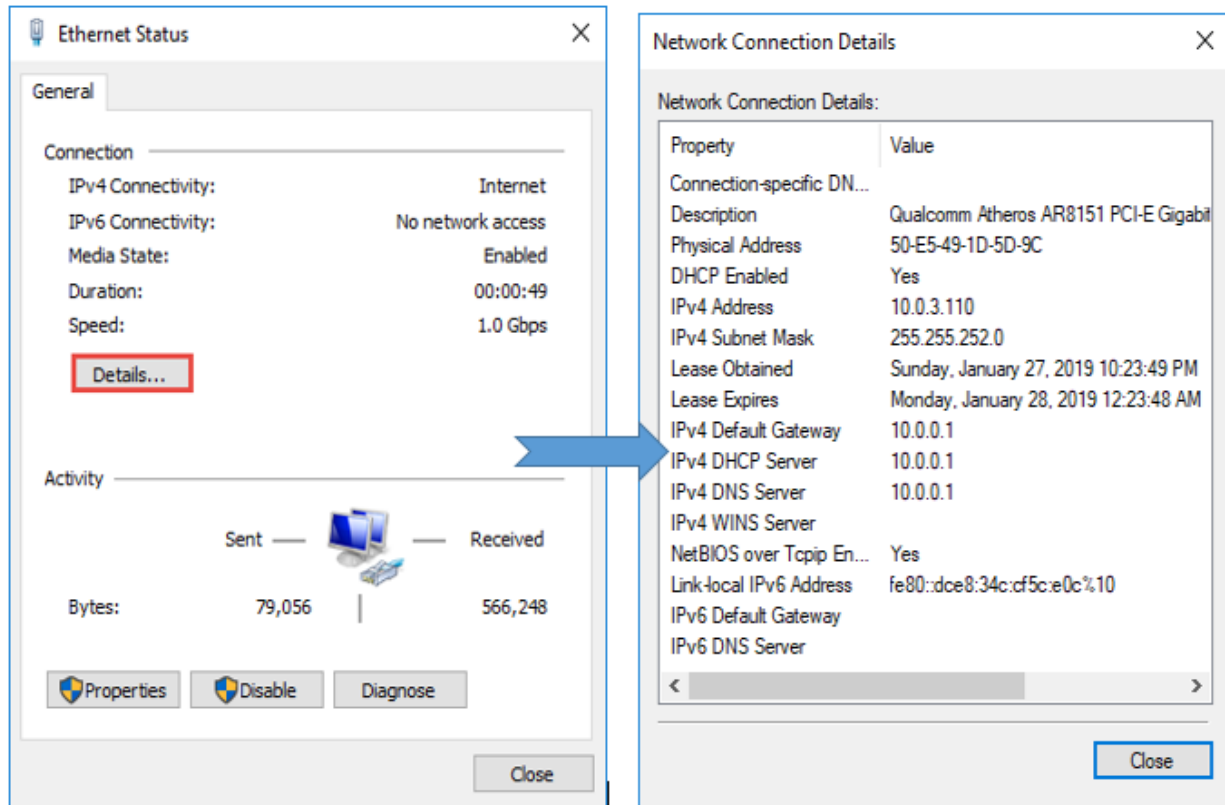
Step 3: Find the IP address

Right click the Ethernet icon and select Status from the context menu.



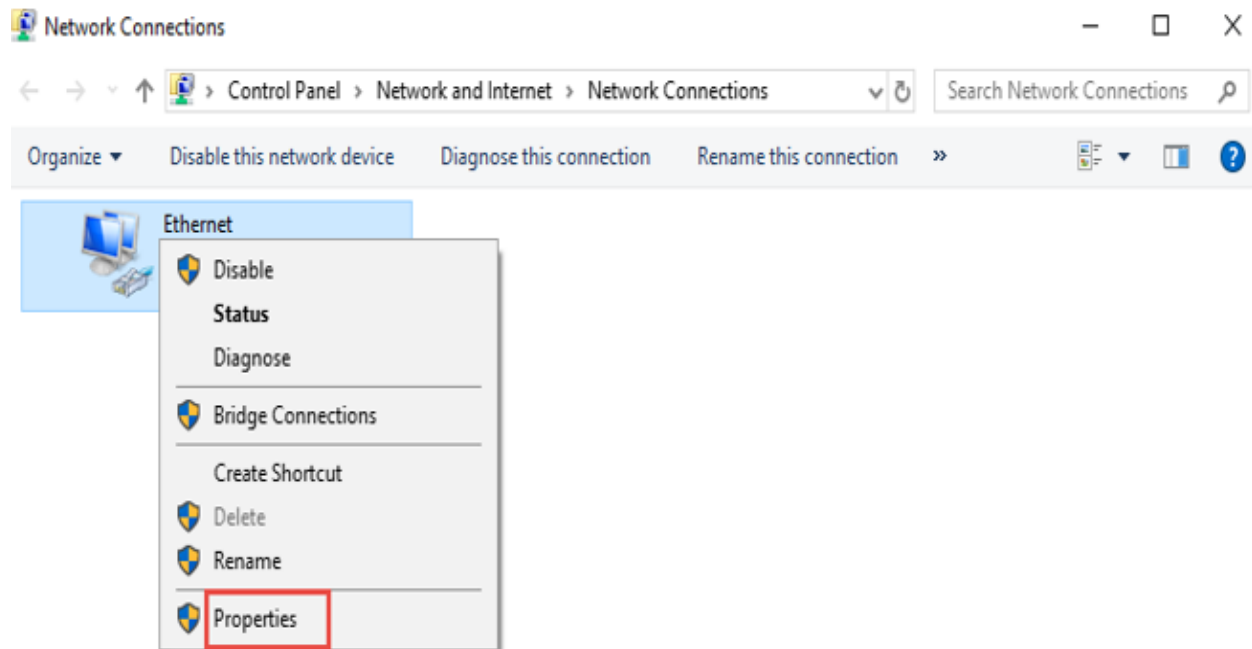


Then click Details... to view all detailed information of network connection.

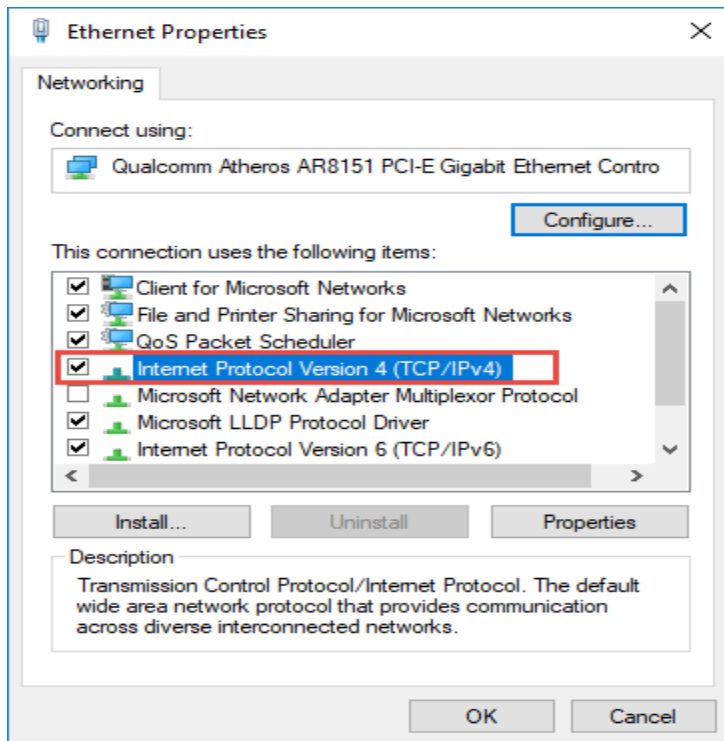


Step 4: Set the IP address

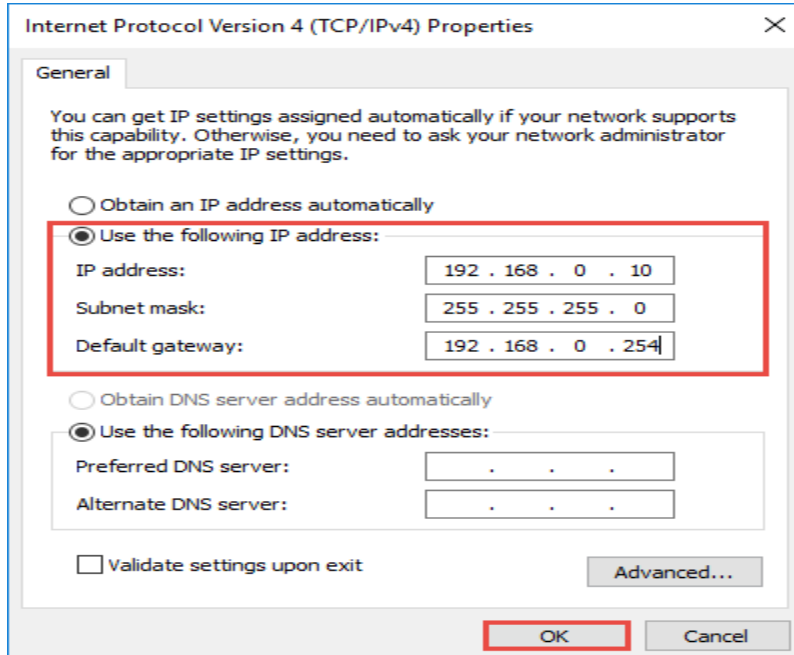
Right Click Local Area Connection and select Properties.



Then double click Internet Protocol Version 4 (TCP/IPv4).



Select use the following IP address: and type in the IP address, Subnet mask and Default gateway.  
Click OK to apply the settings.



Note: If you need to set a static DNS server, select Use the following DNS server address: and input the address of DNS server. By default, the computer obtains the address automatically.

## Task 2:- Assign dynamic IP address for computer

- Change to dynamic IP address (DHCP) from Settings

To enable DHCP to obtain a TCP/IP configuration automatically on Windows 10, use these steps:

**Step 1:-** Open Settings on Windows 10.

Step 2:- Click on Network & Internet.

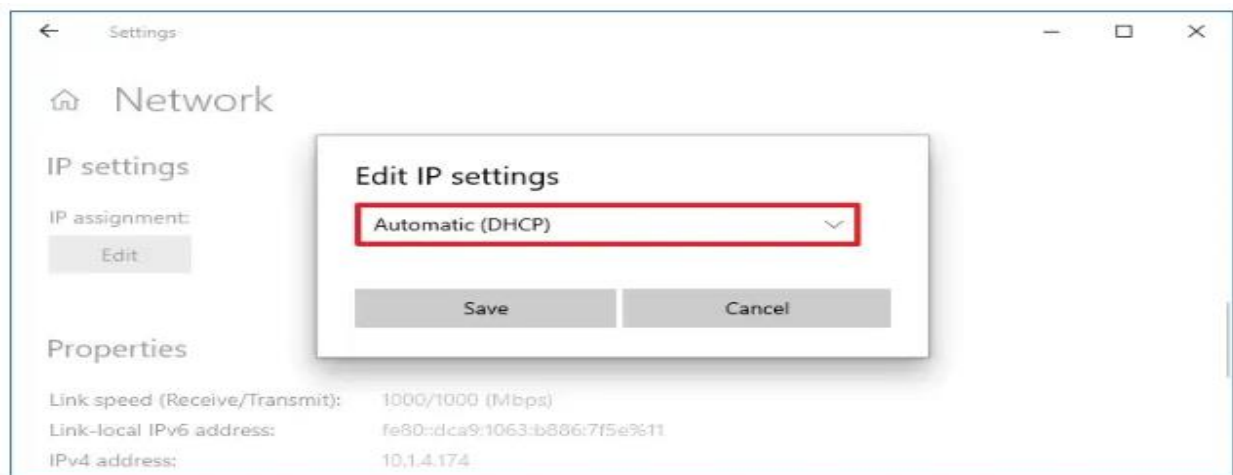
Step 3:- Click on Ethernet or Wi-Fi.

Step 3:- Click the network connection.

Step 4:- Under the “IP settings” section, click the Edit button.



**Step 6:-** Use the Edit IP settings drop-down menu and select the Automatic (DHCP) option.



**Step 7:-** Click the Save button.

**Notes:-** Once you complete the steps, the networking stack configuration will reset, and your device will request an IP address from the DHCP server (usually your router).

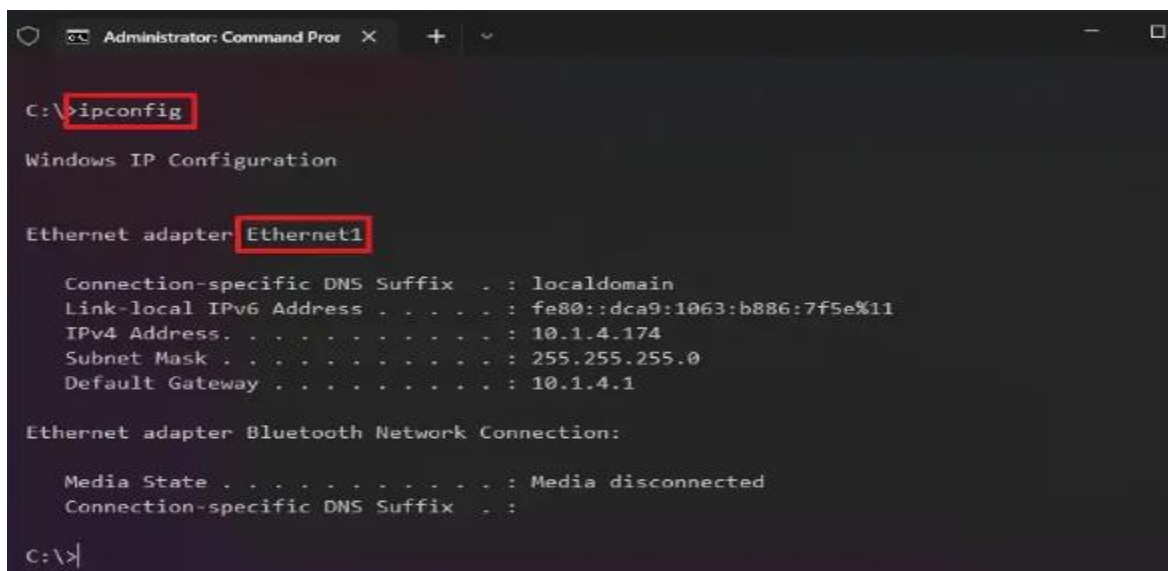
- **Change to dynamic IP address (DHCP) from Command Prompt**

To switch from a static TCP/IP configuration to a dynamically assigned configuration using DHCP with Command Prompt, use these steps:

Step 1:- Open Start.

Step 2:- Search for Command Prompt, right-click the top result, and select the Run as administrator option.

Step 3:-Type the following command to note the name of the network adapter and press Enter



```
Administrator: Command Prom...
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet1

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::dca9:1063:b886:7f5e%11
    IPv4 Address. . . . . : 10.1.4.174
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.4.1

Ethernet adapter Bluetooth Network Connection:

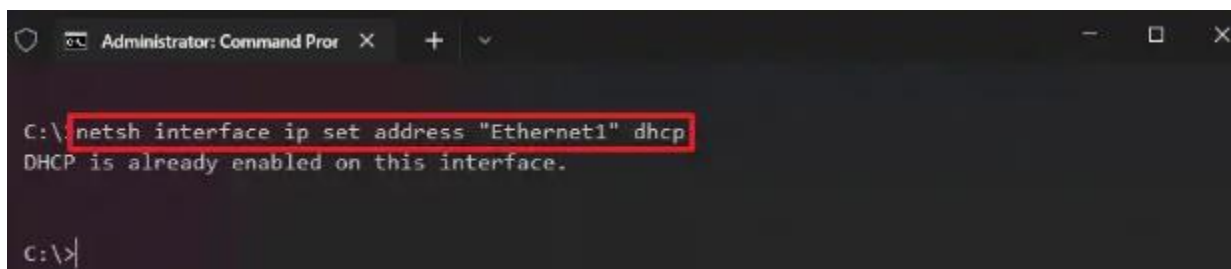
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\>
```

Step 4:- Type the following command to configure the network adapter to obtain its TCP/IP configuration using DHCP and press Enter:

```
netsh interface ip set address "Ethernet1" dhcp
```

In the command, make sure to change “Ethernet1” for the adapter’s name that you want to configure.



```
Administrator: Command Prom...
C:\>netsh interface ip set address "Ethernet1" dhcp
DHCP is already enabled on this interface.

C:\>
```

After completing the steps, the network adapter will stop using a static IP address, and it’ll obtain a configuration automatically from the DHCP server.

- **Change to dynamic IP address (DHCP) from PowerShell**

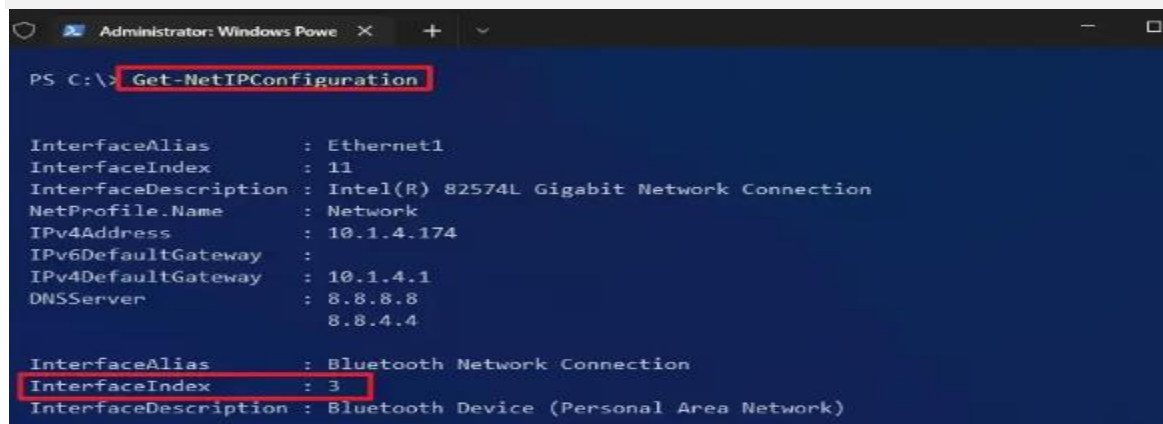
To remove a static IP and DNS addresses to use a dynamic configuration using PowerShell, use these steps:

Step 1:- Open Start.

Step 2:- Search for PowerShell, right-click the top result, and select the Run as administrator option.

Step 3:- Type the following command to note the “InterfaceIndex” number for the network adapter and press Enter:

```
Get-NetIPConfiguration
```



```

PS C:\> Get-NetIPConfiguration

InterfaceAlias      : Ethernet1
InterfaceIndex      : 11
InterfaceDescription : Intel(R) 82574L Gigabit Network Connection
NetProfile.Name     : Network
IPv4Address         : 10.1.4.174
IPv6DefaultGateway  :
IPv4DefaultGateway  : 10.1.4.1
DNSServer           : 8.8.8.8
                   : 8.8.4.4

InterfaceAlias      : Bluetooth Network Connection
InterfaceIndex      : 3
InterfaceDescription : Bluetooth Device (Personal Area Network)
  
```

Step 4:- Type the following command to enable the network adapter to obtain its TCP/IP configuration using DHCP and press Enter:

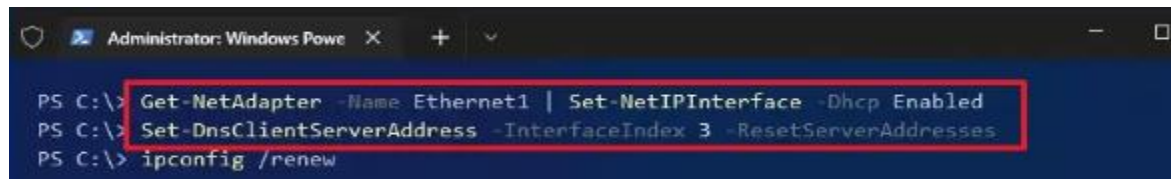
```
Get-NetAdapter -Name Ethernet1 | Set-NetIPInterface -Dhcp Enabled
```

In the command, make sure to change “Ethernet0” for the adapter’s name that you want to configure.

Step 5:- Type the following command to enable the network adapter to obtain its DNS configuration using DHCP and press Enter:

```
Set-DnsClientServerAddress -InterfaceIndex 3 -ResetServerAddresses
```

In the command, change “3” for the InterfaceIndex for the adapter to configure.



```

PS C:\> Get-NetAdapter -Name Ethernet1 | Set-NetIPInterface -Dhcp Enabled
PS C:\> Set-DnsClientServerAddress -InterfaceIndex 3 -ResetServerAddresses
PS C:\> ipconfig /renew
  
```

**Note:** - Once you complete the steps, the IP and DNS addresses will be reset from the adapter, and your computer will receive a new dynamic configuration from DHCP.

- **Change to dynamic IP address (DHCP) from Control Panel**

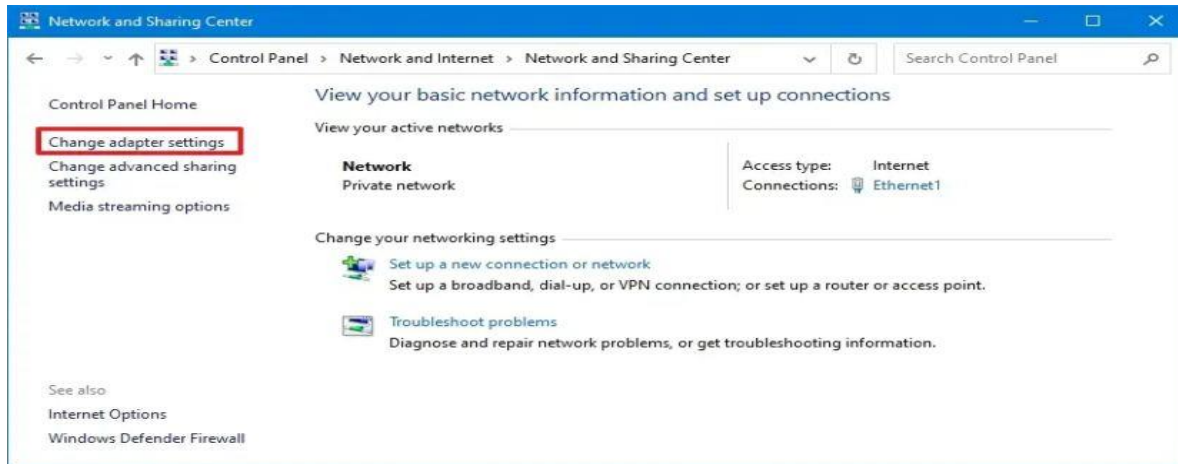
To configure a network adapter to use a dynamic IP address using Control Panel, use these steps:

Step 1:- Open Control Panel.

Step 2:- Click on Network and Internet.

Step 3:- Click on Network and Sharing Center.

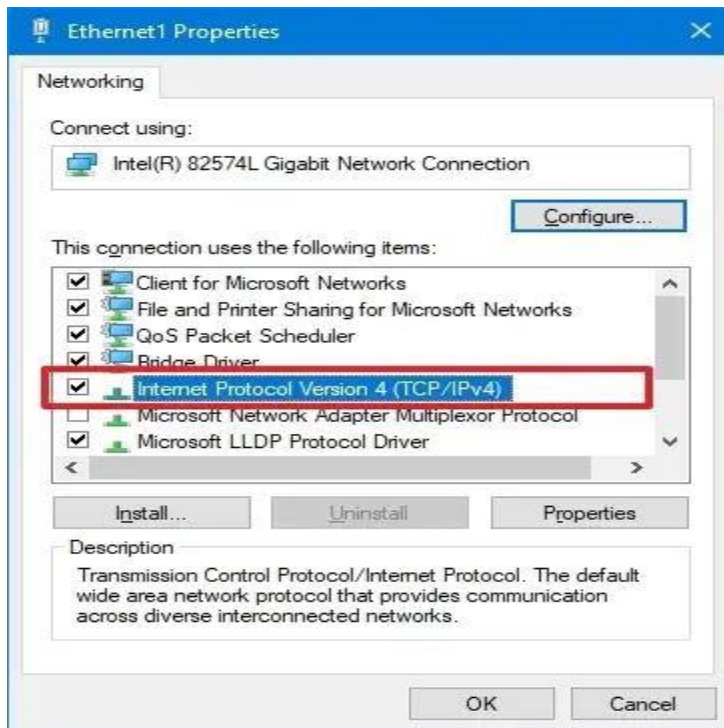
Step 4:- On the left pane, click the “Change adapter settings” option.



Step 5:- Right-click the network adapter and select the Properties option.

Step 6:- Select the “Internet Protocol Version 4 (TCP/IPv4)” option.

Step 7:- Click the Properties button.





Step 8:- Select the “Obtain an IP address automatically” option.

Step 9:- Select the “Obtain the following DNS server address automatically” option.



Step 10:- Click the OK button.

**Note:-** After completing the steps, the statically assigned TCP/IP configuration will no longer be available, and the computer will automatically request a dynamic network configuration from the network.

### Task 3:- Test the configuration of IP address

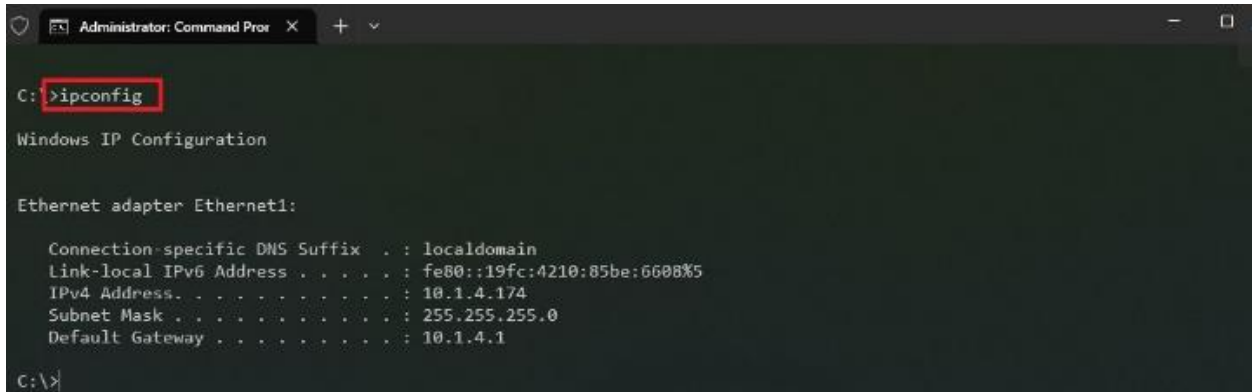
To get started with ipconfig on Windows 10, use these steps:

Step 1:- Open **Start**.

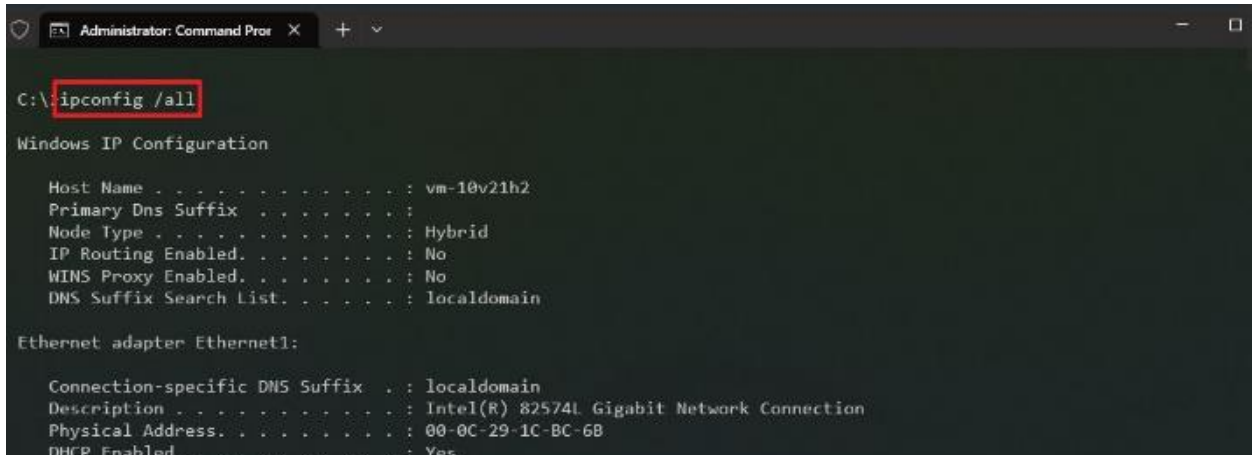
Step 2:- Search for **Command Prompt**, right-click the top result, and select the **Run as administrator** option.

Step 3:- Type the following command to view a summary of the TCP/IP network configuration and press **Enter**: *ipconfig*

- **Quick tip:** In Command Prompt, you can use the CLS command to clear the screen after you no longer need the information to continue running commands without clutter.



Step 4: -Type the following command to view the complete TCP/IP network configuration and press **Enter**: *ipconfig /all*.



Once you complete the steps, you will have an overview of the PC's entire TCP/IP configuration.

### Refresh network settings

To release and renew the network configuration with Command Prompt, use these steps:

Step 1: Open **Start**.

Step 2:- Search for **Command Prompt**, right-click the top result, and select the **Run as administrator** option.

Step 3:- Type the following command to remove the current network configuration and press **Enter**: *ipconfig /release*

Step 4:- Type the following command to reconfigure the network configuration and press **Enter**: *ipconfig /renew*



```

Administrator: Command Prom...
C:\> ipconfig /release

Windows IP Configuration

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::19fc:4210:85be:6608%5
    Default Gateway . . . . . : 

C:\> ipconfig /renew

Windows IP Configuration

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::19fc:4210:85be:6608%5
    IPv4 Address. . . . . : 10.1.4.174
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.4.1

C:\>
  
```

After you complete the steps, the first command will clear the current configuration, and the second command will fetch new settings from the DHCP server to resolve connectivity issues. If the dynamically assigned settings have not expired in the server, it is common to see the same IP address reconfigured on the device.

### Refresh DNS settings

To flush and rebuild the current DNS cache entries on Windows 10, use these steps:

Step 1:- Open **Start**.

Step 2:- Search for **Command Prompt**, right-click the top result, and select the **Run as administrator** option.

Step 3:- Type the following command to clear the DNS system cache on the device and press **Enter**: *ipconfig /flushdns*

```

Administrator: Command Prom...
C:\> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\>
  
```

Once you complete the steps, the entries stored in the DNS cache of Windows 10 will be deleted and refreshed. Usually, this command will come in handy when you cannot connect to another computer or website using the host or domain name due to outdated information in the local cache.

## LAP Test

Task 1:- assign the following IP address for your computer

- IP: - 192.168.10.12
- Subnet mask : - 255.255.255.0
- Default IP address: - 192.168.0.220

Task 2:- Connect your computer with internet connection and assign dynamic IP address.

Task 3:- using configuration test commands check the IP address of your computer assigned on task 2.

## Unit Two: Network protocols application

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Common network protocol applications
- Evaluating user requirement and recommend network-protocol services
- Applying IP addressing scheme
- Network layers

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Understand common network protocol applications
- Evaluate user requirement and recommend network-protocol services
- Apply IP addressing scheme
- Understand Network layers

## 2. Introduction to network protocol applications

Network protocol applications refer to the specific software or programs that utilize network protocols to perform various tasks or enable specific functionalities within a computer network. These applications are designed to communicate, exchange data, and provide services over the network by adhering to standardized protocols.

### 2.1 Common network protocol applications

It seems like you might be looking for information on how network protocols are applied in real-world scenarios or applications. Let us explore some practical applications of network protocols:

#### 1. Web Browsing (HTTP/HTTPS):

- **Protocol:** HTTP (Hypertext Transfer Protocol) and its secure version HTTPS are fundamental for web browsing. When you access a website, your browser communicates with the web server using these protocols to request and receive web pages.

#### 2. Email Communication (SMTP, POP3, IMAP):

- **Protocols:** SMTP (Simple Mail Transfer Protocol) is used for sending emails, while POP3 (Post Office Protocol) and IMAP (Internet Message Access Protocol) are used for retrieving emails from mail servers. These protocols enable email communication between clients and servers.

#### 3. File Transfer (FTP, SFTP):

- **Protocols:** FTP (File Transfer Protocol) and its secure version SFTP (SSH File Transfer Protocol) are used for transferring files between computers. These protocols are commonly used for uploading and downloading files to and from servers.

#### 4. Remote Login (SSH):

- **Protocol:** SSH (Secure Shell) is used for secure remote login to a computer or server. It provides a secure way to access and manage remote systems over an unsecured network.

#### 5. Voice and Video Calls (VoIP, RTP):

- **Protocols:** VoIP (Voice over Internet Protocol) is a technology that enables voice communication over the internet. RTP (Real-Time Transport Protocol) is often used to transmit audio and video in real-time during VoIP calls.

#### 6. Domain Name Resolution (DNS):

- **Protocol:** DNS (Domain Name System) translates human-readable domain names into IP addresses. This is crucial for accessing websites using domain names rather than numerical IP addresses.
7. **Network Management (SNMP):**
- **Protocol:** SNMP (Simple Network Management Protocol) is used for monitoring and managing network devices. It allows administrators to collect information, configure devices, and receive notifications about network events.
8. **Instant Messaging (XMPP, IRC):**
- **Protocols:** XMPP (Extensible Messaging and Presence Protocol) and IRC (Internet Relay Chat) are protocols used for real-time messaging and chat applications. They enable users to send messages, join chat rooms, and share files.
9. **Video Streaming (RTSP, HLS):**
- **Protocols:** RTSP (Real Time Streaming Protocol) and HLS (HTTP Live Streaming) are used for streaming audio and video content over the internet. They facilitate the efficient delivery of multimedia content to end-users.
10. **Database Communication (JDBC, ODBC):**
- **Protocols:** JDBC (Java Database Connectivity) and ODBC (Open Database Connectivity) are protocols that enable communication between applications and databases. They allow applications to query, update, and manage data in databases.

These are just a few examples, and there are many other network protocols designed for specific applications and services. The use of these protocols ensures efficient and secure communication across diverse networked environments.

OSI Model	TCP/IP Hierarchy	Protocols				
7 <sup>th</sup> Application Layer	Application Layer	HTTP	SMTP	POP3	FTP	...
6 <sup>th</sup> Presentation Layer						
5 <sup>th</sup> Session Layer						
4 <sup>th</sup> Transport Layer	Transport Layer	TCP		UDP		
3 <sup>rd</sup> Network Layer	Network Layer	IP				ICMP
2 <sup>nd</sup> Link Layer	Link Layer	ARP RARP Ethernet		PPP	...	
1 <sup>st</sup> Physical Layer						

Figure 2. 1 Protocol hierarchies

## 2.2 Evaluating user requirement and recommend network-protocol services

To recommend network protocol services based on user requirements, it's crucial to understand the specific needs and objectives of the user or organization. Here is a general process to evaluate user requirements and recommend appropriate network protocol services:

### 1. Gather User Requirements:

- **Interview:** Engage with the user or organization to understand their specific requirements. Ask questions about the nature of their network, the type of applications they use, the level of security needed, scalability requirements, and any specific industry standards or regulations they must comply with.

### 2. Identify Key Applications and Services:

- **List Applications:** Identify the key applications and services that the user relies on. For example, if they heavily use web applications, email, file transfer, or video conferencing, this will influence the choice of protocols.

### 3. Consider Security Requirements:

- **Security Policies:** Understand the user's security policies and requirements. If strong encryption and secure data transfer are critical, protocols like HTTPS, SFTP, and SSH may be preferred.

### 4. Evaluate Performance Needs:

- **Bandwidth Requirements:** Assess the required network performance in terms of bandwidth, latency, and reliability. For high-performance requirements, protocols like TCP/IP, UDP, and specialized protocols for streaming may be considered.
5. **Account for Scalability:**
    - **Scalability Needs:** Determine if the network is expected to scale in the future. Protocols and services that support scalability and load balancing may be preferred in such cases.
  6. **Review Compatibility and Integration:**
    - **Existing Infrastructure:** Consider the existing network infrastructure and ensure that the recommended protocols are compatible and easily integrable with the current systems and devices.
  7. **Compliance with Standards:**
    - **Regulatory Compliance:** If the user operates in an industry with specific regulations (e.g., healthcare, finance), ensure that the recommended protocols comply with relevant standards and regulations.
  8. **Cost Considerations:**
    - **Budget Constraints:** Take into account the budget constraints of the user. Some protocols and services may have associated costs, and it's essential to recommend solutions that align with the budget.
  9. **User Experience and Accessibility:**
    - **User Interface:** Consider the user experience and ease of use. Choose protocols that provide a seamless and user-friendly experience for both administrators and end-users.
  10. **Future Expansion and Technology Trends:**
    - **Technology Trends:** Consider emerging technologies and trends in networking. Ensure that the recommended protocols align with future expansion plans and technological advancements.

### 2.3 Applying IP addressing scheme

Applying an IP addressing scheme involves assigning IP addresses to devices on a network in a structured and organized manner. This ensures efficient use of IP addresses, simplifies network management, and facilitates troubleshooting. Below are the general steps and considerations for applying an IP addressing scheme:

Page 36 of 46	Ministry of Labor and Skills Author/Copyright	Install and Manage Network Protocols Level - III	Version -1 November, 2023
---------------	--	---	------------------------------

## Applying an IP Addressing Scheme:

### 1. Define Network Requirements:

- Understand the size and requirements of your network.
- Determine the number of subnets needed based on different departments, physical locations, or functional requirements.

### 2. Choose IP Address Classes:

- Decide whether to use IPv4 or IPv6 based on the network's requirements. Most networks currently use IPv4.

### 3. Select IP Addressing Scheme Type:

- Choose between static IP addressing and dynamic IP addressing (e.g., DHCP). In many cases, a combination of both is used.

### 4. Divide the Network into Subnets:

- Divide the network into subnets based on logical or physical segmentation. This could be done by departments, floors, or geographical locations.

### 5. Choose Subnet Mask:

- Determine the appropriate subnet mask for each subnet. This is crucial for defining the range of IP addresses within a subnet.

### 6. Define IP Address Range for Each Subnet:

- Assign a range of IP addresses to each subnet. Specify the starting and ending addresses for hosts within the subnet.

### 7. Assign Static IP Addresses:

- For critical devices or servers, consider assigning static IP addresses to ensure consistency.

### 8. Implement Dynamic Host Configuration Protocol (DHCP):

- If using DHCP, configure the DHCP server to dynamically assign IP addresses to devices on the network.

### 9. Document the IP Addressing Scheme:

- Maintain clear documentation of the IP addressing scheme, including subnet details, assigned IP ranges, static IP assignments, and any reserved addresses.

### 10. Implement Network Address Translation (NAT) if Needed:

- If the network is connected to the internet, consider implementing NAT to allow multiple devices on the local network to share a single public IP address.



### 11. Consider VLANs (Virtual Local Area Networks):

- If using VLANs, coordinate IP addressing to match VLAN segmentation. VLANs enable logical segmentation within a physical network.

### 12. Test the IP Addressing Scheme:

- Before deploying the scheme across the entire network, conduct testing in a controlled environment to identify and resolve any issues.

### 13. Monitor and Update:

- Regularly monitor the IP addressing scheme for any changes, additions, or modifications. Update documentation accordingly.

- **Example:**

Let's consider a simplified example for a small office:

- **Network Size:** 192.168.0.0/24 (Class C)
- **Subnets:**
  - HR: 192.168.0.0/26 (192.168.0.1 to 192.168.0.62)
  - Sales: 192.168.0.64/26 (192.168.0.65 to 192.168.0.126)
  - IT: 192.168.0.128/26 (192.168.0.129 to 192.168.0.190)
- **Static IP Addresses:**
  - DHCP Server: 192.168.0.2
  - Gateway Router: 192.168.0.1
  - DNS Server: 192.168.0.10

Remember, the actual scheme will depend on the specific requirements and structure of your network. Regularly review and update the addressing scheme as the network evolves.

## 2.4. Network layers

The OSI (Open Systems Interconnection) model and the TCP/IP model are two widely used frameworks for understanding and implementing network protocols. Both models divide the networking process into layers, each responsible for specific functions. Here's an overview of the layers in both models:

### 1. OSI Model:

#### 1. Physical Layer (Layer 1):

- Concerned with the physical connection between devices.
- Deals with transmission and reception of raw bit streams over a physical medium.

Page 38 of 46	Ministry of Labor and Skills Author/Copyright	Install and Manage Network Protocols Level - III	Version -1 November, 2023
---------------	--	---	------------------------------

- Examples: Cables, connectors, hubs.
2. **Data Link Layer (Layer 2):**
    - Responsible for framing, addressing, and error detection in the data link.
    - Ensures data integrity and controls access to the physical medium.
    - Examples: Ethernet, MAC addresses.
  3. **Network Layer (Layer 3):**
    - Handles logical addressing and routing of data between devices on different networks.
    - Examples: IP (Internet Protocol), routing.
  4. **Transport Layer (Layer 4):**
    - Manages end-to-end communication, segmenting, and reassembling data.
    - Provides error checking and flow control.
    - Examples: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
  5. **Session Layer (Layer 5):**
    - Establishes, maintains, and terminates sessions (dialogue) between applications.
    - Manages dialog control and synchronization.
    - Examples: NetBIOS, RPC (Remote Procedure Call).
  6. **Presentation Layer (Layer 6):**
    - Translates data between the application layer and the lower layers.
    - Handles data compression, encryption, and formatting.
    - Examples: SSL/TLS, JPEG, ASCII.
  7. **Application Layer (Layer 7):**
    - Provides network services directly to end-users or applications.
    - Supports user interfaces and network services like email and file transfer.
    - Examples: HTTP, FTP, SMTP.
2. **TCP/IP Model (Four-Layer Model):**
  3. **Link Layer (Network Interface Layer):**
    - Combines functionalities of the OSI physical and data link layers.
    - Manages hardware addressing and access to the physical medium.
  4. **Internet Layer:**
    - Equivalent to the OSI network layer.
    - Responsible for logical addressing and routing.

- Uses the Internet Protocol (IP).

#### 5. **Transport Layer:**

- Similar to the OSI transport layer.
- Manages end-to-end communication and error recovery.
- Includes TCP and UDP.

#### 6. **Application Layer:**

- Combines functionalities of the OSI session, presentation, and application layers.
- Provides network services directly to end-users.
- Includes application protocols such as HTTP, FTP, and DNS.

The TCP/IP model is more commonly referenced in practical networking, while the OSI model is often used as a conceptual framework. Both models serve as guides for understanding network communication and are essential for networking professionals in designing, implementing, and troubleshooting networks.





