Competency Based Learning Materials (CBLM)

IT Support Service

Level-4

Module: Troubleshooting Network

Code: CBLM-OU-ICT-ITSS-04-L4-V1

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

Copyright

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

This Competency Based Learning Materials (CBLM) on "Troubleshooting Network" 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.

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

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

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

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

How to use this Competency Based Learning Materials (CBLMs)

The module, Troubleshooting Network 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.

Table of Content

Module Content

Unit of Competency: Troubleshoot Network

Module Title: Troubleshooting Network

Module Description: This module discusses the aspects that must be given attention when Troubleshooting Network. It shows the knowledge and skills requirements for interpreting methodology and plan, identifying the problem, identifying the Solution, solving the Problem and cleaning workplace and updating document

Nominal Duration: 50 Hours

Learning Outcomes:

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

1. Interpret methodology and plan
2. Identify the problem
3. Identify the Solution
4. Solve the Problem
5. Clean workplace and update document

Assessment Criteria:

1. Troubleshoot methodology is interpreted
2. Network tools and utilities for troubleshooting are interpreted
3. Network design, support and maintenance documents are reviewed
4. Computer manuals and maintenance documents are reviewed
5. Appropriate person is consulted for identifying problems if required.
6. Plan of action is interpreted
7. Network Fault is identified
8. Faulty hardware or software component are detected.
9. The problem scenarios are observed
10. Problems are detected using diagnostic tools
11. Appropriate person (if required) is consulted and solution is identified
12. Types of solutions are identified
13. Replacement of faulty hardware equipment is performed if required
14. Replaced equipment is tested
15. Configuration is performed as per solution requirement
16. Network activity is tested.
17. Tools and equipment are stored as per workplace procedures.
18. Network and computer maintenance and troubleshooting document are updated

Learning Outcome-1: Interpret Methodology and Plan

Assessment Criteria:

1. Troubleshoot methodology is interpreted
2. Network tools and utilities for troubleshooting are interpreted
3. Network design, support and maintenance documents are reviewed
4. Computer manuals and maintenance documents are reviewed
5. Appropriate person is consulted for identifying problems if required.
6. Plan of action is interpreted

Content:

1. Network Troubleshooting methodology
2. Network tools and utilities
    - Cabling tools
        - Ethernet cable
        - Fiber Optic
        - N-MAP
        - Wireshark
    - Windows/Linux CLI
        - Lookup
        - Netstat
        - Ipconfig/ Ifconfig
        - Tracert
        - Ping
        - Pathing
        - ARP
        - IP table
        - TCP Dump
3. Reviewing Network design, support and maintenance documents
4. Reviewing Computer manuals and maintenance documents
5. Consulting Appropriate person for identifying problems.
6. Plan of action

Resources Required/ Conditions:

The trainees must be provided with the following:

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

Methodologies

1. Lecture/discussion
2. Demonstration/application
3. Presentation
4. Blended delivery methods

Assessment Methods

1. Written test
2. Demonstration
3. Observation with checklist
4. Oral questioning
5. Portfolio

Learning Experience-1: Interpret Methodology and Plan

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

Learning Steps	Resources specific instructions
1. Trainee will ask the instructor about interpreting methodology and plan	1. Instructor will provide the learning materials "**Interpret methodology and plan"**
2. Read the Information sheet/s	2. Information Sheet No: 1 Interpret methodology and plan
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 1 Interpret methodology and plan Answer key No. 1 Interpret methodology and plan
4. Read the Job Sheet and Specification Sheet and perform job	4. Activity- Sheet No: 1- Interpret methodology and plan

Information Sheet-1: Interpret Methodology and Plan

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

1.1 Interpret Troubleshoot methodology
1.2 Interpret Network tools and utilities for troubleshooting
1.3 Review Network design, support and maintenance documents
1.4 Review Computer manuals and maintenance documents
1.5 Consult Appropriate person for identifying problems if required.
1.6 Interpret Plan of action

1.1 Network Troubleshooting methodology

Network troubleshooting methodology refers to a systematic approach for resolving network issues. It involves following a logical sequence of steps to identify the root cause of the problem and implement an effective solution. Here's a common framework used in network troubleshooting:

Interpret Troubleshoot methodology

Certainly! Let's delve into the world of troubleshooting methodology. Whether you're an IT professional, a curious learner, or someone dealing with everyday issues, understanding this systematic approach can be immensely helpful.

What Is Troubleshooting?

Troubleshooting is essentially a problem-solving method used to identify, analyze, and resolve issues in various systems, whether they involve technology, business processes, or everyday scenarios1. It's like being a detective for problems!

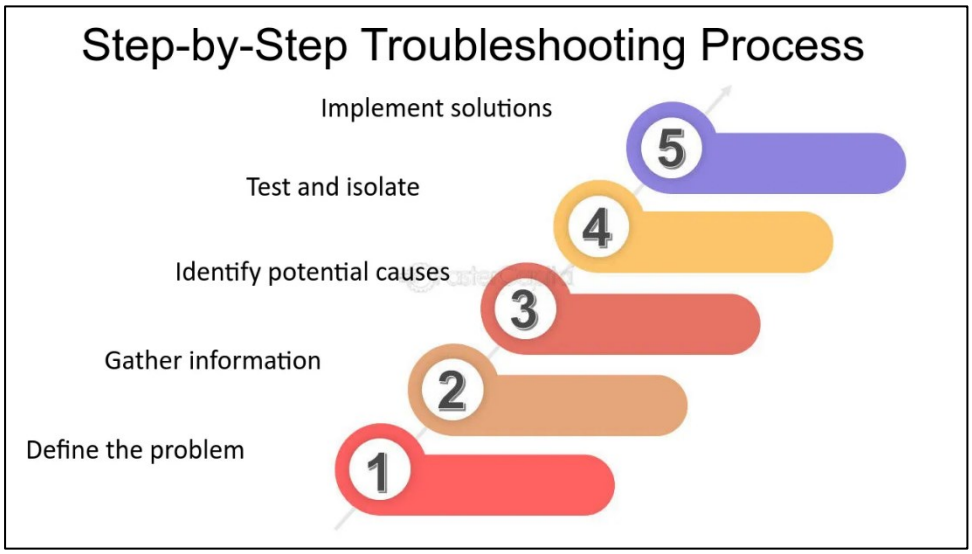


Fig: Interpret Troubleshoot methodology

a Define the Problem

Gather information about the symptoms: Is there complete loss of connectivity, slow performance, or difficulty accessing specific resources?

When did the problem start? Did any changes occur on the network around that time (hardware/software updates, new devices added)?

Who is affected? Is it one device or the entire network?

b Gather Information

Document the network configuration, including IP addresses, subnet masks, default gateways, and firewall rules.

Check network logs for any error messages or unusual activity.

Interview users to understand their specific experiences with the network issue.

c Develop a Theory

Based on the information collected, analyze potential causes.

Consider common network problems like:

Physical connection issues (loose cables, damaged equipment)

Incorrect network configuration (IP settings, subnet masks)

Software problems (outdated drivers, malware)

Overloaded network resources

Security issues (firewalls blocking traffic)

d Test the Theory

Use troubleshooting tools like ping, tracert, and lookup to diagnose connectivity and DNS issues.

Isolate the problem by systematically testing different network components (e.g., restarting devices, testing specific cables).

e Implement a Solution:

Based on the test results, fix the identified problem. This might involve:

Replacing faulty cables or equipment

Reconfiguring network settings

Updating software or drivers

Implementing security measures

f Verify System Functionality

Test the network thoroughly to ensure the implemented solution resolved the issue.

g Document the Process

Record the troubleshooting steps taken, the identified cause, and the implemented solution. This will be helpful for future reference and knowledge sharing.

1.2 Network tools and utilities

Network tools and utilities are like the toolbox for network administrators and anyone who needs to diagnose and maintain a computer network. They're essentially software programs that help you:

These tools provide information about your network devices, their configuration, and how data is flowing. This can be crucial for identifying bottlenecks or pinpointing where a connection issue arises.

Fix what is wrong

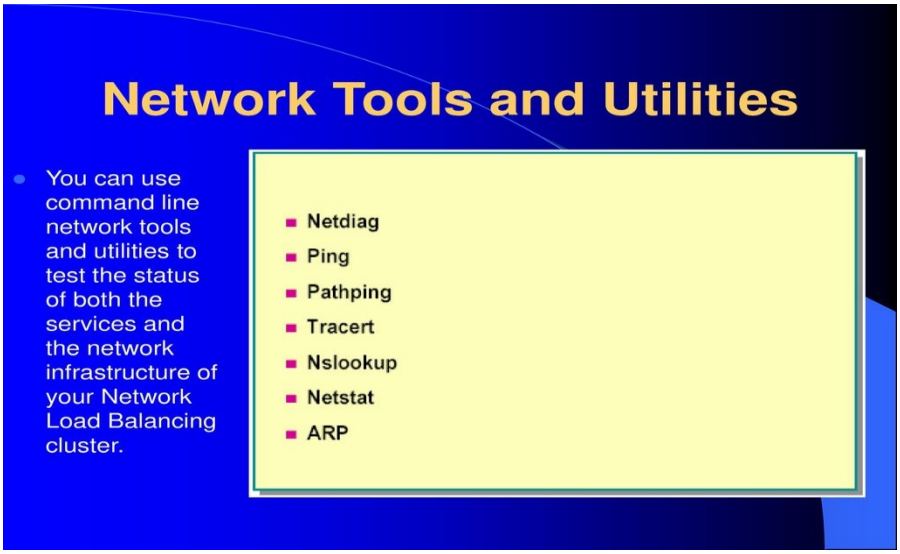
Many tools allow you to troubleshoot network problems. They can help you check if devices are communicating, identify faulty cables, or diagnose configuration errors.

Manage your network

Some utilities offer features for managing network devices, configuring settings, or monitoring performance over time.

Here's a breakdown of some common network tools and utilities:

Basic Troubleshooting Tools (often built-in to operating systems):

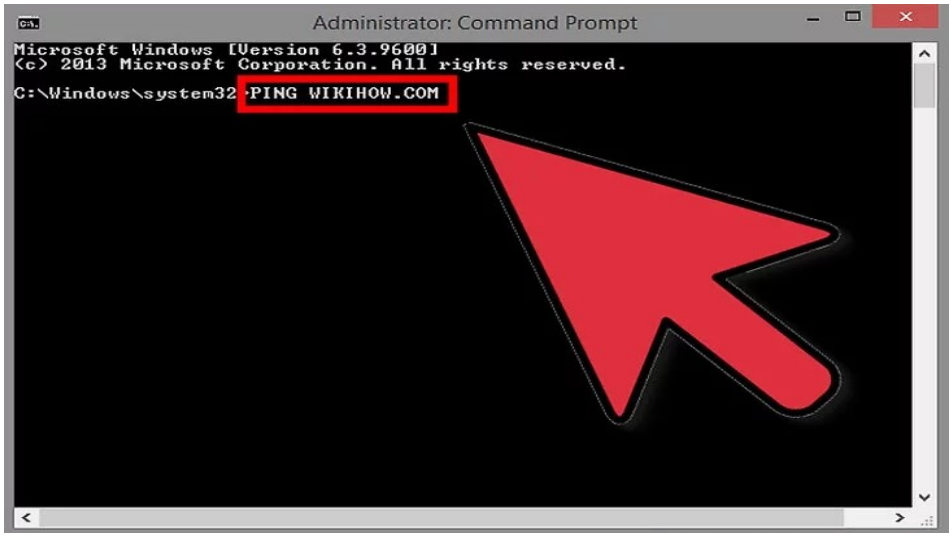


Net Diag: This is one of the favorite tools among Network Administrators to identify and troubleshoot a system with networking issues. Net diag performs a number of network configuration tests (all in order) to output a detailed report that helps Network Engineers to analyze and diagnose the problems. You can check the detailed tests in Microsoft's TCP/IP troubleshooting tools. There are a few useful switches that can be used with Net diag to customize the output. One such useful switch is /fix that troubleshoots DNS problems.

```
C:\Users\dawgotra>net diag
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

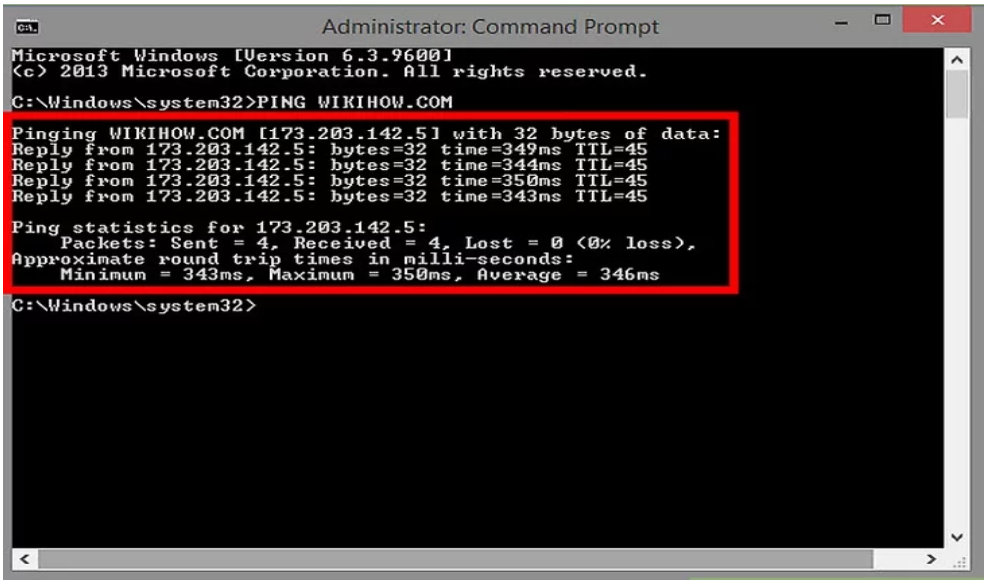
Ping: This is a common networking tool to test the communication between the source and destination hosts. You can test the systems and devices in LAN and also test the websites or default gateway for communication. Ping command shows the packets sent and received between two hosts and also lets you know the percentage of data loss.

1. Open the Command Prompt or Terminal. Every operating system has a command line interface that will allow you to run the Ping command. The Ping command operates virtually identically on all systems.
   If using Windows, open the Command Prompt. Click the Start button and enter cmd into the Search field. Windows 8 users can type "cmd" while on the Start screen. Press Enter to launch the Command Prompt.
   If using Mac OS X, open the Terminal. Open your Applications folder, and then open the Utilities folder. Select Terminal.
   If using Linux, Open a Telnet/Terminal window. It is most often found in the Accessories folder in your Applications directory.
   In Ubuntu, you can use the keyboard shortcut Ctrl + Alt + T to open the terminal.

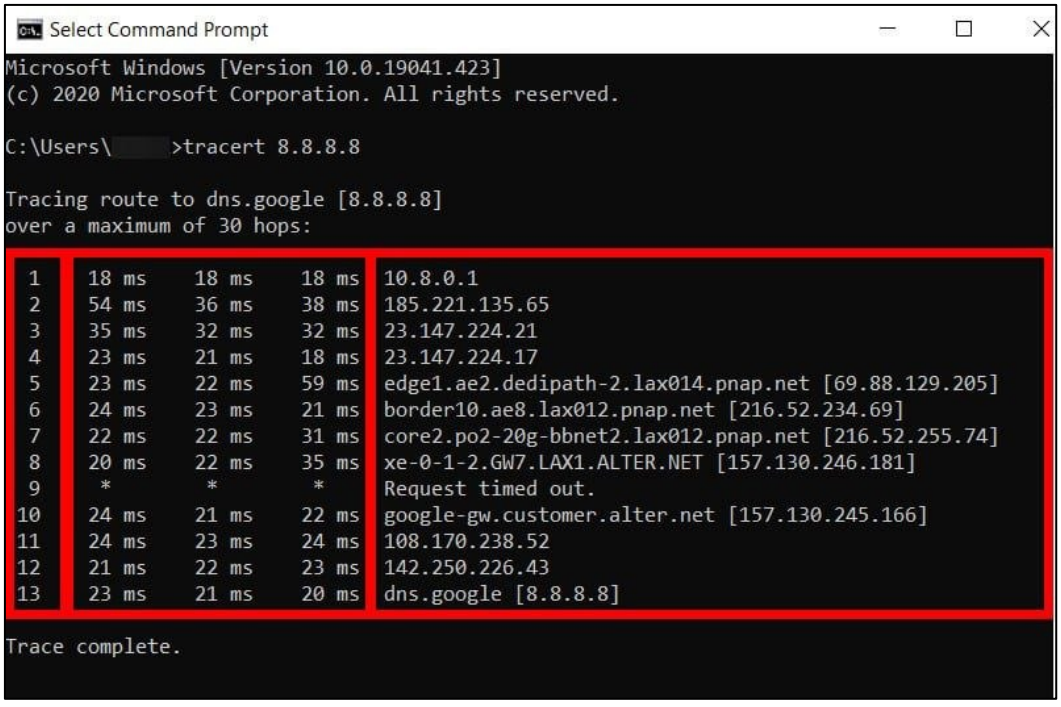


2. **Enter the Ping command. Type ping *hostname* or ping *IP address*.**
   A hostname is typically a website address. Replace *hostname* with the website that or server that you want to ping. For example, to ping wikiHow's main web server, type ping www.wikihow.com.

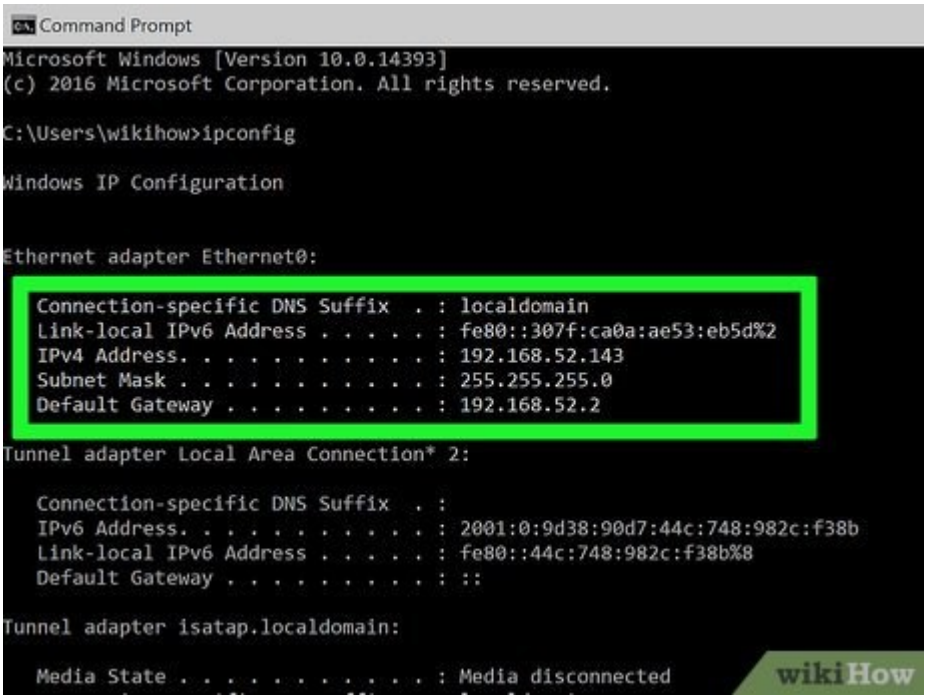
An IP address is a computer's location on a network, either locally or on the internet. If you know the IP address that you want to ping, replace *IP address* with it.[2] For example, to ping the IP address 192.168.1.1, type ping 192.168.1.1.
To have your PC ping itself, type ping 127.0.0.1.



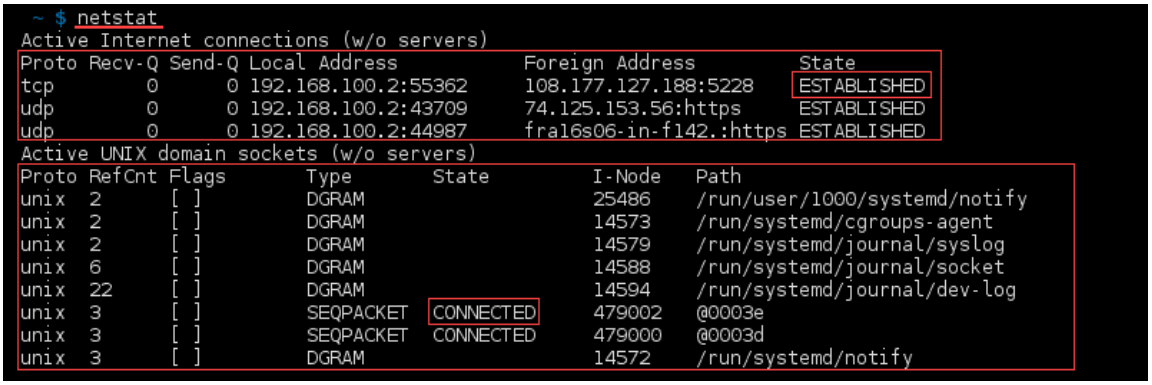
Tracert: Free command-line utility that lists the probable hops to a network or internet destination address.



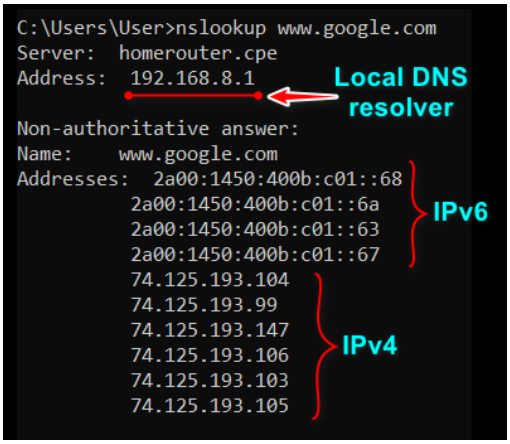
Ipconfig: This command-line tool reports the IPv4 and IPv6 addresses, subnets, and default gateways for all network adapters on a PC.



Netstat: This tool displays active connections on your computer.



Nslookup: Available for Windows, Unix, Linux, and Mac OS, this tool gives you DNS server diagnostics.



ARP: The ARP (address resolution protocol) is used by Network nodes to map network address to the MAC address. This is a useful tool to diagnose Network communication.

You can use ARP command in MSDOS to view the ARP cache in a windows network. Using ARP standalone will show all the available switches.

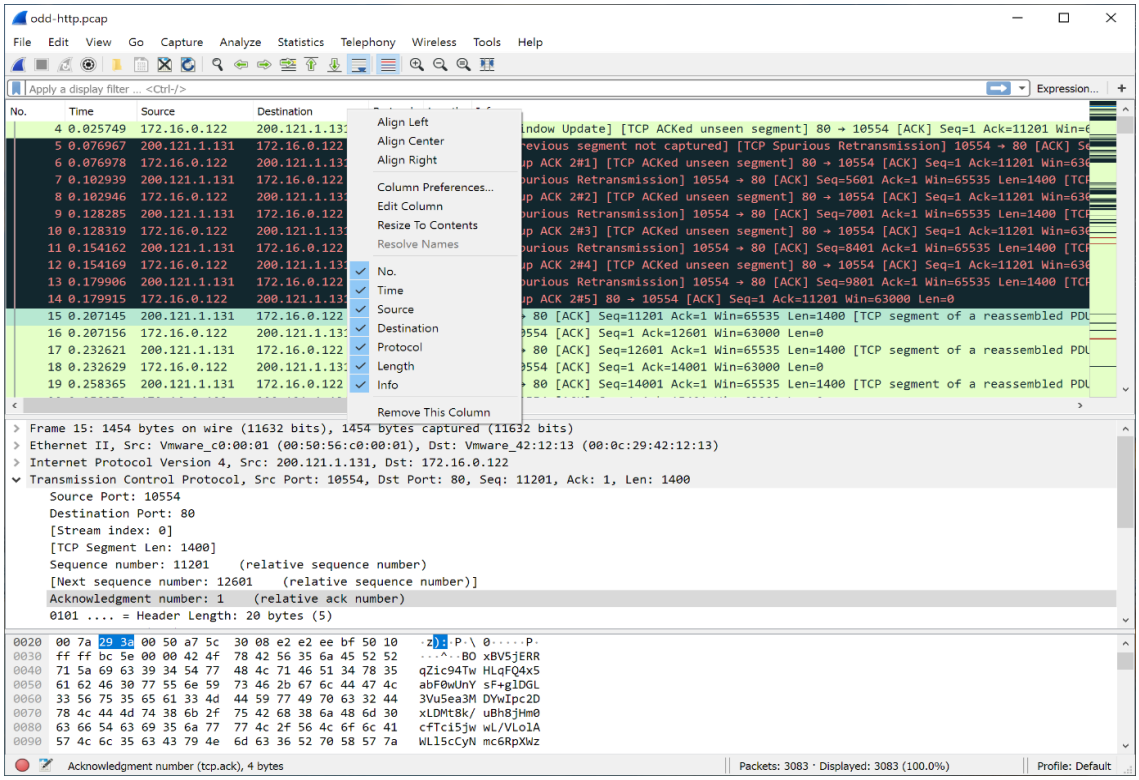
```
C:\Users\dawgotra>arp -a

Interface: 192.168.1.6 --- 0x7
  Internet Address      Physical Address      Type
  192.168.1.1           b8-c1-a2-4d-ec-e4     dynamic
  192.168.1.2           b0-48-7a-99-8f-06     dynamic
  192.168.1.25          94-0c-6d-be-1d-91     dynamic
  192.168.1.145         c4-2f-90-ac-24-36     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Netsh: With netsh, you can not only view but also change the network configuration of both local and remote hosts. You can use netsh as a command in command prompt and also run it as a batch file to modify the network configurations of remote systems. Once you use netsh command and press enter, you need to input the relevant context before using the netsh command.

```
C:\Users\dawgotra>netsh
netsh>/?

The following commands are available:

Commands in this context:
..              - Goes up one context level.
?               - Displays a list of commands.
abort           - Discards changes made while in offline mode.
add             - Adds a configuration entry to a list of entries.
advfirewall     - Changes to the `netsh advfirewall' context.
alias           - Adds an alias.
branchcache     - Changes to the `netsh branchcache' context.
bridge          - Changes to the `netsh bridge' context.
bye             - Exits the program.
commit          - Commits changes made while in offline mode.
delete          - Deletes a configuration entry from a list of entries.
dhcpclient      - Changes to the `netsh dhcpclient' context.
dnsclient       - Changes to the `netsh dnsclient' context.
dump            - Displays a configuration script.
```

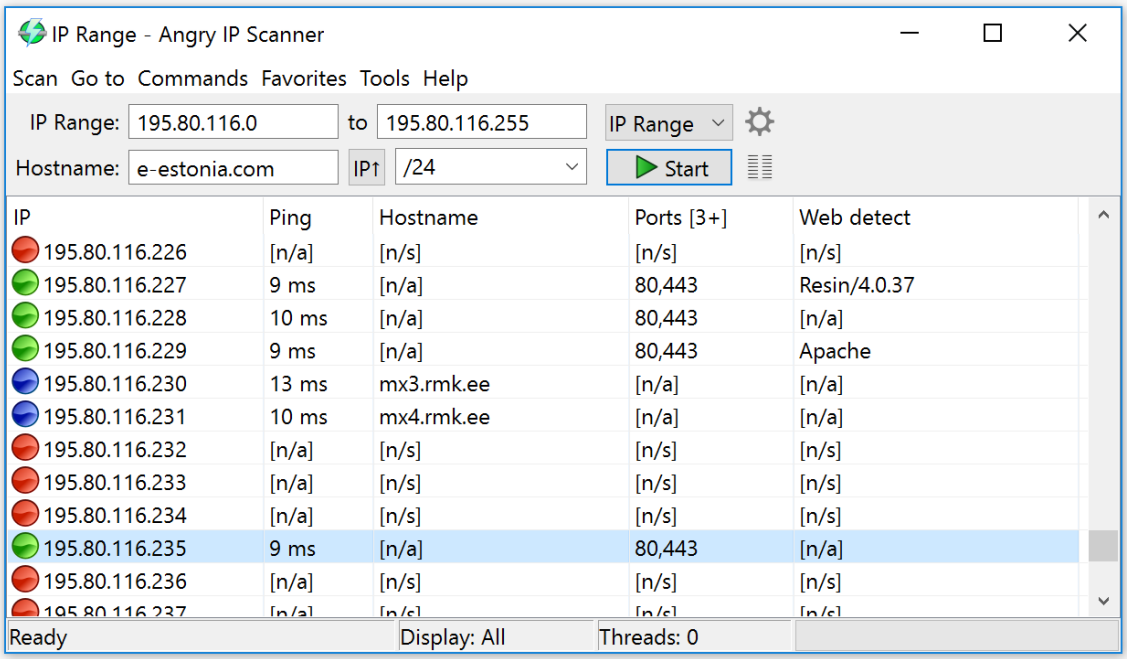
Network Analyzers:

Wireshark (free, open-source): A powerful tool that captures and analyzes network traffic, allowing you to see exactly what data is flowing across your network.



Network Scanners:

Angry IP Scanner (free, open-source): Quickly scans a network to identify active devices and gather information about them (IP address, operating system, etc.)

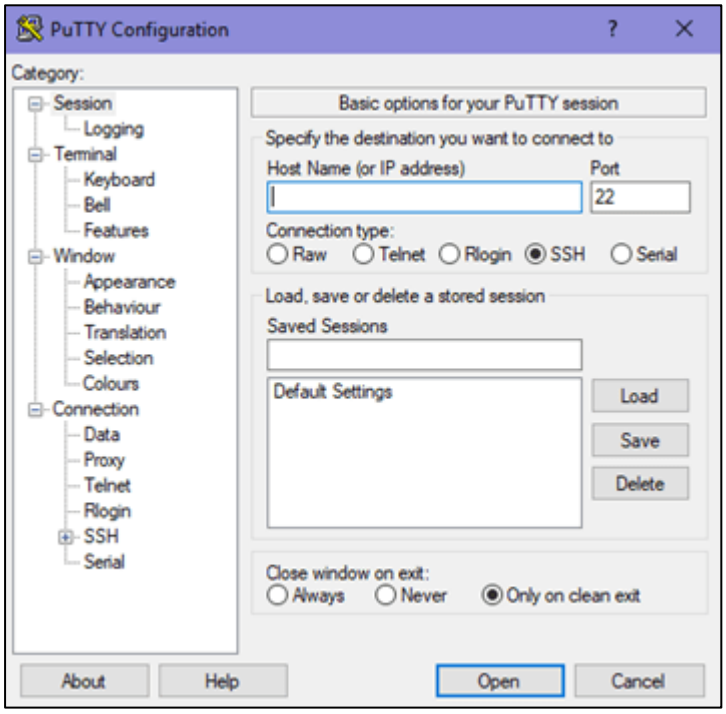


Network Configuration Tools:

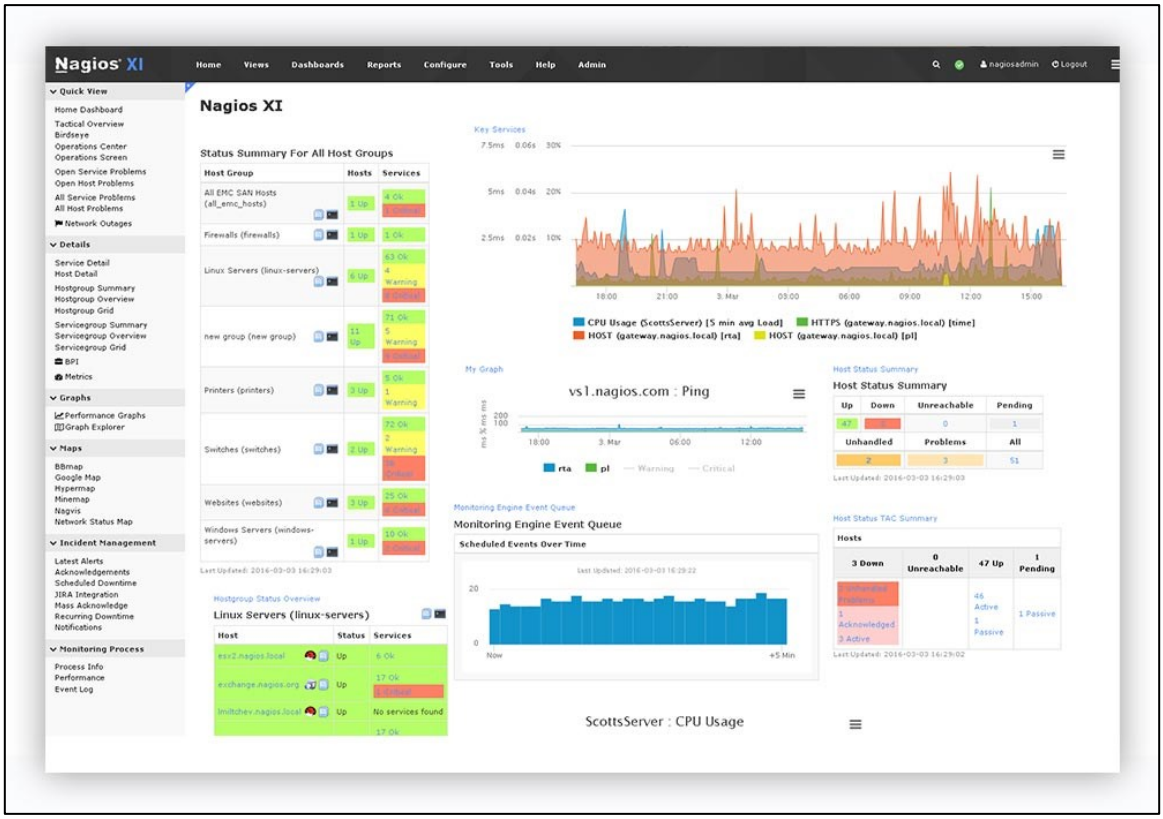
Netstat (command-line): Provides detailed information about network connections, routing tables, and other network protocol statistics.

```
C:\Windows\system32>
C:\Windows\system32>netstat -aon

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING       4704
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       880
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       1144
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       4584
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       660
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       520
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       708
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       1952
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       652
  TCP    192.168.122.176:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.122.176:49679  52.139.250.253:443     ESTABLISHED     432
  TCP    192.168.122.176:49719  52.139.250.253:443     ESTABLISHED     4992
```

Putty (free, open-source): Securely connects to and configures network devices with a command-line interface.



Advanced Monitoring Tools:
Nagios (open-source): A popular tool for monitoring network performance, uptime, and resource utilization.

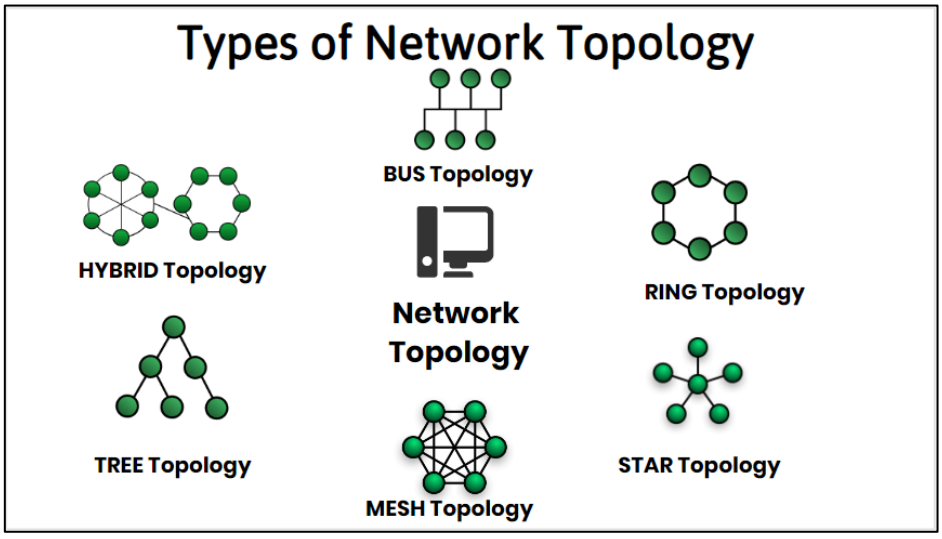


1.3 Reviewing network design, support, and maintenance documents

Reviewing network design, support, and maintenance documents is a crucial step in understanding, maintaining, and troubleshooting your network. These documents serve as a blueprint for your network's functionality and provide vital information for keeping it running smoothly. Here's what to focus on when reviewing these documents:

Network Design Documents:

Network Topology: This section should illustrate the physical layout of your network, including how devices are connected (e.g., star, mesh, bus).

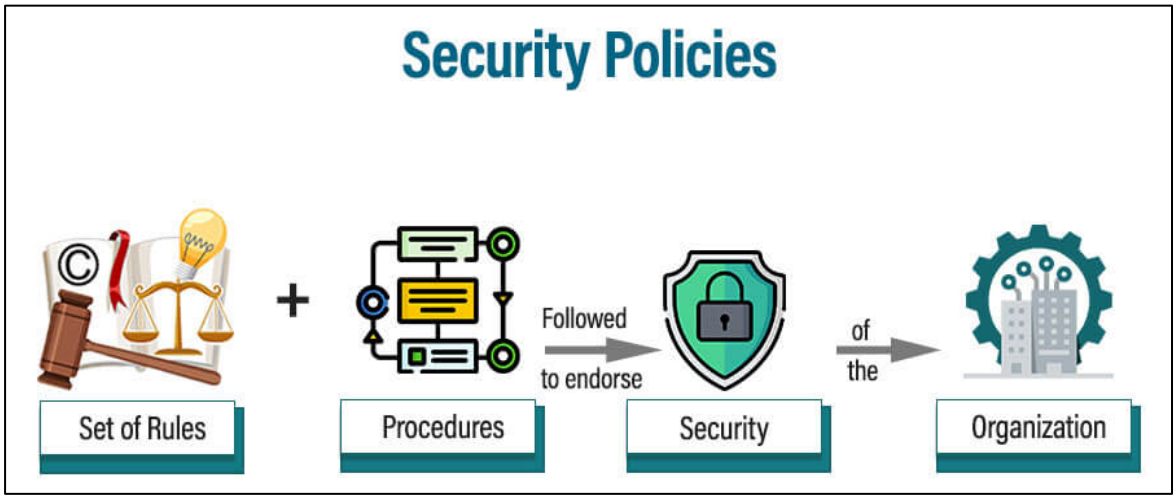


Hardware and Software Inventory: This should list all network devices (routers, switches, firewalls, etc.) with their models, specifications, and locations. Any network software applications should also be documented here.

IP Addressing Scheme: This section defines how IP addresses are assigned to devices on your network. It should include the subnet mask, default gateway, and any VLAN configurations.

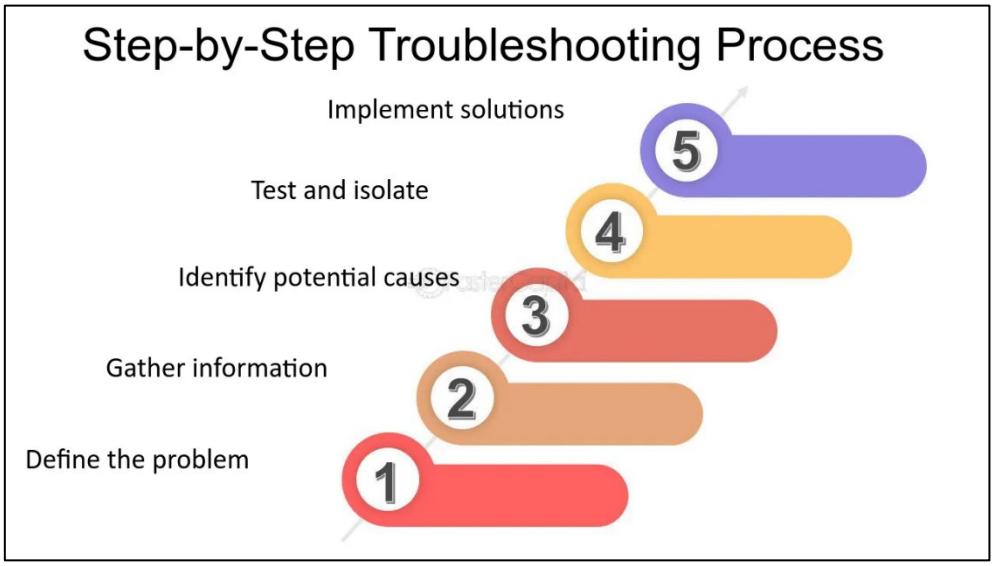
Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	172.17.10.1	255.255.255.0	N/A
S2	VLAN 1	172.17.10.2	255.255.255.0	N/A
S3	VLAN 1	172.17.10.3	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.254
PC2	NIC	172.17.10.22	255.255.255.0	172.17.10.254
PC3	NIC	172.17.10.23	255.255.255.0	172.17.10.254
PC4	NIC	172.17.10.27	255.255.255.0	172.17.10.254

Security Policies: This section should outline any security measures in place, such as firewalls, access control lists (ACLs), and encryption protocols.

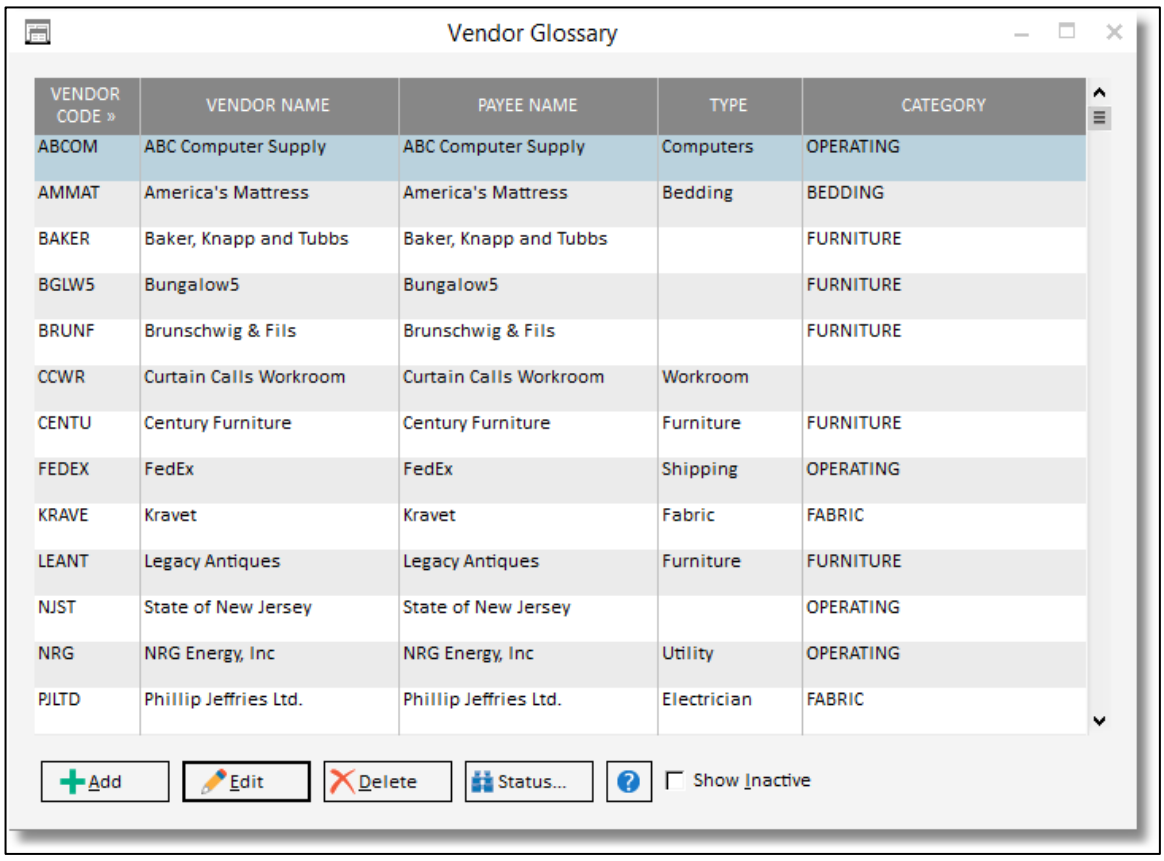


Network Support Documents:

Troubleshooting Procedures: These documents detail step-by-step guides for resolving common network issues like connectivity problems, slow performance, or security breaches.



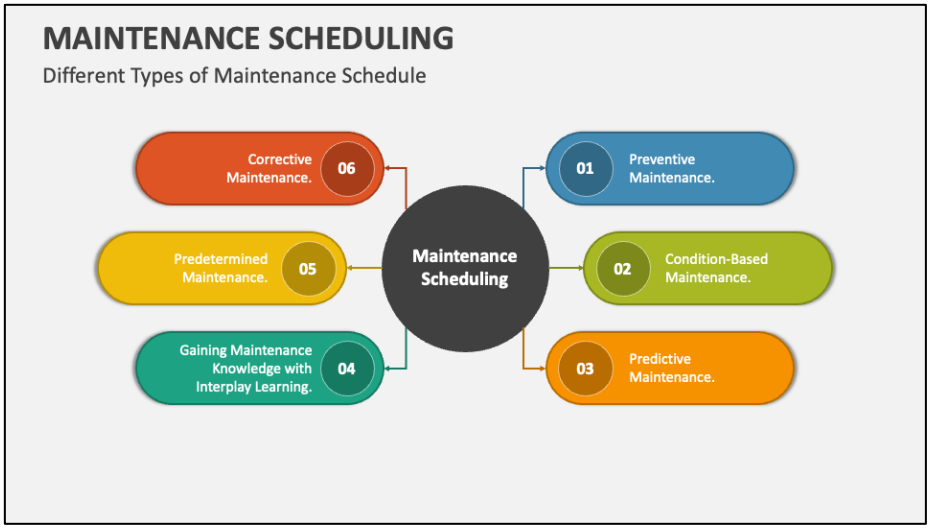
Vendor Manuals: These are the official manuals from the manufacturers of your network devices and provide detailed information on their configuration and troubleshooting.



Network Maintenance Documents:

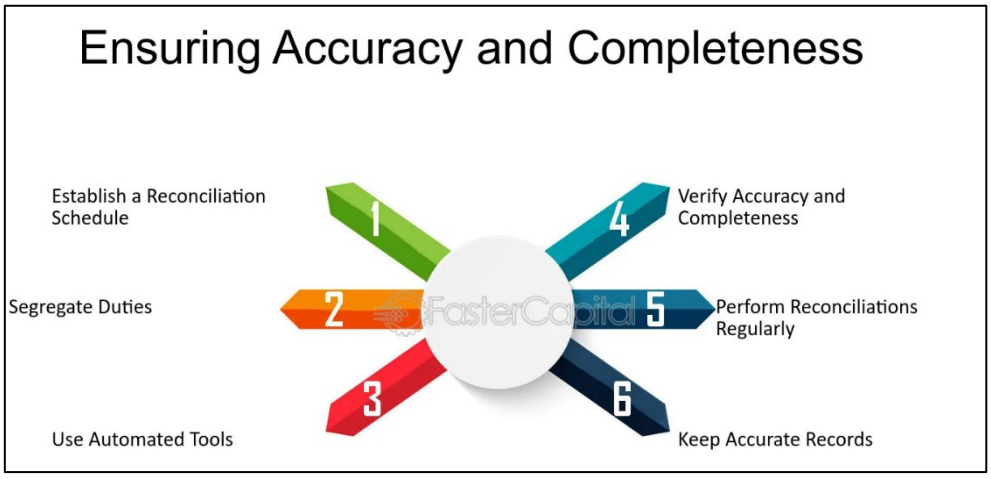
Maintenance Schedules: This section outlines a schedule for routine maintenance tasks like software updates, firmware upgrades, and physical cleaning of devices.

Backup and Recovery Procedures: These documents explain how network configurations and data are backed up and how to restore them in case of failure.

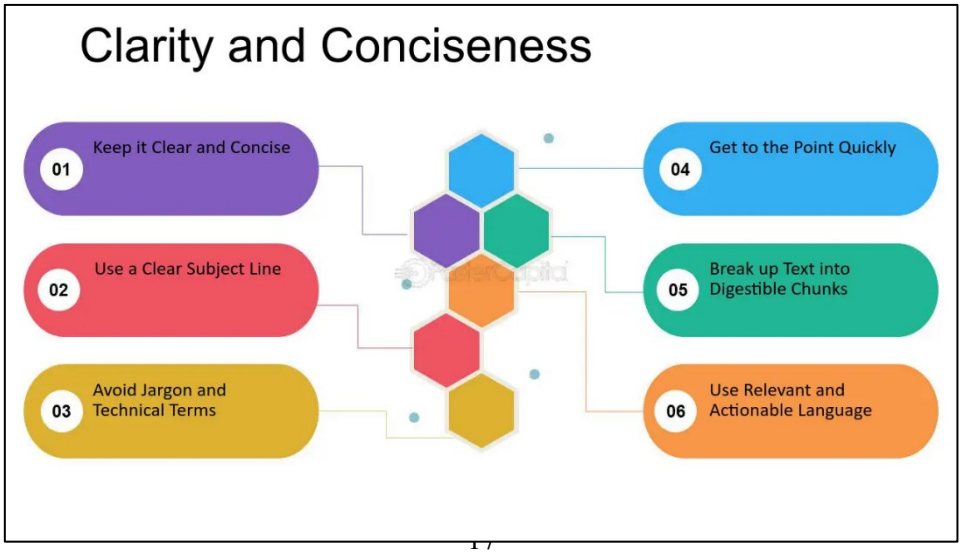


Review Process:

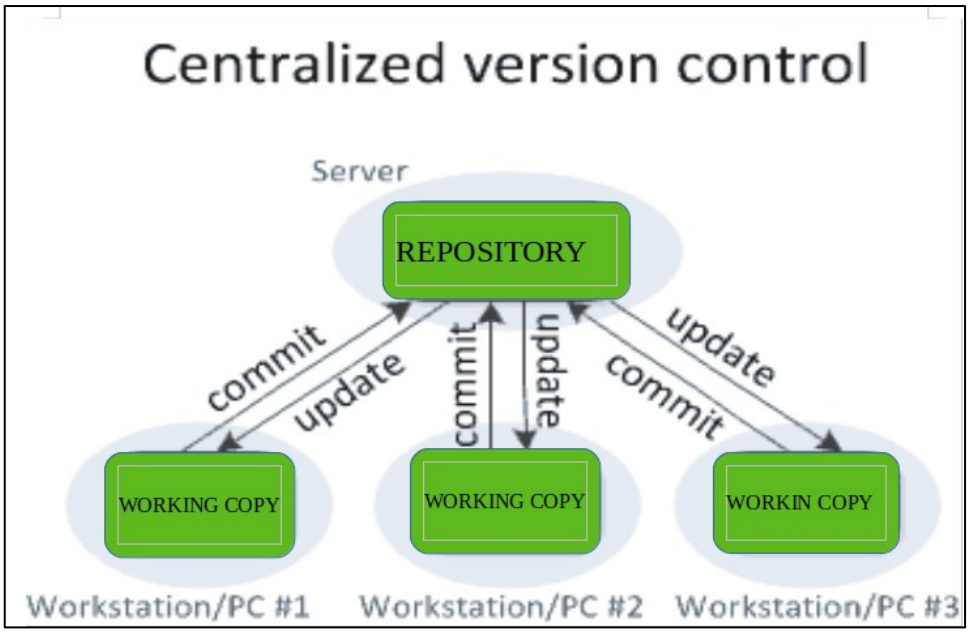
Accuracy and Completeness: Ensure the documents accurately reflect your current network configuration.



Clarity and Organization: The information should be well-organized, easy to understand, and use consistent terminology.



Version Control: There should be a system in place to track document versions and ensure everyone is working with the latest information.



Accessibility: The documents should be readily available to authorized personnel who need to troubleshoot or maintain the network.

1.4 Reviewing computer manuals and maintenance documents

Reviewing computer manuals and maintenance documents is essential for anyone who wants to keep their computer running smoothly and troubleshoot problems effectively. These documents provide valuable information about the hardware, software, and recommended maintenance practices for your specific system. Here's a breakdown of what to focus on when reviewing these documents:

User Manuals:

Hardware Specifications: This section details the technical specifications of your computer components like processor, RAM, storage capacity, and graphics card. Understanding these specs can help you determine if your computer meets the requirements for running specific software or troubleshoot performance issues.

Software Installation and Configuration: The manual may provide instructions on installing and configuring the operating system and pre-installed software. This can be helpful if you need to reinstall the operating system or troubleshoot software-related problems.

Troubleshooting Guides: The user manual may include basic troubleshooting steps for common issues like startup problems, device connection errors, or software crashes.

Maintenance Documents:
Cleaning Procedures: These sections provide instructions on how to safely clean your computer's internal components like dust filters and fans to prevent overheating and ensure proper airflow.

Hardware Upgrades: Some manuals may include information on compatible upgrade options for memory, storage, or graphics cards. This can be helpful if you're looking to improve your computer's performance.

Backup and Recovery: The documents may explain how to back up important data and restore it in case of system failure or accidental data loss.
General Tips for Reviewing Manuals:

Identify Your Specific Model: Ensure you're referring to the manual for your exact computer model, as specifications and features can vary. Many manufacturers provide downloadable manuals on their websites.

Focus on Relevant Sections: Prioritize sections related to your current task (troubleshooting, maintenance, upgrades). Most manuals are quite comprehensive, so skimming through irrelevant sections might save you time.

Look for Visual Aids: Pay attention to diagrams and illustrations that can help you visualize hardware components or understand installation procedures.

Search Functionality: Many manuals offer a search function to quickly locate specific keywords or topics.

Additional Resources:
Manufacturer Websites: Most computer manufacturers provide support pages on their websites with downloadable manuals, knowledge base articles, and community forums where you can find solutions to common problems.

Online Tech Communities: There are many online communities dedicated to troubleshooting computer problems. You can search for specific issues you're facing and find solutions or advice from other users and tech experts.

When it comes to identifying network or computer problems, consulting the appropriate person depends on the nature of the issue, your technical expertise, and the resources available within your organization. Here's a breakdown to help you decide who to consult:

For basic troubleshooting:
Yourself: If you're comfortable with basic troubleshooting steps, you can often resolve minor issues yourself. Many operating systems have built-in diagnostic tools, and online

resources offer solutions for common problems. Refer to the user manuals and troubleshooting guides mentioned previously.

Colleagues: If you're stuck, seek help from colleagues who might have experience with similar problems. This can be a good option for issues related to specific software or network configurations within your department.

For more complex issues:
IT Help Desk: Many organizations have an internal IT help desk staffed with technicians who can assist with common computer and network problems. They can provide initial troubleshooting guidance, diagnose issues remotely, and escalate complex problems to the appropriate team.

Network Administrator/Network Engineer: For network-specific problems like connectivity issues, slow performance, or security concerns, consulting the network administrator or network engineer is ideal. They have in-depth knowledge of your network infrastructure and the expertise to diagnose and resolve complex network problems.

System Administrator/IT Specialist: For issues related to specific software, hardware malfunctions, or system configuration, consulting a system administrator or IT specialist is recommended. They can diagnose software problems, perform hardware diagnostics, and implement solutions like software.

A plan of action is a detailed roadmap that outlines the steps you need to take to achieve a specific goal. It breaks down complex tasks into manageable chunks and ensures you have a clear direction to follow. Here's a breakdown of the key elements of a good plan of action:

1. Define Your Goal:
What do you want to achieve? Be clear and specific about your desired outcome.
For example, your goal could be to "troubleshoot and resolve a network connectivity issue" or "develop and implement a Competency Based Learning program on network troubleshooting."

2. Break Down the Goal into Steps:
Identify the key tasks or activities required to reach your goal.
List these steps in a logical sequence, considering any dependencies between them (e.g., you can't troubleshoot an issue until you understand its symptoms).

3. Assign Resources:
What resources will you need to complete each step?
This could include people (with specific skills), equipment, materials, or budget.

4. Set Timelines
Establish a timeframe for each step or for the entire plan.
Be realistic about the time needed for each task and consider potential delays.

5. Identify Potential Challenges
What obstacles or roadblocks could you encounter along the way?
Anticipate these challenges and brainstorm potential solutions or mitigation strategies.

6. Establish Monitoring and Evaluation
How will you track your progress?
Define key milestones or metrics to measure your success and identify areas that might need adjustments.

7. Communication Plan (Optional)
If you're working with a team, establish a communication plan to keep everyone informed about progress, challenges, and any changes to the plan.

Benefits of a Plan of Action
Clarity and Focus: A plan keeps you focused on your goal and helps avoid distractions.
Improved Efficiency: By breaking down tasks, you can identify the most efficient way to achieve your objective.

Better Resource Allocation: A plan ensures you have the right resources allocated to the right tasks at the right time.

Increased Accountability: Setting deadlines and milestones fosters accountability and motivates progress.

Adaptability: Plans can be flexible. If you encounter challenges, you can adjust the plan as needed.

Self-Check-1: Interpret Methodology and Plan

1. What is a core principle of network troubleshooting methodology?

   Answer

2. What does a network ping tool help diagnose?

   Answer

3. What information might you find in a network design document?

   Answer

4. Why is it important to review computer maintenance documents?

   Answer

5. Who should you consult first for basic computer troubleshooting?

   Answer

6. What should you include when explaining a network problem to a technician?

   Answer

7. What is the benefit of breaking down a troubleshooting plan into steps?

   Answer

8. What does assign resources to a plan of action involve?

   Answer

9. Why is it important to consider potential challenges in your plan?

   Answer

10. How does a plan of action promote better resource allocation?

    Answer

Answer Key-1: Interpret Methodology and Plan

1. What is a core principle of network troubleshooting methodology?
   Answer: Following a systematic approach to identify the root cause of a network issue.

2. What does a network ping tool help diagnose?
   Answer: Basic connectivity problems by sending and receiving data packets.

3. What information might you find in a network design document?
   Answer: The physical layout of your network, including how devices are connected.

4. Why is it important to review computer maintenance documents?
   Answer: To learn proper cleaning procedures and identify compatible upgrade options.

5. Who should you consult first for basic computer troubleshooting?
   Answer: You can often resolve minor issues yourself or seek help from colleagues.

6. What should you include when explaining a network problem to a technician?
   Answer: Specific symptoms, when the problem started, and any troubleshooting steps taken.

7. What is the benefit of breaking down a troubleshooting plan into steps?
   Answer: Improves efficiency and ensures a logical approach to resolving the issue.

8. What does assigning resources to a plan of action involve?
   Answer: Identifying people with specific skills, equipment, or budget needed for each step.

9. Why is it important to consider potential challenges in your plan?
   Answer: To anticipate obstacles and brainstorm solutions for a smoother troubleshooting process.

10. How does a plan of action promote better resource allocation?
    Answer: By ensuring the right resources are allocated to the right tasks at the right time.

Activity Sheet 1: Troubleshoot Methodology and Plan

Write Down some step Troubleshoot Methodology and Plan

Troubleshoot	Methodology and Plan

Learning Outcome-2: Identify The Problem

Assessment Criteria:

1. Network Fault is identified
2. Faulty hardware or software component are detected.
3. The problem scenarios are observed
4. Problems are detected using diagnostic tools

Content:

1. Network Fault
    - Wired Network
        - Cabling
        - PatchPanel
        - Fiber Optics
        - Vlan misconfiguration
    - Wireless Network fault
        - Coverage issues
        - Communication issue
        - Capacity
        - Overlap
        - Attenuation
    - Bandwidth issues
    - DNS issues
    - Malfunctioning devices
    - DHCP issue
    - IP configuration issue
    - Routing issues
2. Faulty hardware or software component.
3. The problem scenarios
4. Diagnostic tools

Resources Required/ Conditions:

The trainees must be provided with the following:

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

Methodologies

1. Lecture/discussion
2. Demonstration/application
3. Presentation
4. Blended delivery methods

Assessment Methods

1. Written test
2. Demonstration
3. Observation with checklist
4. Oral questioning
5. Portfolio

Learning Experience-2: Identify The Problem

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

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

Information Sheet-2: Identify The Problem

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

2.1 Identify Network Fault
2.2 Detect Faulty hardware or software component.
2.3 Observe The problem scenarios
2.4 Detect Problems using diagnostic tools

2.1 Network Fault

A network fault refers to any event or condition that disrupts the normal operation of a computer network. This can manifest in various ways, impacting network performance, connectivity, or both.

Types of Network Faults:

Hardware Faults: These are physical malfunctions of network devices like routers, switches, cables, or network interface cards (NICs) in computers. Faulty hardware can cause complete loss of connectivity, slow performance, or data errors.

Software Faults: Bugs or glitches in network operating systems, device firmware, or security software can lead to network issues. These might include routing problems, configuration errors, or security breaches.

Environmental Faults: Extreme temperatures, power surges, or physical damage to cables due to construction or pests can disrupt network functionality.

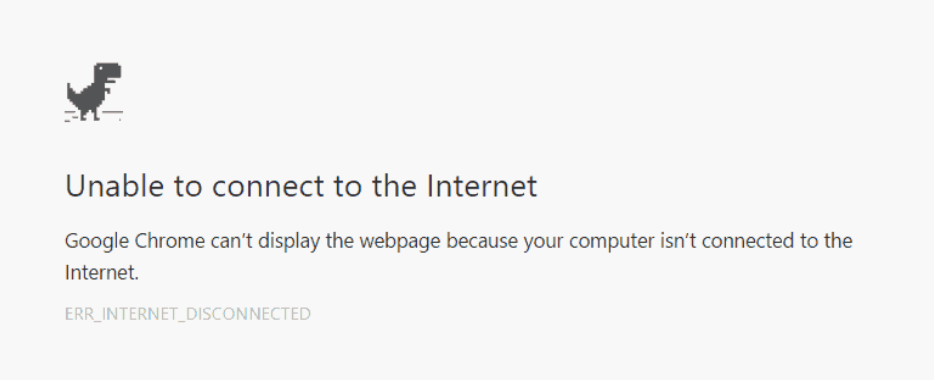
Signs of a Network Fault:

Loss of connectivity: Devices are unable to connect to the network or the internet.

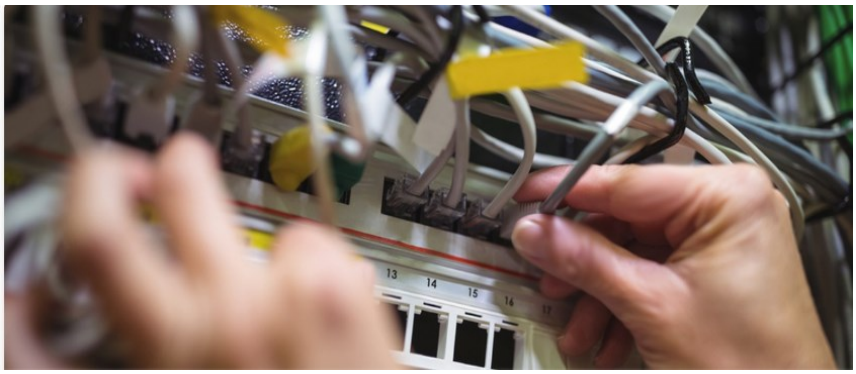
Slow network performance: Experiencing sluggish loading times, delays in data transfer, or lagging applications.

Intermittent connectivity: Connections dropping frequently or devices having difficulty staying online.

Error messages: Network diagnostic tools or operating systems might display error messages indicating specific issues.



Troubleshooting Network Faults:



Systematic approach: Follow a network troubleshooting methodology to isolate the root cause of the problem. This typically involves gathering information, testing potential causes, and implementing solutions.

Network tools and utilities: Utilize tools like ping, tracert, and network scanners to diagnose connectivity issues, identify faulty devices, or monitor network performance.

Impact of Network Faults:
Reduced productivity: Network downtime or slow performance can significantly hinder workflow and employee productivity.

Data loss: Network faults can lead to data loss if proper backups are not in place.

Security risks: Certain network faults can create security vulnerabilities, making your network susceptible to cyberattacks.

Prevention of Network Faults:

Regular maintenance: Perform routine maintenance tasks like updating firmware, patching software vulnerabilities, and keeping network devices clean.

Monitoring and diagnostics: Proactively monitor network performance and utilize diagnostic tools to identify potential problems before they escalate.

Backups and redundancy: Implement a backup plan to safeguard data and consider redundant network components to minimize downtime in case of failures.

Wired Network

Cabling fault

A cabling fault refers to any malfunction or imperfection in a network cable that hinders its ability to transmit data signals properly. These faults can cause a variety of network issues, ranging from complete loss of connectivity to slow performance and data errors.

Some common cabling faults:

Physical Damage: Cuts, crimps, or excessive bends in the cable can disrupt signal transmission. This can be caused by improper installation, stepping on cables, or furniture pressing against them.

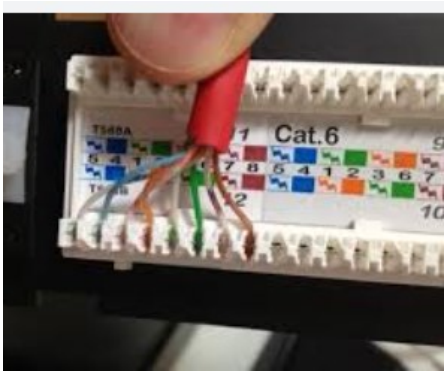
Termination Issues: Problems with the connectors on either end of the cable, such as loose pins, faulty crimping, or damaged RJ-45 jacks, can prevent a proper connection.

Cable Quality: Using low-quality cables that don't meet industry standards (like Cat5e or Cat6) can lead to signal degradation, especially over longer distances.

Incorrect Cable Type: Using the wrong cable type for the network application can cause compatibility issues. For example, using a phone cable instead of a dedicated network cable won't support the necessary data transfer speeds.

Crosstalk: Electrical interference between adjacent cables can corrupt data signals. This can occur when cables are bundled too tightly together or run parallel to power cables**ch Panel Faults**

A patch panel is a hardware component in a network rack that serves as an organized connection point between network cables and network devices like switches or routers. Faults in a patch panel can also lead to network connectivity problems.



Some common patch panel faults:

Loose Connections: Cables not securely plugged into the patch panel ports can cause intermittent connectivity or complete loss of connection.

Incorrect Patching: Patching cables incorrectly between the patch panel and network devices can disrupt communication paths. This is why proper labeling of both patch panel ports and device ports is crucial.

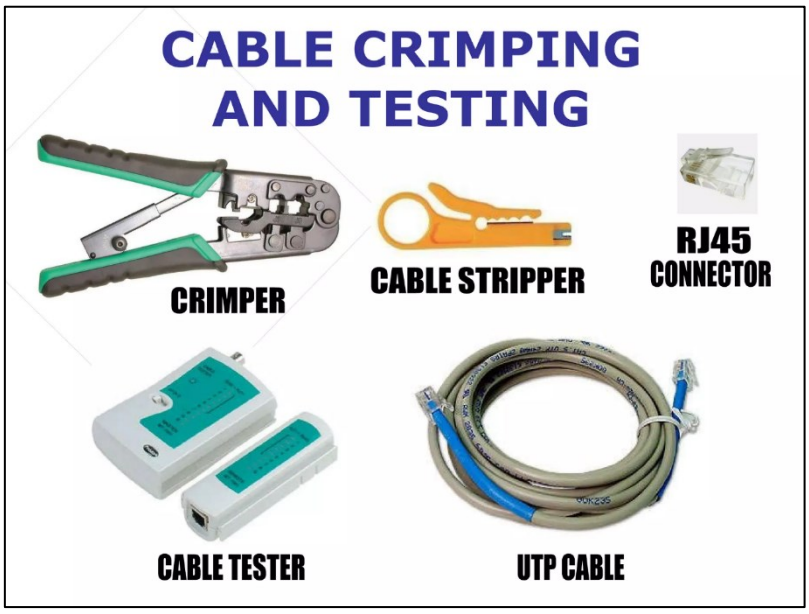
Damaged Patch Panel Ports: Physical damage to the RJ-45 jacks on the patch panel itself, like bent pins or faulty internal components, can prevent a proper connection with the network cable.

Dust and Debris: Accumulation of dust or debris inside the patch panel can interfere with cable connections.

Troubleshooting Cabling and Patch Panel Faults

Visual Inspection: Start by visually inspecting cables for any physical damage, loose connections, or improper labeling. Also, check for dust buildup within the patch panel.

Cable Testing Tools: Utilize cable testers to diagnose faults like continuity issues, shorts, or opens in the cable.



Port Testing: Some network switches can perform diagnostic tests on individual ports to identify faulty connections.

Process of Elimination: Systematically test and replace cables or patch panel ports to isolate the problematic component.

Fiber Optics

Fiber optics is a technology that uses light pulses transmitted through thin glass or plastic fibers to transmit data over long distances. Compared to traditional copper cables, fiber optic cables offer several advantages:

Higher Bandwidth: Fiber optics can transmit significantly more data at faster speeds compared to copper cables.

Lower Signal Loss: Light signals experience minimal degradation over long distances, making fiber optics ideal for high-bandwidth applications.

Immunity to Interference: Fiber optic cables are not susceptible to electromagnetic interference (EMI) which can disrupt data signals in copper cables.

Security: It's more difficult to intercept data transmitted through fiber optic cables compared to copper due to the nature of light transmission.

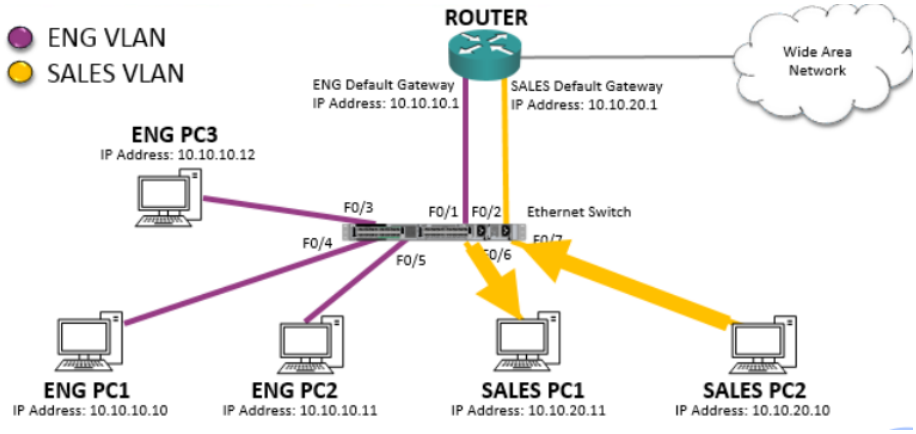
Here's a breakdown of the key components in a fiber optic network:

Fiber Optic Cable: The core component, made of glass or plastic fibers that transmit light pulses.

Transceivers: These devices convert electrical signals from network devices to light pulses for transmission over the fiber optic cable and vice versa on the receiving end.

Repeaters: Used to amplify the light signal over long distances to maintain signal strength.

VLAN Misconfiguration



A Virtual Local Area Network (VLAN) is a logical grouping of network devices within a physical network. VLANs segment the network into smaller broadcast domains, improving security, performance, and manageability.

Common VLAN misconfigurations can lead to network connectivity issues and security vulnerabilities:

Incorrect Port Assignment: Assigning devices to the wrong VLAN can prevent them from communicating with other devices on the intended network segment.

Untagged Ports: Leaving switch ports untagged can allow unauthorized devices to access other VLANs.

Security Misconfiguration: Not properly configuring security policies on VLANs can create security gaps and expose sensitive data to unauthorized access.

Broadcast Storms: Misconfigured VLANs can lead to broadcast storms, where a single broadcast message gets flooded across the entire network, overwhelming devices and causing performance degradation.

Troubleshooting Fiber Optic and VLAN Issues

Fiber Optic Issues:

Visual Inspection: Check for physical damage to the fiber optic cable, like cracks or bends. Tools like fiber optic scopes can help examine internal fiber integrity.

Light Power Meter: Measure the light power levels at both ends of the cable to identify signal attenuation.

Fiber Tester: Utilize specialized fiber optic testers to diagnose faults like breaks, high attenuation, or connector problems.

VLAN Issues:

Verify Port Configuration: Ensure devices are assigned to the correct VLAN on the switch ports they are connected to.

Check for Untagged Ports: Identify and properly configure any untagged switch ports to prevent unauthorized access.

Review Security Policies: Verify that security policies are correctly implemented on each VLAN to control traffic flow and access permissions.

Network Monitoring Tools: Utilize network monitoring tools to identify unusual traffic patterns or broadcast storms that might indicate VLAN misconfiguration.

Wireless network faults

Wireless network faults encompass a variety of issues that can disrupt the performance or connectivity of your Wi-Fi network. These faults can be frustrating for users and can significantly impact productivity or entertainment activities.

Some common wireless network faults and troubleshooting techniques:

Types of Wireless Network Faults:

Signal Strength Issues: Weak signal strength can cause slow connection speeds, dropped connections, or limited network range. This can be caused by factors like distance from the router, physical obstructions, interference from other devices, or using an outdated Wi-Fi standard (802.11b/g).

Router or Access Point Malfunctions: Hardware issues with the router or access point itself, such as overheating or outdated firmware, can lead to connectivity problems or erratic performance.

Wireless Security Issues: Incorrectly configured security settings or outdated encryption protocols can make your network vulnerable to unauthorized access and potential security breaches.

Channel Overlap: Multiple Wi-Fi networks in close proximity operating on the same channel can cause interference and slow down overall performance.

Device Driver Issues: Outdated or incompatible network drivers on your Wi-Fi adapter can lead to connectivity problems or limited functionality.

Troubleshooting Wireless Network Faults:

Signal Strength Check: Use built-in Wi-Fi signal strength indicators on your devices or dedicated Wi-Fi analyzer apps to identify areas with weak signal. Try relocating your router or access point to a more central location and away from obstructions.

Restart Devices: A simple reboot of your router or access point and your Wi-Fi enabled devices can often resolve minor glitches and improve performance.

Verify Security Settings: Ensure you're using a strong WPA2 encryption protocol and a complex password for your Wi-Fi network. Avoid using outdated protocols like WEP.

Change Wi-Fi Channel: Use a Wi-Fi scanner app to identify less congested channels and adjust your router's channel settings accordingly to minimize interference.

Update Device Drivers: Check for and install the latest updates for your Wi-Fi adapter drivers on your computer or other devices.

Advanced Troubleshooting: For more complex issues, consider tools like Wireshark to analyze network traffic and identify potential sources of interference. Firmware updates for your router might also be available to address bugs or improve performance.

These three terms - Coverage Issues, Communication Issues, and Capacity - represent different aspects of a wireless network fault. Here's a breakdown of each:

1. Coverage Issues:

This refers to problems with the signal strength and range of your Wi-Fi network. When experiencing coverage issues, you might encounter:

Limited Network Reach: Certain areas within your home or office might have weak or no Wi-Fi signal, making it difficult to connect devices or maintain a stable connection.

Dead Zones: Specific locations might have no Wi-Fi signal at all, preventing any devices from connecting in those areas.

Slow Speeds in Certain Areas: Even if devices can connect in some areas, the signal strength might be weak, leading to slow internet speeds and buffering issues.

Causes of Coverage Issues:

Router Placement: The location of your router significantly impacts signal strength. Placing it in a corner or surrounded by thick walls can weaken the signal.

Physical Obstructions: Walls, furniture, and even metal objects can absorb or weaken the Wi-Fi signal, creating coverage gaps.

Large Homes or Buildings: For larger spaces, a single router might not be enough to provide adequate coverage throughout.

Interference: Other electronic devices operating on the same frequency can interfere with your Wi-Fi signal, causing signal degradation.

2. Communication Issues:

This refers to problems establishing or maintaining a connection between your devices and the Wi-Fi network. Communication issues can manifest as:

Difficulty Connecting: Devices might have trouble connecting to the Wi-Fi network initially, requiring multiple attempts or manual configuration.

Frequent Disconnections: Devices might connect successfully but drop the connection repeatedly, causing disruptions and frustration.

Slow Data Transfer Speeds: Even with a seemingly stable connection, data transfer speeds might be slower than expected, impacting downloads, uploads, and streaming activities.

Causes of Communication Issues:

Incorrect Login Credentials: Typos or errors in entering the Wi-Fi password can prevent devices from connecting.

Outdated Router Firmware: Outdated firmware on your router might have bugs that lead to connection problems.

Device Driver Issues: Outdated or incompatible network drivers on your Wi-Fi adapter can cause communication issues.

Wireless Security Issues: Incorrectly configured security settings or incompatible encryption protocols might hinder communication.

Hardware Malfunctions: Faulty hardware in your router or Wi-Fi adapter on your device can lead to connection problems.

3. Capacity:

This refers to the overall ability of your Wi-Fi network to handle the number of connected devices and the amount of data traffic they generate. Capacity issues arise when:

Too Many Devices: A large number of devices connected to the network (laptops, phones, smart home devices, etc.) can overload its capacity, leading to slow speeds and dropped connections for everyone.

Bandwidth-intensive Activities: Activities like streaming high-definition videos, online gaming, or large file downloads require significant bandwidth and can strain the network's capacity, impacting overall performance for other devices.

Limited Bandwidth Plan: If you have a limited internet bandwidth plan from your service provider, exceeding the data cap can lead to throttling or slower speeds for all devices on your network.

Resolving these Network Faults:

By understanding the specific issue you're facing (coverage, communication, or capacity), you can implement targeted solutions:

For Coverage Issues: Reposition your router, consider a mesh Wi-Fi system for larger spaces, or use Wi-Fi range extenders.

For Communication Issues: Verify login credentials, update router firmware and device drivers, check security settings, or troubleshoot hardware malfunctions.

For Capacity Issues: Limit the number of connected devices, prioritize bandwidth-intensive activities, or upgrade your internet plan for more bandwidth.

Overlap:

This refers to the phenomenon where multiple Wi-Fi networks operating on the same channel interfere with each other. Imagine multiple radio stations trying to broadcast on the same frequency – the signals get muddled, and it becomes difficult to clearly hear any one station. Here's how overlap affects your Wi-Fi:

Signal Interference: When multiple Wi-Fi networks on the same channel are in close proximity, their signals can overlap and interfere with each other. This can lead to:

Slower Speeds: The overlapping signals can disrupt data transmission, resulting in slower internet browsing, downloads, and uploads.

Increased Latency: Latency refers to the time it takes for data to travel between devices. Overlap can increase latency, causing delays and lag in online gaming, video conferencing, or real-time applications.

Dropped Connections: Severe overlap might lead to complete disconnections from the Wi-Fi network as devices struggle to maintain a stable signal.

2. Attenuation:

This refers to the weakening of the Wi-Fi signal as it travels through the air. Similar to how a flashlight beam gets dimmer the further it travels, Wi-Fi signals lose strength with distance. Here's how attenuation impacts your network:

Reduced Range: As the signal weakens with distance from the router, the effective range of your Wi-Fi network decreases. This can create areas with weak or no signal, limiting your network's reach.

Slower Speeds at the Fringes: Even if devices can connect in areas further away from the router, the weakened signal can lead to slower internet speeds compared to locations closer to the access point.

Connection Issues: Extremely weak signals due to high attenuation can make it difficult for devices to connect or maintain a stable connection to the network.

Overlap vs. Attenuation:

Overlap is an external factor: It's caused by the presence of other Wi-Fi networks in the vicinity using the same channel.

Attenuation is an inherent characteristic: It's the natural weakening of the signal due to distance and physical barriers.

Troubleshooting Overlap and Attenuation:

Identify Overlap: Use Wi-Fi scanner apps to identify the channels used by surrounding networks.

Change Wi-Fi Channel: If your router allows it, choose a less congested channel with minimal overlap for improved performance.

Reduce Attenuation: Reposition your router to a central location with minimal obstructions like walls or furniture. Consider mesh Wi-Fi systems for larger areas or Wi-Fi range extenders to boost signal strength in specific zones.

Bandwidth issues refer to a network fault where the available data transfer capacity of your network is insufficient to handle the current demand. Imagine a highway with a limited number of lanes. If too much traffic tries to use the highway at once, things slow down, and everyone experiences delays. Similarly, with bandwidth limitations on a network, data transfer speeds become sluggish, impacting various functionalities.

Bandwidth issues manifest as a network fault:

Slow Speeds: The most noticeable symptom is a significant slowdown in internet browsing, downloading files, uploading data, or streaming online content. Even simple tasks like loading web pages can take much longer than usual.

Lag and Buffering: Online gaming, video conferencing, and real-time applications can experience lag and buffering due to delays in data transmission caused by insufficient bandwidth.

Connection Drops: In extreme cases, devices might struggle to maintain a stable connection, leading to frequent dropouts and disruptions.

Causes of Bandwidth Issues:

Limited Bandwidth Plan: If you have a limited internet bandwidth plan from your service provider, exceeding the data cap can throttle your internet speed or restrict data usage for the rest of the billing cycle.

Too Many Connected Devices: A large number of devices connected to your Wi-Fi network (laptops, phones, smart home devices, etc.) can overload its capacity, especially if they are all actively transferring data.

Bandwidth-Intensive Activities: Activities like streaming high-definition videos, online gaming, video conferencing, or large file downloads require significant bandwidth and can strain the network's capacity, impacting overall performance for other devices.

Outdated Network Equipment: Older routers or network adapters might not be able to handle the demands of modern internet speeds and protocols, leading to bottlenecks and slower performance.

Troubleshooting Bandwidth Issues:

Monitor Bandwidth Usage: Many internet service providers offer tools to monitor your bandwidth usage. Identify peak usage times and adjust your online activities accordingly.

Prioritize Bandwidth-Intensive Tasks: Schedule bandwidth-hungry activities like downloads or video conferencing for times when fewer devices are connected to minimize congestion.

Reduce the Number of Connected Devices: Disconnect inactive devices from your Wi-Fi network to free up bandwidth for the devices you're currently using.

Upgrade Your Internet Plan: If you consistently exceed your data cap or experience frequent slowdowns, consider upgrading to a higher bandwidth internet plan from your service provider.

Invest in Newer Network Equipment: Upgrading your router to a newer model that supports faster Wi-Fi standards and can handle more connected devices can significantly improve bandwidth capacity.

Quality of Service (QoS): Some routers offer Quality of Service (QoS) features that prioritize bandwidth allocation for specific devices or applications, ensuring smoother performance for critical tasks.

DNS (Domain Name System) issues are a type of network fault that disrupt the process of translating human-readable website addresses (like [invalid URL removed]) into machine-readable IP addresses (like 8.8.8.8). Imagine a phonebook where the names are all scrambled. You know the name of the person you want to call, but you can't find their number because of the disorganization. Here's how DNS issues manifest as a network fault:

Website Not Found Errors: When you try to access a website, you might encounter error messages like "website not found," "DNS server not responding," or "failed to resolve host."

Slow Website Loading: Even if a website eventually loads, it might take significantly longer than usual due to delays in DNS resolution.

Incorrect Website: In rare cases, a faulty DNS resolution might redirect you to a completely different website than the one you intended to visit.

Causes of DNS Issues:

Incorrect DNS Server Settings: Your computer or network device might be configured to use an incorrect DNS server address, leading to failed resolution attempts.

Overloaded or Unavailable DNS Server: The DNS server you're trying to use might be overloaded with requests or experiencing technical difficulties, causing delays or outages.

Temporary Internet Issues: General internet connectivity problems might prevent your device from communicating with the DNS server effectively.

Local Network Issues: Problems with your router or network configuration within your local network can disrupt DNS communication.

Issues with Your ISP's DNS Servers: Problems with your internet service provider's DNS servers can impact a larger number of users within their network.

Troubleshooting DNS Issues:

Verify DNS Server Settings: Check your network configuration settings and ensure you're using the correct DNS server addresses provided by your internet service provider (ISP) or a reliable public DNS server like Google Public DNS (8.8.8.8) or OpenDNS (208.67.222.222).

Restart Devices: A simple reboot of your computer, router, and modem can often resolve temporary glitches and improve communication with DNS servers.

Flush Your DNS Cache: Your device caches previously accessed website resolutions. Flushing the DNS cache can clear out outdated entries and force your device to obtain fresh information from the DNS server.

Use Public DNS Servers: If you suspect issues with your ISP's DNS servers, try switching to a reliable public DNS server as an alternative.

Contact Your ISP: If the problem persists, consider contacting your internet service provider for further assistance and to report any potential issues with their DNS servers.

Malfunctioning devices are a common network fault that can disrupt network functionality in various ways. Imagine a faulty car on a highway – it can slow down

traffic, cause accidents, and disrupt the overall flow. Similarly, a malfunctioning device on a network can have cascading effects, impacting performance, connectivity, or even network security.

Malfunctioning devices can manifest as network faults:

Hardware Failure: Physical malfunctions in network devices like routers, switches, firewalls, access points, network interface cards (NICs) in computers, or even cabling can disrupt network communication. This might include issues like overheating, faulty components, or physical damage.

Software Issues: Bugs, glitches, or outdated firmware on network devices can lead to unexpected behavior, configuration errors, or security vulnerabilities. These can cause slowdowns, connectivity drops, or even complete network outages.

Driver Issues: Outdated or incompatible network drivers on user devices (computers, laptops, etc.) can lead to difficulties connecting to the network, experiencing slow speeds, or encountering unexpected errors.

Impact of Malfunctioning Devices:

Performance Degradation: Faulty devices can introduce bottlenecks, slow down data transfer speeds, and lead to sluggish network performance overall.

Connectivity Issues: Malfunctioning devices can disrupt network communication, causing devices to lose connection or experience frequent dropouts.

Security Risks: Outdated firmware or security vulnerabilities in network devices can create security gaps and make your network susceptible to cyberattacks.

Troubleshooting Malfunctioning Devices:

Identify the Problem Device: Utilize network monitoring tools or isolate the issue by disconnecting devices one at a time to pinpoint the source of the malfunction.

Restart Devices: A simple reboot of network devices can often resolve temporary glitches and improve performance.

Update Firmware: Check for and install the latest firmware updates for your network devices to address bugs and improve functionality.

Replace Hardware: For persistent hardware failures, consider replacing the malfunctioning device with a new one. This might involve replacing a faulty router, switch, network card, or even a cable.

Update Network Drivers: Ensure user devices have the latest network drivers installed for smooth network connectivity.

Consult with an IT Professional: For complex issues or hardware replacements beyond your expertise, consider seeking assistance from an IT professional.

Prevention:

Regular Maintenance: Schedule regular maintenance tasks like updating firmware, patching software vulnerabilities, and keeping network devices clean and dust-free.

Monitoring and Diagnostics: Utilize network monitoring tools to proactively identify potential issues with devices before they escalate and disrupt network operations.

Backups and Redundancy: Implement backup plans for critical network data and consider redundant network components to minimize downtime in case of device failures.

DNS issues

DHCP (Dynamic Host Configuration Protocol) is a critical service on a network that automatically assigns IP addresses and other configuration settings to devices. A DHCP issue can disrupt this process, leading to connectivity problems for devices attempting to join the network. Imagine a library where everyone needs a borrower's card to check out books. If the system assigning these cards malfunctions, people can't borrow books, hindering the library's core function.

DHCP issues manifest as a network fault:

Symptoms of DHCP Issues:

Unable to Connect to Network: Devices might be unable to connect to the network entirely, often displaying error messages related to IP address acquisition.

Incorrect IP Address Assignment: Devices might receive an invalid or conflicting IP address, leading to network connectivity issues or conflicts with other devices.

Limited Network Functionality: Even if a device obtains an IP address, it might have limited functionality due to missing configuration settings typically provided by DHCP.

Causes of DHCP Issues:

DHCP Server Issues: The DHCP server itself might be malfunctioning due to hardware failures, software bugs, or configuration errors. This can prevent it from assigning IP addresses or providing the necessary configuration information.

Insufficient IP Address Pool: If the DHCP server has run out of available IP addresses in its pool to assign to new devices, it can lead to connection issues for additional devices trying to join the network.

Conflicting IP Addresses: Another device on the network might already be using the IP address that the DHCP server tries to assign, causing a conflict and preventing a successful connection.

Incorrect Client Configuration: The network settings on the device attempting to connect might be misconfigured, preventing it from properly receiving or utilizing the IP address and settings provided by the DHCP server.

Troubleshooting DHCP Issues:

Verify DHCP Server Status: Ensure the DHCP server is running and functioning properly. Check for any error messages in server logs that might indicate the cause of the issue.

Review IP Address Pool: Verify that the DHCP server has a sufficient number of IP addresses available in its pool to accommodate new devices.

Check for IP Address Conflicts: Use network scanning tools to identify any potential IP address conflicts on the network that might be preventing devices from obtaining an address.

Restart Devices: A simple reboot of the DHCP server, router, and the device experiencing connection problems can often resolve temporary glitches and allow for a successful DHCP lease renewal.

Review Client Configuration: Ensure the network settings on the device are configured to obtain an IP address automatically (DHCP) and not set to a static IP address that might be causing conflicts.

Consult Network Documentation: Refer to your network documentation or the DHCP server's manual for specific troubleshooting steps related to the configuration and functionality of your specific system.

Seek Professional Help: For complex issues beyond your expertise, consider seeking assistance from a network administrator or IT professional to diagnose and resolve the DHCP fault.

Preventing DHCP Issues:

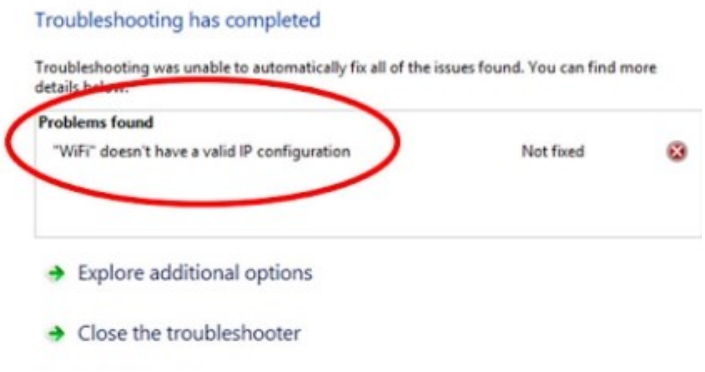
Regular maintenance: Perform routine maintenance tasks on the DHCP server to ensure its smooth operation and address any potential software issues.

Monitor IP Address Pool: Proactively monitor the available IP addresses in the DHCP pool and adjust the pool size if necessary, to accommodate future network growth.

Segmenting the Network: Segmenting your network into smaller subnets with dedicated DHCP servers can help manage IP address allocation more efficiently and reduce the risk of conflicts.

IP configuration issue

An IP configuration issue refers to a problem with the settings that define a device's identity and communication parameters on a network. Imagine a house on a street. The house needs an address (IP address) to identify its location, and it needs to know the address of the local mail center (default gateway) to send and receive mail (data). An IP configuration issue is like having the wrong address or the wrong mail center information, preventing proper communication.



The components involved in IP configuration and how issues with them can manifest as network faults:

IP Address: A unique numerical address that identifies a device on a network. Without a valid IP address, a device is essentially invisible and cannot communicate with other devices.

Subnet Mask: Defines the network and subnet portion of the IP address, specifying which devices belong to the same local network segment. An incorrect subnet mask can lead to communication issues between devices on the same network.

Default Gateway: The IP address of the router or gateway device that directs network traffic between the local network and the wider internet. Without a valid default gateway, devices won't know how to route their data packets to reach their intended destinations.

DNS Server: The IP address of a server that translates human-readable website addresses (like [invalid URL removed]) into machine-readable IP addresses. Incorrect DNS server settings can prevent devices from accessing websites properly.

Symptoms of IP Configuration Issues:

Unable to Connect to Network: Devices might be completely unable to connect to the network, displaying error messages related to IP address configuration.

Limited Network Access: Devices might connect to the network but have limited functionality, such as being unable to access the internet or communicate with other devices on the network.

Slow Network Performance: Incorrect IP configuration can lead to inefficient routing of data packets, resulting in slower network speeds and sluggish performance.

Causes of IP Configuration Issues:

Manual Configuration Errors: Manually assigning incorrect IP addresses, subnet masks, default gateways, or DNS server addresses can lead to connectivity problems.

DHCP Issues: If the DHCP server malfunctioning or encountering issues (as explained previously), devices might not be able to obtain a valid IP configuration automatically.

Conflicting IP Addresses: Two devices on the network might be assigned the same IP address, causing a conflict and preventing one or both devices from connecting properly.

Incorrect Network Settings: Network settings on the device itself might be misconfigured, preventing it from utilizing the obtained IP configuration effectively.

Troubleshooting IP Configuration Issues:

Verify Configuration: Double-check the manually configured IP address, subnet mask, default gateway, and DNS server settings on the device for any typos or errors.

Restart Devices: A simple reboot of the device, router, and modem can sometimes resolve temporary glitches and allow for a successful DHCP lease renewal or configuration application.

Use DHCP: If your network utilizes DHCP, configure devices to obtain an IP address automatically (DHCP) instead of using static IP addresses to avoid manual configuration errors.

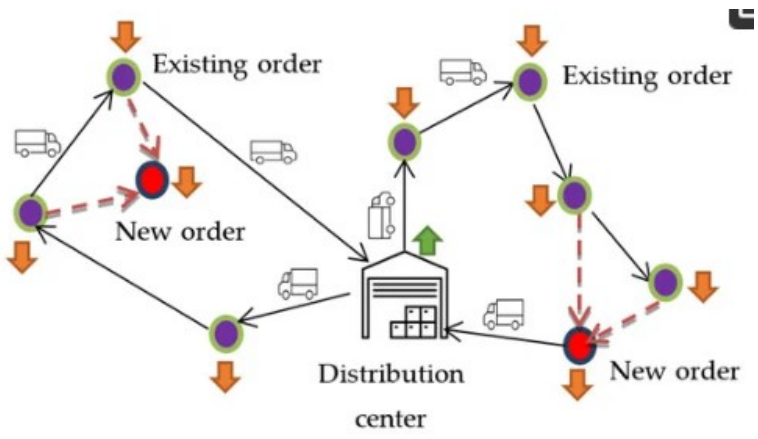
Release and Renew IP Address (Windows): On Windows devices, utilize the "ipconfig /release" and "ipconfig /renew" commands in the Command Prompt to release the current IP configuration and obtain a new one from the DHCP server.

Check Network Documentation: Refer to your network documentation or router's manual for specific instructions on configuring network settings for your devices.

Consult a Network Professional: For complex issues or if you're unsure about manual configuration, consider seeking assistance from a network administrator or IT professional to diagnose and address the IP configuration fault.

Routing issues

Routing issues occur when data packets traveling across a network are unable to find the most efficient path to their intended destination. Imagine a delivery truck on a complex highway system. If the GPS malfunctions or there are unexpected road closures, the truck might get stuck in traffic or take a much longer route to reach its destination.



Routing issues manifest as a network fault:

Slow Network Performance: Data packets taking longer or more convoluted routes to reach their destination can significantly slow down network performance, impacting internet browsing speeds, file transfers, and online applications.

Connection Timeouts: If the routing process takes too long or encounters errors, connections might time out before data reaches its destination, leading to disruptions in online activities.

Website Not Found Errors: In severe cases, routing issues can prevent data packets from reaching their intended destination entirely, resulting in "website not found" or "connection failed" errors.

Causes of Routing Issues:

Incorrect Routing Table Configuration: The routing table on routers determines the path data packets take to reach their destination. Errors or inconsistencies in the routing table configuration can lead to inefficient or incorrect routing.

Network Congestion: Overloaded networks with high traffic volume can cause congestion, making it difficult for data packets to find clear paths and leading to slowdowns and delays.

Hardware Malfunctions: Faulty routers or other network equipment can malfunction and disrupt the routing process, causing connectivity issues.

Outdated Routing Protocols: Networks utilizing outdated routing protocols might not be able to adapt to changes in network topology or traffic patterns, leading to inefficient routing decisions.

Security Threats: Malicious actors might attempt to manipulate routing tables or exploit vulnerabilities in routing protocols to disrupt network traffic or redirect data for malicious purposes.

Troubleshooting Routing Issues:

Verify Routing Table Configuration: Check the routing table on your router (if accessible) for any errors or inconsistencies in the listed routes and destination networks.

Monitor Network Traffic: Utilize network monitoring tools to identify potential bottlenecks or congestion points on the network that might be impacting routing efficiency.

Restart Network Devices: A simple reboot of routers and network equipment can sometimes resolve temporary glitches and improve routing functionality.

Update Routing Protocols: Consider updating routing protocols to the latest versions to ensure they leverage the most efficient routing algorithms and adapt to changes in the network environment.

Consult Network Documentation: Refer to your network documentation or router's manual for specific instructions on managing routing tables or troubleshooting routing issues on your network.

Seek Professional Help: For complex network configurations or suspected security threats, consider seeking assistance from a network administrator or IT professional with expertise in routing protocols and network troubleshooting.

Prevention Tips:

Regular Maintenance: Perform routine maintenance tasks on routers and network equipment to ensure smooth operation and address potential software issues that might impact routing functionality.

Monitor Network Performance: Proactively monitor network performance metrics like latency and throughput to identify any potential routing inefficiencies before they significantly impact user experience.

Segmenting the Network: Segmenting large networks into smaller subnets with dedicated routers can help optimize routing paths and reduce congestion on the network.

Security Measures: Implement appropriate security measures to protect your network from unauthorized access and potential manipulation of routing protocols by malicious actors.

2.2 Faulty hardware or software component.

Faulty hardware or software components can disrupt the proper functioning of various electronic devices, including those on a network. Here's a breakdown of how both hardware and software faults can manifest:

Hardware Faulty Components:

Physical Damage: Physical damage to components like circuit boards, cables, connectors, or internal parts in devices can cause malfunctions and disrupt functionality. This can be due to overheating, dust buildup, accidental drops, or liquid spills.

Component Failure: Electronic components can wear out over time or simply malfunction due to manufacturing defects. This can affect components like network cards, memory modules, hard drives, processors, or power supplies in computers, routers, switches, or another network equipment.

Overheating: Excessive heat buildup due to inadequate ventilation or a malfunctioning cooling system can damage internal components and lead to unexpected shutdowns, performance issues, or permanent hardware failure.

Signs of Faulty Hardware:

Random Crashes or Freezes: Devices might experience unexpected crashes, freezes, or blue screen errors (on Windows) indicating hardware malfunctions.

Unusual Noises: Loud fan noises, grinding sounds, or clicking noises coming from devices can be signs of overheating or failing components.

Performance Degradation: Devices might exhibit slower performance, lagging behavior, or difficulty completing tasks, potentially due to failing hardware.

Connectivity Issues: Network devices with faulty hardware components might experience connectivity problems, dropped connections, or reduced performance.

Software Faulty Components:

Bugs and Glitches: Software bugs are programming errors that can cause unexpected behavior, crashes, or instability in applications or operating systems.

Outdated Software: Outdated software might lack security patches or compatibility with newer hardware, leading to performance issues or vulnerabilities.

Malware Infections: Malicious software like viruses or malware can disrupt system functions, corrupt files, or steal data, causing various problems on the device.

Driver Issues: Outdated or incompatible device drivers can lead to conflicts with hardware components, resulting in malfunctions or limited functionality.

Signs of Faulty Software:

Error Messages: Frequent error messages, pop-ups, or notifications can indicate software issues or malware infections.

Slow Performance: Software problems can slow down your device's overall performance, making it sluggish to respond to commands or applications.

Unexpected Behavior: Applications might crash unexpectedly, behave erratically, or display unusual functionality due to software faults.

Security Issues: Signs of a software issue might include frequent pop-ups with security warnings, unexpected browser redirects, or sluggish performance – potentially caused by malware.

Troubleshooting Faulty Hardware or Software:

Identify the Problem: Use system logs, error messages, or visual clues to pinpoint the source of the issue (hardware component or specific software).

Restart Device: A simple restart can often resolve temporary glitches in both hardware and software and allow the device to reboot cleanly.

Update Software: Ensure your operating system, applications, and device drivers are updated to the latest versions to address known bugs and improve compatibility.

Run System Scans: Utilize built-in antivirus or anti-malware software to scan for and remove potential malware infections that might be causing disruptions.

Hardware Diagnostics: Some devices offer built-in diagnostic tools or allow for manual testing of hardware components to identify potential malfunctions.

Replace Components: For confirmed hardware failures, consider replacing the faulty component (if possible) or seeking professional repair services.

Reinstall Software: In severe software cases, reinstalling the operating system or affected software can be a last resort to restore functionality to a clean state.

2.3 The problem scenarios are observed

Observing network problems requires a combination of awareness of user experience, monitoring tools, and some basic troubleshooting steps. Here's how to approach different problem scenarios:

1. Coverage Issues:

User Experience: Look for signs like weak or no Wi-Fi signal on devices in certain areas, frequent disconnections when moving around, or buffering issues while streaming in specific locations.

Troubleshooting: Use a Wi-Fi scanner app on your phone or computer to visualize signal strength throughout your space. Identify areas with weak signal or dead zones.

2. Communication Issues:

User Experience: Pay attention to difficulties connecting devices to the network, frequent dropouts after connecting, or slow data transfer speeds even with a seemingly stable connection.

Troubleshooting: Try connecting a device with a wired connection (Ethernet cable) directly to the router. If the wired connection works well, the issue might be with the Wi-Fi adapter on your device or wireless interference. Verify login credentials for the Wi-Fi network on your devices.

3. Capacity Issues:

User Experience: Monitor overall internet performance during peak usage times. Look for signs like slow browsing, sluggish downloads, lagging online games, or video conferencing disruptions. Observe if the issues coincide with a high number of devices connected to the network.

Troubleshooting: Use your router's web interface (if accessible) or ISP-provided tools to monitor bandwidth usage. Identify times with peak traffic and adjust online activities accordingly. Disconnect inactive devices from the Wi-Fi network to free up bandwidth for the devices you're currently using.

4. Overlap and Attenuation:

User Experience: Similar to coverage issues, look for areas with weak signal strength or frequent disconnections. Overlap can also manifest as slow speeds for no apparent reason.

Troubleshooting: Use a Wi-Fi scanner app to identify channels used by surrounding Wi-Fi networks. If your router allows it, try changing your Wi-Fi channel to a less congested one. Reposition your router to a central location with minimal obstructions like walls or furniture. Consider mesh Wi-Fi systems for larger areas or Wi-Fi range extenders to boost signal strength in specific zones.

5. Bandwidth Issues:

User Experience: The most noticeable sign is a significant slowdown in internet browsing, downloading files, uploading data, or streaming online content. You might also experience lag and buffering in online applications.

Troubleshooting: Contact your internet service provider (ISP) to inquire about your bandwidth plan and data usage. Consider upgrading to a higher bandwidth plan if you consistently exceed your data cap or experience frequent slowdowns. Monitor bandwidth usage using tools provided by your ISP and schedule bandwidth-intensive activities for times with fewer connected devices.

6. DNS Issues:

User Experience: Encountering error messages like "website not found," "DNS server not responding," or "failed to resolve host" when trying to access websites are telltale signs of DNS issues. Websites might also take significantly longer to load than usual.

Troubleshooting: Try flushing your DNS cache on your device. This clears out outdated website resolutions and forces your device to obtain fresh information from the DNS server. Alternatively, try using a public DNS server like Google Public DNS (8.8.8.8) or OpenDNS (208.67.222.222) instead of your ISP's DNS servers.

7. Malfunctioning Devices:

User Experience: Network disruptions caused by malfunctioning devices can manifest as unexpected disconnections, slowdowns, or even complete network outages. You might also notice unusual behavior on the malfunctioning device itself.

Troubleshooting: Isolate the issue by disconnecting devices one by one to pinpoint the source of the malfunction. Restart devices like routers, switches, and the device experiencing connection problems. Update firmware on network devices to address bugs and improve functionality. Consider seeking assistance from an IT professional for complex issues or hardware replacements.

8. DHCP Issues:

User Experience: Devices might be unable to connect to the network entirely or receive an invalid or conflicting IP address, leading to limited functionality or no internet access at all.

Troubleshooting: Restart the DHCP server (if accessible) and the router to resolve temporary glitches. Check for error messages in server logs that might indicate the cause of the issue. Consult your network documentation or the DHCP server's manual for specific troubleshooting steps related to your system.

9. IP Configuration Issues:

User Experience: Similar to DHCP issues, devices might be unable to connect to the network or have limited functionality due to incorrect IP address configuration.

Troubleshooting: Double-check the manually configured IP address, subnet mask, default gateway, and DNS server settings on the device for any typos or errors. Verify that the network settings on the device are configured to obtain an

2.4 Problems are detected using diagnostic tools

Diagnostic tools are digital aids used to identify and troubleshoot problems within a network. They offer a more systematic approach to network fault detection compared to simply observing user experience. Here's how diagnostic tools can be utilized for problem detection procedures:

1. Network Monitoring Tools:

Functionality: These tools provide real-time or historical data on various network metrics like bandwidth usage, latency (signal delay), packet loss (data transmission errors), and device uptime.

Problem Detection: Significant fluctuations in these metrics can indicate potential bottlenecks, congestion points, or failing hardware. For example, high packet loss might suggest faulty cables or overloaded network switches.

2. Packet Capture and Analysis Tools:

Functionality: These tools capture data packets traveling across the network and allow for in-depth analysis of their content, origin, and destination.

Problem Detection: By examining captured packets, you can identify issues like routing errors, protocol malfunctions, or suspicious activity that might indicate security threats.

3. Ping and Traceroute Tools:

Functionality: "Ping" sends a test message to a specific device on the network to measure its response time (latency). "Traceroute" maps the path a data packet takes to reach its destination, identifying hops (network segments) along the way.

Problem Detection: High ping times can indicate congestion or connection issues between your device and the target. Traceroute can reveal bottlenecks or outages along the data transfer path.

4. Wi-Fi Scanner Apps:

Functionality: These mobile applications scan the surrounding Wi-Fi environment, displaying information like signal strength on different channels, nearby networks, and their security settings.

Problem Detection: Weak signal strength, overlapping channels with neighboring networks, or excessive interference can be identified and addressed to improve Wi-Fi performance.

5. Event Logs:

Functionality: Most network devices like routers, switches, or firewalls maintain event logs that record system activity, errors, and warnings.

Problem Detection: By reviewing event logs, you can identify error messages or unusual activity that might pinpoint the source of a network fault.

6. Built-in System Diagnostics:

Functionality: Operating systems and network devices often come with built-in diagnostic tools that can test specific functionalities or troubleshoot common issues.

Problem Detection: These tools can be helpful for identifying problems with network adapters, network connectivity, or basic configuration errors.

Using Diagnostic Tools Effectively:

Identify the Problem: Before diving into diagnostic tools, clearly define the network issue you're experiencing (slow speeds, connection drops, etc.). This will guide your choice of tools and troubleshooting steps.

Start Simple: Begin with basic tools like ping or traceroute to isolate broad connectivity issues. Gradually move towards more advanced tools like packet capture for deeper analysis.

Interpret Results: Diagnostic tools often generate reports or data visualizations. Understanding how to interpret these results is crucial for pinpointing the root cause of the problem.

Consult Resources: Many diagnostic tools come with user manuals or online resources that explain their functionalities and how to interpret the results they provide.

Self-Check-2: Identify the Problem

1. How can you identify a network fault?
   Answer:
2. What are some signs of a faulty hardware component on a network?
   Answer:
3. How can outdated software cause network problems?
   Answer:
4. Describe a scenario where you might suspect a DHCP issue on your network.
   Answer:
5. What information can a Wi-Fi scanner app provide to help diagnose network problems?
   Answer:
6. Briefly explain how a ping test can be used to troubleshoot network connectivity.
   Answer:
7. What can you learn by reviewing event logs on a network device?
   Answer:
8. Why is it important to define the network problem you're experiencing before using diagnostic tools?
   Answer:
9. What are some preventative measures you can take to minimize network faults caused by faulty hardware or software?
   Answer:
10. How can observing user experience help identify bandwidth issues on a network?
    Answer:

Answer Key-2: Identify The Problem

1. How can you identify a network fault?
   Answer: There are two main approaches: observing user experience (weak Wi-Fi signal, frequent disconnects) and utilizing network diagnostic tools (monitoring bandwidth usage, analyzing packet loss).
2. What are some signs of a faulty hardware component on a network?
   Answer: Signs include unexpected crashes, unusual noises from devices, performance degradation, and connectivity issues on network devices like routers.
3. How can outdated software cause network problems?
   Answer: Outdated software might lack security patches or compatibility with newer hardware, leading to performance issues, vulnerabilities, or connection errors.
4. Describe a scenario where you might suspect a DHCP issue on your network.
   Answer: If multiple devices are unable to connect to the network entirely, or receive invalid IP addresses, a DHCP issue that prevents proper IP address assignment might be the culprit.
5. What information can a Wi-Fi scanner app provide to help diagnose network problems?
   Answer: A Wi-Fi scanner app can reveal signal strength on different channels, identify nearby networks and their security settings, helping diagnose issues like overlapping channels or weak signal strength.
6. Briefly explain how a ping test can be used to troubleshoot network connectivity.
   Answer: A ping test sends a message to a specific device and measures its response time (latency). High ping times can indicate congestion or connection issues between your device and the target.
7. What can you learn by reviewing event logs on a network device?
   Answer: Event logs record system activity, errors, and warnings. Reviewing them can reveal error messages or unusual activity that might pinpoint the source of a network fault.
8. Why is it important to define the network problem you're experiencing before using diagnostic tools?
   Answer: Knowing the issue (slow speeds, connection drops) helps you choose the appropriate tools. For example, a ping test might be suitable for basic connectivity issues, while packet capture is needed for deeper analysis.
9. What are some preventative measures you can take to minimize network faults caused by faulty hardware or software?
   Answer: Regularly update software, perform system scans for malware, utilize surge protectors for devices, and maintain proper ventilation to prevent overheating.
10. How can observing user experience help identify bandwidth issues on a network?
    Answer: If internet browsing, downloads, or streaming become significantly slow, especially during peak usage times with many devices connected, it might indicate bandwidth limitations.

Task Sheet-2.1: Identify the problem

Performance Objective: At the end of this task, the trainee should be able to identify and diagnose network faults using user experience observations and diagnostic tools.

Identify the Problem: Ask users about any network issues they are experiencing. Look for signs like:

- Slow browsing speeds
- Frequent disconnections
- Limited internet access for certain applications
- Weak or no Wi-Fi signal in specific areas
- Difficulty connecting new devices to the network

Analyze Problem Scenarios:

Match User Experience to Potential Causes: Based on the observed issues, consider the following scenarios:

- Coverage Issues: Weak or no signal in certain areas
- Communication Issues: Devices struggling to connect or maintain connection
- Capacity Issues: Slowdowns during peak usage times with many connected devices
- Overlap and Attenuation: Slow speeds or disconnects due to Wi-Fi interference
- Bandwidth Issues: Significant slowdowns in browsing, downloads, or streaming
- DNS Issues: Difficulty accessing websites or slow loading times
- Malfunctioning Devices: Unexpected disconnections or complete network outages

Initial Troubleshooting:

- Restart Devices: Reboot routers, switches, and any devices experiencing connection problems. Simple restarts can often resolve temporary glitches.
- Verify Network Credentials: Ensure devices are using the correct Wi-Fi network name and password (SSID and key).
- Test Wired Connection: If possible, connect a device directly to the router with an ethernet cable. This helps isolate issues with Wi-Fi adapter or wireless interference.

Utilize Diagnostic Tools:

- Choose Appropriate Tool: Depending on the suspected issue, select the most relevant diagnostic tool:
- Network Monitoring Tools: Monitor bandwidth usage, latency, packet loss, and device uptime to identify bottlenecks or congestion.

- Ping and Traceroute Tools: Use ping to measure response times and traceroute to map data packet paths to diagnose connectivity issues.
- Wi-Fi Scanner Apps: Scan for signal strength on different channels and identify nearby networks to identify interference.
- Event Logs: Review event logs on network devices for error messages or unusual activity that might pinpoint the fault.
- Built-in System Diagnostics: Utilize tools provided by your operating system or network devices for troubleshooting specific functionalities.

Analyze Diagnostic Results:

- Interpret Data: Understand the information provided by the chosen tool. Look for anomalies, fluctuations, or error messages that indicate potential causes.
- Narrow Down the Problem: Based on the analysis, further isolate the source of the network fault.

Learning Outcome-3: Identify The Solution

Assessment Criteria:

1. Appropriate person (if required) is consulted and solution is identified
2. Types of solutions are identified

Content:

1. Appropriate person (if required) consultation
2. Types of solutions

Resources Required/ Conditions:

The trainees must be provided with the following:

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

Methodologies

1. Lecture/discussion
2. Demonstration/application
3. Presentation
4. Blended delivery methods

Assessment Methods

1. Written test
2. Demonstration
3. Observation with checklist
4. Oral questioning
5. Portfolio

Learning Experience-3: Identify The Solution

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

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

Information Sheet-3: Identify The Solution

Learning Objectives:

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

3.1 Consult appropriate person (if required) and identify solution
3.2 Identify Types of solutions

3.1 Consult appropriate person (if required) and identify solution

When troubleshooting network faults, you can often identify and resolve the issue yourself using the techniques outlined in the previous task sheet. However, there are situations where consulting with a more appropriate person is recommended. Here's a breakdown of when to seek consultation and who the appropriate person might be:

Scenarios for Consultation:

Limited Technical Expertise: If you lack the confidence or knowledge to interpret diagnostic results, implement complex solutions, or understand the potential impact of configuration changes, consider seeking help.

Suspected Hardware Failure: While some basic hardware troubleshooting can be done (reboots, cable checks), diagnosing and repairing internal hardware faults in routers, switches, or other network devices often requires specialized skills and tools.

Advanced Network Configurations: Complex network setups with multiple devices, VLANs (Virtual Local Area Networks), or security configurations might require the expertise of a network administrator to troubleshoot and optimize.

Persistent or Recurring Issues: If you've followed the troubleshooting steps and the network fault persists or keeps recurring, seeking professional help can identify the root cause and implement a permanent solution.

Security Concerns: If you suspect a security breach, malware infection, or unauthorized access attempt on your network, consulting with a network security specialist is crucial to address the issue and implement appropriate security measures.

Appropriate Person for Consultation:

IT Help Desk or Network Administrator: In a corporate or organizational setting, your IT department or a designated network administrator will likely be the most appropriate person to consult. They possess the technical expertise and access to specialized network management tools to diagnose and resolve complex network issues.

Technical Support from ISP (Internet Service Provider): For issues related to your internet connection itself (signal strength, outages, bandwidth limitations), contacting your

internet service provider's technical support can provide insights and potential solutions specific to their network infrastructure.

Computer Technician or Network Consultant: For home networks or situations where an IT department isn't readily available, consider consulting with a computer technician or network consultant who specializes in network troubleshooting and repair.

Online Resources and Forums: Online resources and forums dedicated to networking topics can be a valuable source of information and troubleshooting tips. However, it's important to exercise caution and verify the credibility of information before implementing solutions suggested online.

Benefits of Consultation:

Faster Resolution: Experienced professionals can diagnose and resolve issues more quickly, minimizing downtime and ensuring network stability.

Expertise and Resources: They possess the knowledge and tools to address complex network problems beyond the scope of basic troubleshooting.

Preventative Measures: Consulting with a network professional can help identify potential weaknesses in your network security and suggest preventative measures to avoid future issues.

3.2 Types of solutions

In the context of network troubleshooting, there are various types of solutions you can implement depending on the identified problem. Here's a breakdown of some common solution categories:

1. Hardware Solutions:

Repair or Replacement: If faulty hardware components like network cards, routers, switches, or cables are causing the issue, repairs or replacements might be necessary. In some cases, repairs might be cost-effective, while complete replacements might be needed for outdated or malfunctioning devices.

Upgrades: For situations where network performance limitations are due to insufficient hardware capabilities (older router with limited bandwidth), upgrading network devices to models with better specifications can be a solution.

2. Software Solutions:

Updates and Patches: Outdated software on network devices or user devices can lead to compatibility issues or security vulnerabilities. Keeping operating systems, firmware, and applications updated with the latest patches addresses bugs and improves overall network functionality.

Driver Updates: Outdated or incompatible device drivers can cause network connectivity problems. Regularly updating device drivers ensures proper communication between hardware components and the operating system.

Security Software Updates: Maintaining up-to-date antivirus, anti-malware, and firewall software is crucial to protect your network from malicious software and unauthorized access attempts.

3. Network Configuration Changes:

Wi-Fi Channel Selection: Overlapping Wi-Fi channels from neighboring networks can cause interference and slow down speeds. Changing your Wi-Fi channel to a less congested one can improve signal quality and network performance.

Security Settings: Utilizing strong encryption protocols (WPA2 or WPA3) and complex passwords for your Wi-Fi network enhances network security and minimizes the risk of unauthorized access.

IP Address Management: In complex networks, managing IP address assignments efficiently can prevent conflicts and ensure proper device communication. Techniques like DHCP reservations or static IP assignments might be implemented.

Bandwidth Allocation: If specific devices are consuming excessive bandwidth and impacting overall network performance, implementing Quality of Service (QoS) settings can prioritize bandwidth allocation for critical applications.

4. Optimization Techniques:

Device Positioning: Strategically placing your router in a central location with minimal obstructions (walls, furniture) can improve Wi-Fi signal strength and coverage throughout your space.

Wireless Repeaters or Mesh Systems: For larger areas or areas with weak Wi-Fi signal, wireless repeaters or mesh Wi-Fi systems can extend the network's reach and provide improved coverage.

Disabling Unused Services: Disabling unnecessary services or features on network devices can free up resources and potentially improve network performance.

5. Security Solutions:

Firewalls and Intrusion Detection Systems (IDS): Firewalls act as a barrier between your network and the internet, filtering incoming and outgoing traffic based on security policies. Intrusion detection systems monitor network activity for suspicious behavior and can alert you to potential security threats.

Guest Network Creation: Creating a separate guest network for visitors isolates their devices from your main network, protecting sensitive data and resources on your primary network.

Vulnerability Scans: Regularly conducting vulnerability scans on your network devices can identify potential security weaknesses that attackers might exploit. These scans help prioritize patching and remediation efforts.

Choosing the Right Solution:

The type of solution you implement depends on the specific network fault you're addressing. By accurately diagnosing the problem, you can choose the most appropriate course of action, whether it's a hardware replacement, software update, network configuration change, optimization technique, or security solution. Remember, consulting with a network professional can be invaluable for identifying the root cause of the problem and recommending the most effective solution.

Self-Check-3: Identify the Solution

You suspect a hardware failure in your router, but lack the skills to repair it yourself. Who might be the most appropriate person to consult?

1. Besides replacing outdated network devices, what other solution type might improve network performance limitations?
   Answer:

2. When troubleshooting network connectivity issues, should you update your antivirus software as a hardware or software solution?
   Answer:

3. What's one benefit of consulting a network professional when identifying solutions for network faults?
   Answer:

4. Give an example of a network configuration change that could improve Wi-Fi signal strength.
   Answer:

Answer Key-3: Identify The Solution

1. You suspect a hardware failure in your router, but lack the skills to repair it yourself. Who might be the most appropriate person to consult?
   Answer: An IT Help Desk or Network Administrator (in a corporate setting) or a Computer Technician (for home networks) could provide assistance with hardware repairs or replacements.

2. Besides replacing outdated network devices, what other solution type might improve network performance limitations?
   Answer: Updating software like firmware on network devices or device drivers can address bugs and improve compatibility, potentially leading to better performance.

3. When troubleshooting network connectivity issues, should you update your antivirus software as a hardware or software solution?
   Answer: Software solution. Updating antivirus software addresses potential software issues like malware infections that might disrupt network functionality.

4. What's one benefit of consulting a network professional when identifying solutions for network faults?
   Answer: Network professionals possess expertise and tools to diagnose complex issues and recommend the most effective solutions, saving you time and ensuring network stability.

5. Give an example of a network configuration change that could improve Wi-Fi signal strength.
   Answer: If experiencing weak Wi-Fi signal, changing your Wi-Fi channel to a less congested one can minimize interference from neighboring networks and improve signal quality.

Learning Outcome-4: Solve The Problem

Assessment Criteria:

1. Replacement of faulty hardware equipment is performed if required
2. Replaced equipment is tested
3. Configuration is performed as per solution requirement
4. Network activity is tested.

Content:

1. Replacement of faulty hardware equipment
    - Replacement of network card
    - Cable
    - Switch
    - Router
    - Wireless access point
    - Modem
    - Software
    - Mother board components
2. Testing procedure of Replaced equipment
3. Network Configuration
4. Testing Network activity.

Resources Required/ Conditions:

The trainees must be provided with the following:

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

Methodologies

1. Lecture/discussion
2. Demonstration/application
3. Presentation
4. Blended delivery methods

Assessment Methods

1. Written test
2. Demonstration
3. Observation with checklist
4. Oral questioning
5. Portfolio

Learning Experience-4: Solve The Problem

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

Learning Steps	Resources specific instructions
1. Student will ask the instructor about Fixing the problem	1. Instructor will provide the learning materials "**Solve the Problem"**
2. Read the Information sheet/s	2. Information Sheet No: 4 Solve the Problem
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 4 Solve the Problem Answer key No. 4 Solve the Problem
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No: 4 Solve the Problem Specification Sheet: 4 Solve the Problem

Information Sheet-4: Solve The Problem

Learning Objectives:

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

4.1 Perform Replacement of faulty hardware equipment if required
4.2 Test Replaced equipment
4.3 Perform Configuration as per solution requirement
4.4 Test Network activity.

4.1 Replacement of faulty hardware equipment

Replacing faulty hardware equipment is a crucial step in network troubleshooting when other solutions like software updates or configuration changes haven't resolved the issue.

A faulty network card (NIC) can disrupt your internet connection or cause slow and unreliable network performance. Replacing a network card is a relatively straightforward process for most computers. Here's a breakdown of the steps involved:

Identifying a Faulty Network Card:

Symptoms: Look for signs like complete loss of internet connectivity, frequent disconnections, slow download/upload speeds, or inability to detect available networks.

Device Manager: Check your device manager for any error messages or exclamation marks next to the network adapter. This might indicate a driver issue or hardware malfunction.

Diagnostic Tools: Utilize network diagnostic tools like ping tests or tracertoute to identify connectivity issues that might point towards a faulty network card.

Before Replacement:

Troubleshooting: Try basic troubleshooting steps like restarting your computer, updating network drivers, or disabling/re-enabling the network adapter before resorting to replacement.

Compatibility: Ensure the replacement network card (NIC) is compatible with your computer's motherboard slot (PCI, PCIe) and operating system. Consult your computer's user manual or manufacturer's website for compatibility information.

Replacement Process:

Power Down and Unplug: Power down your computer and unplug it from the power source. This is crucial to prevent electrical damage during the replacement process.

Open the Computer Case: Carefully remove the side panel of your computer case to access the internal components. Refer to your computer's manual or online resources for specific instructions on opening the case.

Locate the Network Card: The network card will typically be a small circuit board inserted into a PCI or PCIe slot on your motherboard. Identify the slot it's currently occupying.

Unscrew and Remove: Locate the retaining screw holding the network card in place. Unscrew it carefully and gently remove the network card from the slot.

Install the New Network Card: Align the replacement network card with the appropriate slot on your motherboard and carefully insert it. Secure it in place with the retaining screw you removed earlier.

Close the Case and Reconnect: Close the computer case securely and reconnect all previously disconnected cables.

Power On and Install Drivers: Power on your computer. The operating system might automatically detect the new network card and install the necessary drivers. If not, you might need to download and install drivers from the network card manufacturer's website.

Verification and Testing:

Device Manager: Open your device manager and verify that the network adapter is recognized and functioning properly.

Network Connection: Connect to your Wi-Fi network or wired ethernet connection depending on your setup. Test your internet connection by browsing the web or running a speed test.

Performance Monitoring: Monitor your internet performance after replacing the network card. Look for improvements in connection stability and download/upload speeds.

Replacing Network Cables:

Identifying Faulty Cable: Look for physical damage to the cable like cuts, exposed wires, or loose connectors. You can also try using a different cable with a known working device to isolate the issue.

Replacement Process: Simply swap the faulty cable with a new one of the same category (Cat5e, Cat6, etc.) ensuring secure connections at both ends to the devices. Short, high-quality cables are generally preferred.

Replacing Network Switches:

Identifying Faulty Switch: Look for unusual behavior like blinking lights on specific ports, dropped connections on connected devices, or overall network performance

degradation. Consider the number of devices you need to connect when choosing a replacement switch.

Replacement Process: 1. Power down all connected devices and the switch itself. 2. Disconnect all network cables from the switch. 3. Physically replace the switch with the new one. 4. Reconnect the network cables to their respective ports on the new switch, ideally maintaining the same port configuration as the old switch (if applicable). 5. Power on the new switch and then power on the connected devices one by one.

Replacing Routers:

Identifying Faulty Router: Signs include frequent reboots, weak Wi-Fi signal, limited bandwidth for connected devices, or inability to connect to the internet. Consider the internet speed you subscribe to and the number of devices you need to support when choosing a replacement router.

Replacement Process: 1. Power down the router and your modem. 2. Disconnect all cables from the router, including the power cable, internet cable from the modem, and any ethernet cables from devices. 3. Replace the router with the new one. 4. Reconnect the internet cable from the modem to the WAN port of the new router. 5. Connect ethernet cables from your devices to the LAN ports of the new router (if needed). 6. Power on the modem first, followed by the router. 7. Configure the new router's internet connection settings based on your ISP's instructions (usually done through a web interface). This might involve entering your username, password, and any specific configuration details.

Replacing Wireless Access Points:

Identifying Faulty Access Point: Look for weak or inconsistent Wi-Fi signal in specific areas, difficulty connecting devices to the wireless network, or frequent disconnections. Consider the coverage area you need and any additional features like mesh capabilities when choosing a replacement access point.

Replacement Process: 1. Power down the access point and any connected devices. 2. Disconnect the power cable and ethernet cable from the access point. 3. Replace the access point with the new one. 4. Reconnect the ethernet cable from your network (switch or router) to the WAN/LAN port of the new access point (depending on the configuration). 5. Power on the access point and any connected devices. 6. Configure the new access point's Wi-Fi settings (SSID, password, security type) to match your existing network or set up a new network as desired (usually done through a web interface).

Modem Replacement:

Identifying a Faulty Modem: Look for signs like complete loss of internet connection, frequent disconnects, or inability to synchronize with your ISP's network. Your ISP might also notify you if there's an issue with your modem.

Replacement Process:

Contact your ISP: Before replacing the modem yourself, contact your internet service provider (ISP) to confirm the issue and inquire about their replacement procedures. They might provide a new modem or require you to return the old one.

Disconnect the Old Modem: Power down the modem and unplug it from the power outlet and the coaxial cable connection.

Connect the New Modem: Follow the instructions provided by your ISP to connect the new modem. This typically involves connecting the coaxial cable from the wall outlet to the cable port on the modem and connecting an ethernet cable from the modem's LAN port to your router's WAN port.

Activate the New Modem: Contact your ISP to activate the new modem. They might need the serial number or MAC address of the new modem to complete the activation process.

Important Note: Replacing a modem might involve configuration changes specific to your ISP's network. Always consult your ISP for instructions to ensure proper functionality after replacement.

2. Software Replacement (Not Applicable to Hardware)

Network functionality relies on software running on various devices like routers, switches, or network adapters. However, replacing software isn't typically a troubleshooting step for network issues. Instead, you would update the software to the latest version:

Updating Firmware: Most network devices allow firmware updates which address bugs, improve performance, and sometimes introduce new features. Check the manufacturer's website or the device's web interface for available firmware updates and follow the provided instructions for installation.

Updating Network Drivers: Outdated network drivers on your computer can cause connectivity issues. Update your network drivers through your operating system's device manager or by downloading the latest drivers from the network card manufacturer's website.

3. Motherboard Components (Advanced Troubleshooting):

Replacing motherboard components for network troubleshooting is an advanced procedure and not recommended for beginners. Motherboard components like the network interface card (NIC) are typically soldered onto the motherboard, making replacement a delicate task. Here's a general overview:

Identifying Faulty Motherboard NIC: Symptoms are similar to a faulty network card, such as no internet connection, slow speeds, or inability to detect networks. However,

exhausting other troubleshooting steps like software updates and external network card replacements is crucial before suspecting a faulty motherboard NIC.

Replacement Process: This is a complex process involving desoldering the faulty NIC from the motherboard and soldering a new compatible NIC in its place. Specialized tools and soldering skills are required. Consider seeking professional help from a computer repair technician if this is the suspected issue.

4.2 Testing Procedure for Replaced Network Equipment

Once you've replaced a faulty network device (router, switch, network card, etc.), it's crucial to verify that the replacement functions correctly and resolves the network issue you were experiencing. Here's a breakdown of the testing procedures you can follow:

Basic Functionality Tests:

Power On and Initial Connection: Power on the replaced equipment and any connected devices. Verify that they all power on successfully.

Physical Connections: Double-check that all cables (power, ethernet, coaxial for modems) are securely connected to the new device and the appropriate ports on other devices.

LED Status Lights: Refer to the user manual for information on the meaning of LED lights on the new device. Ensure they display the expected behavior based on the current network activity (e.g., solid light for a wired connection, blinking light for transferring data).

Network Connectivity Tests:

Device Connectivity: Use a computer or other network-enabled device to attempt connecting to the network. This could be through a wired ethernet connection or by connecting to the Wi-Fi network (if applicable).

Internet Access: Once connected to the network, try accessing the internet by browsing a website or using an internet application. Verify that you have a stable and functioning internet connection.

Performance Monitoring: Run basic internet speed tests to gauge your download and upload speeds. Compare these results with your ISP's advertised speeds or previous performance measurements before replacing the equipment.

Advanced Tests (Optional):

Network Tools: If you're comfortable with network diagnostics, utilize tools like ping tests or tracertoute to verify that data packets are being routed correctly and without excessive delays or losses.

Stress Testing (Optional): For critical network setups, consider stress testing the new equipment by connecting multiple devices and simulating heavy network traffic. This helps identify any potential bottlenecks or limitations of the replaced equipment.

Network configuration refers to the process of setting up and managing the devices and software that make up a network. It involves defining how these elements interact to enable communication and data flow efficiently and securely. Here's a breakdown of the key aspects of network configuration:

Network Devices:

Routers: Routers are central devices that act as traffic directors, sending data packets to their intended destinations on the network or the internet. Configuration typically involves setting up internet connection details (provided by your ISP), managing wireless network settings (SSID, password, security), and defining firewall rules to control incoming and outgoing traffic.

Switches: Switches connect multiple devices on a network segment, allowing them to communicate directly with each other. Configuration might involve setting up VLANs (Virtual Local Area Networks) to segment the network for security or performance reasons.

Wireless Access Points (WAPs): WAPs extend the reach of your Wi-Fi network, providing wireless connectivity to devices like laptops, smartphones, and tablets. Configuration typically involves setting up the SSID, password, security type (WPA2 or WPA3 recommended), and optimizing channels to minimize interference from other networks.

Network Interface Cards (NICs): NICs are network adapters installed in computers or other devices, enabling them to connect to a network. Configuration on the device itself might be limited, but network settings like IP address, subnet mask, and default gateway can be defined through the operating system.

4.3 Software Configuration:

Operating Systems: Network settings on individual devices, like IP addresses, subnet masks, and default gateways, are typically configured through the operating system's network settings menu.

Network Management Software: For larger or complex networks, network management software can be used to centrally configure, monitor, and troubleshoot network devices and resources.

Network Protocols:

TCP/IP: The Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of protocols that defines how data is formatted, addressed, and transmitted over networks. Understanding basic TCP/IP concepts is crucial for network configuration tasks.

DNS (Domain Name System): DNS translates human-readable website addresses (like [invalid URL removed]) into machine-readable IP addresses that computers can understand. Configuring DNS servers on your network devices ensures proper website resolution.

Security Considerations:

Firewalls: Firewalls act as a barrier between your network and the internet, filtering incoming and outgoing traffic based on predefined security rules. Configuring firewalls helps protect your network from unauthorized access and malicious attacks.

Encryption: Utilizing strong encryption protocols like WPA2 or WPA3 for your Wi-Fi network safeguards your wireless data from eavesdropping.

Access Control: Implementing access control measures like user authentication and authorization limits access to network resources and reduces security risks.

4.4 Testing Network activity

Testing network activity is a crucial step in diagnosing network issues, monitoring performance, and ensuring the overall health of your network. Here's a breakdown of various methods you can use to test network activity:

Basic Tests:

Ping Test: The ping test is a fundamental tool for verifying network connectivity between two devices. It sends a data packet to a specific IP address and measures the time it takes for a response to return. This helps identify basic connectivity issues or delays in data transmission. You can use the "ping" command in your command prompt (Windows) or terminal (Mac) to perform a ping test.

Traceroute: Traceroute is a diagnostic tool that shows the route a data packet takes to reach its destination. It lists the IP addresses of each network device (routers, hops) along the path. This helps identify potential bottlenecks or issues with specific network segments causing delays or connection problems. You can use the "tracert" command (Windows) or "traceroute" command (Mac) to perform a traceroute.

Performance Tests:

Internet Speed Tests: Numerous online internet speed test services can measure your download and upload speeds. These tests compare your actual internet speed to the speeds advertised by your internet service provider (ISP). This helps identify potential limitations with your internet plan or troubleshoot issues related to your network equipment.

File Transfer Tests: Transferring a large file between two devices on your network can provide a practical assessment of real-world network performance. The time it takes to complete the transfer can indicate potential bandwidth limitations or bottlenecks within your network.

Self-Check-4: Solve The Problem

1. What are some signs that might indicate faulty hardware equipment on a network?
   Answer:

2. Before replacing network hardware, what troubleshooting steps should be considered?
   Answer:

3. What factors should be considered when replacing a network card?
   Answer:

4. How can you verify that a replacement router is functioning correctly?
   Answer:

5. What is the difference between replacing hardware and updating software for network troubleshooting?
   Answer:

6. What are some benefits of testing replaced network equipment?
   Answer:

7. What basic tests can be used to verify network connectivity after replacing equipment?
   Answer:

8. What does "Network Configuration" refer to?
   Answer:

9. What are some security considerations when configuring a network?
   Answer:

10. How can testing network activity be helpful for troubleshooting?
    Answer:

Answer Key-4: Solve The Problem

1. What are some signs that might indicate faulty hardware equipment on a network?
   Answer: Signs can include complete loss of internet connection, frequent disconnects, slow speeds, unexpected device crashes, or unusual noises from network equipment.
2. Before replacing network hardware, what troubleshooting steps should be considered?
   Answer: Before resorting to replacement, try simple troubleshooting steps like restarting devices, updating software (firmware or drivers), or checking for loose cables.
3. What factors should be considered when replacing a network card?
   Answer: Ensure compatibility with your computer's motherboard slot (PCI, PCIe) and operating system. Choose a card that meets your current and future bandwidth or performance needs.
4. How can you verify that a replacement router is functioning correctly?
   Answer: Check for basic functionality like powering on, connecting devices, and accessing the internet. Run internet speed tests and compare results to your ISP's advertised speeds.
5. What is the difference between replacing hardware and updating software for network troubleshooting?
   Answer: Hardware replacement involves physically swapping out a faulty device like a router or network card. Software updates involve installing newer versions of firmware on network equipment or drivers on your computer to address bugs and improve functionality.
6. What are some benefits of testing replaced network equipment?
   Answer: Testing ensures the replacement functions correctly, resolves the initial network issue, and verifies proper functionality of features like Wi-Fi connectivity.
7. What basic tests can be used to verify network connectivity after replacing equipment?
   Answer: Try a ping test to a specific IP address and see if you get a response. Attempt connecting to the internet with a web browser and verify successful browsing.
8. What does "Network Configuration" refer to?
   Answer: Network configuration involves setting up and managing network devices and software. This includes defining how devices interact, internet connection details, security settings, and wireless network settings (SSID, password).
9. What are some security considerations when configuring a network?
   Answer: Utilize strong encryption (WPA2/WPA3) for your Wi-Fi, configure firewalls to filter incoming traffic, and implement access control measures to limit access to network resources.
10. How can testing network activity be helpful for troubleshooting?
    Answer: Testing can identify issues like slow speeds, high latency (delays), or packet loss. Tools like ping tests, internet speed tests, and network monitoring software can provide valuable insights into network performance.

Task Sheet-4.1: Solve The Problem

Performance Objective: By the end of this task, the trainee should be able to: Troubleshoot network issues and replace faulty hardware equipment if necessary. Test

1. Identify the Network Issue:
   - Describe the symptoms of the network problem (e.g., no internet connectivity, slow speeds, frequent disconnections).
   - Utilize network diagnostics tools like ping tests, traceroute, or network monitoring software to pinpoint the potential source of the issue.

2. Troubleshoot Software Issues:
   - Restart all network devices (router, modem, computer).
   - Update network drivers or firmware on network equipment (if applicable).
   - Verify network cable connections are secure.
   - (Optional for advanced users) Check for configuration errors on network devices.

3. Replacement of Faulty Hardware (if required):

   Before Replacement:
   - Back up configuration settings on the old device (if possible).
   - Ensure compatibility of replacement hardware with your network setup.

   Replacement Process:
   - Power down and disconnect all cables from the faulty device.
   - Physically replace the faulty equipment with the new one.
   - Reconnect cables securely.
   - Power on the new device and any connected devices.

4. **Testing** Replaced **Equipment:**
   - Verify basic functionality (power on, device lights indicate normal operation).
   - Connect devices to the network (wired or wireless).
   - Test internet connectivity by browsing a website.
   - Run a ping test to a known internet address.

5. **Testing Replaced Equipment:**
   - Verify basic functionality (power on, device lights indicate normal operation).
   - Connect devices to the network (wired or wireless).
   - Test internet connectivity by browsing a website.
   - Run a ping test to a known internet address.

6. **Testing Replaced Equipment:**
   - Verify basic functionality (power on, device lights indicate normal operation).
   - Connect devices to the network (wired or wireless).
   - Test internet connectivity by browsing a website.
   - Run a ping test to a known internet address.

Learning Outcome-5: Clean Workplace and Update Document

Assessment Criteria:

1. Tools and equipment are stored as per workplace procedures.
2. Network and computer maintenance and troubleshooting document are updated

Content:

1. Storing Tools and equipment.
2. Updating Network and computer maintenance and troubleshooting document

Resources Required/ Conditions:

The trainees must be provided with the following:

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

Methodologies

1. Lecture/discussion
2. Demonstration/application
3. Presentation
4. Blended delivery methods

Assessment Methods

1. Written test
2. Demonstration
3. Observation with checklist
4. Oral questioning
5. Portfolio

Learning Experience-5: Update Document

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

Learning Steps	Resources specific instructions
1. Student will ask the instructor about updating document	1. Instructor will provide the learning materials "**Clean workplace and update document"**
2. Read the Information sheet/s	2. Information Sheet No: 5 Clean workplace and update document
3. Complete the Self Checks & Check answer sheets.	3. Self-Check/s Self-Check No: 5 Clean workplace and update document Answer key No. 5 Clean workplace and update document
4. Read the Job Sheet and Specification Sheet and perform job	4. Job- Sheet No: 5 Clean workplace and update document Specification Sheet: 5 Clean workplace and update document

Information Sheet-5: Clean Workplace and Update Document

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

5.1 Store Tools and equipment as per workplace procedures.
5.2 Update Network and computer maintenance and troubleshooting document.

5.1 Storing Tools and equipment

Dry and Clean Environment: Store your tools and equipment in a dry, clean area to prevent rust, corrosion, or mold growth. Avoid damp basements, garages with leaky roofs, or areas prone to humidity.

Temperature Control: Extreme temperature fluctuations can damage delicate tools or equipment. Aim for moderate and stable temperatures. Attics or uninsulated sheds might not be ideal storage locations.

Organized and Accessible: Having a designated storage space for each tool or piece of equipment makes them easy to find and prevents clutter. Utilize toolboxes, cabinets, shelves, or pegboards for organized storage.

Specific Storage Techniques:

Metal Tools: Wipe down metal tools with a rag coated in light machine oil to prevent rust. Hang them on pegboards or store them in drawers lined with tool mats to prevent scratches.

Sharp Tools: Store knives, scissors, and other sharp objects in designated sheaths, holders, or locked drawers to prevent accidental injuries.

Power Tools: Store power tools in their original cases (if available) to keep all components together and protected. Disconnect batteries and remove any loose attachments before storage.

Large Equipment: Larger equipment like lawnmowers or bicycles might require specific storage solutions. Consider using floor space efficiently with wall-mounted racks or overhead storage solutions.

Delicate Equipment: For sensitive equipment like electronics or measuring tools, invest in padded cases or protective boxes to prevent damage from bumps or shocks.

Here's a breakdown of the updating procedure for your Network and Computer Maintenance and Troubleshooting Document:

Review and Identify Changes:

Technology Advancements: Research new tools, software, and troubleshooting techniques that have emerged since the previous version of your document.

Evolving Threats: Update information on current security threats and best practices for mitigating them (e.g., new types of malware, phishing scams).

User Feedback: Consider any feedback or suggestions from users who have referred to the document in the past.

5.2 Update Network and computer maintenance and troubleshooting document.

Hardware/Software Updates: Account for changes in operating systems, software updates, or new hardware components that might require updated troubleshooting steps or configuration procedures.

Updating the Document:

Review Existing Content: Carefully examine the existing document to ensure all information remains accurate and relevant.

Incorporate New Information: Integrate the identified changes and updates into the relevant sections of the document.

Maintain Consistency: Ensure the updated document maintains a consistent tone, structure, and level of detail for user clarity.

Version Control: Implement a version control system (e.g., date or version number) to track changes and differentiate between versions of the document.

Self-Check-5: Clean Workplace and Update Document

1. Why is proper storage important for network and computer tools and equipment?
   Answer:

2. What are some key considerations for storing network cables?
   Answer:

3. How often should you update your Network and Computer Maintenance and Troubleshooting Document?
   Answer:

4. What resources can be helpful for updating the Network and Computer Maintenance and Troubleshooting Document?
   Answer:

5. What are some benefits of keeping your Network and Computer Maintenance and Troubleshooting Document updated?
   Answer:

Answer Key-5: Clean Workplace and Update Document

1. Why is proper storage important for network and computer tools and equipment?
   Answer: Proper storage protects your tools and equipment from damage (rust, corrosion, breakage) and extends their lifespan. It also ensures they are organized and easily accessible when needed, promoting efficient work.

2. What are some key considerations for storing network cables?
   Answer: Avoid coiling cables too tightly, which can damage them over time. Store them in labeled containers or hang them on pegboards to prevent tangles.

3. How often should you update your Network and Computer Maintenance and Troubleshooting Document?
   Answer: It's recommended to review the document at least annually, but consider updating it more frequently if there are significant changes in technology, security threats, or user needs.

4. What resources can be helpful for updating the Network and Computer Maintenance and Troubleshooting Document?
   Answer: Utilize websites of reputable tech companies, software vendors, and hardware manufacturers for updated information and troubleshooting guides. Professional IT organizations and publications can also offer valuable insights on best practices.

5. What are some benefits of keeping your Network and Computer Maintenance and Troubleshooting Document updated?
   Answer: An updated document ensures users have access to accurate troubleshooting steps and avoids wasted time on outdated procedures. It also helps users maintain a secure network environment by including information on new security threats and mitigation techniques.

Review Of Competency

Below is yourself assessment rating for module **"Troubleshooting Network"**

SL NO	Assessment of performance Criteria	Yes	No
1.	Troubleshoot methodology is interpreted		
2.	Network tools and utilities for troubleshooting are interpreted		
3.	Network design, support and maintenance documents are reviewed		
4.	Computer manuals and maintenance documents are reviewed		
5.	Network Fault is identified		
6.	Faulty hardware or software component are detected.		
7.	The problem scenarios are observed		
8.	Problems are detected using diagnostic tools		
9.	Appropriate person (if required) is consulted and solution is identified		
10.	Types of solutions are identified		
11.	Replacement of faulty hardware equipment is performed if required		
12.	Replaced equipment is tested		
13.	Configuration is performed as per solution requirement		
14.	Network activity is tested.		
15.	Tools and equipment are stored as per workplace procedures.		
16.	Network and computer maintenance and troubleshooting document are updated		

I now feel ready to undertake my formal competency assessment.

Signed:

Date:

Development of CBLM

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

SL No.	Name & Address	Designation	Contact Number
1	Anisuzzaman Tuheen	Writer	01714-422225
2	Md. Faruk	Editor	01849-153713
3	Engr. Md. Zuwel Parves	Co-Ordinator	01737-278906
4	Md. Saif Uddin	Reviewer	01723-004419

Reference

1. https://gemini.google.com/
2. https://chat.openai.com/