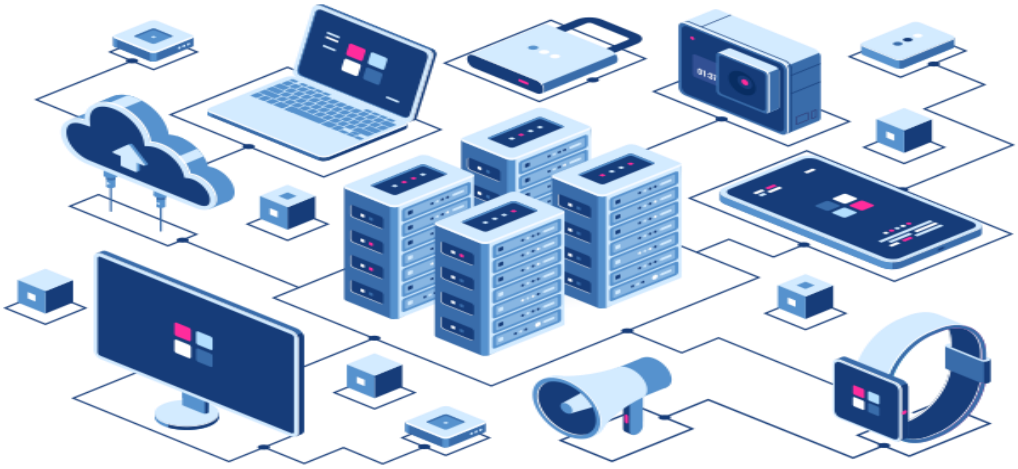
Hardware and Network servicing

Level-IV

Based on November 2023, Curriculum Version 2



Module Title: - Build Internet Infrastructure

Module Code: EIS HNS4 M02 1123

Nominal duration: 50 Hours

Prepared by: Ministry of Labor and Skill

November 2023

Addis Ababa, Ethiopia

Contents

Acknowledgment iii
Introduction to the Module v
Module Instruction v
Acronym iv
Unit one: Plan and design internet infrastructure 6
1.1. Introduction to Internet Infrastructure 7
1.2. Confirming internet service 15
1.3. Ensuring Hardware, Software and security Requirements 17
1.4. Internet Protocol Address allocation 23
Self-Check 1 34
Unit Two: Install and configure internet infrastructure and services 35
2.1. Installing and testing cables 36
2.2. Mail servers 40
2.4. Hardware and software for internet connection 44
2.5. Configuring Domain names and internet protocol address 44
2.6. Deploying and configuring Software 47
Self check 2 50
Unit Three : Test security and internet access 51
Introdction to Internet security 52
Security access level 52
3.1.1. System Security, capability and reliability 55
3.2. Making system changes 60
Self check 3 63
Unit Four: Ensure user accounts are verified for security 64

4.1 Verifying user settings for security policy 65

4.2 Displaying legal notices 65

4.3 Checking and verifying passwords 66

Self- check 4 69

Operation sheet 4: Configure Group Policy 70

Lap Tests 72

Unit Five: Manage and support internet 73

5.1. Managing Internet Infrastructure 74

5.2. Tools and equipment 75

Internet performance 76

Self check 5 77

Unit Six: Plan and Organize Work 78

6.1. Setting objectives 79

6.2. Planning and prioritizing work activity 82

6.3. Scheduling work activities 84

6.4. Implementing work plan 85

Self-Check 6 88

Reference 89

Participants of this Module preparation 90

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

LAN: Local Area Network
OHS: Occupational Health Safety
PC : Personal computer
ATM: Automated Teller Machine
FDDI: Fiber Distirbuted Data Interface
AC: Alternative Current
IGES: Graphics Exchange Specification
ISO: International Standards Organization
RFI: Request for Information
NIC: Network Interface Card
IP: Internet Protocol
SMTP: Simple Mail Transfer Protocol
FTP: File Transfer Protocol
HTTP: Hyper Text Transfer Protocol
HTTPS: Hyper Text Transfer Protocol Secured
DHCP: Dynamic Host configuration
DNS: Doman Name system
EMI: Electromagnetic interference
CAT: Category
TP: Twisted Pair
RJ: Register Jack
TIA: Telecommunications Industries Association
EIA: Electronics Industry Association
MTA: Mail transfer agents
MDA: mail delivery agents
IPv4: Internet Protocol version 4
IANA: Internet Assigned Numbers Authority
FTP: File Transfer Protocol
DMZ: Demilitarized Zone
NAT: Network Address Translation
OS: Operating System
ACL: Access Control List
CSS: Cascade sheet

Introduction to the Module

Internet is a global network system connecting thousands of computers all over the world so as to share information and services. The Internet protocol suite is a framework defined through the Internet standards. Methods are divided right into a layered set of protocols on this architecture. The Internet gives a huge variety of statistics and communique offerings, which includes forums, databases, email, and hypertext. It is made of the neighborhood to global personal, public networks connected through plenty of digital, wireless, and networking technologies.

This module is designed to meet the industry requirement under the **hardware and Networking service** occupational standard, particularly for the unit of competency: **Build Internet infrastructure.**

This module covers the units:

- Internet infrastructure
- Install and configure internet
- Internet security and access
- User account and account security
- Internet management and support

Learning Objective of the Module

- Plan and design internet infrastructure
- Install and configure internet infrastructure and services
- Test security and internet access
- Ensure user accounts are verified for security
- Manage and support internet
- Plan and Organize Work

Module Instruction

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

1. Read the information written in each unit
2. Accomplish the Self-checks at the end of each unit
3. Perform Operation Sheets which were provided at the end of units
4. Do the “LAP test” given at the end of each unit and
5. Read the identified reference book for Examples and exercise

Unit one: Plan and design internet infrastructure

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

- Introduction to Internet Infrastructure
  - Business Needs and Functions
  - LAN Communication Technologies
  - Internet Technologies
  - OH&S requirements
- confirming internet service
- Ensuring hardware, software, and security requirements
- Internet protocol address allocation

This guide 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:

- Define the term Internet Infrastructure
- Define Business Needs and Functions
- Explain LAN Communication Technologies
- Specified hardware , software and security requirement
- Define network protocol allocation

1.1. Introduction to Internet Infrastructure

One of the greatest things about the internet is that nobody really owns it. It is a global collection of networks, both big and small. These networks connect in many different ways to form the single entity that we know as the internet. Since its beginning in 1969, the internet has grown from four host computer systems to tens of millions. The Internet Society, a nonprofit group established in 1992, oversees the formation of the policies and protocols that define how we use and interact with the internet.

Internet Infrastructure

- Internet Infrastructure is a set of physical and logical components that provide connectivity, security, routing, management, access, and other integral features on a network.
- During a network's planning phase, Network Professionals select the hardware and software components that will compose the network infrastructure and specify the particular location, installation, and configuration of those components.
- It is rare for a network designer to have the opportunity to design a network from scratch, with no pre-existing influences.
- Nearly always, the designer must incorporate some existing elements into the network design, such as specific applications, operating systems, protocols, or hardware components.
- Implementing a network infrastructure is the process of evaluating, purchasing, and assembling the specified components, and installing them in the manner prescribed by the design plan.
- The implementation process begins with installing the network's hardware infrastructure, including computers, cables, and connectivity devices such as hubs, switches, and routers, as well as printers and other peripherals.
- Once the hardware is in place, the Technicians install and configures the operating systems, applications, and other software.
- The significance of the network infrastructure does not end when the construction of the network is complete, however.
- The personnel responsible for maintaining the network must have an intimate knowledge of the network's infrastructure to expand the network, perform upgrades, and troubleshoot problems.

Business Needs and Functions

- Business functions are the things a business does to provide the product or service that it offers. At the highest level is the primary business function.
- This principal function reflects why the company exists.

Examples of a primary business function include

- Providing tutoring services to college students
- Manufacturing precision parts for airplanes
- Building custom homes

- Some businesses have one primary business function, while others may have more than one. However, it's possible to articulate these as a single function.
- For example, a business that provides computer security and help desk management might have a primary function of providing comprehensive IT services.
- The Internet has revolutionized the way companies do business. With its help, the global marketplace is more accessible, connected, inclusive, and diverse.
- The Internet provides many benefits for business development, communication, and collaboration.
- Today companies and organizations are using high-speed Internet to accelerate their business operations and growth strategy.
- They rely strongly on this technology to enhance productivity and achieve operational efficiency. So choosing the right business internet connection can seem like a hard process.
- There are a huge number of providers on the market offering a surplus of different packages and service levels – so where do you start?

1: Understand your business' needs

- In order to choose a suitable business internet connection, you'll need to understand your organization's current and future IT requirements.

2: Find out which types of internet connection are available to you

- Not all business internet connection types are available in all parts of the country. Your choices will probably include the following:

3: Figure out what you're paying for

- ISP marketing is often price-focused, but when you're buying for business it's even more important to read the small print.

- Prices quoted online tend to reflect the basic, entry-level package and are sometimes conditional on signing up for a minimum period but be wary of committing for longer than two years as services, providers, technology and pricing change frequently in this market.

Assessing User Requirements

In general, users primarily want application availability in their networks. The chief components of application availability are response time, throughput, and reliability:

- Response time is the time between entry of a command or keystroke and the host system's execution of the command or delivery of a response.
- User satisfaction about response time is generally considered to be a monotonic function up to some limit, at which point user satisfaction falls off to nearly zero.
- Applications in which fast response time is considered critical include interactive online services, such as automated tellers and point-of-sale machines.
- Applications that put high-volume traffic onto the network have more effect on throughput than end-to-end connections. Throughput-intensive applications generally involve file-transfer activities.
- However, throughput-intensive applications also usually have low response-time requirements. Indeed, they can often be scheduled at times when response-time–sensitive traffic is low (for example, after normal work hours).
- Although reliability is always important, some applications have genuine requirements that exceed typical needs. Organizations that require nearly 100% uptime conduct all activities online or over the telephone. Financial services, securities exchanges, and emergency/police/military operations are a few examples. These situations imply a requirement for a high level of hardware and topological redundancy. Determining the cost of any downtime is essential in determining the relative importance of reliability to your network.

- You can assess user requirements in a number of ways. In general, you can use the following methods to obtain this information:
  - **User community profiles**. Outline what different user groups require. This is the first step in determining network requirements.
  - **Interviews, focus groups, and surveys**.
    - ✓ Build a baseline for implementing a network. Understand that some groups might require access to common servers.
    - ✓ Others might want to allow external access to specific internal computing resources.
    - ✓ Certain organizations might require IS support system to be managed in a particular way according to some external standard.
    - ✓ Focus groups can also be used to gather information and generate discussion among different organizations with similar (or dissimilar) interests.
    - ✓ Finally, formal surveys can be used to get a statistically valid reading of user sentiment regarding a particular service level or proposed networking architecture.
  - **Human factors tests**. The most expensive, time-consuming, and possibly revealing method is to conduct a test involving representative users in a lab environment.
    - ✓ This is most applicable when evaluating response-time requirements.
    - ✓ You might set up working systems and have users perform normal remote host activities from the lab network, for example.
    - ✓ By evaluating user reactions to variations in host responsiveness, you can create benchmark thresholds for acceptable performance.

LAN Communication Technologies

- A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.
- This section focuses on the selection of appropriate LAN technologies for a network.
- Many options are available. At the more traditional end of the LAN technology spectrum, we have various flavors of Ethernet and Token Ring.
- Competing with these technologies are some very interesting modern alternatives such as ATM and wireless networking.

- Each of these different technologies has its strengths and weaknesses. Some are strikingly effective in certain situations, while difficult in others.
- We should consider four main factors when selecting a LAN technology:
  - Cost efficiency
  - Installed base
  - Maintainability
  - Performance

Cost Efficiency

- Cost efficiency is one of the most important factors that must be considered while selecting LAN technology.
- Generally, it was considered that faster technology is more expensive but this was not universally true.

Installed Base

- The installed base is considered another important factor in cost-effectiveness.
- There are very less chances that you are using scratch for building a new network.
- Generally, there are existing applications, existing equipment, servers, and a cable plant. There is an availability of alternative network technology which is cheaper.
- If you are switching to that then you require a very high cost for changing your installed base. So in this situation staying with existing technology may be considered more cost-effective.

Maintainability

- Maintenance is considered the one of biggest hidden network costs.
- Generally, your design targets are centered toward reliability, the reliability is reduced as you cut more corners.
- Lower reliability is usually converted into very high maintenance costs for the network.

Performance

- Everyone tries to put their efforts into building the fastest and best network. Here best means the network that will fulfill the need of the business.
- If the network does not support the application for which it was built but has unbelievable throughput and low latency, then that network becomes useless.

Internet Technologies

- The Internet is a collection of computers that communicate using a standard set of protocols.
- Since there are now millions of computers involved in the Internet, it has grown to be a major means of communication and allows for users to interact with little regard to distance or location.
- Associated with the Internet is a set of technologies ranging from network protocols to browsers that have been developed to support Internet operations.
- This topic gives a description of the basis of these Internet technologies and how these can be used by corporations to improve their operations.

Network standards

- Standards are a necessary part of most technological developments, and have been developed since the early days of the industrial revolution.
- The use of interchangeable parts by Eli Whitney is an example of the early use of standards, although these standards were necessarily ad-hoc in nature.
- As the process of industrialization has gathered pace so too has the formulation of standards, ranging from standards of measurements (the metric standard is an example) to that of computer networks.
- Complete and adequate standards allow for interaction between individuals, groups and corporations since each party can base their operations on the same standards and avoid the needless confusion that will otherwise necessarily result.

Standards Organizations

- The first mechanism is where a body, usually international in nature, develops a standard based on a consideration of the multiple factors that are of concern. An example is the Initial Graphics Exchange Specification (IGES) which was adopted as a standard in 1981 to allow for the exchange of Computer Aided Design drawings.
- This method of developing standards tends to be extremely slow with frequent delays caused by the deliberations of the, usually, many bodies involved.

- The main advantage of this method of developing standards is that a wide variety of considerations can be brought to bear in the standard and methods are usually developed for maintaining the standard.

De Facto Standards

- The second mechanism of developing a standard is what may be thought of as a direct result of widespread use. If, for example, a computer file format is in widespread use then this can become a de facto standard. An example is the DXF file format for Computer Aided Design files that was used initially by the AutoCAD computer package.
- As this package had the main market share of CAD packages on personal computers, then the DXF file format became a de facto standard.
- The main advantage of developing standards in this manner is that of speed since such standards can be very quick to emerge. The main disadvantages are that these standards can change very quickly, they can be proprietary in nature, and there may be no international body that maintains the standard so that it can fragment.
- In terms of computer networks then separate standards have been developed by each of these two methods.
- The standards organization manner of developing standards has resulted in the ISO model while the (approximately) de facto manner has resulted in the development of TCP/IP.

ISO MODEL

- The International Standards Organization (ISO), based in Geneva Switzerland, is composed of groups for various countries that set standards working towards the establishment of world-wide standards for communication and data exchange.
- One notable accomplishment has been the development of a reference model that contains specifications for a network architecture for connecting dissimilar computers, with a main goal being that of producing an open and nonproprietary method of data communication.
- This reference model, called the Open Systems Interconnect Reference Model (OSI RM), was developed in 1981 (?) and revised in 1984.
- The OSI RM uses 7 layers, each independent of each other, to allow computers to exchange data. To transfer a message from user A to user B, the data has to pass through

the 7 layers on user's A machine, before being transmitted through the selected medium. At the receiving computer of user B, the data must then pass through the 7 layers again, this time in reverse sequence, before being received by user B. For data to be transferred, it must pass through all 7 players on both computers.

- The layers are arranged in order as follows:
  - **Layer 7, Application Layer.** This layer defines network applications such as error recovery, flow control and network access. Note that user applications are not part of the layers.
  - **Layer 6, Presentation Layer.** This layer determines the format used to exchange data in such aspects as data translation, encryption and protocol conversion. The data from user A is translated to a common syntax that can be understood by user B. In this way it specifies how applications can connect to the network and to user B.
  - **Layer 5, Session Layer.** This layer controls the communication session between computers. It is responsible for establishing and removing communication sessions between computers. Additional address translations and security are also performed. This layer therefore instigates a data transfer session between user A and user B so that an extended data transfer can take place.
  - **Layer 4, Transport Layer.** This layer is responsible for ensuring that data is delivered free of error and provides some flow control. This layer ensures that data is transferred as part of the session instigated by the Session Layer.
  - **Layer 3, Network Layer.** This layer handles the delivery of data by determining the route for the information to follow. The data is divided into packets with addressing information attached. It also translates address from names into numbers. Intermediate addresses are also attached.
  - **Layer 2, Data Link Layer.** This layer defines the network control mechanism and prepares the packets for transmission.
  - **Layer 1, Physical Layer.** This layer is concerned with the transmission of binary data between stations and defines the connections. The connection definition includes such aspects as mechanical, electrical, topology and bandwidth aspects.

OHS requirements

- OHS requirements are the rules and standards that apply to occupational health and safety (OH&S) in different workplaces and industries.
- OH&S is the practice of managing risks to the health and safety of everyone in the workplace, including workers, customers, visitors and suppliers.
- OH&S aims to prevent or reduce workplace injuries, illnesses and incidents, and to promote worker health, safety and wellbeing.
- Some common elements of OHS requirements are:
  - OH&S policy: outlines the organization's commitment and approach to OH&S.
  - OH&S management system: provides a framework for planning, implementing, operating, auditing and reviewing OH&S activities and performance.
  - OH&S risk assessment: identifies and evaluates the hazards and risks in the workplace and determines the appropriate control measures.
  - OH&S training and education program: provides workers with the necessary information, instruction and supervision to perform their work safely and competently.
  - OH&S consultation and communication process: involves workers and other stakeholders in OH&S decision making and feedback.
  - OH&S monitoring and evaluation process: measures and reports on OH&S performance and outcomes, and identifies areas for improvement.
  - OH&S compliance process: ensures the organization meets its legal and regulatory obligations regarding OH&S .

1.2. Confirming internet service

- To design a network that meets customers' needs, the organizational goals, organizational constraints, technical goals, and technical constraints must be identified. This section describes the process of determining which applications and network services already exist and which ones are planned, along with associated organizational and technical goals and constraints. We begin by explaining how to assess the scope of the design project. After gathering all customer requirements, the designer must identify

and obtain any missing information and reassess the scope of the design project to develop a comprehensive understanding of the customer's needs.

- Assessing the Scope of a Network Design Project.
- When assessing the scope of a network design, consider the following:
  - Whether the design is for a new network or is a modification of an existing network.
  - Whether the design is for an entire enterprise network, a subset of the network, or a single segment or module. For example, the designer must ascertain whether the design is for a set of Campus LANs, a WAN, or a remote-access network.
  - Whether the design addresses a single function or the network's entire functionality.

Developing the design requirements

- Developing the design requirements is a crucial step in the engineering design process.
- It involves defining the characteristics and features that your solution must have to meet the needs and expectations of your users and stakeholders.
- To develop the design requirements, you can follow these technics:
  - Review your problem statement and research findings to identify the main goals and objectives of your project, user needs and preferences, and constraints and criteria.
  - Brainstorm possible design requirements based on your problem statement and research findings. You can use different types of design requirements, such as cost, aesthetics, performance, environmental, manufacturing, etc. You can also use existing products or solutions as examples or inspiration for your design requirements.
  - Prioritize and select the most important and relevant design requirements for your project. You can use different methods to prioritize and select your design requirements, such as ranking, rating, voting, matrix, etc. You can also involve your users and stakeholders in this process to get their feedback and input.
  - Write down your design requirements in a clear and concise way. You can use a table or a list to organize your design requirements. You can also use SMART criteria (Specific, Measurable, Achievable, Relevant, and Time-bound) to make sure your design requirements are well-defined and realistic.

- Review and revise your design requirements as needed. You can test your design requirements against your problem statement and research findings to make sure they are aligned and consistent. You can also update your design requirements as you learn more from your prototyping and testing phases.

1.3. Ensuring Hardware, Software and security Requirements

- The following are the methods of connecting a computer to the Internet using software and hardware peripherals.
  - Connecting a computer using Wireless Broadband
  - Connecting a computer using an Ethernet Cable
  - Connecting a Computer Using Dial-Up Community

Hardware Requirement

- To connect the Internet, any one of the following is mandatory.
  - Modem is used to connect Internet through Telephone connection.
  - NIC- Network Interface Card(wired/ wireless) facility is the most important hardware required to connect Internet. For example, Laptop can be connected Internet through the wired/wireless.
  - Dongle is used to connect the Internet using cellular network
  - Wi-Fi router or Hotspot is used to connect the Internet using wireless network
  - Electronic device which supports cellular network
  - Internet Connectivity such as Dial-up connection, ISDN, DSL, Cable TV, wired and wireless (Cellular) Network.

Software Requirement

The operating system should support TCP (Transfer Control Protocol) / IP (Internet Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), HTTP (Hyper Text Transfer Protocol) and HTTPS (Hyper Text Transfer Protocol Secured) protocols. Browsers and other Internet clients access to the web applications such as Gmail, Whatsapp, Facebook, Twitter etc.

Network security

- Cybercrime is one of the fastest-growing forms of criminal activity. The global cost of dealing with the damage caused by cybercrime is estimated to reach $6 trillion by 2021 doubling the damage recorded in 2015. According to some reports, the average cost of a cyberattack is more than $1 million, and is also expected to rise.
- It's more important than ever to ensure you're providing your customers with the best network security possible. Unfortunately, hackers and cyber attackers are persistent and devious, which means you must proactively leverage-networking security tools to establish and maintain an effective line of defense.
- This piece will provide a rundown of the key things you need to know about the different types of network security tools.

Network security types

- Network security refers to the various countermeasures put in place to protect the network and data stored on or passing through it. Network security works to keep the network safe from cyber-attacks, hacking attempts, and employee negligence.
- There are three components of network security: **hardware**, **software**, and **cloud services**.
- Hardware appliances are servers or devices that perform certain security functions within the networking environment. Hardware can be installed out of the path of network traffic, or "out-of-line," but it's more commonly installed in the path of traffic, or "in-line."
- The advantage of this is that in-line security appliances are able to stop data packets that have been flagged as potential threats, whereas out-of-line appliances simply monitor traffic and send alerts when they detect something malicious.
- Network security software, which includes antivirus applications, can be installed on devices and nodes across the network to provide added detection and threat remediation.
- Cloud services refer to offloading the infrastructure to a cloud provider.
- The set-up is generally similar to how network traffic passes through in-line hardware appliances, but incoming network traffic is redirected to the cloud service instead.
- The cloud service does the work of scanning and blocking potential threats for you before the traffic is allowed onto your network.

Different types of network security devices and tools

You can incorporate quite a few different networking security tools into your line-up of services. The following list is by no means exhaustive, but available security tools can include

- **Access control.** This refers to controlling which users have access to the network or especially sensitive sections of the network. Using security policies, you can restrict network access to only recognized users and devices or grant limited access to noncompliant devices or guest users.
- **Antivirus and anti-malware software.** Malware,
  - ✓ malicious software," is a common form of cyber-attack that comes in many different shapes and sizes.
  - ✓ Some variations work quickly to delete files or corrupt data, while others can lie dormant for long periods of time and quietly allow hackers a back door into your systems.
  - ✓ The best antivirus software will monitor network traffic in real time for malware, scan activity log files for signs of suspicious behavior or long-term patterns, and offer threat remediation capabilities.
- **Application security.** Each device and software product used within your networking environment offers a potential way in for hackers. For this reason, it is important that all programs be kept up-to-date and patched to prevent cyber attackers from exploiting vulnerabilities to access sensitive data. Application security refers to the combination of hardware, software, and best practices you use to monitor issues and close gaps in your security coverage.
- **Behavioral analytics.**
  - ✓ In order to identify abnormal behavior, security support personnel need to establish a baseline of what constitutes normal behavior for a given customer's users, applications, and network.
  - ✓ Behavioral analytics software is designed to help identify common indicators of abnormal behavior, which can often be a sign that a security breach has occurred. By having a better sense of each customer's baselines, MSPs can more quickly spot problems and isolate threats.

- **Data loss prevention.**
  - Data loss prevention (DLP) technologies are those that prevent an organization's employees from sharing valuable company information or sensitive data whether unwittingly or with ill intent outside the network.
  - DLP technologies can prevent actions that could potentially expose data to bad actors outside the networking environment, such as uploading and downloading files, forwarding messages, or printing.
- **Distributed denial of service prevention.**
  - Distributed denial of service (DDoS) attacks is becoming increasingly common.
  - They function by overloading a network with one-sided connection requests that eventually cause the network to crash. A DDoS prevention tool scrubs incoming traffic to remove non legitimate traffic that could threaten your network, and may consist of a hardware appliance that works to filter out traffic before it reaches your firewalls.
- **Email security**
  - Email is an especially important factor to consider when implementing networking security tools.
  - Numerous threat vectors, like scams, phishing, malware, and suspicious links, can be attached to or incorporated into emails.
  - Because so many of these threats will often use elements of personal information in order to appear more convincing, it is important to ensure an organization's employees undergo sufficient security awareness training to detect when an email is suspicious.
  - Email security software works to filter out incoming threats and can also be configured to prevent outgoing messages from sharing certain forms of data.
- **Firewalls.** Firewalls are another common element of a network security model. They essentially function as a gatekeeper between a network and the wider internet. Firewalls filter incoming and, in some cases, outgoing traffic by comparing data packets against predefined rules and policies, thereby preventing threats from accessing the network.

- **Mobile device security.** The vast majority of us have mobile devices that carry some form of personal or sensitive data we would like to keep protected. This is a fact that hackers are aware of and can easily take advantage of. Implementing mobile device security measures can limit device access to a network, which is a necessary step to ensuring network traffic stays private and doesn't leak out through vulnerable mobile connections.
- **Network segmentation.** Dividing and sorting network traffic based on certain classifications streamlines the job for security support personnel when it comes to applying policies. Segmented networks also make it easier to assign or deny authorization credentials for employees, ensuring no one is accessing information they should not be. Segmentation also helps to sequester potentially compromised devices or intrusions.
- **Security information and event management**. These security systems (called SIEMs) combine host-based and network-based intrusion detection systems that combine real-time network traffic monitoring with historical data log file scanning to provide administrators with a comprehensive picture of all activity across the network. SIEMs are similar to intrusion prevention systems (IPS), which scan network traffic for suspicious activity, policy violations, unauthorized access, and other signs of potentially malicious behavior in order to actively block the attempted intrusions. An IPS can also log security events and send notifications to the necessary players in the interest of keeping network administrators informed.
- **Web security.** Web security software serves a few purposes. First, it limits internet access for employees, with the intention of preventing them from accessing sites that could contain malware. It also blocks other web-based threats and works to protect a customer's web gateway.

The principles of network security

There are three principles within the concept of network security; **Confidentiality**, **integrity**, and **availability**—which together are sometimes referred to as the "CIA triad." A network can only be considered secure when it has all three elements in play simultaneously.

Confidentiality

- It works to keep sensitive data protected and sequestered away from where it can be accessed by the average user.

Availability

- The principle of availability, which seeks to ensure that data and resources are kept accessible for those who are authorized to access them.
- Challenges to availability can include DDoS attacks or equipment failure

Integrity.

- The principle of integrity seeks to protect information from intentional or accidental changes in order to keep the data reliable, accurate, and trustworthy.

Every decision made regarding network security should be working to further at least one of these principles..

Why are these network security concepts so important?

Cyber-attacks are on the rise, with a recent report from Positive Technologies showing that government and healthcare organizations are becoming prime targets for hackers. The report also shows the goal of more than half of cybercrimes is data theft, and that financial gain was the motivation behind 42% of cyber-attacks against individuals—and behind 30% of cyber-attacks against organizations.

As our world becomes increasingly digitized, we rely more and more on the internet and networks to function. This in turn requires that the internet and networks provide us with reliable and secure service.

However, as more of our personal and sensitive data is stored in electronic repositories and archives, hackers are turning their attention to networked systems. For this reason, it is imperative that MSPs and security support personnel offer customers robust security systems that protect data from various threat vectors.

1.4. Internet Protocol Address allocation

- An IP address is an address used in order to uniquely identify a device on an IP network.
- The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask.
- The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100).
- The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.
- Here is how binary octets convert to decimal: The right most bit, or least significant bit, of an octet holds a value of 2^0. The bit just to the left of that holds a value of 2^1. This continues until the leftmost bit, or most significant bit, which holds a value of 27. So if all binary bits are a one, the decimal equivalent would be 255 as shown here:

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

(128+64+32+16+8+4+2+1=255)

Here is a sample octet conversion when not all of the bits are set to 1.

0 1 0 0 0 0 0 1

0 64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)

And this sample shows an IP address represented in both binary and decimal.

10. 1. 23. 19 (decimal)

00001010.00000001.00010111.00010011 (binary)

These octets are broken down to provide an addressing scheme that can accommodate large and small networks. There are five different classes of networks, A to E. This document focuses on classes A to C, since classes D and E are reserved and discussion of them is beyond the scope of this document.

Given an IP address, its class can be determined from the three high-order bits (the three left-most bits in the first octet). Figure 1 shows the significance in the three high order bits and the

range of addresses that fall into each class. For informational purposes, Class D and Class E addresses are also shown.

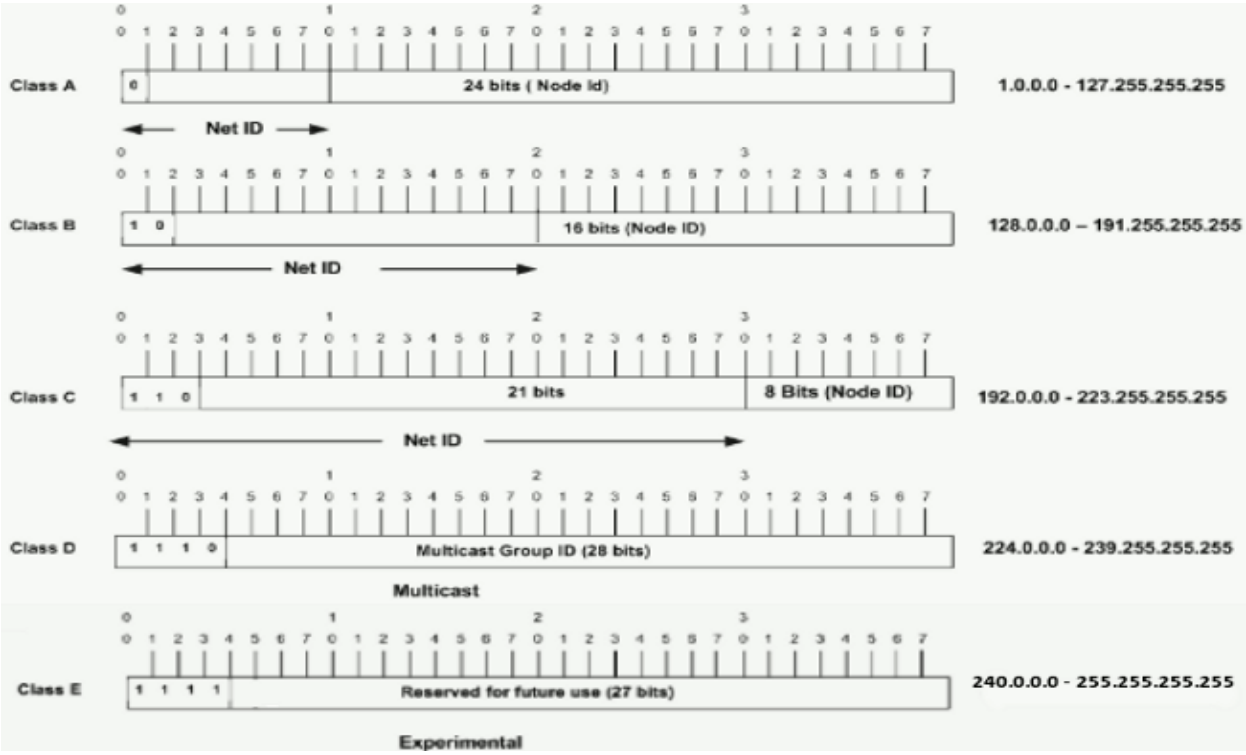


Figure 1.1 Class IP address

In a Class A address, the first octet is the network portion, so the Class A example in Figure 1 has a major network address of 1.0.0.0 - 127.255.255.255. Octets 2, 3, and 4 (the next 24 bits) are for the network manager to divide into subnets and hosts as he/she sees fit. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16777214 hosts!).

In a Class B address, the first two octets are the network portion, so the Class B example in Figure1 has a major network address of 128.0.0.0 - 191.255.255.255. Octets 3 and 4 (16 bits) are for local subnets and hosts. Class B addresses is used for networks that have between 256 and 65534 hosts.

In a Class C address, the first three octets are the network portion. The Class C example in Figure1 has a major network address of 192.0.0.0 - 223.255.255.255. Octet 4 (8 bits) is for local subnets and hosts - perfect for networks with less than 254 hosts.

Network Masks

A network mask helps you know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

An IP address on a Class A network that has not been subnetted would have an address/mask pair similar to: 8.20.15.1 255.0.0.0. In order to see how the mask helps you identify the network and node parts of the address, convert the address and mask to binary numbers.

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = 11111111.00000000.00000000.00000000

Once you have the address, the mask represented in binary, then identification of the network, and host ID is easier. Any address bits which have corresponding mask bits set to 1 represent the network ID. Any address bits that have corresponding mask bits set to 0 represent the node ID.

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = 11111111.00000000.00000000.00000000

---

net id | host id

netid = 00001000 = 8 hostid = 00010100.00001111.00000001 = 20.15.1

Subnetting

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

Each data link on a network must have a unique network ID, with every node on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, it allows you to create a network of interconnecting subnetworks. Each data link on this network would then have a unique network/subnetwork ID. Any device, or gateway, that connects *n* networks/subnetworks has *n* distinct IP addresses, one for each network / subnetwork that it interconnects.

In order to subnet a network, extend the natural mask with some of the bits from the host ID portion of the address in order to create a subnetwork ID. For example, given a Class C network of 204.17.5.0 which has a natural mask of 255.255.255.0, you can create subnets in this manner:

204.17.5.0 - 11001100.00010001.00000101.00000000
255.255.255.224 - 11111111.11111111.11111111.11100000
----------|sub|----

By extending the mask to be 255.255.255.224, you have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets. With these three bits, it is possible to create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device since host ids of all zeros or all ones are not allowed (it is very important to remember this). So, with this in mind, these subnets have been created.

204.17.5.0 255.255.255.224 host address range 1 to 30

204.17.5.32 255.255.255.224 host address range 33 to 62

204.17.5.64 255.255.255.224 host address range 65 to 94

204.17.5.96 255.255.255.224 host address range 97 to 126

204.17.5.128 255.255.255.224 host address range 129 to 158

204.17.5.160 255.255.255.224 host address range 161 to 190

204.17.5.192 255.255.255.224 host address range 193 to 222

204.17.5.224 255.255.255.224 host address range 225 to 254

The network subnetting scheme in this section allows for eight subnets, and the network might appear as:

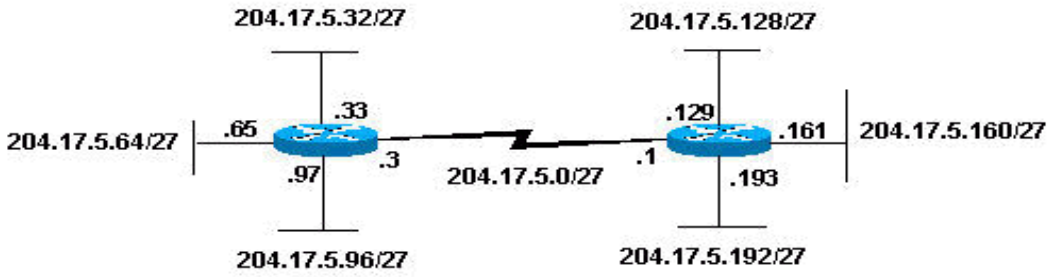


Fig. 1.2 shows subnet on router

Notice that each of the routers in Figure 1.2 is attached to four subnetworks, one subnetwork is common to both routers. Also, each router has an IP address for each subnetwork to which it is attached. Each subnetwork could potentially support up to 30 host addresses.

This brings up an interesting point. The more host bits you use for a subnet mask, the more subnets you have available. However, the more subnets available, the less host addresses available per subnet. For example, a Class C network of 204.17.5.0 and a mask of 255.255.255.224 (/27) allows you to have eight subnets, each with 32 host addresses (30 of which could be assigned to devices). If you use a mask of 255.255.255.240 (/28), the break down is:

204.17.5.0 - 11001100.00010001.00000101.00000000
255.255.255.240 - 11111111.11111111.11111111.11110000
----------|sub |------

Since you now have four bits to make subnets with, you only have four bits left for host addresses. So in this case you can have up to 16 subnets, each of which can have up to 16 host addresses (14 of which can be assigned to devices).

Question 1: Given Class C Network 204.17.5.0/28. How many subnets & hosts we have in the network. Show each of subnets & hosts address range?

Take a look at how a Class B network might be subnetted. If you have network 172.16.0.0, then you know that its natural mask is 255.255.0.0 or 172.16.0.0/16. Extending the mask to anything beyond 255.255.0.0 means you are subnetting. You can quickly see that you have the ability to create a lot more subnets than with the Class C network. If you use a mask of 255.255.248.0 (/21), how many subnets and hosts per subnet does this allow for?

172.16.0.0 - 10101100.00010000.00000000.00000000
255.255.248.0 - 11111111.11111111.11111000.00000000
----------| sub|----------

You use five bits from the original host bits for subnets. This allows you to have 32 subnets (2^5). After using the five bits for subnetting, you are left with 11 bits for host addresses. This allows each subnet so have 2048 host addresses (2^{11}), 2046 of which could be assigned to devices.

Examples

Sample Exercise 1

Now that you have an understanding of subnetting, put this knowledge to use. In this example, you are given two addresses / mask combinations, written with the prefix/length notation, which have been assigned to two devices. Your task is to determine if these devices are on the same subnet or different subnets. You can use the address and mask of each device in order to determine to which subnet each address belongs.

Device A: 172.16.17.30/20

Device B: 172.16.28.15/20

Determine the Subnet for Device A:

172.16.17.30 - 10101100.00010000.00010001.00011110
255.255.240.0 - 11111111.11111111.11110000.00000000
----------| sub|----------
Subnet = 10101100.00010000.00010000.00000000 = 172.16.16.0

Looking at the address bits that have a corresponding mask bit set to one, and setting all the other address bits to zero (this is equivalent to performing a logical "AND" between the mask and address), shows you to which subnet this address belongs. In this case, Device A belongs to subnet 172.16.16.0.

Determine the Subnet for Device B:

172.16.28.15 - 10101100.00010000.00011100.00001111
255.255.240.0 - 11111111.11111111.11110000.00000000
----------| sub|----------
Subnet = 10101100.00010000.00010000.00000000 = 172.16.16.0

From these determinations, Device A and Device B have addresses that are part of the same subnet.

Sample Exercise 2

Given the Class C network of 204.15.5.0/24, subnet the network in order to create the network in 1.1 with the host requirements shown.

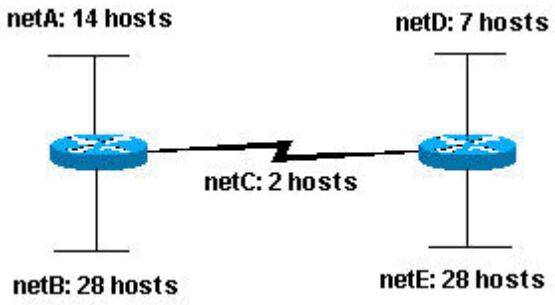


Figure 1.1

Looking at the network shown in figure1.1, you can see that you are required to create five subnets. The largest subnet must support 28 host addresses. Is this possible with a Class C network? And if so, then how?

You can start by looking at the subnet requirement. In order to create the five needed subnets you would need to use three bits from the Class C host bits. Two bits would only allow you four subnets (2^2).

Since you need three subnet bits that leaves you with five bits for the host portion of the address. How many hosts do this support? $2^5 = 32$ (30 usable). This meets the requirement.

Therefore you have determined that it is possible to create this network with a Class C network. An example of how you might assign the subnetworks is:

Net A: 204.15.5.0/27 host address range 1 to 30

Net B: 204.15.5.32/27 host address range 33 to 62

Net C: 204.15.5.64/27 host address range 65 to 94

Net D: 204.15.5.96/27 host address range 97 to 126

Net E: 204.15.5.128/27 host address range 129 to 158

Question 2: Given Class C Network 192.168.10.0/25. How many subnets & hosts we have in the network. Show each of subnets & hosts address range?

Sample Exercise 3

A company would like to break its Class B network IP address 172.16.0.0 into 60 different subnets. Find ranges of IP addresses for each subnet and new mask.

Solution

Class B network has 16 host bits

Class B subnet mask = 255.255.0.0 = 11111111.11111111.00000000.00000000

60 = 00111100 we need at least 6 additional network bits

New Mask

11111111.11111111.11111(1)00.00000000=255.255.252.0 and bit with parenthesis is the increment bit. Start with the given network IP address and add the increment to the subnetted octet:

172.16.0.0

172.16.4.0

172.16.8.0 … etc.

Now add each end range, which is the last possible IP address before the next range:

Subnet 1: 172.16.0.0 – 172.16.3.255

Subnet 2: 172.16.4.0 – 172.16.7.255

Subnet 3: 172.16.8.0 – 172.16.11.255

Subnet 4: 172.16.12.0 – 172.16.15.255

…

Subnet 60: 172.16.236.0 – 172.16.239.255

Assign these ranges to the new networks, but the first and last addresses from each range (network / broadcast IP) are unusable.

Sample Exercise 4

A company would like to break its Class B private IP address 172.16.0.0 into as many subnets as possible provided that they can get at least 300 clients per subnet. Find ranges of IP addresses for each subnet and new mask.

Solution

Class B mask = 11111111.11111111.00000000.00000000

300 = 100101100 we need at least 9 host bits to remain

New Mask

11111111.11111111.111111(1)0.00000000=255.255.254.0 and bit with parenthesis is the increment bit. Start with the given network address and add the increment to the subnetted octet:

172.16.0.0

172.16.2.0

172.16.4.0 … etc.

Now add each end range, which is the last possible IP address before the next range :

Subnet 1: 172.16.0.0 – 172.16.1.255

Subnet 2: 172.16.2.0 – 172.16.3.255

Subnet 3: 172.16.4.0 – 172.16.5.255

Subnet 4: 172.16.6.0 – 172.16.7.255

…

Subnet 128: 172.16.254.0 – 172.16.255.255

Assign these ranges to the new networks, but the first and last addresses from each range (network / broadcast IP) are unusable.

Class A Subnetting

Remember, the first octet of a Class A network is used to represent the network and the remaining three octets are used to represent the host. The default format for a Class A IPv4 address is Network.

Let us consider an example of Class A network 10.0.0.0 - 255.0.0.0. The binary representation of the above network and subnet mask is

Component	**Binary**	**Decimal**
Address Part	00001010.00000000.00000000.00000000	10.0.0.0
Subnet Mask	11111111.00000000.00000000.00000000	255.0.0.0

- If all the bits in the host part are "0", that represents the network address.
- If all the bits in the host part are "0" except the last bit, it is the first usable IPv4 address.
- If all the bits in the host part are "1" except the last bit, it is the last usable IPv4 address.
- If all the bits in the host part are "1", that represents the direct broadcast address.
- All the IPv4 addresses between the first and last IPv4 addresses (including the first and last) can be used to configure the devices.

Class A - One Bit Subnetting

If we include one bit from the host part to the network part, the subnet mask is changed into 255.128.0.0 The single bit can have two values in second octet, either 0 or 1.

00001010.0 | 0000000.00000000.00000000

11111111.1 | 0000000.00000000.00000000

That means we can get two subnets if we do single bit subnetting. The subnet mask for one bit subnetting is 255.128.0.0.

Net no.	Net Id.	Host Addresses	Broadcast Id.
Subnet 1	10.0.0.0	10.0.0.1 – 10.127.255.254	10.127.255.255
Subnet 2	10.128.0.0	10.128.0.1 – 10.255.255.254	10.255.255.255

The network 10.0.0.0 is divided into two networks, each network has **8,388,608** total IPv4 Addresses and **8,388,606** usable IPv4 Addresses (two IPv4 Addresses are used in each subnet to represent the network address and the directed broadcast address).

Question 3: A company would like to break its Class A network IP address 10.0.0.0 into 4 different subnets. Find ranges of IP addresses for each subnet and new mask.

Class A - 3 Bit Subnetting

If we include three bits from the host part to the network part, the subnet mask is changed into 255.224.0.0 the three bits added to network part can have eight possible values in the second octet and that are 000, 001, 010, and 011, 100, 101, 110 and 111.

00001010.000 | 00000.00000000.00000000

11111111.111 | 00000.00000000.00000000

That means, we can get eight networks if we do three bit subnetting and the subnet mask will be 255.224.0.0.

Net no.	Net Id.	Host Addresses	Broadcast Id.
Subnet 1	10.0.0.0	10.0.0.1 – 10.31.255.254	10.31.255.255
Subnet 2	10.32.0.0	10.32.0.1 – 10.63.255.254	10.63.255.255
Subnet 3	10.64.0.0	10.64.0.1 – 10.95.255.254	10.95.255.255
Subnet 4	10.96.0.0	10.96.0.1 – 10.127.255.254	10.127.255.255
Subnet 5	10.128.0.0	10.128.0.1 – 10.159.255.254	10.159.255.255

Subnet 6	10.160.0.0	10.160.0.1 – 10.191.255.254	10.191.255.255
Subnet 7	10.192.0.0	10.192.0.1 – 10.223.255.254	10.223.255.255
Subnet 8	10.224.0.0	10.224.0.1 – 10.255.255.254	10.255.255.255

The network 10.0.0.0 is divided into eight networks, each network has **2,097,152** total IPv4 Addresses and **2,097,150** usable IPv4 Addresses (two IPv4 Addresses are used in each subnet to represent the network address and the directed broadcast address).

Self-Check 1

Read the all instraction proberly

Part-I: Choose the correct answer

1. Which one of the following is the first step to understand during designing a network?

a. Network device b. Maintain device c. Network requirement d. None

2. _____is a collective term for all hardware and software systems that constitute essential components in the operation of the Internet

a. Internet infrastructure b. Domain name c. Authentication d. Web hosting

3. One of the following is not methods to obtain information during assessing user requirements

a. Interviews, focus groups, and surveys c. User community profiles

b. Human factors tests d. Reliability of network.

4. _____ is one of the fastest-growing forms of criminal activity.

a. Cybercrime b. Security C. Cloud service d. Fraud

5. Protocols are?

a. Agreements on how communication components to communicate.

b. Wireless communication channels sued for transferring data.

c. Physical communication channels sued for transferring data.

d. Logical communication channels for transferring data.

6. A protocol which resolving domain name is _____.

a. DHCP b. SMTP c. POP3 d. DNS

7. A _____ helps you know which portion of the address identifies the network and which portion of the address identifies the node.

a. Network address b. Network mask c. Network Protocol d. None of the above

8. Which one of the following ids the default mask of Class B network?

a. 255.0.0.0 b.255.255.255.0 c. 255.255.0.0 d. all

9. Which class of a network is used for experimental testing?

a. Class E b. Class D c. Class B d. Class A

Part II give short answer

1. What is subneting
2. Why is subnetting important in networking

Unit Two: Install and configure internet infrastructure and services

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

- Installing and testing cables
- Mail servers
- workstation software
- hardware and software for internet connection
- Deploying and configuring Software

This guide 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:

- Identify cables, Install and test
- Explain about mail servers
- Define workstation software
- Explain about hardware and software for internet connection
- Discuss and configure domain names and internet protocol address

2.1. Installing and testing cables

There are many different types of cable found in the networking environment, and some are more common than others Twisted Pair (TP) Cable

Twisted pair cables consist of one or more pairs of insulated copper wires that are twisted together and housed in a protective jacket.

Used by modern Ethernet technology made of copper.

- A twisted pair cable is susceptible to electromagnetic interference (EMI), a type of noise
- The number of twists per unit length affects the amount of resistance that the cable has to interference.
- Cable suitable for data transmission, known as CAT5, has 3-4 turns per inch, making it more resistant to interference
- In an Ethernet environment, the distance limitation is approximately 328 feet (100 meters).

- The connector used for twisted pair cable is RJ-45
  - Types of twisted pair cable:
    - unshielded twisted pair (UTP)
    - shielded twisted pair (STP)

Unshielded twisted pair (UTP) is the most commonly encountered type of network cable
Inexpensive, offers a high bandwidth, and is easy to install

- Used to connect workstations, hosts and network devices.
  - ✓ The most common number of pairs is four.
  - ✓ Each pair is identified by a specific color code
  - ✓ Many different **categories** have been developed over time

Types which are still commonly found include Categories 3, 5, 5e and 6

Cat 3: used for phone lines (not data grade) , Cat 5: 100Mbps, Cat 5e: 1000 Mpbs (Gigabit Ethernet) , Cat 6: up to 10 Gbps, has added separator between each pair for hire speed

Shielded twisted pair (STP) - Usually Category 5, 5e, or 6 cable that has a foil shielding to protect from outside electromagnetic interference (EMI).

- is used in areas where EMI and RFI are so strong
- very expensive, not flexible

Electronics Industry Association/ Telecommunications Industries Association (TIA/EIA) organization defines two different patterns, or wiring scheme **T568A and T568B**.

On a network installation, one of the two wiring schemes (T568A or T568B) should be chosen and followed. It is important that the same wiring scheme is used for every termination in that project.

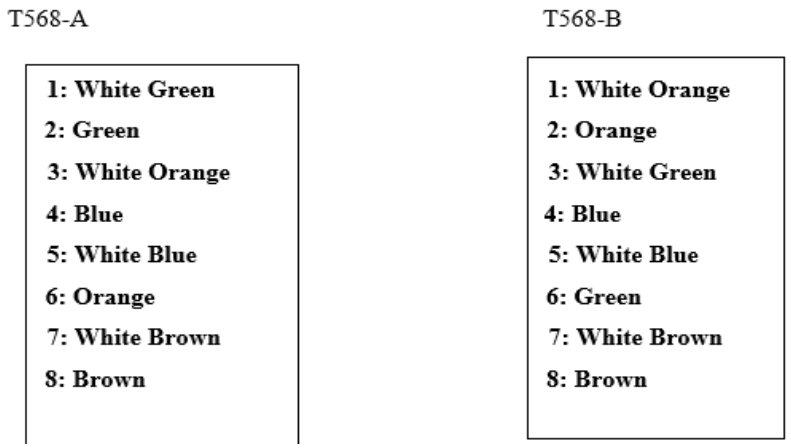


Fig.2.1 Figure shows color arrangement

There are three different types of twisted pair cables that are used in networks:

Straight-through - Connects dissimilar (different) devices, such as

- Switch to router
- Hub to PC
- switch to PC

Crossover - Connects similar devices, such as

- Switch to switch
- Switch to hub
- Hub to hub
- Router to router
- PC to PC

Console (or Rollover) - Connects a computer to the console port of a router or switch to do initial configuration

Coaxial Cable

Coaxial cable has improved data carrying characteristics, but twisted pair cabling has replaced coax in local area networking uses

The reasons for the replacement - coax is physically harder to install, more expensive, and harder to troubleshoot

Usually constructed of either copper or aluminium, and is used by cable television companies to provide service

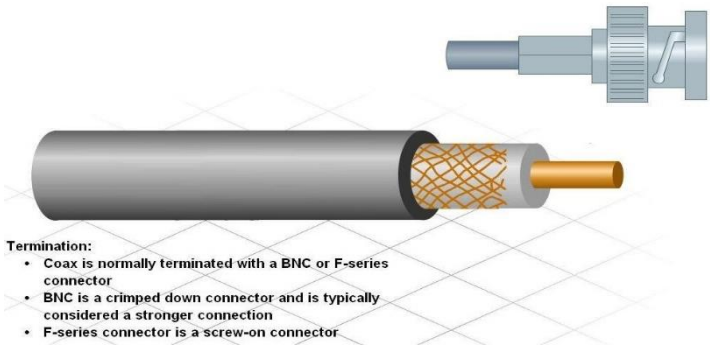


Fig.2.2 Coatxial cable

Fiber Optic Cable

Made of glass or plastic, have a very high bandwidth, which enables them to carry very large amounts of data.

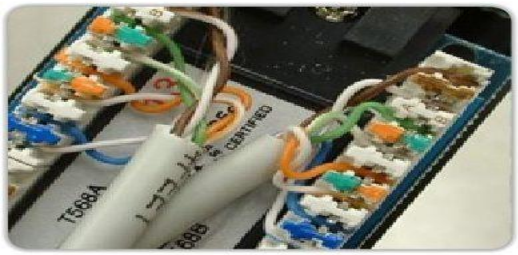
- A medium that is not susceptible to EMI, and can transmit data faster and farther than copper.
- Depending on the type of fiber optics, distance limitations can be several miles (kilometers).
- Used in backbone networks, large enterprise environments and large data centre Unlike TP and coax, fiber optic cables transmit data using pulses of light.
- Not normally found in home or small business environments, but widely used in enterprise environments and large data centers
- It is immune to EMI
- Support a large amount of bandwidth making them ideally suited for high-speed data backbones

- Also used to connect ISPs on the Internet

Network devices are usually connected to patch panels. **Patch panels** act like switchboards that connect workstation cables to other devices.


Front of Patch Panel


Rear of Patch Panel


Close Up of Back of Patch Panel


Punchdown Tool

Fig. 2.3 shows cable connection

Cable testing

- It is important to verify a new cable operates correctly
- The first test is a visual inspection
- Then use cable tester instruments to check the cable electrically
- Using cable tester, continuity test verifies that there is end-to-end connectivity

Structured Cabling

When designing a structured cable project, the first step is to obtain an accurate floor plan. The floor plan allows the technician to:

- identify possible wiring closet locations,
- cable runs, and
- which electrical areas to avoid

Cabling best practices

- It is important that the type of cables and components used on a network adhere to the standards required for that network
- Cable standards specify maximum lengths for different types of cables. Always adhere to the length restrictions for the type of cable being installed
- Important to install cable away from sources of interference such as high-voltage cables and fluorescent lighting. Televisions, computer monitors and microwaves are other possible sources of interference. In some environments it may be necessary to install data cables in conduit
- Label all cables as they are installed, and record the location of cables in network documentation

2.2. Mail servers

A mail server (sometimes called an email server) is a software program that sends and receives email. Often, it is used as a blanket term for both mail transfer agents (MTA) and mail delivery agents (MDA), each of which perform a slightly different function. Mail servers play a crucial role in the email delivery process. Without them, users would have no way of transferring those messages to and from other mail clients.

Mail client

Mail servers send messages from one mail client to another. A mail client (also called an *email client* or *message user agent*) is a web-based or desktop application that receives and stores email messages. Some of the most widely-used mail clients include Microsoft Outlook, Gmail, and Apple Mail.

How do mail servers deliver email messages?

Email messages are sent and received using two types of mail servers: outgoing mail servers, or mail transfer agents (MTA), and incoming mail servers, or “mail delivery agents” (MDA). MTAs retrieve outgoing email messages from the sender’s mail client, then deliver them to MDAs, which are responsible for temporarily storing and delivering email messages to the recipient’s mail client.

Mail servers deliver email messages between mail clients by using email protocols, which tell the server how to process incoming requests, where to forward the messages, and how to deliver them to the intended mail client.

When sending an email from one client to another, the MTA uses an outgoing mail protocol, like the Simple Mail Transfer Protocol (SMTP), to check the sender's email envelope data and determine where the message needs to be sent. SMTP does this by using the Domain Name System (DNS) to translate the recipient's domain into an IP address.

Then, it locates a mail delivery agent by querying mail exchange (MX) records. The MX record tells the server how to route the message to its final destination. Once the MX record returns the appropriate destination, the MDA uses an incoming mail protocol, like the Internet Message Access Protocol (IMAP) or Post Office Protocol Version 3 (POP3), to retrieve the email message from the mail server and deliver it to the specified mail client (or clients).

What is the difference between a mail client and a mail server?

While mail clients and mail servers are both used to send and receive email messages, they are not the same. A mail client is an application that allows users to retrieve, store, and format emails to be sent. Mail servers, meanwhile, are software programs that use email protocols to move email messages between mail clients.

To illustrate this difference, imagine that Alice wants to send Carol a letter. Alice addresses the letter to Carol, then leaves it in their mailbox. A postal worker retrieves the letter from the mailbox and delivers it to a post office, where it is sorted and transferred to the correct location. Finally, another postal worker delivers the letter to Carol's mailbox, where it can be stored until they are ready to retrieve it.

Similarly, a user may write and address an email to its intended recipient (or recipients), but the mail server, like the postal worker, is responsible for accepting the message, transferring it to an incoming mail server, then delivering it to the correct inbox, where it is stored.

What are the types of mail servers?

Mail servers can be divided into two categories: **incoming mail servers** and **outgoing mail servers.** An incoming mail server stores mail and sends it to a user's inbox. Post Office

Protocol 3 (POP3) and Internet Message Access Protocol (IMAP) are the two main types of incoming mail servers.

POP3, for example, downloads email from a server and stores incoming email messages on a single device until the user opens the email client. Once the user downloads the email, it is automatically deleted from the server, unless the "keep mail on server" setting is enabled. Many internet service providers offer their users POP3 email accounts, as they are more space efficient.

IMAP servers enable users to preview, delete and organize emails before transferring them to multiple devices from the email server. Copies of emails are left on the server until the user deletes them.

An outgoing mail server operates by having a user's machine communicate with Simple Mail Transfer Protocol (SMTP), which handles the email delivery process. SMTP servers work with other types of mail servers, namely POP3 or IMAP, to send emails from email clients.

Sending an email Sending process

The following technics show the general process of sending an email:

1. The user composes an email using a third-party email client, such as Outlook, and hits Send.
2. The email client connects to the SMTP server.
3. The SMTP server identifies and processes the recipient's email address, the body of the message and additional attachments.
4. If the domain name is the same as the sender's, the message is routed directly over POP3 or IMAP. If the domain name is different, the SMTP server communicates with the domain name system (DNS) to find the recipient's server. The DNS translates the recipient's email domain name into an Internet Protocol (IP) address.
5. The recipient's IP address connects to the SMTP server. Once the IP is identified, the sent message is routed between unrelated SMTP servers until it arrives at its destination.
6. The recipient's SMTP server handles the email. It checks the message and directs it over to an IMAP or POP3 server. The email is then placed in a mail queue until the recipient retrieves it.

This image shows the path an email takes through a mail server. On-premises vs. cloud mail servers Email servers can be located on premises or be cloud-based. On-premises servers are physical servers that are at an organization's location. The organization must manage and maintain all servers and infrastructure. Cloud-based servers are virtual and are hosted using cloud computing. There is no one right option for every organization, as it depends on the business.

On-premises mail servers use the organization's servers, receiving all emails and sending them to an indexed database. On-premises servers typically require a larger upfront investment for hardware, installation and management. The potential for scalability is also less immediate compared to email servers hosted in the cloud. The organization is responsible for providing security.

Cloud-based email servers, such as Amazon Simple Email Service (SES), operate the same way as on-premises servers, but the data is stored in a cloud environment that a separate vendor provides. There is typically a monthly fee included, set up as a pay-as-you-go pricing method. Scaling is usually easier and more immediate compared to on-premises servers since an organization is just using more of the vendor's resources instead of having to add more physical server space. The cloud vendor provides security.

Considerations for choosing a mail server

An organization must take the following into account before choosing a mail server:

- **Security**. Email services should use advanced tools to protect information. Other features an email provider may provide include encryption, antimalware, spam filtering and data loss prevention tools.
- **Cost**. On-premises email servers cost more upfront but also provide more fine-grained control over systems and security. Cloud-based email services typically have less upfront cost and require less maintenance.
- **Archiving and storage**. Ensure a vendor offers sufficient storage for email archiving. Some services may also offer an option to move old messages to an archive automatically.
- **Compatibility**. Email services may also offer options to sync with web-based and mobile applications, such as email, calendar and contact applications.

What are examples of mail servers?

There are many different free and paid mail servers that use SMTP. Some examples are the following:

- Amazon SES is a cloud-based platform with an SMTP interface.
- Halon MTA is an email operations and security platform that uses SMTP.
- Microsoft Exchange Server is a paid email, calendaring, contact, scheduling and collaboration platform that is deployed on the Windows Server operating system.
- Open SMTPD is a free MTA developed as part of the Open BSD
- Open-X change is a free web-based collaboration and office productivity software suite with email and scheduling capabilities.
- Oracle Beehive is a paid collaboration platform that combines email, instant messaging and conferencing.

2.4. Hardware and software for internet connection

Good networks do not happen by accident. They are the result of hard work by network designers and technicians, who identify network requirements and select the best solutions to meet the needs of a business.

The technics required to design a good network are as follows:

- Verify the business goals and technical requirements.
- .Determine the features and functions required to meet the needs identified in
- Perform a network-readiness assessment.
- Create a solution and site acceptance test plan.
- Create a project plan.

2.5. Configuring Domain names and internet protocol address

A domain name is a linkage string which defines a jurisdiction of administrative self-rule, sanction or limitation within the Internet. Domain names are defined by the protocols and directives of the Domain Name System (DNS). Any name registered in the DNS is a domain name. Domain names are used in various networking contexts and application-specific nomenclature and addressing tenacities. In general, a domain name represents an Internet Protocol (IP) resource, such as a computer used to access the

Internet, a web-server hosting a web site, or the web site itself or any other service presented via the Internet. In 2017, 330.6 million domain names had been registered across the globe.

Domain names are systematized on the secondary levels i.e. subdomains of the DNS root domain, which is unnamed. The primary set of domain names are the top-level domains (TLDs), including the generic top-level domains (gTLDs), which include the most famous domains like the .com, .info, .net, .edu, and .org, and the country code top-level domains (ccTLDs) like co.in, .co.uk, etc. Beyond these TLD's in the DNS hierarchy are the secondary and tertiary domain names that are typically open for reservation by end-users which would be used to connect local area networks LAN to the Internet, or to create other publicly accessible Internet resources or run web sites.

The registration of these domain names is governed by domain name registrars who sell the Domain names along with other services associated with it to the public.

An Internet Protocol address (IP address) is a numerical tag assigned to each Device which may be a computer, server, network, storage, mobile or any IT appliance which is connected to a network of computing devices and servers which use an Internet Protocol for communication amongst each other within the network. An IP address serves two principal functions: network interface identification and location tracing.

Internet Protocol version 4 (IPv4) which is the older version of the 2, defines an IP address as a 32-bit number. However, because of the rapid growth of the Internet users as well as devices and the exhausting supply of available IPv4 addresses, a new version of IP (IPv6), using 128 bits for the IP address, was developed in 1995, and standardized as RFC 2460 in 1998. IPv6 deployment has been ongoing since the mid-2000s.

IP addresses are usually mentioned and demonstrated in human-readable notations, such as 115.124.127.198 in IPv4, and 2400:5300:0: b:51 in IPv6. The IP address space is administered globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIR) in charge for their predefined geographical territories for assignment of IP address to end users and Internet service providers. IPv4 addresses

are circulated by IANA to the RIRs in slabs of approximately 16.8 million IP addresses each. Each Internet Service Provider or local network administrator needs to assign an IP address to each machine (PC or Server) connected within its network configuration. Such assignments may be on a static (permanently assigned) or dynamic basis, depending on its software and practices.

An IP address helps with two primary functions, firstly it identifies the host's network interface, and it provides the location of it in the IT network, and thus ensuring the ability of addressing that host. The role has been described as follows: A name description indicates what it is & the address indicates the location of it lastly the route indicates how to reach there.

The intent of the new design was not only to deliver a sufficient quantity of IP addresses, but also redefine routing in the Internet by more competent aggregation of subnetwork routing prefixes. This resulted in decelerated growth of routing tables in routers.

IP addresses are allocated to a machine or device either automatically allocating a dynamic IP at the time of booting, or perpetually by static configuration of the host's hardware or software. Insistent configuration is also known as using a static IP address. In contrast, when a computer's IP address is allocated afresh each time it restarts, this is dynamic IP address allocation.

The configuration of a static IP address is subject to the software or hardware installed in the machine. Servers used for the network infrastructure, such as routers and mail servers, are typically configured with static addressing. The primary reason is Static addresses are always convenient for locating servers inside an enterprise, therefore in critical times like trouble shooting the location tracing of the server becomes expedient.

Dynamic IP addresses are allocated using techniques such as Zero-configuration networking for self-configuration, or by the Dynamic Host Configuration Protocol (DHCP) & Domain Name System (DNS) from a network server. The address allocated with DHCP has an expiration phase, after which the IP address would be assigned to another device, or to the original connected host in case if it is still powered. A network

administrator may implement a DHCP method so that the same host always receives a specific address.

Domain names are assigned to an IP address, which is used in the communication with the PC Server. Domain names are words, alphabets with other elements like the TLD or the gTLD's which are separated from each other using full-stops. For example, the name of the domain is ESDS or Host but when the TLD like .co.in is attached with it then it becomes a valid domain name. The .co.in is the country level domain. Some other top-level domains are .com, .edu for education, .gov for government, .net for network, and .org for nonprofit organizations.

Other top-level domains are for geographic locations, such as .us for the United States, .ca for Canada, .co.in for India and .uk for United Kingdom. Within a country, mid-level domains may be used to further refine the address. The remainder of the address for both domains is up for sale. InterNIC is the organization currently responsible for managing the .com and .net top-level domains. Organizations can request for any name and it can be granted permission to use that name if it is not in registered or allocated to anyone else on the internet; and also as long as they pay the appropriate registration fees.

Its mandatory that all information sent on the Internet must use a valid IP address, this process is a mandate which will translate a domain name into an IP address. This mandate is defined a Domain Name Server or DNS as its most popularly known. The DNS interconnects a domain name with the allocated IP and returns a valid IP address when a domain is called for in the internet. If your PC is connected to the Internet, it either has a fixed IP address of a DNS or a IP address is allocated dynamically whenever a connection is established, via a modem or when the computer is first turned on.

2.6. Deploying and configuring Software

- The internet offers a range of services to its consumers. We can upload and download the files/ data via the internet as it is a pool of knowledge. We can access or obtain information as needed. It is quite popular because of the variety of senders available on the Internet.

- Web services have grown in popularity as a result of these offerings. To access/exchange a large amount of data such as software, audio clips, video clips, text files, other documents, etc., we require internet services. We must use an Internet service to connect to the Internet.

- Data can be sent from Internet servers to your machine via Internet service. Some of the internet services are FTP, Telnet, VoIP, etc.

  Basic Software Components required to access Internet are:

  Operating System: It is required to make the computer working and also to get connected to internet.

  Internet Browser: It is a software used to locate, retrieve the contents from the world wide web and display it on the user's Screen. Example: Internet Explorer, Netscape. It adds to the meaning of www by converting HTML pages into simple language.

  - **Firewall:** While sharing information on such a big network, one may face security hazards. These could be virus, information theft, hacking, etc. In order to be safe it is recommended to use protection tools Firewall is one of them. If follows your instructions to make your computer secure, It restricts harmful information and programs coming your way.
  - **TCP/IP Protocol:** This are set of standards which have to be followed while, communicating on internet.

  How Internet Works

  TCP/IP Stack: Internet is used basically for data and information transfer and sharing on a large network. This transfer must be in a secure way, and to make it sure some set of protocols have to be followed. TCP/IP, software which was originally designed for the UNIX operating system, provides this to the computer. This is now available for almost every operating system.

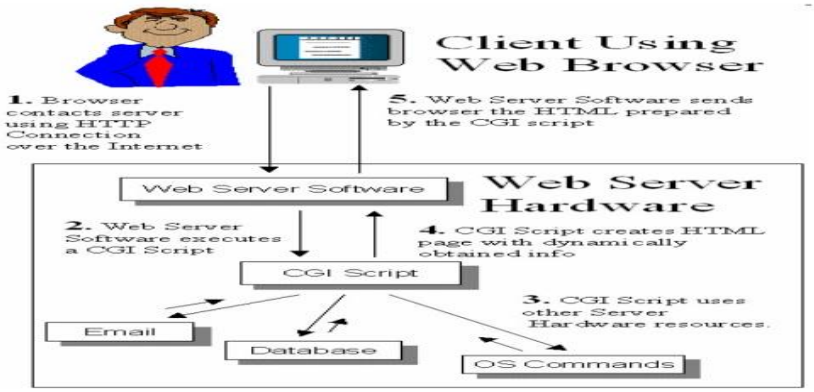


Fig. Shows how Client access Internet

Hypertext Transfer Protocol (HTTP)

- The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems.
- HTTP is the foundation of data communication for the World Wide Web. HTTP functions as a request-response protocol in the client-server computing model. In HTTP, a web browser, for example, acts as a client, while an application running on a computer hosting a web site functions as a server.
- The client submits an HTTP request message to the server. The server, which stores content, or provides resources, such as HTML files, or performs other functions, returns a response message to the client.
- A response contains completion status information about the request and may contain any content requested by the client in its message body.

Self check 2

Directions: Answer all the questions accordingly.

Part I. Say true if the statement is correct false if the statement is false

1. A mail server is responsible for handling and storing emails for users.
2. Twisted pair cables are commonly used in networking and can be found in various categories, such as Cat5e and Cat6.
3. A mail server uses protocols like SMTP (Simple Mail Transfer Protocol) for sending emails and POP3 (Post Office Protocol) or IMAP (Internet Message Access Protocol) for receiving emails.
4. The physical layer of the OSI model is concerned with the transmission and reception of raw data bits over a physical medium, such as network cables.

Part II: Fill blank space in provided space

1. _____ is a software used to locate, retrieve the contents from the world wide web and display it on the user's Screen.
2. _____ show the primary pieces of your network and how those pieces are connected.
3. _____ is a software program that sends and receives email.
4. _____Connects dissimilar (different) devices, such as o Switch to router o Hub to PC
5. _____is an application protocol for distributed, collaborative, hypermedia information systems.

Unit Three : Test security and internet access

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

- Testing and verifying security access level
- Monitoring and evaluating security system capability and reliability
- Making system changes for protection
- Confirming availability of internet access

This guide 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:

- Discuss and understand security access level and features
- Monitor and evaluate security system capability and reliability
- Authorize availability of internet access

Introdction to Internet security

Security access level

- Access levels are a way for organizations to control who has access to information or resources. They are also known as security labels, permissions, roles, rights, or privileges.
- Access levels are often used to determine whether someone should be able to view certain documents or perform certain tasks. For example, they might allow employees to see their pay stubs but not their tax returns.
- An organization's access levels are determined by its policies and procedures. These policies and procedures are typically written down and stored electronically. The policies and procedures document defines the rules that govern access levels.
- The access level of an account is determined by the permissions that you grant to that account when you create it. When a user logs in, Windows will check his/her access level and then apply any necessary adjustments. If the user's access level is lower than what is required for the action being performed, Windows will deny the request.

Access Level in Security

- In general, access level determines how much power a user has on a system. It can be used to limit the amount of damage that a malicious user could do if they gain administrative access to your system. This is especially important for computers running as servers, where unauthorized users may gain access to sensitive information stored on the server.
- When setting up a new user account, you must specify the access level for that account. You can set the access level using the Local Security Policy tool.

Importance of access level

- Access level helps protect against unauthorized changes made to a system. An attacker who gains access to a system through some other means (e.g., social engineering) might not know about the access level of the accounts he/she needs to change. If the attacker tries to make changes to the system without knowing the proper access level, the

changes might fail because the account doesn't have enough authority to perform the requested operation.

- Another reason why access level is important is that it provides a mechanism for restricting access to sensitive information. A user with administrator access might be able to view all files on the system, but a user with a standard access level cannot see those same files.

User-Level Mean

- User-level refers to the privileges granted to a particular user account. User-level controls which applications can run under that account. For example, a normal user account usually has no special privileges. However, if you assign this user account administrative rights, the user can install programs and modify settings.

Components of an Access Level

- The components of an access level include:
  - **Administrator:** Full access to the system. Allows the user to perform most operations on the system. Can add, remove, and edit users, groups, and domains; manage passwords; configure services; and more.
  - **Standard:** Limited access to the system. Does not allow the user to perform many functions. Cannot delete, rename, move, copy, or format drives. Only allows the user to print documents.
  - **Guest:** No access to the system. Users with guest accounts can log onto the computer, but they cannot perform any actions. They cannot use the mouse, open windows, or even save their work.

Database Access Levels

- A database access level is similar to an access level in that it limits the type of data that a user can read from a database. Database access levels are assigned at the table, column, or row level. These levels determine whether a user can select rows in a table, view columns in a table, or query tables based on specific criteria.There are five types of database access levels:
- **Read-only:** The user can only view data in the database. He or she cannot update, insert, or delete data.

- **Select:** The user can select data from the database. He or she cannot update, insert, delete, or alter data.
- **Update:** The user can update data in the database, and they cannot select data.
- **Insert:** The user can insert data into the database. He or his cannot select data. **Delete:** The user can delete data from the database.

Internet Access Settings and Security Levels

we can assign a security level to internet access settings based on how well access to the internet is secured:

- Split Tunnel ON (Security Level 1):
  - Only traffic to trusted internet destinations is secured by tunneling through OpenVPN Cloud other internet traffic exits directly using local internet
  - Cyber Shield Domain filtering is effective
  - Cyber Shield Traffic filtering while not being used at full potential because all the monitored traffic is trusted can still be effective because it can detect and block malicious traffic from a compromised endpoint.
- Split Tunnel OFF (Security Level 2):
  - All traffic is tunneled and can be examined by 3rd party security solutions stack (for example, UTM, Secure Web Gateway, etc.) deployed in any of your private networks acting as an internet gateway to OpenVPN Cloud
  - Cyber Shield Domain filtering is effective
  - Cyber Shield Traffic filtering is effective
- Restricted Internet (Security Level 3)
  - All traffic to the internet is blocked except to trusted internet destinations which are tunneled to OpenVPN Cloud
  - Cyber Shield Traffic filtering while not being used at full potential because all the monitored traffic is trusted can still be effective because it can detect and block malicious traffic from a compromised endpoint.

3.1.1. System Security, capability and reliability

- Attacks to a network can be devastating and can result in a loss of time and money due to damage or theft of important information or assets. Intruders can gain access to a network through software vulnerabilities, hardware attacks or even through less high-tech methods such as guessing someone's username and password Intruders who gain access by modifying software or utilize software vulnerabilities are often called **hackers**. Once the hacker gains access to the network, four types of threat may arise:
  - Information theft
  - Identity theft
  - Data loss / manipulation
  - Disruption of service

Sources of network intrusion

External Threats: Arise from individuals working outside of an organization.

- They do not have authorized access to the computer systems or network.
- Work their way into a network mainly from the Internet, wireless links or dialup access servers.

Internal Threats: Occur when someone has authorized access to the network through a user account or have physical access to the network equipment.

- They often know what information is both valuable and vulnerable and how to get to it.
- Not all internal attacks are intentional. Such as a virus

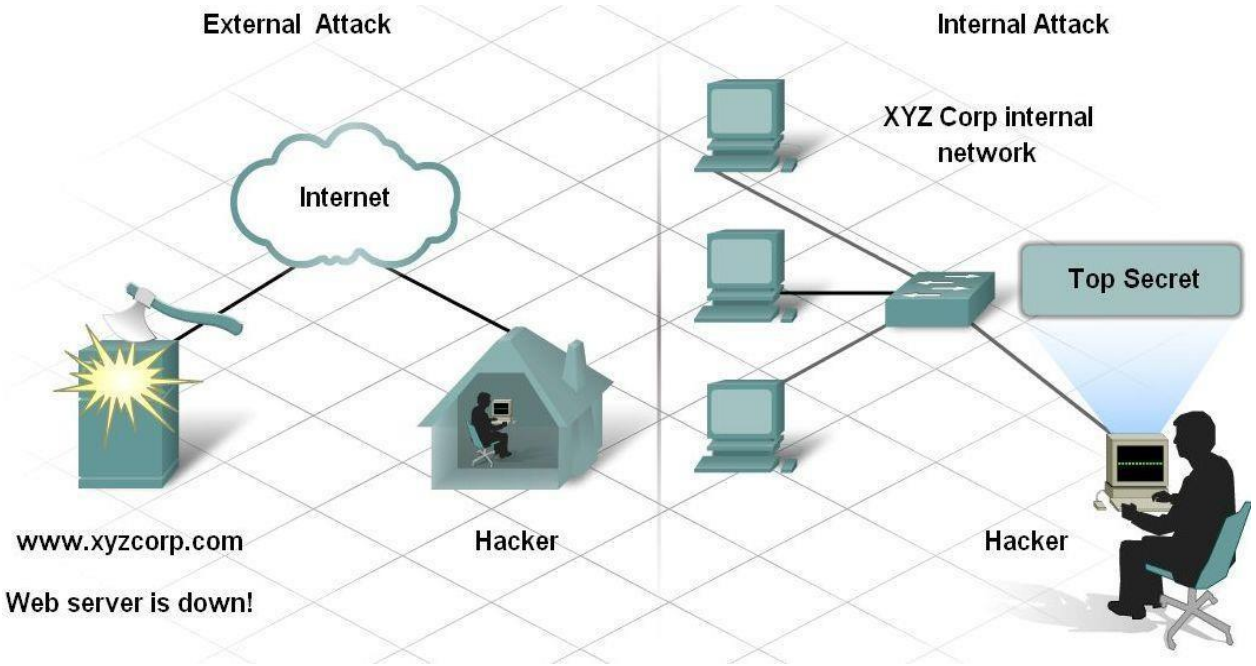


Fig.3.1 show internal and external attack

To ensure privacy and security on the internet, it's important to be aware of different types of internet attacks. Common internet security threats include:

Social Engineering and Phishing: One of the easiest ways for an intruder to gain access, whether internal or external is by exploiting human behaviour.

One of the more common methods of exploiting human weaknesses is called Social Engineering

Social engineering refers to the ability of something or someone to manipulate the behaviour of a group of people.

- In the context of computer and network security Social Engineering refers to a collection of techniques used to deceive internal users into performing specific actions or revealing confidential information
- Attacker takes advantage of unsuspecting legitimate users to gain access to internal resources and private information, such as bank account numbers or passwords.

Social engineers can be internal or external to the organization, but most often do not come faceto-face with their victims

Four of the most commonly used techniques in social engineering are**: pretexting**, **phishing**, **vishing and Pharming**

Pretexting: Form of social engineering where an invented scenario (the pretext) is used on a victim in order to get the victim to release information or perform an action. The target is typically contacted over the telephone.

- For pretexting to be effective, the attacker must be able to establish legitimacy with the intended target, or victim.
- This often requires some prior knowledge or research on the part of the attacker.

For example, if an attacker knows the target's social security number, they may use that information to gain the trust of their target. The target is then more likely to release further information

Phishing: A form of social engineering where the phisher pretends to represent a legitimate outside organization.

- They typically contact the target individual (the phishee) via email.

The victim usually gets an e-mail from what looks like a reputable (honest) source (bank, insurance company, amazon.com, PayPal, etc) looking for verification of passwords or other personal account information.

•The phisher might ask for verification of information, such as passwords or usernames.

Vishing / Phone Phishing: A new form of social engineering that uses Voice over IP (VoIP).

- An unsuspecting user is sent a voice mail instructing them to call a number which appears to be a legitimate telephone-banking service.
- The call is then intercepted by a thief. Bank account numbers or passwords entered over the phone for verification are then stolen.

Pharming: Rerouting a request for a legitimate web site to a fake site that collect personal information

a. Usually, the fake site address may be just one letter out

i.www.bankofireland.com

ii.www.bankofirelnad.com

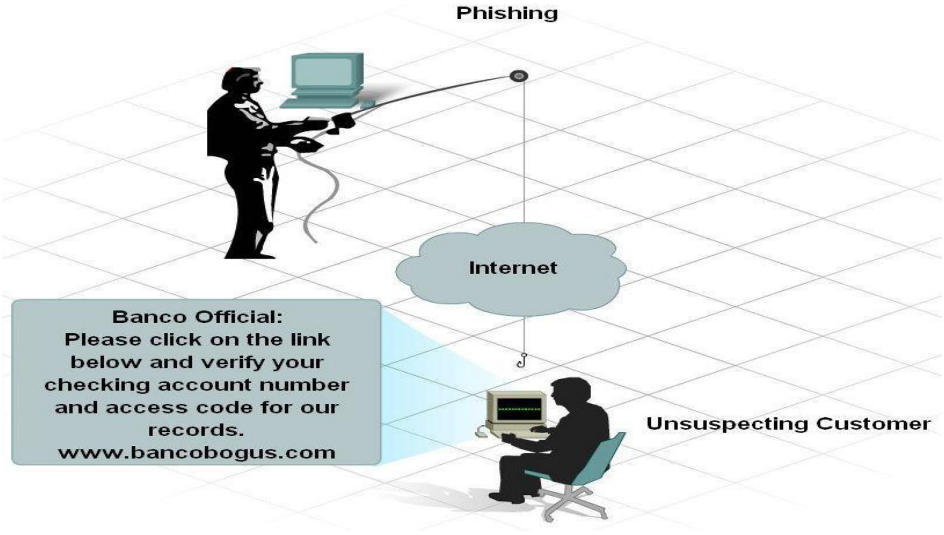


Fig.3.2 Figure shows phishing

Ransomware

- Ransomware is a type of malware that prevents you from using your computer or accessing specific files on your computer unless a ransom is paid. It is often distributed as a trojan – that is, malware disguised as legitimate software. Once installed, it locks your system's screen or certain files until you pay.
- Because of their perceived anonymity, ransomware operators typically specify payment in cryptocurrencies such as Bitcoin. Ransom prices vary depending on the ransomware variant and the price or exchange rate of digital currencies. It isn't always the case that if you pay, the criminals will release the encrypted files.
- Ransomware attacks are on the rise, and new ransomware variants continue to emerge. Some of the most talked-about ransomware variants include Maze, Conti, GoldenEye, Bad Rabbit, Jigsaw, Locky, and WannaCry.

Botnets

- The term botnet is a contraction of "robot network". A botnet is a network of computers that have been intentionally infected by malware so they can carry out automated tasks on the internet without the permission or knowledge of the computers' owners.

- Once a botnet's owner controls your computer, they can use it to carry out malicious activities. These include:
  - Generating fake internet traffic on third party websites for financial gain.
  - Using your machine's power to assist in Distributed Denial of Service (DDoS) attacks to shut down websites.
  - Emailing spam to millions of internet users.
  - Committing fraud and identity theft.
  - Attacking computers and servers.
- Computers become part of a botnet in the same ways that they are infected by any other type of malware – for example, opening email attachments that download malware or visiting websites infected with malware. They can also spread from one computer to another via a network. The number of bots in a botnet varies and depends on the ability of the botnet owner to infect unprotected devices.

Wi-Fi threats, in public and at home

- Public Wi-Fi carries risks because the security on these networks – in coffee shops, shopping malls, airports, hotels, restaurants, and so on – is often lax or non-existent. The lack of security means that cybercriminals and identity thieves can monitor what you are doing online and steal your passwords and personal information.
- Other public Wi-Fi dangers include:
  - **Packet sniffing** – attackers monitor and intercept unencrypted data as it travels across an unprotected network.
  - **Man-in-the-middle-attacks** – attackers compromise a Wi-Fi hotspot to insert themselves into communications between the victim and the hotspot to intercept and modify data in transit.
  - **Rogue Wi-Fi networks** – attackers set up a honeypot in the form of free Wi-Fi to harvest valuable data. The attacker's hotspot becomes the conduit for all data exchanged over the network.

Information Security

Organizations and people that use computers can describe their needs for information security and trust in systems in terms of three major requirements:

- **Confidentiality**: controlling who gets to read information;
- **Integrity**: assuring that information and programs are changed only in a specified and authorized manner; and
- **Availability**: assuring that authorized users have continued access to information and resources.
- These three requirements may be emphasized differently in various applications. For a national defense system, the chief concern may be ensuring the confidentiality of classified information, whereas a funds transfer system may require strong integrity controls. The requirements for applications that are connected to external systems will differ from those for applications without such interconnection. Thus the specific requirements and controls for information security can vary.

3.2. Making system changes

Network Protection

- A basic part of network security is dividing a network into zones based on security requirements. This can be done using subnets within the same network, or by creating Virtual Local Area Networks (VLANs), each of which behaves like a complete separate network. Segmentation limits the potential impact of an attack to one zone, and requires attackers to take special measures to penetrate and gain access to other network zones.
- **Regulate Access to the Internet via Proxy Server**
  Do not allow network users to access the Internet unchecked. Pass all requests through a transparent proxy, and use it to control and monitor user behavior. Ensure that outbound connections are actually performed by a human and not a bot or other automated mechanism. Whitelist domains to ensure corporate users can only access websites you have explicitly approved.
- **Place Security Devices Correctly**
  Place a firewall at every junction of network zones, not just at the network edge. If you can’t deploy full-fledged firewalls everywhere, use the built-in firewall functionality of

your switches and routers. Deploy anti-DDoS devices or cloud services at the network edge. Carefully consider where to place strategic devices like load balancers – if they are outside the Demilitarized Zone (DMZ), they won't be protected by your network security apparatus.

- **Use Network Address Translation**

  Network Address Translation (NAT) lets you translate internal IP addresses into addresses accessible on public networks. You can use it to connect multiple computers to the Internet using a single IP address. This provides an extra layer of security, because any inbound or outgoing traffic has to go through a NAT device, and there are fewer IP addresses which makes it difficult for attackers to understand which host they are connecting to.

- **Monitor Network Traffic**

  Ensure you have complete visibility of incoming, outgoing and internal network traffic, with the ability to automatically detect threats, and understand their context and impact. Combine data from different security tools to get a clear picture of what is happening on the network, recognizing that many attacks span multiple IT systems, user accounts and threat vectors.

- Achieving this level of visibility can be difficult with traditional security tools. Cynet 360 is an integrated security solution offering advanced network analytics, which continuously monitors network traffic, automatically detect malicious activity, and either respond to it automatically or pass context-rich information to security staff.

Internet access and availability

Internet access

- Internet access is the process of connecting to the internet using personal computers, laptops or mobile devices by users or enterprises. Internet access is subject to data signaling rates and users could be connected at different internet speeds. Internet access enables individuals or organizations to avail internet services/web-based services.
- Internet access is often provided at home, schools, workplaces, public places, internet cafes, libraries and other locations. The internet began to gain popularity with dial-up internet access. In a relatively short time, internet access technologies changed,

providing faster and more reliable options. Currently, broadband technologies such as cable internet and ADSL are the most widely used methods for internet access. The speed, cost, reliability and availability of internet access depends on the region, internet service provider and type of connection.

- There are many different ways to obtain internet access, including:
  - Wireless connection
  - Mobile connection
  - Hotspots
  - Dial-up
  - Broadband
  - DSL
  - Satellite
- Access to computers or smart devices is one of the important factors for understanding the level of internet access for a region. However, internet access is not uniformly distributed within or between countries. A digital divide exists between many countries and regions. Good internet access is associated with regions with high-income populations, a high development index and high technological development.

Internet Availability

Internet Availability is defined as the ability to route a data packet from Customer's environment located within a cabinet or suite in the Space, to the egress point to the public Internet. Measurement — SunGard will measure availability of the SunGard Internet protocol network by computing the total number of successful performance measurements between agents as a percentage of the total number of attempts between agents.

Self check 3

Directions: Answer all the questions accordingly.

Part I: write **true** if the statement is correct and false if the statement is incorrect

1. Network Address Translation translate internal IP addresses into addresses accessible on public networks
2. Malware allowing attackers to compromise systems, steal data and do damage.
3. Exploiting vulnerabilities in software used in the organization, to gain unauthorized access, compromise or sabotage systems.
4. Internal Threats do not have authorized access to the computer systems or network.
5. Access levels are a way for organizations to control who has access to information or resources.

Part II Choose the correct answer from the alternatves provived

1. What are some common methods of access the internet?

   a.Wired connection b. Wi-fi connection

   c. Mobile data d.Satellite connection

2. Which of the following are common security measuresto protect internet acess

   a. Using strong password
   b. Enabling two factor authentication
   c. Regularly updating software and devices
   d. Avoid sharing personal information
   e. All of the above

Unit Four: Ensure user accounts are verified for security

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

- Confirming user settings with security policy
- Displaying legal notices for users
- Checking and verifying passwords with business

This guide 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:

- Discuss user settings with security policy
- Explain legal notices for users
- Check and verify passwords with business

4.1 Verifying user settings for security policy

- Security Policy identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources.
- Effective IT Security Policy is a model of the organization’s culture, in which rules and procedures are driven from its employees' approach to their information and work.
- Thus, an effective IT security policy is a unique document for each organization, cultivated from its people’s perspectives on risk tolerance, how they see and value their information, and the resulting availability that they maintain of that information.
- For this reason, many companies will find a boilerplate IT security policy inappropriate due to its lack of consideration for how the organization’s people actually use and share information among themselves and to the public.
- The objectives of security policy is the preservation of confidentiality, integrity, and availability of systems and information used by an organization’s members.

4.2 Displaying legal notices

- Group policy used to configure the legal notices on the domain computers. It is possible to configure Windows Server to display a message to users when they log on.
- When you configure legal notice, the legal notice message appears when the user hits CTRL+ALT+DEL. While I was working as system admin, I got the task to configure a logon banner. This was for Windows Server 2008 R2 and I am sure the steps covered in this post should work with next versions of server releases.
- Configuring legal notices on domain computer using Group policy
- Login to the domain controller with an administrator account.

4.3 Checking and verifying passwords

- A password is a case-sensitive string that can contain up to 104 characters. Valid characters for passwords are letters, numbers, and other symbols.
- When you set a password for an account, the operating system (OS) stores the password in an encrypted format in the account database. But simply having a password is not enough. The key to preventing unauthorized access to network resources is to use secure passwords than average passwords in that secure passwords are made difficult to guess and crack by using combinations of all the available characters available. Passwords are not necessarily required by a network operating system. In situations where security is not an issue, it is possible to modify an account so that it no longer needs a password.
- In most circumstances, however, passwords are required because they help ensure the security of a network environment. The first thing the administrator should do when setting up an account is to enter an initial password. This will prevent unauthorized users from logging on as administrator and creating accounts.
- Users should create their own unique password and should change it periodically. The account administrator can require users to do this automatically by setting a password-change time interval for the user.
- Some guidelines exist that govern the use of passwords. All users, including the administrator, should:
  - Avoid obvious passwords such as birthdates, social security numbers, or the names of spouses, children, pets, and so on.
  - Memorize the password, rather than write it down and tape it to the monitor.
  - Remember the password expiration date, if there is one so that the password can be changed before it expires and the user is locked out of the system.
  - A Strong Password is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.
- The following are general recommendations (guidelines) for creating a Strong Password:
  - A Strong Password should -

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~! @#$%^&*()_-+=)

A Strong Password should not -

- Spell a word or series of words that can be found in a standard dictionary
- Spell a word with a number added to the beginning and the end
- Be based on any personal information such as user id, family name, pet, birthday, etc

Password policies

- Password policies are a set of rules that helps you to manage password attributes and controls security for passwords. You can enhance password and account security on all user accounts in the Access Manager perspective of Management Console.
- Which includes the following: -
  - Set a complex password requirement
  - Enhances password security by enabling users to specify a complex password when logging into Management Console.
  - Enforce password history
  - Enables system administrators to enhance security by ensuring that old passwords are not continually reused. For this policy to be effective, do not let users change their password immediately after setting a new one. You can control this by setting the minimum age of the password.
  - Enforce a password expiry policy
  - Enables system administrators to enhance security by ensuring that new passwords are created and associated with user accounts.
  - Lock accounts after a number of failed login attempts
  - Enables a three strikes login policy which is used to prevent computer password attacks. The policy creates a condition where a user will be locked out of their account after a number of attempts. By default, this setting is set to 3 login attempts.
  - Enforce an account expiry after new account creation

- Enhances account security by forcing users to change their passwords when a new account is created for them.
- Display the number of failed login attempts
- Enables users to track the number of failed login attempts before they get locked out of the account.
- Display the last successful login
- Enables users to track their last successful login.
- Account lockout policies
- Account lockout polices control how and when accounts are locked out of the domain or the local system. These policies are:

Account lockout threshold

- Account lockout threshold sets the number of logon attempts that are allowed before an account is locked out. If you decide to use lockout controls, you should set this field to a value that balances the need to prevent account cracking against the needs of users who are having difficulty accessing their accounts.
- The best security policy (rules instructing the operating system how to perform certain tasks, whether or not to require certain actions, and so forth) is to lock the account indefinitely. When you do that, only administrators can unlock the account which aims at to prevent hackers from trying to access the system again and will force users who are locked out to seek help from an administrator, which is usually a good idea.
- Reset Account Lockout Threshold After: - Every time a logon attempt fails, windows raise the value of a threshold that tracks the number of bad logon attempts. Reset account lockout threshold after determines how long account threshold is maintained. This threshold is reset in one of two ways. If a user logon successfully and if the waiting period for reset account lockout threshold after has elapsed since the last bad logon attempt. By default, the lockout threshold is maintained for one minute, but you can set any value from 1 to 99,999 minutes. As with account threshold, you need to select a value that balances security needs against user access needs. A good value is from one to two hours which is long enough to force hackers to wait longer than they want to before trying to access the account again.

Self- check 4

Directions: Answer all the questions accordingly.

Part I: Choose the correct answer from the give alternatives

1. What is the primary purpose of a security policy?

   a. To maximize profits b. To minimize employee productivity

   c. To protect assets and information d. To restrict access to the internet

2. Which of the following is NOT typically included in a security policy?

   a. Password requirements b. Company mission statement

   c. Incident response procedures d. Data encryption standards

3. What does the term "least privilege" refer to in the context of security policies?

   a. Giving employees maximum access rights

   b. Providing access based on job responsibilities

   c. Allowing unrestricted access to sensitive data

   d. None of the above

Part II: Discuss the following question

1. What is security policy?

_____
_____
_____

2. Explain in details password and password policy

_____
_____
_____

3. Define legal notes with example

_____
_____
_____

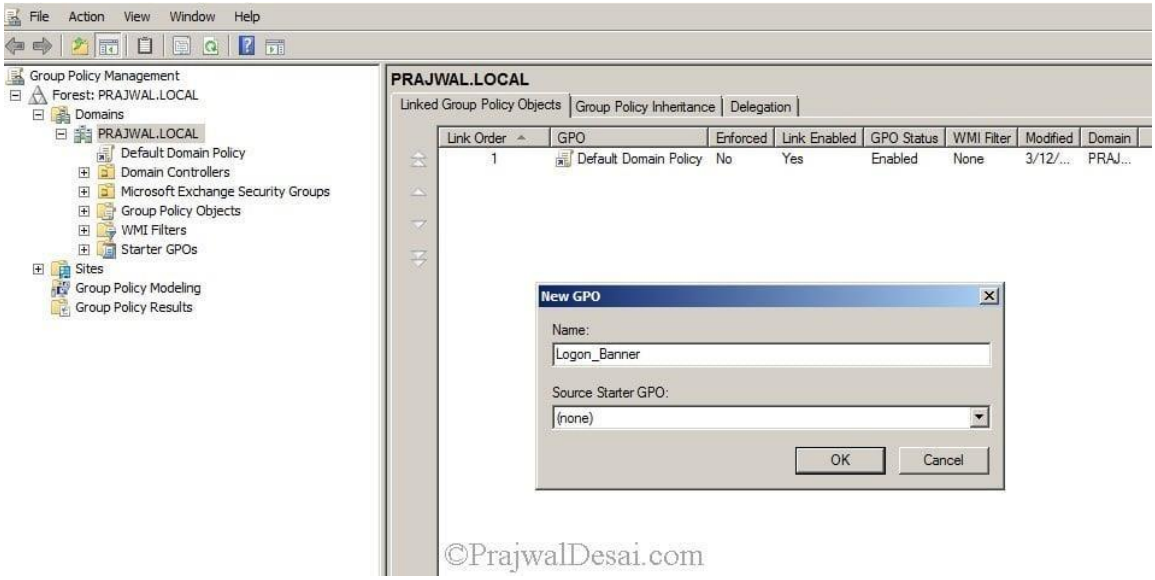
Operation sheet 4: Configure Group Policy

Operation Title: To Configure Group Policy

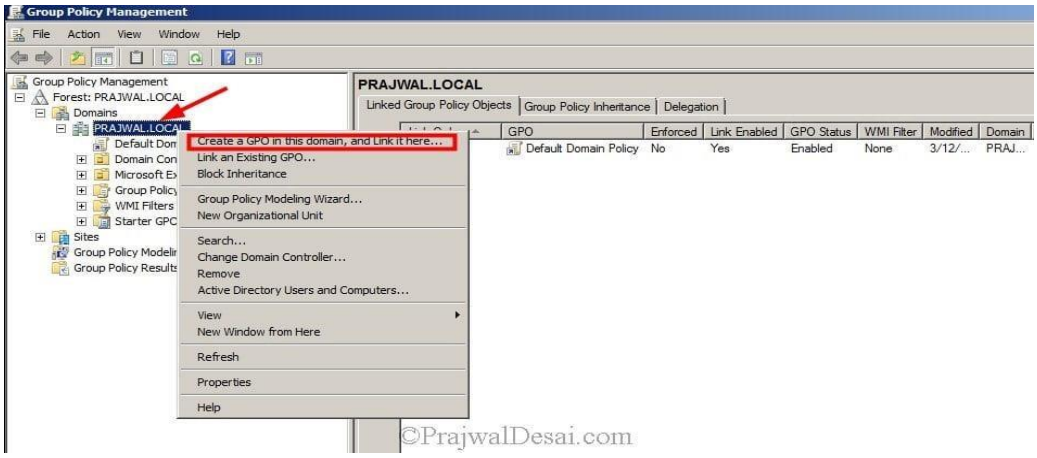
Purpose: To understand about policy in user account

Click Start > Administrative Tools > Group Policy Management.

Under Domains, right click your domain and click Create a GPO in this domain, and link it here

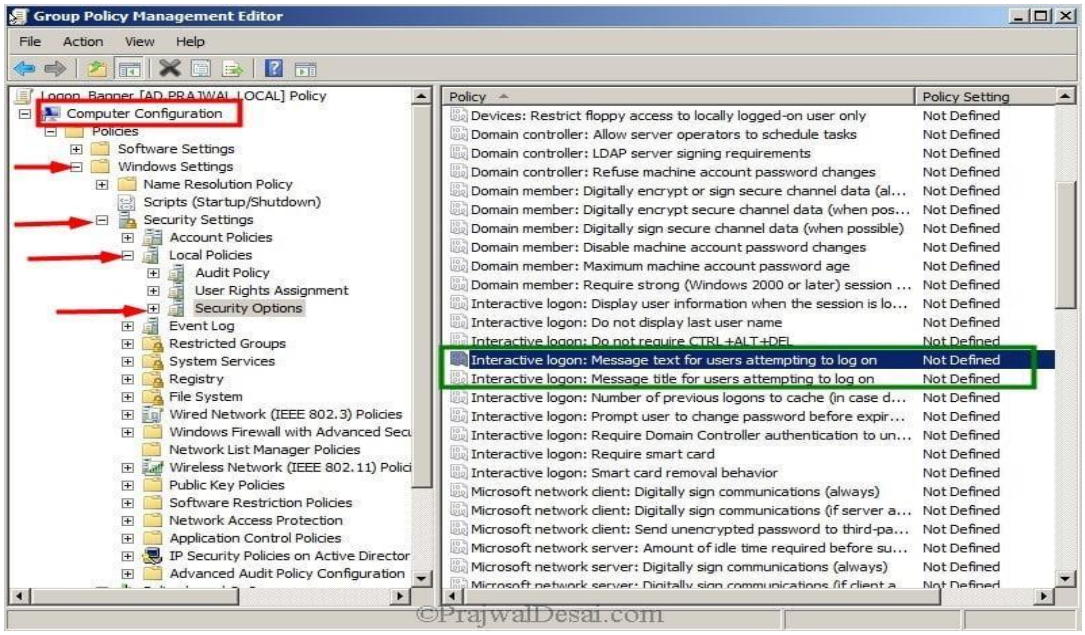


Create a policy and name it as Logon Banner. Click OK.



Right click this new policy Logon Banner and click Edit. You should see Group Policy Management Editor.

In the next step expand Computer Configuration > Policies > Windows Settings >Security Settings > Local Policies. Now click Security Options.



On the right pane look for the policy Interactive Logon: Message text for users attempting to log on. This security setting specifies a text message that is displayed to users when they log on. You can paste the Logon text that is to be displayed to the users before they log in. Click Apply and OK.

Lap Tests

Instructions: Given necessary templates, tools and materials you are required to perform the following tasks accordingly.

Task 1: Assign window password length

Task 2: create Group Policy

Unit Five: Manage and support internet

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

- Managing Internet Infrastructure
- Tools and equipment
- Monitoring network traffic access
- Internet performance

This guide 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:

- Manage Internet Infrastructure
- Idintfy Tools and equipment
- Monitor network traffic access
- Describe Internet performance

5.1. Managing Internet Infrastructure

Managing internet infrastructure involves overseeing and maintaining the components and systems that collectively enable the functioning of the internet. This encompasses a wide range of activities and considerations to ensure that the infrastructure is secure, efficient, and reliable.

- **Network Design and Architecture**: Planning and designing the overall structure of the network based on requirements, scalability, and redundancy.
- **Hardware Management**: Procuring, installing, and maintaining networking hardware such as routers, switches, and servers, and updating firmware and software regularly.
- **Software and Protocol Management**: Implementing and managing networking protocols and standards, such as TCP/IP, and keeping software applications and operating systems up to date.
- **Security Measures**: Implementing robust security policies and measures to protect against cyber threats, such as firewalls, intrusion detection systems, and encryption protocols, and regularly auditing and assessing security vulnerabilities.
- **Monitoring and Analytics**: Implementing monitoring tools to track network performance and detect anomalies, analyzing data and performance metrics to optimize efficiency and troubleshoot issues, and utilizing analytics for capacity planning and predicting future needs.
- **Backup and Disaster Recovery**: Implementing backup solutions for critical data and configurations, developing and testing disaster recovery plans to minimize downtime in the event of a catastrophic failure, and storing backups in secure and geographically diverse locations.
- **Resource Scaling and Optimization**: Scaling resources based on demand to ensure optimal performance and cost-effectiveness, and optimizing network configurations and protocols to improve speed and reliability.

5.2. Tools and equipment

Common tools and equipment used for internet infrastructure:-

- **Networking Hardware:**
  - Routers, Switches, Hubs, Modems, Access Points, Firewalls, Load Balancers
- **Servers:**
  - Web Servers , Database Servers , Application Servers, File Servers, DNS Servers
- **Networking Cables:**
  - Ethernet Cables , Fiber Optic Cables
- **Networking Tools:**
  - Crimping Tools ,Cable Testers, Tone and Probe Kit, Cable Strippers, Punch Down Tools
- **Power Equipment:**
  - Uninterruptible Power Supply , Power Distribution Units , Surge Protectors
- **Security Equipment:**
  - Firewalls, Intrusion Detection Systems , Virtual Private Network ,Appliances, Security Cameras
- **Testing Equipment:**
  - Network Analyzers, Cable Certifiers, Spectrum Analyzers
- **Cooling Systems:**
  - Air Conditioners, HVAC Systems, Cooling Fans
- **Backup Systems:**
  - Network Attached Storage ,Tape Drives, Cloud Backup Services
  - Ping and Traceroute Utilities
  - Network Analyzers
- **Collaboration Tools:**
  - Messaging Platforms
  - Video Conferencing Systems

Internet performance

Internet performance refers to the quality and efficiency of the delivery of data and services over the Internet. It encompasses various factors that collectively determine how well users can access and interact with online content, applications, and services.

- **Speed**: Internet performance is often closely associated with speed, which refers to how quickly data can be transferred between devices and servers. It is typically measured in terms of bandwidth, represented in megabits per second (Mbps) or gigabits per second (Gbps). Higher speeds generally result in faster downloads, quicker webpage loading times, and smoother streaming experiences.
- **Latency**: Latency is the delay or lag between sending a request and receiving a response. Low latency is crucial for real-time applications such as online gaming, video conferencing, and VoIP (Voice over Internet Protocol). Latency is typically measured in milliseconds (ms), and lower values indicate better performance.
- **Reliability**: Internet performance is influenced by the reliability of the network infrastructure. A reliable network ensures consistent connectivity without frequent disruptions or downtime. Redundancy measures, failover mechanisms, and high network availability contribute to improved reliability.
- **Packet Loss**: Packet loss occurs when data packets do not reach their intended destination. It can lead to degraded performance and disruptions in communication. Maintaining low packet loss is essential for a smooth and reliable internet experience, particularly for applications that require a continuous data stream.
- **Jitter**: Jitter refers to the variation in latency over time. Inconsistent latency, or jitter, can affect the quality of real-time applications. For example, jitter can result in choppy voice or video calls. Stable and predictable latency is important for applications that demand a consistent data flow.

Self check 5

Directions: Answer all the questions accordingly.

Part I: Discuss the following question

1. Speed is a crucial aspect of internet performance, and higher speeds generally result in faster downloads, quicker webpage
2. Testing Equipment, such as Network Analyzers and Cable Certifiers, is crucial for diagnosing and resolving issues in internet infrastructure.
3. Network Design and Architecture involves planning and designing the overall structure of the network based on requirements, scalability, and redundancy.
4. Managing internet infrastructure involves overseeing and maintaining the components and systems that collectively enable the functioning of the internet.

Part II: Discuss the following question

1. What internet infrastructure procedures and policies?

   _____
   _____
   _____

2. Explain in details Network Border Protection

   _____
   _____
   _____

3. List the two principles for filtering at the firewall level discuss them in details

_____
_____
_____

Unit Six: Plan and Organize Work

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

- Objectives are consistent with and linked to work activities in accordance with organizational aims.
- Objectives are stated as measurable targets with clear time frames
- Tasks/work activities to be completed are identified and prioritized as directed
- Schedule of work activities is coordinated with personnel concerned

Work plans are implemented in accordance with set time frames, resources and standards. This guide 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:

- Define Objective consistent linked to work activities in accordance with organizational aims.
- Objectives are stated as measurable targets with clear time frames
- Identify Tasks/work activities to be completed are identified and prioritized as directed
- Develop Schedule of work activities is coordinated with personnel concerned

Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below and try to understand what are being discussed. Ask your teacher for assistance if you have hard time understanding them.
3. Read the information written in the information Sheets
4. Accomplish the Self-checks

6.1. Setting objectives

Objectives are reliable with and connected to work activities in accordance with organizational aims. Objectives are confirmed as measurable targets with clear time frames. A specific result that a person or system aims to achieve within a time frame and with available resources. Objectives should be consistent with the organization work activities and accordance with the organization aims. While setting objectives they should be stated as measurable target with clear time frame. Team members should reflect support and commitment in the objective. Organizations need to identify realistic and attainable objectives. In general, objectives are more specific and easier to measure than goals. Objectives are basic tools that motivate all planning and strategic activities. They serve as the basis for creating policy and evaluating performance. Some examples of business objectives include minimizing expenses, expanding internationally, or making a profit.

General Objective

General objectives are wide goals to be achieved. The general objectives of the study state what the student expects to achieve by the study in general terms. General objectives are usually less in number.

Example:

The general objective of the study is to evaluate factors which affect employee's motivation at Bishoftu Polytechnic College.

Specific Objective

Specific objectives are short term & narrow in focus. General objectives can broken into small logically connected parts to form specific objectives.

Example:

The specific objective of the study is as follows:

- To investigate those factors that affect employee's motivation.
- To examine the instrument managers use to motivate their employees.
- To assess the relationship between job performance and employees motivation.
- To identify the factors which improves the satisfaction level of the employees.

Characteristics of a specific objective

It is always expressed in terms of the student. It is clear, in other words it is exact and supports only one understanding. It describes a visible behavior on the part of the subject. It specifies, where appropriate, the special conditions in which this behavior is manifested and the criteria which will make it possible to judge whether the objective has been attained.

The Goals

These are specific interim or ultimate time-based measurements to be achieved by implementing strategies in pursuit of the company's objectives, for example, to achieve sales of $3m in three years time. Goals should be quantifiable, consistent, realistic and achievable. They can relate to factors like market (sizes and shares), products, finances, profitability, utilization, efficiency.

Develop SMART objectives

Every business needs to set objectives for it in order to focus the company on specific aims over a period of time. Typically, these company objectives are cascaded into department, team and finally individual employee goals and objectives. This process aligns the tasks and responsibilities of each employee directly to overall company objectives, ensuring that employees are doing the things that they need to do for the company to be successful. This alignment helps employees better understand the importance of their job and increases engagement and commitment. When developing employee goals, it is important that they be clearly understood and structured so that the employee and their manager can measure and monitor success. A very successful approach to developing objectives is the SMART method.

SMART objectives are an acronym that describes the key characteristics of meaningful objectives, which are:

S – Specific

M – Measurable

A – Attainable

R – Relevant

T – Time-based

Specific

Objectives should be specific; meaning concrete, detailed, focused and well defined. Objectives need to specify what needs to be done to meet the desired outcome. When setting specific objectives, consider:

- WHAT needs to be done?
- WHY is it important to do it?
- WHO is going to do it?
- WHEN does it need to be done?
- How is it going to get done?

Measurable

When objectives are measurable, progress can easily be mapped and roadblocks identified. Further, when progress can be measured, it can be compared with competitors and other companies in the same field/market. Measurable objectives can be very motivating to staff since they can see how far they come and have a clear view of their goal. When setting measurable objectives, consider:

- HOW will they be measured?
- WHAT is the measurement source?
- WHO will do the measuring?

Attainable

Objectives need to be attainable. If the objective is too far in the future or not reasonably achieved, staff will not be motivated. Objectives can challenge staff without frustrating them and causing unnecessary stress.

When setting attainable objectives, consider:

- Can we get it done in the proposed timeframe?
- Do we have the resources to reach the objective?
- Do I understand the limitations and constraints?
- Has anyone else done this successfully?

Relevant

There should be a clearly understood link between the actions of an employee and the expected results.

When setting relevant objectives, consider:

- Will this objective lead to the desired results?
- Is this supporting team, department and company objectives?

Time-based

Objectives should be time-based. Time constraints encourage individuals to complete their tasks. When objectives have deadlines, it is easier to organize what needs to happen and when. When setting time-based objectives, consider:

- When is the deadline for this objective?
- When should each stage be completed?

6.2. Planning and prioritizing work activity

Breaking tasks down into subtasks

When you are faced with a big task, it helps if you break the task down into smaller, more manageable parts. This will help you avoid stress and procrastination. People who procrastinate often comment that when they wait until the last minute, they feel overwhelmed, and the task seems insurmountable. By setting priorities and breaking the bigger project into smaller tasks, the work is more manageable and less intimidating.

Here is one way to break tasks down.

- **Look at the big picture.** Make sure you understand what the end product is supposed to look like.
- **Examine the parts of the task.** Figure out step-by-step what you need to do because it's not going to happen through magic.
- **Think about the logical order of completing the pieces.** What should you do first, second, third, etc.?
- **Create a timeline for completing your tasks.** Having a deadline will make you more focused for each task.
- **Have a plan to help you stay on track.** Put the time you will spend on the project into your schedule so that you can set aside the time for it. Stick with this plan. A plan is only good if you see it through.

- **Complete your task early enough to have some time left for a final review.**

Prioritizing tasks

When you have a long To Do list, it can be quite great. In fact, you can feel so stressed by a lengthy To Do list that the feeling of being stressed can stop you in your tracks, preventing you from accomplishing anything at all. One way to stop feeling stressed and get back to accomplishing the tasks on your To Do list is to prioritize tasks. This technique is effective for work-related tasks and for personal tasks as well.

Importance of prioritizing tasks

Simply, you prioritize, if you want to know,

- What to do next in your flow of work.
- What is the next most important thing to do?

Why to prioritize?

- Minimize stress
- Maximize efficiency
- Help your target group (Boss or customer or both).
- Do you wisely use your time? That´s the initial importance of prioritizing

Possible criteria for choosing the next task

- Is it an urgent or important request from outside? (From your boss, your customer, anybody else?)
- Is it an immediate urgent require?
- Does it lead to your goal?

Priority setting is the top activity and skill at time management

In view of the fact that priority setting has much to do with the ability to make best decisions, because it is based on some other skills and is the core activity of time management, decision making will be covered in an own page. Priority setting is a continuous decision making process building a ranking among two or more possibilities. Deciding normally deals with the discrimination of two possibilities, leaving one alternative behind in favor of the other.

6.3. Scheduling work activities

Scheduling is the art of planning your activities so that you can achieve your goals and priorities in the time you have available. When it's done effectively, it helps you:

- Understand what you can realistically achieve with your time.
- Make sure you have enough time for essential tasks.
- Add contingency time for "the unexpected."
- Avoid taking on more than you can handle.
- Work steadily toward your personal and career goals.
- Have enough time for family and friends, exercise, and hobbies.
- Achieve a good work-life balance.

How to Schedule Your Time

Scheduling is the process by which you plan how you'll use your time. Doing it well can maximize your effectiveness and reduce your stress levels.

Follow this six-step process to prepare your schedule:

1: Identify Available Time. Start by establishing the time you want to make available for your work.

2: Schedule Essential Actions.

3: Schedule High-Priority Activities.

4: Schedule Contingency Time.

5: Schedule Discretionary Time.

6: Analyze Your Activities.

What are Activity Schedules?

An activity schedule is a type of visual support that provides permanent visual reminders of the order of events or tasks that occur in a given period of time. It describes when an activity will happen, when it will end, and what will occur after that (Ganz, 2007). In other words, activity schedules function similarly to day planners or to-do lists. Although all activity schedules visually organize events or tasks in a sequential manner, there are several different ways to represent items on the schedule and to format the schedule itself. For instance, depending on how the learner makes sense of information, small objects might be used to represent activities on the schedule. Other learners might benefit from simple photograph/ picture and word pairings to label activities, while others might use a more traditional written or typed to-do list. Activity schedules can be located in one particular spot, or they can be portable, by using a clipboard or binder for a paper-based schedule or a smart phone or tablet for an electronically-based one.

6.4. Implementing work plan

Definition of work plan

A work plan is used to organize, visualize and provide a context for the project they are about to embark on. It lays out why the project exists and what it hopes to accomplish. It also details tasks that lead to the final deliverable and defines the roles and responsibilities of the team.

Work plan is planning activities: step-by step, you can work through the development of a work plan that:

- Identifies the tasks to be done;
- Who is going to be responsible for doing them;
- When they must be done; and

- The resources needed.

Work-plan objectives

A work-plan should outline the primary objectives of the team. Where there is an overall strategic plan for the office level, the overall objectives should be directly derived from the source – but only those that apply to the work-planning time period. Objectives that apply to a future time period should be omitted. The work-plan should clearly articulate what areas of focus are most important for the upcoming work year or budgetary cycle.

Implementation Work plan:

A Work plan or work implementation plan is a key strategic document that keeps teams on track throughout a project, indicating how a project is expected to run along with who is responsible for what. It is an extremely valuable planning tool — one that can be the difference between project success and project failure. It is also a comprehensive document, and if you have never built one before, the concept can feel a bit overwhelming.

A project implementation plan is a document that defines how a project will be executed. Implementation plans outline the project's goals, scope, and purpose, as well as listing the resources (including team members) necessary for a successful project.

Project implementation plans are sometimes called “strategic plans” because they lay out the strategy proposed for a project. But we like the longer name because it conveys more than just strategy: It suggests a process going into action, and it answers the question of how a team will arrive at a goal.

A project implementation plan serves as a critical reference point throughout the project's lifecycle, ensuring everyone is on the same page and everything is on the right track. It's a vital document for guiding decision-making, mitigating risks, and ultimately ensuring the successful completion of the project from start to finish.

Work plan includes a timeline, budget, and risk analysis. A pilot site is identified, and a method for assessing the success of the pilot is determined. The implementation plan

should be divided into milestones to measure progress against objectives and identify specific people responsible for each milestone.

Work plans and implementation are reviewed based on accurate, relevant and current information and this review is done based on the outcome of the work and feedback from different stakeholders. The results of review are provided to concerned parties to be used as the basis for adjustments/simplifications to be made to policies, process and activities. Work performance evaluation should be conducted based on organization rules and regulations and the report of this evaluation should be documented as per the requirement of the organization. Finally recommendations based on the result of the evaluation are presented to appropriate personnel.

Self-Check 6

Directions: Answer all the questions accordingly.

1. **Part I:** write **true** if the statement is correct and false if the statement is incorrect
2. Breaking tasks down into subtasks helps avoid stress and procrastination by making the work more manageable and less intimidating.
3. Prioritizing tasks is important to minimize stress, maximize efficiency, and ensure alignment with team, department, and company objectives.
4. SMART objectives are characterized by being Specific, Measurable, Attainable, Relevant, and Time-based.
5. Scheduling helps in maximizing effectiveness, reducing stress levels, and ensuring a good work-life balance.

Part I: Choose the best answer from the provided answer

1. You have a business selling produce and aim to sell 2000 Birr worth of fruit per week. Which organizational strategy is this an example of?
   A. Program objective
   B. Mission statement
   C. Vision statement
   D. Revenue cycle
2. Which of the following is an example of a vision statement?
   A. To serve the community daily by providing affordable healthcare and a tradition of caring.
   B. To bring inspiration and knowledge to every child in the world.
   C. To prepare fast, healthy meals for people on the go.
   D. To be an innovative leader by delivering quality public safety services.
3. What does the "R" in SMART stand for?
   A. Repeatable - you must be able to do the goal over and over again.
   B. Responsible -a goal must allow you to take charge.
   C. Realistic- you must be able to accomplish the goal
   D. Respectful - a goal must allow you to be kind and polite.

Reference

- "Tubes: A Journey to the Center of the Internet" by Andrew Blum
- "Where Wizards Stay Up Late: The Origins of the Internet" by Katie Hafner and Matthew Lyon
- "The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works" by Douglas E. Comer
- "Networked: The New Social Operating System" by Lee Rainie and Barry Wellman
- "The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World" by Michael Miller
- "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" by Bruce Schneier
- "DNS and BIND" by Cricket Liu
- "IPv6 Essentials" by Silvia Hagen
- "The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win" by Gene Kim, Kevin Behr, and George Spafford
- "Internet Architecture and Innovation" by Barbara van Schewick

Participants of this Module preparation

No	Name	Qualification	Field of Study	Organization/ Institution	Mobile number	E-mail
1)	Zerihun Abatae	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	APTC	0936325182	yinebebtairu07@gmail.com