Competency Based Learning Material (CBLM)

IT Support Services

Level-4

Module: Performing SOHO Networking

Code: CBLM-OU-ICT-ITSS-01-L4-V1

National Skills Development Authority
Prime Minister's Office
Government of the People's Republic of Bangladesh

Copyright

National Skills Development Authority
Prime Minister's Office
Level: 10-11, Biniyog Bhaban,
E-6 / B, Agargaon, Sher-E-Bangla Nagar Dhaka-1207, Bangladesh.
Email: ec@nsda.gov.bd
Website: www.nsda.gov.bd.
National Skills Portal: http:\\skillsportal.gov.bd

Approved by ___ th Authority meeting held on .....

How to use this Competency Based Learning Material (CBLM)

The module, Performing SOHO Networking contains training materials and activities for you to complete. These activities may be completed as part of structured classroom activities or you may be required you to work at your own pace. These activities will ask you to complete associated learning and practice activities in order to gain knowledge and skills you need to achieve the learning outcomes.

1. Review the **Learning Activity** page to understand the sequence of learning activities you will undergo. This page will serve as your road map towards the achievement of competence.

2. Read the **Information Sheets.** This will give you an understanding of the jobs or tasks you are going to learn how to do. Once you have finished reading the **Information Sheets** complete the questions in the **Self-Check.**

3. **Self-**Checks are found after each **Information Sheet**. **Self-Checks** are designed to help you know how you are progressing. If you are unable to answer the questions in the **Self-Check** you will need to re-read the relevant **Information Sheet**. Once you have completed all the questions check your answers by reading the relevant **Answer Keys** found at the end of this module.

4. Next move on to the **Job Sheets. Job Sheets** provide detailed information about *how to do the job* you are being trained in. Some **Job Sheets** will also have a series of **Activity Sheets**. These sheets have been designed to introduce you to the job step by step. This is where you will apply the new knowledge you gained by reading the Information Sheets. This is your opportunity to practice the job. You may need to practice the job or activity several times before you become competent.

5. Specification **sheets**, specifying the details of the job to be performed will be provided where appropriate.

6. A review of competency is provided on the last page to help remind if all the required assessment criteria have been met. This record is for your own information and guidance and is not an official record of competency

When working though this Module always be aware of your safety and the safety of others in the training room. Should you require assistance or clarification please consult your trainer or facilitator.

When you have satisfactorily completed all the Jobs and/or Activities outlined in this module, an assessment event will be scheduled to assess if you have achieved competency in the specified learning outcomes. You will then be ready to move onto the next Unit of Competency or Module

Table of Contents

Module Content

Unit of Competency	**Perform SOHO Networking**
Unit Code	**OU-ICT-ITSS-01-L4-V1**
Module Title	**Performing SOHO Networking**
Module Descriptor	This module covers the knowledge, skills and attitudes required to Perform SOHO Networking. It includes the task of interpreting SOHO Network, plan for SOHO Network, implementing wired SOHO network, implementing Wireless SOHO network and securing SOHO network.
Nominal Hours	50 Hours
Lerning Outcome	After completing the practice of the module, the trainees will be able to perform the following jobs: 1. Interpret SOHO network 2. Plan for SOHO network 3. Implement wired SOHO network 4. Implement wireless SOHO network 5. Secure SOHO network

Assessment Criteria:

1. SOHO Network is defined
2. Types of SOHO Network is identified
3. Functions of SOHO network is interpreted
4. Naming convention is interpreted
5. Network model is defined
6. SOHO Network equipment is identified
7. Basic purpose of LAN is identified and defined
8. Basic functions of LAN are identified and defined.
9. Small Office Home Office (SOHO) networking is designed.
10. Required tools and equipment's are identified and listed
11. Materials and consumables are identified and listed
12. Budget is prepared and documented for Network as per Requirements
13. Budget is sent to appropriate person for approval as per workplace practice
14. Configuration requirements are identified
15. Tools and equipment are selected and collected from vendor
16. Materials and consumables are collected
17. SOHO Networks is installed and configured.
18. Necessary settings for LAN are configured
19. IP assign type is selected
20. IP address is assigned

21. Computer name is ensured and workgroup name are documented and confirmed
22. Documents and file sharing setting are confirmed
23. Add Printer and enable sharing are confirmed
24. Access requirements are determined and sharing is confirmed
25. Wireless Configuration requirements are identified
26. Tools and equipment for wireless configuration are selected and collected
27. Materials and consumables are collected
28. Wireless SOHO Networks is installed and configured.
29. Necessary settings for WLAN are configured
30. IP address is Assigned as required
31. Computer name is ensured and workgroup name are documented and confirmed
32. Documents and file sharing setting are confirmed
33. Printer is added and enable sharing are confirmed
34. Access requirements are determined and sharing is confirmed.
35. Security problems for SOHO networking is interpreted
36. MAC filtering is interpreted
37. Unauthorize device is controlled
38. Default firewall is enabled

Learning Outcome-1: Interpret SOHO Network

Assessment Criteria	1. SOHO Network is defined 2. Types of SOHO Network is identified 3. Functions of SOHO network is interpreted 4. Naming convention is interpreted 5. Network model is defined 6. SOHO Network equipment is identified
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Switch 6. Router 7. Networking related Tools and accessories 8. Multimedia Projector 9. Paper, Pen, Pencil and Eraser
Contents	1 Networking ▪ Internet ▪ Intranet ▪ Extranet 2 SOHO Network 3 Types of SOHO Network 4 Functions of SOHO network 5 Naming convention ▪ NetBIOS ▪ Hierarchical naming system 6 Network model ▪ Workgroup ▪ Domain ▪ Standalone 7 SOHO Network equipment ▪ Home router ▪ Switch, Wireless Access Point, ▪ IP Telephone ▪ Alexa ▪ Google Assistant
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work

	8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning

Learning Experience-1: Interpret SOHO Network

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
1. Trainee will ask the instructor about the learning materials	1. Instructor will provide the learning materials "Interpret SOHO Network"
2. Read the Information sheet and complete the Self Checks & Check answer sheets on "Interpret SOHO Network"	2. Read Information sheet 1: Interpret SOHO Network 3. Answer Self-check 1: Interpret SOHO Network 4. Check your answer with Answer key 1: Interpret SOHO Network
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	5. Job/Task Sheet and Specification Sheet Task Sheet 1.1: Interpret Functions of SOHO Network Specification Sheet 1.1: Interpret Functions of SOHO Network

Information Sheet-1: Interpret SOHO Network

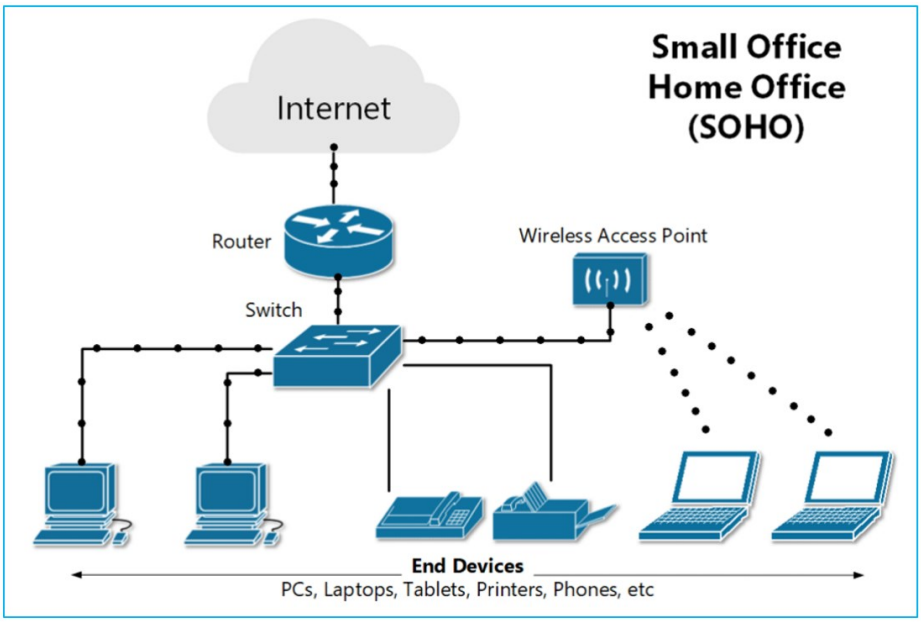
Learning Objective: After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

1.1 Networking
- Internet
- Intranet
- Extranet

1.2 SOHO Network
1.3 Types of SOHO Network
1.4 Functions of SOHO network
1.5 Naming convention
- NetBIOS
- Hierarchical naming system

1.6 Network model
- Workgroup
- Domain
- Standalone

1.7 SOHO Network equipment
- Home router
- Switch, Wireless Access Point,
- IP Telephone
- Alexa
- Google Assistant



1.1 Computer Networking

Computer networking connects computing and IoT devices, facilitating data exchange and resource sharing through established protocols to transmit information over various physical or wireless technologies.

Computing devices include laptops, desktops, servers, smartphones, tablets, and a growing number of IoT devices like cameras, door locks, doorbells, refrigerators, AV systems, thermostats, and sensors.

Aspect	Computer Networking	Computer Network
Definition	The broader field or concept of connecting computing devices together to enable communication and resource sharing.	The actual interconnected system of computing devices, peripherals, and infrastructure components that enable communication and data exchange.
Focus	Focuses on principles, technologies, and practices involved in designing, implementing, and managing networks.	Focuses on the physical or virtual infrastructure that facilitates communication and data exchange between devices.
Scope	Covers planning, setup, and maintenance.	The implemented system itself.
Activities Involved	Designing, configuring, and securing networks.	Setting up connections and managing devices.
Examples	Studying protocols, security, and network design.	Using LAN, WAN, or the Internet.

Internet, Intranet and Extranet

- **Internet**

  A worldwide network of computers and servers enabling users to access a wide range of information and services.

Figure: Internet

- **Intranet**

  Private network within an organization that allow only the authorized users to facilitating internal communication, collaboration, and operational management.

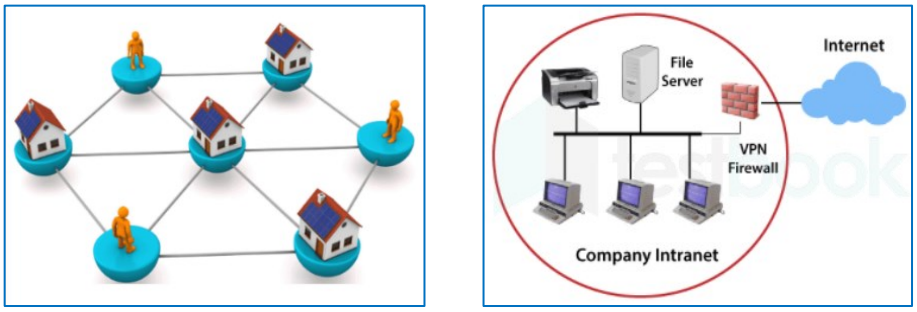


Figure: Intranet

- **Extranet**

  A controlled extension of an organization's intranet, offering limited access to external users such as customers or partners, enabling them to connect to designated sections of the intranet for collaborative communication and interaction.

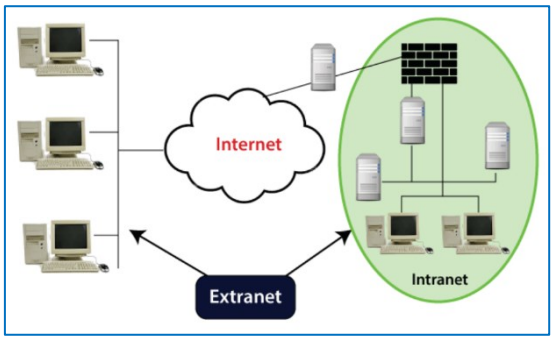


Figure: Extranet

Key difference between Internet, Intranet and Extranet:

Point of difference	Internet	Intranet	Extranet
Accessibility of network	Public	Private	Private
Coverage	All over the world.	Restricted area upto an organization.	Restricted area upto an organization and some of its stakeholders or so.
Accessibility of content	It is accessible to everyone connected.	It is accessible only to the members of organization.	Accessible only to the members of organization and external members with logins.
Purpose of the network	It's purpose is to share information throughout the world.	It's purpose is to share information throughout the organization.	It's purpose is to share information between members and external, members.
Users	General public.	Employees of the organization.	Employees of the organization which are connected.
Relation	It is the network of networks.	It is derived from Internet.	It is derived from Intranet.

1.2 SOHO Network

SOHO networks, standing for Small Office / Home Office architectures, are simple network setups primarily utilized in homes or small enterprises. They typically consist of a single device, often combining the functions of a router and a switch, providing internet access and network connectivity to connected devices such as PCs and printers.

SOHO architecture utilizes Ethernet technology to connect devices, enabling internet access through a switch/router. Devices connect via Ethernet cables such as CAT5 or CAT6. Wireless networking adds access points, providing internet access to connected devices.

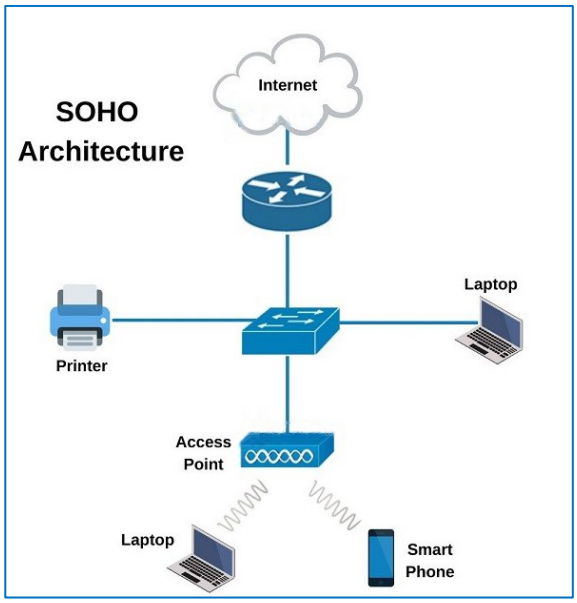


Figure: SOHO Network

A SOHO network involves setting up a local network within a smaller workspace, such as a home or small office, to enable devices to communicate and share resources. This network can be wired or wireless and usually incorporates a central router or hub that allows devices to connect and communicate.

1.3 Types of SOHO Network

There are typically two main types of SOHO networks:

i) **Wired SOHO Network:** This type of network primarily relies on physical Ethernet cables to connect devices to the network. Devices such as computers, printers, and routers are connected via Ethernet cables to a central switch or router, which provides network connectivity and internet access.

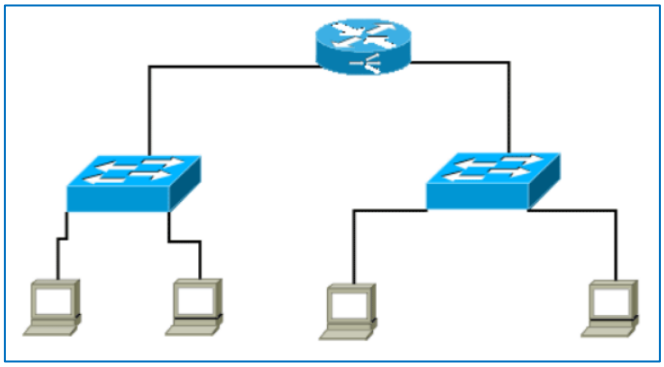


Figure: Wired SOHO Network

ii) **Wireless SOHO Network:** In this type of network, devices connect to the network wirelessly using Wi-Fi technology. A wireless router or access point broadcasts a wireless signal, allowing devices such as laptops, smartphones, tablets, and printers to connect to the network without the need for physical cables.

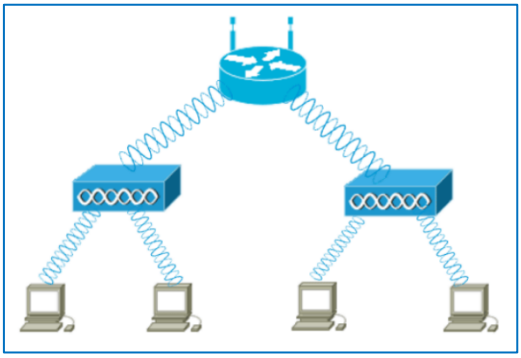
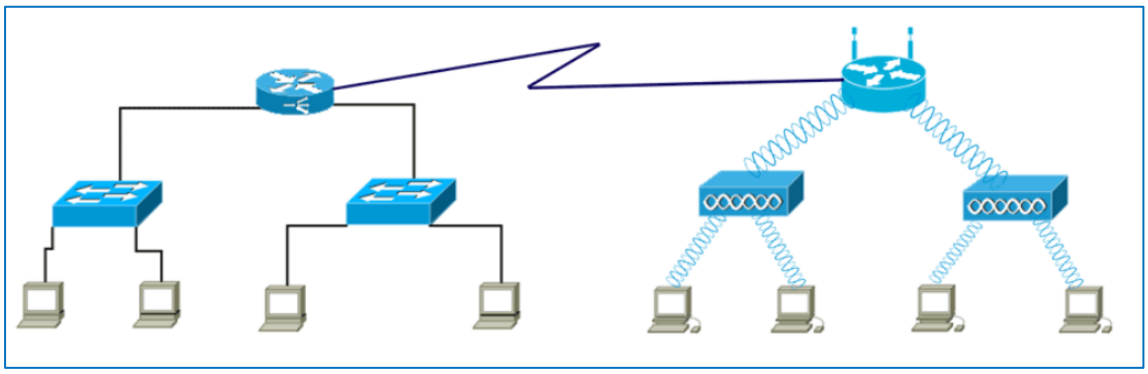


Figure: Wired SOHO Network

These two types of SOHO networks can also be combined, with some devices connected via Ethernet cables and others connecting wirelessly, providing flexibility and convenience for users.

The following image shows a SOHO Ethernet LAN combines wired and wireless connectivity.



1.4 Functions of SOHO network

The functions of a SOHO (Small Office/Home Office) network typically include:

Internet Access: Providing connectivity to the internet for browsing, email, and other online services.

File Sharing: Allowing users to share files and resources such as documents, images, and videos among connected devices.

Printer Sharing: Enabling multiple devices to use a single printer connected to the network.

Device Connectivity: Facilitating communication and data exchange between computers, smartphones, tablets, printers, and other networked devices.

Network Security: Implementing measures to protect the network and its data from unauthorized access, viruses, malware, and other cyber threats.

Wireless Connectivity: Supporting wireless connectivity for devices that cannot be connected via Ethernet cables, providing flexibility and mobility within the network.

Remote Access: Allowing users to access files, printers, and other network resources remotely from outside the network, typically through VPN (Virtual Private Network) connections.

Backup and Data Storage: Providing options for data backup and storage solutions to ensure data protection and recovery in case of system failures or disasters.

1.5 Naming convention

A naming convention is a set of rules or standards that you use to label and identify your network components, such as routers, switches, servers, cables, and ports. In this article, you will learn how to create a naming convention for network documentation that is simple, logical, and scalable.

NetBIOS: NetBIOS (Network Basic Input/Output System) is a legacy networking protocol used for communication between devices on a local area network (LAN). It was developed by IBM and later extended by Microsoft. NetBIOS provides services such as naming, session establishment, and datagram distribution.

NetBIOS naming convention follows a flat namespace, where each device on the network is identified by a single unique name of up to 16 characters. These names are not hierarchical and are often simple identifiers like "COMPUTER1" or "PRINTER".

NetBIOS computer names:

Allowed characters: NetBIOS computer names can contain all alphanumeric characters except for the extended characters that appear in the following **Disallowed characters list.** Names can contain a period, but names can not start with a period.

Disallowed characters: NetBIOS computer names should not contain the following characters:

- backslash (\)
- slash (/)
- colon (:)
- asterisk (*)
- question mark (?)
- quotation mark (")
- less than sign (<)
- greater than sign (>)
- vertical bar (|)
- Computers that are members of an Active Directory domain should not have names that contain only numerals. This is a DNS restriction.

Name length rules:

- Minimum name length: One character
- Maximum name length: 15 characters

NetBIOS domain names:

Allowed characters: NetBIOS domain names can contain all alphanumeric characters except for the extended characters that appear in the **Disallowed characters** list. Names can contain a period, but names cannot start with a period.

Disallowed characters: The DNS host name checking function verifies NetBIOS domain names. These names cannot contain the following characters:

- comma (,)
- tilde (~)
- colon (:)
- exclamation point (!)
- at sign (@)
- number sign (#)
- dollar sign ($)
- percent (%)
- caret (^)
- apostrophe (')
- period (.)
- parentheses (())
- braces ({})
- underscore (_)
- white space (blank)
- backslash (\)
- slash (/)

Name length rules:

- Minimum name length: One character
- Maximum name length: 15 characters

Hierarchical naming system: On the other hand, a hierarchical naming system organizes names into a structured hierarchy, similar to the way file systems organize files into directories and subdirectories. This approach allows for more systematic and organized naming, making it easier to manage and scale large networks.

For example, in a hierarchical naming system, devices may be named based on their location, function, or department within an organization. Names may include levels of hierarchy, separated by periods or slashes, such as "HQ.Server.Room1" or "Sales.Printer.Floor2".

1.6 Network model

The term "network model" refers to the organizational structure and management approach used to connect and administer computers and devices within a network.

Workgroup network Model: In a workgroup network model, devices are connected to a common network, but there is no centralized server controlling user accounts or resources. Each device operates independently, managing its own user accounts and security settings. Resource sharing, such as file and printer sharing, is typically done directly between devices without centralized management.

Characteristic of Workgroup Model:

- All computers are equal
- Also, knon as peer-to-peer
- Each computer maintains own set of Resources, Accounts and security information

Domain: In a domain network model, devices are organized into a centralized network infrastructure controlled by a server known as a domain controller. The domain controller manages user accounts, security policies, and network resources centrally. Users log in to the domain controller to access network resources, and centralized administration allows for easier management of security and resources across the network.

Characteristic of Domain Model:

- Centralizes all shared resources
- Single point of administrative and security control
- Simpler to manage from administrative and security standpoint
- Requires at least one domain controller (DC)

Standalone: In a standalone network model, individual devices operate independently of each other and are not connected to a larger network infrastructure. Each device functions as a standalone entity, with no centralized administration or resource sharing with other devices on the network. Standalone networks are common in home or small office environments where there is no need for centralized management or resource sharing.

1.7 SOHO Network equipment

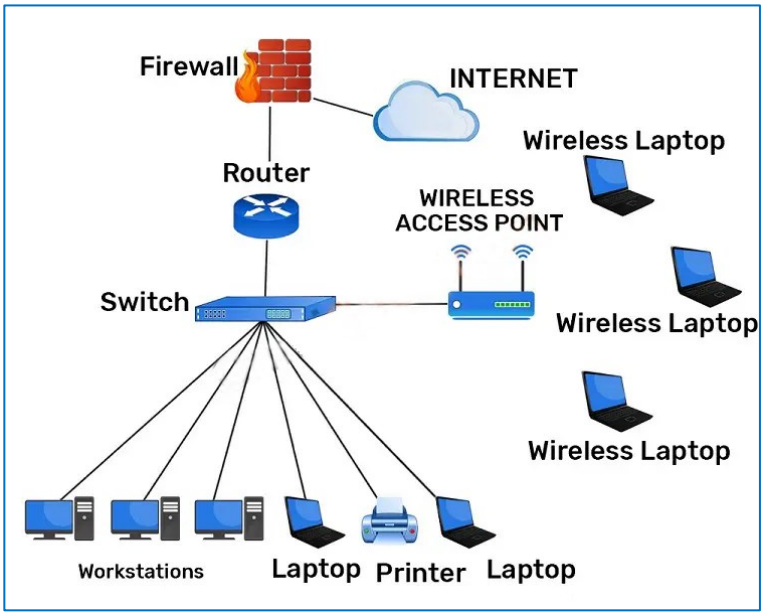


Figure: Router

Home router: A router is a networking device that connect multiple networks together. They also connect computers on those networks to the Internet. Routers enable all networked computers to share a single Internet connection, which saves money. A router acts a dispatcher. It analyzes data being sent across a network, chooses the best route for data to travel, and sends it on its way. Routers operate at Layer 3 (network layer) of the OSI model; a router uses the destination IP address in a data packet to determine where to forward the packet.

Routers:

- Connect one network to another via modem
- Route traffic between devices and network
- Transmit packets between networks
- Provides Wi-Fi functionality

Figure: Switch

Switch: A network switch connects devices together on a single computer network. A switch is also called switching hub, bridging hub, or MAC bridge. Switches use MAC addresses to forward data to the correct destination. A switch is considered a Layer 2 device,

operating at the data link layer; switches use packet switching to receive, process and forward data.

A network switch is a small hardware device that joins multiple computers together within one local area network (LAN). Switches are incapable of joining multiple networks or sharing an Internet connection. A switch acts as a controller, connecting computers, printers, and servers to a network in a building or a campus.

Switchs:

- Connect to multiple devices
- Control network access
- Monitor network usage
- Rapid communication with internal network
- Limited to devices plugged in via ethernet cable

Here are some of the most common types of network switches, with more info on each below:

- KVM Switch
- Managed Switch
- Unmanaged Switch
- Smart Switch
- PoE Switch

Wirelwss Access Point: Access points are devices that extend the wireless coverage of a network. They allow wireless devices to connect to the network and access resources from areas with weak or non-existent wireless signals. Access points are easy to install and maintain and can be used to expand the coverage of your network, making them an ideal solution for small businesses and home offices. Access points also provide scalability, allowing you to add additional units to expand the range and capacity of your network as your business grows.

Fig: Wirelwss Access Point

IP Telephone: An IP telephone, or VoIP phone, uses internet protocols to make and receive calls, offering features like call forwarding and voicemail. It's cost-effective and flexible, ideal for businesses of all sizes.

Alexa: Alexa is an artificial intelligence digital assistant developed by Amazon. Using voice commands, users can talk to Alexa to perform device shortcuts, play media, and control third-party devices and applications through Alexa Skills.

Figure: Wirelwss Access Point

Figure: Wirelwss Access Point

Google Assistant: Google Assistant is a virtual assistant developed by Google, available on a variety of devices including smartphones, smart speakers, smart displays, and other smart home devices. It utilizes artificial intelligence and natural language processing to provide users with assistance and information through voice commands and text interactions.

Google Assistant can perform tasks such as answering questions, providing weather updates, setting reminders and alarms, sending messages, making phone calls, playing music, controlling smart home devices, and more. It can also integrate with various Google services such as Gmail, Calendar, Maps, and Search to provide personalized assistance based on user preferences and habits.

Self-Check Sheet-1: Interpret SOHO Network

1. What is Computer networking?

   Answer:

2. What are the key differences between Internet, Intranet and Extranet?
   Answer:

3. Define SOHO network?
   Answer:

4. What are the functions of a SOHO network?
   Answer

5. What are the disallowed characters for NetBIOS computer names?
   Answer:

6. What are the equipments typically used for SOHO network?
   Answer:

Answer Key-1: Interpret SOHO Network

1. **What is Computer networking?**

Answer: Computer networking connects computing and IoT devices, facilitating data exchange and resource sharing through established protocols to transmit information over various physical or wireless technologies.
Computing devices include laptops, desktops, servers, smartphones, tablets, and a growing number of IoT devices like cameras, door locks, doorbells, refrigerators, AV systems, thermostats, and sensors.

2. **What are the key differences between Internet, Intranet and Extranet?**

Answer: The key difference between Internet, Intranet and Extranet are given bellow:

Point of difference	Internet	Intranet	Extranet
Accessibility of network	Public	Private	Private
Coverage	All over the world.	Restricted area upto an organization.	Restricted area upto an organization and some of its stakeholders or so.
Accessibility of content	It is accessible to everyone connected.	It is accessible only to the members of organization.	Accessible only to the members of organization and external members with logins.
Purpose of the network	It's purpose is to share information throughout the world.	It's purpose is to share information throughout the organization.	It's purpose is to share information between members and external, members.
Users	General public.	Employees of the organization.	Employees of the organization which are connected.
Relation	It is the network of networks.	It is derived from Internet.	It is derived from Intranet.

3. **Define SOHO network?**

Answer: SOHO networks, standing for Small Office / Home Office architectures, are simple network setups primarily utilized in homes or small enterprises. They typically consist of a single device, often combining the functions of a router and a switch, providing internet access and network connectivity to connected devices such as PCs and printers.

4. **What are the functions of a SOHO network?**

Answer: The functions of a SOHO network include:

- Internet access
- File and printer sharing
- Device connectivity
- Network security
- Wireless connectivity
- Remote access
- Backup and data storage.

5. **What are the disallowed characters for NetBIOS computer names?**

Answer: NetBIOS computer names can not contain the following characters:

- backslash (\)
- slash (/)
- colon (:)
- asterisk (*)
- question mark (?)
- quotation mark (")
- less than sign (<)
- greater than sign (>)
- vertical bar (|)
- Computers that are members of an Active Directory domain should not have names that contain only numerals. This is a DNS restriction.

6. **What are the equipments typically used for SOHO network?**

Answer: NetBIOS computer names can not contain the following characters:

- Computers/ workstations
- Home router
- Switch
- Wirelwss Access Point
- IP Telephone
- Alexa
- Google Assistant

Task Sheet-1.1: Interpret Functions of SOHO Network

Performance Objective: At the end of this task, the trainee should be able to Interpret Functions of SOHO Network including connectivity, resource sharing, internet access, and communication.

Working steps:

Step 1: Introduction

- Briefly introduce the topic of interpreting the functions of a SOHO network.
- Highlight the importance of understanding the core functions of SOHO networks for effective network design and management.

Step 2: Connectivity

- Discuss the role of connectivity in a SOHO network, enabling devices to communicate and share data.
- Interpret how devices within a SOHO network are connected to each other through wired (Ethernet) or wireless (Wi-Fi) connections.
- Explain the importance of reliable and stable connectivity for seamless operation of networked devices.

Step 3: Resource Sharing

- Interpret how SOHO networks facilitate resource sharing among devices, including files, printers, and internet connections.
- Discuss the use of file sharing protocols such as SMB (Server Message Block) or NFS (Network File System) for sharing files and folders across the network.
- Explain the concept of print sharing, allowing multiple devices to access and use a single printer connected to the network.
- Highlight the benefits of resource sharing in improving productivity and collaboration within a SOHO environment.

Step 4: Internet Access

- Interpret how SOHO networks provide internet access to connected devices, allowing users to browse the web, send emails, and access online services.
- Discuss the role of the router in providing internet connectivity, including functions such as NAT (Network Address Translation) and DHCP (Dynamic Host Configuration Protocol).
- Explain the importance of configuring internet access securely to protect against unauthorized access and cyber threats.

Step 5: Communication

- Interpret how SOHO networks support communication among users through email, messaging, and VoIP (Voice over Internet Protocol) services.

- Discuss the use of email servers and clients for sending and receiving emails within the network.
- Explain how messaging applications and services enable real-time communication and collaboration among users.
- Discuss the role of VoIP services in making voice calls over the internet, reducing communication costs for businesses and individuals.

Step 6: Conclusion

- Summarize the key functions of a SOHO network covered in the task, including connectivity, resource sharing, internet access, and communication.
- Emphasize the importance of reliability, security, and scalability in ensuring effective functionality of SOHO networks.
- Encourage trainees to apply their understanding of SOHO network functions in real-world scenarios and network management tasks.

Specification Sheet-1.1: Interpret Functions Of SOHO Network

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Hand Gloves	Pair	1
2	Apron	No.	1
3	Googles	No.	1
4	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Unit	Quantity
1	Presentation slides	No.	1
2	Computers and internet access	No.	10
3	Networking tools (analyzers, packet sniffers, monitoring software)	Set	1
4	Simulation software	No.	1

Necessary Equipment

Sl. No	Name of Equipment	Unit	Quantity
5	Routers	No.	1
6	Switches	No.	1
7	Computers	No.	1
8	Printers	No.	1
9	Network cables	No.	1

Necessary Materials

Sl. No.	Name of materials	Unit	Quantity
1	Handouts	No.	10
2	Training manuals or guides	No.	10
3	Presentation slides	No.	1
4	Training manuals or guides	No.	10
5	Whiteboard or flip chart	No.	1

Learning Outcome-2: Plan For SOHO Network

Assessment Criteria	1. Basic purpose of LAN is identified and defined. 2. Basic functions of LAN are identified and defined. 3. Small Office Home Office (SOHO) networking is designed. 4. Required tools and equipment's are identified and listed. 5. Materials and consumables are identified and listed. 6. Budget is prepared and documented for Network as per Requirements. 7. Budget is sent to appropriate person for approval as per workplace practice.
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Switch 6. Router 7. Networking related Tools and accessories 8. Multimedia Projector 9. Paper, Pen, Pencil and Eraser
Contents	1. Basic Networking (LAN, MAN, WAN) 2. Purpose of LAN, MAN, WAN 3. Basic functions of LAN, MAN, WAN 4. Network topology 5. Network Protocol 6. Documentation process for network address plan. 7. Host name assigning procedure 8. Small Office Home Office (SOHO) 9. Tools and equipment's required for stablishing SOHO ▪ Crimping tool ▪ Connector ▪ Boot cap ▪ Face plate modular ▪ Punching tool ▪ Screw driver set ▪ Cable tester ▪ Cable cutter ▪ Patch cord ▪ RACK ▪ Cable Tray ▪ Cable Manager ▪ Patch panel ▪ Switch ▪ Access point 10. Materials and consumables required for stablishing SOHO ▪ Cable Tag ▪ Cable tie

	▪ Cable Channel 11. Budget for Network as per Requirements
Training Methods	1 Blended 2 Discussion 3 Presentation 4 Demonstration 5 Guided Practice 6 Individual Practice 7 Project Work 8 Problem Solving 9 Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1 Written Test 2 Demonstration 3 Oral Questioning

Learning Experience-2: Plan For SOHO Network

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
4. Trainee will ask the instructor about the learning materials	6. Instructor will provide the learning materials "Plan for SOHO network"
5. Read the Information sheet and complete the Self Checks & Check answer sheets on "Plan for SOHO network"	7. Read Information sheet 1: Plan for SOHO network 8. Answer Self-check 1: Plan for SOHO network 9. Check your answer with Answer key 1: Plan for SOHO network
6. Read the Job/Task Sheet and Specification Sheet and perform job/Task	10. Job/Task Sheet and Specification Sheet Task Sheet 2.1: Prepare a Plan for SOHO network Specification Sheet 2.1: Prepare a Plan for SOHO network

Information Sheet-2: Plan For SOHO Network

Learning Objective: After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

2.1 Basic Networking (LAN, MAN, WAN)
2.2 Purpose of LAN, MAN, WAN
2.3 Basic functions of LAN, MAN, WAN
2.4 Network topology
2.5 Network Protocol
2.6 Documentation process for network address plan.
2.7 Host name assigning procedure
2.8 Small Office Home Office (SOHO)
2.9 Tools and equipment's required for stablishing SOHO

- Crimping tool
- Connector
- Boot cap
- Face plate modular
- Punching tool
- Screw driver set
- Cable tester
- Cable cutter
- Patch cord
- RACK
- Cable Tray
- Cable Manager
- Patch panel
- Switch
- Access point

2.10 Materials and consumables required for stablishing SOHO

- Cable Tag
- Cable tie
- Cable Channel

2.11 Budget for Network as per Requirements

2.1 Basic Networking (LAN, MAN, WAN)

Networking: Computer networking connects computing and IoT devices, facilitating data exchange and resource sharing through established protocols to transmit information over various physical or wireless technologies.

Computing devices include laptops, desktops, servers, smartphones, tablets, and a growing number of IoT devices like cameras, door locks, doorbells, refrigerators, AV systems, thermostats, and sensors.

Types of Computer Networks:

There are mainly five types of Computer Networks. These are:

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Personal Area Network (PAN)
- Campus Area Network (CAN)

i) Local Area Network (LAN)

A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

Regardless of size, a LAN's single defining characteristic is that it connects devices that are in a single, limited area. In contrast, a wide area network (WAN) or metropolitan area network (MAN) covers larger geographic areas. Some WANs and MANs connect many LANs together.

WLAN: A Wireless Local Area Network, or WLAN, operates on similar principles as LANs, but with the added convenience of wireless technology. WLANs eliminate the need for Ethernet cables, making them a versatile choice for businesses and homes.

Just like LANs, WLANs support various applications, including data transfer, internet access, and seamless connectivity between devices.

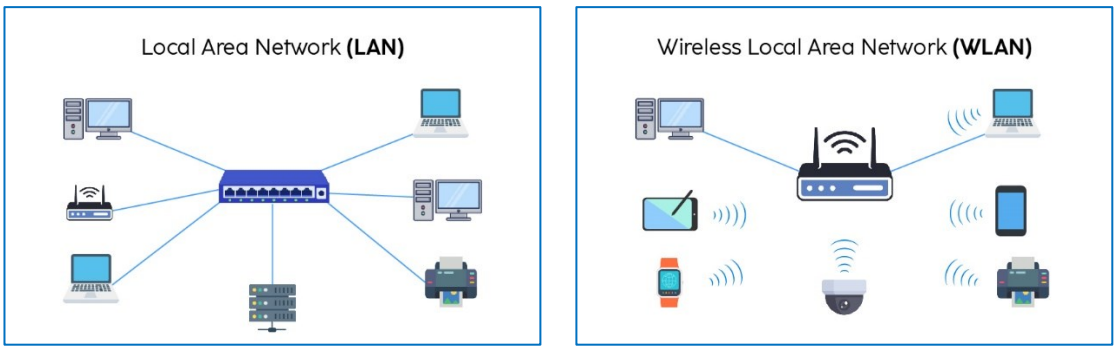


Figure: LAN

ii) Metropolitan Area Network (MAN)

A Metropolitan Area Network (MAN) is a network spanning a city, connecting multiple LANs and WANs to facilitate high-speed data communication and resource sharing. It serves to link LANs within a city, enabling the exchange of data and sharing of resources. MANs cover several kilometers, providing faster connectivity than LANs but smaller than WANs, typically operating at speeds in Mbps. MANs are complex to design and maintain due to their intricate architecture.

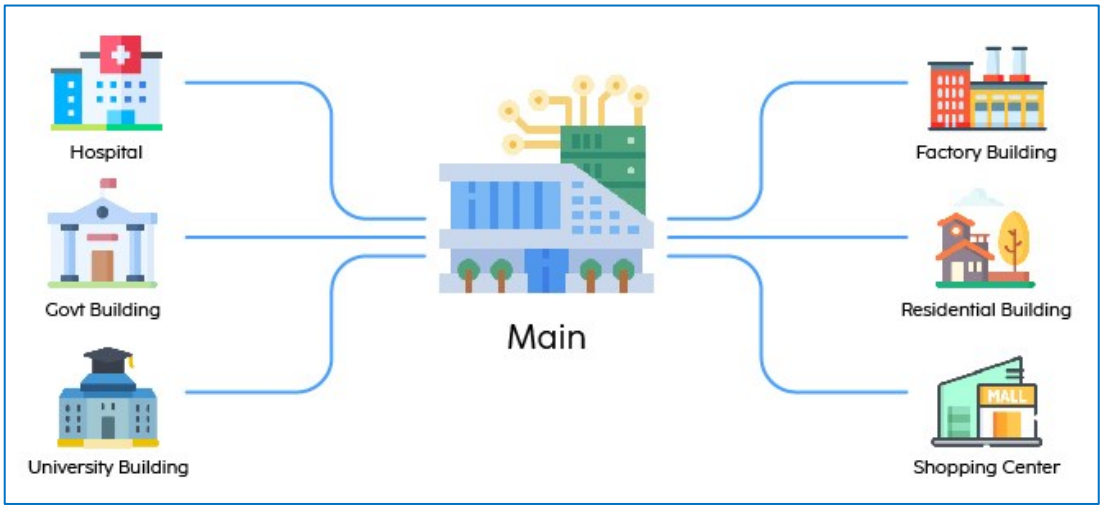


Figure: Metropolitan Area Network (MAN)

iii) Wide Area Network (WAN)

A WAN extends over a large geographical area and connects individual users or multiple LANs. The Internet can be considered a WAN. Large organizations use WANs to connect their various sites, remote employees, suppliers, and data centers so they can run applications and access necessary data.

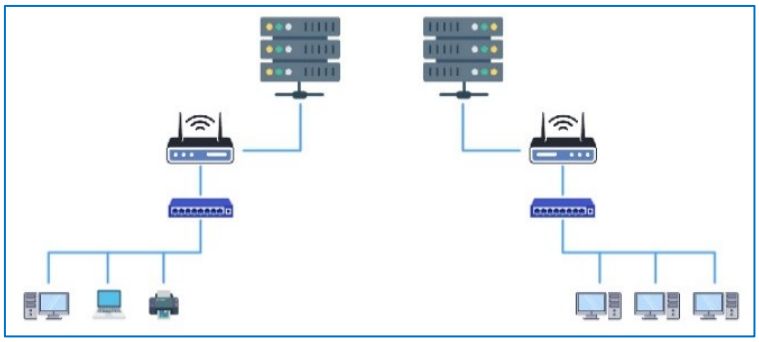


Figure: Wide Area Network (WAN

Physical connectivity in WANs can be achieved by leased lines, cellular connections, satellite links, and other means.

iv) Personal Area Network (PAN)

A Personal Area Network, or PAN, is the most fundamental type of network, primarily designed for personal use. It typically encompasses devices such as wireless modems, a couple of computers, mobile phones, printers, and more.

Figure: Personal Area Network (PAN)

The scope of a PAN is relatively small, usually limited to a single individual within a specific building. PANs are known for their inherent security and are an excellent choice for small, controlled areas where users can seamlessly connect their devices for sharing and communication.

v) Campus Area Network (CAN)

Campus Area Networks (CANs) extend beyond LAN boundaries, making them ideal for university campuses, school districts, and small business offices. They facilitate resource sharing and communication across multiple nearby buildings, enhancing productivity and data accessibility.

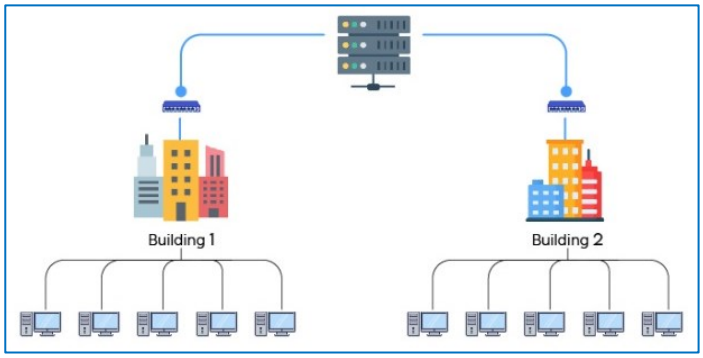


Figure: Campus Area Network (CAN)

2.2 Purpose of LAN, MAN, WAN

The main purposes of LANs (Local Area Networks) include

- Resource sharing
- Communication
- Fast data transfer
- Centralized management
- Cost efficiency
- Increased productivity
- Security

The main purposes of a Metropolitan Area Network (MAN)

- Connect multiple LANs within a city.
- Facilitate high-speed data communication.
- Enable resource sharing across a city.
- Provide internet access to users and organizations.

- Support bandwidth-intensive applications.
- Enhance connectivity for local businesses and institutions.
- Promote collaboration and economic development within the metropolitan area.

The main purposes of a Wide Area Network (WAN)

- Connect geographically dispersed locations.
- Facilitate global connectivity.
- Support centralized services.
- Enable remote access.
- Enhance disaster recovery and business continuity.
- Support multimedia applications.
- Promote collaboration and productivity.

2.3 Basic functions of LAN, MAN, WAN

Basic Functions of LAN (Local Area Network)

- Connects devices within a limited area.
- Facilitates resource sharing and fast communication.
- Provides centralized management of network resources.
- Supports local applications and services.

Basic Functions MAN (Metropolitan Area Network)

- Connects multiple LANs within a city or metropolitan area.
- Facilitates high-speed data communication and collaboration.
- Provides internet access and connectivity services.
- Supports applications requiring higher bandwidth.

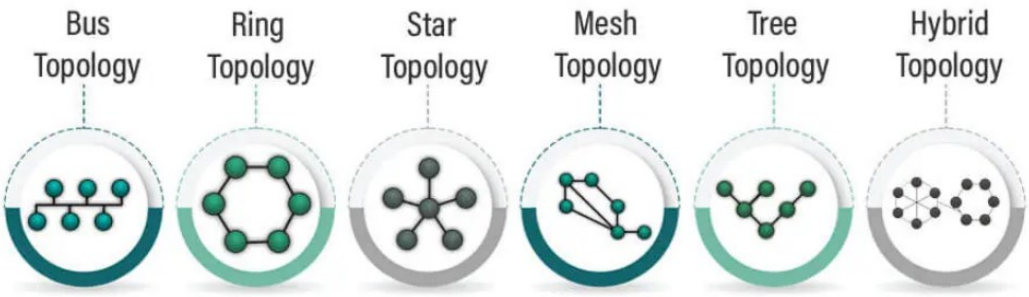
Basic Functions WAN (Wide Area Network)

- Connects multiple LANs within a city.
- Facilitates high-speed data communication and collaboration.
- Provides internet access and connectivity services.
- Supports applications requiring higher bandwidth.

2.4 Network Topology

Network Topology: Network topology is used to describe the physical and logical structure of a network. It maps the way different nodes on a network--including switches and routers--are placed and interconnected, as well as how data flows. Diagramming the locations of endpoints and service requirements helps determine the best placement for each node to optimize traffic flows.

Type of Network Topology:



Bus Topology: The bus topology connects each device on the network to a common main cable, creating a single communication path for all nodes. One point transmits data along a single route to another point. We cannot transmit data in both ways. Linear Bus Topology is the term used for this topology when it has exactly two endpoints and is primarily utilized for small networks.

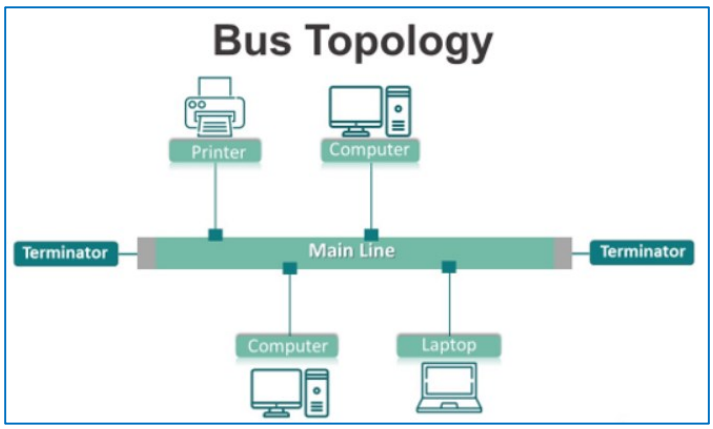


Figure: Bus Topology

Ring Topology: The devices in a ring topology, such as computers, printers, or servers, are interconnected in a circular or ring-like pattern, which forms a closed loop. Two other devices link each device in the Ring topology., positioned on either side. The last device in the chain connects to the first device, completing the circuit. Each device in a ring topology is linked to two other devices, one on either side, forming a continuous ring or loop. In a ring topology, data is transmitted in one direction around the circle, with each device on the network reading and passing on the data until it reaches its destination.

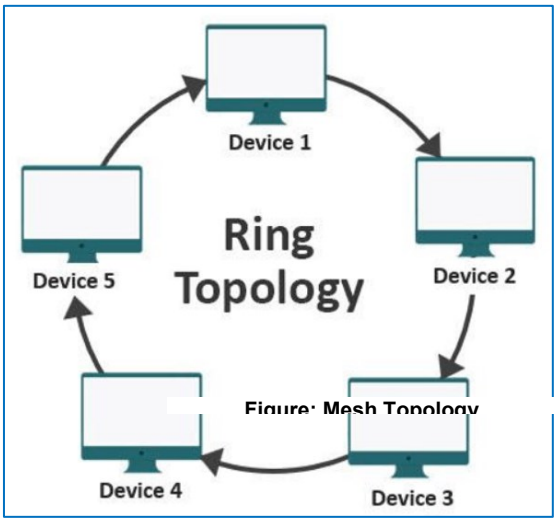


Figure: Ring Topology

Star Topology: In a star topology network, all devices directly link to a central switch or hub, serving as the central connection point. In this topology, Devices transmit data through the central hub, which then distributes the data to all devices connected. Hubs can either be active or passive, with active hubs containing repeaters and passive hubs being classified as non-intelligent nodes. Each node is connected directly to a central node, which serves as a repeater during data transmission.

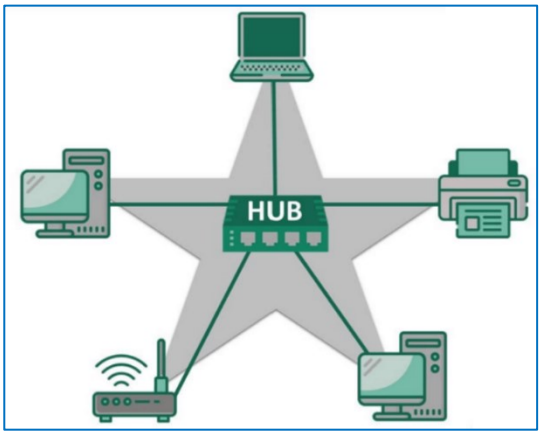


Figure: Star Topology

Mesh Topology:

Network channels connect each node to all the other nodes in a mesh topology. Mesh topology is a point-to-point connection, which means that there are multiple paths that data can take between any two devices, providing redundancy and fault tolerance in case of a network failure.

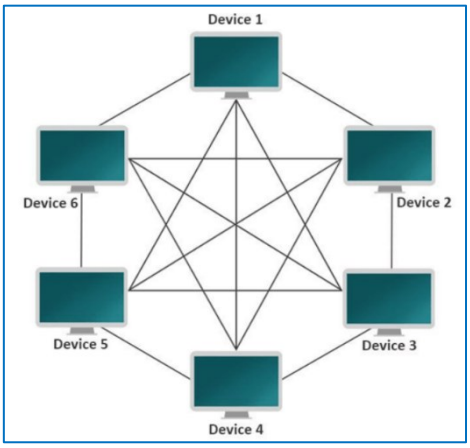


Figure: Mesh Topology

The mesh topology supports two data transmission techniques: routing and flooding. The routing technique equips the nodes with routing logic, such as selecting the shortest distance path to the destination node or avoiding routes with broken connections. On the other hand, the flooding technique involves broadcasting the data to all network nodes, eliminating the need for the routing logic. While this technique enhances the network's robustness, it may also generate unwanted network traffic and result in a heavy load on the network.

Tree Topology:

A tree topology consists of a hierarchical structure that resembles a tree. In this type of network topology, a central node, also known as the root node, connects to one or more nodes, which in turn connect to additional nodes.

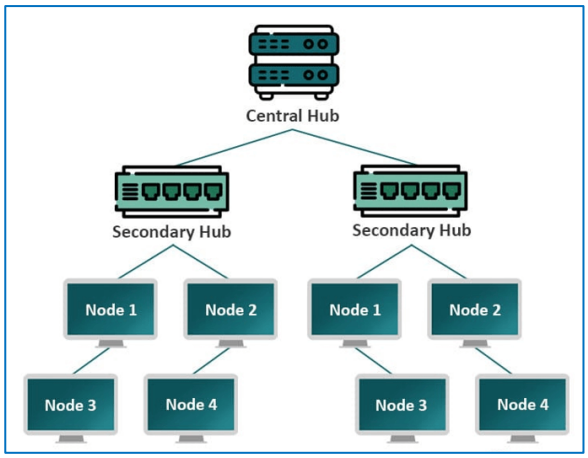


Figure: Tree Topology

In a tree topology, "level 1" nodes refer to the nodes directly connected to the root node, while nodes connected to level 1 nodes are referred to as "level 2" nodes, and so on. This hierarchical structure can expand to multiple levels, creating a large and complex network.

Hybrid Topology:

Hybrid topology refers to combining two or more different network topologies. It combines the advantages of each topology to create a more robust and flexible network infrastructure.

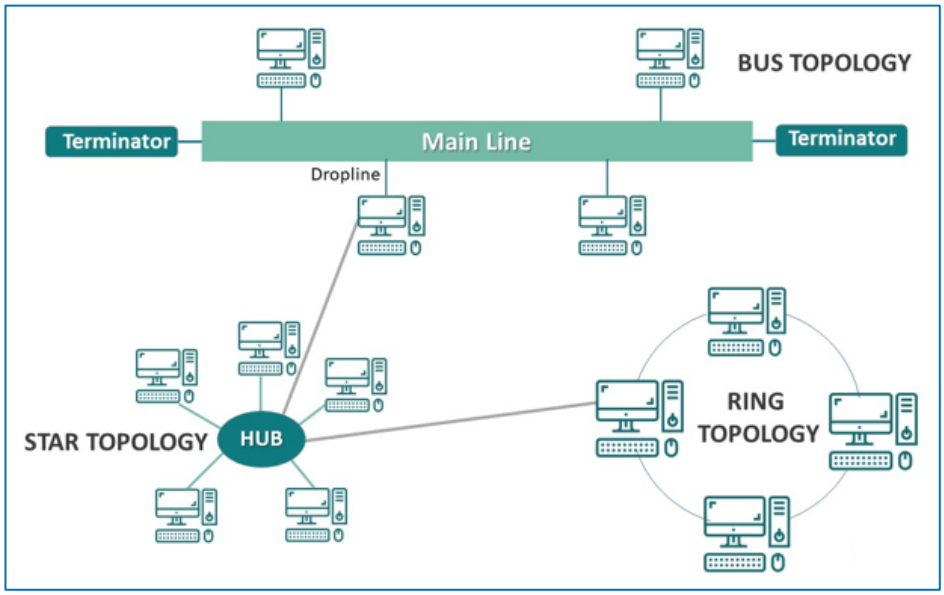


Figure: Hybrid Topology

2.5 Network Protocol

A network protocol is a set of rules that govern data communication between different devices in the network. It determines what is being communicated, how it is being communicated, and when it is being communicated. It permits connected devices to communicate with each other, irrespective of internal and structural differences.

some important network protocols:

Some protocols are:

TCP/IP (Transmission Control Protocol/Internet Protocol):

- Widely used suite of protocols for internet communication.
- TCP ensures reliable data delivery by establishing a connection, sequencing data packets, and retransmitting lost packets.
- IP handles addressing and routing of data packets across networks.
- Essential for communication between devices on the internet.

HTTP (Hypertext Transfer Protocol):

- Standard protocol for transmitting web pages and other resources on the World Wide Web.
- Facilitates communication between web servers and clients (web browsers).
- Defines how messages are formatted and transmitted, including requests from clients and responses from servers.

HTTPS (Hypertext Transfer Protocol Secure):

- Secure version of HTTP that encrypts data exchanged between a web server and a client.
- Provides confidentiality and integrity of data transmitted over the internet.
- Utilizes SSL/TLS encryption protocols to establish a secure connection.

DNS (Domain Name System):

- Converts domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) used by computers to locate resources on the internet.
- Facilitates navigation and access to websites by translating human-readable domain names into machine-readable IP addresses.
- Hierarchical distributed system that includes DNS servers responsible for different domains.

DHCP (Dynamic Host Configuration Protocol):

- Automates the assignment of IP addresses, subnet masks, and other network configuration parameters to devices on a network.
- Allows devices to obtain network configuration dynamically without manual intervention.
- Reduces administrative overhead and simplifies network management.

FTP (File Transfer Protocol):

- Standard protocol for transferring files between a client and a server on a computer network.
- Supports various operations such as uploading, downloading, renaming, and deleting files.

- Can operate in either active or passive mode for data transfer.

SMTP (Simple Mail Transfer Protocol):

- Standard protocol for sending and relaying email messages between email servers.
- Defines how email messages are formatted, transmitted, and delivered to recipient mail servers.

POP3 (Post Office Protocol version 3):

- Protocol used by email clients to retrieve email messages from a mail server.
- Typically downloads messages from the server to the client's device and deletes them from the server.

IMAP (Internet Message Access Protocol):

- Protocol used by email clients to access and manage email messages stored on a mail server.
- Allows users to view, organize, and manipulate messages without downloading them to the client device.

SSH (Secure Shell):

- Protocol for secure remote access and control of a computer or server over an insecure network.
- Encrypts data exchanged between the client and server, providing confidentiality and integrity.

SSL/TLS (Secure Sockets Layer/Transport Layer Security):

- Protocols used to secure communication over the internet, commonly used in HTTPS, SMTPS, and other secure applications.
- Provide encryption, authentication, and data integrity to ensure secure data transmission.

ARP (Address Resolution Protocol):

- Protocol used to map IP addresses to MAC addresses on a local network.
- Allows devices to determine the hardware address associated with an IP address for communication within the same network segment.

Important Network protocol at a glance:

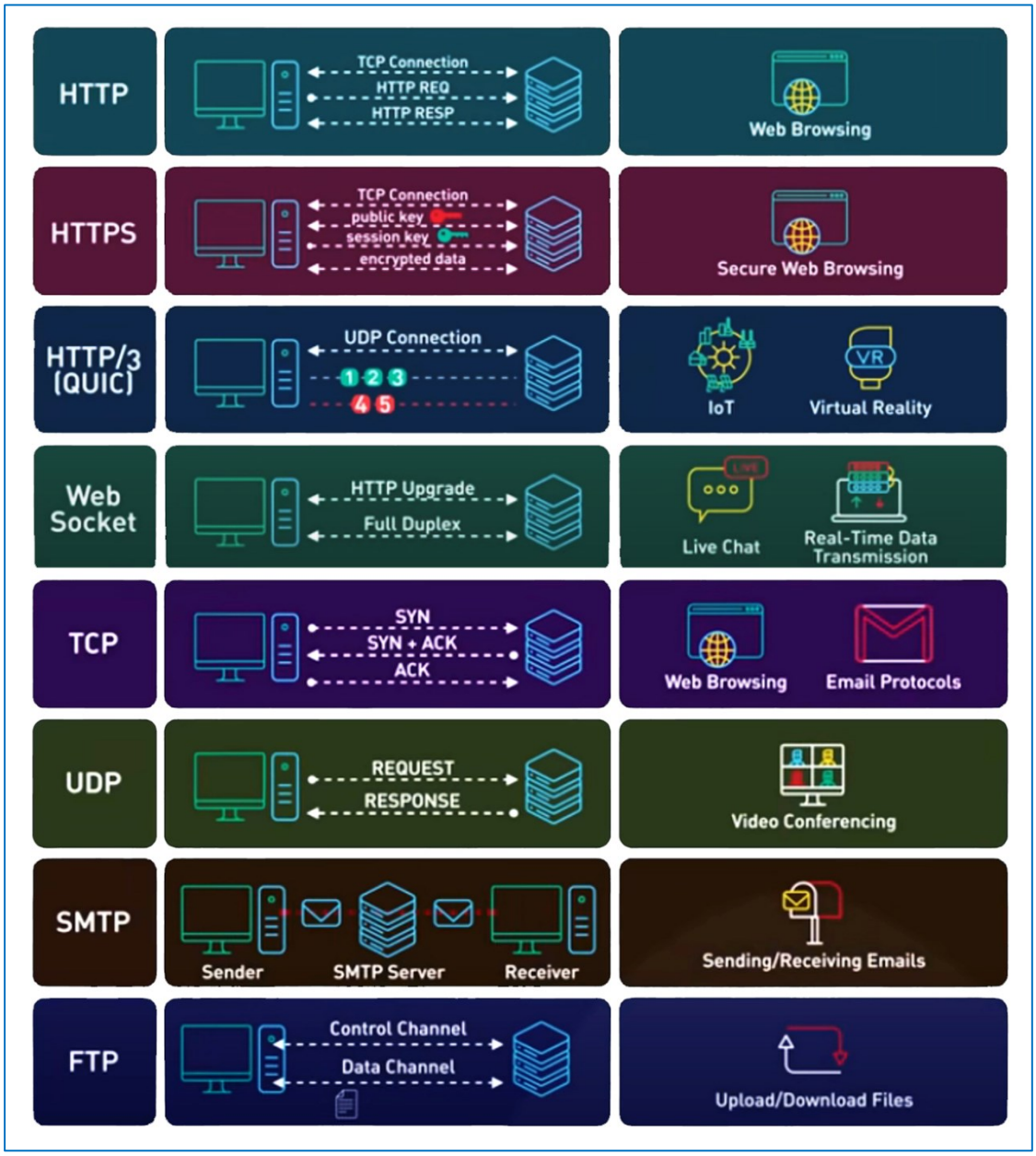


Figure: Network protocols

2.6 Documentation process for network address plan.

Creating a documentation process for a network address plan involves several key steps to ensure clarity, organization, and accuracy. The structured approach to documenting a network address plan is given bellow:

1. **Define Objectives and Scope:**
   - Clearly outline the purpose and objectives of the network address plan documentation.
   - Specify the scope of the documentation, including the network infrastructure, devices, and address allocation policies to be covered.

2. **Inventory Network Components:**
   - Identify all network devices, including routers, switches, firewalls, servers, printers, and end-user devices.
   - Document the physical and logical locations of each device within the network topology.
3. **Address Allocation Scheme:**
   - Define the IP address allocation scheme, including address classes, subnetting strategy, and addressing hierarchy.
   - Specify the IP address ranges reserved for different network segments, departments, or purposes.
4. **Subnet Design:**
   - Design the subnet structure based on network requirements, such as the number of hosts per subnet, scalability, and security considerations.
   - Document subnet masks, subnet IDs, broadcast addresses, and available IP address ranges for each subnet.
5. **IP Address Assignment Policies:**
   - Establish policies for assigning IP addresses to devices, including static IP assignments for servers, network infrastructure, and reserved addresses.
   - Define procedures for dynamic IP address allocation using DHCP (Dynamic Host Configuration Protocol).
6. **Documentation Format:**
   - Choose a documentation format that suits the organization's needs, such as spreadsheets, diagrams, text documents, or specialized network management tools.
   - Ensure consistency and clarity in formatting, labeling, and organization of information.
7. **Network Diagrams:**
   - Create network diagrams illustrating the network topology, device locations, subnet assignments, and connectivity between network segments.
   - Include details such as IP addresses, subnet masks, gateway addresses, and VLAN configurations.
8. **Access Control Lists (ACLs) and Security Policies:**
   - Document access control lists (ACLs) and security policies for controlling traffic flow, filtering packets, and enforcing security measures.

- Specify firewall rules, NAT (Network Address Translation) configurations, and VPN (Virtual Private Network) settings.

9. **Documentation Review and Validation:**
   - Review the documentation for accuracy, completeness, and consistency with network configurations and policies.
   - Validate IP address assignments, subnet configurations, and network diagrams against actual network implementations.
10. **Version Control and Maintenance:**
    - Implement version control mechanisms to track changes and updates to the network address plan documentation.
    - Regularly review and update the documentation to reflect changes in network infrastructure, addressing requirements, and security policies.

2.7 Host name assigning procedure

Assigning host names involves several steps to ensure consistency, organization, and ease of management within a network environment. The procedure for assigning host names is given bellow:

1. **Define Naming Convention:**
   - Establish a naming convention that aligns with organizational standards and reflects the purpose or function of each device.
   - Consider including location, department, function, or other relevant identifiers in the host names to facilitate identification and categorization.
2. **Choose Descriptive Names:**
   - Select descriptive and meaningful names that accurately represent the role or function of each device.
   - Avoid using ambiguous or generic names that may cause confusion or overlap with other devices in the network.
3. **Avoid Special Characters:**
   - Use alphanumeric characters (letters and numbers) only in host names, avoiding special characters such as spaces, underscores, or punctuation marks.
   - Ensure that host names comply with DNS (Domain Name System) naming standards and restrictions.
4. **Assign Sequential Numbers:**
   - Consider assigning sequential numbers or identifiers to devices within the same category or function to maintain consistency and organization.

- Use leading zeros for numerical identifiers to ensure uniformity in sorting and readability (e.g., PC001, PC002, PC003).

5. **Document Host Names:**
   - Maintain a centralized documentation system to record and track assigned host names, along with corresponding IP addresses, device types, locations, and other relevant information.
   - Update the documentation regularly to reflect changes in host names or network configurations.
6. **Automate Host Name Assignment:**
   - Implement automated tools or scripts to streamline the host name assignment process, especially in large or dynamic network environments.
   - Use DHCP (Dynamic Host Configuration Protocol) options or DNS dynamic update mechanisms to automatically register and assign host names to devices.
7. **Verify Name Availability:**
   - Before assigning a host name to a new device, verify that the chosen name is not already in use by another device in the network.
   - Check DNS records and network documentation to avoid conflicts and ensure uniqueness of host names.
8. **Test and Validate:**
   - After assigning host names, test connectivity and accessibility of devices using their assigned names to ensure proper DNS resolution and network functionality.
   - Validate that host names are accurately reflected in DNS records and are accessible from other devices within the network. ame assigning procedure

2.8 Small Office Home Office (SOHO)

SOHO networks, standing for Small Office / Home Office architectures, are simple network setups primarily utilized in homes or small enterprises. They typically consist of a single device, often combining the functions of a router and a switch, providing internet access and network connectivity to connected devices such as PCs and printers.

SOHO architecture utilizes Ethernet technology to connect devices, enabling internet access through a switch/router. Devices connect via Ethernet cables such as CAT5 or CAT6. Wireless networking adds access points, providing internet access to connected devices.

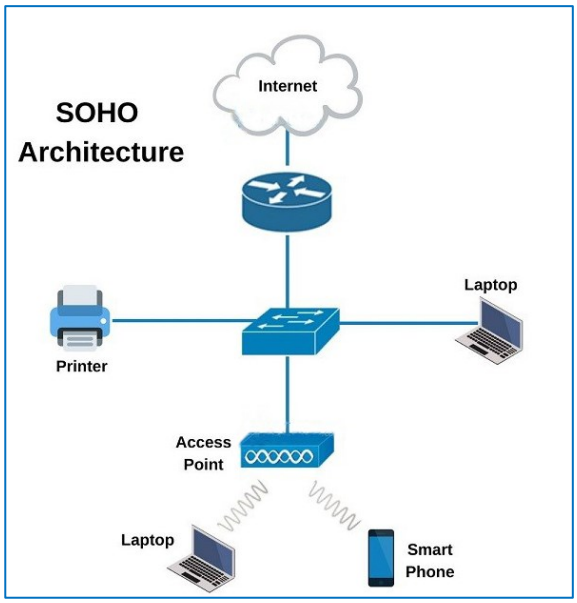


Figure: SOHO Network

A SOHO network involves setting up a local network within a smaller workspace, such as a home or small office, to enable devices to communicate and share resources. This network can be wired or wireless and usually incorporates a central router or hub that allows devices to connect and communicate.

Types of SOHO Network

There are typically two main types of SOHO networks:

iii) **Wired SOHO Network:** This type of network primarily relies on physical Ethernet cables to connect devices to the network. Devices such as computers, printers, and routers are connected via Ethernet cables to a central switch or router, which provides network connectivity and internet access.

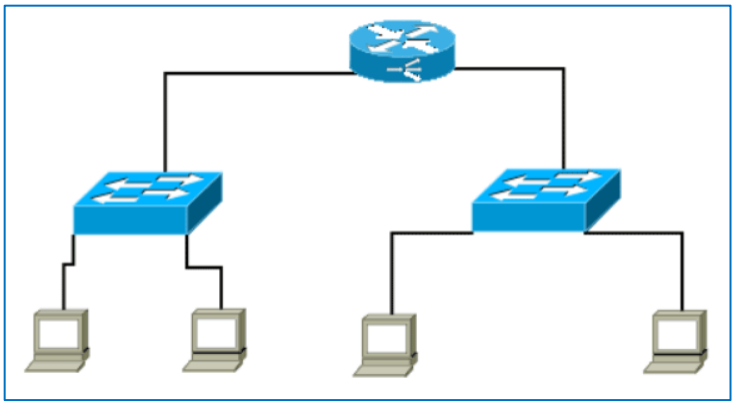


Figure: Wired SOHO Network

iv) **Wireless SOHO Network:** In this type of network, devices connect to the network wirelessly using Wi-Fi technology. A wireless router or access point broadcasts a wireless signal, allowing devices such as laptops, smartphones, tablets, and printers to connect to the network without the need for physical cables.

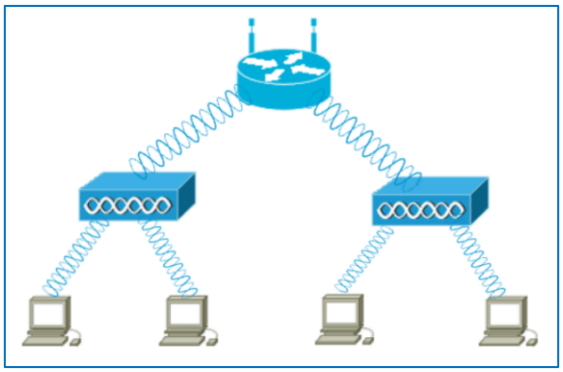
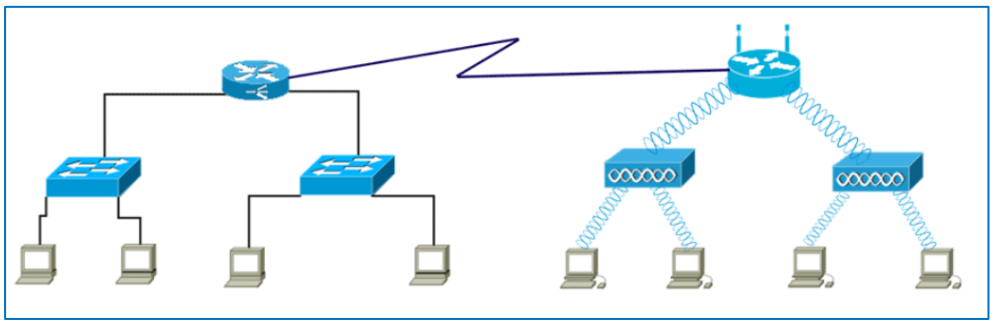


Figure: Wired SOHO Network

These two types of SOHO networks can also be combined, with some devices connected via Ethernet cables and others connecting wirelessly, providing flexibility and convenience for users.

The following image shows a SOHO Ethernet LAN combines wired and wireless connectivity.

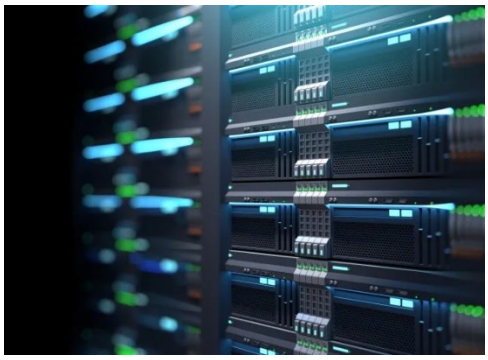


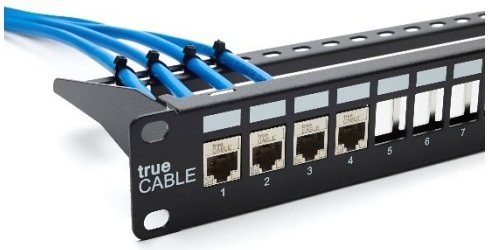
2.9 Tools and equipment's required for stablishing SOHO

Tools and equipment's Name	Description	Image
Crimping tool	A crimping tool is a handy device that allows you to create secure connections between wires and connectors. It works by deforming the connector onto the wire, ensuring a strong bond. With a	

	crimping tool, you can easily join electrical wires, network cables, coaxial cables, and more.	
Connector	The eight-pin RJ45 connector is a standardised interface which often connects a computer to a Local Area Network (LAN). This type of connector was originally developed for telephone communications but is now used in a range of applications. The abbreviation, RJ45, stands for Registered Jack-45.	
Boot cap	The RJ45 boots cover protects RJ45 connectors from dust and Oxidation extending the RJ plug's life time. Protect the connector of the cable, preventing the lan cable being torn, extending the life of your cables. To prevent dust and water from entering the crystal head, resulting in poor contact.	
Face plate modular	The modular Faceplate is an accessory that allows the installation of RJ45 ports on the user's desktop by connecting to the structured cabling system. Being a modular product guarantees flexibility because it can be assembled with the modules that best suit your project.	

Punching tool	A punch down tool, which can also be named an RJ45 punch down tool, or Krone tool, is a hand tool widely used to terminate the Ethernet cables by inserting the cable wires into the insulation-displacement connectors (IDC) on the punch down blocks, patch panels, keystone modules, and surface mount of boxes.	
Screw driver set	Screwdriver, tool, usually hand-operated, for turning screws with slotted heads. For screws with one straight diametral slot cut across the head, standard screwdrivers with flat blade tips and in a variety of sizes are used.	
Cable tester	Network cable testers are designed to test the connectivity of the cables. They can check if a properly wired connection is available from one end of the cable to the other. Some advanced models can even measure the cable length, identify open circuits, short circuits, or reversed connections.	
Cable cutter	Wire and cable cutters are tools that have been designed to properly cut either wire or cable with minimal damage to the insulation or internal conductors of the wire or cable. Having a clean cut on a wire or cable can improve the quality of an electrical connection.	

Patch cord	A patch cable, patch cord or patch lead is an electrical or fiber-optic cable used to connect ("patch in") one electronic or optical device to another for signal routing. Devices of different types (e.g., a switch connected to a computer, or a switch to a router) are connected with patch cords.	
RACK	A server rack houses and organizes critical IT systems, which can be configured to support a wide range of requirements. Often called server rack cabinet, it is enclosed to ensure security. Server racks are most commonly found in data center environments, but can also be used in smaller computer closets.	
Cable Tray	A cable tray is a unit or assembly of units or sections and associated fittings forming a rigid structural system used to securely fasten or support cables and raceways.	
Cable Manager	Network cable management is a device used to manage and organize network cables, which can neatly arrange and organize various types of network cables. It has been widely used in various network cabling applications.	

Patch panel	Patch panels simplify cable management, enhance troubleshooting, and provide documentation and traceability for all connected workstations. A patch panel is an important network component that aids in the connection, organization, and overall management of network cables.	
Switch	A network switch allows two or more IT devices to communicate with one another. In addition to connecting to end devices like PCs and printers, switches may be connected to other switches, routers, and firewalls, all of which can provide connectivity to additional devices.	
Access point	An access point (AP) is a term used for a network device that bridges wired and wireless networks. Consumer APs are often called a "wireless router" because they typically also serve as both internet routers and firewalls.	

2.10 Materials and consumables required for stablishing SOHO

Cable Tag: Cable tags are used for clear, concise cable identification. Cable identification tags are used in both indoor and outdoor applications and are typically attached to a wire or cable bundle with cable ties. To meet all requirements, there are a wide variety of label materials with different properties.

Cable Tie: A cable tie (also known as a hose tie, tie wrap, wire tie, zap-straps, or zip tie) is a type of fastener for holding items together, primarily electrical cables and wires.

Cable Channel: Electric cable channels are integral components in the organization and protection of wiring systems.

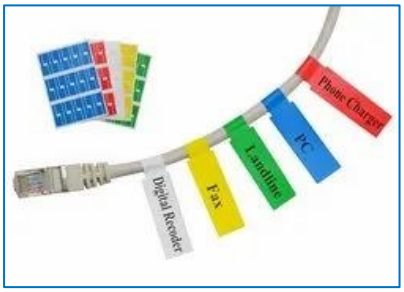


Figure: Cable Tag

Figure: Cable Tie

Figure: Cable Channel

2.11 Budget for Network as per Requirements

To prepare a budget for your network requirements and document the budget, follow these steps:

1. **List Network Components:**
   - Create a list of all network components required for your setup, including:
     - Home router
     - Switch
     - Wireless Access Point (WAP)
     - Network cable CAT6 (50 meters)
     - RJ45 connectors (10 pieces)
     - Boot caps (10 pieces)
2. **Research Prices:**
   - Research prices for each network component from different vendors or online retailers.
   - Consider factors such as brand reputation, quality, warranty, and shipping costs.
3. **Calculate Costs:**
   - Calculate the total cost for each network component based on the prices obtained in step 2.
   - Include any applicable taxes or additional fees in your calculations.
4. **Consider Additional Expenses:**
   - Factor in any additional expenses such as installation costs, labor fees, or shipping charges.
   - Account for potential future expansion or upgrades to your network.
5. **Document the Budget:**
   - Create a budget document using spreadsheet software or budgeting tools.
   - List each network component along with its corresponding cost and quantity.
   - Include a subtotal for each category (e.g., hardware, cables, connectors).
   - Calculate the total budget by summing up all the subtotals.
6. **Allocate Funds:**
   - Determine the source of funds for your network budget, whether it's personal savings, a dedicated budget allocation, or a combination of both.
   - Allocate funds to each category based on your budget document, ensuring that you have sufficient funds to cover all expenses.
7. **Review and Adjust:**
   - Review your budget document to ensure accuracy and completeness.

- Adjust your budget as needed to accommodate any changes in prices, quantities, or requirements.
- Consider prioritizing essential components if your budget is limited.

8. **Finalize and Approve:**
   - Finalize your budget document and obtain approval from relevant stakeholders, if applicable.
   - Keep a copy of the budget document for reference and tracking purposes.
9. **Monitor Expenses:**
   - Monitor your expenses throughout the procurement process to ensure adherence to the budget.
   - Document any deviations from the budget and adjust accordingly to avoid overspending.

Self-Check Sheet-2: Plan For SOHO Network

1. **What are the types of Computer Networks?**

2. **What are the purposes of LANs?**

3. **What is network topology?**

4. **What are the Types of Network Topology?**

5. **Define Star Topology.**

6. **What is Network Protocol?**

Answer Key-2: Plan For SOHO Network

1. **What are the types of Computer Networks?**

   Answer: There are mainly five types of Computer Networks. These are:
   - Local Area Network (LAN)
   - Metropolitan Area Network (MAN)
   - Wide Area Network (WAN)
   - Personal Area Network (PAN)
   - Campus Area Network (CAN)

2. **What are the purposes of LANs?**

   Answer: The main purposes of LANs (Local Area Networks) include:
   - Resource sharing
   - Communication
   - Fast data transfer
   - Centralized management
   - Cost efficiency
   - Increased productivity
   - Security

3. **What is network topology?**

   Answer: Network topology is used to describe the physical and logical structure of a network. It maps the way different nodes on a network--including switches and routers--are placed and interconnected, as well as how data flows. Diagramming the locations of endpoints and service requirements helps determine the best placement for each node to optimize traffic flows Resource sharing.

4. **What are the Types of Network Topology?**

   Answer: The main types of network topology are:
   - Bus Topology
   - Ring Topology
   - Star Topology
   - Mesh Topology
   - Tree Topology
   - Hybrid Topology

5. Define Star Topology.

Answer: In a star topology network, all devices directly link to a central switch or hub, serving as the central connection point. In this topology, Devices transmit data through the central hub, which then distributes the data to all devices connected. Hubs can either be active or passive, with active hubs containing repeaters and passive hubs being classified as non-intelligent nodes. Each node is connected directly to a central node, which serves as a repeater during data transmission.

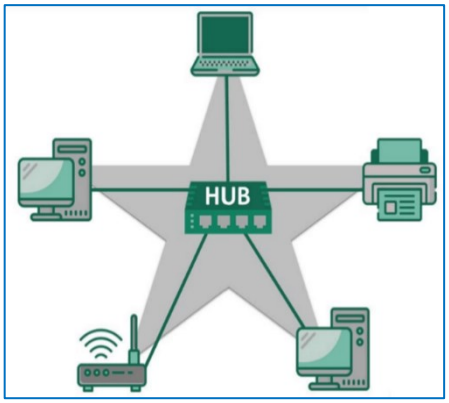


Figure: Star Topology

6. What is Network Protocol?

Answer: A network protocol is a set of rules that govern data communication between different devices in the network. It determines what is being communicated, how it is being communicated, and when it is being communicated. It permits connected devices to communicate with each other, irrespective of internal and structural differences. Example: TCP/IP, HTTP, HTTPS, DHCP, FTP, SMTP, POP3, IMAP etc.

Task Sheet-2.1: Plan For SOHO Network

Performance Objective: At the end of this task, the trainee should be able to Control unauthorize device in SOHO network.

Working steps:

Step 1: Introduction

- Introduce the task of planning for a SOHO network, highlighting the importance of careful consideration and thorough planning.
- Explain the objectives and assessment criteria for the task.

Step 2: Identify Requirements

- Discuss the specific requirements and objectives of the SOHO network, such as the number of users, types of devices, network bandwidth, and security needs.
- Consider factors such as budget constraints, physical space limitations, and future scalability.

Step 3: Design Network Layout

- Sketch a network layout diagram depicting the physical and logical components of the SOHO network, including routers, switches, access points, and devices.
- Determine the placement of network equipment and devices to optimize performance and coverage.

Step 4: Select Networking Equipment

- Research and select appropriate networking equipment based on the requirements identified earlier, such as routers, switches, access points, and network cables.
- Consider factors such as performance, reliability, security features, and cost-effectiveness.

Step 5: Implement Security Measures

- Develop a security plan for the SOHO network, including measures to protect against unauthorized access, malware, and data breaches.
- Implement security protocols such as WPA2 encryption for Wi-Fi networks, firewall configurations, and regular software updates.

Step 6: Develop Maintenance Procedures

- Outline maintenance procedures to ensure the smooth operation and reliability of the SOHO network, including regular backups, firmware updates, and system monitoring.
- Establish protocols for troubleshooting network issues and addressing security incidents.

Step 7: Conclusion

- Summarize the key components of the SOHO network plan developed during the task.

- Emphasize the importance of ongoing monitoring and maintenance to ensure the security and performance of the network.

Specification Sheet-2.1: Plan For SOHO Network

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Hand Gloves	Pair	1
2	Apron	No.	1
3	Googles	No.	1
4	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Unit	Quantity
1	Network monitoring tools or software for analyzing network performance and security.	No.	1

Necessary Equipment

Sl. No	Name of Equipment	Unit	Quantity
1	Computer	No.	10
2	routers	No.	1
3	switches	No.	1
4	access point	No.	1

Necessary Materials

Sl. No.	Name of materials	Unit	Quantity
1	Network cables, etc	Meter	100
2	Paper or whiteboard for sketching network layout diagrams.	No.	1
3	Documentation templates for recording network requirements, equipment selections, and maintenance procedures.	No.	10

Learning Outcome-3: Implement Wired SOHO Network

Assessment Criteria	1. Configuration requirements are identified 2. Tools and equipment are selected and collected from vendor 3. Materials and consumables are collected 4. SOHO Networks is installed and configured 5. Necessary settings for LAN are configured 6. IP assign type is selected 7. IP address is assigned 8. Computer name is ensured and workgroup name are documented and confirmed 9. Documents and file sharing setting are confirmed 10. Add Printer and enable sharing are confirmed 11. Access requirements are determined and sharing is confirmed
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Switch 6. Router 7. Networking related Tools and accessories 8. Multimedia Projector 9. Paper, Pen, Pencil and Eraser
Contents	1 Configuration requirements for SOHO network 2 Tools and equipment's required for stablishing SOHO ▪ Crimping tool ▪ Connector ▪ Boot cap ▪ Face plate modular ▪ Punching tool ▪ Screw driver set ▪ Cable tester ▪ Cable cutter ▪ Patch cord ▪ RACK ▪ Cable Tray ▪ Cable Manager ▪ Patch panel ▪ Switch ▪ Access point SOHO Network 3 Materials and consumables required for wired SOHO ▪ Cable Tag

	▪ Cable tie ▪ Cable Channel 4 • Installation and configuration technique of SOHO Networks 5 Settings of LAN configuration 6 IP address 7 Subnet mask 8 DNS 9 TCP / IP protocol 10 IPv4, Ipv6 11 Document and file sharing technique 12 Printer sharing technique for both normal and network printer 13 Access requirements for resource sharing
Training Methods	1 Blended 2 Discussion 3 Presentation 4 Demonstration 5 Guided Practice 6 Individual Practice 7 Project Work 8 Problem Solving 9 Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1 Written Test 2 Demonstration 3 Oral Questioning

Learning Experience-3: Implement Wired SOHO Network

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
7. Trainee will ask the instructor about the learning materials	11. Instructor will provide the learning materials "Implement wired SOHO network"
8. Read the Information sheet and complete the Self Checks & Check answer sheets on "Implement wired SOHO network"	12. Read Information sheet 1: Implement wired SOHO network 13. Answer Self-check 1: Implement wired SOHO network 14. Check your answer with Answer key 1: Implement wired SOHO network
9. Read the Job/Task Sheet and Specification Sheet and perform job/Task	15. Job/Task Sheet and Specification Sheet Task Sheet 3.1: install and configure SOHO Network Specification Sheet 1.1: install and configure SOHO Network Task Sheet 3.2: Share Documents and files Specification Sheet 3.2: Share Documents and files Task Sheet 3.3: Add Printer and enable sharing Specification Sheet 3.3: Add Printer and enable sharing

Information Sheet-3: Implement Wired SOHO Network

Learning Objective:

After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

3.1 Configuration requirements for SOHO network

3.2 Tools and equipment's required for stablishing SOHO

- Crimping tool
- Connector
- Boot cap
- Face plate modular
- Punching tool
- Screw driver set
- Cable tester
- Cable cutter
- Patch cord
- RACK
- Cable Tray
- Cable Manager
- Patch panel
- Switch
- Access point SOHO Network

3.3 Materials and consumables required for wired SOHO

- Cable Tag
- Cable tie
- Cable Channel

3.4 Installation and configuration technique of SOHO Networks

3.5 Settings of LAN configuration

3.6 IP address

3.7 Subnet mask

3.8 DNS

3.9 TCP / IP protocol

3.10 IPv4, Ipv6

3.11 Document and file sharing technique

3.12 Printer sharing technique for both normal and network printer

3.13 Access requirements for resource sharing

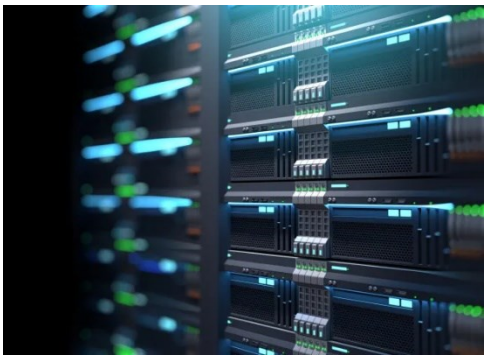
3.1 Configuration requirements for SOHO network

- Network Planning and Design
- Wireless Router Setup
- Wireless Security Configuration
- Network Addressing
- Quality of Service (QoS)
- Firmware Updates and Security Patching
- Monitoring and Management
- Documentation and Backup

3.2 Tools and equipment's required for stablishing SOHO Network

Tools and equipment's Name	Description	Image
Crimping tool	A crimping tool is a handy device that allows you to create secure connections between wires and connectors. It works by deforming the connector onto the wire, ensuring a strong bond. With a crimping tool, you can easily join electrical wires, network cables, coaxial cables, and more.	
Connector	The eight-pin RJ45 connector is a standardised interface which often connects a computer to a Local Area Network (LAN). This type of connector was originally developed for telephone communications but is now used in a range of applications. The abbreviation, RJ45, stands for Registered Jack-45.	

Boot cap	The RJ45 boots cover protects RJ45 connectors from dust and Oxidation extending the RJ plug's life time. Protect the connector of the cable, preventing the lan cable being torn, extending the life of your cables. To prevent dust and water from entering the crystal head, resulting in poor contact.	
Face plate modular	The modular Faceplate is an accessory that allows the installation of RJ45 ports on the user's desktop by connecting to the structured cabling system. Being a modular product guarantees flexibility because it can be assembled with the modules that best suit your project.	
Punching tool	A punch down tool, which can also be named an RJ45 punch down tool, or Krone tool, is a hand tool widely used to terminate the Ethernet cables by inserting the cable wires into the insulation-displacement connectors (IDC) on the punch down blocks, patch panels, keystone modules, and surface mount of boxes.	
Screw driver set	Screwdriver, tool, usually hand-operated, for turning screws with slotted heads. For screws with one straight diametral slot cut across the head, standard screwdrivers with flat blade tips and in a variety of sizes are used.	

Cable tester	Network cable testers are designed to test the connectivity of the cables. They can check if a properly wired connection is available from one end of the cable to the other. Some advanced models can even measure the cable length, identify open circuits, short circuits, or reversed connections.	
Cable cutter	Wire and cable cutters are tools that have been designed to properly cut either wire or cable with minimal damage to the insulation or internal conductors of the wire or cable. Having a clean cut on a wire or cable can improve the quality of an electrical connection.	
Patch cord	A patch cable, patch cord or patch lead is an electrical or fiber-optic cable used to connect ("patch in") one electronic or optical device to another for signal routing. Devices of different types (e.g., a switch connected to a computer, or a switch to a router) are connected with patch cords.	
RACK	A server rack houses and organizes critical IT systems, which can be configured to support a wide range of requirements. Often called server rack cabinet, it is enclosed to ensure security. Server racks are most commonly found in data center environments, but can also be used in smaller computer closets.	

Cable Tray	A cable tray is a unit or assembly of units or sections and associated fittings forming a rigid structural system used to securely fasten or support cables and raceways.	
Cable Manager	Network cable management is a device used to manage and organize network cables, which can neatly arrange and organize various types of network cables. It has been widely used in various network cabling applications.	
Patch panel	Patch panels simplify cable management, enhance troubleshooting, and provide documentation and traceability for all connected workstations. A patch panel is an important network component that aids in the connection, organization, and overall management of network cables.	
Switch	A network switch allows two or more IT devices to communicate with one another. In addition to connecting to end devices like PCs and printers, switches may be connected to other switches, routers, and firewalls, all of which can provide connectivity to additional devices.	

Access point	An access point (AP) is a term used for a network device that bridges wired and wireless networks. Consumer APs are often called a "wireless router" because they typically also serve as both internet routers and firewalls.	

3.3 Materials and consumables required for wired SOHO

Cable Tag: Cable tags are used for clear, concise cable identification. Cable identification tags are used in both indoor and outdoor applications and are typically attached to a wire or cable bundle with cable ties. To meet all requirements, there are a wide variety of label materials with different properties.

Cable Tie: A cable tie (also known as a hose tie, tie wrap, wire tie, zap-straps, or zip tie) is a type of fastener for holding items together, primarily electrical cables and wires.

Cable Channel: Electric cable channels are integral components in the organization and protection of wiring systems.

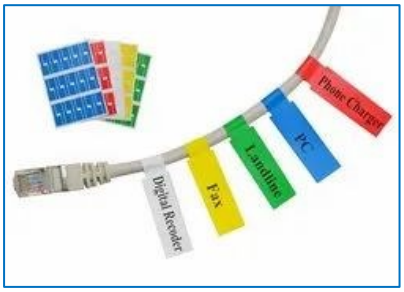


Figure: Cable Tag

Figure: Cable Tie

Figure: Cable Channel

3.4 Installation and configuration technique of SOHO Networks

To install and configure a wired SOHO (Small Office/Home Office) network, follow these steps:

1. **Plan the Network Layout:**
   - Determine the layout and topology of your network, including the placement of devices such as routers, switches, and computers.
   - Consider factors such as the location of power outlets, cable runs, and proximity to network equipment.
2. **Gather Necessary Equipment:**

- Acquire the necessary network equipment, including:
- Router: Provides internet connectivity and acts as a gateway for the network.
- Switch: Connects devices within the network and allows them to communicate with each other.
- Ethernet cables: Use CAT5e or CAT6 cables for wired connections between devices.
- Network adapters: Install Ethernet network adapters in computers if they are not already built-in.
- Optional: Patch panel, cable management tools, and wall plates for professional cable management.

3. **Install Network Hardware:**
   - Place the router in a central location where it can provide optimal coverage and connectivity to all devices.
   - Connect the router to the modem provided by your internet service provider (ISP) using an Ethernet cable.
   - Install the switch in a convenient location and connect it to the router using another Ethernet cable.
   - Connect computers, printers, and other devices to the switch using Ethernet cables.
4. **Configure Router Settings:**
   - Access the router's web-based management interface using a web browser on a connected computer.
   - Follow the manufacturer's instructions to log in to the router's configuration page (usually via a default IP address such as 192.168.1.1) using the default username and password.
   - Configure basic settings such as network name (SSID), wireless security settings (WPA2 passphrase), and DHCP settings (if applicable).
   - Set up port forwarding, firewall rules, and other advanced settings as needed for your network requirements.
5. **Configure Switch Settings:**
   - Switches typically do not require configuration for basic network operation.
   - If your switch has management capabilities, access its management interface and configure settings such as VLANs, port mirroring, and Quality of Service (QoS) as needed.
6. **Test Connectivity:**
   - Power on all network devices and ensure that they are properly connected to the network.

- Verify connectivity between devices by pinging their IP addresses from a command prompt or terminal.
- Test internet connectivity by accessing websites or performing speed tests using connected devices.

7. **Document Network Configuration:**
   - Document the network configuration, including IP addresses, device names, and network settings, for future reference and troubleshooting.
   - Keep a record of router and switch configurations, including login credentials, in a secure location.

8. **Optimize and Secure the Network:**
   - Optimize network performance by ensuring proper cable management, minimizing cable runs, and avoiding physical interference.
   - Implement security measures such as enabling WPA2 encryption for Wi-Fi networks, changing default passwords, and disabling remote management features if not needed.
   - Regularly update router firmware and switch firmware to patch security vulnerabilities and ensure compatibility with new technologies.

3.5 Settings of LAN configuration

In a SOHO (Small Office/Home Office) network, LAN (Local Area Network) configuration settings typically include the following:

1. **IP Address Assignment:**
   - Decide whether IP addresses will be assigned dynamically (via DHCP) or statically (manually).
   - Configure DHCP settings on the router to allocate IP addresses to devices dynamically, including the range of IP addresses, subnet mask, default gateway, and DNS server addresses.
   - Alternatively, assign static IP addresses to devices manually within the same subnet, ensuring that each device has a unique IP address.

2. **Subnet Configuration:**
   - Determine the subnet mask for the network, which defines the range of IP addresses available for use.
   - Choose an appropriate subnet size based on the number of devices in the network and future scalability requirements.

- Configure the router's LAN interface with the appropriate subnet mask to segment the network into smaller subnets if needed.

3. **LAN Interface Settings:**
   - Configure the LAN interface of the router with an appropriate IP address within the chosen subnet.
   - Specify the LAN interface as the default gateway for devices on the network, allowing them to access the internet and communicate with devices outside the local network.
4. **DNS Configuration:**
   - Specify DNS (Domain Name System) server addresses to be used by devices on the network for name resolution.
   - DNS servers can be provided by the ISP (Internet Service Provider) or configured manually to use public DNS servers such as Google DNS (8.8.8.8, 8.8.4.4) or Cloudflare DNS (1.1.1.1, 1.0.0.1).
5. **Network Services and Features:**
   - Enable or disable network services and features as needed, such as:
   - DHCP server: Enable DHCP service on the router to automatically assign IP addresses to devices on the network.
   - NAT (Network Address Translation): Enable NAT to allow devices on the private LAN to access the internet using a single public IP address.
   - Firewall: Configure firewall settings to control inbound and outbound traffic, restrict access to specific services, and protect against unauthorized access.
6. **LAN Security Settings:**
   - Implement security measures to protect the LAN from unauthorized access and malicious activity, including:
   - Wi-Fi security: Enable WPA2 encryption and configure a strong Wi-Fi passphrase to secure wireless networks.
   - Access control: Restrict access to network resources by configuring access control lists (ACLs) or MAC address filtering on the router.
   - Guest network: Set up a separate guest network with limited access to the LAN for visitors or temporary devices.
7. **Network Monitoring and Management:**
   - Configure monitoring and management features to monitor network performance, troubleshoot issues, and ensure smooth operation, including:

- SNMP (Simple Network Management Protocol): Enable SNMP on network devices to monitor and manage them remotely using network management software.
- Logging and alerts: Configure logging and alerting settings to receive notifications of network events, errors, or security incidents.

3.6 IP address

An IP address, short for Internet Protocol address, is a distinctive numerical label assigned to every device connected to a computer network the Internet Protocol for communication. It performs two primary functions: it identifies the host or network interface, and it provides the location of the host in the network, allowing the establishment of a path to that host.
IP addresses can be **Static**, meaning they do not change, or **Dynamic**, meaning they can change each time a device connects to the internet.
There are two versions of IP addresses commonly in use:
IPv4: This is the original version and defines an IP address as a 32-bit number. Example: 192.0.2.1.
IPv6: This newer version was created to deal with the exhaustion of IPv4 addresses and uses 128 bits for the IP address, allowing for a much larger number of unique addresses. Example: 2001:db8:0:1234:0:567:8:1.

Class A Public & Private IP Address Range
Class A addresses are for networks with large number of total hosts. Class A allows for 126 networks by using the first octet for the network ID. The first bit in this octet, is always zero. The remaining seven bits in this octet complete the network ID. The 24 bits in the remaining three octets represent the hosts ID and allows for approximately 17 million hosts per network. Class A network number values begin at 1 and end at 127.

Public IP Range: 1.0.0.0 to 127.0.0.0
First octet value ranges from 1 to 127
Private IP Range: 10.0.0.0 to 10.255.255.255
Subnet Mask: 255.0.0.0 (8 bits)
Number of Networks: 126
Number of Hosts per Network: 16,777,214

Class B Public & Private IP Address Range
Class B addresses are for medium to large sized networks. Class B allows for 16,384 networks by using the first two octets for the network ID. The first two bits in the first octet are always 1 0. The remaining six bits, together with the second octet, complete the network ID. The 16 bits in the third and fourth octet represent host ID and allow for approximately 65,000 hosts per network. Class B network number values begin at 128 and end at 191.

Public IP Range: 128.0.0.0 to 191.255.0.0
First octet value ranges from 128 to 191
Private IP Range: 172.16.0.0 to 172.31.255.255 (See Private IP Addresses below for more information)
Subnet Mask: 255.255.0.0 (16 bits)
Number of Networks: 16,382

Number of Hosts per Network: 65,534

Class C Public & Private IP Address Range

Class C addresses are used in small local area networks (LANs). Class C allows for approximately 2 million networks by using the first three octets for the network ID. In a class C IP address, the first three bits of the first octet are always 1 1 0. And the remaining 21 bits of the first three octets complete the network ID. The last octet (8 bits) represent the host ID and allows for 254 hosts per network. Class C network number values begins at 192 and end at 223.

Public IP Range: 192.0.0.0 to 223.255.255.0
First octet value ranges from 192 to 223
Private IP Range: 192.168.0.0 to 192.168.255.255 (See Private IP Addresses below for more information)
Special IP Range: 127.0.0.1 to 127.255.255.255 (See Special IP Addresses below for more information)
Subnet Mask: 255.255.255.0 (24 bits)
Number of Networks: 2,097,150
Number of Hosts per Network: 254

Class D IP Address Range

Class D IP addresses are not allocated to hosts and are used for multicasting. Multicasting allows a single host to send a single stream of data to thousands of hosts across the Internet at the same time. It is often used for audio and video streaming, such as IP-based cable TV networks. Another example is the delivery of real-time stock market data from one source to many brokerage companies.
Range: 224.0.0.0 to 239.255.255.255
First octet value ranges from 224 to 239
Number of Networks: N/A
Number of Hosts per Network: Multicasting

Class E IP Address Class

Class E IP addresses are not allocated to hosts and are not available for general use. These are reserved for research purposes.

Range: 240.0.0.0 to 255.255.255.255
First octet value ranges from 240 to 255
Number of Networks: N/A
Number of Hosts per Network: Research/Reserved/Experimental

APIPA: Automatic Private IP Addressing (APIPA) is a feature in operating systems (such as Windows) that allows computers to self-configure IP addresses and subnet masks when their DHCP server is unavailable. The IP address range for APIPA is 169.254.0.1-169.254.255.254, with the subnet mask of 255.255.0.0.

Special IP Addresses

IP Range: 127.0.0.1 to 127.255.255.255 are network testing addresses (also referred to as loop-back addresses). These are virtual IP addresses; in that they cannot be assigned to a device. Specifically, IP 127.0.0.1 is often used to troubleshoot network connectivity issues using the ping command. Specifically, it tests a computer's TCP/IP network software driver to ensure it is working properly.

3.7 Subnet mask

A subnet mask is a 32-bit value that specifies the boundrary between the network prefix and suffix. 1 bit represent the network portion and 0 bits represent the host portion.

Dotted decimal IP	192.168.0.0/25	
Subnet Mask	255.255.255.128	
Equivalent dotted binary	11111111.11111111.11111111.	10000000
	Network bits	Host bit

3.8 DNS

DNS (Domain Name System) is a hierarchical and distributed naming system used to translate human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) used by computers to locate resources on the internet.

3.9 TCP / IP protocol

An internet protocol called TCP/IP, also known as Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to connect network devices The TCP/IP protocol can also be used in a private network, such as an intranet or extranet.

The suite is designed to be robust, able to automatically recover from the failure of any device on the network. It includes several protocols, with TCP and IP being the two main ones:

This protocol defines how applications can create channels of communication across a network. It manages how a message is assembled into smaller packets before they are transmitted over the internet and ensures that packets are reassembled in the correct order at the destination address.

IP (Internet Protocol):

This protocol defines how to address and route each packet to ensure it reaches the right destination. Each gateway computer on the network checks the IP address to determine where to forward the message.

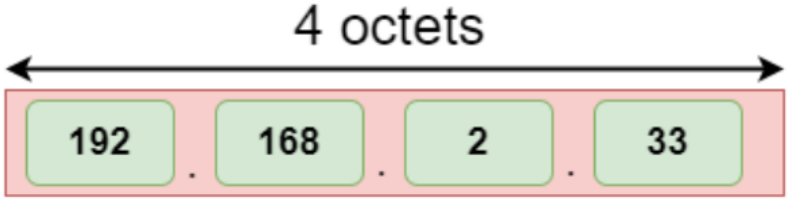
Common protocols included in the TCP/IP suite are:

HTTP (Hypertext Transfer Protocol): Handles communication between a web server and a web browser.

FTP (File Transfer Protocol): Manages the transmission of files between computers.
SMTP (Simple Mail Transfer Protocol): Used for sending emails.
DNS (Domain Name System): Translates domain names to IP addresses.

3.10 IPv4, Ipv6

IPv4:
IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.
The address format of IPv4 is given bellow.



An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255.

For example, 66.94.29.13

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

Representation of 8 Bit Octet

128	64	32	16	8	4	2	1

The above representation shows the structure of 8- bit octet.
Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

Step 1: First, we find the binary number of 66.

128	64	32	16	8	4	2	1
0	1	0	0	0	0	1	0

To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

Step 2: Now, we calculate the binary number of 94.

128	64	32	16	8	4	2	1
0	1	0	1	1	1	1	0

To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

Step 3: The next number is 29.

128	64	32	16	8	4	2	1
0	0	0	1	1	1	0	0

To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

Step 4: The last number is 13.

128	64	32	16	8	4	2	1
0	0	0	0	1	1	0	1

To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

IPv6:

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-

bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

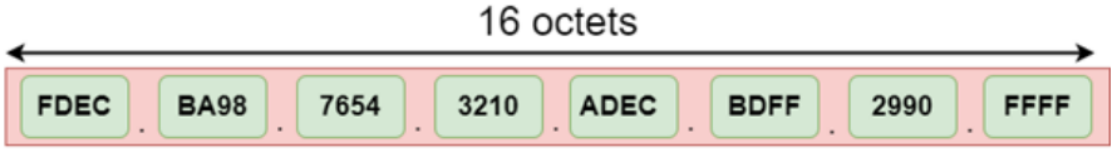
It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

- Dual stacking: It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
- Tunneling: In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
- Network Address Translation: The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion (3.4*1038) addresses.

IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time.

The address format of IPv6 is given bellow.



IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

Differences between IPv4 and IPv6

	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.

Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

3.11 Document and file sharing technique

Document and file sharing techniques vary depending on factors such as the size of the files, the number of users involved, security requirements, and the infrastructure available. Here are several common techniques for document and file sharing:

Email Attachments: One of the simplest methods for sharing files is through email attachments. Users can attach documents or files to an email message and send them to one or more recipients. However, email attachments are limited in size, and large files may not be suitable for this method.

File Transfer Protocol (FTP): FTP is a standard network protocol used for transferring files between a client and a server on a computer network. Users can upload files to an FTP server or download files from an FTP server using FTP client software.

File Sharing Services: There are many online file sharing services that allow users to upload and share files with others over the Internet. These services often provide features such as file synchronization, version control, and access control. Examples include Dropbox, Google Drive, Microsoft OneDrive, and Box.

Network File Sharing (SMB/CIFS): Network file sharing protocols such as Server Message Block (SMB) and Common Internet File System (CIFS) enable users to share files and folders over a local area network (LAN). Users can access shared files and folders from other computers on the network as if they were local files.

Peer-to-Peer (P2P) File Sharing: P2P file sharing allows users to share files directly with each other without the need for a central server. Users connect to a decentralized network and can download files from other users who have the same files available for sharing. Examples of P2P file sharing protocols include BitTorrent and Gnutella.

Cloud Storage: Cloud storage services allow users to store files and data online and access them from anywhere with an Internet connection. Users can share files with others by providing them with a link or granting them access to specific files or folders. Examples include Dropbox, Google Drive, Microsoft OneDrive, and Amazon S3.

Secure File Sharing: For sensitive or confidential files, organizations may use secure file sharing methods such as encrypted email, secure FTP (SFTP), or encrypted file sharing services that provide end-to-end encryption and other security features to protect data privacy.

Collaboration Platforms: Collaboration platforms and project management tools often include built-in document and file sharing capabilities. These platforms allow teams to collaborate on documents, share files, assign tasks, and track project progress in a centralized workspace. Examples include Microsoft Teams, Slack, Asana, and Trello.

3.12 Printer sharing technique for both normal and network printer

Sharing printers, whether they are normal (local) printers or network printers, allows multiple users to access a single printer, which can be cost-effective and convenient.

To share both types normal and network printers follow the given instructions:

Sharing a Normal (Local) Printer on a Windows Network:

1. Connect the printer to one of the computers and install the necessary drivers.
2. Open **Settings** on the computer connected to the printer.
3. Go to **Devices** > **Printers & scanners.**
4. Select the printer you want to share and click on **Printer properties**.
5. In the printer properties window, navigate to the Sharing tab.
6. Check the Share this printer option.
7. Assign a share name to the printer to easily identify it on the network.

Sharing a Network Printer:

1. Network printers are designed to connect directly to the network via Ethernet or Wi-Fi.
2. Install the printer drivers on each computer that needs access to the printer.
3. Use the printer's IP address to add it as a network printer on each computer:
   - Go to **Settings** > **Devices** > **Printers & scanners.**
   - Click **Add a printer or scanner.**
   - Choose **The printer that I want is not listed.**
   - Select **Add a printer using a TCP/IP address or hostname,** and enter the printer's IP address.

3.13 Access requirements for resource sharing

Access requirements for resource sharing, whether it's printers, files, or other network resources, depend on the specific resource being shared and the security considerations of the organization. However, some common access requirements for resource sharing include:

Authentication: Users should authenticate themselves before accessing shared resources to ensure that only authorized individuals can access sensitive information.

Authentication methods may include usernames and passwords, biometric authentication, smart cards, or multi-factor authentication (MFA).

Authorization: Once authenticated, users must be authorized to access specific resources based on their roles, responsibilities, and permissions. Authorization controls determine what actions users can perform on shared resources, such as read, write, modify, or delete permissions.

Access Control Lists (ACLs): Access control lists define the permissions granted to users or groups for accessing resources. ACLs specify which users or groups have access to specific resources and what actions they can perform on those resources. Administrators can configure ACLs to enforce security policies and restrict unauthorized access.

Group Policies: Group policies allow administrators to manage and enforce security settings, configurations, and access controls across multiple users and computers in an organization's network. Group policies can be used to define access restrictions, password policies, software installation rules, and other security-related settings.

Encryption: Encrypting shared resources helps protect sensitive information from unauthorized access or interception. Encryption techniques such as SSL/TLS (Secure Sockets Layer/Transport Layer Security) can secure data in transit, while encryption algorithms like AES (Advanced Encryption Standard) can protect data at rest.

Network Segmentation: Segregating network resources into separate segments or VLANs (Virtual Local Area Networks) can help limit the scope of resource access and mitigate the risk of unauthorized access or lateral movement by attackers. Network segmentation can be implemented using firewalls, routers, and access control mechanisms.

Auditing and Logging: Logging access to shared resources allows administrators to monitor user activity, track changes, and detect suspicious or unauthorized behavior. Auditing logs can provide valuable insights into who accessed which resources, when, and what actions were performed, aiding in security incident response and compliance efforts.

Compliance Requirements: Organizations may need to adhere to industry-specific regulations, standards, or internal policies governing access to sensitive information and resources. Compliance requirements may dictate specific access controls, encryption protocols, audit logging practices, and other security measures to protect sensitive data and ensure regulatory compliance.

What is File Sharing?

- Sharing of data on a network
- Allows multiple users to access a particular file /folder by enabling them to
  - Read
  - Modify

- Copy or
- Print

Type of File Shiring

- Default Share
  - Dose not Provide security.
  - Requires no configaration.
  - Require share desination
  - Default local share or Default network share.
- Restricted share
  - Provides security by limiting the number of users accessing the share at a particular time.
  - Designate specific user to access the share
  - Allot permissions to control user activity on the share

Self-Check Sheet-3: Implement Wired SOHO Network

1. **Define Subnet mask?**

2. **What is DNS?**

3. **What is the purpose of an IP address?**

4. **How many bits does an IPv4 address consist of?**

5. **What does APIPA stand for, and what does it allow computers to do?**

Answer Key-3: Implement Wired SOHO Network

1. Define Subnet mask?

Answer: A subnet mask is a 32-bit value that specifies the boundrary between the network prefix and suffix. 1 bit represent the network portion and 0 bits represent the host portion.

Dotted decimal IP	192.168.0.0/25	
Subnet Mask	255.255.255.128	
Equivalent dotted binary	11111111.11111111.11111111.	10000000
	Network bits	Host bit

2. What is DNS?

Answer: DNS (Domain Name System) is a hierarchical and distributed naming system used to translate human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.0.2.1) used by computers to locate resources on the internet.

3. What is the purpose of an IP address?

Answer: An IP address is a numerical label assigned to devices on a network to identify them and facilitate communication.

4. How many bits does an IPv4 address consist of?

Answer An IPv4 address consists of 32 bits.

5. What does APIPA stand for, and what does it allow computers to do?

Answer: APIPA stands for Automatic Private IP Addressing, and it allows computers to self-configure IP addresses and subnet masks when their DHCP server is unavailable.

Task Sheet-3.1: Install And Configure SOHO Network

Performance Objective: At the end of this task, the trainee should be able to install and configure SOHO Network.

Working steps:

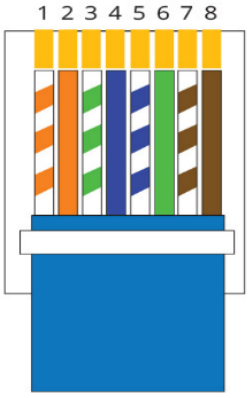
Step 1. Collect the PPE

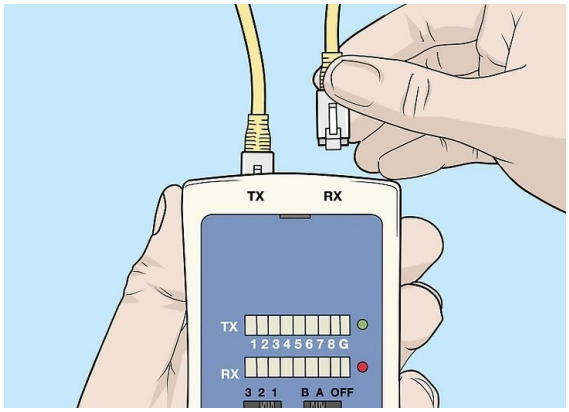
Step 2. Collect the required Tools & Equipment's

Step 3. Prepare the Lan Cable Standard of T568B,

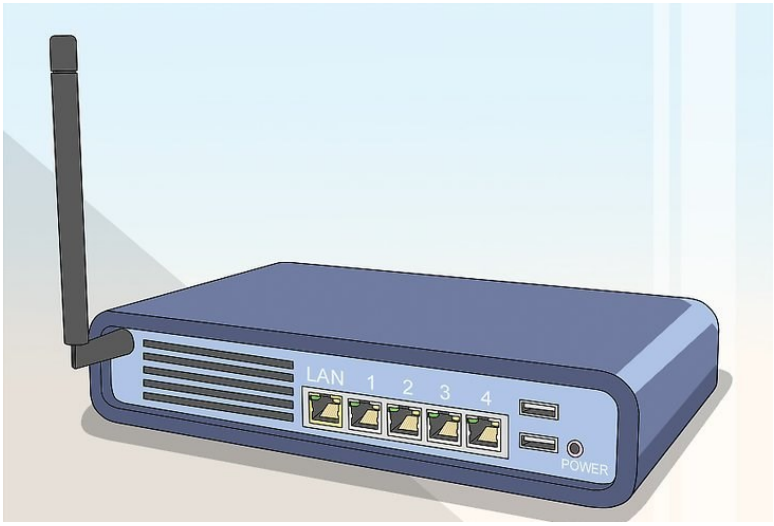
- Cat5e or higher (Cat6/Cat6a/Cat7) depending on your network speed requirement.
- Use RJ45 Ethernet Cable Connectors These are the modular plugs that attach to the ends of the cable.
- Use Wire Cutter or Scissors Cut the cable to your desired length.
- Use Wire Stripper or a Sharp Knife For stripping the protective jacket off the cable to expose the wires.
- Use a Cable Tester Once the cables are connected, turn the tester on to begin the test. The tester will cycle through 8 positions and a ground connection, each represented by a light on the tester

Sample:



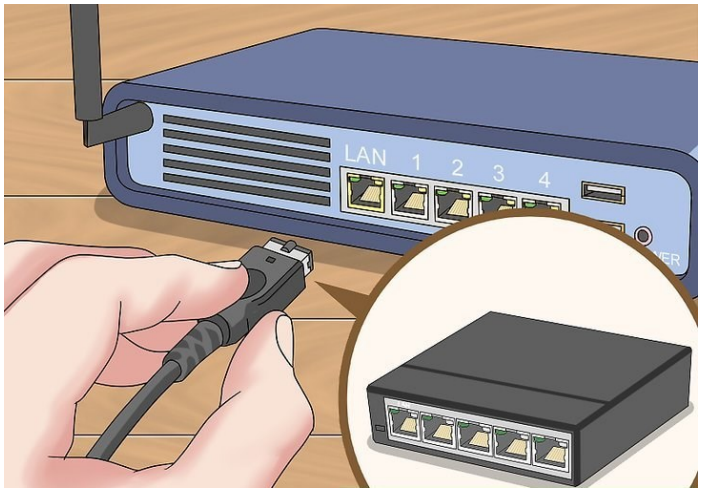


Step 4. Obtain the network hardware These pieces of hardware are the "hub" of your LAN, and all of your computers will be connected to them.

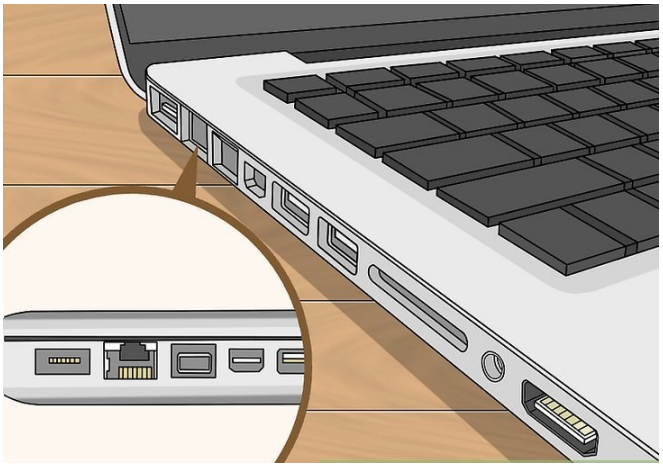


Step 5. Connect your modem or Internet Cable Supplied by ISP to the WAN port on the router. This port may be labeled "INTERNET" instead. This will provide internet access to every computer that is connected to your LAN.

Step 6. Connect the switch to a LAN port on the router. using a network switch to connect more computers, connect it to one of the LAN ports on the router. You can use any open port on the switch to make the connection. When connected, the router will provide IP addresses for every computer that is connected to either device.



Step 7. Find the Ethernet port on your PC. You can usually find this on the back of your desktop tower, or along the side or back of a laptop.

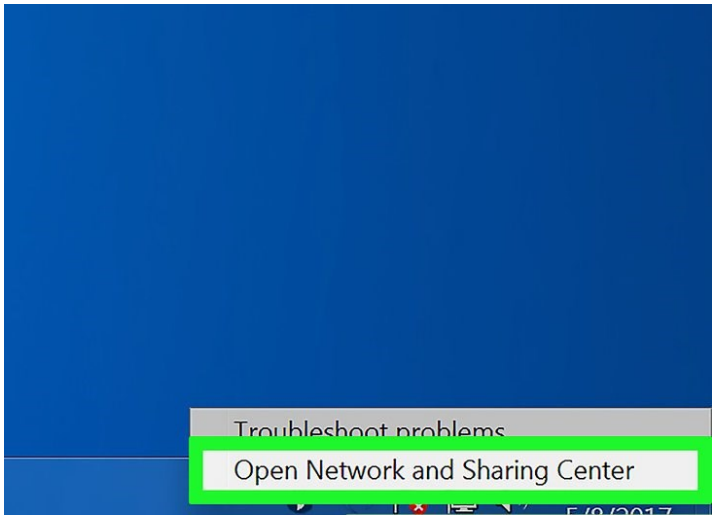


Step 8. **Plug the other end of the cable into an open LAN port.** This can be any open LAN port on either the router or the switch, depending on your LAN.

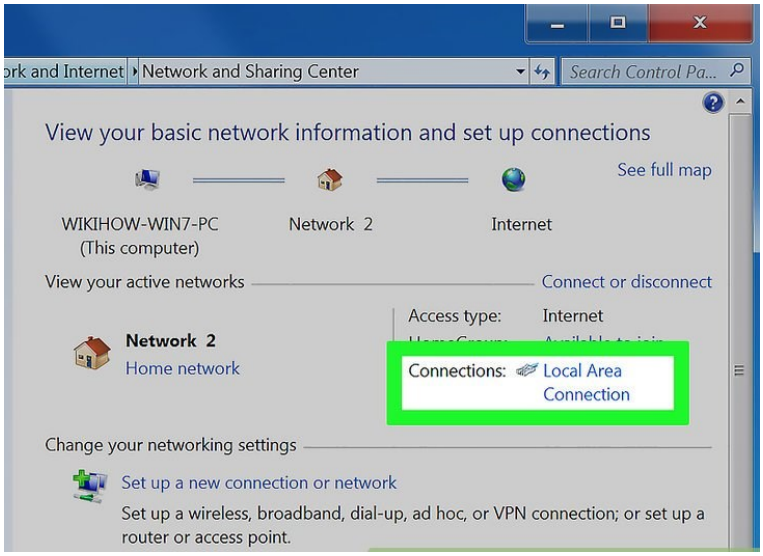
Step 9. **Test out your network (router only):** If you're using a router, your work is complete. Once all of the computers are connected to a LAN port, they will be assigned IPs automatically and will appear on the network.

Step 10. Assigning IP Addresses (No Router) **Right-click on your network connection.** You'll see this in your System Tray. Connect your computers through a switch with no router, assign each computer on the network its own individual IP address. Think of a Class C IP address as a mailing address.

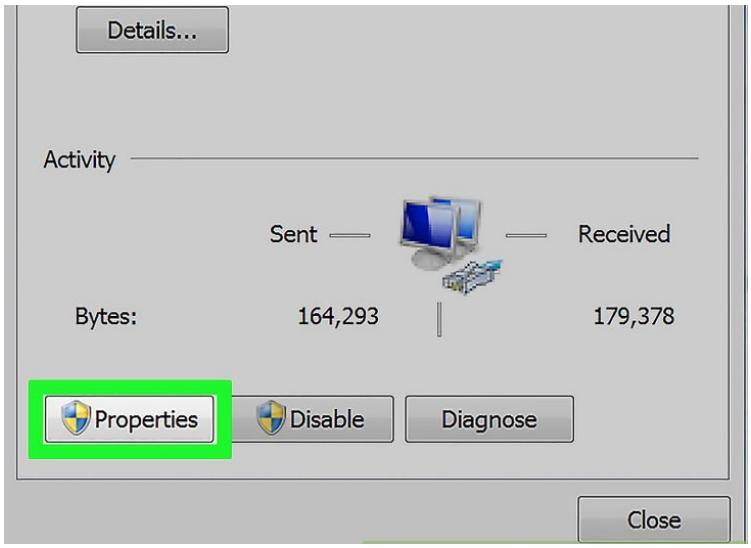
Click Open Network and Sharing Center.



Step 11. **Click the Local Area Connection link at the top of the window.** You'll see this next to "Connections".

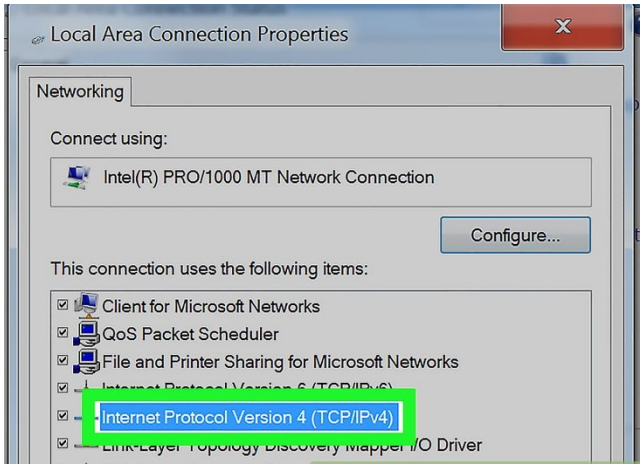


Step 12. **Click Properties.**

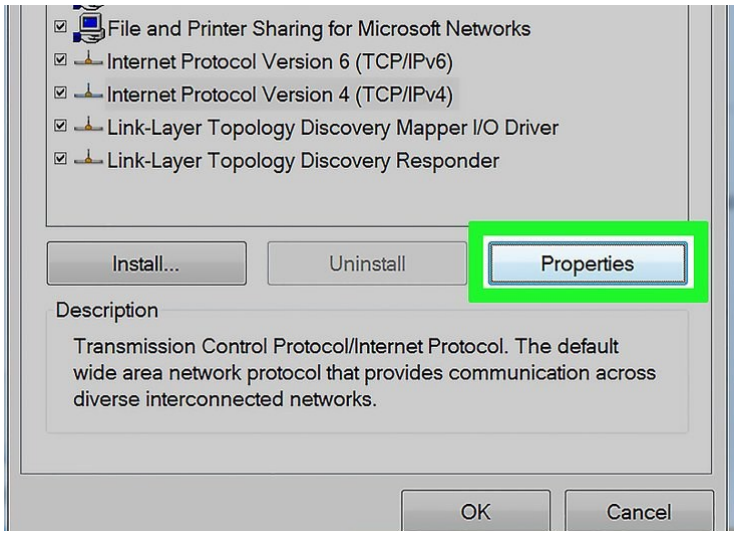


Step 13. **Click Internet Protocol Version 4 (TCP/IPv4).** Make sure you don't uncheck it, just highlight it.

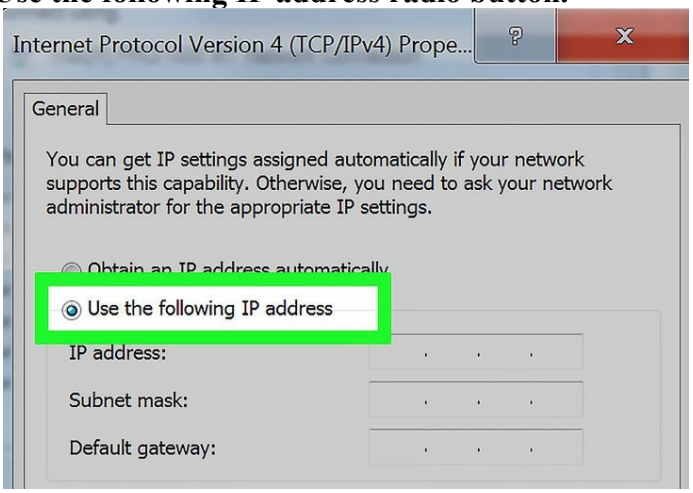
Step 14.



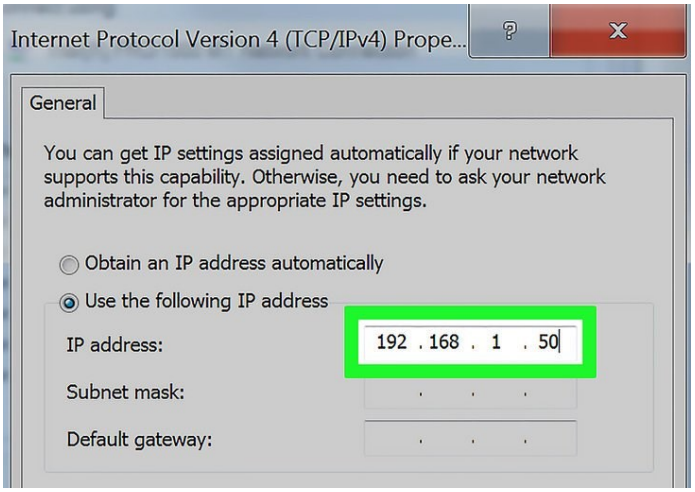
Step 15. Click Properties.



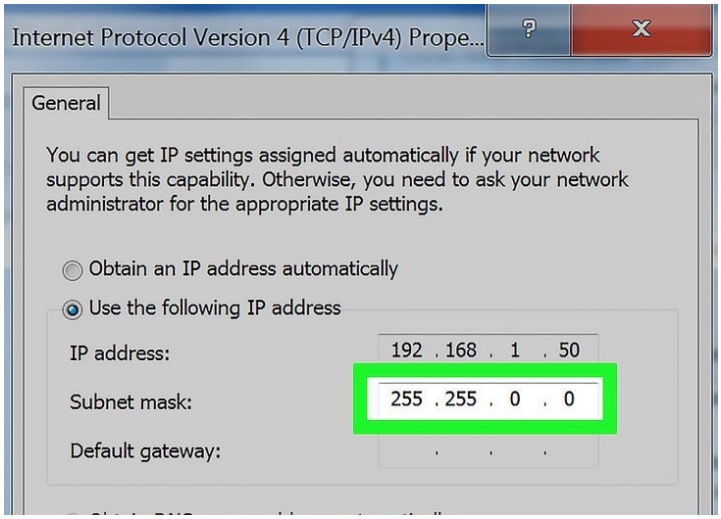
Step 16. Click the Use the following IP address radio button.



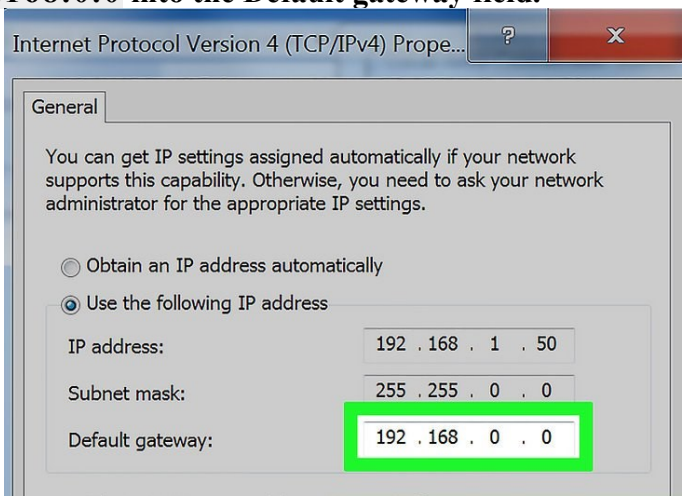
Step 17. Type Class C IP `192.168.1.50` into the IP address field.



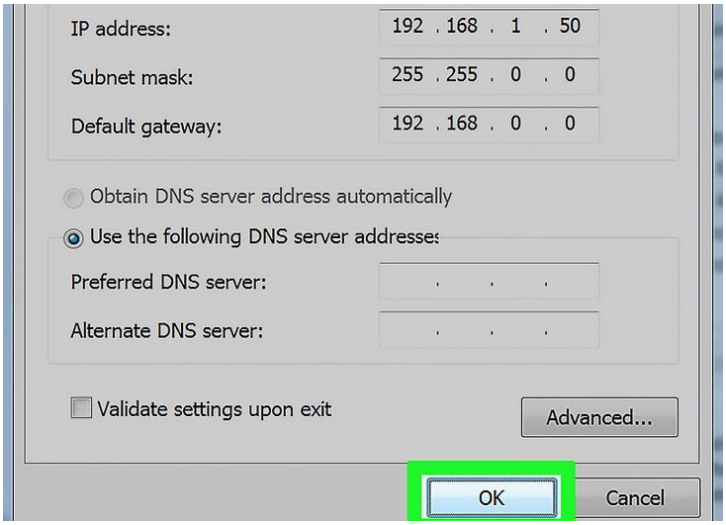
Step 18. Type `255.255.0.0` into the Subnet mask field.



Step 19. Type `192.168.0.0` into the Default gateway field.



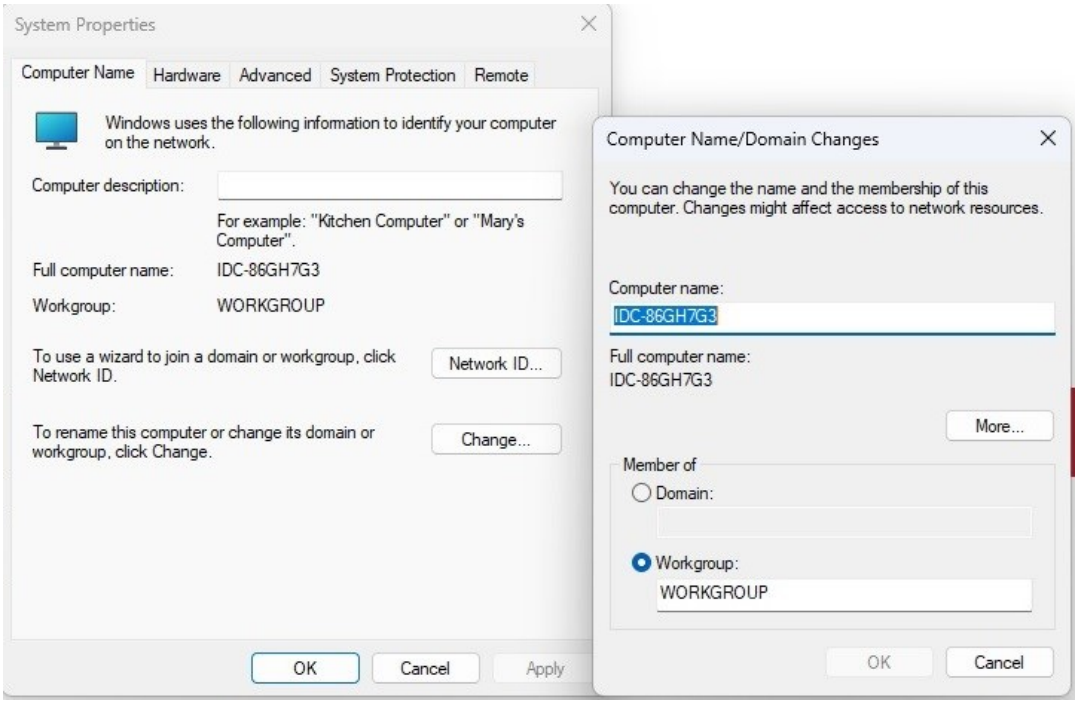
Click OK. This will save the settings for that computer. This computer is now configured on your network with a unique IP address.



Step 20. Open the Internet Protocol Version 4 properties on the next computer. Follow the steps above on the second computer to open the Internet Protocol Version 4 (TCP/IPv4) Properties window.
Enter the same values for Subnet mask and Default gateway. These values should be the same as they were on the first computer (255.255.0.0 and 192.168.0.0 respectively).

Step 21. Confirm Computer name and workgroup name and documented

Type “Workgroup” into the search field at the top left of the Settings app and then click on “Change workgroup name”. Windows opens a new window in which the name of your workgroup appears after “Workgroup” – it is “WORKGROUP” by default. Noted this Workgroup Name & PC Name.



Specification Sheet-3.1: Install And Configure SOHO Network

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
5	Hand Gloves	Pair	1
6	Apron	No.	1
7	Googles	No.	1
8	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Specification	Unit	Quantity
10	Cutting Plair	Wire Cutting Plair Multi size	No.	1
11	Wire Striper		No.	1
12	Clumping Tools	Clumping Tools for RJ45 Connector	No.	1
13	Star Screw Driver		No.	1

Necessary Equipment

Sl. No	Name of Equipment	Specification	Unit	Quantity
1	Cable Tester	Cable Tester for RJ 45 Connection, Led & Buzzer System	No.	1
2	Multimeter		No.	1

Necessary Materials

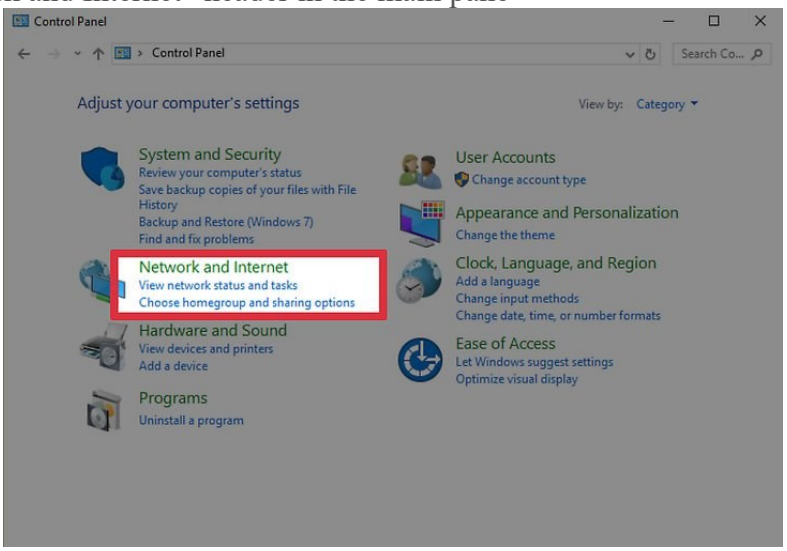
Sl. No.	Name of materials	Specification	Unit	Quantity
6	UTP Cable	CAT6 or CAT5	meter	10
7	RJ 45 Connector		No.	2
8	Router	4/5 Port Minimum	No.	1
9	NET Switch		No.	1
10	Computer/Laptop		No.	2

Task Sheet-3.2: Share Documents And Files

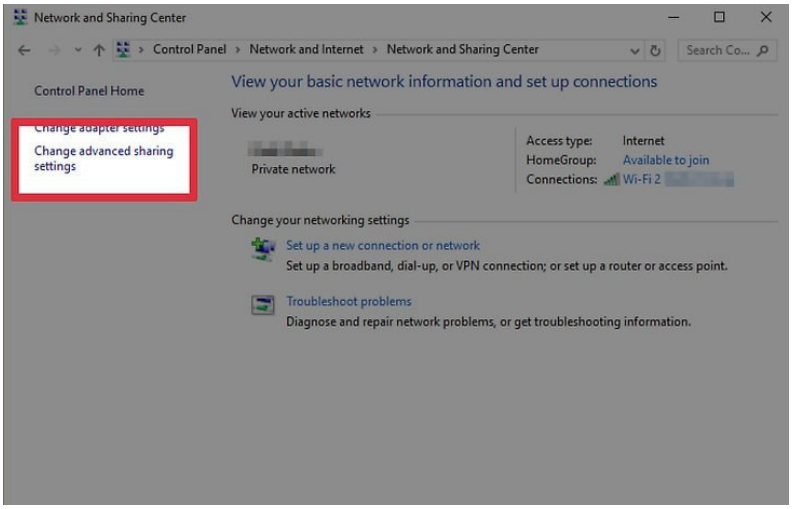
Performance Objective: At the end of this task, the trainee should be able to Share Documents and files.

Working steps:

Step 1. Collect the PPE
Step 2. Collect the required Tools & Equipment's
Step 3. Prepare the Lan Cable Standard of T568B,
Step 4. Type "Control Panel" in Search box and press ↵ Enter. you'll see the Control Panel.
Step 5. Click the "View network status and tasks" link. This link appears just beneath the "Network and Internet" header in the main pane

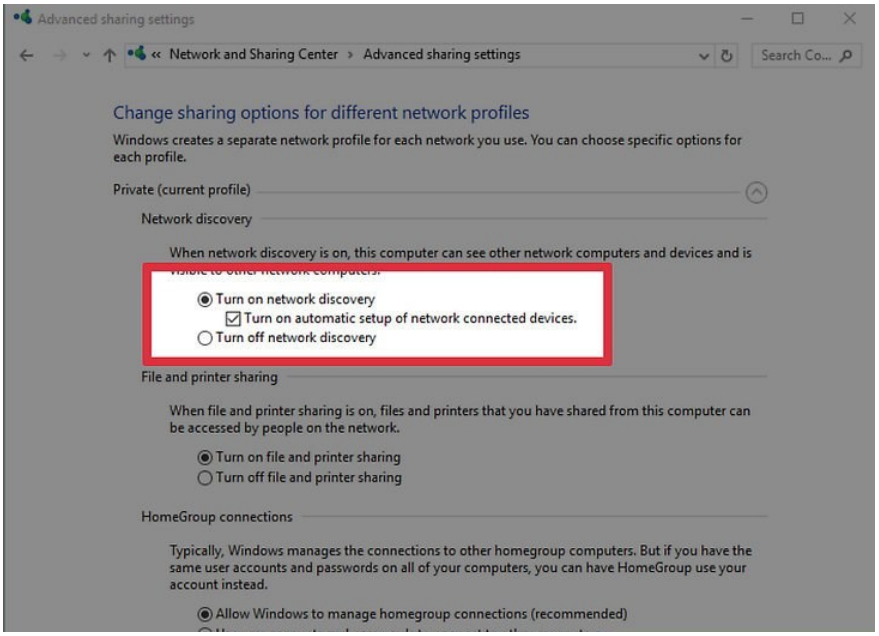


Step 6. **Click "Change advanced settings."** Now you'll see options for File and Printer sharing.

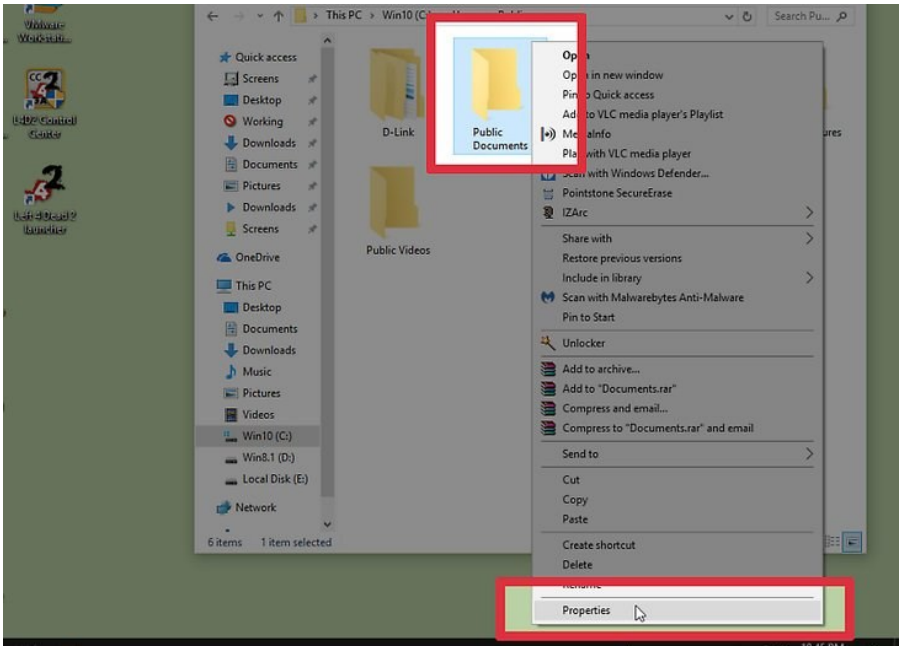


Step 7. **Select "Turn on file and printer sharing" and click "Save Changes."** If you are prompted to enter your Administrator password to save the changes, do so.

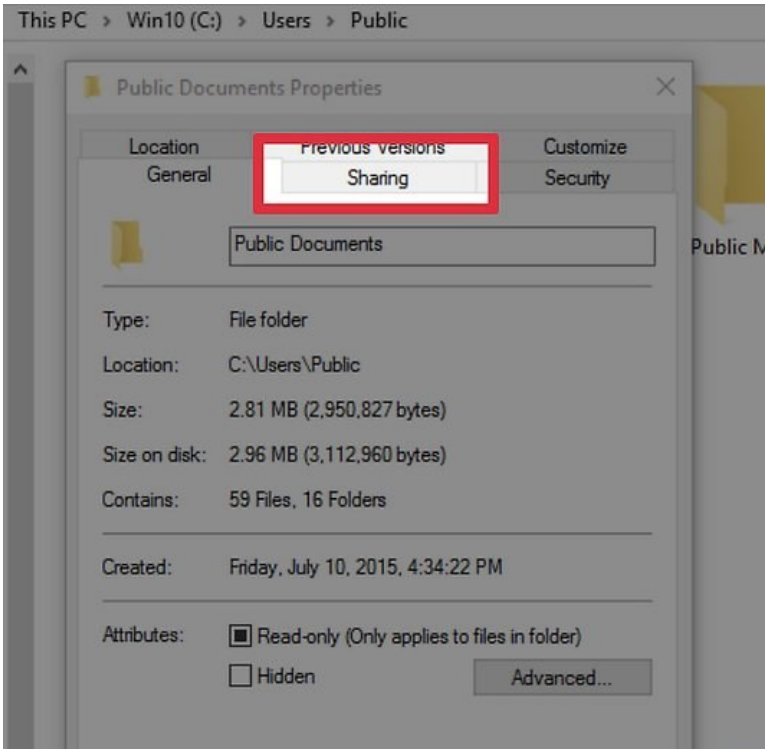
Note: Screenshot shows "Turn on network discovery", it should have been *File and printer sharing*



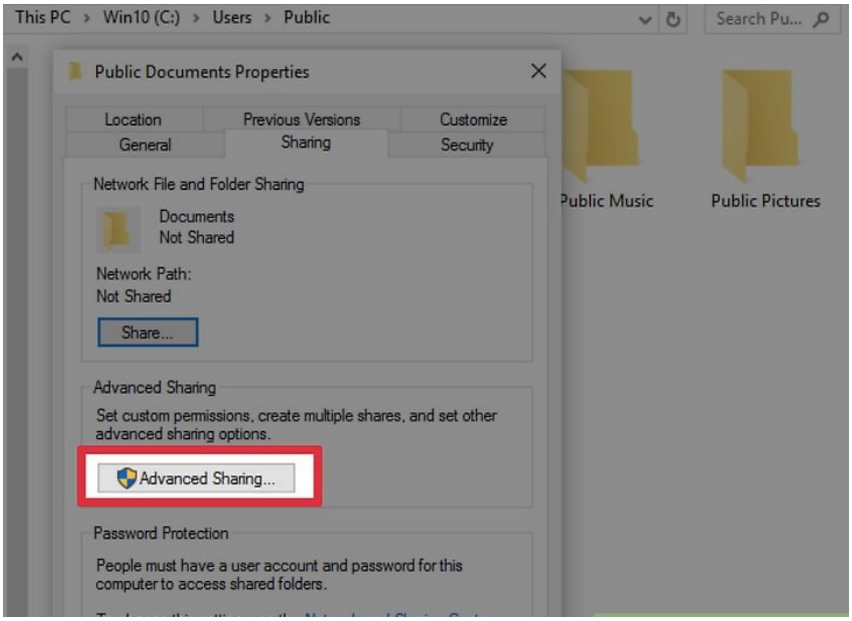
Step 8. **Navigate to the folder you want to share.** You'll need to select a folder to share rather than an individual file. **Right-click the folder and select "Properties."** A Properties panel for this folder will appear on the screen



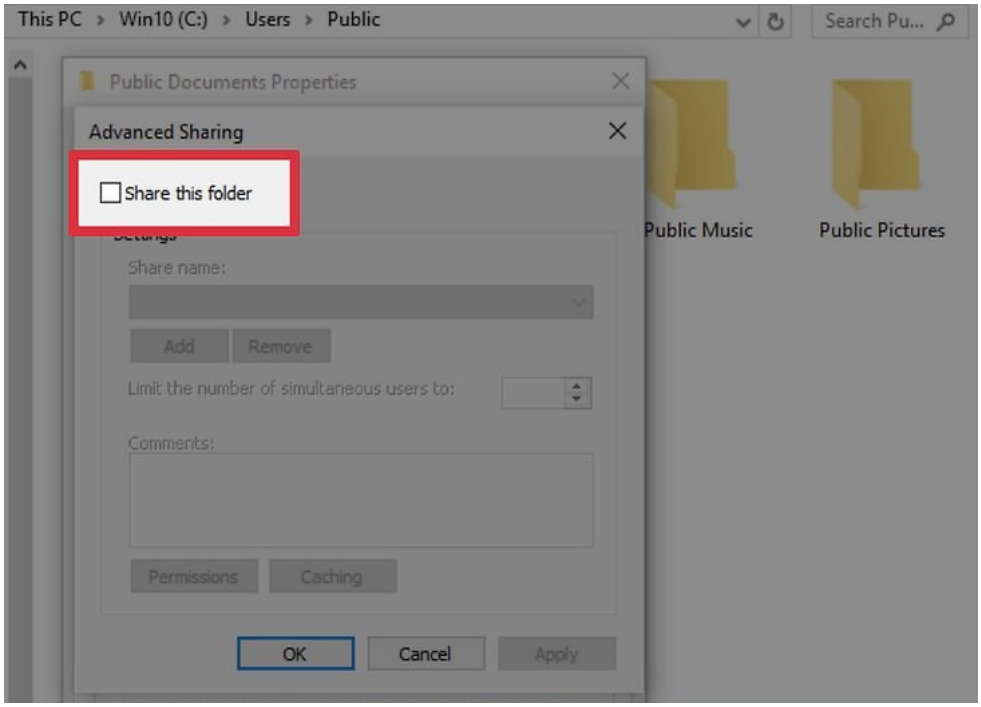
Step 9. **Click to the "Sharing" tab.** Since the folder is not yet shared, you'll see "Not Shared" just below its name under "Network File and Folder Sharing."



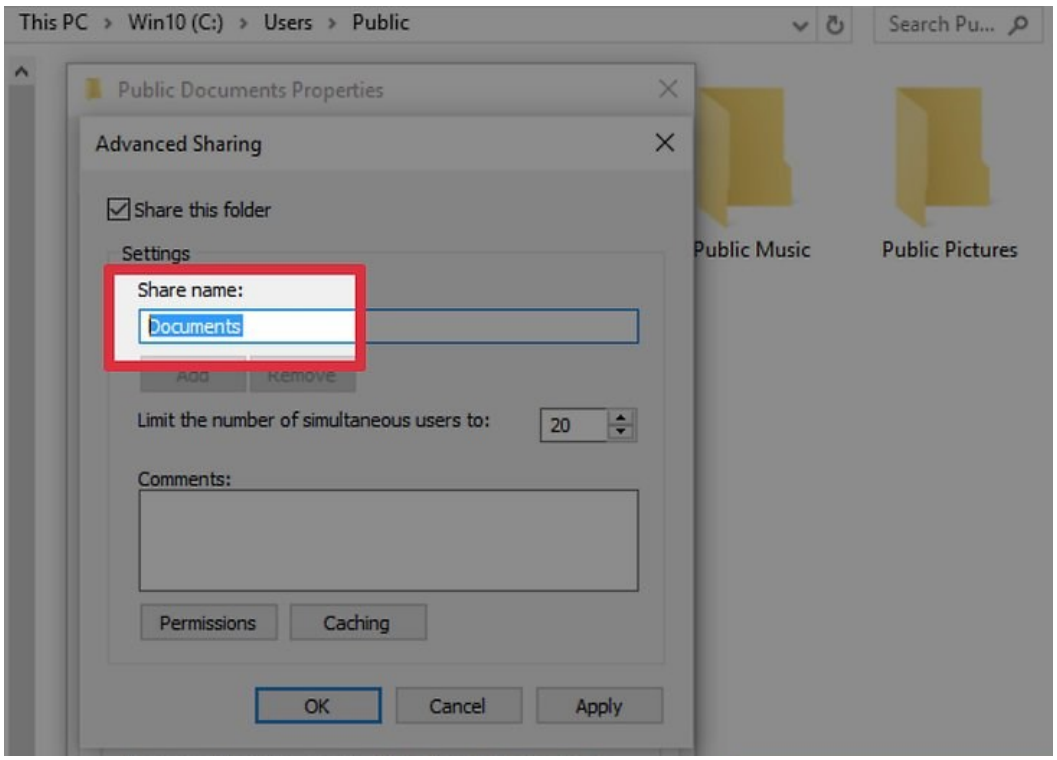
Step 10. **Click the "Advanced Sharing" button.** The contents of this window are mostly grayed-out.



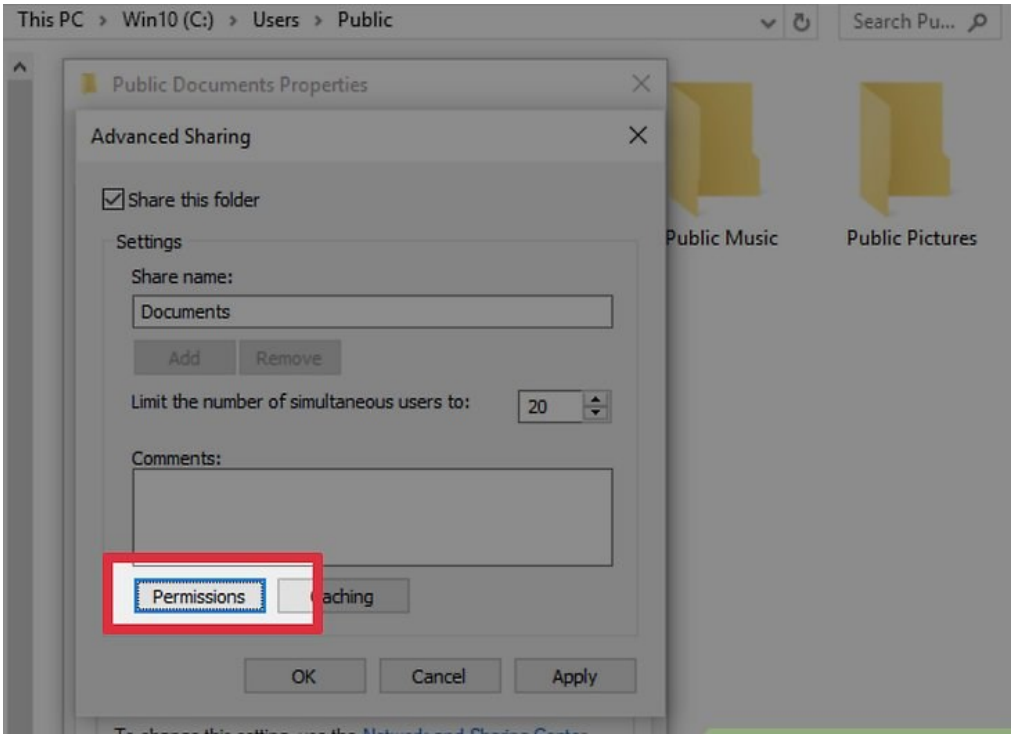
Step 11. **Place a check next to "Share this folder."** The previously grayed-out contents are now editable.



Step 12. Type **a name for the shared folder under "Shared Name."** The name you type here is what other users will see when they access the folder.

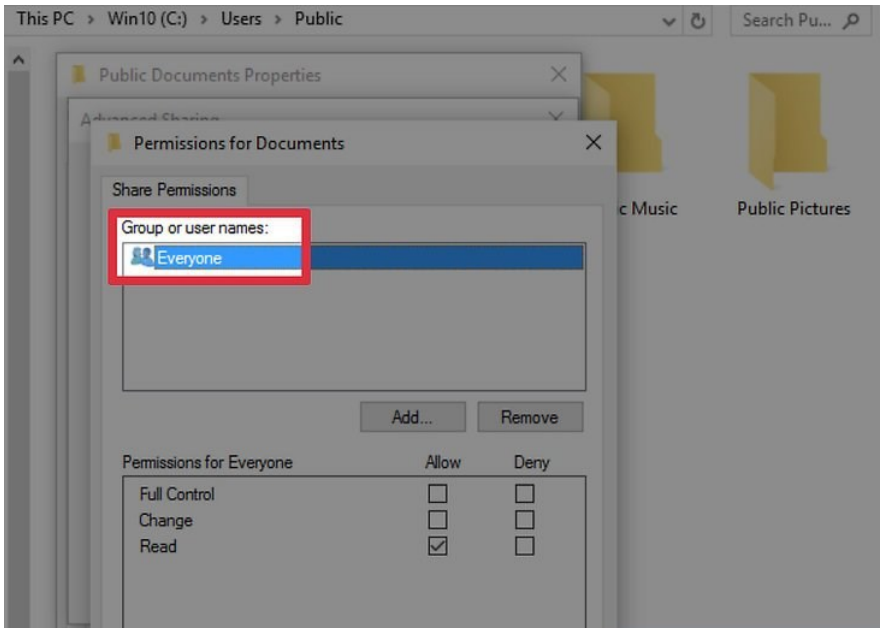


Step 13. **Click the "Permissions" button.** Now you'll set the permissions for all users on the network who will access the folder



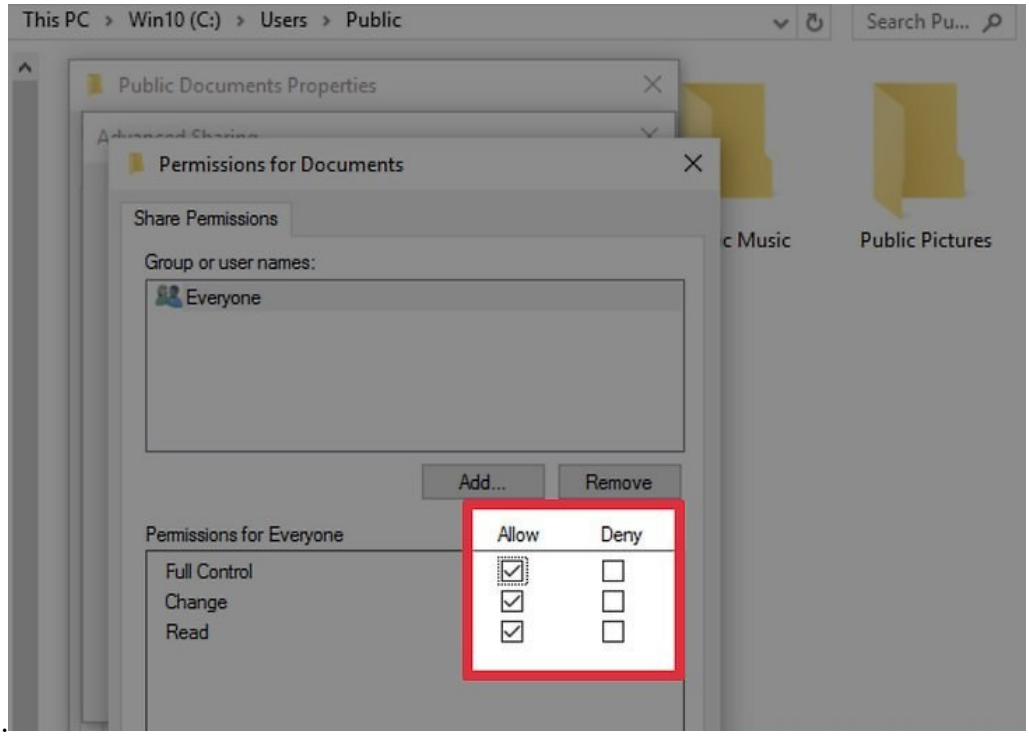
Step 14. Click **to highlight the "Everyone" group.** When this group is selected, you'll be able to change everyone on the network's permissions for this folder at once.

- If you'd rather just share the folder with one person, click "Add" and then select the person's username from the list. Then, click to select that user.



Step 15. **Set the permissions for the user(s) you selected.** Place checks next to "Allow" or "Deny" for each of the following options:

- Full Control: Allows everyone to read, delete, and edit files in this folder. This also grants this user the ability to change permissions on the folder.
- Change: Allows everyone to read, delete, and edit files in the folder but not change permissions.
- Read: Allows everyone to view files in the folder and run programs. Users cannot change files in the folder if this is the only option allowed.



Step 16. Click **"OK" to save your changes.** The folder is now shared.

Specification Sheet-3.2: Documents And File Sharing

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Hand Gloves	Pair	1
2	Apron	No.	1
3	Googles	No.	1
4	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Specification	Unit	Quantity
1	Cutting Plair	Wire Cutting Plair Multi size	No.	1
2	Wire Striper		No.	1
3	Clumping Tools	Clumping Tools for RJ45 Connector	No.	1
4	Star Screw Driver		No.	1

Necessary Equipment

Sl. No	Name of Equipment	Specification	Unit	Quantity
	Cable Tester	Cable Tester for RJ 45 Connection, Led & Buzzer System	No.	1
	Multimeter		No.	1

Necessary Materials

Sl. No.	Name of materials	Specification	Unit	Quantity
1	Router	4/5 Port Minimum	No.	1
2	NET Switch		No.	1
3	Computer/Laptop		No.	2

Task Sheet-3.3: Add Printer And Enable Sharing

Performance Objective: At the end of this task, the trainee should be able to install and configure SOHO Network.

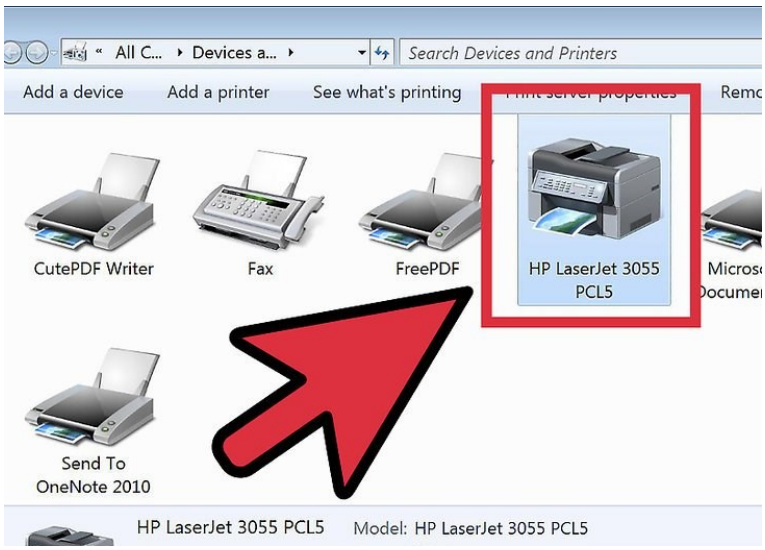
Working steps:

Step 1. Collect the PPE

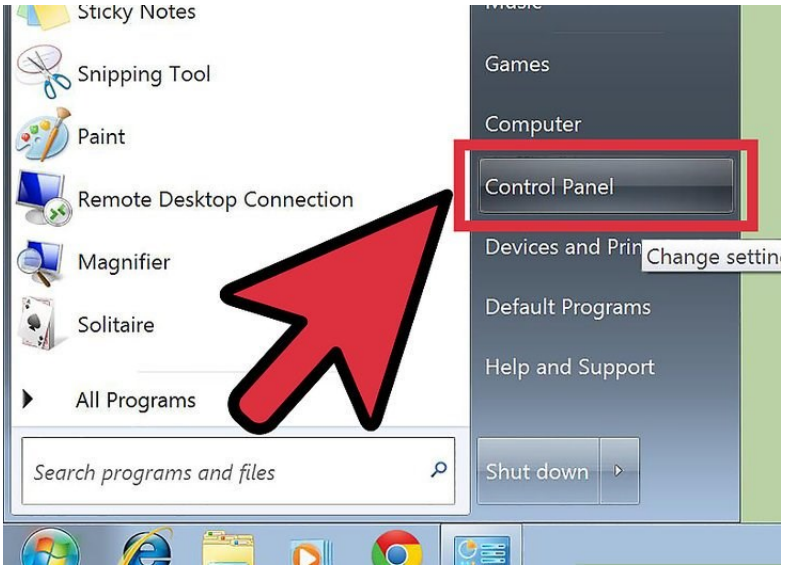
Step 2. Collect the required Tools & Equipment's

Step 3. Prepare the Lan Cable Standard of T568B,

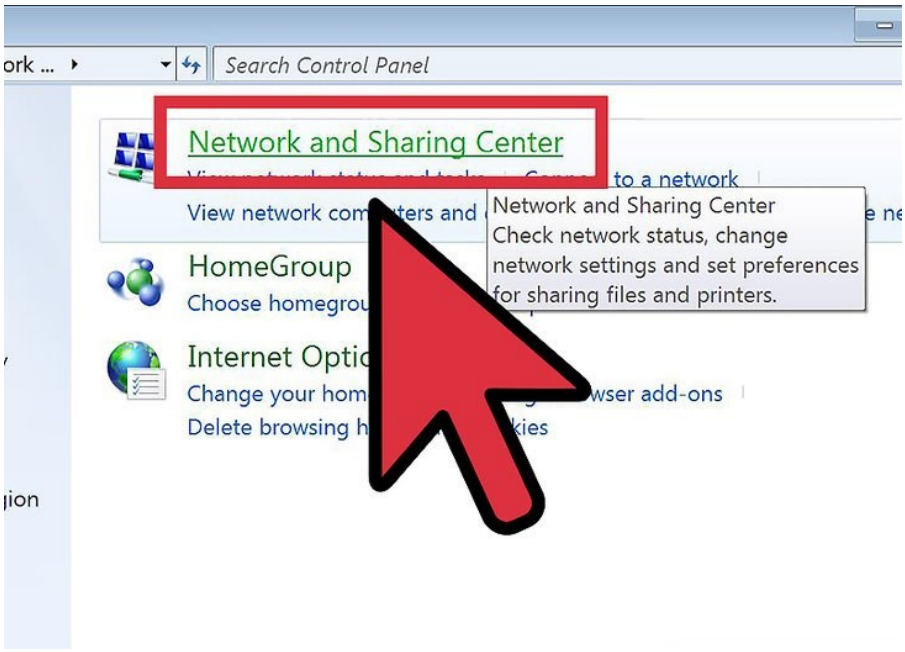
Step 4. Install the printer drivers. In order to share a printer, it must be installed on the computer it is connected to. Most modern printers connect via USB and will install automatically when they are connected.



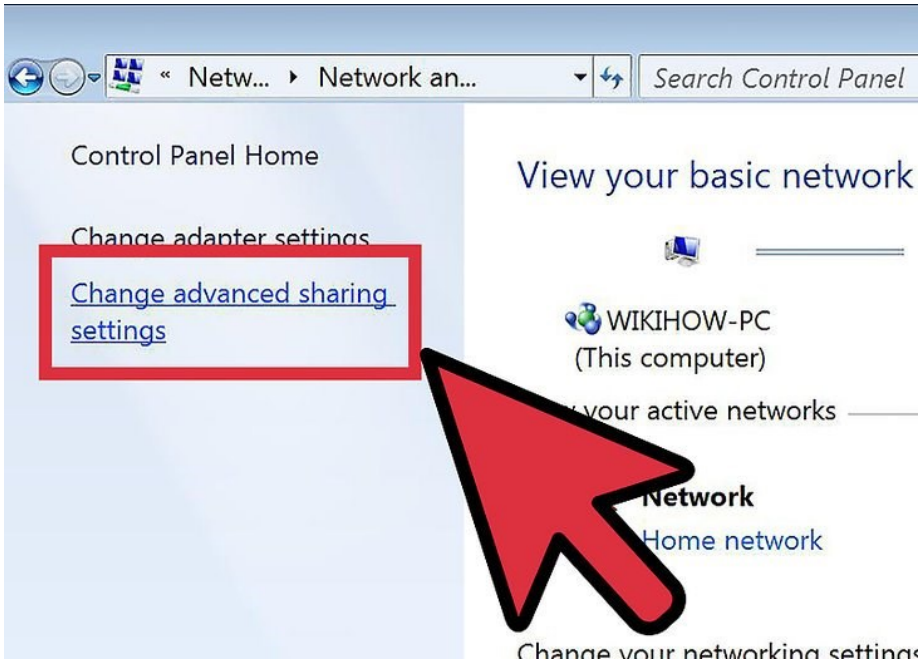
Step 5. Open the Control Panel. You can access the Control Panel in Windows by clicking the Start menu and selecting Control Panel.



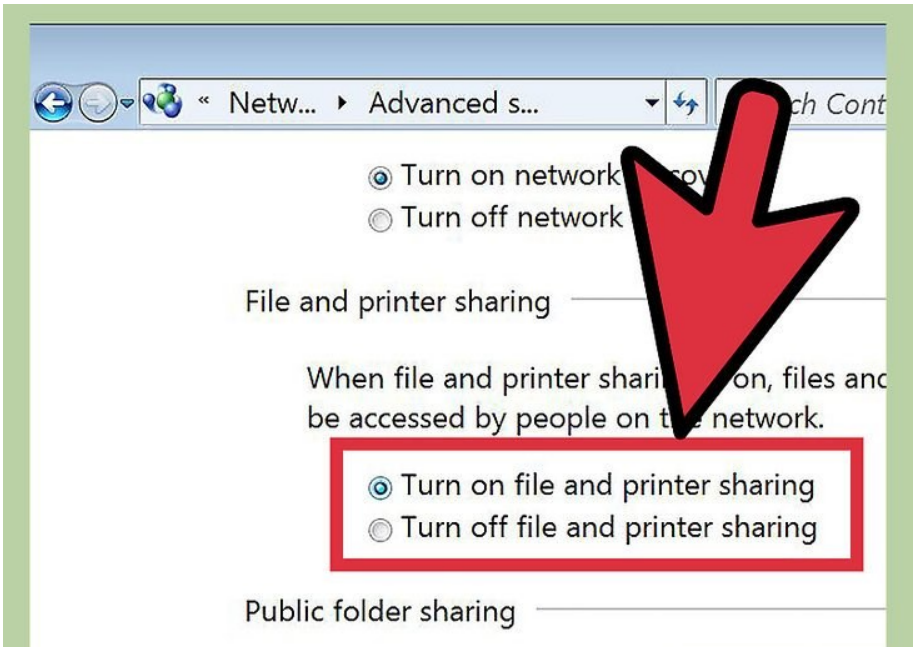
Step 6. **Open the Network and Sharing Center.** your Control Panel is in Category view, click "Network and Internet", and then select "Network and Sharing Center". Click on "Network and Internet". If your Control Panel is in Icon view, click the "Network and Sharing Center" icon.



Step 7. Click the "Change advanced sharing settings" link. This is located in the left navigation pane of the Network and Sharing Center.

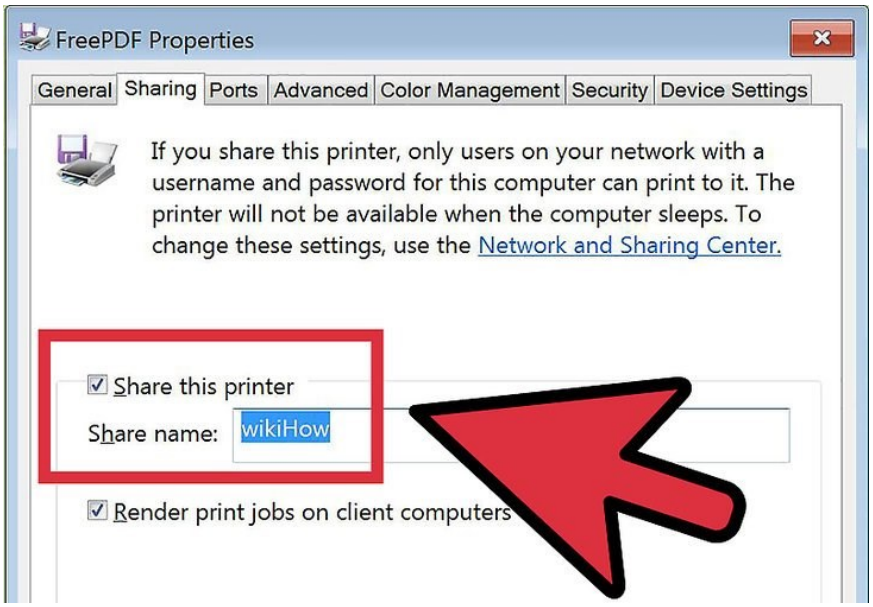


Step 8. Enable "File and printer sharing". Toggle this on to allow other devices to connect to your printer. This will also allow you to share files and folders with other computers on the network.



Step 9. Toggle the password protection. You can decide whether or not you want to enable password protection for your printer. If it is turned on, only users who have a user account on your computer will be able to access the printer.

Step 10. **Share the printer.** Now that file and printer sharing has been turned on, you will need to share the printer itself. To do this, go back to the Control Panel and open the Devices and Printers option. Right-click on the printer you want to share and click "Printer properties". Click the Sharing tab, and then check the "Share this printer" box.



Step 11. Connecting to a Shared Printer

Add a network printer in Windows. Open the Control Panel and select "Devices and Printers". Click the "Add a printer" button at the top of the window. Wait for the scan to complete, and the printer should appear in the list of available printers. Select it and click Next to add it to your computer.

Specification Sheet-3.3: Documents And File Sharing

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Hand Gloves	Pair	1
2	Apron	No.	1
3	Googles	No.	1
4	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Specification	Unit	Quantity
1	Cutting Plair	Wire Cutting Plair Multi size	No.	1
2	Wire Striper		No.	1
3	Clumping Tools	Clumping Tools for RJ45 Connector	No.	1
4	Star Screw Driver		No.	1

Necessary Equipment

Sl. No	Name of Equipment	Specification	Unit	Quantity
	Cable Tester	Cable Tester for RJ 45 Connection, Led & Buzzer System	No.	1
	Multimeter		No.	1

Necessary Materials

Sl. No.	Name of materials	Specification	Unit	Quantity
1	Router	4/5 Port Minimum	No.	1
2	NET Switch		No.	1
3	Computer/Laptop		No.	2

Learning Outcome-4: Implement Wireless SOHO Network

Assessment Criteria	1 Wireless Configuration requirements are identified 2 Tools and equipment for wireless configuration are selected and collected 3 Materials and consumables are collected 4 Wireless SOHO Networks is installed and configured. 5 Necessary settings for WLAN are configured 6 IP address is Assigned as required 7 Computer name is ensured and workgroup name are documented and confirmed 8 Documents and file sharing setting are confirmed 9 Printer is added and enable sharing are confirmed 10 Access requirements are determined and sharing is confirmed
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Switch 6. Router 7. Networking related Tools and accessories 8. Multimedia Projector 9. Paper, Pen, Pencil and Eraser
Contents	1 Configuration requirements for wireless SOHO network 2 Tools and equipment's required for stablishing wireless 3 SOHO 3.1 Switch 3.2 Router 3.3 Access point 4 Installation and configuration technique of wirless SOHO Networks 5 Settings of WLAN configuration 6 IP address 7 Subnet mask 8 TCP / IP protocol 9 IPv4, Ipv6 10 Document and file sharing technique 11 Printer sharing technique for both normal and network printer 12 Access requirements for resource sharing

Training Methods	▪ Blended ▪ Discussion ▪ Presentation ▪ Demonstration ▪ Guided Practice ▪ Individual Practice ▪ Project Work ▪ Problem Solving ▪ Brainstorming
Assessment Methods	Assessment methods may include but not limited to ▪ Written Test ▪ Demonstration ▪ Oral Questioning

Learning Experience-4: Implement Wireless SOHO Network

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
1. Trainee will ask the instructor about the learning materials	1. Instructor will provide the learning materials "Implement wireless SOHO network"
2. Read the Information sheet and complete the Self Checks & Check answer sheets on "Implement wireless SOHO network"	2. Read Information sheet 1: Implement wireless SOHO network 3. Answer Self-check 1: Implement wireless SOHO network 4. Check your answer with Answer key 1: Implement wireless SOHO network
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	5. Job/Task Sheet and Specification Sheet Task Sheet 4.1: Install and Configure wireless SOHO Networks Specification Sheet 4.1: Install and Configure wireless SOHO Networks Task Sheet 4.2: Share printer on Windows 10 Specification Sheet 4.2 Share printer on Windows 10 Task Sheet 4.3: Share Document and file Specification Sheet 4.3 Share Document and file

Information Sheet-4: Implement Wireless SOHO Network

Learning Objective:

After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

4.1 Configuration requirements for wireless SOHO network
4.2 Tools and equipment's required for stablishing wireless
4.3 SOHO network
- Switch
- Router
- Access point

4.4 Installation and configuration technique of wirless SOHO Networks
4.5 Settings of WLAN configuration
4.6 IP address
4.7 Subnet mask
4.8 TCP/IP protocol
4.9 IPv4, Ipv6
4.10 Document and file sharing technique
4.11 Printer sharing technique for both normal and network printer
4.12 Access requirements for resource sharing

4.1 Configuration requirements for wireless SOHO network

- Network Planning and Design
- Wireless Router Setup
- Wireless Security Configuration
- Network Addressing
- Quality of Service (QoS)
- Firmware Updates and Security Patching
- Monitoring and Management
- Documentation and Backup

4.2 Tools and equipment's required for stablishing wireless SOHO Network

Router: This is the central device that enables wireless communication between devices in your network and connects them to the internet.

Access Points (optional): If you have a large area to cover or if your wireless router's coverage is insufficient, you may need additional wireless access points to extend your network's range.

Ethernet Cables: Although wireless networking is the primary focus, you may still need Ethernet cables for initial setup and for connecting devices that don't support Wi-Fi or require a more stable connection.

Switch: If you have multiple wired devices to connect, you may need a network switch to expand the number of Ethernet ports available on your router.

Wireless Network Adapter (for devices without built-in Wi-Fi): Some older devices or desktop computers may require a separate wireless network adapter to connect to your wireless network.

Wireless Network Interface Cards (NICs): A wireless network interface card (NIC) helps establish wireless connectivity within the network. This card assures great mobility and flexibility when devices connect with each other wirelessly in the network.

Ethernet Media Converters: These devices play a crucial role in SOHO networks by ensuring flexibility and seamless interconnections. They help connect structured copper-based cabling systems with advanced fiber optic systems.

Security Software and Encryption: Ensure you have appropriate security software installed on your devices and configure encryption (such as WPA3) on your wireless network to protect against unauthorized access.

4.3 SOHO network

SOHO networks, standing for Small Office / Home Office architectures, are simple network setups primarily utilized in homes or small enterprises. They typically consist of a single device, often combining the functions of a router and a switch, providing internet access and network connectivity to connected devices such as PCs and printers.

SOHO architecture utilizes Ethernet technology to connect devices, enabling internet access through a switch/router. Devices connect via Ethernet cables such as CAT5 or CAT6. Wireless networking adds access points, providing internet access to connected devices.

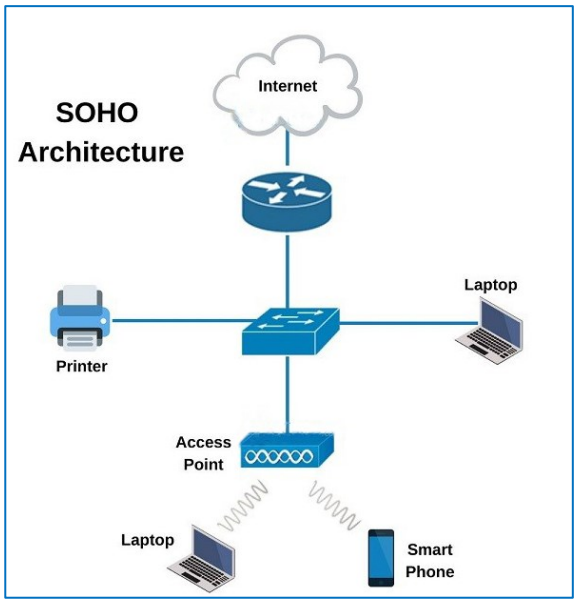


Figure: SOHO Network

A SOHO network involves setting up a local network within a smaller workspace, such as a home or small office, to enable devices to communicate and share resources. This network can be wired or wireless and usually incorporates a central router or hub that allows devices to connect and communicate.

SOHO Network equipments:

- **Switch:**

Figure: Switch

A network switch connects devices together on a single computer network. A switch is also called switching hub, bridging hub, or MAC bridge. Switches use MAC addresses to forward data to the correct destination. A switch is considered a Layer 2 device, operating at the data link layer; switches use packet switching to receive, process and forward data.

A network switch is a small hardware device that joins multiple computers together within one local area network (LAN). Switches are incapable of joining multiple networks or sharing an Internet connection. A switch acts as a controller, connecting computers, printers, and servers to a network in a building or a campus.

Switchs:

- Connect to multiple devices
- Control network access

- Monitor network usage
- Rapid communication with internal network
- Limited to devices plugged in via ethernet cable

Here are some of the most common types of network switches, with more info on each below:

- KVM Switch
- Managed Switch: Managed switches provide performance information, can be fully customized, and are fully configurable.
- Unmanaged Switch: An unmanaged switch has no settings to configure and simply plugs in and runs.
- Smart Switch
- PoE Switch

- **Router:**

A router is a networking device that connect multiple networks together. They also connect computers on those networks to the Internet. Routers enable all networked computers to share a single Internet connection, which saves money. A router acts a dispatcher. It analyzes data being sent across a network, chooses the best route for data to travel, and sends it on its way. Routers operate at Layer 3 (network layer) of the OSI model; a router uses the destination IP address in a data packet to determine where to forward the packet.

Figure: Router

Routers:

- Connect one network to another via modem
- Route traffic between devices and network
- Transmit packets between networks
- Provides Wi-Fi functionality

- **Access point: Access Point:** Access points are devices that extend the wireless coverage of a network. They allow wireless devices to connect to the network and access resources from areas with weak or non-existent wireless signals. Access points are easy to install and maintain and can be used to expand the coverage of your network, making them an ideal solution for small businesses and home offices. Access points also provide scalability, allowing you to add additional units to expand the range and capacity of your network as your business grows.

Fig: Wirelwss Access Point

Types of Access Points in Networking:

Root access point: Directly connected to a wired LAN and delivers a connection point for wireless users.

Repeater access point: Extends the range of the network by accelerating traffic between wireless users and the wired network.

Bridges: Joins multiple networks by determining a wireless link with alternative access point.

Workgroup bridge: Connects network-enabled devices to an access point, working as a client.

4.4 Installation and configuration technique of wirless SOHO Networks

To install and configure a wireless SOHO (Small Office/Home Office) network, you can follow these general steps:

i) **Determine Network Requirements:** Assess the specific needs of your SOHO environment, such as the number of devices, types of applications, and coverage area.

ii) **Select Network Equipment:** Choose the necessary networking hardware, including a modem, router (often with built-in wireless capability), and possibly additional access points for larger areas.

iii) **Connect the Swicth and Router:** Connect your Router to the internet service provider (ISP) and then connect the router to the Switch. This will form the basis of your network infrastructure.

iv) **Configure the Router:** Access the router's web-based setup page using a browser. Here, you will configure network settings like the SSID (network name), security settings (preferably WPA2 or WPA3), and passwords.

v) **Connect Devices to the Network:** Once the router is configured, you can start connecting devices wirelessly by selecting the network SSID and entering the password.

vi) **Enable Network Security:** Ensure that your network is secure by enabling firewall settings on the router and using strong, unique passwords for network access.

vii) **Share Network Resources:** Set up file sharing, printers, and other resources as needed within your network for easy access among connected devices.

4.5 Settings of WLAN configuration

To configure the settings of a WLAN (Wireless Local Area Network) on a Windows operating system, you can follow these steps:

i) **Access Network Settings:**

- Click on the **Start** menu and select **Settings**.
- Choose **Network & Internet** and then select **Wi-Fi.**

ii) **Open Wi-Fi Settings:**

- Under the Wi-Fi section, you will find options to change your network settings.
- Click on **Manage known networks** to view and configure your saved wireless networks.

iii) **Adjust Network Properties:**

- Select the network you wish to configure and click on **Properties**.
- Here, you can set the network profile type, manage IP settings, and configure other options like metered connections.

iv) **Advanced Adapter Options:**

- For more advanced settings, go back to the **Network & Internet** section and click on **Advanced network settings.**
- Under **Related settings**, select **More network adapter options.**
- Right-click on your wireless adapter and choose **Properties.**
- Navigate to the **Networking** tab to access properties like Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6).

v) **Configure Security Settings**:

- Within the Wi-Fi properties, you can also set up security options such as WPA2 or WPA3 encryption for secure connections.

4.6 IP address

An IP address, short for Internet Protocol address, is a distinctive numerical label assigned to every device connected to a computer network the Internet Protocol for communication. It performs two primary functions: it identifies the host or network interface, and it provides the location of the host in the network, allowing the establishment of a path to that host.

IP addresses can be **Static**, meaning they do not change, or **Dynamic**, meaning they can change each time a device connects to the internet.

There are two versions of IP addresses commonly in use:
IPv4: This is the original version and defines an IP address as a 32-bit number. Example: 192.0.2.1.
IPv6: This newer version was created to deal with the exhaustion of IPv4 addresses and uses 128 bits for the IP address, allowing for a much larger number of unique addresses. Example: 2001:db8:0:1234:0:567:8:1.

Class A Public & Private IP Address Range
Class A addresses are for networks with large number of total hosts. Class A allows for 126 networks by using the first octet for the network ID. The first bit in this octet, is always zero. The remaining seven bits in this octet complete the network ID. The 24 bits in the remaining three octets represent the hosts ID and allows for approximately 17 million hosts per network. Class A network number values begin at 1 and end at 127.

Public IP Range: 1.0.0.0 to 127.0.0.0
First octet value ranges from 1 to 127
Private IP Range: 10.0.0.0 to 10.255.255.255
Subnet Mask: 255.0.0.0 (8 bits)
Number of Networks: 126
Number of Hosts per Network: 16,777,214

Class B Public & Private IP Address Range
Class B addresses are for medium to large sized networks. Class B allows for 16,384 networks by using the first two octets for the network ID. The first two bits in the first octet are always 1 0. The remaining six bits, together with the second octet, complete the network ID. The 16 bits in the third and fourth octet represent host ID and allow for approximately 65,000 hosts per network. Class B network number values begin at 128 and end at 191.

Public IP Range: 128.0.0.0 to 191.255.0.0
First octet value ranges from 128 to 191
Private IP Range: 172.16.0.0 to 172.31.255.255 (See Private IP Addresses below for more information)
Subnet Mask: 255.255.0.0 (16 bits)
Number of Networks: 16,382
Number of Hosts per Network: 65,534

Class C Public & Private IP Address Range
Class C addresses are used in small local area networks (LANs). Class C allows for approximately 2 million networks by using the first three octets for the network ID. In a class C IP address, the first three bits of the first octet are always 1 1 0. And the remaining 21 bits of the first three octets complete the network ID. The last octet (8 bits) represent the host ID and allows for 254 hosts per network. Class C network number values begins at 192 and end at 223.

Public IP Range: 192.0.0.0 to 223.255.255.0
First octet value ranges from 192 to 223
Private IP Range: 192.168.0.0 to 192.168.255.255 (See Private IP Addresses below for more information)
Special IP Range: 127.0.0.1 to 127.255.255.255 (See Special IP Addresses below for more information)
Subnet Mask: 255.255.255.0 (24 bits)
Number of Networks: 2,097,150
Number of Hosts per Network: 254

Class D IP Address Range
Class D IP addresses are not allocated to hosts and are used for multicasting. Multicasting allows a single host to send a single stream of data to thousands of hosts across the Internet at the same time. It is often used for audio and video streaming, such as IP-based cable TV networks. Another example is the delivery of real-time stock market data from one source to many brokerage companies.
Range: 224.0.0.0 to 239.255.255.255
First octet value ranges from 224 to 239
Number of Networks: N/A
Number of Hosts per Network: Multicasting

Class E IP Address Class
Class E IP addresses are not allocated to hosts and are not available for general use. These are reserved for research purposes.

Range: 240.0.0.0 to 255.255.255.255
First octet value ranges from 240 to 255
Number of Networks: N/A
Number of Hosts per Network: Research/Reserved/Experimental

APIPA: Automatic Private IP Addressing (APIPA) is a feature in operating systems (such as Windows) that allows computers to self-configure IP addresses and subnet masks when their DHCP server is unavailable. The IP address range for APIPA is 169.254.0.1-169.254.255.254, with the subnet mask of 255.255.0.0.

Special IP Addresses
IP Range: 127.0.0.1 to 127.255.255.255 are network testing addresses (also referred to as loop-back addresses). These are virtual IP addresses; in that they cannot be assigned to a device. Specifically, IP 127.0.0.1 is often used to troubleshoot network connectivity issues using the ping command. Specifically, it tests a computer's TCP/IP network software driver to ensure it is working properly.

4.7 Subnet mask

A subnet mask is a 32-bit value that specifies the boundrary between the network prefix and suffix. 1 bit represent the network portion and 0 bits represent the host portion.

Dotted decimal IP	192.168.0.0/25	
Subnet Mask	255.255.255.128	
Equivalent dotted binary	11111111.11111111.11111111.	10000000
	Network bits	Host bit

4.8 TCP / IP protocol

An internet protocol called TCP/IP, also known as Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to connect network devices The TCP/IP protocol can also be used in a private network, such as an intranet or extranet.

The suite is designed to be robust, able to automatically recover from the failure of any device on the network. It includes several protocols, with TCP and IP being the two main ones:

This protocol defines how applications can create channels of communication across a network. It manages how a message is assembled into smaller packets before they are transmitted over the internet and ensures that packets are reassembled in the correct order at the destination address.

IP (Internet Protocol):

This protocol defines how to address and route each packet to ensure it reaches the right destination. Each gateway computer on the network checks the IP address to determine where to forward the message.

Common protocols included in the TCP/IP suite are:

HTTP (Hypertext Transfer Protocol): Handles communication between a web server and a web browser.

FTP (File Transfer Protocol): Manages the transmission of files between computers.

SMTP (Simple Mail Transfer Protocol): Used for sending emails.

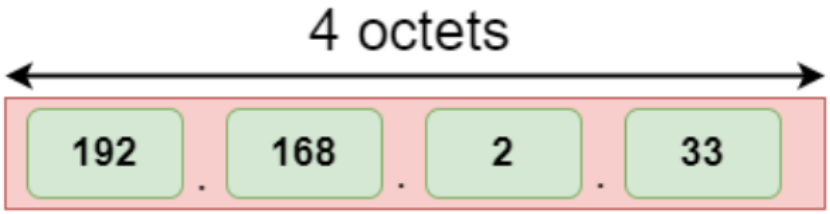
DNS (Domain Name System): Translates domain names to IP addresses.

4.9 IPv4, Ipv6

IPv4:

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

The address format of IPv4 is given bellow.



An IPv4 is a 32-bit decimal address. It contains 4 octets or fields separated by 'dot', and each field is 8-bit in size. The number that each field contains should be in the range of 0-255.

For example, 66.94.29.13

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

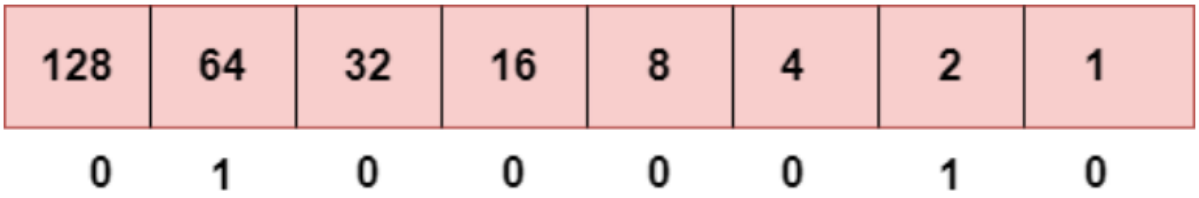
In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

Each bit in an octet can be either 1 or 0. If the bit the 1, then the number it represents will count, and if the bit is 0, then the number it represents does not count.

Representation of 8 Bit Octet

The above representation shows the structure of 8- bit octet.
Now, we will see how to obtain the binary representation of the above IP address, i.e., 66.94.29.13

Step 1: First, we find the binary number of 66.



To obtain 66, we put 1 under 64 and 2 as the sum of 64 and 2 is equal to 66 (64+2=66), and the remaining bits will be zero, as shown above. Therefore, the binary bit version of 66 is 01000010.

Step 2: Now, we calculate the binary number of 94.

128	64	32	16	8	4	2	1
0	1	0	1	1	1	1	0

To obtain 94, we put 1 under 64, 16, 8, 4, and 2 as the sum of these numbers is equal to 94, and the remaining bits will be zero. Therefore, the binary bit version of 94 is 01011110.

Step 3: The next number is 29.

128	64	32	16	8	4	2	1
0	0	0	1	1	1	0	0

To obtain 29, we put 1 under 16, 8, 4, and 1 as the sum of these numbers is equal to 29, and the remaining bits will be zero. Therefore, the binary bit version of 29 is 00011101.

Step 4: The last number is 13.

128	64	32	16	8	4	2	1
0	0	0	0	1	1	0	1

To obtain 13, we put 1 under 8, 4, and 1 as the sum of these numbers is equal to 13, and the remaining bits will be zero. Therefore, the binary bit version of 13 is 00001101.

IPv6:

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

- Dual stacking: It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.
- Tunneling: In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
- Network Address Translation: The translation allows the communication between the hosts having a different version of IP.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion (3.4*1038) addresses.

IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time.

The address format of IPv6 is given bellow.

IPv6 is a 128-bit hexadecimal address. It contains 8 fields separated by a colon, and each field is 16-bit in size.

Differences between IPv4 and IPv6

	Ipv4	Ipv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
VLSM	It supports VLSM (Virtual Length Subnet Mask). Here, VLSM means that Ipv4 converts IP addresses into a subnet of different sizes.	It does not support VLSM.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.

Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and Authentication	It does not provide encryption and authentication.	It provides encryption and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

4.10 Document and file sharing technique

Document and file sharing techniques vary depending on factors such as the size of the files, the number of users involved, security requirements, and the infrastructure available. Here are several common techniques for document and file sharing:

Email Attachments: One of the simplest methods for sharing files is through email attachments. Users can attach documents or files to an email message and send them to one or more recipients. However, email attachments are limited in size, and large files may not be suitable for this method.

File Transfer Protocol (FTP): FTP is a standard network protocol used for transferring files between a client and a server on a computer network. Users can upload files to an FTP server or download files from an FTP server using FTP client software.

File Sharing Services: There are many online file sharing services that allow users to upload and share files with others over the Internet. These services often provide features such as file synchronization, version control, and access control. Examples include Dropbox, Google Drive, Microsoft OneDrive, and Box.

Network File Sharing (SMB/CIFS): Network file sharing protocols such as Server Message Block (SMB) and Common Internet File System (CIFS) enable users to share files and folders over a local area network (LAN). Users can access shared files and folders from other computers on the network as if they were local files.

Peer-to-Peer (P2P) File Sharing: P2P file sharing allows users to share files directly with each other without the need for a central server. Users connect to a decentralized network and can download files from other users who have the same files available for sharing. Examples of P2P file sharing protocols include BitTorrent and Gnutella.

Cloud Storage: Cloud storage services allow users to store files and data online and access them from anywhere with an Internet connection. Users can share files with others by providing them with a link or granting them access to specific files or folders. Examples include Dropbox, Google Drive, Microsoft OneDrive, and Amazon S3.

Secure File Sharing: For sensitive or confidential files, organizations may use secure file sharing methods such as encrypted email, secure FTP (SFTP), or encrypted file sharing services that provide end-to-end encryption and other security features to protect data privacy.

Collaboration Platforms: Collaboration platforms and project management tools often include built-in document and file sharing capabilities. These platforms allow teams to collaborate on documents, share files, assign tasks, and track project progress in a centralized workspace. Examples include Microsoft Teams, Slack, Asana, and Trello.

4.11 Printer sharing technique for both normal and network printer

Sharing printers, whether they are normal (local) printers or network printers, allows multiple users to access a single printer, which can be cost-effective and convenient.

To share both types normal and network printers follow the given instructions:

Sharing a Normal (Local) Printer on a Windows Network:

8. Connect the printer to one of the computers and install the necessary drivers.
9. Open **Settings** on the computer connected to the printer.
10. Go to **Devices** > **Printers & scanners.**
11. Select the printer you want to share and click on **Printer properties**.
12. In the printer properties window, navigate to the Sharing tab.
13. Check the Share this printer option.
14. Assign a share name to the printer to easily identify it on the network.

Sharing a Network Printer:

1. Network printers are designed to connect directly to the network via Ethernet or Wi-Fi.
2. Install the printer drivers on each computer that needs access to the printer.
3. Use the printer's IP address to add it as a network printer on each computer:
   - Go to **Settings** > **Devices** > **Printers & scanners.**
   - Click **Add a printer or scanner.**
   - Choose **The printer that I want is not listed.**
   - Select **Add a printer using a TCP/IP address or hostname,** and enter the printer's IP address.

4.12 Access requirements for resource sharing

Access requirements for resource sharing, whether it's printers, files, or other network resources, depend on the specific resource being shared and the security considerations of the organization. However, some common access requirements for resource sharing include:

Authentication: Users should authenticate themselves before accessing shared resources to ensure that only authorized individuals can access sensitive information. Authentication methods may include usernames and passwords, biometric authentication, smart cards, or multi-factor authentication (MFA).

Authorization: Once authenticated, users must be authorized to access specific resources based on their roles, responsibilities, and permissions. Authorization

controls determine what actions users can perform on shared resources, such as read, write, modify, or delete permissions.

Access Control Lists (ACLs): Access control lists define the permissions granted to users or groups for accessing resources. ACLs specify which users or groups have access to specific resources and what actions they can perform on those resources. Administrators can configure ACLs to enforce security policies and restrict unauthorized access.

Group Policies: Group policies allow administrators to manage and enforce security settings, configurations, and access controls across multiple users and computers in an organization's network. Group policies can be used to define access restrictions, password policies, software installation rules, and other security-related settings.

Encryption: Encrypting shared resources helps protect sensitive information from unauthorized access or interception. Encryption techniques such as SSL/TLS (Secure Sockets Layer/Transport Layer Security) can secure data in transit, while encryption algorithms like AES (Advanced Encryption Standard) can protect data at rest.

Network Segmentation: Segregating network resources into separate segments or VLANs (Virtual Local Area Networks) can help limit the scope of resource access and mitigate the risk of unauthorized access or lateral movement by attackers. Network segmentation can be implemented using firewalls, routers, and access control mechanisms.

Auditing and Logging: Logging access to shared resources allows administrators to monitor user activity, track changes, and detect suspicious or unauthorized behavior. Auditing logs can provide valuable insights into who accessed which resources, when, and what actions were performed, aiding in security incident response and compliance efforts.

Compliance Requirements: Organizations may need to adhere to industry-specific regulations, standards, or internal policies governing access to sensitive information and resources. Compliance requirements may dictate specific access controls, encryption protocols, audit logging practices, and other security measures to protect sensitive data and ensure regulatory compliance.

What is File Sharing?

- Sharing of data on a network
- Allows multiple users to access a particular file /folder by enabling them to
  - Read
  - Modify
  - Copy or
  - Print

Type of File Shiring

- Default Share
  - Dose not Provide security.
  - Requires no configaration.
  - Require share desination
  - Default local share or Default network share.
- Restricted share
  - Provides security by limiting the number of users accessing the share at a particular time.
  - Designate specific user to access the share
  - Allot permissions to control user activity on the share

Self-Check Sheet-4: Implement Wireless SOHO Network

1. What is Computer networking?

2. What is the purpose of a wireless router in a network?

3. Why might additional access points be necessary in a wireless network?

4. What role do Ethernet cables play in a wireless network?

5. What is the purpose of an IP address?

6. How many bits does an IPv4 address consist of?

7. What does APIPA stand for, and what does it allow computers to do?

Answer Key-4: Implement Wireless SOHO Network

1. **What is Computer networking?**

   Answer: Computer networking connects computing and IoT devices, facilitating data exchange and resource sharing through established protocols to transmit information over various physical or wireless technologies.
   Computing devices include laptops, desktops, servers, smartphones, tablets, and a growing number of IoT devices like cameras, door locks, doorbells, refrigerators, AV systems, thermostats, and sensors.

2. **What is the purpose of a wireless router in a network?**

   Answer: A **wireless** router serves as the central hub for wireless communication, connecting various devices to each other and to the internet.

3. **Why might additional access points be necessary in a wireless network?**

   Answer: Additional access points extend the wireless network's coverage, especially useful in large areas or where the router's signal is weak.

4. **What role do Ethernet cables play in a wireless network?**

   Answer: Ethernet cables are used for the initial setup of network devices and to provide a stable connection for devices that either do not have Wi-Fi capability or require a more reliable connection than wireless can provide.

5. **What is the purpose of an IP address?**

   Answer: An IP address is a numerical label assigned to devices on a network to identify them and facilitate communication.

6. **How many bits does an IPv4 address consist of?**

   Answer An IPv4 address consists of 32 bits.

7. **What does APIPA stand for, and what does it allow computers to do?**

   Answer: APIPA stands for Automatic Private IP Addressing, and it allows computers to self-configure IP addresses and subnet masks when their DHCP server is unavailable.

Task Sheet-4.1: Install And Configure Wireless SOHO Networks

Performance Objective: At the end of this task, the trainee should be able to Install and Configure wireless SOHO Networks.

Working steps:

Setting up a wireless Small Office/Home Office (SOHO) network involves configuring a wireless router or access point to provide Wi-Fi connectivity to devices within your home or office. Here's a step-by-step guide to installing and configuring a wireless SOHO network:

1. **Plan Your Network:**
   - Determine the coverage area for your wireless network.
   - Identify the devices you want to connect wirelessly, such as laptops, smartphones, tablets, and IoT devices.
   - Consider potential sources of interference and plan your wireless access point placement accordingly.
2. **Gather Necessary Equipment:**
   - Wireless router or access point: Choose a router or access point that fits your network's requirements in terms of coverage, speed, and features.
   - Ethernet cable: You'll need this to connect your router to your modem.
   - Power cables: Ensure you have power outlets available for your router and any additional access points.
3. **Physical Setup:**
   - Connect your wireless router to your modem using an Ethernet cable. The modem typically has a dedicated port labeled "Internet" or "WAN" for this purpose.
   - Power on your modem and router.
   - If you're setting up additional access points for extended coverage, place them in strategic locations and connect them to your router using Ethernet cables.
   - Power on your access points.
4. **Access Router Configuration:**
   - Open a web browser on a device connected to your network.
   - Enter the router's IP address into the address bar. This is typically something like 192.168.1.1 or 192.168.0.1. You can find this information in the router's manual or on a sticker on the router itself.
   - Log in to the router's admin interface using the default username and password. These are often "admin" for both the username and password, but consult your router's documentation for specifics.
5. **Configure Wireless Settings:**

- Navigate to the wireless settings section of the router's configuration interface.
- Set a name (SSID) for your wireless network. Choose a unique name that's easy to identify.
- Choose a security mode (WPA2-PSK is recommended for best security) and set a strong passphrase for your wireless network.
- Optionally, configure other wireless settings such as channel selection, transmit power, and guest network settings.

6. **Enable DHCP (Dynamic Host Configuration Protocol):**
   - DHCP automatically assigns IP addresses to devices on your network, simplifying the process of connecting new devices.
   - In the router's configuration interface, locate the DHCP settings and ensure DHCP is enabled.
7. **Test Your Network:**
   - Connect a wireless device to your network using the SSID and passphrase you configured.
   - Ensure that the device can access the internet and communicate with other devices on the network.
   - Test connectivity from multiple locations to ensure adequate coverage.
8. **Secure Your Network:**
   - Change the default admin username and password for your router to prevent unauthorized access.
   - Regularly update your router's firmware to patch security vulnerabilities.
   - Consider enabling features like MAC address filtering, firewall settings, and disabling WPS (Wi-Fi Protected Setup) if not needed.
9. **Document Your Network Configuration:**
   - Keep a record of your network settings, including the router's IP address, SSID, passphrase, and DHCP settings.
   - This documentation will be useful for troubleshooting and future reference.

Specification Sheet-4.1: Install And Configure Wireless SOHO Networks

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Hand Gloves	Pair	1
2	Apron	No.	1
3	Googles	No.	1
4	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Unit	Quantity
1	Network configuration software (e.g., router setup wizard)	No.	1
2	Wireless network management software	No.	1
3	Network monitoring tools	No.	1

Necessary Equipment

Sl. No	Name of Equipment	Unit	Quantity
1	Wireless router or access point	No.	1
2	Wireless network adapters for devices (e.g., laptops, smartphones)	No.	1
3	Ethernet cables (for connecting wired devices to the router/access point)	Meter	100
4	Power outlets (for powering the router/access point)	No.	1

Necessary Materials

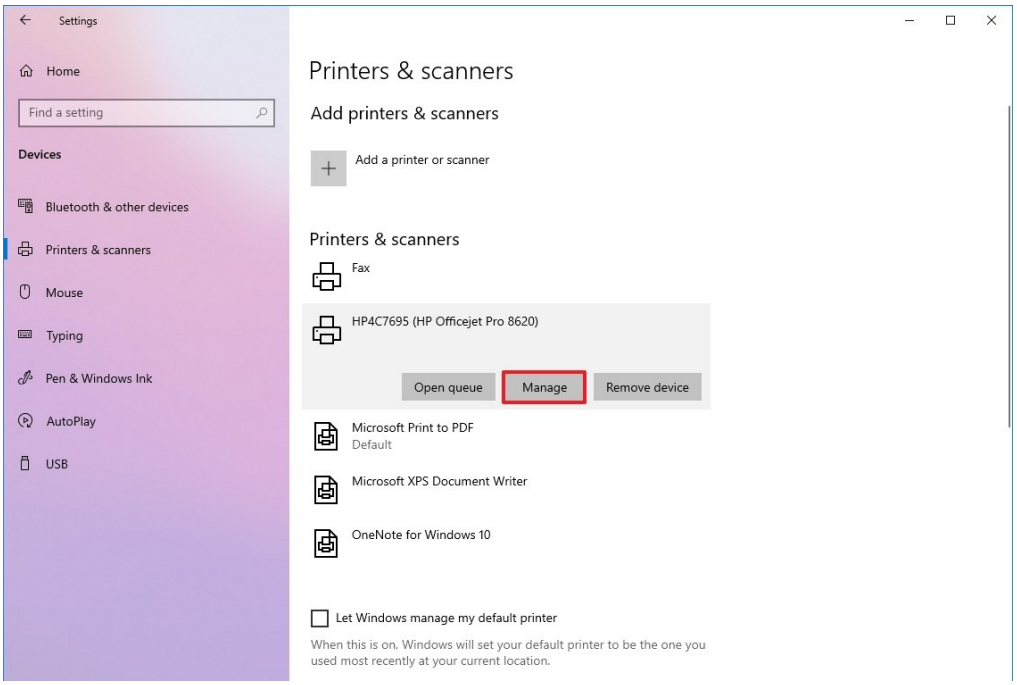
Sl. No.	Name of materials	Unit	Quantity
1	Documentation and manuals provided by the router/access point manufacturer	No.	1
2	Network access control policies	No.	1
3	Administrative credentials (username and password) for router/access point configuration	No.	1
4	Internet connection (from ISP)	No.	1

Task Sheet-4.2: Share Printer On Windows 10

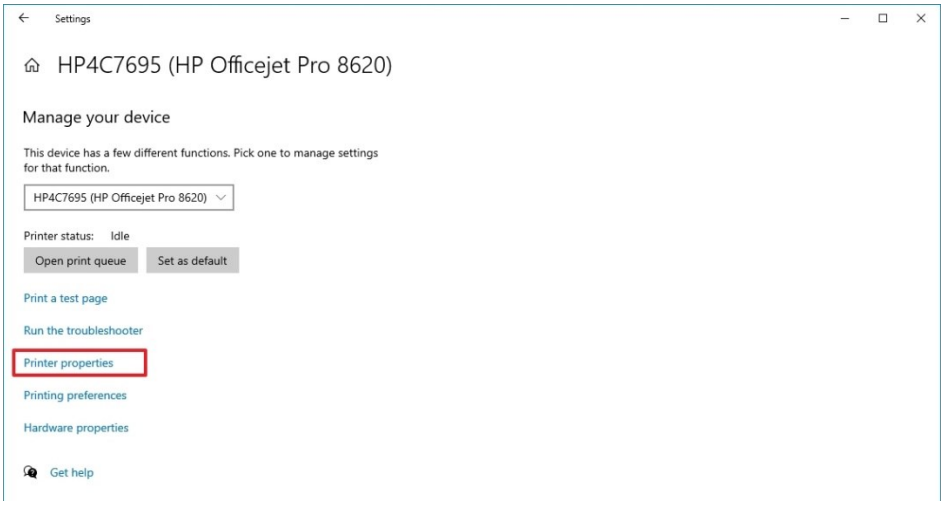
Performance Objective: At the end of this task, the trainee should be able to share printer on Windows 10.

Working steps:

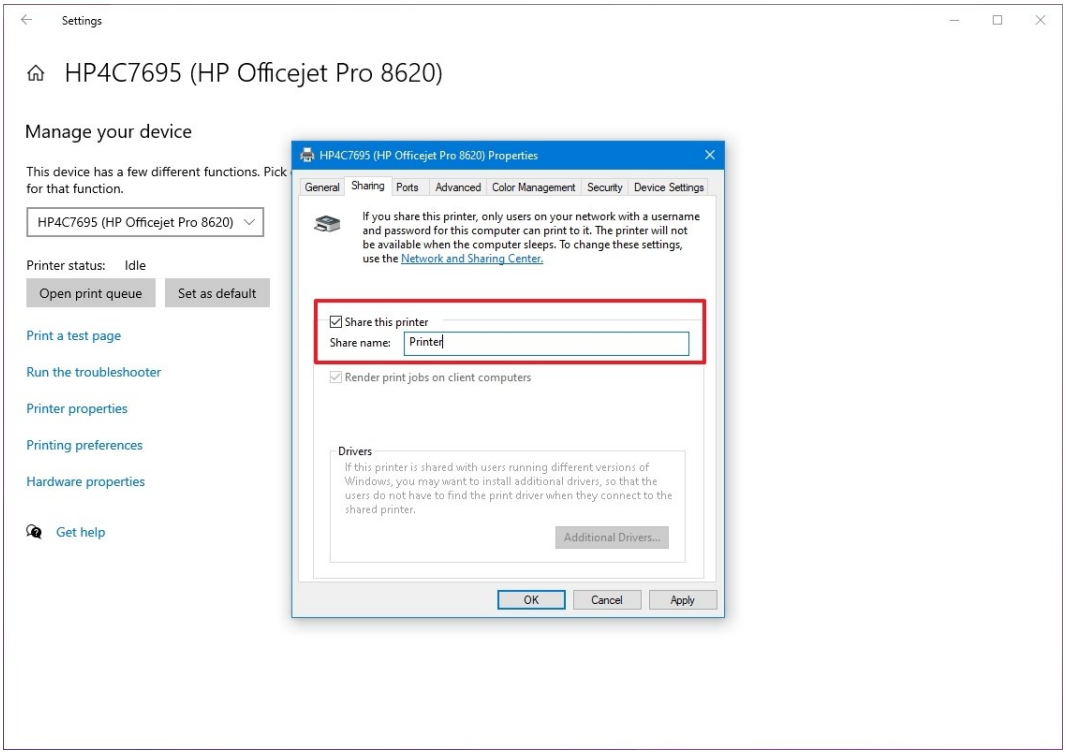
1. Open **Settings**.
2. Click on **Devices**.
3. Click on **Printers & scanners.**
4. Under the "Printer & scanners" section, select the printer to share in the network.
5. Click the **Manage** button.



6. Click the Printer **properties** option.



7. Click the **Sharing** tab.
8. Check the "**Share this printer**" option.
9. In the "Share name" field, specify a new short and descriptive name.



10. Click the **Apply** button.
11. Click the **OK** button.

Specification Sheet-4.2: Documents And File Sharing

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Hand Gloves	Pair	1
2	Apron	No.	1
3	Googles	No.	1
4	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Unit	Quantity
1		No.	1
2		No.	1
3		No.	1

Necessary Equipment

Sl. No	Name of Equipment	Unit	Quantity
1	Printer	No.	1
2	Computer	No.	1
3	Network connection (wired or wireless)	No.	1

Necessary Materials

Sl. No.	Name of materials	Unit	Quantity
1	Documentation and manuals provided by the printer manufacturer	No.	1
2	Administrative credentials	No.	1
3	Optional: Ethernet cable or Wi-Fi network for connecting the printer to the Windows 10 computer	No.	1
4	Optional: Printer drivers for other devices that will access the shared printer (may be required for proper printing functionality)	Set	1

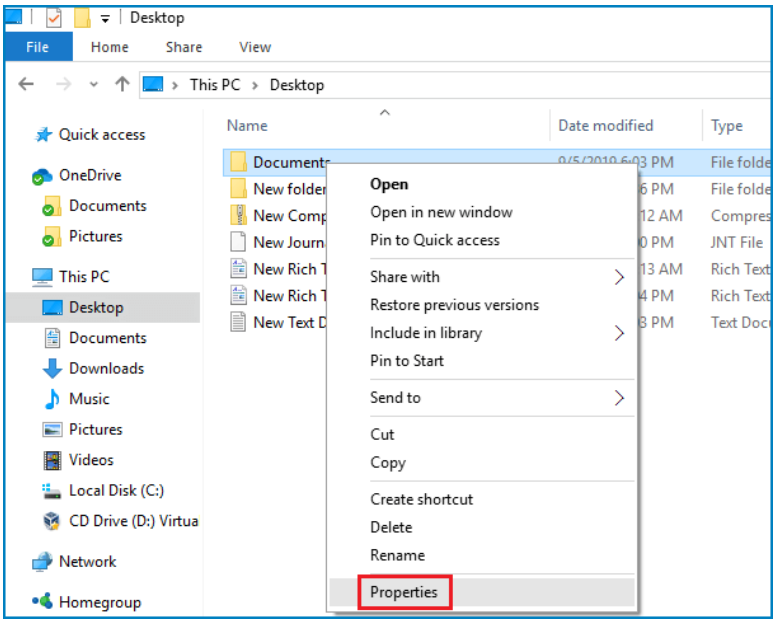
Task Sheet-4.3: Share Document And File

Performance Objective: At the end of this task, the trainee should be able to Share Document and file in SOHO Network.

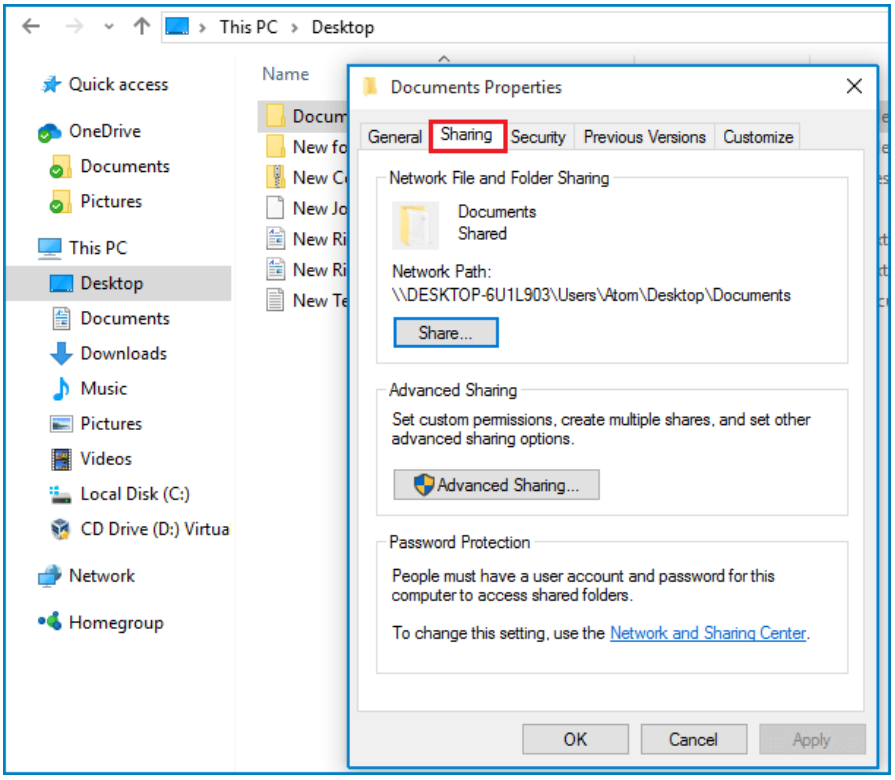
Working steps:

Step 1. Open **File Explorer** and go to the file or folder that you want to share.

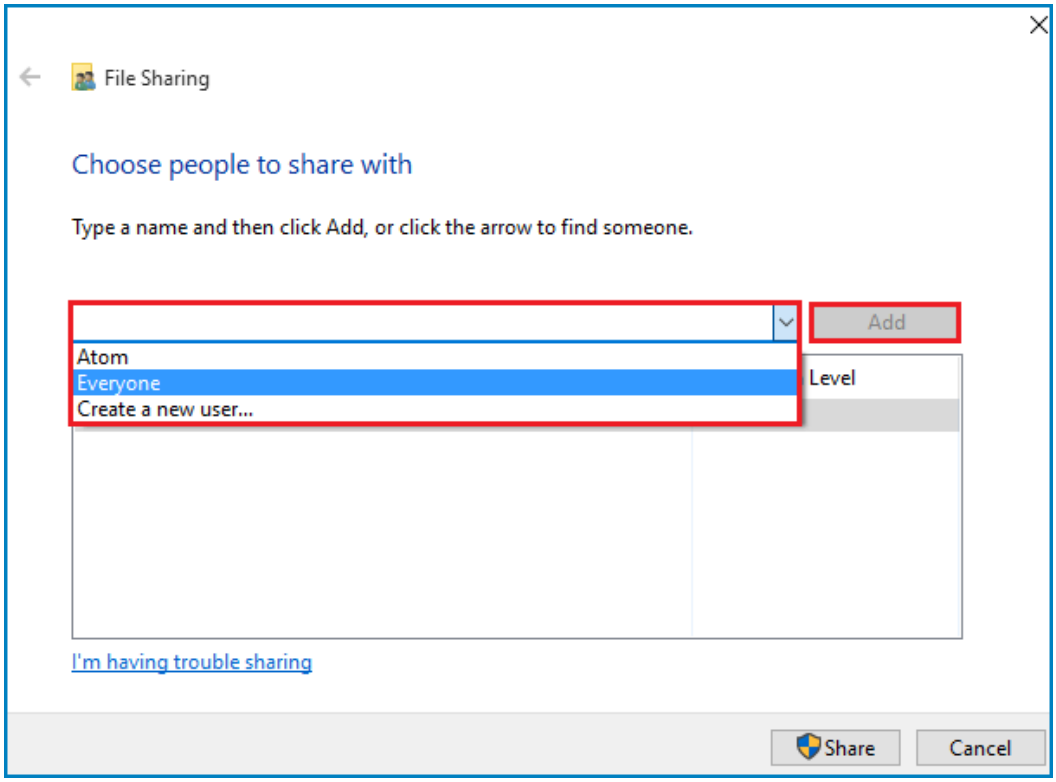
Step 2. Right click the folder and choose **Properties**.



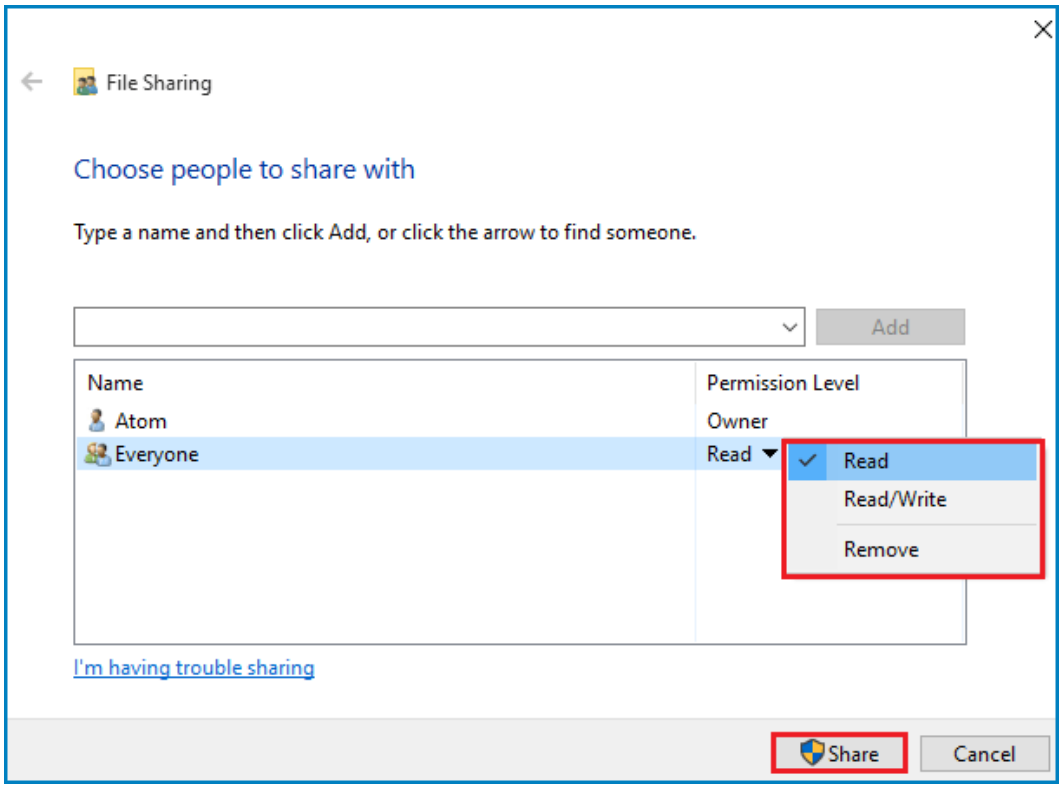
Step 3. In the **Document Properties** panel, select **Sharing** tab.



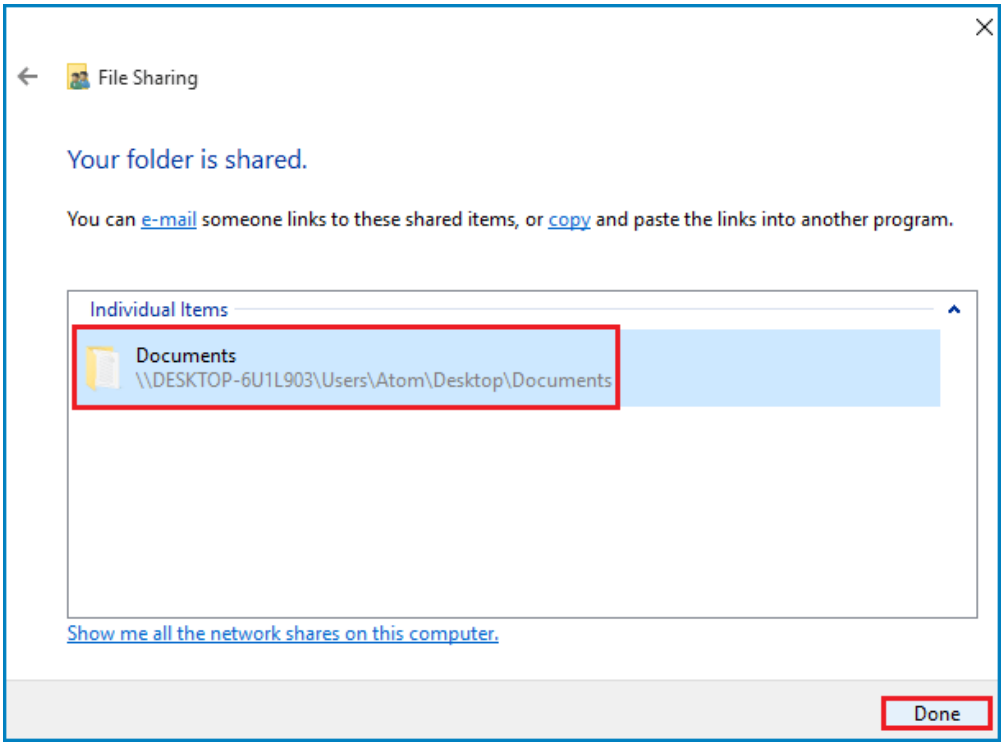
Step 4. Click the **Share** button under the Sharing tab.



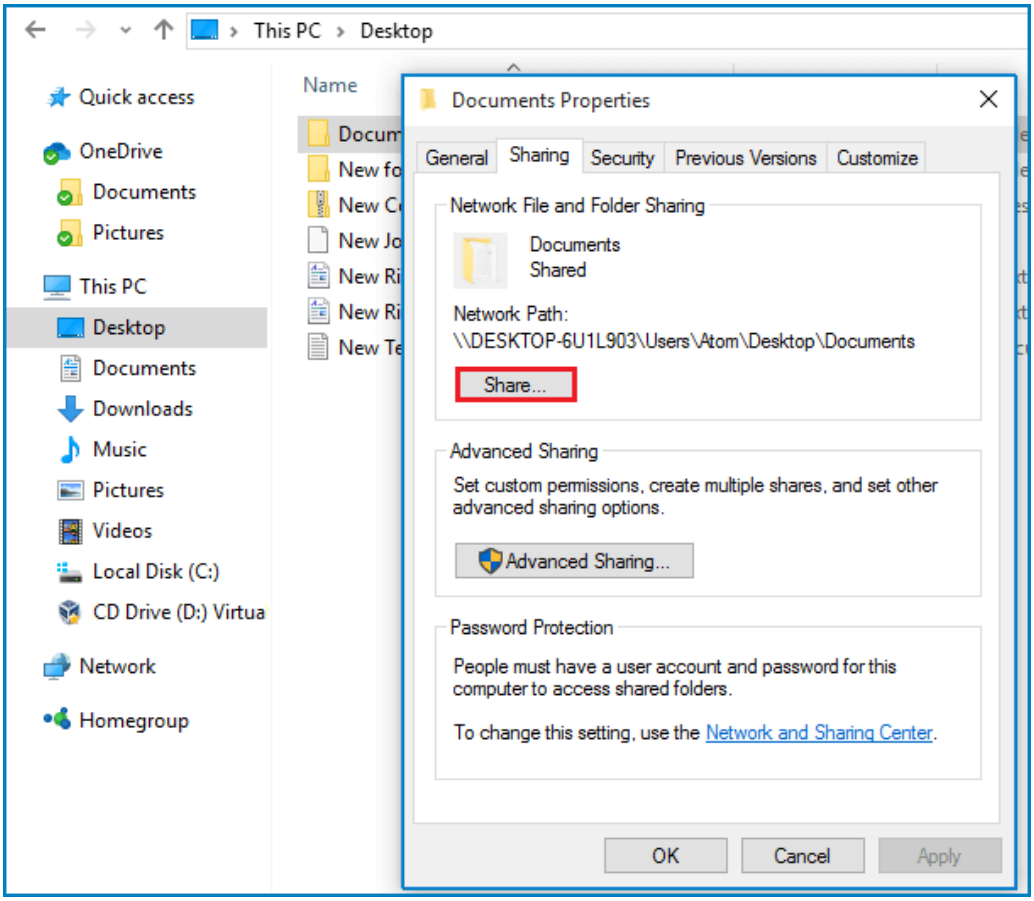
Step 5. Go to **Choose people to share** with to select the user or group, and then click **Add**.



Step 6. Select a type of **Permission Level**, and then click **Share button**.



Step 7. Note the file sharing network path, click the **Done** button, and then close the Document Properties panel.



Specification Sheet-4.3: Documents And File Sharing

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Hand Gloves	Pair	1
2	Apron	No.	1
3	Googles	No.	1
4	Safety Show	Pair	1

Necessary Equipment

Sl. No	Name of Equipment	Unit	Quantity
1	Printer	No.	1
2	Computer	No.	1
3	Network connection (wired or wireless)	No.	1

Necessary Materials

Sl. No.	Name of materials	Unit	Quantity
1	documentation and manuals provided by the operating system or file management software	No.	1
2	Administrative credentials (username and password) for the computer or server hosting the documents/files	No.	1
3	File organization structure (folders, directories) for organizing shared documents/files	No.	1
4	Optional: Backup solution for ensuring data integrity and availability	Set	1
5	Optional: File encryption software for securing sensitive documents/files		1

Learning Outcome-5: Secure SOHO Network

Assessment Criteria	1. Security problems for SOHO networking is interpreted 2. MAC filtering is interpreted 3. Unauthorize device is controlled 4. Default firewall is enabled
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Switch 6. Router 7. Networking related Tools and accessories 8. Multimedia Projector 9. Paper, Pen, Pencil and Eraser
Contents	1 Security problems of SOHO networking ▪ Zone Model ▪ Segmentation ▪ Sniffing ▪ ARP Interception 2 MAC filtering 3 MAC filtering technique 4 Unauthorize device control procedure 5 Default firewall
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning

Learning Experience-5: Secure SOHO Network

In order to achieve the objectives stated in this learning guide, you must perform the learning steps below. Beside each step are the resources or special instructions you will use to accomplish the corresponding activity.

Learning Activities	Recourses/Special Instructions
1. Trainee will ask the instructor about the learning materials	1. Instructor will provide the learning materials "Secure SOHO Network"
2. Read the Information sheet and complete the Self Checks & Check answer sheets on "Secure SOHO Network"	2. Read Information sheet 1: Secure SOHO Network 3. Answer Self-check 1: Secure SOHO Network 4. Check your answer with Answer key 1: Secure SOHO Network
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	5. Job/Task Sheet and Specification Sheet Task Sheet 5.1: Control unauthorize device in SOHO network Specification Sheet 5.1: Control unauthorize device in SOHO network

Information Sheet-5: Secure SOHO Network

Learning Objective:

After completion of this information sheet, the learners will be able to explain, define and interpret the following contents:

5.1 Security problems of SOHO networking
- Zone Model
- Segmentation
- Sniffing
- ARP Interception

5.2 MAC filtering
5.3 MAC filtering technique
5.4 Unauthorize device control procedure
5.5 Default firewall

5.1 Security problems of SOHO networking

Small Office/Home Office (SOHO) networking environments face several security challenges due to their typically limited resources, lack of dedicated IT staff, and often less stringent security measures compared to larger enterprises. Some common security problems encountered in SOHO networking include:

Weak Passwords: Users may set weak or default passwords for network devices, such as routers and Wi-Fi access points, leaving them vulnerable to brute force attacks or unauthorized access.

Outdated Firmware and Software: Failure to regularly update firmware and software on networking devices, computers, and other connected devices can leave them susceptible to known vulnerabilities and exploits.

Lack of Encryption: Failure to encrypt sensitive data transmitted over the network, such as login credentials, financial information, or personal data, can lead to interception by attackers.

Default Configurations: Many SOHO networking devices come with default configurations that are insecure, such as open Wi-Fi networks, default administrative credentials, and unnecessary open ports, making them easy targets for attackers.

No Firewall or Misconfigured Firewall: Lack of a firewall or misconfigured firewall rules can expose the network to unauthorized access and attacks from the internet.

Unauthorized Access: Failure to secure remote access to network devices, such as routers and surveillance cameras, can lead to unauthorized access by attackers.

Phishing and Social Engineering: Users in SOHO environments may be more susceptible to phishing attacks and social engineering tactics due to lack of security awareness training and education.

BYOD (Bring Your Own Device) Risks: Employees and family members may connect personal devices to the network without adequate security measures, introducing malware, viruses, and other threats.

Physical Security: Lack of physical security for networking equipment, such as routers and switches, can result in unauthorized access or tampering by individuals with physical access to the premises.

IoT (Internet of Things) Devices: Many SOHO networks incorporate IoT devices with poor security practices, such as default passwords, lack of regular updates, and vulnerabilities that can be exploited by attackers.

Data Backup and Recovery: Failure to implement regular data backup procedures and disaster recovery plans can result in data loss due to hardware failures, malware attacks, or other unforeseen events.

Zone Model

The Zone Model is a network security approach that involves breaking down a network into different zones or segments based on their security requirements and trust levels. Each zone represents a distinct level of security and access controls. For instance, a typical zone model might include the Internet, DMZ (Demilitarized Zone), internal networks, and highly secure internal networks. Security policies are then implemented to regulate traffic flow between these zones, with stricter controls enforced for traffic crossing between zones of differing trust levels.

Segmentation

Network segmentation is a technique that involves dividing a larger network into smaller subnetworks or segments. This helps to improve the performance, security, and manageability of the network. By segmenting the network, it is possible to control network traffic, limit the impact of security breaches, and enforce security policies more effectively. There are several methods that can be used to implement network segmentation, including VLANs (Virtual Local Area Networks), subnetting, and physical network segmentation.

Sniffing

"Sniffing" is a term used to describe the practice of capturing and analyzing network traffic. This is usually done for purposes such as monitoring, troubleshooting or even intercepting sensitive information. Network sniffing tools capture packets of data as they travel across a network and display their contents. While sniffing can be used for legitimate purposes by network administrators and security professionals, it can also be misused by attackers to eavesdrop on sensitive information such as passwords, usernames, and other confidential data.

ARP Interception

ARP (Address Resolution Protocol) interception is a technique used in network attacks to intercept and manipulate ARP traffic. ARP is responsible for resolving IP addresses to MAC addresses on a local network. In ARP interception attacks, an attacker sends forged ARP messages to associate their MAC address with the IP address of another device on the network. This redirects traffic intended for that device to the attacker's system. Such attacks can be used for various malicious purposes, such as intercepting traffic, launching man-in-the-middle attacks, or conducting network reconnaissance.

5.2 MAC filtering

MAC (Media Access Control) filtering is a security feature used in network devices such as routers, switches, and access points to control access to the network based on the MAC addresses of devices. Each network interface card (NIC) in a device has a unique MAC address assigned by the manufacturer.

MAC filtering works by creating a whitelist or blacklist of MAC addresses that are allowed or denied access to the network. When MAC filtering is enabled, the device checks the MAC address of incoming network traffic against the configured list and either permits or blocks the traffic accordingly.

There are two primary modes of MAC filtering:

1) **Whitelist (Allow mode):** In this mode, only devices with MAC addresses listed in the whitelist are allowed to connect to the network. All other devices are denied access.
2) **Blacklist (Deny mode):** In this mode, devices with MAC addresses listed in the blacklist are denied access to the network. All other devices are allowed to connect.

5.3 MAC filtering technique

MAC filtering technique typically works:

1) **Configuration:** The network administrator configures the MAC filtering settings on the network device, such as a router or access point. This involves accessing the device's administration interface and navigating to the MAC filtering section.
2) **Whitelist or Blacklist Creation:** The administrator creates a list of MAC addresses that are either allowed (whitelist) or denied (blacklist) access to the network. Each entry in the list corresponds to the MAC address of a specific device.
3) **Enablement:** The MAC filtering feature is enabled on the network device. Depending on the configuration, it may be set to either allow all devices except those on the blacklist or deny all devices except those on the whitelist.
4) **MAC Address Verification:** When a device attempts to connect to the network, the network device examines the MAC address of the incoming traffic. If MAC filtering

is enabled, it compares the MAC address of the incoming device with the entries in the whitelist or blacklist.

5) **Access Decision:** Based on the comparison, the network device either permits or denies access to the network for the connecting device:
    - If the device's MAC address matches an entry in the whitelist, access is granted.
    - If the device's MAC address matches an entry in the blacklist, access is denied.
    - If the device's MAC address does not match any entries and the MAC filtering mode is set to deny (or whitelist mode with no entries), access is denied.
    - If the device's MAC address does not match any entries and the MAC filtering mode is set to allow (or blacklist mode with no entries), access is granted.

6) **Logging and Monitoring:** Some network devices may provide logging and monitoring capabilities for MAC filtering events. This allows administrators to track which devices are attempting to connect to the network and whether their access requests were granted or denied.

5.4 Unauthorize device control procedure

Implementing procedures and security measures to detect, identify, and mitigate unauthorized devices accessing the network is crucial:

1) **Network Inventory and Documentation:** Maintain an updated inventory of all networked devices, including their names, MAC addresses, IP addresses, and assigned users
2) **Network Monitoring:** It is important to use network monitoring tools to continuously monitor network traffic and device connections. These tools can help detect any suspicious activities or unauthorized devices attempting to connect to the network.
3) **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** Implement IDS/IPS solutions to automatically detect and respond to unauthorized devices or suspicious network activities. These systems can analyze network traffic in real-time and trigger alerts or block connections based on predefined rules.
4) **MAC Filtering:** As previously discussed, use MAC filtering to control access to the network based on MAC addresses. Configure the network devices to only allow connections from devices with approved MAC addresses while blocking unauthorized devices.
5) **Network Access Control (NAC):** Implement NAC solutions to enforce security policies and authenticate devices before granting access to the network. NAC solutions can perform posture assessments, verify device compliance with security policies, and quarantine devices that fail to meet requirements.
6) **Security Policies and User Training:** It is important to establish clear security policies regarding device usage and network access. Employees and network users should be educated about the risks associated with connecting unauthorized devices to the network and the importance of adhering to security policies.

7) **Regular Audits and Reviews:** Conduct periodic audits and reviews of network devices, configurations, and access logs to identify any unauthorized devices or security vulnerabilities. Address any issues promptly to maintain the integrity and security of the network.
8) **Continuous Improvement:** Continuously assess and improve the network security posture by incorporating feedback from security incidents, conducting regular security assessments, and staying informed about emerging threats and best practices in network security.

5.5 Default firewall

The term "default firewall" can refer to the firewall software that comes pre-installed and enabled by default on an operating system. Here are a few examples:

1) **Windows Firewall:** This is the default firewall solution included with Microsoft Windows operating systems. It provides basic inbound and outbound traffic filtering capabilities, allowing users to create custom rules and exceptions.
2) **iptables (Linux):** On Linux-based systems, iptables is a widely used firewall management tool. It comes pre-installed on many Linux distributions and provides packet filtering, network address translation (NAT), and other advanced firewall features.

Self-Check Sheet-5: Secure SOHO Network

1. What is Sniffing?

2. What are the primary modes of MAC filtering?

3. What is windows firewall?

4. What does ARP Interception entail?

5. How would you define Network segmentation?

Answer Key-5: Secure SOHO Network

1. **What is Sniffing?**

   Answer: "Sniffing" is a term used to describe the practice of capturing and analyzing network traffic. This is usually done for purposes such as monitoring, troubleshooting or even intercepting sensitive information. Network sniffing tools capture packets of data as they travel across a network and display their contents. While sniffing can be used for legitimate purposes by network administrators and security professionals, it can also be misused by attackers to eavesdrop on sensitive information such as passwords, usernames, and other confidential data.

2. **What are the primary modes of MAC filtering?**

   Answer: There are two primary modes of MAC filtering:

   1) **Whitelist (Allow mode):** In this mode, only devices with MAC addresses listed in the whitelist are allowed to connect to the network. All other devices are denied access.
   2) **Blacklist (Deny mode):** In this mode, devices with MAC addresses listed in the blacklist are denied access to the network. All other devices are allowed to connect.

3. **What is windows firewall?**

   Answer: This is the default firewall solution included with Microsoft Windows operating systems. It provides basic inbound and outbound traffic filtering capabilities, allowing users to create custom rules and exceptions.

4. **What does ARP Interception?**

   Answer: ARP (Address Resolution Protocol) interception is a technique used in network attacks to intercept and manipulate ARP traffic. ARP is responsible for resolving IP addresses to MAC addresses on a local network. In ARP interception attacks, an attacker sends forged ARP messages to associate their MAC address with the IP address of another device on the network.

5. **How would you define Network segmentation?**

   Network segmentation is a technique that involves dividing a larger network into smaller subnetworks or segments. This helps to improve the performance, security, and manageability of the network. By segmenting the network, it is possible to control network traffic, limit the impact of security breaches, and enforce security policies more effectively. There are several methods that can be used to implement network segmentation, including VLANs (Virtual Local Area Networks), subnetting, and physical network segmentation.

Task Sheet-5.1: Control Unauthorize Device In SOHO Network

Performance Objective: At the end of this task, the trainee should be able to Control unauthorize device in SOHO network.

Working steps:

Step 1: Network Inventory

- Conduct an inventory of all authorized devices connected to the network.
- Document MAC addresses, IP addresses, and other identifying information for each authorized device.

Step 2: Network Segmentation:

- Segment the network into separate VLANs or subnets based on device type or security requirements.
- Implement access control policies to restrict communication between network segments.

Step 3: Access Control Lists (ACLs):

- Configure ACLs on routers, switches, and firewalls to control traffic flow.
- Block unauthorized devices by specifying allowed MAC addresses or IP addresses.

Step 4: Network Authentication:

- Implement network authentication mechanisms such as WPA2-Enterprise for Wi-Fi networks.
- Require users and devices to authenticate before gaining access to the network.

Step 5: MAC Address Filtering:

- Enable MAC address filtering on network devices to allow only authorized MAC addresses to connect.
- Maintain a whitelist of approved MAC addresses and deny access to unauthorized devices.

Step 6: Network Monitoring:

- Deploy network monitoring tools to detect unauthorized devices or anomalies in network traffic.
- Set up alerts to notify administrators of unauthorized device connections.

Step 7: Endpoint Security:

- Install antivirus software, firewalls, and intrusion detection/prevention systems on all devices.
- Enable automatic updates and patches to address security vulnerabilities.

Step 8: Regular Audits:

- Conduct regular audits of network devices to identify and remove unauthorized devices.
- Review access logs and security alerts for signs of unauthorized access.

Step 9: Guest Network Isolation:

- Set up a separate guest network for visitors, isolated from the main network.
- Implement access controls and bandwidth limitations to restrict guest network access.

Specification Sheet-5.1: Control Unauthorize Device In SOHO Network

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
5	Hand Gloves	Pair	1
6	Apron	No.	1
7	Googles	No.	1
8	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Unit	Quantity
1	Network monitoring software	No.	1
2	Access control software	No.	10
3	Security policy management tools	Set	1
4	Network inventory management tools	No.	1

Necessary Equipment

Sl. No	Name of Equipment	Unit	Quantity
1	Routers	No.	1
2	Switches	No.	1
3	Firewalls	No.	1
4	Access points	No.	1
5	Network monitoring devices	No.	1

Necessary Materials

Sl. No.	Name of materials	Unit	Quantity
1	Network access control policies	No.	10
2	Documentation templates for network inventory	No.	10
3	Security guidelines and best practices documentation	No.	1
4	Training materials for employee education on network security	No.	10

Task Sheet-5.2: Enable Default Firewall In Windows

Performance Objective: At the end of this task, the trainee should be able to Enable default firewall in windows.

Working steps:

Step 1: Open Windows Security Settings

- Press the Windows key, type "Windows Security," and select the matching result.
- Alternatively, you can access Windows Security from the Control Panel or Settings app.

Step 2: Navigate to Firewall & Network Protection

- In the Windows Security app, click on "Firewall & network protection" from the left sidebar.

Step 3: Enable Windows Defender Firewall

- Under the Firewall & network protection section, locate the Windows Defender Firewall option.
- Click on the toggle switch to turn on the firewall. You may need to confirm the action with administrative privileges.

Router/Firewall Appliance:

Step 1: Access Device Configuration:

- Open a web browser and enter the IP address of your router or firewall appliance in the address bar.
- Log in to the device's administrative interface using the username and password.

Step 2: Navigate to Firewall Settings:

- Locate the firewall settings or configuration section within the device's interface.

Step 3: Enable Firewall:

- Depending on the device, there may be an option to enable the firewall with a single click or by configuring specific rules and policies.

Step 4: Save Changes

- After enabling the firewall and configuring any necessary rules, save your changes and reboot the device if required for the settings to take effect.

Specification Sheet-5.2: Enable Default Firewall In Windows

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Hand Gloves	Pair	1
2	Apron	No.	1
3	Googles	No.	1
4	Safety Show	Pair	1

Necessary Tools

Sl. No	Name of Tools	Unit	Quantity
1	Operating system configuration tools (e.g., Windows Security settings)	No.	1
2	Router/firewall appliance	No.	1
3	Security policy management tools	Set	1
4	Network inventory management tools	No.	1

Necessary Equipment

Sl. No	Name of Equipment	Unit	Quantity
1	Documentation and manuals provided by the operating system or device manufacturer	No.	1
2	Network access control policies	No.	1
3	Administrative credentials (username and password)	No.	1
4	Internet connection	No.	1
5	Computer or device used for configuration	No.	1

Necessary Materials

Sl. No.	Name of materials	Unit	Quantity
1	Network access control policies	No.	10
2	Documentation templates for network inventory	No.	10
3	Security guidelines and best practices documentation	No.	1
4	Training materials for employee education on network security	No.	10

Reference of resources used for informations and job procedure (if any)

NB: After completion of all LO, then complete the following review of competency

Review of Competency

Below is yourself assessment rating for module "Performing SOHO Networking"

Assessment of performance Criteria	Yes	No
SOHO Network is defined		
Types of SOHO Network is identified		
Functions of SOHO network is interpreted		
Naming convention is interpreted		
Network model is defined		
SOHO Network equipment is identified		
Basic purpose of LAN is identified and defined		
Basic functions of LAN are identified and defined.		
Small Office Home Office (SOHO) networking is designed.		
Required tools and equipment's are identified and listed		
Materials and consumables are identified and listed		
Budget is prepared and documented for Network as per Requirements		
Budget is sent to appropriate person for approval as per workplace practice		
Configuration requirements are identified		
Tools and equipment are selected and collected from vendor		
Materials and consumables are collected		
SOHO Networks is installed and configured.		
Necessary settings for LAN are configured		
IP assign type is selected		
IP address is assigned		
Computer name is ensured and workgroup name are documented and confirmed		
Documents and file sharing setting are confirmed		
Add Printer and enable sharing are confirmed		
Access requirements are determined and sharing is confirmed		
Wireless Configuration requirements are identified		
Tools and equipment for wireless configuration are selected and collected		
Materials and consumables are collected		
Wireless SOHO Networks is installed and configured.		

Necessary settings for WLAN are configured		
IP address is Assigned as required		
Computer name is ensured and workgroup name are documented and confirmed		
Documents and file sharing setting are confirmed		
Printer is added and enable sharing are confirmed		
Access requirements are determined and sharing is confirmed.		
Security problems for SOHO networking is interpreted		
MAC filtering is interpreted		
Unauthorize device is controlled		
Default firewall is enabled		

I now feel ready to undertake my formal competency assessment.

Signed:

Date:

Development of CBLM

The Competency based Learning Material (CBLM) of **'Perform SOHO Networking' (Occupation: IT Support Service, Level-4)** for National Skills Certificate is developed by NSDA with the assistance of SIMEC System Ltd., ECF Consultancy & SIMEC Institute of Technology JV (Joint Venture Firm) in the month of July, 2024 under the contract number of package SD-9B dated 15th January 2024.

SL No.	Name & Address	Designation	Contact Number
1	Anisuzzaman Tuheen	Writer	01714-422225
2	Engr. Md. Zuwel Parves	Editor	01737-278906
3	Engr. Md. Zuwel Parves	Co-Ordinator	01737-278906
4	Md. Saif Uddin	Reviewer	01723-004419