የሥራና ክህሎት ሚኒስቴር
Ministry of Labor and Skills

HARDWARE AND NETWORKING SERVICE LEVEL- IV

Based on November, 2023Version-II

MODULE TITLE: - Provide Network System Administration

MODULE CODE: EIS HNS4 M04 1123

NOMINAL DURATION: 45 Hours

Prepared by: - Ministry of Labor and Skill

November 2023
Addis Ababa, Ethiopia

Table of Contents

Acknowledgment

Ministry of Labor and Skills wish to extend thanks and appreciation to the many representatives of TVET instructors and respective industry experts who donated their time and expertise to the development of this Teaching, Training and Learning Materials (TTLM).

Acronym

5G:-	Fifth-Generation
ACLs:-	Access Control Lists
ATP:-	Advanced Threat Protection
DPI:-	Deep Packet Inspection
DRP:-	Disaster Recovery Plan
IEEE:-	Institute Of Electrical And Electronics Engineers
PoE :-	Power Over Ethernet
QoS:-	Quality Of Service
SLA:-	Service Level Agreement
SNMP:-	Simple Network Management Protocol
SQL:-	Standard Query Language
SSDs:-	Solid-State Drives
VLANs:-	Virtual Local Area Networks
Wi-Fi:-	Wireless Fidelity
WSUS:-	Windows Server Update Services

Introduction to module

This module defines the competence required to design and implement an infrastructure for internet services. Network systems administration refers to the management and maintenance of computer networks within an organization. It involves the configuration, monitoring, and troubleshooting of network infrastructure to ensure its optimal performance, security, and availability.

Disaster recovery for a network involves implementing strategies and procedures to restore network functionality and data in the event of a major disruption or catastrophic event.

This module is designed to meet the industry requirement under the **Hardware and Networking Service** occupational standard, particularly for the unit of competency: **Providing Network System Administration** This module covers the units:

- Client access and security
- Disseminate disaster recovery plan
- Monitor network performance
- Migrate to New Technology

This guide will also assist you to attain the learning outcome stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Understand network system administration
- Explain accounts and files privilege
- Determine access privileges
- Maintain System integrity and security
- Understand concepts of disaster recovery plan
- Understand Backup and restore
- Analyze and respond information
- Monitor software and files
- Monitoring performance indicators
- Upgrade technology skills
- Identify upgraded equipment.
- Use new or upgrade equipment

Module Instruction

For effective use this modules trainees are expected to follow the following module instruction:

1. Read the specific objectives of this Learning Guide.
2. Read the information that this module contain.
3. Complete the Self-check.
4. Submit your accomplished Self-check.
5. Do the Operations which in the module.
6. Do the LAP test

Unit One: Client access and security

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Overview of Network System Administration
- Accounts and files privilege
- Determining access privileges
- Maintaining System integrity and security

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Understand Network System Administration
- Explain Accounts and files privilege
- Determine access privileges
- Maintain System integrity and security

1.1. Basic concept of network system administration

Network system administration involves managing and maintaining the operation, security, and performance of a network infrastructure. It encompasses various tasks and responsibilities to ensure the network functions reliably and efficiently. Network administration aims to manage, monitor, maintain, secure, and service an organization's network. However, the specific tasks and procedures may vary depending on the size and type of an organization.

Network administration primarily consists of, but is not limited to, network monitoring, network management, and maintaining network quality and security.

Network monitoring is essential to monitor unusual traffic patterns, the health of the network infrastructure, and devices connected to the network. It helps detect abnormal activity, network issues, or excessive bandwidth consumption early on and take preventative and remedial actions to uphold the network quality and security. Network management encompasses multiple administrative functions, including network planning, implementation, and configuration. It involves:

- Re-planning the network based on changing organizational requirements
- Implementing the network for maximum efficiency
- Configuring various networking and security protocols
- Applying security patches and updating the firmware of the networking infrastructure, such as routers, hubs, switches, and firewalls
- Assessing the network for weaknesses
- Evaluating quality and capacity to increase or decrease network capacity and manage resource wastage

Network security employs various techniques to ensure a network is secure. For example, it uses multiple tools such as firewalls, intrusion detection or prevention systems, and anti-malware software to prevent or detect malicious activity in the network.

Network administration goals

Network administration aims to ensure a reliable, secure network conducive to business operations. Generally, network administration goals include:

- Maintain a resilient, high-quality network
- Plan and improve network capacity to enable seamless network access and operations

- Leverage networking tools for network systems administration and better network administration control
- Track and document relevant changes
- Evaluate possible risks and orchestrate effective mitigations
- Prevent activities compromising or using the network as an attack vector
- Identify and mitigate intrusions to avoid security breaches

1.1.1 Network administration key areas

Networks administration consists of five key areas:

1. **Fault management**: - Monitors the network infrastructure to identify and address issues potentially affecting the network. It uses standard protocols such as Simple Network Management Protocol (SNMP) to monitor network infrastructure.

2. **Configuration management**: - Tracks configuration and related changes of network components, including switches, firewalls, hubs, and routers. As unplanned changes can affect the network drastically and potentially cause downtime, it is essential to streamline, track, and manage configuration changes.

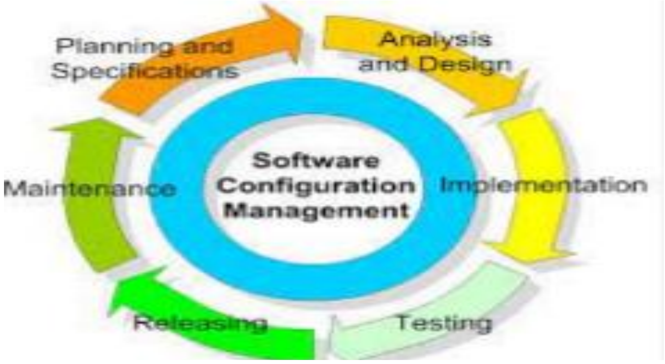

Planning and Specifications
Analysis and Design
Software Configuration Management
Maintenance
Implementation
Releasing
Testing

Figure 1. 1 Configuration management steps

3. **Account management**: - Tracks network utilization to bill and estimate the usage of various departments of an organization. In smaller organizations, billing may be irrelevant. However, monitoring utilization helps spot specific trends and inefficiencies.

4. **Performance management**: - Focuses on maintaining service levels needed for efficient operations. It collects various metrics and analytical data to continually assess network performance, including response times, packet loss, and link utilization.

5. **Security management**:- Aims to ensure only authorized activity and authenticated devices and users can access the network. It employs several disciplines such as threat management,

intrusion detection, and firewall management. It also collects and analyzes relevant network information to detect and block malicious or suspicious activity.

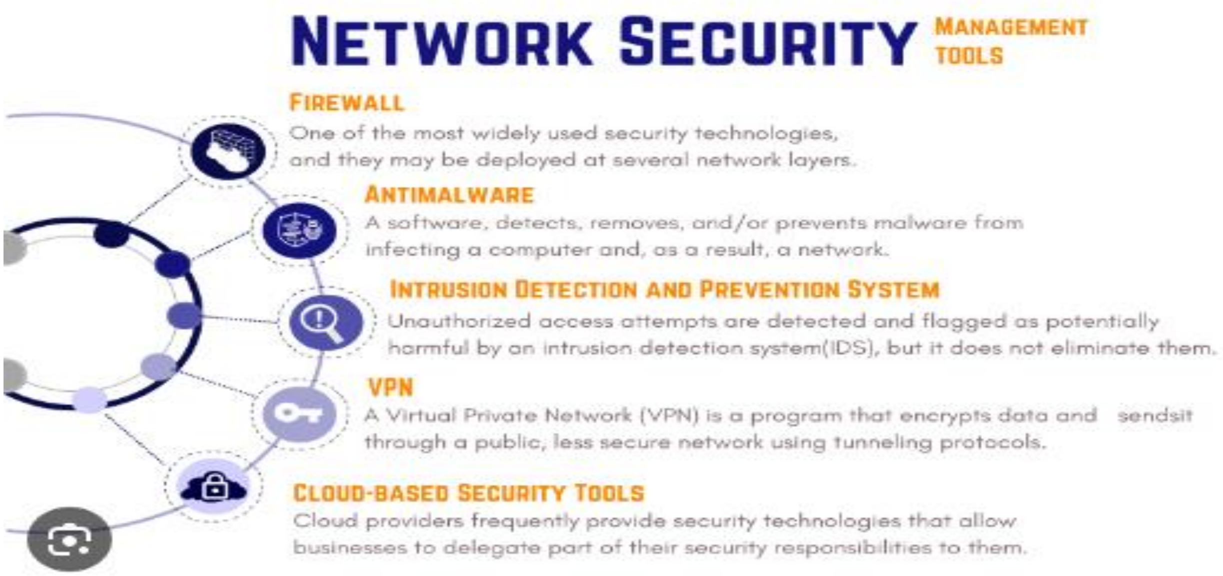

NETWORK SECURITY
MANAGEMENT TOOLS
FIREWALL
One of the most widely used security technologies, and they may be deployed at several network layers.
ANTIMALWARE
A software, detects, removes, and/or prevents malware from infecting a computer and, as a result, a network.
INTRUSION DETECTION AND PREVENTION SYSTEM
Unauthorized access attempts are detected and flagged as potentially harmful by an intrusion detection system(IDS), but it does not eliminate them.
VPN
A Virtual Private Network (VPN) is a program that encrypts data and sendsit through a public, less secure network using tunneling protocols.
CLOUD-BASED SECURITY TOOLS
Cloud providers frequently provide security technologies that allow businesses to delegate part of their security responsibilities to them.

Figure 1. 2 Network security management

1.1.2. Network administrator tools and software

Network administrators use various networking software and tools to optimally perform network operations, including compliance, automation, configuration, real-time monitoring and alerting, network inventory management, performance management, and vulnerability assessment.

Due to the increasing number of networking components in an organization’s network, it becomes difficult to manage the network manually, which is also error-prone. By implementing basic and advanced tools, network administrators can automate several tasks and focus on more value-adding tasks needing their attention.

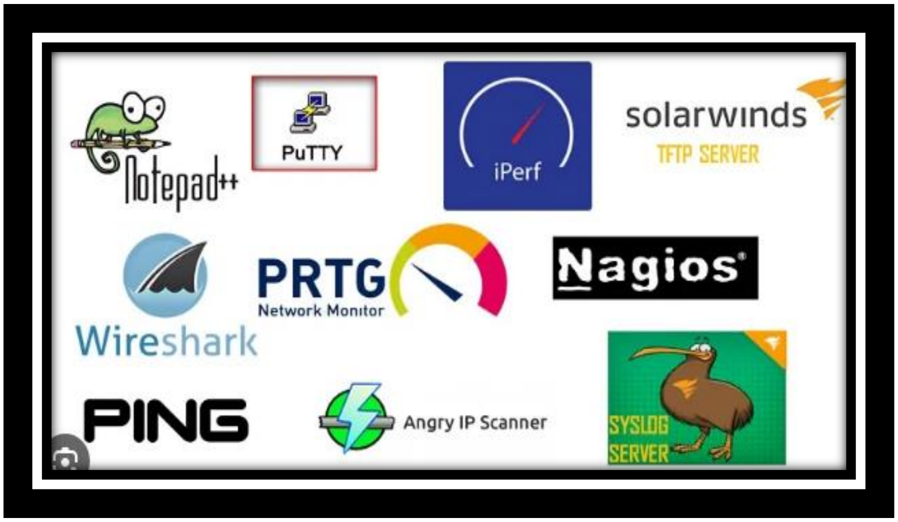


Figure 1. 3 Network administrator tools

1.1.3. Responsibilities of network administrator

A network administrator focuses on the day-to-day aspects of managing and maintaining a network. The roles and responsibilities of network administrators are outlined below.

- Is responsible for managing and maintaining the network in real time
- Ensures the network is secure by blocking suspicious activity and mitigating the risk of security breaches
- Implements security programs based on hardware and software
- Manages on-site networking servers responsible for business operations
- Ensures network integrity and resilience to maintain service levels
- Tests the network to uncover weaknesses and mitigate them
- Monitors and tracks utilization
- Applies utilization, authentication, and authorization policies to maintain the quality and security of the network

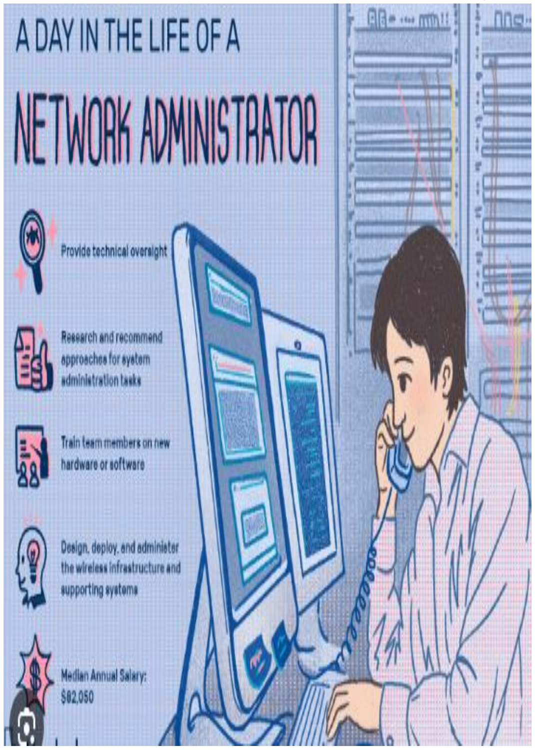

A DAY IN THE LIFE OF A
NETWORK ADMINISTRATOR
Provide technical oversight
Research and recommend approaches for system administration tasks
Train team members on new hardware or software
Design, deploy, and administer the wireless infrastructure and supporting systems
Median Annual Salary: $82,050

Figure 1. 4 Responsibilities of network administrator

1.2. Accounts and files privilege

Applying account and file privileges involves configuring access controls to ensure that only authorized users can access specific accounts and files. Here are some steps to apply account and file privileges effectively:

1. **User Account Creation:** Create user accounts for individuals who require access to the system or files. Each user should have a unique username and password combination.
2. **User Groups:** Group users based on their roles and responsibilities. This simplifies privilege management by assigning privileges to groups rather than individual users.
3. **Principle of Least Privilege:** Follow the principle of least privilege, which means granting users the minimum level of privileges required to perform their job functions. Avoid giving excessive permissions that could potentially lead to security vulnerabilities.
4. **Access Control Lists (ACLs):** Utilize access control lists to define access permissions for files and directories.
5. **File Ownership**: Assign appropriate file ownership to ensure accountability and control. Only authorized users or groups should own sensitive files or directories.
6. **Regular Access Reviews**: Perform regular access reviews to identify and remove unnecessary or outdated privileges. This helps maintain a clean and secure access control environment.
7. **Password Policies:** Enforce strong password policies to protect user accounts. Require users to create passwords that meet complexity requirements (e.g., minimum length, a combination of letters, numbers, and special characters) and encourage regular password updates.
8. **Regular Auditing and Monitoring:** Implement logging and monitoring mechanisms to track user activities, access attempts, and changes to account and file privileges. Regularly review logs and audit trails to identify suspicious behavior and potential security breaches.
9. **Training and Awareness**: Provide training and awareness programs to educate users about the importance of account and file privilege management. Users should understand their responsibilities in safeguarding sensitive data and be aware of best practices for access control.

1.3. Determine access privileges

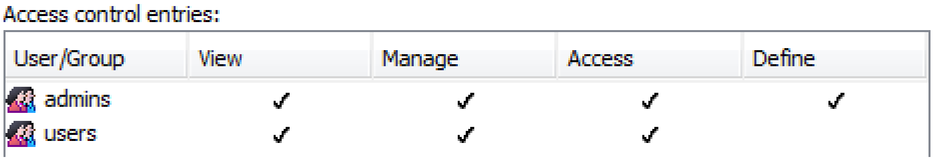
When a user tries to perform a privileged operation, the system checks the user's access token to determine whether the user holds the necessary privileges1. If the user holds the necessary privileges, the system checks whether the privileges are enabled.

Access privileges can be viewed and modified in the Operations Server console. The following primary roles can be subdivided into additional categories if necessary to match your organization:

- **System Administrator:** Responsible for configuring and maintaining the Operations Center environment, including:
  - ➢ Defining adapter connections to key components such as databases and remote management systems
  - ➢ Defining service model hierarchies, automations, and operations,
  - ➢ Defining custom classes, behavior models, and property pages
  - ➢ Defining calendars, schedules, and jobs
  - ➢ Creating custom SQL Views
  - ➢ Creating Layout views
  - ➢ Determining which users should have access to specific element hierarchies
- **Security Manager:** Responsible for enforcing company security policies regarding user access to the system, user identification and authorization, password rules, access privileges, and so on. Also responsible for managing users and groups and enforcing password policies and rules.
- **End Users:** Responsible for analyzing and reporting information collected in Operations Center from various sources. You should organize users who have similar authorization to access data into groups, such as by job function or security clearance level.

Table 1. 1 Access Control Privileges

Access Privilege	**Description**
View	The user can view elements, as well as their alarms and properties, and relationships to other elements that the user can view. Note for T/EC adapters: Any user with the View permission can suppress a T/EC alarm; however, this user cannot acknowledge or close the alarm.

<table>
<tr><td>Manage</td><td>The user can perform nonintrusive actions (such as Ping or TraceRoute) as well as update element information (such as custom properties).
Note for T/EC adapters: Any user with the Manage permission can acknowledge or close a T/EC alarm.</td></tr>
<tr><td>Access</td><td>The user can access remote managed elements by using “connect to” operations with adapters that support cut-through telnet such as the Event Manager, OpenView, and Netcool*. An example operation is using the Console capability in the <b>Elements</b> hierarchy.</td></tr>
<tr><td>Define</td><td>The user can perform administrative tasks such as adding scripts, sites, and service model elements, as well as creating, deleting, and changing the definition of adapters, service models and SLAs in Operations Center.</td></tr>
<tr><td>Undefined</td><td>Not defining access privileges avoids conflicts. For example, the two groups in the following figure have the following permissions at the top (root) Access Control level:

Access control entries:
<table><tr><th>User/Group</th><th>View</th><th>Manage</th><th>Access</th><th>Define</th></tr><tr><td>admins</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td>users</td><td>✓</td><td>✓</td><td>✓</td><td></td></tr></table>
The admins group has Define privileges explicitly defined. The users group has undefined Define privileges. Therefore, a member of both groups has Define privileges.</td></tr>
</table>

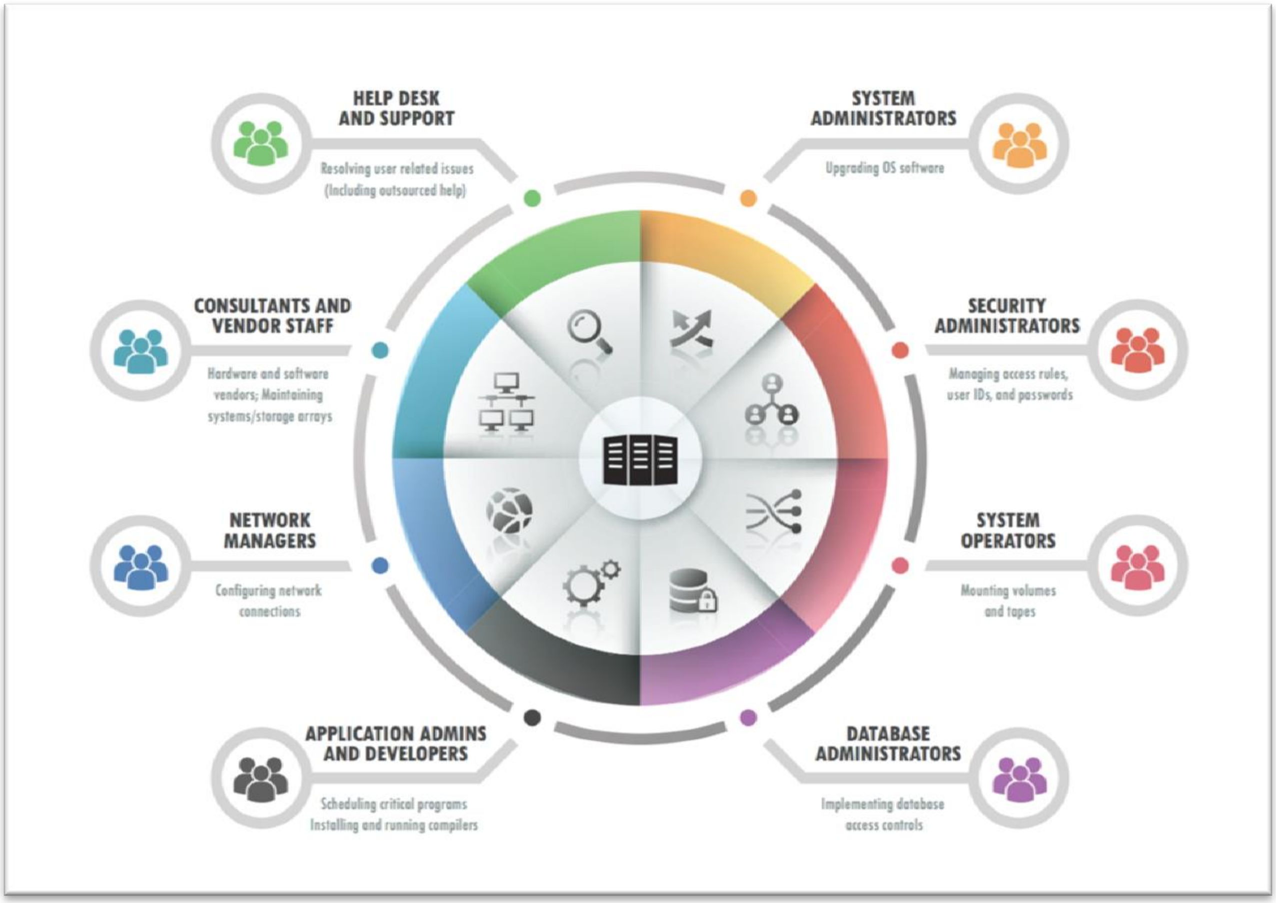

HELP DESK AND SUPPORT
Resolving user related issues (Including outsourced help)
SYSTEM ADMINISTRATORS
Upgrading OS software
CONSULTANTS AND VENDOR STAFF
Hardware and software vendors; Maintaining systems/storage arrays
SECURITY ADMINISTRATORS
Managing access rules, user IDs, and passwords
NETWORK MANAGERS
Configuring network connections
SYSTEM OPERATORS
Mounting volumes and tapes
APPLICATION ADMINS AND DEVELOPERS
Scheduling critical programs Installing and running compilers
DATABASE ADMINISTRATORS
Implementing database access controls

Figure 1. 5 Determining access privileges

1.4. Maintain System integrity and security

1.4.1. System integrity

System integrity refers to the state of a computer system or network being complete, accurate, and secure. It involves ensuring that the system operates as intended, without unauthorized modifications, corruption, or compromise. System integrity encompasses various aspects, including data integrity, configuration integrity, and overall security.

Data Integrity: Data integrity refers to the accuracy, consistency, and reliability of data stored within a system. It ensures that data remains unchanged and uncorrupted throughout its lifecycle. Measures such as data validation, checksums, and error detection techniques are used to maintain data integrity.

Configuration Integrity: Configuration integrity involves verifying and maintaining the integrity of system configurations, settings, and parameters.

It ensures that the system is properly configured according to established standards and best practices. Unauthorized changes to system configurations can introduce vulnerabilities or disrupt system functionality.

Software Integrity: Software integrity focuses on ensuring that software applications and programs are free from defects, vulnerabilities, or unauthorized modifications. It involves implementing secure coding practices, performing regular software updates and patching, and conducting code reviews and software testing to identify and fix vulnerabilities.

Hardware Integrity: Hardware integrity refers to the assurance that computer hardware components are functioning correctly and have not been tampered with or compromised. It involves validating the authenticity and integrity of hardware components, monitoring for hardware failures, and protecting against unauthorized modifications or hardware-based attacks.

System Security: System security is a critical aspect of system integrity. It involves protecting the system against unauthorized access, data breaches, malware, and other security threats. This includes implementing access controls, strong authentication mechanisms, encryption, intrusion detection and prevention systems, and ongoing monitoring and auditing of system activities.

Maintaining system integrity is essential to ensure the reliability, availability, and confidentiality of information, as well as the proper functioning of computer systems and networks. It requires a combination of technical controls, security measures, and proactive monitoring to prevent unauthorized changes, detect potential vulnerabilities, and respond promptly to security incidents.

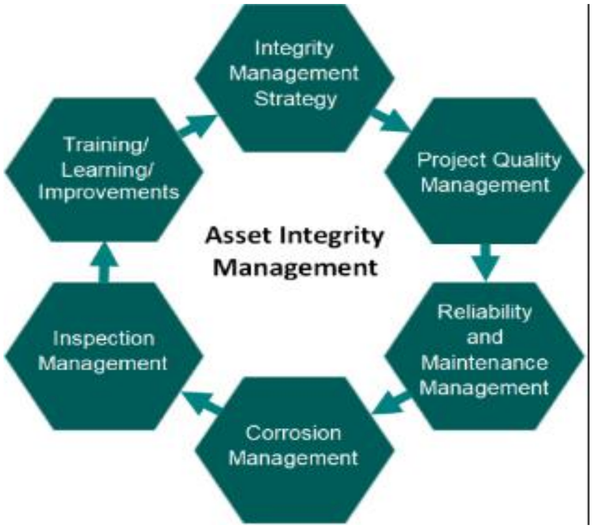

Integrity Management Strategy
Project Quality Management
Reliability and Maintenance Management
Corrosion Management
Inspection Management
Training/ Learning/ Improvements
Asset Integrity Management

Figure 1. 6 System integrity management

1.4.2. System security

The security of a computer system is a crucial task. It is a process of ensuring the confidentiality and integrity of the OS. Security is one of most important as well as the major task in order to keep all the threats or other malicious tasks or attacks or program away from the computer's software system.

A system is said to be secure if its resources are used and accessed as intended under all the circumstances, but no system can guarantee absolute security from several of various malicious threats and unauthorized access.

The security of a system can be threatened via two violations:

Threat: A program that has the potential to cause serious damage to the system.

Attack: An attempt to break security and make unauthorized use of an asset.

Security violations affecting the system can be categorized as malicious and accidental threats. Malicious threats, as the name suggests are a kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors and security breaches. Accidental Threats, on the other hand, are comparatively easier to be protected against.

Example: Denial of Service DDoS attack.

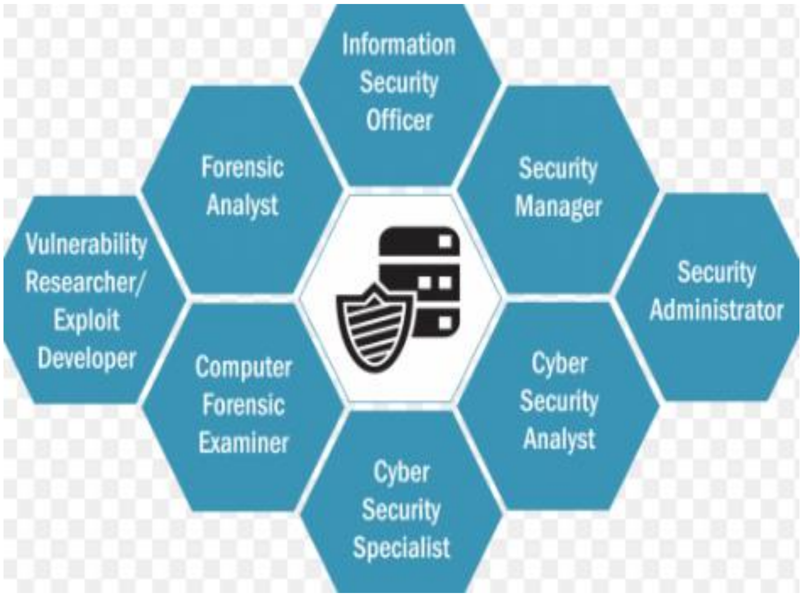

Information Security Officer
Forensic Analyst
Security Manager
Vulnerability Researcher/ Exploit Developer
Security Administrator
Computer Forensic Examiner
Cyber Security Analyst
Cyber Security Specialist

Figure 1. 7 Network security

Self-check - 1

Part I:- Say **True** if the given statement is correct else say **False**

_______1. When determining access privileges in a network system, factors such as user's physical location and job title should be considered.

_______2. Granting all users the highest level of access possible is a recommended approach for determining access privileges.

_______3. Storing sensitive data in plain text files is a secure practice for maintaining system integrity and security.

Part II: - Select the appropriate answer from the given alternative

_______1. When referring to accounts and files privilege in network system administration, what does the term "privilege escalation" mean?

A. Granting additional permissions to a user

B. Revoking all access privileges from a user

C. Assigning a new username to a user

D. Changing the file ownership to a different user

_______2. In the context of determining access privileges, what is the principle of "least privilege"?

A. Granting users the highest level of access possible

B. Assigning access privileges based on job titles

C. Limiting user access to only the resources necessary for their tasks

D. Providing all users with equal access privileges

_______3. Which of the following is an example of a multifactor authentication method for determining access privileges?

A. Using a username and password combination

B. Requiring a fingerprint scan and a password

C. Granting access based solely on IP address

D. Sharing a single password among multiple users

_______4. What is the purpose of implementing intrusion detection systems (IDS) in network system administration?

A. To prevent unauthorized access to the system

B. To monitor network traffic and detect potential security breaches

C. To encrypt sensitive data during transmission

D. To manage user accounts and access privileges

________5. Which of the following is an example of a security measure for maintaining system integrity and security?

A. Regularly updating antivirus software

B. Sharing passwords with coworkers for convenience

C. Allowing unrestricted remote access to the system

D. Storing sensitive data in plain text files

Part II: - Give short answer

1. What are the responsibilities of system administrator?
2. Demonstrate the difference between system security and system integrity with example?
3. List and explain Network administration key areas?

Operation sheet 1.1

Operation title: - Accounts and files privilege

Purpose:- Protect and give privilege for user account and computer files
Instruction: Use the figure below, given equipment and task. You have given 45 Minute for the task and you are expected to complete tasks.

- **Tools and requirement:,-** Computes

Task 1:- Give full access privilege for user

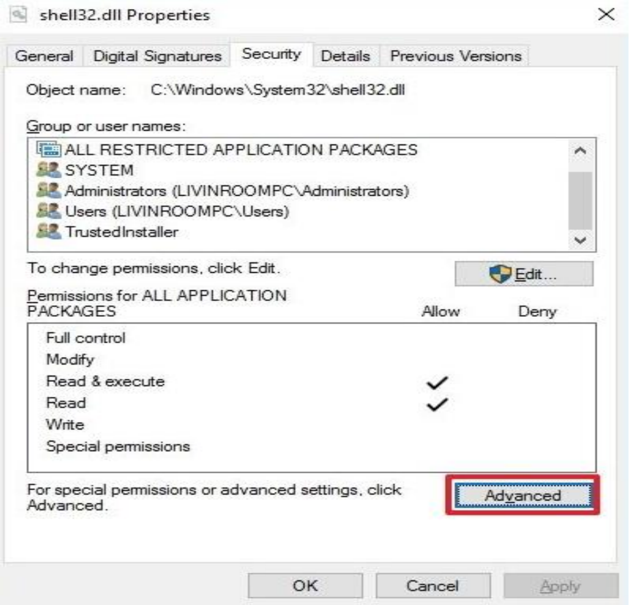
Step 1:- Open **File Explorer**.

Step 2:- Browse and find the file or folder you want to have full access.

Step3:- Right-click it, and select **Properties**.

Step 4:- Click the **Security** tab to access the NTFS permissions.

Step 5:- Click the **Advanced** button.



Object name: C:\Windows\System32\shell32.dll

Group or user names:

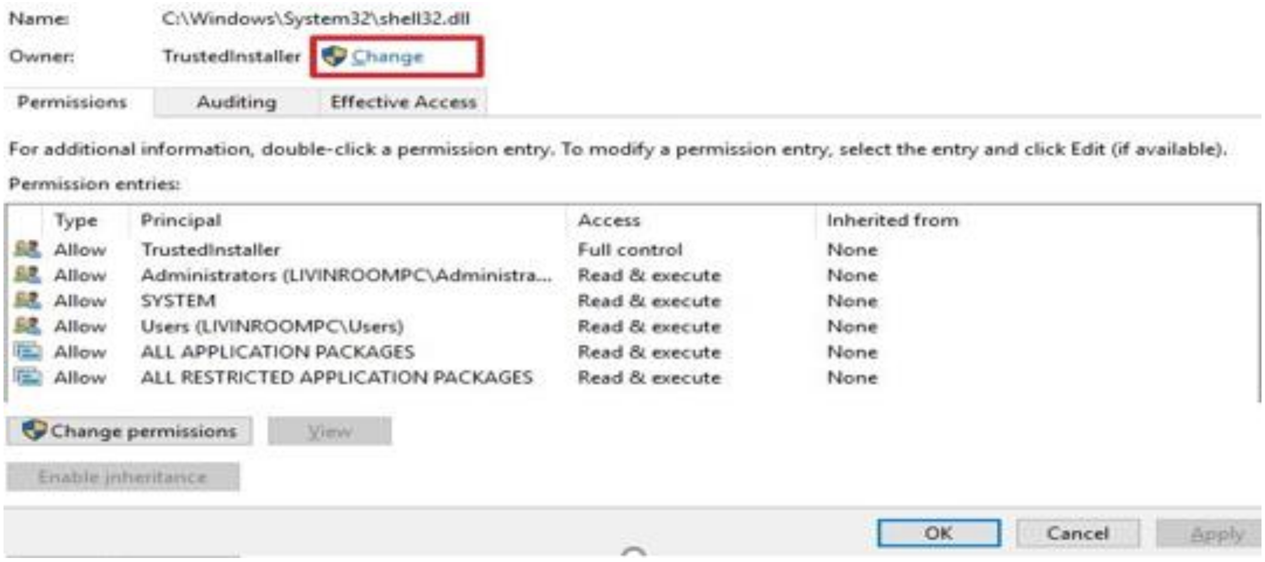
ALL RESTRICTED APPLICATION PACKAGES
SYSTEM
Administrators (LIVINROOMPC\Administrators)
Users (LIVINROOMPC\Users)
TrustedInstaller

To change permissions, click Edit.

Permissions for ALL APPLICATION PACKAGES	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.

Step 6:- On the "Advanced Security Settings" page, you need to click the **Change** link, in the Owner's field.



Name: C:\Windows\System32\shell32.dll

Owner: TrustedInstaller Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

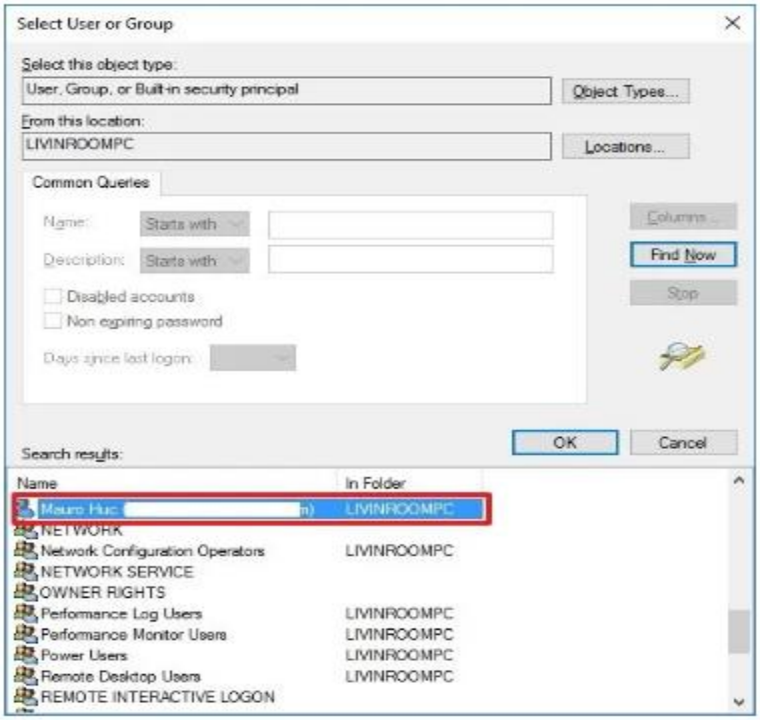
Permission entries:

Type	Principal	Access	Inherited from
Allow	TrustedInstaller	Full control	None
Allow	Administrators (LIVINROOMPC\Administra...	Read & execute	None
Allow	SYSTEM	Read & execute	None
Allow	Users (LIVINROOMPC\Users)	Read & execute	None
Allow	ALL APPLICATION PACKAGES	Read & execute	None
Allow	ALL RESTRICTED APPLICATION PACKAGES	Read & execute	None

Step 7:- Click the **Advanced** button.

Step 8:- On the "Select User or Group" page, click the **Find Now** button.

Step 9:- From the search result, select your user account, and click **OK**.



Select User or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
LIVINROOMPC

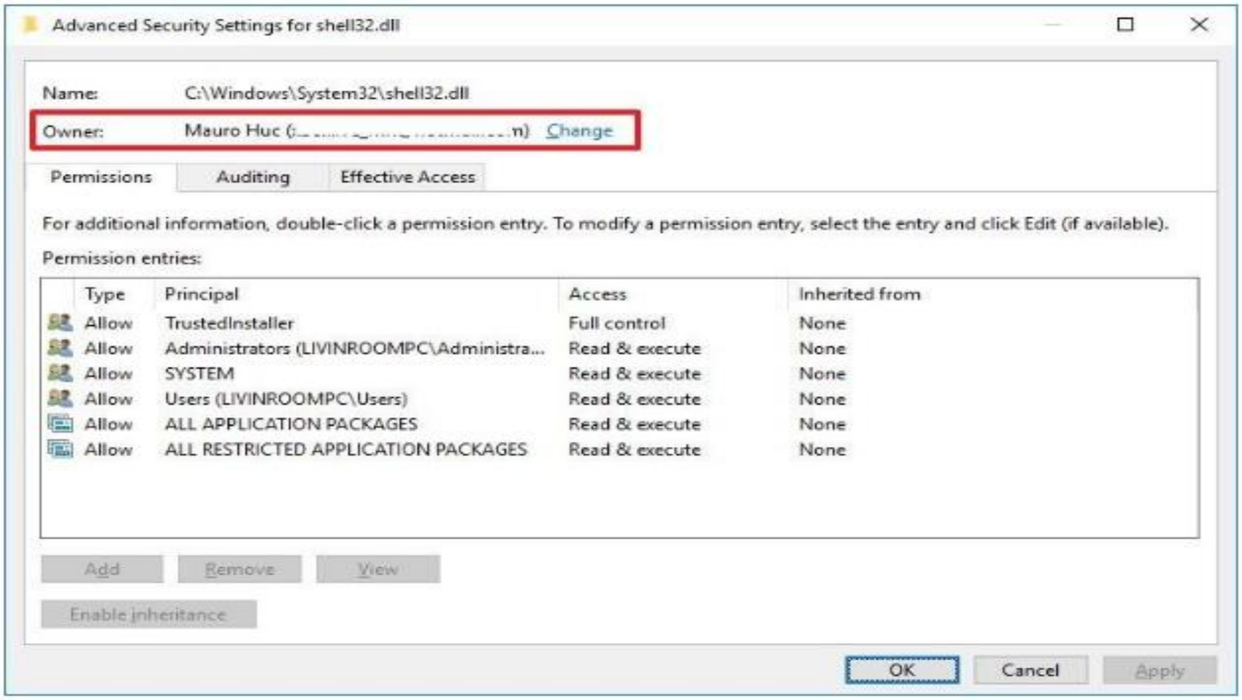
Search results:

Name	In Folder
Mauro Huc [redacted] n)	LIVINROOMPC
NETWORK	
Network Configuration Operators	LIVINROOMPC
NETWORK SERVICE	
OWNER RIGHTS	
Performance Log Users	LIVINROOMPC
Performance Monitor Users	LIVINROOMPC
Power Users	LIVINROOMPC
Remote Desktop Users	LIVINROOMPC
REMOTE INTERACTIVE LOGON	

Step 10:- On the "Select User or Group" page, click **OK**.

Step 11:-Click **Apply**.

Step 12:- Click **OK**.



Name: C:\Windows\System32\shell32.dll

Owner: Mauro Huc ([redacted]n) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	TrustedInstaller	Full control	None
Allow	Administrators (LIVINROOMPC\Administra...	Read & execute	None
Allow	SYSTEM	Read & execute	None
Allow	Users (LIVINROOMPC\Users)	Read & execute	None
Allow	ALL APPLICATION PACKAGES	Read & execute	None
Allow	ALL RESTRICTED APPLICATION PACKAGES	Read & execute	None

Step 13:- Click **OK** again.

Step 14:- Click **OK** one more time to complete this task.

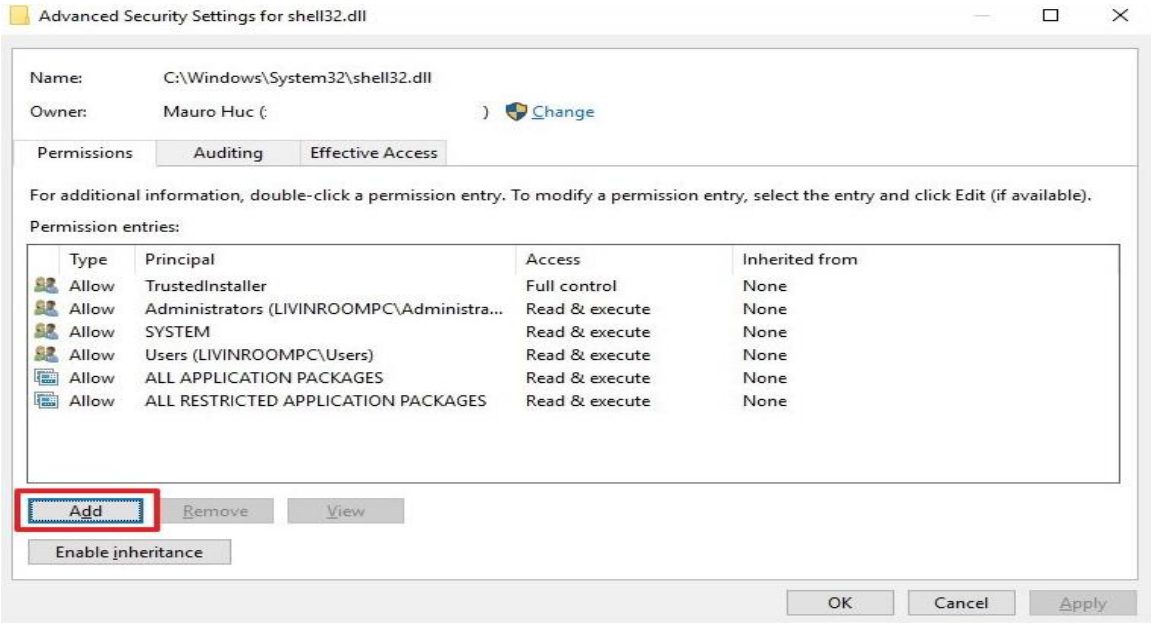
Task 2:- Replace ownership on sub containers and object

Step 1:- Right-click the file or folder and select **Properties**.

Step 2:- Click the **Security** tab to access the NTFS permissions.

Step 3:- Click the **Advanced** button.

Step 4:- Under the Permissions tab, click **Add**.



Name: C:\Windows\System32\shell32.dll

Owner: Mauro Huc ( ) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

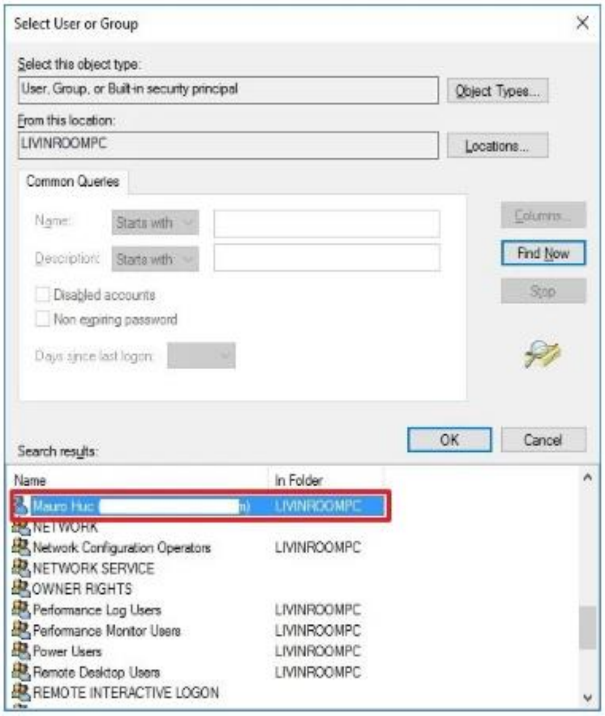
Type	Principal	Access	Inherited from
Allow	TrustedInstaller	Full control	None
Allow	Administrators (LIVINROOMPC\Administra...	Read & execute	None
Allow	SYSTEM	Read & execute	None
Allow	Users (LIVINROOMPC\Users)	Read & execute	None
Allow	ALL APPLICATION PACKAGES	Read & execute	None
Allow	ALL RESTRICTED APPLICATION PACKAGES	Read & execute	None

Step 5:- Click **Select a principal** to add your user account.

Step 6:- On the "Select User or Group" page, click the **Find Now** button.

Step 7:- From the search result, select your user account, and click **OK**.

Step 8:- On the "Select User or Group" page, click **OK**.



Select User or Group

Select this object type: User, Group, or Built-in security principal

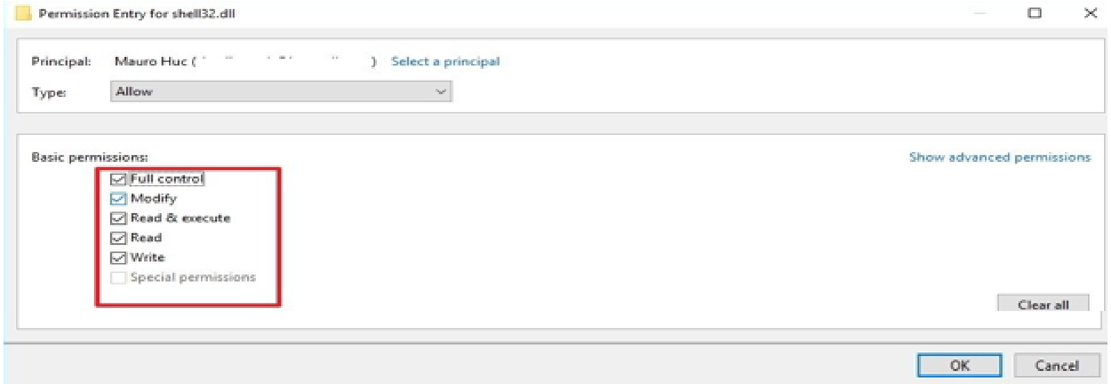
From this location: LIVINROOMPC

Search results:

Name	In Folder
Mauro Huc [redacted]	LIVINROOMPC
NETWORK	
Network Configuration Operators	LIVINROOMPC
NETWORK SERVICE	
OWNER RIGHTS	
Performance Log Users	LIVINROOMPC
Performance Monitor Users	LIVINROOMPC
Power Users	LIVINROOMPC
Remote Desktop Users	LIVINROOMPC
REMOTE INTERACTIVE LOGON	

Step 10:-On "Permission Entry", check the **Full control** option.

Step 11:-Click **OK**



Permission Entry for shell32.dll

Principal: Mauro Huc ([redacted]) Select a principal

Type: Allow

Basic permissions:

☑ Full control
☑ Modify
☑ Read & execute
☑ Read
☑ Write
□ Special permissions

Step 12:- Click **OK**.

Step 13:- Click **Apply**.

Step 14:- Click **OK**.

Step 15:- Click **OK** to close the file or folder properties to complete the task.

LAP Test

Task 1. Create one administrator account and standard account in one computer

Task 2. On the above administrator account on local desk C:/ create one folder called user privilege

Task 3. Give full access privilege for the above created standard account

Unit Two: Disseminate disaster recovery plan

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Basic concepts of disaster recovery plan
- Backup and restore

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Basic concepts of disaster recovery plan
- Backup and restore

2.1. Basic concepts of disaster recovery plan

A Disaster Recovery Plan (DRP) is a structured approach to responding to and recovering from events that can cause data loss, system downtime, and other disruptions to normal business operations. Modern organizations have to operate on a 24/7 basis in order to stay competitive in the market. It is important to create a disaster recovery (DR) plan so as to ensure that your business can continue to operate even during a DR event. However, when designing a DR plan, many businesses overlook the importance of network disaster recovery. In this blog post, we will discuss what network disaster recovery planning entails and how to securely protect your organization against network failures.

A network disaster recovery plan includes a set of procedures required to effectively respond to a disaster that affects a network and causes its disruption. Network disaster recovery planning generally entails:

- Listing the steps which should be undertaken in order to restore network connectivity
- Identifying people responsible for conducting network disaster recovery
- Assessing possible consequences of a network failure
- Determining the best strategies to mitigate them

The main purpose of network disaster recovery is to ensure that business services can be delivered to customers despite a disruption in network connectivity. However, disasters come in different forms and sizes, which makes it hard to predict what their impact would be, which network components would be affected, and how many resources would be required to restore network connectivity.

Possible Causes of Network Failures

Network services are required for ensuring an uninterrupted flow of communications and data transfer within your IT infrastructure. Various factors can lead to network failure. These include:

- **Hardware failure**. Network equipment such as routers, switches, modems, gateways, or any other device can fail and, as a result, affect the performance of all other devices connected to them.

- **Cascading failure**. A single network consists of multiple routers, nodes, or switches. One of those network components might become overloaded and stop working, which can trigger a cascade of failures within a single network.
- **Issues with the internet connection**. Failure to set up an internet connection can cause problems with network connectivity and interrupt data transfer.
- **Human errors**. Sometimes, network connectivity problems might be the result of mistakes made by employees when working with network equipment or manually configuring network components.
- **Network attacks**. Network services can get disrupted after a cyber-attack, whose aim is to prevent the organization from delivering its services, forcing it to shut down.
- **Natural or man-made disaster**. Disasters of any type can significantly damage or even destroy your production center and virtual infrastructure, thus causing significant business losses.

Figure 2. 1 Tips for Disaster Recovery Planning

2.2. Backup and restore

2.2.1. Backup for disaster recovery

Backup is a crucial element of disaster recovery, providing a means to safeguard critical data, applications, and systems in case of unforeseen events. It involves creating duplicate copies of essential information and storing them on separate devices or off-site locations. These backups are performed regularly to capture the most up-to-date data and ensure its availability for recovery purposes.

In the event of a disaster or data loss, such as hardware failures, natural disasters, cyberattacks, or accidental deletions, the backups serve as a reliable source for restoring the affected systems. By having comprehensive backups, organizations can minimize downtime and mitigate the potential loss of data, enabling them to recover quickly and resume normal operations. Backup strategies often include different levels of redundancy, encryption, and verification processes to ensure the integrity and security of the stored information.

There are several types of backups that can be employed, each offering different levels of data protection and recovery options. Some common types of backups include:

1. **Full Backup:** A full backup involves creating a complete copy of all data and files in a system or storage device. It captures all data, regardless of whether it has changed since the last backup. Full backups are comprehensive but can be time-consuming and require significant storage space.

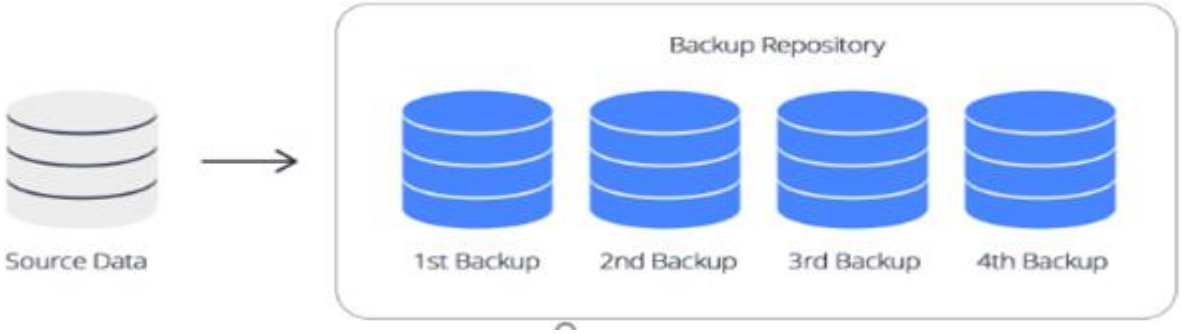


Figure 2. 2 Full Backup

2. **Incremental Backup:** Incremental backups only capture and store changes made since the last backup, whether it was a full or incremental backup. This approach is more efficient in terms of time and storage space, as it only backs up the modified or new data. However, recovery from incremental backups may require multiple backup sets to be restored.

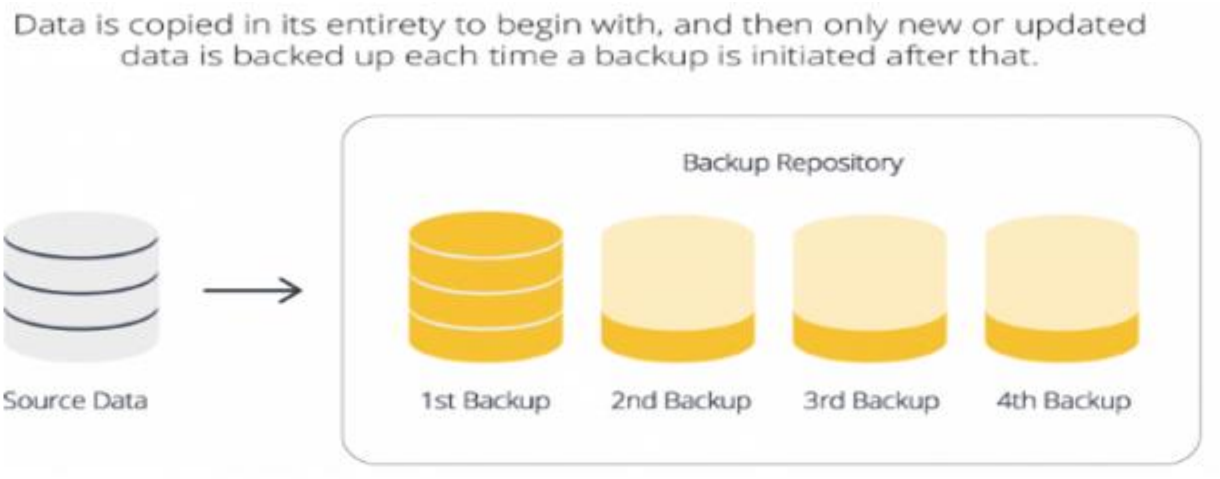

Data is copied in its entirety to begin with, and then only new or updated data is backed up each time a backup is initiated after that.
Backup Repository
Source Data
1st Backup
2nd Backup
3rd Backup
4th Backup

Figure 2. 3 Incremental Backup

3. **Differential Backup:** Differential backups capture all changes made since the last full backup. Unlike incremental backups, which only include changes since the last backup (whether full or incremental), differential backups include changes since the last full backup. This results in faster recovery compared to incremental backups, as only the last full backup and the differential backup need to be restored.

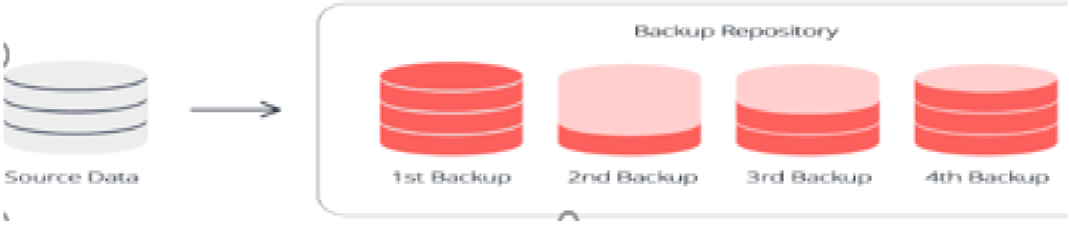
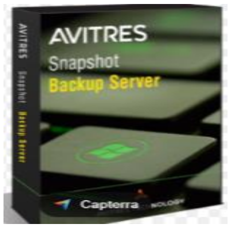


Figure 2. 4 Differential Backup

4. **Mirror Backup:** A mirror backup creates an exact replica of the source data or system. It involves copying all files and directories to a separate storage device or location. Mirror backups provide a straightforward recovery process, as the backup is a direct copy of the original data. However, they can consume significant storage space and may not offer versioning or point-in-time recovery capabilities.

5. **Snapshot Backup:** Snapshot backups capture the state of a system or data at a specific point in time. Instead of copying all data, snapshot backups store the differences or changes made since the



previous snapshot. This allows for fast and efficient backups and provides the ability to restore data to specific points in time.

6. **Cloud Backup:** Cloud backup involves storing data backups in off-site cloud storage. It offers the advantage of scalability, accessibility from anywhere with an internet connection, and built-in redundancy provided by the cloud service provider. Cloud backups can be performed using various backup methods, such as full, incremental, or snapshot backups.

The choice of backup type depends on factors such as the data volume, frequency of changes, recovery requirements, available storage resources, and budgetary considerations. A combination of backup types can be employed to create a comprehensive backup strategy that meets specific needs for data protection and recovery.

2.2.2. Restore for disaster recovery

In the context of disaster recovery, the term "restore" refers to the process of recovering and returning critical data, applications, and systems to their operational state following a disruptive event or data loss. The restore phase is a key component of the overall disaster recovery plan and involves the following:

1. **Assess the situation**: Before initiating the restore process, assess the extent of the damage caused by the disaster and determine the scope of the restoration effort. Identify the affected systems, applications, and data that need to be restored.
2. **Activate the disaster recovery plan**: Refer to the documented disaster recovery plan, which should outline the procedures and guidelines for restoring various components of the IT infrastructure. Follow the plan's instructions to ensure a structured and organized approach to the restore process.
3. **Retrieve backups**: Retrieve the backup copies of the affected data, applications, or systems from the designated backup storage location. This may involve accessing backup tapes, disk-based backups, or cloud-based backups depending on the backup strategy and technology in place.
4. **Validate backup integrity:** Verify the integrity and consistency of the backup data before proceeding with the restore process. This step ensures that the backups are viable and can be relied upon for successful recovery.

5. **Restore data and applications**: Start the restoration of data and applications based on the recovery priorities defined in the disaster recovery plan. Begin with the most critical systems and work your way down to less critical ones. Follow the appropriate procedures for each type of backup (e.g., full backups, incremental backups) to restore the data and applications to their original or alternative locations.
6. **Test and verify**: After the restore process, conduct thorough testing to validate the restored data, applications, and systems. Perform functional tests, check for data integrity, and ensure that the restored components are working correctly.
7. **Update configurations and connections:** Adjust configurations and re-establish connections as necessary to integrate the restored systems back into the production environment.
8. **Document the restore process**: Maintain detailed documentation of the restore process, including the steps performed, any issues encountered, and the actions taken to resolve them.

Self-check - 2

Part I:- Say **True** if the given statement is correct else say **False**

_______1. A disaster recovery plan (DRP) only focuses on recovering data and does not address other aspects of business operations.

_______2. Backup and restore processes are only necessary for natural disasters and do not apply to other types of disruptions.

_______3. Having a backup solution in place guarantees instant recovery of data and systems in the event of a disaster.

_______4. Data backup and replication are interchangeable terms, representing the same process.

Part II: - Select the appropriate answer from the given alternative

_______1. What is the primary goal of a disaster recovery plan (DRP)?

A. Preventing disasters from occurring

B. Minimizing the impact of disasters on business operations

C. Recovering data and systems instantly after a disaster

D. Eliminating the need for regular backups

_______2. What is the purpose of conducting a business impact analysis (BIA) in the context of a disaster recovery plan?

A. Identifying critical business functions and their dependencies

B. Assessing the likelihood of specific disaster events occurring

C. Implementing cybersecurity measures to prevent data breaches

D. Evaluating the effectiveness of backup and restore processes

_______3. Which of the following is an example of an off-site backup location?

A. An external hard drive connected to the same server

B. A cloud storage service hosted by a third-party provider

C. shared network folder on the same local network

D. An additional internal hard drive within the same computer

_______4. What does the term "recovery point objective" (RPO) refer to in backup and restore?

A. The maximum tolerable downtime after a disaster

B. The amount of data that can be recovered within a specific timeframe

C. The point in time to which data can be restored after a disaster

D. The frequency at which backups are performed

________5. Which of the following is a common backup strategy for ensuring redundancy and data availability?

A. Full backup performed daily

B. Incremental backup performed weekly

C. Differential backup performed monthly

D. Snapshot backup performed hourly

Part II: - Give short answer

1. List and explain types of backups?
2. Demonstrate the main purpose of network disaster recovery in large and small organization?
3. Demonstrate disaster restore phase?

Operation sheet 2.1

Operation title: - Create a full backup of Windows 10 with the system image tool

Purpose: - Protect and save personal information from disaster.

Instruction: Use the figure below, given equipment and task. You have given 45 Minute for the task and you are expected to complete tasks.

- **Tools and requirement:-**Compute

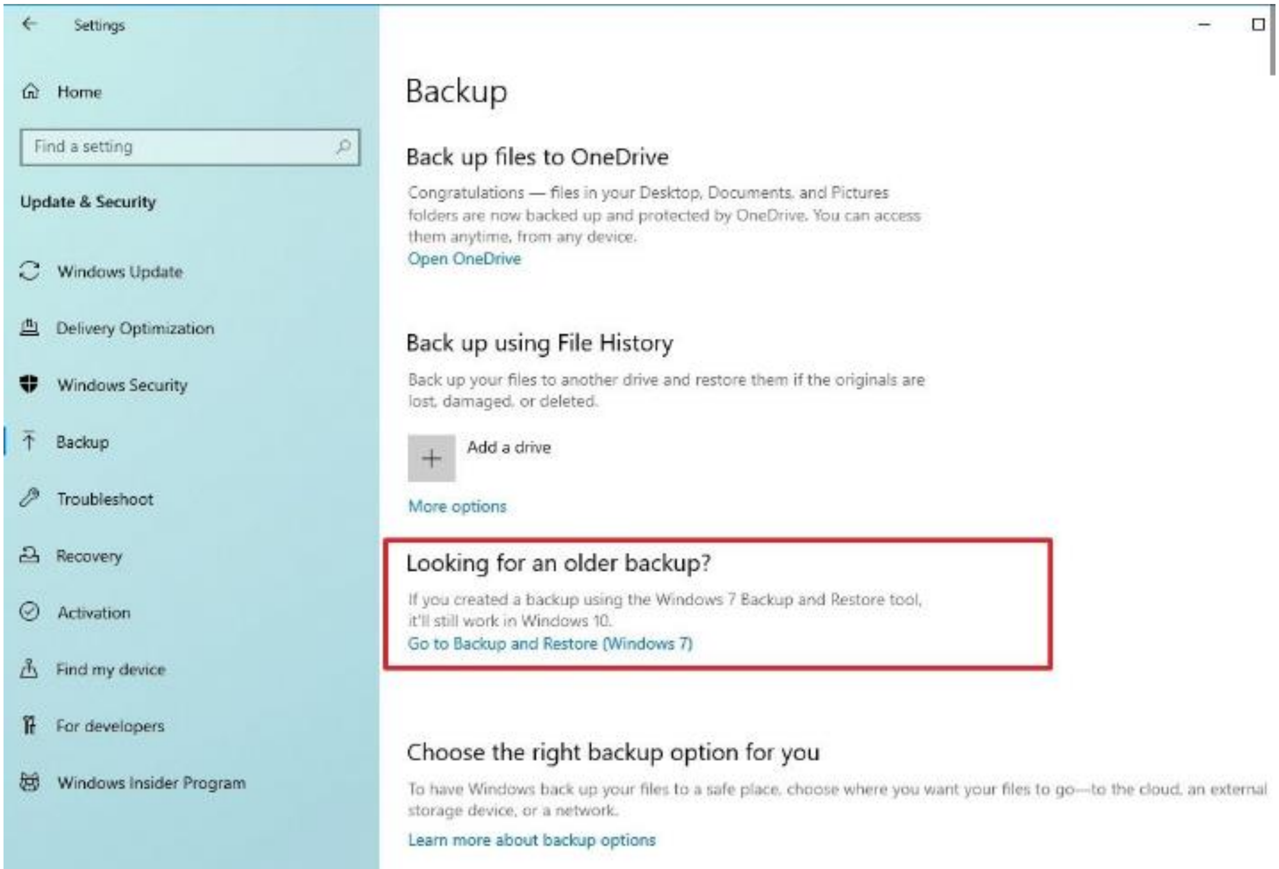
Procedures:-

Step 1:- Open **Settings**.

Step 2:- Click on **Update & Security**.

Step 3:- Click on **Backup**.

Step 4:- Under the "Looking for an older backup?"



Backup

Back up files to OneDrive

Congratulations — files in your Desktop, Documents, and Pictures folders are now backed up and protected by OneDrive. You can access them anytime, from any device.

Open OneDrive

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Add a drive

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

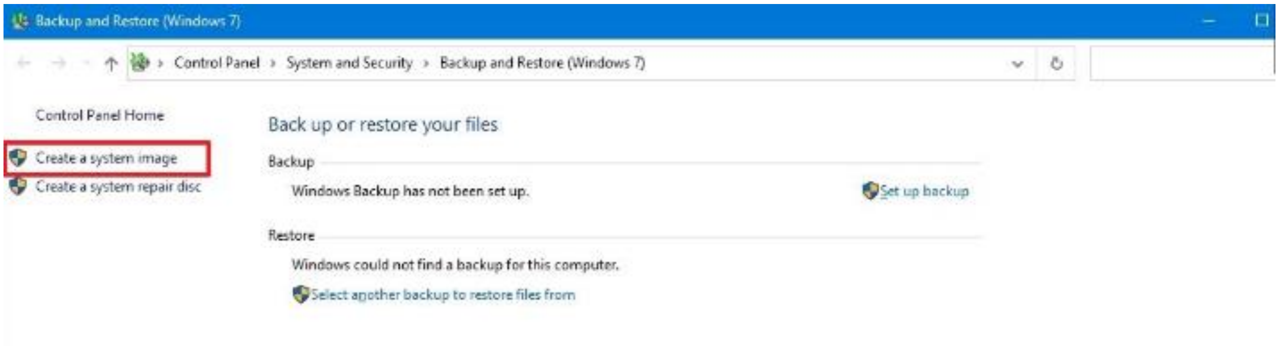
Go to Backup and Restore (Windows 7)

Choose the right backup option for you

To have Windows back up your files to a safe place, choose where you want your files to go—to the cloud, an external storage device, or a network.

Learn more about backup options

Step 5:- Click the **"Create a system image"** option from the left pane.



Backup and Restore (Windows 7)

Control Panel › System and Security › Backup and Restore (Windows 7)

Control Panel Home

Create a system image

Create a system repair disc

Back up or restore your files

Backup

Windows Backup has not been set up.

Set up backup

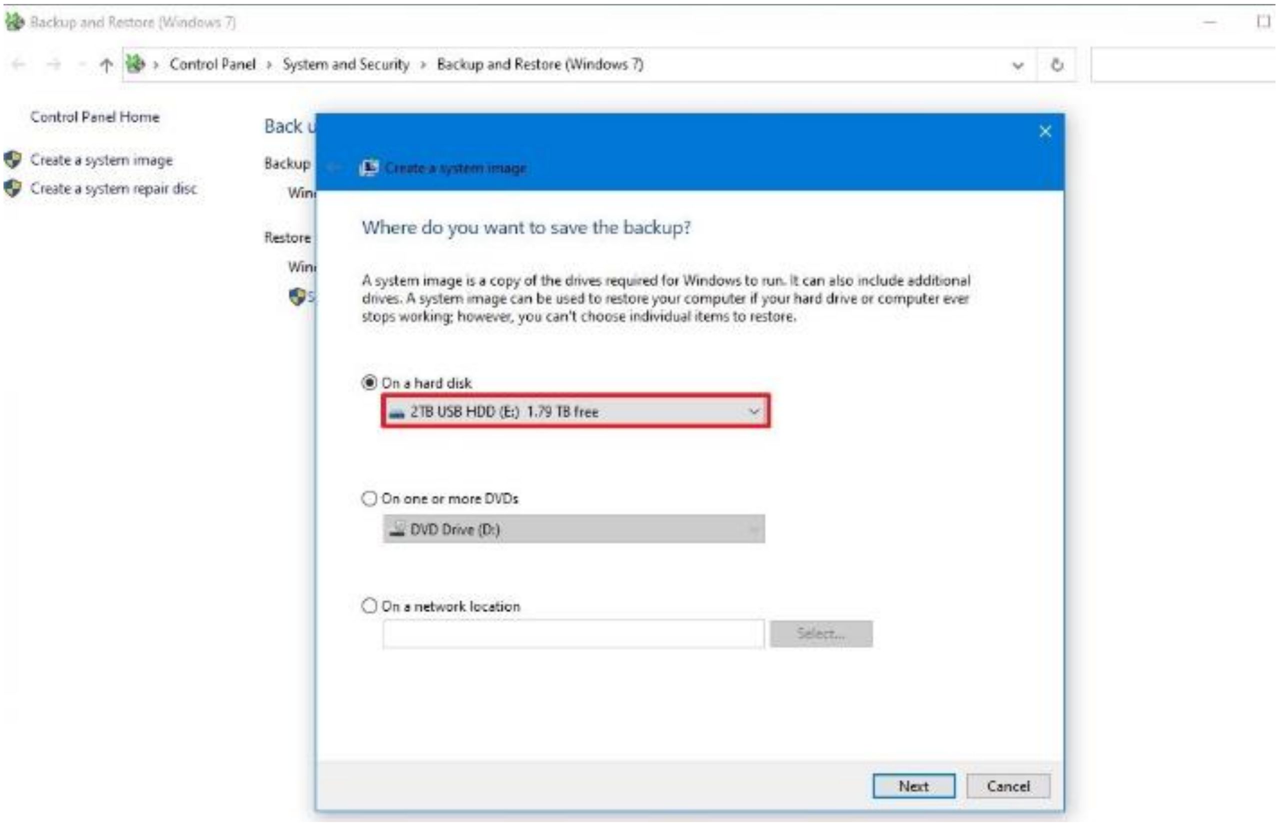
Restore

Windows could not find a backup for this computer.

Select another backup to restore files from

Step 6:- Select the **"On a hard disk"** option.

Step 7: -Use the "On a hard disk" drop-down menu and select the location to export the Windows 10 full backup.



Backup and Restore (Windows 7)

Control Panel › System and Security › Backup and Restore (Windows 7)

Control Panel Home

Create a system image

Create a system repair disc

Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore.

● On a hard disk

2TB USB HDD (E:) 1.79 TB free

○ On one or more DVDs

DVD Drive (D:)

○ On a network location

Select...

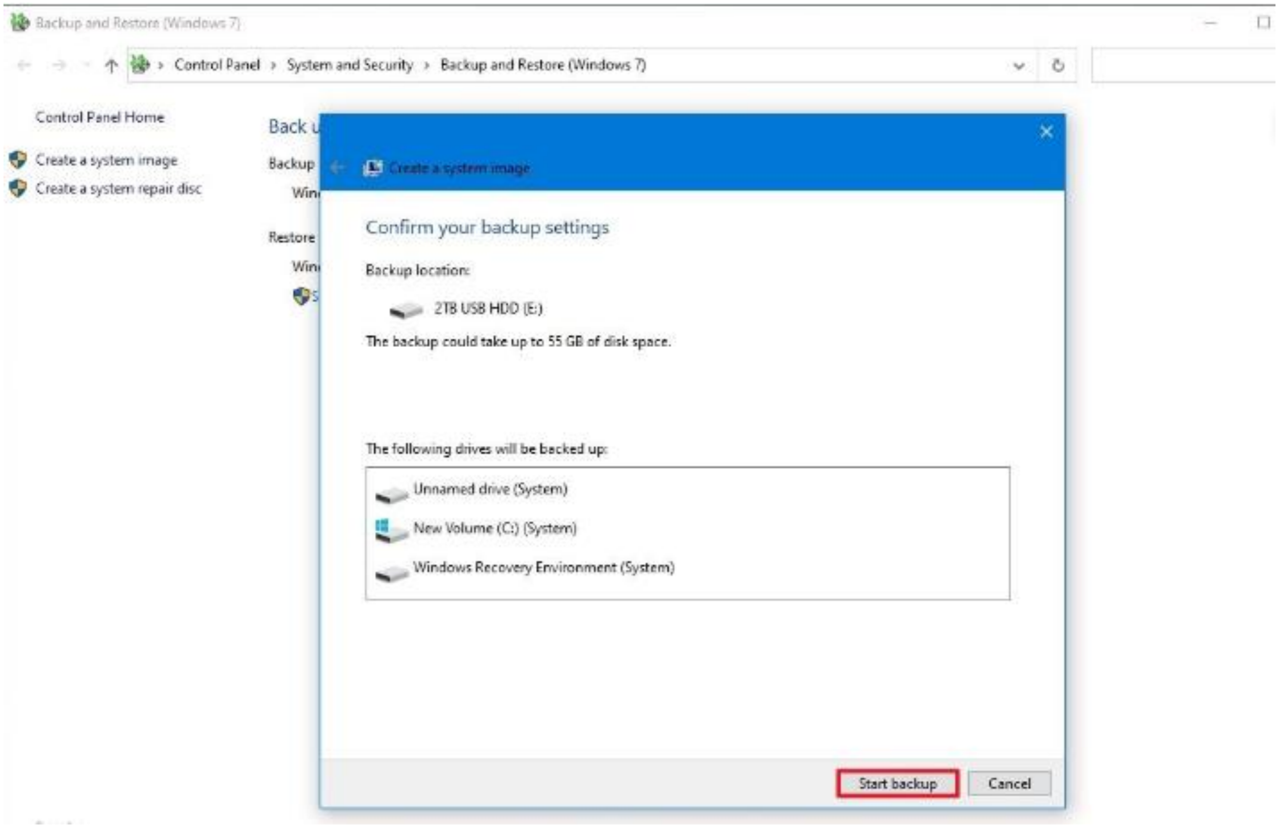
Next Cancel

Step 8: -Click the **Next** button.

Step 9:- (Optional) Select any additional hard drives to include them in the backup.

Step 10:- Click the **Next** button.

Step 11:- Click the **Start backup** button.


Backup and Restore (Windows 7)
Control Panel > System and Security > Backup and Restore (Windows 7)
Control Panel Home
Create a system image
Create a system repair disc
Back u
Backup
Win
Restore
Win
Create a system image
Start backup
Cancel

Confirm your backup settings

Backup location:

2TB USB HDD (E:)

The backup could take up to 55 GB of disk space.

The following drives will be backed up:

- Unnamed drive (System)
- New Volume (C:) (System)
- Windows Recovery Environment (System)

Step 12:- Click the **No** button.

Step 13:- Click the **Close** button.

Operation sheet 2.2

Operation title: - Restore a backup with system image tool on Windows 10

Purpose: - To recover distorted or damage information.

Instruction: Use the figure below, given equipment and task. You have given 45 Minute for the task and you are expected to complete tasks.

Tools and requirement:-Compute Windows 10 USB bootable drive

Procedures:-

Step 1:- Connect the drive with the full back up to the device.

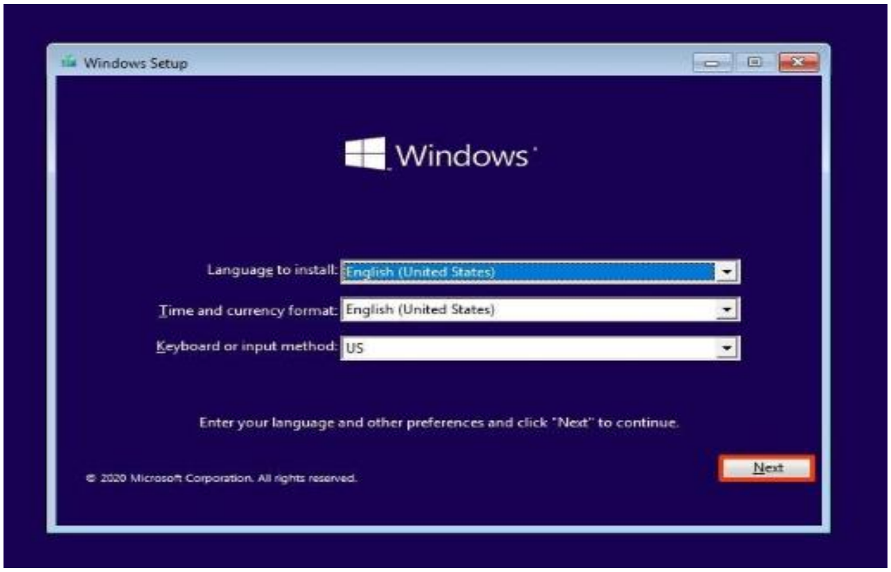
Step 2:- Connect the Windows 10 USB bootable drive to the computer.

Step 3:- Start the computer.

Step 4:- On the USB bootable drive startup prompt, press any key to continue.

Quick tip: If the device does not start in the Windows Setup wizard, you will need to access the Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) to change the boot order settings. You can use this guide to access the BIOS/UEFI, but the steps are usually different per manufacturer and device model. It is recommended to check your manufacturer support website for more specific details.

Step 5:- On the "Windows Setup" page, click the **Next** button.



Language to install: English (United States)

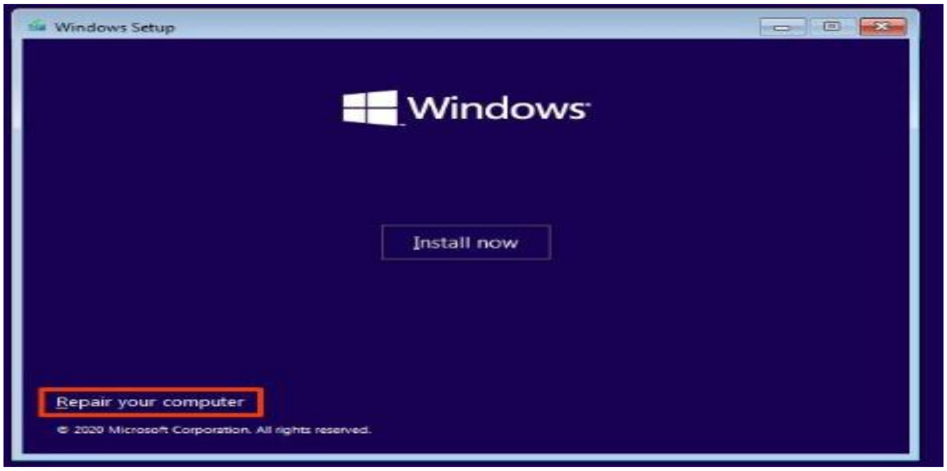
Time and currency format: English (United States)

Keyboard or input method: US

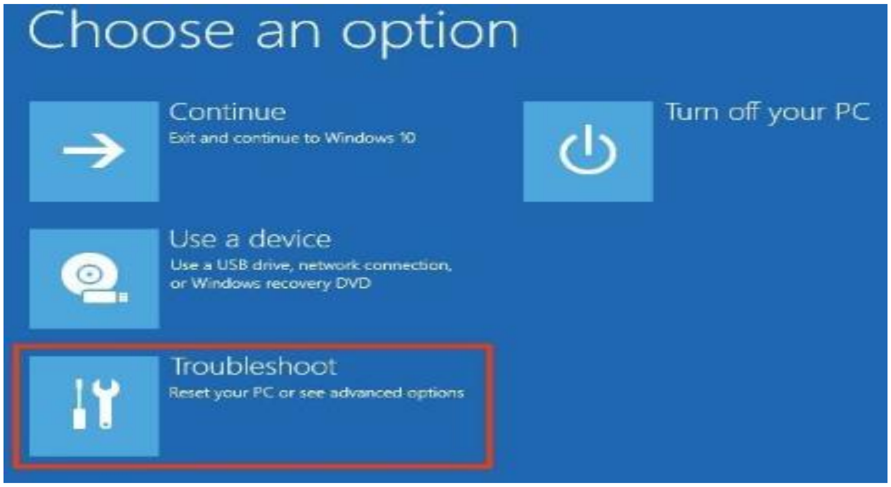
Enter your language and other preferences and click "Next" to continue.

© 2020 Microsoft Corporation. All rights reserved.

Step 6:- Click the **"Repair your computer"** option from the bottom-left corner of the screen.



Step 7:- Click the **Troubleshoot** option.



Choose an option

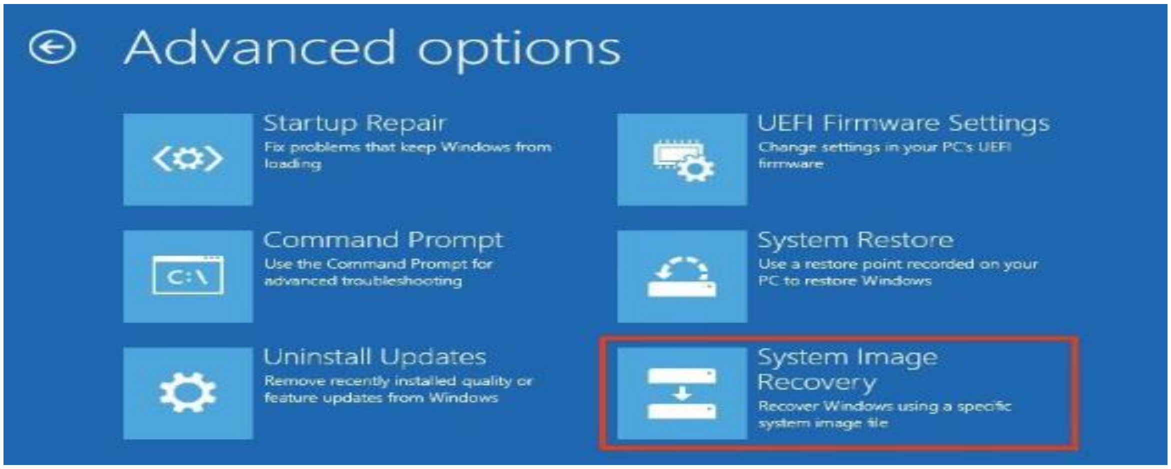
Continue
Exit and continue to Windows 10

Turn off your PC

Use a device
Use a USB drive, network connection, or Windows recovery DVD

Troubleshoot
Reset your PC or see advanced options

Step 8:- Click the **"System Image Recovery"** option



Advanced options

Startup Repair
Fix problems that keep Windows from loading

UEFI Firmware Settings
Change settings in your PC's UEFI firmware

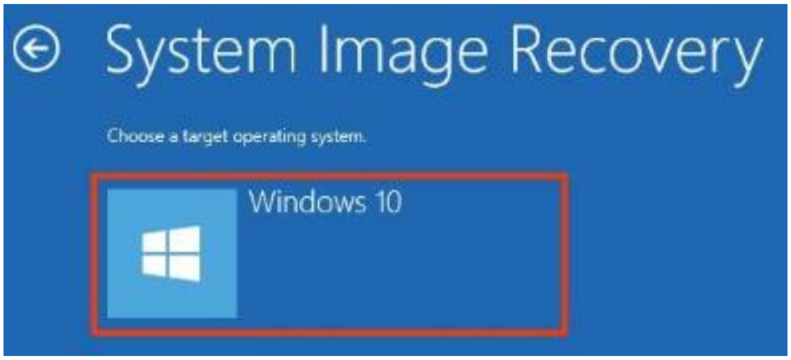
Command Prompt
Use the Command Prompt for advanced troubleshooting

System Restore
Use a restore point recorded on your PC to restore Windows

Uninstall Updates
Remove recently installed quality or feature updates from Windows

System Image Recovery
Recover Windows using a specific system image file

Step 9:- Select the **Windows 10** option as the target operating system.



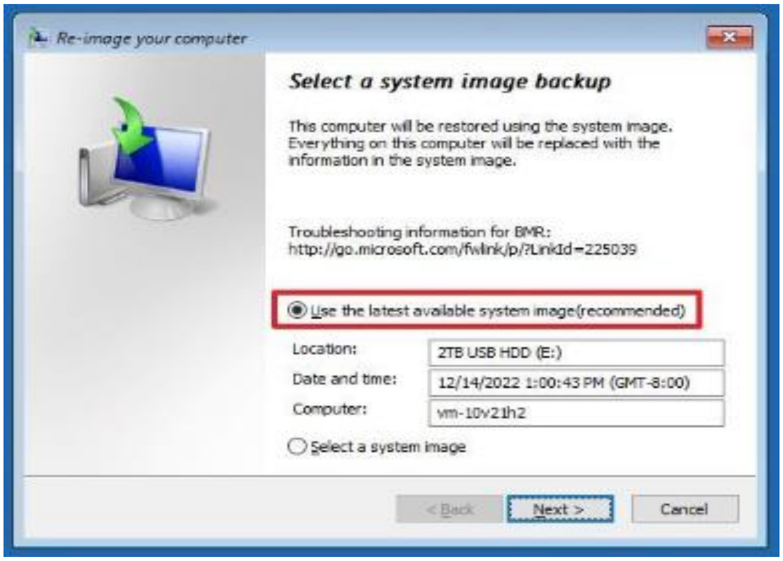
System Image Recovery

Choose a target operating system.

Windows 10

Step 10:- On the "Re-image your computer" page, select the **"Use the latest available system image"** option.

Quick tip: You can use the "Select a system image" option if you have multiple backups and you are trying to restore an older version of the system and files.



Re-image your computer

Select a system image backup

This computer will be restored using the system image. Everything on this computer will be replaced with the information in the system image.

Troubleshooting information for BMR:
http://go.microsoft.com/fwlink/p/?LinkId=225039

● Use the latest available system image(recommended)

Location: 2TB USB HDD (E:)
Date and time: 12/14/2022 1:00:43 PM (GMT-8:00)
Computer: vm-10v21h2

○ Select a system image

Step 11:- Click the **Next** button.

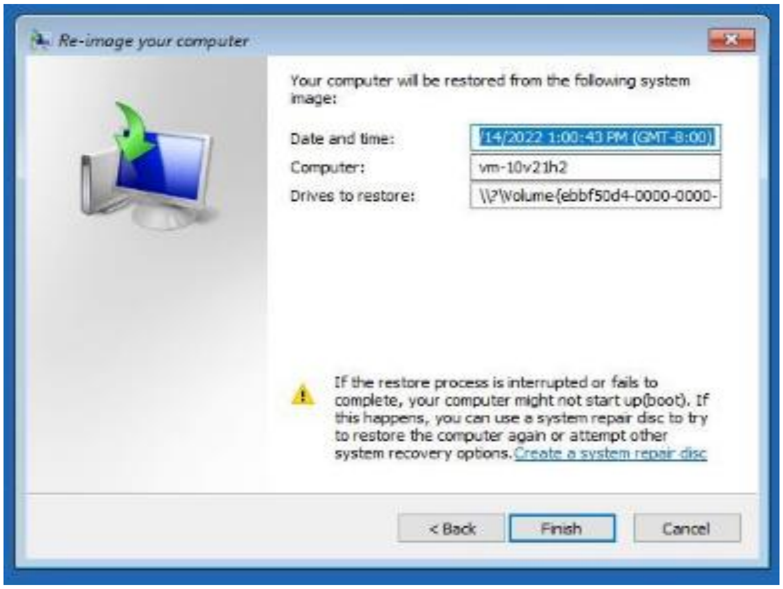
Step 12:-(Optional) Carefully select the **"Format and repartition disks"** option before restoring the backup (if you are restoring the backup on a new drive).

Quick tip: If you choose this option, use the **Exclude disks** option to prevent formatting secondary drives that may contain data.

Step 13:- (Optional) Check the **"Only restore system drivers"** option (if the backup contains a copy of multiple drives and you only want to restore the operating system).

Step 14:- Click the **Next** button.

Step 15:- Click the **Finish** button.



Your computer will be restored from the following system image:

Date and time: /14/2022 1:00:43 PM (GMT-8:00)

Computer: vm-10v21h2

Drives to restore: \\?\Volume{ebbf50d4-0000-0000-

If the restore process is interrupted or fails to complete, your computer might not start up(boot). If this happens, you can use a system repair disc to try to restore the computer again or attempt other system recovery options. Create a system repair disc

Step 16:- Click the **Yes** button.

Quick tip:- After you complete the steps, the recovery process will start on the computer. The time to finish the restoration will depend on the amount of data and hardware configuration.

If you are about to restore a device, do not interrupt the process, as it can cause the backup to fail, making it unbootable. It is always recommended to have the laptop connected to a power source and a desktop computer to an uninterruptible power supply (UPS) to avoid problems.

Once the backup has been restored, open **Settings → Update & Security →Windows Update**, and click the **Check for Updates** button to quickly install any missing security updates.

LAP Test

Task 1:- Create a full backup of Windows 10 with the system image tool

Task 2:- Restore damage computer by using bootable Windows 10 operating system.

Unit Three : Monitor network performance

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Performing diagnostic test
- Analyzing and responding information
- Monitoring software and files
- Monitoring performance indicators
- Improving network and systems

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Perform diagnostic test
- Analyze and responding information
- Monitor software and files
- Monitor performance indicators
- Improve network and systems

3.1. Basic concept of monitor network performance

Monitoring network performance involves the systematic observation and analysis of a computer network to ensure it operates efficiently, reliably, and securely. This process encompasses various aspects such as bandwidth utilization, latency, packet loss, and device health. By continually assessing these factors, network administrators can identify and address potential issues before they impact the user experience. Bandwidth monitoring helps optimize data transmission capacity, latency monitoring ensures timely data delivery, and packet loss monitoring aids in maintaining a stable and responsive network. Additionally, network performance monitoring includes traffic analysis, security surveillance, and quality of service assessments to ensure that resources are allocated effectively, potential security threats are detected, and the overall quality of communication meets the desired standards. Utilizing specialized tools and reporting mechanisms, organizations can maintain a proactive approach to network management, enhancing the overall reliability and performance of their network infrastructure.

3.2. Performing diagnostic test

Performing network diagnostic tests involves a systematic process to assess and analyze the health, performance, and functionality of a computer network. Here are the general steps you can follow to conduct network diagnostic tests:

- **Identify the Issue:**
  - ➢ Begin by identifying the specific issue or symptoms that require diagnostic testing. This could include slow network performance, connectivity problems, or unexpected outages.
- **Define Testing Objectives:**
  - ➢ Clearly define the objectives of your diagnostic tests. Determine what aspects of the network you need to evaluate, such as bandwidth, latency, packet loss, or device health.
- **Select Appropriate Tools:**
  - ➢ Choose the appropriate network diagnostic tools for the specific tests you want to perform. There are various tools available for different aspects of network analysis, including:
    - ✓ **Ping and Traceroute:** For assessing connectivity and latency.

- ✓ **Network Performance Monitoring Tools:** Such as Wireshark, Nagios, or PRTG for detailed analysis of network traffic.
- ✓ **Bandwidth Testing Tools:** Like Speedtest.net or iPerf for measuring available bandwidth.
- ✓ **Device Monitoring Software:** To assess the health and performance of network devices.

- **Execute Diagnostic Tests:**
  - ➢ Perform the selected diagnostic tests. For example:
    - ✓ Use ping to check connectivity and measure round-trip times.
    - ✓ Conduct traceroute to identify the path and latency between your computer and a destination.
    - ✓ Run bandwidth tests to evaluate the network's capacity.
    - ✓ Utilize network monitoring tools to analyze traffic patterns and identify potential issues.
- **Interpret Results:**
  - ➢ Analyze the results of the diagnostic tests. Look for anomalies, deviations from expected values, or patterns that may indicate network issues. Pay attention to any packet loss, latency spikes, or irregularities in traffic.
- **Diagnose Network Issues:**
  - ➢ Based on the results, diagnose the root causes of identified network issues. This may involve troubleshooting hardware, configuration settings, or addressing issues related to network congestion.
- **Implement Solutions:**
  - ➢ Once the issues are identified, implement appropriate solutions. This could include adjusting network configurations, upgrading hardware, optimizing settings, or addressing specific issues with network devices.
- **Document and Report:**
  - ➢ Document the results of your diagnostic tests and the actions taken to address any issues. This documentation is valuable for future reference and can help in maintaining a proactive approach to network management.
- **Continuous Monitoring:**

- Establish a routine for continuous monitoring of the network. Regularly perform diagnostic tests to identify and address potential issues before they impact network performance.

3.3. Analyze and respond information

Analyzing and responding to information in a network involves monitoring network traffic, identifying potential issues or anomalies, and taking appropriate actions to ensure network security, performance, and reliability. Here are some ways of analyze and respond to information in a network:

1. **Implement network-monitoring tools**: Use network monitoring software or tools to capture and analyze network traffic. These tools can provide real-time visibility into network activity, including bandwidth utilization, packet loss, latency, and security events.
2. **Establish baseline and thresholds**: Establish a baseline of normal network behavior by monitoring network traffic patterns over time. Set thresholds or alerts for abnormal network behavior, such as unusually high traffic volume, network congestion, or security breaches.
3. **Monitor network traffic**: Continuously monitor network traffic to identify any anomalies or deviations from the baseline. Observe patterns, trends, and irregularities that may indicate network performance issues or security incidents.
4. **Analyze network logs**: Analyze log files generated by network devices, servers, and security systems. Logs can provide valuable information about network events, errors, and security incidents. Look for any suspicious or unusual activities that may require investigation or response.
5. **Identify security threats**: Use intrusion detection and prevention systems (IDS/IPS) or security information and event management (SIEM) solutions to detect and respond to security threats. Analyze network traffic for signs of malware infections, unauthorized access attempts, or other malicious activities.
6. **Investigate network issues**: When an issue or anomaly is detected, investigate the root cause by analyzing relevant network logs, traffic patterns, and system configurations. Identify the source of the problem, whether it's a misconfiguration, hardware failure, software bug, or security incident.

7. **Respond to network incidents**: Take appropriate actions to address network incidents or issues. This may involve implementing security measures, such as blocking malicious IP addresses or isolating compromised devices. Troubleshoot network performance problems and apply necessary fixes or optimizations.
8. **Document and report**: Keep detailed records of network incidents, actions taken, and their outcomes. Document any changes made to network configurations or security settings. Prepare reports summarizing network performance, security incidents, and actions taken for management and future reference.
9. **Continuous improvement:** Regularly review and update network monitoring and response strategies based on lessons learned from past incidents. Stay updated with emerging threats, new technologies, and best practices in network monitoring and security.

Analyzing and responding to information in a network requires a proactive and vigilant approach. It is crucial to have skilled network administrators or security professionals who can effectively interpret network data, identify potential risks or issues, and take prompt actions to maintain the network's integrity and performance.

3.4. Monitor software and files

To monitor software and files using a network, you can employ various network monitoring techniques and tools. Here are some steps to monitor software and files using a network:

1. **Choose network-monitoring tools**: Select network monitoring software or tools that offer features for monitoring software and file activities. Look for tools that provide real-time monitoring, alerting, and reporting capabilities specific to software and file monitoring.
2. **Install monitoring agents or software:** Install monitoring agents or software on the systems or servers where the software and files are located. These agents will collect data and send it to the central monitoring system for analysis.
3. **Set up file integrity monitoring:** Implement file integrity monitoring (FIM) to detect unauthorized changes to files. FIM tools can monitor file attributes, checksums, or digital signatures to ensure the integrity and security of critical files. Any unauthorized modifications can trigger an alert.
4. **Monitor network traffic:** Utilize network-monitoring tools to capture and analyze network traffic that is related to software and file activities. This can help identify any unusual or unauthorized network connections, file transfers, or software downloads.

5. **Enable logging and auditing:** Enable logging and auditing features on servers and systems hosting the software and files. Configure the logging settings to capture relevant information about software installations, file accesses, modifications, and user activities. Regularly review the logs for any suspicious or unauthorized activities.
6. **Configure alerts and notifications:** Set up alerts and notifications within the network monitoring tools to inform you of any abnormal software or file-related activities. Configure the alerts to be sent via email, SMS, or other communication channels, ensuring that the right individuals or teams are notified promptly.
7. **Perform regular analysis and reporting:** Regularly analyze the collected data, generate reports on software, and file activities. Look for patterns, trends, or anomalies that may indicate security risks, compliance violations, or performance issues. Share these reports with relevant stakeholders for visibility and informed decision-making.
8. **Maintain patch management and vulnerability scanning:** Regularly apply software patches and updates to address known vulnerabilities. Conduct vulnerability scans to identify any weaknesses in software or files that could be exploited by attackers. Monitor the results of patching and vulnerability scanning activities to ensure compliance and mitigate risks.
9. **Continuously review and refine monitoring strategies:** Review your monitoring strategies and tools periodically to ensure they remain effective and aligned with your organization's evolving needs. Stay informed about emerging threats, new monitoring technologies, and best practices in software and file monitoring to enhance your monitoring capabilities.

3.5. Monitor performance indicators

Monitoring the performance indicators of a network is essential to ensure its optimal functionality. To monitor network performance, start by identifying relevant performance indicators such as bandwidth utilization, latency, packet loss, network throughput, and response times. Next, select network monitoring tools that can collect and analyze data on these indicators. Deploy monitoring agents or sensors on critical network devices and configure real-time monitoring to continuously track performance metrics. Set up performance thresholds and alerts to receive notifications when indicators exceed or fall below acceptable levels. Analyze historical data to identify trends and patterns, and periodically conduct performance assessments. Utilize network traffic analysis tools to examine traffic patterns and generate performance reports to gain insights into the network's health. Continuously review and optimize your monitoring strategy to align with evolving network requirements and industry best practices.

Monitoring network performance involves selecting relevant performance indicators, deploying monitoring tools and agents, configuring real-time monitoring, setting up thresholds and alerts, analyzing historical data, conducting periodic assessments, utilizing network traffic analysis, and generating performance reports. By following these steps, you can proactively identify and address performance issues, optimize network resources, and ensure a reliable and efficient network infrastructure. Regularly reviewing and optimizing your monitoring strategy is crucial to stay aligned with changing network requirements and technological advancements.

3.6. Improve network and systems

Improving network and systems involves implementing strategies to enhance performance,

A step to enhance your network performance can enhance your overall productivity and business continuity.

1. Reconfigure Your Network

CONFIGURING YOUR NETWORK

- Installing network support on user workstations, so they can "talk" to your network.

Your network configuration can affect performance. For instance, if you install an update and it doesn't configure your devices, this can have a large impact on your performance. A good example is the personal area network devices that should not be more than 10 meters apart.

Devices with short-range connectivity should be close to each other to prevent network delays between the hardware components.

Reconfiguring your hardware components will help the devices communicate with each other effectively.

2. Check for System Defects And Viruses

Viruses and system defects can break down a network infrastructure and degrade the network performance. Some malwares can also control programs and applications in your network. A flaw in the components or system can cause a network to behave unexpectedly.

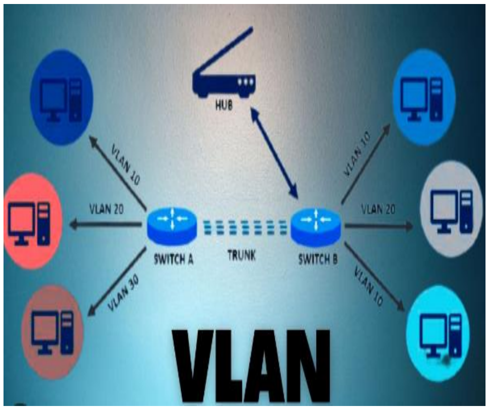
Cable defects such as core rapture are a good example of issues that can cause failure in the conduction of electricity, interfering with communication in a network. Checking for malware and fixing system defects can address the situation and restore optimal performance.

3. Upgrade and Update Firmware and Software

Often, businesses cannot keep up with the pace of technology and balance with the software they run. You may end up having software running on outdated technology in your network. You can also have old machines with new programs.

Usually, there is no guarantee that programs and the existing technology are fully compatible, which can negatively impact the network performance. Outdated software and programs also have bugs that can break down your infrastructure.

4. **Use Virtual Local Area Networks (VLANs)**



VLANs reduce broadcast traffic, ease administration and confine broadcast domains. You can use the technology to segment your network resources such that critical areas are given the highest priority. With VLANs, you can separate or partition the network without rewiring the entire office.

VLANs also play a vital role in enhancing security. Splitting network components and prioritizing tasks in the network can create room for performance optimization.

5. Provide a Guest Network

Having multiple users on a network increases traffic, which affects network performance. An enterprise network accommodating hundreds of guest users is bound to experience slowdowns. Guests can demand bandwidth that your business would otherwise be using on other important tasks.

6. User Education

Educating your team on user behavior can enhance network performance. Often, employees use their free time on their computers. They could choose to stream a show or play video games, unaware of the impact of the activities on the network resources.

In this case, employees should be educated on how the downtime activities of their computers affect network performance. They are likely to settle for other activities that don't strain the resources with this knowledge.

Educating your employees on best practices for spending time on their computers, running processes, and utilizing network resources can help improve performance.

7. Network Monitoring:- Monitoring your network for traffic jams and bottlenecks can help you diagnose problems, solve them in good time, and prevent advancing network issues. For instance, if the network admin identifies backups as the reason behind substandard network performance, they can schedule them for a time when the personnel are not utilizing most of the network resources.

Regular network monitoring can help you spot the bottlenecks, address them, and enhance network performance.

Figure 1. 8 Network Monitoring

Self-check - 3

Part I:- Say **True** if the given statement is correct else say **False**

_______1. Performing diagnostic tests involves analyzing and responding to information.

_______2. Monitoring software and files is not a part of the diagnostic testing process.

_______**3.** Diagnostic testing does not involve monitoring performance indicators.

Part II: - Select the appropriate answer from the given alternative

_______1. What is the purpose of analyzing and responding to information in network administration?

A. Improving network aesthetics
C. Identifying performance bottlenecks
B. Monitoring software license usage
D. Ensuring physical security measures

_______2. which of the following is a common performance indicator monitored in network administration.

A. Keyboard typing speed
C. File compression ratio
B. Server room temperature
D. Network bandwidth utilization

_______3. How does improving network and systems contribute to network administration?

A. Increasing software licensing costs
B. Enhancing data backup and recovery
C. Monitoring physical server dimensions
D. Optimizing network configurations

_______4. How does improving network and systems contribute to network administration?

A. Monitoring office supply inventory
B. Increasing software licensing compliance
C. Enhancing network security measures
D. Optimizing printer paper tray configurations

Part III: - Give short answer

1. List and explain ways of analyze and respond to information in a network?
2. Demonstrate the way of improve network and systems?
3. Demonstrate the technic of monitor software and files using a network?

Operation sheet 3.1.

Operation title: - Diagnostic network performance

Purpose: - To recover network problem and test performance.

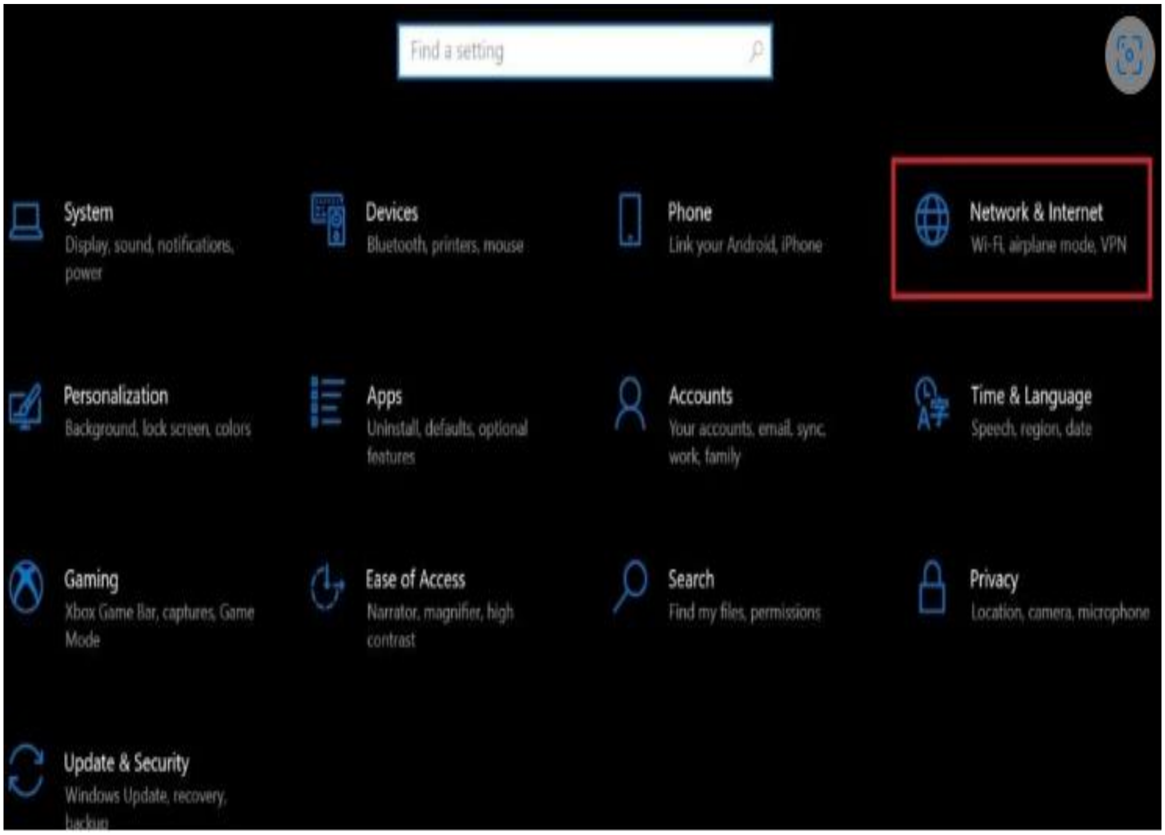
Instruction: Use the figure below, given equipment and task. You have given 45 Minute for the task and you are expected to complete tasks.

Tools and requirement:-Compute

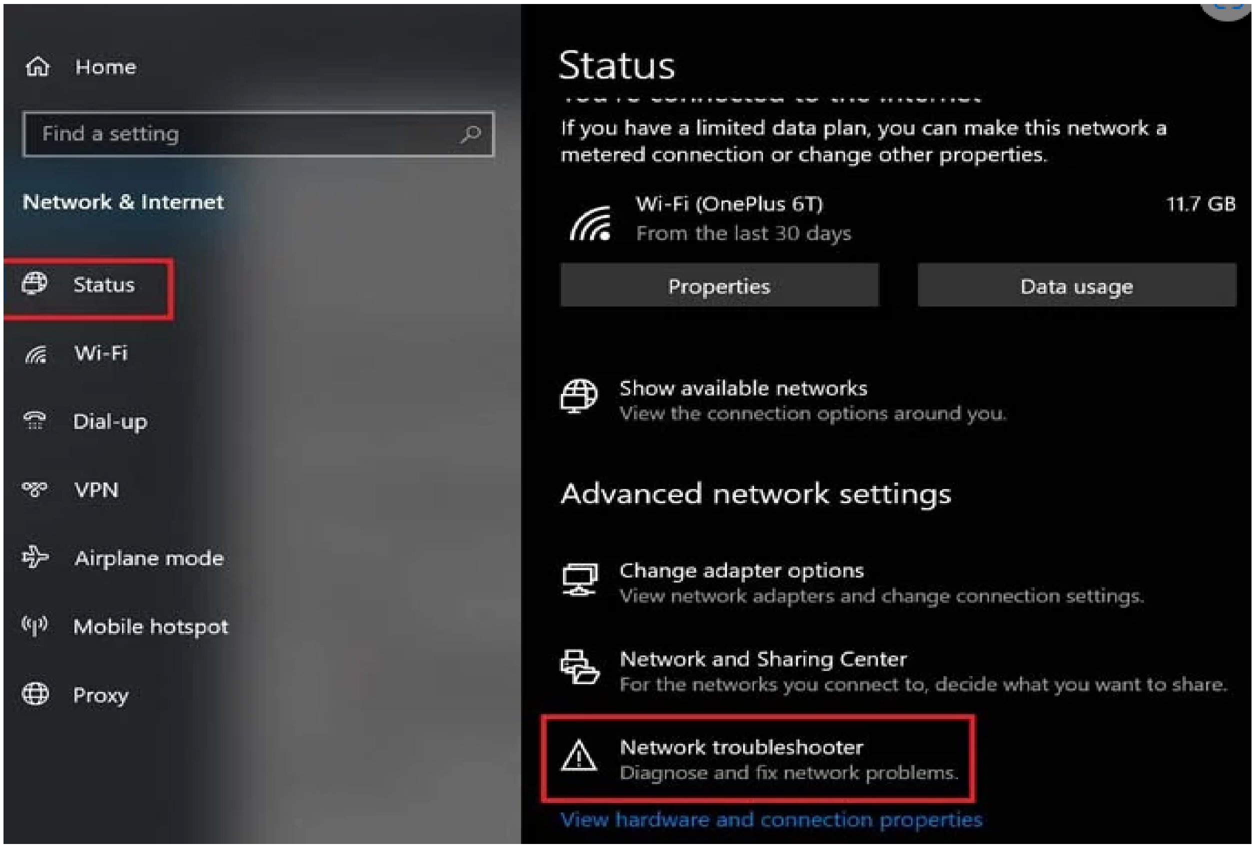
Procedures:-

Step 1:- Press **Windows + I** to open **Settings**

Step 2:- Click on **Network and Internet**


Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Xbox Game Bar, captures, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Search
Find my files, permissions
Privacy
Location, camera, microphone
Update & Security
Windows Update, recovery, backup

Step 3:- Under the left-hand panel, option **Status** navigate to **Network Troubleshooter** and click it



Status

If you have a limited data plan, you can make this network a metered connection or change other properties.

Wi-Fi (OnePlus 6T) 11.7 GB
From the last 30 days

Show available networks
View the connection options around you.

Advanced network settings

Change adapter options
View network adapters and change connection settings.

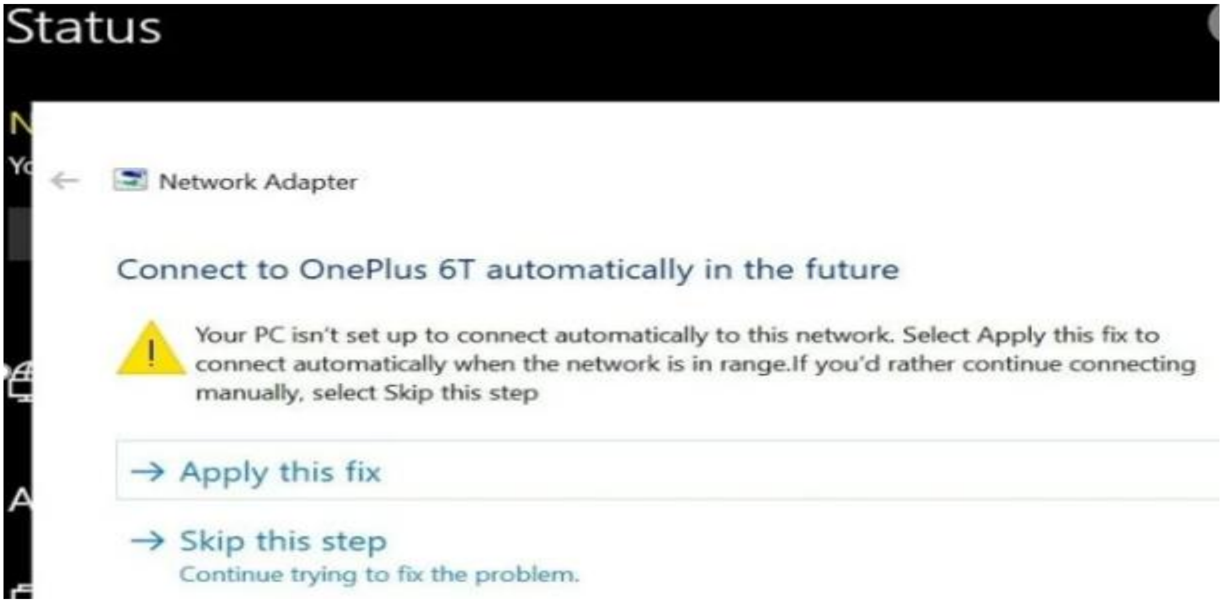
Network and Sharing Center
For the networks you connect to, decide what you want to share.

Network troubleshooter
Diagnose and fix network problems.

View hardware and connection properties

Step 4:- Then the tool will start to run a network check to find what can be possibly wrong with the connectivity

I will show you how it will work. Let’s say I am not connected to my preferred network. Then upon running a network check using the Network Troubleshooter, I will get the following result.



Connect to OnePlus 6T automatically in the future

Your PC isn’t set up to connect automatically to this network. Select Apply this fix to connect automatically when the network is in range.If you’d rather continue connecting manually, select Skip this step

Continue trying to fix the problem.

Operation sheet 3.2.

Operation title: - Speed up Internet connection on Windows 10

Purpose: - To increase download and upload speed of internet connection.

Instruction: Use the figure below, given equipment and task. You have given 45 Minute for the task and you are expected to complete tasks.

Tools and requirement:-Compute, Internet, Internet cable, NW driver

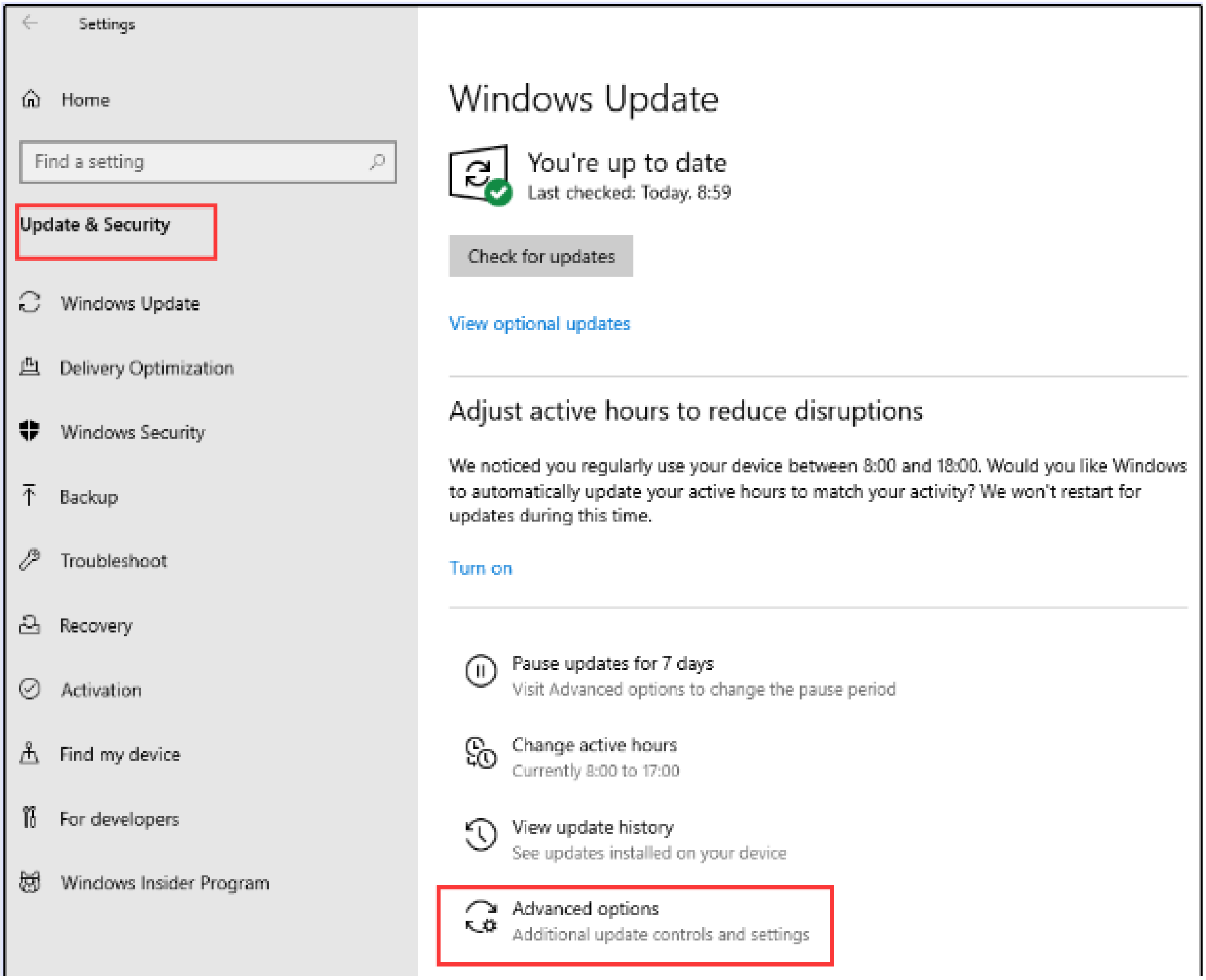
Procedures:-

To **speed up Windows 10 internet**, you can make some small changes on Windows 10 to quickly resolve these culprits for slow internet speed and enjoy faster internet in five ways.

Way 1. Change Bandwidth Limit to Speed up Internet on Windows 10

Step 1. Open the Settings on your Windows 10.

Step 2. Click Update & Security →Advanced options in turn.



You're up to date
Last checked: Today, 8:59

Adjust active hours to reduce disruptions

We noticed you regularly use your device between 8:00 and 18:00. Would you like Windows to automatically update your active hours to match your activity? We won't restart for updates during this time.

Visit Advanced options to change the pause period

Currently 8:00 to 17:00

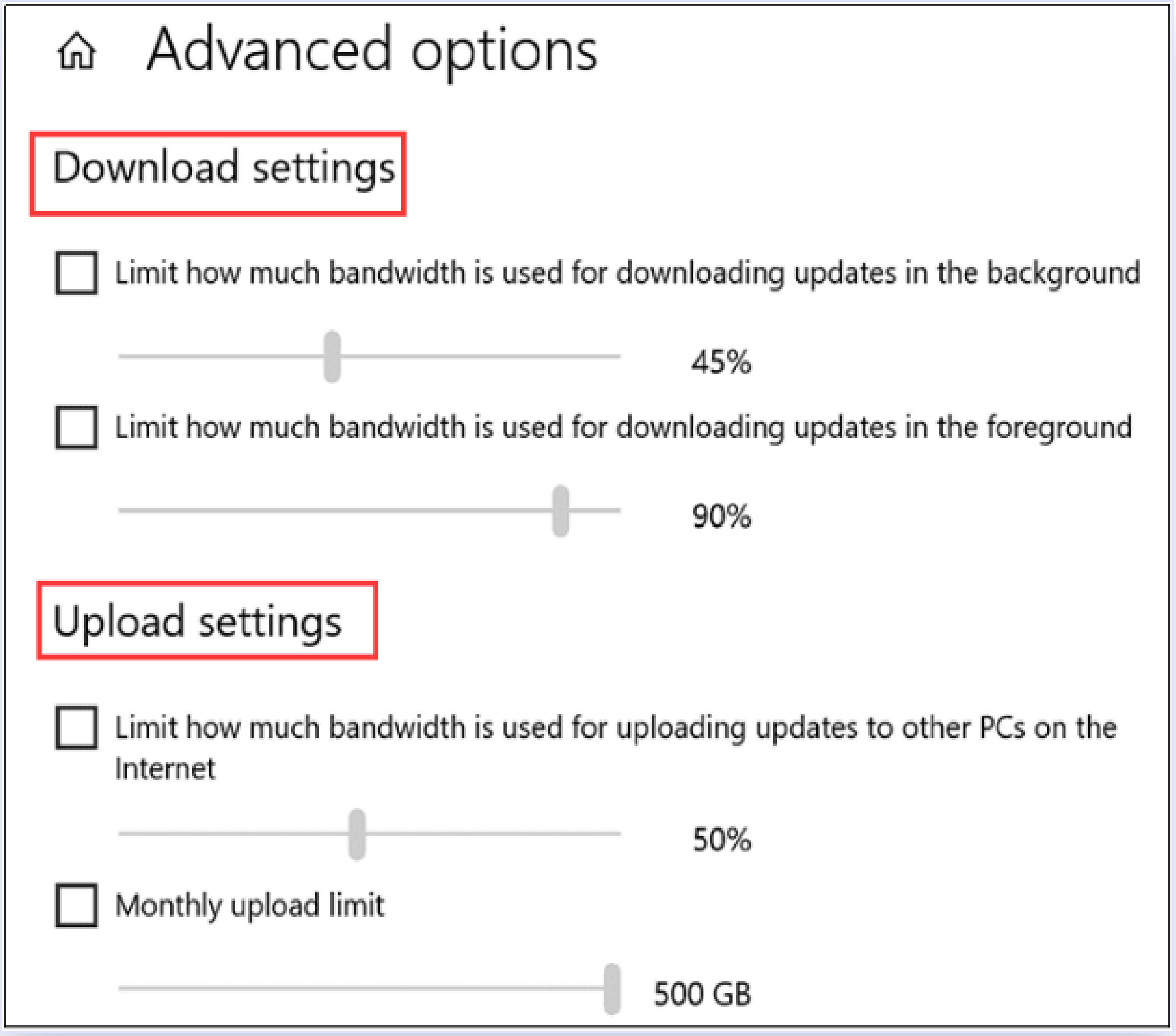
See updates installed on your device

Additional update controls and settings

Step 3. In the Advanced options window, scroll down to find Delivery Optimization and click it.

Step 4. Choose advanced options again at the bottom.

Step 5. After that, you will see an adjuster for both Download settings and Upload settings. Here, you can reset the amount of bandwidth that Windows can use for your core tasks.



Advanced options

Download settings

□ Limit how much bandwidth is used for downloading updates in the background

45%

□ Limit how much bandwidth is used for downloading updates in the foreground

90%

Upload settings

□ Limit how much bandwidth is used for uploading updates to other PCs on the Internet

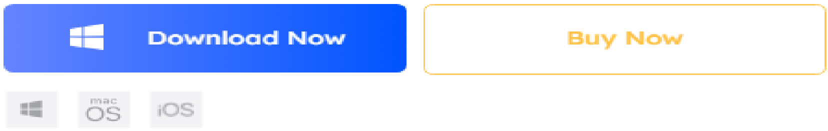
50%

□ Monthly upload limit

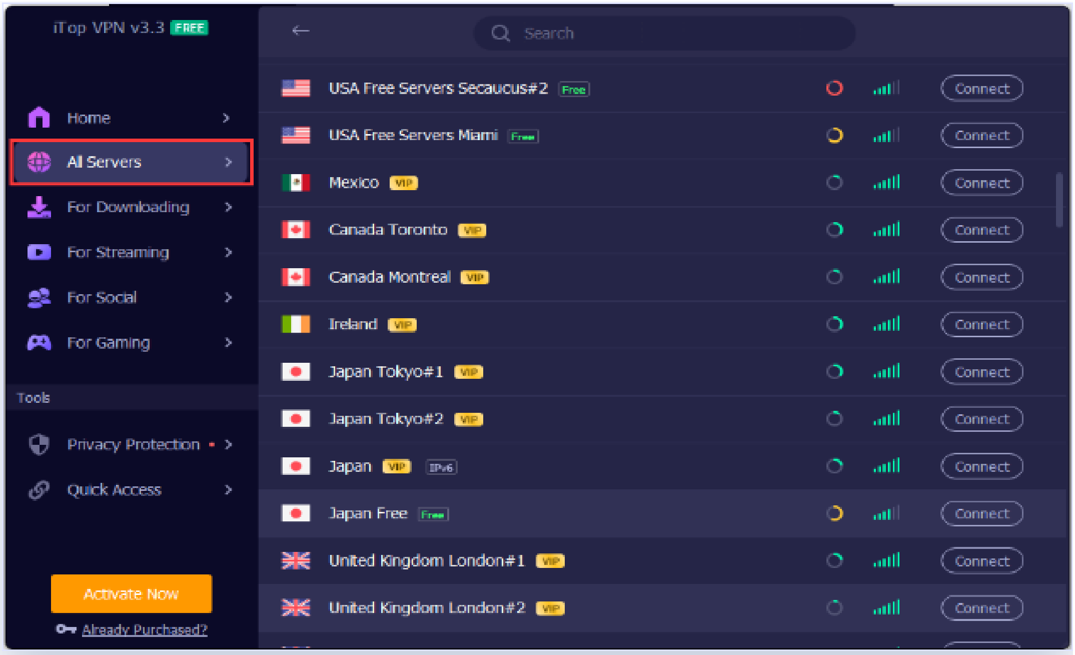
500 GB

Way 2. Get the Best VPN to Speed up Internet on Windows 10

Step 1. Download this free VPN on your Windows and launch it.

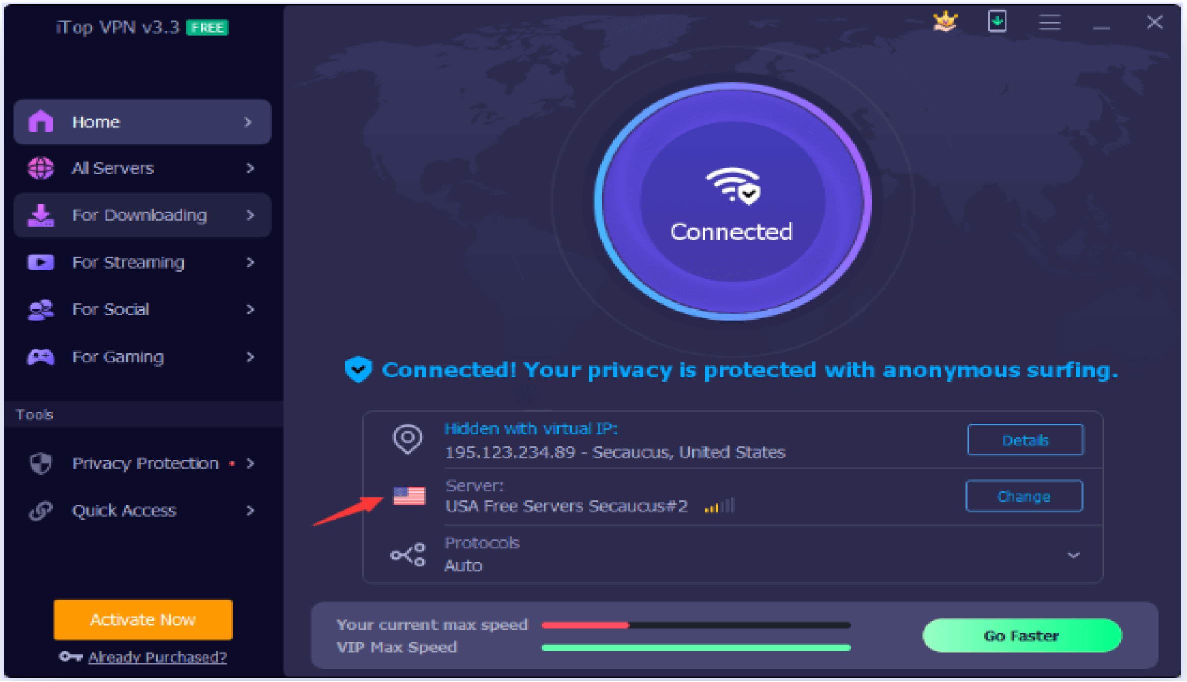


Step 2. Click All Servers in the left navigator. You will see a long list of all available servers in multiple countries, like USA, Mexico, Canada, United Kingdom, etc.



USA Free Servers Secaucus#2 Free — Connect
USA Free Servers Miami Free — Connect
Mexico VIP — Connect
Canada Toronto VIP — Connect
Canada Montreal VIP — Connect
Ireland VIP — Connect
Japan Tokyo#1 VIP — Connect
Japan Tokyo#2 VIP — Connect
Japan VIP IPv6 — Connect
Japan Free Free — Connect
United Kingdom London#1 VIP — Connect
United Kingdom London#2 VIP — Connect

Step 3. To speed up internet on Windows 10, select a server (USA, for instance) and click Connect. Then you can enjoy faster speeds with the USA server in no time.



Connected! Your privacy is protected with anonymous surfing.

Hidden with virtual IP: 195.123.234.89 - Secaucus, United States

Server: USA Free Servers Secaucus#2

Protocols: Auto

Your current max speed

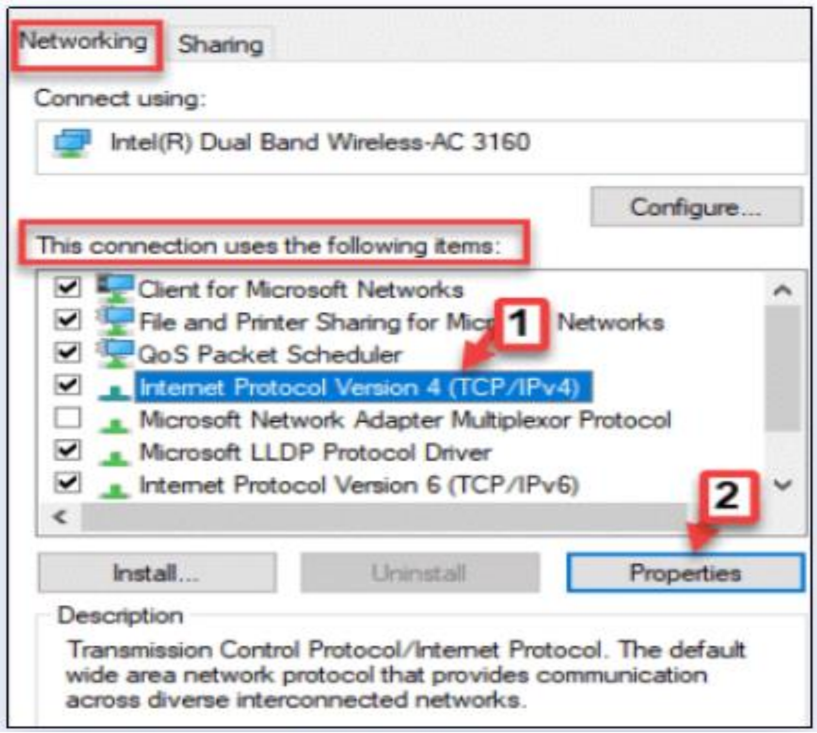
VIP Max Speed

Way 3. Reset DNS Settings to Speed up Internet on Windows 10

Step 1. Search view network connections in search box of Windows 10 and enter it.

Step 2. Then right click on your network adapter and select Properties at the bottom.

Step 3. Now, select Internet Protocol Version 4 from the list under Networking and click on the Properties tab.



Connect using:

Intel(R) Dual Band Wireless-AC 3160

This connection uses the following items:

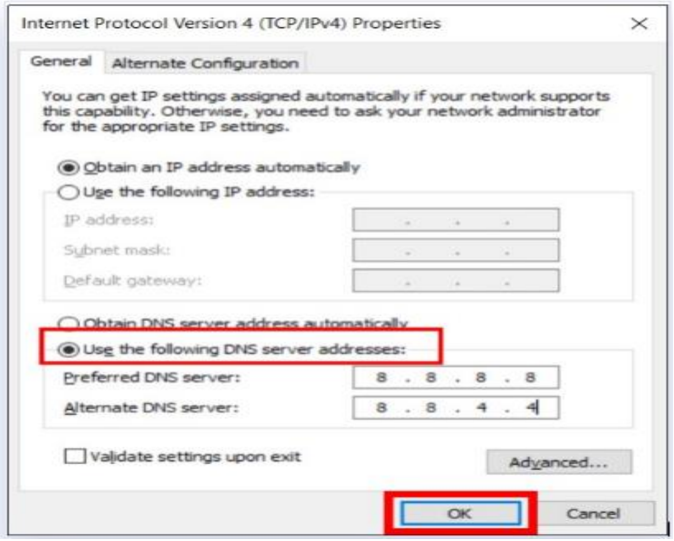
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Step 4. Now, select Use the following DNS server addresses and type to enter Google DNS as follows: 8.8.8.8

8.8.4.4



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: 8 . 8 . 4 . 4

□ Validate settings upon exit

Step 5. Lastly, click on Apply and select OK.

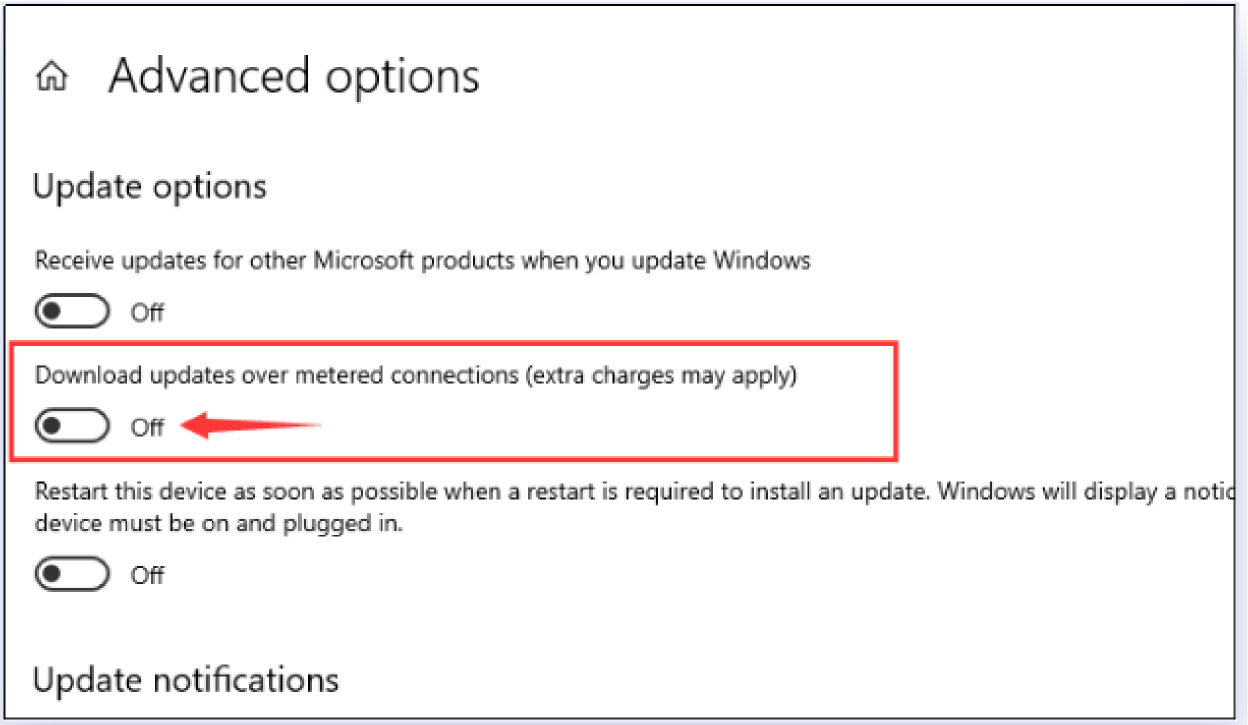
Way 4. Change Adapter Settings to Speed up Internet on Windows 10

Step 1. Press Windows + I key together to open Settings on Windows 10.

Step 2. Now, select Update & Security and click Windows Update from the left menu.

Step 3. Then click on Advanced options from the right side.

Step 4. Turn off Download updates over metered connections (extra charges may apply).



Advanced options

Update options

Receive updates for other Microsoft products when you update Windows
Off

Download updates over metered connections (extra charges may apply)
Off

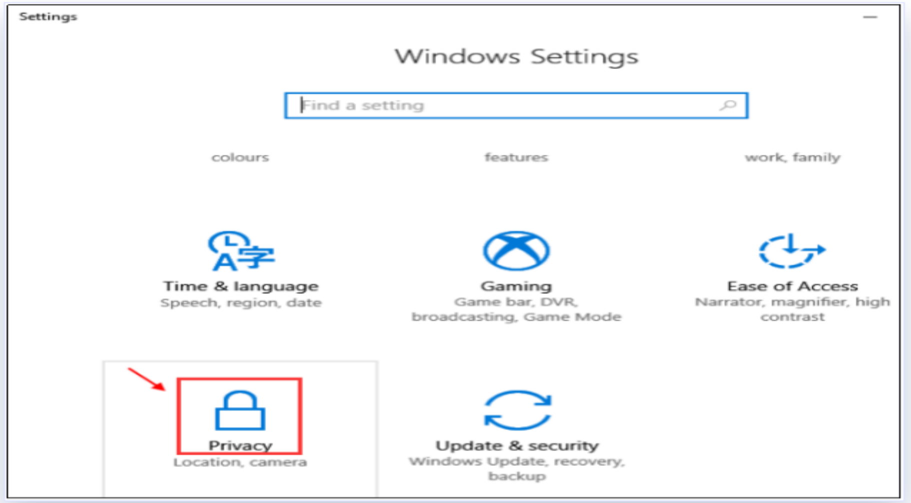
Restart this device as soon as possible when a restart is required to install an update. Windows will display a notic
device must be on and plugged in.
Off

Update notifications

Way 5. Turn off Background Apps to Speed up Internet on Windows 10

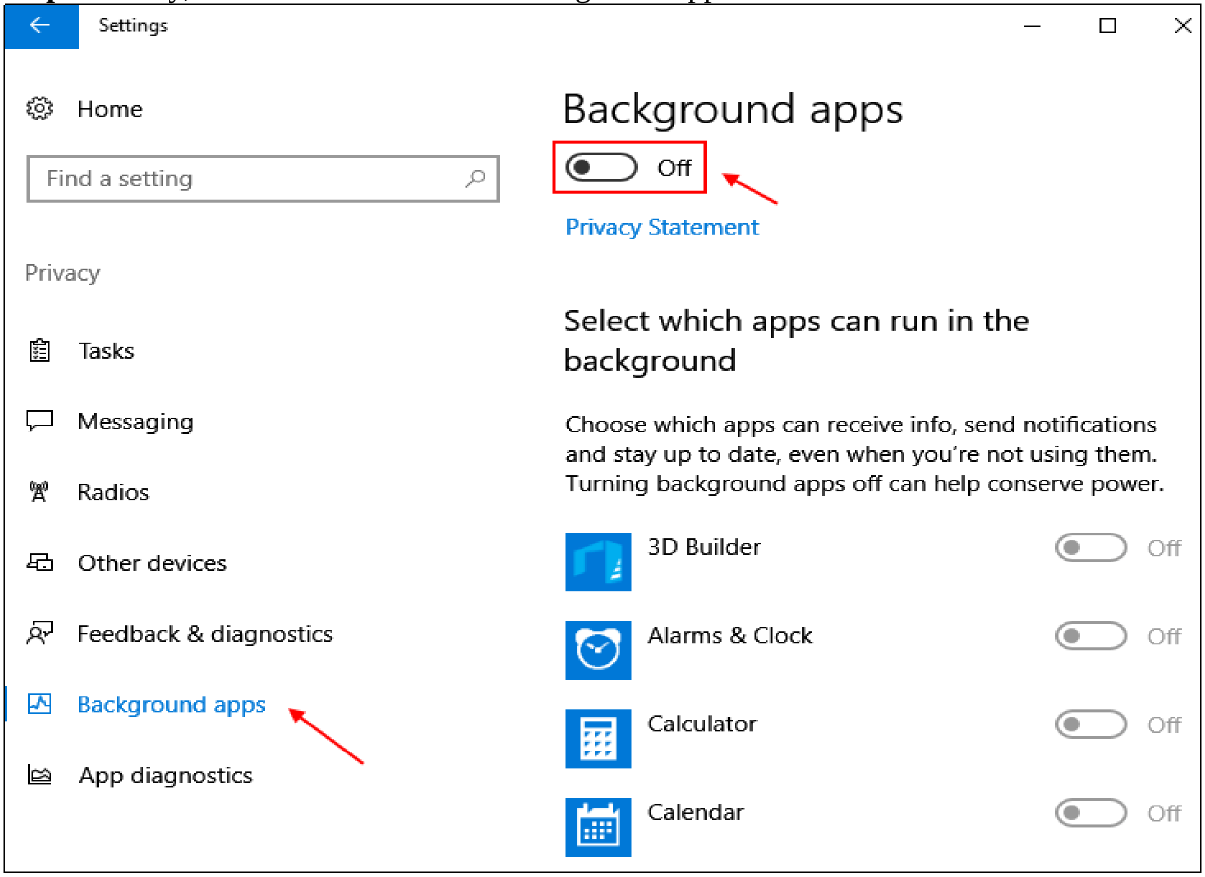
Step 1. Open Settings panel as mentioned in the foregoing part.

Step 2. Then click on Privacy.



Step 3. Now, choose background apps from the left menu.

Step 4. Lastly, switch the button under Background apps to off.



Background apps

Off

Select which apps can run in the background

Choose which apps can receive info, send notifications and stay up to date, even when you're not using them. Turning background apps off can help conserve power.

3D Builder	Off
Alarms & Clock	Off
Calculator	Off
Calendar	Off

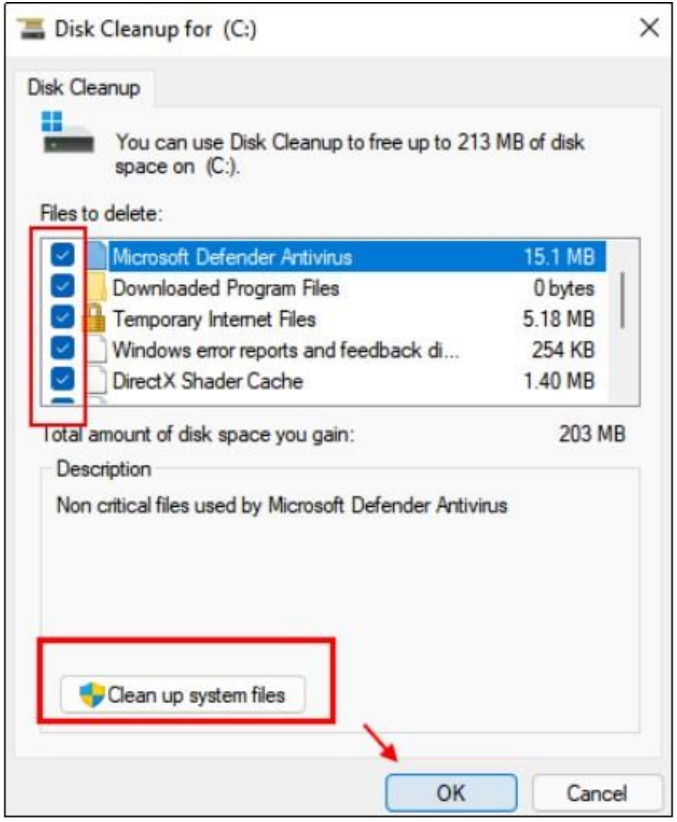
Way 6. Clear Temp and Cached Files to Speed up Internet on Windows 10

Step 1. Search Disk Cleanup in your Windows 10 search box.

Step 2. Next, click on Disk Cleanup.

Step 3. Select C Drive in the pop-up box.

Step 4. Then, select all files from the files list and click OK to delete all useless files on your PC at present.



Disk Cleanup for (C:)

Disk Cleanup

You can use Disk Cleanup to free up to 213 MB of disk space on (C:).

Files to delete:

☑	Microsoft Defender Antivirus	15.1 MB
☑	Downloaded Program Files	0 bytes
☑	Temporary Internet Files	5.18 MB
☑	Windows error reports and feedback di...	254 KB
☑	DirectX Shader Cache	1.40 MB

Total amount of disk space you gain: 203 MB

Description

Non critical files used by Microsoft Defender Antivirus

Step 5. Continue to click on Clean up system files.

Step 6. Also, do remember to clear your recycle bin.

LAP Test

Task 1:- Diagnostic and test network performance

Task 2:- Test download and upload speed of your computer Internet

Unit Four : Migrate to New Technology

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Developing new skills.
- Upgraded technology skills
- Identifying upgraded equipment.
- Sources of information for new or upgraded equipment
- Using new or upgraded equipment

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Develop new skills.
- Upgraded technology skills
- Identify upgraded equipment.
- Understand Sources of information for new or upgraded equipment
- Use new or upgraded equipment

4.1. Basic concept of Migrating to new technology

Migrating to new technology involves the strategic transition from existing technological systems to advanced solutions. This process entails a comprehensive assessment of current infrastructure, careful planning, and seamless execution to optimize efficiency and stay competitive. Successful migration requires evaluating compatibility, scalability, and security aspects, along with effective change management to mitigate disruptions. Post-migration, ongoing support and monitoring are essential to ensure the smooth integration of new technology, enhancing operational capabilities and positioning the organization for sustained growth in a dynamic technological landscape.

4.2. Develop new skills.

Developing new skills in new technology requires a systematic approach and a commitment to continuous learning. Here are steps to help you develop new skills in emerging technologies:

1. **Identify the technology**: Start by identifying the specific technology or field you want to develop skills in. Research and understand its fundamentals, applications, and potential impact in your industry or area of interest.
2. **Set clear goals**: Define your learning goals and objectives. Determine what specific skills, knowledge, or certifications you want to acquire in the new technology.
3. **Assess existing skills**: Evaluate your existing skills and knowledge related to the technology. Identify any foundational knowledge or transferable skills that can serve as a starting point for your learning journey.
4. **Select learning resources**: Identify high-quality learning resources that suit your preferred learning style. These resources may include online courses, tutorials, books, video lectures, forums, or workshops.
5. **Create a learning plan**: Develop a learning plan that outlines the topics, concepts, and skills you need to cover. Break down the learning process into manageable chunks and set a schedule or timeline for your learning activities.
6. **Embrace continuous learning:** Technology evolves rapidly, so commit to continuous learning. Stay curious, explore new developments, and keep up with industry news and updates. Dedicate time regularly to learn and stay updated on advancements in the technology you're focusing on.

4.3. Upgraded technology skills

Upgrading technology skills is an ongoing process that requires dedication, perseverance, and a commitment to lifelong learning. Embrace new challenges, be proactive in seeking opportunities, and apply your upgraded skills in practical settings to maximize their impact.

To upgrade your technology skills, you can follow these one:

- Identify Areas for Improvement:
- Set Clear Goals
- Create a Learning Plan:
- Engage in Practical Projects:
- Stay Updated and Practice Continuously
- Seek Feedback and Networking

4.4. Identify upgraded equipment.

Upgraded equipment refers to the improved or advanced versions of technological devices or tools used in various domains. It involves the enhancement of hardware components, software capabilities, performance, features, or functionalities of a specific piece of equipment. Upgrades can include improvements in processing power, memory capacity, storage capacity, connectivity options, display quality, battery life, security features, or any other aspect that enhances the overall performance or user experience of the equipment. Upgraded equipment often incorporates the latest technological advancements and innovations to deliver superior performance, increased efficiency, and enhanced capabilities compared to previous versions or older models.

1. **Computers:**

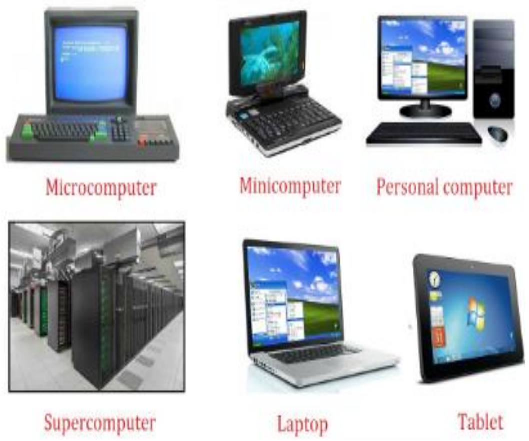


figure 1. 9 upgraded computer

- High-performance desktop computers with advanced processors, increased RAM, and faster storage options like solid-state drives (SSDs).
- Laptops with improved battery life, higher screen resolutions, and enhanced graphics capabilities.
- Workstations designed for intensive tasks such as video editing, 3D rendering, or scientific

simulations, featuring powerful processors, ample RAM, and dedicated graphics cards.

2. **Smartphones:**
   - Flagship smartphones with faster processors, larger RAM capacity, and improved camera technologies.
   - Devices with 5G connectivity for faster internet speeds and lower latency.
   - Smartphones equipped with advanced biometric authentication methods like facial recognition or under-display fingerprint sensors.

Figure 4. 1 upgraded smartphone

3. **Networking:**
   - Upgraded routers with the latest Wi-Fi standards (such as Wi-Fi 6 or Wi-Fi 6E) offering faster speeds and better network performance.
   - Network switches with higher port densities, increased bandwidth, and support for advanced features like Power over Ethernet (PoE) or Quality of Service (QoS).
   - Firewall appliances with enhanced security capabilities, such as intrusion prevention systems (IPS), deep packet inspection (DPI), or advanced threat protection (ATP).

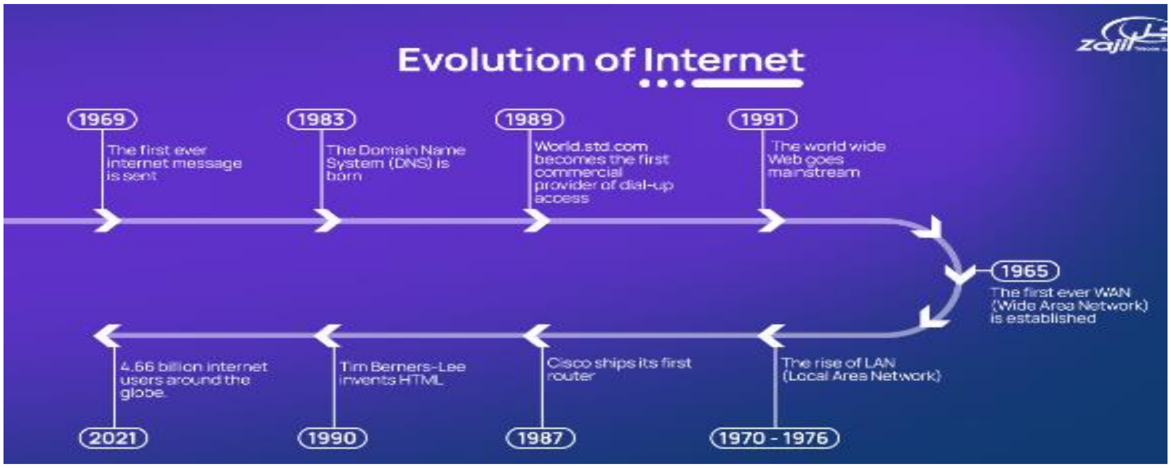

Evolution of Internet
zajil
1969
The first ever internet message is sent
1983
The Domain Name System (DNS) is born
1989
World.std.com becomes the first commercial provider of dial-up access
1991
The world wide Web goes mainstream
1965
The first ever WAN (Wide Area Network) is established
1970 - 1976
The rise of LAN (Local Area Network)
1987
Cisco ships its first router
1990
Tim Berners-Lee invents HTML
2021
4.66 billion internet users around the globe.

Figure 4. 2 History of network

4. **Cameras and Photography:**
    - Digital cameras with higher megapixel counts, improved low-light performance, and advanced autofocus systems.
    - Mirrorless cameras with faster burst shooting rates, improved image stabilization, and high-resolution electronic viewfinders.
    - Drones equipped with high-resolution cameras, obstacle avoidance sensors, and intelligent flight modes for aerial photography and videography.

Figure 4. 3 History of camera

5. **Virtual Reality (VR) and Augmented Reality (AR):**
    - VR headsets with higher display resolutions, wider field of view, and improved tracking accuracy.
    - AR glasses with lightweight designs, better transparent display technology, and enhanced gesture recognition.

- Controllers and haptic devices that provide more precise and immersive interactions within virtual environments.

Figure 4. 4 Virtual Reality (VR) and Augmented Reality (AR)

4.5. Understand Sources of information for new or upgraded equipment

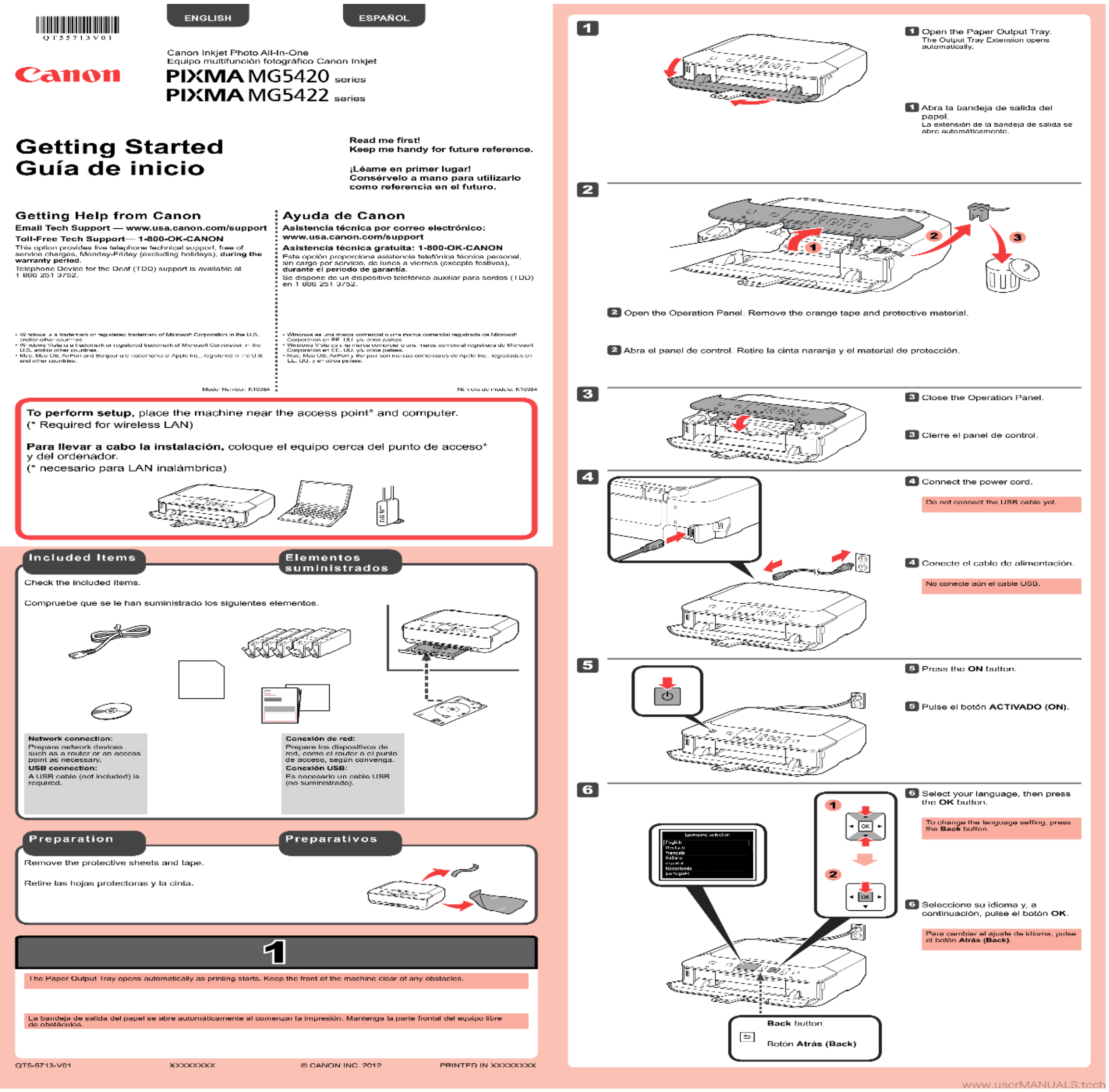
1. **Manufacturer Websites:** The official websites of equipment manufacturers provide comprehensive and accurate information about their products. These websites often include detailed specifications, features, pricing, and availability of the latest models or upgrades.
2. **Technology News Websites**: Websites that specialize in technology news and reviews, such as CNET, Engadget, The Verge, PCMag, and Gizmodo, offer up-to-date coverage on new and upgraded equipment. They provide in-depth articles, reviews, comparisons, and expert insights into the latest technology trends and advancements.
3. **Industry-specific Publications**: Industry publications and magazines dedicated to specific fields or sectors often feature articles and reviews about new or upgraded equipment. Examples include Wired, Popular Science, IEEE Spectrum, or Automotive News, depending on your area of interest.
4. **Online Forums and Communities:** Online forums and communities focused on specific equipment or technology domains are valuable sources of information. Platforms like Reddit, specialized forums, or dedicated Facebook groups allow users to discuss, share experiences, and ask questions about new or upgraded equipment.
5. **Professional Networks and Colleagues**: Networking with professionals in your industry or field can provide valuable insights into new or upgraded equipment. Engaging with colleagues, attending industry events, or joining professional organizations can help you

tap into their expertise and firsthand experiences with the equipment you are interested in.

4.6. Use new or upgraded equipment

When organizations want to make a significant change to their business systems, new technology or new equipment is generally part of the change. Using new or upgraded equipment typically involves several steps to ensure a smooth and efficient transition. Here is a general guide:

1. **Read the Manual**:- Start by thoroughly reading the user manual or any accompanying documentation that comes with the equipment. This will provide you with a detailed understanding of its features, functionalities, and proper usage.



ENGLISH ESPAÑOL

QT55713V01

Canon

Canon Inkjet Photo All-In-One
Equipo multifunción fotográfico Canon Inkjet
PIXMA MG5420 series
PIXMA MG5422 series

Getting Started
Guía de inicio

Read me first!
Keep me handy for future reference.

¡Léame en primer lugar!
Consérvelo a mano para utilizarlo como referencia en el futuro.

Getting Help from Canon
Email Tech Support — www.usa.canon.com/support
Toll-Free Tech Support— 1-800-OK-CANON
This option provides live telephone technical support, free of service charges, Monday-Friday (excluding holidays), **during the warranty period.**
Telephone Device for the Deaf (TDD) support is available at 1-866-251-3752.

- Windows is a trademark or registered trademark of Microsoft Corporation in the U.S. and/or other countries.
- Windows Vista is a trademark or registered trademark of Microsoft Corporation in the U.S. and/or other countries.
- Mac, Mac OS, AirPort and Bonjour are trademarks of Apple Inc., registered in the U.S. and other countries.

Model Number: K10384

Ayuda de Canon
Asistencia técnica por correo electrónico: www.usa.canon.com/support
Asistencia técnica gratuita: 1-800-OK-CANON
Esta opción proporciona asistencia telefónica técnica personal, sin cargo por servicio, de lunes a viernes (excepto festivos), **durante el período de garantía.**
Se dispone de un dispositivo telefónico auxiliar para sordos (TDD) en 1-866-251-3752.

- Windows es una marca comercial o una marca comercial registrada de Microsoft Corporation en EE. UU. y/u otros países.
- Windows Vista es una marca comercial o una marca comercial registrada de Microsoft Corporation en EE. UU. y/u otros países.
- Mac, Mac OS, AirPort y Bonjour son marcas comerciales de Apple Inc., registradas en EE. UU. y en otros países.

Número de modelo: K10384

To perform setup, place the machine near the access point* and computer.
(* Required for wireless LAN)

Para llevar a cabo la instalación, coloque el equipo cerca del punto de acceso* y del ordenador.
(* necesario para LAN inalámbrica)

Included Items **Elementos suministrados**

Check the included items.

Compruebe que se le han suministrado los siguientes elementos.

Network connection:
Prepare network devices such as a router or an access point as necessary.
USB connection:
A USB cable (not included) is required.

Conexión de red:
Prepare los dispositivos de red, como el router o el punto de acceso, según convenga.
Conexión USB:
Es necesario un cable USB (no suministrado).

Preparation **Preparativos**

Remove the protective sheets and tape.

Retire las hojas protectoras y la cinta.

1

The Paper Output Tray opens automatically as printing starts. Keep the front of the machine clear of any obstacles.

La bandeja de salida del papel se abre automáticamente al comenzar la impresión. Mantenga la parte frontal del equipo libre de obstáculos.

QT5-5713-V01 XXXXXXXX © CANON INC. 2012 PRINTED IN XXXXXXXX

1 Open the Paper Output Tray.
The Output Tray Extension opens automatically.

1 Abra la bandeja de salida del papel.
La extensión de la bandeja de salida se abre automáticamente.

2 Open the Operation Panel. Remove the orange tape and protective material.

2 Abra el panel de control. Retire la cinta naranja y el material de protección.

3 Close the Operation Panel.

3 Cierre el panel de control.

4 Connect the power cord.

Do not connect the USB cable yet.

4 Conecte el cable de alimentación.

No conecte aún el cable USB.

5 Press the **ON** button.

5 Pulse el botón **ACTIVADO (ON)**.

6 Select your language, then press the **OK** button.

To change the language setting, press the **Back** button.

6 Seleccione su idioma y, a continuación, pulse el botón **OK**.

Para cambiar el ajuste de idioma, pulse el botón **Atrás (Back)**.

Back button

Botón **Atrás (Back)**

Figure 4. 5 User manual of printer

2. **Familiarize Yourself**: Take some time to get familiar with the equipment. Explore its buttons, controls, and settings. Understand how to power it on/off, adjust settings, and navigate through different menus or options.
3. **Practice Hands-On:** Engage in hands-on practice with the equipment. Start with simple tasks or basic functions to gain confidence and gradually progress to more complex operations. Experiment with different settings and features to understand their impact and functionality.
4. **Seek Training or Tutorials**: If available, attend training sessions or workshops related to the equipment. Alternatively, search for online tutorials, video guides, or forums where you can learn from others' experiences and expertise.
5. **Troubleshooting and Maintenance:** Familiarize yourself with common troubleshooting techniques specific to the equipment. Learn how to identify and resolve common issues that may arise during usage.

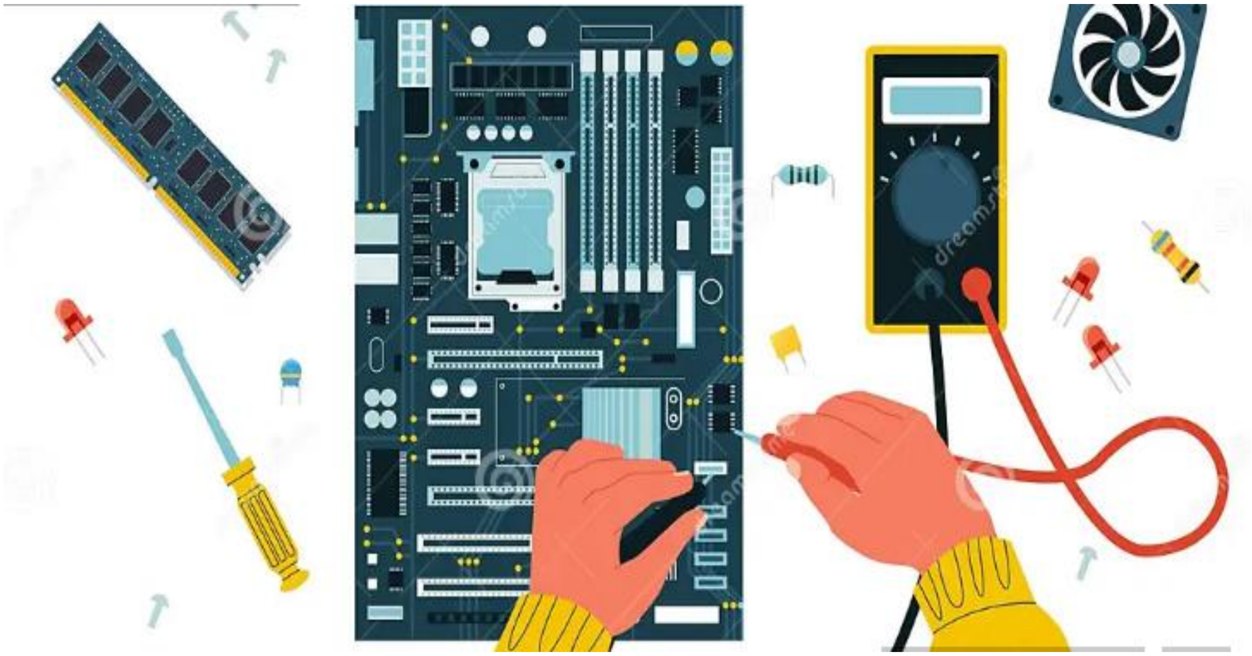


Figure 4. 6 Troubleshooting and Maintenance

Self-check - 4

Part I: - Say **True** if the given statement is correct else say **False**

_______1. Upgrading technology skills involves identifying upgraded equipment.

_______2. Understanding sources of information for new or upgraded equipment is necessary when upgrading technology skills.

_______3. Using new or upgraded equipment is not important in the process of upgrading technology skills.

Part II: - Select the appropriate answer from the given alternative

1. Which of the following is a benefit of identifying upgraded equipment when upgrading technology skills?

A. It improves physical fitness
C. It boosts creativity in art and design
B. It enhances problem-solving abilities
D. It promotes healthy eating habits

2. How does using new or upgraded equipment contribute to upgrading technology skills?

A. It improves social interaction skills
B. It enhances critical thinking abilities
C. It promotes physical well-being
D. It develops musical talent

3. Which of the following is an example of upgraded equipment in the context of upgrading technology skills?

A. Pencil and paper
C. Smartphone
B. Typewriter
D. Abacus

4. Which of the following is a direct outcome of upgrading technology skills?

A. Building a sandcastle
C. Writing poetry
B. Solving complex technological problems
D. Playing sports

Part III: - Give short answer

1. List and explain Sources of information for new or upgraded equipment?
2. Demonstrate the way of develop new skills in emerging technologies?
3. List and explain upgraded equipment in ICT?

Reference Books

1. The Practice of System and Network Administration
2. Network Security Essentials: Applications and Standards" by William Stallings
3. Network Programmability and Automation: Skills for the Next-Generation Network Engineer" by Jason Edelman, Scott S. Lowe, and Matt Oswalt
4. Network Management: Principles and Practice" by Mani Subramanian:
5. Network Analysis, Architecture, and Design" by James D. McCabe

List of website

1. https://www.windowscentral.com/how-make-full-backup-windows-10#section-how-to-restore-a-backup-with-system-image-tool-on-windows-10
2. https://www.comparitech.com/net-admin/network-troubleshooting-tools/
3. https://www.itechguides.com/how-to-get-administrator-privileges-on-windows-10/
4. Make an administrator account to a standard user on Windows 10/11 (softwareok.com)
5. https://www.devicemag.com/network-testing-tool/
6. https://www.itopvpn.com/blog/speed-up-internet-on-windows-10-3123

Developer profile

No	Name	Qualification (Level)	Field of Study	Organization/ Institution	Mobile number	E-mail
1	Zerihun Abate	MSc	ITM	Sebata PTC	0911858358	zedoabata2017@gmail.com
2	Abebe Mintefa	MSc	ITM	Ambo TVETC	0929362458	tolabula@gmail.com
3	Endale Berekat	Bsc	Computer Science	M/G/M/B/P/T/C	0915439694	zesaron1221@gmail.com
4	Yinebeb Tamiru	Bsc	Computer science	Akaki PTC	0936325182	yinebebtamiru07@gmail.com