

Learning Outcome 1: Establish Network Media Connectivity



Indicative contents

1.1 Identification of Network Requirements.

1.2 Termination of Network cables

1.3 Connection of Network Media



Key readings 1.1.1.: Description of network concepts and technologies

1. Identification of network requirements

1.1. Description of network concepts and technologies

- **Definitions of network:** a network consists of two or more computer that are linked in order to share resources (**such as printers and CDs**), exchange files, or allow electronic communications. The computer on a network may linked through cables, telephone lines, radio waves, satellites, or infrared light beams.
- **Network classifications/types:**
Classifying network by components roles: Networks can be classified into different categories based on various criteria, including their size, scope, purpose, and architecture. Some common network classifications:
 - ❖ **Based on Size:**
 - **Personal Area Network (PAN):** A small network typically within a range of a few meters, used for connecting personal devices like smartphones, laptops, and tablets.
 - **Local Area Network (LAN):** Covers a limited geographic area, such as a home, office, or campus. LANs connect devices like computers, printers, and servers.
 - **Metropolitan Area Network (MAN):** Larger than a LAN but smaller than a WAN, covering a city or a large campus. MANs are used by organizations with multiple locations in a city.
 - **Wide Area Network (WAN):** Spans a large geographic area, often connecting LANs or MANs across different cities, regions, or countries. The internet is the most extensive WAN.
 - **Global Area Network (GAN):** A network that covers a global or international scale, often using satellite links and undersea cables. The internet can be considered a GAN.
 - ❖ **Based on Purpose:**
 - **Public Network:** Open to the public, such as the internet, where anyone can access and use its resources.
 - **Private Network:** Restricted to a specific organization, group, or individuals. Examples include corporate intranets and private cloud networks.
 - **Hybrid Network:** Combines elements of both public and private networks, often for security and cost considerations. Hybrid clouds, which use a mix of public and private cloud services, are an example.

- **Peer-to-Peer (P2P) Network:** Devices in this type of network communicate directly with each other without a central server. Common in file sharing applications.

❖ **Based on Topology:**

- **Star Topology:** Devices connect to a central hub or switch.
- **Bus Topology:** Devices share a single communication line.
- **Ring Topology:** Devices form a closed-loop or ring.
- **Mesh Topology:** Devices connect to multiple other devices, creating redundancy.
- **Hybrid Topology:** A combination of two or more different topologies.

• **Based on Ownership and Control:**

- **Public Network:** Owned and operated by a public entity or organization and accessible to anyone.
- **Private Network:** Owned and operated by a specific organization, restricting access to authorized users.
- **Community Network:** Shared by a specific community or group, often for a common purpose, such as a housing complex or university campus network.
- **Cooperative Network:** Jointly owned and operated by multiple organizations or entities for mutual benefit.

❖ **Based on Network Services and Applications:**

- **Data Network:** Primarily used for data transmission and communication, such as the internet and corporate data networks.
- **Voice Network:** Designed for voice communication, such as traditional telephone networks (PSTN) and Voice over IP (VoIP) networks.
- **Video Network:** Focused on transmitting video content, including cable TV networks and streaming platforms.
- **IoT Network:** Supports the connectivity of Internet of Things (IoT) devices, sensors, and machines.

❖ **Based on Architecture:**

- **Client-Server Network:** Devices are categorized as clients (requesters) and servers (providers of services or resources). Common in corporate networks and the internet.
- **Peer-to-Peer (P2P) Network:** Devices communicate directly with each other without a central server. Often used in file-sharing applications and some blockchain networks.

• **Network benefits**

Networks offer numerous benefits across various domains and industries due to their ability to connect devices, systems, and people. Here are some key advantages of networks:

- **Communication:** Networks enable efficient and effective communication, allowing people to share information, collaborate, and exchange messages in real time. This is crucial for business operations, remote work, and social interactions.
- **Data Sharing:** Networks facilitate the sharing of data and resources. Users can access shared files, databases, and applications, leading to improved productivity and collaboration.
- **Resource Sharing:** Devices and resources such as printers, scanners, and storage devices can be shared across a network, reducing costs and optimizing resource utilization.
- **Centralized Data Management:** Networks allow for central storage and management of data, making it easier to back up, secure, and access data when needed.
- **Remote Access:** With network connectivity, users can access data and applications from remote locations, enabling flexible work arrangements and remote troubleshooting and support.
- **Cost Efficiency:** Sharing resources and centralized management can lead to cost savings in terms of hardware, software, and maintenance.
- **Global Connectivity:** The internet, a global network, offers access to information, services, and markets worldwide, fostering globalization and international trade.
- **Security:** While networks can pose security challenges, they also enable the implementation of security measures, such as firewalls, intrusion detection systems, and encryption, to protect data and resources.
- **Data Backup and Disaster Recovery:** Networks make it easier to back up data and implement disaster recovery plans, reducing the risk of data loss and downtime.
- **Resource Optimization:** Networks can optimize resource usage through load balancing and efficient routing, ensuring that resources are used effectively.
- **Monitoring and Management:** Network management tools allow administrators to monitor network performance, troubleshoot issues, and make adjustments to optimize network operation.
- **Innovation and Development:** Networks are the foundation for many technological advancements, such as the Internet of Things (IoT), cloud computing, and edge computing, driving innovation in various industries.
- **Accessibility and Inclusivity:** Networks can enhance accessibility by providing online education, telehealth services, and access to information for people with disabilities or those in remote areas.
- **Environmental Benefits:** By enabling remote work and virtual meetings,

networks can reduce the need for commuting, leading to lower carbon emissions and environmental benefits.

- **Entertainment and Content Delivery:** Networks enable the streaming of movies, music, and online gaming, providing entertainment options and revenue streams for content creators.
- **Research and Collaboration:** Networks facilitate collaborative research, connecting scientists, researchers, and institutions globally, leading to advancements in various fields.
- **E-commerce and Online Shopping:** Networks have transformed the retail industry, making it possible for consumers to shop online, compare prices, and access a wide range of products and services.
- **Community and Social Interaction:** Social networks and online communities bring people together, fostering social interaction, information sharing, and support networks.

- **Advantages and Disadvantages of network**

Networks, whether they are computer networks, social networks, or any other type of interconnected systems, come with various advantages and disadvantages. Here are some of the key advantages and disadvantages of networks:

Advantages of Networks:

- **Communication:** Networks enable efficient communication between individuals, devices, or systems, regardless of their physical locations. This facilitates the exchange of information, collaboration, and coordination.
- **Resource Sharing:** Networks allow for the sharing of resources such as files, printers, and software applications. This can lead to cost savings and improved efficiency in organizations.
- **Centralized Data Management:** In computer networks, data can be stored centrally, making it easier to manage and backup. This centralization can enhance data security and accessibility.
- **Remote Access:** Networks enable remote access to resources and data, allowing individuals to work from different locations and enhancing flexibility.
- **Redundancy and Reliability:** Some networks are designed with redundancy, which means that if one component fails, there are backup options to ensure system reliability.
- **Resource Optimization:** Networks can optimize resource usage by load balancing and efficient routing, ensuring that resources are used effectively.
- **Global Connectivity:** The internet is a global network that provides access to information and services worldwide, facilitating international communication

and commerce.

Disadvantages of Networks:

- **Security Risks:** Networks can be vulnerable to security threats such as hacking, viruses and malware. Protecting networked systems is an ongoing challenge.
- **Complexity:** As networks grow in size and complexity, they become more challenging to manage and troubleshoot. Complex networks may require specialized expertise.
- **Maintenance Costs:** Networks require ongoing maintenance, including hardware upgrades, software updates, and security measures. These costs can add up over time.
- **Privacy Concerns:** Networks can potentially compromise individual privacy, as personal data may be accessible or vulnerable to surveillance.
- **Downtime:** Network failures or outages can disrupt communication and business operations. Downtime can result in financial losses and customer dissatisfaction.
- **Bandwidth Limitations:** In data networks, bandwidth limitations can lead to slow data transfer speeds and congestion, affecting performance.
- **Technical Issues:** Networks can experience technical problems, including connectivity issues, hardware failures, and software glitches, which may require troubleshooting and downtime.

It's important to note that the advantages and disadvantages of networks can vary depending on the specific type of network (e.g., computer networks, social networks, telecommunications networks) and their intended use.

- **Application of network**

Networks have a wide range of applications across various domains and industries. Their primary function is to facilitate the exchange of information and resources between different entities or nodes. Here are some common applications of networks:

- **Computer Networks:**
- **Internet:** The global network that connects millions of computers and devices worldwide, enabling communication, information sharing, and online services.
- **Local Area Networks (LANs):** Networks that connect devices within a limited geographic area, such as a home, office, or campus, to share resources like printers and files.
- **Wide Area Networks (WANs):** Networks that span larger geographical areas, often connecting multiple LANs and providing long-distance communication

capabilities.

- **Intranets and Extranets:** Internal corporate networks (intranets) and extended networks (extranets) for secure communication and collaboration within and between organizations.

Telecommunications:

- **Telephone Networks:** Traditional voice communication networks, including landlines and cellular networks.
- **Voice over IP (VoIP):** Networks that transmit voice and multimedia content over the internet, offering cost-effective communication.
- **Fiber Optic Networks:** High-speed data transmission networks using optical fibers, commonly used in long-distance and high-bandwidth applications.

Data Centers:

- **Data Center Networks:** Networks within data centers that connect servers, storage, and networking equipment to support cloud computing, web services, and big data applications.

Transportation:

- **Traffic Control Systems:** Networks used in traffic lights, sensors, and cameras to manage traffic flow, improve safety, and reduce congestion.
- **Fleet Management:** Networks for tracking and managing vehicles in logistics and transportation companies.

Healthcare:

- **Health Information Exchange (HIE):** Networks that enable the secure sharing of patient health records and medical data among healthcare providers for improved patient care.
- **Telemedicine:** Networks that support remote medical consultations and diagnosis, bringing healthcare services to remote or underserved areas.

Financial Services:

- **Electronic Banking:** Networks that enable online banking, ATM transactions, and electronic fund transfers.
- **Stock Exchanges:** Networks that facilitate trading and real-time financial data transmission for stock markets worldwide.

Manufacturing and Industrial Automation:

- **Industrial Control Systems (ICS):** Networks used in factories and industrial environments to control machinery and automation processes.
- **Internet of Things (IoT):** Networks connecting various sensors and devices to collect and transmit data for monitoring and control.

Entertainment and Media:

- **Streaming Services:** Networks that deliver multimedia content, such as video and music streaming, to users over the internet.
- **Online Gaming:** Networks that enable multiplayer online gaming experiences,

including cloud gaming services.

Education:

- **E-Learning:** Networks that support online education platforms, virtual classrooms, and remote learning opportunities.

Social Networks:

- **Social media:** Online platforms connecting individuals and organizations for social interaction, content sharing, and communication.

Agriculture:

- **Precision Agriculture:** Networks and IoT devices used in farming to monitor crops, manage resources, and improve crop yields.

Smart Cities:

- **Public Wi-Fi:** Networks that provide internet access in public spaces, promoting connectivity and digital services in urban areas.

- **Network technologies**

Network technologies encompass a wide range of tools, protocols, hardware, and software used to create and manage computer networks. These technologies enable the efficient transfer of data, communication between devices, and the sharing of resources. Here are some key network technologies:

- **Ethernet:** Ethernet is a widely used wired networking technology that defines how data packets should be placed on a network cable. It operates over various media types, including copper and fiber-optic cables, and supports different data speeds (e.g., 10/100/1000/10000 Mbps).
- **Wi-Fi (Wireless LAN):** Wi-Fi technology enables wireless local area networks (WLANs). It allows devices to connect to a network without physical cables, making it especially useful for mobile devices like smartphones and laptops. Various Wi-Fi standards (e.g., 802.11n, 802.11ac, 802.11ax) offer different data rates and features.
- **Bluetooth:** Bluetooth is a short-range wireless technology primarily used for connecting devices like smartphones, headphones, and IoT devices. It's commonly used for file sharing, audio streaming, and peripheral device connections.
- **Cellular Networks:** Cellular technology provides wireless connectivity for mobile phones and other devices. It includes generations like 2G, 3G, 4G, and 5G, with each generation offering improved data speeds and capabilities.
- **IP (Internet Protocol):** IP is a fundamental network protocol that governs how data packets should be addressed and routed across the internet. IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) are the most commonly used versions.
- **TCP/IP (Transmission Control Protocol/Internet Protocol):** TCP/IP is a suite of

protocols used for communication over the internet and local networks. It includes protocols like HTTP, FTP, SMTP, and DNS, which enable various network services.

- **DNS (Domain Name System):** DNS is a technology that translates human-readable domain names (e.g., `www.example.com`) into IP addresses (e.g., `192.168.1.1`). It's essential for browsing the internet.
- **Firewalls:** Firewalls are security devices or software that protect networks by monitoring and controlling incoming and outgoing network traffic. They can block malicious traffic and unauthorized access.
- **Routers:** Routers are network devices that connect different networks and determine the best path for data packets to travel between them. They play a critical role in directing traffic on the internet.
- **Switches:** Switches are devices that connect multiple devices within a local network and efficiently forward data packets only to their intended recipients. They operate at Layer 2 (Data Link Layer) of the OSI model.
- **Load Balancers:** Load balancers distribute network traffic across multiple servers to ensure even utilization and high availability. They are often used in web applications and server farms.
- **VPN (Virtual Private Network):** VPN technology creates a secure and encrypted connection over a public network, such as the internet. It's commonly used for remote access, privacy, and secure communication.
- **VoIP (Voice over IP):** VoIP technology allows voice calls to be transmitted over IP networks. It's the basis for services like Skype, Zoom, and business phone systems.
- **IoT (Internet of Things) Protocols:** IoT networks use various protocols such as MQTT, CoAP, and Zigbee to enable communication between IoT devices and platforms.

These are just a few examples of network technologies, and the field is constantly evolving as new innovations emerge. Network technologies are crucial for modern communication, data sharing, and the functioning of the internet.

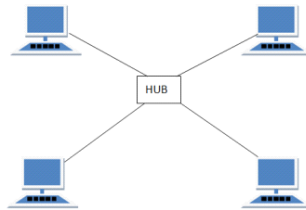
- **Network topology types**

Network topology refers to the physical or logical layout of devices and connections in a computer network. Different network topologies are used depending on the specific requirements of the network, such as scalability, fault tolerance, and cost. Here are some common network topology types:

Star Topology:

- **Description:** In a star topology, all devices (computers, printers, etc.) are connected to a central hub or switch.

- **Advantages:** Easy to install and manage, fault isolation (a problem in one device does not affect others), centralized control.
- **Disadvantages:** If the central hub or switch fails, the entire network can be affected.



Bus Topology:

- **Description:** In a bus topology, all devices are connected to a single central cable (the "bus").
- **Advantages:** Simple and inexpensive to set up, suitable for small networks.
- **Disadvantages:** Susceptible to cable failure, limited scalability, performance degrades as more devices are added.

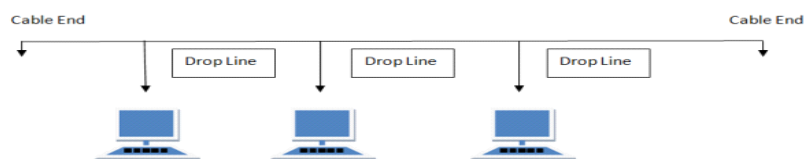


Fig.1: Bus topology

- **Ring Topology:**
- **Description:** In a ring topology, devices are connected in a circular or ring-like fashion, where each device is connected to exactly two other devices.
- **Advantages:** Even data distribution, no collisions, predictable performance.
- **Disadvantages:** A failure in one device or cable segment can disrupt the entire network, typically slower than star or bus topologies.

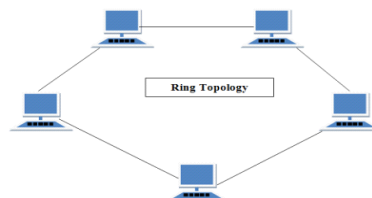


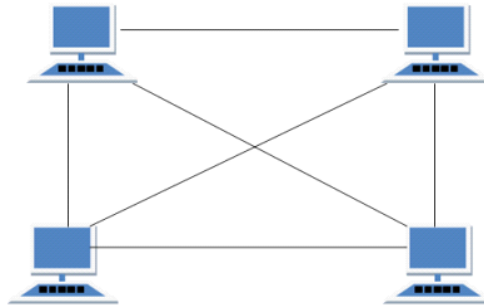
Fig.2: Star topology

Mesh Topology:

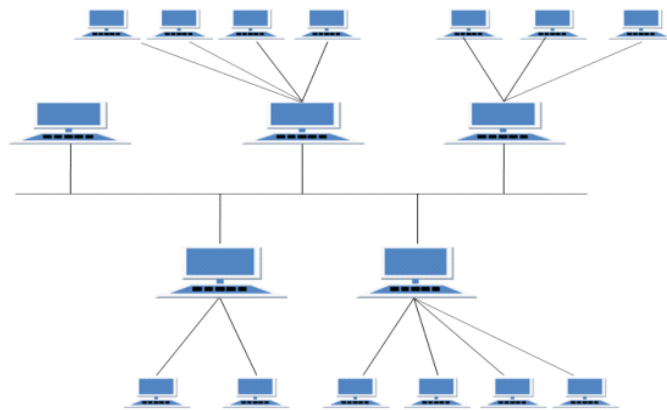
- **Description:** In a mesh topology, every device is connected to every other device. There are two variations: full mesh (all devices connect to all others)

and partial mesh (only some devices connect to all others).

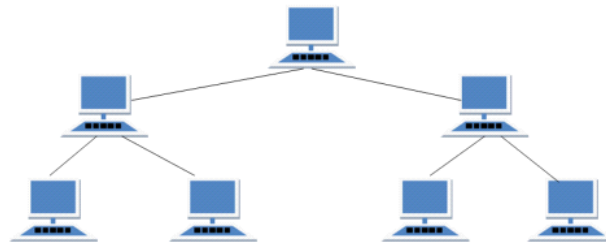
- **Advantages:** High redundancy, fault tolerance, can handle heavy traffic loads.
- **Disadvantages:** Expensive to implement and manage, complex cabling, scalability challenges in full mesh.



- **Hybrid Topology:**
- **Description:** Hybrid topologies are a combination of two or more different topology types. For example, a network might use a combination of star and ring topologies.
- **Advantages:** Can leverage the strengths of multiple topologies, adaptable to specific network requirements.
- **Disadvantages:** Can be complex to design and manage.



- **Tree Topology (Hierarchical Topology):**
- **Description:** Tree topology combines characteristics of star and bus topologies. Multiple star-configured networks are connected to a linear bus backbone.
- **Advantages:** Scalable, combines benefits of star and bus topologies.
- **Disadvantages:** Costly and complex to implement, failure of the backbone can disrupt the entire network.



Each topology has its own strengths and weaknesses, and the right choice can greatly impact a network's performance and reliability.

- **Network components**

Computer networks consist of various components that work together to facilitate communication, data sharing, and resource access among connected devices. These components can be categorized into several broad categories:

End Devices:

- **Computers:** Such as desktops, laptops, servers, and workstations.
- **Mobile Devices:** Such as smartphones, tablets, and wearable devices.
- **Printers:** For document and image printing.
- **IP Phones:** Voice-over-IP (VoIP) phones for voice communication over the network.
- **IoT Devices:** Sensors, cameras, and other Internet of Things (IoT) devices.
- **Networking Hardware:**
- **Router:** A device that connects different networks and directs traffic between them.
- **Switch:** A device that connects devices within a local network and efficiently forwards data packets based on MAC addresses.
- **Hub:** An older networking device that broadcasts data packets to all connected devices.
- **Access Point (AP):** Facilitates wireless connectivity by allowing devices to connect to a wired network wirelessly (Wi-Fi).
- **Firewall:** A security device or software that monitors and controls network traffic, often used to protect against unauthorized access and threats.
- **Modem:** Converts digital data from a network into a format suitable for transmission over specific types of media (e.g., DSL, cable, fiber).
- **Gateway:** Acts as an entry and exit point between different networks, translating data formats and protocols.
- **Network Infrastructure:**
- **Cabling:** Includes Ethernet cables (e.g., CAT6), fiber-optic cables, and coaxial cables for wired connections.

- **Wireless Infrastructure:** Access points, wireless controllers, and antennas for Wi-Fi networks.
- **Network Servers:** Systems responsible for hosting applications, files, and services on the network.
- **Data Centers:** Facilities housing network equipment, servers, and storage devices for centralized data processing and storage.
- **Racks and Cabinets:** Housing units for organizing and securing network equipment.
- **Networking Software and Protocols:**
 - **Operating Systems:** Such as Windows, Linux, and macOS, which include networking features and protocols.
 - **Network Protocols:** TCP/IP, UDP, HTTP, FTP, SNMP, DNS, DHCP, etc., enabling communication and data transfer.
 - **Network Management Software:** Tools for monitoring, configuring, and managing network devices.
 - **Virtualization Software:** Such as VMware and Hyper-V, used for creating virtual network environments and virtual servers.
- **Network Services and Applications:**
 - **Email Services:** Like Microsoft Exchange and SMTP/POP/IMAP servers.
 - **Web Services:** Hosting websites and web applications.
 - **File Sharing Services:** Such as Network Attached Storage (NAS) and cloud-based file sharing platforms.
 - **VoIP Services:** Voice over IP services for telephony and video conferencing.
 - **DNS Servers:** Resolving domain names to IP addresses.
 - **DHCP Servers:** Assigning IP addresses automatically to devices on the network.
- **Security Components:**
 - **Firewalls:** As mentioned earlier, protecting the network from threats.
 - **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** Monitoring and preventing unauthorized access and attacks.
 - **Antivirus and Antimalware Software:** Protecting end devices from malicious software.
 - **Virtual Private Networks (VPNs):** Securing data transmitted over public networks.
 - **Authentication and Access Control Systems:** Managing user access rights and permissions.



Theoretical Activity 1.1.2: Identification of network Materials, Tools and Equipment

Tasks:

- 1: Answer the following questions related to the description tools, materials and equipment.
 - i. Differentiate the term networking tools, equipment and materials used in networking
 - ii. Give examples of tools, equipment and materials as used in networking.
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class
- 4: For more clarification, read the **key readings 1.1.2**
- 5: In addition, ask questions where necessary.



Key readings 1.1.2.: Identification of network Materials, Tools and Equipment

1. Identification of network Materials, Tools and Equipment based on network requirements.

a. Tools

In networking, tools refer to various software and hardware utilities used for the setup, management, troubleshooting, and optimization of network systems. These tools help network administrators and engineers ensure the network operates efficiently and securely.

b. Equipment

In networking, equipment refers to the hardware devices used to establish, manage, and support a network's infrastructure. These devices facilitate connectivity, data transfer, and communication between various network components.

c. Materials

In networking, materials refer to the physical components and resources used to build and maintain the network infrastructure. These materials are essential for establishing connections, ensuring proper organization, and supporting network operations.

1.1. Tools

- **Cutting Tools and Stripping tools**



- **Drilling Tools**



- **Fixing Tool**

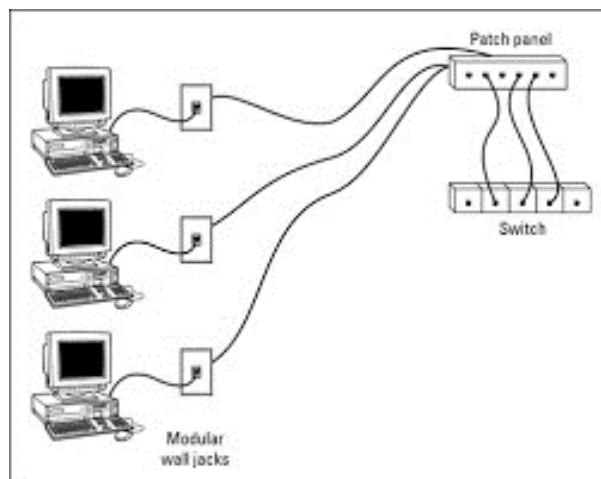


- **Patching Panel**



How to Wire a Patch Panel

- Buy a patch panel. ...
- Design a cable map. ...
- Remove cable jackets from incoming Ethernet cables. ...
- Remove internal plastic jackets (if any) ...
- Untwist and spread the cable wires. ...
- Set your wires to the panel connector. ...
- Complete your connections.



How to Wire a Patch Panel



Internet connections are required in areas with large populations such as business settings and work environments. In such areas where employees are

spread across various offices and floors, the computers are oftentimes connected to central servers. It is so simple to wire the internet to the server, but obviously creates a large build-up of cables around the server area, which must be routed and terminated with absolute care. Because it is barely possible to hardwire each Ethernet cable, the solution is to terminate the incoming cables at a patch panel. This makes it easy to connect the server to the patch panel with the help of short cables, which can as well be moved easily when there is a need to. To achieve this kind of wiring, consider the following guide on how to wire a patch panel:

Buy a patch panel

When buying the patch panel, ensure it has 110 style insulation displacement connectors. Similarly, make sure that there are enough patch connectors that can fit the Ethernet cables. Be sure to conduct a little research so that you can buy the right patch panel.

Design a cable map

This will be the only guide indicating to which panel connector a particular incoming cable is connected. Remember, there could be a need for system upgrades changes in future, so prepare the right map and label the patch panels accurately for this as well as problem diagnosis.

Remove cable jackets from incoming Ethernet cables

Cable jackets must be removed from the incoming Ethernet cables, and this is best done with the help of wire strippers. Cut the jacket approximately 1.5 inches from the cable, remove and discard it. Wire strippers are also available in hardware and electrical stores.

Remove internal plastic jackets (if any)

Sometimes you will be handling Cat6 type incoming Ethernet cables. These often come with an internal plastic jacket, which too should be removed. Use wire cutters in this operation and exercise absolute care. If you are using Cat5e incoming cables, however, you will not be required to undertake this step.

Untwist and spread the cable wires

Inside the Ethernet cables, you will find four pairs of twisted wires. Unwind these wires, but be careful not to mix them up. Four of the wires have solid colors while the rest have a strip of white alongside the solid color.

Set your wires to the panel connector

Each of the wires should then be set to the patch panel. The connector pins are fitted with labels containing color codes, which should guide you in selecting the

type of wire that goes to a particular connector.

Complete your connections

Using a patch panel punch down tool, press each of the wires down firmly. This ensures that the wire is held in place by the insulation connector teeth. If this tool has a cutting edge, place it over the cut end of your Ethernet cables to cut off any extra wire while pressing. If it lacks the cutting edge, on the other hand, use your wire cutter to remove the excess wires that are spread over the edges of your connector.

How to make Ethernet cable

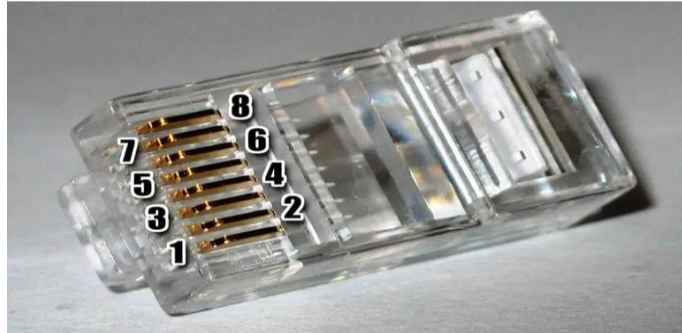
RJ45 cable is used for connect the ALL HMI and engineer station through a switch to communicated each other. It is used to download the any modification and which is made in graphics in engineering station. RJ45 cable also used for communicate the printer with computer

Required tool and materials:

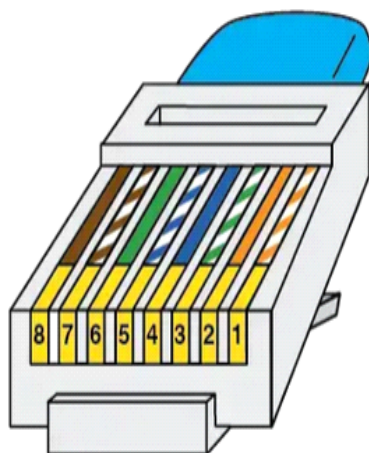
- Ethernet Cable – Category 5e or CAT5e or CAT6
- RJ-45 Crimping tool
- RJ45 Crimp able Connectors



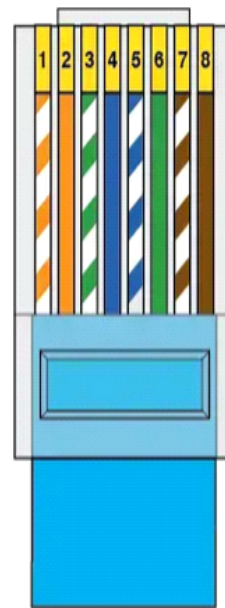
Introduction: There are four pairs of wires in an Ethernet cable, and an Ethernet connector (8P8C) has eight pin slots. Each pin is identified by a number, starting from left to right, with the clip facing away from you.



RJ45 PINOUT T-568B



- 1 | White/Orange
- 2 | Orange
- 3 | White/Green
- 4 | Blue
- 5 | White/Blue
- 6 | Green
- 7 | White/Brown
- 8 | Brown



There is two kinds of Ethernet cable is used for communication.

- Straight Through
- Cross over cable

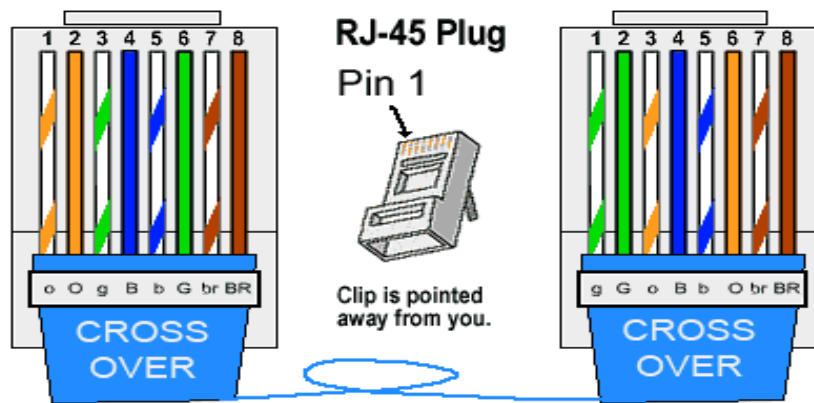
Straight Through cable:

STRAIGHT THROUGH Ethernet cables are the standard cable used for almost all purposes and are often called “patch cables”. It is highly recommended you duplicate the color order as shown on the left. Note how the green pair is not side-by-side as are all the other pairs. This configuration allows for longer wire runs.

Important Instruction: Always remember that both end connector clip facing away from you when check the color.

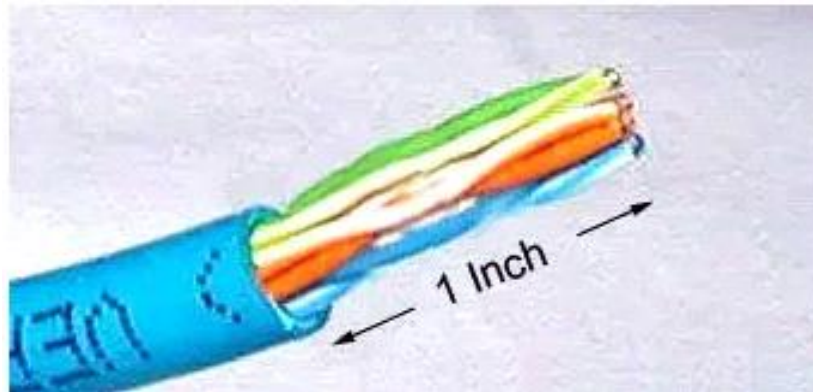
CROSSOVER CABLES –

The purpose of a Crossover Ethernet cable is to directly connect one computer to another computer (or device) without going through a router, switch or hub.

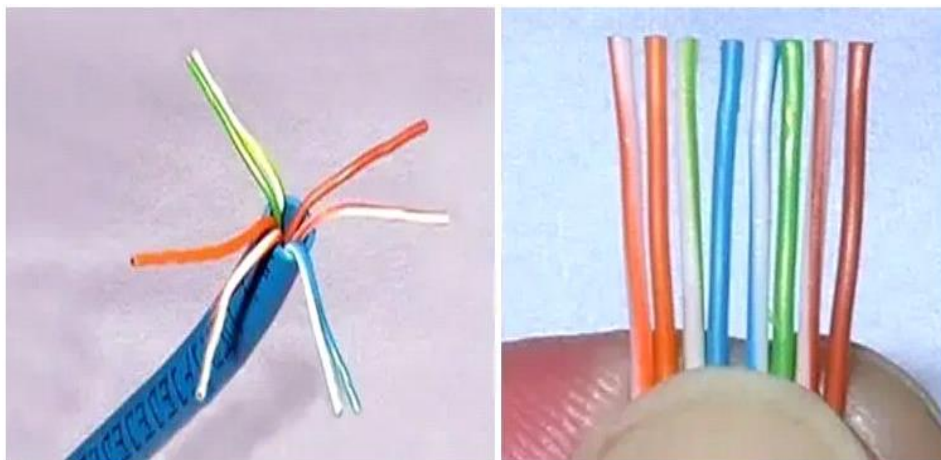


Procedure to make Ethernet cable :

Step 1: Cut into the plastic sheath about **1 inch** (2.5 cm) from the end of the cut cable. Do not cut deep which may cause damage the insulation of core.

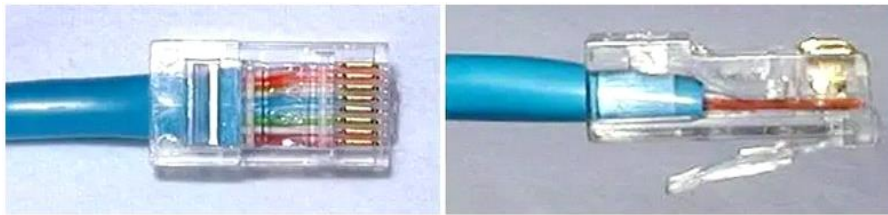


Step 2: Unwind and pair the similar colors. Pinch the wires between your fingers and straighten them out in a sequence of color as u want to make cable (Straight cable or cross over cable). The color order is important to get correct

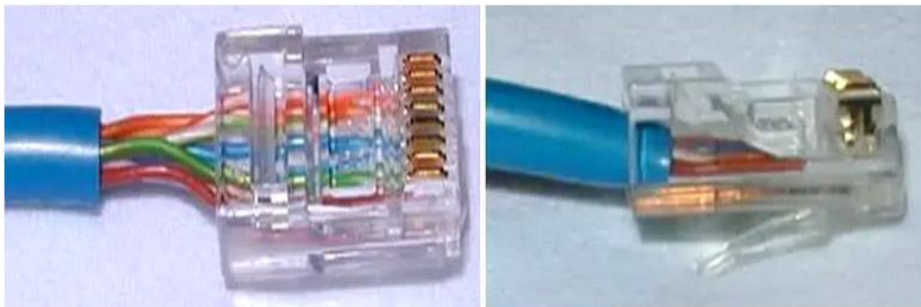


Step 3: A straight cut across the 8 wires to shorten them to **1/2 Inch** (1.3 cm) from the cut sleeve to the end of the wires by crimping tool. Carefully push all 8 unstrapped colored wires into the connector. Plastic sleeve should be inserted

proper in connector.



Wrong way: The plastic sleeve is not inside the connector where it can be locked into place. The wires are too long. The wires should extend only 1/2 inch from the blue cut sleeve. The wires do not go all the way to the end of the connector. The wires are too short.



Crimping the cable: Carefully place the connector into the Ethernet Crimper and cinch down on the handles tightly. The copper splicing tabs on the connector will pierce into each of the eight wires. There is also a locking tab that holds the plastic sleeve in place for a tight compression fit. When you remove the cable from the crimper, that end is ready to use.

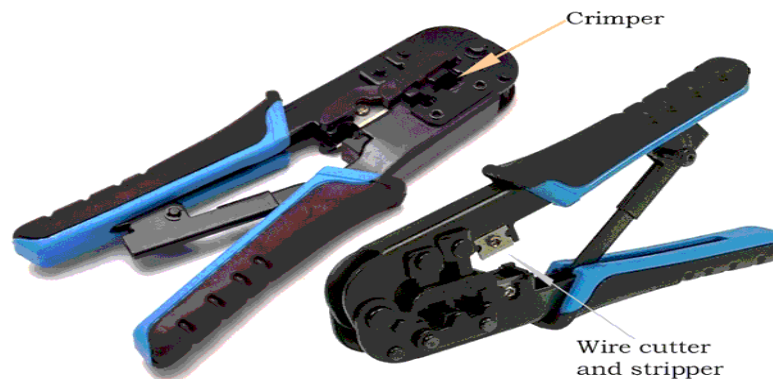


Test the cable: Check the continuity of both connectors each other. Check the cable throw a cable tester or ping from a computer. To check the cable through computer connects both connector in two computers for cross cable and straight cable connect through a switch then ping the computer.

N.B: When you connect two devices of different types together, you use a straight through cable. When you connect two devices of the same type

together, you use a crossover cable. All cables are straight through if you insert a network device between two devices of the same kind.

- **Crimping tools**



Crimping tools are used for the following purposes.

- To cut the network cable of the required length from the bundle.
- To remove the outer and inner jackets of the network cable.
- To attach the connectors on both ends of the cable.

- **Testing tool**



Network cable testing and troubleshooting tools

A network cable testing and troubleshooting tool is used for the following purposes.

- To measure the length of a segment or network cable.
- To detect loose connectors.
- To identify an un-labeled network cable from all network cables.
- To find a break in the network cable.
- To certify the cable installation.

1.2. Equipment

- **Computer:** A *computer* is a machine that can be programmed to carry out sequences of arithmetic or logical operations (computation) automatically.
- **UPS:** An **uninterruptible power supply (UPS)** or **uninterruptible power source**

is a type of continual power system that provides automated backup electric power to a load when the input power source or mains power fails. A UPS differs from a traditional auxiliary/emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions by switching to energy stored in battery packs, super capacitors.



- **Inverter:** An inverter converts the DC voltage to an AC voltage. In most cases, the input DC voltage is usually lower while the output AC is equal to the grid supply voltage of either 120 volts, or 240 Volts depending on the country.



- **Switch:** A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the

destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.



- **Glue gun:** Hot-melt adhesive, also known as hot glue, is a form of thermoplastic adhesive that is commonly sold as solid cylindrical sticks of various diameters designed to be applied using a hot glue gun.



- **Rack:**

What is a Network Rack?

Known by many names, a **network rack** is a metal frame chassis that holds, stacks, organizes, secures and protects various computer network and server hardware devices. The term “network” refers to the rack actually housing this type of hardware.

Network Rack Equipment

These racks can house a lot of different types of equipment. Network equipment is really just an umbrella term that encapsulates various kinds of technology. Some of these devices include the following:

- **Switches** – Multi-port, high-speed devices that receive data and redirect them to the correct destination on a local area network (LAN). Information can only go across a single network using a switch.
- **Routers** – Similar to switches, routers receive and forward information, but they can carry data over multiple networks. This is why, for example, different devices or networks can access the Internet using one single router.
- **Modems** – This device actually connects the source of your internet to your router. This is typically done using an ethernet cord.



- **Brackets**

In networking, brackets typically refer to physical enclosures or mounting devices.



- **Patch panel:** A patch panel in a local area network (LAN) is a mounted hardware assembly that contains ports that are used to connect and manage incoming and outgoing LAN cables. A patch panel provides a way to keep large numbers of cables organized, enabling flexible connectivity into network hardware located in a data center or an access or wiring closet



- **Repeater**



In telecommunications, a repeater is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction.

Regenerator: In the context of networking, a "regenerator" typically refers to a network device or component that is used to boost or regenerate the strength of optical signals. Optical signals can degrade as they travel long distances in optical fiber cables, and regenerators are employed to restore the signal quality.

1.3. Materials

- **Network Cables (twisted, coaxial, and Fiber optic)**



Image 1. Twisted pair cable

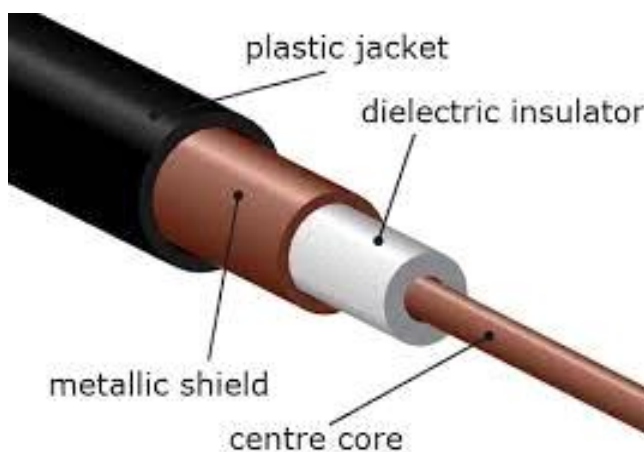


Image 2. Coaxial cables

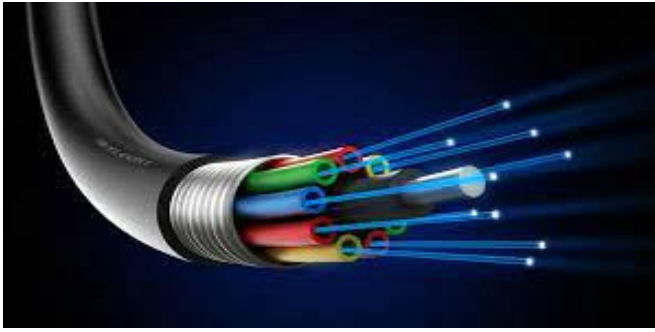
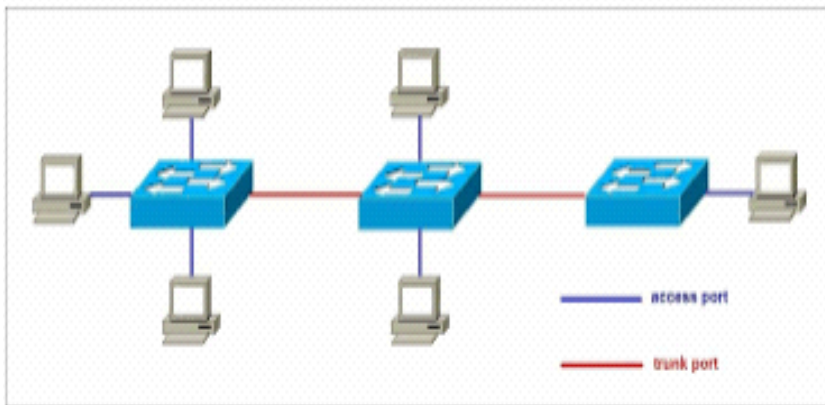


Image 3. Fiber Optics

- **Trunk**

In networking, a trunk is a communication link that carries multiple data signals or network traffic between devices, typically switches or routers, using VLAN (Virtual Local Area Network) tagging.



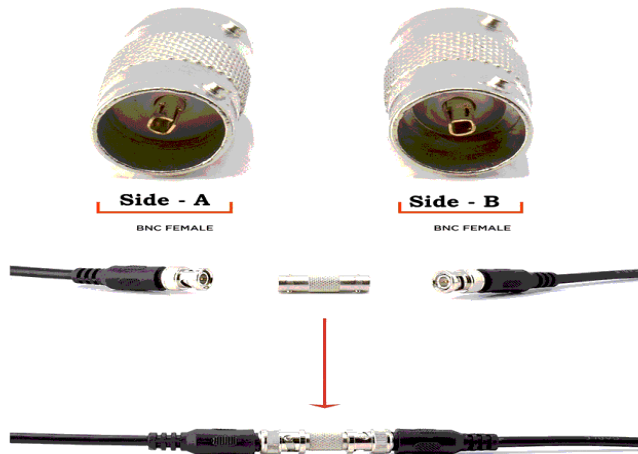
- **Connectors**

A connector is a device that terminates a segment of cabling or provides an entry point for network devices such as computers, hubs and routers. These can in turn be differentiated according to their external appearance and connection characteristics.

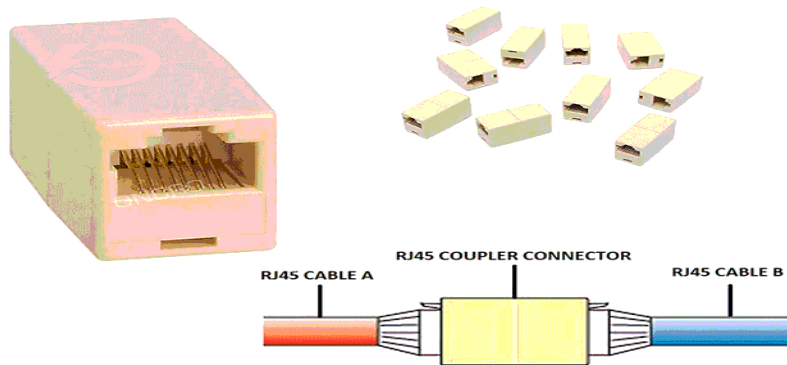
Types of Connectors

That's all for this tutorial. If you like this tutorial, please don't forget to share it with friends through your favorite social network.

Barrel connectors that are used to connect coaxial cables are known as **BNC barrel connectors**. The following image shows BNC barrel connectors.



Barrel connectors that are used to connect STP or UTP cables are known as **Ethernet LAN jointers** or **couplers**. The following image shows Ethernet LAN jointers or couplers.



Barrel connectors do not amplify the signals. It means, after joining, the total cable length must not exceed the maximum supporting length of the cable. For example, a standard UTP cable supports a maximum distance of 100 meters. You can join two UTP cables if their sum is not more than 100.

For example, you can join the following cables.

Cable 1 (45 meters) + cable 2 (30 meters) = joint cable (75 meters = 45 meters + 30 meters)

The length of the joint cable is less than 100 meters.

But you can't join the following cables.

Cable 1 (65 meters) + cable 2 (45 meters) = joint cable (110 meters = 65 meters + 45 meters)

The length of the joint cable is more than 100 meters.

F connectors

An **F** connector is used to attach a coaxial cable to a device. **F** connectors are

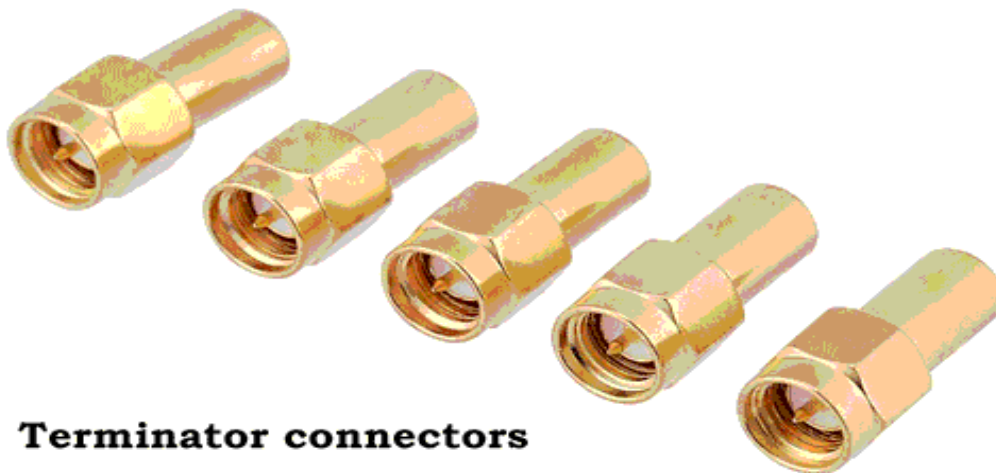
mostly used to install home appliances such as dish TV, cable internet, CCTV camera, etc. The following image shows F connectors.



Terminator connectors

When a device places signals on the coaxial cable, the signals travel along the end of the cable. If another device is connected to the other end of the cable, the device will receive the signal. But if the other end of the cable is open, the signals will bounce and return in the same direction they came from. To stop signals from bouncing back, all endpoints must be terminated.

A terminator connector is used to terminate the endpoint of a coaxial cable. The following image shows terminator connectors.



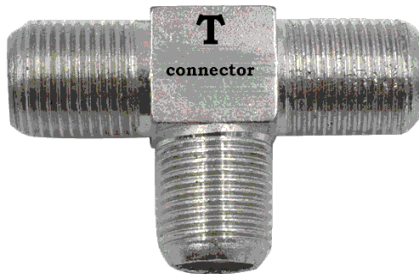
Terminator connectors

T type connectors

A T connector creates a connection point on the coaxial cable. The connection

point is used to connect a device to the cable.

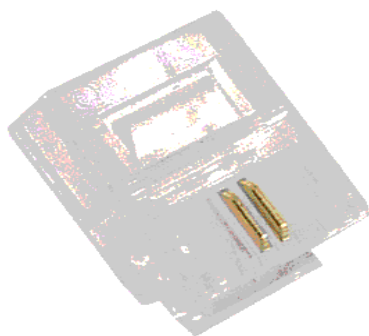
The following image shows T-type connectors.



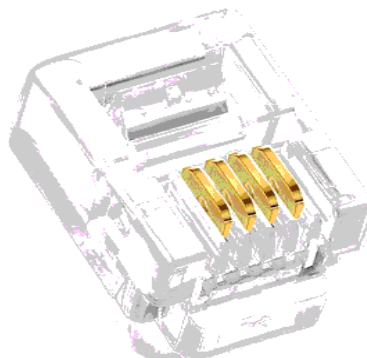
RJ-11 Connectors

RJ-11 connectors have the capacity for six small pins. However, in many cases, only two or four pins are used. For example, a standard telephone connection uses only two pins, and a DSL modem connection uses four pins. They have a small plastic flange on top of the connector to ensure a secure connection.

The following image shows RJ-11 connectors.



**2 - Pins RJ-11
for phone lines**

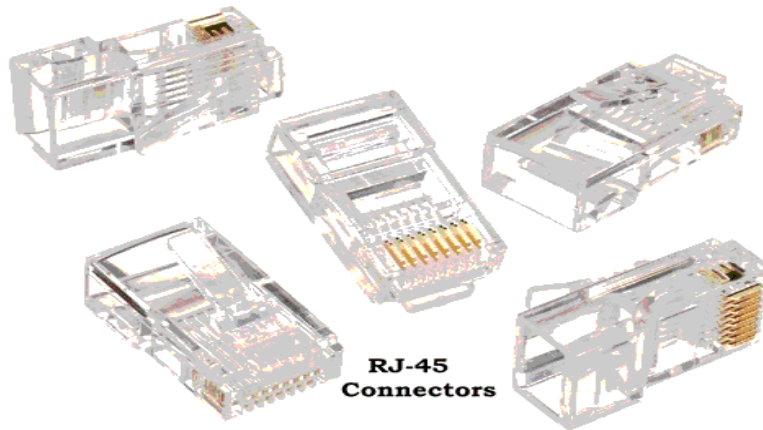


**4 - Pins RJ-11
for DSL modem**

RJ-45 connectors

RJ-45 connectors look like RJ-11 connectors, but they are different. They have 8 pins. They are also bigger in size than RJ-11. RJ-45 connectors are mostly used in computer networks. They are used with STP and UTP cables. Some old Ethernet implementations use only four of the eight pins. Modern Ethernet implementation uses all 8 pins to achieve the fastest data transfer speed.

The following image shows RJ-45 connectors.



DB-9 (RS-232) connectors

A DB-9 or RS-232 connector connects a device over a serial port. It has 9 pins. It is available in both male and female connectors. It is used for asynchronous serial communication. The other side of the cable can be connected to any popular connector type. For example, you can connect one side of the cable with a DB-9 connector and the other side of the cable with another DB-9 connector or with an RJ-45 connector or with a USB connector.

The following image shows DB-9 connectors.



One of the most popular uses of a DB-9 connector is to connect the serial port on a computer with an external modem.

Universal serial bus (USB) connectors

USB connectors are the most popular. They support 127 devices in the series. All modern computers have USB ports. Most devices that you can connect to the system have USB ports. Some examples of devices that support or have USB ports are mice, printers, network cards, digital cameras, keyboards, scanners,

mobile phones, and flash drives.



If the device has a USB port, you can use a cable that has a USB connector on both ends to connect the device to the computer. If the device does not have a USB port, you can still connect the device to the USB port. For that, you can use a cable that has a USB connector on one side and the corresponding connector on the other.

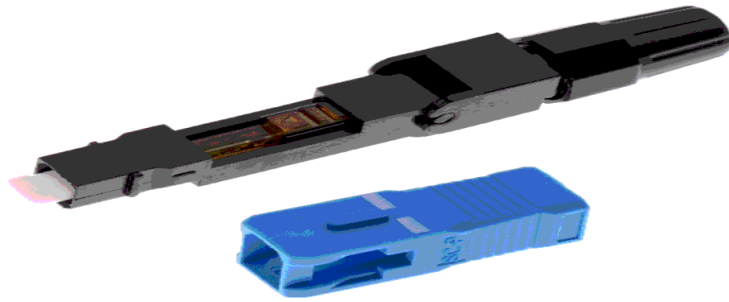
Fiber cable connectors

A variety of connectors are used to connect fiber cables. Some popular connectors are ST, SC, LC, and MTRJ. Let's discuss these connectors.

SC connectors

SC connectors are also known as **subscriber connectors**, **standard connectors**, or **square connectors**. An SC connector connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pulling the connector from the terminating device. It uses a push-pull connector similar to audio and video plugs and sockets.

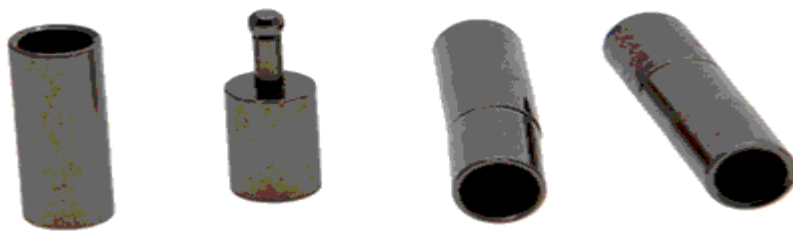
The following image shows SC connectors.



Straight tip (ST) connectors

Straight tip (ST) connectors are also known as **bayonet connectors**. They have a long tip extending from the connector. They are commonly used with MMF cables. They use a half-twist bayonet type of lock. An ST connector connects to a terminating device by pushing the connector into the terminating equipment and then twisting the connector housing to lock it in place.

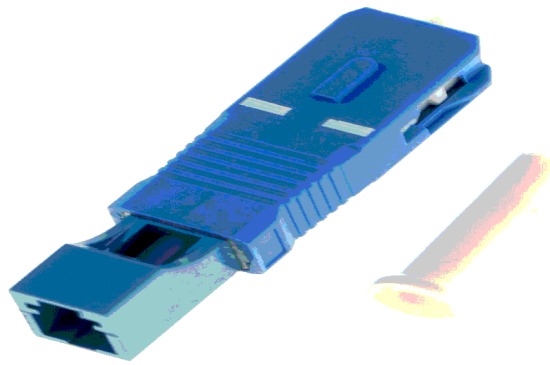
The following image shows ST connectors.



LC connectors

LC connectors are known as **Lucent Connectors**. For a secure connection, they have a flange on top, similar to an RJ-45 connector. An LC connector connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pressing the tab on the connector and pulling it out of the terminating device.

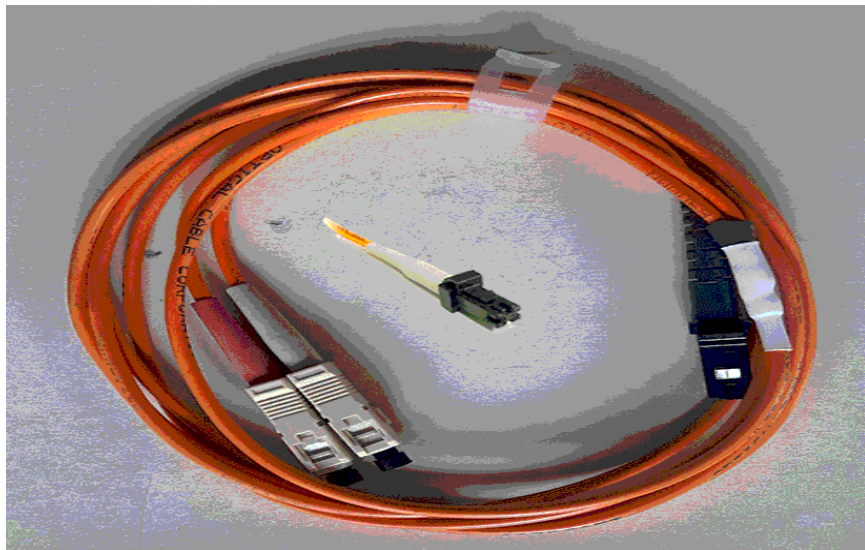
The following image shows LC connectors.



MTRJ connectors

An MTRJ connector connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pulling the connector from the terminating device. It includes two fiber strands: a transmit strand and a receive strand in a single connector.

The following image shows MTRJ connectors.



- **Cable Ties :**



- **Cable clips**



- **Cable Sockets**



- **Wall plugs**





Practical Activity 1.1.3: Selection of tools, materials and equipment for network installation.



Task:

1: With referring to the key readings 1.1.3, Read the following task:

As someone who learned network tools, materials and equipment, you are asked to go in the workshop and select the right tools, material and equipment to be used while installing a Network.

2: Perform the task by following the instructions related to the task.

3: Ask for clarification if any and assistance where needed.

4: Present your work to trainer or whole class.

5: Perform the task provided in application of learning 1.1



Key readings 1.1.3.: Selection of tools, materials and equipment for network installation.

1. Selection of tools, materials, and equipment for Network installation

1.1. Steps to select tools, materials and equipment

Step 1: Assess Requirements:

Understand the Network Design: Determine the network topology, size, and specific needs (e.g., LAN, WAN, Wi-Fi).

- ✓ **Identify Network Components:** Know what devices and infrastructure are required, such as routers, switches, and access points.

Step 2: Select Tools:

- ✓ **Network Testing Tools:** Choose tools for testing and diagnosing network issues, such as network analyzers, cable testers, and signal strength meters.
- ✓ **Configuration Tools:** Ensure you have software or devices for configuring network devices, such as network configuration utilities or management software.

• Step 3: Choose Materials:

- ✓ **Cables:** Select appropriate cables based on network requirements, such as Ethernet cables (Cat5e, Cat6) for wired connections and fiber optic cables for high-speed connections.
- ✓ **Connectors and Patch Panels:** Choose connectors (RJ45 for Ethernet) and patch panels for organizing and managing network cables.
- ✓ **Cable Management:** Obtain materials for organizing cables, such as cable ties, clips, and conduits.

• Step 4: Pick Equipment:

- ✓ **Network Devices:** Select routers, switches, and access points that meet the network's needs and specifications.
- ✓ **Modems:** Choose a modem suitable for the internet service provider (ISP) and the type of connection (DSL, cable, fiber).
- ✓ **Network Racks and Shelves:** If applicable, choose racks and shelves for mounting and organizing network devices.

Step 5: Verify Compatibility:

- ✓ **Check Specifications:** Ensure all tools, materials, and equipment are compatible with each other and meet the network's requirements.
- ✓ **Consider Future Expansion:** Select components that allow for scalability and future upgrades if needed.

1.2. The requirement assessment for each selection of tools, materials and equipment during networking installation

Assess Requirements to Select Tools

- Comprehensive Capabilities (bandwidth analysis, device monitoring)
- Network Environment (operating systems, hardware, and protocols)
- Vendor Compatibility
- Network Growth
- Data Protection
- Budget Consideration

Assess Requirements to Select Choose Materials

- Network Type
- Network Topology
- Hardware Compatibility
- Bandwidth Requirements
- Material Quality
- Environmental Factors
- Physical Security

Assess Requirements to Select Equipment

- Network Size and Scope
- Device Compatibility
- Future Growth
- High Availability
- Initial Cost



Points to Remember

- A network consists of two or more computers that are linked in order to share resources.
- Networks can be classified into different categories based on various criteria, including their size, purpose and architecture.
- Networks offer a wide range of benefits like Communication, Data Sharing, Resource Sharing, Flexibility and Mobility and Cost Efficiency.
- Networks offer numerous advantages like Communication, Resource Sharing, Centralized Data Management, Redundancy and Reliability, Global Connectivity etc..
- Disadvantages of Networks are: Security Risks, Complexity, Maintenance Costs, Privacy Concerns, Bandwidth Limitation etc..
- Networks can be applied in Telecommunications, Data Centers, Transportation, Healthcare, Financial Services, Entertainment and Media, Education etc..
- Network technologies encompass a wide range of tools, protocols, hardware, and software.
- Network topologies types are Bus Topology, Star Topology, Ring Topology, Mesh Topology and Tree Topology.
- Network components are classified based on End Devices, Networking Hardware, Network Infrastructure, Networking Software and Protocols.
- In networking, tools are software or utilities used for tasks like monitoring, configuration, and troubleshooting, such as network analysers or configuration tools. Materials refer to the physical components and resources used in setting up and maintaining networks, like cables, connectors, and network cards. Equipment encompasses the larger hardware devices that facilitate network connectivity and communication, including routers, switches, and modems.
- While selecting materials, tools and equipment for networking installation make sure that you emphasize on the understanding of network design and network components as well as following the steps.



Application of learning 1.1.

A small company is opening a new office with 15 employees. The company needs a reliable network to support daily operations, including internet access, file sharing, and communication. You have been asked to identify and select the necessary network components to set up infrastructure.



Indicative content 1.2: Termination of Network Cables



Duration: 5 hrs



Theoretical Activity 1.2.1: Description of network cable installation types



Tasks:

- 1: you are requested to answer the following questions:
 - i. What are the network cable installation types
 - ii. Explain network cable installation types
 - iii. Provide the use cases of each cable installation types.
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class.
- 4: For more clarification, read the key readings 1.2.1.
- 5: In addition, ask questions where necessary.



Key readings 1.2.1: Description of network cable installation types

1. Description of network cable installation types

1.1. Network cable installation types

- **Open wire:** was an early transmission technology in telecommunication, first used in telegraph.



- **Aerial cable**

Aerial cable consists of fully insulated conductors suspended above the ground.



- **Network cable termination in above-ground conduits** refers to the process of ending or connecting network cables, such as Ethernet cables, that have been

routed through conduits installed above ground. These conduits are protective tubes, often made of PVC, metal, or other durable materials, that safeguard cables from environmental damage, physical wear, and interference.

- **Underground**

Network cable termination in underground conduits refers to the process of connecting or terminating network cables that are installed within protective conduits buried below ground. These conduits shield the cables from environmental factors like moisture, soil pressure, and physical damage, ensuring the long-term reliability and performance of the network.

- **Underwater**

Submarine cable is used only when no other cable system can be used. It supplies circuits that must cross expanses of water or swampy terrain.



- **Network cable termination "built-in"** typically refers to the process of terminating network cables within structures or enclosures that are integrated into walls, floors, or ceilings of a building.
- **Network cable termination "semi built-in"** refers to a hybrid approach where network cables are partially integrated into the building's structure, but with certain elements of the cabling and termination points remaining accessible or visible. This method balances the aesthetic and protective benefits of a fully built-in system with the flexibility and accessibility of more traditional installations.

1.2. Network Cable termination are:

- ✓ Twisted pair cabling,
- ✓ Fiber-optic cabling,
- ✓ Coaxial cabling
- ✓ Shielded twisted pair.



Twisted Pair Cabling

Twisted pair cabling is a type of communications cable in which two conductors of a single circuit are twisted together for the purposes of improving electromagnetic compatibility



Unshielded twisted pair or UTP: UTP cable has four pairs, or eight colour-coded copper wires twisted together and covered with a plastic sheath. Their electromagnetic interference gets cancelled due to the twisting effect. UTP cables are primarily used in LANs, telephone wires and ethernet cables.

Shielded twisted pair or STP: STP cable uses the techniques of wire twisting, shielding, and cancellation. Each wire pair is covered in a metallic foil. Then four pairs of wires are then covered by an external metallic braid. STP cables reduce crosstalk both within the cable with pair-to-pair coupling and from outside the cable.

Categories of twisted pair cables

The EIA has classified the twisted pair cables into seven distinct categories –

- Category 1 or Cat 1 – UTP cables with data rate < 0.1 Mbps, used in telephone lines
- Category 2 or Cat 2 – UTP cables with a data rate of 2 Mbps, used in transmission lines
- Category 3 or Cat 3 – UTP cables with a data rate of 10 Mbps, used in LANs or 10baseT Ethernet
- Category 4 or Cat 4– UTP cables with a data rate of 20 Mbps, used in token ring networks
- Category 5 or Cat 5 – UTP cables with a data rate of 100 Mbps, used in LANs or 100baseT Ethernet
- Category 5e or Cat 5e – 1000baseT Ethernet with a data rate of 1000 Mbps
- Category 6 or Cat 6 – UTP cables with a data rate of 200 Mbps, used in high-speed LANs
- Category 7 or Cat 7 – STP used in super high-speed Gigabit Ethernet.

🌈 Fiber Optic Cables

Compared to copper wired cables, **fiber optic cables** provide higher bandwidth and can transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems. They carry communication signals using pulses of light generated by small lasers or light-emitting diodes (LEDs).



The main difference between Twisted pair cabling and Fiber-optic cabling
Twisted pair cabling and fiber-optic cabling are two common types of cables used in network infrastructure, but they differ significantly in their design, performance, and applications. Here are the main differences between the two:

1. Construction:

- **Twisted Pair Cabling:**
 - **Structure:** Consists of pairs of insulated copper wires twisted together. The twisting reduces electromagnetic interference (EMI) from external sources and crosstalk between adjacent pairs.
 - **Types:** Common types include **Unshielded Twisted Pair (UTP)** and **Shielded Twisted Pair (STP)**. UTP is more common for general networking, while STP is used in environments with higher EMI.
- **Fiber-Optic Cabling:**
 - **Structure:** Composed of thin strands of glass or plastic fibers that transmit data as light signals. Each fiber consists of a core (where the light travels), cladding (which reflects the light back into the core), and a protective outer coating.
 - **Types:** Two main types are **Single-mode fiber (SMF)**, used for long-distance communication, and **Multi-mode fiber (MMF)**, used for shorter distances.

2. Data Transmission:

- **Twisted Pair Cabling:**
 - **Signal Type:** Transmits data as electrical signals.
 - **Speed and Bandwidth:** Capable of supporting speeds up to 10 Gbps (Cat6a and Cat7 cables) over short distances. However, higher speeds over longer distances are limited due to signal degradation.
- **Fiber-Optic Cabling:**
 - **Signal Type:** Transmits data as light pulses, which allows for much higher speeds and bandwidth.
 - **Speed and Bandwidth:** Capable of supporting speeds up to 100 Gbps and beyond, with much greater bandwidth capacity than twisted pair cabling. It is also less susceptible to signal degradation over long distances.

3. Distance:

- **Twisted Pair Cabling:**
 - **Range:** Typically, effective up to 100 meters (328 feet) for Ethernet networking (e.g., Cat5e, Cat6). Beyond this distance, signal boosters or repeaters are needed to maintain performance.

- **Fiber-Optic Cabling:**

- **Range:** Capable of transmitting data over much longer distances without significant signal loss. Single-mode fiber can transmit over distances of up to 40 kilometers (25 miles) or more, while multi-mode fiber is generally used for shorter distances, up to a few kilometers.

4. Interference and Security:

- **Twisted Pair Cabling:**

- **Interference:** Susceptible to electromagnetic interference (EMI) and radio frequency interference (RFI), although shielded twisted pair (STP) can mitigate this to some extent.
- **Security:** Electrical signals can be intercepted and tapped, making twisted pair cabling less secure compared to fiber-optic.

- **Fiber-Optic Cabling:**

- **Interference:** Immune to EMI and RFI because it uses light rather than electrical signals for data transmission.
- **Security:** Much more secure, as intercepting light signals is significantly more difficult, and attempts to tap into a fiber-optic cable usually result in noticeable signal loss.

5. Cost:

- **Twisted Pair Cabling:**

- **Cost:** Generally, less expensive to purchase and install than fiber-optic cabling. The associated equipment (e.g., switches, routers) is also typically less costly.
- **Installation:** Easier and less expensive to install, especially for shorter distances and in existing infrastructure.

- **Fiber-Optic Cabling:**

- **Cost:** More expensive due to the materials (glass or plastic fibers) and the need for specialized equipment and expertise for installation and termination.
- **Installation:** Requires more precision and care during installation, often involving splicing or specialized connectors, leading to higher installation costs.

6. Applications:

- **Twisted Pair Cabling:**

- **Common Uses:** Widely used for local area networks (LANs), telephone lines, and general office networking due to its cost-effectiveness and ease of use.
- **Suitability:** Ideal for short to medium distances and environments where high bandwidth and speed are not critical over long distances.

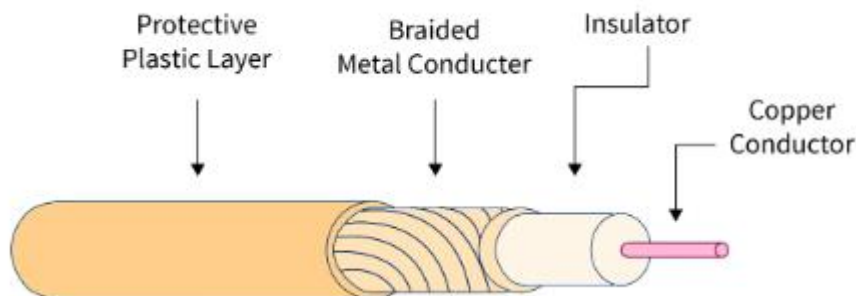
- **Fiber-Optic Cabling:**

- **Common Uses:** Used for backbone infrastructure, long-distance telecommunications, data centers, and high-speed internet connections.
- **Suitability:** Best for environments requiring high bandwidth, long-

distance transmission, and secure communication.

Coaxial Cable

A coaxial cable is a type of shielded and insulated copper cable that is used in computer networks and to deliver cable TV services to end users.



Shielded Twisted Pair

Shielded Twisted Pair (STP) cabling is a type of network cabling designed to reduce electromagnetic interference (EMI) and radio frequency interference (RFI), making it suitable for environments where such interference could impact network performance. STP cables have additional shielding layers around the twisted pairs of wires, providing better protection than unshielded twisted pair (UTP) cables.

Comparison of **Coaxial Cable** and **Shielded Twisted Pair (STP) Cable** in networking

Feature	Coaxial Cable	Shielded Twisted Pair (STP) Cable
Construction	Central conductor, dielectric insulation, shield, outer jacket	Twisted pairs of insulated wires, shielding around pairs or entire bundle
Signal Transmission	Electrical signals along the central conductor	Electrical signals over twisted pairs
Shielding	Robust shielding with foil or braided mesh around the conductor	Shielding around each pair or overall bundle, often with a drain wire
Interference	Excellent resistance to EMI and RFI	Good resistance to EMI and RFI, less than coaxial cable
Bandwidth	High-frequency support, capable of high data rates	Typically supports lower frequencies, but effective for high-speed Ethernet
Distance	Effective over longer distances without significant signal degradation	Effective up to about 100 meters (328 feet) for Ethernet

Typical Applications	Cable TV, broadband internet, broadcasting, CCTV	Ethernet networking, telecommunications, industrial environments
Cost	Generally, more expensive per meter	Less expensive than coaxial but more expensive than Unshielded Twisted Pair (UTP)
Installation Flexibility	More rigid and less flexible, challenging in tight spaces	More flexible and easier to install, suitable for building infrastructure
Typical Use Cases	High-frequency applications, cable modems, legacy systems	Local area networks (LANs), data centers, environments with high electrical noise



Theoretical Activity 1.2.2.: Description of network cables Trunking materials



Tasks:

- 1: you are requested to answer the following questions related to the Description of network cables Trunking:
 - i. What is network cable trunking?
 - ii. Describe Network cables Trunking materials.
 - iii. State the importance of cable trunking in network installation.
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class.
- 4: For more clarification, read the key **readings 1.2.2**
- 5: In addition, ask questions where necessary.



Key readings 1.2.2.: Description of network cables Trunking materials

1. Description of network cables Trunking materials

• **Network cable trunking** refers to the system of channels or conduits used to organize, protect, and route multiple network cables throughout a building or facility. This method ensures that cables are neatly managed, reduces clutter, and helps maintain a clean and efficient network installation.

• **Network cables Trunking materials are:**

- ✓ Plastic,
- ✓ Wood and

✓ **Stainless**

- a. **Plastic trunking is an enclosure made by plastic** especially PVC. This trunking has prevailed as a material for cable trunking, thanks to its robust characteristics. It is flame-resistant, largely withstands UV radiation and offers smooth surfaces which look great around walls or floor lines. Residential or office environments will often use plastic/PVC trunking.
- b. **Stainless steel (Metal Trunking)** It is an enclosure made by metal especially stainless steel. You can choose aluminium trunking for walls or steel trunking if you want to run cables under the floor. If electrical cables need to be run underground, then flush floor trunking is a great option. For more industrial applications or areas of high footfall metal trunking rules.
- c. **Wooden trunking** is a cable enclosure made by wood. These wooden cable trunkings are eco-friendly and are non-conductors of electricity with absolute flame-retardant features.

2. Cable trunking is crucial in network installation for several key reasons:

✓ **Organization:**

✚ **Efficient Cable Management:** Trunking systems neatly organize cables, preventing them from becoming tangled or cluttered. This helps in maintaining a structured and efficient network setup.

✚ **Easier Identification:** With cables neatly routed in trunking, it is easier to identify and manage individual cables for troubleshooting and maintenance.

✓ **Protection:**

✚ **Physical Protection:** Trunking protects cables from physical damage caused by environmental factors, accidental impacts, or sharp objects. This reduces the risk of cable wear and breakage.

✚ **Environmental Protection:** Helps shield cables from dust, moisture, and other environmental elements that could impact their performance and longevity.

✓ **Safety:**




✚ **Reduced Tripping Hazards:** By concealing cables within trunking, you minimize tripping hazards and potential accidents, creating a safer work environment.

✚ **Compliance with Standards:** Cable trunking helps meet safety regulations and building codes that require organized and protected cable installations.

✚ **Neat Appearance:** Trunking provides a clean and professional appearance by hiding cables from view. This is particularly important in office environments and public spaces where visual appeal matters.

✚ **Improved Workspace:** A well-organized cabling system enhances the overall look of the installation area, making it more presentable and less cluttered.

✓ **Accessibility:**

-  **Ease of Access:** Trunking systems often have removable covers or access points, making it easier to add, remove, or reconfigure cables without significant disruption.
-  **Maintenance and Upgrades:** Simplifies the process of cable maintenance and upgrades, as technicians can access and manage cables without disturbing the entire network setup.
- ✓ **Scalability:**
-  **Future proofing:** Trunking systems can be designed to accommodate additional cables or future expansions, allowing for easy network upgrades and scalability without needing a complete overhaul.



Practical Activity 1.2.3: Network cables Trunking



Task:

1: With referring to the key readings 1.2.3, you are requested to perform the given task. The task should be done individually.

According to theoretical activity we have done on 1.2.2 you are asked to make installation of network trunks that will be used to carry cables in the room provided and perform the cables trunking in the network installation provided.

2: Present your work to the trainer and whole class.

5. Ask for more clarifications.

6: Perform the task provided in application of learning 1.2.2





Key readings 1.2.3.: Network cables Trunking

1. Network cables Trunking




Trunking: the purpose of trunking is to organize and protect network cables as they run through a building, ensuring a clean and efficient cable management system.

1.1. Steps for performing network trunking



✓ Planning:

-  **Design the Route:** Determine the path for trunking based on the network design, considering factors like cable type, distance, and obstacles.
-  **Select Trunking Material:** Choose appropriate trunking (plastic, metal, etc.) based on the environment and cable type.

✓ **Installation:**

-  **Mount Trunking:** Attach trunking to walls, ceilings, or floors using appropriate mounts or adhesive.
-  **Route Cables:** Feed network cables through the trunking, ensuring they are organized and not strained.
-  **Secure and Cover:** Close the trunking with covers or lids to protect the cables and maintain a neat appearance.

✓ **Testing:**

-  **Check Cable Routing:** Ensure cables are not kinked or damaged and that they are properly secured.
-  **Verify Installation:** Confirm that the trunking is securely mounted and that cables are easily accessible for future maintenance.

In Summary: Trunking involves planning, installing, and securing cable management systems to route and protect network cables.



Theoretical Activity 1.2.3: Description of network cables termination



Tasks:

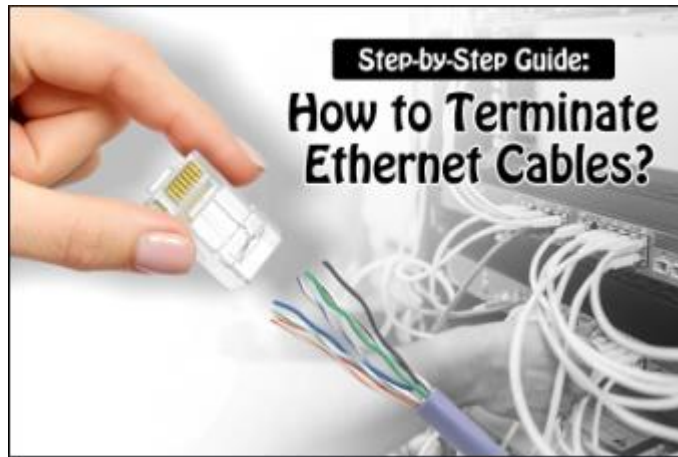
- 1: you are requested to answer the following questions related to the description of network cables Termination:
 - i. Describe Network cables Termination
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class.
- 4: For more clarification, read the key readings 1.2.1.3
- 5: In addition, ask questions where necessary.



Key readings 1.2.3.: Description of network cable termination

1. Description of network cables termination

Network cable termination is the process of attaching connectors to the ends of network cables to enable them to interface with network devices. Proper termination ensures that the network cables can transmit data effectively and reliably.



Cable Termination steps include Preparing Cables by stripping cable jackets and Untwist pairs, Trim excess wires to ensure they are even and fit into the connector, Insert wires into the correct slots of the RJ45 connector according to the termination standard (T568A or T568B), Use a crimping tool to secure the connector and ensure all wires are properly terminated.

Steps:

Preparation:

- ✚ Strip Cable: Remove the outer insulation of the cable to expose the individual wires, taking care not to damage them.
- ✚ Arrange Wires: Arrange the wires according to the wiring standard (e.g., T568A or T568B for Ethernet).

Termination




Connector Installation:

- ✚ For Ethernet (RJ45): Insert the wires into the RJ45 connector and use a crimping tool to secure the connector.
- ✚ For Fiber Optic: If using fiber optic cables, perform splicing or attach fiber connectors following precise procedures.
- ✚ Panel or Outlet Mounting: Install the terminated connectors into patch panels, wall outlets, or other network devices.

Testing:

- ✚ Cable Testing: Use a cable tester to check for continuity, correct pin configuration, and signal integrity.
- ✚ Performance Check: Ensure that the terminated connections meet network specifications and perform at the required speed and reliability.

Finalization:

-  Documentation: Label cables and document their connections for future reference.
-  Inspection: Perform a final inspection to ensure everything is properly installed, organized, and functioning correctly.
-  Termination: Involves preparing, connecting, and testing cables to ensure reliable network connections.

Both processes are essential for maintaining an organized, efficient, and functional network infrastructure.



Practical Activity 1.2.4. Network cables Termination



Task:

- 1: With referring to key reading 1.2.4, read the task described below:
As a trainee who learned cable termination. You are asked to terminate the network cables for 5 computers, 2 printers that will be connected to the office's network switch and patch panel.
- 2: Perform the task by following the instructions related to the task
- 3: Ask for assistance and more clarifications where needed
- 4: Present the results to the trainer or whole class
- 5: Read key readings 1.2.4. in the trainee manual.



Key readings 1.2.4.: Network cable Termination

1. Network cables Termination

Performing cable terminating to ensure a reliable and efficient network. Here's a comprehensive guide on how to perform these tasks:

Cable Terminating

Tools and Materials

1. **Cables:** Cat5e, Cat6, Cat6a, or Cat7.
2. **RJ45 Connectors:** Standard connectors for Ethernet cables.
3. **Crimping Tool:** For securing RJ45 connectors to the cable.
4. **Cable Stripper:** To remove the outer insulation of the cable.
5. **Punch Down Tool:** For terminating cables into keystone jacks or patch panels.

6. Cable Tester: To verify the termination and connectivity of the cables.

Steps to Terminate an Ethernet Cable

1. Strip the Cable:

- Use the cable stripper to remove about 1 inch (2.5 cm) of the outer jacket, exposing the inner twisted pairs of wires.

2. Untwist and Arrange Wires:

- Untwist the wire pairs and arrange them according to either the T568A or T568B wiring standard. T568B is more common in the U.S.
- The order for T568B is:
 - Pin 1: White/Orange
 - Pin 2: Orange
 - Pin 3: White/Green
 - Pin 4: Blue
 - Pin 5: White/Blue
 - Pin 6: Green
 - Pin 7: White/Brown
 - Pin 8: Brown

3. Cut Wires to Length:

- Ensure the wires are even and cut them to fit into the RJ45 connector properly.

4. Insert Wires into RJ45 Connector:

- Push the wires into the connector, ensuring each wire is in the correct slot. The wires should reach the end of the connector.

5. Crimp the Connector:

- Use the crimping tool to secure the connector onto the cable. This process also connects the metal contacts within the connector to the wires.

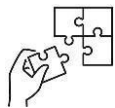
6. Test the Cable:

- Use a cable tester to verify that the cable is terminated correctly and is functional.



Points to Remember

- **Network cables installation types** are Open-Wire, Aerial, Above-Grounds Conduits, Underground, Underwater, built in and Semi built in.
- **Network cables Trunking materials** are Plastic, Wood, and Stainless.
- **Network cable trunking** refers to the system of channels or conduits used to organize, protect, and route multiple network cables throughout a building or facility.
- **Cable trunking** is crucial in network installation for several key reasons like: Organization, Protection, Safety.
- **Trunking Installation steps include:** Planning and Preparation, selection of Materials and Tools, Fix or Mounting Trunking and Routing Cables through the trunking.
- **Cable termination** use in networking are Twisted pair cabling, Fiber-optic cabling, Coaxial cabling and Shielded twisted pair.
- **Cable Terminating:** Cable terminating involves attaching connectors to the ends of network cables, allowing them to be plugged into devices, patch panels, or wall jacks.



Application of learning 1.2.

XYZ complex market would like to install Network in their buildings. You are one of the technician team that is going to install that network and you are assigned to perform the following tasks:

You are asked to install the network trunking system using above-Grounds Conduits installation type and perform cable termination.



Indicative content 1.3: Connection of network media



Duration: 5 hrs



Theoretical Activity 1.3.1: Description of network media



Tasks:

- 1: you are requested to answer the following questions related to the classification of IP address.
 - i. Explain labelling in networking.
 - ii. Differentiate Patching and Tagging in networking.
 - iii. Explain how to build design in networking media.
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class
- 4: For more clarification, read the **key readings 1.3.1**.
- 5: In addition, ask questions where necessary.



Key readings 1.3.1.: Description of network media

1. Description of network media

• Labelling in Networking

Labelling in networking refers to the practice of assigning identifiable names or tags to network components, connections, and configurations to facilitate management, troubleshooting, and documentation. This can include:

1. Cable Labelling

Cable labelling involves marking network cables with identifiers that describe their purpose, source, and destination. This helps in managing and tracing cables easily.

Examples: A label might read “To Switch Port 12” or “From Router WAN Port”.

2. Device Labelling

Device labelling involves assigning unique and descriptive names or tags to network devices, such as routers, switches, and servers. This helps identify each device's role and location within the network.

Examples: A router might be labelled as “CoreRouter01” to indicate it’s a core router in the network. Similarly, a switch might be labelled “Switch-Floor1” to specify its location.

3. Port Labelling

Port labelling involves marking individual ports on network devices like switches and routers to indicate their function, network membership, or connection details. This simplifies port management and troubleshooting.

Examples: A switch port label might read “Port 5 - Network 10 - Desk 12” to indicate which Network the port is associated with and the location it connects to.

4. Patch Panel Labelling

Patch panel labelling involves marking ports on a patch panel to show the cable connections from various network devices. This aids in organizing and managing network connections efficiently.

Examples: Labels on a patch panel might read “Patch 1 - Server Room” or “Patch 2 - Main Switch”, indicating where each cable is routed to or from.

- **Benefits of Network Labelling:**

- ✓ **Simplifies Troubleshooting:** Clearly labelled cables and devices make it easier to identify and fix network issues.
- ✓ **Improves Organization:** Helps keep the network infrastructure organized and manageable.
- ✓ **Aids Documentation:** Provides a clear reference for network diagrams, configurations, and maintenance records.
- ✓ **Facilitates Maintenance:** Labels allow for quick identification and management of network components during upgrades or repairs.

- **Patching and Tagging in Networking**

Patching and **tagging** are key concepts in network management, each serving different purposes in maintaining and organizing network connections and traffic.

2. Patching

Patching in networking refers to the physical process of connecting network devices or segments using cables. This step involves creating connections between various network components such as switches, routers, servers, and computers.

The purpose of patching is to establish physical communication paths between network devices and to facilitate data exchange across the network by linking devices to switches or routers.

Example: You are setting up a new workstation in an office, you need to connect a new computer to an existing network that has a central switch, Use an Ethernet patch cable to connect the new computer to the network switch.

Steps: Identify an available port on the network switch, Plug one end of the Ethernet cable into this port, Connect the other end of the cable to the Ethernet port on the new computer.

3. Tagging

Tagging in networking involves adding metadata or identifiers to network packets to manage and differentiate traffic. This metadata helps network devices understand and properly handle the packets based on their tags.

The purpose of tagging is to provide additional information about the packets for routing and processing, another purpose is to ensure that network devices handle packets according to their specific attributes or requirements.

Example: Suppose you need to ensure that different types of network traffic (such as data and voice) are handled appropriately by your network devices, You want to manage traffic so that voice and data packets are processed according to their needs.

Set up the network devices (such as switches or routers) to add tags or markers to the packets. For example, you might use QoS (Quality of Service) tags to prioritize voice traffic over regular data traffic.

Network devices will add tags to packets, such as indicating that a packet is high-priority voice traffic.

- **Key Differences between tagging and Patching**

Patching deals with physical connections, establishing how devices are linked together in a network.

Tagging involves adding logical identifiers to packets, helping devices manage and route traffic effectively.

Patching connects network devices to enable physical data transmission.

Tagging helps manage and process data packets based on additional metadata, improving traffic handling and efficiency.

- **Build Design**

Build design involves creating a detailed plan that covers the network's physical and logical aspects, ensuring that all components work together efficiently and securely. This design serves as a roadmap for the implementation and management of the network, helping to ensure that it meets organizational needs and performance standards.

The elements to consider while Build design of network:

- 1. Network Topology Design**

Network topology refers to the arrangement of various elements (links, nodes, etc.) in a computer network. This section includes diagrams and explanations of how different network devices are connected and interact with each other.

Example: A diagram showing a star topology where all computers are connected to a central switch. The design will specify connections, including routers, switches, and endpoints.

- 2. IP Addressing Scheme**

This section details how IP addresses will be assigned across the network. It

includes the plan for subnetting, IP address ranges for different segments, and the assignment of IP addresses to devices.

Example: A table listing IP address ranges for different subnets, such as “192.168.1.0/24 for Office Network” and “192.168.2.0/24 for Guest Network.” It also specifies reserved addresses for routers and servers.

3. Device Configuration

Details on the configuration of network devices such as routers, switches, and firewalls. This includes the setup of IP addresses, VLANs (if applicable), routing protocols, and security settings.

Example: Instructions for configuring a router with an IP address of 192.168.1.1, subnet mask of 255.255.255.0, and specific routing protocols like OSPF or EIGRP.

4. Cabling and Connectivity

Specifies the types of cables and connectors used, along with their routes and connections. This section ensures that all devices are properly interconnected.

Example: A schematic showing the paths for Ethernet cables, including connections between switches and computers, and any necessary patch panels or cable management systems.

5. Security Measures

Outlines the security protocols and measures to be implemented in the network. This includes firewall rules, access controls, and encryption standards.

Example: Details on setting up firewall rules to block unauthorized access, configuring VPNs for secure remote access, and implementing network segmentation for sensitive data protection.

6. Redundancy and Failover

Plans for ensuring network reliability and availability. This includes redundant connections, backup systems, and failover strategies to maintain network functionality in case of device or link failures.

Example: A plan for redundant internet connections with failover mechanisms, such as a backup ISP, and details on implementing redundant power supplies for critical network devices.

7. Performance Considerations

Addresses the performance requirements of the network, including bandwidth, latency, and Quality of Service (QoS) configurations to prioritize critical applications.

Example: Specifications for bandwidth allocation and QoS policies to ensure that video conferencing and VoIP traffic receive higher priority compared to regular data traffic.

8. Documentation and Maintenance

Provides guidance on documenting the network configuration and maintaining the network. This includes updates, troubleshooting procedures, and contact

information for support.

Example: A maintenance schedule with regular checks and updates, and a troubleshooting guide for common issues, along with contact details for network support personnel.



Practical Activity 1.3.2: Connecting network media



Task:

1: Referring to previous activities (1.3.1) and the key readings 1.3.2., Read the given task. The task should be done **individually**.

As a trainee who has recently studied network labeling, patching, tagging, and network design, you are assigned a project to set up a new office network. The office needs a well-organized and functional network to support its daily operations. Your tasks include labeling network components, connecting them using patching and tagging techniques, and providing a comprehensive network build design.

2: Perform the task by following the instructions related to the task.

3: Ask for clarifications and assistance where needed.

4: Present your work to the trainer and whole class.

6: Perform the task provided in application of learning 1.3



Key readings 1.3.2: Connecting network media

1. Steps and processes for performing labelling, patching, tagging and Build design:

a. Labeling

1. Prepare Labels:

- Obtain a label maker or label stickers.
- Decide on a clear and consistent labeling scheme for all devices and cables (e.g., "Router-01," "Switch-01," "PC-01").

2. Label Devices:

- Label the router, switch, each computer, and network printer with their respective identifiers.
- For instance, stick "Router-01" on the router, "Switch-01" on the switch, and "Printer-01" on the network printer.

3. Label Cables:

- Attach labels to both ends of each Ethernet cable to indicate the devices they connect (e.g., "PC-01 to Switch-01 Port 1").
- Ensure that the labels are easily visible and durable.

4. Documentation:

- Create a labeling chart or document detailing each device's label and its function or connection (e.g., "PC-01" connects to "Switch-01 Port 1").

b. Patching and Tagging

1. Connect Devices:

- Plug one end of an Ethernet patch cable into the network port of each computer and the network printer.
- Plug the other end of the cable into the appropriate port on the switch.

2. Ensure Correct Connections:

- Double-check that each device is connected to the correct port on the switch as per your labeling chart.
- For instance, connect "PC-01" to Port 1 on "Switch-01," and "PC-02" to Port 2.

3. Tag Network Connections:

- If applicable, add tags or identifiers to network ports on the switch and router.
- Ensure tags correspond with your documentation for easy identification.

4. Verify Connectivity:

- Ensure that each device can establish a connection through the switch.
- Test connectivity by checking that each computer can communicate with the network printer and other devices.

3. Build Design

1. Create Network Topology Diagram:

- Draw a visual representation of the network layout, showing the router at the center, connected to the switch, which in turn connects to each computer and the network printer.
- Use network design software or manual drawing for this purpose.

2. Develop IP Addressing Scheme:

- Allocate IP addresses to each device based on the subnet. For example:
 - Router: 192.168.1.1
 - PC-01: 192.168.1.2
 - PC-02: 192.168.1.3
 - Printer: 192.168.1.4
- Document the IP address for each device in your design.

3. Document Cabling and Connectivity:

- Create a detailed diagram showing how cables are routed between devices.
- Include information on cable lengths, types, and connection points.

4. Write Configuration Instructions:

- Prepare detailed instructions for configuring the router and switch:
 - Router configuration (e.g., setting IP address 192.168.1.1, configuring DHCP if needed).
 - Switch configuration (e.g., setting up ports, VLANs if required).

5. Include Security and Maintenance Guidelines:

- Document recommended security settings (e.g., setting up firewall rules, access controls).
- Outline maintenance procedures (e.g., regular checks, firmware updates).

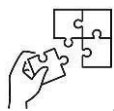
6. Review and Finalize:

- Review all documentation and designs for accuracy.
- Make sure that all devices are correctly labeled, connected, and configured as per the build design.



Points to Remember

- **Labelling** in Networking refers to the practice of assigning identifiable names or tags to network components, connections, and configurations to facilitate management, troubleshooting, and documentation. This can include: Cable Labelling, Device Labelling, Port Labelling, Patch Panel Labelling.
- **Patching** in networking refers to the physical process of connecting network devices or segments using cables. This step involves creating connections between various network components such as switches, routers, servers, and computers.
- **Tagging** in networking involves adding metadata or identifiers to network packets to manage and differentiate traffic. This metadata helps network devices understand and properly handle the packets based on their tags.
- **Build design** involves creating a detailed plan that covers the network's physical and logical aspects, ensuring that all components work together efficiently and securely. This design serves as a roadmap for the implementation and management of the network, helping to ensure that it meets organizational needs and performance standards.
- Steps and processes for performing **labelling, patching, tagging and Build design**



Application of learning 1.3.

A new office is opening near your school, the office needs an installed network for communication. Your task involves labelling all network cables connected to the following components, including the router, switch, computers, and printer, to ensure easy identification and management, then after perform patching and tagging each network connection, using labelled Ethernet cables to connect devices to the switch, and verify that all connections are functional.



Learning outcome 1 end assessment

Written assessment

Practical assessment

XYZ Hospital want to install network infrastructure to improve efficiency, patient care, and staff communication. The hospital's operations struggle with communication between staffs and patients. The hospital has hired a professional networking company to implement the installation, ensuring all departments and critical equipment are connected to a secure, high-speed network, with minimal disruption to hospital operations. As one of the technicians from networking company, you are asked to identify and select tools, materials and equipment, install trunks and terminate cables accordingly, and finally connect all the network media for the devices.

END



Reference

Books:

Kurose, J. F., & Ross, K. W. (2017). *Computer networking: A top-down approach*. Boston: Pearson.

Odom, W. (2020). *CCNA 200-301 official cert guide*. Indianapolis: Cisco Press.

Rathbone, A. (2018). *Networking all-in-one for dummies*. Hoboken: Wiley.

Web links :

CableOrganizer. (n.d.). How to terminate RJ45. CableOrganizer. Retrieved from <https://www.cableorganizer.com/learning-center/how-to/how-to-terminate-RJ45.php>

FS Community. (n.d.). Network communication cables that power your internet. FS Community. Retrieved from <https://community.fs.com/article/network-communication-cables-that-power-your-internet.html>

Lehr, W. (2016). Network requirements. In L. Peterson & B. Davie, *Computer Networks: A Systems Approach* (pp. 1-15). Retrieved from <https://book.systemsapproach.org/foundation/requirements.html>

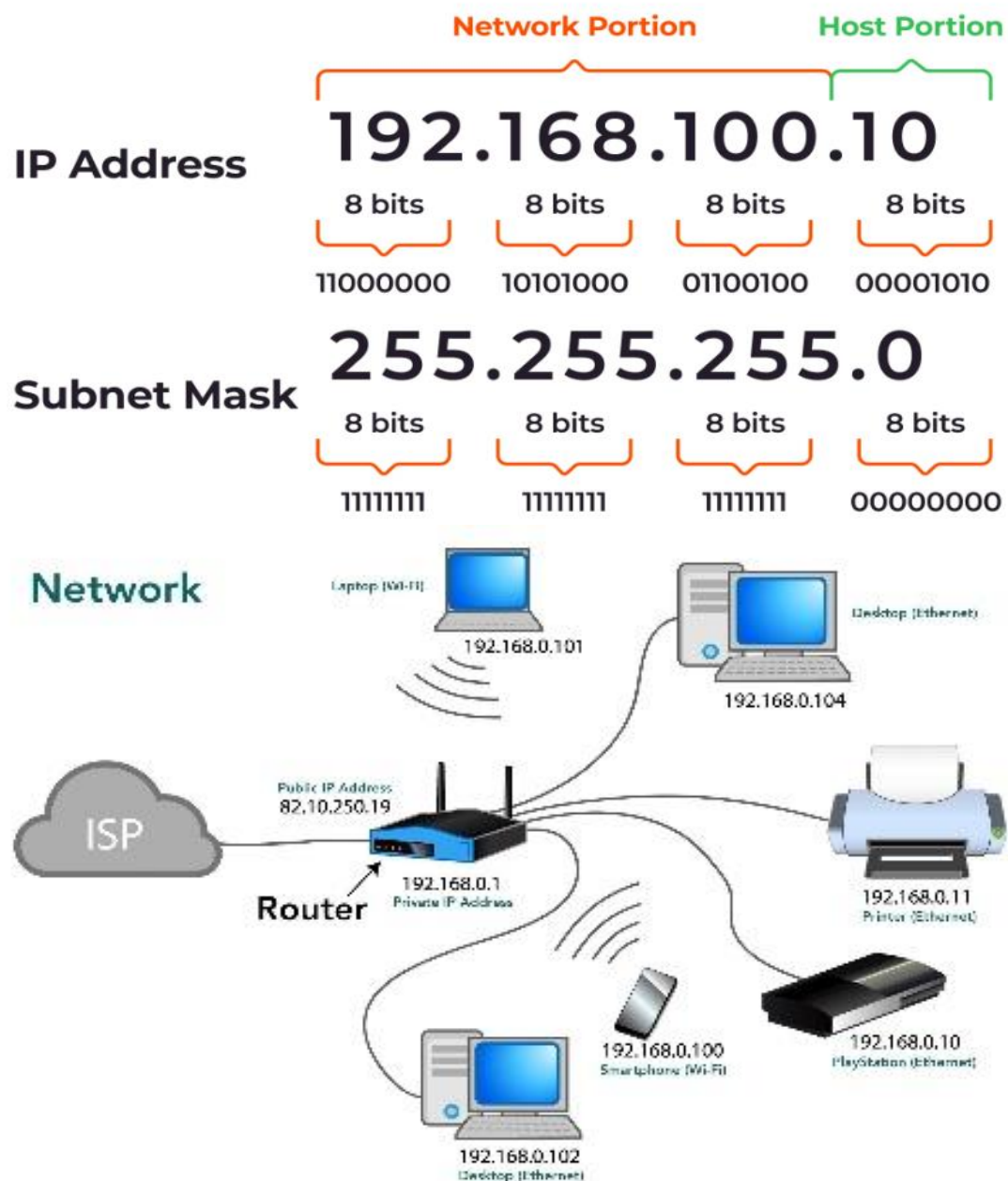
NIBusinessInfo. (n.d.). Assess your networking needs and requirements. NIBusinessInfo.co.uk. Retrieved from <https://www.nibusinessinfo.co.uk/content/assess-your-networking-needs-and-requirements>

Oracle. (n.d.). Determining network requirements. In *Deployment Planning Guide*. Retrieved from https://docs.oracle.com/cd/F26413_51/books/DeplmtPlan/c-Determining-Network-Requirements-xo1030684.html

The Network Installers. (n.d.). Network installation requirements. The Network Installers. Retrieved from <https://thenetworkinstallers.com/blog/network-installation-requirements/>

VCELink. (2021, November 5). How to terminate ethernet cable. VCELink Blog. Retrieved from https://www.vcelink.com/blogs/focus/how-to-terminate-ethernet-cable?srsltid=AfmBOoqByC3Mi1XPhKAI3iM98yLJN95LBv_nW7oSG5o_doHDqfaDicsC

Learning Outcome 2: Perform Basic Network Configuration.



Indicative contents

- 2.1 Classification of IP Addresses.
- 2.2 Calculation of IP addresses subnet masks.
- 2.3 Assigning IP Address.
- 2.4 Configuration of Basics Network Device.
- 2.5 Testing network Interconnection.

Key Competencies for Learning Outcome 2: Perform Basic Network Configuration.

Knowledge	Skills	Attitudes
<ul style="list-style-type: none">● Describe IP Addressing● Identify Principles of subnetting● Describe basics of network device● Describe network interconnection testing	<ul style="list-style-type: none">● Assign and configure IP addresses on devices● Configure basics network devices● Perform Subnetting● Perform network interconnection testing	<ul style="list-style-type: none">● Having Curiosity● Being Patient● Having Persistence● Being a Critical Thinker● Having attention to Detail● Being adaptive● Having Ethical Behaviour● Being a Continuous Learner● Having Empathy● Having Security Consciousness.



Duration: 35 hrs



Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Classify accurately the IP Addresses in accordance with network requirements.
2. Calculate precisely the IP address subnet masks based on the network topology.
3. Assign correctly the IP Addresses to devices in accordance with network topology.
4. Configure effectively the basic network devices based on manufactures' guide.
5. Test correctly the network interconnection in accordance with network Functionalities.



Resources

Equipment	Tools	Materials
<ul style="list-style-type: none">• Computer• Inverter• Battery• UPS• Router• Switch	<ul style="list-style-type: none">• Networking toolkit• Drilling tools• Fixing tool• Testing tools	<ul style="list-style-type: none">• Network cables• Connectors• Flexible PIPE Cables• Cables Ties• Cables clips



Indicative content 2.1: Classification of IP Addresses



Duration: 7 hrs



Theoretical Activity 2.1.1: Description of IP address configuration



Tasks:

- 1: You are asked to answer the following questions related to the classification of IP address.
 - a. Define an IP Address.
 - b. Explain the types of IP Addresses.
 - c. Describe the IP address versions.
 - d. Explain the IP address classes.
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class
- 4: For more clarification, read the **key readings 2.1.1**.
- 5: In addition, ask questions where necessary.



Key readings 2.1.1.: Description of IP address configuration

1. Classification of IP Addresses

1.1. IP Address Definition

- ✓ An **IP Address (Internet Protocol Address)** is a unique numerical identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication. This address serves two main purposes: identifying the host or network interface and providing the location of the device in the network. IP addresses are essential for enabling devices, such as computers, smartphones, servers, and other networked equipment, to send and receive data across the network, ensuring that the data reaches the correct destination.
- ✓ **Internet Protocol (IP)** is a set of rules and standards that govern how data is transmitted across networks, particularly the internet. It is one of the core protocols in the Internet Protocol Suite, often referred to as the TCP/IP suite. The primary purpose of IP is to deliver packets of data from the source device to the destination device based on their IP addresses.

1.2. Types of IP Addresses

IP addresses are categorized into several types based on their scope, visibility, and

specific use cases. The main types of IP addresses are:

1. Private IP Address

Private IP addresses are used within private networks, such as in homes, offices, or organizations. These addresses allow devices within the same local network to communicate with each other but are not directly accessible from the internet. Private are being used inside a network.

Examples:

- ✓ **192.168.1.1**: A common IP address used for routers within a home network.
- ✓ **10.0.0.1**: Often used in larger networks, like in offices or enterprises.

2. Public IP Address

Public IP addresses are used for devices that need to communicate over the internet. These addresses are globally unique and are assigned by Internet Service Providers (ISPs). They allow devices to be accessed directly from any other device on the internet.

Examples:

- ✓ **8.8.8.8**: The IP address of Google's public DNS server.
- ✓ **216.58.217.206**: An IP address used by one of Google's web servers.

Note: The public and private IP addresses are indicative of the location of the network.

3. Static IP Address

A static IP address is a fixed IP address manually configured and assigned to a device. Unlike dynamic IP addresses, static IPs do not change over time, making them ideal for servers, network devices, and services that need a consistent address for access.

Examples:

- ✓ **203.0.113.10**: A static IP address used by a company's web server.
- ✓ **198.51.100.25**: A static IP address assigned to a corporate mail server.

4. Dynamic IP Address

Dynamic IP addresses are automatically assigned to devices by a DHCP (Dynamic Host Configuration Protocol) server. These addresses may change over time as devices connect and disconnect from the network. Dynamic IPs are commonly used for personal devices like laptops, smartphones, and home computers.

Examples:

- ✓ **192.168.1.105**: A dynamically assigned IP address to a laptop in a home network.
- ✓ **172.20.10.7**: A dynamic IP assigned to a smartphone connected to a Wi-Fi network.

5. Loopback IP Address

Loopback IP addresses are special IP addresses used by a device to communicate with itself. They are commonly used for testing and development purposes to ensure that the IP stack on the device is working correctly.

Examples:

- ✓ **127.0.0.1:** The loopback IP address in IPv4, often referred to as "localhost."
- ✓ **::1:** The loopback address in IPv6.

6. Multicast IP Address

Multicast IP addresses are used to send data to multiple devices simultaneously. They are typically used in applications like streaming video or audio, where data needs to be sent to a group of devices.

Examples:

- ✓ **224.0.0.1:** A multicast IP address used to send data to all hosts on a local network.
- ✓ **239.255.255.250:** A multicast address used by the Simple Service Discovery Protocol (SSDP) in UPnP (Universal Plug and Play) devices.

7. Broadcast IP Address

A broadcast IP address is used to send data to all devices within a specific network segment. It allows for one-to-all communication within a network.

Examples:

- ✓ **192.168.1.255:** The broadcast address for the network 192.168.1.0/24, sending data to all devices in that subnet.

1.3. IP address versions

IP address versions refer to the main formats or protocols used for assigning addresses to devices on a network.

There are two main versions of IP (Internet Protocol) addresses in use today: **IPv4** and **IPv6**. These versions differ in their address formats, capabilities, and the number of addresses they can provide.

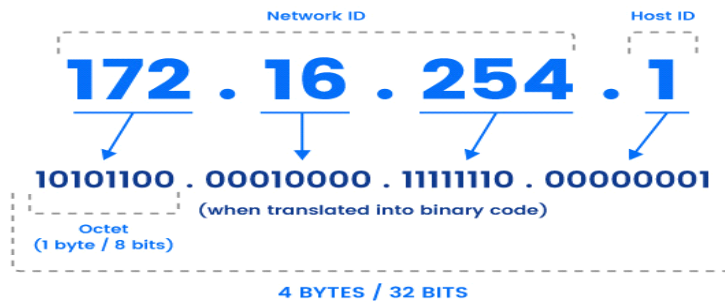
1. IPv4 (Internet Protocol version 4)

IPv4 is the fourth version of the Internet Protocol and the most widely used. It was developed in the early 1980s and is still the dominant protocol for most internet traffic today.

Address Format:

- ✓ **32-bit Address:** IPv4 uses a 32-bit address scheme, which allows for approximately 4.3 billion unique addresses (2^{32}).
- ✓ **Dotted Decimal Notation:** IPv4 addresses are typically written in a format known as dotted decimal notation, where the address is divided into four 8-bit octets, each represented by a decimal number and separated by periods (dots). For example, 192.168.1.1.

IPv4 Address Format (Dotted-Decimal Notation)



Advantages of IPv4

- ✓ **Widespread Adoption:** It is the most widely used internet protocol, ensuring broad compatibility across devices, networks, and services.
- ✓ **Simplicity:** IPv4 uses a straightforward, easy-to-read dotted decimal address format, making it easier to manage and understand.
- ✓ **Extensive Support:** With a long history, IPv4 has abundant documentation, tools, and resources, making network management and troubleshooting easier.
- ✓ **Efficiency for Small Networks:** IPv4's address space is adequate for smaller networks, and it supports Network Address Translation (NAT) to manage address shortages effectively.

Limitations:

- ✓ **Address Exhaustion:** With the rapid growth of the internet and the proliferation of devices, the pool of available IPv4 addresses has become insufficient. This shortage led to the development of IPv6.

2. IPv6 (Internet Protocol version 6)

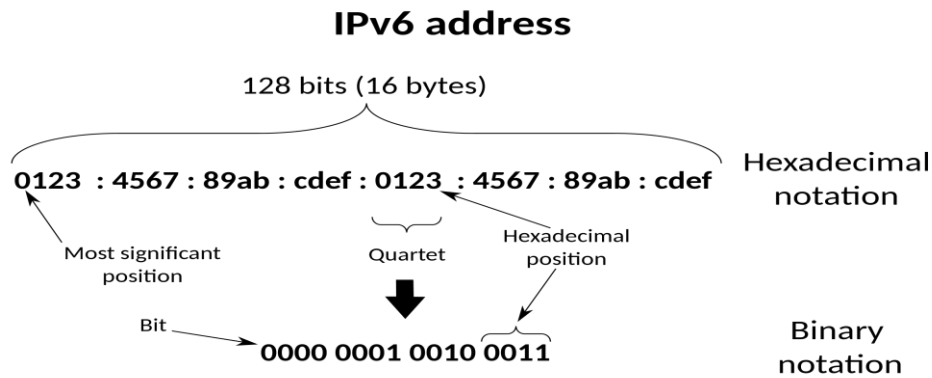
IPv6 is the successor to IPv4, developed to address the limitations of IPv4, particularly the exhaustion of available IP addresses. It was introduced in the late 1990s and has been gradually adopted alongside IPv4.

Address Format:

- ✓ **128-bit Address:** IPv6 uses a 128-bit address scheme, allowing for a virtually unlimited number of unique addresses (2^{128}), which is 340 undecillion addresses (340 followed by 36 zeros).
- ✓ **Hexadecimal Notation:** IPv6 addresses are written in eight groups of four hexadecimal digits, separated by colons. Leading zeros in each group can be omitted, and consecutive groups of zeros can be replaced with a double colon (::) for simplicity.

Example:

- ✓ **2001:0db8:85a3:0000:0000:8a2e:0370:7334:** A typical IPv6 address.
- ✓ **::1:** The loopback address in IPv6, equivalent to 127.0.0.1 in IPv4.



Advantages:

- ✓ **Larger Address Space:** IPv6's vast address space accommodates the growing number of internet-connected devices, including IoT (Internet of Things) devices.
- ✓ **Built-in Security:** IPv6 was designed with security features like IPsec (Internet Protocol Security) as a fundamental component.
- ✓ **Simplified Header Structure:** IPv6 has a simplified header structure compared to IPv4, which improves routing efficiency.
- ✓ **Auto-configuration:** IPv6 supports both stateful (e.g., DHCPv6) and stateless address configuration, making network management easier.

Difference between IPv4 vs IPv6

Both IPv4 and IPv6 identify connected devices on the network. However, there are slight differences in the way they operate. IPv6 is the newer IP version and was introduced to address the limitations IPv4 posed on the availability of IP addresses.

The following is a list of differences between IPv4 and IPv6:

- ✓ IPv4 is 32-bit, whereas IPv6 is 128-bit.
- ✓ In IPv4, binary bits are separated by a dot (.); IPv6 separates binary bits by a colon (:).
- ✓ IPv4 follows the numeric addressing method and IPv6 is alphanumeric.
- ✓ IPv4 offers 12 header fields and IPv6 offers eight header fields.
- ✓ IPv4 has checksum fields but IPv6 doesn't.
- ✓ IPv4 supports broadcast address, which is a type of special address that transmits data packets to every node on the network. IPv6 doesn't support broadcast, but instead uses a multicast address, which is a logical identifier for a collection of hosts on a network.
- ✓ IPv4 supports Variable Length Subnet Mask, but IPv6 doesn't.

1.4. Identification of IP address classes

IP addresses are divided into five different classes (A, B, C, D, and E) based on the

first few bits of the address, which determine the range of the network and host portions. These classes were created to accommodate networks of different sizes.

Class A

Class A addresses are designed for very large networks. They use a 32-bit address space where the first octet (8 bits) specifies the network, and the remaining 24 bits are used for host addresses. This format allows for 128 possible networks, though technically only 126 are usable since 0.0.0.0 is reserved for the default network and 127.0.0.0 is reserved for loopback tests. Each network in Class A can support approximately 16.7 million hosts, making it suitable for large organizations or ISPs that require a vast number of IP addresses. The addresses in Class A range from 1.0.0.0 to 126.0.0.0, and an example is 10.0.0.1, often used in private networks.

Class B

Class B addresses are intended for medium-sized networks. They allocate the first 16 bits (two octets) of the address for network identification, and the remaining 16 bits for host addresses. This structure supports about 16,384 possible networks and allows for up to 65,534 hosts per network. Class B addresses range from 128.0.0.0 to 191.255.0.0. This class is ideal for organizations like universities or large businesses that need a moderate number of addresses. An example of a Class B address is 172.16.0.1, frequently used in private networks.

Class C

Class C addresses are used for smaller networks. They reserve the first 24 bits (three octets) for network identification, leaving only 8 bits for host addresses. This configuration supports around 2 million possible networks but limits each network to 254 hosts. The address range for Class C is 192.0.0.0 to 223.255.255.0. This class is commonly employed in small business or home networks where a large number of networks are needed but each network needs only a few hosts. A typical Class C address example is 192.168.1.1, often seen in private home networks.

Class D

Class D addresses are designated for multicast purposes, rather than traditional network or host assignments. They use the address range from 224.0.0.0 to 239.255.255.255. The first four bits of a Class D address are set to 1110, which identifies the address as a multicast address. This class enables a single packet to be sent to multiple destinations simultaneously, which is useful for applications like streaming media or conference calls. An example of a multicast address is 224.0.0.1, used for local network multicast groups.

Class E

Class E addresses are reserved for experimental or future use and are not typically used in regular networking. They span the range from 240.0.0.0 to 255.255.255.255, with the first four bits set to 1111. This class was set aside for research purposes and potential future applications, with the intention of providing a pool of addresses for experimental protocols or innovations. Since they are not used in standard IP communication, there are no typical use cases or examples for Class E addresses.

The table summarizes the IP address classes and their features:

Class	Address Range	First Octet	Network Portion	Host Portion	Number of Networks	Hosts per Network	Purpose
A	1.0.0.0 to 126.0.0.0	0xxxxxxx	8 bits	24 bits	128 (126 usable)	~16.7 million	Very large networks, e.g., ISPs
B	128.0.0.0 to 191.255.0.0	10xxxxxxx	16 bits	16 bits	16,384	~65,534	Medium-sized networks, e.g., universities
C	192.0.0.0 to 223.255.255.0	110xxxxxx	24 bits	8 bits	~2 million	254	Small networks, e.g., home networks
D	224.0.0.0 to 239.255.255.255	1110xxxx	Not used	Not used	N/A	N/A	Multicasting
E	240.0.0.0 to 255.255.255.255	1111xxxx	Reserved	Reserved	N/A	N/A	Experimental, future use



Practical Activity 2.1.2: Configuration of IP Address



Task:

1: Referring to previous activities (2.1.1) and key readings 2.1.2., Read the given task.

As a trainee who studied IP address configuration and network setup, you are tasked to configure the IP Addresses of a small office network for a new department. The office consists of four computers, one network printer, switch and a router to manage the internal network. You need to configure the IP addresses for each device, set up the router, and verify that all devices can communicate with each other.

2: Perform the given task by following instructions related to the task.

3: Ask more clarifications if any and assistance where needed.

4: Present your work to the trainer and whole class.

5: Read key reading (2.1.2) and ask clarification where necessary.

6: Perform the task provided in application of learning 2.1



Key readings 2.1.2: Configuration of IP Address

Steps to Configure IP Addresses in Cisco Packet Tracer

1. Set Up the Network Topology

- a. **Open Cisco Packet Tracer** and create a new project.
- b. **Drag and Drop** the devices you need onto the workspace: Routers, Switches, PCs, Servers and Printers, etc.

2. Connect the Devices

- a. **Select the Cable Type:**
 - **Copper Straight-Through:** For connecting devices to switches and routers.
 - **Copper Crossover:** For connecting similar devices directly (usually not needed with modern switches and routers).
- b. **Connect Devices:**
 - Use the **Connections** tool (lightning bolt icon) to drag and drop cables between devices.

3. Configure the Router

- a. **Access Router Configuration:**

Click on the **Router**.

Go to the **CLI** tab for command-line configuration.
- b. **Enter Configuration Mode:**

Type enable to enter privileged EXEC mode.

Type configure terminal to enter global configuration mode.

c. Configure Interface IP Address:

- ✓ Identify the interface you want to configure (e.g., GigabitEthernet0/0).
- ✓ Enter interface configuration mode:

Router(config)# interface gig0/0

- ✓ Assign an IP address and subnet mask:

Router(config-if)# ip address [IP_ADDRESS] [SUBNET_MASK]

- ✓ Activate the interface:

Router(config-if)# no shutdown

- ✓ Exit the interface configuration mode:

Router(config-if)# exit

d. Save Configuration:

- ✓ Save the configuration to the router's startup configuration:

Router# write memory

4. Configure the Switch (Optional)

a. Access Switch Configuration:

- Click on the **Switch**.
- Go to the **CLI** tab.

b. Enter Configuration Mode:

- Type enables to enter privileged EXEC mode.
- Type configure terminal to enter global configuration mode.

c. Configure VLAN Interface IP Address (For management):

- Enter VLAN interface configuration mode:

Switch(config)# interface vlan 1

- Assign an IP address and subnet mask:

Switch(config-if)# ip address [IP_ADDRESS] [SUBNET_MASK]

- Activate the interface:

Switch(config-if)# no shutdown

- Exit the configuration mode:

Switch(config-if)# exit

d. Save Configuration:

- Save the configuration:

Switch# write memory

5. Configure IP Addresses on PCs

a. Access PC Configuration:

- Click on the **PC**.
- Go to the **Desktop** tab.
 - Select **IP Configuration**.

b. Assign IP Address:

Enter the IP address, subnet mask, and default gateway for the PC:

- **IP Address:** The unique IP address for the PC.
- **Subnet Mask:** Typically 255.255.255.0 for most small networks.
- **Default Gateway:** The IP address of the router's interface connected to the PC's network.

c. Apply Configuration:

- Click on **Save** or **Close** to apply the configuration.

6. Verify Connectivity

a. Ping Test:

- Use the **Command Prompt** on a PC to test connectivity to other devices:
ping [DESTINATION_IP]

b. Check Router and Switch Interfaces:

- On the **Router**, use:
Router# show ip interface brief
- On the **Switch**, use:
Switch# show ip interface brief

c. Verify Routing (if applicable):

- Check routing tables if configuring multiple routers:
Router# show ip route

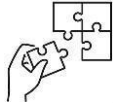
By following these steps, you can configure IP addresses for devices in Cisco Packet Tracer, set up your network, and verify that all devices can communicate effectively. This process helps ensure that your network is properly configured and operational.



Points to Remember

- An **IP Address (Internet Protocol Address)** is a unique numerical identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- The main types of IP addresses are:
 - ✓ **Private IP Address** that used within private networks,
 - ✓ **Public IP Address** that used for devices that need to communicate over the internet.
 - ✓ **Static IP Address** is a fixed IP address manually configured and assigned to a device.
 - ✓ **Dynamic IP Address** that are automatically assigned to devices by a DHCP (Dynamic Host Configuration Protocol) server.
 - ✓ **Loopback IP Address** are special IP addresses used by a device to communicate with itself.
 - ✓ **Multicast IP Address** are used to send data to multiple devices simultaneously.
 - ✓ **Broadcast IP Address** is used to send data to all devices within a specific network segment.

2. **IP address versions:** There are two main versions of IP (Internet Protocol) addresses in use today: **IPv4** and **IPv6**.
3. **Identification of IP address classes:** IP addresses are divided into five different classes (A, B, C, D, and E) based on the first few bits of the address, which determine the range of the network and host portions.
4. **Steps to Configure IP Addresses in Cisco Packet Tracer**
 1. Set Up the Network Topology
 2. Connect the Devices
 3. Configure the Router
 4. Configure the Switch (Optional)
 5. Configure IP Addresses on PCs
 6. Verify Connectivity



Application of learning 2.1.

In ICT Company, a new office is opening with four computers, one network printer, a switch, and a router. As a network technician assigned to this branch, you are tasked with configuring the IP addresses for all network devices. You need to set up the router with the correct IP address scheme, configure each computer and the network printer with appropriate IP addresses, and ensure that all devices are connected through the switch. After configuration, you will need to verify that all devices can communicate with each other and confirm that network services are functioning correctly.



Indicative content 2.2: Calculation of IP addresses subnet masks



Duration: 7 hrs



Theoretical Activity 2.2.1: Description of IP address subnet masks



Tasks:

- 1: Read and answer the following questions related to the description of site survey
 - i. What are subnet masks
 - ii. What are the Benefits of subnetting
 - iii. Discuss on Binary system
 - iv. What are the Types of Subnetting
 - v. Explain Logical and bitwise Operators
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class
- 4: For more clarification, read the **key readings 2.2.1**.
- 5: In addition, ask questions where necessary.



Key readings 2.2.1.: Description of IP address subnet masks

1. Calculation of IP addresses subnet masks

1.1. Introduction to Subnet Masks

A subnet mask is a fundamental concept in networking used to divide an IP address into its network and host components. It determines which portion of an IP address identifies the network and which part identifies the individual device (host) within that network.

A **subnet mask** is a 32-bit address that accompanies an IP address to specify which part of the IP address refers to the network and which part refers to the host within that network. It is used in conjunction with an IP address to create a network segment, making it easier to manage and organize network traffic.

Format: A subnet mask is expressed in the same format as an IP address, consisting of four octets (e.g., 255.255.255.0).

Binary Representation: In binary form, the subnet mask consists of a series of contiguous 1s followed by contiguous 0s. The 1s identify the network portion, and the 0s identify the host portion.

Example:

For the IP address 192.168.1.10 with a subnet mask of 255.255.255.0:

- **Subnet Mask (Binary):** 11111111.11111111.11111111.00000000
 - **Network Portion:** Defined by the 1s in the subnet mask.
 - **Host Portion:** Defined by the 0s in the subnet mask.
- **Benefits of subnetting**
 1. **Improved Network Organization:** Simplifies network management by dividing it into smaller, manageable subnets.
 2. **Enhanced Security:** Isolates network segments to control and limit security threats.
 3. **Efficient IP Use:** Optimizes IP address allocation and reduces wastage.
 4. **Better Performance:** Reduces broadcast traffic, minimizing network congestion.
 5. **Scalability:** Facilitates network growth by allowing flexible subnet additions.
 6. **Simplified Routing:** Streamlines routing and reduces complexity in routing tables.
 7. **Effective Troubleshooting:** Improves network monitoring and problem isolation.
 8. **Compliance:** Helps meet regulatory requirements for data and network segmentation.

1.2. Binary System

The binary system is a method of representing numbers using only two digits: 0 and 1. It is the foundation of all digital systems, including computers, where it is used to perform calculations, store data, and manage operations.

The binary system is integral to subnetting because IP addresses are expressed in binary form. An IP address, such as 192.168.1.0, is represented in binary as 11000000.10101000.00000001.00000000. Subnetting involves manipulating these binary digits to divide a larger network into smaller subnets.

For example, the subnet mask 255.255.255.0 corresponds to 11111111.11111111.11111111.00000000 in binary. By adjusting the number of binary digits assigned to the network and host portions of the address, different subnet masks are created, defining the boundaries of each subnet.

1.3. Types of Subnetting

1. Fixed-Length Subnet Mask (FLSM):

FLSM is used when each subnet in a network requires the same number of IP addresses. This method involves using a consistent subnet mask across all subnets, which simplifies network management but may lead to inefficiencies in IP address utilization.

Example: With a network 192.168.1.0/24, applying a /26 subnet mask (255.255.255.192 in decimal or 11111111.11111111.11111111.11000000 in binary) creates four subnets, each with 64 IP addresses.

2. Variable-Length Subnet Mask (VLSM):

VLSM allows for different subnet sizes within the same network by using

different subnet masks. This flexibility optimizes IP address allocation, ensuring that each subnet has exactly the number of addresses needed.

Example: Starting with 192.168.1.0/24, you might use a /25 mask for one large subnet and /27 masks for smaller subnets, efficiently using the available IP space.

1.4. Logical and Bitwise Operators in Subnetting

Logical and bitwise operators are used to perform calculations when subnetting, particularly in determining network and broadcast addresses.

1. AND Operator:

The bitwise AND operator is used to calculate the network address by applying the subnet mask to an IP address. It compares each bit of the IP address and the subnet mask; if both bits are 1, the resulting bit is 1, otherwise, it is 0.

Example: To find the network address of 192.168.1.10 with a subnet mask of 255.255.255.0:

11000000.10101000.00000001.00001010 (IP Address)	11000000.10101000.000001.00001010	\backslash (\text{IP Address})
11111111.11111111.11111111.00000000 (Subnet Mask)	11111111.11111111.11111111.00000000	\backslash (\text{Subnet Mask})
11000000.10101000.00000001.00000000 (Network Address)	11000000.10101000.00000001.00000000	\backslash (\text{Network Address})

2. OR Operator:

The bitwise OR operator is used to calculate the broadcast address. By OR-ing the IP address with the inverted subnet mask, you can find the broadcast address for the subnet.

Example: If the subnet mask is 255.255.255.0, its binary complement (inverted bits) is 00000000.00000000.00000000.11111111. OR-ing this with the network address gives the broadcast address.



Practical Activity 2.2.2: Calculating IP address subnet masks



Task:

1: Referring to previous activities 2.2.1 and key readings 2.2.2, Read the task below.

As a trainee who studied subnet mask, You are tasked to design a network for a small office. The office requires 6 subnets to accommodate different departments, and each subnet should be able to support up to 30 devices. You have been given

the IP address range 192.168.1.0/24 to work with. Your goal is to calculate the appropriate subnet mask to meet these requirements.

- 2: Perform the task by following the instructions related to the task.
- 3: Ask more clarifications if any and assistance if needed.
- 4: Present your work to the trainer and whole class.
- 5: Read key reading (2.2.2) and ask clarification where necessary.
- 6: Perform the task provided in application of learning 2.2



Key readings 2.2.2: Calculating IP Address subnetmask

Steps to Calculate the Subnet Mask

Calculating a subnet mask in networking involves a series of activities that allow you to divide a larger network into smaller, more manageable sub-networks (subnets). This process helps optimize the allocation of IP addresses and improves network performance. The key activities to be done when calculating a subnet mask are:

1. Determine the Requirements

- **Understand the Network Needs:** Identify the number of required subnets and the number of hosts (devices) needed for each subnet.
- **Example:** If you need 6 subnets and each subnet must support up to 30 devices, you need to plan for this in your calculations.

2. Identify the IP Address Range

- **Starting IP Address:** Begin with the given IP address range. This could be something like 192.168.1.0/24.
- **Class Identification:** Determine the class of the IP address to understand the default subnet mask. For example, 192.168.1.0 is a Class C address with a default subnet mask of 255.255.255.0.

3. Calculate the Number of Required Subnet Bits

- **Formula:** Use the formula $2^n \geq \text{Number of Subnets}$, where n is the number of bits you need to borrow from the host portion to create the required subnets.
- **Example:** To create 6 subnets, find the smallest n where $2^n \geq 6$. Here, $n = 3$ because $2^3 = 8$, which is greater than or equal to 6.

4. Determine the Subnet Mask

- **Modify the Default Subnet Mask:** Extend the default subnet mask by adding the number of bits calculated in the previous step to the network portion.
- **Example:** Starting with the default Class C subnet mask 255.255.255.0 (or /24 in CIDR notation), add 3 bits to the network portion, resulting in 255.255.255.224 (or /27 in CIDR).

5. Calculate the Subnet Addresses

- **Determine Subnet Blocks:** Divide the network into blocks based on the new subnet mask. Calculate the first IP address of each subnet by incrementing the previous subnet's starting address by the size of the subnet.
- **Example:** With a subnet mask of /27, each subnet has $2^{(32-27)} = 32$ IP addresses. The subnets will be 192.168.1.0/27, 192.168.1.32/27, 192.168.1.64/27, and so on.

6. Identify Usable IP Ranges

- **Calculate Host Range:** For each subnet, determine the range of usable IP addresses, excluding the network address (first IP) and the broadcast address (last IP).
- **Example:** In the subnet 192.168.1.0/27, the usable IP range is 192.168.1.1 to 192.168.1.30.

7. Verify Network and Broadcast Addresses

- **Network Address:** This is the first address in the subnet and is used to identify the subnet itself.
- **Broadcast Address:** This is the last address in the subnet and is used to communicate with all devices within that subnet.
- **Example:** For the subnet 192.168.1.32/27, the network address is 192.168.1.32, and the broadcast address is 192.168.1.63.

8. Document the Subnets

- **Record Subnet Information:** Document the subnet address, subnet mask, range of usable IP addresses, network address, and broadcast address for each subnet.
- **Example:**

Subnet	Subnet Mask	Usable IP Range	Network Address	Broadcast Address
192.168.1.0	255.255.255.224 (/27)	192.168.1.1 - 192.168.1.30	192.168.1.0	192.168.1.31
192.168.1.32	255.255.255.224 (/27)	192.168.1.33 - 192.168.1.62	192.168.1.32	192.168.1.63

9. Implement and Verify Subnets

- **Configure Devices:** Assign the calculated IP addresses and subnet masks to the devices in each subnet.
- **Test Connectivity:** Verify that devices within the same subnet can communicate with each other and that devices in different subnets communicate via routing protocols as expected.

10. Review and Adjust as Needed

- **Review Allocations:** Ensure that each subnet is correctly sized and addresses

are efficiently utilized.

- **Make Adjustments:** If necessary, adjust the subnet sizes or create additional subnets to meet changing network requirements.

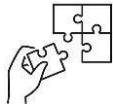
These steps are fundamental to designing a well-structured network, ensuring optimal use of IP address space, and enabling efficient network management.



Points to Remember

- **A subnet mask** is a fundamental concept in networking used to divide an IP address into its network and host components. It determines which portion of an IP address identifies the network and which part identifies the individual device (host) within that network.
- A **subnet mask** is a 32-bit address that accompanies an IP address to specify which part of the IP address refers to the network and which part refers to the host within that network. It is used in conjunction with an IP address to create a network segment, making it easier to manage and organize network traffic.
- **Format:** A subnet mask is expressed in the same format as an IP address, consisting of four octets (e.g., 255.255.255.0).
 - **Benefits of subnetting** are Improved Network Organization, Enhanced Security, Efficient IP Use, Better Performance, Scalability, Simplified Routing, Effective Troubleshooting and Compliance.
 - The binary system is a method of representing numbers using only two digits: 0 and 1. It is the foundation of all digital systems, including computers, where it is used to perform calculations, store data, and manage operations.
 - **Types of Subnetting:**
 - ✓ **Fixed-Length Subnet Mask (FLSM):** FLSM is used when each subnet in a network requires the same number of IP addresses.
 - ✓ **Variable-Length Subnet Mask (VLSM):** VLSM allows for different subnet sizes within the same network by using different subnet masks.
- **Logical and Bitwise Operators in Subnetting** are used to perform calculations when subnetting, particularly in determining network and broadcast addresses.
 - ✓ **AND Operator:** The bitwise AND operator is used to calculate the network address by applying the subnet mask to an IP address.
 - ✓ **OR Operator:** The bitwise OR operator is used to calculate the broadcast address.
- **Steps to Calculate the Subnet Mask:**
 1. Determine the Requirements
 2. Identify the IP Address Range
 3. Calculate the Number of Required Subnet Bits

4. Determine the Subnet Mask
5. Calculate the Subnet Addresses
6. Identify Usable IP Ranges
7. Verify Network and Broadcast Addresses
8. Document the Subnets
9. Implement and Verify Subnets
10. Review and Adjust as Needed



Application of learning 2.2.

In Musanze District, a small office is expanding and requires a network redesign to accommodate six different departments, each needing its own subnet. As a network trainee who has studied subnet masks, you are assigned to design the network for this expansion. You are provided with the IP address range 192.168.1.0/24. Your task is to calculate the appropriate subnet mask that will allow for six subnets, each capable of supporting up to 30 devices. You need to create and configure the subnets, ensuring that each department has its own subnet with the required number of IP addresses. After setting up the subnets, verify that each department's network segment is correctly configured and able to support the devices.



Indicative content 2.3: Assigning IP Address



Duration: 7 hrs



Theoretical Activity 2.3.1: Identify IP address assignment



Tasks:

- 1: Read and answer the following question related to the identification of IP address assignment.
 - i. Differentiate Static, Dynamic and Automatic IP Address.
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class
- 4: For more clarification, read the **key readings 2.3.1**.
- 5: In addition, ask questions where necessary.



Key readings 2.3.1.:

1. Static IP Address

A static IP address is a fixed, manually assigned IP address that remains constant over time. It does not change unless manually reconfigured.

Characteristics:

- ✓ **Consistency:** Always the same, providing a stable and consistent address for devices.
- ✓ **Configuration:** Set manually on the device or in the network configuration settings.
- ✓ **Use Cases:** Commonly used for servers, printers, network hardware, and devices requiring a consistent address (e.g., web servers, email servers).

Advantages:

- ✓ **Reliable Access:** Ensures reliable access to network resources or services.
- ✓ **Easier Remote Access:** Simplifies remote access and management since the IP address does not change.
- ✓ **Simplified DNS Configuration:** Easier to configure DNS for services needing a constant address.

Disadvantages:

- ✓ **Administrative Overhead:** Requires manual setup and management, which can be cumbersome for large networks.
- ✓ **Potential for IP Conflicts:** Higher risk of IP conflicts if not managed properly, especially in larger networks.

2. Dynamic IP Address

A dynamic IP address is assigned automatically by a DHCP (Dynamic Host Configuration Protocol) server from a pool of available addresses. It can change over time based on lease duration and server configuration.

Characteristics:

- ✓ **Automatic Assignment:** IP addresses are assigned dynamically when a device connects to the network.
- ✓ **Lease Duration:** Typically assigned for a specific period, after which it may change.
- ✓ **Use Cases:** Common in most client devices, such as computers, smartphones, and tablets, where the network requires flexibility.

Advantages:

- ✓ **Ease of Management:** Requires minimal administrative intervention as IP addresses are assigned and managed automatically.
- ✓ **Efficient IP Address Use:** Addresses are reused efficiently among multiple devices, reducing wastage.
- ✓ **Scalability:** Suitable for large networks with many devices, as it simplifies IP management.

Disadvantages:

- ✓ **Potential for Address Changes:** IP addresses may change over time, which can complicate remote access or network configurations that rely on fixed addresses.
- ✓ **Dependency on DHCP:** Requires a functioning DHCP server for address assignment.

3. Automatic IP Address

Automatic IP addresses are assigned using a protocol such as Automatic Private IP Addressing (APIPA) when a DHCP server is unavailable. These addresses are typically in the range of 169.254.x.x.

Characteristics:

- ✓ **Fallback Mechanism:** Used as a fallback mechanism when a device cannot obtain an IP address from a DHCP server.
- ✓ **APIPA Range:** Typically falls within the 169.254.0.0/16 range.
- ✓ **Use Cases:** Often used in small or ad-hoc networks where devices need to communicate with each other without a DHCP server.

Advantages:

- ✓ **Automatic Configuration:** Automatically assigned without user intervention, useful in the absence of a DHCP server.
- ✓ **Simplicity:** Allows devices to communicate within the same local network even when DHCP is not available.

Disadvantages:

- ✓ **Limited Range:** Only suitable for local communication and does not provide

internet access or network communication beyond the local network.

- ✓ **No Internet Connectivity:** Devices with APIPA addresses cannot access external networks or the internet.

Summary

Type	Description	Advantages	Disadvantages
Static IP Address	Fixed IP address manually assigned and remains constant.	Reliable access, easier remote access, simplified DNS configuration.	Administrative overhead, potential for IP conflicts.
Dynamic IP Address	Automatically assigned by a DHCP server from a pool of addresses and can change over time.	Easy management, efficient use of IP addresses, scalable for large networks.	IP address changes can complicate configurations, requires a functioning DHCP server.
Automatic IP Address	Assigned automatically in the absence of a DHCP server, typically within the 169.254.x.x range using APIPA.	Automatic configuration when DHCP is unavailable, allows local communication.	Limited to local network, no internet access, and not suitable for larger or more complex networks.



Practical Activity 2.3.2: Assigning IP Address



Task:

1: Referring to previous activities 2.3.1 and key readings 2.3.2. Read the following task.

As a networking student who has studied various IP address configurations, you are tasked with setting up a network for a small office. The network needs to support a shared printer with a static IP address, several office computers using dynamic IP addresses, and temporary devices that may rely on automatic IP addressing if the DHCP server is unavailable.

2: Perform the task assigned.

3: Ask more clarifications if any and assistance where needed.

4: Present your work to the trainer and whole class.

5: Read key reading (2.3.2) and ask clarification where necessary.

6: Perform the task provided in application of learning 2.3.



Key readings 2.3.2: Assigning IP Address

Steps for assigning static, dynamic, and automatic IP addresses to the devices in a network:

1. Assign a Static IP Address

- a. **Identify Device:** Determine which device will receive the static IP address (e.g., a network printer, server).
- b. **Choose IP Address:** Select an IP address that is outside the DHCP range to avoid conflicts (e.g., 192.168.1.200).
- c. **Access Device Settings:**
 - For network printers, use the device's control panel or web interface.
 - For other devices, access network settings through the operating system.
- d. **Configure IP Address:**
 - Enter the chosen IP address.
 - Set the subnet mask (e.g., 255.255.255.0).
 - Enter the default gateway (e.g., 192.168.1.1).
 - Optionally, configure DNS servers if needed.
- e. **Save and Apply Settings:** Confirm the configuration and save the settings.
- f. **Verify Connectivity:** Test the device to ensure it is reachable from other devices on the network.

2. Configure Dynamic IP Addressing

- a. **Set Up DHCP Server:**
 - Ensure a DHCP server is operational, typically integrated into a router or dedicated server.
 - Access the DHCP server's configuration interface.
- b. **Define DHCP Scope:**
 - Specify the IP address range that the DHCP server will assign (e.g., 192.168.1.100 to 192.168.1.199).
- Set lease duration if needed.
- c. **Connect Devices:**
 - Connect devices (e.g., computers, printers) to the network.
 - Devices will automatically request and receive an IP address from the DHCP server.
- d. **Verify IP Assignment:**
 - Check that each device receives an IP address within the defined range.
 - Ensure devices can access network resources and communicate with each other.

3. Manage Automatic IP Addressing

- a. **Prepare for Temporary Network:**
 - If the DHCP server is not available, devices will use APIPA to assign themselves IP

addresses in the range 169.254.x.x.

b. **Connect Temporary Devices:**

- Connect devices (e.g., laptops, smartphones) to the network.
- Devices will automatically use APIPA if they cannot obtain an IP address from a DHCP server.

c. **Verify APIPA:**

- Check that devices are assigned IP addresses in the 169.254.x.x range.
- Ensure that devices can communicate with each other within the local network.

d. **Monitor for DHCP Availability:**

- If the DHCP server becomes available, devices will switch to dynamic IP addresses assigned by the DHCP server.



Points to Remember

- **Static IP Address** is a fixed, manually assigned IP address that remains constant over time. It does not change unless manually reconfigured.
- **Dynamic IP Address** is assigned automatically by a DHCP (Dynamic Host Configuration Protocol) server from a pool of available addresses. It can change over time based on lease duration and server configuration.
- **Automatic IP Address** are assigned using a protocol such as Automatic Private IP Addressing (APIPA) when a DHCP server is unavailable. These addresses are typically in the range of 169.254.x.x.
- Steps for configuring static, dynamic, and automatic IP addresses in a network:

1. Assign a Static IP Address

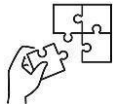
- ✓ Identify Device
- ✓ Choose IP Address
- ✓ Access Device Settings
- ✓ Configure IP Address
- ✓ Save and Apply Settings
- ✓ Verify Connectivity

2. Configure Dynamic IP Addressing

- ✓ Set Up DHCP Server
- ✓ Define DHCP Scope
- ✓ Connect Devices
- ✓ Verify IP Assignment

3. Manage Automatic IP Addressing

- ✓ Prepare for Temporary Network
- ✓ Connect Temporary Devices
- ✓ Verify APIPA
- ✓ Monitor for DHCP Availability



Application of learning 2.3.

In Musanze District, a new smart office building has been established for the district's administrative functions. As a network technician responsible for setting up the network, you are tasked with assigning IP addresses to various devices within the office. The office network includes:

- **Five computers** for staff members.
- **Two network printers.**
- **A Wi-Fi router** providing wireless access to visitors and mobile devices.

Your task is to assign IP addresses to these devices using static for 2 printers and 5 desktop computers of staff members, dynamic (DHCP) for staff telephones and their personal computer (laptops), and provide automatic IP configurations that can be used when DHCP server is down.



Indicative content 2.4: Configuration of Basics Network Device.



Duration: 7 hrs



Theoretical Activity 2.4.1: Describing Basics of network device



Tasks:

- 1: Read and answer the following questions
 - i. Explain Device Configuration Modes.
 - ii. What is Host name in networking?
 - iii. What is Banner message?
 - iv. What is the meaning of Reload Device in networking?
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class
- 4: For more clarification, read the **key readings 2.4.1.**
- 5: In addition, ask questions where necessary.



Key readings 2.4.1.: Describing Basics of network device

1. Device Configuration Modes

Device configuration modes refer to the different states or environments a networking device (such as a router, switch, or firewall) can be in when you're setting it up or managing it. Each mode allows you to perform specific types of configuration tasks.

The common device configuration modes, particularly in the context of Cisco networking devices:

1.1. User EXEC Mode

- ✓ The initial mode you enter when you access a Cisco device.
- ✓ This mode provides basic access to the device, allowing you to view some information but not make any major changes.
- ✓ The command prompt typically ends with a > symbol (e.g., Router>).

Key Features:

- ✓ Limited access: Can view the status but cannot make configuration changes.
- ✓ Commands: Mostly monitoring and basic diagnostics, such as ping, show version, etc.

Example Command:

Router>

1.2. Privileged EXEC Mode

- ✓ Also known as enable mode, this mode allows access to all the commands available in the device.
- ✓ You can perform high-level management tasks, including viewing the running configuration and restarting the device.
- ✓ The command prompt ends with a # symbol (e.g., Router#).

Key Features:

- ✓ Full access: Can view all device settings and perform operational commands.
- ✓ Commands: Includes all User EXEC mode commands plus the ability to enter Global Configuration Mode.

Example Command:

```
Router>enable  
Router#
```

1.3. Global Configuration Mode

- ✓ This mode allows you to make changes to the device's overall configuration.
- ✓ You can configure device-wide settings such as hostname, interfaces, routing protocols, etc.
- ✓ The command prompt changes to Router(config)# to indicate that you are in configuration mode.

Key Features:

- ✓ Central configuration: You can modify the device's main settings.
- ✓ Commands: Includes commands for setting up interfaces, protocols, and device features.

Example Command:

```
Router#configure terminal  
Router(config)#
```

1.4. Interface Configuration Mode

- ✓ A sub-mode of Global Configuration Mode used specifically for configuring individual network interfaces.
- ✓ The command prompt changes to indicate the interface being configured, such as Router(config-if) #.

Key Features:

- ✓ Interface-specific: Configure settings like IP addresses, duplex modes, and speed on a specific interface.
- ✓ Commands: Includes ip address, duplex, speed, and other interface-related commands.

Example Command:

```
Router(config)#interface GigabitEthernet 0/0  
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

1.5. Line Configuration Mode

- ✓ Another sub-mode of Global Configuration Mode, used to configure the settings for various lines such as console, auxiliary, and virtual terminal (VTY) lines.
- ✓ The command prompt changes to Router(config-line)#.

Key Features:

- ✓ Line-specific configuration: Configure access settings for terminal sessions, such as login and password.
- ✓ Commands: Includes password, login, and other line-specific commands.

Example Command:

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
```

1.6. VLAN Configuration Mode

- ✓ A sub-mode used to configure VLANs (Virtual Local Area Networks) on switches.
- ✓ The command prompt changes to Switch(config-vlan)#.

Key Features:

- ✓ VLAN-specific: Configure VLAN IDs, names, and associated parameters.
- ✓ Commands: Includes vlan, name, and other VLAN-related commands.

Example Command:

```
Switch(config)#vlan 10
Switch(config-vlan)#name Sales
```

1.7. Router Configuration Mode

- ✓ A sub-mode of Global Configuration Mode used for configuring routing protocols like OSPF, EIGRP, or BGP.
- ✓ The command prompt changes to indicate the routing protocol being configured, such as Router(config-router)#.

Key Features:

- ✓ Protocol-specific: Set up and manage routing protocols.
- ✓ Commands: Includes network, router-id, passive-interface, etc.

Example Command:

```
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

1.8. ROMMON Mode

- ✓ Short for ROM Monitor mode, this is a special mode used for troubleshooting or recovering a device when it cannot boot normally.
- ✓ The command prompt typically appears as rommon>.

Key Features:

- ✓ Low-level access: Perform recovery tasks such as loading a new IOS image.
- ✓ Commands: Mostly used for device recovery and troubleshooting.

Example Command:

```
rommon 1>confreg 0x2142
```

2. Key elements in configuration of network devices

In network management, configuring key elements such as the hostname, banner messages, and device passwords is essential for maintaining secure and organized operations. Setting the hostname helps identify devices within a network, while banner messages provide important information or warnings to users upon access. Configuring ports ensures proper connectivity and performance, and setting device passwords protects against unauthorized access. Regularly saving configurations and reloading devices as needed ensures that changes are applied and preserved, contributing to a stable and secure network environment. Below are the explanation of the key elements in network configuration with cisco packet tracer.

2.1. Hostname

The hostname is the name assigned to a network device (such as a router, switch, or server) to identify it on a network. It's important for distinguishing one device from another, especially when managing multiple devices within a network.

The purpose of hostname is to makes it easier to identify devices in a network and simplifies network management, especially in large environments.

Example:

```
Router(config)#hostname OfficeRouter
```

```
OfficeRouter(config)#
```

In this example, the router's hostname is set to "OfficeRouter," making it identifiable in the network.

2.2 Banner Message

A banner message is a text message displayed to users when they connect to a network device. It often provides important information or warnings before users access the device.

Types of Banners:

- ✓ **Message of the Day (MOTD):** Displayed to all users upon connection.
- ✓ **Login Banner:** Displayed just before the login prompt.
- ✓ **Exec Banner:** Displayed after a user successfully logs in.

Banner message is often used to display legal disclaimers or usage policies and Can be used to provide general information or reminders to users.

Example:

```
Router(config)#banner motd # Unauthorized access is prohibited. #
```

In this example, users will see the message "Unauthorized access is prohibited." when they attempt to connect to the router.

2.3. Reload Device

Reloading a device means restarting it, which can be necessary after

configuration changes, software updates, or to resolve issues.

The purposes of reload device are **Apply Changes**: Some configurations require a restart to take effect and **Troubleshooting**: Resolves issues by clearing the device's memory and processes.

Example:

```
Router#reload
```

After issuing this command, the router will restart, and all settings that have been saved will be applied.

2.4. Configure Port

Configuring a port involves setting the parameters for a specific interface or connection point on a network device. This can include setting IP addresses, enabling or disabling the port, and configuring speed or duplex settings.

Purpose:

- ✓ **Network Connectivity**: Ensures devices are correctly connected and can communicate with the network.
- ✓ **Performance Optimization**: Adjust settings like speed and duplex to optimize performance.

Example:

```
Router(config)#interface GigabitEthernet 0/1
```

```
Router(config-if)#ip address 192.168.1.2 255.255.255.0
```

```
Router(config-if)#no shutdown
```

In this example, the IP address is configured on the GigabitEthernet 0/1 interface, and the interface is enabled with the no shutdown command.

2.5 Configure Device Passwords

Setting passwords on network devices is crucial for securing access. Passwords can be configured for different levels of access, such as console access, VTY (remote) access, and privileged EXEC mode.

The purposes of device passwords configuration are **Security**: Prevents unauthorized access to the device and **Access Control**: Allows different levels of access based on user roles.

Types of Passwords:

- ✓ **Console Password**: Controls access via the physical console port.
- ✓ **VTY Password**: Controls remote access via Telnet or SSH.
- ✓ **Enable Password**: Protects privileged EXEC mode.

Example:

```
Router(config)#line console 0
```

```
Router(config-line)#password cisco123
```

```
Router(config-line)#login
```

```
Router(config)#line vty 0 4
```

```
Router(config-line)#password cisco321
```

```
Router(config-line)#login
```

```
Router(config)#enable secret supersecurepassword
```

In this example, a password is set for console access (cisco123), VTY access (cisco321), and the privileged EXEC mode (supersecurepassword).

2.6. Save Configuration

Saving the configuration ensures that all changes made to the device's settings are retained even after a restart. In Cisco devices, the running configuration is saved to the startup configuration.

Purpose:

- ✓ **Persistence:** Ensures that configurations are not lost after a device reboot.
- ✓ **Reliability:** Helps maintain a stable and consistent network environment.

Example:

```
Router#copy running-config startup-config
```

In this example, the current running configuration is saved to the startup configuration, so it will be reloaded the next time the device is restarted.



Practical Activity 2.4.1: Configuring Basic network devices



Task:

1: Referring to previous activities (2.4.1) and key readings 2.4.2; Read the following task.

As a trainee who has recently learned about network device configuration, you are asked to set up a small office network of IT lab using three network switches. Your task is to configure each switch by assigning a unique hostname (Switch-1, Switch-2, Switch-3) for easy identification, setting up a banner message (Unauthorized access to Switch-1,2,3 is prohibited) to display a warning against unauthorized access, and configuring all the passwords required (e.g for one switch: c0ns0le1, vtypass1, enablepass1) to secure access to the switches. You also need to enable and configure the necessary ports on each switch to connect computers and other devices. Additionally, you must save the configurations on all switches to ensure they are retained after a reboot, and then perform a reload of each switch to apply and verify the settings. The task must be performed using Cisco Packet tracer.

2: Perform the task given.

3: Ask more clarifications if any and assistance where needed.

4: Present your work to the trainer and whole class.

5: Read key reading (2.4.2) and ask clarification where necessary.

6: Perform the task provided in application of learning 2.4



Key readings 2.4.2: Configuring Basic network devices

Device Configuration steps specifically using a Cisco Packet Tracer:

1. Access the Switch

Step 1: Open Cisco Packet Tracer and drag a switch (e.g., 2960 Switch) into the workspace.

Step 2: Access the switch's CLI by clicking on the switch and selecting the "CLI" tab.

2. Configure the Hostname

Step 3: Enter global configuration mode.

At the CLI prompt, enter global configuration mode:

Switch> enable

Switch# configure terminal

The prompt changes to Switch(config)#.

Step 4: Set the hostname.

Assign a unique hostname:

Switch(config)# hostname Switch-1

The prompt changes to Switch-1(config)#, indicating the hostname has been successfully changed.

3. Set Banner Message

Step 5: Configure the banner message.

Set the Message of the Day (MOTD) banner:

Switch-1(config)# banner motd # Unauthorized access to Switch-1 is prohibited.
#

This message will be displayed when someone logs into the switch.

4. Configure Device Passwords

a. Console Password:

Step 6: Configure the console password.

Enter console line configuration mode:

Switch-1(config)# line console 0

Set the console password:

Switch-1(config-line)# password c0ns0le1

Switch-1(config-line)# login

Exit console line configuration mode by typing exit.

b. VTY (Telnet/SSH) Password:

Step 7: Set the VTY password for remote access:

Enter VTY line configuration mode:

Switch-1(config)# line vty 0 4

Set the VTY password:

Switch-1(config-line)# password vtypass1

Switch-1(config-line)# login

Exit VTY line configuration mode by typing exit.

c. Enable Secret Password:

Step 8: Set the enable secret password for privileged EXEC mode:

In global configuration mode, type:

Switch-1(config)# enable secret enablepass1

This command encrypts the password for enhanced security.

5. Configure IP Address on the Management Interface (VLAN 1)

Step 9: Enter interface configuration mode.

Type the following command to enter the management interface (VLAN 1) configuration:

Switch-1(config)# interface vlan 1

Step 10: Assign the IP address and subnet mask.

Set the IP address and subnet mask for the management interface:

Switch-1(config-if)# ip address 192.168.1.1 255.255.255.0

Step 11: Enable the interface.

Switch-1(config-if)# no shutdown

6. Save the Configuration

Step 12: Save the running configuration to the startup configuration.

Exit to privileged EXEC mode by typing exit until you reach the Switch-1# prompt.

Save the configuration with:

Switch-1# copy running-config startup-config

Confirm the command by pressing Enter when prompted.

7. Reload the Switch

Step 13: Reload the switch.

In privileged EXEC mode, type:

Switch-1# reload

Confirm the reload by typing yes or pressing Enter when prompted.

The switch will restart, applying all the configurations you've made.



Points to Remember

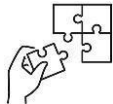
- **Device Configuration Modes**

Device configuration modes refer to the different states or environments a networking device (such as a router, switch, or firewall) can be in when you're setting it up or managing it. Each mode allows you to perform specific types of configuration tasks.

The common device configuration modes, particularly in the context of Cisco networking devices are:

1. User EXEC Mode

2. Privileged EXEC Mode
 3. Global Configuration Mode
 4. Interface Configuration Mode
 5. Line Configuration Mode
 6. VLAN Configuration Mode
 7. Router Configuration Mode
 8. ROMMON Mode
- **Key elements in configuration of network devices** are hostname, banner messages, device passwords, configure ports, configure devices password, saving configurations and reloading devices.
 - **Device Configuration steps specifically using a Cisco Packet Tracer:**
 1. Access the Switch
 2. Configure the Hostname
 3. Set Banner Message
 4. Configure Device Passwords
 5. Configure IP Address on the Management Interface
 6. Save the Configuration
 7. Reload the Switch



Application of learning 2.4.

In Kigali City, a new training center has been established to provide networking and IT courses. As part of the initial setup, you, a network technician, are tasked with configuring the network devices in the training lab. The lab consists of three Cisco switches that need to be properly configured to ensure secure and efficient network operation.

Your tasks include setting up the hostname for each switch, configuring a banner message to display important information when users log in, setting passwords for secure access, configuring the necessary ports, and saving the configurations to ensure they persist after a reboot. Additionally, you need to perform a device reload to verify that the configurations have been saved successfully.



Indicative content 2.5: Testing network Interconnection



Duration: 7 hrs



Theoretical Activity 2.5.1: Description of network Interconnection testing.



Tasks:

- 1: Read and answer the following questions:
 - i. Explain physical testing in networking.
 - ii. Explain what unit testing is in the context of networking.
 - iii. Discuss Network Integration Testing.
- 2: Provide the answer for the asked questions and write them on papers.
- 3: Present the findings/answers to the whole class
- 4: For more clarification, read the **key readings 2.5.1**.
- 5: In addition, ask questions where necessary.



Key readings 2.5.1.: Description of network Interconnection testing

1. Physical Testing

In networking, physical testing involves evaluating the hardware components of a network, such as routers, switches, cables, and other network devices, to ensure they operate correctly and meet required specifications.

Key Aspects:

- ✓ **Cable Testing:** Verifying that network cables (Ethernet, fiber optic) are functioning correctly, testing for continuity, signal strength, and any interference.
- ✓ **Hardware Performance:** Assessing the performance of network devices under load conditions to ensure they handle traffic as expected.
- ✓ **Connectivity Tests:** Ensuring physical connections are established correctly, and devices can communicate over the network.

Example: Using a network cable tester to check for wiring faults in Ethernet cables, ensuring that they are correctly connected and free of shorts or open circuits.

2. Unit Testing

Unit testing in the context of a Local Area Network (LAN) might imply testing individual components of software or hardware which operate within that LAN.

3. Integration Testing

Integration Testing in a Local Area Network (LAN) involves testing the combined parts of a network system and ensuring that they function correctly when they interact with each other.

The goal is to detect any interface defects between the modules in a network setting.

Network functionality testing is important for a number of reasons, including:

- Preventing downtime: Identifying and resolving problems before they cause network outages can save businesses time and money.
- Improving security: Identifying and remediating vulnerabilities can help to protect businesses from cyberattacks.
- Optimizing performance: Measuring and optimizing network performance can help to ensure that applications are running smoothly and that users are experiencing good performance.
- Ensuring compliance: Verifying compliance with regulations can help businesses to avoid fines and penalties.



Practical Activity 2.5.2: Testing network interconnection.



Task:

- 1: Referring to previous activities 2.5.1 and key readings 2.5.2; Read the following task.
As network Technician, install a small local area network or use the one installed during previous activities and apply physical, unity testing and integration testing.
- 2: Perform the task given by following the instructions related to the task.
- 3: Ask more clarifications if any and assistance where needed.
- 4: Present your work to the trainer and whole class.
- 5: Read key reading (2.5.2) and ask clarification where necessary.
- 6: Perform the task provided in application of learning 2.5.



Key readings 2.5.2: Testing network interconnection.

1. Physical Testing

Testing a Network Switch Installation

1. **Cable Testing:** Use a network cable tester to check the Ethernet cables connecting a new switch to routers and computers.
Example: Ensure that cables are not only correctly wired but also free from interference. Test cables for continuity to verify there are no breaks or shorts.
2. **Hardware Verification:** Check that the switch is powered on and that all LEDs indicating port status are functioning correctly.
Example: Verify that the switch's power supply is stable and that there are no hardware faults visible on the device.

3. **Connectivity Checks:** Confirm that all cables are securely connected to the correct ports on the switch.

Example: Ensure that the connection between the switch and the router is secure and that no loose connections exist.

4. **Environmental Testing:** Ensure the switch is operating within the recommended temperature range and has adequate ventilation.

Example: Place temperature sensors in the equipment room to monitor that the cooling system is effectively keeping the switch within its operating temperature limits.

2. Unit Testing

Testing a Router's DHCP Configuration

1. **Configuration Validation:** Verify the router's DHCP settings, such as the IP address range, lease time, and DNS server assignments.

Example: Use the router's CLI to check that DHCP is configured to assign IP addresses in the range 192.168.1.100 to 192.168.1.200.

2. **Service Testing:** Test the DHCP server functionality by connecting a client device and checking if it receives an IP address from the router.

Example: Connect a laptop to the network and ensure it obtains an IP address from the router's DHCP pool, and verify that the IP address is within the correct range.

3. **Function Testing:** Ensure that the DHCP server assigns IP addresses correctly and that the devices can access the network.

Example: Use the ipconfig command on a client device to check that it has received a proper IP configuration.

4. **Failover Testing:** Simulate a DHCP server failure by shutting down the router and verifying that a backup DHCP server can take over.

Example: Configure a secondary DHCP server and test that it begins assigning IP addresses when the primary server is down.

3. Integration Testing

Testing a Network Setup with Multiple Routers and Switches

1. **End-to-End Connectivity Testing:** Verify that devices on different subnets can communicate with each other through multiple routers and switches.

Example: Ping a device on 192.168.1.0/24 from a device on 192.168.2.0/24 to ensure routing is functioning correctly.

2. **Protocol and Service Integration:** Test the interaction between OSPF and BGP routing protocols on multiple routers.

Example: Configure OSPF on Router A and BGP on Router B and ensure that routes are exchanged correctly between the two protocols.

3. **Load and Performance Testing:** Simulate high network traffic and monitor performance metrics like bandwidth and latency.

Example: Use network traffic generators to create load and measure the impact on network performance using tools like iPerf or NetFlow.

4. **Interoperability Testing:** Ensure that routers and switches from different manufacturers work together as intended.

Example: Connect a Cisco router with a Juniper switch and verify that they can exchange traffic without issues.

5. **Security Testing:** Check the effectiveness of firewalls and access control lists (ACLs) in blocking unauthorized access.

Example: Attempt to access restricted network resources from a test device to verify that security policies are correctly enforced.

6. **Redundancy and Failover Testing:** Test network redundancy and failover mechanisms to ensure continuity in case of device failure.

Example: Disconnect the primary network link and verify that traffic is correctly rerouted through a backup link.

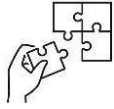
In Summary:

- **Physical Testing:** Focuses on checking the physical network components (e.g., cables, hardware) for correct installation and performance.
- **Unit Testing:** Involves verifying individual network configurations or services to ensure they function as expected in isolation.
- **Integration Testing:** Tests the interaction and performance of combined network components to ensure they work together seamlessly and meet overall network requirements.



Points to Remember

- **Physical Testing:** In networking, physical testing involves evaluating the hardware components of a network, such as routers, switches, cables, and other network devices, to ensure they operate correctly and meet required specifications.
- **Unit testing:** in the context of Networking imply testing individual components of software or hardware which operate within that Network.
- **Integration Testing** involves testing the combined parts of a network system and ensuring that they function correctly when they interact with each other.
- **Steps in Physical Testing:** Focuses on checking the physical network components (e.g., cables, hardware) for correct installation and performance.
- **Steps in Unit Testing:** Involves verifying individual network configurations or services to ensure they function as expected in isolation.
- **Steps in Integration Testing:** Tests the interaction and performance of combined network components to ensure they work together seamlessly and meet overall network requirements.



Application of learning 2.5.

In Kigali City, the Training Center has recently completed the installation of its new network infrastructure. As a trainee who has studied network testing methodologies, you are now tasked with ensuring that the network is functioning correctly by performing three key types of tests: physical testing, unit testing, and integration testing.

Your objective is to verify that all network components, including switches, routers, cables, and connected devices, are working properly and that the network as a whole is performing as expected.



Learning outcome 2 end assessment

Theoretical assessment

Practical assessment

You are a network technician assigned to a newly established office branch in Musanze District. The office consists of four computers, one network printer, a switch, and a router. Your task is to design and implement the network, ensuring proper IP addressing, subnetting, and configuration of all network devices. After setting up the network, you will conduct testing to verify that all components are functioning correctly.

Tasks:

- You have been allocated the IP address range 192.168.10.0/24. The office has four departments, each requiring its subnet. The IP address scheme must allow for future expansion, so plan your subnets accordingly.
- Calculate the appropriate subnet masks and assign IP addresses to each department, ensuring that each subnet can support at least 30 devices.
- Assign static IP addresses to the computers and network printer within each subnet.
- Configure the router with the correct IP address scheme and ensure it manages the internal network effectively.
- Assign appropriate hostnames to the router and switch. For example, use Officer router and Office Switch.
- Configure a banner message on the router and switch to display a welcome message and a warning that unauthorized access is prohibited.
- Configure the switch ports to connect the four computers and the network printer.
- Set up strong passwords for accessing the router and switch to secure the network devices.
- Perform physical testing to ensure all devices are connected correctly and powered on.
- Conduct unit testing by verifying the configuration and operation of each individual network device (computers, network printer, router, switch).
- Perform integration testing by ensuring that all network components (computers, printer, router, switch) communicate effectively with each other.
- Test connectivity between subnets and verify that network services such as file sharing and printing are functioning correctly.
- Configure DHCP on the router to assign IP addresses dynamically to any additional devices that might be connected to the network in the future.
- Verify that the dynamic IP assignment works correctly by connecting a new device to the network and confirming it receives an IP address automatically.

- Document the IP address scheme, subnet calculations, and configuration settings for all network devices.



Reference

Books:

Burgess, M. (2016). *Network troubleshooting: A practical guide*. London: Addison-Wesley.

Hunter, D. (2018). *Networking fundamentals: A beginner's guide*. Berkeley: McGraw-Hill Education.

Odom, W. (2020). *CCNA 200-301 official cert guide*. Indianapolis: Cisco Press.

Web links :

Academia. (n.d.). Networking fundamentals. Retrieved from https://www.academia.edu/23703156/Chapter_1_Networking_Fundamentals_Chapter_1_Networking_Fundamentals

CBT Nuggets. (2021, November 5). Networking basics: What is IPv4 subnetting? CBT Nuggets Blog. Retrieved from <https://www.cbtnuggets.com/blog/technology/networking/networking-basics-what-is-ipv4-subnetting>

Cisco Systems. (n.d.). IP addressing. Cisco. Retrieved from <https://www.cisco.com/en/US/docs/security/vpn5000/manager/reference/guide/appA.html#:~:text=Each%20device%20on%20an%20IP,255.0%2C%20and%20198.41>

FS Community. (n.d.). Know IP address and subnet mask. FS Community. Retrieved from <https://community.fs.com/article/know-ip-address-and-subnet-mask.html>

Microsoft. (n.d.). TCP/IP addressing and subnetting. Microsoft Support. Retrieved from <https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting>

NetSecCloud. (n.d.). Understanding IP addresses and subnet masks: A basic guide. NetSecCloud. Retrieved from <https://netseccloud.com/understanding-ip-addresses-and-subnet-masks-a-basic-guide>

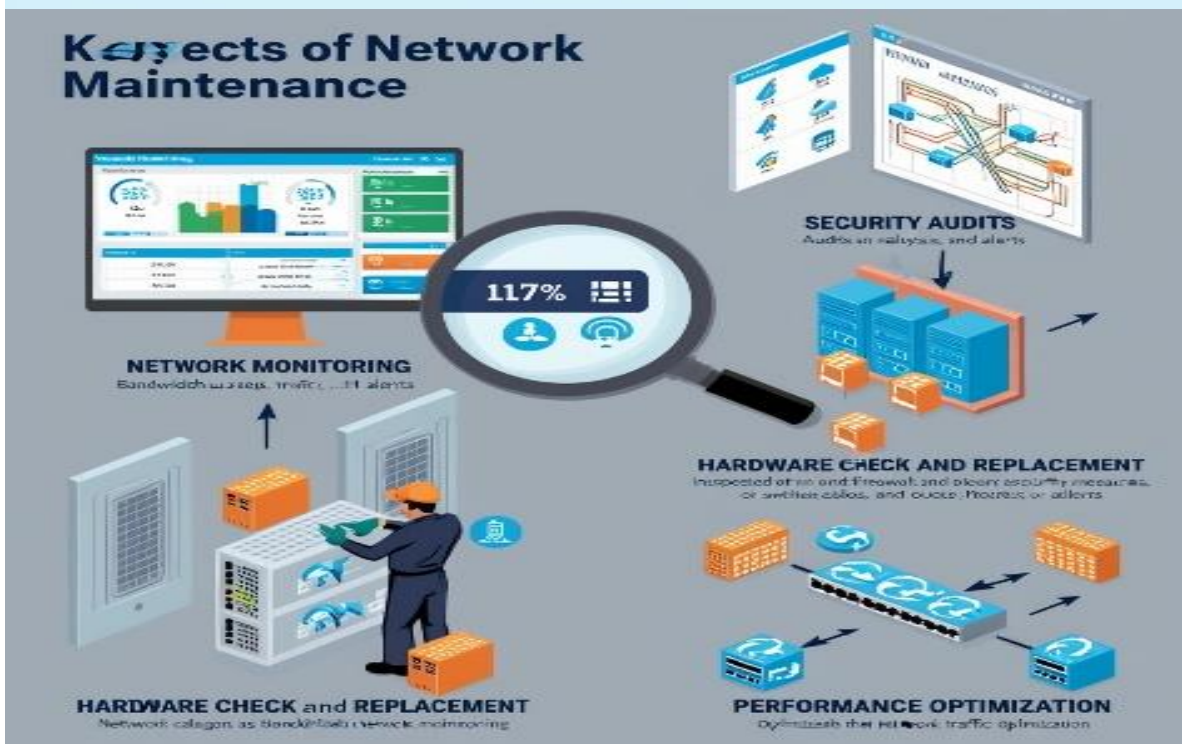
Techtarget. (n.d.). Introduction to IP addressing and subnetting. Retrieved from <https://www.techtarget.com/searchnetworking/tip/Introduction-to-IP-addressing-and-subnetting>

University of Houston-Clear Lake. (n.d.). IP addressing. UHCL Information Security. Retrieved from <https://www.uhcl.edu/information-security/tips-best-practices/ipaddressing>

Learning Outcome 3: Maintain Network System



Key Aspects of Network Maintenance



Indicative contents

3.1 Performing preventive maintenance

3.2 Performing corrective maintenance.

3.3 Troubleshooting network

3.4 Elaboration of maintenance report

Key Competencies for Learning Outcome 3: Maintain Network system

Knowledge	Skills	Attitudes
<ul style="list-style-type: none">● Description of preventive maintenance in network system● Description of corrective maintenance in network system● Introduction to troubleshooting network● Description of maintenance report	<ul style="list-style-type: none">● Performing preventive maintenance● Performing corrective maintenance● Troubleshooting network system● Elaborating maintenance report	<ul style="list-style-type: none">● Being a Critical Thinker in troubleshooting● Having Curiosity for preventive maintenance● Having Adaptability in corrective maintenance● Having Collaborative Spirit for elaboration of maintenance report



Duration: 15 hrs



Learning outcome 3 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Perform properly Preventive maintenance as per manufacturer's guidelines.
2. Perform properly Corrective Maintenance based on problems
3. Check properly network protection measures in accordance with the installation design.
4. Handle properly network issues-based system diagnosis.
5. Elaborate efficiently maintenance report based on network status.



Resources

Equipment	Tools	Materials
<ul style="list-style-type: none">• Computer• Router• battery• Visual Equipment	<ul style="list-style-type: none">• Network Toolkit• Testing tools	<ul style="list-style-type: none">• Cables and accessories• Electricity• Internet bundles• Power Extension



Indicative content 3.1: Performing preventive maintenance



Duration: 4 hrs



Theoretical Activity 3.1.1: Description of hardware and software Preventive maintenance



Tasks:

- 1: Read and answer the following questions
 - i. Differentiating hardware and software preventive maintenance.
 - ii. What are examples of hardware preventive maintenance in networking?
 - iii. What are examples of software preventive maintenance in networking?
- 2: Provide the answers for the asked questions and write them on paper/flipchart
- 3: Present your findings to the class
- 4: For more clarifications, read key readings 3.1.1.
- 5: In addition, ask questions where necessary.



Key readings 3.1.1.: Description of hardware and software Preventive maintenance

1. Hardware preventive maintenance

In networking, hardware preventive maintenance is crucial for ensuring that network equipment remains reliable and performs optimally. The following are key aspects of preventive maintenance specific to networking hardware:

1.1. Schedule Regular Cleaning:

- **Dust Removal:** Regularly clean networking equipment, such as routers, switches, and servers, to prevent dust accumulation. Dust can clog vents, reduce airflow, and cause overheating, which may lead to hardware failure.
- **Port and Connector Cleaning:** Ensure that ports and connectors (like Ethernet ports, fiber optic connectors) are free from dust and debris to maintain good signal quality.
- **Cable Management:** Regularly inspect and clean network cables to prevent dust buildup, tangling, or wear, which can affect performance and cause signal degradation.

1.2. Setting of Preventive Measures:

- **Firmware and Software Updates:** Regularly update the firmware and software of networking devices to fix bugs, patch security vulnerabilities, and improve performance.
- **Power Protection:** Use uninterruptible power supplies (UPS) and surge protectors to protect networking equipment from power surges, spikes, and

outages.

- **Regular Backups:** Implement and regularly test backup procedures for network configurations and settings to quickly restore functionality in case of a failure.
- **Monitoring Tools:** Use network monitoring tools to set up alerts for unusual activity or signs of impending hardware issues.

1.3. Check Physical Equipment Condition:

- **Visual Inspection:** Regularly inspect network hardware for physical damage, such as cracks, corrosion, or loose connections that could impact performance or cause failures.
- **Component Testing:** Test critical components like power supplies, fans, and internal connections to ensure they are working correctly. Replace any parts showing signs of wear or failure.
- **Cabling:** Ensure network cables are not frayed, kinked, or improperly connected. Check that all cables are securely connected and that there is no excessive strain on connectors.

1.4. Check Environment Condition:

- **Temperature Control:** Ensure that networking equipment is kept in a temperature-controlled environment. Overheating can lead to reduced performance or hardware damage.
- **Humidity Control:** Maintain proper humidity levels to prevent static discharge, which can damage sensitive networking components.
- **Airflow Management:** Ensure adequate ventilation and airflow around network equipment to prevent overheating. Avoid blocking vents and ensure that cooling systems are functioning properly.
- **Physical Security:** Make sure that network equipment is housed in a secure location, such as a locked server room or cabinet, to prevent unauthorized access and physical tampering.

By implementing these preventive maintenance practices, network administrators can help ensure the longevity, stability, and reliability of the network infrastructure.

2. Software preventive maintenance

Software preventive maintenance in networking involves a series of ongoing tasks designed to ensure that network software and systems remain secure, up-to-date, and perform efficiently. Below are the key components of software preventive maintenance in networking:

2.1. Regular Change of Network Device Credentials:

- **Periodic Password Updates:** Regularly change the credentials (usernames and passwords) used to access network devices such as routers, switches, and firewalls. This reduces the risk of unauthorized access due to compromised credentials.

- **Enforce Strong Password Policies:** Implement and enforce strong password policies, including the use of complex passwords, to enhance security.
- **Multi-Factor Authentication (MFA):** Where possible, enable MFA on network devices to provide an additional layer of security.

2.2. Network Monitoring Software Licensing and Application:

- **License Management:** Ensure that all network monitoring software is properly licensed and that licenses are up to date. Unlicensed or expired software may not function properly or could be a security risk.
- **Software Compliance Checks:** Regularly review and ensure compliance with software licensing agreements to avoid legal and operational issues.
- **Optimal Deployment:** Make sure that network monitoring tools are correctly deployed and configured to effectively monitor network performance, detect anomalies, and alert administrators to potential issues.

2.3. Updating and Upgrading Network Monitoring Software and Device Firmware:

- **Regular Software Updates:** Keep all network-related software, including monitoring tools, security software, and management applications, up to date. Software updates often include critical security patches and performance improvements.
- **Firmware Upgrades:** Regularly update the firmware of network devices (such as routers, switches, firewalls, and access points) to the latest version. Firmware upgrades can provide important security fixes, new features, and enhanced performance.
- **Compatibility Checks:** Before applying updates or upgrades, check for compatibility with existing hardware and software to prevent potential conflicts or disruptions in service.
- **Backup Configurations:** Always back up current configurations and settings before performing updates or upgrades to ensure that systems can be restored quickly if something goes wrong.
- **Test Before Deployment:** Test updates and upgrades in a controlled environment before deploying them across the network to minimize the risk of issues in the live environment.

3. Benefits of Software Preventive Maintenance:

- **Security:** Regular credential changes and updates help protect the network from unauthorized access and vulnerabilities.
- **Performance:** Keeping software and firmware up to date ensures that the network runs efficiently and that any known bugs or issues are resolved.
- **Reliability:** Proper licensing and regular maintenance help prevent software malfunctions and reduce the risk of network downtime.
- **Compliance:** Staying compliant with software licensing and security policies helps avoid legal issues and potential fines.

By regularly performing these software preventive maintenance tasks, network administrators can help ensure the security, stability, and optimal performance of their network infrastructure.

There are many different preventive measures that you can take to protect your network. Some of the most important measures include:

- **Identifying threats:** The first step to preventing threats is to identify them. This can be done by using a variety of tools and techniques, such as network monitoring, vulnerability scanning, and penetration testing.
- **Mitigating threats:** Once you have identified a threat, you need to take steps to mitigate it. This may involve patching vulnerabilities, installing security software, or changing security policies.
- **Monitoring:** It is important to monitor your network on an ongoing basis to identify new threats and to assess the effectiveness of your preventive measures.

4. Preventive Measures for Specific Threats

In addition to general preventive measures, there are also specific preventive measures that you can take to protect against specific threats. For example, to protect against malware, you can install anti-malware software and keep your software up to date. To protect against phishing attacks, you can educate your employees about phishing and how to spot it.

Here are three threats to your network:

Threats refer to any potential dangers that could compromise the security, integrity, availability, or functionality of a network and its associated resources.

1. **Malware:** Malware is software that is designed to harm your computer or steal your information. It can be installed on your computer through a variety of ways, such as clicking on a malicious link, opening an infected attachment, or downloading a file from an untrusted source. Once malware is on your computer, it can steal your personal information, install other malware, or even take control of your computer.



2. **Phishing:** Phishing is a type of social engineering attack that tries to trick you into

giving up your personal information, such as your passwords or credit card numbers. Phishing scams often come in the form of emails or text messages that



appear to be from a legitimate source, such as your bank or credit card company. The email or text message will typically contain a link that, when clicked, will take you to a fake website that looks like the real website. If you enter your personal information on the fake website, it will be stolen by the scammers.

3. **Ransomware:** Ransomware is a type of malware that encrypts your files and then demands a ransom payment in exchange for the decryption key. If you do not pay the ransom, you will not be able to access your files. Ransomware attacks can be very costly, both in terms of the ransom payment and the downtime that they can cause.



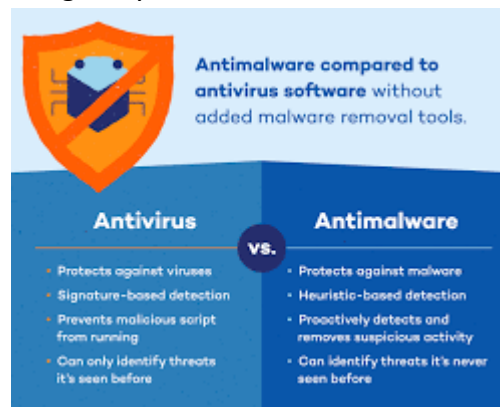
These are just a few of the many threats that can face your LAN. It is important to take steps to protect your LAN from these threats by installing antivirus and anti-malware software, keeping your software up to date, and being careful about what information you share online.

Threat 1: Malware

Preventive measures:

- Install and use antivirus and anti-malware software: Antivirus and anti-malware software can help to protect your computer from malware by scanning for and removing malicious software. Make sure to update your antivirus and anti-

malware software regularly to ensure that it has the latest definitions.



- **Keep your software up to date:** Software updates often include security patches that can help to protect your computer from malware. Make sure to install software updates as soon as they are available.
- **Be careful about what you download:** Only download files from trusted sources. Avoid clicking on links in emails or text messages from unknown senders.
- **Use strong passwords:** Strong passwords are at least 12 characters long and include a mix of upper and lowercase letters, numbers, and symbols. Avoid using easily guessable passwords, such as your birthday or pet's name.
- **Enable Windows Defender Firewall:** Windows Defender Firewall is a built-in firewall that can help to protect your computer from malware. Make sure that Windows Defender Firewall is turned on and that it is configured to block incoming connections from untrusted sources.

Threat 2: Phishing

Preventive measures:

- Be suspicious of emails and text messages that ask for personal information: Legitimate companies will never ask you to provide personal information via email or text message. If you receive an email or text message that asks for personal information, do not reply to it. Instead, contact the company directly to verify the authenticity of the request.
- Hover over links before clicking on them: This will reveal the actual URL of the link. If the URL looks suspicious, do not click on it.
- Look for red flags: Phishing emails and text messages often contain red flags, such as typos, grammatical errors, or odd phrasing. If you notice any red flags, do not reply to the email or text message.
- Be careful about what information you share online: Do not share personal information, such as your social security number or credit card number, on social media or other public websites.
- Educate yourself about phishing: There are many resources available online that can teach you about phishing and how to protect yourself from it.

Threat 3: Ransomware

Preventive measures:

- Back up your data regularly: The best way to protect yourself from ransomware is to back up your data regularly. This will ensure that you have a copy of your data in case your computer is infected with ransomware.
- Keep your software up to date: Software updates often include security patches that can help to protect your computer from ransomware. Make sure to install software updates as soon as they are available.
- Be careful about what you click on: Ransomware can be installed on your computer by clicking on a malicious link or opening an infected attachment. Avoid clicking on links or opening attachments from unknown senders.
- Use a firewall: A firewall can help to protect your computer from ransomware by blocking unauthorized access to your computer. Make sure that your firewall is turned on and that it is configured to block incoming connections from untrusted sources.
- Be aware of the latest ransomware threats: Ransomware is constantly evolving, so it is important to be aware of the latest threats. You can stay up-to-date on the latest ransomware threats by following cybersecurity news and blogs.



Practical Activity 3.1.2: Implementation of network hardware and software preventive measures

Task:

1: Referring to previous activity 3.1.1. And key readings 3.1.2; Read carefully the given task.

As IT, you are requested to perform Preventive Maintenance on a Small Office Network include cleaning network devices, updating firmware, and checking environmental conditions.

2: Perform the task given by following instructions

3: Ask clarifications if any and assistance where needed.

4: Present your work to trainer and whole class.

5: Read key readings 3.1.2 in trainee's manual



Key readings 3.1.2: Implementation of Network Hardware and software preventive measures

Steps for Cleaning Network Devices:

- 1. Power Down the Devices:**
 - Safety First: Before you begin cleaning, turn off and unplug the network devices (routers, switches, etc.) to avoid electrical hazards and prevent damage.
- 2. Gather Cleaning Supplies:**
 - Compressed Air: For blowing dust out of vents and components.
 - Soft Cloth: Lint-free microfiber cloths are ideal for wiping surfaces.
 - Isopropyl Alcohol (Optional): For cleaning stubborn spots or connectors.
 - Small Brush (Optional): A soft brush can help remove dust from hard-to-reach areas.
- 3. Remove External Dust and Debris:**
 - Exterior Cleaning: Use a dry microfiber cloth to wipe down the exterior surfaces of the device, including the front, sides, and back.
 - Vents and Ports: Use compressed air to blow dust out of ventilation grilles and ports. Hold the canister upright and use short bursts to avoid condensation.
- 4. Clean Internal Components:**
 - Open the Case (if applicable): If you have access to internal components (e.g., in a server or desktop router), carefully open the case following the manufacturer's instructions.
 - Remove Dust: Use compressed air to blow dust off internal components such as fans, heatsinks, and circuit boards. Avoid direct contact with internal components to prevent static damage.
 - Clean Fan Blades: If applicable, gently hold the fan blades in place while using compressed air to clean them. This prevents damage to the fan bearings.
- 5. Clean Connectors and Ports:**
 - Inspect for Dust: Check connectors and ports for dust or debris.
 - Clean Connectors (if necessary): Dampen a soft cloth with isopropyl alcohol and gently clean the connectors. Ensure that the cloth is not too wet to avoid moisture damage. Allow the connectors to dry completely before reassembly.
- 6. Reassemble and Power On:**
 - Reassemble the Device: If you opened the case, carefully reassemble the device according to the manufacturer's instructions.
 - Reconnect and Power Up: Plug the device back in and power it on. Verify that it is functioning correctly.

Steps for Updating Firmware:

- 1. Review Documentation:**
 - Read the Release Notes: Check the release notes or changelog for the new

firmware version to understand what changes or improvements are included.

- Check Compatibility: Ensure the firmware version is compatible with your device model and current setup.
- 2. Backup Configuration:**
 - Save Current Configuration: Before updating the firmware, backup the current configuration of your device. This can typically be done through the device's management interface or command line.
 - Store Backup Safely: Save the backup file in a secure location, such as an external drive or cloud storage.
- 3. Download Firmware:**
 - Obtain Firmware: Download the latest firmware version from the manufacturer's official website or support portal.
 - Verify Integrity: Check the downloaded firmware file's integrity (e.g., using checksums) to ensure it has not been corrupted or tampered with.
- 4. Prepare the Device:**
 - Power Stability: Ensure the device is connected to a stable power source to avoid interruptions during the update process.
 - Close Active Sessions: Close any active sessions or applications that are using the device to prevent conflicts.
- 5. Access Device Management Interface:**
 - Log In: Access the device's management interface through a web browser or command line using the device's IP address.
 - Navigate to Firmware Update Section: Locate the section or menu for firmware updates, which is usually found under system settings or maintenance.
- 6. Upload Firmware:**
 - Select Firmware File: Choose the firmware file you downloaded earlier and upload it to the device using the management interface.
 - Start the Update: Initiate the firmware update process. This may take several minutes, during which the device may reboot.
- 7. Monitor the Update:**
 - Watch Progress: Monitor the update process to ensure it completes successfully. Avoid interrupting the update to prevent bricking the device.
 - Check for Errors: If any errors occur, follow the troubleshooting steps provided by the manufacturer.
- 8. Verify Update:**
 - Check Firmware Version: After the update, verify that the firmware version has been successfully updated by checking the device's status or version information.
 - Test Device Functionality: Ensure that the device is functioning correctly and that all features and settings are working as expected.
- 9. Restore Configuration (if needed):**

- Reapply Configuration: If the firmware update reset the device to default settings, reapply the configuration from the backup you created earlier.

10. Document the Update:

- Record Details: Note the date of the firmware update, the new version number, and any changes made. This documentation helps with future maintenance and troubleshooting.

11. Schedule Regular Updates:

- Plan Future Updates: Set up a schedule or process for regularly checking for and applying firmware updates to keep the device secure and up to date.



Points to Remember

✓ **Malware**

Preventive measures:

- ✓ Install and use antivirus and anti-malware software
- ✓ Keep your software up to date
- ✓ Be careful about what you download
- ✓ Use strong passwords
- ✓ Enable Windows Defender Firewall

✓ **Phishing**

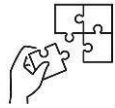
Preventive measures:

- ✓ Be suspicious of emails and text messages that ask for personal information
- ✓ Hover over links before clicking on them
- ✓ Look for red flags
- ✓ Be careful about what information you share online
- ✓ Educate yourself about phishing

✓ **Ransomware**

Preventive measures:

- ✓ Back up your data regularly
- ✓ Keep your software up to date
- ✓ Be careful about what you click on
- ✓ Use a firewall
- ✓ Be aware of the latest ransomware threats



Application of learning 3.1.

ABC School has a growing number of students and staff, and their network infrastructure is becoming strained. The school's IT department has identified issues with network performance and security, including slow internet speeds and occasional unauthorized access attempts. To address these concerns, the school decides to bring in a Network Technician to perform preventive maintenance and upgrades.



Indicative content 3.2: Performing Corrective Maintenance



Duration: 3 hrs



Theoretical Activity 3.2.1: Description of Corrective maintenance



Tasks:

1. Read carefully the questions below and answer them.
 - i. Identify common network problems and their causes.
- 2: Provide the answers for the asked questions and write them on paper/flipchart
- 3: Present your findings to the class
- 4: For more clarifications, read key readings 3.1.1.
- 5: In addition, ask questions where necessary.



Key readings 3.2.1.: Description of Corrective maintenance

1. Corrective Maintenance

Corrective maintenance in networking refers to the process of identifying, diagnosing, and resolving issues or failures in a network to restore its normal functioning. This type of maintenance is typically performed after a problem, such as a network outage, degraded performance, or hardware failure, has occurred. The goal is to fix the malfunction, replace faulty components, and reconfigure systems as needed to ensure the network operates efficiently and reliably.

2. Common network problems and their causes

Slow Network Performance

- Cause: Bandwidth congestion due to too many devices or high network traffic, outdated hardware, or improper configurations.

Network Connectivity Issues

- Cause: Faulty or loose cables, network misconfigurations, IP address conflicts, or hardware failures like faulty routers/switches.

Intermittent Network Outages

- Cause: Environmental interference (e.g., electromagnetic interference), hardware issues (e.g., failing switches/routers), or unreliable power sources.

Security Breaches

- Cause: Weak passwords, outdated security protocols, lack of firewall protection,

or unpatched software vulnerabilities.

High Packet Loss

- Cause: Poor cabling, overloaded network devices, network congestion, or malfunctioning hardware (e.g., NICs or routers).



Practical Activity 3.2.2: Performing corrective maintenance

Task:

1: Read carefully and perform the task outlined below:

You are tasked with setting up a small office network for a new department in your company. The network consists of a router, a switch, and eight client computers. The network is used for accessing shared files, communicating via email, and connecting to the internet. By using packet tracer. Configure the network devices with appropriate IP addresses, subnet masks, and default gateways. Verify that all client computers can successfully ping the router and access the internet.

- ✓ Randomly :(1) disable a network connection, such as a cable or a network interface card, on one of the client computers. (2) Set incorrect router settings.
- ✓ Observe the network behaviours and identify the symptoms of the malfunction.
- ✓ Document the observed symptoms and the affected client computer.

2: Perform the task by following the instructions

3: Ask for clarifications or assistance where needed.

4: Present your work to trainer or whole class

5: Read key readings 3.2.2 in trainee's manuals



Key readings 3.2.2: Performing corrective maintenance

Key points to consider during every network corrective maintenance process:

1. Problem Identification

- **Issue Detection:** Monitor network performance and user reports to identify any abnormalities, such as slow connections, dropped packets, or loss of connectivity.
- **Error Logs and Alerts:** Review system logs, alerts from monitoring tools, and error messages to pinpoint the specific issue.
- **User Feedback:** Collect feedback from users experiencing problems to

understand the nature and extent of the issue.

2. Diagnostic and Analysis

- **Root Cause Analysis:** Determine the underlying cause of the problem through systematic troubleshooting steps.
- **Device Testing:** Test network devices (e.g., routers, switches, firewalls) to verify their functionality and identify any hardware failures.
- **Connectivity Checks:** Perform connectivity tests, such as ping tests, traceroutes, and checking link status, to locate the source of network failures.
- **Configuration Review:** Examine the configuration settings of affected devices to ensure they are correctly set up and functioning as intended.

3. Immediate Resolution

- **Quick Fixes:** Implement temporary solutions if needed to restore network functionality while preparing for a permanent fix (e.g., restarting a malfunctioning device).
- **Device Replacement:** Replace any faulty hardware components, such as cables, NICs, or network devices, that are causing the issue.
- **Configuration Adjustments:** Correct any misconfigurations that were identified during the diagnostic phase.

4. Testing and Validation

- **Functionality Testing:** After applying the fix, test the network thoroughly to ensure that the issue has been resolved and that all systems are functioning normally.
- **User Confirmation:** Verify with users that the problem has been resolved and that network performance has returned to normal levels.
- **Monitoring:** Continue monitoring the network for a period after the fix to ensure no new issues arise and that the problem does not recur.

5. Documentation

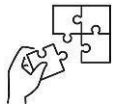
- **Incident Report:** Document the issue, the steps taken to resolve it, and the results of the corrective actions.
- **Configuration Changes:** Record any configuration changes made to network devices as part of the corrective maintenance.
- **Lessons Learned:** Note any insights gained during the troubleshooting process

that could help prevent similar issues in the future.



Points to Remember

- Performing corrective maintenance involves identifying, isolating, and repairing faults or issues in a system or equipment to restore its functionality and operational efficiency
- Steps for corrective maintenance
 1. Problem Identification
 2. Diagnostic and Analysis
 3. Immediate Resolution
 4. Testing and Validation
 5. Documentation



Application of learning 3.2.

XYZ Company experiences frequent network slowdowns, particularly during peak business hours. The IT team identifies the problem as an overloaded network switch that is dropping packets due to high traffic. To resolve the issue, they replace the switch with a higher-capacity model and reconfigure the network to balance the load. After implementation, the network performance improves, and the IT team sets up monitoring to ensure the problem doesn't recur.



Indicative content 3.3: Troubleshooting network



Duration: 6 hrs



Theoretical Activity 3.3.1: Identification of network problems and solutions



Tasks:

- 1: Read carefully and answer the following question:
 - i. Identify the main troubleshooting process in networking
 - ii. Explain the main troubleshooting process in networking.
 - iii. Identify the common problems found networking
- 2: Provide the answers for the asked questions and write them on the paper/flipchart
- 3: Present your findings to trainer and whole class.
- 4: For more clarifications, read key readings 3.3.1 in trainee manual



Key readings 3.3.1.: Identification of network problems and solutions

1. Checking Hardware and Software Functionalities

Troubleshooting a network is the process of identifying, diagnosing, and resolving issues that are affecting the network's performance or functionality. It is the first step in corrective maintenance.

Regularly checking network hardware and software functionalities is essential for maintaining the performance and reliability of your network.

By following checkpoints and practical steps outlined below, you can ensure that your systems are running optimally and are prepared to handle any challenges that arise.

1.1 Hardware

When checking network hardware functionality, two key factors are taken into account: connectivity and device status.

1. **Connectivity:** Ensures that all hardware components are properly connected and communicating with each other.

Checkpoints:

- **Cabling:**

- ✓ Inspect Ethernet cables for any visible damage, such as fraying or cuts.
- ✓ Ensure that cables are properly plugged into devices (computers, switches, routers) and are securely connected.
- **Network Devices**
- ✓ Confirm that all network devices (routers, switches, access points) are powered on and functioning.
- ✓ Check for proper LED indicators on devices to ensure they are connected and operational.
- **Network Configuration**
- ✓ Use network diagnostic tools (e.g., ping, traceroute) to test connectivity between devices.
- ✓ Verify that devices are on the same subnet and can communicate with each other.

2. Status: Identifies the current operational state of hardware components.

Checkpoints:

- ✓ Check power status indicators (LEDs) on hardware devices
- ✓ Access the router's web interface to view connected devices and their status.
- ✓ Look for any devices that are not connected or showing error messages.

1.2 Software

When checking network software functionality, the following key factors are taken into account: Software performance, Status, Updates and Services of features.

1. Performance: Evaluates the efficiency and speed of software applications and systems.

Checkpoints:

- ✓ Measure response times and performance of software applications.
- ✓ Monitor CPU, memory, and disk usage on network devices to ensure they are not overloaded.
- ✓ Conduct speed tests to measure the upload and download speeds of the network.
- ✓ Compare results with expected performance levels to identify any differences
- ✓ Check for any applications consuming excessive bandwidth.

2. Status: Determines the operational state and readiness of software applications.

Checkpoints:

- ✓ Check for error messages or system alerts indicating software issues.
- ✓ Ensure all software services are running as expected.
- ✓ Verify log files for any anomalies or warnings.

3. Updates: Ensures that software is up-to-date with the latest versions and patches.

Checkpoints:

- ✓ Update applications regularly to benefit from new features and bug fixes.
- ✓ Check for compatibility with the current operating system version.
- ✓ Enable automatic updates where possible.
- 4. Services or Features:** Verifies that all required software services and features are enabled and functioning.

Checkpoints:

- ✓ List all necessary services and features for the software.
- ✓ Confirm that each service is running and properly configured.
- ✓ Test specific features to ensure they perform as expected.

1.3 Main troubleshooting process in networking

- 1. Identify the Problem:** Collect details from users, logs, and monitoring systems.
- 2. Define the Scope of the Problem:** Determine whether the issue is local (one device or user), segment-based (a part of the network like a switch or router), or affecting the entire network.
- 3. Establish a Theory of Probable Cause: Check Simple Causes First:** Consider basic issues like misconfigurations, loose cables, or incorrect settings.
- 4. Test the Theory to Determine Cause:** Test different potential causes systematically to narrow down the problem and Use troubleshooting tools such as **ping**, **tracert**, **nslookup**, or **network analyzers** to gather data.
- 5. Establish an Action Plan:** Once the root cause is identified, plan out steps to resolve the issue. This might include reconfiguring devices, replacing faulty equipment, or updating software/firmware.
- 6. Implement the Solution:** Apply the fix as outlined in the action plan. If possible, do this in a test environment first to avoid causing further network disruptions.
- 7. Verify the Solution:** After applying the solution, confirm that it resolves the issue. Test network functionality and ensure the problem doesn't reoccur.
- 8. Document the Problem and Solution:** Record the issue, cause, and solution in detail to assist with future troubleshooting and prevent the issue from happening again.
- 9. Monitor for Recurrence:** Keep an eye on the network for any signs that the problem might reoccur, and ensure that no other network components are impacted by the changes made.

1.4 Common problem found in networking**Hardware-Related Issues**

- ✓ Physical Damage: Cables may be cut, bent, or damaged, affecting connectivity.
- ✓ Device Failures: Routers, switches, or modems might malfunction.
- ✓ Incorrect Configuration: Devices may be misconfigured, preventing proper communication.

Software-Related Issues

- ✓ Driver Problems: Outdated or corrupted drivers can cause network instability.

- ✓ Firewall Interference: Firewalls may block necessary traffic, hindering connectivity.
- ✓ Malware or Viruses: Malicious software can disrupt network operations.
- ✓ Configuration Errors: Incorrect network settings can lead to connectivity issues.

Connectivity Problems

- ✓ Limited Bandwidth: Insufficient bandwidth can slow down network performance.
- ✓ Interference: Wireless networks can be affected by interference from other devices or environmental factors.
- ✓ Network Congestion: Heavy traffic can overload network resources.

Authentication and Access Issues

- ✓ Incorrect Credentials: Users may enter incorrect passwords or usernames.
- ✓ Access Restrictions: Network policies may prevent access to certain resources.

1.5 Troubleshooting Tips

When encountering network problems, consider these troubleshooting steps:

- ✓ Check Physical Connections: Ensure cables are securely plugged in and not damaged.
- ✓ Restart Devices: Restarting routers, modems, and computers can often resolve temporary issues.
- ✓ Update Drivers: Keep device drivers up-to-date.
- ✓ Check Network Settings: Verify that network settings are correct and consistent.
- ✓ Scan for Malware: Run antivirus scans to detect and remove malicious software.
- ✓ Test Connectivity: Use tools like ping or tracert to diagnose connectivity issues.



Practical Activity 3.3.2: Checking network functionalities.



Task:

1: Refer to the previous activity 3.3.1 and key readings 3.3.2.; Read carefully the task described below:

According to key readings in trainee's manual you are asked to set up a network with a router, switch, and multiple client computers. Configure the devices with correct IP settings and confirm all clients can ping the router and access the internet. Next, inspect and resolve any physical cable or device issues. Verify network components' functionality by updating firmware, and ensure all software, including security patches, is up to date.

2: Perform the activity mentioned above by following instructions

3: Ask for clarification and assistance if needed.

4: Present your work to trainer and whole class.

5: Read key readings 3.3.2 in trainees manual



Key readings 3.3.2: Checking network Functionalities

Step-by-Step Guide to Check network Functionalities

Follow the following steps for effective check and maintain the functionalities of your network, ensuring a reliable and efficient network environment.

steps for both hardware and software-related network troubleshooting:

1. Identify the Problem

- **Gather Information:** Speak to users experiencing the problem to understand the symptoms, when the issue started, and how it manifests.
- **Check Network Documentation:** Review network diagrams, configurations, and logs to understand the network setup.
- **Define the Problem:** Clearly identify what is not working as expected. Is it a connectivity issue, a performance problem, or something else?

2. Establish a Theory of Probable Cause

- **Consider Common Issues:** Think about common causes of the problem based on symptoms (e.g., a specific error message might suggest a known issue).
- **List Possible Causes:** Develop a list of potential causes, including hardware failures, configuration errors, or software bugs.

3. Test the Theory to Determine the Cause

- **Start with the Most Likely Cause:** Test your theory by checking the most likely sources of the problem.
- **Perform Simple Tests:** Use basic tools like **ping** and **tracert** to test connectivity and path to the destination.
- **Check Physical Connections:** Ensure all cables, ports, and devices are correctly connected and functioning.

4. Plan of Action

- **Determine the Fix:** Based on the identified cause, decide on the appropriate corrective action.
- **Consider the Impact:** Evaluate the impact of your fix on the network, especially during working hours.

5. Implement the Solution

- **Apply the Fix:** Implement the solution, whether it's replacing faulty hardware, reconfiguring a device, or applying a software update.
- **Monitor the Results:** After applying the fix, monitor the network to ensure the problem is resolved.

6. Verify Full System Functionality

- **Test Network Performance:** Ensure that the network is fully operational by testing all affected components.
- **Check with Users:** Confirm with users that the problem is resolved and that no new issues have arisen.

7. Document Findings and Actions

- **Record the Issue:** Document the problem, the steps taken to resolve it, and the final solution.
- **Update Network Documentation:** If necessary, update network diagrams, configurations, and logs with any changes made during troubleshooting.

Hardware Troubleshooting Steps:

- **Check Physical Connections:** Ensure cables, connectors, and ports are properly connected and functioning.
- **Inspect Network Devices:** Look for hardware failures like broken switches, routers, or network interface cards (NICs).
- **Replace or Repair Faulty Hardware:** Swap out components or repair them as needed.
- **Check Device Indicators:** LED indicators on devices can provide quick clues about the status of hardware components.

Software Troubleshooting Steps:

- **Review Configuration Settings:** Check for misconfigurations in network devices like routers, switches, firewalls, or servers.
- **Check for Software Updates:** Ensure that all devices are running the latest firmware and software versions.
- **Analyze Logs:** Review logs from network devices, servers, and applications for error messages or warnings.
- **Use Diagnostic Tools:** Tools like Wireshark for packet analysis, NetFlow for traffic monitoring, and SNMP for device management can help identify software-related issues.

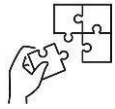
These steps provide a structured approach to troubleshooting network issues, whether they're related to hardware or software.



Points to Remember

- Troubleshooting a network is the process of identifying, diagnosing, and resolving issues that are affecting the network's performance or functionality.
- Follow the following steps for effective check and maintain the functionalities of your network, ensuring a reliable and efficient network environment.
 - ✓ Identify the Problem
 - ✓ Establish a Theory of Probable Cause

- ✓ Test the Theory to Determine the Cause
- ✓ Plan of Action
- ✓ Implement the Solution
- ✓ Verify Full System Functionality
- ✓ Document Findings and Actions



Application of learning 3.3.

You are a member of the IT team at a small office where employees are experiencing frequent network disruptions and slow internet speeds. Your assignment is to investigate and fix these issues by inspecting both physical connections and device configurations. Start by checking cables and network hardware for faults, then move on to diagnosing software issues, such as outdated firmware or misconfigured settings. Ensure that all systems are up-to-date and functioning properly. Finally, document the troubleshooting steps and solutions for future reference.



Indicative content 3.4: Elaboration of maintenance report



Duration: 2 hrs



Theoretical Activity 3.4.1: Description of maintenance report



Tasks:

- 1: Read and answer the following questions:
 - i. What is maintenance report
 - ii. What is the primary purpose of a maintenance report?
 - iii. Who is the typical target audience for a maintenance report?
 - iv. Name the essential components/elements of a maintenance report.
- 2: Provide the answers for the questions asked and write the answer on paper
- 3: Present the findings to the class
- 4: Ask questions where necessary.
- 5: Read key readings 3.4.1 in the trainee manual.



Key readings 3.4.1.: Description of maintenance report

1. Description of maintenance report

A **maintenance report** is a comprehensive document that records the activities performed during maintenance tasks, the condition of the equipment or system before and after maintenance, and any recommendations for future actions.

A well-prepared maintenance report is essential for documenting the maintenance process, ensuring that all necessary actions have been taken, and providing valuable insights for future maintenance planning.

This report is essential for ensuring transparency, accountability, and continuous improvement in maintenance practices.

2. Purpose of a maintenance report

The primary purpose of a maintenance report in networking is to document the status, actions, and results of maintenance activities performed on the network infrastructure.

3. Major Types of Maintenance Reports

Here are the major types of maintenance reports that are commonly used:

3.1. Preventive Maintenance Report

- **Purpose:** To document scheduled maintenance activities aimed at preventing equipment failures.
- **Contents:**

- ✓ List of preventive tasks performed.
- ✓ Equipment condition before and after maintenance.
- ✓ Compliance with the maintenance schedule.
- ✓ Recommendations for future preventive actions.

3.2. Corrective Maintenance Report

- **Purpose:** To record maintenance activities carried out to correct equipment failures or issues.
- **Contents:**
 - ✓ Detailed description of the problem.
 - ✓ Diagnostic methods used.
 - ✓ Corrective actions taken.
 - ✓ Tools and materials used.
 - ✓ Equipment status after maintenance.

3.3. Predictive Maintenance Report

- **Purpose:** To detail maintenance activities based on predictive data analysis and condition monitoring.
- **Contents:**
 - ✓ Data from sensors and monitoring tools.
 - ✓ Analysis and interpretation of data.
 - ✓ Predictions about potential equipment failures.
 - ✓ Maintenance actions taken based on predictions.
 - ✓ Future maintenance recommendations.

3.4. Routine Maintenance Report

- **Purpose:** To summarize regular, routine maintenance tasks performed on equipment.
- **Contents:**
 - ✓ List of routine tasks performed.
 - ✓ Frequency of tasks.
 - ✓ Equipment condition during routine checks.
 - ✓ Any issues identified and addressed.
 - ✓ Recommendations for adjustments to routine schedules.

3.5. Emergency Maintenance Report

- **Purpose:** To document unscheduled maintenance activities carried out in response to urgent equipment failures.
- **Contents:**
 - ✓ Description of the emergency situation.
 - ✓ Immediate actions taken.
 - ✓ Root cause analysis.
 - ✓ Detailed description of repairs.
 - ✓ Preventive measures to avoid future emergencies.

4. Benefits of maintenance reports

Maintenance reports provide numerous advantages to organizations, equipment managers, and maintenance teams. Including:

a. Improved Asset Management

Maintenance reports give a clear picture of how assets are performing and their condition.

This information can be used to schedule maintenance activities more efficiently and optimize asset utilization.

b. Reduced Downtime and Costs

By providing a record of all maintenance activities and their outcomes, maintenance reports can help businesses identify and address repeated issues leading to unexpected costs.

c. Improved Communication and Collaboration

Maintenance reports can be shared with all stakeholders, including maintenance teams, operations teams, and management. This promotes transparency and improves communication and collaboration between all parties.

d. Data-Driven Decision Making/informed decision making

Maintenance reports provide valuable data that can be used to make informed decisions regarding asset management, maintenance scheduling, and equipment replacement.

e. Enhance communication and Customer Satisfaction

Maintenance reports facilitate clear communication between maintenance teams, management, and clients, ensuring everyone is informed about equipment status and maintenance activities.

Well-documented maintenance reports can improve customer satisfaction by demonstrating professionalism, accountability, and effective service delivery.

5. The target audience for a maintenance report

The typical target audience for a maintenance report depends on the specific context and purpose of the report. However, some common groups that might receive maintenance reports include:

- **Management:** This includes senior executives, department heads, and other decision-makers who need to understand the overall health and performance of the organization's assets.
- **Maintenance staff:** This includes technicians, mechanics, and other personnel responsible for maintaining and repairing assets.
- **Finance department:** This group needs to understand the costs associated with maintenance and repairs.
- **Regulatory bodies:** In some industries, regulatory agencies require organizations to submit maintenance reports to ensure compliance with safety standards.

- **Stakeholders:** This could include investors, customers, or other interested parties who want to know about the organization's asset management practices.

Ultimately, the target audience for a maintenance report will depend on the specific needs and interests of the organization.

6. Elements of Maintenance Report

6.1. Client Information:

- **Client Name:** The name of the individual or organization requesting the maintenance service.
- **Contact Information:** Phone number, email address, and physical address of the client.
- **Service Location:** The specific location where the maintenance was performed.

6.2. Status Before Maintenance

- **Condition Assessment:** A detailed description of the equipment or system's condition prior to maintenance, including any observed issues or malfunctions.
- **Operational Status:** Note whether the equipment was operational, partially operational, or non-operational.
- **Previous Maintenance Records:** Reference any prior maintenance activities and their outcomes.

6.3. Implementation of Solution

- **Description of Work Performed:** Outline the specific maintenance tasks carried out, including repairs, replacements, and adjustments.
- **Timeline:** Indicate the date and duration of the maintenance work.
- **Challenges Encountered:** Mention any difficulties faced during the maintenance process and how they were resolved.

6.4. Used Tools, Materials, and Equipment

- **Tools Used:** List all tools utilized during the maintenance process (e.g., wrenches, screwdrivers, diagnostic tools).
- **Materials and Parts:** Specify any materials or replacement parts used (e.g., filters, lubricants, components).
- **Equipment:** Mention any specialized equipment employed for the maintenance tasks.

6.5. Status After Maintenance

- **Condition Assessment:** Describe the condition of the equipment or system after maintenance, highlighting improvements made.
- **Operational Status:** Indicate whether the equipment is fully operational, partially operational, or still experiencing issues.
- **Testing Results:** Include any tests conducted post-maintenance to verify

functionality and performance.

6.6. Recommendations

- **Future Maintenance:** Suggest a schedule for routine maintenance to prevent future issues.
- **Upgrades or Replacements:** Recommend any upgrades or replacements that could enhance performance or reliability.
- **Training Needs:** Identify any training requirements for the client's staff to ensure proper operation and maintenance of the equipment.



Practical Activity 3.4.2: Elaborating Maintenance report



Task:

1: Referring to the activity 3.4.1 and key readings 3.4.2.; Read the given task.

Inspect network hardware for wear and performance issues, documenting any anomalies or potential failures. Verify software updates and patches are current to ensure system security and stability. Provide recommendations for necessary repairs or upgrades based on findings.

2: Perform the given task by following the instructions.

3: Present the work to trainer or whole class.

5: Read key readings 3.4.2 in trainee Manual

6: Perform the task provided in application of learning 3.4



Key readings 3.4.2: Elaborating Maintenance report

1. Elaborating Maintenance report

The report serves as a valuable tool for tracking maintenance history, identifying potential issues, and planning future maintenance schedules.

2. Elements of a Maintenance Report

- **Client Information:** Clearly identify the client or asset owner, including name, contact information, and asset details.
- **Status Before Maintenance:** Describe the condition of the equipment or system before the maintenance work began. Include any existing problems or malfunctions.
- **Implementation of Solution:** Outline the steps taken to address the identified issues. Provide a detailed explanation of the maintenance tasks performed.
- **Used Tools, Materials, and Equipment:** List all the tools, materials, and

equipment utilized during the maintenance process.

- **Status After Maintenance:** Describe the condition of the equipment or system after the maintenance work is completed. Include any performance improvements or remaining issues.
- **Recommendations:** Provide suggestions for future maintenance or improvements based on the findings of the report.

SAMPLE OF NETWORK MAINTENANCE REPORT

Date:

[Insert Date]

Client Information

- **Client Name:** XYZ Enterprises
- **Client Contact:** KAMANA Jhon
- **Address:** 567 Dawn Town, City, Kigali
- **Client ID:** 4321

Status Before Maintenance

- **Initial Condition:**
 - **Network Devices:** Routers, switches, and access points showing intermittent connectivity issues.
 - **Observed Issues:** Frequent network drops, slow internet speed, and unresponsive network devices.
 - **Operational Impact:** Reduced productivity due to network interruptions affecting communication and access to critical applications.

Implementation of Solution

- **Actions Taken:**
 - Inspected and rebooted all network devices.
 - Updated firmware on routers and switches.
 - Replaced faulty Ethernet cables.
 - Reconfigured network settings for optimal performance.
 - Conducted a comprehensive network diagnostics test.
- **Step-by-Step Process:**
 - 1. Inspection and Reboot:**

Inspected all routers, switches, and access points for visible damage or loose connections.

Rebooted all devices to clear temporary issues.
 - 2. Firmware Update:**

Checked current firmware versions.

Downloaded and installed the latest firmware updates for routers and switches.
 - 3. Cable Replacement:**

Identified and replaced damaged or worn-out Ethernet cables.
 - 4. Reconfiguration:**

Accessed network device settings and optimized configurations for better performance.

Adjusted settings for QoS (Quality of Service) to prioritize critical traffic.

5. Diagnostics Test:

Ran network diagnostics to check for latency, packet loss, and overall performance.

Identified and resolved minor configuration issues.

- **Technicians Involved:**

- Technician 1: Michael MUNYURWA
- Technician 2: Lisa MURAVA

Used Tools, Materials, and Equipment

- **Tools:**

- Network diagnostic tools (e.g., Wireshark)
- Firmware update utilities
- Cable testers
- Screwdrivers and pliers

- **Materials:**

- Replacement Ethernet cables (Cat6)
- Firmware files

- **Equipment:**

- Laptops for configuration and diagnostics
- Safety gear

Status After Maintenance

- **Final Condition:**

- Network devices are fully operational with stable connectivity.
- Improved internet speed and overall network performance.
- No unresponsive devices detected.

- **Issues Resolved:**

- Network drops and slow internet speed.
- Faulty cables replaced, eliminating physical connection issues.

- **Operational Status:**

- The network is functioning optimally, supporting all network-dependent operations without interruption.

Recommendations

- **Future Maintenance:**

- Schedule bi-monthly network maintenance checks.
- Regularly update firmware to keep network devices secure and efficient.

- **Upgrades:**

- Consider upgrading to gigabit switches for faster internal data transfer.
- Explore the implementation of a network monitoring solution for real-time performance tracking.

- **Operational Guidelines:**

- Educate employees on basic troubleshooting steps to minimize downtime.
- Ensure network devices are properly ventilated and protected from physical damage.

Prepared by:

- **Technician 1:** MUKUNZI XY

- **Technician 2:** KARIZA WRT

Approved by:

- **Supervisor:** RUGERO FRT

Date: [Insert Date]

Client Acknowledgment:

I acknowledge that the maintenance activities described above were performed to my satisfaction.

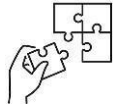
Client Signature:

Date:



Points to Remember

- Detailed maintenance report would serve as a valuable tool for the IT department to improve network reliability and performance, as well as to communicate effectively with management and staff about the state of the network.
- **Elements of a Maintenance Report**
- **Client Information:** Clearly identify the client or asset owner, including name, contact information, and asset details.
- **Status Before Maintenance:** Describe the condition of the equipment or system before the maintenance work began. Include any existing problems or malfunctions.
- **Implementation of Solution:** Outline the steps taken to address the identified issues. Provide a detailed explanation of the maintenance tasks performed.
- **Used Tools, Materials, and Equipment:** List all the tools, materials, and equipment utilized during the maintenance process.
- **Status After Maintenance:** Describe the condition of the equipment or system after the maintenance work is completed. Include any performance improvements or remaining issues.
- **Recommendations:** Provide suggestions for future maintenance or improvements based on the findings of the report.



Application of learning 3.4.

You are a member of the IT team at a small office where employees are experiencing frequent network disruptions and slow internet speeds. Your assignment is to investigate and fix these issues by inspecting both physical connections and device configurations. Start by checking cables and network hardware for faults, then move on to diagnosing software issues, such as outdated firmware or misconfigured settings. Ensure that all systems are up-to-date and functioning properly. Finally, document the troubleshooting steps and solutions for future reference.



Learning outcome 3 end assessment

Theoretical assessment

Part1: Multiple-Choice Questions

1. **Which of the following is a common practice in hardware preventive maintenance for network equipment?**
 - A) Updating firmware regularly
 - B) Installing antivirus software
 - C) Cleaning dust from hardware components
 - D) Configuring network security settings
2. **What is the primary purpose of software preventive maintenance in a network environment?**
 - A) To increase the physical lifespan of devices
 - B) To prevent hardware failures
 - C) To enhance software performance and security
 - D) To reduce the need for hardware upgrades
3. **Which tool is most commonly used to check the integrity of network cables during preventive maintenance?**
 - A) Multimeter
 - B) Cable tester
 - C) Network analyzer
 - D) Packet sniffer
3. **During preventive maintenance, why is it important to keep firmware up to date on network devices?**
 - A) To ensure compatibility with older software
 - B) To avoid overheating of hardware components
 - C) To prevent unauthorized physical access to devices
 - D) To patch security vulnerabilities and improve device performance
4. **What should be done before performing any hardware preventive maintenance on network equipment?**
 - A) Disconnect the device from the network
 - B) Update the operating system
 - C) Back up the current configuration
 - D) Install a new antivirus program

Part2: Answer true or false questions related to corrective maintenance in networking.

1. Corrective maintenance involves making changes to a network configuration after a failure or problem has been identified.
2. Corrective maintenance in networking is only performed on software components, not hardware.
3. Replacing a faulty network switch with a new one is an example of corrective maintenance.
4. Corrective maintenance is typically performed on a scheduled basis, even if no issues are present.
5. The primary goal of corrective maintenance is to restore network functionality after a disruption.
6. Corrective maintenance should always be documented to ensure a record of what was done and why.
7. Updating antivirus software to protect against new threats is considered corrective maintenance.
8. Corrective maintenance is only necessary when a complete network failure occurs.

Part3:

1. What are the three main ways of reporting the outcome of a network maintenance activity?
2. Why is it important to include the tools, materials, and equipment used in a maintenance report?

Practical assessment

ABC Corp, a mid-sized business, has been experiencing intermittent connectivity issues, slow network speeds, and frequent downtime. The network infrastructure includes multiple switches, routers, firewalls, and access points supporting both wired and wireless connections across several floors. The IT team is tasked with diagnosing and resolving these issues to ensure long-term network stability.

END



Reference

Books:

D'Eramo, J. (2019). *Data center networking: A practical guide*. Burlington, MA: Elsevier.

Hawkins, R. (2019). *Cloud networking essentials*. Farnham, UK: Wiley.

Limoncelli, T. (2017). *Network administration: A practical approach*. Sebastopol, CA: O'Reilly Media.

Odom, W., & Wallace, K. (2021). *CCNP enterprise core ENCOR official cert guide*. Indianapolis: Cisco Press.

Stallings, W. (2018). *Network security essentials: A beginner's guide*. Boston: Pearson.

Web links :

ConnectWise. (n.d.). Network maintenance checklist: Tasks. ConnectWise. Retrieved from <https://www.connectwise.com/blog/rmm/network-maintenance-checklist-tasks>

Evernex. (n.d.). Network maintenance checklist: A guide for IT professionals. Evernex. Retrieved from <https://evernex.com/blog/network-maintenance-checklist-a-guide-for-it-professionals/>

HowToNetwork. (n.d.). Network maintenance tasks. HowToNetwork. Retrieved from <https://www.howtonetwork.org/tshoot/module-1/network-maintenance-tasks/>

Network Lessons. (n.d.). Network maintenance. Retrieved from <https://networklessons.com/cisco/ccie-routing-switching-written/network-maintenance#:~:text=Network%20maintenance%20basically%20means%20you,Monitoring%20and%20improving%20network%20performance>

NileSecure. (n.d.). Network maintenance. NileSecure. Retrieved from <https://nilesecure.com/network-management/network-maintenance>

Worldwide Services. (n.d.). Network maintenance guide and upkeep. Worldwide Services. Retrieved from <https://worldwideservices.net/network-maintenance-guide-upkeep/>

WPGC. (n.d.). Mastering network maintenance: 11 essential tasks for peak performance. WPGC. Retrieved from <https://wpgc.io/blog/mastering-network-maintenance-11-essential-tasks-for-peak-performance/>



October 2024