Competency Based Learning Materials

(CBLM)

IT Support Service

Level-3

Module: Performing Basic Networking

Code: CBLM-OU-ICT-ITSS-04-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

This Competency Based Learning Materials (CBLM) on "Performing Basic Networking" under the IT Support Service, Level-3 qualification is developed based on the national competency standard approved by National Skills Development Authority (NSDA)

This document is to be used as a key reference point by the competency-based learning materials developers, teachers/trainers/assessors as a base on which to build instructional activities.

This Competency Based Learning Materials is a document for the development of curricula, teaching and learning materials, and assessment tools. It also serves as the document for providing training consistent with the requirements of industry in order to meet the qualification of individuals who graduated through the established standard via competency-based assessment for a relevant job.

This document has been developed by NSDA in association with industry representatives, academia, related specialist, trainer and related employee.

Public and private institutions may use the information contained in this CBLM for activities benefitting Bangladesh.

List of Abbreviations

CS	-	Competency Standard
ISC	-	Industry Skills Council
NSDA	-	National Skills Development Authority
NSQF	-	National Skills Qualifications Framework
BNQF	-	Bangladesh National Qualifications Framework
OSH	-	Occupational Safety and Health
PPE	-	Personal Protective Equipment
SCVC	-	Standards and Curriculum Validation Committee
STP	-	Skills Training Provider
SOP	-	Standard Operating Procedure
UoC	-	Unit of Competency
EC	-	Executive Committee
CBT&A	-	Competency based Training & Assessment
CBC	-	Competency based Curriculum
CAD	-	Course Accreditation Document
CBLM	-	Competency Based Learning Materials

How to use this Competency Based Learning Materials (CBLMs)

The module, Performing Basic 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

Approved by __ th Authority Meeting of NSDA Held on ----------

Table of Content

MODULE CONTENT

Unit of Competency: Perform Basic Networking

Module Title: Performing Basic Networking

Module Description: This module discusses the aspects that must be given attention when Perform Basic Networking. It shows the knowledge and skills requirements for includes interpreting the concept of networking, interpreting the network layout, connecting devices to the existing network, troubleshooting in existing network, creating documentation for maintenance.

Nominal Duration: 50 **Hours**

Learning Outcomes:

Upon completion of this module the trainees must be able to:

1. Interpret the concept of networking
2. Interpret the network layout
3. Connect devices to the existing network
4. Troubleshoot in existing network
5. Create documentation for maintenance

Assessment Criteria:

1.1 Network is defined
1.2 Types of networks is interpreted
1.3 IP properties is interpreted
1.4 Network connectivity tools identified
1.5 Transmission media determined.

2.1 Organizational requirements are collected and documented to setup an existing network.
2.2 Network layout is collected
2.3 Existing network topology and network protocol is identified and documented
2.4 Network design plan is interpreted.
2.5 IP Addressing scheme is interpreted

3.1. Required transmission media, tools and equipment are selected and collected.
3.2. Cabling is performed as per layout
3.3. Connections is established as per layout design.
3.4. Device is connected with the existing network with appropriate transmission media infrastructure
3.5. IP properties is assigned and connectivity is tested as per work plan.

4.1 Network design, support and maintenance documents are reviewed.
4.2 Appropriate person is consulted for identifying problems if required.
4.3 Faulty hardware or software component are detected.
4.4 Solution of Problem is performed.
4.5 Network functionality is tested.
4.6 Maintenance and troubleshooting documents are updated.
4.7 Tools and equipment are stored as per workplace procedures.

5.1 All the settings are documented
5.2 Configuration and PC network IP address are documented for future maintenance purpose.

Learning Outcome 1: Interpret the concept of networking

Assessment Criteria:

1. Network is defined
2. Types of networks is interpreted
3. IP properties is interpreted
4. Network connectivity tools identified
5. Transmission media determined.

Content:

1. Network
2. Types of networks
3. IP properties
4. Network connectivity tools
5. Transmission media.

Resources Required/ Conditions:

The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application
- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 1: Interpret the concept of networking

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 Steps	Resources specific instructions
1. Trainee will ask the instructor about Interpret the concept of networking	1. Instructor will provide the learning materials "Performing Basic Networking"
2. Read the Information sheet/s	2. Information Sheet No: 1 Interpret the concept of networking
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 1 Interpret the concept of networking Answer key No. 1 Interpret the concept of networking
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No: 1- Interpret the concept of networking Specification Sheet 1 – Interpret the concept of networking

Information Sheet 1: Interpret the concept of networking

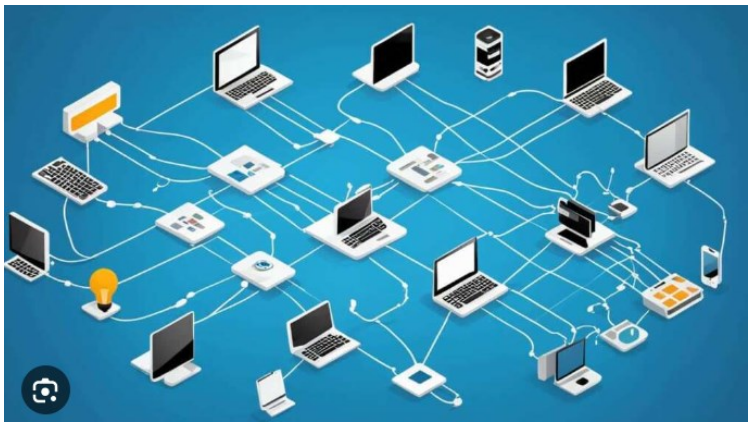
Learning Objectives:

After completion of this information sheet, the learners will be able to:

1.1 Define Network
1.2 Interpret Types of networks
1.3 Interpret IP properties
1.4 Identify Network connectivity tools
1.5 Determine Transmission media.

1.1 Network

A network is a collection of interconnected nodes or devices that can communicate and share resources with each other. These nodes can be computers, servers, routers, switches, printers, or any other device capable of sending or receiving data. The purpose of a network is to facilitate communication and resource sharing among these devices.



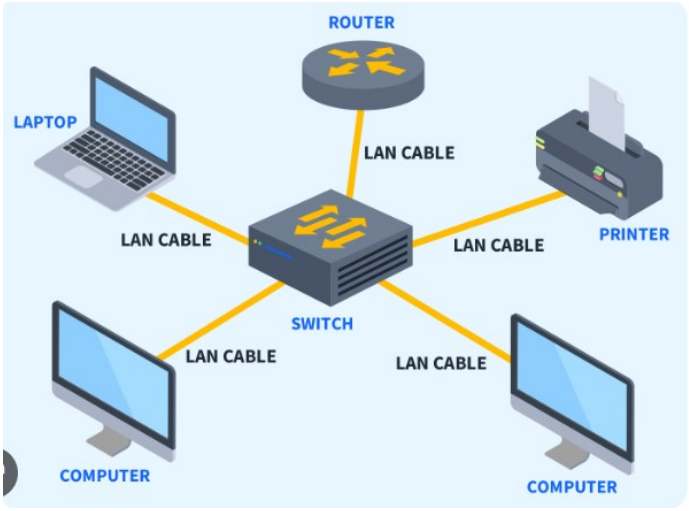
1.2 Types of networks

Networks can be classified into several types based on their geographical scope, architecture, and purpose.

Local Area Network (LAN):

A LAN is a network that typically spans a small geographical area, such as a single building, office, or campus.

Devices in a LAN are connected using wired or wireless technologies like Ethernet or Wi-Fi.



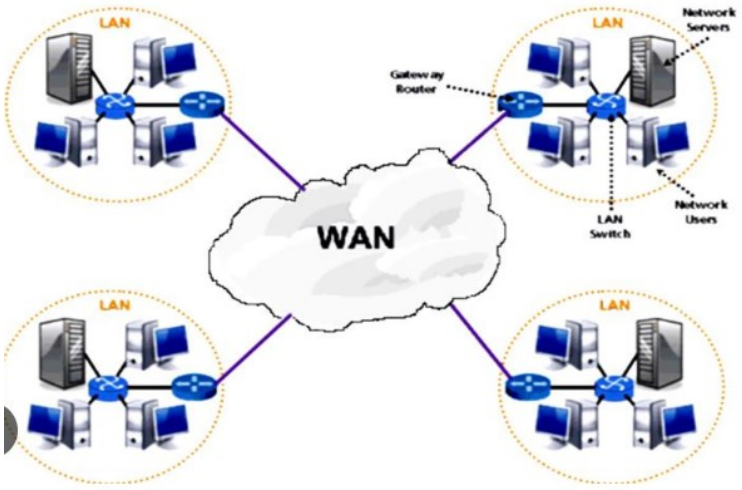
LANs are commonly used in homes, schools, and businesses for local communication and resource sharing.

Wide Area Network (WAN):

A WAN covers a large geographical area, such as a city, country, or even multiple countries.

WANs connect LANs and other networks over long distances using various communication technologies like leased lines, satellite links, or fiber-optic cables.

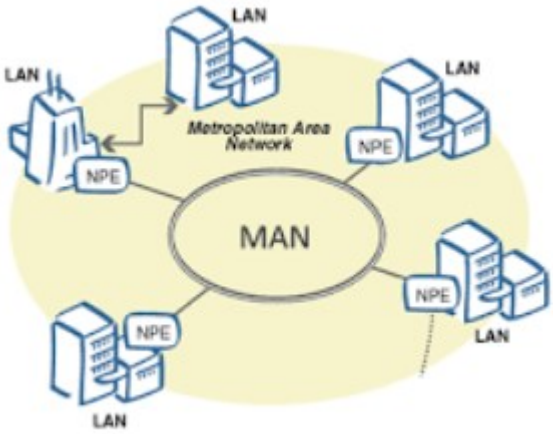
The Internet is the largest WAN, connecting millions of devices and networks worldwide.



Metropolitan Area Network (MAN):

A MAN is a network that spans a metropolitan area, such as a city or a large campus.

MANs provide high-speed connections between LANs and other networks within the same geographical area.



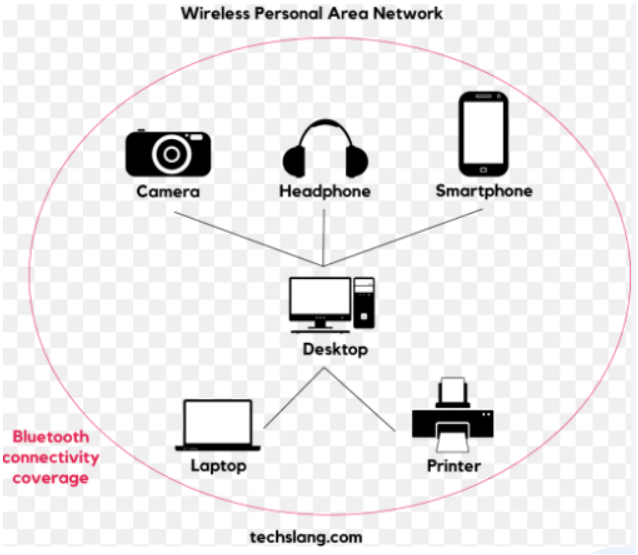
They are often used by businesses and government agencies for interconnecting their offices and facilities.

Personal Area Network (PAN):

A PAN is a network used for communication among devices in close proximity to an individual, typically within a range of a few meters.

Examples of PAN technologies include Bluetooth and infrared (IR).

PANs are commonly used for connecting personal devices like smartphones, tablets, and wearable devices.



Wireless LAN (WLAN):

A WLAN is a type of LAN that uses wireless communication technologies like Wi-Fi to connect devices within a local area.

WLANs provide flexibility and mobility, allowing devices to connect to the network without the need for physical cables.

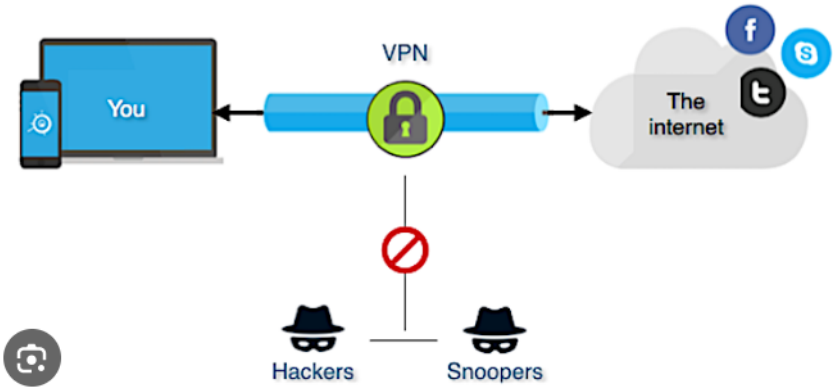
They are widely used in homes, offices, and public spaces for wireless internet access.

Virtual Private Network (VPN):

A VPN is a network that provides secure communication over a public network, such as the Internet.

VPNs use encryption and tunneling protocols to create a private and secure connection between remote users and a private network.

They are commonly used by businesses to enable remote access to their internal networks and to secure data transmission over untrusted networks.

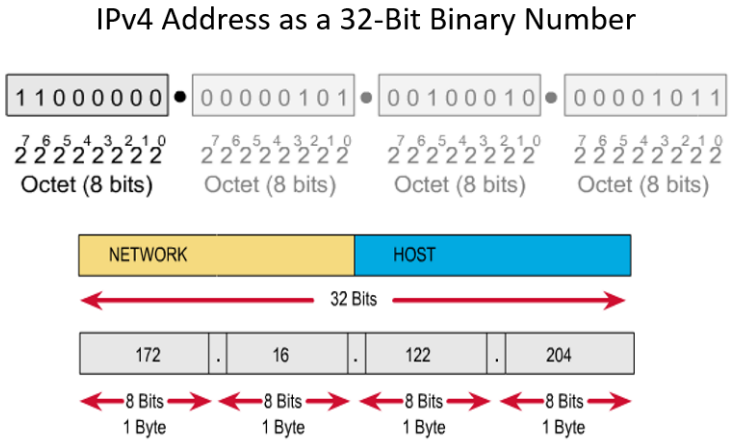


1.3 IP properties

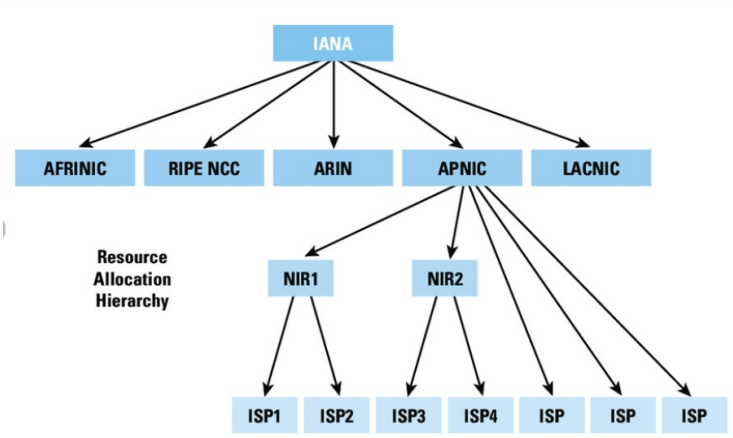
IP properties refer to various characteristics and attributes associated with IP (Internet Protocol) addresses, which are numerical identifiers assigned to devices participating in a network. Here are some important IP properties:

Uniqueness: Each device on a network must have a unique IP address to ensure proper communication. No two devices within the same network can have the same IP address simultaneously.

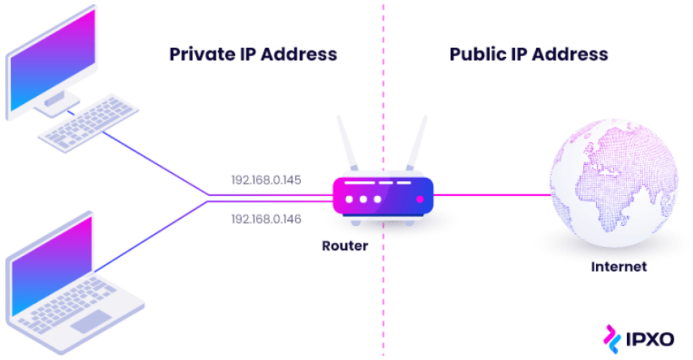
Addressing: IP addresses are typically represented in either IPv4 (32-bit) or IPv6 (128-bit) format. IPv4 addresses are written in decimal format separated by periods (e.g., 192.168.1.1), while IPv6 addresses are represented as hexadecimal strings separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).



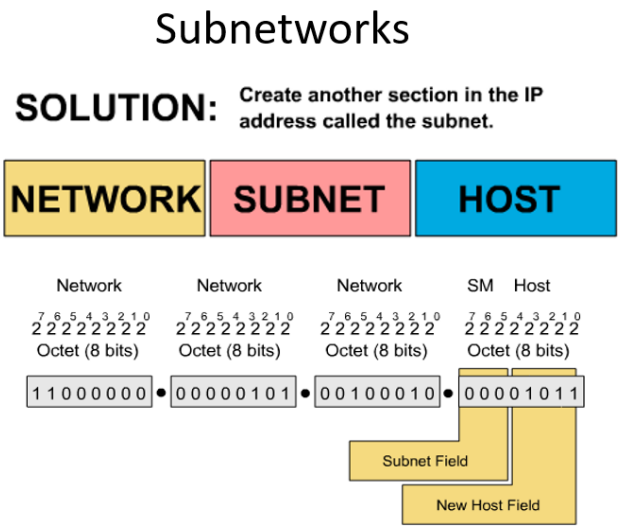
Hierarchical Structure: IP addresses are structured hierarchically, allowing for efficient routing and addressing. In IPv4, addresses are divided into network and host portions, with each portion serving a specific purpose in routing data across networks. IPv6 further enhances this hierarchical structure to accommodate the larger address space.

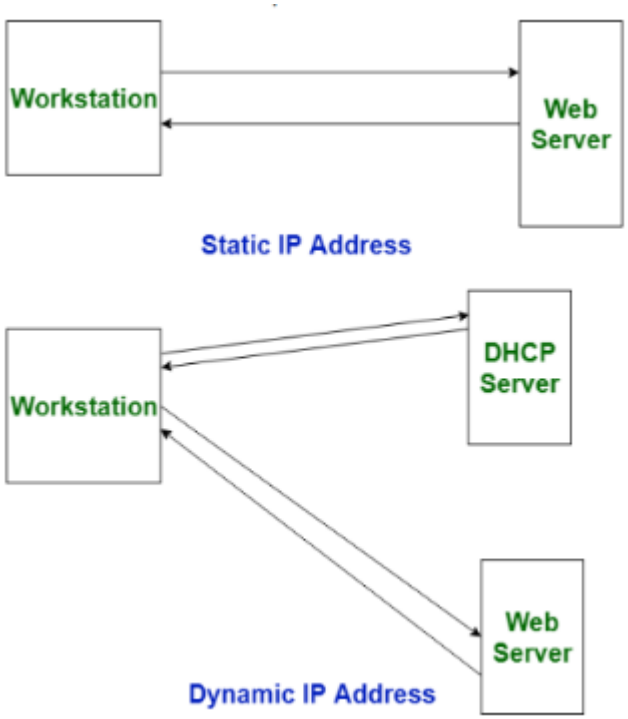


Public vs. Private: IP addresses can be categorized as either public or private. Public IP addresses are globally routable and are used to identify devices on the Internet. Private IP addresses, on the other hand, are reserved for use within private networks and are not directly accessible from the Internet.



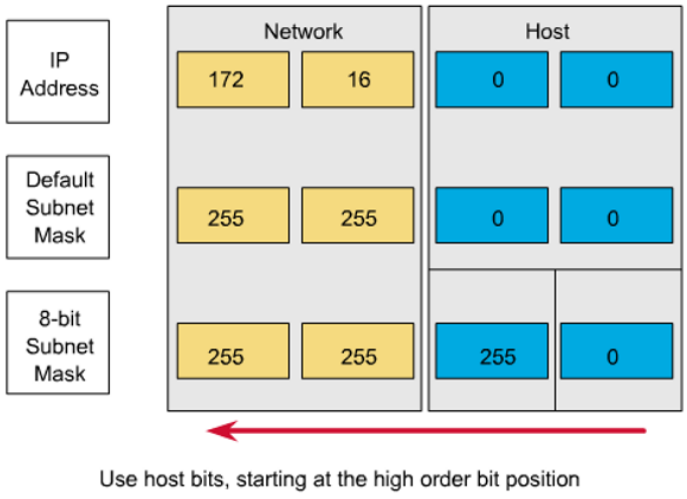
Dynamic vs. Static: IP addresses can be assigned dynamically or statically. With dynamic addressing, IP addresses are assigned dynamically by a DHCP (Dynamic Host Configuration





Protocol) server when a device connects to a network. Static addressing involves manually assigning IP addresses to devices, ensuring consistency but requiring administrative overhead.

Subnetting: Subnetting is the process of dividing a network into smaller subnetworks (subnets) to improve network performance, security, and management. Subnetting allows for more efficient use of IP address space and enables better organization of network resources.



Address Resolution: Address resolution mechanisms, such as ARP (Address Resolution Protocol) for IPv4 and NDP (Neighbor Discovery Protocol) for IPv6, are used to map IP addresses to physical MAC (Media Access Control) addresses on local networks. These protocols facilitate communication between devices within the same subnet.

Creating a Subnet

Class C address 197.15.22.131 with a subnet mask of 255.255.255.224 (3 bits borrowed)

11000101	00001111	00010110	100	00011
Network Field			SN	Host Field

The address 197.15.22.131 would be on the subnet 197.15.22.128.

Determining Subnet Mask Size

CIDR Notation:

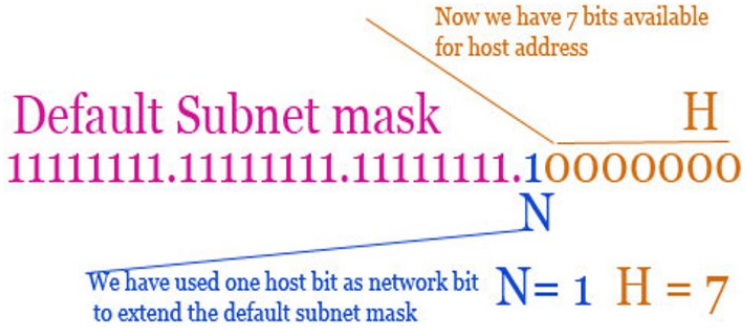
CIDR notation is a compact way of representing IP address ranges and subnet masks. It consists of an IP address followed by a slash ("/") and a number indicating the number of bits used for the network portion of the address.

For example, "192.168.1.0/24" represents the IP address range from 192.168.1.0 to 192.168.1.255, with a subnet mask of 255.255.255.0.

Private and Public IP Addresses:

Class C Sub netting

192.168.10.0/25



N = 1 [Number of host bit used in network]
H = 7 [Remaining host bits]
Total subnets (2^N) :- $2^1 = 2$
Block size (256 - subnet mask) :- 256 - 128 = 128
Valid subnets (Count blocks from 0) :- 0,128
Total hosts (2^H) :- $2^7 = 128$
Valid hosts per subnet (Total host - 2) :- 128 - 2 = 126

Subnets	Subnet 1	Subnet 2
Network ID	0	128
First host	1	129
Last host	126	254
Broadcast ID	127	255

Class B Sub netting

172.16.0.0/17

N = 1 [Number of host bit used in network]
H = 7 [Remaining host bits]
Total subnets (2^N) :- $2^1 = 2$
Block size (256 - subnet mask) :- 256 - 128 = 128
Valid subnets (Count blocks from 0) :- 0,128
Total hosts (2^H) :- $2^{15} = 32768$
Valid hosts per subnet (Total host - 2) :- 32768 - 2 = 32766

Subnets	Subnet 1	Subnet 2
Network ID	172.16.0.0	172.16.128.0
First host	172.16.0.1	172.16.128.1
Last host	172.16.127.254	172.16.255.254
Broadcast ID	172.16.127.255	172.16.255.255

172.16.0.0/17
N = 2
H = 6
Total subnets (2^N) :- $2^2 = 4$
Block size (256 - subnet mask) :- 256 - 192 = 64
Valid subnets (Count blocks from 0) :- 0,64,128,192
Total hosts (2^H) :- $2^{14} = 16384$
Valid hosts per subnet (Total host - 2) :- 16384 - 2 = 16382

Subnets	Subnet 1	Subnet 2	Subnet 3	Subnet 4
Network ID	172.16.00	172.16.64.0	172.16.128.0	172.16.192.0
First host	172.16.0.1	172.16.64.1	172.16.128.1	172.16.192.1
Last host	172.16.62.254	172.16.127.254	172.16.190.254	172.16.255.254
Broadcast ID	172.16.63.255	172.16.127.255	172.16.191.255	172.16.255.255

Network connectivity tools

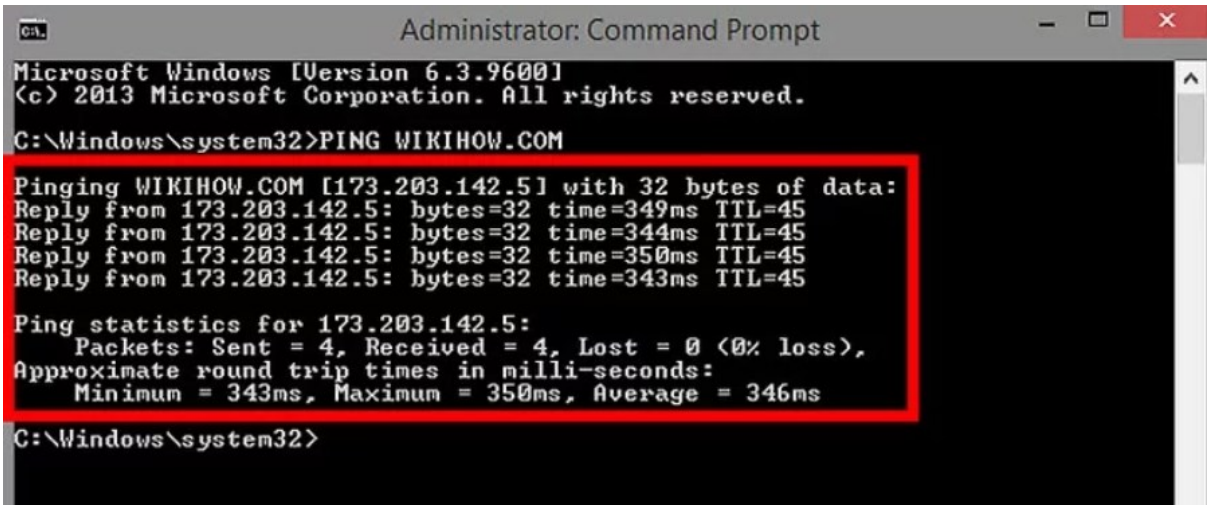
Network connectivity tools are essential for diagnosing, monitoring, and troubleshooting issues related to network connectivity. These tools help network administrators and engineers identify problems, analyze network performance, and ensure that devices within the network can communicate effectively. Here are some common network connectivity tools:

Ping:

Ping is a basic network utility used to test the reachability of a host on an IP network.

It sends ICMP (Internet Control Message Protocol) echo request packets to the target host and waits for ICMP echo reply packets.

Ping is useful for verifying network connectivity and measuring round-trip times between devices.

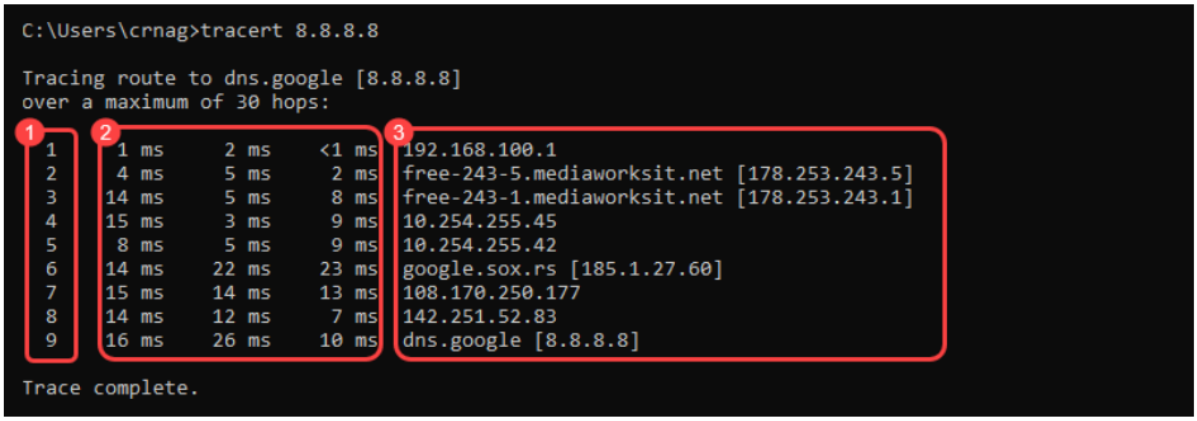


Traceroute/Tracert:

Traceroute (on Unix/Linux) or Tracert (on Windows) is a tool used to trace the path that packets take from a source to a destination.

It sends ICMP or UDP packets with increasing TTL (Time to Live) values and listens for ICMP Time Exceeded messages from routers along the path.

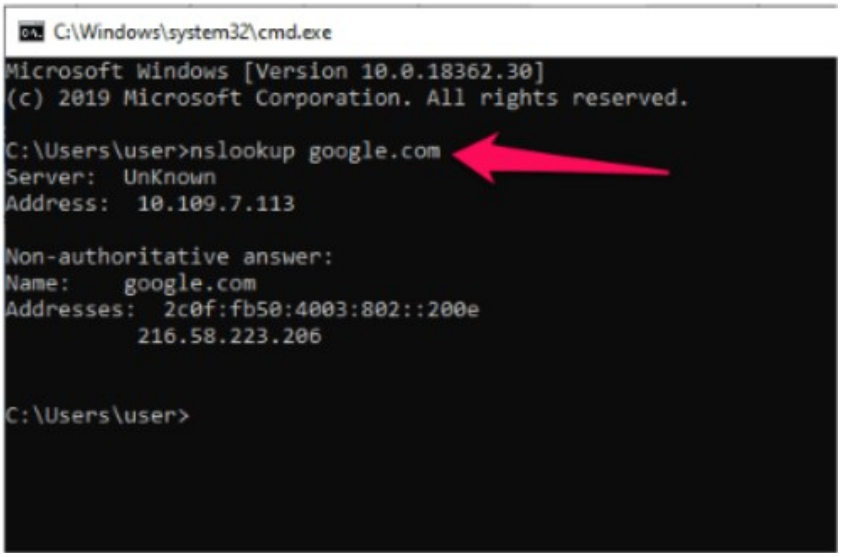
Traceroute helps identify network hops and latency issues between the source and destination.



Nslookup/Dig:

Nslookup (Windows) and Dig (Unix/Linux) are DNS (Domain Name System) lookup tools used to query DNS servers for information about domain names and IP addresses.

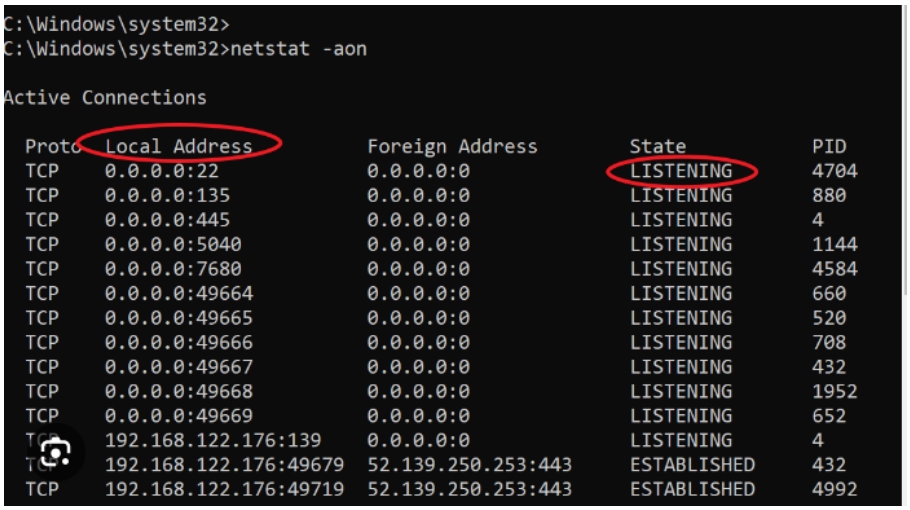
They can be used to resolve domain names to IP addresses, perform reverse DNS lookups, and query DNS records such as MX (Mail Exchange) and TXT (Text) records.



Netstat:

Netstat (Network Statistics) is a command-line tool used to display network connections, routing tables, and network interface statistics.

It provides information about active TCP/IP connections, listening ports, routing information, and network interface utilization.

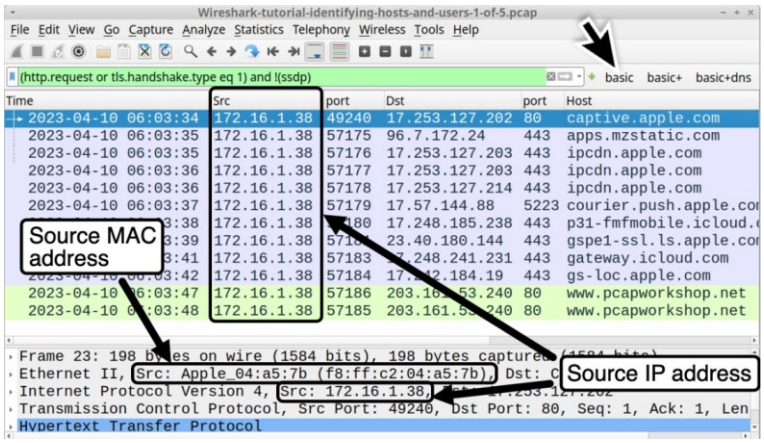


Wireshark:

Wireshark is a powerful network protocol analyzer that captures and displays packets flowing through a network interface.

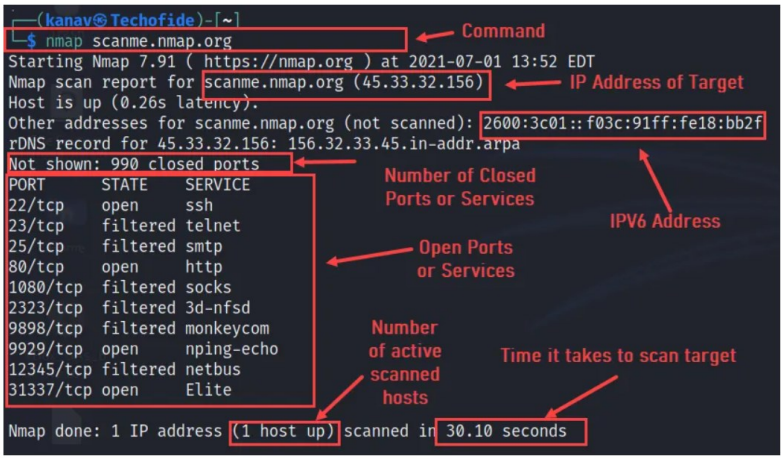
It allows users to inspect packet headers, analyze network traffic, and troubleshoot network issues at the packet level.

Wireshark supports various protocols and provides detailed information about packet captures.



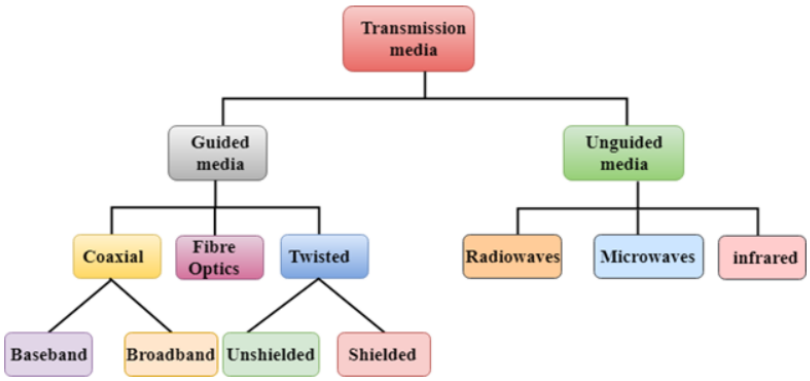
Nmap:

Nmap (Network Mapper) is a network scanning tool used for network discovery and security auditing.
It scans networks to identify open ports, detect hosts, and determine services running on remote systems.
Nmap can be used to assess network security and identify potential vulnerabilities.



Transmission media

Transmission media, also known as communication channels or simply "media," are the physical pathways through which data is transmitted from one device to another in a data communication network. Different types of transmission media have distinct characteristics, including bandwidth, transmission speed, distance limitations, susceptibility to interference, and cost.

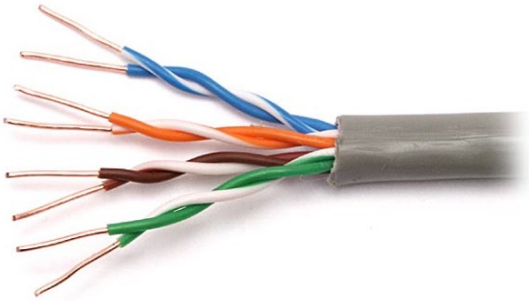


Some common types of transmission media:

Twisted Pair Cable:

Twisted pair cables consist of pairs of insulated copper wires twisted together.

They are commonly used in Ethernet networks for connecting computers, switches, and routers.



Twisted pair cables are relatively inexpensive, easy to install, and suitable for short to medium distances.

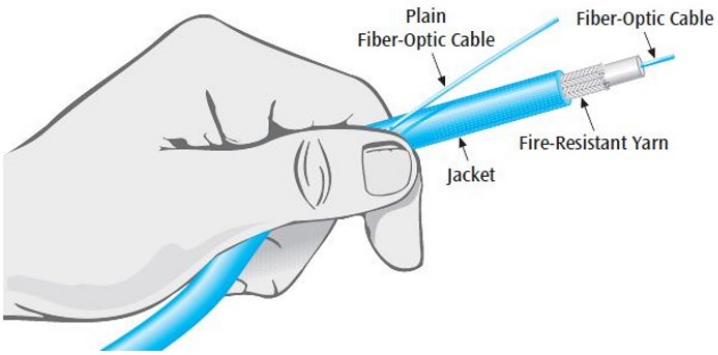
Coaxial Cable:

Coaxial cables consist of a central conductor surrounded by an insulating layer, a metallic shield, and an outer insulating layer.

They are often used in cable television (CATV) networks and broadband Internet connections.

Coaxial cables provide higher bandwidth than twisted pair cables and can support longer distances.

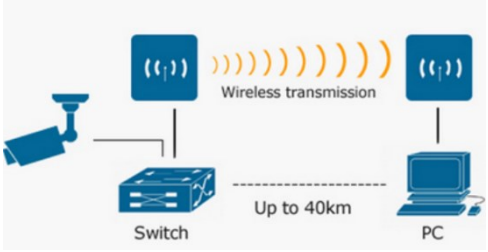
Fiber Optic Cable: Fiber optic cables use optical fibers made of glass or plastic to transmit data using light signals.



They offer high bandwidth, low attenuation, and immunity to electromagnetic interference.
Fiber optic cables are widely used in long-distance telecommunications networks, backbone infrastructure, and high-speed Internet connections.

Wireless Transmission:

Wireless transmission uses electromagnetic waves to transmit data without the need for physical



cables.

Common wireless technologies include Wi-Fi (IEEE 802.11), Bluetooth, cellular networks (e.g., 4G LTE), and satellite communication.
Wireless transmission provides mobility and flexibility but may suffer from limited range, interference, and security concerns.

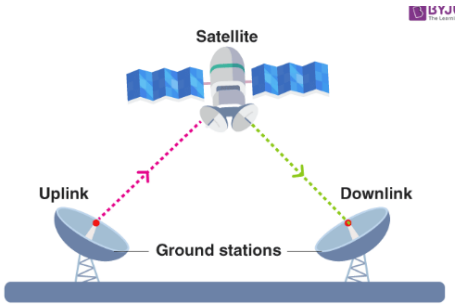
Microwave Transmission:

Microwave transmission uses high-frequency radio waves to transmit data between two fixed points.

It is often used for point-to-point communication links over long distances, such as in microwave relay systems and satellite communication.

Satellite Communication:

Satellite communication involves transmitting data between Earth-based stations and satellites in orbit around the Earth.
It is used for long-distance communication links, including satellite TV, GPS navigation, and satellite Internet.



Self-Check Sheet 1: Interpret the concept of networking

1. What is a network?

2. What are the types of networks?

3. What are some properties of IP addresses?

4. Name some network connectivity tools.

5. What are examples of transmission media?

6. What is the purpose of a network?

7. What is a LAN?

8. Why is uniqueness important for IP addresses?

9. What is the purpose of Traceroute/Tracert?

10. What are the advantages of fiber optic cable?

Answer Key 1: Interpret the concept of networking

1. What is a network?
   Answer: A network is a collection of interconnected devices or nodes that can communicate and share resources with each other.
2. What are the types of networks?
   Answer: Types of networks include LAN (Local Area Network), WAN (Wide Area Network), MAN (Metropolitan Area Network), PAN (Personal Area Network), WLAN (Wireless LAN), VPN (Virtual Private Network), and more.
3. What are some properties of IP addresses?
   Answer: IP properties include uniqueness, addressing, hierarchical structure, public vs. private designation, dynamic vs. static assignment, subnetting, and address resolution.
4. Name some network connectivity tools.
   Answer: Network connectivity tools include Ping, Traceroute/Tracert, Nslookup/Dig, Netstat, Wireshark, Nmap, Netcat (nc), and more.
5. What are examples of transmission media?
   Answer: Transmission media include twisted pair cable, coaxial cable, fiber optic cable, wireless transmission, microwave transmission, satellite communication, and power line communication (PLC).
6. What is the purpose of a network?
   Answer: The purpose of a network is to facilitate communication and resource sharing among interconnected devices or nodes.
7. What is a LAN?
   Answer: A LAN (Local Area Network) is a network that typically spans a small geographical area, such as a single building or office.
8. Why is uniqueness important for IP addresses?
   Answer: Uniqueness ensures that each device on a network has a distinct identifier, preventing address conflicts and enabling proper communication.
9. What is the purpose of Traceroute/Tracert?
   Answer: Traceroute is used to trace the path that packets take from a source to a destination, helping identify network hops and latency issues.
10. What are the advantages of fiber optic cable?
    Answer: Fiber optic cable offers high bandwidth, low attenuation, immunity to electromagnetic interference, and is suitable for long-distance communication.

Learning Outcome 2: Interpret the network layout

Assessment Criteria:

2.1 Organizational requirements are collected and documented to setup an existing network.
2.2 Network layout is collected
2.3 Existing network topology and network protocol is identified and documented
2.4 Network design plan is interpreted.
2.5 IP Addressing scheme is interpreted

Content:

1. Organizational requirements.
2. Network layout
3. Network topology and network protocol
4. Network design plan.
5. IP Addressing scheme

Resources Required/ Conditions:

The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application
- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 2: Interpret The network layout

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 Steps	Resources specific instructions
1. Student will ask the instructor about the network layout	1. Instructor will provide the learning materials "Performing Basic Networking"
2. Read the Information sheet/s	2. Information Sheet No: 2 Interpret The network layout
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 2 - Interpret The network layout Answer key No. 2 - Interpret The network layout
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No: 2 - The network layout Specification Sheet: 2- The network layout

Information Sheet 2: Interpret the network layout

Learning Objectives:

After completion of this information sheet, the learners will be able to:

1. Collect and document Organizational requirements to setup an existing network.
2. Collect Network layout
3. Identify and document Existing network topology and network protocol
4. Interpret Network design plan
5. Interpret IP Addressing scheme

Organizational requirements

To effectively collect and document information for setting up an existing network, you'll need to consider several organizational requirements. Here's a breakdown of what's typically involved:

Understand Organizational Goals:

Before collecting any information, it's crucial to understand the organization's goals and objectives related to the network. This could include improving performance, enhancing security, reducing costs, or supporting new business initiatives.

Identify Stakeholders:

Determine who the key stakeholders are within the organization who will be affected by the network setup or who will provide valuable input. This may include IT managers, network administrators, department heads, and end-users.

Gather Existing Documentation:

Collect any existing documentation related to the network, such as network diagrams, configuration files, inventory lists, and security policies. This information will serve as a foundation for understanding the current state of the network.

Conduct Site Surveys:

Perform site surveys to gather information about the physical infrastructure, including the layout of the building(s), location of networking equipment, cable runs, and power sources. This helps in planning for equipment placement and cable management.

Inventory Network Devices:

Create an inventory of all network devices, including routers, switches, firewalls, servers, access points, and endpoints. Record details such as make, model, serial numbers, firmware versions, and configurations.

Document Network Topology:

Map out the network topology to understand how devices are interconnected and how data flows within the network. This may involve creating diagrams using tools like Microsoft Visio or Lucidchart.

Assess Network Performance:

Evaluate the performance of the existing network, including bandwidth utilization, latency, packet loss, and error rates. Use network monitoring tools to gather data and identify any areas for improvement.

Review Security Policies and Compliance Requirements:

Ensure that the network setup complies with the organization's security policies and any regulatory requirements applicable to the industry. Document security measures such as access controls, encryption protocols, and security audits.

Document User Requirements:

Gather requirements from end-users regarding network performance, reliability, and accessibility. This may involve conducting interviews or surveys to understand their needs and expectations.

Create Documentation Templates:

Develop standardized templates for documenting network configurations, policies, procedures, and troubleshooting guides. This ensures consistency and facilitates future updates and maintenance.

Establish Change Management Procedures:

Define procedures for making changes to the network configuration, including approvals, testing, and rollback plans. Documenting change management processes helps minimize disruptions and ensure accountability.

Plan for Future Growth:

Anticipate future growth and scalability requirements of the network. Document plans for expanding capacity, adding new services or technologies, and accommodating changes in organizational needs.

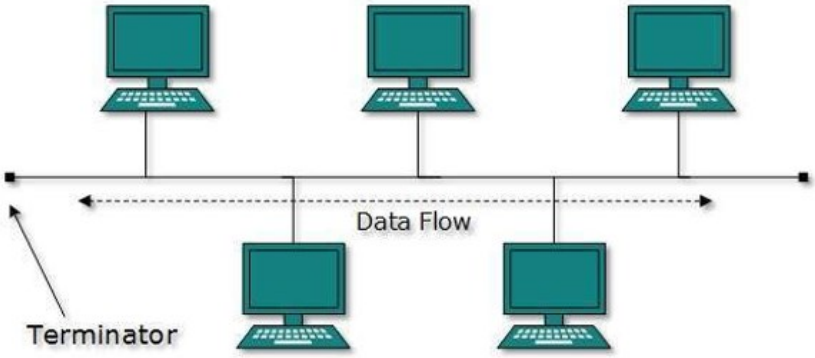
The network layout

The network layout, also known as the network topology, refers to the physical and logical arrangement of devices and connections within a network. It defines how devices are interconnected and how data flows between them. Network layout plays a crucial role in determining the performance, scalability, reliability, and security of a network. Here are some common network layouts:

Bus Topology:

In a bus topology, all devices are connected to a single cable (the bus), forming a linear arrangement.

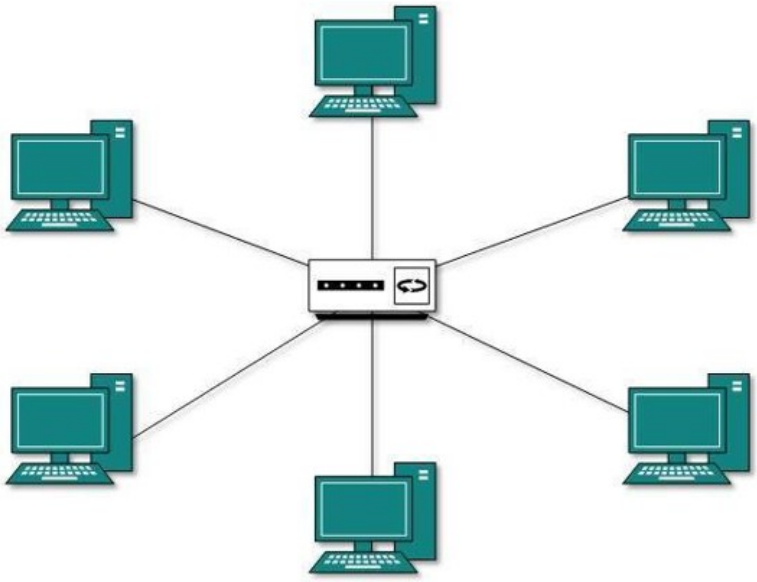
Data is transmitted along the bus, and each device receives the data but only processes information intended for it.



Bus topologies are simple and inexpensive but can suffer from signal degradation and limited scalability.

Star Topology:

In a star topology, each device is connected to a central hub or switch, creating a central point of connection.



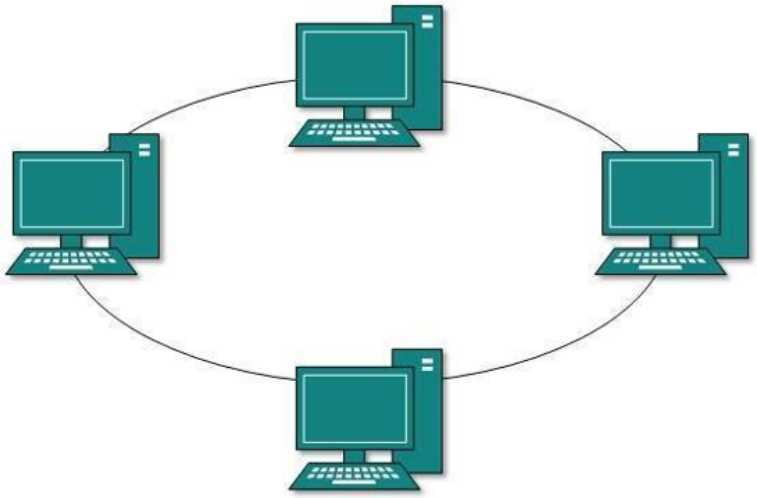
Data travels through the hub or switch, which manages communication between devices.

Star topologies offer high reliability, easy scalability, and efficient troubleshooting but require more cabling than other topologies.

Ring Topology:

In a ring topology, each device is connected to two neighboring devices, forming a closed loop or ring.

Data travels around the ring in one direction, passing through each device until it reaches its destination.

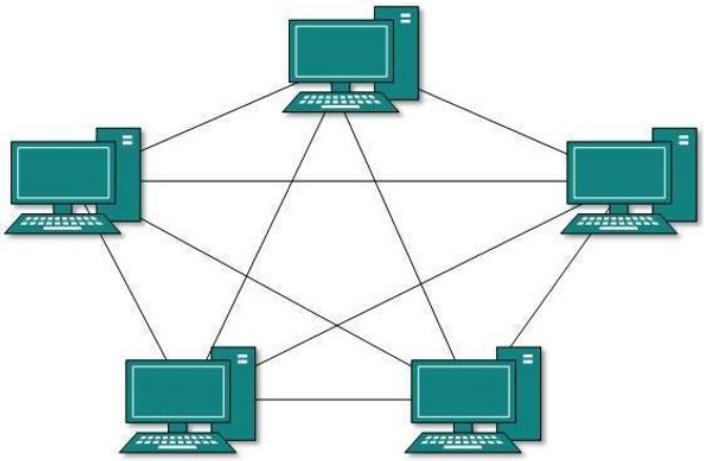


Ring topologies are resilient to cable failures but can suffer from performance degradation if a device fails or if the ring is interrupted.

Mesh Topology:

In a mesh topology, every device is connected to every other device, creating multiple paths for data transmission.

Mesh topologies provide redundancy and fault tolerance, as data can be rerouted through alternate paths if one link fails.

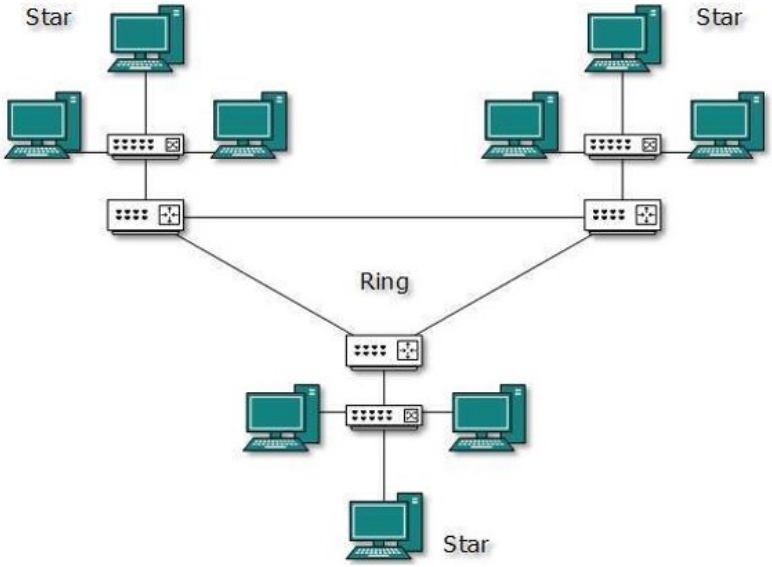


Mesh topologies are complex and expensive to implement but offer high reliability and scalability.

Hybrid Topology:

A hybrid topology combines two or more basic topologies to form a more complex network layout.

For example, a hybrid topology may include a combination of star and bus topologies, or a combination of ring and mesh topologies.

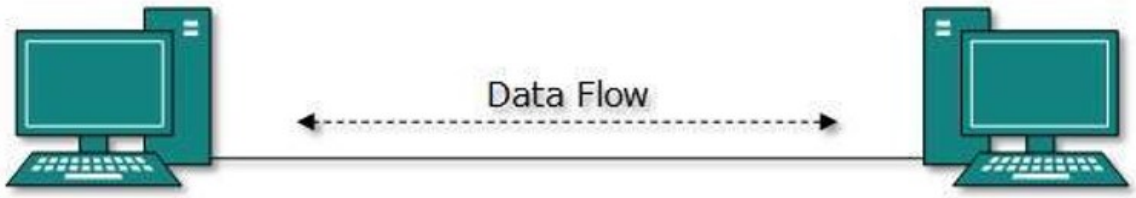


Hybrid topologies allow organizations to tailor their network layouts to specific requirements, balancing cost, performance, and scalability.

Point-to-Point Topology:

In a point-to-point topology, two devices are directly connected without any intermediary devices.

Point-to-point connections are commonly used for establishing dedicated links between locations, such as leased lines or point-to-point wireless links.



Network Protocol

A network protocol is a set of rules and conventions that governs communication between devices in a network. These protocols define how data is formatted, transmitted, received, and interpreted by devices, ensuring that data can be exchanged reliably and efficiently across the network. Network protocols enable devices from different manufacturers and with different operating systems to communicate with each other seamlessly.

Some key aspects of network protocols:

Data Formatting: Protocols specify the structure and format of data packets, including headers, payloads, and any other necessary information. This ensures that devices can interpret incoming data correctly.

Data Transmission: Protocols define how data is transmitted over the network, including the method of encoding, modulation, and transmission medium (e.g., wired or wireless).

Addressing: Protocols establish addressing schemes to identify the source and destination of data packets. These addresses may include IP addresses, MAC addresses, or other identifiers depending on the protocol.

Routing: Protocols determine how data packets are routed through the network from the source to the destination. This may involve selecting the best path based on factors like network congestion, latency, and reliability.

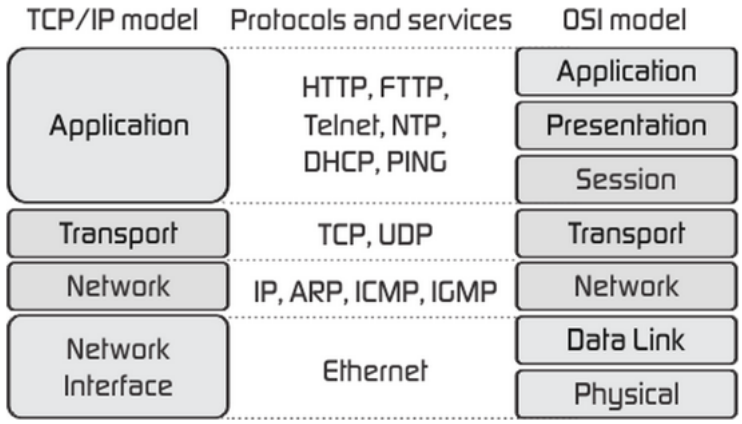
Error Handling: Protocols include mechanisms for detecting and correcting errors that may occur during data transmission. This ensures data integrity and reliability.

Flow Control: Protocols implement flow control mechanisms to manage the rate of data transmission between devices, preventing data loss or congestion.

Security: Many protocols include security features to protect data from unauthorized access, interception, or modification. This may include encryption, authentication, and access control mechanisms.

Some common network protocols include:

TCP/IP (Transmission Control Protocol/Internet Protocol): The TCP/IP protocol suite is the foundation of the Internet and is used for communication between devices on the Internet and many local area networks. TCP provides reliable, connection-oriented communication, while IP handles addressing and routing of data packets.



HTTP (Hypertext Transfer Protocol): HTTP is the protocol used for transferring hypertext documents on the World Wide Web. It defines how web browsers and web servers communicate, enabling the retrieval and display of web pages.

SMTP (Simple Mail Transfer Protocol): SMTP is a protocol used for sending email messages between email servers. It defines how email messages are transmitted and delivered over the Internet.

FTP (File Transfer Protocol): FTP is a protocol used for transferring files between a client and a server on a computer network. It provides a standard method for uploading, downloading, and managing files on remote servers.

DNS (Domain Name System): DNS is a protocol used for translating domain names into IP addresses. It enables users to access websites and other resources on the Internet using human-readable domain names.

Network design plan

A network design plan is a comprehensive document that outlines the blueprint for creating or improving a computer network. It details the architecture, layout, and specifications of the network, as well as the strategies and methodologies for its implementation. A well-designed network plan ensures that the network meets the organization's requirements for performance, reliability, security, and scalability. Here are key components typically included in a network design plan:

Introduction:

Provides an overview of the organization's goals and objectives for the network.
Describes the purpose and scope of the network design plan.

Current Network Assessment:

Evaluates the existing network infrastructure, including hardware, software, and configurations.
Identifies strengths, weaknesses, opportunities, and threats (SWOT analysis) of the current network.

Requirements Analysis:

Defines the functional and technical requirements of the network based on the organization's needs.
Considers factors such as performance, reliability, security, scalability, and budget constraints.

Network Architecture:

Describes the overall architecture of the network, including the physical and logical layout.
Specifies the types of devices, their locations, and their interconnections (e.g., routers, switches, servers, endpoints).
Determines the network topology (e.g., star, bus, ring, mesh) based on the requirements and constraints.

IP Addressing and Subnetting Plan:

Develops an IP addressing scheme for the network, including IP address ranges, subnet masks, and gateway addresses.
Defines the allocation of IP addresses to devices and subnetworks to optimize address space utilization.

Security Plan:

Outlines security measures to protect the network from unauthorized access, data breaches, and other threats.

Specifies authentication mechanisms, access controls, encryption protocols, firewalls, intrusion detection/prevention systems, and security policies.

Quality of Service (QoS) Plan:

Addresses requirements for network performance, including bandwidth, latency, and reliability.

Defines QoS policies and mechanisms for prioritizing traffic, managing congestion, and ensuring service level agreements (SLAs) are met.

Network Management Plan:

Defines procedures and tools for managing, monitoring, and maintaining the network.

Specifies roles and responsibilities of network administrators, procedures for configuration management, backup and recovery strategies, and documentation standards.

Implementation Plan:

Details the step-by-step process for implementing the network design, including timelines, milestones, and resource allocation.

Identifies potential risks and mitigation strategies to ensure a smooth deployment.

Testing and Validation Plan:

Outlines procedures for testing and validating the network design before and after deployment.

Includes criteria for evaluating performance, functionality, and security of the network.

Training Plan:

Defines training requirements for IT staff and end-users to ensure they can effectively use and support the new network.

Specifies training materials, schedules, and delivery methods.

Documentation:

Provides comprehensive documentation of the network design, including diagrams, configurations, policies, procedures, and troubleshooting guides.

Ensures that the network design plan can be easily understood, maintained, and updated over time.

Self-Check Sheet 2: Interpret the network layout

1. What is the first step in setting up an existing network?

2. Why is it important to collect organizational requirements?

3. What is network layout?

4. How can network layout be documented?

5. What is network topology?

6. Why is it important to identify existing network topology?

7. What are some common network topologies?

8. What are network protocols?

9. Why is it important to document existing network protocols?

10. What is an IP addressing scheme?

Answer Key 2: Interpret the network layout

1. What is the first step in setting up an existing network?
   Answer: The first step is to collect and document organizational requirements to understand the needs and objectives of the network setup.
2. Why is it important to collect organizational requirements?
   Answer: Collecting organizational requirements helps ensure that the network setup aligns with the organization's goals and objectives, leading to a more effective and efficient network design.
3. What is network layout?
   Answer: Network layout refers to the physical or logical arrangement of devices, connections, and protocols within a network.
4. How can network layout be documented?
   Answer: Network layout can be documented using diagrams, such as network topology diagrams, that illustrate the connections between devices and the overall structure of the network.
5. What is network topology?
   Answer: Network topology defines how devices are interconnected and how data flows between them in a network.
6. Why is it important to identify existing network topology?
   Answer: Identifying existing network topology helps understand the current configuration of the network, which is essential for planning upgrades or modifications.
7. What are some common network topologies?
   Answer: Common network topologies include star, bus, ring, mesh, and hybrid topologies.
8. What are network protocols?
   Answer: Network protocols are sets of rules and conventions that govern communication between devices in a network.
9. Why is it important to document existing network protocols?
   Answer: Documenting existing network protocols helps ensure interoperability and compatibility with new network components or configurations.
10. What is an IP addressing scheme?
    Answer: An IP addressing scheme is a systematic plan for assigning IP addresses to devices within a network, defining how addresses are allocated and managed.

Task Sheet 2.1: Interpret the network layout

TASK SHEET 2.1
Title: Interpret the network layout
Performance Objective: At the end of this task, the trainee should be able to Gather information about the organization's goals, objectives, and needs related to the network setup.
1. Interpret Schedule meetings minutes with key stakeholders, such as IT managers, department heads, and end-users, to discuss requirements.
2. Interpret questionnaires or surveys to gather input from relevant parties.
3. Interpret Document requirements related to performance, reliability, security, scalability, and budget constraints.
4. Interpret network diagrams, schematics, or documentation from the IT department or network administrators.
5. Interpret site surveys to observe the placement of networking equipment, cable runs, and other infrastructure components.
6. Interpret network diagrams to visualize the current network layout.
7. Interpret network design documentation, including architectural diagrams, specifications, and implementation plans.
8. Identify key components of the design plan, such as hardware and software requirements, security measures, and scalability strategies.
9. Interpret the alignment of the design plan with organizational goals and technical feasibility.
10. Interpret IP addressing documentation, including addressing plans, subnetting schemes, and allocation strategies.
11. Interpret IP address assignments and subnet configurations to ensure efficient utilization of address space.
12. Interpret existing network infrastructure and adherence to industry standards (e.g., RFC 1918 for private IP addresses).

Specification sheet 2.1: Interpret the Network Layout

A. Supplies Documents

- Sample format of Network Layout

B. Tools and Material required:

- Notebook
- Handbook
- Office Stationeries

C. Equipment:

- Laptop/Computer

Learning Outcome 3: Connect devices to the existing network

Assessment Criteria:

1. Required transmission media, tools and equipment are selected and collected.
2. Cabling is performed as per layout
3. Connections is established as per layout design.
4. Device is connected with the existing network with appropriate transmission media infrastructure
5. IP properties is assigned and connectivity is tested as per work plan.

Content:

1. Required transmission media
    - Wired
    - Wireless
2. Tools and equipment.
    - Crimping tool
    - Connector
    - Boot cap
    - Face plate modular
    - Punching tool
    - Screw driver set
    - Cable tester
    - Cable cutter
    - Patch cord
    - Cable Tag
    - Cable tie
3. Cabling procedure
4. Assigning IP properties
    - IP address
    - Subnetmask
    - Gateway
    - DNS
5. Testing connectivity.

Resources Required/ Conditions:

The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application
- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 3: Connect devices to the existing 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 Steps	Resources specific instructions
1. Student will ask the instructor about devices connecting to the existing network.	1. Instructor will provide the learning materials "Performing Basic Networking"
2. Read the Information sheet/s	2. Information Sheet No 3: Connect devices to the existing network.
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No 3: Connect devices to the existing network. Answer key No. 3: Connect devices to the existing network
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No 3-1: Connect devices to the existing network Specification Sheet 3-1: Connect devices to the existing network

Information Sheet 3: connect Devices to the existing network.

Learning Objectives:

After completion of this information sheet, the learners will be able to:

1. Select and collect required transmission media, tools and equipment.
2. Perform cabling as per layout
3. Establish connections as per layout design.
4. Connect device with the existing network with appropriate transmission media infrastructure
5. Assign IP properties and test connectivity as per work plan.

Transmission media

Transmission media are the physical mediums used to transmit data signals from one device to another within a computer network. The choice of transmission media depends on factors such as the distance between devices, the data transfer rate required, cost considerations, and environmental factors. Here are some common types of transmission media used in networking:

Twisted Pair Cable:

Twisted pair cable consists of pairs of insulated copper wires twisted together. It is commonly used in Ethernet networks for short to medium-distance connections, such as within buildings or office environments.

Twisted pair cable is available in two main categories: unshielded twisted pair (UTP) and shielded twisted pair (STP). UTP is more commonly used due to its lower cost and flexibility, while STP provides better protection against electromagnetic interference (EMI) and crosstalk.

Coaxial Cable:

Coaxial cable consists of a central conductor surrounded by insulation, a metallic shield, and an outer insulating layer. It is commonly used for cable television (CATV) and broadband internet connections.

Coaxial cable offers higher bandwidth and longer transmission distances compared to twisted pair cable, making it suitable for applications requiring high data transfer rates over longer distances.

Fiber Optic Cable:

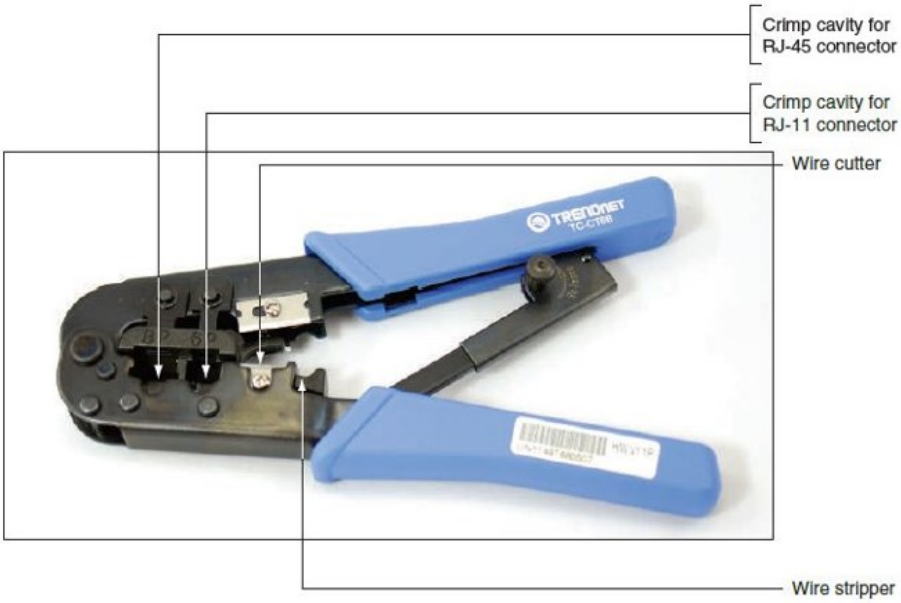
Fiber optic cable uses thin strands of glass or plastic fibers to transmit data signals using light pulses. It offers the highest bandwidth and longest transmission distances of any transmission medium.

Fiber optic cable is immune to electromagnetic interference and provides secure data transmission, making it ideal for high-speed internet connections, long-distance communication links, and networking environments with high levels of EMI.

Tools and equipment

Crimping tool

A crimping tool is a hand tool used to attach connectors to the ends of cables. It is commonly used in networking for terminating Ethernet cables with RJ45 connectors, which are used to connect devices to network switches, routers, and other networking equipment. Crimping tools are essential for ensuring secure and reliable connections between cables and connectors. Here's how a crimping tool works and its key features:



Functionality:

The primary function of a crimping tool is to attach connectors, such as RJ45 connectors, to the ends of cables. This process is known as crimping.

Crimping involves placing the connector onto the stripped end of the cable, aligning the wires according to the correct pinout configuration, and then compressing the connector onto the wires using the crimping tool. The crimping tool applies pressure to the connector, deforming it around the cable's wires, creating a secure and electrically conductive connection.

Connector

A connector is a device used to establish a physical and electrical connection between two or more components within a network or electronic system. Connectors come in various shapes, sizes, and types, each designed for specific applications and requirements. In networking, connectors play a crucial role in facilitating communication between devices by allowing the transmission of data signals, power, or both. Here are some key aspects of connectors:

Functionality:

- The primary function of a connector is to join two or more components together to enable the transfer of signals, power, or both.
- Connectors provide a secure and reliable interface between devices, ensuring proper alignment, contact, and conductivity.
- Connectors may include pins, sockets, contacts, or terminals that establish electrical connections between mating components.

Types of Connectors:

RJ45 Connector:

The RJ45 connector is the most common type of connector used in networking for terminating Ethernet cables. It is used to connect devices such as computers, routers, switches, and network interface cards (NICs) to Ethernet networks.

The RJ45 connector has eight pins arranged in a modular plug, which are crimped onto the ends of twisted pair cables using a crimping tool.

Fiber Optic Connector:

Fiber optic connectors are used to terminate fiber optic cables, which transmit data signals using light pulses. They come in various types, such as SC, LC, ST, and MTP/MPO connectors, each with specific characteristics and applications.

Fiber optic connectors provide low insertion loss, high reliability, and immunity to electromagnetic interference, making them ideal for high-speed data transmission over long distances.

Coaxial Connector:

Coaxial connectors are used to terminate coaxial cables, which are commonly used for cable television (CATV), broadband internet, and RF communication applications.

The most common types of coaxial connectors include F-type connectors, BNC connectors, and SMA connectors, each with unique characteristics and applications.

Modular Connector (RJ11/RJ12):

Modular connectors, such as RJ11 and RJ12 connectors, are used for terminating telephone cables. They are similar in appearance to RJ45 connectors but have fewer pins.

RJ11 connectors are commonly used for connecting telephones, fax machines, and modems to telephone lines, while RJ12 connectors are used for connecting multiple telephone lines or extensions.

Power Connector:

Power connectors are used to deliver electrical power to devices within a network or electronic system. They come in various types, including barrel connectors, DC power jacks, and AC power plugs.

Power connectors may include features such as locking mechanisms, polarized designs, and strain relief to ensure a secure and reliable connection.

Boot cap

In the context of networking and cabling, a boot cap refers to a protective covering or boot that is attached to the end of a connector, such as an RJ45 connector on an Ethernet cable. The boot cap is typically made of a flexible and durable material, such as rubber or plastic, and is designed to provide protection and strain relief for the connector and the cable.

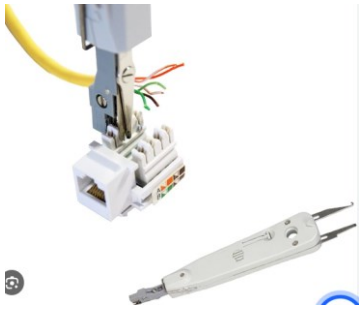
Face plate modular

A faceplate modular, often referred to simply as a modular faceplate, is a component used in networking and telecommunications infrastructure to organize and terminate multiple network connections in a structured manner. It typically consists of a mounting plate with multiple ports or openings, into which modular connectors, such as RJ45 jacks or keystone jacks, can be inserted and secured.

Punching tool

A punching tool, also known as a punch down tool or impact tool, is a handheld tool used in networking and telecommunications to terminate and secure wires into connectors or terminal blocks. It is commonly used

for terminating twisted pair cables onto punch down blocks, patch panels, keystone jacks, and other termination points in network installations.



Screw driver set

In networking, a screwdriver set is a collection of tools used for installing, maintaining, and troubleshooting networking equipment and infrastructure. While the specific tools included in a screwdriver set may vary, they typically consist of various types and sizes of screwdrivers that are commonly used in networking applications. Here are the key aspects of a screwdriver set in networking.

Types of Screwdrivers:

Phillips Screwdrivers: Phillips screwdrivers are one of the most common types of screwdrivers used in networking. They feature a cross-shaped tip that fits into Phillips head screws, which are frequently used to secure components such as network switches, routers, and patch panels.

Flathead Screwdrivers: Flathead screwdrivers, also known as slotted screwdrivers, have a flat, straight tip that fits into slotted or flathead screws. While less common in networking equipment, flathead screws may still be encountered in certain installations.

Torx Screwdrivers: Torx screwdrivers are used for screws with a star-shaped or six-pointed recessed socket. They are commonly found in certain types of network equipment, such as server racks and specialized networking hardware.

Hex Screwdrivers (Allen Keys): Hex screwdrivers, also known as Allen keys or hex keys, are used for hexagonal screws and bolts. They are commonly used in rack mounting hardware, cable management accessories, and other networking components.

Cable tester

A cable tester is a diagnostic tool used to verify the integrity and functionality of various types of cables commonly used in networking and telecommunications installations. It helps ensure that cables are properly installed, terminated, and functioning as intended. Cable testers come in different forms and with varying features, but they typically provide several common functions and capabilities.

Functions:

Continuity Testing:

Cable testers can verify the continuity of conductors within a cable by checking for continuity between the wire pairs at each end of the cable. This ensures that all conductors are properly connected and that there are no breaks or shorts in the cable.

Wire Mapping:

Cable testers can identify the wiring configuration (pinout) of a cable by mapping the connections between the wire pairs at each end of the cable. This helps ensure that the cable is terminated correctly according to the appropriate wiring standard (e.g., TIA/EIA-568 for Ethernet cables).

Length Measurement:

Some cable testers can measure the length of a cable by sending signals down the cable and measuring the time it takes for the signals to travel from one end to the other. This helps determine the distance of the cable run and identify any discrepancies or irregularities in cable length.

Fault Identification:

Cable testers can detect common faults such as opens, shorts, and crossed wires in a cable. They provide visual and/or audible indicators to alert the user to the presence of faults and help pinpoint their location within the cable.

Cable cutter

A cable cutter is a tool used to cut and trim cables with precision and efficiency. It is commonly used in networking and telecommunications installations to prepare cables for termination, splicing, or termination into connectors. Cable cutters come in various forms and sizes, each designed for specific cable types and diameters.

Patch cord

A patch cord, also known as a patch cable or patch lead, is a short length of cable with connectors on both ends, typically used to connect network devices, such as computers, switches, routers, and patch panels, in a local area network (LAN) or telecommunications system. Patch cords are commonly used in networking environments to establish temporary or permanent connections between devices and network infrastructure components.

Cable Tag

A cable tag is a label or tag affixed to a cable, typically near its termination points or at regular intervals along its length, to provide identification and organization within a network or cabling infrastructure. Cable tags serve several important purposes in networking and telecommunications installations, helping to facilitate cable management, troubleshooting, and maintenance activities.

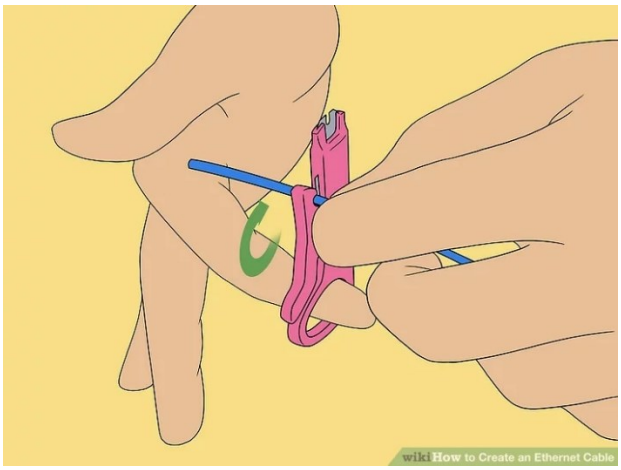
Cable tie

A cable tie, also known as a zip tie, wire tie, or hose tie, is a type of fastening device used to securely bundle and organize cables, wires, hoses, and other items in various applications, including networking and cabling installations. Cable ties are widely used in both residential and commercial settings to manage and organize cables and wires, ensuring a neat and tidy appearance while also providing strain relief and protection for the cables.

Step by step Cabling procedure:

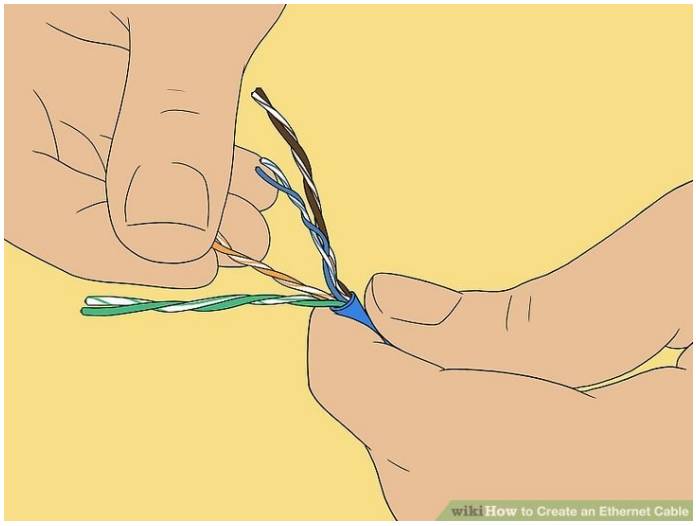
Step 1:

Strip your cable. Use your cable strippers at about 1-2 inches from the end of the cable to remove the outer jacket.



Step 2:

Untwist the twisted pair wires all the way back to the jacket. This can be done just like a regular twist-tie on a loaf of bread, but with four of them of different colors.

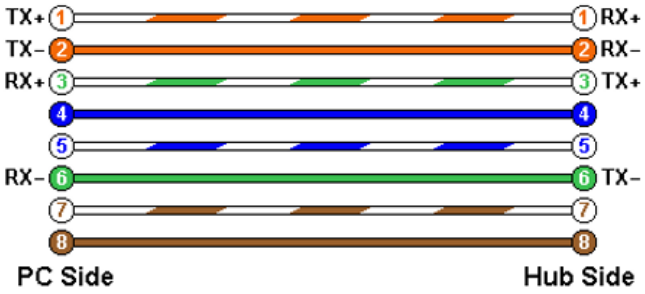


Step 3:

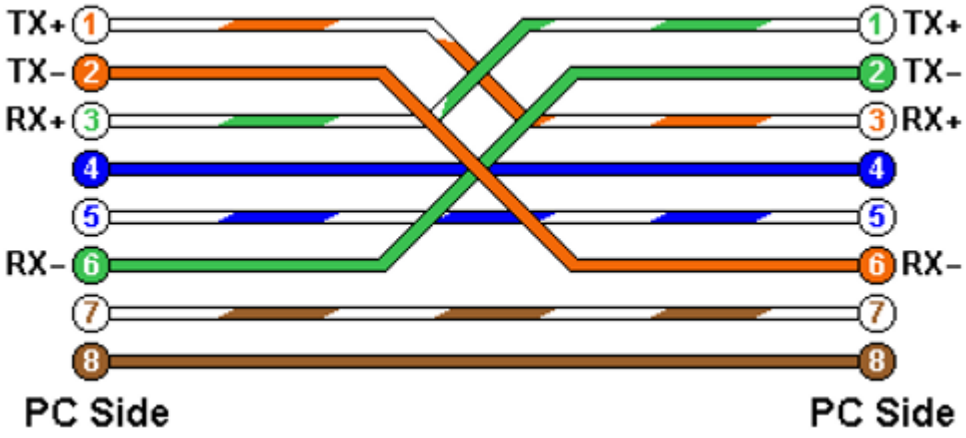
Align the untwisted wires in the order necessary for your needs. For this scenario, you'll be making a straight-through cable, which has both ends of the cable with the same alignment of wires, so it's easy enough to do. Since this is your first cable, we'll consult the cheat sheet to know what order we're aligning in!

Pin	100BaseT Purpose	T568A Wiring	T568B Wiring
1	Transmit+	Pair 3: White/green	Pair 2: White/orange
2	Transmit-	Pair 3: Green	Pair 2: Orange
3	Receive+	Pair 2: White/orange	Pair 3: White/green
4	(Used only on Gigabit Ethernet)	Pair 1: Blue	Pair 1: Blue
5	(Used only on Gigabit Ethernet)	Pair 1: White/blue	Pair 1: White/blue
6	Receive-	Pair 2: Orange	Pair 3: Green
7	(Used only on Gigabit Ethernet)	Pair 4: White/brown	Pair 4: White/brown
8	(Used only on Gigabit Ethernet)	Pair 4: Brown	Pair 4: Brown

Straight Through Cable

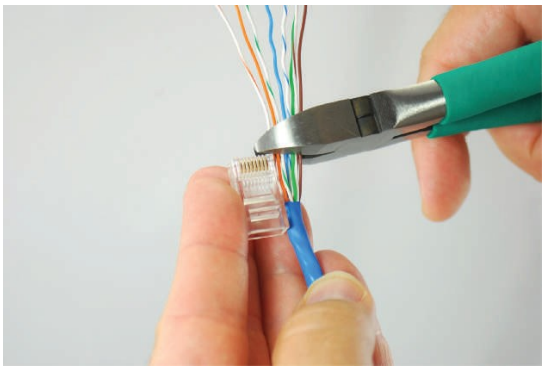


Crossover connection



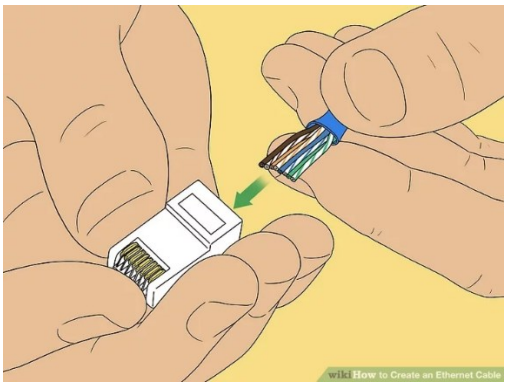
Step 4:

Cut the extra wire. Once you've untwisted the wires, you'll have a superfluous amount of copper wiring left; we don't need this much, but it's good to have it in the previous step to help in aligning the colors properly. Use the wire-cutting scissors to cut these off.



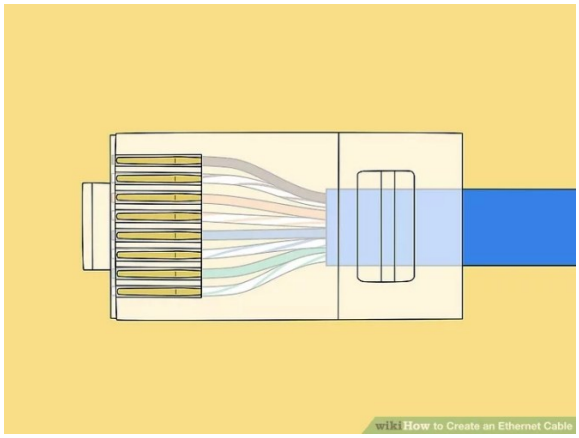
Step 5:

Push the remaining wires into the RJ45 head. Be careful not to bend the wires while pushing them in or you run the risk of creating a bad cable. You also don't want too little or too much wire left in the head; there's no definite length necessary, but it's pretty obvious to tell if there's too much cable or not enough. A short length of the jacket should be up the RJ45 head; use this knowledge as a reference.



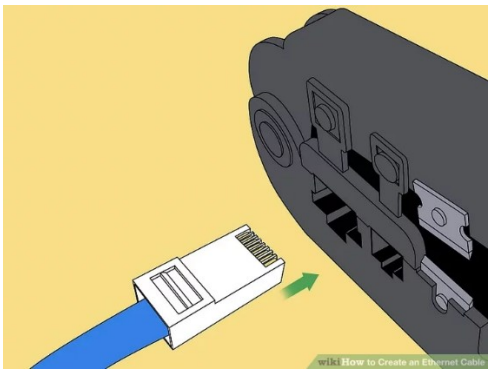
Step 6

Double-check that the wires are all the way up into the gold pins of the head and made it up in the proper order. (Consult your cheat sheet if needed!)



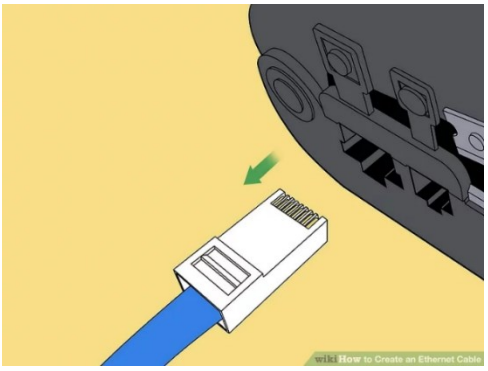
Step 7:

Push the head into the open space of the crimping tool and squeeze it closed, hard. If you don't crimp the cable all the way, the head may come off.



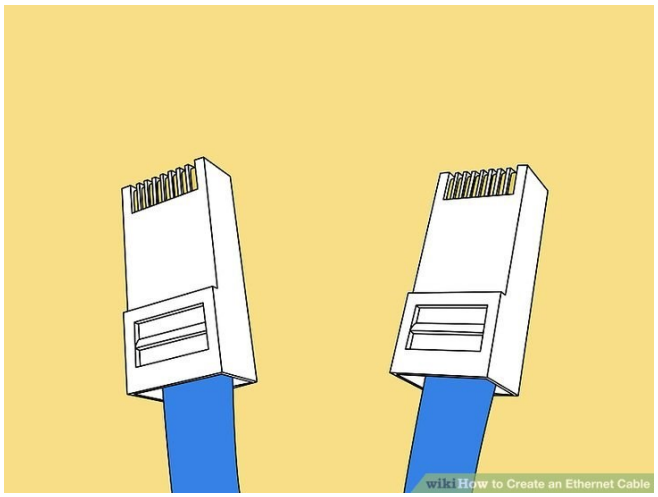
Step 8:

Open the crimping tool and remove your newly-crimped Ethernet connector.



Step 9:

Repeat the crimping process on the other side of the cable if you're making a completely new cable. If you're repairing one end, this won't apply to you, so move on.



Step 10:

Plug one end of the cable into the tan, two-port end of the cable tester, and the other end into the other part of the tester with the graphic display window. Turn it on and listen for the beep. If it beeps once, you successfully made an Ethernet cable; if it beeps twice, some part of the cable is messed up and needs repairing. Depending on the error, the cable may or may not still be usable.

Assigning IP properties

Assigning IP properties involves configuring the essential network settings for devices to communicate over an IP-based network. These settings include IP addresses, subnet masks, default gateways, and DNS servers. Here's an overview of the process:

IP Address Assignment:

Static IP Addressing: In a static IP addressing scheme, each device on the network is manually configured with a unique IP address. Administrators assign IP addresses based on a predetermined addressing plan to ensure consistency and avoid conflicts.

Dynamic IP Addressing:

Dynamic IP addressing relies on DHCP (Dynamic Host Configuration Protocol) servers to automatically assign IP addresses to devices when they connect to the network. DHCP servers maintain a pool of available IP addresses and lease them to devices for a specified period.

Subnet Mask Configuration:

The subnet mask defines the network portion and host portion of an IP address. It is used by devices to determine whether a destination IP address is on the same local network or a remote network.

Subnet masks are typically expressed in dotted decimal notation (e.g., 255.255.255.0) or using CIDR (Classless Inter-Domain Routing) notation (e.g., /24).

Default Gateway Setting:

The default gateway, also known as the router or gateway address, is the IP address of the device that serves as the exit point for traffic destined for remote networks.

Devices use the default gateway to forward packets to destinations outside their local subnet.

DNS (Domain Name System) Configuration:

DNS servers translate domain names (e.g., www.example.com) into IP addresses that computers can use to locate resources on the internet or within a network.

Devices are configured with one or more DNS server IP addresses to resolve domain names to IP addresses.

Testing connectivity

Testing connectivity involves verifying that network devices can communicate with each other successfully over the network. It ensures that data can flow between devices without issues, enabling efficient operation of the network infrastructure. Here's how testing connectivity is typically performed:

Ping Test:

The ping command is a widely used tool for testing connectivity between devices on a network.

To perform a ping test, enter the command "ping" followed by the IP address or hostname of the target device in the command prompt or terminal.

The ping utility sends ICMP (Internet Control Message Protocol) echo request packets to the target device and waits for an ICMP echo reply.

A successful ping test indicates that there is connectivity between the source and destination devices. It also provides information about round-trip time (RTT) and packet loss.

Traceroute/Tracepath Test:

Traceroute (on Windows) or tracepath (on Linux/Unix) is a tool used to trace the route that packets take from the source device to the destination device.

Traceroute/tracepath provides a list of the intermediate devices (routers) that the packets pass through, along with the RTT for each hop.

This test helps identify network issues, such as routing loops, delays, or packet loss, by showing the path and latency between the source and destination.

Telnet/SSH Test:

Telnet and SSH (Secure Shell) are network protocols used to establish remote terminal sessions with devices.

Testing connectivity with Telnet or SSH involves attempting to establish a connection to the target device using the Telnet or SSH client software.

A successful Telnet/SSH connection indicates that there is connectivity between the source and destination devices, and that the target device is accepting connections on the specified port.

Network Protocol Testing:

Applications or services that rely on specific network protocols, such as HTTP, FTP, SMTP, or SNMP, can be tested to ensure connectivity and proper operation.

For example, testing HTTP connectivity involves attempting to access a web server using a web browser or HTTP client software, and verifying that web pages can be loaded successfully.

Physical Connectivity Checks:

Physical layer connectivity checks involve verifying that network cables are properly connected and that networking devices (e.g., switches, routers) have their corresponding ports enabled and configured correctly.

Visual inspection and cable testing tools can be used to check for cable faults, damaged connectors, or unplugged cables.

Firewall and Security Checks:

Firewall and security settings on devices can sometimes block or restrict network traffic, affecting connectivity.

Testing connectivity involves verifying that firewall rules and security policies allow the necessary network traffic to pass through, and troubleshooting any issues that may arise.

Self-Check Sheet 3: Devices connection to the existing network.

1. What is the purpose of selecting and collecting required transmission media, tools, and equipment?

2. What are some examples of transmission media commonly used in networking?

3. Why is it important to perform cabling as per the layout design?

4. What steps are involved in establishing connections as per the layout design?

5. How do you connect a device with the existing network using appropriate transmission media infrastructure?

6. What is the purpose of assigning IP properties to devices in a network?

7. How do you test connectivity after assigning IP properties?

8. What role does proper cable management play in cabling installations?

9. Why is it important to adhere to the work plan when performing network installations?

10. What are some common challenges faced during network installations, and how can they be addressed?

Answer Key 3: Devices connection to the existing network.

1. What is the purpose of selecting and collecting required transmission media, tools, and equipment?
   Answer: The purpose is to gather the necessary materials and tools needed for cabling installations, ensuring the availability of appropriate transmission media and equipment for establishing network connections.
2. What are some examples of transmission media commonly used in networking?
   Answer: Examples include twisted pair cables, fiber optic cables, and coaxial cables, each with its own advantages and applications in network installations.
3. Why is it important to perform cabling as per the layout design?
   Answer: Performing cabling according to the layout design ensures that cables are routed efficiently and in compliance with the planned network infrastructure, minimizing disruptions and optimizing cable management.
4. What steps are involved in establishing connections as per the layout design?
   Answer: The steps include routing cables along designated pathways, terminating cables with connectors, labeling cables and ports, and securing connections to networking devices and equipment.
5. How do you connect a device with the existing network using appropriate transmission media infrastructure?
   Answer: Connect the device to the existing network using compatible transmission media, such as Ethernet cables for wired connections or wireless access points for wireless connections, ensuring proper termination and configuration.
6. What is the purpose of assigning IP properties to devices in a network?
   Answer: Assigning IP properties, such as IP addresses, subnet masks, default gateways, and DNS server addresses, enables devices to communicate effectively over an IP-based network.
7. How do you test connectivity after assigning IP properties?
   Answer: Testing connectivity involves using tools such as ping, traceroute, and Telnet to verify that devices can communicate with each other successfully and that network services are accessible.
8. What role does proper cable management play in cabling installations?
   Answer: Proper cable management ensures that cables are organized, labeled, and secured appropriately, minimizing cable clutter, reducing the risk of damage or interference, and simplifying maintenance and troubleshooting.
9. Why is it important to adhere to the work plan when performing network installations?
   Answer: Adhering to the work plan ensures that installations are carried out efficiently, accurately, and in accordance with project requirements, timelines, and budget constraints.
10. What are some common challenges faced during network installations, and how can they be addressed?
    Answer: Common challenges include cable length limitations, compatibility issues, and environmental factors. These challenges can be addressed through proper planning, testing, and collaboration with stakeholders to identify and resolve issues effectively.

Task Sheet 3.1: Connect device to the existing network.

Title: Connect DEVICE to the existing network.
Performance Objective: By the end of this task, the trainee should be able to install and configure network infrastructure components according to the specified layout design and work plan.
1. Identify the necessary transmission media, tools, and equipment needed for the installation.
2. Gather twisted pair cables, fiber optic cables, connectors, patch panels, racks, crimping tools, cable testers, and other required items.
3. Refer to the provided layout design to determine cable routes, termination points, and equipment locations.
4. Lay out cables along designated pathways, ensuring proper organization and cable management.
5. Terminate cables with appropriate connectors according to the layout specifications.
6. Connect cables to patch panels, switches, routers, and other networking devices based on the layout design.
7. Label cables and ports clearly to facilitate identification and troubleshooting.
8. Determine the appropriate transmission media infrastructure (e.g., Ethernet cables, wireless access points) for connecting devices to the existing network.
9. Configure and install network interfaces on devices, ensuring compatibility with the network infrastructure.
10. Establish connections between devices and the existing network, following industry standards and best practices.
11. Configure IP addresses, subnet masks, default gateways, and DNS server addresses on devices as per the IP addressing scheme defined in the work plan.
12. Ensure that IP properties are assigned correctly and consistently across all devices.
13. Use appropriate testing tools (e.g., ping, traceroute, Telnet) to verify connectivity between devices and across the network.
14. Test network services and applications to ensure they are accessible and functioning as expected.
15. Troubleshoot any connectivity issues and address them promptly to ensure network reliability and performance.

Specification Sheet 3.1

A. Tools and Material required:

- Crimping tool
- Connector
- Boot cap
- Face plate modular
- Punching tool
- Screw driver set
- Cable tester
- Cable cutter
- Patch cord
- Cable Tag
- Cable tie

B. Equipment:

- Laptop/Computer

Learning Outcome 4: Troubleshoot in existing network

Assessment Criteria:

1. Network design, support and maintenance documents are reviewed.
2. Appropriate person is consulted for identifying problems if required.
3. Faulty hardware or software component are detected.
4. Solution of Problem is performed.
5. Network functionality is tested.
6. Maintenance and troubleshooting documents are updated.
7. Tools and equipment are stored as per workplace procedures.

Content:

1. Reviewing Network design, support and maintenance documents.
2. Appropriate person consultation.
3. Faulty hardware or software component.
4. Testing procedure of Network functionality.
5. Maintenance and troubleshooting documents.
6. Storing procedure of Tools and equipment.

Resources Required/ Conditions:

The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application
- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 4: Troubleshooting in existing 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 Steps	Resources specific instructions
1. Student will ask the instructor about Troubleshooting in existing network.	1. Instructor will provide the learning materials "**Performing Basic Networking"**
2. Read the Information sheet/s	2. Information Sheet No: 4 Troubleshooting in existing network
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 4 Troubleshooting in existing network Answer key No. 4 Troubleshooting in existing network
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No: 4 Troubleshooting in existing network Specification Sheet: 4 Troubleshooting in existing network

Information Sheet 4: Troubleshoot in existing network

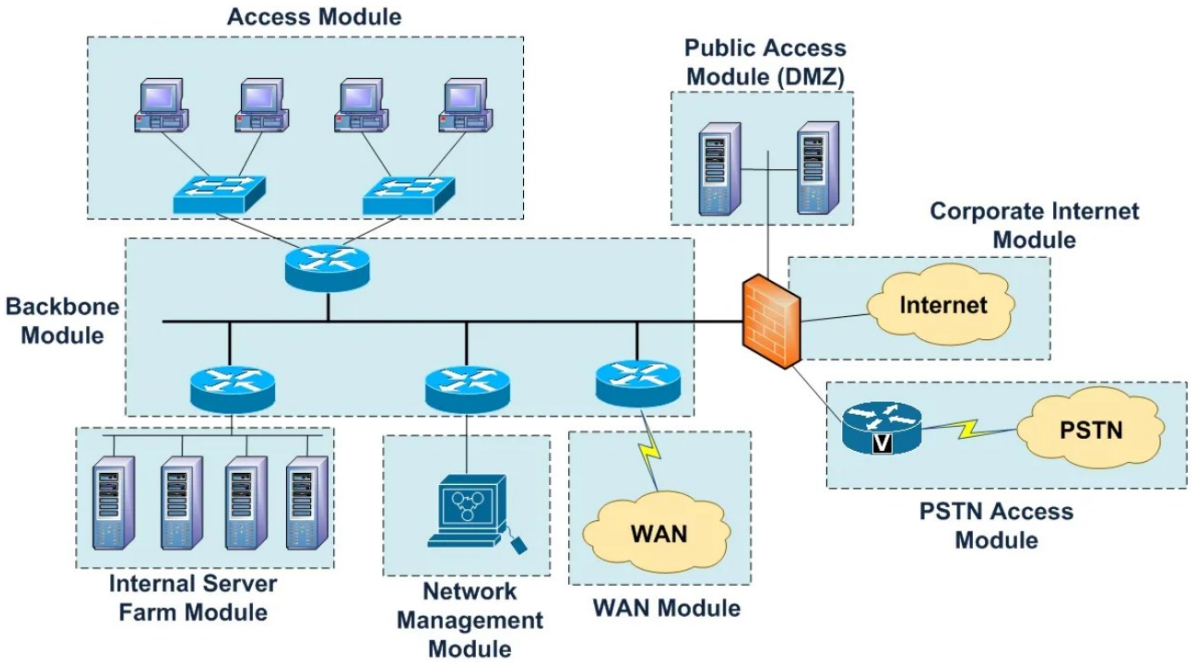
Learning Objectives:

After completion of this information sheet, the learners will be able to:

1. Review Network design, support and maintenance documents.
2. Consult Appropriate person for identifying problems if required.
3. Detect Faulty hardware or software component.
4. Perform solution of Problem.
5. Test Network functionality.
6. Update Maintenance and troubleshooting documents.
7. Store Tools and equipment as per workplace procedures.

Reviewing Network design, support and maintenance documents.

Reviewing network design, support, and maintenance documents is crucial for effective troubleshooting, as these documents provide valuable insights into the network architecture, configuration, and operational procedures.



Reviewing process supports troubleshooting efforts:

Network Design Documentation:

Topology and Configuration: Reviewing network design documents helps troubleshooters understand the network's topology, including the layout of devices, connections, and routing protocols.

Segmentation and Subnetting: Understanding how the network is segmented and submitted aids in isolating and diagnosing issues within specific network segments.

Redundancy and Failover:

Examining redundancy and failover mechanisms documented in the design helps troubleshooters identify backup paths or redundant devices that may be involved in fault recovery.

Security Measures:

Reviewing security measures documented in the design assists in identifying potential security-related issues and ensuring compliance with security policies during troubleshooting.

Support Documentation:

Incident Management Procedures: Support documentation provides guidelines for reporting, escalating, and resolving network incidents, ensuring that troubleshooting efforts follow established protocols and are documented properly.

Troubleshooting Workflows:

Documentation outlining troubleshooting workflows and procedures helps troubleshooters follow a systematic approach to identify and resolve network issues efficiently.

Historical Data:

Support documentation may include records of past incidents, their resolutions, and any relevant troubleshooting steps taken. Reviewing this historical data can provide insights into recurring issues or patterns that may aid in troubleshooting current problems.

Maintenance Documentation:

Configuration Records:

Maintenance documentation contains records of network device configurations, software versions, and firmware updates. Reviewing these records helps troubleshooters identify misconfigurations or outdated software/firmware that may contribute to network issues.

Change Logs:

Monitoring change logs documented during network maintenance activities can help identify recent changes that may have introduced or contributed to network problems.

Performance Monitoring Data:

Maintenance documentation may include performance monitoring data, such as logs, reports, or graphs showing network traffic patterns, bandwidth utilization, and error rates. Analyzing this data can help troubleshooters identify performance-related issues and bottlenecks.

Continuous Improvement:

Feedback Mechanisms:

Troubleshooting efforts can benefit from feedback mechanisms that capture insights and lessons learned during the troubleshooting process. This feedback can inform updates to network documentation, improving its accuracy and relevance for future troubleshooting scenarios.

Training and Knowledge Sharing:

Continuous improvement initiatives may include training programs and knowledge-sharing sessions aimed at enhancing troubleshooters' skills and familiarity with network documentation, enabling them to troubleshoot more effectively.

Appropriate person consultation

Consulting appropriate persons for identifying network problems involves engaging individuals or groups with expertise in networking, IT infrastructure, and related areas. Here's how to effectively consult appropriate persons for identifying network problems:

IT Support Team:

IT support personnel handle day-to-day user issues, including network connectivity problems reported by end-users.

They can provide insights into common network issues experienced by users, such as slow internet access, dropped connections, or inability to access network resources.

Consult them to gather information about reported network problems, troubleshoot user connectivity issues, and identify patterns or recurring issues.

External Consultants or Vendors:

External consultants or vendors specializing in networking and IT infrastructure may provide valuable expertise and insights.

They can conduct network assessments, audits, or performance evaluations to identify problems and recommend solutions.

Consult them for independent assessments, specialized expertise, or assistance with complex network issues that require external support.

End-Users:

End-users are the individuals who interact with the network on a daily basis to perform their tasks.

They may encounter network problems or usability issues that go unnoticed by technical staff.

Consult them to gather feedback, identify user-experience issues, and understand how network problems impact their productivity and workflow.

Detecting Faulty hardware or software component

Identifying faulty hardware or software components in an existing network requires careful analysis and diagnostic procedures.

List of potential faulty hardware or software components commonly encountered in network environments:

Faulty Hardware Components:

- Network Switches: Defective ports, failed power supplies, malfunctioning fans, or faulty backplanes can lead to network connectivity issues or performance degradation.
- Routers: Hardware failures in routers, such as failed interfaces, memory corruption, or overheating, can result in routing issues, packet loss, or network instability.
- Network Interface Cards (NICs): Faulty NICs may exhibit symptoms like intermittent connectivity, packet loss, or inability to establish network connections.
- Servers: Hardware failures in servers, including faulty hard drives, memory modules, power supplies, or CPU overheating, can cause server outages or service disruptions.
- Wireless Access Points (WAPs): Faulty WAPs may experience signal degradation, intermittent connectivity, or complete failure, impacting wireless network performance and coverage.
- Firewalls: Hardware failures in firewalls, such as failed power supplies, CPU overheating, or hardware component failures, can compromise network security and access control.

Faulty Software Components:

- Operating Systems: Software issues in operating systems, such as corrupted system files, driver conflicts, or software bugs, can cause system crashes, application errors, or performance degradation.
- Network Protocols: Software bugs or implementation errors in network protocols, such as TCP/IP, DHCP, DNS, or routing protocols, can lead to communication errors, packet loss, or network instability.
- Network Services: Faulty network services, such as DHCP servers, DNS servers, or directory services, may experience service disruptions, authentication failures, or data corruption.
- Applications: Software bugs or compatibility issues in network applications, such as email servers, web servers, or database servers, can result in application crashes, data loss, or service unavailability.
- Firmware: Outdated or corrupted firmware in network devices, such as routers, switches, or WAPs, can cause device malfunctions, security vulnerabilities, or compatibility issues with other network components.
- Detecting faulty hardware or software components in an existing network involves a systematic approach to identifying and diagnosing issues that may impact the network's performance, reliability, or security.
- To detect faulty hardware or software components in an existing network:

Hardware Diagnostics:

Use hardware diagnostic tools provided by network device manufacturers to test the functionality of network hardware components, including switches, routers, access points, and network adapters.

Conduct hardware tests to check for hardware failures, such as faulty ports, overheating, power supply issues, or hardware component failures.

2. Software Diagnostics:

Review software configuration settings, firmware versions, and software patches installed on network devices and servers to ensure they are up-to-date and free from known vulnerabilities or software bugs.

Perform software diagnostics on servers, operating systems, and network applications to identify software-related errors, crashes, or performance issues that may impact network operations.

Testing procedure of Network functionality

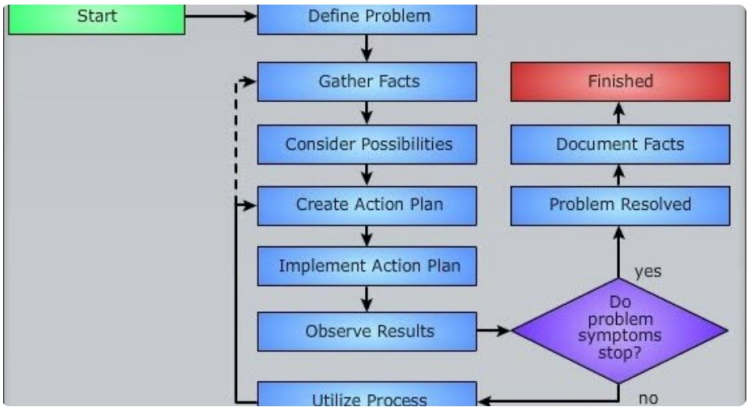
Conduct functional testing to verify that network devices and services perform as expected and meet specified requirements.

Test network connectivity, including wired and wireless connections, to ensure that devices can communicate with each other and access network resources.

Test routing and switching functionality to verify proper packet forwarding, VLAN configuration, and routing table updates.

Test network services, such as DHCP, DNS, FTP, HTTP, SMTP, and SNMP, to ensure that they are accessible, responsive, and functioning correctly.

Test security features, including firewalls, VPNs, access control lists (ACLs), and encryption protocols, to verify that network security policies are enforced and effective.



Maintenance and troubleshooting documents:

Maintenance and troubleshooting documents are essential resources used by IT professionals to manage, maintain, and troubleshoot network infrastructure, systems, and applications effectively. These documents provide comprehensive guidelines, procedures, and reference materials to ensure the smooth operation of IT environments and address technical issues promptly. Maintenance and troubleshooting documents may include:

Maintenance Documentation:

- Configuration Records: Document detailed configurations of network devices, servers, and applications, including settings, parameters, and policies.
- Inventory Management: Maintain an inventory of hardware assets, software licenses, firmware versions, and maintenance contracts to track assets and ensure compliance.
- Scheduled Maintenance Procedures: Document routine maintenance tasks, such as software updates, patch management, backup and recovery procedures, and hardware inspections.

Troubleshooting Documentation:

- Troubleshooting Workflows: Define step-by-step workflows and decision trees for diagnosing and resolving common network issues, system errors, or application failures.
- Knowledge Base Articles: Create a repository of troubleshooting articles, FAQs, best practices, and solutions for known issues encountered in the IT environment.
- Diagnostic Tools and Utilities: Document procedures for using diagnostic tools, network monitoring software, packet analyzers, and system utilities to diagnose network and system problems.
- User Support Documentation: Provide user-friendly guides, tutorials, or self-help resources for end-users to troubleshoot common issues, reset passwords, or resolve software-related problems independently.
- Disaster Recovery Plans: Develop disaster recovery plans outlining procedures for data backup, replication, failover, and recovery in the event of hardware failures, natural disasters, or cyber-attacks.

Self-Check Sheet 4: Troubleshooting in existing network

1. What is the purpose of reviewing network design, support, and maintenance documents?
2. Why is it important to consult appropriate persons when identifying network problems?
3. How do you detect faulty hardware or software components in a network?
4. What steps are involved in performing the solution of a network problem?
5. What is the purpose of testing network functionality?
6. Why is it important to update maintenance and troubleshooting documents regularly?
7. How should tools and equipment be stored according to workplace procedures?
8. What are the benefits of consulting appropriate persons when identifying network problems?
9. What role does testing play in maintaining network functionality?
10. Why is it important to update maintenance and troubleshooting documents regularly?

Answer Key 4: Troubleshooting in existing network

1. What is the purpose of reviewing network design, support, and maintenance documents?
   Answer: Reviewing these documents ensures that network infrastructure is well-designed, properly supported, and effectively maintained to meet business needs.

2. Why is it important to consult appropriate persons when identifying network problems?
   Answer: Consulting experts ensures accurate problem identification and effective troubleshooting by leveraging specialized knowledge and experience.

3. How do you detect faulty hardware or software components in a network?
   Answer: Faulty components can be detected through systematic testing, analysis of error logs, diagnostic tools, and physical inspection of hardware.

4. What steps are involved in performing the solution of a network problem?
   Answer: Solution involves diagnosing the root cause, implementing corrective actions, testing the solution, and documenting the resolution process.

5. What is the purpose of testing network functionality?
   Answer: Testing ensures that the network operates as intended, meets performance requirements, and remains reliable and secure.

6. Why is it important to update maintenance and troubleshooting documents regularly?
   Answer: Regular updates ensure that documentation reflects the current state of the network, incorporates lessons learned, and remains relevant for troubleshooting and maintenance tasks.

7. How should tools and equipment be stored according to workplace procedures?
   Answer: Tools and equipment should be stored in designated areas, properly labeled, secured when not in use, and maintained in good condition.

8. What are the benefits of consulting appropriate persons when identifying network problems?
   Answer: Consulting appropriate persons ensures accurate problem diagnosis, efficient troubleshooting, and timely resolution of network issues.

9. What role does testing play in maintaining network functionality?
   Answer: Testing verifies that network components operate correctly, identify potential issues, and ensure optimal performance and reliability.

10. Why is it important to update maintenance and troubleshooting documents regularly?
    Answer: Regular updates ensure that documentation reflects the current state of the network, incorporates lessons learned, and remains relevant for troubleshooting and maintenance tasks.

Task Sheet 4.1:

Task Sheet 4.1: Troubleshooting in existing network
Performance Objective: By the end of this task, the trainee should be able to review documentation, identify and resolve issues, test network functionality, update maintenance documents, and store tools and equipment properly.
1. Consult with relevant stakeholders or experts when identifying network issues.
2. Seek assistance from network administrators, system engineers, or technical support personnel to diagnose complex problems.
3. Identify and diagnose faulty hardware or software components in the network.
4. Use diagnostic tools, error logs, and physical inspections to detect hardware failures, software errors, or configuration issues.
5. Take corrective actions such as replacing faulty hardware, updating software, or reconfiguring network settings to address issues.
6. Test the functionality and performance of the network after implementing solutions.
7. Update maintenance and troubleshooting documents based on lessons learned and changes in network configuration.
8. Document solutions, test results, and any modifications made to the network infrastructure during troubleshooting and maintenance activities.
9. Store network tools and equipment according to established workplace procedures.
10. Follow guidelines for organizing, labeling, and securing tools and equipment in designated storage areas.

Specification Sheet 4.1:

A. Tools and Material required:

- Notebook
- Handbook

B. Equipment:

- Laptop/Computer

Learning Outcome 5: Create documentation for maintenance

Assessment Criteria:

1. All the settings are documented
2. Configuration and PC network IP address are documented for future maintenance purpose

Content:

1. Documentation Procedure
2. Configuration and PC network IP address documentation

Resources Required/ Conditions:

The trainees must be provided with the following:

- Handouts or reference materials/books/ CBLMs on the above stated contents
- PCs/printers or laptop/printer with internet access
- Digital projector and Screen
- Bond paper
- Ball pens/pencils and other office supplies and materials
- Relevant learning materials
- Workplace or simulated environment

Methodologies

- Lecture/discussion
- Demonstration/application
- Presentation
- Blended delivery methods

Assessment Methods

- Written test
- Demonstration
- Observation with checklist
- Oral questioning
- Portfolio

Learning Experience 5: Create documentation for maintenance

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 Steps	Resources specific instructions
1. Student will ask the instructor about creating documentation for maintenance	1. Instructor will provide the learning materials "**Performing Basic Networking"**
2. Read the Information sheet/s	2. Information Sheet No: 5 creating documentation for maintenance
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 5 creating documentation for maintenance Answer key No. 5 creating documentation for maintenance
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No: 5 creating documentation for maintenance Specification Sheet: 5 creating documentation for maintenance

Information Sheet 4: Creating documentation for maintenance

Learning Objectives:

After completion of this information sheet, the learners will be able to:

1. Document All the settings
2. Document Configuration and PC network IP address for future maintenance purpose

Documentation procedures

Documentation procedures are systematic guidelines outlining how information should be recorded, organized, and managed within an organization. These procedures ensure consistency, accuracy, and accessibility of documentation across different departments and projects. Here's an outline of the documentation procedure:

Define Documentation Standards:

- Establish standards for document formatting, structure, and content to ensure consistency and clarity.
- Define document templates, styles, and guidelines for creating and organizing documentation.

Identify Document Types:

- Determine the types of documents needed for various processes, projects, or activities within the organization.
- Identify document categories such as policies, procedures, guidelines, specifications, reports, and forms.

Document Creation:

- Assign responsibility for creating and maintaining documents to designated personnel or teams.
- Use approved templates and formats to create documents, ensuring adherence to established standards.
- Include relevant information such as titles, dates, authorship, version numbers, and revision history in documents.

Review and Approval:

- Establish procedures for reviewing and approving documents before finalization and distribution.
- Implement a review process involving subject matter experts, stakeholders, or supervisors to ensure accuracy, completeness, and compliance with requirements.
- Obtain approvals from authorized personnel or stakeholders before documents are considered final.

Distribution and Access Control:

- Define procedures for distributing documents to intended recipients, whether electronically or in print.
- Implement access controls to restrict document access based on user roles, permissions, or confidentiality requirements.
- Maintain a centralized repository or document management system to store and manage documents securely.

Document Revision and Version Control:

- Implement a version control system to track document revisions, updates, and changes over time.
- Assign unique version numbers or revision codes to each document version to facilitate tracking and identification.
- Document changes made in each revision, including reasons for changes and the individuals involved.

Document Retrieval and Retrieval:

- Ensure that documents are easily retrievable by authorized users when needed for reference, review, or use.
- Organize documents logically within the document repository or management system, using folder structures, tags, or metadata.
- Implement search capabilities to enable users to locate specific documents efficiently based on keywords, titles, or categories.
- Training and Documentation Awareness:
- Provide training and guidance to personnel on documentation procedures, standards, and tools.
- Promote awareness of documentation requirements and the importance of accurate and timely documentation across the organization.
- Offer support and resources to help users create, manage, and access documents effectively.

Configuration and PC network IP address documentation

Documentation of configuration and PC network IP addresses is crucial for managing and maintaining a network infrastructure effectively. Here's an explanation of each:

Configuration Documentation:

Configuration documentation refers to recording detailed information about the settings, parameters, and configurations of network devices, servers, and applications. This documentation ensures that IT staff have a clear understanding of how the network is configured and how different components interact with each other. Here are key aspects of configuration documentation:

- **Network Devices:** Document configurations for routers, switches, firewalls, access points, and other network devices. Include details such as device models, firmware versions, interface configurations, VLAN settings, routing protocols, and security policies.
- **Servers:** Document configurations for servers, including operating system settings, hardware specifications, network settings, services, and applications installed. Record information such as server roles, domain membership, IP addresses, DNS settings, and backup configurations.
- **Network Services:** Document configurations for network services such as DHCP, DNS, Active Directory, email servers, web servers, and database servers. Include information about service settings, protocols, port numbers, access controls, and authentication mechanisms.
- **Security Settings:** Record security configurations for firewalls, VPNs, intrusion detection/prevention systems, and antivirus software. Document firewall rules, VPN configurations, security policies, encryption algorithms, and authentication methods.
- **Change Management:** Maintain records of changes made to network configurations, including details such as change requests, approvals, implementation dates, and impact assessments. This helps track changes and ensures accountability.

PC Network IP Address Documentation:

PC network IP address documentation involves recording and managing IP addresses assigned to individual computers, servers, and network devices on the network. This documentation helps in managing IP address allocation, troubleshooting network connectivity issues, and ensuring proper IP address assignment. Here's how to document PC network IP addresses:

- **IP Address Assignment:** Record IP addresses assigned to PCs, servers, printers, and other network devices. Include both IPv4 and IPv6 addresses, subnet masks, and default gateway addresses.
- **Static IP Addresses:** Document static IP addresses assigned manually to devices that require fixed IP addresses for specific purposes, such as servers, network equipment, and printers.
- **Dynamic IP Addresses:** Maintain records of IP addresses assigned dynamically through DHCP (Dynamic Host Configuration Protocol). Include lease durations, DHCP server configurations, and DHCP scope details.
- **Hostname and MAC Address:** Associate each IP address with the corresponding hostname (computer name) and MAC (Media Access Control) address of the device. This helps in identifying devices on the network and troubleshooting connectivity issues.
- **Subnet and VLAN Information:** Record subnet information and VLAN assignments for IP addresses to organize devices into logical network segments. Document VLAN IDs, subnet masks, and VLAN configurations.
- **DNS and DHCP Integration:** Ensure consistency between IP address documentation and DNS (Domain Name System) records. Update DNS records with IP address changes and ensure that DHCP server configurations align with IP address assignments.
- **IP Address Management (IPAM) Tools:** Consider using IPAM software or tools to automate IP address management tasks, track IP address usage, detect conflicts, and generate reports. These tools help streamline IP address documentation and management processes.

Self-Check Sheet 5: Creating documentation for maintenance

1. Why is documentation important in network management?

2. What is configuration documentation?

3. What is the purpose of PC network IP address documentation?

4. How does documentation procedure help in maintaining network consistency?

5. What information should be included in PC network IP address documentation?

Answer Key 5: Creating documentation for maintenance

1. Why is documentation important in network management?
   Answer: Documentation ensures that network configurations, IP addresses, and procedures are recorded accurately for reference, troubleshooting, and maintenance purposes.

2. What is configuration documentation?
   Answer: Configuration documentation records detailed information about the settings, parameters, and configurations of network devices, servers, and applications.

3. What is the purpose of PC network IP address documentation?
   Answer: PC network IP address documentation tracks and manages the assignment of IP addresses to individual computers, servers, and network devices on the network.

4. How does documentation procedure help in maintaining network consistency?
   Answer: Documentation procedures establish standards for creating, organizing, and managing network documentation, ensuring consistency, accuracy, and accessibility across the organization.

5. What information should be included in PC network IP address documentation?
   Answer: PC network IP address documentation should include details such as static and dynamic IP addresses, subnet masks, default gateway addresses, hostnames, MAC addresses, and VLAN assignments.

Review of Competency

Below is yourself assessment rating for module **"Perform Basic Networking"**

SL no	Assessment of performance Criteria	Yes	No
1.	Network is defined		
2.	Types of networks is interpreted		
3.	IP properties is interpreted		
4.	Network connectivity tools identified		
5.	Transmission media determined.		
6.	Organizational requirements are collected and documented to setup an existing network.		
7.	Network layout is collected		
8.	Existing network topology and network protocol is identified and documented		
9.	Network design plan is interpreted.		
10.	IP Addressing scheme is interpreted		
11.	Required transmission media, tools and equipment are selected and collected.		
12.	Cabling is performed as per layout		
13.	Connections is established as per layout design.		
14.	Device is connected with the existing network with appropriate transmission media infrastructure		
15.	IP properties is assigned and connectivity is tested as per work plan.		
16.	Network design, support and maintenance documents are reviewed.		
17.	Appropriate person is consulted for identifying problems if required.		
18.	Faulty hardware or software component are detected.		
19.	Solution of Problem is performed.		
20.	Network functionality is tested.		
21.	Maintenance and troubleshooting documents are updated.		
22.	Tools and equipment are stored as per workplace procedures		
23.	All the settings are documented		
24.	Configuration and PC network IP address are documented for future maintenance purpose		

I now feel ready to undertake my formal competency assessment.

Signed:

Date:

Development of CBLM

The Competency based Learning Material (CBLM) of '**Performing Basic Networking' (Occupation: IT Support Service, Level-3)** 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 June, 2024 under the contract number of package SD-9B dated 15th January 2024.

SL No.	Name & Address	Designation	Contact Number
1	Md. Abdul Hye Siddiqui	Writer	01819-725610
2	Engr. Md. Zuwel Parves	Editor	01737-278906
3	Engr. Md. Zuwel Parves	Co-Ordinator	01737-278906
4	Md. Saif Uddin	Reviewer	01723-004419

REFERENCE:

1. https://www.wikihow.com/Create-an-Ethernet-Cable