TVET CERTIFICATE IV in NETWORKING

Wireless Network indoor

NEWWI401

Setup Wireless Network Indoor

Competence

Credits: 12

Learning hours:

120

Sector: ICT

Sub-sector: Networking

Module Note Issue date: July, 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: 89

Learning Unit 1 - Concepts of Wireless Network

LO1.1 – Description of RFID technology and its functionality

- Content/Topic 1: Introduction to RFID Technology

Radio frequency identification (RFID) is a fast developing technology that provides wireless identification and tracking capacity. Nowadays, many applications such as preventing theft of automobiles and merchandise, collecting tolls without stopping, gaining entrance to buildings, controlling access of vehicles to gated communities, corporate campuses and airports, providing ski lift access, tracking library goods, asset identification, retailing and supply chain management, animal tracking, among others, take advantage of RFID systems.

RFID is generally characterized by the use of simple devices on one end, called tags of transponders, and more complex devices on the other end of the link, called readers or interrogators. The tags are made up of an antenna and an application specific integrated circuit chip, contains memory where data is stored. They include a matching network located in between the antenna and the chip, to achieve proper impedance matching. The readers are composed of an antenna, radio frequency module, which is responsible for communicating with a host computer or controller connected to the reader in order to centrally process information coming from readers. The Figure bellow shows the schematic of a typical RFID system.

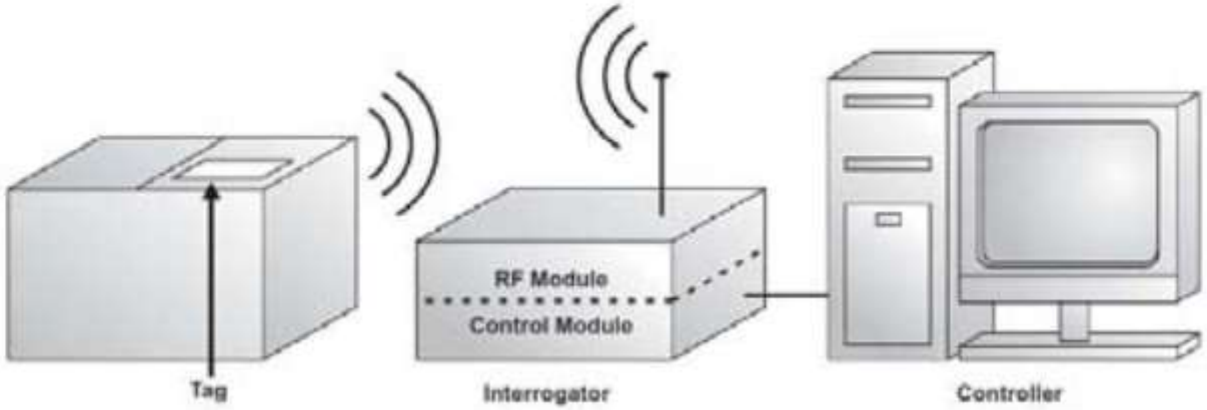


Figure1: Basic building blocks of an RFID system with a host controller

RFID systems data is transferred in one direction, from the tag to the reader or read-write (two ways communication).

RFID Tags

Tags are one of the elementary units of RFID system. They are attached to the objects or products that are to be identified. A tag consists of an integrated circuit and a coupling element, i.e. antenna. Depending on the type of the tag, it may or may not have an on-board power source. The type of tags defines the RFID variants. The choice of tags also outlines the area of application for which the RFID system is chosen for.

Based on their power usage, there are three types of RFID tags which are briefly presented in the following sections

Active Tags

Active tags are supported by ultra-high frequency and microwave systems. They are the most expensive ones due to their read and write capability, larger memory and on-board power source. The on-board power source accommodates the microchip and transceiver. Active tags can communicate independently and they do not have to rely on the reader's emitted power for communication. Active systems have a read range of more than 100 meters.

Semi-Passive Tags

Semi-passive tags are supported only by ultra-high frequency systems. Like active tags, semi passive tags also have an on-board power source but only used for powering the tag's microchip. They have to rely on the reader for data transmission. This type of tag is smaller compared to the active ones and has a shorter read range of 60 to 80 meters.

Passive Tags

This variant is supported by the low frequency, high frequency, ultra-high frequency and microwave systems. Passive tags have no internal power source. They have to rely solely on the reader's energy in order to energize and transmit. It has the smallest read range from 0.1 to 5 typically 7 meters. Passive tags are the cheapest, thinnest and most flexible among the three which makes them very popular in the supply chain and retail industry.

RFID Reader

In an RFID system, a reader is one of the most important building blocks. A reader is basically a transceiver to interrogate the tags and read the information stored within. It has computational resources comparable to a computer. It generates and transmits electromagnetic wave through its antenna, internal or external to the reader and couples with the tags. It energizes and supplies power for data transmission to the tags if necessary. Readers can be classified in terms of mobility, i.e. stationary and mobile or handheld readers. They are generally connected to a computer or in the case of handheld readers a mobile computer can be built in the device providing a user interface to the user. For more sophisticated data, processing, it sends the received information to the data processing subsystem or back end server. Hence the reader leaves most of the information and computational work for the connected back end server.

Data Processing Subsystems

Irrespective of the type of the technology, i.e. the type of the readers and the tags, a back end database or server is used to facilitate the system operation. A backend system pools collected data together to enable big data analytics and drive business operations by interfacing with other resource management software.

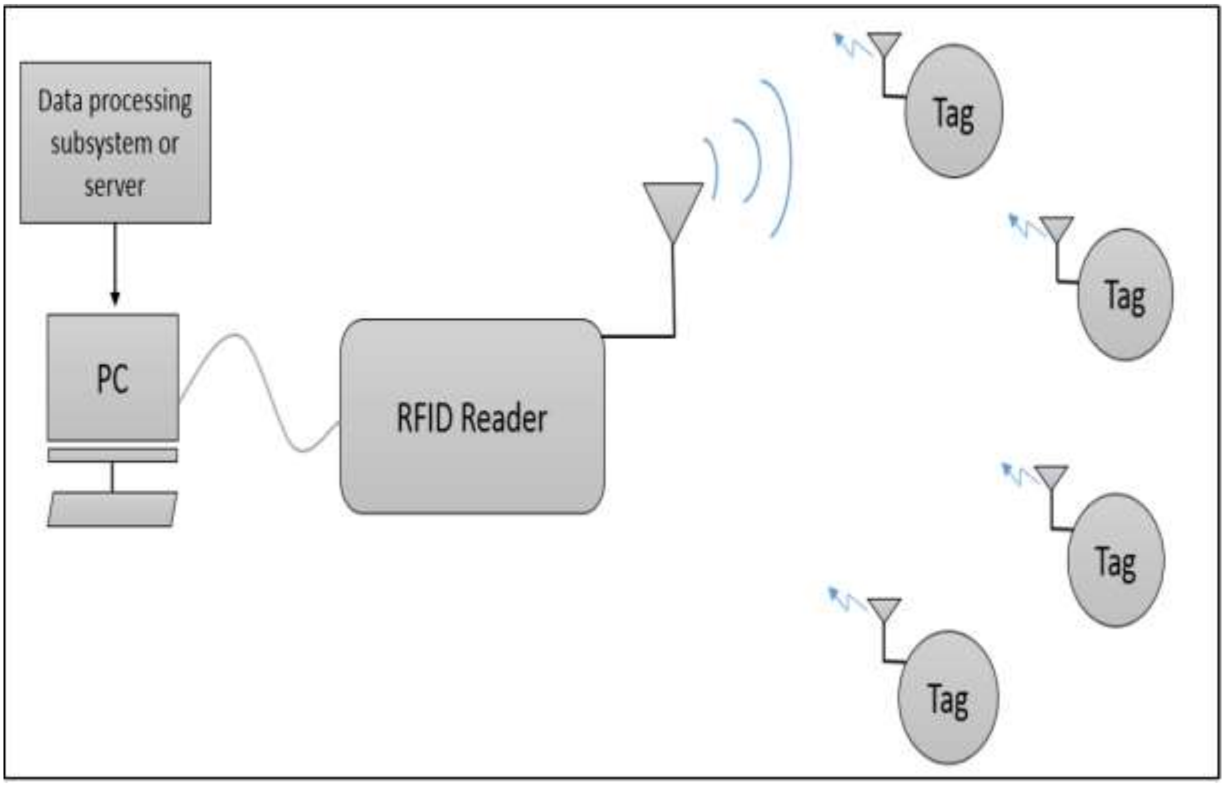


Figure2: Basic operation of RFID system.

- Content/Topic 2: Use of wireless

✓ **Why have Wireless LANs become so popular.**

An increasing number of LAN users are becoming mobile. These movable users require that they are connected to the network regardless of where they are because they want simultaneous access to the network. This makes the use of cables, or wired LANs, impractical if not impossible.

Wireless LANs are very easy to install. There is no requirement for wiring every workstation and every room. This ease of installation makes wireless LANs inherently flexible. If a workstation must be moved, it can be done easily and without additional wiring, cable drops or reconfiguration of the network.

Another advantage is its portability. If a company moves to a new location, the wireless system is much easier to move than ripping up all of the cables that a wired system would have snaked throughout the building. Most of these advantages also translate into monetary savings.

- ✓ **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, or office building. This gives users the ability to move around within the area and remain connected to the network.

Wireless network refers to any type of computer network that uses wireless (usually, but not always radio waves) for network connections. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

- ✓ **Comparing a WLAN to a LAN**

A wired network is described as an interconnection that involves cables which establish a connection between devices on the network. Data is transferred from one device to another using Ethernet cables.

Wireless networks are configurations that operate on radio frequency or microwave signals. The radio signals allow wireless enabled devices to communicate with one another without having to be connected to the network via an Ethernet cable.

- Content/Topic 3: Description of WLANs Standards

The 802.11 WLAN Standards

Origins and Evolution

The development of wireless LAN standards by the IEEE began in the late 1980s, following the opening up of the three ISM radio bands for unlicensed use by the FCC in 1985, and reached a major milestone in 1997 with the approval and publication of the 802.11 standard. This standard, which initially specified modest data rates of 1 and 2 Mbps, has been enhanced over the years, the many revisions being denoted by the addition of a suffix letter to the original 802.11, as for example in 802.11a, b and g. The 802.11a and 802.11b extensions were ratified in July 1999, and

802.11b, offering data rates up to 11 Mbps, became the first standard with products to market under the Wi-Fi banner. The 802.11g specification was ratified in June 2003 and raised the PHY layer data rate to 54 Mbps, while offering a degree of interoperability with 802.11b equipment with which it shares the 2.4 GHz ISM band.

Table 1 summarizes the 802.11 standard's relentless march through the alphabet, with various revisions addressing issues such as security, local regulatory compliance and mesh networking, as well as other enhancements that will lift the PHY layer data rate to 600 Mbps.

Table 1: The IEEE 802.11 Standard Suite

Standard	**Key features**
802.11a	High speed WLAN standard, supporting 54 Mbps data rate using OFDM modulation in the 5 GHz ISM band.
802.11b	The original Wi-Fi standard, providing 11 Mbps using DSSS and CCK on the 2.4 GHz ISM band.
802.11d	Enables MAC level configuration of allowed frequencies, power levels and signal bandwidth to comply with local RF regulations, thereby facilitating international roaming.
802.11e	Addresses quality of service (QoS) requirements for all 802.11 radio interfaces, providing TDMA to prioritize and error-correction to enhance performance of delay sensitive applications.
802.11f	Defines recommended practices and an Inter-Access Point Protocol to enable access points to exchange the information required to support distribution system services. Ensures inter-operability of access points from multiple vendors, for example to support roaming.
802.11g	Enhances data rate to 54 Mbps using OFDM modulation on the 2.4 GHz ISM band. Interoperable in the same network with 802.11b equipment.
802.11h	Spectrum management in the 5 GHz band, using dynamic frequency selection (DFS) and transmit power control (TPC) to meet European requirements to minimize interference with military radar and satellite communications.

802.11i	Addresses the security weaknesses in user authentication and encryption protocols. The standard employs advanced encryption standard (AES) and 802.1x authentication.
802.11j	Japanese regulatory extension to 802.11a adding RF channels between 4.9 and 5.0 GHz.
802.11k	Specifies network performance optimization through channel selection, roaming and TPC. Overall network throughput is maximized by efficiently loading all access points in a network, including those with weaker signal strength.
802.11n	Provides higher data rates of 150, 350 and up to 600 Mbps using MIMO radio technology, wider RF channels and protocol stack improvements, while maintaining backward compatibility with 802.11 a, b and g.
802.11p	Wireless access for the vehicular environment (WAVE), providing communication between vehicles or from a vehicle to a roadside access point using the licensed intelligent transportation systems (ITS) band at 5.9 GHz.
802.11r	Enables fast BSS to BSS (Basic Service Set) transitions for mobile devices, to support delay sensitive services such as VoIP on stations roaming between access points.
802.11s	Extending 802.11 MAC to support ESS (Extended Service Set) mesh networking. The 802.11s protocol will enable message delivery over self-configuring multi-hop mesh topologies.
802.11t	Recommended practices on measurement methods, performance metrics and test procedures to assess the performance of 802.11 equipment and networks. The capital T denotes a recommended practice rather than a technical standard.
802.11u	Amendments to both PHY and MAC layers to provide a generic and standardized approach to inter-working with non-802.11 networks, such as Bluetooth, ZigBee and WiMAX.
802.11v	Enhancements to increase throughput, reduce interference and improve reliability through network management.
802.11w	Increased network security by extending 802.11 protection to management as well as data frames.

✓ **Wi-Fi Certificate**

Wi-Fi CERTIFIED™ is an internationally-recognized seal of approval for products indicating that they have met industry-agreed standards for interoperability, security, and a range of application specific protocols.

Wi-Fi CERTIFIED products have undergone rigorous testing by one of independent Authorized Test Laboratories. When a product successfully passes testing, the manufacturer or vendor is granted the right to use the Wi-Fi CERTIFIED logo. 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.

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. At retail, the Wi-Fi CERTIFIED logo gives consumers confidence that a product will deliver a good user experience. Service providers and enterprise IT managers specify Wi-Fi CERTIFIED to reduce support costs and ensure a product has met industry-agreed requirements.

A company must be a member of Wi-Fi Alliance® and achieve certification to use the Wi-Fi CERTIFIED logo and Wi-Fi CERTIFIED certification marks.

Figure3: Wi-Fi CERTIFIED logo

- ✓ **Supporting Mobility**

Mobility enables users to physically move while using an appliance, such as a handheld PC or data collector. Many jobs require workers to be mobile, these include inventory clerks, healthcare workers, policemen, and emergency care specialists. Of course, wire line networks require a physical tether between the user's workstation and the network's resources, which makes access to these resources impossible while roaming about the building or elsewhere. This freedom of movement results in significant return on investments due to gains in efficiency.

Mobile applications requiring wireless networking include those that depend on real-time access to data usually stored in centralized databases. If your application requires mobile users to be immediately aware of changes made to data, or if information put into the system must immediately be available to others, then you have a definite need for wireless networking. For accurate and efficient price markdowns, for example, many retail stores use wireless networks to interconnect handheld bar-code scanners and printers to databases that have current price information. This enables the printing of the correct price on the items, satisfying both the customer and the business owner.

Another example of the use of wireless networking is in auto racing. Formula-1 and Indy racecars have sophisticated data-acquisition systems that monitor the various on-board systems in the car. When the cars come around the track and pass the respective teams in the pit, this information is downloaded to a central computer, thereby enabling real-time analysis of the performance of the race car.

- Content/Topic 3: Identification of Benefits of Wireless

There are many benefits of wireless network, some of them are the following:

- **Mobility:** Mobility enables users to physically move while using an appliance, such as a handheld PC or data collector.
- **Installation in Difficult-to-Wire Areas:** The implementation of wireless networks offers many tangible cost savings when performing installations in difficult-to-wire areas. If rivers, freeways, or other obstacles separate buildings that you want to connect, a wireless solution may be much more economical than installing physical cable or leasing communications circuits, such as T1 service or 56Kbps lines.
- **Increased Reliability:** A problem inherent to wired networks is the downtime due to cable faults. In fact, cable faults are often the primary cause of system downtime. Moisture erodes metallic conductors via water intrusion during storms and accidental spillage or leakage of liquids. With wired networks, users may accidentally break their network connector when trying to disconnect their PC from the network to move it to a different location. An advantage of wireless networking, therefore, results from the use of less cable. This reduces the downtime of the network and the costs associated with replacing cables.
- **Reduced Installation Time:** The installation of cabling is often a time-consuming activity. For LANs, installers must pull twisted-pair wires above the ceiling and drop cables through walls to network outlets that they must affix to the wall. These tasks can take days or weeks, depending on the size of the installation while wireless network installation doesn’t need this. The deployment of wireless networks greatly reduces the need for cable installation, making the network available for use much sooner.

The advantages of wireless networking also include:

1. Wireless routers are equipped with modem, network switch (a device that has multiple connection ports for connecting computers and other network devices), wireless access points.

2. Wireless Router can be connected to/from anywhere in your immediate environment or house. That means you can log on and surf the Internet from anywhere around your surroundings.

3. Some of the wireless routers are equipped with a built in firewall to ward of intruders. The configuration options of the firewall are an important consideration when buying a router. Virtually everyone buys and sell online one way or the other, buying a wireless router with good firewall configuration options can be helpful for security and privacy.

4. The broadband router wireless VoIP technology enables you to connect to the Internet, using any ordinary phone device. You can then make calls to anybody in the world via your Internet connection. Wireless router provides strong encryption (WPA or AES) and features the filters MAC address and control over SSID authentication.

- Content/Topic 4: Description of Wireless Technologies

Wireless technology provides the ability to communicate between two or more entities over distances without the use of wires or cables of any sort. This includes communications using radio frequency (RF) as well as infrared (IR) waves.

The birth of wireless technology started with the discovery of electromagnetic waves by Heinrich Hertz (1857–1894). Guglielmo Marconi (1874–1937) established the very first commercial RF communications, the wireless telegraph, in the late 1890s, more than fifty years after the first commercial wired telegraph service that was demonstrated in 1832 by Samuel F. B. Morse (1791–1872). Marconi was also the first to transmit radio signals to a mobile receiver on ships in the early 1900s. Wireless technology has always been preceded by wired technology and is usually more expensive, but it has provided the additional advantage of mobility, allowing the user to receive and transmit information while on the move.

Another major thrust of wireless technology has been in the area of broadcast communications like radio, television, and direct broadcast satellite. A single wireless transmitter can send signals to several hundreds of thousands of receivers as long as they all receive the same information. Today, wireless technology encompasses such diverse communication devices as garage-door openers, baby monitors, walkie-talkies, and cellular telephones, as well as transmission systems such as point-to-point microwave links, wireless Internet service, and satellite communications.

Wireless technology involves transmitting electromagnetic signals over the air. Interference and obstacles that block RF signals are common problems with wireless technology. Wireless technology allows users to communicate simultaneously over the same medium without their signals interfering with one another. This is made possible because of two physical phenomena, the weakening of electromagnetic signals with distance, and the electromagnetic spectrum. While listening to a radio station as one drives along a highway, one can observe how an RF or IR signal rapidly loses its strength as it travels away from the transmitter. Thus, two people can transmit at the same time if they are sufficiently far apart. If there are no obstacles, signals fall as the square of the distance. This is called free space loss.

RF and IR signals can also be generated at different frequencies that do not interfere with each other. The range of frequencies is from a few cycles per second called hertz (Hz) in honor of the scientist who discovered electromagnetic waves to trillions of hertz, and is called the electromagnetic spectrum. Visible light is included on this spectrum. The 3 kilohertz (kHz) to 300 gigahertz (GHz) frequency range is the RF spectrum. The IR spectrum corresponds to frequencies beyond 300 GHz. There are strict government regulations on the usage of chunks of the RF spectrum (called frequency bands) in all nations of the world.

Wireless technology is often employed to provide communications in places where it is difficult to run cables, for mobile communications, as extensions to wired communications, and for emergency deployment. Bluetooth is a new cable replacement wireless technology that can connect almost any appliance that can be networked to any other appliance, a digital camera to a laptop, or a coffee machine to the Internet, for example. Bluetooth applications include cordless telephones, laptops, and other devices.

Wireless technology can also be classified based on voice or data applications or based on mobility fixed, stationary, portable, and mobile. Cordless and cellular telephones are common examples of voice applications. Cordless telephones operate in unlicensed bands, and cell phones in licensed bands, at frequencies around 1,000 megahertz (MHz). Satellites have been used for a long time to provide voice communications.

Today, it is also possible to access the Internet using wireless technology. Cellular digital packet data (CDPD) service is available for accessing the Internet in the same licensed frequency bands as cell phones. It is possible to buy a CDPD modem for handheld computers and palmtops and to browse the web and send e-mail without connecting via a cable to the Internet. Wireless local area networks (WLANs) in unlicensed bands are also very popular, both in companies and for residential networking, for shared access to the Internet.

Modern fixed wireless technology applications include wireless local loops (WLLs) that provide local telephone service using rooftop antennas, and local multipoint distribution service (LMDS), a digital wireless transmission at 28 GHz that can provide several megabits per second of data for access to the Internet. Stationary wireless technology includes desktop computers that connect to the Internet using WLANs. Cordless phones, laptops, and palmtop computers with wireless connectivity fall into the portable category, while cell phones are the most common example of mobile wireless technology.

Wireless access to the Internet is expected to exceed wired access (if not already) in the next few years, and the prospects for the future are exciting.

- Content/Topic 5: Description of Wireless infrastructure components and small Wireless deployment.

✓ **Wireless NICs**

Stands for "Network Interface Card" and is pronounced "nick." A NIC is a component that provides networking capabilities for a computer. It may enable a wired connection (such as Ethernet) or a wireless connection (such as Wi-Fi) to a local area network. A wireless network interface card (WNIC) is a network interface card which enable a computer to be connected to a wireless network.

As wireless networking became more popular, wireless NICs also grew in popularity. Instead of an Ethernet port, wireless NICs are designed for Wi-Fi connections and often have an antenna to provide better wireless reception for the computer. Older wireless cards have PCI connections while most modern wireless NICs connect to a PCI Express slot.

✓ **Wireless Home Router**

A router is a device that communicates between the internet and the devices in your home that connect to the internet. As its name implies, it “routes” traffic between the devices and the internet.

Figure 4: An example of a wireless home router

A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Depending on the manufacturer and model, it can function in a wired local area network, in a wireless-only LAN, or in a mixed wired and wireless network.

✓ **Wireless Access Point**

The access point is a device that links a wireless network to a wired LAN. It increases the effective range of a wireless network and provides additional network management and security features. Wireless networks of three or fewer PCs do not require an access point for ad hoc networking. Access points are useful for larger networks, and they are particularly well-suited for adding wireless capability to an existing wired network.

- ✓ **Wireless Antennas**

In radio engineering, an antenna or aerial is the interface between radio waves propagating through space and electric currents moving in metal conductors, used with a transmitter or receiver.

Simply speaking, Antenna is a device which converts electrical signals to EM waves or vice versa. In the case of a transmitting antenna, the electrical signal from the transmitting circuit is converted to EM waves and is radiated into the atmosphere. In the case of a receiving antenna, the EM waves in the atmosphere is captured and is converted back to electrical signals for further processing.

WiFis Wireless Networks works the same as the above mentioned communication manner but instead of the voice, we will be transmitting network data packets. The Wireless Router/Access Point converts these data packets to EM waves, radiated out through the transmitting antenna and the antenna in the Client device (mobile device) converts the EM waves back to electrical signals for data processing.

- ✓ **Small wireless Deployment solutions**

Deploying a wireless network installation involves selecting the wireless LAN standard that will best meet your networking environment's needs and specifications, properly addressing the potential for interference and other network speed considerations, and implementing a comprehensive network security policy.

Deployment Planning

The first step in planning a wireless LAN deployment should be to decide on your wireless networking technology standard. Keep in mind that the standard you ultimately select will need to accommodate your network access points and routers as well as the entire collection of wireless network interface cards (NICs) for your computers and other network resources. The main wireless standards in use today are 802.11a, which has a theoretical maximum speed of 11 Mbps; 802.11b, which maxes out at 54 Mbps; 802.11g, which also maxes out at 54 Mbps; and 802.11n, which has a theoretical maximum speed of 250 Mbps. Newer standards like 802.11n can also work with older standards but do so with a considerable negative impact on wireless network performance.

Before designing a networking solution, obtain the following information:

1. Scale of the customer's network, including the area to be covered by the network and the number of terminals to be supported on the network. This information helps determine the number of APs to be deployed.
2. The customer's security requirements, for example, whether the customer needs advanced security features and whether the egress gateway devices need to work in dual-system hot standby mode. This information helps select egress device models.

Solution Design

- Identify the areas of coverage for wireless users. While identifying the areas of coverage, be sure to identify whether you want to provide wireless service outside the building, and if so, determine specifically where those external areas are.
- Determine how many wireless APs to deploy to ensure adequate coverage.
- Determine where to place wireless APs.
- Select the channel frequencies for wireless APs.

Hardware Installation

Install hardware, connect cables, and power on devices based on the network device installation position design and device interconnection information gathered during deployment planning and solution design.

Security

Security is critical for your wireless network, even more so in some respects than with a wired network due to the threat of Wi-Fi eavesdroppers and hackers. Whether your wireless LAN will be deployed in your home or business, an integrated security policy that accommodates all of your users, computers and data on both the wireless and wired networks should be planned and implemented prior to deploying your wireless network. User authentication, proper authorization of access point and network interface cards, data encryption (WEP or WPA/WPA2), personal firewalls on computers and other security safeguards all need to be researched and addressed as part of implementing your network security policy.

- Content/Topic 6: Description of 802011 WLAN Topologies

✓ **Wireless Topology Modes**

The simplest wireless network consists of two or more PCs communicating directly with each other without cabling or any other intermediary hardware. More complicated wireless networks use an access point to centralize wireless communication, and to bridge wireless network segments to wired network segments. These two different methods, or modes, are called ad hoc mode and infrastructure mode.

- ✓ **Ad Hoc mode**

Ad hoc mode is sometimes called peer-to-peer mode, with each wireless node in direct contact with each other node in a decentralized free-for-all. Ad hoc mode does not use an access point and instead uses a mesh topology. Two or more wireless nodes communicating in ad hoc mode form what's called an Independent Basic Service Set (IBSS). This is a basic unit of organization in wireless networks. Think of an IBSS as a wireless workgroup and you're not far off the mark. Ad hoc mode networks work well for small groups of computers (fewer than a dozen or so) that need to transfer files or share printers. Ad hoc networks are also good for temporary networks, such as study groups or business meetings.

- ✓ **Infrastructure mode**

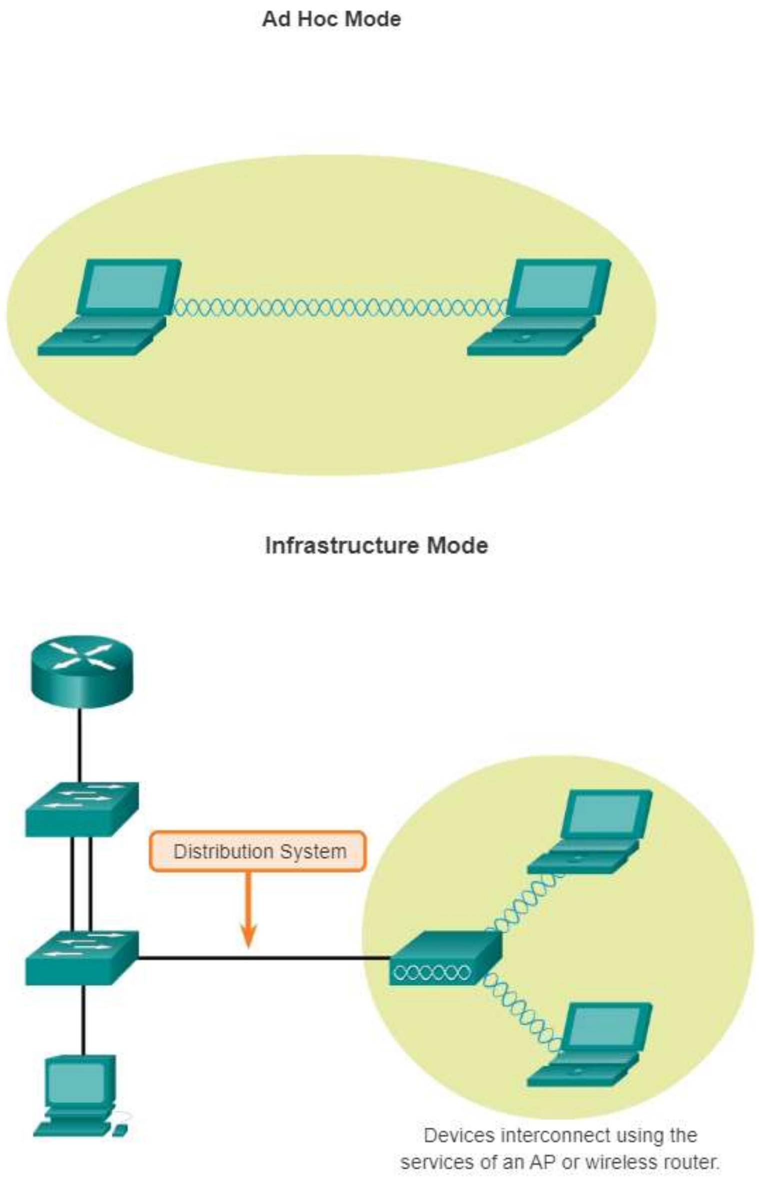
Wireless networks running in infrastructure mode use one or more WAPs to connect the wireless network nodes centrally. This configuration is similar to the star topology of a wired network. You also use infrastructure mode to connect wireless network segments to wired segments. If you plan to set up a wireless network for a large number of PCs, or you need to have centralized control over the wireless network, infrastructure mode is what you need.

A single WAP servicing a given area is called a Basic Service Set (BSS). This service area can be extended by adding more access points. This is called, appropriately, an Extended Service Set (ESS).

NOTE: A lot of techs have dropped the word "basic" from the Extended Basic Service Set, the early name for an infrastructure-mode wireless network with more than one WAP. Accordingly, you'll see the initials for the Extended Basic Service Set as ESS. Using either EBSS or ESS is correct.

Wireless networks running in infrastructure mode require a little more planning- such as where you place the WAPs to provide adequate coverage-than ad hoc mode networks, and they provide a stable environment for permanent wireless network installations. Infrastructure mode is better suited to business networks, or networks that need to share dedicated resources such as Internet connections and centralized databases.

The following Figures display an example of ad hoc mode and example of infrastructure mode respectively.



Ad Hoc Mode

Infrastructure Mode

Devices interconnect using the services of an AP or wireless router.

Figure 5&6: Ad Hoc and Infrastructure modes

- Content/Topic 7: Description of RF Fundamental.

Wireless communications must utilize one of two primary media: sound waves or electromagnetic (EM) waves. When one human speaks to another human, the sound waves travel through the air and are interpreted by the receiving human’s ears. These sound waves form the most ancient kind of wireless communications. However, sound waves do not provide an effective form of wireless communications over great distances because of the tremendous interference in the sound wave spectrums (frequency ranges) and the massive amounts of power required to send a sound wave over those great distances. Electromagnetic waves, on the other hand, offer a very effective means of wireless communications due to the very structured way the frequencies can be divided and the low amounts of power required to communicate across a vast expanse.

In this section, you will first learn about electromagnetic waves and how they can be used for wireless communications. You will then move on to the specific electromagnetic waves that are used within IEEE 802.11–based networks, specifically radio frequency (RF) waves. Next, you will discover the calculations that you can make against RF waves using RF math, and you'll learn also about antennas, including both the types of antennas and their functionality.

- ✓ **Radio frequency**

Waves: A wave, in the domain of physics, can be defined as a motion through matter.

Electric Fields: electric field is the space within which an electrically charged object will feel a pull or a push, depending on whether the charge on the object is unlike (pull) or like (push) that of the pulling or pushing source. Positively charged objects attract negatively charged objects, and negatively charged objects attract positively charged objects. The measurable strength of this attraction is greater when the objects are closer together and lesser when they are farther apart. The electric field represents the space within which this attraction can be detected, although theoretically, the attraction extends infinitely, though it cannot be measured.

Magnetic Fields: A magnetic field is a force produced by a moving electric charge that exists around a magnet or in free space. Magnetic fields extend out from the attracting center, and the space in which it can affect objects is considered the extent of the magnetic field. A changing magnetic field generates an electric field.

Electromagnetic Waves: Now that you have definitions of electric fields and magnetic fields, you are ready to understand electromagnetic waves. An electromagnetic wave is a propagating combination of electric and magnetic fields. Remember that a magnetic field can generate an electric field and an electric field can generate a magnetic field. While the analogy is not perfect, consider that a chicken produce an egg that produce a chicken that produce an egg again and again in the same way. The alternating current (AC) in the antenna generates a magnetic field around the antenna that generates an electric field that generates a magnetic field again and again in the same way.

The electric and magnetic fields are oscillating perpendicular to each other, and they are both perpendicular to the direction of propagation, as is shown in the bellow Figure. You can see that the electric field is parallel to the generating wire (antenna) and the magnetic field is perpendicular to the generating wire. The wave is traveling out from the generating wire. A very specific form (wavelength and frequency) of these electromagnetic waves is used to communicate wirelessly in IEEE 802.11 networks. This form of wave is a radio frequency wave, often shortened to RF wave. An RF-based system, then, is a system that relies on the phenomenon of electromagnetic wave theory to provide data and voice communications wirelessly.

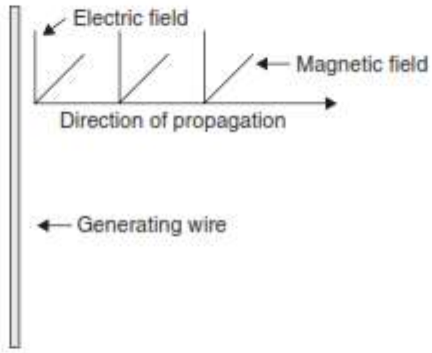


Figure7: Electromagnetic wave propagation direction

- ✓ **Principles of antennas**

The antenna plays an essential role in sending and receiving information in the wireless communication systems. In addition to communication systems antennas are used in astronomy, geophysical probing, medicine and biological tissues, and radio frequency identification systems. Based on their geometrical structure, antennas may be classified into wire antennas; aperture type antennas; micro-strip antennas; array antennas; reflector antennas; lens antennas.

- ✓ **Antennas radiation Principles**

After an RF signal has been generated in a transmitter, some means must be used to radiate this signal through space to a receiver. The device that does this job is the antenna. The transmitter signal energy is sent into space by a transmitting antenna; the RF signal is then picked up from space by a receiving antenna. The RF energy is transmitted into space in the form of an electromagnetic field. As the traveling electromagnetic field arrives at the receiving antenna, a voltage is induced into the antenna (a conductor).The RF voltages induced into the receiving antenna are then passed into the receiver and converted back into the transmitted RF information. The design of the antenna system is very important in a transmitting station. The antenna must be able to radiate efficiently so the power supplied by the transmitter is not wasted. An efficient transmitting antenna must have exact dimensions. The dimensions are determined by the transmitting frequencies. The dimensions of the receiving antenna are not critical for relatively low radio frequencies. However, as the frequency of the signal being received increases, the design and installation of the receiving antenna become more critical. An example of this is a television receiving antenna. If you raise it a few more inches from the ground or give a slight turn in direction, you can change a snowy blur into a clear picture.

- ✓ **Radio frequency mathematics**

Because the wireless network uses an RF signal, you must understand the basics of RF math in order to determine if the output power of an RF transmitter is strong enough to get a detectable and usable signal to the RF receiver.

In order to understand and perform RF math, there are a few basic things you will need to know. First, you'll need to understand the units of power that are measured in RF systems. Second, you'll need to understand how to measure power gains and losses. Third, and finally, you'll need to understand how to determine the output power you will need at a transmitter in order to get an acceptable signal to a receiver. This is true if you are creating a point-to-point connection using wireless bridges or if you are installing an access point in an access role. In both cases, a sufficient signal must reach the receiver listening on the other end of the connection.

- **Watt:** The *watt* (W) is a basic unit of power equal to one joule per second. It is named after James Watt, an eighteenth-century Scottish inventor who also improved the steam engine, among other endeavors. This single watt is equal to one ampere of current flowing at one volt. Think of a water hose with a spray nozzle attached. You can adjust the spray nozzle to allow for different rates of flow. This flow rate is like the amperes in an electrical system. Now, the water hose also has a certain level of water pressure regardless of the amount that is actually being allowed to flow through the nozzle. This pressure is like the voltage in an electrical system. If you apply more pressure or you allow more flow with the same pressure, either way, you will end up with more water flowing out of the nozzle. In the same way, increased voltages or increased amperes will result in increased wattage, since the watt is the combination of the amperes and volts.

- **Mill watt:** WLANs do not need a tremendous amount of power to transmit a signal over an acceptable distance. For example, you can see a 7-watt light bulb from more than 50 miles (83 kilometers) away on a clear night with line of sight. Remember, visible light is another portion of the same electromagnetic spectrum, and so this gives you an idea of just how far an electromagnetic signal can be detected. This is why many WLAN devices use a measurement of power that is 1/1000 of a watt. This unit of power is known as a milliwatt. 1 W, then, would be 1000 milliwatts (mW).

Enterprise-class devices will often have output power levels of 1–100 mW, while SOHO wireless devices may only offer up to 30 mW of output power. Some wireless devices may support up to 300 mW of output power, but these are the exception to the rule.

For indoor use, it is generally recommended that you transmit at power levels of no more than 100 mW. In most cases, the minimum gain that will be provided by any connected antennas is a 2 dBi gain, which will explained later. This means that the output power would actually be approximately 160 mW in the propagation direction of this antenna. This usually provides sufficient coverage for indoor WLANs.

- **Decibel (dB)**: The *decibel* is a comparative measurement value. In other words, it is a measurement of the difference between two power levels. For example, it is common to say that a certain power level is 6 dB stronger than another power level or that it is 3 dB weaker. These statements mean that there has been 6 dB of gain and 3 dB of loss, respectively. Because a wireless receiver can detect and process very weak signals, it is easier to refer to the received signal strength in dBm rather than in mW.

For example, a signal that is transmitted at 4 W of output power (4000 mW or 36 dBm) and experiences ⍰63 dB of loss has a signal strength of 0.002 mW (⍰27 dBm). Rather than saying that the signal strength is 0.002 mW, we say that the signal strength is ⍰27 dBm.

A decibel is 1/10 of a *bel.* You could equally say that a bel is 10 decibels. The point is that the decibel is based on the bel, which was developed by Bell Laboratories in order to calculate the power losses in telephone communications as ratios.

In other words, 1 bel is a ratio of 10:1 between two power levels. Therefore, a power ratio of 200:20 is 1 bel (10:1) and

200:40 is .5 bels (5:1) and 200:10 is 2 bels (20:1). In the end, the decibel is a measurement of power that is used very frequently in RF mathematics.

dBm: The abbreviation *dBm* represents an absolute measurement of power where the *m* stands for *milliwatts.* Effectively, dBm references decibels relative to 1 milliwatt such that 0 dBm equals 1 milliwatt. Once you establish that 0 dBm equals 1 milliwatt, you can reference any power strength in dBm. The formula to get dBm from milliwatts is

dBm=10* log10(Power$_{mW}$)

For example, if the known milliwatt power is 30 mW, the following formula would be accurate: 10* log10 (30) = 14.77 dBm

This result would often be rounded to 15 dBm for simplicity; however, you must be very cautious about rounding if you are calculating a link budget because your end numbers can be drastically incorrect if you've done a lot of rounding along the way.

- ➢ **dBi:** The abbreviation *dBi* (the *i* stands for isotropic) represents a measurement of power gain used for RF antennas. It is a comparison of the gain of the antenna and the output of a theoretical isotropic radiator. An *isotropic radiator* is an ideal antenna that we cannot create with any known technology. This is an antenna that radiates power equally in all directions.

✓ **Spread spectrum**

Spread-Spectrum techniques are methods by which a signal (e.g. an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth.

These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection, and to limit power flux density (e.g. in satellite downlinks).

Spread spectrum is designed to be used in wireless applications (LANs and WANs). In wireless applications, all stations use air (or a vacuum) as the medium for communication. Stations must be able to share this medium without interception by an eavesdropper and without being subject to jamming from a malicious intruder.

To achieve these goals, spread spectrum techniques add redundancy, they spread the original spectrum needed for each station. If the required bandwidth for each station is B, spread spectrum expands it to Bss such that Bss >> B. The expanded bandwidth allows the source to wrap its message in a protective envelope for a more secure transmission.

✓ **RF in perspective**

All RF waves have characteristics that vary to define the wave. Some of these properties can be modified to modulate information onto the wave. These properties are **wavelength, frequency, amplitude**, and **phase**.

Wavelength: The *wavelength* of an RF wave is calculated as the distance between two adjacent identical points on the wave. For example, Figure below shows a standard sine wave. Point A and Point B mark two identical points on the wave, and the distance between them is defined as the wavelength. The wavelength is frequently measured as the distance from one crest of the wave to the next. The wavelength is an important measure of which you should be aware. The wavelength dictates the optimum size of the receiving antenna, and it determines how the RF wave will interact with its environment.

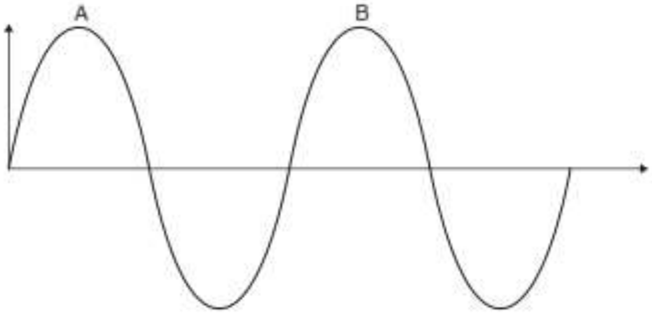


Figure8: Wavelength measurement

You will learn about frequency next, but it is important you understand that the wavelength and the frequency are interrelated. In fact for a given medium, if you know the wavelength, you can calculate the frequency and if you know the frequency, you can calculate the wavelength.

One of the great discoveries in the history of electromagnetism is that electromagnetic waves travel at the speed of light. Since we know the speed of light to be 299,792,458 meters per second, we also know that this is the speed at which electromagnetic waves travel in a vacuum. This was theorized by James Clerk Maxwell and proved through experimentation by Heinrich Hertz.

Since we know that RF waves travel at the speed of light, we can calculate the frequency when we know the wavelength or the wavelength when we know the frequency.

The following formula can be used to calculate the wavelength in meters when the frequency is known:

λ = 299,792,458/ f → here, **λ** is the wavelength in meters and *f* is the frequency in *hertz* and the medium is a vacuum.

Frequency: Frequency refers to the number of wave cycles that occur in a given window of time. Usually measured in second intervals, a frequency of 1 kilohertz (KHz) would represent 1000 cycles of the wave in 1 second.

To remember this, just keep in mind that a wave cycles frequently and just how frequently it cycles determines its frequency. Since all electromagnetic waves, including radio waves, move at the speed of light, the frequency is related to the wavelength. In other words, we observe that wavelength, frequency, and medium are interdependent.

Higher frequencies have shorter wavelengths, and lower frequencies have longer wavelengths.

Amplitude: Given the explanation in the preceding section, you might be tempted to think that the volume of sound waves is dependent on the frequency, since lower-frequency waves are heard at a greater distance; however, there is actually another characteristic of waves that impacts the volume.

Remember, at greater distances, shorter-wavelength waves are more difficult to detect as the waveform spreads ever wider (though this may be more a factor of the antenna used than of the waveform itself). The characteristic that defines the volume is known as **amplitude**. In sound wave engineering, an increase in amplitude is equivalent to an increase in volume; hence, an amplifier adds to the volume, or makes the sound louder. While the frequency affects the distance a sound wave can travel, the amplitude affects the ability to detect (hear) the sound wave at that distance.

An RF wave with greater amplitude is easier to detect than an RF wave with lesser amplitude, assuming all other factors are equal. In other words, in a vacuum, an RF wave will be said to have better quality at a distance if it has greater amplitude.

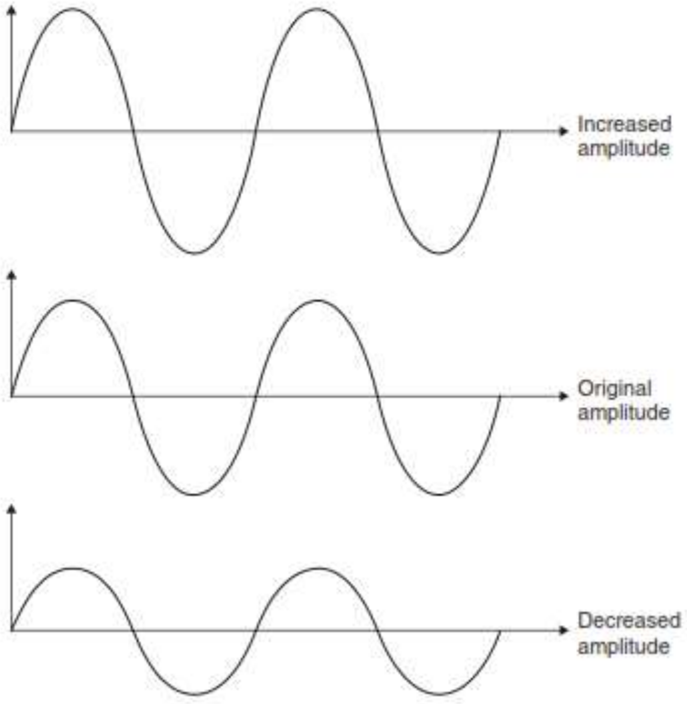


Figure9: RF waves at different amplitudes

Phase: Unlike wavelength, frequency, and amplitude, *phase* is not a characteristic of a single RF wave but is instead a comparison between two RF waves. If two copies of the same RF wave arrive at a receiving antenna at the same time, their phase state will impact how the composite wave is able to be used. When the waves are in phase, they strengthen each other, and when the waves are out of phase, they sometimes strengthen and sometimes cancel each other. In specific out-of-phase cases, they only cancel each other.

Phase is measured in degrees, though real-world analysis usually benefits only from the knowledge of whether the waves are in phase or out of phase. Two waves that are completely out of phase would be 180 degrees out of phase, while two waves that are completely in phase would be 0 degrees out of phase.

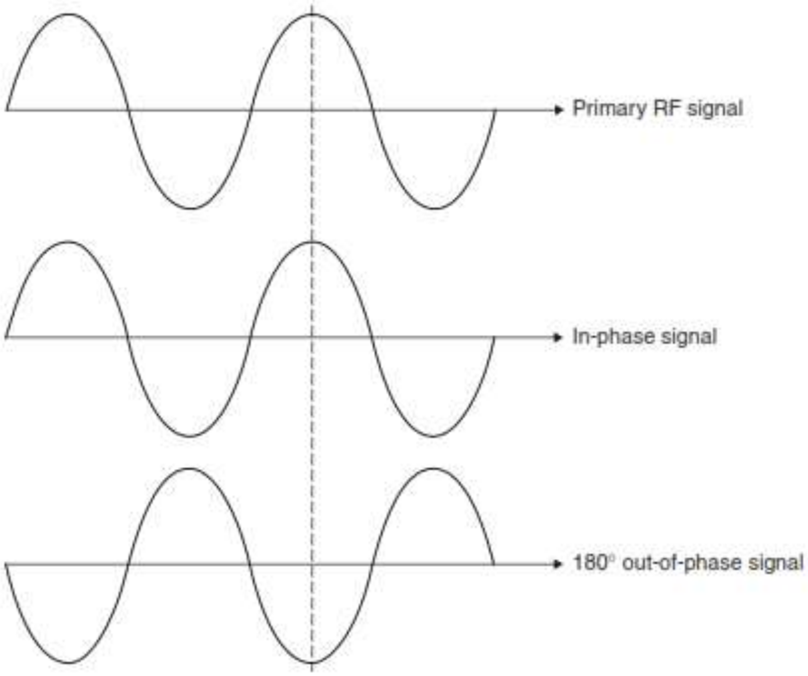


Figure10: RF wave phases

- Content/Topic 8: Application of wireless

✓ **Network extension**

WiFi Range Extenders boost the existing WiFi in your home by receiving the wireless signals from your router and repeating them with powerful amplifiers and antennas, extending your coverage by up to twice the range. To extend your network follow the following steps

1. **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.

2. **Connect the bridge to your network**

   If your router supports Wi-Fi Protected Setup, or WPS, setup is easy. Simply press the WPS buttons on your bridge and router to link them wirelessly. Look for the Wi-Fi Protected Setup (WPS) logo on your router to make sure it supports this preferred security standard. Otherwise, you'll need to connect the bridge to your PC via Ethernet to configure your bridge. On your PC, open a web browser and enter the IP Address of your bridge.

3. Plug in network devices
4. Now that your bridge is connected to your network, connect your wired devices directly to the bridge via Ethernet. That's is it. Your wireless bridge will automatically connect any attached devices to your primary network over Wi-Fi.

✓ **Building to building**

If you're setting up Wi-Fi in a large space, you may want to supplement traditional Wi-Fi with in-building wireless solutions. If you're working with substantial square footage, a distributed antenna system (DAS) is a popular choice because it's scalable to even the largest buildings. This set up includes a central controller connected to a carrier base station, but it also makes use of multiple antennas distributed throughout the building.

✓ **Last mile data delivery**

Broadband communications and home networking are becoming household words as more and more homes are utilizing many network-enabled devices. On one hand, the term broadband implies high-speed digital communications, requiring wider bandwidth for transmission, and can be employed for the distribution of high-speed data, voice, and video throughout the home. Therefore, the last mile broadband access specifies the connectivity mechanism from the local signal distributor and the home (or the end user). Several companies are providing methods to connect and provide services of voice, data, music, video, and other forms of communication. They include wired solutions such as Public Switched Telephone Network (PSTN), cable, and fiber optics, as well as wireless options such as fixed wireless and satellite.

Home networking has become a convergence point for the next generation digital infrastructure. As technology has advanced, household appliances, televisions, stereos, home security systems, and nearly everything that operates on electrical energy is becoming digitally controlled and potentially connectable to a network. It is becoming a key technology that will enable new-breed of information appliances to connect to, and communicate over, rapidly expanding digital network.

Broadband communications and home networking are becoming household words as more and more homes are utilizing many network-enabled devices. On one hand, the term broadband implies high-speed digital communications, requiring wider bandwidth for transmission, and can be employed for the distribution of high-speed data, voice, and video throughout the home. Therefore, the last mile broadband access specifies the

connectivity mechanism from the local signal distributor and the home (or the end user). Several companies are providing methods to connect and provide services of voice, data, music, video, and other forms of communication. They include wired solutions such as Public Switched Telephone Network (PSTN), cable, and fiber optics, as well as wireless options such as fixed wireless and satellite.

Home networking has become a convergence point for the next generation digital infrastructure. As technology has advanced, household appliances, televisions, stereos, home security systems, and nearly everything that operates on electrical energy is becoming digitally controlled and potentially connectable to a network. It is becoming a key technology that will enable new-breed of information appliances to connect to, and communicate over, rapidly expanding digital network.

Broadband communications and home networking are becoming household words as more and more homes are utilizing many network-enabled devices. On one hand, the term broadband implies high-speed digital communications, requiring wider bandwidth for transmission, and can be employed for the distribution of high-speed data, voice, and video throughout the home. Therefore, the last mile broadband access specifies the connectivity mechanism from the local signal distributor and the home (or the end user).

Last Mile Broadband Wireless Access technologies are a relatively new service that is being used by telecommunication companies to carry IP data from central locations on their networks to small low-cost antennas that are mounted on their subscribers’ roofs.

Last Mile Broadband Wireless Access technologies are a relatively new service that is being used by telecommunication companies to carry IP data from central locations on their networks to small low-cost antennas that are mounted on their subscribers’ roofs.

Several companies are providing methods to connect and provide services of voice, data, music, video, and other forms of communication. They include wired solutions such as Public Switched Telephone Network (PSTN), cable, and fiber optics, as well as wireless options such as fixed wireless and satellite.

Rapid growth in demand for high-speed Internet/Web access and multiline voice for residential and small business customers has created a demand for last mile broadband access. Typical peak data rates for a shared broadband pipe for residential customers and small offices/home offices (SOHO) are around 5–10 Mb/s on the downlink (from the hub to the terminal) and 0.5–2 Mb/s on the uplink (from the terminal to the hub). This asymmetry arises from the nature and dominance of Web traffic. Voice and videoconferencing exhibit symmetric traffic. While long-term evolution of Internet services and the resulting traffic is hard to predict, demand for data rates and quality of broadband last mile services will certainly increase dramatically in the near future. There are many wireless systems in several bands competing for the “last mile”. Methods considered include point-to-point, point-to-multipoint, and multipoint-to-multipoint for bringing broadband communications information and provide networking capabilities amongst the end users.

Broadband access is currently offered through digital subscriber line (xDSL) [47, 48], cable, and broadband wireless access (BWA), which can also be referred to as fixed broadband wireless access (FBWA) networks. Each of these techniques has their own unique cost, performance, and deployment trade-offs. While cable and DSL are already being deployed on a large scale basis, BWA is emerging as an access technology with several advantages. These include avoiding distance limitations of DSL and high costs of cable, rapid deployment, high scalability, lower maintenance and upgrade costs, and incremental investment to match market growth. Nevertheless, a number of important issues including spectrum efficiency, network scalability, self-installable CPE antennas, and reliable non-line-of-sight (NLOS) operation need to be resolved before BWA can penetrate the market successfully.

Rapid growth in demand for high-speed Internet/Web access and multiline voice for residential and small business customers has created a demand for last mile broadband access. Typical peak data rates for a shared broadband pipe for residential customers and small offices/home offices (SOHO) are around 5–10 Mb/s on the downlink (from the hub to the terminal) and 0.5–2 Mb/s on the uplink (from the terminal to the hub). This asymmetry arises from the nature and dominance of Web traffic. Voice and videoconferencing exhibit symmetric traffic. While long-term evolution of Internet services and the resulting traffic is hard to predict, demand for data rates and quality of broadband last mile services will certainly increase dramatically in the near future. There are many wireless systems in several bands competing for the “last mile”.

The following are the Methods for bringing broadband communications information and provide networking capabilities amongst the end users:

- Point-to-point
- Point-to-multipoint
- Multipoint-to-multipoint

Broadband access is currently offered through digital subscriber line (DSL), cable, and broadband wireless access (BWA), which can also be referred to as fixed broadband wireless access (FBWA) networks. Each of these techniques has their own unique cost, performance, and deployment trade-offs. While cable and DSL are already being deployed on a large scale basis, BWA is emerging as an access technology with several advantages. These include avoiding distance limitations of DSL and high costs of cable, rapid deployment, high scalability, lower maintenance and upgrade costs, and incremental investment to match market growth. Nevertheless, a number of important issues including spectrum efficiency, network scalability, self-installable CPE antennas, and reliable non-line-of-sight (NLOS) operation need to be resolved before BWA can penetrate the market successfully.

- ✓ **Mobility, SOHO**

Wireless technology is becoming an integral part of everyday lives. Most people have a cellular phone or a personal digital assistant (PDA) used for voice communications, checking emails, or organizing personal information. This is the technology of 21st century, which has incredible opportunities and various applications. Recent advances in networking technology have enabled portable computing devices to link up with servers through wireless networks, such as IEEE 802.11b and Bluetooth, to access information from them, and to delegate heavy task to them. A typical IEEE802.11b wireless LAN consists of more than one station (i.e. access point), whose typical radio area is within at most a few hundred meters, connected through a local area network. The data flows and interactions between mobile users, sensors and their supporting computing infrastructure are clearly very different from those of today's popular interment applications such as email, instant messaging or the World Wide Web.

- ✓ **Access role**

Wireless technology provides a convenient mechanism for accessing user resources. These technologies have become ubiquitous in the workplace environment. The advent of wireless technologies adds increased functionality but also adds security risks and concerns that must be managed and mitigated.

By using wireless devices within the [LEP] network for business purposes, all staff are subject to policies managing their use. Wireless (Wi-Fi) transmissions used to access [LEP] networks and devices shall be encrypted. If sent across a public or open network, both the authentication data (e.g. a user ID and password) and the data itself, shall be encrypted with strong encryption. Data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission security protocols along with approved encryption techniques are utilized.

LO1.2. Description of Wireless Network operations

- Content/Topic 1: Introduction to Wireless Network operations

Wireless network refers to any type of computer network that uses wireless (usually, but not always radio waves) for network connections. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

Wireless Networking

A wireless network is a flexible data communications system, which uses wireless media such as radio frequency technology to transmit and receive data over the air, minimizing the need for wired connections (What is Wireless LAN, White Paper). Wireless networks are used to augment rather than replace wired networks and are most commonly used to provide last few stages of connectivity between a mobile user and a wired network. Bluetooth and 802.11b have the potential to dramatically alter how people use devices to connect and communicate in everyday life. Bluetooth is a low-power, short-range technology for ad hoc cable replacement; it enables people to wirelessly combine devices wherever they bring them.

Conversely, 802.11b is a moderate-range, moderate-speed technology based on Ethernet; it allows people to wirelessly access an organizational network throughout a campus location. Although the technologies share the 2.4 GHz band, have some potentially overlapping applications, and have been pitted against each other in the press, they do not compete and can even been successfully combined for corporate use.

One thing is clear, wireless technologies will continue to evolve and offer organizations and end users higher standard of life by making us more mobile and increasing our ability to interact with each other, removing distance as a barrier. There will be a time when a traveler can sit in any airport or hotel and surf the Web or connect to the home office and work. Users will be able to surf or work in places such as malls, parks, or (with smaller handheld computers) just walking down the street.

Advantages and disadvantages of Wireless Network

Advantage of Wireless Networking

The advantages of wireless networking include:

1. Wireless routers are equipped with modem, network switch (a device that has multiple connection ports for connecting computers and other network devices), wireless access points.

2. Wireless Router can be connected to/from anywhere in your immediate environment or house. That means you can log on and surf the Internet from anywhere around your surroundings.

3. Some of the wireless routers are equipped with a built in firewall to ward of intruders. The configuration options of the firewall are an important consideration when buying a router. Virtually everyone buys and sell online one way or the other, buying a wireless router with good firewall configuration options can be helpful for security and privacy.

4. The broadband router wireless VoIP technology enables you to connect to the Internet, using any ordinary phone device. You can then make calls to anybody in the world via your Internet connection. Wireless router provides strong encryption (WPA or AES) and features the filters MAC address and control over SSID authentication.

Disadvantages of WLAN

1. When the number of computers that use the network increases, the data transfer to the computer each will be reduced.

2. When standards change, it may be necessary to replace the wireless card and / or access point.

3. The low bandwidth wireless means some applications like video streaming to be more effective on the LAN cable.

4. Security is more difficult to guarantee and requires no configuration.

5. 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.

6. 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.

7. Long-term cost-efficient is more difficult to achieve static environments that require few moves and changes.

- Content/Topic 2: Operation of Wireless Network

✓ **The 802.11 Frame Structure**

The IEEE 802.11 standard, lays down the architecture and specifications of wireless local area networks (WLANs). WLAN or WiFi uses high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

The 802.11 MAC sub layer provides an abstraction of the physical layer to the logical link control sub layer and upper layers of the OSI network. It is responsible for encapsulating frames and describing frame formats.

MAC Sub layer Frame Structure of IEEE 802.11

The main fields of a frame in WLANs as laid down by IEEE 802.11 are as depicted in the following diagram −

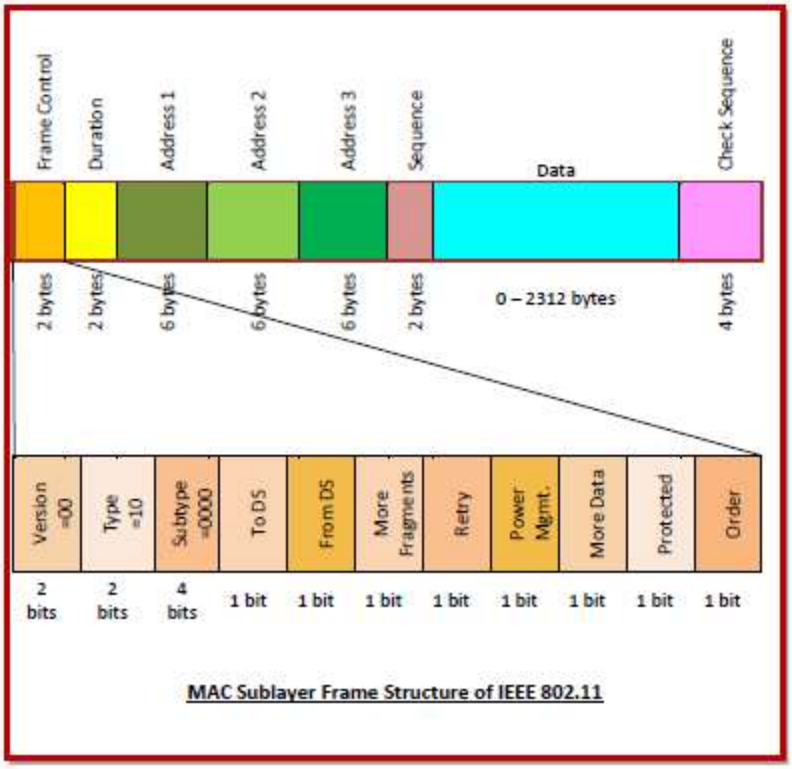


Figure11: 802.11 Frame Structure

- ✓ **The 802.11 Frame structure Control frames**

It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame. The different subfields presented in Frame control are the following:

- **Protocol version** − the first sub-field is a two – bit field set to 00. It has been included to allow future versions of IEE 802.11 to operate simultaneously.
- **Type** − It is a two-bit subfield that specifies whether the frame is a data frame, control frame or a management frame.
- **Subtype** − it is a four – bit subfield states whether the field is a Request to Send (RTS) or a Clear to Send (CTS) control frame. For a regular data frame, the value is set to 0000.
- **To DS** − A single bit subfield indicating whether the frame is going to the access point (AC), which coordinates the communications in centralized wireless systems.
- **From DS** − A single bit subfield indicating whether the frame is coming from the AC.
- **More Fragments** − A single bit subfield which when set to 1 indicates that more fragments would follow.

- **Retry** − A single bit subfield which when set to 1 specifies a retransmission of a previous frame.
- **Power Management** − A single bit subfield indicating that the sender is adopting power-save mode.
- **More Data** − A single bit subfield showing that sender has further data frames for the receiver.
- **Protected Frame** − A single bit subfield indicating that this is an encrypted frame.
- **Order** − the last subfield, of one – bit, informs the receiver that to the higher layers the frames should be in an ordered sequence.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.
- Address fields: There are three 6-byte address fields containing addresses of source, immediate destination and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers. It detects duplicate frames and determines the order of frames for higher layers. Among the 16 bits, the first 4 bits provides identification to the fragment and the rest 12 bits contain the sequence number that increments with each transmission.
- **Data** − this is a variable sized field that carries the payload from the upper layers. The maximum size of data field is 2312 bytes.
- **Frame Check Sequence (FCS)** − It is a 4-byte field containing error detection information.

✓ **Wireless Frame Type**

There are three types of wireless frame: **management** frames, **Control** frames, and **Data** frames.

✓ **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 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.

The following 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)

- ✓ **CSMA/CA**

Carrier Sense Multiple Access/Collision Avoidance (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", because only a single device can use any network at a time, network nodes must have a way to access the network media without stepping on each other's data packets. Wired Ethernet networks use carrier sense multiple access/collision detection (CSMA/CD), but Wi-Fi networks use carrier sense multiple access/collision avoidance (CSMA/CA).

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.

- ✓ **Discovering Aps**

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

- Content/Topic 3: Channel Management

- ✓ **Frequency Channel Saturation**

Saturated network channel or 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. Any SSID from any WAP will conflict if it is on the same channel. The name of the SSID does not prevent this interference from happening. In fact, WAP that are broadcasting the same SSID should be on different channels to prevent interference. There are three channels (1, 6, and 11) that do not overlap and should be used effectively for channel management by WAP that are located physically closer to each other.

There are some techniques used to 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.

✓ Selecting Channels

Wi-Fi channels are smaller bands within Wi-Fi frequency bands that are used by your wireless network to send and receive data.

The reason that certain channels aren't the best choice to use is because they have interference. There are a couple different ways this interference is caused: Co-Channel interference results when there are numerous devices all competing for time to talk on the same channel. Adjacent-Channel interference occurs when devices from overlapping channels are trying to talk over each other.

Channels that have interference from other devices are considered to be 'crowded'. The time it takes to transmit data is increased and you are left waiting for your Internet request to be made. The channels with the most interference are those that overlap with each other.

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.

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.

The reason why you have to change or adjusting your channel selections

- 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.

To view all information about your wireless network settings, use “**netsh wlan show all”** command in the command prompt.

How do I change the WiFi channel I'm using?

To change what WiFi 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 WiFi 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 WiFi channel it is using.

LO1.3. Identification of Wireless LAN threats

- Content/Topic 1: Introduction to wireless LAN Security

There are a number of basic fundamentals that a person or company needs to be aware of when deploying a wireless network. The first is a basic understanding of what frequencies will be used by the equipment being deployed; this is very important when deploying a wireless network as it affects the amount of interference that the network will be subject to depending on the specific environment. At this point in time, there are two main frequency bands that are used for wireless LANs (802.11); these include the 2.4 GHz and 5 GHz bands. From a security perspective, the choice of frequency does not greatly affect the security risk of the network. What it does affect is the number of available non-overlapping channels that are available on the network; for the most part this will not affect security except when an attacker is attempting to jam or block a specific frequency to force wireless endpoints to switch Access Points (AP).

Endpoint devices identify wireless networks using a service set identifier (SSID) along with a set of security parameters. On most wireless deployments, the SSID is broadcast from the APs allowing the clients the ability to easily associate. It is possible to not broadcast the SSID which provides a little protection from those wireless network attackers with little operating knowledge; however, for an experienced wireless attacker this is not a very effective security measure. The real security for a wireless network comes from the selection of a proven security technique, there have been a number of different security techniques deployed that have been broken. As of this writing the most secure technique is **IEEE 802.11i** which is also known as **WPA2**. This standard provides two different modes of operation including one typically referred to as Personal or Pre-Shared Key (PSK) and Enterprise:

- **WPA2-Personal** - utilizes a shared key that is communicated to both sides (AP and client) before establishing a wireless connection; this key is then used to secure the traffic.
- **WPA2-Enterprise** - utilizes the IEEE 802.1x protocol to authenticate a wireless client using an authentication server before traffic is allowed.

- Content/Topic 2: Identification of Wireless LANs threats

There are a number of main threats that exist to wireless LANs, these include:

- Rogue Access Points
- Denial of Service
- Configuration Problems (Mis-Configurations/Incomplete Configurations)
- Passive Capturing

Let's go through each of these in more detail.

- ✓ **Denial of Service attack**

It is one of the simplest network attacks to perpetrate because it only requires limiting access to services. This can be done by simply sending a large amount of traffic at a specific target. Of course, the amount of traffic required to affect a target device can be much higher than the capabilities of a single machine. However, the flooding of traffic is not the only way to limit access to services; for wireless networks it can be much easier as the signal can be interfered with through a number of different techniques. When a wireless LAN is using the 2.4 GHz band, interference can be caused by something as simple as a microwave oven or a competing access point on the same channel. Because the 2.4 GHz band is limited to only 3 non-overlapping channels, an attacker just needs to cause enough interference into these three channels to cause service interruption.

- ✓ **Management Frame DoS Attacks**

In Management Frame DoS Attacks, a malicious user initiates a DoS attack using RF jamming devices that produce accidental interference. It is likelier that they will attempt to manipulate management frames to consume the AP resources and keep channels too busy to service legitimate user traffic.
Management frames can be manipulated to create various types of DoS attacks. Two common management frame attacks include:

A spoofed disconnect attack - 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.

- ✓ **Rogue Access Points**

One method that is often used by attackers targeting wireless LANs is to setup a rogue access point that is within the range of the existing wireless LAN. The idea is to 'fool' some of the legitimate devices into associating to this access point over the legitimate access points. To really be effective, this type of attack requires some amount of physical access; this is required because if a user associates with a rogue access point then is unable to perform any of their normal duties the vulnerability will be short lived and not that effective. If an attacker is able to gain access to a physical port on a company network and then hook the access point into this port, it is possible to get devices to associate with the rogue access point and capture data through it for an extended period of time. The exception to this is when the wireless LAN being targeted only provides Internet access; it is much easier for a rogue access point to offer simple Internet access and leave the user unaware of their vulnerability for an extended amount of time.

A rogue access point can also be used in conjunction with a denial of service attack. For example, a rogue access point could be setup in a channel not used by the legitimate access point and then a denial of service attack could be launched at the channel currently being used causing endpoint devices to try to re-associate onto a different channel which is used by the rogue access point.

- ✓ **Configuration Problems**

Simple configuration problems are often the cause of many vulnerabilities, this is because some of the access points delivered with no security configuration. A novice user can set up one of these devices quickly and gain access. However, they also open up their network to external use without further configuration. Other potential issues with configuration include weak passphrases, weak security deployments (i.e. WEP vs WPA vs WPA2), and default SSID usage among others.

- ✓ **Passive Capturing**

Passive capturing is performed by simply getting within range of a target wireless LAN and then listening and capturing data. This information can be used for a number of things including attempting to break existing security settings and analyzing non-secured traffic. It is almost impossible to really prevent this type of attack because of the nature of a wireless network; what can be done is to implement high security standards using complex parameters.

- **Man-in-the-Middle (MITM) Attack**

Man-in-the-middle attacks (MITM) are a common type of cyber security attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen to, hence the name “man-in-the-middle.”

The following analogy will let you understand well Man-in-the-Middle Attack procedure: Alice and Bob are having a conversation; Eve wants to eavesdrop on the conversation but also remain transparent. Eve could tell Alice that she was Bob and tell Bob that she was Alice. This would lead Alice to believe she’s speaking to Bob, while actually revealing her part of the conversation to Eve. Eve could then gather information from this, alter the response, and pass the message along to Bob (who thinks he’s talking to Alice). As a result, Eve is able to transparently hijack their conversation.

✓ **Man-in-the-Middle Attack Techniques**

Sniffing: Attackers use packet capture tools to inspect packets at a low level. Using specific wireless devices that are allowed to be put into monitoring or promiscuous mode can allow an attacker to see packets that are not intended for it to see, such as packets addressed to other hosts.

Packet Injection: An attacker can also leverage their device’s monitoring mode to inject malicious packets into data communication streams. The packets can blend in with valid data communication streams, appearing to be part of the communication, but malicious in nature. Packet injection usually involves first sniffing to determine how and when to craft and send packets.

Session Hijacking: Most web applications use a login mechanism that generates a temporary session token to use for future requests to avoid requiring the user to type a password at every page. An attacker can sniff sensitive traffic to identify the session token for a user and use it to make requests as the user. The attacker does not need to spoof once he has a session token.

SSL Stripping: Since using HTTPS is a common safeguard against ARP or DNS spoofing, attackers use SSL stripping to intercept packets and alter their HTTPS-based address requests to go to their HTTP equivalent endpoint, forcing the host to make requests to the server unencrypted. Sensitive information can be leaked in plain text.

✓ **How to detect a Man-in-the-Middle-Attack?**

Detecting a Man-in-the-middle attack can be difficult without taking the proper steps. If you aren't actively searching to determine if your communications have been intercepted, a Man-in-the-middle attack can potentially go unnoticed until it's too late. Checking for proper page authentication and implementing some sort of tamper detection are typically the key methods to detect a possible attack, but these procedures might require extra forensic analysis after-the-fact. It's important to take precautionary measures to prevent MITM attacks before they occur, rather than attempting to detect them while they are actively occurring. Being aware of your browsing practices and recognizing potentially harmful areas can be essential to maintaining a secure network.

Learning Unit 2 - Planning and Conduct Site survey

LO2. 1. Analysis of facilities and existing WIFI &WIRED network

- Content/Topic 1: Planning and site survey process

✓ **Performing an initial environment evaluation**

Establishing User Requirements

If the wireless LAN is being implemented to support a large user group it will be important to gather a wide range of views on user requirements, perhaps by using a questionnaire or by interview. As a first step it may be necessary to raise awareness by demonstrating the technology to the prospective user group, so that they are better able to give an informed view on requirements. User requirements should be expressed in terms of the user experience rather than any particular solution or technical attribute, as they are independent of specific technologies. For example, in relation to performance expectations, a PHY layer data rate is a technical attribute, whereas the transfer time for a specified large file size is what the user is really concerned about. Common categories of user requirement are listed and discussed in the following table

Table2: Categories of User Requirement

Requirement type	**Considerations**
Usage model	What user activities does the WLAN have to support? Are users routinely transferring large files over the network, such as Internet downloads or video editing? Is the WLAN required to support applications such as voice or video streaming, either now or in the future?
Performance expectations	What are the user's performance expectations? If large data files are commonly used, what are the required transfer times?
Areal coverage	What is the operating area in which users will need wireless network coverage? Do usage requirements vary at different locations within this area? Is future growth of the required coverage area expected?
Mobility	If users will move within the operating area while working, will they need to access the WLAN from several fixed locations or will they need continuous service while in motion (mobility); for example to support voice services?
Device interoperability	What types of user devices will need to connect to the network?

User population	What is the total number of users and user devices that are required to be supported? How many users will typically require concurrent service? How much future growth is the network expected to cater for?
Security	How confidential is the information transferred across the network? What level of protection is required against unauthorized access?
Battery life	If mobile devices will be used in the network, how often will the user need to recharge battery operated devices? (Electrical power source)
Economic	What budget is available to implement the WLAN? Are there specific requirements that deliver high value and may justify a higher cost solution?

Establishing Technical Requirements

Technical requirements follow from user requirements, by translating these into the specific technical attributes that are needed to deliver the user requirements. For example, if there is a user requirement for rapid transfer of large files, for example for video editing applications, this will translate into a technical requirement for a high effective data rate. Some technical attributes, such as operating range and those relating to interference and coexistence, will be clarified following site surveying and initial planning of the physical layout of the network hardware.

Table3: WLAN Technical Attributes

Requirement type	Considerations
Effective data rate	The required data rate for a single user will be dictated by the usage model, for example by the typical file size and upload/download time, or by the requirements for voice or video streaming. As discussed in Chapter 6, effective data rates can be significantly lower than a standard PHY layer data rate, and will be further affected by adverse environmental factors such as RF interference.
Network capacity	The required data rate for a single user will be dictated by the usage model, for example by the typical file size and upload/download time, or by the requirements for voice or video streaming. As discussed in Chapter 6, effective data rates can be significantly lower than a standard PHY layer data rate, and will be further affected by adverse environmental factors such as RF interference.

Network capacity	What is the overall network capacity needed to provide the required level of service, given the current and future expected size of the user group and number of user devices? Required capacity will be a key factor both in the technology selection and in determining the appropriate physical architecture for the WLAN.
Quality of service	If the usage model includes applications such as VoWLAN, then guaranteed quality of service will be an important attribute to ensure performance expectations are met.
Application support	Are there specific technical attributes required to support particular usage models?
Network topology	What types of connections are required to meet user requirements? For example, peer-to-peer for local data sharing, point-to-point for linking buildings, etc.
Security	If users' confidentiality requirements are high, then data encryption, network access monitoring and other security measures will be required.
Interference and coexistence	If the WLAN will have to operate in an environment with other wireless networks, such as Bluetooth, or alongside cordless phones, then coexistence will need to be a consideration.
Technology maturity	Before standards have been agreed early products have an interoperability risk, while a fully mature technology may have limited scope for future development and risk early obsolescence as new usage models arise. The significance of this attribute will depend on whether the user requirements are within the proven capabilities of existing technology or require a leading edge solution.
Operating range	The required range will be determined by the physical extent and nature of the operating area, as well as the layout of components such as access points. The overall link budget will be important in implementing point-to-point connections (wireless bridges between buildings).
Network scalability	If the WLAN is likely to require more than a few access points, or significant future growth is anticipated, then ease of initial configuration and ongoing network management tasks will be a requirement, at least for the network manager.

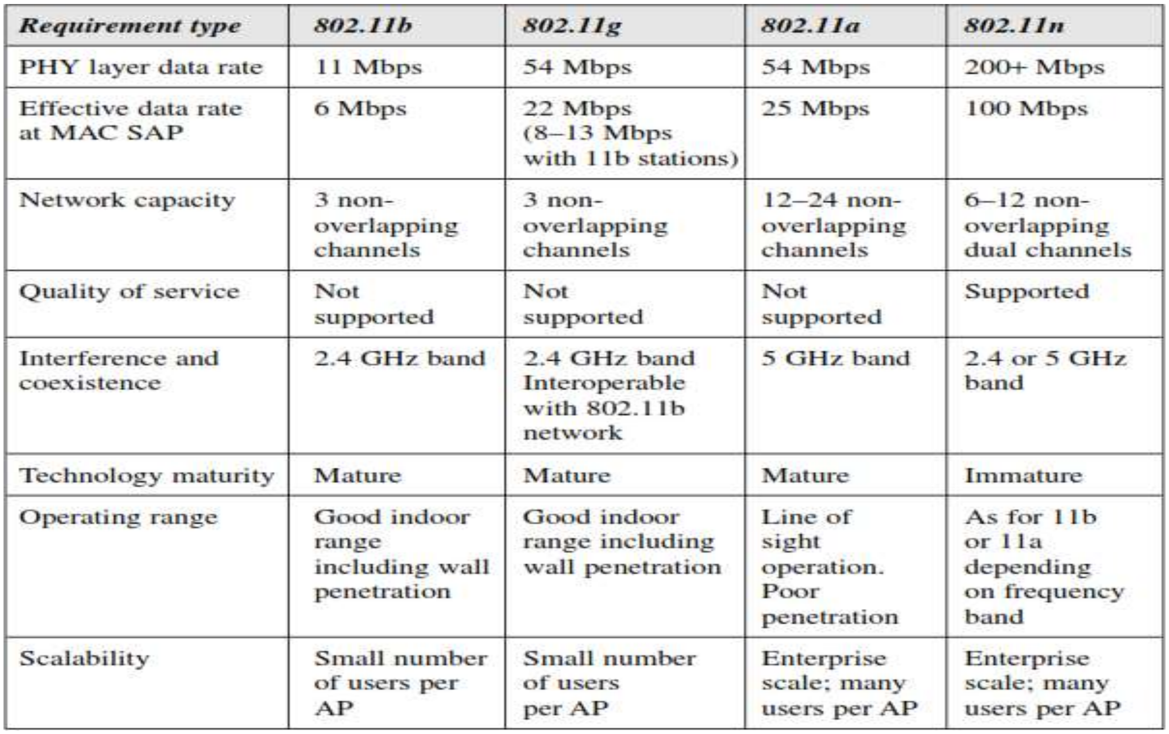
Evaluating available Technologies

Having established the technical attributes necessary to meet user requirements, the available technologies can then be directly assessed against these attributes. A simple table, similar to the example shown in the table above, can be used to display the assessment, resulting in a transparent and objective comparison of the available solutions. More sophisticated evaluation methods can also be applied, for example, by assigning a weighting factor to each requirement and a score to each technical solution depending on the extent to which it meets the requirements.

Network Capacity: The total required network capacity will be determined by the sum of the bandwidth requirements of the maximum number of concurrent users expected on the network, with some allowance being made for the fact that this maximum will occur infrequently and some limited degradation of performance may be acceptable during brief periods of high usage. If this requirement exceeds the capacity of a single access point then multiple access points will be required, up to the limit imposed by the number of available non-overlapping channels.

Operating Range: The operating range of a wireless network link is influenced by a wide range of factors, from the modulation and coding scheme being used to the nature of the materials used in the construction of the building in which the network operates.

Table 4: WLAN Technologies; Technical Attribute Comparison



Requirement type	*802.11b*	*802.11g*	*802.11a*	*802.11n*
PHY layer data rate	11 Mbps	54 Mbps	54 Mbps	200+ Mbps
Effective data rate at MAC SAP	6 Mbps	22 Mbps (8–13 Mbps with 11b stations)	25 Mbps	100 Mbps
Network capacity	3 non-overlapping channels	3 non-overlapping channels	12–24 non-overlapping channels	6–12 non-overlapping dual channels
Quality of service	Not supported	Not supported	Not supported	Supported
Interference and coexistence	2.4 GHz band	2.4 GHz band Interoperable with 802.11b network	5 GHz band	2.4 or 5 GHz band
Technology maturity	Mature	Mature	Mature	Immature
Operating range	Good indoor range including wall penetration	Good indoor range including wall penetration	Line of sight operation. Poor penetration	As for 11b or 11a depending on frequency band
Scalability	Small number of users per AP	Small number of users per AP	Enterprise scale; many users per AP	Enterprise scale; many users per AP

- ✓ **Selection of proper APs for the deployment**

Whether you're installing access points at a large office, home, warehouse or open area like a park or boardwalk, taking the following steps will typically leave you with a usable WiFi network that will stay connected and provide that bandwidth throughput that you expect.

1. Understand all of your network requirements

Knowing your network requirements is perhaps the most essential stage of any WiFi installation. Think about how many people, or more specifically, how many devices, will be connecting to the network and what types of activities they will be doing

2. Choose the right equipment for your wireless network

Once you determine your requirements, it's a lot easier to find the right access point, but the large selection can still present a challenge.

3. Be aware of the network limitations of your devices

It's important to remember that network performance does not solely depend on your Internet connection and network equipment. The devices you use to access the Internet may also have limitations that you should take into account when planning your wireless access point installation.

4. Consider the various types of cables you will need to use

It's weird but wireless Internet does require wires. At the very least, every single access point you use will require at least one cable, either for data connectivity or power. We typically recommend using POE (power over Ethernet) switches in order to deliver data connectivity and power using a single Cat5 or Cat6 cable.

5. Be aware of nearby interference that can impact your wireless access point installation

To understand interference, you first have to understand how WiFi works. Your access point is essentially using radio frequencies to communicate with your devices and transfer data in the form of packets. WiFi broadcasts on the 2.4 Ghz and 5 Ghz spectrum and within those spectrums a few of the channels are typically used for WiFi.

6. Select a proper location for your wireless access point

There is a common misconception that the best place to position your access point is somewhere central. This can be true in some cases, such as in small apartments or small offices under 1000 sq feet but in a world full of wireless devices, you want to have your access points in a place where people are going to be using those devices. This doesn't mean you should put an access point in every room, but it does prove that proper wireless access point installation requires proper planning.

- ✓ **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.

- Content/Topic 2: Environment evaluation, Collecting and determining information about RF Plan

- ✓ **Surveying the RF environment**

Conducting a site survey is an important step in planning and designing all but the simplest WLAN. It is important to determine the impact of environmental factors on radio wave propagation in the operating area of the LAN, and also to test for the presence of RF signals that will interfere with WLAN performance. The objective of the site survey is to gather enough information to plan the number and location of access points to provide the required coverage, in terms of achieving a minimum required data rate over the operating area.

There are two types of site survey that can be performed which are noise and interference survey and a propagation and signal strength survey.

Noise and Interference Survey: This survey looks specifically for the presence of radio interference coming from other sources, such as nearby networks, military installations, etc., that could degrade WLAN performance.

Propagation and Signal Strength Survey: A well-executed propagation and signal strength survey will help to ensure that network resources are correctly located so that the planned network will not suffer from coverage holes, resulting in areas of poor network performance, and will also ensure that network capacity is properly planned.

- ✓ **Physical site survey**

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 is 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.

- ✓ **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.

- ✓ **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.

- ✓ **Analysis of existing system**

Analysis of existing system is helpful for describing what exists now, especially when it might be changed or replaced. It describes the state, problems, devices and user system requirements of existing network.

- **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.

- **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.

Supposed that today, the network is 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. You must understand the data and application requirements in order to define the expected use cases.

LO2.2. Identification of security requirements

- Content/Topic 1: Identification of WLAN security requirement

✓ **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**.

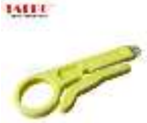
LO2.3. Identification of tools, equipment and materials used in WLAN installation

- Content/Topic 1: Tools used to install WLAN

Everything below is recommended for your tool bag, but some items are optional depending on your working environment.

Table 5: Tools used for installation of an indoor wireless network

Item	**Description**
First Aid Kit	Any compact, portable first aid kit
Ethernet crimper	A crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them to hold each other. The result of the tool's work is called a crimp. Network cables and phone cables are created using a crimping tool (shown here in the first column) to join RJ-45 and RJ-11 connectors to both ends of phone or Cat 5 cable.
6-in 1 Screwdriver	A tool with a flattened or cross-shaped tip that fits into the head of a screw to turn it.
8 inch Adjustable box wrench	A wrench or spanner is a tool used to provide grip and mechanical advantage in applying torque to turn objects usually rotary fasteners, such as nuts and bolts or keep them from turning.
Utility knife	A cutting tool having a sharp replaceable blade that can be retracted into a usually metal handle

Edge cutters	A small, hand-held tool used to cut electric wires.
Measuring tape	A long, thin piece of plastic, cloth, or metal that is marked with units of length (such as inches or centimeters) and that is used for measuring a length of an object or space.
Eye protection glasses	Safety glasses, are forms of protective eyewear that usually enclose or protect the area surrounding the eye in order to prevent particulates, water or chemicals from striking the eyes.
Ear plugs	
Flashlight or Headlamp	A headlamp or flashlight is an electric light tool which gets its power from batteries used as a light source in place where usual right is not enough or at night.
 Cable stripper	CAT5 cable jacket stripper, part # 15015
Wire stripper	A small, hand-held tool used to strip the electrical insulation from electric wires.
8 inch needle-nose pliers	Needle-nose pliers (also known as pointy-nose pliers, long-nose pliers, pinch-nose pliers or snipe-nose pliers) are both cutting and holding pliers used by artisans, jewellery designers, electricians, network engineers and other tradesmen to bend, re-position and snip wire.

Small magnetic level	Magnetic level gauges use magnetism to link the indicator in a gauge to a float inside of a vessel in order to accurately show the level of fluid within.
Cable tacker staple gun	Arrow Fastener T59 Wiring Tacker
Hammer drill	Standard corded drill with "hammer" option. Less expensive than cordless.
Masonry drill bits	For concrete, brick, or stone (Note: not SDS bits)
Regular drill bits	Any set of wood and metal drill bits.
Heavy-duty driver bits	Standard flat head and Phillips driver bits.
Hammer	A tool with a heavy metal head mounted at right angles at the end of a handle, used for jobs such as breaking things and driving in nails.

- Content/Topic 2: Materials and Equipment used to setup a 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.

- ✓ **UTP Patch cord cables**

A patch cable is a length of cable sold with connectors already installed on either end. UTP is Unshielded Twisted Pair cable, which is the most widely used cable type for Ethernet networks.

- ✓ **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.

- ✓ **Battery**

A battery is a device consisting of one or more electrochemical cells with external connections for powering electrical devices such as flashlights, mobile phones and any other portable electric device.

- ✓ **Binoculars**

A 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.

✓ **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

✓ **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.

LO2.4. Design and interpret Building blueprint

- Content/Topic 1: Designing the physical architecture and Schematic diagram of a wireless network system

✓ **Physical architecture Design**

Having built up a picture of the RF environment and gathered data on propagation and signal strength in the operating area, a provisional physical layout of the WLAN can be created. The objective of this stage is to establish a layout of hardware that will ensure complete RF coverage and deliver the required bandwidth to wireless client stations.

Network Physical Layout Design

Planning the physical architecture starts with the floor plans of the operating area and the results of the propagation and signal strength survey, and results in a layout plan detailing;

- the required number of access points

- an optimal antenna type and location
- non-conflicting operating channel
- Proper power setting for each access point.

The channel allocation patterns are based on the three non-overlapping channels 1, 6 and 11 in the 2.4 GHz band. However, in those regulatory domains that permit 13 channels in this band, it is possible to operate four access points with minimal frequency overlap on channels 1, 5, 9 and 13, potentially increasing network capacity by one-third.

Pilot Testing

The design process described above will have established a layout of WLAN hardware which aims to deliver the required data throughput with complete RF coverage of the operating area. A pilot test of the design solution, prior to complete installation, will be helpful to ensure that no requirements have been missed and no limitations of the selected technology have been overlooked.

A pilot test will involve the installation of a number of access points of the same type as are intended for the final installation, to cover part of the operating area. Selecting the part of the operating area that posed the greatest difficulty in the design stage, either because of interference or identified propagation issues will provide the most robust challenge to the design solution.

The pilot test should include monitoring and user responses to the day-to-day performance of the pilot installation, as well as stress testing running under extreme load conditions.

The results of the pilot test will either validate the installation proposed at the design stage, or they may indicate that adjustments in the design are necessary if user requirements and performance expectations are to be fully met.

Interpret 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:

- Number of rooms
- New builds vs. remodels
- Hardware needs
- IT resources (hiring agencies vs. in-house staff)

- Ongoing maintenance and upgrades

✓ **Schematic diagram of a wireless network system**

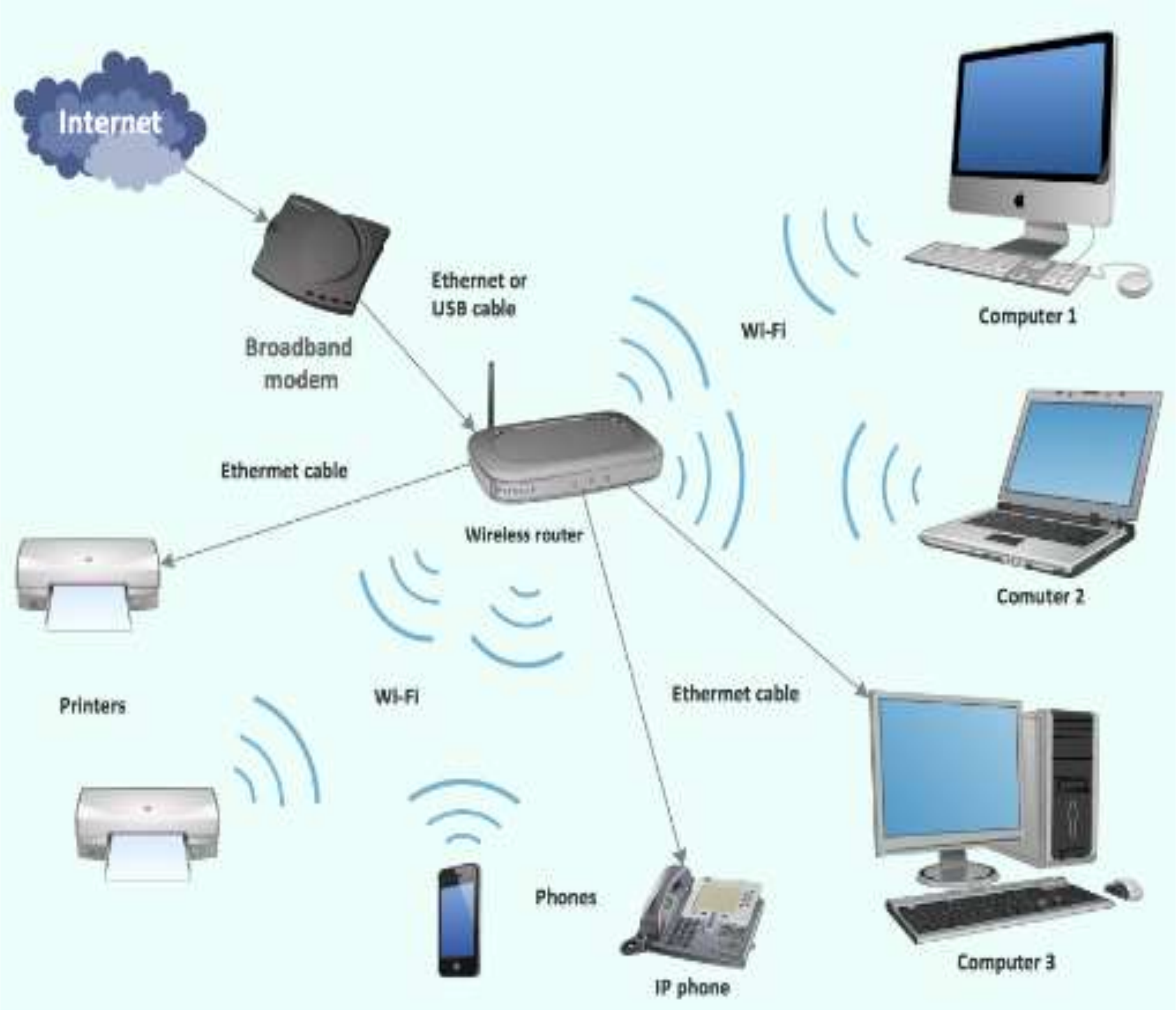


Fig.12: Indoor Wireless network diagram

Learning Unit 3: Configure and Maintain wireless network

LO3.1 Implement SOHO and Enterprise wireless

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

✓ **WLAN Devices**

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

➢ **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
- 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:

- 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.

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**

➢ **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 click apply to confirm.

➢ **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.

➢ **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.

➢ **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.**

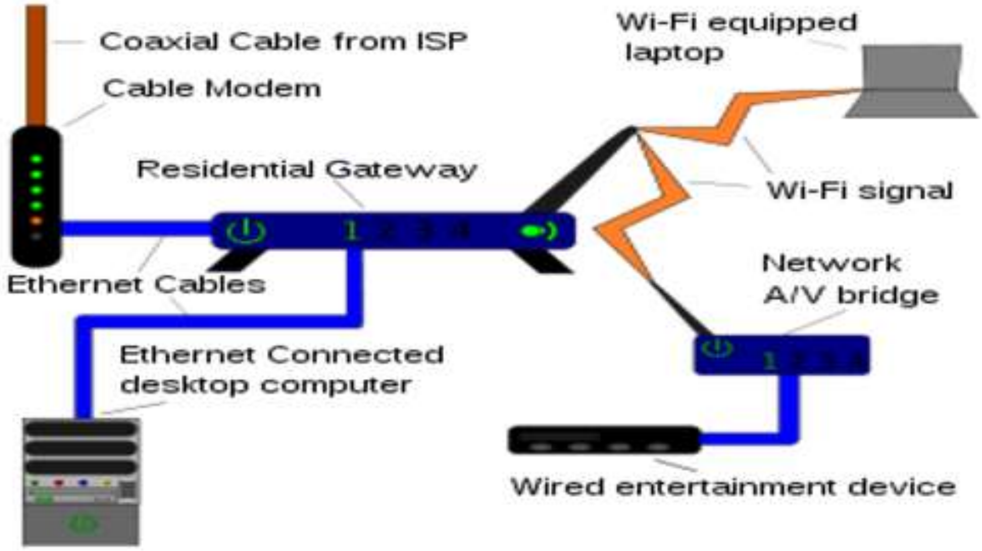


Fig.13: A diagram of a network with a Wireless bridge

- **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!

- **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.

- **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.

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

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

- **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.

How to Install a PC Cards?

- Shutdown the computer and unplug it from the power
- 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.

- **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.

- **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.

- **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.

- **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.

- **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.

LO3.2. Apply security to the technology applied

- Content/Topic 1: Identifying and preventing WLAN 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**

Man-**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. Testing and verification of wireless access point connection and security arrangements

- Content/Topic 1: Wireless LAN Testing considerations

The following are the aspects to consider when planning the testing of a WLAN:

✓ **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

At the end of testing, you have to 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. Troubleshooting of 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 2: 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 192.168.1.5 with a subnet mask of 255.255.255.0, verify that the IP address of the station adapter is similar to 192.168.1.X with a subnet 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. Documentation of 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 problems 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: Suggestion of solutions on problems found

Problem finding

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.

Most of the organizations are stuck with reactive mode due to the complexities of using the existing network management tools. At the same time, business users are more service-focused and less particular about the underlying technology. Organizations demand reliable network maintenance support services that help to get their job done. In spite of using the latest gigabit network hardware, enterprises are plagued with intermittent bandwidth issues, performance issues, and complaints from users of slow network response.

- Content/Topic 4: 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.

- Content/Topic 5: 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 6: Network Devices, equipment and materials used

When you are developing your report, remember to include the network devices, equipment and materials used for better understanding of someone who will read your report.

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
  - **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.

LO4.2. Writing report on the work done

- 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

Network Performance Optimization

Network performance optimization is the process of assessing the network's status on an ongoing basis by monitoring and discovering network traffic and logs. Possible monitoring targets include the following: data rates, available bandwidth, WAN link status, backup time, device response rate, and component failures. The methods in which we will use to discover performance issues may include the following:

Packet shaping this technique is used by specifying what traffic at what rate (rate limiting) in a span of time (bandwidth throttling) you are going to allow in or out of your network.

Traffic shaping is more common at the border routers of an environment working to delay traffic where appropriate as it enters the network.

Traffic policing and traffic contract are terms used to describe how packets are allowed in/out of the network and at what time. Enforcing compliance with the traffic contract is how traffic sources are aware of what traffic policy is in effect. Traffic shaping shapes the traffic into optimal network utilization for the allocated bandwidth on a particular link.

Load balancing Load balancing is a technique used on computer networks to distribute the incoming traffic upon other network devices if there are indications of increased network traffic or “load.” Load balancing allows a group or cluster of data center servers to share the inbound traffic all the while seeming as if there actually is only one external connection. Once traffic enters the network via the one external entry point, it is distributed among other servers internally connected to share the high traffic volumes.

High availability High availability is a system design protocol, which once implemented assures a specific degree of uptime continuity in a specific period of time. The goal of high availability is to ensure users have the maximum uptime so they can access network resources anytime and anywhere. Reducing unplanned downtime increases a business's potential productivity.

Caching engines Cache is data that is copied from the original data and is saved for computers to access locally instead of having to retrieve the same data again from the source server. Accessing cached data is quicker since it is stored in a temporary location for a specific amount of time. Cache engines are servers that are dedicated to caching data for clients. If an item in cache is not used often enough, it is discarded until the client requests it again. Common implementations of cache engines will target Web server content.

Fault tolerance Fault tolerance allows continued operations in the event of a system or system component failure.

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 performance evaluation then 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 problems 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: 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.

- Content/Topic 4: Description of solution implementation

Most of the organizations are stuck with reactive mode due to the complexities of using the existing network management tools. At the same time, business users are more service-focused and less particular about the underlying technology. Organizations demand reliable network maintenance support services that help to get their job done. In spite of using the latest gigabit network hardware, enterprises are plagued with intermittent bandwidth issues, performance issues, and complaints from users of slow network response.

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

Solution implementation involves but not limited to:

- To be committed to a solution
- Take responsibilities and accept the decision.
- Identification and selection of who will implement the solution.
- Carrying out the chosen solution.
- Exploring the best possible means of implementing the solution.

- Content/Topic 5: 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 6: Network Devices, equipment and materials used

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 7: Description of the network status 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. The following is an example of the report form that summarizing the status of network and after work and the work of a network technician.

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	
Customer Name:	
Website /Email address	
PO BOX :	
Office /Mobile Phone Contact :	
Customer office Location:	
Status Before Work:	
User manual and previous report:	
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:	

- Content/Topic 8: Writing technical journal and recommendation report

When it comes to the writing of a technical journal and recommendation report, the format is very important because it is unique from other reports in that it carries technical information. A technical journal and recommendation report contains technical information which should be planned well. You need to understand all the structure to achieve your objective. It should contain the following:

The title page

The title page comes first when you write your technical journal report. The title page contains the title of the journal report the date and the institution details. This first page is also referred to as the cover page. The title is a separate entity when it comes to word count, so you should not include it on your word count.

Introduction

In the introduction, you are supposed to highlight the main aims of the journal report to the reader. Let the reader understand the purpose of you writing. You can also comment on the flow of the journal report so that the reader can know what to expect. You should avoid copying the introduction given in the lab hand out and instead come up with your own.

Experimental details

This is the part that you need to state every detail of the experiment starting from the equipment that you used to the procedure for the test. This section can be omitted if the report did not involve an experiment at all.

Results and discussions

This is where you are expected to explain the results that you obtained from your experiments. You should give a clear explanation so that the reader cannot ask themselves any question on your results.

The body

The body is the most important part of your journal report because it carries your content. You should introduce small subheadings in your journal report as per the point being put across. This will make your work look more presentable as the reader will be guided with this subheading what point you are talking about. You can also place your points in number form or list so that it becomes easier for your reader to understand what you are talking about. You should also separate your points to avoid bringing confusion in your work; each point should be under its subtopic.

Conclusions

When it comes to the writing of your conclusion what you need to do is write a summary of the main points in the body of your report and wrap it up. In conclusion, you also need to use words that suggest you are concluding your work to prepare the reader psychologically, that you are about to finish. Remember also that the conclusion should be short and precise avoid a lot of stories in your concluding paragraph, spare all the stories for the body of your report.

Recommendations

The recommendation usually comes after the conclusion. In the recommendation, you are supposed to suggest solutions to the challenges that are there in the body. This is where your opinion is welcomed.

Reference

In the reference, you need to list all the materials that you used in your research. You may have quoted some text somewhere, so it is at this point that you need to list it so that it does not become a plagiarized work. When you write the reference, you acknowledge that the content that you used is from a certain source.

Appendices

You may have used other materials to put across your points in the journal report such as graphs or diagrams but are not necessarily required in the report. This is the place where you should mention them.

REFERENCES

Agrawal, Rajneesh. 2013. Wireless Networks. New Delhi: Excel Books private ltd.

Authors, WDNDW. 2013. Wireless Networking in the developping World. Alike: Creative Communs Attribution

Beatriz, Glisic Savo & Lorenzo. 2009. Advanced Wireless Networks. John Wiley & Sons.

E.Batista. 2003. Step Back for Wireless ID Tech. Wired News.

Gonzalez, Gerard Zamora. 2013. "Radion Frequenct Identification (RFID) Tags and Reader Antennas Based on Conjugate Matching and Mathematical Concepts." 5-35.

2020. https://www.Cisco-CCNA-Wireless-Training.aspx. July 28. https://www.Cisco-CCNA-Wireless-Training.aspx.

2020. https://www.ciscopress.com/articles/article.asp?p=1271797&seqNum=2. July 27. https://www.ciscopress.com/articles/article.asp?p=1271797&seqNum=2.

J.M. Keenam, A.J. Motley. 1990. "Radio coverage in buildings." British telecom technology journal (British telecom technology Journal) 19-24.

K.Finkelzelle. 2003. The RFID Handbook, Second Edition. John Wiley&Sons.

R.Want. 1999. Bridging Real and Virtual Worlds with Electronic Tags. Proc. ACM Sigghi.

—. 2004. Enebling Ubiquitous Sensing With RFID. Proc.ACM Sigghi.

Rackly, Steve. 2007. Wireless Network Technology. Oxford.

Steve, Rackley. 2011. Wireless Network Technology: From Principles to Successful Implementation. Elsevier.

Stojmenovic. 2006. Handbook of Wireless Network & Mobile Computing. John Wiley& Sons.