TVET CERTIFICATE III in COMPUTER SYSTEMS TECHNOLOGY

WIRELESS LOCAL AREA NETWORK SETUP (WLAN).

COSWN301

Set up wireless Local Area network (WLAN)

Competence

Credits: 8

Learning hours: 80

Sector: ICT

Sub-sector: COMPUTER MAINTENANCE

Module Note Issue date: October, 2020

Purpose statement

This core module describes the skills, knowledge and attitude required to identify wireless local network components adequately. The learner will be able to install and configure wireless network components, perform WLAN network security, verify WLAN connectivity, conduct standard tests, measurements and write technical report.

Table of contents

Total Number of Pages: 61

Learning Unit 1 – Apply WLAN concepts.

LO1.1 – Describe WLAN technology and its functionality

- Content/Topic 1: Introduction to WLAN technology and its functionality.

Wireless is a communication of two or more devices without the use of wires/cables.

Wireless network is a computer network that uses wireless data connections between network nodes.

Wireless networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.

There are four main types of wireless networks:

- Wireless Local Area Network (LAN): Links two or more devices using a wireless distribution method, providing a connection through access points to the wider Internet.
- Wireless Metropolitan Area Networks (MAN): Connects several wireless LANs.
- Wireless Wide Area Network (WAN): Covers large areas such as neighboring towns and cities.
- Wireless Personal Area Network (PAN): Interconnects devices in a short span, generally within a person's reach.

Why use wireless?

We use Wireless networks to enable multiple devices to use the same internet connection remotely, as well as share files and other resources. They also allow mobile devices, such as laptops, tablets and iPod to move around within the network area freely and still maintain a connection to the internet and the network.

Why have Wireless LANs become so popular?

Wireless LANs is obviously more convenient than wired Ethernet cables. It is quite easy to use at any time.

- The main cause of popularity of WLAN is about security and speed of scalability.
- Wireless network has a very good speed than wired because it uses DHCP for IP Addressing.
- The security of wireless is actually very good because it uses the latest encryption technology, which is difficult for hackers.

Wireless LANs

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc.

This gives users the ability to move around within the area and yet still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet

Comparing a WLAN to a LAN

While **wireless LANs** refer to any **local area network** (**LAN**) that a mobile user can connect to through a wireless (radio) connection; Wi-Fi (short for "Wireless Fidelity") is a term for certain types of **WLANs** that use specifications in the 802.11 wireless protocol family.

~ LAN devices are based on IEEE8012.3 standards while WLAN devices are based on IEEE802.11 standards.

~ LAN devices use electric signals to transmit data while WLAN devices use high energy radio frequency waves to transmit the data.

~ LAN refers to a wired network while WLAN is used to refer to a wireless network.

~ LAN used commonly in fixed networks while WLAN is common in areas where computers are moved quite often.

~ LAN use CSMA/CD to detect collisions in the network while WLAN use CSMA//CA to avoid collisions in the network.

~ With WLAN the users can access network from anywhere within the range, while with LAN the user's location is limited to the use of cable connected to the port.

~ WLANs connect clients to the network through a wireless access point (AP) or wireless router, instead of an Ethernet switch.

~ WLAN does not need cable to transfer files, while LAN needs cable.

~ WLAN is more convenient to users compared to LAN.

~ WLAN is less secured while LAN is more secured.

- Content/Topic 2: Description of WLAN Standards, Wi-Fi Certification and Mobility

A. WLAN Standards

Generally, Wireless standards were driven by two factors:

- **Speed** - getting data transmitted faster between PCs and access points
- **Security** - making sure that the wireless capability is not abused

You need to be aware of both factors when choosing WLAN equipment.

Each network can be broken down by a few different settings:

- **Speed**: How much data the network can transmit. This is calculated in Mbps (1 million bits per second)
- **Frequency**: What radio frequency the network is carried on. These are either 5 GHZ or 2.4 GHZ.

IEEE802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer **communication** in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.

802.11 and *802.11x* refers to a family of specifications developed by the IEEE for ***w****ireless* ***LAN*** (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

There are several specifications in the *802.11* family:

- **802.11** — applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- **802.11a** — an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz Frequency band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- **802.11b** (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz Frequency band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- **802.11e** — a wireless draft standard that defines the ***Q****uality* ***o****f* ***S****ervice* (QoS) support for LANs, and is an enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. 802.11e adds QoS features and multimedia support to the existing IEEE 802.11b and IEEE 802.11a wireless standards, while maintaining full backward compatibility with these standards.
- **802.11g** — applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz Frequency bands.
- **802.11n** — 802.11n builds upon previous 802.11 standards by adding ***m****ultiple-****i****nput* ***m****ultiple-****o****utput* (MIMO). The additional transmitter and receiver antennas allow for increased data throughput through spatial multiplexing and increased range by exploiting the spatial diversity through coding

schemes. The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g.

- **802.11ac** — 802.11ac builds upon previous 802.11 standards, particularly the 802.11n standard, to deliver data rates of 433Mbps per spatial stream, or 1.3Gbps in a three-antenna (three stream) design. The 802.11ac specification operates only in the 5 GHz frequency range and features support for wider channels (80MHz and 160MHz) and beamforming capabilities by default to help achieve its higher wireless speeds.
- **802.11ac Wave 2** — 802.11ac Wave 2 is an update for the original 802.11ac spec that uses MU-MIMO technology and other advancements to help increase theoretical maximum wireless speeds for the spec to 6.93 Gbps.
- **802.11ad** — 802.11ad is a wireless specification under development that will operate in the 60GHz frequency band and offer much higher transfer rates than previous 802.11 specifications, with a theoretical maximum transfer rate of up to 7Gbps (Gigabits per second).
- **802.11ah**— Also known as Wi-Fi HaLow, 802.11ah is the first Wi-Fi specification to operate in frequency bands below one gigahertz (900 MHz), and it has a range of nearly twice that of other Wi-Fi technologies. It's also able to penetrate walls and other barriers considerably better than previous Wi-Fi standards.
- **802.11r** - 802.11r, also called *Fast **B**asic **S**ervice **S**et* (BSS) Transition, supports VoWi-Fi handoff between access points to enable VoIP roaming on a Wi-Fi network with 802.1X authentication.
- **802.1X** — Not to be confused with 802.11x (which is the term used to describe the family of 802.11 standards) 802.1X is an IEEE standard for port-based Network Access Control that allows network administrators to restricted use of IEEE 802 LAN service access points to secure communication between authenticated and authorized devices.

B. Wi-Fi Certification

A Wi-Fi Certificate protects the registration process and encrypts log-in credentials when connecting to public Wi-Fi, ultimately providing secure network access and increasing trust in public hotspots and sign-up services.

Wi-Fi Certification means that a product has been tested in numerous configurations with a diverse sampling of other devices to validate interoperability with other Wi-Fi CERTIFIED equipment operating in the same frequency band.

Wi-Fi Certification is available for a wide range of consumer, enterprise, and operator-specific products, including smartphones, appliances, computers and peripherals, networking infrastructure, and consumer electronics.

C. Supporting Mobility

Mobility support within WiMAX network architecture is based on mobile IP framework. Mobile IP is an IETF protocol that allows mobile users to move from one network to another while maintaining their IP address
This work proposes a two-tier approach for mobility support in wireless sensor networks.

- Content/Topic 3: Identification of the advantages and disadvantages of Wireless

D. Benefits/advantages of Wireless

- **Increased Mobility:** Wireless networks allow mobile users to access real-time information so they can roam around your company's space without getting disconnected from the network. This increases teamwork and productivity company-wide that is not possible with traditional networks.
- **Installation Speed and Simplicity:** Installing a wireless network system reduces cables, which are cumbersome to setup and can impose a safety risk, should employees trip on them. It can also be installed quickly and easily, when compared to a traditional network.
- **Wider Reach of the Network:** The wireless network can be extended to places in your organization that are not accessible for wires and cables.
- **More Flexibility:** Should your network change in the future, you can easily update the wireless network to meet new configurations.
- **Reduced Cost of Ownership over Time:** Wireless networking may carry a slightly higher initial investment, but the overall expenses over time are lower. It also may have a longer lifecycle than a traditionally connected network.
- **Increased Scalability:** Wireless systems can be specifically configured to meet the needs of specific applications. These can be easily changed and scaled depending on your organization's needs.
- **Easier to provide connectivity** in areas that are difficult to lay cable.
- **Portable** or semi-permanent buildings can be connected using WLAN.

E. **Disadvantages of WLAN**

- When the number of computers that use the network increases, the data transfer to the computer each will be reduced.
- When standards change, it may be necessary to replace the wireless card and / or access point.

- The low bandwidth wireless means some applications like video streaming to be more effective on the LAN cable.
- Security is more difficult to guarantee and requires no configuration.
- The device operates on a limited distance from the access point, the distance is determined by the standard used and buildings and other obstacles between the access point and the user.
- A LAN cable most likely be required to provide a backbone to WLAN, WLAN should be a supplement to the LAN cable and not a complete solution.
- Long-term cost-efficient is more difficult to achieve static environments that require few moves and changes.

- Content/Topic 4: Description of Wireless infrastructure components.

F. Wireless Infrastructure components

Infrastructure mode is an 802.11-networking framework in which devices communicate with each other by first going through an Access Point (AP).

In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network.

When one AP is connected to wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS).

An Extended Service Set (ESS) is a set of two or more BSSs that form a single subnetwork.

Most corporate wireless LANs operate in infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers.

Infrastructure components of wireless are:

- **Wireless NICs:** WNIC, a **wireless** network interface card is a **network card**, which is used to connect radio-based computer networks. WNICs uses an antenna to communicate through microwaves and is typically connected using the computer's PCI bus or USB port.
- **Wireless Home Router:** is a device that performs the functions of a router and also includes the functions of a wireless access point.
- **Wireless Access Points:** is a networking hardware device that allows other Wi-Fi devices to connect to a wired network.
- **Wireless Antennas:** is the part of a radio communications system that radiates and/or collects radio frequency energy. Wi-Fi ***wireless*** networking works by sending radio transmissions on specific frequencies where listening devices can receive them.

How to use Wireless Antennas?

Wireless antennas are typically connected via low loss coaxial cable either to an amplifier, splitter, filter or directly to a wireless access point or router.

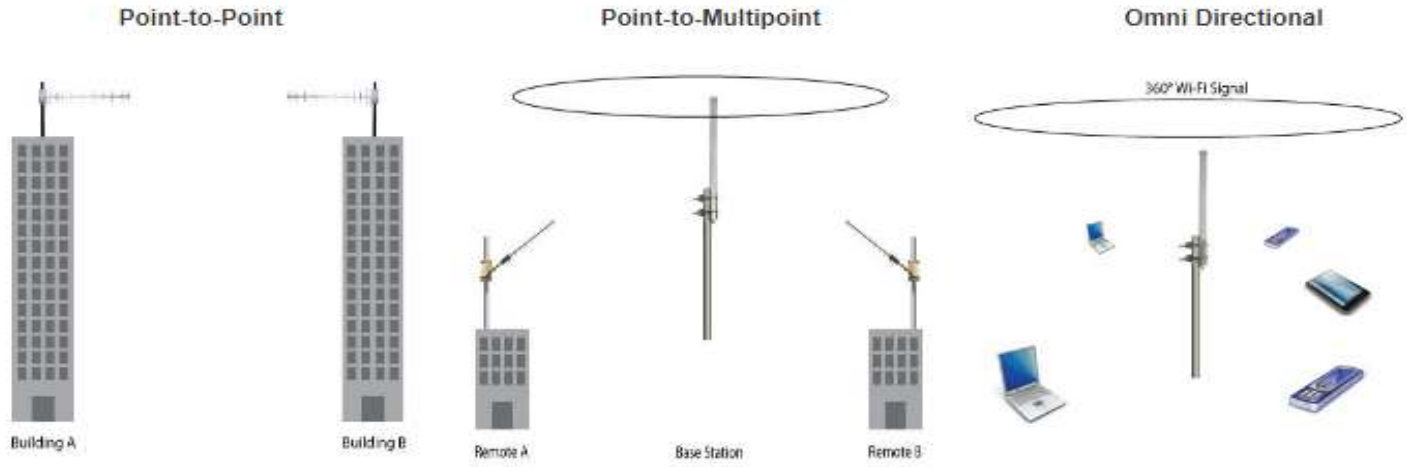
For outdoor applications wireless antennas are often attached via mounting clamps to a mast or to the side of a building via mounting brackets.

Wireless Antennas used indoors are typically ceiling mounted or sometimes mounted high up on a wall.

Types of Antennas.

There are three main antenna categories available for wireless LANs: **Omni-directional**, **Semi-directional** and **Highly directional**.

- **Omni-directional** – Omni directional antennas are designed to radiate a signal in all directions.
- **Semi-directional** – Semi directional antennas are designed to provide specific, directed signal coverage over large areas.
- **Highly-directional** - Highly directional *antennas* are used for point-to-point links; for example, between two buildings.



- Content/Topic 5: Small Wireless Deployment Solutions

Wireless technology involves transmitting electromagnetic signal over the air and allow multiple users to communicate over the same medium without their signal interfacing.

Recall that wireless networks are half-duplex networks. If more than one device were to send at the same time, a collision would result. If a collision occurs, the data from both senders would be unreadable and would need to be resent. This is a waste of time and resources.

There are three mode of wireless transmission.

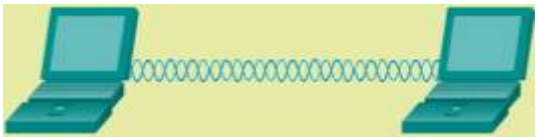
- **Radio based:** It has a wavelength between 1m – 100km and frequency 3 KHz – 300 KHz. They are generated by an electronic device called a transmitter connected to an antenna which radiates the waves, and received by a radio receiver connected to another antenna.

  Example**:** Radio, Telephone system, TV, Navigator, Radar system.
- **Microwaves based:** Communication is like Radio based but the differences are based on wavelength and frequency. It has a wavelength between 1mm – 1m and frequency 3 KHz – 300 KHz.
- **Optical wireless:** Refers to the combined use of two technologies - conventional Radio-Frequency (RF) wireless and Optical Fiber - for telecommunication. Long-range links are provided by optical fiber (also known as *fiber optic* cables), and links from the long-range end-points to end users are accomplished by RF wireless. In short-range like the use of remote control, it is established by two or more devices equipped with infrared transmitters and receivers, it is called sometimes LIFI (light fidelity)

- Content/Topic 6: Description of IEEE802.11 WLAN Topologies

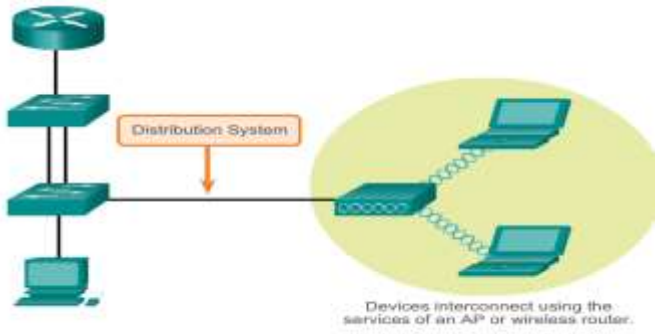
- **Wireless Topology Modes:** Regardless of the type of PHY chosen, IEEE 802.11 supports three basic topologies for WLANs; the Independent Basic Service Set (**IBSS**), the Basic Service Set (**BSS**), and the Extended Service Set (**ESS**).
  - **IBSS (Independent Basic Service Set):** There are no AP; Client devices can communicate with others directly without a central device. Also called a peer-to-peer communication.
  - **BSS (Basic Service Set):** You have only one AP and many clients.
  - **ESS (Extended Service Set):** You have two or more APs connected together and many clients.
- **Ad Hoc Mode:** When two devices connect wirelessly without the aid of an infrastructure device, such as a wireless router or AP. Examples include Bluetooth and Wi-Fi Direct.

  Briefly, Ad Hoc Mode has the following characteristics:
  - ✓ Independent Basic Service Set (IBSS)
  - ✓ No need of central access point
  - ✓ All nodes need to use the same SSID and channel
  - ✓ Not scalable



- **Infrastructure Mode:** is an 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure **mode**, **wireless** devices can communicate with each other or can communicate with a wired network.

Briefly, infrastructure mode has the following characteristics:



- Extended Service Set (ESS)
- Central access point is needed
- "Connects "a WLAN to an Ethernet network
- Clients and AP's must use the same SSID
- Channel is set in AP and discovered by clients
- Scalable

Note:

An SSID (service set identifier) is the primary name associated with an 802.11 wireless local area network (WLAN) including home networks and public hotspots. Client devices use this name to identify and join wireless networks.

An **SSID** is simply the technical term for a network name. When you set up a wireless home network, you give it a name to distinguish it from other networks in your neighborhood. You'll see this name when you connect your computer to your wireless network. WPA2 is a standard for wireless security.

LO1.2 – Describe WLAN Operations

- Content/Topic 1: Description of Wireless Network operations

A. Introduction to wireless network operations

Wireless Local Area Networks use radio, infrared and microwave transmission to transmit data from one point to another without cables. Therefore, **WLAN** offers way to build a Local Area Network without cables.

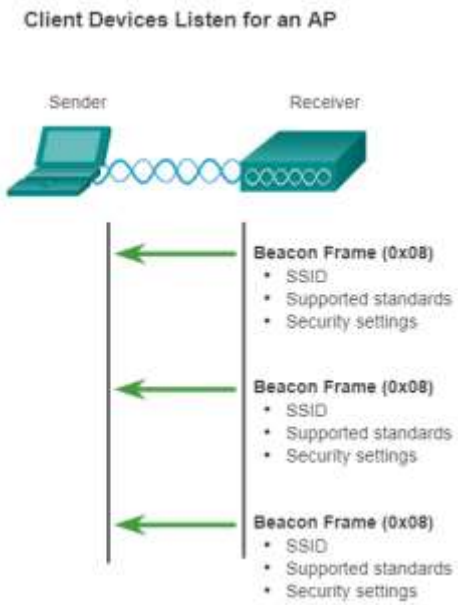
Wireless operations permit services, such as mobile and interplanetary communications, that are impossible or impractical to implement with the use of wires. The term is commonly used in the telecommunications industry to refer to telecommunications systems (e.g. radio transmitters and receivers, remote controls, etc.) which use

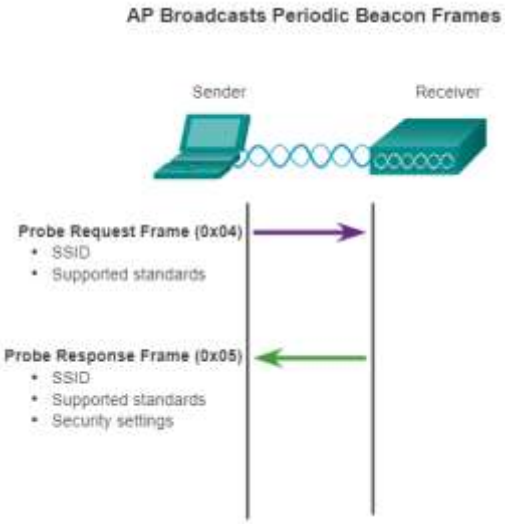
some form of energy (e.g. radio waves, acoustic energy,) to transfer information without the use of wires. Information is transferred in this manner over both short and long distances.

B. Wireless operations

Wireless devices must discover and connect to an AP or wireless router. Wireless clients connect to the AP using a scanning (probing) process. This process can be **passive** or **active**:

- **Passive mode:** The AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings. The primary purpose of the beacon is to allow wireless clients to learn which networks and APs are available in a given area, thereby allowing them to choose which network and AP to use.





- **Active mode:** Wireless clients must know the name of the SSID. The wireless client initiates the process by broadcasting a probe request frame on multiple channels. The probe request includes the SSID name and standards supported. Active mode may be required if an AP or wireless router is configured to not broadcast beacon frames

C. 802.11 Frame Structure

MAC layer provides functionality for several tasks like control medium access, can also offer support for roaming, authentication, and power conservation. The basic services provided by MAC are the mandatory asynchronous data service and an optional time-bounded service.

IEEE 802.11 defines two MAC sub-layers:

1. **Distributed Coordination Function (DCF)**

DCF uses CSMA/CD as access method as wireless LAN cannot implement CSMA/CD. It only offers asynchronous service.

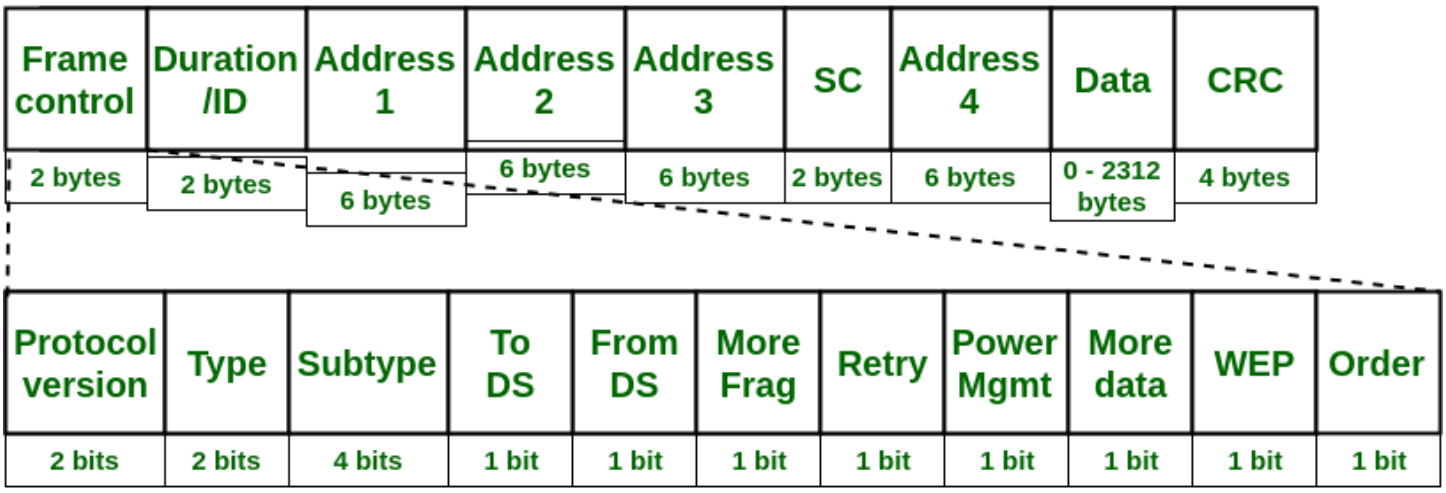
2. **Point Coordination Function (PCF)**

Port Control Protocol (**PCP**) is a computer networking protocol that allows hosts on IPv4 or IPv6 networks to control how the incoming IPv4 or IPv6 packets are translated and forwarded by an upstream router that performs network address translation (NAT) or packet filtering.

PCP is implemented on top of DCF and mostly used for time-service transmission. It uses a centralized, contention-free polling access method. It offers both asynchronous and time-bounded service.

PCF is a media access control (MAC) technique used in IEEE 802.11 based WLANs, including Wi-Fi. It resides in a point coordinator also known as access point (AP), to coordinate the communication within the network.

The MAC layer frame consist of 9 fields. The following figure shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.



- **Frame Control (FC):** It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:
  - **Version:** It is a 2 bits long field which indicates the current protocol version which is fixed to be 0 for now.
  - **Type:** It is a 2 bits long field which determines the function of frame i.e management (00), control (01) or data (10). The value 11 is reserved.

- **Subtype:** It is a 4 bits long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.
- **To DS:** It is a 1 bit long field which when set indicates that destination frame is for DS (distribution system).
- **From DS:** It is a 1 bit long field which when set indicates frame coming from DS.
- **More frag (More fragments):** It is 1 bit long field which when set to 1 means frame is followed by other fragments.
- **Retry:** It is 1 bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
- **Power Mgmt (Power management):** It is 1 bit long field which indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
- **More data:** It is 1 bit long field which is used to indicates a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
- **WEP (Wired Equivalent Privacy):** Also called Protected Frame. It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.
- **Order:** It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

❖ **Duration/ID:** It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in μs).

❖ **Address 1 to 4** : Depending on whether the 802.11 traffic is upstream or downstream, the definition of each of the four MAC address fields in the layer 2 header will change.

- **Address 1: Source Address (SA)** The MAC address of the original sending station is known as the SA. The source address can originate from either a wireless station or the wired network.
- **Address 2: Destination Address (DA)** The MAC address that is the final destination of the layer 2 frame is known as the DA. The final destination may be a wireless station or could be a destination on the wired network such as a server or a router.
- **Address 3: Transmitter Address (TA)** The MAC address of an 802.11 radio that is transmitting the frame onto the half-duplex 802.11 medium is known as the TA.

- **Address 4: Receiver Address (RA)** The MAC address of the 802.11 radio that is intended to receive the incoming transmission from the transmitting station is known as the RA. Usually missing because it is used only in ad hoc mode

❖ **SC (Sequence control):** It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.

❖ **Data:** Also called Frame body. It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).

❖ **CRC (Cyclic redundancy check):** It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

D. Wireless Frame Type

Wireless LANs come in three frame types:

❖ **Management frames:** Used for joining and leaving a wireless cell. Another name for Management Frames is "MAC protocol Data Unit"(MMPDU). Type value is 00.

The followings are the list of all 12 of the Management frame subtypes as defined by 802.11 standard

- **Association request frame** - (0x00) Sent from a wireless client, it enables the AP to allocate resources and synchronize. The frame carries information about the wireless connection including supported data rates and SSID of the network to the wireless client that wants to associate. If the request is accepted, the AP reserves memory and establishes an association ID for the device.
- **Association response frame** - (0x01) Sent from an AP to a wireless client containing the acceptance or rejection to an association request. If it is an acceptance, the frame contains information, such as an association ID and supported data rates.
- **Re-association request frame** - (0x02) A device sends a re-association request when it drops from range of the currently associated AP and finds another AP with a stronger signal. The new AP coordinates the forwarding of any information that may still be contained in the buffer of the previous AP.
- **Re-association response frame** - (0x03) Sent from an AP containing the acceptance or rejection to a device re-association request frame. The frame includes information required for association, such as the association ID and supported data rates.

- **Probe request frame** - (0x04) Sent from a wireless client when it requires information from another wireless client.
- **Probe response frame** - (0x05) Sent from an AP containing capability information, such as the supported data rates, after receiving a probe request frame.
- **Beacon frame** - (0x08) Sent periodically from an AP to announce its presence and provide the SSID and other preconfigured parameters.
- **Disassociation frame** - (0x0A) Sent from a device wanting to terminate a connection. Allows the AP to relinquish memory allocation and remove the device from the association table.
- **Authentication frame** - (0x0B) The sending device sends an authentication frame to the AP containing its identity.
- **De-authentication frame** - (0x0C) Sent from a wireless client wanting to terminate connection from another wireless client.
- **Announcement Traffic Indication Message (ATIM)** - are used in IEEE 802.11 ad hoc or Independent BSS (Basic Service Set) networks to announce the existence of buffered frames. These messages are sent between wireless stations to prevent them entering power saving mode and to indicate there is data to follow.
- **Action -** are a type of management frame used to trigger an action in the cell.

❖ **Control frames:** Used to acknowledge when data frames are received. Type value is 01.

Followings are the list of control frame subtypes as defined by 802.11 standard

- **Request to Send (RTS) frame** - The RTS and CTS frames provide an optional collision reduction scheme for APs with hidden wireless clients. A wireless client sends an RTS frame as the first step in the two-way handshake, which is required before sending data frames.
- **Clear to Send (CTS) frame** - A wireless AP responds to an RTS frame with a CTS frame. It provides clearance for the requesting wireless client to send a data frame. The CTS contributes to collision control management by including a time value. This time delay minimizes the chance that other wireless clients will transmit while the requesting client transmits.
- **Acknowledgment (ACK) frame** - After receiving a data frame, the receiving wireless client sends an ACK frame to the sending client if no errors are found. If the sending client does not receive an ACK frame within a predetermined period of time, the sending client resends the frame.

- **Power Save (PS) Poll:** allows the client to indicate to the AP that it is going to sleep until the next beacon. The AP buffers frames while asleep, then lets the client know that frames are buffered via an advertisement in the beacon.
- **Contention-Free(CF)-End (PCF only):** Occurs when the AP is functioning in PCF mode. During the CFP, the AP polls only clients in PCF mode about their intention to send data.
- **Other Frames:** CF-End+CF-ACK (PCF only), Black-ACK(HCF), Black Ack Request(HCF)

❖ **Data frames:** Frames that contain data. Type value is 10.

- Data+CF-Ack (PCF only)
- Data+CF-Poll (PCF only)
- Data+CF-Ack+CF-Poll (PCF only)
- Null data (no data transmitted)
- CF-Ack (no data transmitted) (PCF only)
- CF-Poll (no data transmitted) (PCF only)
- Data+CF-Ack+CF-Poll (PCF only)
- Qos Data (HCF)
- Qos Null (No Data) (HCF)
- QosData+CF-Ack (HCF)
- QosData+CF-Poll (HCF)
- QosData+CF-Ack+CF-Poll (HCF)
- QosCf-Poll(HCF)
- Qos CF-ACK+CF-Poll (HCF)

E. CSMA/CA

CSMA/CA is a **network** multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle".

CSMA/CA does not deal with the recovery after a collision. It checks whether the medium is in use or not. If it is busy, then the transmitter waits until it is idle state, before it starts transmitting data. This effectively minimizes the possibility of collisions and makes more efficient use of the medium.

Wi-Fi systems are half-duplex, shared media configurations; therefore, wireless clients can transmit and receive on the same radio channel. This creates a problem because a wireless client cannot hear while it is sending;

thus, making it impossible to detect a collision. To address this problem, the IEEE developed an additional collision avoidance mechanism called the Distributed Coordination Function (DCF). Using DCF, a wireless client transmits only if the channel is clear. All transmissions are acknowledged; therefore, if a wireless client does not receive an acknowledgment, it assumes a collision occurred and retries after a random waiting interval.

F. Discovering Aps

Discovering Aps is the process through which the wireless client's devices connect to the Aps using scanning (probing) process. This process can be **passive mode** and **active mode**.

- Content/Topic 2: Channel Management

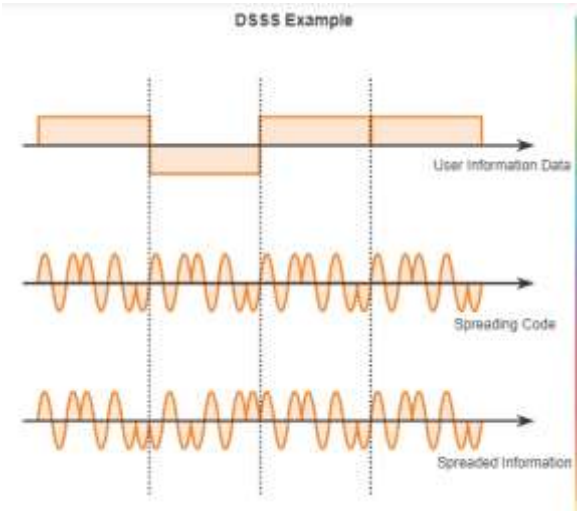
A. Frequency Channel Saturation

-Saturated network link is a **link** that should transmit more frames than is possible on its physical support.

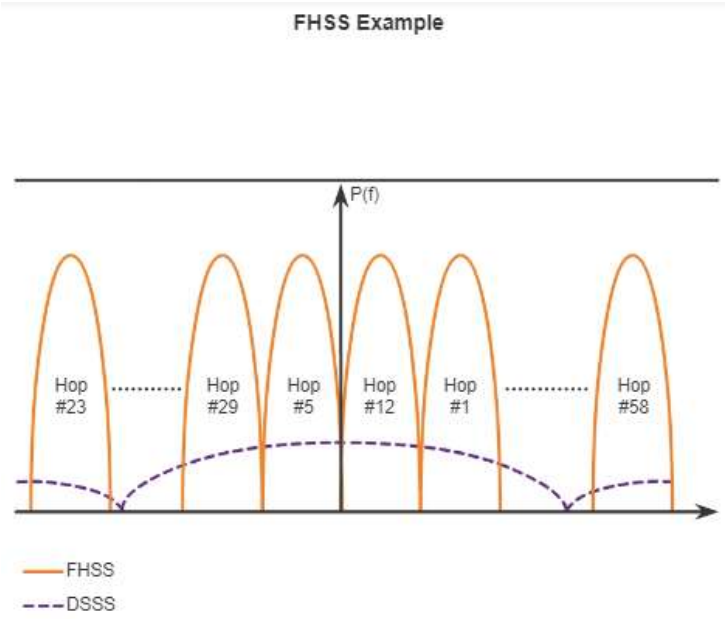
-Channel saturation happens when too many Wireless Access Points ("WAP") have a **Wi-Fi** Network SSID operating on the same channel and are too close together. This causes interference which in turn causes network slowness and network disconnects.

The techniques listed below mitigate channel saturation by using the channels in a more efficient way:

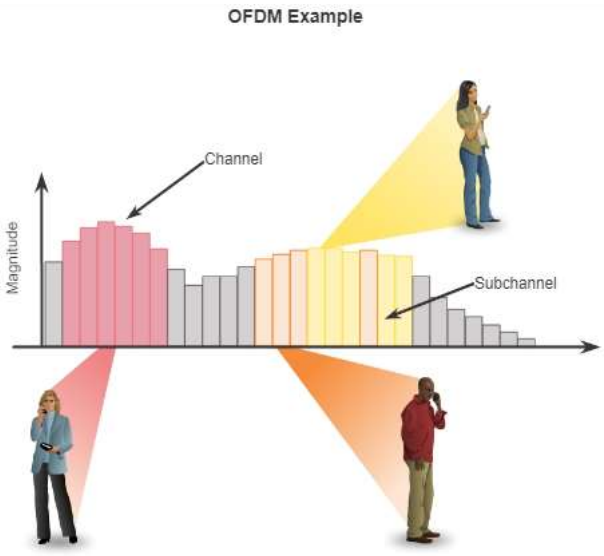
- **Direct-sequence spread spectrum (DSSS)** - DSSS is a spread-spectrum modulation technique. Spread-spectrum is designed to spread a signal over a larger frequency band making it more resistant to interference. With DSSS the signal is multiplied by a "crafted noise" known as a spreading code. Because the receiver knows about the spreading code and when it was added, it can mathematically remove it and re-construct the original signal. In effect, this creates redundancy in the transmitted signal in an effort to counter quality loss in the wireless medium. DSSS is used by 802.11b. Also used by cordless phones operating in the 900 MHz, 2.4 GHz, 5.8 GHz bands, CDMA cellular, and GPS networks.



- **Frequency-hopping spread spectrum (FHSS)** - FHSS also relies on spread-spectrum methods to communicate. It is similar to DSSS but transmits radio signals by rapidly switching a carrier signal among many frequency channels. With the FHSS, sender and receiver must be synchronized to "know" which channel to jump. This channel hopping process allows for a more efficient usage of the channels, decreasing channel congestion. Walkie-talkies and 900 MHz cordless phones also use FHSS, and Bluetooth uses a variation of FHSS. FHSS is also used by the original 802.11 standard.



- **Orthogonal frequency-division multiplexing (OFDM)** - OFDM is a subset of frequency division multiplexing in which a single channel utilizes multiple sub-channels on adjacent frequencies. Sub-channels in an OFDM system are precisely orthogonal to one another which allow the sub-channels to overlap without interfering. As a result, OFDM systems are able to maximize spectral efficiency without causing adjacent channel interference. In effect, this makes it easier for a receiving station to "hear" the signal. Because OFDM uses sub-channels, channel usage is very efficient. OFDM is used by a number of communication systems including 802.11a/g/n/ac.



- **<u>Selecting Channels</u>**

Wi-Fi channels are smaller bands within Wi-Fi frequency bands that are used by your wireless network to send and receive data. Depending on which frequency band your router is using, you have a certain number of Wi-Fi channels to choose from:

- 11 Wi-Fi channels are in the 2.4 GHz frequency band.
- 45 Wi-Fi channels are in the 5 GHz frequency band.

Your choice of wireless channels can have a big effect on network performance. Your goal is to choose settings that avoid interference from other networking and radio frequency equipment.

Selecting Wi-Fi channel is primarily for those using 2.4GHz Wi-Fi. If you're using the latest 5Ghz Wi-Fi, you shouldn't need to worry too much about which channel you're using, although you may want to switch to a different available channel if nearby connections are using the same channel. 5GHz Wi-Fi operates on a much higher frequency than 2.4GHz Wi-Fi so it isn't subject to the same common microwave interference that can affect 2.4Ghz Wi-Fi.

When Channel Management is enabled, the Access Point automatically assigns wireless radio channels used by clustered access points.

The **automatic channel assignment** reduces mutual interference (or interference with other access points outside of its cluster) and maximizes Wi-Fi bandwidth to help maintain the efficiency of communication over the wireless network.

If significant channel interference is detected, the Channel Manager automatically re-assigns some or all of the APs to new channels per an efficiency algorithm (or *automated channel plan*).

You must start channel management to get automatic channel assignments, because it is disable by default on a new AP.

Type "**netsh wlan show all" in the command prompt to view all information related to wireless.**

Consider adjusting your channel selections in the following situations:

- You are experiencing interference (shown by lost connections or slow data transfers).
- You want to improve your wireless coverage.
- You use multiple access points or wireless routers, which requires you to use different channels on the devices.
- You aren't the only person nearby running a wireless network.

In addition, instead of trying to cover everywhere in your home, use a combination of access points and antennas and other equipment to create local "**spotlights**" of strong transmission.

What if a channel I want to use has too much interference?

Unfortunately, you can't completely avoid interference just by using other channels. Wireless protocols 802.11b and 11g only have three non-overlapping channels. When four or more channels are used in the same area, the level of interference can increase notably. If you and your close neighbor both have a router and a wireless

access point, a total of four powerful transmitters are in close proximity and you both experience some interference.

If you're experiencing a severe problem, a practical and sociable thing is to talk to your neighbors using wireless networks that can be seen when you scan. Together, you can choose optimal channels for your respective networks. Tune your equipment to channels that at least five channels apart. So, for example, you might use channels 1 and 8, and your neighbor might use 5 and 11. Setting Power to Half or quarter should be considered.

You might be able to place routers and access points farther away from each other inside your homes. After all, the kinds of physical barriers that reduce your transmission range also reduce the signal that your neighbor doesn't want to see.

Using a directional antenna, or an antenna cable to shift an antenna, can help you both.

How do I change the Wi-Fi channel I'm using?

To change what Wi-Fi channel you are currently using, log in to your router's settings by typing its IP address (can be found on your router) into the address bar on your browser. Use the username and password you designated when creating your Wi-Fi network. (If you are still using the router's factory set username and password, we suggest changing to something more unique and secure!) From here, you can go to your router's wireless settings to change the Wi-Fi channel it is using.

Many routers are set up to automatically choose what Wi-Fi channel to use; and they may not choose 1, 6, or 11. The Wi-Fi channel your router chooses actually depends on the hardware itself.

LO1.3 – Identify WLAN Threats.

- Content/Topic 1: Identification of Wireless LAN Threats

WLAN Threat is an effort to obtain illegal admission to your network to take data without your knowledge, or execute other malicious pursuits. Your network security is at risk or vulnerable if or when there is a weakness or vulnerability within your computer network. The followings are the types of network threats.

1. **DoS Attack (Denial of Service Attack)**

Wireless DoS attacks can be the result of:

- **Improperly configured devices** - Configuration errors can disable the WLAN. For instance, an administrator could accidently alter a configuration and disable the network, or an intruder with administrator privileges could intentionally disable a WLAN.

- **Malicious user intentionally interfering with the wireless communication** - Their goal is to disable the wireless network completely or to the point where no legitimate device can access the medium.
- **Accidental interference** - WLANs operate in the unlicensed frequency bands and; therefore, all wireless networks, regardless of security features, are prone to interference from other wireless devices. Accidental interference may occur from such devices as microwave ovens, cordless phones, baby monitors, and more. The 2.4 GHz band is more prone to interference than the 5 GHz band.

2. Management Frame DoS Attacks

Management frames can be manipulated to create various types of DoS attacks. Two common management frame attacks include:

- **A spoofed disconnect attack (SDA)** - This occurs when an attacker sends a series of "disassociate" commands to all wireless clients within a BSS. These commands cause all clients to disconnect. When disconnected, the wireless clients immediately try to re-associate, which creates a burst of traffic. The attacker continues sending disassociate frames and the cycle repeats itself.
- **A CTS flood** - This occurs when an attacker takes advantage of the CSMA/CA contention method to monopolize the bandwidth and deny all other wireless clients access to the AP. To accomplish this, the attacker repeatedly floods the BSS with Clear to Send (CTS) frames to a bogus STA. All other wireless clients sharing the RF medium receive the CTS and withhold their transmissions until the attacker stops transmitting the CTS frames.

3. Rogue Aps

These are the APs or wireless routers that have either been:

- Connected to a corporate network without explicit authorization and against corporate policy. Anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network resources.
- Connected or enabled by an attacker to capture client data such as the MAC addresses of clients (both wireless and wired), or to capture and disguise data packets, to gain access to network resources, or to launch man-in-the-middle attack.

4. **Packet Sniffing:** When information is sent back and forth over a network, it is sent in what we call packets. Since wireless traffic is sent over the air, it's very easy to capture. Quite a lot of traffic (FTP, HTTP, SNMP) is sent in the clear, meaning that there is no encryption and files are in plain text for anyone to read. So using a tool like Wire shark allows you to read data transfers in plain text! This can lead to

stolen passwords or leaks of sensitive information quite easily. Encrypted data can be captured as well, but it's obviously much harder for an attacker to decipher the encrypted data packets.

5. **Password Theft:** When communicating over wireless networks, think of how often you log into a website. You send passwords out over the network, and if the site doesn't use SSL or TLS, that password is sitting in plain text for an attacker to read. There are even ways to get around those encryption methods to steal the password. I'll talk about this with man in the middle attacks.

6. **Jamming:** There are a number of ways to jam a wireless network. One method is flooding an AP with de-authentication frames. This effectively overwhelms the network and prevents legitimate transmissions from getting through. This attack is a little unusual because there probably isn't anything in it for the hacker. One of the few examples of how this could benefit someone is through a business jamming their competitors Wi-Fi signal. This is highly illegal (as are all these attacks), so businesses would tend to shy away from it. If they got caught they would be facing serious charges.

7. **War Driving:** War driving comes from an old term called war dialing, where people would dial random phone numbers in search of modems. War driving is basically people driving around looking for vulnerable APs to attack. People will even use drones to try and hack APs on higher floors of a building. A company that owns multiple floors around ten stories up might assume nobody is even in range to hack their wireless, but there is no end to the creativity of hackers!

8. **Bluetooth Attacks:** There are a variety of Bluetooth exploits out there. These range from annoying pop up messages, to full control over the a victims Bluetooth enabled device. Check out this blog post on hacking bluetooth for an in depth look.

9. **WEP/WPA Attacks:** Attacks on wireless routers can be a huge problem. Older encryption standards are extremely vulnerable, and it's pretty easy to gain the access code in this case. Once someone on your network, you've lost a significant layer of security. APs and routers are hiding your IP address from the broader Internet using Network Address Translation (unless you use IPv6 but that's a topic for another day). This effectively hides your private IP address from those outside your subnet, and helps prevent outsiders from being able to directly attack you. The keyword there is that it *helps* prevent the attacks, but doesn't stop it completely. Now that you don't trust anything on the Internet anymore, let's build that confidence back up.

10. Man-in-the-Middle Attack

Man-in-the-middle attack (**MITM**) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other.

One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Example:

1. Alice sends a message to Bob, which is intercepted by Mallory:

   Alice "Hi Bob, it's Alice. Give me your key." → Yve Bob
2. Mallory relays this message to Bob; Bob cannot tell it is not really from Alice:

   Alice Yve "Hi Bob, it's Alice. Give me your key." → Bob
3. Bob responds with his encryption key:

   Alice Yve ← [Bob's key] Bob
4. Mallory replaces Bob's key with her own, and relays this to Alice, claiming that it is Bob's key:

   Alice ← [Mallory's key] Yve Bob
5. Alice encrypts a message with what she believes to be Bob's key, thinking that only Bob can read it:

   Alice "Meet me at the bus stop!" [encrypted with Mallory's key] → Yve Bob
6. However, because it was actually encrypted with Mallory's key, Mallory can decrypt it, read it, modify it (if desired), re-encrypt with Bob's key, and forward it to Bob:

   Alice Yve "Meet me at the van down by the river!" [encrypted with Bob's key] → Bob
7. Bob thinks that this message is a secure communication from Alice.

- Content/Topic 2: Identification of ways to make yourself less susceptible to wireless attacks.

- **Use WPA2 security:** This takes enough work to crack that most hackers will look for an easier target. Make sure WPS (stands for Wi-Fi Protected Setup) is turned off.
- **Minimize Your Networks Reach:** Try to position your router in the center of your home or building. There are tools available to measure the reach of your network, and you can adjust the signal level. Try to make

it so that the signal beyond your walls is degraded enough that it isn't usable. You may also consider using directional antennae if central placement is not an option.

- **Use Firewalls:** Make sure your APs firewall is enabled. If you can afford a hardware firewall and feel you need the extra security, go ahead and install one. Household networks generally can get away with the standard router firewall, and operating system firewalls.
- **Use a VPN on Open Networks:** If you really must use public WiFi, set up a VPN. Most smart phones have this capability. You can set one up on your PC. This allows you to communicate through an encrypted tunnel back to your home or office. You can even send web traffic through a VPN.
- **Update Software and Firmware:** Keep your system up to date with the latest patches, and make sure any online applications you use are updated as well. Check for AP firmware updates related to security flaws, and implement them as soon as possible. Remember to follow best practices for network modification to ensure you don't interrupt a critical task. Check out your updates in a test lab to make sure that they don't interfere with an important application. Don't perform updates during normal operating hours if possible, and if you must update during work hours make sure everyone is aware that network connectivity could slow down, or be cut off temporarily while you work.
- **Use Strong Passwords:** I recommend you use at least a 15 character password. Use a mix of upper/lowercase letters, numbers, and symbols. Again, don't make it easy. Is the only capital letter at the start? Is there an exclamation at the end? Are there any words in there? These are common bad password practices, and hackers love them.
- **Change the Login Credentials:** Make sure you change the administrative login credentials. This is often something like admin/admin or admin/password by default.
- **Disable your SSID (service set identifier) Broadcast**: This isn't a security measure. The right tools will still find your network's SSID (this is the name of your network in case you didn't know). However, there's a small chance it could help your network fly under the radar.
- **Enable MAC Filtering:** Again, MAC filtering is not security. A knowledgeable hacker knows how to monitor your network and copy the MAC address of a connected device. They can then spoof their own MAC to appear as an authorized device to gain access. However, this is another annoyance for them to deal with.

Learning Unit 2 – Plan and Conduct Site Survey.

LO2.1 – Analyze facilities and existing Wi-Fi & Wired Network

- Content/Topic 1: Analyzing facilities and existing Wi-Fi &Wired Network

A. Site Planning process

- **Perform an initial environment evaluation**

You must know what to look for and questions to ask to effectively determine the environment type and the appropriate deployment type.

- **Select the proper APs for the deployment**

You must understand AP and antenna types to determine the products that are best suited for the environment to provide optimal performance and RF coverage

- **Enter the collected and determined information into Visual RF Plan**

VisualRF Plan is the pre-deployment site planning tool. In most instances, you can perform a standard deployment based on the VisualRF Plan output without a physical site survey. This is called a "virtual" site survey. For complex deployments, you can use VisualRF Plan to generate a basic foundation for planning. But then you should visit the site to verify AP location and signal coverage.

B. Environment evaluation

a. **Physical site survey:** This is a process of planning and designing a wireless network to provide wireless solution that will deliver the required wireless coverage, data rates, network capacity, roaming capacity and quality of service.

The wireless survey usually involves a site visit to test RF interference and identify the best location for access point.

Wireless site survey are conducted by using computer software that collects and analyze WLAN metrics and RF Spectrum characteristics. There are three types of wireless physical site survey; passive, active and predictive.

- **Passive physical site survey methodology**

During a passive survey, a site survey application passively listens to WLAN traffic to detect active access points, measure signal strength and noise level.

For system design purposes, one or more temporary access points are deployed to identify and qualify access point locations.

This used to be the most common method of pre-deployment Wi-Fi survey.

- **Active survey methodology**

During an active survey, the wireless adapter is associated with one or several access points to measure round-trip time, throughput rates, packet loss, and retransmissions.

Active surveys are used to troubleshoot Wi-Fi networks or to verify performance post-deployment.

- **Spectrum clearing methodology**

Predictive surveys are performed with a software program. The program uses the information about the coverage area to perform AP placements based on RF algorithms.

b. Survey Methods

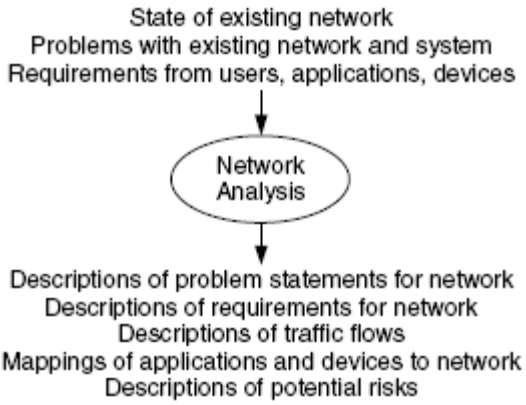
The ***Survey method*** is the technique of gathering data by asking questions to people who are thought to have desired information. There are actually three types of survey methods/techniques/approaches that people use namely questionnaire, interviews, and observation.

c. RF site survey

RF site survey is to supply enough information to determine the number and placement of access points that provides adequate coverage throughout the facility. In most implementations, *adequate coverage* means support of a minimum data rate. A RF site survey also detects the presence of interference coming from other sources that could degrade the performance of the wireless LAN.

d. Analysis of existing system

it's used for describing something that exists now, especially when it might be changed or replaced. The **existing system** needs to be changed. the demolition of **existing** buildings to make way for new office blocks. **Existing**, happening or being dealt with now: **existing**, present, immediate**.**



e. Current network usage:

It provides basic network utilization data in relation to the available network capacity.

Use the Windows key + I keyboard shortcut to open the Settings app. Click Data **usage**. Under Overview, you'll see the total data **usage** from the last 30 days for Wi-Fi and Ethernet connections. Click the **Usage** details link to view **network** data **usage** for all your applications installed on your computer.

f. Future network usage

It is critically important to understand the application and the types of devices that will be used to connect to the network. Application Requirements You must consider current and future applications that may be deployed.

Today, the network may need to support only data applications that are used to run the business. However, in the future the network may need to support voice or multicast video delivery. To begin to understand the data requirements, you must understand the application requirements and define the expected use cases.

C. Consideration for wireless site survey.

When conducting a wireless site survey, consider the following:

1. **Understand the wireless requirements**. You must have a good understanding of specific requirements for the network that impacts signal coverage. For example, maximum range between a client device and the access point decreases as data rate and resulting performance increases. Thus, you need to know the target data rates (and throughput) to interpret correctly survey results.

2. **Obtain a facility diagram**. Before getting too far with the site survey, locate a set of building blueprints or city maps. If none are available, prepare a drawing that depicts the location of walls, walkways, etc. Site survey tools import diagrams in various image formats. Of course mapping software is a good source for outdoor city surveys. If all else fails for in-building surveys, consider taking a digital photograph of the fire escape diagram, which is usually present on hallway walls.

3. **Visually inspect the facility**. Walk through the facility before performing any testing to verify the accuracy of the facility diagram. This is a good time to note any potential attenuation barriers that may affect the propagation of RF signals.

4. **Assess existing network infrastructure**. Determine the capacity of any existing wired networks that can interface the access points or mesh nodes. Most buildings have Ethernet and in some cases optical fiber networks. Check on how much of the existing networks can be made available for supporting the wireless network.

5. **Identify coverage areas**. On the facility diagram or city map, indicate all areas where coverage is needed, such as offices, hallways, stairwells, utility rooms, bathrooms, break rooms, patios, parking garages, and elevators. Also, identifying where users will not wireless coverage is important to avoid wasting time surveying unnecessary areas.

6. **Determine preliminary access point locations**. By considering the location of wireless users and range estimations of the wireless LAN products you're using, approximate the locations of access points that will provide adequate coverage throughout the user areas.

7. **Verify access point locations**. This is when the site survey testing begins. Most wireless LAN vendors provide wireless site survey software that identifies the associated access point, data rate, signal strength, and signal quality. Alternately, you can use a third party site survey tool available from several different companies, such as AirMagnet, Berkeley Varitronics Systems, and Ekahau.

8. **Document findings**. Once you're satisfied that the location of access points you've identified will provide adequate signal coverage, document your findings on the facility diagrams by depicting the location of each access point. The installers will need this information.

LO2.2 – Identify Security requirements

- Content/Topic 1: Identification of security requirements.

Network security is important for home networks as well as in the business world. Most homes with high-speed internet connections have one or more wireless routers, which could be exploited if not properly secured. A solid network security system helps reduce the risk of data loss, theft and sabotage.

Network security is a set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data using both software and hardware technologies. The followings are the security requirements.

✓ **Authentication**: Authentication is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. It is a process in which the credentials provided are compared to those on file in a database of authorized users' information on an authentication server.

- If the credentials match, the process is completed and the user is granted authorization for access.

Authorization: It is the process of an administrator granting rights and the process of checking user account permissions for access to resources

Authentication factors:

- **Knowledge factors authentication:** The use of personal identification number (PIN), a user name, and password or the answer to a secret question.
- **Possession factors authentication** The use of items that the user has with them, typically a hardware device such as a security token or a mobile phone used in conjunction with a software token.
- **Inherence factors authentication**: consisting of elements that are integral to the individual in question, in the form of biometric data.
- **Two factors authentication**: Consisting what you have and what you know. For example, ATM and Password.

✓ **Confidentiality**: Confidentiality refers to protecting **information** from being accessed by unauthorized parties. The information being sent across the **network** transmitted in such a way that only the intended recipient(s) can read it.

✓ **Auditing**: Wireless auditing is a process of verification by the security **auditor** which is done to find out how secure the **wireless network** of your company is which is executed with an **audit** of the accessible **wireless networks**.

LO2.3 – Identify tools, equipment and materials used in WLAN

- Content/Topic 1: Identification of tools, equipment and materials used in WLAN.

- **Spectrum analyzer**

A **spectrum analyzer** measures the magnitude of an input signal versus frequency within the full frequency range of the instrument. The primary use is to measure the power of the spectrum of known and unknown signals or a **spectrum analyzer** is a device that displays signal amplitude (strength) as it varies by signal frequency. The frequency appears on the horizontal axis, and the amplitude is displayed on the vertical axis.

- **Protocol analysis software**

A **protocol analyzer** is a tool (hardware or software) used to capture and analyze signals and data traffic over a communication channel. Such a channel varies from a local computer bus to a satellite link, that provides a means of communication using a standard communication **protocol** (networked or point-to-point).

- **Laptop with PC Card and utilities**

A **PC Card** (previously known as a PCMCIA **card**) is a credit **card**-size memory or I/O device that fits into a personal **computer**, usually a notebook or laptop **computer**. Probably the most common use of a **PC Card** is the telecommunications modem for notebook computers.

- **Access point**

An **access point** is a device, such as a wireless router, that allows wireless devices to connect to a **network**. Most **access points** have built-in routers, while others must be connected to a router in order to provide **network access**.

- **Antennas**

An **antenna** is the interface between radio waves propagating through space and electric currents moving in metal conductors, used with a **transmitter** or **receiver** in transmission, or an antenna is a transducer that converts radio frequency (RF) fields into alternating current or vice versa. There are both receiving and transmission antennas for sending or receiving radio transmissions.

- **Batteries**

An electric **battery** is a device consisting of one or more electrochemical cells with external connections provided to power electrical devices such as flashlights, smartphones, and **electric cars.**

- **Binoculars**

Binoculars or **field glasses** are two telescopes mounted side-by-side and aligned to point in the same direction, allowing the viewer to use both eyes (binocular vision) when viewing distant objects (zooming).

- **Communication devices**

A **communication device** is a hardware **device** capable of transmitting an analog or digital signal over the telephone, other **communication** wire, or wirelessly. ... Other examples of **communication devices** include a network interface card (NIC), Wi-Fi **devices**, and an access point

- **Camera**

A camera is an optical instrument for recording or capturing images, which may be stored locally, transmitted to another location, or both. The images may be individual still photographs or sequences of images constituting videos or movies.

- **Measuring devices**

A measuring instrument is a device for measuring a physical quantity. In the physical sciences, quality assurance, and engineering, measurement is the activity of obtaining and comparing physical quantities of real-world objects and events.

- **Marking tape**

This is an instrument used to mark hazards, divide spaces or provide directions.

- **Rolling carts**

This is a vehicle with either two or four wheels, pulled by horse and used for carrying instruments.

- **Mounting tools and devices**

It depends on a lot of things like:

- Home size
- Home construction type
- Where you regularly use Wi-Fi
- Layout of your home
- Placement of your Wi-Fi points

The bigger your house, the more add-on points you'll need to have whole-home Wi-Fi coverage

LO2.4 – Design and interpret Building blueprint.

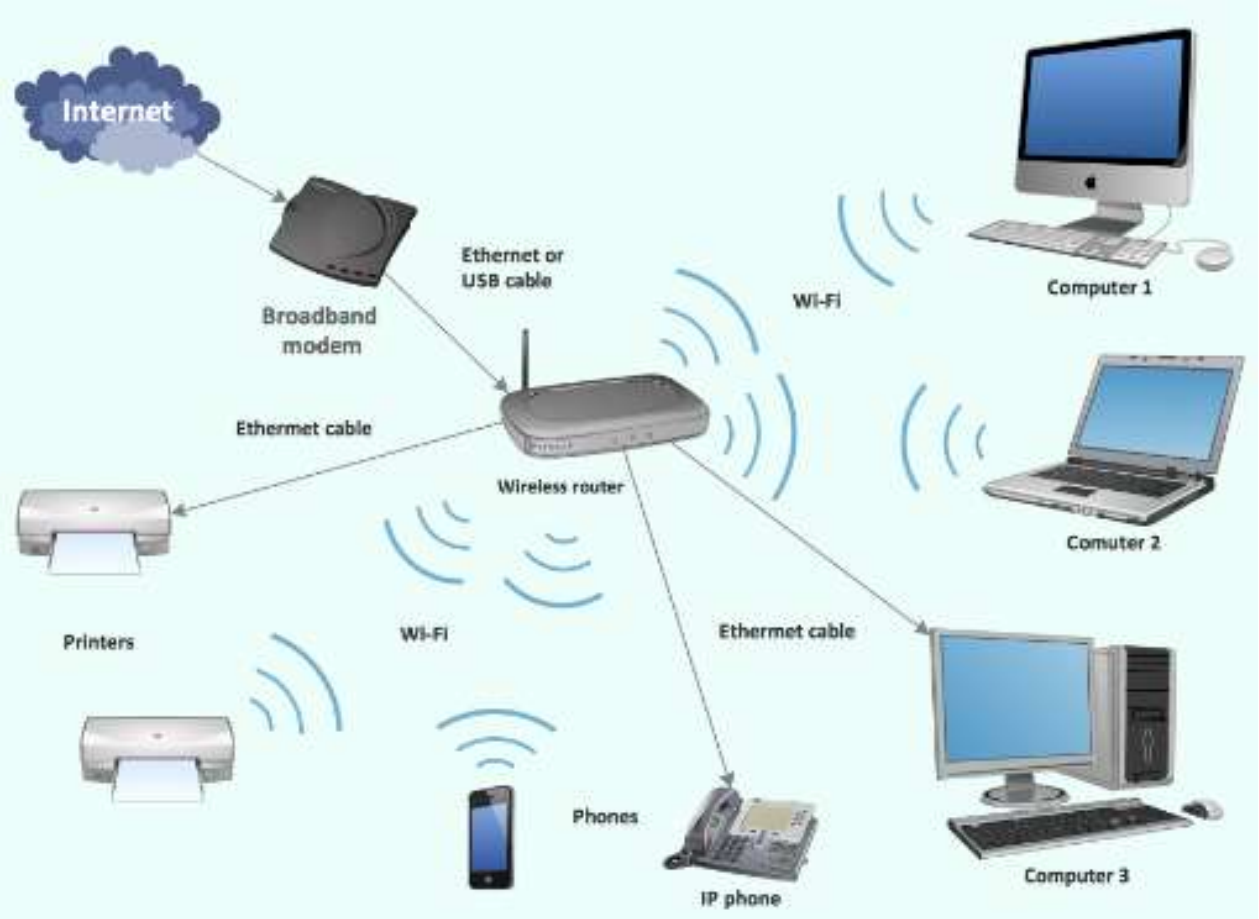
- Content/Topic 1: Designing and interpreting building blueprint

When **designing** a **wireless network**, it is necessary to consider various factors including the nature of the site, point-to-point bridging, WLAN roaming, applications of the **wireless network**, the number of users, construction materials, types and capabilities of **wireless** client devices and the infrastructure devices.

Criteria for Wi-Fi design and capacity planning include:

- Cabling requirements
- Number of rooms
- New builds vs. remodels
- Hardware needs
- IT resources (hiring agencies vs. in-house staff)
- Ongoing maintenance and upgrades

Referring to the below network diagram, draw a schematic diagram of your school network system using Edraw max, Packet Tracer, or VisualRF.



LO3.1 – **Implement WLAN**

- Content/Topic 1: Installation, configuration and managing WLAN devices

WLAN Devices are the devices that can serve a variety of function depending on where in the system they reside.

a. **Access points.**

An **access point** is a device, such as a wireless router, that allows wireless devices to connect to a network. Most **access points** have built-in routers, while others must be connected to a router in order to provide network **access**.

Tips for Your Wireless Access Point Installation:

- Understand all of your network requirements
- Choose the right equipment for your wireless network
- Be aware of the network limitations of your devices
- Consider the various types of cables you will need to use
- Be aware of nearby interference that can impact your wireless access point installation
- Select a proper location for your wireless access point
- Measure signal strength before making final access point placements

To install a wireless access point, turn off your computer and modem and follow these steps:

- Connect the Ethernet port of your cable modem or router to your wireless access point's Internet (or WAN) port using an Ethernet network cable.
- Connect your wireless access point to your computer using an Ethernet network cable.
- Turn on your DSL or cable modem and wait about two minutes.
- Connect the power adapter to your wireless access point, plug it into an electrical outlet, and wait about one minute.
- Turn on your computer.

To configure Access point, follow these steps:

- Open the access point's web-based setup page by entering the default IP Address on the Address bar then press **[Enter]**. If a new window prompts for credentials, leave the **User name** blank and enter "admin" as your **Password** then click **OK**.

- On the web-based setup page, click on **Wireless**.
- Enter the **Network Name (SSID)**. The **SSID Broadcast** should be set to **Enabled** so that wireless devices will be able to detect the wireless network of your Linksys access point.
- Click **Wireless Security** and select your desired **Security Mode**.
- Enter your desired password in the **Passphrase** field.
- Click **Save changes**

b. **Enterprise WLAN switches and controllers.**

These are the devices, which can be standalone **switches** or integrated into a blade on an enterprise class **switch**, are useful for the management and control of **WLAN** access points. A WLAN controller manages wireless network access points that allow wireless devices to connect to the network. It takes the bandwidth coming from a router and stretches it so that many devices can go on the network from farther distances away.

Setting up Cisco Wireless Controller using Cisco WLAN Express (Wired Method):

- Connect a laptop's wired Ethernet port directly to the Service port of the WLC. The port LEDs blink to indicate that both the machines are properly connected.
- Configure DHCP option on the laptop that you have connected to the Service port. This assigns an IP address to the laptop from the WLC Service port 192.168.1.X, or you can assign a static IP address 192.168.1.X to the laptop to access the WLC GUI; both options are supported.
- Open any supported web browsers and type http://192.168.1.1 in the address bar.
- Create an administrator account by providing the name and password. Click **Start** to continue.
- In the **Set Up Your Controller** dialog box, enter the following details:
    - System Name for the WLC
    - Current time zone
    - NTP Server (optional)
    - Management IP Address
    - Subnet Mask
    - Default Gateway
    - Management VLAN ID—If left unchanged or set to 0, the network switch port must be configured with a native VLAN 'X0'

- In the **Create Your Wireless Networks** dialog box, in the **Employee Network** area, use the checklist to enter the following data:
    - Network name/SSID
    - Security
    - Pass Phrase, if Security is set to WPA/WPA2 Personal
    - DHCP Server IP Address—If left empty, the DHCP processing is bridged to the management interface.
- (Optional) In the **Create Your Wireless Networks** dialog box, in the **Guest Network** area, use the checklist to enter the following data:
    - Network name/SSID
    - Security
    - VLAN IP Address, VLAN Subnet Mask, VLAN Default Gateway, VLAN ID
    - DHCP Server IP Address—If left empty, the DHCP processing is bridged to the management interface.
- In the **Advanced Setting** dialog box, in the **RF Parameter Optimization** area, do the following:
    - Select the client density as Low, Typical, or High.
    - Configure the RF parameters for RF Traffic Type, such as Data and Voice.
    - Change the Service port IP address and subnet mask, if necessary.
- Click next
- Review your settings and then click **Apply** to confirm.

c. **Remote office WLAN switches controllers**

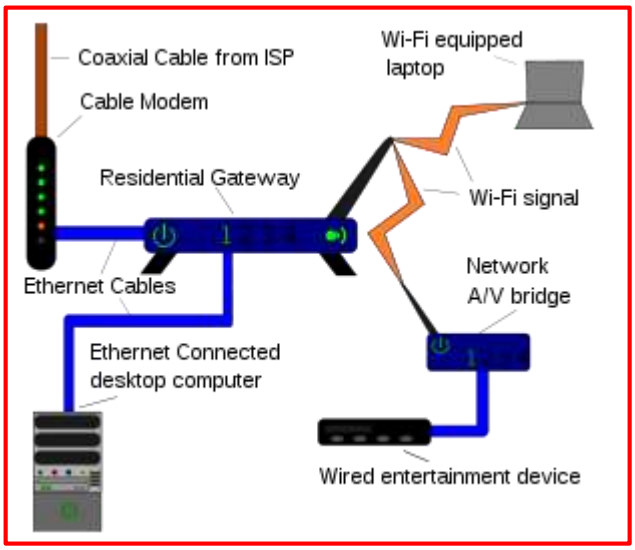
These are the devices, which can be standalone **switches** or integrated into a blade on an enterprise class **switch**, are useful for the management and control of **WLAN** access points. A WLAN controller manages wireless network access points that allow wireless devices to connect to the network. It takes the bandwidth coming from a router and stretches it so that many devices can go on the network from farther distances away.

d. **Power over Ethernet injectors and switches**

Power over Ethernet switch is all in one box in which no additional devices and the port on it can be used to manage both network and power.

Power over Ethernet injector is a device used to add PoE capability to non-PoE network link.

e. **WLAN bridges**



A **wireless bridge** is a type of networking hardware device that enables the connection of two different local area network (LAN) segments by **bridging** a **wireless** connection between them

Setting up WLAN Bridge

- **Position the bridge.** Place the wireless bridge within range of your wireless router's signal, and also within a cable's length of your wired devices.
- **Connect the bridge to your network**. If your router supports Wi-Fi Protected Setup, or WPS, setup is easy.
- **Plug in network devices.**

f. **Residential WLAN gateways**

It is a small consumer-grade router, which provides network access between wireless local area network (WLAN) hosts to a wireless wide area network (WAN) via a modem.

How do I setup a wireless gateway?

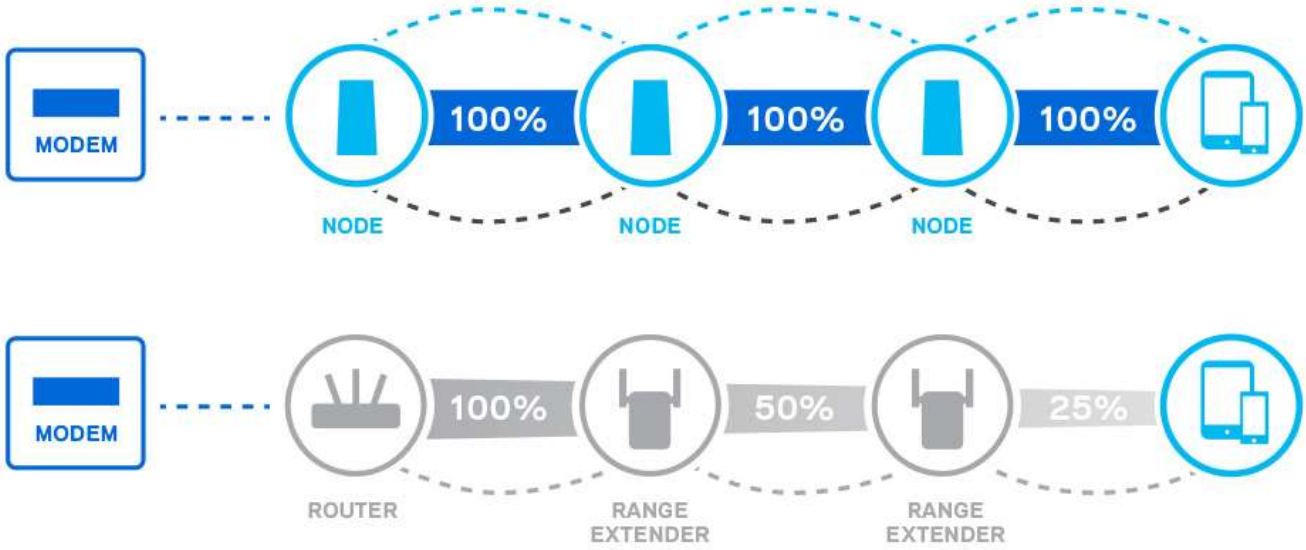
- Place your wireless router.
- Configure your wireless router gateway.
- Connect your gateway to your new router.
- Change your wireless router's admin password.
- Update the router's firmware.
- Establish a password for your Wi-Fi network.
- Enjoy your Wi-Fi network!

g. **Enterprise encryption gateway**

It is a layer 2 encryption device, similar to VPN, that allows for strong authentication and encryption for data across a wireless medium.

h. **WLAN mesh routers**

Mesh WiFi or Whole Home WiFi systems consists of a main router that connects directly to your modem, and a series of nodes (like WiFi Range extender), placed around your house for full WiFi coverage. They are all part of a single wireless network and share the same SSID and password, unlike traditional WiFi routers.



Before you install your mesh network, prepare for home for optimal results:

- **Internet coverage area**: A typical router offers much greater distance line-of-sight than when the signal must pass through dense objects like brick walls or metal objects. Buy as many mesh nodes as you need to cover your network's intended square footage, accounting for architectural barriers to signal propagation.
- **Router location**: Find the ideal location for your router. Usually, this location is in the center of the house, but not near an obstruction like a fireplace.
- **Node location**: Find the best location in your rooms for each satellite node. Nodes connect to electrical outlets. They should also be away from possible sources of interference, such as cordless phones and microwave ovens.
- **Mounting nodes**: If possible, measure a place to mount your node where it'll be out of the way. Nodes that need to reach through ceilings should be placed higher up, while nodes that need to reach through floors should be lower down.
- **Mesh Network specifications**: Examine the specifications of each mesh network you're considering. Pay close attention to the maximum range of each satellite node, and plan node placement to be, at most, two-thirds of that distance, if possible. You can always add more nodes to the network as needed.

How to Setup a Mesh Network?

Although each mesh-network vendor's setup process differs in detail, they all follow the same general procedure:

- After you've chosen a system, download its app to your phone.
- Unplug your router and connect the main node to it using an Ethernet cable. Reconnect your router and let it and the main node power up.
- You'll be prompted to log into your account with the mesh network or create one if you don't currently have one.
- Scan the QR code on the bottom of the main node, or input a serial number, to link your account and the main node.
- Offer, as prompted, a name or location for the main node. Indicate the number of satellite nodes. Don't worry if you overestimate or underestimate it, as you can add nodes later.
- Plug in the nodes one at a time. As each node is added, you'll be asked which room of the house it's located in.
- After you've added all your planned nodes, go to each room of your house and any outdoor areas and check your network speed.

- Content/Topic 2: Installation, configuration and managing WLAN client devices

WLAN Client Devices are the devices that server the specific function in the network.

A. PC Cards:

These are the type of removable computer peripheral that used either to provide a computer with extra storage, or to give a machine additional input and output capabilities.

- **NIC (Network Interface Card)**

NIC is also referred to as an Ethernet card and network adapter. It **is** an expansion card that enables a computer to connect to a network; such as a home network, or the Internet using an Ethernet cable with an RJ-45 connector.

- **WNIC**

A **wireless network interface controller** (**WNIC**) is a network interface controller which connects to a wireless radio-based computer network, rather than a wired network, such as Token Ring or Ethernet.

<u>To install PC Cards, follow the following steps:</u>

- Shutdown the computer.
- Open up the computer case.
- Remove the PC card slot cover.
- Insert the new PCI card.
- Fasten the PCI card to the case with the screw in the slot cover.
- Carefully attach any internal or external cables between the PCI card and the hardware peripherals.
- Close the computer case.
- Power up the computer.

<u>To configure Advanced Wi-Fi Adapter in Windows 10</u>

- In the **Search** box, type ***Device Manager***.
- Touch or click **Device Manager** (Control Panel).
- In the Device Manager window, touch or click the arrow sign next to **Network Adapters**.
- Double-tap or double-click the Intel Wi-Fi, Intel PRO, Wireless or Centrino listing.
- Touch or click the **Advanced** tab. **Note**: Depending on the Wireless Adapter installed, some of these options may not be available.
- In the Property: box, touch or click **802.11n Channel Width for 2.4GHz** and select **Auto** from the drop-down menu under Value.
- In the Property: box, touch or click **802.11n Channel Width for 5.2Ghz** and select **Auto** from the drop-down menu under Value.
- In the Property: box, touch or click **802.11n Mode** and select **Enabled** from the drop-down menu under Value.
- In the Property: box, touch or click **Fat Channel Intolerant** and select **Disabled** from the drop-down menu under Value.

- In the Property: box, touch or click **Roaming Aggressiveness** and select **1. Lowest** from the drop-down menu under Value. **Note**: This setting is suggested for home wireless networks. When you are on a business network and move from place to place, the setting should be set to 3. Medium.
- In the Property: box, touch or click **Intel® Throughput Enhancement or Throughput Booster** and select **Disabled** from the drop-down menu under Value. **Note**: When you only have one device on the wireless network or are streaming video, you may want to enable this feature. However, this prevents other computers on your network from having equal access to the wireless network.
- In the Property: box, touch or click **Transmit Power** and select **5. Highest** from the drop-down menu under Value.
- In the Property: box, touch or click **Wireless Mode** and select the highest number available from the drop-down menu under Value.
- Touch or click the **Power Management** tab.
- Make sure the check box to the left of **Allow the computer to turn off this device to save power**, is unchecked.
- Click **OK**

B. PCI and Mini–PCI cards

PCI stand for "Peripheral Component Interconnect." **PCI** is a hardware bus **used** for adding internal components to a desktop computer. For example, a **PCI card** can be inserted into a **PCI** slot on a motherboard, providing additional I/O ports on the back of a computer. Each card required an open slot on the motherboard and a removable panel on the back of the system unit. Adding PCI cards was an easy way to upgrade a computer, since you could add a better video card, faster wired or wireless networking, or add new ports, like USB 2.0. The installation of PCI and Mini-PCI cards is the same as other card, the difference is configurations which is specific to the Cards.

C. Wireless presentation gateways

WPG enables users to connect over 802.11b/g/n to send content from PCs and laptops to projectors or any display with a standard VGA input. Users can wirelessly play multimedia files, present office documents, and mirror the screen from the desktop directly to the projector or display.

D. USB

A Universal Serial Bus (**USB**) is a common interface that enables communication between devices and a host controller such as a personal computer (PC). It connects peripheral devices such as digital cameras, mice, keyboards, printers, scanners, media devices, external hard drives and flash drives.

E. Compact Flash

A **CompactFlash** card (**CF** card) is a memory card format developed by SanDisk in 1994 that uses **flash** memory technology to store data on a very small portable device. It has no moving mechanical parts and **does** not need a battery to retain data.

F. SD devices

consist of a **SD Card** (Secure Digital **Card**) is an ultra-small flash **memory card** designed to provide high-capacity **memory** in a small size. **SD cards** are **used in** many small portable devices such as digital video camcorders, digital cameras, handheld computers, audio players and mobile phones.

LO3.2 – **Apply security to the technology applied**

- Content/Topic 1: Identification and preventing WLAN Security Attacks

Wireless attack is a malicious action against wireless system information or wireless network. The followings are the examples of Wireless security attacks.

- **Eavesdropping**

Occurs when an attacker receives a data communication stream and record and analyze it only. In eavesdropping, the received communication stream resent without any modification. This also called passive attack.

- **Hijacking**

Hijacking is a type of network security attack in which the attacker takes control of a communication.

- **Man–in–the–middle**

M*an*-**i**n-**t**he-**m**iddle *attack* is an active Internet attack where the person attacking attempts to intercept, read or alter information moving between two computers.

- **Denial of service (DoS)**

Denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

- **Management interface exploits**

Management interface is a network interface dedicated to configuration and management operations. Management interfaces are typically connected to dedicated out of band management networks (either VPNs or physical networks), and non-management interfaces are not allowed to carry device or network management traffic. This greatly reduces the attack surface of the managed devices, as external attackers cannot access management functions directly, and thus improves network security.
In some cases, serial ports are used to access the command line interface directly, avoiding transport over a generic network stack completely, providing a further layer of isolation from network attacks.

- **Encryption cracking**

Network **encryption cracking** is the breaching of network encryptions (e.g., WEP, WPA, ...), usually through the use of a special **encryption cracking** software. It may be done through a range of attacks (active and passive) including injecting traffic, decrypting traffic, and dictionary-based attacks.
in **active attacks** the attacker intercepts the connection and modifies the information. Whereas, **in a passive attack**, the attacker intercepts the transit information with the intention of reading and analyzing the information not for altering it.

- ➔ Potential threats from **Passive attacks** can be eliminated by implementing good network encryption
- ➔ **Active attacks** can be prevented by using Firewalls and IPS (Intrusion Prevention Systems).

- **Authentication cracking**

Also called "**Password cracking**" is the process of attempting to gain unauthorized access to restricted systems using common passwords or algorithms that guess passwords. In other words, it is an art of obtaining the correct password that gives access to a system protected by an authentication method.

There are a number of **techniques that can be used to crack passwords**. We will describe the most commonly used ones below;

- **Dictionary attack**– This method involves the use of a wordlist to compare against user passwords.

- **Brute force attack**– This method is similar to the dictionary attack. Brute force attacks use algorithms that combine alpha-numeric characters and symbols to come up with passwords for the attack. For example, a password of the value “password” can also be tried as p@$$word using the brute force attack.
- **Rainbow table attack**– This method uses pre-computed hashes. Let’s assume that we have a database which stores passwords as md5 hashes. We can create another database that has md5 hashes of commonly used passwords. We can then compare the password hash we have against the stored hashes in the database. If a match is found, then we have the password.
- **Guess**– As the name suggests, this method involves guessing. Passwords such as qwerty, password, admin, etc. are commonly used or set as default passwords. If they have not been changed or if the user is careless when selecting passwords, then they can be easily compromised.
- **Spidering**– Most organizations use passwords that contain company information. This information can be found on company websites, social media such as Facebook, Twitter, etc. Spidering gathers information from these sources to come up with word lists. The word list is then used to perform dictionary and brute force attacks.

- **MAC spoofing**

A **MAC spoofing attack** is where the intruder sniffs the network for valid **MAC** addresses and attempts to act as one of the valid **MAC** addresses. The intruder then presents itself as the default gateway and copies all of the data forwarded to the default gateway without being detected.

- **Peer–to–peer attacks**

It's when servers are flooded with connections from valid sources, and then the attacker sets up and tears down TCP connections. It's when an attacker exploits bugs in **peer**-to-**peer** servers to execute a DoS **attack**. It's when a network is flooded with malicious packets in order to overwhelm its bandwidth.

- **Social engineering**

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

LO3.3 – **Troubleshoot Local Area Network.**

- Content/Topic 1: Identification of Wireless LAN Testing Considerations

When planning the testing of a WLAN, consider the following forms of testing:

- **Signal Coverage Testing**

Signal coverage testing determines where client devices are able to satisfy coverage requirements. This testing may be part of performing a WLAN site survey or done after the network is installed to determine the as-installed signal coverage.

- **Performance Testing**

Performance testing determines whether the WLAN can satisfy user needs for using specific applications over the WLAN.

- **In-Motion Testing**

In-motion testing determines whether users can continue to make use of applications while roaming throughout the coverage areas, especially when the roaming requires handoffs between access points.

- **Security Vulnerability Testing**

Security vulnerability testing ensures that the WLAN implements required security mechanisms and offers sufficient protection to unauthorized access and passive monitoring.

- **Acceptance/Verification Testing**

After installing a WLAN, it is important to run a series of acceptance/verification tests to ensure that the WLAN satisfies all requirements. This is especially important if the organization is having a contractor install the WLAN.

- **Simulation Testing**

In some cases, such as when implementing a very large WLAN, it may be beneficial to simulate the behavior of the WLAN before actually installing it. This can provide helpful feedback when designing the system, especially if the WLAN will have critical performance requirements.

- **Prototype Testing**

Prototype testing involves implementing an individual function of the WLAN that is not well understood before deploying the complete system. For example, an organization may not be very familiar with 802.1X authentication systems and may benefit by implementing the 802.1X authentication in a lab environment with a limited number of test client devices.

- **Pilot Testing**

Before installing the WLAN across the entire organization, which may include numerous buildings and different applications, it is strongly advisable to install the system in a limited number of facilities (ideally one) and make that one work effectively first. After you work out all the problems, you can install the WLAN at the

remaining location without the need for extensive rework because the problems will likely have been solved during the pilot testing.

- Content/Topic 2: Test Documentation

- **Test Documentation**

At the conclusion of testing, produce a test report, that addresses the following elements:

- **Background**

Explain what is being tested and why the testing is being done

- **Test team**

Identify all people who were involved with the testing and their roles

- **Requirements summary**

Briefly describe the WLAN requirements and reference the requirements document for more details.

- **Test methods and tools**

Describe how the testing was accomplished and the tools that were used to collect the data.

- **Test results and analysis**

Include all applicable test data. Many test tools put data in a format that you can include in your test report. If this is too cumbersome for inclusion directly within the test report, reference applicable test files. Also, explain the results, including any underlying issues that might be causing problems.

- **Recommendations**

Explain what changes should be made to the network to counteract issues found during testing.

⚠ Thus, test documentation becomes a vital part of a WLAN. Managers and support staff can refer back to test reports in the future to better understand why changes were made to the network and what might be useful to fix future problems. As a result, be certain to fully document any testing that you do.

LO3.4 – Troubleshoot WLAN Problems

- Content/Topic 1: Troubleshooting Wireless Station Connection to AP

Troubleshooting is a skill learned through experience with trial and error. One methodology is to develop a process to check for symptoms, identify the problem, find the source of the problem, attempt a repair and check the results.

- **Can Any Wireless Stations Connect to the AP?**

When you troubleshoot problems with wireless stations, you must isolate whether the symptom is displayed on a single station or all stations. If the symptoms are the same with all stations, the problem can be the AP configuration, rather than the station.

- **Troubleshooting Wireless Stations**
    - ❖ Check the station's state:
    - Wireless network detected?
    - Signal interference?
    - Station associated?
    - ❖ Check the wireless NIC:
    - Properly installed?
    - Up-to-date drivers?
    - Enabled?
    - TCP/IP installed and set to receive a DHCP address?
    - ❖ Check the wireless LAN settings:
    - SSIDs are case sensitive
    - Station configuration
    - WLAN's security requirements Check the station's status on the AP

- **Wireless Network Detected**

The wireless station must be within range of the AP in order to receive a radio signal (RF energy) strong enough for a connection to occur and be maintained.

- **Signal Interference**

There are a number of factors which can play a role in radio signal interference. It could be caused by the antenna on the AP not being connected or properly installed. Building construction materials, such as steel and wood, and objects with high water content absorb RF energy and affect signal strength. Interference from devices such as microwave ovens and 2.4 MHz cordless phones can cause RF interference and should be considered when placing the AP. Stronger signals are not always better signals! In an enclosed area, radio signals that are excessively strong may be reflected (bounce off) off objects and cause multipath interference.

- **Site Survey**

A site survey is strongly recommended prior to installation of a wireless network and should be performed on the actual site under normal operating conditions. Such a survey is critical because the RF behavior varies with the physical properties of the site. You cannot accurately predict the behavior without doing a site survey. You

may face intermittent connectivity in certain locations or during certain environmental conditions. The intermittent connectivity can indicate that a site survey was not performed or that the site survey did not consider these factors and placement of the APs should be re-evaluated.

- **Station Status**

Use the Web user interface of the AP to view the wireless station status. Check station status to see if wireless stations are associated with the AP. The Event log of the AP also displays valuable information on why or why not a station may not be associating to the AP.

- **Using the Correct SSID**

SSIDs are case sensitive and some special characters are allowed (spaces), so verify that the station has an exact match for the WLAN's SSID configured on the AP.

- **Station Configuration**

Here you can verify that the SSID and the Wireless Network Key (if applicable) are configured exactly to match the configuration on the AP.

- **Correct Security Settings**

Another reason the wireless station may not be associating is the security settings. These must match exactly. For example, if you network requires static WEP keys and you don't have any configured, you will not be allowed to connect to the network. The reverse of this is also true: If your station has WEP configured and your network is wide open with no keys, most stations will not connect in this situation either. Of course, these rules also apply for more advanced security schemes.

- **TCP/IP Protocol Installed and Configured**

The AP can also be configured to work with a DHCP server in order to provide the IP addresses to the wireless stations. Check and verify the wireless network connection is installed and configured properly to receive an IP address from a DHCP server.

Ensure the radio button for "Obtain an IP address automatically" is selected. This will allow the station to receive an IP address automatically from a DHCP server.

- Content/Topic 1: Troubleshooting AP Connection to Wired LAN

- **Port Configuration on Wired/Wireless**

There are two sides to every connection. This applies to the connection between the AP and the rest of the wired network as well. The speed and duplex capabilities should match as closely as possible. ProCurve

recommends allowing both ends of the connection to auto-negotiate speed and duplex settings. Give equal attention to the switch port to which the AP is connected and to the AP's Ethernet port.

- **Network Cable**

Physical connectivity between the AP and wired network is often overlooked, but is the basis of communications between the two networks. If you have intermittent connectivity or connectivity with errors, the cable connection may be loose or there is a possibility that the cable length is greater than the recommended Ethernet segment length.

Be sure that an AP is connected to a switch with a straight through cable. Do not exceed the Ethernet cable length recommendation of a Category 5e 10/100BASE−TX 100 m/328 ft. Interference occurs when you run a network cable near high power equipment. This interference is especially common when you run the cables in warehouses and factories. Replace the network cable if intermittent problems exist between the AP and the wired network.

- **Troubleshooting the AP**
  - ❖ Check the hardware and software:
    - Power operating & stable?
    - Up-to-date software image and configuration file?
    - Indicator LEDs
  - ❖ Check the radio:
    - Is the country code set (if applicable)?
    - Is the AP radio enabled?
    - Is the SSID enabled?
    - Is AP detection scanning turned off?
  - ❖ Check for mismatches in:
    - SSID (including case and spaces)
    - WEP key or WPA pre-shared key
    - Radio settings (frequency and speed)
    - Is the IP configuration in the same subnet as the wired switch connection?

- **Check for Power Issues with the AP**

If using the AC power adapter, ensure that the power source circuit is active, properly grounded and the power cable is securely plugged into the AC outlet and the back of the AP. If using Power over Ethernet (PoE), make sure the AP is connected to a switch which can provide the necessary power to the AP.

- **Check for Booting Issues with the AP**

In some cases, the AP fails to boot completely. This failure can happen if the software on the access point is corrupt. In order to resolve this issue, reinstall the software on the AP.

- **Check AP LED Behavior**

During the system initialization:

The Power LED first turns on immediately, then the Power, LAN, Radio 1, and Radio 2 LEDs turn on and off several times during phases of the initialization.

When the system initialization completes successfully:

• The Power LED remains on green.

• The LAN and Radio LEDs on the top of the access point go into their normal operational mode:

- If the RJ-45 network port and radio interfaces are connected to active network devices, the LEDs should be blinking at a rate proportional to the traffic rate. If there is no network activity, the LEDs should still be blinking at approximately 5 second intervals.
- If the RJ-45 network port is not connected to an active network device and the radio interfaces are disabled, the LEDs should be off.

If the LED display is different than what is described above, the system initialization has not completed correctly.

- **Check AP Has Correct IP Address**

If you cannot ping the AP, check the IP addresses that are assigned to the AP and wireless station. Make sure that they are in the same subnet. For example, if the IP address of the AP is 10.20.50.25 with a mask of 255.255.255.0, verify that the IP address of the station adapter is similar to 10.20.50.X with a mask of 255.255.255.0.

- **Check AP is Broadcasting the SSID**

The “broadcasting the SSID” setting allows you to choose whether wireless stations that do not specify an SSID are allowed to associate with the AP. When configuring a wireless LAN interface on the AP, ensure the Closed-System check box is unchecked.

Closed-System: Prohibits the broadcasting of the AP’s SSID, if enabled. The network name will also not be displayed in the List of Available Networks on a wireless station. (Default is disabled, allowing SSID broadcasting)

If you have communication problems and the access point Closed-System check box is checked (enabled), change the setting to uncheck the box and see if the wireless station can communicate. Leave the setting as unchecked for the duration of this troubleshoot.

- **Check AP Radio Settings**

The data rate setting on the AP radio defines the rate at which the AP transmits information.

When you configure the AP radio, you must consider the type of wireless stations that are present in the wireless network. If the AP has the radio mode set as an 802.11g radio, then only 802.11g wireless stations on the WLAN will be able to connect.

However, if you have a mixed environment of both 802.11b and 802.11g stations in a WLAN network, you must ensure that the AP radio mode is set to 802.11b/g. When working in its mixed “b/g” mode, the AP will experience reduced data throughput, even if there are no 802.11b stations active in the network.

Learning Unit 4 – Document the work done.

LO4.1 – Document on network status

Content/Topic 1: Description of network status before

- **Status of network infrastructure**

Network infrastructure refers to all of the resources of a **network** that make **network** or internet connectivity, management, business operations and communication possible.

The entire network infrastructure is interconnected, and can be used for internal communications, external communications or both. A typical network infrastructure includes:

- Networking Hardware:
  - Routers
  - Switches
  - LAN cards
  - Wireless routers
  - Cables
- Networking Software:
  - Network operations and management
  - Operating systems
  - Firewall
  - Network security applications
- Network Services:
  - T-1 Line
  - DSL
  - Satellite
  - Wireless protocols
  - IP addressing

When you are making a report you have to describe or to make a good explanation on how the network was before you start to work.

- **Describe problems found**

To describe the network problem found is to explain the Status of network infrastructure and describe problems of network to be handled.

Simple network troubleshooting steps that help to diagnose and refine the problem.

- **Check the hardware**. Check all your hardware to make sure it's connected properly, turned on, and working.
- **Use ipconfig**. Open the command prompt and type "ipconfig" (without the quotes) into the terminal. The Default Gateway (listed last) is your router's IP. Your computer's IP address is the number next to "IP Address." If your computer's IP address starts with 169, the computer is not receiving a valid IP address. If it starts with anything other than 169, your computer is being allocated a valid IP address from your router.

  Try typing in "ipconfig /release" followed by "ipconfig /renew" to get rid of your current IP address and request a new one. This will in some cases solve the problem. If you still can't get a valid IP from your router, try plugging your computer straight into the modem using an Ethernet cable. If it works, the problem lies with the router.
- **Use ping and tracert**. If your router is working fine, and you have an IP address starting with something other than 169, the problem's most likely located between your router and the internet. At this point, it's time to use the **ping** tool. Try sending a ping to a well-known, large server, such as Google, to see if it can connect with your router. You can ping Google DNS servers by opening the command prompt and typing "ping 8.8.8.8"; you can also add "-t" to the end (ping 8.8.8.8 -t) to get it to keep pinging the servers while you troubleshoot. If the pings fail to send, the command prompt will return basic information about the issue.

  You can use the **tracert** command to do the same thing, by typing "tracert 8.8.8.8"; this will show you each step, or "hop," between your router and the Google DNS servers. You can see where along the pathway the error is arising. If the error comes up early along the pathway, the issue is more likely somewhere in your local network.
- **Perform a DNS check**. Use the command "nslookup" to determine whether there's a problem with the server you're trying to connect to. If you perform a DNS check on, for example, google.com and receive results such as "Timed Out," "Server Failure," "Refused," "No Response from Server," or "Network Is Unreachable," it may indicate the problem originates in the DNS server for your destination. (You can also use nslookup to check your own DNS server.)

- **Contact the ISP**. If all of the above turn up no problems, try contacting your internet service provider to see if they're having issues. You can also look up outage maps and related information on a smartphone to see if others in your area are having the same problem.
- **Check on virus and malware protection**. Next, make sure your virus and malware tools are running correctly, and they haven't flagged anything that could be affecting part of your network and stopping it from functioning.
- **Review database logs**. Review all your database logs to make sure the databases are functioning as expected. If your network is working but your database is full or malfunctioning, it could be causing problems that flow on and affect your network performance.

Content/Topic 2: Review of user manual and previous report

As the purpose of network documentation is to keep networks running as smoothly as possible while minimizing downtime when repairs are necessary.

Essential parts of network documentation include:

- Map of the entire network to include locations of hardware and the cabling that connects the hardware
- Server information such as data on the individual servers, schedules and locations of backups
- Software information such as current versions, dates, licensing and support
- Vendor and contractor information
- Service agreements
- Detailed record of problems and solutions: dated along with procedures and results

Notation that helps administrators remember key details are the basics of network documentation while visual representations assist in helping administrators understand how equipment and the notation relates to one another.

A user guide or user's guide, also commonly known as a manual, is a technical communication document intended to give assistance to people using a particular system. So maybe there are some other technicians came before you have to consult what they said, like the problems they faced and how they resolved those issues.

Having an expert review any existing *network implementation plan* document will definitely help identify any gaps or risks that may have not been highlighted. The *network implementation plan review* service provides this

additional level of diligence needed to ensure project tasks are optimally planned and deliver on the promise with minimum risk.

Content/Topic 3: Solving problem.

- **Suggestion of solutions on problems found**

Before you start trying to troubleshoot any issue, you want to have a clear understanding of what the problem is, how it came up, who it's affecting, and how long it's been going on.

By gathering the right information and clarifying the problem, you'll have a much better chance of resolving the issue quickly, without wasting time trying unnecessary fixes.

On this level, you have to suggest the solutions to the problem found by explaining clearly the task to be accomplished regarding to the network devices, equipment, and materials to be used.

- **Description of solution implementation**

Organizations demand reliable network maintenance support services that help to get their job done.

Solution implementation involves:

- Being committed to a solution.
- Accepting responsibility for the decision.
- Identifying who will implement the solution.
- Resolving to carry out the chosen solution.
- Exploring the best possible means of implementing the solution.

- **Description of procedures of the task accomplished**

Procedure is a sequence of steps that include preparation, conduct and completion of a task. Each step can be a sequence of activities and each activity a sequence of actions.

Procedures is needed when you have to perform the complex task or when the task is routine and you want it to be performed consistently. Procedures are driven by completion of the task; It includes:

- Meet with the teams responsible for the procedure
- Start with a short introduction
- Make a list of required resources
- Document the current procedure
- Add supporting media
- Include any relevant resources

- Check the procedure is accurate
- Test in a controlled environment
- Make improvements if necessary
- Deploy

Content/Topic 4: Network Devices, equipment and materials used

Having the right Network Devices, equipment and materials in place can simplify your network management responsibilities, helping you to keep your network running tip-top and your sanity in check.

While developing the report, you have to include the network devices, equipment and materials used. The following are the examples of network devices, equipment and materials that can be used:

- LAN Cable
- Connectors
- Crimping tools
- Krone tools
- UTP Connector
- Punch down tool
- Cable tester
- Coaxial cable
- USB Wireless interface
- Wireless pc card
- WAP
- ADSL Modem
- Cable modem
- Router
- Switch

Content/Topic 5: Description of the network status after work, Technical journal and recommendation report

A. Status of network after work

After your work, you have to describe current network status by showing clearly the problems solved with more explanation, and give recommendation for further usage.

B. Technical journal

The definition of **journal** is a **diary** you keep of daily events or of your thoughts or a publication dealing with a specific industry or field for example IT Field as computer network. An **example** of a **journal** is a **diary** in which you write about what happens to your network status and what you are thinking possible upgrading if there any clarification. (The terms "**journal**" and "diary" apply to a record of events that is maintained on a regular basis).

C. Recommendation Reports

A recommendation report is a paper that compares two or more computer network status and makes a recommendation about which is the best status. Because the status of the report is to recommend a course of action, it is called a recommendation report.

LO4.2 – Develop the design concept according to selected materials

Content/Topic 1: Reporting the work done.

Report Writing Format

Here are the main sections of the standard report writing format: Title Section – 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. ... Body – This is the main section of the report.

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

- **Title Section**: 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.
- **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.

LO4.3 – Write technical journal and recommendation

Content/Topic 1: Writing technical journal and recommendation

A **technical journal** is a document that describes the process, progress, or results of **technical** or scientific research or the state of a **technical** or scientific research problem. It might also include recommendations and conclusions of the research.

Template:

WORK REPORT OF A NETWORK TECHNICIAN

Company/Technician Address
Company /Technician Name: Website /Email address PO BOX : Office /Mobile Phone Contact : Company /Technician office Location:
Customer Address
Company/ Individual Person Name: Website /Email address PO BOX : Office /Mobile Phone Contact : Company /Individual Person office Location:
Status Before Work
User manual and previous report
Solutions on problems found
Solution and Implementation
procedures of the task accomplished

Network Devices, equipment and materials used
Status After Work **Observations /Recommendations**
Customer Verification Names: Signature /stamp Date:
Company /Technician Verification Name: Signature/stamp Date:

REFERENCES

- Jim Geier (2010). Designing and Deploying 802.11ac Wireless Networks. Cisco Press. Pp 273-403.
- Gordon Colbach (2017). Wireless Networking: Introduction to Bluetooth and WiFi. Independently published. Pp 27-87.
- Matthew S. Gast (2005). 802.11 Wireless Networks. The Definitive Guide, Second Edition. O'Reilly Media. Pp 187-317.
- Vangie Beal (2020), 802.11 IEEE wireless LAN standards, URL: https://www.webopedia.com/TERM/8/802_11.html Accessed on 12th October, 2020
- Samantha Albano (July 9, 2018), WiFi channels explained, URL: https://www.minim.co/blog/wifi-channels-explained Accessed on 13th October, 2020.
- Lawrence C. Miller (n.d), How to Install Your Wireless Access Point, URL: https://www.dummies.com/computers/computer-networking/wireless/how-to-install-your-wireless-access-point/ Accessed on 13th October, 2020
- Cisco Wireless Controller Configuration Guide, Release 8.0 (n.d), URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_010.html Accessed on 14th October, 2020
- Daniel Anglin Seitz (June 2020), How to Setup a Mesh Network, URL: https://www.lifewire.com/how-to-set-up-a-mesh-network-4690007 Accessed on 14th October, 2020
- Michael Brown (June 2017), How to set up a wireless router, URL: https://www.pcworld.com/article/249185/how-to-set-up-a-wireless-router.html Accessed on 14th October, 2020
- Fiona Hutcheson (August 2011), How to Extend Your Network with a Wireless Bridge, URL: http://blog.dlink.com/how-to-extend-your-network-with-a-wireless-bridge/ Accessed on 15th October, 2020
- Mark Kyrnin (June 2020), Installing a PCI Adapter Card, URL: https://www.lifewire.com/pci-adapter-card-installation-833860 Accessed on 15th October, 2020
- Wireless LAN Operations (n.d), URL: https://www.ii.pwr.edu.pl/~kano/course/module8/#8.0.1.1 Accessed on 16th October, 2020
- Testing a Wireless LAN (n.d), https://cdn.ttgtmedia.com/searchNetworking/downloads/17_1587058898_ch17.pdf Accessed on 16th October, 2020

- Troubleshooting_WLAN_Connectivity (n.d), URL: http://www.idc-online.com/technical_references/pdfs/data_communications/Troubleshooting_WLAN_Connectivity.pdf Accessed on 16th October, 2020.
- Nam Hoang (2018), Configure the Wireless Adapter Settings for Optimal Performance, URL: https://support.cyberpowerpc.com/hc/en-us/articles/360014067574-Configure-the-Wireless-Adapter-Settings-for-Optimal-Performance Accessed on 17 October, 2020.