Competency Based Learning Material (CBLM)

IT Support Service

Level-4

Module: Setting-up and Expanding Networks

Code: CBLM-ICT-ITSS-02-L4-V1

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

Copyright

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

This Competency Based Learning Materials (CBLM) on "Set-up and Expand Networks" under the IT Support Service, Level-4" qualification is developed based on the national competency standard approved by National Skills Development Authority (NSDA)

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

National Skills Development Authority (NSDA) is the owner of this document. Other interested parties must obtain written permission from NSDA for reproduction of information in any manner, in whole or in part, of this Competency Standard, in English or other language.

It serves as the document for providing training consistent with the requirements of industry in order to meet the qualification of individuals who graduated through the established standard via competency-based assessment for a relevant job.

This document has been developed by NSDA with the assistance of related specialist/trainer /related employee

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

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

How to use this Competency Based Learning Material (CBLM)

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

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

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

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

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

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

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

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

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

Table of Contents

Module Content

Unit of Competency	**Set-up and Expand Networks**
Unit Code	**OU-ICT-ITSS-02-L4-V1**
Module Title	**Setting-up and Expanding Networks**
Module Descriptor	This unit covers the knowledge, skills and attitude required to set-up and expand networks. It includes the task of gathering organizational requirements of an existing network, planning and design to expand an existing network, expanding the existing network, testing newly expanded network, and maintaining record of maintenance.
Nominal Hours	40 Hours
Learning Outcome	After completing the practice of the module, the trainees will be able to perform the following jobs: 1. Gather organizational requirements of an existing network. 2. Plan and design to expand an existing network. 3. Expand the existing network. 4. Test the newly expanded network. 5. Maintain record of maintenance

Assessment Criteria

1. Organizational requirements to expand an existing network are collected.
2. Existing network design is reviewed for expansion of the network.
3. Collected information is documented.
4. Collected information is analyzed and a network design plan is prepared.
5. The network design plan is reviewed and approved by the appropriate person in the organization.
6. Required equipment and tools are listed and the estimated budget is calculated and documented.
7. Estimated budget and required equipment list are discussed with and approved by the appropriate person.
8. According to the approved network design plan an existing network is deployed
9. If the Internet is in the plan, the network is connected to the Internet.
10. Equipment and materials are collected to expand the network.
11. Nodes are connected to the network.
12. Deployment of the network is performed.
13. Network diagnostic tools are installed for network testing.
14. Using network diagnostic tools, network is tested.
15. Congestion of the network is observed.
16. Reachability to Internet (if available) is tested.
17. Network maintenance plan is completed.
18. Network maintenance plan is approved by the appropriate person or from the organization.
19. Approved network maintenance plan is documented.
20. Support plan for the network is documented.
21. User manual for the network is prepared.

Learning Outcome-1: Gather Organizational Requirements of An Existing Network

Assessment Criteria	1. Organizational requirements to expand an existing network are collected. 2. Existing network design is reviewed for expansion of the network. 3. Collected information is documented
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Multimedia Projector 6. Paper, Pen, Pencil, and Eraser 7. Internet Facilities 8. Whiteboard and Marker
Contents	1 Organizational expansional requirements ▪ Within network (Same network) ▪ Intra-network (Subnetting) ▪ External Network (Different network) 2 Review process of existing network design for expansion 3 Process to collect information from existing networks and nodes. 4 Process to document the information from existing networks and nodes.
Activities/job/Task	1. Conduct interviews with key stakeholders (department heads, IT staff, users) to understand their current and future network needs. 2. Review existing documentation like network diagrams, policies, and service level agreements (SLAs) to understand the current network infrastructure and its limitations. 3. Analyze the existing network topology (star, mesh, etc.) to assess its scalability and suitability for expansion
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning 4. Portfolio

Learning Experience-1: Gather Organizational Requirements of an Existing Network

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

Learning Activities	Recourses/Special Instructions
1. Students will ask the instructor about "Gather organizational requirements of an existing network."	A. Instructor will provide the learning materials "Gather organizational requirements of an existing network."
2. Read the Information sheet and complete the Self-check & Check answer sheets on "Gather organizational requirements of an existing network."	1. Read Information sheet: a. Organizational expansion requirements b. Review process of existing network design for expansion c. Process to collect information from existing networks and nodes. d. Process to document the information from existing networks and nodes. 2. Answer Self-check 1: Gather organizational requirements of an existing network. 3. Check your answer with Answer key 1: Gather organizational requirements of an existing network
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	4. Job/Task Sheet and Specification Sheet **Job Sheet 1.1:** Conduct interviews with key stakeholders (department heads, IT staff, users) to understand their current and future network needs. **Job Sheet 1.2:** Review existing documentation like network diagrams, policies, and service level agreements (SLAs) to understand the current network infrastructure and its limitations. **Job Sheet 1.3:** Analyze the existing network topology (star, mesh, etc.) to assess its scalability and suitability for expansion. **Specification Sheet 1.1:** Gather organizational requirements of an existing network. Task Sheet 1.2: Gather organizational requirements of an existing network.

Information Sheet-1: Gather Organizational Requirements of an Existing Network

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

1.1 Organizational expansional requirements
   A. Within network (Same network)
   B. Intra-network (Subnetting)
   C. External Network (Different network)
1.2 Review process of existing network design for expansion
1.3 Process to collect information from existing networks and nodes.
1.4 Process to document the information from existing networks and nodes.

1.1 Organizational expansion requirements

Organizational expansion requirements require assessing network capacity, scalability, and security measures. This may include subnetting for efficient resource allocation and establishing secure connections with external networks. So, we can classify this among the three categories:

A. Within network (Same network)
   When organizations grow, their network requirements often expand within the existing network infrastructure. This expansion within the same network involves accommodating more devices, users, or services without altering the network's fundamental architecture. Here are key considerations:

   - Capacity Planning: Assess the current network capacity to determine if it can support additional devices or services. Consider factors such as bandwidth, switch port availability, and server capacity.

   - Scalability: Evaluate the scalability of network devices such as switches, routers, and access points. Ensure they can handle increased traffic and connections without performance degradation.

   - Security: Review and enhance network security measures to accommodate new devices or services. This may involve updating firewall rules and access control lists or implementing additional security protocols.

   - Quality of Service (QoS): Determine if QoS parameters need adjustment to prioritise critical traffic types as the network expands. This ensures that

essential services receive adequate bandwidth and that latency requirements are met.

B. Intra-network (Subnetting)
Subnetting involves dividing a larger network into smaller, manageable subnetworks to improve efficiency and security. When expanding within the same network through subnetting, consider the following:

- Address Space Planning: Determine the appropriate IP address space for the new subnets based on the organization's growth projections and current address allocation.

- Subnet Design: Design subnets based on geographical location, departmental segregation, or functional requirements. Ensure each subnet has sufficient IP addresses to accommodate future growth.

- Routing Configuration: Configure routing protocols to enable communication between subnets while maintaining security and performance. Implement routing policies to control traffic flow between different parts of the network.

- Security Measures: Implement subnet-level security measures such as access control lists (ACLs), VLAN segmentation, and network segmentation to isolate and secure sensitive network segments.

C. External Network (Different network)
Expanding into external networks involves connecting to networks outside the organization's immediate infrastructure. Consider the following when expanding into different networks:

- Interconnection Technologies: Evaluate interconnection technologies such as VPNs (Virtual Private Networks), MPLS (Multiprotocol Label Switching), or leased lines to establish connectivity with external networks.

- Network Address Translation (NAT): Implement NAT mechanisms to facilitate communication between internal and external networks while hiding internal IP addresses from external entities.

- Firewall Configuration: Configure firewalls to enforce security policies and filter traffic between internal and external networks. Define rules to allow only authorised traffic to traverse the network boundary.

- Traffic Prioritization: Prioritize network traffic to ensure essential services have adequate bandwidth and quality of service when communicating with external networks.

1.2 Review process of existing network design for expansion

Reviewing the existing network design is crucial to ensure compatibility, efficiency, and scalability before expanding. The process involves:

- Assessment of Current Design: Evaluate the current network infrastructure, considering topology, equipment, protocols, and configurations to identify strengths, weaknesses, and potential bottlenecks.

- Gap Analysis: Identify gaps between current network capabilities and anticipated expansion requirements. This involves analyzing factors such as bandwidth, latency, security, and scalability to determine areas for improvement.

- Documentation Review: Examine existing network documentation, including network diagrams, configuration files, and inventory lists, to gain insights into the network's structure and components.

- Stakeholder Consultation: Engage with network administrators, IT personnel, and department heads to gather insights, requirements, and concerns regarding network expansion. This ensures alignment with organizational goals and user needs.

- Risk Assessment: Conduct a risk assessment to identify potential risks and vulnerabilities associated with network expansion. This includes assessing the impact of expansion on network performance, security, and compliance with regulatory requirements.

- Feasibility Analysis: Evaluate the feasibility of proposed expansion plans based on technical, financial, and operational considerations. This includes assessing resource availability, budget constraints, and potential disruptions to ongoing operations.

1.3 Process to collect information from existing networks and nodes

Collecting information from existing networks and nodes is essential for understanding the current infrastructure and planning for expansion. The process involves the following steps:

- Network Inventory: Begin by compiling an inventory of all network devices, including routers, switches, firewalls, servers, and endpoints. Document their make, model, serial numbers, firmware versions, and configurations.

- Topology Mapping: Create a network topology map to visualise the interconnections between devices and the overall network layout. This helps identify network segments, bottlenecks, and potential points of failure.

- Configuration Backup: Back up the configurations of network devices to preserve their current settings and ensure rapid recovery in case of configuration errors or device failures. Use automated tools or scripts to streamline the backup process.

- Traffic Analysis: Analyze network traffic using packet sniffers or network monitoring tools to identify patterns, trends, and anomalies. This provides insights into network utilization, bandwidth requirements, and potential performance issues.

- Security Assessment: Perform a security assessment to identify network vulnerabilities, misconfigurations, and compliance gaps. This includes scanning for open ports, outdated firmware, weak encryption, and unauthorized devices.

- Performance Monitoring: Monitor network performance metrics such as latency, packet loss, throughput, and error rates to assess the network's health and efficiency. Use monitoring tools to collect real-time data and generate performance reports.

- Documentation Review: Review existing network documentation, including network diagrams, configuration files, change logs, and incident reports. This provides context and historical insights into the evolution of the network infrastructure.

- User Feedback: Gather feedback from network users, administrators, and other stakeholders to understand their experiences, challenges, and requirements. This helps identify user-centric issues and opportunities for improvement.

1.4 Process to document the information from existing networks and nodes

Documenting information from existing networks and nodes is crucial for maintaining an organized and up-to-date record of the network infrastructure. The process involves the following steps:

- Create a Documentation Framework: Establish a standardized framework for organizing network documentation. This framework should include categories such as network topology, device configurations, IP addressing schemes, security policies, and troubleshooting procedures.

- Network Diagrams: Develop detailed network diagrams that illustrate the physical and logical layout of the network. Include information about device placement,

interconnections, VLANs, subnets, and routing protocols. Use diagramming tools such as Visio or Lucid chart for clarity and consistency.

- Device Inventory: Maintain an inventory of network devices, including routers, switches, firewalls, servers, and endpoints. Document each device's make, model, serial number, firmware version, physical location, and role within the network.

- Configuration Management: Store and organize device configurations in a centralized repository. This includes configuration files for routers, switches, firewalls, and other network devices. Use version control systems or configuration management tools to track changes and maintain a history of configurations.

- IP Address Management (IPAM): Implement an IPAM solution to manage IP address allocation and assignment. Document IP address ranges, subnets, DHCP scopes, and static IP assignments. Ensure consistency and avoid IP address conflicts by regularly updating the IPAM database.

- Security Policies and Procedures: Document network security policies, procedures, and best practices. This includes firewall rules, access control lists (ACLs), encryption standards, authentication mechanisms, and incident response protocols. Review and update security documentation regularly to address emerging threats and compliance requirements.

- Regular Updates and Reviews: Regularly update and review network documentation to reflect changes in the network environment. Schedule periodic audits to verify the accuracy and completeness of documentation. Encourage collaboration among team members to contribute updates and improvements to network documentation.

Self-Check-1: Gather Organizational Requirements of an Existing Network

Questionnaire

1. What are the key considerations for expanding within the same network infrastructure?
   Answer

2. How does subnetting contribute to network expansion within the same network?
   Answer

3. What technologies can be evaluated for connecting to external networks during expansion?
   Answer

4. Why is a risk assessment necessary during the existing network design review process for expansion?
   Answer

5. What role does stakeholder consultation play in the review process of existing network design?
   Answer

6. How can network documentation assist in understanding the current infrastructure during the information collection process?
   Answer

7. What tools can be used for network traffic analysis during the information collection?
   Answer

8. Why is it important to gather user feedback during the information collection process?
   Answer

9. How can network diagrams assist in documenting information from existing networks and nodes?
   Answer

10. What steps are involved in documenting information from existing networks and nodes?
    Answer

Answer Key-1: Gather Organizational Requirements of an Existing Network

1. What are the key considerations for expanding within the same network infrastructure?
   Answer: Capacity planning, scalability assessment, security enhancement, and quality of service prioritization are vital considerations.

2. How does subnetting contribute to network expansion within the same network?
   Answer: Subnetting divides a larger network into smaller, manageable subnetworks, improving efficiency and security while accommodating growth.

3. What technologies can be evaluated for connecting to external networks during expansion?
   Answer: VPNs, MPLS, and leased lines are common interconnection technologies for connecting to external networks.

4. Why is a risk assessment necessary during the existing network design review process for expansion?
   Answer: A risk assessment identifies potential risks and vulnerabilities associated with network expansion, aiding in mitigation planning.

5. What role does stakeholder consultation play in the review process of existing network design?
   Answer: Stakeholder consultation helps gather insights, requirements, and concerns, ensuring alignment with organizational goals and user needs.

6. How can network documentation assist in understanding the current infrastructure during the information collection process?
   Answer: Network documentation provides insights into the network's structure, components, and historical evolution.

7. What tools can be used for network traffic analysis during the information collection?
   Answer: Packet sniffers and network monitoring tools are commonly used for network traffic analysis.

8. Why is it important to gather user feedback during the information collection process?
   Answer: User feedback provides insights into user experiences, challenges, and requirements, aiding in identifying user-centric issues and improvement opportunities.

9. How can network diagrams assist in documenting information from existing networks and nodes?
   Answer: Network diagrams illustrate the physical and logical layout of the network, providing a visual representation for documentation purposes.

10. What steps are involved in documenting information from existing networks and nodes?
    Answer: Establishing a documentation framework, creating network diagrams, maintaining device inventory, managing configurations, implementing IP address management, documenting security policies, and conducting regular updates and reviews.

Learning Outcome-2: Plan And Design to Expand an Existing Network

Assessment Criteria	1. Collected information are analyzed and a network design plan is prepared. 2. Network design plan is reviewed and approved from the appropriate person of the organization. 3. Required equipment and tools are listed and estimated budget calculated and documented. 4. Estimated budget and required equipment list are discussed with and approved by the appropriate person arch tools are identified;
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Multimedia Projector 6. Paper, Pen, Pencil, and Eraser 7. Internet Facilities 8. Whiteboard and Marker
Contents	1 Information required to collect from existing network: ▪ Network topology ▪ Protocol to be used • NFS • HTTP • HTTPS • FTP • SNMP ▪ Address plan ▪ IP routing ▪ NAT ▪ PAT 2 Review process of network design plan 3 Estimating and budgeting for equipment and tools
Activities/job/Task	1 Plan and design to expand an existing network using following Activity: ▪ Analyze the collected information to identify gaps between current network capabilities and anticipated future needs. ▪ Analyze the collected information to identify gaps between current network capabilities and anticipated future needs.

	▪ Create different network design options considering scalability, security, budget, and future flexibility. ▪ Evaluate each design option based on its technical feasibility, cost-effectiveness, and alignment with organizational goals. ▪ Select the optimal design option and refine it based on further analysis and feedback. ▪ Create a comprehensive document outlining the chosen design, including topology, components, specifications, and implementation steps. ▪ Obtain formal approval for the network design plan from the appropriate authority within the organization. ▪ Based on the approved design plan, create a detailed list of all required hardware, software, and tools for the network expansion. ▪ Present the budget estimation to the relevant authority for discussion and approval.
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning 4. Portfolio

Learning Experience-2: Plan And Design to Expand an Existing Network

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

Learning Activities	Recourses/Special Instructions
1. Student will ask the instructor about "Plan and design to expand an existing network."	1. Instructor will provide the learning materials "Plan and design to expand an existing network."
2. Read the Information sheet and complete the Self Checks & Check answer sheets on "Plan and design to expand an existing network."	1. Read Information sheet: a. Information required to collect from existing network b. Review process of network design plan c. Estimating and budgeting for equipment and tools 2. Answer Self-check 2: Plan and design to expand an existing network. 3. Check your answer with Answer key 2: Plan and design to expand an existing network
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	1. Job/Task Sheet and Specification Sheet **Job Sheet 2.1:** Plan and design to expand an existing network. **Specification Sheet 2.1:** Plan and design to expand an existing network. Task Sheet 2.1: Plan and design to expand an existing network.

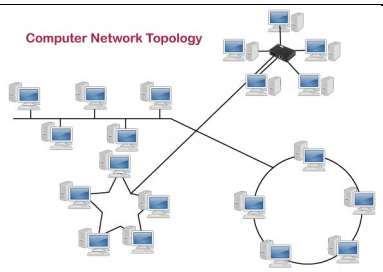
Information Sheet-2: Plan And Design to Expand an Existing Network

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

2.1 Information required to collect from existing network
2.2 Review process of network design plan
2.3 Estimating and budgeting for equipment and tools

2.1 Information required to collect from existing network

Network Topology:

A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topologies are often represented as a graph.	 Figure 1: Network Topology

Network topologies describe the arrangement of networks and the relative location of traffic flows. Administrators can use network topology diagrams to determine the best placements for each node and the optimal path for traffic flow. With a well-defined and planned-out network topology, an organization can more easily locate faults and fix issues, improving its data transfer efficiency.

Impotency of network topology

Network topology plays a major role in how a network functions. Namely, the topology has a direct effect on network functionality. Choosing the right topology can help increase performance, as a properly chosen and maintained network topology increases energy efficiency and data transfer rates.

Types of Network Topology:

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology. The various network topologies are-

- Bus Topology,
- Ring Topology,
- Tree Topology,
- Star Topology,
- Mesh Topology, and

- Hybrid Topology.

a. Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.

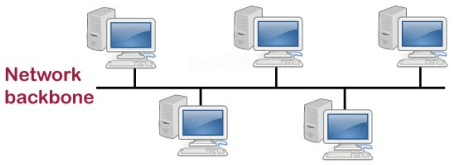


Figure 2: Bus Topology

b. Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A few repeaters are used for Ring topology with many nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

Figure 3: Ring Topology

c. Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node, and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

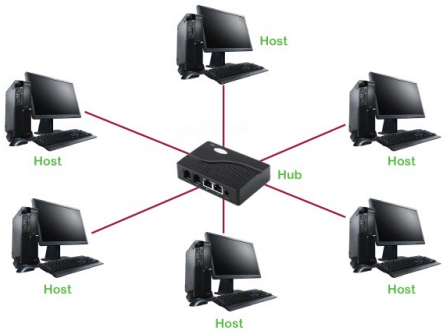


Figure 4: Star Topology

d. Tree Topology:

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.

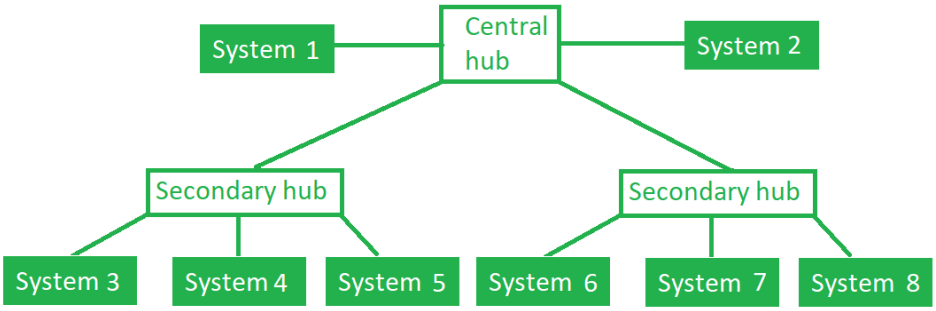


Figure 5: Tree Topology

In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

e. Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

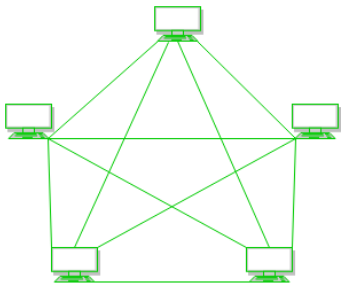


Figure 6: Mesh Topology

Every device is connected to another via dedicated channels. These channels are known as links.

- Suppose, the N number of devices relate to each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N (N-1).
- Suppose, N number of devices relate to each other in a mesh topology, then the total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 54/2 = 10.

f. Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination

of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.

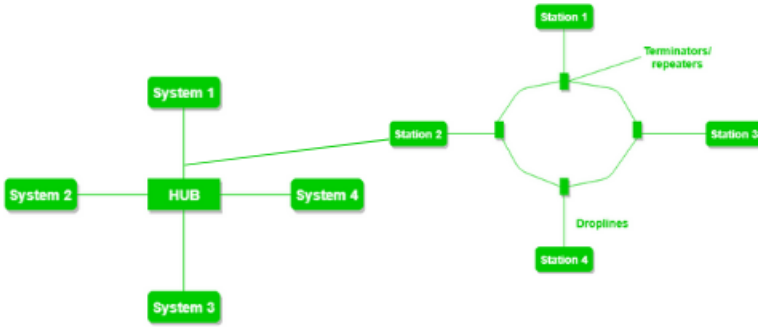


Figure 7: Hybrid Topology

The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

Network protocol?

In networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless.

Standardized protocols are like a common language that computers can use, similar to how two people from different parts of the world may not understand each other's native languages, but they can communicate using a shared third language. If one computer uses the Internet Protocol (IP) and a second computer does as well, they will be able to communicate — just as the United Nations relies on its 6 official languages to communicate amongst representatives from all over the globe. But if one computer uses IP and the other does not know this protocol, they will be unable to communicate.

On the Internet, there are different protocols for different types of processes. Protocols are often discussed in terms of which OSI model layer they belong to.

What are the layers of the OSI model?

The Open Systems Interconnection (OSI) model is an abstract representation of how the Internet works. It contains 7 layers, with each layer representing a different category of networking functions.

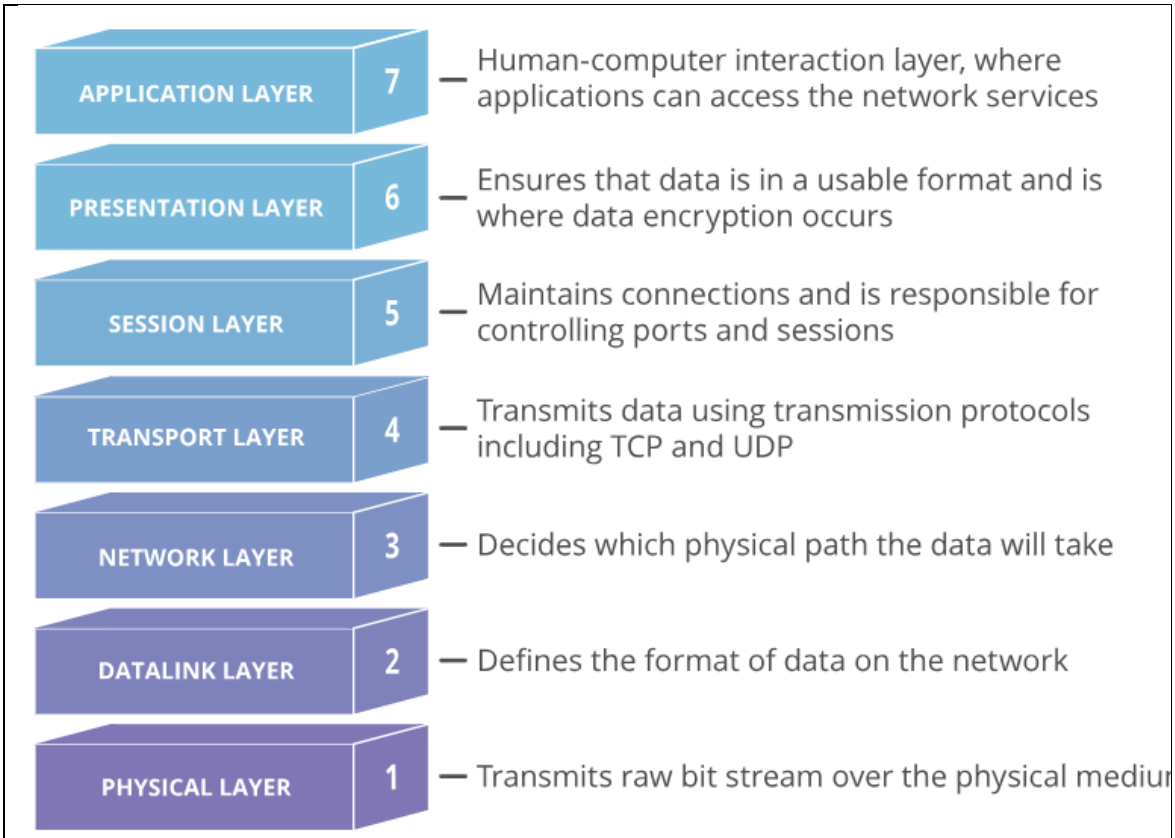


Figure 8: OSI Model Layer

Protocols make these networking functions possible. For instance, the Internet Protocol (IP) is responsible for routing data by indicating where data packets come from and what their destination is. IP makes network-to-network communications possible. Hence, IP is considered a network layer (layer 3) protocol.

NFS (Network File System)

NFS is a distributed file system protocol that allows a user on a client computer to access files over a network as if they were local to that computer. Here's a basic description of how NFS works and some considerations for its use:

- Client-Server Architecture: NFS operates on a client-server architecture. The system exporting the file system is the NFS server, while the systems mounting the exported file systems are NFS clients.
- Exporting File Systems: On the NFS server, administrators specify which directories or file systems are to be made available to NFS clients. These directories are then "exported" to the network.

- Mounting File Systems: On the NFS client, administrators specify which remote directories they want to access. These directories are then "mounted" onto the local file system, making them accessible to users and applications on the client system.

- File Access: Once mounted, the files and directories on the NFS server can be accessed and manipulated by users and applications on the client system just like

local files. NFS transparently handles the network communication and file operations.

- Network Transparency: NFS provides network transparency, meaning that users and applications don't need to be aware that the files they're accessing are located on a remote server. They interact with the files in the same way they would with local files.

- Performance Considerations: NFS performance can be affected by factors such as network latency, server load, and the size of files being transferred. Optimizing network performance and properly configuring NFS settings can help improve performance.

- Security: NFS originally lacked strong security features, but newer versions (such as NFSv4) include support for stronger authentication and encryption mechanisms. It's important to configure NFS securely to protect sensitive data from unauthorized access.

- Compatibility: NFS is widely supported on Unix-like operating systems, including Linux and various flavors of Unix. It's less commonly used on Windows systems, although there are third-party NFS clients available for Windows.

Overall, NFS is a convenient and efficient way to share files and directories across a network, particularly in Unix/Linux environments. However, proper configuration and security measures are important to ensure reliable and secure operation.

HTTP (Hypertext Transfer Protocol)

HTTP is the foundation of data communication for the World Wide Web. It's a protocol that defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands. Here's an overview of HTTP:

- Request-Response Model: HTTP operates on a request-response model. A client (usually a web browser) sends a request to a server for a specific resource, such as a web page or an image. The server then processes the request and sends back a response containing the requested resource, along with metadata such as headers and status codes.
- Stateless Protocol: HTTP is stateless, meaning that each request from a client to a server is independent and unrelated to any previous requests. This simplifies implementation and improves reliability but requires additional mechanisms (such as cookies or sessions) for maintaining state between requests if needed.

- URI (Uniform Resource Identifier): Resources on the web, such as web pages, images, and files, are identified by URIs. A URI typically consists of a scheme (e.g., "http://" for HTTP), a domain name, and a path to the resource on the server.

- Methods: HTTP defines several request methods, or verbs, that indicate the desired action to be performed on the resource. Common methods include GET (retrieve a resource), POST (submit data to be processed), PUT (create or update a resource), DELETE (remove a resource), and others.
- Headers: HTTP messages include headers, which contain metadata about the request or response. Headers can convey information such as the content type, content length, caching directives, and more.
- Status Codes: HTTP responses include status codes that indicate the outcome of the request. Status codes are grouped into different categories, such as 1xx for informational responses, 2xx for successful responses, 3xx for redirection, 4xx for client errors, and 5xx for server errors.
- Security: HTTP by itself does not provide encryption or authentication, leaving transmitted data vulnerable to interception or tampering. HTTPS (HTTP Secure) adds a layer of encryption using SSL/TLS protocols to ensure the confidentiality and integrity of data transmitted over the network.
- Versioning: HTTP has undergone several revisions over the years. The latest major version as of my last update is HTTP/2, which introduced improvements in performance, such as multiplexing and header compression.

HTTP is fundamental to the functioning of the modern web, enabling the retrieval and display of web pages, the submission of form data, and various other interactions between clients and servers.

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is the secure version of HTTP, designed to provide secure communication over the internet. It adds a layer of encryption to HTTP, ensuring that data exchanged between the client and server is encrypted and protected from eavesdropping and tampering. Here's an overview of HTTPS:

- Encryption: HTTPS encrypts data using SSL (Secure Sockets Layer) or its successor, TLS (Transport Layer Security). This encryption ensures that even if intercepted, the data remains unreadable to unauthorized parties.
- Authentication: HTTPS uses digital certificates to authenticate the identity of the website or server. These certificates are issued by trusted Certificate Authorities (CAs) and contain information about the website's owner and public key.
- Secure Communication: When a client connects to a website using HTTPS, the server presents its digital certificate to the client to prove its identity. The client verifies the certificate against a list of trusted CAs and ensures that the certificate is valid and not expired. Once the authentication is successful, the client and server establish a secure connection and exchange encrypted data.
- URL Scheme: HTTPS URLs begin with "https://" instead of "http://", indicating that the communication between the client and server is encrypted and secured.

- Data Integrity: HTTPS ensures data integrity by using cryptographic mechanisms to detect any tampering or modification of the transmitted data. If the data is altered during transmission, the recipient will detect it and reject the communication.
- Compatibility: Most modern web browsers support HTTPS, and many websites have migrated to HTTPS to ensure the security and privacy of their users' data. Additionally, search engines like Google prioritize HTTPS websites in search results, encouraging wider adoption.
- Performance: While HTTPS adds overhead due to encryption and decryption processes, advancements in SSL/TLS protocols and server optimizations have minimized the performance impact. In fact, the benefits of security and privacy outweigh the slight performance trade-off.
- Mixed Content: HTTPS pages should not contain mixed content, meaning that all resources (such as images, scripts, and stylesheets) should also be loaded over HTTPS to avoid security warnings and potential vulnerabilities.

Overall, HTTPS is essential for securing sensitive data transmitted over the internet, such as login credentials, financial information, and personal data. It helps protect users' privacy and prevents unauthorized access to sensitive information.

FTP (File Transfer Protocol)

FTP is a standard network protocol used for transferring files between a client and a server on a computer network, typically the internet. Here's an overview of FTP:

- Client-Server Architecture: FTP operates on a client-server model. The FTP server runs on a remote machine, while the FTP client is software installed on the user's local machine.
- Authentication: Users typically authenticate themselves to the FTP server using a username and password. Some FTP servers may allow anonymous access, where users can log in without providing credentials.
- Commands: FTP clients interact with FTP servers using a set of commands defined by the FTP protocol. These commands include actions such as uploading files (PUT), downloading files (GET), navigating directories (CD), listing directory contents (LS), and deleting files (DELETE), among others.
- Modes of Operation:
  - Active Mode: In active mode FTP, the client initiates a data connection to the server for file transfers. This mode may encounter issues with firewalls and network address translation (NAT) devices.
  - Passive Mode: In passive mode FTP, the server initiates a data connection to the client for file transfers. Passive mode is often used to bypass firewall restrictions and NAT issues.

- Data Transfer: FTP supports two modes of data transfer: ASCII mode and binary mode.
  - ASCII Mode: Used for transferring text files, ASCII mode converts the end-of-line characters to match the conventions of the destination platform.

- Binary Mode: Used for transferring binary files, such as images or executables, without any conversion.

- Security: Traditional FTP does not encrypt data during transmission, making it vulnerable to eavesdropping and data interception. FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol) are secure alternatives that provide encryption and authentication mechanisms to protect data in transit.
- Port Numbers: FTP uses two port numbers for communication:
  - Port 21: The default control port for FTP commands and responses.
  - Port 20: Used for data transfer in active mode FTP.
- Usage: FTP is commonly used for uploading website files to a web server, downloading software updates from a repository, transferring large files between computers, and sharing files within an organization.

SNMP (Simple Network Management Protocol)

SNMP is a protocol used for managing and monitoring network devices and their functions. It's commonly used in network management systems to collect information from various devices, monitor their status, and manage configuration changes. Here's an overview of SNMP:

- Agent-Manager Architecture: SNMP operates on a client-server architecture, where managed devices (such as routers, switches, servers, printers, etc.) run SNMP agents. These agents collect and store management information and respond to requests from SNMP managers. SNMP managers are typically network management systems that monitor and control managed devices.
- Managed Information: SNMP manages information in the form of variables organized in a hierarchical structure called the Management Information Base (MIB). Each variable in the MIB represents a specific aspect of a managed device or system, such as CPU utilization, network traffic, system uptime, and more.
- GET and SET Operations: SNMP uses two primary operations for interacting with managed devices:
  - GET: SNMP managers can retrieve the value of specific variables from SNMP agents using GET requests. This allows managers to collect information about the status and performance of managed devices.
  - SET: SNMP managers can also modify the values of variables in SNMP agents using SET requests. This enables managers to remotely configure devices and change their behavior.
- Traps and Notifications: SNMP agents can also send unsolicited messages called traps or notifications to SNMP managers to inform them about significant events or conditions, such as system errors, interface status changes, or threshold crossings. This allows managers to proactively monitor the network and respond to critical events promptly.
- Versions: SNMP has several versions, including SNMPv1, SNMPv2c, SNMPv2u, and SNMPv3. Each version offers different levels of security and functionality:

- SNMPv1 and SNMPv2c: These versions lack strong security features and use community strings for authentication, making them vulnerable to unauthorized access and data interception.
- SNMPv3: SNMPv3 introduces robust security features, including message encryption, user authentication, and access control, to protect sensitive information and ensure the integrity of SNMP communication.

Network Addressing Plan

Designing a network address plan for expanding a network involves careful consideration of IP addressing, subnetting, routing, and future growth. Here is a structured approach to creating an effective network address plan for expansion:

- **Assess Current Infrastructure**
  - Understand the current network topology, including the number of devices, subnets, and IP address usage.
  - Identify any limitations or bottlenecks in the existing addressing scheme.

- **Define Addressing Requirements**
  - Determine the number of devices and subnets needed to support the expanded network.
  - Consider factors such as scalability, security, and geographical distribution of resources.
- **Choose IP Addressing Scheme**
  - Select an appropriate IP addressing scheme, such as IPv4 or IPv6, based on compatibility requirements and future-proofing considerations.
  - Decide whether to use private or public IP addresses, considering security and routing implications.

- **Subnetting**
  - Divide the network into smaller subnets to efficiently allocate IP addresses and manage network traffic.
  - Determine the subnet mask and subnet size based on the number of devices and expected growth.
  - Reserve subnets for specific purposes, such as VLANs, servers, wireless networks, and guest networks.

- **Address Assignment**
  - Develop a consistent addressing plan for assigning IP addresses to devices within each subnet.
  - Consider using DHCP (Dynamic Host Configuration Protocol) for dynamic address allocation to simplify management and conserve IP address space.
  - Reserve static IP addresses for critical devices, servers, and network infrastructure components.

Routing and Inter-VLAN Communication:

- Plan routing between subnets to enable communication between different network segments.
- Implement routing protocols such as OSPF (Open Shortest Path First) or BGP (Border Gateway Protocol) to dynamically exchange routing information and optimize network traffic.
- Configure routing policies and access control lists (ACLs) to control traffic flow and enforce security policies.

- **Documentation and Documentation:**
  - Document the network address plan, including IP address assignments, subnet configurations, routing tables, and firewall rules.
  - Maintain accurate records of IP address allocations, leases, and changes to facilitate troubleshooting and auditing.

- **Scalability and Future Growth:**
  - Design the address plan with scalability in mind to accommodate future expansion and new requirements.
  - Reserve address space and subnets for anticipated growth, mergers, acquisitions, and new services.
  - Regularly review and update the address plan to adapt to changing network needs and technologies.
- **Testing and Validation:**
  - Test the network address plan in a lab environment or using network simulation tools to verify its effectiveness and identify any issues.
  - Conduct pilot deployments and gradual rollouts to minimize disruptions and ensure smooth transition to the new address scheme.

By following these steps and considerations, you can develop a robust network address plan for expanding your network that meets current requirements, supports future growth, and enhances overall network performance and reliability.

IP Routing

IP routing is the process that defines the shortest path through which data travels to reach from source to destination. It determines the shortest path to send the data from one computer to another computer in the same or different network. Routing uses different protocols for the different networks to find the path that data follows. It defines the path through which data travel across multiple networks from one computer to other. Forwarding the packets from source to destination via different routers is called routing. The routing decision is taken by the routers.

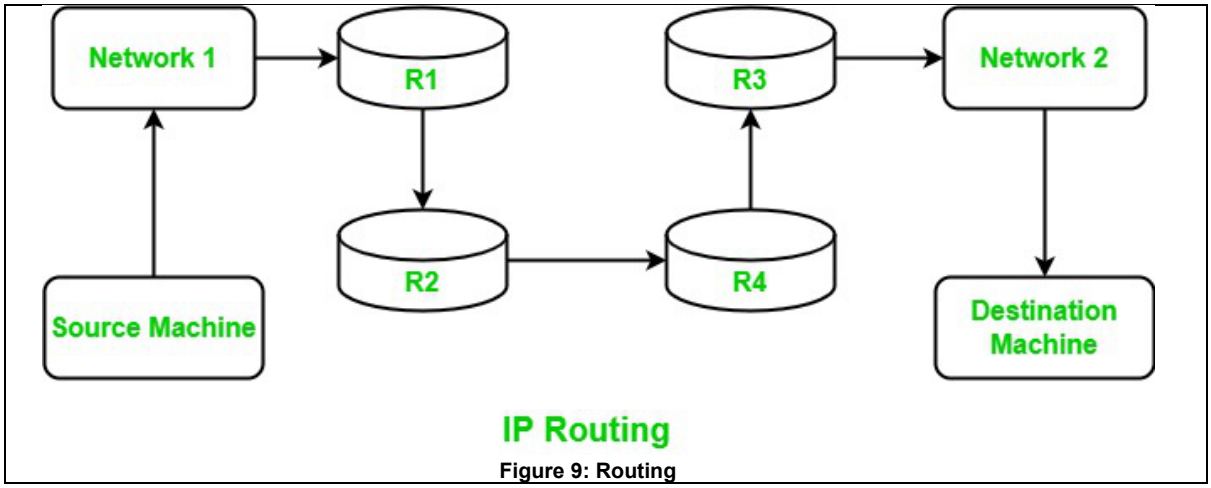


Figure 9: Routing

Terminologies:

- Autonomous System (AS): The collection of networks managed and supervised by a single entity or organization is called an autonomous system.
- Router: A router is a device that forwards the data using routing through multiple networks.
- Routing Table: A routing table is a table present in the router which stores the routing information.

Different Types of Routing: There are three different types of routing:

- Static Routing
- Dynamic Routing
- Default Routing

Static Routing: In this type of routing the routing table is updated by the network administrator.

Dynamic Routing: In this type of routing the routing table is automatically updated using routing protocols.

Default Routing: In this type of routing the router is configured to send all the data towards a specific router. This routing is generally used with stub routers.

How does IP routing work?

When the data is sent from the source to the destination the TCP and other protocols of the source work and form an IP packet that is sent to the network. When an IP packet is sent to the network from the source it has to pass through multiple routers to reach the destination. The router in the network gets the destination address from the packet and through its routing table identifies the next router information to which the data packet has to be passed. The routing table of the router includes various information about the next router, its cost, and other necessary information. The router takes the routing decision with the help of routing protocols and a routing table to which the next router the packet has to be sent to find the best route to reach the destination. Different packets can be sent

through different paths but all the packets reach their intended destination. When the packets reach the destination through different routers it sends them to the TCP for further processing.

Network Address Translation (NAT)

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP addresses is translated into one or more Global IP address and vice versa to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Network Address Translation (NAT) working –
Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.
If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

NAT inside and outside addresses –

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.

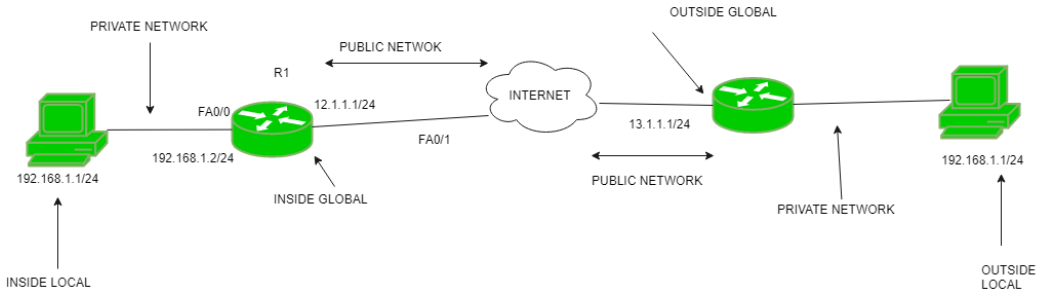


Figure 10: Natting

- **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.
- **Inside global address** – IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside local address** – This is the actual IP address of the destination host in the local network after translation.

- **Outside global address** – This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types- There are 3 ways to configure NAT:

- **Static NAT –** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e. one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.

  Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses which will be very costly.

- **Dynamic NAT –** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.

  Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

- **Port Address Translation (PAT)** – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

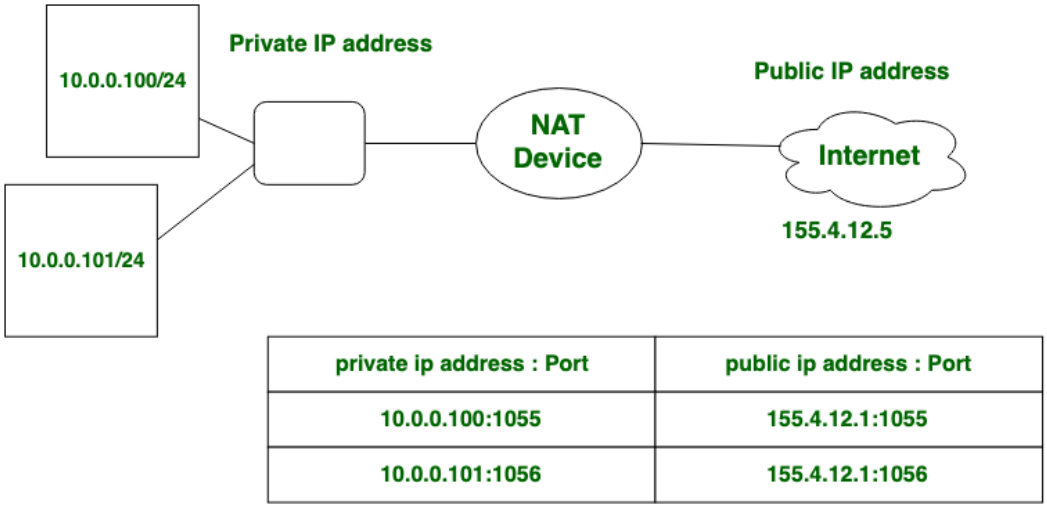


Figure 11: PAT

Example:

Consider a home network with three devices: a computer, a smartphone, and a smart TV. Without PAT, each of these devices would need to have a unique public IP address to connect to the internet. However, with PAT, all of these devices can share a single public IP address and communicate with the internet by using unique port numbers. When the computer sends a request to the internet, PAT assigns it a unique port number and translates the private IP address of the computer into the public IP address of the network. The destination server on the internet receives the request and responds to the unique port number, allowing the computer to receive the response.

2.2 Review process of network design plan

Reviewing the network design plan is a crucial step to ensure its accuracy, feasibility, and effectiveness in meeting the organization's requirements. Here's a structured approach to the review process:

- **Peer Review:**
  - Engage network architects, engineers, and administrators to conduct a peer review of the design plan.
  - Encourage constructive feedback and collaboration to identify potential issues and areas for improvement.

- **Stakeholder Input:**
  - Solicit input from key stakeholders, including IT leadership, department heads, and end users.
  - Ensure that the design plan aligns with organizational goals, budget constraints, and operational needs.

- **Technical Review:**
  - Verify technical aspects of the design plan, such as network topology, addressing scheme, subnetting, routing protocols, security measures, and scalability.
  - Assess the compatibility and interoperability of network devices, software, and protocols.
  - Review redundancy, failover mechanisms, and disaster recovery plans to ensure high availability and resilience.

- **Security Review:**
  - Evaluate security measures incorporated into the design plan, including access controls, encryption, authentication mechanisms, intrusion detection/prevention systems, and compliance with industry standards and regulations (e.g., GDPR, HIPAA, PCI DSS).
  - Conduct vulnerability assessments and penetration testing to identify and mitigate security risks.

- **Performance Review:**
  - Analyze the design plan's performance implications, including network bandwidth, latency, throughput, and Quality of Service (QoS) requirements.
  - Use network simulation tools or modeling techniques to assess performance under various traffic conditions and scalability scenarios.

- **Operational Review:**
  - Consider operational aspects of the design plan, such as ease of management, monitoring, and troubleshooting.
  - Review documentation, training requirements, and support processes to ensure that IT staff are adequately prepared to implement and maintain the network.

- **Budget Review:**

- Evaluate the cost-effectiveness of the design plan, including equipment procurement, implementation costs, ongoing maintenance expenses, and return on investment (ROI).
- Identify potential cost-saving measures and alternatives without compromising the design's functionality or performance.

- **Risk Assessment:**
  - Conduct a risk assessment to identify potential threats, vulnerabilities, and impact scenarios associated with the network design.
  - Develop risk mitigation strategies and contingency plans to address identified risks and minimize their likelihood and impact.

- **Legal and Regulatory Compliance:**
  - Ensure that the design plan complies with applicable laws, regulations, and industry standards governing data privacy, security, and network operations.
  - Review contractual obligations, service level agreements (SLAs), and liability considerations related to network design and implementation.

- **Final Approval:**
  - Consolidate feedback from all review stages and incorporate necessary revisions into the design plan.
  - Obtain final approval from relevant stakeholders, including IT leadership, project sponsors, and regulatory compliance officers.

2.3 Estimating and budgeting for equipment and tools

Estimating and budgeting for equipment and tools in IT support services involves forecasting the costs associated with acquiring and maintaining the hardware and software necessary to deliver effective IT support. Here's a breakdown of the key components:

Identify Needs:

- Equipment: Determine the types of hardware required, such as servers, workstations, network devices (routers, switches), and peripherals (printers, scanners).
- Tools: Identify software tools necessary for support, such as remote desktop tools, ticketing systems, antivirus software, and diagnostic tools.
- Maintenance and Upgrades: Consider ongoing needs for maintenance, upgrades, and replacements.

Cost Estimation:

- Initial Costs: Calculate the upfront costs for purchasing equipment and tools. This includes the cost of hardware, software licenses, and any initial setup or installation fees.
- Recurring Costs: Estimate ongoing costs such as subscription fees for software, maintenance contracts, and potential upgrades.

- Operational Costs: Include costs associated with power consumption, cooling, and other utilities.

Budgeting:

- Create a Budget Plan: Develop a comprehensive budget that includes both initial and recurring costs. This should cover:
- Capital Expenditure (CapEx): One-time costs for purchasing hardware and software.
- Operational Expenditure (OpEx): Recurring costs for maintaining and operating the equipment.
- Contingency Fund: Set aside a contingency fund for unexpected expenses or emergencies.
- Vendor Costs: Factor in any additional costs for support from vendors or third-party service providers.

Cost-Benefit Analysis:

- Evaluate ROI: Consider the return on investment (ROI) for each piece of equipment and tool. Assess how each will impact efficiency, productivity, and overall support effectiveness.
- Prioritize Investments: Prioritize purchases based on critical needs and potential impact on IT support services.

Procurement and Acquisition:

- Vendor Selection: Choose reliable vendors for purchasing equipment and tools. Compare quotes and assess vendor support and warranty options.
- Purchase Agreements: Negotiate terms, warranties, and service agreements to ensure you get the best value.

Monitoring and Review:

- Track Expenses: Monitor actual spending against the budgeted amounts to ensure you stay within financial limits.
- Review and Adjust: Regularly review and adjust the budget based on changes in technology needs, equipment lifecycle, and emerging trends.

Example Budget Breakdown:

1. Hardware:
   - Servers: $10,000
   - Workstations (10 units): $15,000
   - Network Equipment: $5,000
   - Peripherals: $2,000

2. Software:
    - Licenses: $3,000
    - Subscription Fees: $1,200/year
    - Maintenance:
    - Support Contracts: $2,000/year
    - Upgrades and Repairs: $1,000/year
    - Utilities and Miscellaneous:
    - Power and Cooling: $1,500/year
    - Contingency Fund: $2,000

Self-Check-2: Plan and Design To Expand an Existing Network

Questionnaire

1. **What is NFS?**
   Answer:

2. **What is HTTP?**
   Answer:

3. **What is HTTPS?**
   Answer:

4. **What is FTP?**
   Answer:

5. **What is SNMP?**
   Answer:

6. **What is PAT?**
   Answer:

7. **What is the purpose of NFS?**
   Answer:

8. **What is the main function of HTTP?**
   Answer:

9. **How does HTTPS enhance HTTP?**
   Answer:

10. **What are some common use cases for FTP?**
    Answer:

11. **What tasks can be performed using SNMP?**
    Answer:

12. **What role does PAT play in network address translation?**
    Answer:

Answer Key-2: Plan and design to expand an existing network

1. **What is NFS?**
   Answer: NFS stands for Network File System. It's a protocol used for sharing files and directories between UNIX/Linux systems over a network.

2. **What is HTTP?**
   Answer: HTTP stands for Hypertext Transfer Protocol. It's the foundation of data communication for the World Wide Web, facilitating the retrieval and display of web pages and resources.

3. **What is HTTPS?**
   Answer: HTTPS stands for Hypertext Transfer Protocol Secure. It's a secure version of HTTP that adds encryption using SSL/TLS protocols to ensure the confidentiality and integrity of data transmitted over the internet.

4. **What is FTP?**
   Answer: FTP stands for File Transfer Protocol. It's a standard network protocol used for transferring files between a client and a server on a computer network, typically the internet.

5. **What is SNMP?**
   Answer: SNMP stands for Simple Network Management Protocol. It's used for managing and monitoring network devices and functions, facilitating tasks such as device configuration, performance monitoring, and fault detection.

6. **What is PAT?**
   Answer: PAT stands for Port Address Translation, also known as NAT Overload. It's a type of Network Address Translation that allows multiple devices within a private network to share a single public IP address by using unique port numbers to distinguish between different internal devices.

7. **What is the purpose of NFS?**
   Answer: The purpose of NFS is to enable sharing files and directories between UNIX/Linux systems over a network, allowing remote access to files as if they were local.

8. **What is the main function of HTTP?**
   Answer: The main function of HTTP is to facilitate the retrieval and display of web pages and resources on the World Wide Web by defining how messages are formatted and transmitted between web servers and browsers.

9. **How does HTTPS enhance HTTP?**

   Answer: HTTPS enhances HTTP by adding a layer of encryption using SSL/TLS protocols, ensuring the confidentiality and integrity of data transmitted over the internet, thereby providing a secure communication channel.

10. **What are some common use cases for FTP?**

    Answer: Common use cases for FTP include uploading website files to a web server, downloading software updates from a repository, transferring large files between computers, and sharing files within an organization.

11. **What tasks can be performed using SNMP?**

    Answer: SNMP can be used for managing and monitoring network devices and functions, including device configuration, performance monitoring, fault detection, and network troubleshooting.

12. **What role does PAT play in network address translation?**

    Answer: PAT (Port Address Translation) allows multiple devices within a private network to share a single public IP address by using unique port numbers to distinguish between different internal devices during the translation process.

Job Sheet-2.1: Prepare A Computer Network Using Star Topology

Job Name: Prepare a Computer Network using Star Topology

Objective:

To set up a computer network using the Star Topology, ensuring all devices are connected to a central hub/switch, facilitating efficient data communication.

Procedure:

1. Planning the Network:
    a. Determine the number of devices to be connected.
    b. Decide the placement of the switch/hub centrally to minimize cable length.
    c. Plan the layout and labeling of cables for easy identification.

2. Preparing the Ethernet Cables:
    a. Measure and cut the Ethernet cables to the required lengths.
    b. Strip about 1 inch of the outer insulation from both ends of the cables.
    c. Untwist the pairs of wires and arrange them according to the T568B wiring standard.
    d. Insert the wires into the RJ45 connectors and ensure they are in the correct order.
    e. Use the crimping tool to secure the connectors onto the cables.
    f. Repeat this for all cables.

3. Installing Network Interface Cards (NICs):
    a. If the computers do not have built-in NICs, install the NICs into the PCI/PCIe slots.
    b. Secure the NICs with screws if necessary.
    c. Ensure drivers for the NICs are installed on the computers.

4. Connecting Devices to the Switch/Hub:
    a. Connect one end of each Ethernet cable to the NIC on each computer.
    b. Connect the other end of each cable to the switch/hub.
    c. Ensure the connections are secure and properly seated.

5. Powering Up:
    a. Power on the switch/hub.
    b. Power on the computers one by one.
    c. Check for link lights on the NICs and switch/hub to confirm connections.

6. Testing the Network:
    a. Use a cable tester to check the integrity of each Ethernet cable.
    b. Perform a ping test between computers to ensure network connectivity.

c. Verify that each computer can access network resources and the internet if applicable.

Troubleshooting:

1. No Link Light:
    a. Check cable connections and ensure they are properly crimped.
    b. Verify that the NICs are properly installed and recognized by the operating system.
    c. Ensure the switch/hub is powered on and functioning.

2. Intermittent Connectivity:
    a. Check for loose or damaged cables.
    b. Ensure the switch/hub is not overloaded and operating within its capacity.
    c. Verify the NIC drivers are up to date.

3. Slow Network Speed:
    a. Check for network congestion and ensure the switch/hub supports the required speed.
    b. Verify the quality and category of Ethernet cables.

Specification Sheet-2.1: Prepare A Computer Network Using Star Topology

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Antistatic Wrist Strap	Pair	01
2	Safety Glasses	Pair	01
3	Gloves	Pair	01
4	Dust Mask	Pair	01
5	Knee Pads	Pair	01
6	Proper Footwear	Pair	01
7	Work Apron	Pair	01

Necessary tools and equipment

Sl. No	Name of Tools & Equipment	Specification	Unit	Quantity
1	Crimping Tool		PCS	01
2	Cable Tester		PCS	01
3	Screwdrivers		PCS	01
4	Cable Stripper		PCS	01
5	Patch Panel (Optional)		PCS	01
6	Label Maker		PCS	01

Necessary materials

Sl. No.	Name of materials	Specification	Unit	Quantity
a.	Network Switch/Hub	As per Required	PCS	01
b.	Ethernet Cables (CAT5e or higher)	As per Required	As required	01
c.	RJ45 Connectors	As per Required	PCS	100
d.	Network Interface Cards (NICs)	As per Required	PCS	10

Task Sheet-2.2: Plan and design to expand an existing network

Job Sheet: Plan and Design to Expand an Existing Network

Objective:

To plan and design the expansion of an existing network, ensuring seamless integration of new devices and infrastructure with the current setup.

Procedure:

1. Assess the Current Network:
   - Review the existing network layout and configuration.
   - Identify the current network infrastructure, including switches, hubs, routers, and cables.
   - Document the number of devices currently connected and their locations.

2. Determine Expansion Requirements:
   - Identify the number of new devices to be added and their locations.
   - Assess the need for additional network switches or hubs.
   - Determine the required length and type of Ethernet cables.

3. Plan the Network Expansion:
   - Design the expanded network layout, considering the optimal placement of new switches/hubs.
   - Ensure the new layout maintains network efficiency and minimizes cable length.
   - Create a detailed network diagram showing the expanded setup, including device connections and cable paths.

4. Prepare the Necessary Materials:
   - Gather all required materials, including network switches/hubs, Ethernet cables, RJ45 connectors, and other necessary equipment.
   - Label all new cables and devices for easy identification.

5. Install New Network Components:
   - Install any additional network switches/hubs in the planned locations.
   - Run Ethernet cables from the new devices to the nearest switch/hub.
   - Use cable ties, raceways, or ducting to organize and protect cables.

6. Connect and Configure New Devices:

- Attach RJ45 connectors to the Ethernet cables and connect them to the NICs of the new devices.
- Connect the other ends of the cables to the appropriate switch/hub ports.
- Power on the new devices and ensure they are recognized by the network.

7. Update Network Documentation:
   - Update the network configuration documentation to reflect the changes.
   - Include the new network diagram and any relevant configuration details.

8. Test the Expanded Network:
   - Use a cable tester to verify the integrity of all new Ethernet cables.
   - Perform a network connectivity test between the new devices and the existing network.
   - Ensure all devices have network access and can communicate with each other.

Troubleshooting:

No Network Connectivity:

a) Check cable connections and ensure they are properly crimped and secured.
b) Verify that the new switches/hubs are powered on and functioning.
c) Ensure the NICs are properly installed and configured.

Intermittent Connectivity:

a) Check for loose or damaged cables.
b) Ensure the network switches/hubs are not overloaded and operating within their capacity.

- Network Performance Issues:

a) Check for network congestion and ensure the new layout maintains efficiency.
b) Verify the quality and category of Ethernet cables used.

Conclusion:

Planning and designing the expansion of an existing network involves careful assessment, detailed planning, and meticulous execution. Following the outlined steps ensures a smooth integration of new devices and infrastructure, maintaining network performance and reliability.

Specification Sheet-2.2: Plan and design to expand an existing network

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
8	Antistatic Wrist Strap	Pair	01
9	Safety Glasses	Pair	01
10	Gloves	Pair	01
11	Dust Mask	Pair	01
12	Knee Pads	Pair	01
13	Proper Footwear	Pair	01
14	Work Apron	Pair	01

Necessary tools and equipment

Sl. No	Name of Tools & Equipment	Specification	Unit	Quantity
7	Crimping Tool		PCS	01
8	Cable Tester		PCS	01
9	Screwdrivers		PCS	01
10	Cable Stripper		PCS	01
11	Patch Panel (Optional)		PCS	01
12	Label Maker		PCS	01

Necessary materials

Sl. No.	Name of materials	Specification	Unit	Quantity
e.	Network Switch/Hub	As per Required	PCS	01
f.	Ethernet Cables (CAT5e or higher)	As per Required	As required	01
g.	RJ45 Connectors	As per Required	PCS	100
h.	Network Interface Cards (NICs)	As per Required	PCS	10

Learning Outcome-3: Expand The Existing Network

Assessment Criteria	1. According to the approved network design plan an existing network is deployed. 2. The network is connected to the internet. 3. Equipment and materials are collected to expand the network. 4. Nodes are connected to the network. 5. Deployment of network is performed.
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Switch 6. Router 7. Networking related Tools and accessories 8. Multimedia Projector 9. Paper, Pen, Pencil, and Eraser 10. Internet Facilities 11. Whiteboard and Marker
Contents	1 Network design plan. 2 Deployment procedure- ▪ Cable laying process • UTP • Optical fibre ▪ Process to install faceplate, modular. ▪ Procedure to prepare patch cord. ▪ Rack installation process including switch and other equipment's. 3 Configuration process of networking devices such as router, manageable switch, such as- ▪ Assign IP address. ▪ Establish NAT gateway. ▪ Access-list, prefix-list. 4 Node connecting procedure such as- ▪ Server ▪ Client/ Workstation ▪ Router ▪ Switch (Layer-2, Layer -3)

Activities/job/Task	1. Carefully install network cables according to the design, ensuring proper labeling and avoiding bends or damage. 2. Configure network devices (routers, switches, access points) based on the plan, including IP addresses, VLANs, security settings, etc. 3. Carefully install network cables according to the design, ensuring proper labeling and avoiding bends or damage. 4. Thoroughly test each network segment and connection, verifying functionality and performance before proceeding. 5. Connect Network with Internet 6. Test internet connectivity and ensure secure access for authorized users. 7. Ensure all equipment and materials are clearly labeled, tracked, and stored securely throughout the deployment process. 8. Update network documentation with new equipment details, diagrams, and configuration settings.
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning 4. Portfolio

Learning Experience-3: Expand The Existing Network

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

Learning Activities	Recourses/Special Instructions
1. Students will ask the instructor about "Expand the existing network."	1. The instructor will provide the learning materials "Expand the existing network."
2. Read the Information sheet and complete the Self-check & Check answer sheets on "Expand the existing network."	1. Information sheet 3: Expand the existing network. 2. Self-check 3: Expand the existing network. 3. Answer Self-check 3: Expand the existing network.
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	4. **Specification Sheet 3.1:** "Expand the existing network. **Task Sheet 3.1:** "Expand the existing network.

Information Sheet-3: Expand the existing network

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

3.1 Network design plan.
3.2 Deployment procedure.
3.3 Configuration process of networking devices such as routers, manageable switches.
3.4 Node connecting procedures.

1.1 Network design plan

Creating a network design plan for expanding an existing network involves several key steps to ensure scalability, reliability, and security. Here's a comprehensive outline:

a. Assessment of Current Network:
- Review existing network topology, infrastructure, and configurations.
- Identify strengths, weaknesses, opportunities, and threats (SWOT analysis).
- Gather information on current traffic patterns, bandwidth usage, and performance metrics.

b. Define Objectives:
- Determine the goals and requirements of the network expansion.
- Consider factors such as increased bandwidth, improved reliability, support for new services or applications, and scalability for future growth.

c. Capacity Planning:
- Estimate the expected increase in network traffic and bandwidth requirements.
- Evaluate hardware and software requirements to support the expanded network.
- Plan for scalability to accommodate future growth without major overhauls.

d. Topology Design:
- Choose an appropriate network topology (e.g., star, mesh, and ring) based on requirements.
- Consider factors such as fault tolerance, ease of management, and cost-effectiveness.
- Determine the placement of network devices (routers, switches, firewalls) to optimize performance and security.

e. Selection of Hardware and Software:
- Research and select network equipment (routers, switches, access points) based on performance, features, and compatibility with existing infrastructure.
- Evaluate network management and monitoring tools for efficient operation and troubleshooting.
- Consider security appliances and software for protecting the expanded network against threats.

f. Addressing Scheme:

- Plan IP addressing scheme for the expanded network, including subnetting and addressing allocation.
- Ensure compatibility with existing addressing schemes and scalability for future growth.
- Implement IPv6 alongside IPv4 if required.

g. Security Design:

- Define security policies and protocols for the expanded network.
- Implement access control mechanisms, encryption, and authentication protocols to safeguard data and resources.
- Consider deploying intrusion detection/prevention systems (IDS/IPS) and firewall solutions.

h. Redundancy and High Availability:

- Design redundancy into critical network components (e.g., redundant links, failover mechanisms).
- Implement load balancing and failover solutions to ensure high availability of services.
- Plan for disaster recovery and data backup strategies.

i. Implementation Plan:

- Develop a detailed implementation plan with timelines, tasks, and responsibilities.
- Coordinate with stakeholders and IT personnel to minimize disruption during implementation.
- Conduct testing and validation of the expanded network before full deployment.

j. Documentation and Training:

- Document the network design, configurations, and procedures for maintenance and troubleshooting.
- Provide training to IT staff on operating and managing the expanded network.
- Create user documentation and conduct training sessions for end-users if necessary.

k. Monitoring and Maintenance:

- Establish network monitoring tools and procedures to track performance, security, and availability.
- Implement regular maintenance schedules for updating firmware, patches, and configurations.
- Monitor network usage and performance to identify and address potential issues proactively.

1.2 Deployment procedure

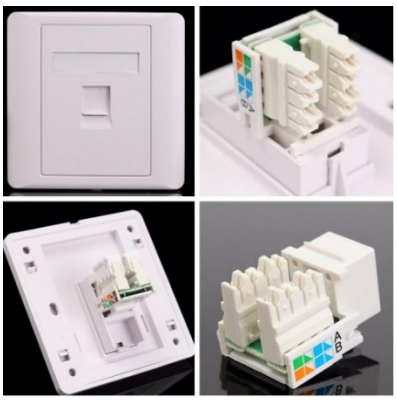
UTP Cable: The Internet plays a pivotal role in our daily lives, from work to entertainment and from shopping to paying utility bills. Ever wondered how the world is connected with the World Wide Web, both in spirit and physical sense? The physical connection is achieved through a UTP cable, also known as an Unshielded Twisted Pair Cable. This twisted pair of cabling offers a steady network tailor-made for data transfer and telephony.

A standard UTP cable consists of a 100-ohm copper cable made with 2 – 1800 unshielded twisted pairs shielded by an outer jacket. As they have no metallic shield, the cable diameter is reduced but cannot avoid electrical interference. The twisting in these cables boosts immunity to EMI and electrical noise. In the mantle of an unshielded twisted pair cable, there are 8 separate wires twisted in 4 pairs. A connector is placed at the end of these cables, usually known as R-J45 plugs.

Workings of a UTP Cable
Inside a shield twisted pair of cables, there are 4 twisted pairs of copper wires surrounded by a protective plastic cover. The greater the number of pairs corresponds to more bandwidth. The two individual copper cables in a single pair are twisted around each other, and later other pairs of such wires are twisted together. It is done to minimize cross-talk and electromagnetic interference as they can reduce network performance in the long run. Each twisted pair of cabling in the UTP cable is color-coded for easy identification. In North America, each wire in a twisted pair is identified by one of 5 colors: blue, orange, green, brown, or slate (gray). Then this copper wire is paired with a different wire from the other color group made up of white, red, black, yellow, or violet. Usually, one copper wire in a twisted pair is solid-colored, and the second one is striped with the color of its mate. Ex: A solid blue colored copper cable is paired with a white and blue striped copper cable. It will make it easy to identify and match them. Alexander Graham Bell invented this twisted pair of cabling in 1881.

Network Pace Plate: A Network Face Plate is a device that allows a single cable to plug into multiple ports. This type of plate has two RJ45 and two TV ports and can be used with fiber optic and copper cable. It also allows for longer/shorter patch cords. It comes in different sizes and has different connector types.

Network faceplates CAT6 Male Connector Factory are commonly used for cables that run behind walls or beneath floors. They are available in a wide range of styles and colours to meet specific networking needs. Fiber-Mart stocks a variety of network faceplates for both single-port and dual-port installations. Each faceplate has one, two, or four ports and meets all international standards. Fiber-Mart also offers worldwide delivery and low prices on faceplates.



Faceplate numbers can be difficult to read if the label has fallen off or is missing. You may need to take the faceplate to the Service Desk to get help. If you're unsure of the faceplate number, you can try looking for it on other faceplates in the room. If the first five digits match, you can be sure it is the correct one. In addition, you can get a sense of the faceplate's location by comparing it to other faceplates in the same room or adjacent rooms.

Rack Design

Rack design is an important factor when it comes to building a server rack. Each design is suitable for different sizes and types of equipment. Some of the available rack designs are:

- Wall-mounted racks. Designed to be attached to walls, which saves floor space and fits in areas too small for other rack types. They are usually smaller than floor-standing racks and cannot support as much weight.
- Enclosed racks. They have removable rear and front doors and side panels, and adjustable vertical mounting rails. They are ideal for heavier and hotter equipment and offer greater security since the panels can be locked.
- Open-frame racks. These are open frames with mounting rails, without doors or side panels. They are suitable when there is no need for airflow control or high security. Open-frame racks are also good for network wiring due to their convenient access and lots of open space for cable management.

Rack Size

The rack size needs to be compatible with the server/equipment. Check the dimensions of the equipment and the rack you want to use, making sure that the fit isn't tight, and that there is about an inch of space from all sides of the device. Check the mountable width, depth, and height of the server.

Server racks usually consist of rack units. A rack unit (1U) is 1.75" (44.45 mm) of vertical space, usually three rack hole spaces. One of the key points to consider when purchasing a rack is the number of rack units your equipment requires.

Usually, a full-size rack is 42U, which means it holds 19" of equipment. However, it is always a good idea to leave extra space for horizontal cable management or future expansions. The width is usually standardized, following the EIA-310-E standard. The equipment depth varies

the most, which is why rails and shelves usually have adjustable depth. The standard depth of a rack is around 42".

Depending on the equipment type, calculate the rack size you need. For example, network switches are usually 1U to 2U, server size ranges from 1U to 4U, while blade servers range from 5U to 10U or more.

Rack Layout

Make sure to plan the equipment layout in advance, before starting the installation. Assess what equipment you want to use, how much space you need, and the order of the units in the rack.

- The heaviest equipment, such as the PDU (power distribution unit) or UPS (uninterruptible power supply) should be at the bottom of the rack. Heavy equipment at the bottom keeps the rack steady and prevents it from becoming top-heavy and tipping over.
- The middle part of the rack usually holds crosses and patch panels. The middle is the most convenient place for that equipment because it is in eye level, and it facilitates the maintenance and connection of twisted pairs. Servers, switches, and other active equipment usually go below the patch panels.
- It is also a good idea to create a layout sheet with information that will later help identify components and configurations. You can update the information sheet to track hardware installation and service dates and use it to keep up with equipment maintenance.
- Label and document your setup, including cabling, to avoid mistakes such as unplugging or restarting a critical system unintentionally. In addition, it helps new staff to quickly get familiar with the different parts of the setup.

Location

- An ideal server room is as secure as possible since the rack contains expensive hardware with critical business data. The best place for a server room is a room with no windows and with restricted access. Locking the room is essential if employees or visitors can access it.
- Another reason for isolating the server room is to reduce the chance of accidents. Having unqualified people around servers exposes them to different risks, including getting the equipment wet, being bumped, or tipped over.

Additionally, since servers generate a lot of heat and can get noisy, they can be an issue for people working in the surrounding area.

Power Supply

The equipment in a server rack usually requires many power outlets, which can be an issue if the cords need to reach a distant wall outlet. A power distribution unit (PDU) resolves that issue and provides a reliable power source required for high-availability IT applications. A PDU can also provide monitoring data, remote management, automated alerts, and individual outlet control.

Another thing to bear in mind is to avoid overloading the circuits, so make sure to check your equipment's rack density. Earthing the equipment is also important as it keeps the server and people safe from shocks.

1.3 Configuration process of networking devices

Network Switch:

Switches are crucial networking devices used to connect devices within a local area network (LAN) and facilitate the exchange of data packets. There are two main types of switches based on the layer of the OSI model at which they operate: Layer 2 switches and Layer 3 switches.

Layer 2 Switch:

A Layer 2 switch operates at the Data Link layer (Layer 2) of the OSI model. Its primary function is to forward Ethernet frames based on the Media Access Control (MAC) addresses of devices connected to it. Here are some key features of Layer 2 switches:

- MAC Address Learning: Layer 2 switches maintain a MAC address table (also known as a CAM table) that maps MAC addresses to the port on which each device is connected. When a device sends a frame to the switch, the switch learns the source MAC address and associates it with the port through which the frame arrived.
- Forwarding Decision: When a switch receives a frame with a destination MAC address, it looks up the MAC address in its table to determine the outgoing port. If the MAC address is found in the table, the switch forwards the frame only to the appropriate port, reducing unnecessary traffic on the network.
- Broadcast and Multicast Handling: Layer 2 switches forward broadcast and multicast frames to all ports except the incoming port. This ensures that devices receive broadcast and multicast traffic as needed.
- No Routing Functionality: Layer 2 switches do not perform routing or make forwarding decisions based on IP addresses. They operate purely at the MAC layer and cannot route traffic between different IP subnets.

Layer 3 Switch:

A Layer 3 switch operates at both the Data Link layer (Layer 2) and the Network layer (Layer 3) of the OSI model. In addition to the functionalities of Layer 2 switches, Layer 3 switches have routing capabilities, allowing them to make forwarding decisions based on IP addresses. Here are some key features of Layer 3 switches:

- IP Routing: Layer 3 switches can route traffic between different IP subnets within the same LAN or VLAN. They maintain a routing table that contains information about the best paths to reach different IP destinations.
- Inter-VLAN Routing: Layer 3 switches can route traffic between different VLANs, allowing communication between devices in different VLANs without the need for an external router.
- Advanced Traffic Filtering: Layer 3 switches can implement access control lists (ACLs) to filter traffic based on IP addresses, TCP/UDP ports, and other criteria. This provides granular control over traffic flows and enhances network security.

Self-Check -3: Expand The Existing Network

1. What are the primary functions of a Layer 2 switch, and how does it differ from a Layer 3 switch?

   Answer:

2. Can you explain the process of configuring PPPoE on a router, including the necessary parameters?

   Answer:

3. When accessing a router's web interface, what are some common default IP addresses, and how can you determine the correct one?

   Answer:

4. What are the advantages of assigning static IP addresses to networking devices over using DHCP?

   Answer:

5. Can you explain the process of establishing a NAT gateway on a router, including the implications for internal and external IP addresses?

   Answer:

6. What are access-lists used for, and how do they work?

   Answer:

7. What is the difference between a standard and extended access-list?

   Answer:

8. Can you provide examples of scenarios where prefix-lists are commonly used?

   Answer:

9. How do you configure a prefix-list on a router, and what parameters can you specify?

   Answer:

10. What security implications should be considered when configuring router access?

    Answer:

11. What are some best practices for saving router configurations?

    Answer:

12. How do you enable an interface on a router or switch, and why is this step necessary?

    Answer:

13. What are VLANs, and how do they enhance network security and efficiency?

    Answer:

14. Can you explain the process of configuring VLANs on a manageable switch, including assigning VLAN IDs and creating VLAN interfaces?

    Answer:

15. What are some common troubleshooting techniques for resolving network connectivity issues?

Answer Key-3: Expand The Existing Network

1. What are the primary functions of a Layer 2 switch, and how does it differ from a Layer 3 switch?

   Answer: A Layer 2 switch forwards frames based on MAC addresses, while a Layer 3 switch can route traffic based on IP addresses in addition to forwarding frames.

2. Can you explain the process of configuring PPPoE on a router, including the necessary parameters?

   Answer: Configuring PPPoE involves specifying the PPPoE username and password provided by the ISP, along with configuring the WAN interface to use PPPoE encapsulation.

3. When accessing a router's web interface, what are some common default IP addresses, and how can you determine the correct one?

   Answer: Common default IP addresses for router web interfaces include 192.168.0.1 and 192.168.1.1. You can determine the correct one by checking the router's documentation or using the command prompt and typing `ipconfig` (for Windows) or `ifconfig` (for Unix-like systems) and looking for the "Default Gateway" IP address.

4. What are the advantages of assigning static IP addresses to networking devices over using DHCP?

   Answer: Assigning static IP addresses ensures that devices always have the same IP address, making it easier to manage and troubleshoot the network. It also eliminates the overhead of DHCP lease negotiation.

5. Can you explain the process of establishing a NAT gateway on a router, including the implications for internal and external IP addresses?

   Answer: Setting up NAT involves mapping private internal IP addresses to public external IP addresses to enable devices on a private network to access the internet. NAT translates the source IP address of outgoing packets to the router's external IP address and maintains a translation table to track connections.

6. What is access-lists used for, and how do they work?

   Answer: Access-lists are used to filter traffic based on specified criteria such as source/destination IP address, protocol, and port number. They work by evaluating incoming or outgoing packets against the configured rules and either permitting or denying them accordingly.

7. What is the difference between a standard and extended access-list?

   Answer: Standard access-lists filter traffic based only on source IP addresses, while extended access-lists can filter traffic based on source/destination IP addresses, protocols, port numbers, and other criteria.

8. Can you provide examples of scenarios where prefix-lists are commonly used?

   Answer: Prefix-lists are commonly used in routing protocols such as BGP (Border Gateway Protocol) to control the advertisement or acceptance of routes based on their IP address prefixes.

9. How do you configure a prefix-list on a router, and what parameters can you specify?

   Answer: To configure a prefix-list, you specify the sequence number, action (permit or deny), and IP address prefix with optional prefix length and ge/le (greater than or less than) parameters.

10. What security implications should be considered when configuring router access?
    Answer: When configuring router access, it's important to consider limiting access to authorized users, enabling strong authentication mechanisms such as SSH, and implementing access-lists to restrict access from unauthorized sources.

11. What are some best practices for saving router configurations?
    Answer: Best practices for saving router configurations include regularly backing up configurations to a secure location, using version control systems for tracking changes, and documenting configuration changes with comments.

12. How do you enable an interface on a router or switch, and why is this step necessary?
    Answer: To enable an interface, you enter interface configuration mode and use the `no shutdown` command. This step is necessary to bring the interface online and allow traffic to pass through it.

13. What are VLANs, and how do they enhance network security and efficiency?
    Answer: VLANs are virtual LANs that segment a physical network into multiple logical networks. They enhance security by isolating traffic within VLANs and efficiency by reducing broadcast domains and optimizing network traffic flow.

14. Can you explain the process of configuring VLANs on a manageable switch, including assigning VLAN IDs and creating VLAN interfaces?
    Answer: Configuring VLANs on a manageable switch involves assigning VLAN IDs to switch ports and creating VLAN interfaces for routing traffic between VLANs or providing inter-VLAN communication.

15. What are some common troubleshooting techniques for resolving network connectivity issues?
    Answer: Common troubleshooting techniques include checking physical connections, verifying IP configurations, testing connectivity using ping and traceroute, reviewing firewall and NAT configurations, and examining router and switch logs for errors.

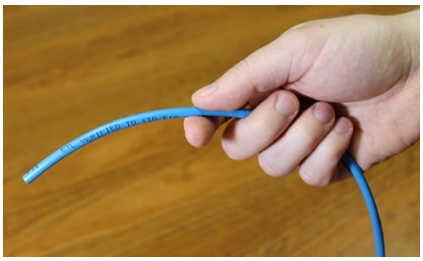
Job Sheet-3.1: Prepare a Network Cable for Computer Networking

Objective: To prepare a network cable with RJ45 connectors for use in computer networking, ensuring proper assembly and testing for reliable performance.

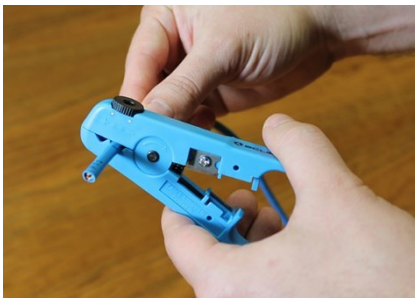
Working Procedure:

Cabling Process:

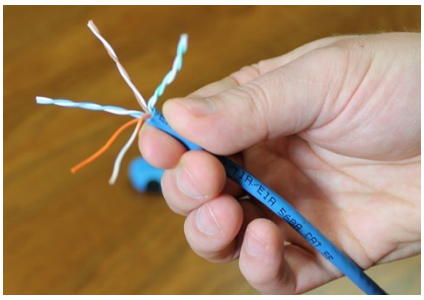
UTP: The following procedure goes over creating your own Ethernet cable. This process can be used to create both Category 5 & 6 cables. In this demonstration we used the 902-351 Crimp Bundle. This is the perfect assortment of tools for someone learning to make their own network cables.



Step 01: Unroll the required length of network cable and add a little extra wire, just in case. If a boot is to be fitted, do so before stripping away the sleeve and ensure the boot faces the correct way. Please note that the cable length should not be more that 100 meters to prevent attenuation (i.e. degradation of signal strength due to losses as signal travel down the length of the cable). Keeping the length within 100 meters from the access point (i.e. face plate) to the patch panel or network switch will ensure good signal strength/quality.

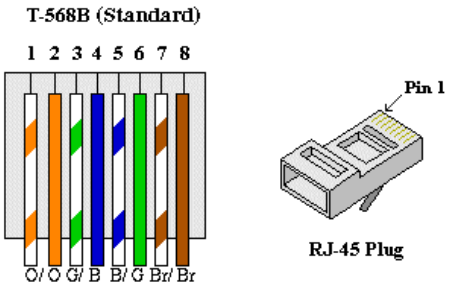


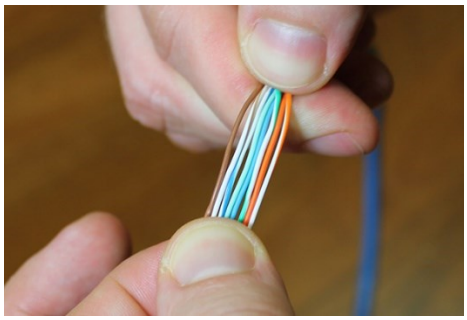
Step 02: Carefully remove the outer jacket of the cable. Be careful when stripping the jacket so as not nick or cut the internal wiring. One good way to do this is to cut lengthwise with snips or a knife along the side of the cable, away from yourself, about an inch toward the open end. This reduces the risk of nicking the wires' insulation. Locate the string inside with the wires, or if no string is found, use the wires themselves to unzip the sheath of the cable by holding the sheath in one hand and pulling sideways with the string or wire. Cut away the unzipped sheath and cut the twisted pairs about 1 1/4" (30 mm). You will notice 8 wires twisted in 4 pairs. Each pair will have one wire of a certain color and another wire that is white with a colored stripe matching its partner (this wire is called a tracer)



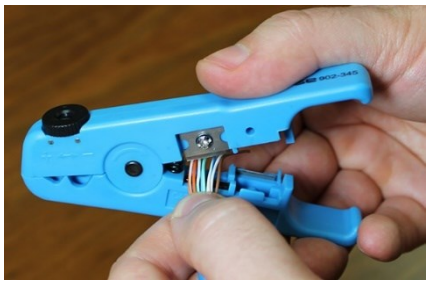
Step 03: Separate your wire pairs: Untwist all 4 pairs of wires and straighten them out the best you can. If there are any white fibers or a plastic divider in the center you can now trim it off.

Step 04: Arrange the wires based on the wiring specifications you are following. There are two methods set by the TIA, 568A and 568B. Which one you use will depend on what is connected. A straight-through cable is used to connect two different-layer devices (e.g. a hub and a PC). Two like devices normally require a cross-over cable. The difference between the two is that a straight-through cable has both ends wired identically with 568B, while a cross-over cable has one end wired 568A and the other end wired 568B.[1] For our demonstration in the following steps, we will use 568B, but the instructions can easily be adapted to 568A.



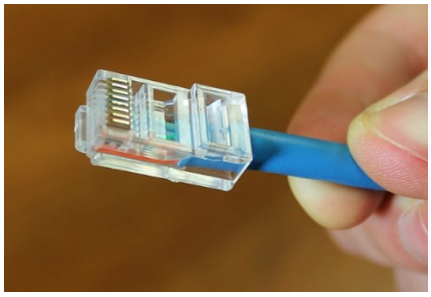


Step 05: Cut the wires: Cut the wires flush about 1/2″ from where the jacket was stripped off the cable. Make sure to leave enough that the ends of the wires can reach the pins of the connectors. The cable needs to go inside the connector housing enough for the crimp tab to come down on top of the jacket and hold it in place.



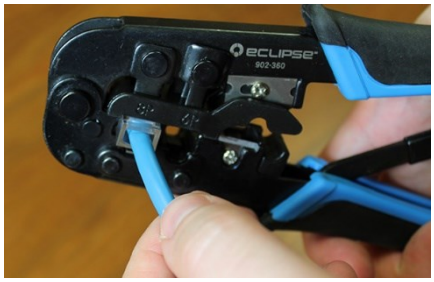
Step 06: Insert wires into connector:

Insert the wires into the connector. Make sure the connector is oriented properly, the release tab should be facing down toward the ground. Ensure all wires are still in the correct order after they are pushed all the way to the pins.



Step 07: Crimp the connector.

Insert your connector with the wire inside the 8P8C slot of your crimp tool. Give the crimp tool a good squeeze to ensure it goes through the full range of motion and creates a proper crimp. Pull your connector out of the crimp tool to show your finished connector. Repeat all of these steps to crimp a connector on the other end of your cable.



Step 08: Test the cable to ensure that it will function in the field. Mis-wired and incomplete network cables could lead to headaches down the road. In addition, with power-over-Ethernet (PoE) making its way into the marketplace, crossed wire pairs could lead to physical damage of computers or phone system equipment, making it even more crucial that the pairs are in the correct order. A simple cable tester can quickly verify that information for you. Should you not have a network cable tester on hand, simply test connectivity pin to pin.

Specification Sheet-3.1: Prepare A Network Cable for Computer Networking

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Antistatic Wrist Strap	Pair	01
2	Safety Glasses	Pair	01
3	Gloves	Pair	01
4	Dust Mask	Pair	01
5	Knee Pads	Pair	01
6	Proper Footwear	Pair	01
7	Work Apron	Pair	01

Necessary tools and equipment

Sl. No	Name of Tools & Equipment	Specification	Unit	Quantity
1	Cable Stripper		PCS	01
2	Crimping Tool		PCS	01
3	Cable Tester		PCS	01
4	Scissors or Cutting Tool		PCS	01
5	Antistatic Wrist Strap		PCS	01
6	Label Maker (optional)		PCS	01

Necessary materials

Sl. No.	Name of materials	Specification	Unit	Quantity
1	Ethernet Cable	CAT5e or higher	Set	As required
2	RJ45 Connectors	-	Set	As required

Job Sheet-3.2: Install a Faceplate for Computer Networking

Job Name: Install a Faceplate for Computer Networking

Objective:
To install a faceplate for computer networking, providing a clean and organized termination point for Ethernet cables in a wall or surface.

Working Procedure:

1. Plan the Installation:
    a. Determine the location for the faceplate.
    b. Ensure the location is accessible and suitable for running Ethernet cables.

2. Prepare the Wall/Site:
    a. Use a stud finder to locate studs and ensure the installation area is clear.
    b. If installing in drywall, mark the outline of the low voltage mounting bracket using a pencil.

3. Cut the Opening:
    a. Use a utility knife to cut along the marked outline for the low voltage mounting bracket.
    b. Ensure the opening is clean and free of debris.

4. Install the Mounting Bracket:
    a. Insert the low voltage mounting bracket into the opening.
    b. Secure the bracket to the wall using screws.

5. Run the Ethernet Cable:
    a. Run the Ethernet cable from the network switch/hub to the faceplate location.
    b. Leave enough cable length at both ends for termination.

6. Strip and Prepare the Cable:
    a. Strip about 1 inch of the outer insulation from the Ethernet cable using a cable stripper.
    b. Untwist and arrange the pairs of wires according to the T568B wiring standard.

7. Terminate the Cable to the Keystone Jack:
    a. Insert each wire into the corresponding slot on the keystone jack following the T568B wiring standard.
    b. Use a punch down tool to secure the wires into the keystone jack.
    c. Trim any excess wire.

8. Attach the Keystone Jack to the Faceplate:

a. Insert the terminated keystone jack into the faceplate.
b. Snap or screw the keystone jack into place securely.

9. Install the Faceplate:
    a. Attach the faceplate to the low voltage mounting bracket using screws.
    b. Ensure the faceplate is level and securely fastened.

10. Test the Connection:
    a. Use a cable tester to check the continuity and wiring of the terminated cable.
    b. Follow the tester's instructions to verify that all wires are correctly connected and there are no shorts or opens.

11. Label the Faceplate (Optional):
    a. Use a label maker to label the faceplate for easy identification, if needed.

Specification Sheet-3.2: Install A Faceplate For Computer Networking

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Antistatic Wrist Strap	Pair	01
2	Safety Glasses	Pair	01
3	Gloves	Pair	01
4	Dust Mask	Pair	01
5	Knee Pads	Pair	01
6	Proper Footwear	Pair	01
7	Work Apron	Pair	01

Necessary tools and equipment

Sl. No	Name of Tools & Equipment	Specification	Unit	Quantity
1	Cable Stripper		PCS	01
2	Punch Down Tool		PCS	01
3	Screwdriver		PCS	01
4	Utility Knife		PCS	01
5	Level		PCS	01
6	Cable Tester		PCS	01
7	Antistatic Wrist Strap		PCS	01
8	Label Maker (optional)		PCS	01

Necessary materials

Sl. No.	Name of materials	Specification	Unit	Quantity
1	Ethernet Cable	CAT5e or higher	As required	As required
2	Faceplate	-	As required	As required
3	Keystone Jack	-	As required	As required
4	Low Voltage Mounting Bracket	-	As required	As required
5	RJ45 Connectors	-	As required	As required

Job Sheet-3.3: Set Up A Server Rack For Computer Networking

Job Name: Set up a Server Rack for Computer Networking

Objective:

To set up a server rack, ensuring the proper installation and organization of servers, network equipment, and other components for efficient operation and easy maintenance**.**

Procedure:

Plan the Rack Layout:

- Determine the placement of servers, switches, PDUs, and other equipment in the rack.
- Plan for adequate airflow, with servers typically placed from bottom to top for stability and weight distribution.
- Ensure network switches and patch panels are accessible for easy cable management.

Install the Rack Rails:

- If required, install rack rails into the server rack according to the manufacturer's instructions.
- Ensure rails are securely fastened and level.

Install Power Distribution Units (PDUs):

- Mount PDUs in the rear or side of the rack.
- Ensure PDUs are accessible for plugging in power cables from servers and other equipment.

Mount Servers and Equipment:

- Begin with the heaviest equipment (typically servers) at the bottom of the rack.
- Use rack screws and cage nuts to secure servers and other rack-mountable equipment to the rack rails.
- Ensure all equipment is level and securely fastened.

Install Network Switches and Patch Panels:

- Mount network switches and patch panels in a location that allows easy cable routing.
- Securely fasten using rack screws and cage nuts.

Organize Cables:

- Run Ethernet and power cables neatly, using cable ties or Velcro straps to bundle and secure them.
- Use cable management arms or brackets to route cables and maintain organization.
- Label all cables at both ends for easy identification.

Connect Power Cables:

- Plug power cables from servers and other equipment into the PDUs.
- Ensure all power connections are secure.

Connect Network Cables:

- Connect Ethernet cables from servers to network switches or patch panels.
- Ensure all connections are secure and properly seated.

Ground the Rack (if required):

- If the rack requires grounding, use a grounding kit to connect the rack to a suitable ground point according to safety regulations.

Install Rack-mountable Monitor, Keyboard, and Mouse (optional):

- If using a rack-mountable console, install it in a convenient location in the rack.
- Connect the console to the servers and ensure it is functioning correctly.

Final Inspection and Testing:

- Double-check all connections for security and proper routing.
- Power on the equipment and verify that all devices are receiving power.
- Test network connections to ensure all servers and equipment are communicating correctly.

Update Documentation:

- Update network diagrams and documentation to reflect the new rack setup.
- Include details such as equipment placement, cable routing, and power connections.

Troubleshooting:

Loose or Unstable Equipment:

- Ensure all rack screws and cage nuts are tightened securely.
- Verify that rack rails are properly installed and level.

Cable Management Issues:

- Use additional cable ties or Velcro straps to secure loose cables.
- Re-route cables to avoid tangling or obstruction.

Power Issues:

- Check power connections to ensure all devices are plugged in securely.
- Verify that the PDUs are functioning correctly and supplying power to all connected devices.

Specification Sheet-3.3: Set Up a Server Rack for Computer Networking

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Antistatic Wrist Strap	Pair	01
2	Safety Glasses	Pair	01
3	Gloves	Pair	01
4	Dust Mask	Pair	01
5	Knee Pads	Pair	01
6	Proper Footwear	Pair	01
7	Work Apron	Pair	01

Necessary tools and equipment

Sl. No	Name of Tools & Equipment	Specification	Unit	Quantity
1	Patch Panels		PCS	01
2	Label Maker		PCS	01
3	Cable Ties/Velcro Straps		PCS	01
4	Rack Rails (if required by server)		PCS	01
5	Grounding Kit (if required)		PCS	01
6	Rack Shelves (for non-rack mountable equipment)		PCS	01

Necessary materials

Sl. No.	Name of materials	Specification	Unit	Quantity
1	Server Rack		As required	As required
2	Servers		As required	As required
3	Network Switches		As required	As required
4	Power Distribution Units		As required	As required
5	Cable Management Arms/Brackets		As required	As required
6	Rack Screws and Cage Nuts		As required	As required
7	Ethernet Cables	CAT5e or higher	As required	As required
8	Power Cables		As required	As required

Job Sheet-3.4: Configure A Router

Job Name: Configure a Router

Objective:

To configure a router to connect to a network, set up basic settings, and ensure proper routing and connectivity.

Working Procedure:
Configuring a TP-Link router using PPPoE (Point-to-Point Protocol over Ethernet) connection is a common setup for connecting to the internet through DSL or fiber optic services. Here's a step-by-step guide to configure a TP-Link router using PPPoE:

Before you begin:

- Make sure you have your PPPoE username and password provided by your Internet Service Provider (ISP).

- Connect your TP-Link router to your computer using an Ethernet cable.

Step 1: Access the Router's Web Interface:

1. Open a web browser (e.g., Chrome, Firefox) on your computer.

2. Enter the default IP address of your TP-Link router into the address bar. The default IP address is typically "192.168.0.1" or "192.168.1.1". You can find this information in the router's user manual or on the manufacturer's website.

3. Press Enter. You will be prompted to enter the router's username and password. The default username and password are usually "admin" (without quotes). If you have changed these credentials before, use the updated ones.

Step 2: Configure PPPoE Connection:

4. Once logged into the router's web interface, navigate to the "Network" or "Internet" section, depending on your router model.

5. Look for the option to set up a new connection or WAN (Wide Area Network) connection type. Select "PPPoE" from the dropdown menu.

6. Enter your PPPoE username and password provided by your ISP into the respective fields.

7. Optionally, you may need to configure additional settings such as VLAN ID, MTU (Maximum Transmission Unit), or service name. Consult your ISP or refer to any documentation provided by them for these details.

8. Save the settings and apply the changes.

Step 3: Restart the Router:

9. Restart your TP-Link router to apply the new PPPoE settings. You can usually do this by powering off the router, waiting for a few seconds, and then powering it back on.

Step 4: Test the Connection:

10. Once the router has restarted, open a web browser on your computer and try accessing a website to verify that the internet connection is working properly.

If you encounter any issues during the configuration process, double-check the entered PPPoE credentials and settings, and ensure that your ISP's service is active and properly configured for PPPoE connections. If problems persist, you may need to contact your ISP for further assistance.

Conclusion:

Configuring a router involves setting up basic network settings, securing the wireless network, and ensuring connectivity. Following these steps ensures a properly configured and secure router, facilitating reliable network access and performance.

Specification Sheet-3.4: Configure A Router

Necessary Personal Protective Equipment (PPE)

Sl. No	Name of PPE	Unit	Quantity
1	Antistatic Wrist Strap	Pair	01
2	Safety Glasses	Pair	01
3	Gloves	Pair	01
4	Dust Mask	Pair	01
5	Knee Pads	Pair	01
6	Proper Footwear	Pair	01
7	Work Apron	Pair	01

Necessary tools and equipment

Sl. No	Name of Tools & Equipment	Specification	Unit	Quantity
1	Router	Any	PCS	01
2	Ethernet Cables	CAT5e or higher	PCS	01
3	Computer or Laptop	Any	PCS	01
4	Power Adapter for Router	As per router required	PCS	01
5	Web Browser	Any	PCS	01

Learning Outcome-4: Test newly expanded network

Assessment Criteria	1. Using network diagnostic tools, the network is tested. 2. Congestion of the network is observed. 3. Reachability to Internet (if available) is tested
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Switch 6. Router 7. Networking related Tools and accessories 8. Multimedia Projector 9. Internet Facilities 10. Whiteboard and Marker
Contents	1. Network diagnostic tools and its uses. ▪ Manage engine. ▪ PRTG ▪ Solarwinds 2. Congestion of the network 3. Test Reachability to Internet 4. Documentation process
Activities/job/Task	1. Test newly expanded network using following activity: ▪ Choose appropriate network diagnostic tools based on the suspected issues and your technical expertise. ▪ Track key performance metrics like latency, jitter, and packet loss to identify areas of slowness or instability. ▪ Evaluate factors like insufficient bandwidth, faulty equipment, misconfigured settings, or malware activity. ▪ Use ping and traceroute to test connectivity to an external server and identify any issues with your internet service provider (ISP). ▪ Check DNS resolution and ensure it accurately translates domain names to IP addresses.
Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning 4. Portfolio

Learning Experience-4: Test newly expanded network

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

Learning Activities	Recourses/Special Instructions
1. Students will ask the instructor about "Test newly expanded network."	1. The instructor will provide the learning materials "Test newly expanded network."
2. Read the Information sheet and complete the self-check & Check answer sheets on "Test newly expanded network."	1. Information sheet 4: Test newly expanded network. 2. Self-check 1: Test the newly expanded network. 3. Check your answer with Answer key 1: Test the newly expanded network.
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	1. Job/Task Sheet and Specification Sheet Test the newly expanded network using the following activity: ▪ Choose appropriate network diagnostic tools based on the suspected issues and your technical expertise. ▪ Track key performance metrics like latency, jitter, and packet loss to identify areas of slowness or instability. ▪ Evaluate factors like insufficient bandwidth, faulty equipment, misconfigured settings, or malware activity. ▪ Use ping and traceroute to test connectivity to an external server and identify any issues with your internet service provider (ISP). ▪ Check DNS resolution and ensure it accurately translates domain names to IP addresses **Specification Sheet 1.1:** Test newly expanded network Task Sheet 1.2: Test newly expanded network.

Information Sheet-4: Test newly expanded network

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

4.1 Network diagnostic tools and its uses.
4.2 Congestion of the network
4.3 Test Reachability to Internet

4.1 Network Diagnostic

Network diagnostics refers to the process of identifying, analyzing, and resolving issues related to computer networks. It involves examining the performance, connectivity, and reliability of network systems to diagnose and troubleshoot problems that may impact their functionality.

Network diagnostics encompasses a range of techniques and tools used to investigate and resolve network issues. These may include:

- **Monitoring Network Performance:** This involves measuring various metrics such as bandwidth usage, latency, packet loss, and network congestion to ensure optimal network performance.
- **Identifying Connectivity Issues:** Network diagnostics helps identify issues related to network connectivity, such as connection drops, intermittent connectivity problems, and slow network speeds.
- **Troubleshooting Hardware and Software:** It involves diagnosing problems related to network hardware (e.g., routers, switches, network interface cards) and software (e.g., operating systems, network protocols, firewall settings).
- **Analyzing Network Traffic:** Network diagnostics tools can capture and analyze network traffic to identify patterns, anomalies, or security threats within the network.
- **Resolving DNS and IP Address Issues:** Diagnosing and resolving problems related to Domain Name System (DNS) resolution and IP address configuration.
- **Testing Connectivity and Reachability:** Tools and techniques are used to test connectivity between network devices and to verify reachability to remote hosts or services.
- **Security Auditing:** Network diagnostics may involve auditing network security settings and configurations to identify vulnerabilities and ensure compliance with security policies.

Network diagnostics tools:

Network diagnostics tools are essential for organizations to monitor their network for performance issues, security risks, and outages. Network diagnostics tools continuously monitor networks for problems then provide alerts and reports to enable admins to quickly and efficiently respond if an issue arises.

Network diagnostics tools are installed on network devices. These tools will monitor all network traffic, and collect data to analyze network performance, status, and reliability. These insights are displayed in a real-time reporting console, with historical insights and analytics. If an issue or security vulnerability is detected, admins will be alerted, and the problem can be remediated.

SolarWinds Network Performance Monitor

SolarWinds is a market leader in the IT management software space. SolarWinds Network Performance Monitor Solution is a highly scalable, multi-vendor network monitoring solution, that provides deep network insights with advanced alerting and mapping. This solution can be used in gathering networks, enabling teams to identify and resolve network issues, like performance errors, outages, and connectivity problems, quickly.

SolarWinds Network Performance Monitor Features:

- Latency tests to monitor network device availability and performance.
- Automated alerting for network performance issues
- Historical network performance tracking, with timelines
- Detailed analytics and contextual reporting with customizable charts and dashboards
- In-depth diagnostics and network insights

4.2 Congestion of the network:

Network Congestion occurs when the traffic flowing through a network exceeds its maximum capacity. In most cases, congestion is a temporary issue with the network caused due to a sudden upsurge of traffic, however, sometimes; a network is continually congested, indicating a deeper problem. End-users perceive network congestion as Network Slowdown or a very large delay in processing requests.

Network congestion is also a contributing factor in the following underlying issues:

- **High Latency –** In a congested network, the time taken by a packet to reach its destination increases significantly, hence a higher latency rate is observed.
- **Connection timeouts** –Ideally, the service should wait for the arrival of packets but in several cases, the connection terminates due to timeout.
- **Packet loss** –Many packets cannot reach their destination if the network is congested and will be dropped eventually due to timeout.

Causes of network congestion:

Excessive bandwidth consumption: Certain users or devices on the network may occasionally utilize more bandwidth than the average user or device. This can put a strain on the network and its routing equipment (routers, switches, and cables), causing network congestion.

- **Poor subnet management:** For better resource management, a big network is divided into subnets. However, network congestion could arise if the subnets are not scaled according to usage patterns and resource requirements.
- **Broadcast Storms**: A broadcast storm occurs when there is a sudden upsurge in the number of requests to a network. As a result, a network may be unable to handle all the requests at the same time.
- **Multicasting**: Multicasting occurs when a network allows multiple computers to communicate with each other at the same time. In multicasting, a collision can occur when two packets are sent at the same time. Such frequent collisions may cause a network to be congested.
- **Border Gateway Protocol:** All traffic is routed by BGP via the shortest possible path. However, while routing a packet, it doesn't consider the amount of traffic present in the route. In such scenarios, there is a possibility all the packets are being routed via the same route which may lead to network congestion.
- **Too many devices:** Every network has a limit on the amount of data it can manage. This capacity establishes a limit on how much bandwidth and traffic your network can handle before performance degrades. If the network has too many devices linked to it, the network may become burdened with data requests.
- **Outdated Hardware:** When data is transmitted over old switches, routers, servers, and Internet exchanges, bottlenecks can emerge. Data transmission can get hampered or slowed down due to outdated hardware. As a result, network congestion occurs.
- **Over-subscription:** A cost-cutting tactic that can result in the network being compelled to accommodate far more traffic than it was designed to handle (at the same time).

Self-Check-4: Test Newly Expanded Network

1. **What is network diagnostics?**

Answer:

2. **What are some common tasks in network diagnostics?**

Answer:

3. **What are some key features of ManageEngine OpManager?**

Answer:

4. **What is the main purpose of PRTG Network Monitor?**

Answer:

5. **How does SolarWinds Network Performance Monitor help in managing networks?**

Answer:

6. **What are some strategies for managing network congestion?**

Answer:

7. **What is Quality of Service (QoS) used for in network management?**

Answer:

8. **How does load balancing help in managing network congestion?**

Answer:

Answer Key-4: Test Newly Expanded Network

1. **What is network diagnostics?**

   Answer: Network diagnostics is the process of analyzing, identifying, and resolving issues within a computer network.

2. **What are some common tasks in network diagnostics?**

   Answer: Tasks include monitoring network performance, identifying connectivity issues, troubleshooting hardware and software, analyzing network traffic, resolving DNS and IP address issues, testing connectivity, and auditing security.

3. **What are some key features of ManageEngine OpManager?**

   Answer: ManageEngine OpManager offers features such as network device monitoring, bandwidth monitoring, alerts and notifications, performance reporting, and configuration management.

4. **What is the main purpose of PRTG Network Monitor?**

   Answer: PRTG Network Monitor is used for comprehensive network monitoring, offering various sensors to monitor devices, services, applications, and traffic.

5. **How does SolarWinds Network Performance Monitor help in managing networks?**

   Answer: SolarWinds NPM provides deep visibility into network performance, offering features like network device monitoring, traffic analysis, intelligent alerts, network mapping, application performance monitoring, and customizable reports.

6. **What are some strategies for managing network congestion?**

   Answer: Strategies include bandwidth management, traffic shaping, network optimization, load balancing, capacity planning, packet prioritization, network segmentation, and monitoring and analysis.

7. **What is Quality of Service (QoS) used for in network management?**

   Answer: QoS is used to prioritize critical traffic over less important traffic, ensuring that essential applications receive sufficient bandwidth during periods of congestion.

8. **How does load balancing help in managing network congestion?**

   Answer: Load balancing distributes network traffic across multiple paths or devices, preventing congestion by evenly distributing traffic and utilizing available network resources more efficiently.

Learning Outcome-5: Maintain Record of Maintenance

Assessment Criteria	1. Network maintenance plan is completed. 2. Network maintenance plan is approved by the appropriate person or from the organization. 3. Approved network maintenance plan is documented. 4. Support plan for the network is documented. 5. User manual for the network is prepared
Conditions and Resources	1. Actual workplace or training environment 2. CBLM 3. Handouts 4. Laptop/ Desktop 5. Multimedia Projector 6. Paper, Pen, Pencil and Eraser 7. Internet Facilities 8. Whiteboard and Marker
Contents	1 Network maintenance plan. 2 Backup of Updated configuration file 3 Implementation process of network maintenance plan 4 Documentation process of network maintenance plan 5 Process to document the support plan. 6 Process to prepare user manual
Activities/job/Task	1. Identify all necessary maintenance tasks for network components, including hardware, software, and security infrastructure. 2. Develop a schedule for routine maintenance (e.g., backups, updates, cleaning), preventive maintenance (e.g., performance checks, diagnostics), and corrective maintenance (e.g., troubleshooting, repairs). 3. Secure formal approval from the designated authority for the network maintenance plan to proceed. 4. Establish a system for version control and updating all documentation as the network evolves or maintenance procedures change. 5. Record detailed notes about the troubleshooting process, including used tools, observed symptoms, and identified issues.

Training Methods	1. Blended 2. Discussion 3. Presentation 4. Demonstration 5. Guided Practice 6. Individual Practice 7. Project Work 8. Problem Solving 9. Brainstorming
Assessment Methods	Assessment methods may include but not limited to 1. Written Test 2. Demonstration 3. Oral Questioning 4. Portfolio

Learning Experience-5: Maintain Record Of Maintenance

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

Learning Activities	Recourses/Special Instructions
1. The student will ask the instructor about "Maintain record of maintenance."	1. The instructor will provide the learning materials "Maintain record of maintenance."
2. Read the Information sheet and complete the Self-check & Check answer sheets on "Maintain record of maintenance."	1. Information sheet 5: Maintain record of maintenance. 2. Answer Self-check 1: Maintain record of maintenance. 3. Check your answer with Answer key 1: Maintain record of maintenance
3. Read the Job/Task Sheet and Specification Sheet and perform job/Task	1. Job/Task Sheet and Specification Sheet 1. Identify all necessary maintenance tasks for network components, including hardware, software, and security infrastructure. 2. Develop a schedule for routine maintenance (e.g., backups, updates, cleaning), preventive maintenance (e.g., performance checks, diagnostics), and corrective maintenance (e.g., troubleshooting, repairs). 3. Secure formal approval from the designated authority for the network maintenance plan to proceed. 4. Establish a system for version control and updating all documentation as the network evolves or maintenance procedures change. 5. Record detailed notes about the troubleshooting process, including used tools, observed symptoms, and identified issues. **Specification Sheet 5.1:** Maintain record of maintenance Task Sheet 5.1: Maintain record of maintenance.

Information Sheet-5: Maintain Record of Maintenance

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

5.1 Network maintenance plan.
5.2 Backup of Updated configuration file
5.3 Implementation process of network maintenance plan
5.4 Documentation process of network maintenance plan
5.5 Process to document the support plan.
5.6 Process to prepare user manual.

5.1 Network maintenance plan.

A network maintenance plan is a systematic approach to managing and sustaining the health, performance, and security of a computer network. It involves regular activities, procedures, and policies aimed at ensuring that the network infrastructure functions optimally and remains resilient against potential issues or threats.

Key components of a network maintenance plan typically include:

- **Routine Maintenance Tasks:** This involves regular activities such as software updates, hardware checks, and system backups to ensure that all components of the network are up to date and functioning properly.
- **Security Measures:** Implementing and updating security protocols, firewalls, intrusion detection systems, and antivirus software to protect the network from cyber threats such as malware, viruses, and hacking attempts.
- **Performance Monitoring:** Continuous monitoring of network performance metrics such as bandwidth usage, latency, and packet loss to identify potential bottlenecks or issues that may affect performance.
- **Troubleshooting and Problem Resolution:** Developing procedures and protocols for diagnosing and resolving network issues in a timely manner to minimize downtime and maintain productivity.
- **Capacity Planning:** Assessing current and future network needs, and adjusting accommodate growth in traffic or new technology requirements.
- **Documentation:** Maintaining comprehensive documentation of the network infrastructure, including configurations, diagrams, and change logs, to facilitate troubleshooting and future planning.
- **Disaster Recovery and Backup:** Implementing backup and disaster recovery solutions to ensure data integrity and continuity of operations in the event of a network failure or data loss.
- **Regular Audits and Compliance Checks:** Conducting periodic audits to ensure that the network meets regulatory requirements and industry standards for security and performance.

5.2 Backup of Updated configuration file

Configuration Backup

Configuration backup is a process of saving your existing network configuration files and creating a repository with all versions stored in incremental versions. Config backups are mostly encrypted before being stored in the database, to ensure high security.

The most critical application to backup configuration is to restore network functions in times of a network disaster. Faulty configuration changes can cause network disasters like a data breach or even a network outage. In such times, network admins can upload a stable configuration version from the repository and restore the network promptly. Configuration backups are also important while auditing to identify where a particular fault originated from and for compliance audits.

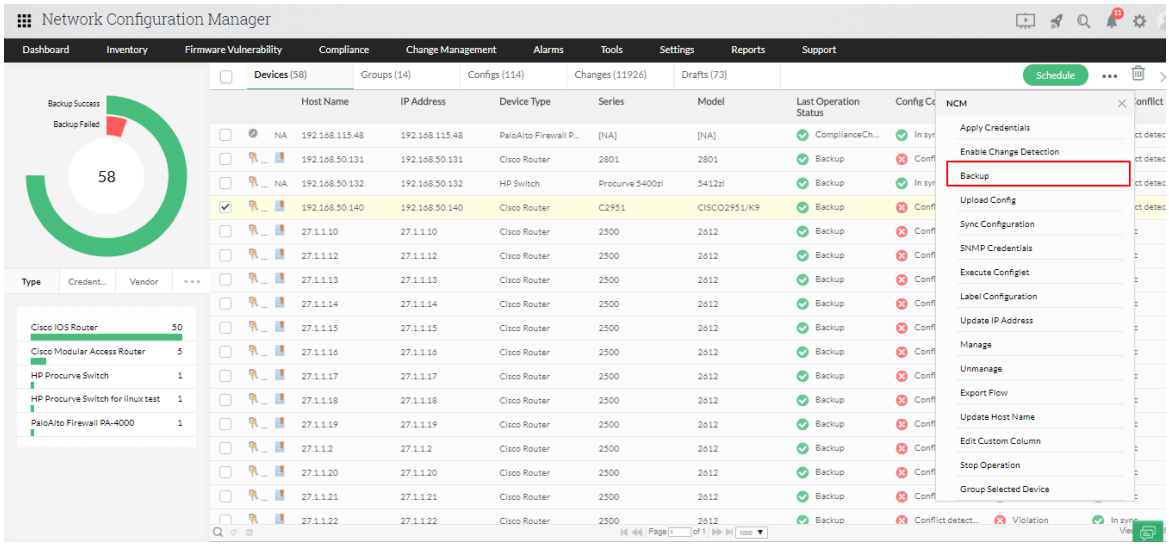
How to backup network configurations

- You can manually copy all network configuration files by logging into each device through Telnet or PuTTY consoles. But this is a time-consuming process, and since configurations are frequently changed, the files need to be backed up as soon as changes are made via a configuration backup software.
- Configuration management tools can help you save time taken to backup configuration files. You can automate network configuration backups of devices which require routine backups and instantly backup configurations of devices in bulk whenever required.
- Apart from performing configuration backup using a configuration backup tool, you can upload configurations into devices. Whenever there is a network outage, the network admin must simply upload the most stable configuration of that device to restore the network.

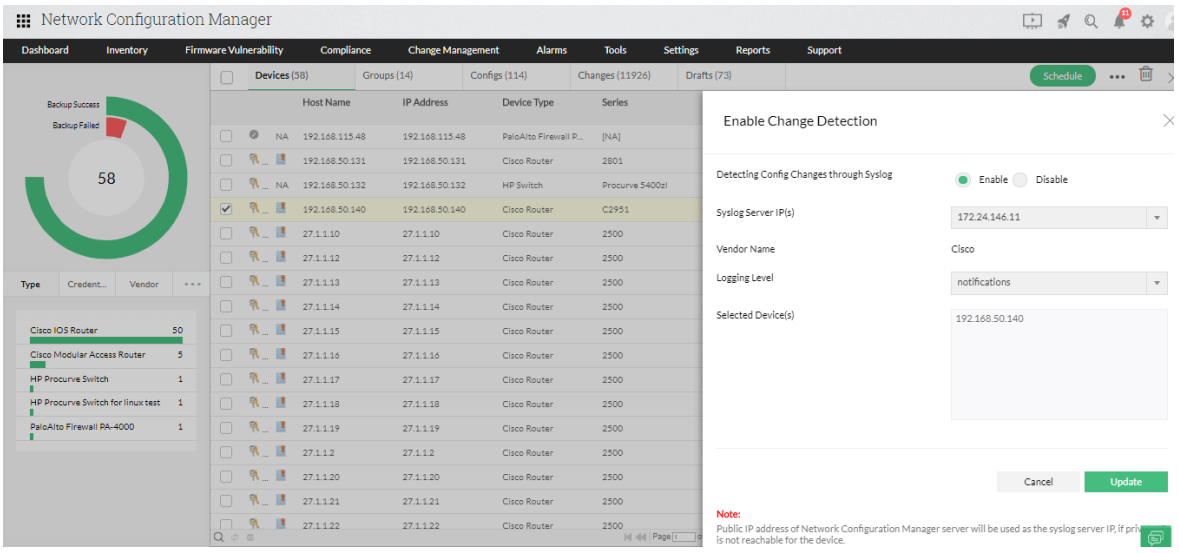
Types of backups in Network Configuration Manager:

With Network Configuration Manager, admins can backup configurations in three ways:

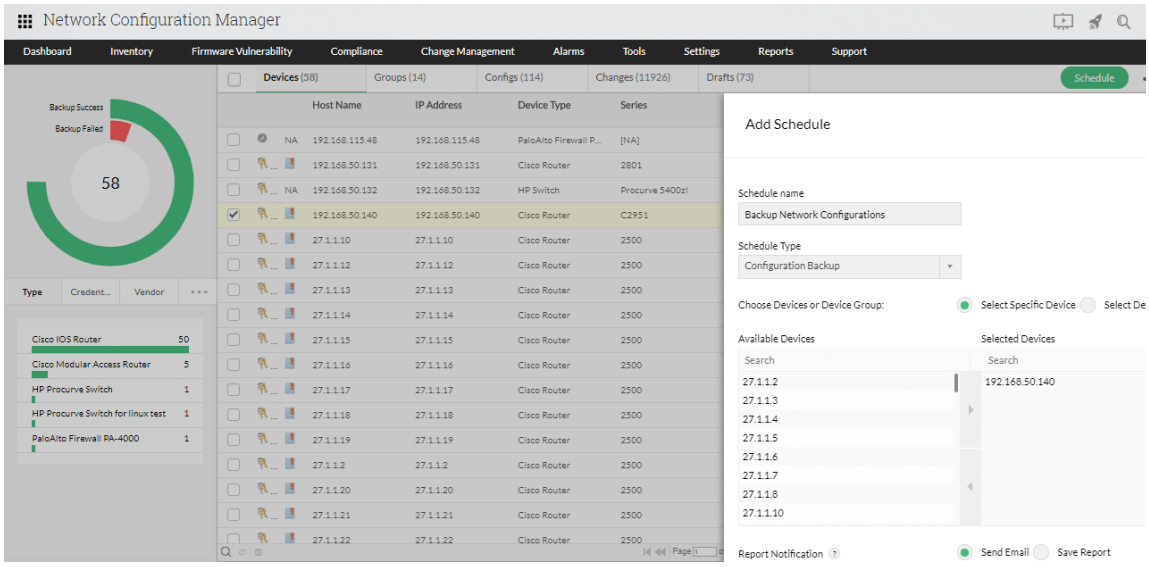
- Manual Backup: Performing configuration backups before carrying out critical configuration changes is important. If those changes go wrong, admins can immediately revert all changes made by uploading an older version of the configuration file. Manual backup enables admins to perform backups of devices whenever required.



- **Real-time change detection-based backup:** Network admins might forget to backup configurations after making certain critical changes. Network Configuration Manager detects these changes in real-time and immediately triggers backups. This syslog-based backup will prevent the loss of all critical changes that the admin made before logging out of the device.



- **Scheduled backup:** Manually triggering backups can be time-consuming and you might also miss backing up configurations of critical devices on your network. Using Network Configuration Manager, admins can automate backups for devices in which configuration changes are made frequently. They can choose to schedule backup for just once or schedule routine backups depending on how frequently changes are made to devices.



5.3 Implementation process of network maintenance plan:

Implementing a network maintenance plan involves several steps to ensure that the plan is effectively executed and maintained over time. Here's a structured approach to implementing a network maintenance plan:

a. Assessment and Planning:

- Assess the current state of the network infrastructure, including hardware, software, security measures, and documentation.
- Identify areas for improvement and prioritize tasks based on criticality and impact on network performance and security.
- Develop a comprehensive maintenance plan that outlines specific tasks, schedules, responsibilities, and resources required for implementation.

b. Resource Allocation:

- Allocate appropriate resources, including personnel, tools, and budget, to support the implementation of the maintenance plan.
- Ensure that staff members responsible for network maintenance are adequately trained and equipped to carry out their tasks effectively.

c. Documentation and Inventory:

- Create detailed documentation of the network infrastructure, including network topology, device configurations, IP addressing schemes, and network diagrams.
- Maintain an up-to-date inventory of network devices, including hardware specifications, serial numbers, firmware versions, and warranty information.

d. Configuration Management:

- Implement configuration management practices to track changes to network configurations and ensure consistency and compliance with best practices.

- Establish procedures for reviewing, approving, and documenting changes to network configurations, including version control and rollback mechanisms.

e. Security Measures:

- Implement security measures to protect the network infrastructure from cyber threats, including firewalls, intrusion detection systems, antivirus software, and encryption protocols.
- Regularly update security patches and firmware updates to address vulnerabilities and ensure that security measures remain effective over time.

f. Performance Monitoring and Optimization:

- Deploy network monitoring tools to continuously monitor network performance metrics, including bandwidth utilization, latency, packet loss, and device health.
- Analyze performance data to identify bottlenecks, optimize network resources, and proactively address potential issues before they impact user experience.

g. Backup and Disaster Recovery

- Implement backup and disaster recovery solutions to protect critical network data and ensure business continuity in the event of data loss or network failure.
- Regularly test backup and recovery procedures to verify their effectiveness and identify any potential gaps or issues that need to be addressed.

h. Regular Maintenance and Review

- Establish a schedule for regular maintenance tasks, including software updates, hardware checks, security audits, and performance tuning.
- Conduct periodic reviews of the network maintenance plan to evaluate its effectiveness, identify areas for improvement, and make necessary adjustments to adapt to changing business requirements and technological advancements.

5.4 Documentation process of network maintenance plan

Documenting the network maintenance plan is essential for ensuring that all aspects of the plan are clearly defined, understood, and followed by the relevant stakeholders. Here is a structured approach to documenting a network maintenance plan:

a. Introduction and Overview:

- Introduce the document, explaining its purpose and scope.
- Give an overview of the network maintenance plan, including its objectives, key components, and benefits to the organization.

b. Network Infrastructure Description:

- Describe the organization's network infrastructure, including its topology, architecture, and components such as routers, switches, firewalls, servers, and endpoints.

- Provide network diagrams and schematics to visually represent the layout and connections of the network infrastructure.

c. Maintenance Tasks and Procedures:

- List all maintenance tasks that need to be performed regularly to ensure the health, performance, and security of the network.
- For each maintenance task, provide detailed procedures, including step-by-step instructions, tools required, and any prerequisites or dependencies.
- Specify the frequency at which each maintenance task should be performed (e.g., daily, weekly, monthly) and assign responsibilities to the appropriate personnel.

d. Configuration Management:

- Document the configuration management process, including procedures for documenting, reviewing, approving, and implementing changes to network configurations.
- Specify the tools and software used for configuration management, such as version control systems or configuration management databases (CMDBs).

e. Security Measures:

- Document the organization's security policies and procedures related to network maintenance, including access control, authentication, encryption, and security monitoring.
- Describe the security measures implemented to protect the network infrastructure from cyber threats, such as firewalls, intrusion detection/prevention systems, and antivirus software.

f. Performance Monitoring and Optimization:

- Document the performance monitoring tools and techniques used to track network performance metrics, such as bandwidth utilization, latency, packet loss, and device health.
- Describe how performance data is analyzed, interpreted, and used to optimize network resources and identify potential issues.

g. Backup and Disaster Recovery:

- Document the backup and disaster recovery procedures, including how data backups are performed, stored, and tested for recoverability.
- Specify the backup schedule, retention policies, and procedures for restoring data in the event of a disaster or data loss.

h. Training and Communication:

- Outline training programs and resources available to personnel responsible for network maintenance to ensure they have the necessary skills and knowledge to perform their duties effectively.
- Describe communication channels and protocols for disseminating information about network maintenance activities, changes, and updates to relevant stakeholders.

i. Revision History and Version Control:

- Maintain a revision history to track changes made to the network maintenance plan over time, including dates of revisions, authorship, and summaries of changes.
- Implement version control mechanisms to ensure that the latest version of the document is readily available and accessible to all stakeholders.

j. Appendices

- Include any additional supplementary information, such as sample templates, checklists, or troubleshooting guides, that may be useful for implementing and executing the network maintenance plan.

Self-Check-5: Maintain Record f Maintenance

1. What is the purpose of a network maintenance plan?
   Answer:
2. Why is it important to back up updated configuration files?
   Answer:
3. What are some key components of a network maintenance plan?
   Answer:
4. What is the role of documentation in network maintenance?
   Answer:
5. How can organizations optimize network performance?
   Answer:
6. What is the purpose of a support plan?
   Answer:
7. How can organizations collect feedback on support services?
   Answer:
8. Why is it important to maintain a knowledge base for support?
   Answer:
9. What are some common channels for requesting support?
   Answer:
10. How can organizations ensure compliance with legal requirements in support services?
    Answer:
11. What is the purpose of a user manual?
    Answer:
12. What should be included in a user manual?
    Answer:
13. Why is it important to update and maintain a user manual?
    Answer:
14. How can organizations distribute user manuals to users?
    Answer:
15. What role does user feedback play in improving a user manual?
    Answer:

Answer Key-5: Maintain Record of Maintenance

1. **What is the purpose of a network maintenance plan?**
   Answer: The purpose of a network maintenance plan is to manage and sustain the health, performance, and security of a computer network.

2. **Why is it important to back up updated configuration files?**
   Answer: It's important to back up updated configuration files to ensure that previous configurations can be restored in case of issues or changes.

3. **What are some key components of a network maintenance plan?**
   Answer: Key components include routine maintenance tasks, security measures, performance monitoring, troubleshooting procedures, and disaster recovery plans.

4. **What is the role of documentation in network maintenance?**
   Answer: Documentation provides a record of network configurations, procedures, and changes, facilitating troubleshooting, compliance, and knowledge sharing.

5. **How can organizations optimize network performance?**
   Answer: Organizations can optimize network performance by monitoring metrics such as bandwidth usage, latency, and packet loss, and making adjustments as needed.

6. **What is the purpose of a support plan?**
   Answer: The purpose of a support plan is to define procedures for providing assistance, resolving issues, and maintaining service levels for users or customers.

7. **How can organizations collect feedback on support services?**
   Answer: Organizations can collect feedback through surveys, customer satisfaction ratings, help desk tickets, and direct communication with users.

8. **Why is it important to maintain a knowledge base for support?**
   Answer: Maintaining a knowledge base helps support teams provide consistent, efficient assistance by documenting solutions to common issues and best practices.

9. **What are some common channels for requesting support?**
   Answer: Common channels include phone, email, chat, ticketing systems, self-service portals, and in-person support desks.

10. **How can organizations ensure compliance with legal requirements in support services?**
    Answer: Organizations can ensure compliance by adhering to relevant laws and regulations, protecting sensitive information, and implementing security measures.

11. **What is the purpose of a user manual?**
    Answer: The purpose of a user manual is to provide instructions and guidance for users on how to use a product or service effectively.

12. **What should be included in a user manual?**
    Answer: A user manual should include clear instructions, visuals, troubleshooting tips, FAQs, and an organized structure for easy reference.

13. **Why is it important to update and maintain a user manual?**
    Answer: Updating and maintaining a user manual ensures that it remains accurate, relevant, and helpful as the product or service evolves over time.

14. **How can organizations distribute user manuals to users?**
    Answer: Organizations can distribute user manuals through printed copies, digital downloads, online documentation portals, and integrated help systems.

15. **What role does user feedback play in improving a user manual?**
    Answer: User feedback helps identify areas for improvement, clarify confusing instructions, and ensure that the user manual meets the needs of its audience.

Task Sheet-5.1: Maintain Record of Maintenance

TASK SHEET 2.1	
Title: Maintain record of maintenance	
1	Performance Objective: At the end of this task, the trainee should be able to interpret network security, configuring firewall services monitoring the threat and document and report the threat.
2	Identify all necessary maintenance tasks for network components, including hardware, software, and security infrastructure.
3	Develop a schedule for routine maintenance (e.g., backups, updates, cleaning), preventive maintenance (e.g., performance checks, diagnostics), and corrective maintenance (e.g., troubleshooting, repairs).
4	Secure formal approval from the designated authority for the network maintenance plan to proceed.
5	Establish a system for version control and updating all documentation as the network evolves or maintenance procedures change.
6	Record detailed notes about the troubleshooting process, including used tools, observed symptoms, and identified issues

Review of Competency

Below is yourself assessment rating for module **"Set-up and Expand Networks"**

Assessment of performance Criteria	Yes	No
Organizational requirements to expand an existing network are collect		
Existing network design is reviewed for expansion of the network		
Collected information is documented		
Collected information are analyzed and a network design plan is prepared.		
Network design plan is reviewed and approved from the appropriate person of the organization		
Required equipment and tools are listed and estimated budget calculated and documented		
Estimated budget and required equipment list are discussed with and approved by the appropriate personarch tools are identified;		
According to the approved network design plan an existing network is deployed		
Network is connected to the internet		
Equipment and materials are collected to expand network		
Nodes are connected to the network		
Deployment of network is performed		
Using network diagnostic tools, network is tested		
Congestion of the network is observed		
Reachability to Internet (if available) is tested		
Network maintenance plan is completed.		
Network maintenance plan is approved by the appropriate person or from the organization		
Approved network maintenance plan is documented		
Support plan for the network is documented		
User manual for the network is prepared		

I now feel ready to undertake my formal competency assessment.

Signed:

Date:

Development of CBLM

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

SL No.	Name & Address	Designation	Contact Number
1	Mir Rashedul Islam	Writer	01920576687
2	Md. Abdul Hye Siddiqui	Editor	01819-725610
3	Md. Zuwel Parves	Co-Ordinator	01737-278906
4	Md. Saif Uddin	Reviewer	01723-004419