TVET CERTIFICATE V in NETWORKING

WIRELESS NETWORK OUTDOOR.

NEWWN501

Use ICT at workplace set up wireless network outdoor.

Competence

Credits: 7

Learning hours: 70

Sector: ICT

Sub-sector: NETWORKING

Module Note Issue date: June, 2020

Purpose statement

This module is intended to the learner pursuing TVET certificate V in networking. At the end of this module the learner will be able to Plan for wireless network outdoor, Select, install and configure wireless devices, finalize build process, and will be able to work competitively in the ICT world under non directive supervision.

Table of contents

	2.5. Precise measurement and assessment of signal strength within and outside building.	
3. Finalize build process	3.1. Regular revision of network for performance issues, planned maintenance or upgrade requirements. 3.2. Regular reporting to client with network documentation and recommendations for performance issues. 3.3. Suitable file documentation according to organizational outlines.	53

Total Number of Pages: 61

Learning Unit 1 – Plan for wireless network outdoor.

LO1.1 – Identify, evaluate and clarify organizational requirements of the client.

Content/Topic 1: Identification of organization wants in regard to work environment

A. Bandwidth

Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time usually one second.

While bandwidth is traditionally expressed in **bits** per second (**bps**), modern network links have greater capacity, which is typically measured in millions of bits per second (**megabits per second**, or Mbps) or billions of bits per second (**gigabits per second**, or Gbps).

Bandwidth connections can be **symmetrical**, which means the data capacity is the same in both directions to upload or download data, or **asymmetrical**, which means download and upload capacity are not equal. In asymmetrical connections, upload capacity is typically smaller than download capacity.

Bandwidth may be characterized as network **bandwidth**, data **bandwidth**, or digital **bandwidth**.

End users pay for the capacity of their network connections, so the greater the capacity of the link, the more expensive it is.

A.1. Bandwidth required

The amount of bandwidth a person or company needs is entirely dependent on how they plan to use the Internet. Streaming or hosting large amounts of video for example, requires far more bandwidth than simply browsing the Internet.

Thus, to find out how much bandwidth organizations need, they need to calculate the maximum number of users who might be using the network connection at one time, then multiply that number times the bandwidth capacity required by each application.

A.3. Common Internet Connection Bandwidth

Modem / Dialup	56 kbit/s
ADSL Lite	1.5 Mbit/s
T1/DS1	1.544 Mbit/s
E1 / E-carrier	2.048 Mbit/s
ADSL1	8 Mbit/s

Ethernet	10 Mbit/s
Wireless 802.11b	11 Mbit/s
ADSL2+	24 Mbit/s
T3/DS3	44.736 Mbit/s
Wireless 802.11g	54 Mbit/s
Fast Ethernet	100 Mbit/s
OC3	155 Mbit/s
Wireless 802.11n	600 Mbit/s
OC12	622 Mbit/s
Gigabit Ethernet	1 Gbit/s
Wireless 802.11ac	1.3 Gbit/s
OC48	2.5 Gbit/s
USB 3.0	5 Gbit/s
Wireless 802.11ad	7 Gbit/s
OC192	9.6 Gbit/s
10 Gigabit Ethernet, USB 3.1	10 Gbit/s
Thunderbolt 3	40 Gbit/s
100 Gigabit Ethernet	100 Gbit/s

B. Network coverage area

Network coverage area is geographical area covered by the network of a service provider. It is the geographic *area* where the station can communicate.

Coverage is a *measure* of how large an *area* around a *wireless* transmitter has sufficient signal strength for *wireless* devices.

How the coverage field extends around a wireless access point depends on how it's designed primarily on the type and number of antennas used.

A classic wireless router with two or more external antennas pointing in different directions has a doughnut-shaped coverage area surrounding it. Directly above and below the router one can therefore end up inside the doughnut hole and have bad or no coverage, even though the router is sending strong signals with high speed.

If you have a wireless access point with built-in antennas along all the sides, you get a spherical coverage area, which basically stretches equally far in all directions.

The first major coverage issue is interference from other wireless signals which can be the neighbor's Wi-Fi network, a baby monitor, Bluetooth speakers, or even a microwave oven.
Another coverage issue is physical obstacles such as reinforced concrete in walls, floors, and ceilings, or heated floors, that can be a murder for Wi-Fi signals.

Content/Topic 2: Establishment of preventive maintenance and diagnostic policy.

An organization should put together a maintenance schedule so someone cleans or replaces the filters, checks the fan, and performs any other work to ensure the equipment is properly protected.

This is even more important if the equipment is not protected and out in the open.

A. Device cleaning

When cleaning computer equipment, you should be aware of things like static discharge, grounding, and what kind of tools you want to use to clean the interior. Remember to not cause a problem while trying to prevent one.

Example of device cleaning tools

- Hardware set that includes screw drivers.
- Compressed air.
- Cleaning cloth.
- Zip ties (optional)
- Scissors (optional)
- Cotton swabs (optional)
- Thermal paste (optional)
- Pencil or pen (optional)

If you keep your device off the floor, don't smoke, and don't have shedding pets, you can probably get away with cleaning once per year. But, always, if device starts getting hotter than usual, open it up to check for any dust or hair buildup and then clean it.

B. Device placement

Wireless device distributed mainly throughout interior spaces, providing service to the surrounding work areas.

Device Placement have been selected traditionally on the basis of coverage, bandwidth, channel reuse, cell-to-cell overlap, security, aesthetics, and deployment feasibility.

Note that keeping device on the floor allows for dust, hair, skin cells, and carpet particles to get inside easier. It is better to keep device on your desk where particles are less prone to getting inside.

C. **Problem solution processes**

C.1. Problem identification stage

Problem identification is the first step in a systematic process to identify, evaluate a problem and explore potential solutions.

There are several possible causes for a **network error**, the administrator should **identify** each probable cause.

Stages:

1. Identify the type of hardware and software.
2. Brief description of the problem.
3. Brief explanation of the steps to isolate the problem.

C.2. Problem resolution.

Problem solving is the process of identifying a **problem**, developing possible solution paths, and taking the appropriate course of action.

The first step in the problem-solving process is to **define** the problem. Combining solutions is the second step in the problem-resolving process.

Content/Topic 3: Identification of Roles and technical responsibilities in network management

A. Network mapper

Network Mapper (Nmap) is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Characteristics of Nmap.

- **Flexible**: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more.
- **Powerful:** Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- **Portable:** Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
- **Easy:** Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
- **Free:** The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.
- **Well Documented:** Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.
- **Supported:** While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the Nmap mailing lists. Most bug reports and questions should be sent to the nmap-dev list, but only after you read the guidelines. We recommend that all users subscribe to the low-traffic nmap-hackers announcement list. You can also find Nmap on Facebook and Twitter. For real-time chat, join the #nmap channel on Freenode or EFNet.
- **Popular:** Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). This is important because it lends Nmap its vibrant development and user support communities.

B. NS lookup

Nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

Nslookup is the name of a program that lets an Internet server administrator or any computer user enter a **host** name (for example, "whatis.com") and find out the corresponding **IP address**. It will also do reverse name lookup and find the host name for an IP address you specify.

How to use NSlookup?

1. Go to Start > Run and type cmd .
2. At a command prompt, type **nslookup**, and then press Enter.
3. Type server <IP address> where IP address is the IP address of your external DNS server.
4. Type set q=M X, and then press Enter.
5. Type <domain name> where domain name is the name of your domain, and then press Enter.

Content/Topic 4: Establishment of Vendor and product service level support agreements.

A. Service-level agreement (SLA)

SLA is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet.

The SLA should include

- The service being provided
- The standards of service
- The timetable for delivery
- Respective responsibilities of supplier and customer
- Provisions for legal and regulatory compliance
- Mechanisms for monitoring and reporting of service
- Payment terms
- How disputes will be resolved
- Confidentiality and non-disclosure provisions
- Termination conditions

The SLA defines the level of service expected by your organization from a vendor, it establishes how the service is to be measured and the remedies or penalties, if any, for non-compliance with the agreed service levels. It should clearly state metrics, responsibilities, expectations and timing and frequency so that, in the

event of issues, there's an objective measure that can be used to gauge compliance with the terms of the contract. It ensures all parties have the same understanding of requirements.

There are three options for structuring SLA: **Service-based, Customer-based**, and **Multi-level or Hierarchical SLAs.**

1. **Customer-based SLA**

   This type of agreement is used for individual customers and comprises all relevant services that a client may need, while leveraging only one contract. It contains details regarding the type and quality of service that has been agreed upon. For example, a telecommunication service includes voice calls, messaging and internet services, but that all exists under a single contract.

2. **Service-based SLA**

   This SLA is a contract that includes one identical type of service for all of its customers. Because the service is limited to one unchanging standard, it is more straightforward and convenient for vendors. For example, using a service-based agreement regarding an IT helpdesk would mean that the same service is valid for all end-users that sign the service-based SLA.

3. **Multi-level SLA**

   This agreement is customized according to the needs of the end-user company. It allows the user to integrate several conditions into the same system to create a more suitable service. It addresses contracts at the following levels:

   a. **Corporate level:**

      This SLA does not require frequent updates since its issues are typically unchanging. It includes a comprehensive discussion of all the relevant aspects of the agreement, and is applicable to all customers in the end-user organization.

   b. **Customer level:**

      This contract discusses all service issues that are associated with a specific group of customers. However, it does not take into consideration the type of user services.

   c. **Service level:**

      In this agreement, all aspects that are attributed to a particular service with regard to a customer group are included.

B. Evaluation process

It involves collecting and analyzing information about a wireless's activities, characteristics, and outcomes. Here are some suggestions for how to properly evaluate a wireless solution that you would want to deploy.

1. Establish which devices you will test with.
2. Identify the applications you will test with.
3. Setup your test environment.
4. Involve an engineer from the vendor you are evaluating.

C. Client

- **External organizations:** these are the conditions, entities, events, and factors surrounding an **organization** that influence its activities and choices, and determine its opportunities and risks.
- **Individuals:** is a singular unit, which **defines** you as a person.
- **Internal departments:** Departments inside the company require interoperability to ensure the job is running smoothly.
- **Internal employees:** Employees who work inside the company require assistance from another individual or department to get their job done.

D. Client's needs

wireless client needs to associate with an Access Point (AP) before it can communicate, while a wired client need to be connected an Ethernet bridge or a switch.

E. Bandwidth

The more bandwidth a data connection has, the more data it can send and receive at one time.

Content/Topic 5: Identification of Technical requirements

A. Network devices

Network devices are components used to connect computers or other electronic devices together so that they can share files or resources like printers or fax machines.

Wired Network Devices

- Hub
- Repeater
- Bridge
- Switch
- Router
- Gateway

- B-router (Bridging router)

Wireless Network Devices.

- Wireless Router
- Wireless Adapter
- Wireless Repeater
- Wireless Phones
- Wireless Access Point
- Modem
- Other devices such as garage door openers, baby monitors, certain video game consoles walkie-talkies, etc….

B. Network cables

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners, ….

1. Twisted pair cable
2. Fiber optic cable
3. Coaxial cable
4. Patch cable

LO 1.2 – Review existing network design documentation

Content/Topic 1: Designing a network

A. Network Schematic diagram

A network Schematic diagram is a visual representation of network architecture. It maps out the structure of a network with a variety of different symbols and line connections. It is the ideal way to share the layout of a network because the visual presentation makes it easier for users to understand how items are connected.

A.1. Tips for Network schematic diagram.

- **Choose a network:** Select the network to illustrate. The diagram could focus on a personal computer, or on an entire company network. Once a focus has been chosen, set limits on what outside connections will be included so that the diagram remains concise.

- **Add relevant equipment:** Begin by placing any involved computers, servers, and other components on the page. Use visual representations and add the names of the components for clarity.
- **Add any other important components:** Add other important components such as internet connections and firewalls. Once again, use visual representations and add text descriptions as needed.
- **Label:** Label each of the items on the page to make it easy for anyone to understand what they're looking at. Alternatively, number the items and attach a legend with descriptions to keep the diagram less cluttered.
- **Draw Connecting Lines:** Use lines with directional arrows to show how each component is related and connected to another.

A.2. Design diagram

There are many different ways to create a network diagram. While they can be created using pen and paper or a white board, a diagramming tool designed for this purpose is a much more efficient and effective approach.

Two types of network diagrams: The **Arrow Diagram** and the **Precedence diagram.**

The **arrow diagram** depicts nodes for events and arrows for activities. The **precedence diagram** depicts activities in the order they occur. If you work in IT, you will most likely use the arrow diagram.

Network diagrams are used whenever project management occurs. because these project management tools are so useful, they can help project management teams to visualize the planning they have put time and effort into, and gives a quick-glance view of the project. It also demonstrates who is responsible for which tasks.

B. Naming standards

Networking standards ensure the interoperability of networking technologies by defining the rules of communication among networked devices. Networking standards exist to help ensure products of different vendors are able to work together in a network without risk of incompatibility.

Standards organizations:

- ✓ International Organization for Standardization (ISO)
- ✓ International Electro-Technical Commission (IEC)
- ✓ Australian Standards (AS) standards
- ✓ American National Standards Institute (ANSI)
- ✓ International Telecommunication Union (ITU)
- ✓ Institute of Electrical and Electronic Engineers (IEEE)

- ✓ Video Electronics Standards Association (VESA)

C. Project-management templates and report writing

New organizational models have implemented project management organization structures to help **plan**, **schedule**, **direct**, and **control** company resources that have been allocated to short-term and long-term projects.

C.1. Report format and content

A technical report should contain the following:

1. **The title page:** The title of report is necessary to orient the reader.
2. **Introduction:** In the introduction, you are supposed to highlight the main aims of the report to the reader. Let the reader understand the purpose of you writing the report.
3. **The summary:** In summary, you need to write an overview of the whole report.
4. **Experimental details:** This is the part that you need to state every detail of the experiment, starting from the equipment that you used to the procedure for the test.
5. **Results:** This is where you are expected to explain the results that you obtained. You should give clear explanation so that the reader cannot ask themselves any question on your results.
6. **The body:** This is where you explain the use of results obtained.
7. **Conclusions:** In conclusion, you also need to use words that suggest you are concluding your work.
8. **Recommendations:** You are supposed to suggest solutions to the challenges that you meet while activity taking place.

LO 1.3 – Identify network topology

Content/Topic 1: Identification of network topology

A. Definition of network topology

Network Topology refers to the layout of a network and how different nodes in a network are connected to each other and how they communicate. Topologies are either physical (the physical layout of devices on a network) or logical (the way that the signals act on the network media, or the way that the data passes through the network from one device to the next).

B. **Network topology types**

B.1. Network Logical Topology

A logical topology is a concept in networking that defines the architecture of the communication mechanism for all nodes in a network.

The logical topology defines how the data should transfer.

The logical topology defines how nodes in a network communicate across its physical topology.

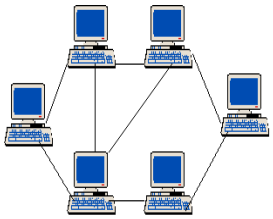
B.2. Network Physical Topology

Physical topology refers to the physical design of the network. The following are the types of Physical topology

a. Mesh Topology

In a mesh network topology every node is connected to every other node in the network. There are two types of mesh topologies.

Full mesh topology: occurs when every node has a circuit connecting it to every other node in a network. Full mesh is very expensive to implement but yields the greatest amount of redundancy, so in the event that one of those nodes fails, network traffic can be directed to any of the other nodes. Full mesh is usually reserved for backbone networks.



Partial mesh topology: is less expensive to implement and yields less redundancy than full mesh topology. With partial mesh, some nodes are organized in a full mesh scheme but others are only connected to one or two in the network. Partial mesh topology is commonly found in peripheral networks connected to a full meshed backbone.

Advantages of a mesh topology

- It is secure network.
- Manages high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.

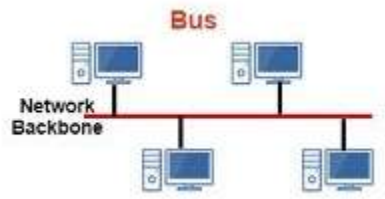
Disadvantages of a mesh topology

- The cost to implement is higher than other network topologies, making it a less desirable option.
- Building and maintaining the topology is difficult and time consuming.

- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.
- It is difficult to expend network.
- It requires a huge amount of cables.

b. Bus topology

In networking a bus is the central cable -- **the main wire** -- that connects all devices on a local-area network (LAN). It is also called the *backbone*. This is often used to describe the main network connections composing the Internet. Bus networks are relatively inexpensive and easy to install for small networks. Ethernet systems use a bus topology.



Advantages of bus topology

- It is simple and easy to use.
- It requires small length of cable to connect computers.
- It is less expensive.
- It is best-suited for small networks.
- It is easy to extend a bus. It allows more computers to join network.
- If one node fails, it does not affect the rest of the network.

Disadvantages of bus topology

- It is difficult to troubleshoot.
- It only supports small number of computers.
- The network speed slows down as the number of computers increases.
- It is not easy to isolate faults in the network nodes.
- It is suitable for networks with low traffic. High traffic increases load on the bus, and the network efficiency drops.
- The cable length is limited. This limits the number of network nodes that can be connected.
- When the number of devices connected to the bus increases, the efficiency decreases.
- It is heavily dependent on the central bus. A fault in the bus leads to network failure.

- Each device on the network "sees" all the data being transmitted, thus posing a security risk.

c. Ring topology

A local-area network (LAN) whose topology is a ring. That is, all of the nodes are connected in a closed loop. Messages travel around the ring, with each node reading those messages addressed to it.

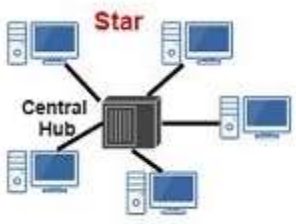
Advantages of ring topology

- In this topology, each node has the opportunity to transmit data. Thus, it is a very organized network topology.
- The adding or removing of network nodes is easy, as the process requires changing only two connections.
- The traffic is unidirectional and the data transmission is high-speed.
- The configuration makes it easy to identify faults in network nodes.
- It is less costly than a star topology.
- It can span larger distances than other types of networks, such as bus networks, because each node regenerates messages as they pass through it.

Disadvantage of ring topology

- Data sent from one node to another has to pass through all the intermediate nodes. This makes the transmission slower in comparison to that in a star topology. The transmission speed drops with an increase in the number of nodes.
- The failure of a single node in the network can cause the entire network to fail.
- The movement or changes made to network nodes affect the entire network's performance.
- There is heavy dependency on the wire connecting the network nodes in the ring.
- One nodes fail, a whole system fails

d. Star topology



In a star network devices are connected to a central computer, called a hub. Nodes communicate across the network by passing data through the hub.

Advantage of star topology

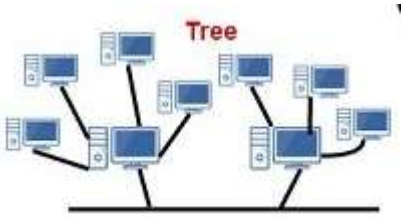
- As the analysis of traffic is easy, the topology poses lesser security risk.

- Adding or removing network nodes is easy, and can be done without affecting the entire network.
- Due to its centralized nature, the topology offers simplicity of operation.
- It also achieves isolation of each device in the network.
- Due to the centralized nature, it is easy to detect faults in the network devices.
- Data packets do not have to pass through many nodes, like in the case of a ring network. Thus, with the use of a high-capacity central hub, traffic load can be handled at fairly decent speeds.
- In a star network, one malfunctioning node doesn't affect the rest of the network.

Disadvantage of star topology

- The number of nodes that can be added, depends on the capacity of the central hub.
- Network operation depends on the functioning of the central hub. Hence, central hub failure leads to failure of the entire network.
- The setup cost is quite high.
- If the central computer fails, the entire network becomes unusable.

e. Tree / Hierarchical / Hybrid topology



This is a type of topology that combines characteristics of linear bus and star topologies. In a tree network, groups of star-configured networks are connected to a linear bus backbone cable.

Advantage of tree topology

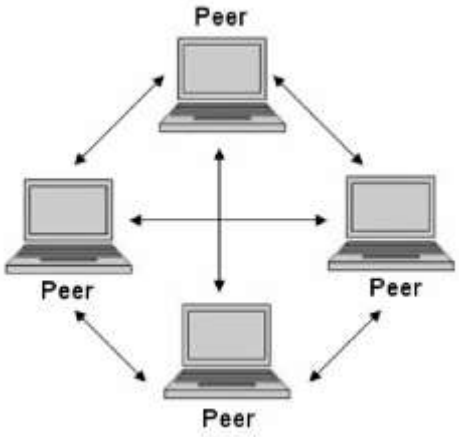
- Fault identification is easy.
- The advantages of centralization that are achieved in a star topology are inherited by the individual star segments in a tree network.
- The tree topology is useful in cases where a star or bus cannot be implemented individually. It is most-suited in networking multiple departments of a university or corporation, where each unit (star segment) functions separately, and is also connected with the main node (root node).
- Each star segment gets a dedicated link from the central bus. Thus, failing of one segment does not affect the rest of the network.
- The network can be expanded by the addition of secondary nodes. Thus, scalability is achieved.

Disadvantage of tree topology

- Owing to its size and complexity, maintenance is not easy and costs are high. Also, configuration is difficult in comparison to that in other topologies.
- As multiple segments are connected to a central bus, the network depends heavily on the bus. Its failure affects the entire network.
- Though it is scalable, the number of nodes that can be added depends on the capacity of the central bus and on the cable type.
- The entire network depends on a central hub and a failure of the central hub can cripple the whole network

f. Point to point

This topology also called Peer-to-peer, or P2P in its abbreviated form, refers to computer networks using a distributed architecture. In P2P networks, all the computers that are part of them are referred to as peers, and they share and exchange workloads. Each peer in a peer-to-peer network is equal to the other peers. There are no privileged peers, and there is no primary administrator device in the center of the network.



The **primary goal** of p2p networks is to share resources and help computers and devices work collaboratively, provide specific services, or execute specific tasks.

#	Advantages of P2P	Disadvantages of P2P
1	No need for a network operating system	Because each computer might be being accessed by others it can slow down the performance for the user.
2	Does not need an expensive server because individual workstations are used to access the files	Files and folders cannot be centrally backed up
3	No need for specialist staff such as network technicians because each user sets their own permissions as to which files they are willing to share.	Files and resources are not centrally organized into a specific 'shared area'. They are stored on individual computers and might be difficult to

		locate if the computer's owner doesn't have a logical filing system.
4	Much easier to set up than a client-server network - does not need specialist knowledge	Ensuring that viruses are not introduced to the network is the responsibility of each individual user
5	If one computer fails it will not disrupt any other part of the network. It just means that those files aren't available to other users at that time.	There is little or no security besides the permissions. Users often don't need to log onto their workstations

LO 1.4 – Identify the components required to be installed to meet the technical requirements

Content/Topic 1: Identification of network components.

Hardware

- Antennas and other connectivity devices
- Digital subscriber line (DSL) modems
- Mobile equipment
- Modem wireless access points
- Personal computers
- Power controllers
- Remote sites
- Servers
- Uninterruptible power supplies (ups)
- Workstations
- Cabling, such Twisted Pair cable (Category 5e, 6 and 7), Coaxial cable, Fiber optic cable.

Software:

- **Commercial applications:** Any software or program that is designed and developed for licensing or sale to end users or that serves a commercial purpose. Commercial software was once considered to be proprietary software, but now a number of free and open-source software applications are

licensed or sold to end users. Off-the-shelf software programs, such as games or those sold in computer specialty stores or even music stores and grocery stores, are some examples of commercial software.

- **Customized software:** A type of software designed for a specific user or group of users within an organization. A customized piece of software is a bespoke solution that has been developed and built with certain requirements in mind for a client. For **example**, car manufacturers simply have nowhere to turn to purchase **software** for the vehicle on-board computer.
- **In-house software:** A software that is produced by a corporate entity for purpose of using it within the organization. In-house software however may later become available for commercial use upon sole discretion of the developing organization. The need to develop such software may arise depending on many circumstances which may be non-availability of the software in the market, potentiality or ability of the corporation to develop such software or to customize a software based on the corporate organization's need.

  For example, a firm may decide to keep certain activities in-house, a process that is at times referred to as insourcing, such as accounting, payroll, marketing, or technical support. While it is common for some companies to outsource those divisions, a firm may maintain flexibility in those operations by keeping them in-house.
- **Organization specific software:** also known as **enterprise application software** (**EAS**), a computer software used to satisfy the needs of an organization rather than individual users. Such organizations include businesses, schools, interest-based user groups, clubs, charities, and governments. Enterprise software is an integral part of a (computer-based) information system; a collection of such software is called an enterprise system
- **Packaged software:** A collection of programs that perform similar functions or have similar features. For example, Microsoft Office includes multiple applications such as Excel, Word, and PowerPoint.

- **Wireless access:** comes in many flavors and designs. The closest to the user is the **software** which consists of the user interface. The front end is simple and used to provide connectivity to the network.

LO 1.5 – Contact vendors and service suppliers

Content/Topic 1: Contacting vendors and service suppliers

Finding a reliable and competitively-priced suppliers and vendors is vital to the success.

The terms that you negotiate with your vendors and suppliers need to be based on the **Specifications of components:**

- **Access Point:** a stand-alone device or computer that allows wireless devices (such as laptop computers) to connect to and communicate with a wired computer network.

  Tips

  - Get a WiFi access point that supports 802.11n, 802.11ac, or 802.11ax.
  - Make sure that it supports 5 GHz, so you can be ready for the future.
  - The more spatial streams, the better!
  - SOHO routers are great, but don't skimp if you really need an enterprise network.
- **Switch:** is a computer networking device that connects devices on a computer network by using packet switching to receive, process and forward data to the destination device.

  Basic switch Specs to consider:

  - Transceivers, Connectors, and Cables Used with Each I/O Module
  - Power requirement
  - Power Supply Cable Specifications
  - Weights and Quantities for the Chassis, Modules, Fan Trays, and Power Supplies
  - Environmental Specifications (Temperature,)
  - Switch dimensions (Width, Depth, Height)
- **Router:** is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet.

  Tips

  - Your router should have a multi-core processor and at least 128MB of RAM
  - The router that you choose should be dual-band or more
  - Router naming conventions should NOT be taken into account when making your buying decision
  - Verify online the real-life speed of the router that you buy

- Your router should have a smartphone app, preferably one that you can use from anywhere on the internet
- The router should have a USB port, preferably USB 3.0
- Advanced QoS instead of plain QoS (Quality of Service)
- Smart-home integration
- Support for Mesh Wi-Fi
- VPN, antivirus, firewall, and other advanced features

➢ **Uninterrupted Power Supply (UPS):** a device allows a computer to keep running for at least a short time when the primary power source is lost. It also provides protection from power surges.

Basic UPS Specs to consider:

- **UPS Type** (Single phase, double phase, DC power)
- **Technology** (Delta conversion, Ferro-Resonant, Hybrid technology, Line interface, On-line, Off-line, Rotary, ….)
- **Protection** (Lightning, Over Voltage, Power failure, Voltage sags,……)

LO 1.6 – Ensure preliminary work is completed within the required timeframe.

Content/Topic 1: Creation of Gantt Chart

In order to specify Something that comes before something else, **define the project** and to **prepare project plans and** schedules that support the **project definition**.

The first task is to produce a **Gantt chart** by plotting each activity on the plan using the early start date and elapsed time.

A Gantt chart is a graphic display of activity durations where activities are listed with other tabular information on the left hand side with time intervals over the bars and activity durations are shown in the form of horizontal bars.

Parts of Gantt chart.

- Activities
- Duration

- Progress

Sample Gantt chart.

Weeks	1	2	3	4	5	6	7	8	9	10
Project activities										
Planning										
Designing										
Coding										
Testing										
Delivery										

LO 1.7 – Ensure clients and users are aware of date and time of installation

Content/Topic 1: Ensuring clients and users are aware of date and time of installation

The implementation of each activity represented on the Gantt chart, it is better to include or communicate the progress to the users for keeping them be satisfied to services.

- **Users**
  - Community members
  - Department
  - Department within the organization
  - Third party.

LO 1.8 – Prepare and check installation and safety equipment

Content/Topic 1: Preparation and checking of installation and safety equipment

- **Safety equipment**
  - **Fire control system equipment:** is a number of components working together, usually a gun data computer, a director, and radar, which is designed to assist a weapon system in targeting, tracking and hitting its target

- **Air conditioning system:** is a device that monitors and maintains the temperature, air distribution and humidity in a network room or data center.
- **Personal Protective Equipment (PPE):** is clothing and equipment worn by employees, students, contractors or visitors to protect or shield their bodies from workplace hazards.

➢ **Safety arrangements**

- **Fire extinguisher:** is an active fire protection device used to extinguish or control small fires, often in emergency situations.
- **Safety clothes:** is **protective clothing**, helmets, goggles, or other garments or equipment designed to protect the wearer's body from injury or infection.

➢ **Checking/testing of devices and equipment**

- **Ping:** is a **networking** utility program or a tool to test if a particular host is reachable. It is a diagnostic that checks if your computer is connected to a server.
- **Traceroute:** is a utility that records the route (the specific gateway **computers** at each hop) through the Internet between your computer and a specified destination computer.

LO 1.9 – Assess on-site safety arrangements for installers and users

Content/Topic 1: Assessing site Safety arrangements for installers and users

➢ **Safety equipment arrangement**

- Fire control system equipment
- Air conditioning system
- PPE

➢ **Checking/testing of devices and equipment**

Measuring the quality of computer network equipment refers to a single device and is composed by a set of test lists, each meant to address a device feature (performance, scalability, conformance, interoperability, etc…)

- Switch
- Router
- Access point

LO 2.1 – **Select appropriate hardware based on identified components**

Content/Topic 1: Selection of hardware components.

Hardware

1. Access points

An access point is a device, such as a wireless router, that allows wireless devices to connect to a network. It's commonly wire connected to Ethernet network's router, hub or switch and then to create a simple wireless network.

This was done by using an Ethernet cable to connect a switch and an AP and the AP would then communicate with Wi-Fi devices and giving them network access. Wireless access point does not route anything. It just converts an existing wired network (LAN) into a wireless one (WLAN). A router can be an access point but an access point cannot be a router.

Depending on the Internet connection used, you will need one of the following two types of routers:

– If you use your home phone for internet access, you will need an **Asymmetric digital subscriber line (ADSL) router.**

– For other connections, such as those provided by cable operators or wireless broadband service provider, you will need a **non-ADSL router.**

The factors considered while selecting the best Wi-Fi router.

1. **Antenna: When you** want to get Wi-Fi access from another room walls or glass. Most routers have internal antennas.
2. **Dual-band: choose** router that allows connection to exceed 5GHz frequency band.
3. **USB Port:** Router with USB port lets you attach a flash drive, hard disk and even a printer, so you can share resources wirelessly over the network.
4. **Security:** Routers offer different security protocols such as WEP, WPA, and WPA2.
5. **Speed Router:** Internet speed is determined by the speed of the router.

2. Bridges

bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments.

Bridge devices work at the data link layer of the Open System Interconnect (OSI) model, connecting two different networks together and providing communication between them.

Bridges are similar to repeaters and hubs in that they broadcast data to every node.

3. Antennas

An antenna is a specialized transducer that converts radio frequency (RF) fields into alternating current (AC) or vice-versa.

There are two basic types of antennas:

- **The receiving antenna**, which intercepts RF energy and delivers AC to electronic equipment, and
- **The transmitting antenna**, which fed with AC from electronic equipment and generates an RF field.

LO 2.2 – Install and configure hardware to provide wireless network access

Content/Topic 1: Identification of antennas & accessories

A. Antennas

- **RF antennas:** RF Antenna input typically used to connect a television antenna, cable TV wire, or satellite feed to a television, VCR, or other device that can process radio-frequency video signals, including some computers. Knowing when to use an RF signal and how it differs from other signals can be useful when setting up some computer and video systems.
- **Microwave:** Microwave is a radio signal in the frequency range from 300 MHz to 300 GHz or from 1 to 300 GHz, depending on the rating system. Except for AM and FM radio, shortwave radio and over-the-air TV, almost all other communications systems transmit microwaves, including satellites, cellular systems, wireless LANs and line-of-sight between buildings and across vast distances
- **Power over Ethernet (POE):** It describes any of several standard ad-hoc systems, which pass electric power along with data on twisted pair Ethernet cabling. This allows a single cable to provide both data connection and electric power to devices such as wireless access points, IP cameras, and VoIP phones.

Power over Ethernet brings many advantages to an installation

Time and cost savings - by reducing the time and expense of having electrical power cabling installed.

Safety - POE delivery is intelligent, and designed to protect network equipment from overload, under powering, or incorrect installation.

Reliability -It can be backed-up by an uninterruptible power supply, or controlled to easily disable or reset devices.

Scalability - having power available on the network means that installation and distribution of network connections is simple and effective.

B. Standards

- **Federal communication Commission:** The FCC (Federal Communication Commission) is the government body responsible for maintaining laws, censorship and broadcast licensing pertaining to interstate and international communications in the United States.

  The FCC is an independent government organization that runs from the proceeds of regulatory fines in its regulation of radio, TV, wire and satellite communications.
- **IEEE:** is widely popular for the development of standards for computer networking and its suite of services. IEEE develops many different standards, such as IEEE 802 and IEEE 802.11 (commonly known as Wi-Fi), and provides ongoing innovation, amendments and maintenance services for these standards.
- **Major organizations:** These are the organizations that Specify the principles and procedures by which the institution assures that it provides an appropriate learning and research environment.

  Examples of major organizations.

  - **American National Standards Institute** (ANSI) is the primary organization for fostering the development of technology standards in the United States.
  - **The British Standards Institution** (BSI) is a service organization that produces standards across a wide variety of industry sectors.
  - **The Internet Engineering Task Force** (IETF) is the body that defines standard Internet operating protocols such as TCP/IP.
  - **Organization for the Advancement of Structured Information Standards** (OASIS) exists to promote product-independent standards for information formats such as XML and HTML.
- **Competing technologies:** competition in the market is provided by standards that allow standardized technology to be used in products and services without any a priori advantage.

C. Wireless broadband technologies

Hotspot: A hot spot (or *hotspot*) is a wireless LAN (local area network) node that provides Internet connection and virtual private network (VPN) access from a given location. For example, a business traveler with a laptop equipped for Wi-Fi can look up a local hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.

A mobile hotspot is an ad hoc wireless access point that is created by a dedicated hardware device or a smartphone feature that shares the phone's cellular data.

Pocket routers access cellular signals and convert 3G and 4G signals to Wi-Fi and vice versa, creating mobile Wi-Fi networks that can be shared by multiple users within about 10 meters of the device. Most wireless carriers offer mobile hotspot devices and the wireless data plans required to enable them.

Another option is using a **smartphone** to connect other devices. Many smartphones enable the creation of a mobile hotspot through tethering, accessing the phone's existing cellular data connection.

The Access Network Query Protocol (ANQP) is a query and response protocol that defines services offered by an access point (AP), typically at a Wi-Fi hot spot.

Content/Topic 2: Installation & Configuration of WiMAX

WiMAX: WiMAX stands for **W**orldwide **I**nteroperability for **M**icrowave **A**ccess**:** Type of wireless technology that provides wireless internet service over longer distances than standard Wi-Fi.

WiMAX is based on standard IEEE 802.16 technology and can provide broadband wireless access up to 30 miles (1mile=1.6km).

WiMAX uses fixed and mobile stations to provide users with access to high-speed voice, data, and Internet connectivity.

WiMAX can provide at-home or mobile Internet access across whole cities or countries.

Uses of WIMAX

- Providing portable mobile broadband connectivity across cities and countries through various devices.
- Providing a wireless alternative to cable and digital subscriber line (DSL) for "last mile" broadband access.

- Providing data, telecommunications (VoIP) and IPTV services (triple play).
- Providing Internet connectivity as part of a business continuity plan.
- Smart grids and metering.

WiMAX Advantages

- A single location can serve hundreds of users
- Single WiMax Base Station (BS) serves hundreds of users
- Much faster deployment of the new user as compared to wired networks
- It creates a volume opportunity for silicon suppliers
- The speed of 10 Mbps at 10 kilometers with a line of sight
- It is considered to be a cheaper alternative to broadband wired technologies viz. ADSL, cable modem etc
- It is standardized, and also have same frequency equipment should work together
- Higher bandwidth
- High coverage range
- High speed can be achieve
- Lower cost
- Communication range up to 100 miles
- Does not require telephone lines
- Provide mobility to a user with access to the internet
- Design with better quality services
- No SIM card requires
- Non-line of sight connection
- It works on an unlicensed frequency spectrum
- Cellular like performance is achieved with mobile WiMAX

WiMAX disadvantages:

- Big installation and operational cost
- Multiple frequencies are used
- A line of sight needed
- Poor bandwidth when serving lots of clients
- Higher latency
- Unreliable service

- Spectral limitation
- Big delay
- Big power consumption
- Interference with other wireless signals
- Hand over and roaming hard to achieve
- Very power intensive technology and also have to require strong electrical support
- Weather conditions like rain could cause interference
- WiMAX is very power consuming
- Multiple frequencies are used for WiMAX deployment
- If there are many users in one sector, then they will have lower speed

Steps for installing the Cisco BWX360 WiMAX Outdoor Modem

1. Choosing locations

First choose the location for the indoor unit:

- When choosing the location, note the specified temperature range of the indoor unit.
- The indoor unit can be operated either on a horizontal surface or mounted on a wall. Always make sure the connections cannot become loose once the system has been put into service and check that the LEDs are clearly visible.
- **Power supply:** Power is supplied to the Cisco BWX360 WiMAX Outdoor Modem via the indoor unit. Therefore, the location must be close to a suitable mains connection (cable length of the supplied power supply unit).
- **Wall duct:** To connect to the outdoor modem, the corresponding Ethernet cable must be fed through the wall to the outside of the building. It must be possible to make a suitable wall duct at or close to the indoor unit. Please note that the maximum permitted cable length is 50 m.
- **PC or network:** Establishing a connection between the indoor unit and a PC or network-switch should ideally be possible from the location via the Ethernet cable. If the PC is moved from its original place, the indoor unit should still be able to be reached simply by using standard cable lengths.
- There should not be any obstructions (walls, trees etc.) in front of the antenna. The best results will be obtained if the outdoor modem is in sight of the WiMAX base station. If necessary, you can also reflect the radio waves off neighboring buildings.
- The antenna mast must be structurally secure. Check how secure the various attachments are.

- The antenna mast must be within reach of the cable. Ideally, the Ethernet cable should be protected outside (from frost, sun, unauthorized and mechanical influences etc.).

2. Setting up the antenna mast.

Please observe all the safety provisions and other notes contained in the assembly instructions for the antenna mast. In particular, make sure the antenna mast has sufficient load capacity. If you are installing the mast on the roof, make sure the roof is fully sealed again afterwards. If necessary, you can attach the mast brackets to the mast when you install it.

3. Protecting the mast against lightning

The antenna must therefore be installed in areas that are protected against lightning. The corresponding separation distance must be complied with. Grounding and lightning protection work may only be carried out by electricians specifically qualified for such work.

The appropriate grounding clamps must be used to create an equipotential bonding between a cable shield and an equipotential bonding bar that complies with regulations

Make sure you ground the metal casing of the outdoor modem according to the instructions.

- Undo or remove the M5 grounding screw on the modem casing.
- Attach the cable lug at the end of the grounding cable and Make sure when you do this that the cable lug cannot come loose.
- Attach the cable lug to the casing with the M5 grounding screw.

4. Assembling the outdoor modem

You basically have three options for installing the outdoor modem:

- Vertically on a mast or
- Tilted up or down on a mast with an angled bracket. Choose the type of installation that allows the best alignment of modem to base station on your building.
- Directly attached to a wall

Vertical installation on a mast

1. Take the four bolts with the welded-on nuts and screw them into the housing with the shorter end of the bolts, so that the nuts are resting on the housing.

2. Attach the housing to the mast using the clamps and secure the clamps with the nuts.

5. Connecting the indoor unit

To connect the indoor unit to the outdoor modem you perform the following steps:

i. *Making a wall duct.* Note how close you are to the indoor unit.

ii. Provisionally laying the Ethernet cable. The cable must satisfy the requirements for cables used outdoors at the relevant installation location

iii. Checking connection options in the house. Fix the wall connection socket in place and connect the cable from outside to it. Or, Connect the cable from outside directly to the indoor unit. For indoor use, you need an RJ45 plug, Feed an Ethernet cable with an RJ45 plug from the indoor unit to a PC or router.

iv. Connecting an Ethernet cable to the outdoor modem.

- Slip the support sleeve over the unassembled cable to be screwed in later.
- Attach a Phoenix connector to the end of the Ethernet cable that is outside. Please read the instructions that come with the plug.
- Insert the RJ45 plug of the assembled cable into the Ethernet socket of the outdoor modem.
- Slide the sleeve over the connected RJ45 plug and screw this into the Ethernet socket. Make sure the connection is water-tight.
- Use cable clamps to attach the cable to the mast. Please note that the cable must be long enough to turn the antenna at a later stage.
- Lay and attach the cable from the antenna mast along a path on which its functionality is not affected by external influences.

6. Launching the user interface

- Open your Web browser.

- Enter the IP address of the Cisco BWX360 WiMAX Outdoor Modem in the browser's address field: http://192.168.2.1 3. Press Enter (Return).

Login

If a system password has been set up on the Cisco BWX360 WiMAX Outdoor Modem, the login screen will now open.

- Enter the system password supplied by your provider in the text box and click Ok. The start page of the user interface opens; in which you can change the language if necessary.

If no system password has been set up on your Cisco BWX360 WiMAX Outdoor Modem, a security warning will appear first. You should then assign a system password as soon as possible.

- Confirm the security warning with Ok. The user interface start-page opens

7. Connecting to the WiMAX network and the Internet

If there is a connection between the PC or laptop and the outdoor modem, the Internet connection must be configured and a radio connection must be established with the base station. You do this in the Basic Setup Wizard.

i. Click the Basic Setup Wizard tab.

ii. Click Next.

iii. If you need help for a particular page, click the question mark button.

iv. Enter the access data and click Next.

v. Turn your Cisco BWX360 WiMAX Outdoor Modem towards the base station.

vi. Click Next.

The frequency scan starts automatically. A progress bar indicates how far the frequency scan has already progressed. In addition, you will see in the Remaining time area roughly how much time is still needed for the complete scan.

8. Precisely aligning the antenna

i. Turn the antenna step by step and have the assistant watch the connection status on the PC.

ii. When a connection to a WiMAX base station has been established, the assistant clicks on Next to make fine adjustments to the antenna.

You will also see the signal quality shown as a percentage as well as an assessment of the connection quality:

Excellent	The wireless connection is at the highest level.
Very good	The wireless connection is very good. You can attempt to improve the connection still further by turning the antenna slightly; however, this is not necessary
Good	The wireless connection is already good. Turn the antenna slightly to further improve the connection.

Sufficient	The wireless connection has been established. Turn the antenna a little at a time to improve the connection.
No connection	If you have turned or moved the antenna too far the wireless connection to the WiMAX base station will break up. Return the antenna to the position it was in when the connection was successfully established. The wireless connection to the WiMAX base station will be restored immediately.

iii. Turn the antenna a little at a time and have the assistant observe the signal strength display. Use this to move the antenna to the position with the best signal strength.

iv. When the antenna is precisely aligned, Click on **End**

9. Finishing off the assembly

i. Tighten the screw fixings. Please be aware of local laws. Installation should be performed by a qualified person.

ii. Attach the Ethernet cable with cable clamps and cable ties. Make sure the cable is protected against the effects of pressure.

iii. Brief the user on what to do if they have any problems or if they need to upgrade the system etc.

Content/Topic 3: Installation & Configuration of HSPA

HSPA: is an amalgamation of two mobile protocols; High Speed Downlink Packet Access (**HSDPA**) and High Speed Uplink Packet Access (**HSUPA**), that extends and improves the performance of existing 3G mobile telecommunication networks using the WCDMA protocols.

WCDMA (Wideband Code Division Multiple Access) is a third-generation (3G) standard that employs the direct-sequence code division multiple access (DS-CDMA) channel access method and the frequency-division duplexing (FDD) method to provide high-speed and high-capacity service. WCDMA is the most commonly used variant of the Universal Mobile Telecommunications System (UMTS).

WCDMA features two modes:

- **Frequency Division Duplex (FDD)**: Separates users by employing both codes as well as frequencies. One frequency is used for the uplink, while another is used for the downlink.
- **Time Division Duplex (TDD):** Separates users by employing codes, frequencies and time, wherein the same frequency is used for both uplink and downlink.

You must have an account with a GSM service provider to use the modem. To use the modem's 3G capability, your account must be with a service provider that offers HSDPA/HSUPA or UMTS service. (The modem is backwards compatible with 2G service.) When you obtain your account, you are given a Subscriber Identity Module (SIM) card containing account information. Before you use the modem, you must insert the SIM card into it.

Your ability to obtain service depends on these factors:

- **Network coverage**—You must be within the network coverage area.
- **Service provider**— If you are within the coverage area of a network that is not operated by your own service provider, you can obtain service only if there is a roaming agreement between your service provider and the network operator.
- **Account provisions**—Your account may restrict your usage to certain networks or limit the amount of time you can use the network.
- **Frequency band**—You cannot connect to networks operating in bands not supported by your modem, regardless of roaming agreements or account provisions.

Steps for installing and configuring HSPA

1. Check the system requirements.

2. Insert the SIM card into the modem.

- If your SIM card is attached to a larger card, detach the SIM card and remove any fragments stuck to it.
- Remove the end cap. The SIM card slot is the uppermost slot above the USB connector.
- Insert the SIM card into the slot.

3. Insert the modem into your computer: Gently insert the modem into the USB slot.

4. Install the software

If the installation process does not start automatically:

- Double-click My Computer (Windows XP) or Computer (Windows Vista) on your desktop.
- Click the TRU-Install drive.
- Under the TRU-Install drive, go to the Win folder and double-click the Setup.exe file.
- Follow the on-screen instructions for installing the software.

5. Connect to the network

To use your account (and connect to your service provider's network), you need to have at least one profile set up on your modem. Depending on how your modem is configured, the profile may already be set up or you may need to create one.

Once the software is successfully installed and the profile is set up, the modem is ready to use.

6. LED operation

The USB modem has two LEDs that show the current status of the modem.

LED	State	Indicates
Power	**Off**	Indicates one of the following states: • The modem is not inserted in the computer. • The computer is off or in "suspend and resume" mode. • The modem radio has been turned off using Watcher or another connection client.
	Solid Blue	The power is on, the modem is working normally
	Blinking Blue	The firmware is being updated. Do not remove the modem from the computer.
	Blinking Amber	The modem is searching for service (initializing)
	Solid Amber	Modem error—either the modem is having a problem initializing (searching for service) or is offline because of a failure. Contact your service provider.
Data	**Off**	The modem is unable to detect 2G or 3G service
	Blinking Amber	The modem has detected a 2G network (EDGE, GPRS, GSM) and is ready to connect.
	Solid Amber	The modem is connected to a 2G network and is able to send and receive data.
	Blinking Blue	The modem has detected a 3G network (UMTS, HSPA) and is ready to connect.
	Solid Blue	The modem is connected to a 3G network and can send and receive data.

Content/Topic 4: Identification of basics on Mobile Communication

a. **Types of wireless network**

Wireless PAN

Wireless personal area networks (WPANs) connect devices within a relatively small area that is generally within a person's reach. For example, both Bluetooth radio and invisible infrared light provides a WPAN for interconnecting a headset to a laptop.

Wireless LAN

A wireless local area network (WLAN) links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for internet access.

To connect to Wi-Fi, sometimes are used devices like a router or connecting Hotspot using mobile smartphones.

Wireless ad hoc network

A wireless ad hoc network, also known as a wireless mesh network or mobile ad hoc network (MANET), is a wireless network made up of radio nodes organized in a mesh topology. Each node forwards messages on behalf of the other nodes and each node performs routing.

Ad hoc networks can "self-heal", automatically re-routing around a node that has lost power. Various network layer protocols are needed to realize ad hoc mobile networks, such as Distance Sequenced Distance Vector routing, Associativity-Based Routing, Ad hoc on-demand Distance Vector routing, and Dynamic source routing.

Wireless MAN

Wireless metropolitan area networks are a type of wireless network that connects several wireless LANs. **WiMAX** is a type of Wireless MAN and is described by the IEEE 802.16 standard

Wireless WAN

Wireless wide area networks are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public Internet access system.

Cellular network

A cellular network or mobile network is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station.

This enables a large number of portable transceivers (e.g., mobile phones, …) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

Global area network

A global area network (GAN) is a network used for supporting mobile across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next.

Space network

Space networks are networks used for communication between spacecraft, usually in the vicinity of the Earth.

b. Mobile network fundamentals

A **mobile network** also called **cellular network**; it is a communication network where the last link is wireless. The network is distributed over land areas called "**cells**", each served by at least one fixed-location transceiver, but more normally, three cell sites or base transceiver stations. These base stations provide the cell with the network coverage which can be used for transmission of voice, data, and other types of content. A cell typically uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed service quality within each cell.

When joined together, these cells provide radio coverage over a wide geographic area. This enables numerous portable transceivers (e.g., mobile phones, tablets and laptops equipped with mobile broadband modems, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

Features Mobile networks.

- More capacity than a single large transmitter, since the same frequency can be used for multiple links as long as they are in different cells
- Mobile devices use less power than with a single transmitter or satellite since the cell towers are closer
- Larger coverage area than a single terrestrial transmitter, since additional cell towers can be added indefinitely and are not limited by the horizon

c. Roaming

It refers to the mobile phone being used outside the range of its home network and connects to another available cell network.

Types roaming

- **Regional or internal roaming:** This type refers to the ability of moving from one region to another region inside national coverage of the mobile operator.
- **National roaming:** This type refers to the ability to move from one mobile operator to another in the same country.
- **International roaming:** This type of roaming refers to the ability to move to a foreign service provider's network.
- **Inter-standards roaming:** This type refers to roaming between two standards.
- **Trombone roaming:** Roaming calls within a local tariff area, when at least one of the phones belong outside that area.

d. GSM, GPRS, CDMA, UMTS.

1. **GSM: Global System for Mobile communications** is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices such as mobile phones and tablets.

   2G networks developed as a replacement for first generation (1G) analog cellular networks, and the GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony. This expanded over time to include data communications, first by circuit-switched transport, then by packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution, or EGPRS). Subsequently, the 3GPP developed third-generation (3G) UMTS standards, followed by fourth-generation (4G) LTE Advanced standards, which do not form part of the ETSI GSM standard.

GSM offers three basic types of services:

- Telephony services or teleservices
- Data services or bearer services
- Supplementary services

a) Telephony services or teleservices

- Voice Calls
- Videotext and Facsmile
- Short Text Messages

b) Data services or bearer services

To receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer.

c) Supplementary services

Supplementary services are additional services that are provided in addition to teleservices and bearer services.

- **Conferencing**: It allows a mobile subscriber to establish a multiparty conversation, i.e., a simultaneous conversation between three or more subscribers to setup a conference call. This service is only applicable to normal telephony.
- **Call Waiting**: This service notifies a mobile subscriber of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call.
- **Call Hold**: This service allows a subscriber to put an incoming call on hold and resume after a while. The call hold service is applicable to normal telephony.
- **Call Forwarding**: Call Forwarding is used to divert calls from the original recipient to another number. It is normally set up by the subscriber himself. It can be used by the subscriber to divert calls from the Mobile Station when the subscriber is not available, and so to ensure that calls are not lost.
- **Call Barring**: Call Barring is useful to restrict certain types of outgoing calls such as ISD or stop incoming calls from undesired numbers. Call barring is a flexible service that enables the subscriber to conditionally bar calls.
- **Number Identification**: There are following supplementary services related to number identification:
    - **Calling Line Identification Presentation**: This service displays the telephone number of the calling party on your screen.
    - **Calling Line Identification Restriction**: A person not wishing their number to be presented to others subscribes to this service.

- **Connected Line Identification Presentation**: This service is provided to give the calling party the telephone number of the person to whom they are connected. This service is useful in situations such as forwarding's where the number connected is not the number dialed.
- **Connected Line Identification Restriction**: There are times when the person called does not wish to have their number presented and so they would subscribe to this person. Normally, this overrides the presentation service.
- **Malicious Call Identification**: The malicious call identification service was provided to combat the spread of obscene or annoying calls. The victim should subscribe to this service, and then they could cause known malicious calls to be identified in the GSM network, using a simple command.

- **Advice of Charge (AoC)**: This service was designed to give the subscriber an indication of the cost of the services as they are used. Furthermore, those service providers who wish to offer rental services to subscribers without their own SIM can also utilize this service in a slightly different form. AoC for data calls is provided on the basis of time measurements.
- **Closed User Groups (CUGs)**: This service is meant for groups of subscribers who wish to call only each other and no one else.
- **Unstructured supplementary services data (USSD)**: This allows operator-defined individual services.

2. **GPRS: General Packet Radio Service** (**GPRS**) is a packet oriented mobile data standard on the 2G and 3G cellular communication network's global system for mobile communications (GSM).
   GPRS extends the GSM Packet circuit switched data capabilities and makes the following services possible:
   - SMS messaging and broadcasting
   - "Always on" internet access
   - Multimedia messaging service (MMS)
   - Push-to-talk over cellular (PoC)
   - Instant messaging and presence—wireless village
   - Internet applications for smart devices through wireless application protocol (WAP)
   - Point-to-point (P2P) service: inter-networking with the Internet (IP)
   - Point-to-multipoint (P2M) service. point-to-multipoint multicast and point-to-multipoint group calls
3. **CDMA: Code-Division Multiple Access** CDMA is an example of multiple access, where several transmitters can send information simultaneously over a single communication channel.

This allows several users to share a band of frequencies. To permit this without undue interference between the users.

4. **UMTS:** The **Universal Mobile Telecommunications System** (**UMTS**) is a third generation mobile cellular system for networks based on the GSM standard.

   UMTS uses wideband code division multiple access (W-CDMA) radio access technology to offer greater and bandwidth to mobile network operators.

   Compared to GSM and other existing mobile networks, UMTS provides a new and important feature, namely it allows negotiation of the properties of a radio bearer.

   UMTS applications and services can be divided into four different classes.

   UMTS traffic classes

   - **Conversational class:** Preserve time relation (variation) between information entities of the stream. Ex: Voice, video telephony, video games.
   - **Streaming class:** Preserve time relation (variation) between information entities of the stream. Ex: Streaming multimedia
   - **Interactive class:** Request response pattern. Ex: Web browsing, network games
   - **Background class:** Destination is not expecting the data within a certain time. Ex: Background download of emails

Content/Topic 5: Description of Very Small Aperture Terminal (V-SAT)

VSAT is a two-way ground station that transmits and receives data from satellites. A VSAT is less than three meters tall and is capable of both narrow and broadband data to satellites in orbit in real-time. The data can then have redirected to other remote terminals or hubs around the planet.

- **V-SAT signal**

A VSAT consists of two parts, a **transceiver** that is placed outdoors in direct line of sight to the satellite and a device that is placed indoors to interface the transceiver with the user's communications device, such as a PC. The transceiver receives or sends a signal to a satellite transponder in the sky. The satellite sends and receives signals from a ground station computer that acts as a hub for the system.

- **Direction of dish caves**

A **satellite dish** is a dish-shaped type of parabolic antenna designed to receive or transmit information by radio waves to or from a communication satellite.

The parabolic shape of a dish reflects the signal to the dish's **focal point**. Mounted on brackets at the dish's focal point is a device called a **feedhorn**. This feedhorn is essentially the front-end of a **waveguide** that gathers the signals at or near the focal point and 'conducts' them to a Low-Noise Block downconverter or LNB.

The LNB converts the signals from electromagnetic or radio waves to electrical signals and shifts the signals from the downlinked C-band to the L-band range. Direct broadcast satellite dishes use an LNBF, which integrates the feedhorn with the LNB.

In a single receiver, residential installation there is a single **coaxial cable** running from the receiver **set-top box** in the building to the LNB (Low noise block) on the dish. The DC electric power for the LNB is provided through the same coaxial cable conductors that carry the signal to the receiver.

In addition, control signals are also transmitted from the receiver to the LNB through the cable. The receiver uses different power supply voltages (13 / 18 V) to select antenna **polarization**, and **pilot tones** (22 kHz) to instruct the LNB to select one of the two frequency bands. In larger installations, each band and polarization is given its own cable.

Content/Topic 6: Description of the types of network

A. Different Types of Wireless

a. **Bluetooth**

- Bluetooth is a wireless technology standard for exchanging data between fixed and mobile devices over short distances.
- Bluetooth is a short-range wireless communication technology that allows devices such as mobile phones, computers, and peripherals to transmit data or voice wirelessly over a short distance.
- The purpose of Bluetooth is to replace the cables that normally connect devices, while still keeping the communications between them secure.
- Bluetooth technology developed in 1994.
- It uses the same 2.4GHz frequency. It creates a 10-meter (33-foot) radius wireless network
- Also called a personal area network (PAN) or piconet.
- Bluetooth uses less power and costs less to implement than Wi-Fi.
- The process of connecting two Bluetooth devices is called "pairing."
- Generally, devices broadcast their presences to one another, and the user selects the Bluetooth device they want to connect to when its name or ID appears on their device.

- This pairing process can vary depending on the devices involved. For example, connecting a Bluetooth device to your iPad can involve different steps from those to pair a Bluetooth device to your car.

b. **Wi-Fi**

Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A common misconception is that the term Wi-Fi is short for "*wireless fidelity*," however, this is not the case.

B. Network:

- **Personal Area Network**

A **personal area network**, or **PAN**, is a computer network organized around an individual person within a single building. This could be inside a small office or residence. A typical PAN would include one or more computers, telephones, peripheral devices, video game consoles and other personal entertainment devices.

If multiple individuals use the same network within a residence, the network is sometimes referred to as a home area network, or HAN. In a very typical setup, a residence will have a single wired Internet connection connected to a modem. This modem then provides both wired and wireless connections for multiple devices. The network is typically managed from a single computer but can be accessed from any device.

This type of network provides great flexibility. For example, it allows you to:

- Send a document to the printer in the office upstairs while you are sitting on the couch with your laptop.
- Upload a photo from your cell phone to your desktop computer.
- Watch movies from an online streaming service to your TV.

- **Local Area Network**

A **local area network**, or **LAN**, consists of a computer network at a single site, typically an individual office building. A LAN is very useful for sharing resources, such as data storage and printers. LANs can be built with relatively inexpensive hardware, such as hubs, network adapters and Ethernet cables.

The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. High speed and relatively low cost are the defining characteristics of LANs.

LANs are typically used for single sites where people need to share resources among themselves but not with the rest of the outside world. Think of an office building where everybody should be able to access files on a

central server or be able to print a document to one or more central printers. Those tasks should be easy for everybody working in the same office, but you would not want somebody just walking outside to be able to send a document to the printer from their cell phone! If a local area network, or LAN, is entirely wireless, it is referred to as a wireless local area network, or WLAN.

- **Metropolitan Area Network**

A **metropolitan area network**, or **MAN**, consists of a computer network across an entire city, college campus or small region. A MAN is larger than a LAN, which is typically limited to a single building or site. Depending on the configuration, this type of network can cover an area from several miles to tens of miles. A MAN is often used to connect several LANs together to form a bigger network. When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN.

- **Wide Area Network**

A **wide area network**, or **WAN**, occupies a very large area, such as an entire country or the entire world. A WAN can contain multiple smaller networks, such as LANs or MANs. The Internet is the best-known example of a public WAN.

LO 2.3 – **Ensure connections are secured against intrusion or data access by unauthorized persons, are safe for users, and are protected from the environment.**

Content/Topic 1: Securing Network Connection

A. Authentication, Authorization and Accounting (AAA) and IP security

Authentication, authorization and accounting (AAA) is a system for tracking user activities on an IP-based network and controlling their access to network resources. AAA is often being implemented as a dedicated server.

Security layer

Describes the practice of combining multiple mitigating security controls to protect resources and data.

Transport layer security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet. It enables privacy, integrity and protection for the data that is transmitted between different nodes on the Internet.

B. Security protocols

Security protocol is a sequence of operations that ensure protection of data. Used with a communications protocol, it provides secure delivery of data between two parties.

B.1. Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN.

B.2. Lightweight extensible authentication protocol (LEAP)

The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows clients to re-authenticate frequently; upon each successful authentication, the clients acquire a new WEP key (with the hope that the WEP keys do not live long enough to be cracked).

B.3. Privacy key management (PKM)

A private key scheme used with EAP and TLS for providing E2E security schemes for wireless technologies.

B.4. Secure sockets layer (SSL)

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

SSL provides a secure channel between two machines or devices operating over the internet or an internal network.

One common example is when SSL used to secure communication between a web browser and a web server. This turns a website's address from HTTP to HTTPS, the ‘S’ standing for ‘secure’.

SSL supports the following information security principles:

- **Encryption**: protect data transmissions (e.g. browser to server, server to server, application to server, etc.)

- **Authentication**: ensure the server you're connected to is actually the correct server.
- **Data integrity**: ensure that the data that is requested or submitted is what is actually delivered.

B.5. Tokens

Token is a representation of something in its particular ecosystem.

A security token is a portable device that authenticates a person's identity electronically by storing some sort of personal information.

The owner plugs the security token into a system to grant access to a network service. Security Token Services (STS) issue security tokens that authenticate the person's identity.

Security tokens come in many different forms:

- Including hardware tokens that contain chips.
- USB tokens that plug into USB ports.
- Wireless Bluetooth tokens or programmable electronic key fobs, which activate devices remotely (for example, to gain access to a car or apartment building).

KEY TAKEAWAYS

- Security tokens authenticate identities electronically by storing personal information.
- They are issued by Security Token Services (STS), which authenticate the person's identity.
- They may be used in place of or in addition to a password to prove the owner's identity.
- Security tokens are not always being secure—they may be lost, stolen, or hacked.

B.6. Wi-Fi protected access (WPA)

WPA is a security protocol designed to create secure wireless (Wi-Fi) networks. It is similar to the WEP protocol, but offers improvements in the way it handles security keys and the way users are authorized.

For an encrypted data transfer to work, both systems on the beginning and end of a data transfer must use the same encryption/decryption key.

While WEP provides each authorized system with the same key, WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that the systems use.

This prevents intruders from creating their own encryption key to match the one used by the secure network.

WPA also implements something called the Extensible Authentication Protocol (EAP) for authorizing users.

Instead of authorizing computers based solely on their MAC address, WPA can use several other methods to verify each computer's identity. This makes it more difficult for unauthorized systems to gain access to the wireless network.

Wi-Fi Protected Access (**WPA**), **Wi-Fi Protected Access II** (**WPA2**), and **Wi-Fi Protected Access 3** (**WPA3**) are three security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

LO 2.4 – **Measure and assess signal strength within and outside building**

Content/Topic 1: Use of Frequency and Spectrum analyzer to measure and assess signal strength.

Knowing the inside and outside functions of your wireless is important to have the wireless working at its best.

However, if you find that the signal does not fluctuate when you are inside or outside of the building it may be that you are too far from a tower/network in order to get a signal.

- ✓ **Frequency and Spectrum analyzer manipulation**

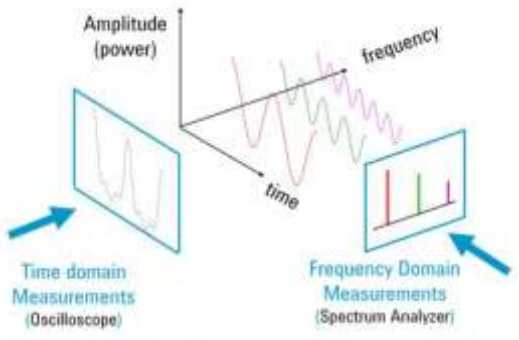
A spectrum **analyzer** is a device that displays signal amplitude (strength) as it varies by signal frequency.

A **spectrum analyzer** measures the amplitude of an input signal versus **frequency** within the full **frequency** range of the instrument.

The frequency appears on the horizontal axis, and the amplitude is displayed on the vertical axis. To the casual observer, a spectrum analyzer looks like an oscilloscope, and in fact, some devices can function either as oscilloscopes or spectrum analyzers.

Spectrum analyzers are used to examine the frequency spectrum of radio frequency (RF) and audio signals.

To fully **understand the performance of your device/system, you will also want to analyze the signal(s) in the frequency-domain.** This is a graphical representation of the signal's amplitude as a function of frequency The spectrum analyzer is to the frequency domain as the oscilloscope is to the time domain.



The figure shows a signal in both the time and the frequency domains. In the time domain, all frequency components of the signal are summed together and displayed. In

the frequency domain, complex signals (that is, signals composed of more than one frequency) are separated into their frequency components, and the level at each frequency is displayed.

If you look at the signal on a spectrum analyzer, you may find that your signal is actually made up of several frequencies.

Some systems are inherently frequency domain oriented. For example, many telecommunications systems use what is called Frequency Division Multiple Access (FDMA) or Frequency Division Multiplexing (FDM). In these systems, different users are assigned different frequencies for transmitting and receiving, such as with a cellular phone.

Radio stations also use FDM, with each station in a given geographical area occupying a particular frequency band. These types of systems must be analyzed in the frequency domain in order to make sure that no one is interfering with users / radio stations on neighboring frequencies.

Measuring with a frequency domain analyzer can greatly reduce the amount of noise present in the measurement because of its ability to narrow the measurement bandwidth.

From the view of the spectrum, the following measurements can easily be made:

- **Frequency**.
- **Power**.
- **Harmonic content**.
- **Modulation**.
- **Spurs**, and **noise**.

Given the capability to measure these quantities, we can determine total harmonic distortion, occupied bandwidth, signal stability, output power, intermodulation distortion, power bandwidth, carrier-to-noise ratio, and a host of other measurements, using just a spectrum analyzer.

a. Signal frequency

Signal frequency is the number of occurrences of a repeating signal per unit time. Calculating the **frequency** of a repeating signal is accomplished by counting the number of times that signal occurs within a specific time period, then dividing the count by the length of the time period.

High frequency signal (HF) is the International Telecommunication Union (ITU) designation for the range of **radio frequency** electromagnetic waves (**radio** waves) between 3 and 30 megahertz (MHz). It is also known

as the decameter band or decameter wave as its wavelengths range from one to ten decameters (ten to one hundred meters).

Wavelength the distance between successive crests of a wave, especially points in a sound wave or electromagnetic wave.

Wavelength is the distance between identical points in the adjacent cycles of a waveform signal propagated in space or along a wire.

Wavelength is inversely related to frequency, which refers to the number of wave cycles per second. The higher the frequency of the signal, the shorter the **wavelength**.

Types of Signal Frequencies and wavelength in Radio Frequency Spectrum

1	**ELF**	**EXTREMELY LOW FREQUENCY** **Frequency:** 3 KHz to 30 KHz, **Wavelength**: 100 km to 10 km
3	**LF**	**LOW FREQUENCY** **Frequency:** 30 KHz to 300 KHz, **Wavelength**: 10 km to 1 km
4	**MF**	**MEDIUM FREQUENCY** **Frequency**: 300 KHz to 30 MHz, **Wavelength**: 100 km to 10 km
5	**HF**	**HIGH FREQUENCY** **Frequency**: 3 MHz to 30 MHz, **Wavelength**: 100 m to 10 m
6	**VHF**	**VERY HIGH FREQUENCY** **Frequency**: 30 MHz to 300 MHz, **Wavelength**: 10 m to 1 m
7	**UHF**	**ULTRA HIGH FREQUENCY** **Frequency**: 300 MHz to 3 GHz, **Wavelength**: 1 m to 100 mm
8	**SHF**	**SUPER HIGH FREQUENCY** **Frequency**: 3 GHz to 30 GHz, **Wavelength**: 100 mm to 10 mm
9	**EHF**	**EXTREMELY HIGH FREQUENCY** **Frequency**: 30 GHz to 300 GHz, **Wavelength**: 10 mm to 1 mm

b. Power

The relationship between power and frequency is inversely proportional to each other. In case of grid connected alternator if the output power of the alternator increases according to the load in the terminal of the alternator

then the frequency of the alternator decreases as well as speed of the alternator slightly decreases for a certain amount of time.

c. Harmonic content

Harmonic is a component frequency of the signal that is an integer multiple of the fundamental frequency. The harmonic current represents energy that cannot be used by any devices on the network.

Harmonics is the generalized term used to describe the distortion of a sinusoidal waveform by waveforms of different frequencies.

Harmonic content: It is a measure of the effective value of the harmonic components of a distorted waveform, which is defined as the Real Mean Square (RMS) of the harmonics expressed in percentage of the fundamental (e.g., current) component. A commonly cited value of 5% is often used as a dividing line between a high and low distortion level.

d. Modulation spurs and noise

Spurs are typically few and low amplitude, but generally undesirable as they contribute to a clock's total jitter. Spurs can be used for evaluation and characterization of timing devices.

We can use lab sources configured for low-level modulation to apply spurious frequency components, directly or indirectly, as input stimuli to a clock device or system. The resulting output clock spurs are then measured with a spectrum analyzer or phase noise analyzer.

Learning Unit 3 – Finalize build process

LO 3.1 – Document the work done

Content/Topic 1: Document the work done

The **document:** is a piece of written, printed, or electronic matter that provides information or evidence or that serves as an official record.

What are types of documents?

- **Academia:** thesis, paper, and journal.
- **Business:** invoice, proposal, contract ….

Measurement study

- **Setup**
  - Can't connect to wireless.
  - Wireless adapter not fixed.
  - Wi-Fi network not showing up.
  - PC not connecting to Wi-Fi.
  - wireless adapter not enabled.
  - Cables from switch to APs broken (problem of cabling).
  - A conflict of IP addresses.
  - The DNS is down.
- **Results**
  - For the DNS you have to use the Nslookup to see your DNS settings.
  - Check the internet protocol properties of the IP version 4.
  - Ping tool to check for the connectivity.
  - Send files or data or packets that can’t exhaust your network performance.
  - Select your Wireless network and click Forget. After you've done that, connect to the same wireless network again.
  - Through Device Manager, locate your wireless adapter and double click it to open its properties. Go to Driver tab and look for Enable button. If you don't see the Enable button, it means that your device is enabled and working.
  - Reset your AP then configure DHCP Protocol to avoid the conflict of IP Address and reconnect your PCs

- Repair/Replace the cable from switch to Aps
- Reboot the modem and router.

Content/Topic 2: Scanning Wi-Fi overview

Wi-Fi Overview

Wi-Fi is the name of a popular wireless networking technology that provides users with wireless high-speed Internet and network connections.

- **Challenge**
  - Rogue Access Points/Ad-Hoc Networks
  - Denial of Service
  - Configuration Problems (Mis-Configurations/Incomplete Configurations)
  - Passive capturing
- **System task**
  - Install wireless intrusion **prevention** systems to monitor the radio spectrum for unauthorized **access points**.
  - Presence of a large number of wireless **access points** can be sensed in airspace of a typical enterprise facility.
  - Buy more bandwidth. ...
  - Build redundancy into your infrastructure. ...
  - Configure your network hardware against Distributed Denial of Services (DDoS) attacks.
  - Deploy anti-DDoS hardware and software modules.
  - Deploy a DDoS protection appliance.
  - Protect your DNS servers.
  - Proper configuration.
  - Implement security mechanism.

Content/Topic 3: Ensuring location privacy

The concept of *location privacy* can be defined as the right of individuals to decide how, when, and for which purposes their location information could be released to other parties. The lack of location privacy protection could be exploited by adversaries to perform various attacks.

- **Threat model**
  - ***Unsolicited advertising*****,** when the location of a user could be exploited, without her consent, to provide advertisements of products and services available nearby the user position.
  - ***Physical attacks or harassment*****,** when the location of a user could allow criminals to carry out physical assaults on specific individuals.
  - ***User profiling and tracking*****,** when the location of a user could be used to infer other sensitive information, such as state of health, personal habits, or professional duties, by correlating visited places or paths.
  - ***Political, religious, sexual persecution and discrimination*****,** when the location of a user could be used to reduce the freedom of individuals, and mobile technologies are used to identify and persecute opponents.
  - ***Denial of service*****,** when the location of a user could motivate an access denial to services under some circumstances.

- **Identification of location privacy**
  - ***Identity privacy*** protects the identity of the users associated with or inferable from location information. To this purpose, protection techniques aim at minimizing the disclosure of data that can let attackers infer a user identity. Identity privacy is suitable in application contexts that do not require the identification of the users for providing a service.
  - ***Position privacy*** protects the position of individual users by perturbing corresponding information and decreasing the accuracy of location information. Position privacy is suitable for environments where users' identities are required for a successful service provisioning. A technique that most solutions exploit, either explicitly or implicitly, consists of reducing the accuracy by scaling a location to a coarser granularity (from meters to hundreds of meters, from a city block to the whole town, and so on).
  - ***Path privacy*** protects the privacy of information associated with users' movements, such as the path followed while travelling or walking in an urban area. Several location-based services (personal navigation systems) could be exploited to subvert path privacy or to illicitly track users.
- **Geographical position**

An access point sends geographical positioning information from the access point to mobile terminals and to a mobile terminal which receives this information and estimates the position thereof based on said information.

Geographical-locating architecture for Wi-Fi 802.11 mobile terminals on ADSL access points generally includes geographical positioning information, i.e., the geographical coordinates of the access point during the registration phase thereof.

The access point includes this geographical information in the information posted so that the mobile terminals can be connected to same. The mobile terminals can thus know the geographical location where they are located with an approximation that will depend directly on the number of access points that the mobile terminal can detect.

- **Channel condition**

  Wireless router and access point manufacturers use channels 1, 6 or 11 as the default channel, you need to analyze your wireless environment to choose the best channel for your access point.

  A Wi-Fi **channel** is the medium through which our wireless networks can send and receive data. For **routers** made in the U.S., the 2.4 GHz band has 11 **channels** and the 5 GHz band has 45 **channels**.

Content/Topic 4: Evaluation of network performance

- **Devices performance**

  When purchasing a new WLAN access point for an enterprise or public facility, make sure your access point is able to:

  - **Provide flawless access and good signal strength.**
  - **Scale to support the required capacity** of users and application traffic.
  - **Load-balance usage volumes** between access points.
  - **Adapt to changes in your physical environments.**
  - **Provide the appropriate level of security** for your organization.
  - **Provide good quality of service to new and old devices.**
  - **Enable visualization and monitoring.**
  - **Provide analytics** about network usage and application bandwidth consumption
  - **Define policies** promoting important traffic and demoting or blocking less important or unwanted traffic.

- **Support cloud-based control** of all access points in your organization, even across multiple physical locations.

- **Testing device performance**
  - **Measures radio transmitter and receiver quality** under a variety of ideal and real-world test conditions.
  - **Exercises the access point's processor and packet buffers** by running full line rate throughput tests to see if the access point can receive, process, and transmit large amounts of data.
  - **Tests the client association manager** by connecting hundreds of client devices to the access point and making sure they can connect, disconnect, send and receive traffic.
  - **Tests the TCP/IP stack** and measures the access point's ability to handle web traffic.
  - **Tests quality of service** on the access point by generating different types of traffic with different quality of service settings. This lets you check the level of performance for each device and each type of traffic with your access points.
  - **Fully tests the policy engine** on the access point by creating many different policies (blocking or preferring different types of traffic) and then sending relevant traffic. For example, with IxVeriWave you can automatically set a policy to block P2P traffic, then simulate P2P traffic and make sure it does not get forwarded.
  - **Tests the client session manager** on the access point to check roaming of clients between WLAN cells
  - **Tests the radio resource management** capability of the access point: IxVeriWave generates different types of interference and checks the access point's ability to operate uninterrupted
  - **Tests the authentication and encryption** mechanisms supported on the access point, and ensures traffic is encrypted properly in all use cases
  - **Tests standards compliance** for dynamic frequency selection (DFS) and Federal Communications Commission (FCC) radar

LO 3.2 – **Provide the report of work done**

Content/Topic 1: Reporting the work done

A report is a document that presents information in an organized format for a specific audience and purpose. Although summaries of reports may be delivered orally, complete reports are almost always in the form of written documents.

According to the Business Dictionary, a report is a document containing information organized in a narrative, graphic, or tabular form that is prepared on periodic, regular, or as required basis.

Types of reports include memos, minutes, lab reports, book reports, progress reports, justification reports, compliance reports, annual reports, and policies and procedures.

Here are the main sections of the standard report writing format:

- **Title Section**: The title of report is necessary to orient the reader. This includes the name of the author(s) and the date of report preparation.
- **Summary**: There needs to be a summary of the major points, conclusions, and recommendations. It needs to be short as it is a general overview of the report. Some people will read the summary and only skim the report, so make sure you include all the relevant information. It would be best to write this last so you will include everything, even the points that might be added at the last minute.
- **Introduction:** The first page of the report needs to have an introduction. You will explain the problem and show the reader why the report is being made. You need to give a definition of terms if you did not include these in the title section, and explain how the details of the report are arranged.
- **Experimental details:** This is the part that you need to state every detail of the experiment, starting from the equipment that you used to the procedure for the test.
- **Results:** This is where you are expected to explain the results that you obtained. You should give clear explanation so that the reader cannot ask themselves any question on your results.
- **Body:** This is the main section of the report. There needs to be several sections, with each having a subtitle. Information is usually arranged in order of importance with the most important information coming first.
- **Conclusion**: This is where everything comes together. Keep this section free of jargon as most people will read the Summary and Conclusion.
- **Recommendations**: This is what needs to be done. In plain English, explain your recommendations, putting them in order of priority.
- **Appendices**: This includes information that the experts in the field will read. It has all the technical details that support your conclusions.

Remember that the information needs to be organized logically with the most important information coming first.

LO 3.3 – **File the documentation**

Content/Topic 1: Filing the documentation

The organized collection of records that describe the structure, purpose, operation, maintenance, and data requirements for a computer program, operating system, or hardware device.

- Instructions for turning the system on and getting the programs initiated (loaded).
- Instructions for obtaining source documents for data entry.
- Instructions for entering data at the terminal, which includes a picture of each screen layout the user will encounter.
- A description of error messages that can occur and the alternative methods for handling them.
- A description of the defaults taken in the programs and the instructions for changing them.
- Instructions for distributing the computer's output, which includes sample pages for each type of report.

It is necessary for storing documents on a storage media, especially for use by computers because of the following benefits:

- Reduced Storage Space
- Enhanced Security
- Improved Regulatory Compliance
- Easier Retrieval
- Better Collaboration
- Better Backup and Disaster Recovery

REFERENCES

- Margaret Rouse (2019), Bandwidth, URL: *https://searchnetworking.techtarget.com/definition/bandwidth* Accessed on 30th May 2020.
- Bandwidth. (n.d). URL: *https://www.networxsecurity.de/?page_id=3770* Accessed on 30th May 2020.
- Nmap. (n.d). URL: *https://nmap.org/* Accessed on 30th May 2020.
- David Zomaya (April 27, 2020), 12 Best Network Diagnostics & Troubleshooting Tools for Network Administrators, URL: *https://www.comparitech.com/net-admin/network-troubleshooting-tools/* Accessed on 1st June 2020.
- Manage your suppliers. (n.d). URL: https://www.infoentrepreneurs.org/en/guides/manage-your-suppliers/ Accessed on 1st June 2020.
- Types of Network Topology. (n.d). URL: *https://www.studytonight.com/computer-networks/network-topology-types* Accessed on 1st June 2020.
- Testing a Wireless LAN. (n.d). URL: *https://cdn.ttgtmedia.com/searchNetworking/downloads/17_1587058898_ch17.pdf* Accessed on 1st June 2020.
- Troubleshooting WLAN Connectivity. (n.d). URL: *http://www.idc-online.com/technical_references/pdfs/data_communications/Troubleshooting_WLAN_Connectivity.pdf* on 2nd June 2020.
- WLAN Access Point: 10 Crucial Capabilities and How to Test for Them. (n.d). URL: *https://www.ixiacom.com/resources/wlan-access-point-10-crucial-capabilities-and-how-test-them* on 2nd June 2020.
- Glenn Elert (1998-2020), Electromagnetic Spectrum, URL: *https://physics.info/em-spectrum/* Accessed on 3rd June 2020.
- Jim Lucas (February 2019), What are Radio Waves? URL: *https://www.livescience.com/50399-radio-waves.html* Accessed on 3rd June 2020.
- Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter). (n.d). URL: *https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/* Accessed on 3rd June 2020.
- Frank Ibikunle (December 2009), WiMAX: Appropriate Technology to Provide Last Mile Access to ICTs Infrastructure and Services in Rural Areas, URL: https://www.intechopen.com/ Accessed on 3rd June 2020.

- Orauariki (April 2017), How to write a business report, URL: *https://www.wgtn.ac.nz/__data/assets/pdf_file/0010/1779625/VBS-Report-Writing-Guide-2017.pdf* Accessed on 3rd June 2020.
- Ciprian Adrian Rusen (Mars, 2020), How to choose a wireless router: 10 things to consider, URL: *https://www.digitalcitizen.life/things-consider-when-buying-wireless-router* Accessed on 20th May, 2020.
- Marco Cremonini (2013), Privacy on the internet, URL: *https://www.sciencedirect.com/topics/computer-science/location-privacy* Accessed on 3rd June 2020.
- Simplilearn (Jul 23, 2019), ITIL® Training and Preparation: SLM, Designing SLA Structures, and SLA Content, URL**:** *https://www.givainc.com/blog/index.cfm/2018/12/3/3-Types-of-Service-Level-Agreements* Accessed on 3rd June 2020.
- Cisco BWX360 WiMAX Outdoor Modem. (n.d). URL: *https://www.cisco.com/c/dam/en/us/td/docs/wireless/broadband_wireless_access/bwx360/install/guide/BWX360_Cisco_INST_2010-04-07.pdf* Accessed on 5th June, 2020
- HSPA Modem. (n.d). *http://www.downloads.netgear.com/files/aircard/2130961_Compass_HSPA_USB_Modem_Installation_Guide_web.pdf* Accessed on 5th June, 2020