IPRC KARONGI
Integrated Polytechnic Regional College
RWANDA POLYTECHNIC
P.O. Box85 KARONGI- RWANDA
Tel:+250 788871075
Email:info@iprcwest.ac.rw
www.iprckarongi.rp.ac.rw

Information Communication Technology Department

IP BASED DEVICES

Program: Information Technology

Module code: ITLID601

Module name: Installation of IP based devices

Credits: 6

Year/ Level: RTQF lev VI, year2

Semester: one

Academic year: 2023/2024

Prerequisites: Small Networks or Introduction to networks

Module leader: Eng. HARERIMANA SOPHONIE San
Assistant Lecturer, RP/IPRC KARONGI.

December 2024

Purpose statement

This core module describes the skills, knowledge and attitude required to install and operate IP based devices. The learner will be able to Identify type of device to install, Install CCTV camera, install printer, operate mobile devices, and maintain IP devices. He/she will be also able to select and arrange different materials, equipment and tools used when installing IP based devices.

Copyright

Module assessment guidelines

Within this module, assessment criteria are used to evaluate the level of attainment students achieve against the learning outcomes. All assessment in Higher Education is criterion referenced, which means that students are assessed based on their performance against clearly stated criteria. The assessment is added after detailed description of a topic. The practical exercises are attached to this document.

Table of Contents

LEARNING UNIT 1 - IDENTIFY TYPE OF DEVICE TO INSTALL

Learning Outcomes:	1.1 Identify all required materials
	1.2 Draw a draft design of the installation
	1.3 Check the functionalities status of the devices
	1.4 Prepare the working environment
Learning hours:	10 Hours

IP based device is Hardware that is connected to a TCP/IP network, including computers, printers, smartphones, tablets, cordless phones, and sensors. For Internet Protocol today, IP mostly refers to the global standard network technology used on the Internet and almost every type of local and long distance digital data network. The Internet protocol is a part of the TCP/IP protocol suite.

Learning Outcome 1.1: Identify all required materials

In this chapters, we are describing the materials needed to install IP devices such as Camera, phones and printers. the tools and other equipment are needed to accomplish the task.

CCTV

CCTV stands for closed-circuit television and is commonly known as video surveillance. “Closed-circuit” means broadcasts are usually transmitted to a limited (closed) number of monitors, unlike “regular” TV, which is broadcast to the public at large. CCTV networks are commonly used to detect and deter criminal activities, and record traffic infractions, but they have other uses.

CCTV technology was first developed in 1942 by German scientists to monitor the launch of V2 rockets. It was later used by American scientists during the testing of the atomic bomb.

How does CCTV work?

Analog and digital systems work quite differently but modern CCTV networks use conversion software and hardware to convert analog to digital. This process is called retrofitting.

A traditional CCTV system comprises:

- One or more cameras (analog or digital), each with a lens equipped with an image sensor
- A recorder – Either a standard video tape recorder for analog systems, or a Direct Video Recorder (DVR) or Network Video Recorder (NVR) for digital systems
- Cables – Either RJ45 for digital or coaxial for analog
- One or more monitors to which the images are transmitted

A camera records images through the lens using image sensors.

These images (and often audio too) are transmitted to **the recorder** or tape, either wirelessly or by cable. Recorders may use analytical software and other smart technologies to scan the data and send automated alerts to either humans, or other systems and devices. This Video Management Software (VMS) records, stores and analyzes video feeds. The software is often self-learning, using machine learning (ML) algorithms that utilize functionality like motion detection, face recognition, people counting, etc.

DVRs are usually part of the CCTV system, connecting to various internal components, not to external networks. DVRs are generally used with analog cameras. In a DVR system, every camera must be connected directly to the recorder.

While DVR systems process footage themselves, NVR systems encode and process data at the camera level, and then stream it to the recorder, which, in turn, is used for storage and remote monitoring. NVR systems usually use IP cameras. In an NVR system, each IP camera connects to the same network.

Monitor(s) can be passively (through software) or actively (by people) monitored. CCTV networks can, and should, themselves be monitored.

Same key CCTV tech terms

Video encoders

Video encoders allows for the migration of analog CCTV systems to some network systems, enabling users to take advantage of cheaper hardware and modern features. The software allows a wired connection and then digitalizes video signals, sending them to a wired or wireless IP-based system.

Image sensors

Cameras use different types of image sensors, which convert light into electronic signals. A sensor comprises multiple photodiodes, or pixels, which register the amount of exposed light and converts it to electrons. The two most popular formats are CMOS (complementary metal oxide semiconductor) and CCD (charged coupled device).

CMOS – These are more cost-effective than CCD sensors. Megapixel (utilizing millions of pixels) CMOS sensors may even rival the quality of CCD sensors.

CCD – These are more costly with a higher power consumption. CCD scanners are generally the best option for inclement light conditions (they have higher light sensitivity) and they are quieter

than CMOS. (While the signal itself is analog, it is converted for transmission by an analog-to-digital converter, which turns the pixels' values into numeric values.)

Image scanning

For digital CCTV, CCD sensors generally use an interlaced scanning method (instant exposure) while CMOS and CCD can use either progressive or interlaced scanning. Analog cameras only use interlaced scanning.

Interlaced (popular for CCD applications) – This technique involves the transmission of odd and even TVLs (l stands for lines) from an image. Cameras with more than 400 lines provide good resolution and more than 700 lines is considered high resolution. These transmissions are repeatedly refreshed, reducing bandwidth and fooling the human brain into believing they are seeing a single, complete picture. That is as long as an interlaced recording is viewed on an interlaced monitor; on a progressive scan monitor, an interlaced image may look jagged. Modern video software will first de-interlace interlaced scans to convert them to progressive scans that can be viewed on analog and progressive scan monitors.

Progressive (popular for CMOS applications) – This method does not divide the image into fields (odd and even lines). Instead, the image is scanned and each line (field) is exposed on a monitor sequentially.

Types of CCTV systems

Analog - Use Bayonet Neill-Concelman (BNC) connectors on coaxial cables to transmit continuous video signals. They are relatively low resolution but cheap and effective. There are more peripherals in an analog system, e.g. standard coaxial cables don't usually transmit audio. Analog signals can be digitized, making it more cost-effective to go digital even with older equipment. The images require a video capture card and can be stored on a PC or tape recorder. A step up, analog HD enables increased resolution over traditional systems (1080 pixels) and are backwards compatible with analog cameras and BNC.

Digital – Digitalize signals at camera level. These systems don't require a video capture card as images are stored directly to a computer but require a (relatively) large amount of space to store recordings, so they are usually heavily compressed.

Network or IP – Used with analog or digital cameras, these systems utilize a video server to

stream footage over the internet. The advantages are the possibility of WiFi and audio, Distributed Artificial Intelligence (DAI) for analyzing image footage, remote access, Power Over Ethernet (POE), and better resolution. Furthermore, IP cameras have the ability to contain more cameras in one, which can cover a wide angle that may normally take multiple cameras or camera systems to cover.

All three options are still equally in use, with a high tendency to IP camera systems and digital video cameras.

CCTV applications

1. **Crime management**

CCTV surveillance can deter potential criminals. When a crime does occur, video footage can help law enforcement to investigate and later provide evidence for prosecution in a law court. Used in conjunction with CCTV, audio, thermal and other types of sensors can alert officials to occurrences that are out of the ordinary, e.g. a fire or gun shots at a location. For businesses, CCTV cameras can detect and monitor in-house criminal activities. Prisons may use video surveillance to prevent drones from delivering drugs and other contraband to prisoners. Security cameras are able to monitor areas that are not easily accessible, e.g. rooftops.

2. **Disaster management**

Using CCTV cameras, emergency services and rescue workers are able to assess and monitor events in real time to relay a "situation" via video to disaster management teams, e.g. from inside a burning building, from a cave or from a helicopter flying over a scene.

3. **City and community street monitoring**

Cameras at traffic lights and elsewhere in cities monitor people to gather traffic statistics as well as evidentiary footage for speeding. An heir to the IoT, the AoT is a Chicago initiative to collect real-time data, primarily weather and environment, about the city. Some sensory nodes include security cameras that analyze the images they record but, in order to protect individuals' privacy, do not transmit or store these images. In the main, a limited number are stored for use by senior researchers in order to "develop the computer vision software". The project has met with some

resistance from privacy watchdogs.

4. **Medical monitoring and diagnosis**

There are about 43 facial muscles that express people's thoughts and feelings. Smart software can identify these expressions, e.g. pain or anxiety, from images more easily that people can. CCTV cameras can also monitor patients – for instance children or the elderly – to identify potential medical crises, e.g. a stroke, or an epileptic or asthma attack.

5. **Behavioral research**

CCTV used to research suicide found that 83 percent of people attempting to throw themselves in front of a train showed specific behaviors. These were later analyzed from CCTV footage and are now used to alert monitor watchers to potential suicides. Surveillance networks are also used by researchers to record crowd activities in public places and prevent anti-social behaviors. For instance, cameras have been used at schools for security, and to record bullying or playground incidents on video.

6. **Retail intelligence**

Market intelligence garnered from video surveillance of customers is being used to analyze buying trends and enable enhanced strategizing, e.g. how do people shop, which aisles do they traverse the most, how likely are they to respond to calls to action within different store layouts. Heat maps can show the highs and lows of shopper traffic at specific locations in a store, helping stores to identify peak buying times, preferred promotion types, and staffing requirements for peak shopping periods.

Type of Tools, materials and equipment used during installation

Digital multimeter: An electronic device used for measuring voltage, resistance and current. It is used for checking voltage and continuity in the CCTV field.	
CCTV Cable crimping tool : Used for crimping and cutting a RJ45 connector to a LAN cable	
CCTV Cable stripper (for RG58,59)	
Cable tester: This is a tool for connectivity measurement, which is used for CAT5 and CAT6 cable testing. This will check every connection of the cable to assure if it is perfect or not.	

Handheld CCTV Monitor: It is a small monitor which has the required video inputs and used for checking the field anytime needed.	
LCD service Monitor CCTV Monitor is one of the most important elements of CCTV systems that provide real-time feedback from CCTV cameras and security surveillance equipment	
Tool Bag: All the tools mentioned must be neatly arranged in a tool bag, otherwise the required tool may not be found at the time of need.	
Drill Machine: Drill machines are two types – a hand drill while the other is a bench drill machine. These are used for camera mounting and also installing cable in conduits	
Measuring Tape: Ideal for any installation, it is used for measuring first. It can be used for measuring the length of cable	

Cleaning Brush: Often dust causes a lot of disorder in the CCTV system and hence it is required to carry a cleaning brush.	

Types of tools and their use

Pliers: Used for holding objects firmly and also cutting wires and cables	
Hammer: Used for hitting, especially for cable clipping works	
Allen keys a spanner designed to fit into and turn an Allen screw	
Soldering iron	
Di-soldering pump	

Types of materials and their use

- ✓ Soldering tin
- ✓ Glue
- ✓ Silicon
- ✓ Insulator tape
- ✓ Screws
- ✓ Universal anchors
- ✓ Trunking

Type of Connectors

BNC Connectors BNC Connectors are components attached to the end of a coaxial cable that connect with an audio, video, data or other device to prevent interference and damage.	
Video balun Balun is to allow the traditional 75-ohm coaxial video cable to be replaced by twisted pair cable in the CCTV security and surveillance environment.	
RJ 45 Connector RJ45 connector is the piece attached to the end of an Ethernet cable that plugs into your IP Camera, computer, router, etc.	

Review Qwestions

1. How does CCTV work?
2. Describe the following:
   a. Video encoders
   b. Image sensors
3. What are the types of CCTV systems
4. Detail the CCTV applications
5. Identify the Type of Tools, materials and equipment used during CCTV installation

Learning Outcome1.2: Draw a draft design of the installation

TYPES OF NETWORK STRUCTURE/TOPOLOGY

What is Network?

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Types of network topologies in a CCTV Security System

- ✓ **Physical Topology:**

Any network can be designed in basically four types of topology. The nomenclature of same is, as per the way devices are connected to each other through different nodes and links.

1. Bus Topology
2. Ring Topology
3. Star Topology
4. Mesh Topology

Bus Topology

This types of topology comes handy when there is already a backbone of optical fiber cable around the perimeter of a premises, as all the devices/cameras in our case are connected to the network through this common backbone. Although it is the simplest way to design the network of a CCTV System, but problem with a Bus Topology is that there is a lot of dependency on the status of the backbone employed in the network. Diagram below shows the indicative representation of a Bus Topology

Ring Topology

As the name suggests, the geometric arrangement of the devices in this case is such that every device is connected in a ring making a closed logical loop in the networks. Every device receives the signal first and then transmits it further to the other device. No of networking devices in this case are increased in terms of Light Interface Units for splicing, pigtails switches etc.

Star Topology

This types of topology in generally used when there is small premises and cabling required is less, as all the devices are networked to a central hub or a core switch directly. In this case network failure for one device does not affect the other devices.

Mesh Topology

Mesh Topology is generally not used in a CCTV network considering high usage of cables in it. Principally in this topology all the devices are connected to each other, giving a lot of redundancy to the network

From the above types of topologies, there is no absolute right or absolute wrong topology. It totally depends on the site condition, budget available, availability of cable route, criticality of the network that decisions are taken accordingly. And one particular topology or a combination of different topologies can be used

- ✓ **Logical topology**

IP Address

An IP address is a number identifying of a computer or another device on the Internet. It is similar to a mailing address, which identifies where postal mail comes from and where it should be delivered. IP addresses uniquely identify the source and destination of data transmitted with the Internet Protocol.

IP Address classes

With an IPv4 IP address, there are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. Each class allows for a range of valid IP addresses, shown in the following table.

Class	Address range	Supports
Class A	**1.0.0.1 to 126.255.255.254**	**Supports 16 million hosts on each of 127 networks.**
Class B	**128.1.0.1 to 191.255.255.254**	**Supports 65,000 hosts on each of 16,000 networks.**
Class C	**192.0.1.1 to 223.255.254.254**	**Supports 254 hosts on each of 2 million networks.**

Fig: IP Address classes

- Ranges 127.x.x.x are reserved for the loopback or localhost, for example, 127.0.0.1 is the loopback address. Range 255.255.255.255 broadcasts to all hosts on the local network.

Class	Address range	Supports
Class A	**1.0.0.1 to 126.255.255.254**	**Supports 16 million hosts on each of 127 networks.**
Class B	**128.1.0.1 to 191.255.255.254**	**Supports 65,000 hosts on each of 16,000 networks.**
Class C	**192.0.1.1 to 223.255.254.254**	**Supports 254 hosts on each of 2 million networks.**
Class D	**224.0.0.0 to 239.255.255.255**	**Reserved for multicast groups.**
Class E	**240.0.0.0 to 254.255.255.254**	**Reserved for future use, or research and development purposes.**

- **Class A:** The first octet is the network portion. Octets 2, 3, and 4 are for subnets/hosts
- **Class B:** The first two octets are the network portion. Octets 3 and 4 are for subnets/hosts
- **Class C:** The first three octets are the network portion. Octet 4 is for subnets/hosts

Static vs. dynamic IP addresses

IP addresses are assigned in two different ways. They may be **dynamically** assigned (they can change automatically) or **statically** assigned (they're intended not to change, and must be changed manually). Most home networks use dynamic allocation. Your router uses **DHCP** to temporarily assign, or "lease," an IP address to your device. After a sometime, this lease "expires," and the router renews your old address or assigns you a new one depending on the router configuration.

NETWORK DEVICES

What are network devices?

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network

Types of Network devices

Commonly used Network devices

1. Switch

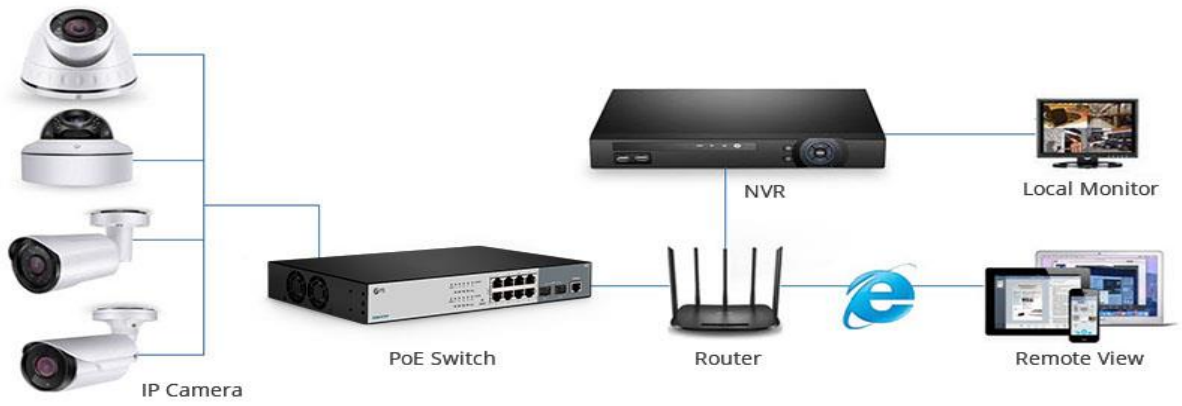
A switch enables multiple devices to be connected onto the same network forinstance CCTV Cameras,NVR,DVR,Computers,etc, and to control or restrict how those devices communicate, you must have the ability to configure the switch. The amount of control you have depends on the type of switch: managed, unmanaged, or somewhere in between. Examining the benefits of each switch type lets you make the right decision for your specific application.

- **PoE Switch for IP Camera Systems**

PoE, short for power over Ethernet, is a technology designed to simplify cabling by simultaneously sending power and data over one Ethernet cable. Nowadays, PoE is commonly used in systems

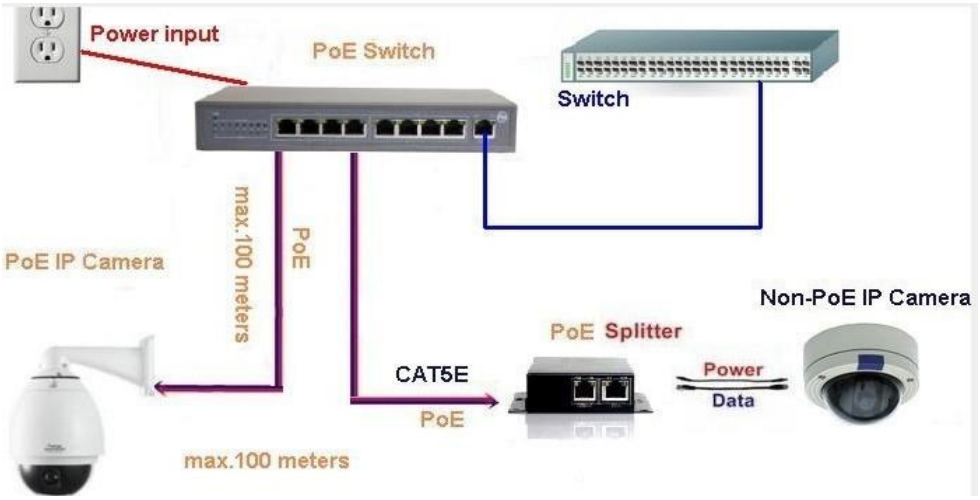
like security camera systems, not only because Ethernet cable is cheap and easy to run, but also because PoE and IP technologies support high-resolution cameras that offer improved video quality for IP camera systems.

A PoE switch for IP cameras is a device used to connect and power the IP cameras via Ethernet cables. The primary function of a PoE switch in IP camera system is to interconnect the cameras to an NVR (Network Video Recorder) and transmit the data (video and audio) to be recorded in such a device.



The benefits of using a PoE switch for IP camera systems are as follows:

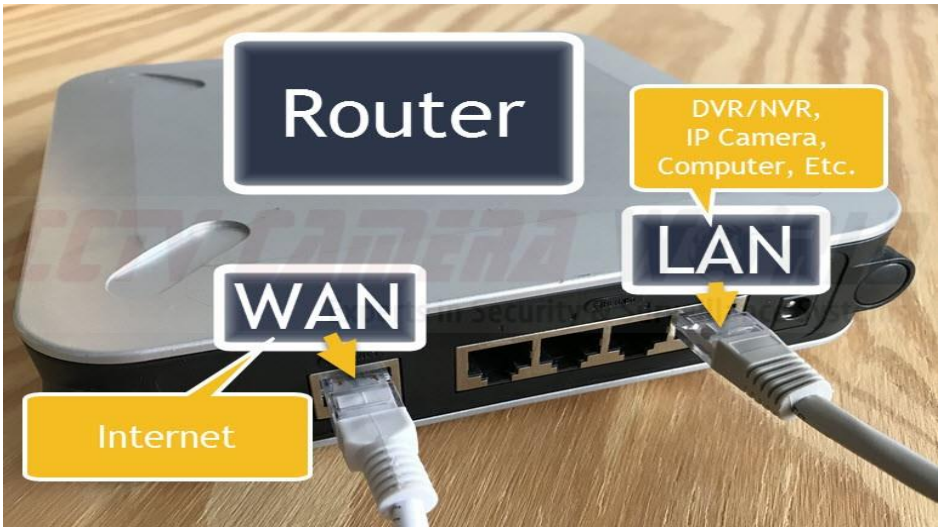
- Longer runs - IP cameras can be installed in locations of longer distance;
- More connected devices - more IP cameras can be connected together;
- Larger power output - more power can be supplied for IP cameras;
- Easier to manage - activity lights on switch will help troubleshoot the IP cameras;



Router

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

A router has a WAN port and also a LAN (Local Area Network) port. The Internet connection coming from the modem connects to the router's WAN port. The LAN port is used for other network devices, such as computers, IP cameras or NVRs to connect to.



ACCESS POINT

While an access point (AP) can technically involve either a wired or wireless connection, it commonly means a wireless device. An AP can operate either as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to anotherWireless access points (WAPs) consist of a transmitter and receiver (transceiver) device used to create a wireless LAN (WLAN). Access points typically are separate network devices with a built-in antenna, transmitter and adapter.

Review questions

1. What is Network?
2.Describe Types of network topologies in a CCTV Security System.
3. what are the IP address classes?
4. Specify the private IP addresses.
5. Explain the Commonly used Network devices

Learning Outcome 1.3: Check the functionalities status of the devices

1. Digital video recorder (DVR)

Selecting the right DVR is an important aspect of the security system. There are many factors which have to be taken into consideration before choosing the right DVR for the installation.
DVR Specifications to consider are:

- **Frame rate**

Frame rate refers to the number of frames a DVR can record at a given resolution each second. Real time is considered to be 30 frames per second (FPS). So in order to record real time video on 16 channels you would need a unit that can record a total of 480 frames per second (FPS).
Some DVRs are able to display live video at 30 FPS on each channel, but what is truly important is the recorded video, not the live video. Also due consideration should be given to the local authorities regulations regarding the FPS, when selecting a DVR.

- **Compression**

Once video is transmitted to the DVR it is compressed to conserve storage and make internet viewing without lags. The compression used can vary from nearly no compression like wavelet or MJPEG, to the higher compression methods like MPEG4 or H.264. Compression methods can vary between DVRs, there are even some that use a combination of compressions, one for recording and one for streaming over the internet. Most of the newer DVRs use H.264 which is 40% more efficient both in storage and internet streaming.

- **Storage capacity**

How much storage a DVR can hold is an important factor to consider. Based on the recording days required and the FPS, the hard drive capacity can be calculated. Most of the DVRs comes with 1, 2 or 3 HDD Bays from capacities ranging from 4TB to 12 TB.

- **Audio Recording**

Audio recording is not required in most of the installations. Some DVR's will accommodate audio recording for all channels while some DVRs will have audio recording for few channels only. Again based on the requirements and the budget allocated for the DVR, the right type of DVR should be chosen. Please check the local laws prior to using the audio recording.

- **Video Output**

DVR's will often only offer BNC video output which would require the use of a BNC to VGA

converter to view the DVR on a standard VGA monitor. The higher end units will have a VGA output as well as a BNC out and also HDMI output.

- **Remote View**

Most DVR's these days are networkable and can allow an individual to log in using internet explorer to view their security cameras. The more advanced units will have a client software that allows an individual to view multiple DVR's at the same time. This software may have features like E-mapping, camera groupings, various user levels, the ability to restrict access to individual functions and cameras for each user and more.

DVRs record video in different resolutions, please check the DVR to know which video resolutions are supported. The following resolutions are available based on the DVR model you are using in your installation.

CIF (352 x 240 or 288),
2CIF (704 x 240 or 288),
4CIF (704 x 480 or 576),
Half D1 (720 x 240 or 288),
D1 (720 x 480 or 576),
960H (960 x 480 or 576),

2. Network Video Recorder (NVR)

A Network Video Recorder (NVR) performs the same function as its DVR cousin in the analog world. It captures each camera's signal, compresses, and records it. The main difference is that the video feeds are digital (and much higher resolution) and not analog.
Software built into the NVR provides features such as intelligent search and zoom, etc. The NVR combines the video streams from the cameras and handles the broadcast over the LAN and internet for local and remote viewing.

3. Cameras

CCTV cameras come in various types, styles, and configurations. A wide range of cameras are available to select from, depending on what will work best for the application. Some of the camera types based on the shape of the camera are Dome, Bullet, and PTZ Speed Dome Cameras. For outdoor applications, cameras installed should be both vandal and weather proof. To capture video images in low lighting conditions, IR Cameras are used, these cameras come fitted with IR illuminators.

- **Dome Cameras**

The "dome" are the most commonly used in indoor applications. The dome shape makes it difficult to tell the direction that these cameras are facing, and thus are ideal for deterring criminals from executing their plans. The dome cameras are easy to install and can be easily mounted on both horizontal and vertical surfaces such as walls and ceilings. Dome Cameras are also available with IR illuminators, which enable the cameras to capture video images in low lighting conditions. The dome shaped, hardened plastic casing that covers the camera also protects it from vandalism.

- **Bullet Cameras** have a long, cylindrical, and tapered shape, similar to that of a "rifle bullet." These cameras are ideal for outdoor use, particularly in applications that require long distance viewing. Bullet Cameras are usually installed inside protective casings, which protect against dust, dirt, rain, hail and other harmful elements. A mounting bracket enables the camera to be pointed in the desired direction. The cameras come fitted with either fixed or varifocal lens.

- **PTZ Speed Domes** are also dome shaped CCTV Cameras, but include pan, tilt and zoom capability. These cameras can be set up to follow pre-programmed routes and presets. Most applications include a joystick-keyboard, operated by surveillance personal. Speed Domes are used to monitor vast areas such as Malls, Supermarkets Aisle, Car Parks, etc. However for reliable security, fixed non-rotating CCTV Cameras, should be installed, as very often during important incidents if the Speed Dome monitored another area no evidence will be captured. All security risk areas like gates, ground floor window rows, doors and fire exits should have their own fixed non-rotating camera, zoomed in on the highest risk area.

4. Backup power UPS

The CCTV system should not be connected directly to raw line power because of the potential problems such as voltage surges, electrical noise etc. It require line conditioning and filtering to provide a source of continuous uninterrupted power at all times including power failure. For this reason, an Uninterrupted Power Supply (UPS) must be used

The following example illustrates how to determine the size and type of UPS system to choose for an installation having 32 cameras, 2 main monitors, 2 Spot monitors and 2 DVRs and a PC. The total backup power required is 729 VA (watts). Since UPS systems are usually available in 250, 500, and 1000 VA ratings, choose the 1000 VA unit. This will provide a good margin of safety.

Equipment	Power (Watts)	Quantity	Total VA*(Volt-Ampere)
IR Bullet Camera	6	16	96
Dome Camera	3	16	48
16 Channel DVR	80	2	160
17" LCD Spot Monitor	50	2	100
PC	300	1	300
Misc	25		25
Total VA Required			**729**
* Assuming resistance load (Power factor = 1) VA = WATTS			

Review questions

1. Give the functionalities status of the devices:
   a.Digital video recorder (DVR)
   b.Network Video Recorder
2. Describe the types of Cameras.
3. why do we need UPS?

TYPES OF NETWORK MEDIA

Network Media

Network media is the actual path over which an electrical signal travels as it moves from one component to another. This chapter describes the common types of network media, including twisted-pair cable, coaxial cable, fiber-optic cable, and wireless.

- Coaxial cable consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor.
- UTP cable is a four-pair wire medium used in a variety of networks.
- STP cable combines the techniques of shielding, cancellation, and wire twisting.
- Fiber-optic cable is a networking medium capable of conducting modulated light transmission.
- Wireless signals are electromagnetic waves that can travel through the vacuum of outer space and through a medium such as air.

1. Twisted-Pair Cable

Twisted-pair cable is a type of cabling that is used for telephone communications and most modern Ethernet networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs. When electrical current flows through a wire, it creates a small, circular magnetic field around the wire. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Thus, the two magnetic fields cancel each other out. They also cancel out any outside magnetic fields. Twisting the wires can enhance this cancellation effect. Using cancellation together with twisting the wires, cable designers can effectively provide self-shielding for wire pairs within the network media.

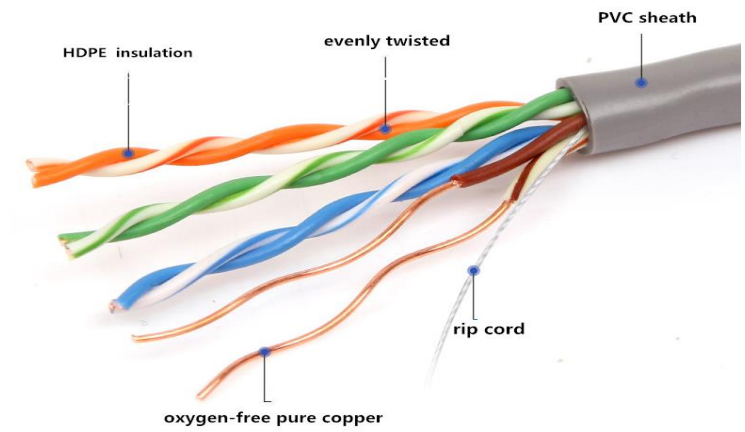
Two basic types of twisted-pair cable exist: unshielded twisted pair (UTP) and shielded twisted pair (STP). The following sections discuss UTP and STP cable in more detail.

1.1.UTP Cable

UTP cable is a medium that is composed of pairs of wires. UTP cable is used in a variety of networks. Each of the eight individual copper wires in UTP cable \is covered by an insulating

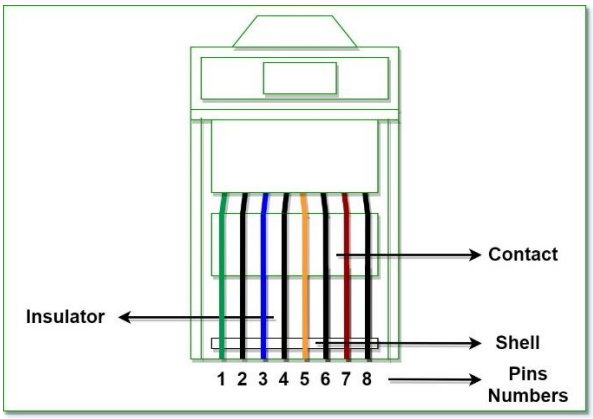
material. In addition, the wires in each pair are twisted around each other.

UTP cable relies solely on the cancellation effect produced by the twisted wire pairs to limit signal degradation caused by electromagnetic interference (EMI) and radio frequency interference (RFI). To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies. UTP cable must follow precise specifications governing how many twists or braids are permitted per meter (3.28 feet) of cable.

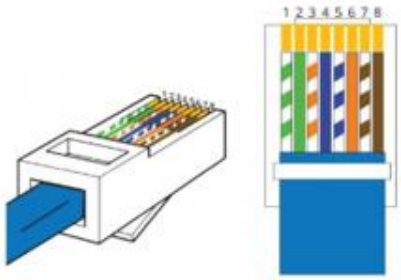


UTP cable often is installed using a Registered Jack 45 (RJ-45) connector. The RJ-45 is an eight-wire connector used commonly to connect computers onto a local-area network (LAN), especially Ethernets.

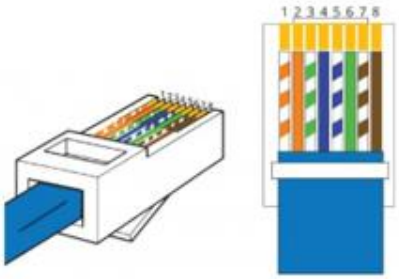
RJ-45 Connectors



Typical RJ45



T-568A



T-568B

When used as a networking medium, UTP cable has four pairs of either 22- or 24-gauge copper wire. UTP used as a networking medium has an impedance of 100 ohms; this differentiates it from other types of twisted-pair wiring such as that used for telephone wiring, which has impedance of 600 ohms.

UTP cable offers many advantages. Because UTP has an external diameter of approximately 0.43 cm (0.17 inches), its small size can be advantageous during installation. Because it has such a small external diameter, UTP does not fill up wiring ducts as rapidly as other types of cable. This can be an extremely important factor to consider, particularly when installing a network in an older building. UTP cable is easy to install and is less expensive than other types of networking media. In fact, UTP costs less per meter than any other type of LAN cabling. And because UTP can be used with most of the major networking architectures, it continues to grow in popularity.

Disadvantages also are involved in using twisted-pair cabling, however. UTP cable is more prone to electrical noise and interference than other types of networking media, and the distance between signal boosts is shorter for UTP than it is for coaxial and fiber-optic cables.

Although UTP was once considered to be slower at transmitting data than other types of cable, this is no longer true. In fact, UTP is considered the fastest copper-based medium today. The following summarizes the features of UTP cable:

- Speed and throughput—10 to 1000 Mbps
- Average cost per node—Least expensive
- Media and connector size—Small
- Maximum cable length—100 m (short)

Commonly used types of UTP cabling are as follows:

Category 1—Used for telephone communications. Not suitable for transmitting data.

Category 2—Capable of transmitting data at speeds up to 4 megabits per second (Mbps).

Category 3—Used in 10BASE-T networks. Can transmit data at speeds up to 10 Mbps.

Category 4—Used in Token Ring networks. Can transmit data at speeds up to 16 Mbps.

Category 5—Can transmit data at speeds up to 100 Mbps.

Category 5e —Used in networks running at speeds up to 1000 Mbps (1 gigabit per second [Gbps]).

Category 6—Typically, Category 6 cable consists of four pairs of 24 American Wire Gauge (AWG) copper wires. Category 6 cable is currently the fastest standard for UTP.

1.2 Shielded Twisted-Pair Cable

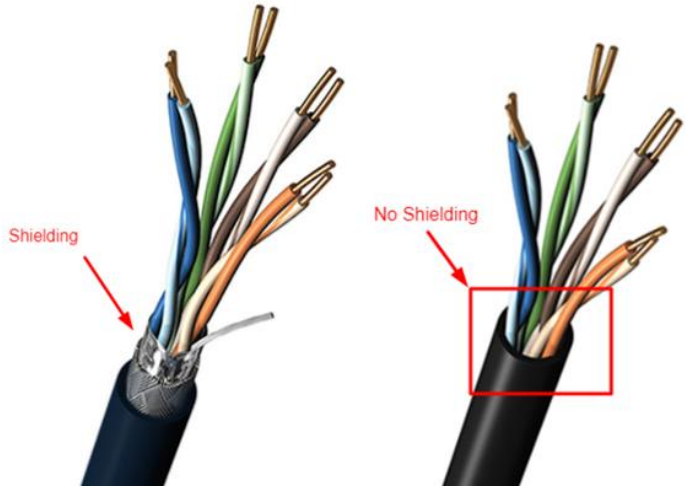
Shielded twisted-pair (STP) cable combines the techniques of shielding, cancellation, and wire twisting. Each pair of wires is wrapped in a metallic foil. The four pairs of wires then are wrapped in an overall metallic braid or foil, usually 150-ohm cable. As specified for use in Ethernet network installations, STP reduces electrical noise both within the cable (pair-to-pair coupling, or crosstalk) and from outside the cable (EMI and RFI). STP usually is installed with STP data connector, which is created especially for the STP cable. However, STP cabling also can use the same RJ connectors that UTP uses.

Sheilded Twisted Pair (STP)

Although STP prevents interference better than UTP, it is more expensive and difficult to install. In addition, the metallic shielding must be grounded at both ends. If it is improperly grounded, the shield acts like an antenna and picks up unwanted signals. Because of its cost and difficulty with termination, STP is rarely used in Ethernet networks. STP is primarily used in Europe.

The following summarizes the features of STP cable:

- Speed and throughput—10 to 100 Mbps
- Average cost per node—Moderately expensive
- Media and connector size—Medium to large
- Maximum cable length—100 m (short)



When comparing UTP and STP, keep the following points in mind:

- The speed of both types of cable is usually satisfactory for local-area distances.
- These are the least-expensive media for data communication. UTP is less expensive than STP.
- Because most buildings are already wired with UTP, many transmission standards are adapted to use it, to avoid costly rewiring with an alternative cable type.

2. Coaxial Cable

Coaxial cable consists of a hollow outer cylindrical conductor that surrounds a single inner wire made of two conducting elements. One of these elements, located in the center of the cable, is a copper conductor. Surrounding the copper conductor is a layer of flexible insulation. Over this insulating material is a woven copper braid or metallic foil that acts both as the second wire in the circuit and as a shield for the inner conductor. This second layer, or shield, can help reduce the amount of outside interference. Covering this shield is the cable jacket.

Coaxial cable supports 10 to 100 Mbps and is relatively inexpensive, although it is more costly than UTP on a per-unit length. However, coaxial cable can be cheaper for a physical bus topology because less cable will be needed. Coaxial cable can be cabled over longer distances than twisted-pair cable. For example, Ethernet can run approximately 100 meters (328 feet) using twisted-pair cabling. Using coaxial cable increases this distance to 500m (1640.4 feet).

For LANs, coaxial cable offers several advantages. It can be run with fewer boosts from repeaters for longer distances between network nodes than either STP or UTP cable. Repeaters regenerate the signals in a network so that they can cover greater distances. Coaxial cable is less expensive than fiber-optic cable, and the technology is well known; it has been used for many years for all types of data communication.

When working with cable, you need to consider its size. As the thickness, or diameter, of the cable increases, so does the difficulty in working with it. Many times cable must be pulled through existing conduits and troughs that are limited in size. Coaxial cable comes in a variety of sizes. The largest diameter (1 centimeter [cm]) was specified for use as Ethernet backbone cable because historically it had greater transmission length and noise-rejection characteristics. This type of coaxial cable is frequently referred to as Thicknet. As its nickname suggests, Thicknet cable can be too rigid to install easily in some situations because of its thickness. The general rule is that the more difficult the network medium is to install, the more expensive it is to install. Coaxial cable is more expensive to install than twisted-pair cable. Thicknet cable is almost never used except for special-purpose installations.

A connection device known as a vampire tap was used to connect network devices to Thicknet. The vampire tap then was connected to the computers via a more flexible cable called the attachment unit interface (AUI). Although this 15-pin cable was still thick and tricky to terminate, it was much easier to work with than Thicknet.

In the past, coaxial cable with an outside diameter of only 0.35 cm (sometimes referred to as Thinnet) was used in Ethernet networks. Thinnet was especially useful for cable installations that required the cable to make many twists and turns. Because it was easier to install, it was also cheaper to install. Thus, it was sometimes referred to as Cheapernet. However, because the outer copper or metallic braid in coaxial cable comprises half the electrical circuit, special care had to be taken to ensure that it was properly grounded. Grounding was done by ensuring that a solid electrical connection existed at both ends of the cable. Frequently, however, installers failed to properly ground the cable. As a result, poor shield connection was one of the biggest sources of connection problems in the installation of coaxial cable. Connection problems resulted in electrical noise, which interfered with signal transmittal on the networking medium. For this reason, despite its small diameter, Thinnet no longer is commonly used in Ethernet networks.

The most common connectors used with Thinnet are BNC, short for British Naval Connector or Bayonet Neill Concelman, connectors. The basic BNC connector is a male type mounted at each end of a cable. This connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector. BNC T-connectors are female devices for connecting two cables to a network interface card (NIC). A BNC barrel connector facilitates connecting two cables together.

Thinnet and BNC Connector

The following summarizes the features of coaxial cables:

- Speed and throughput—10 to 100 Mbps
- Average cost per node—Inexpensive
- Media and connector size—Medium
- Maximum cable length—500 m (medium)

Primary Cable Types

The vast majority of networks today are connected by some sort of wire or cabling, which act as the network transmission medium carrying signals between computers. There is a variety of cable that can meet the varying needs and sizes of networks, from small to large.

Cabling can be confusing. Belden, a leading cable manufacturer, publishes a catalog that lists more than 2,200 types of cabling. Fortunately, only three major groups of cabling connect the majority of networks:

- Coaxial Twisted-pair

    - Unshielded twisted pair
    - Shielded twisted-pair
- Fiber-optic

The next part of this lesson will describe the features and components of these three major cable types. Understanding their differences will help you determine when to use each type of cabling.

Coaxial

At one time, coaxial cable was the most widely used network cabling. There were a couple of reasons for coaxial's wide usage. Coaxial was relatively inexpensive, and it was light, flexible, and easy to work with. It was so popular that it became a safe, easily supported installation.

In its simplest form, coaxial consists of a core made of solid copper surrounded by insulation, a braided metal shielding, and an outer cover. One layer of foil insulation and one layer of braided metal shielding is referred to as dual shielded. However, quad shielding is available for environments that are subject to higher interference. Quad shielding consists of two layers of foil insulation and two layers of braided metal shielding.

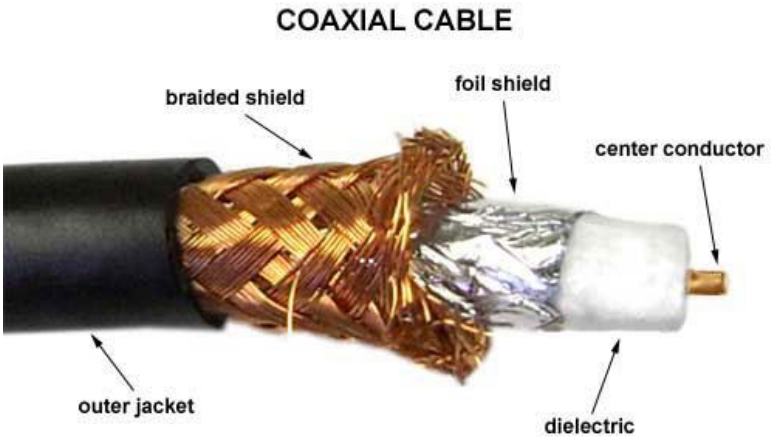


Figure 2.1: Coaxial cable showing various layers

Shielding refers to the woven or stranded metal mesh (or other material) that surrounds some types of cabling. Shielding protects transmitted data by absorbing stray electronic signals, called noise, so that they do not get onto the cable and distort the data.

The core of a coaxial cable carries the electronic signals which make up the data. This core wire can be either solid or stranded. If the core is solid, it is usually copper.

The core is surrounded by a dielectric insulating layer which separates it from the wire mesh. The

braided wire mesh acts as a ground and protects the core from electrical noise and crosstalk. Crosstalk is signal overflow from an adjacent wire.

The conducting core and the wire mesh must always be separated from each other. If they touch, the cable will experience a short, and noise or stray signals on the mesh will flow onto the copper wire. This will destroy the data.

The entire cable is surrounded by a non-conducting outer shield, usually made of rubber, Teflon, or plastic.

Coaxial cable is more resistant to interference and attenuation than twisted-pair cabling. Attenuation is the loss of signal strength which begins to occur as the signal travels further along a copper cable.

Figure 2.2: Attenuation causes signals to deteriorate

The stranded, protective sleeve can absorb stray electronic signals so they do not affect data being sent over the inner copper cable. For this reason, coaxial is a good choice for longer distances and for reliably supporting higher data rates with less sophisticated equipment.

Types of Coaxial Cable

There are two types of coaxial cable:

- Thin (thinnet)
- Thick (thicknet)

What type you select depends on the needs of your particular network.

Thinnet

Thinnet is a flexible coaxial cable about .25 inch thick. Because this type of coaxial is flexible and easy to work with, it can be used in almost any type of network installation. Networks that use thinnet have the cable connected directly to a computer's network adapter card.

Thinnet coaxial cable can carry a signal up to approximately 185 meters (about 607 feet) before the signal starts to suffer from attenuation.

Cable manufacturers have agreed upon certain designations for different types of cable. Thinnet is included in a group referred to as the RG-58 family and has a 50-ohm impedance. Impedance is the resistance, measured in ohms, to alternating current flowing in a wire. The main difference in the RG-58 family is the center core of copper. It can either be a stranded wire or solid copper core.

Cable Description

RG-58 /U Solid copper core

RG-58 A/U Stranded wire core

RG-58 C/U Military specification of RG-58 A/U

RG-59 Broadband transmission such as cable television

RG-6 Larger in diameter and rated for higher frequencies than RG-59, but used for broadband transmissions as wellRG-62 ArcNet networks.

Coaxial Connection Hardware

Both thinnet and thicknet use connection components, known as a BNC (British Naval Connector), to make the connections between the cable and the computers. There are several important components in the BNC family, including the following:

The BNC cable connectorThe BNC cable connector is either soldered or crimped to the end of a cable.

The BNC T connectorThis connector joins the network interface card in the computer to the network cable.

BNC T connector

Coaxial Cable Grades and Fire Codes

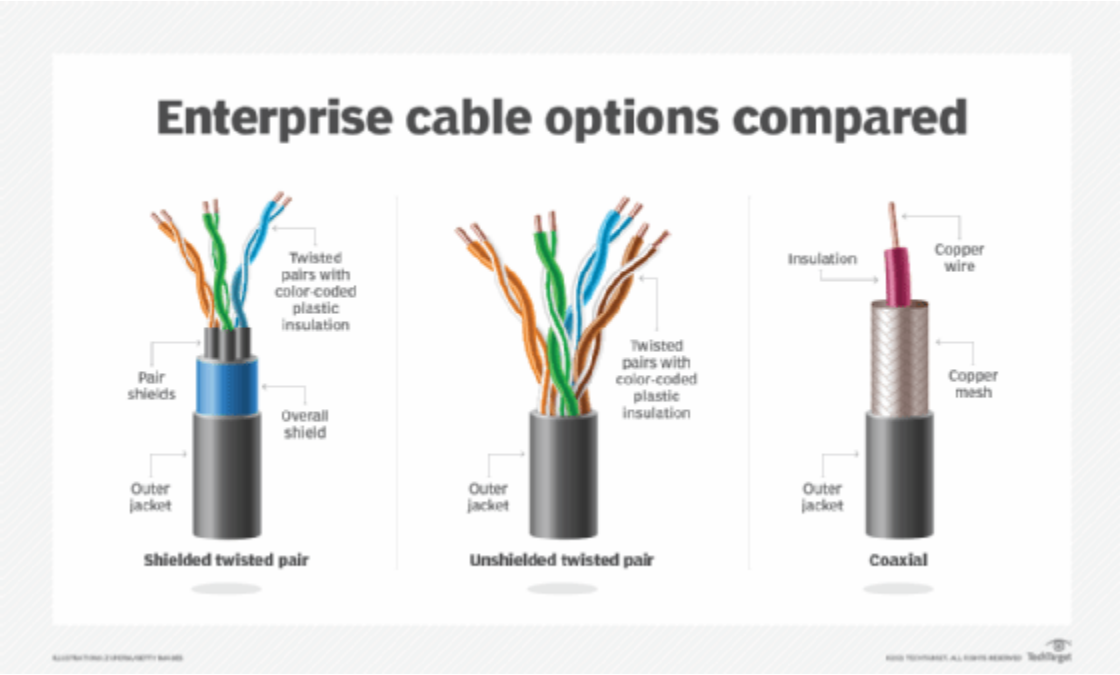
The type of cable grade that you should use depends on where the cables will be in your office. Coaxial cables come in two grades:

- Polyvinyl chloride

- Plenum

Polyvinyl chloride (PVC) is a type of plastic used to construct the insulation and the cable jacket for most types of coaxial cable. PVC coaxial cable is flexible and can be easily routed in the exposed areas of an office. However, when it burns, it gives off poisonous gases.

A plenum is the short space in many buildings between the false ceiling and the floor above; it is used to circulate warm and cold air through the building. Fire codes are very specific on the type of wiring that can be routed through this area, because any smoke or gas in the plenum will eventually become part of the air breathed by everyone in the building.



Plenum cabling refers to coaxial that contains special materials in its insulation and cable jacket. These materials are certified to be fire resistant and produce a minimum amount of smoke. This reduces poisonous chemical fumes. Plenum cable can be used in the plenum area and in vertical runs (for example, in a wall) without conduit. However, plenum cabling is more expensive and less flexible than PVC cable.

Note: Please consult your local fire and electrical codes for specific regulations about running networking cable in your office.

Coaxial Considerations

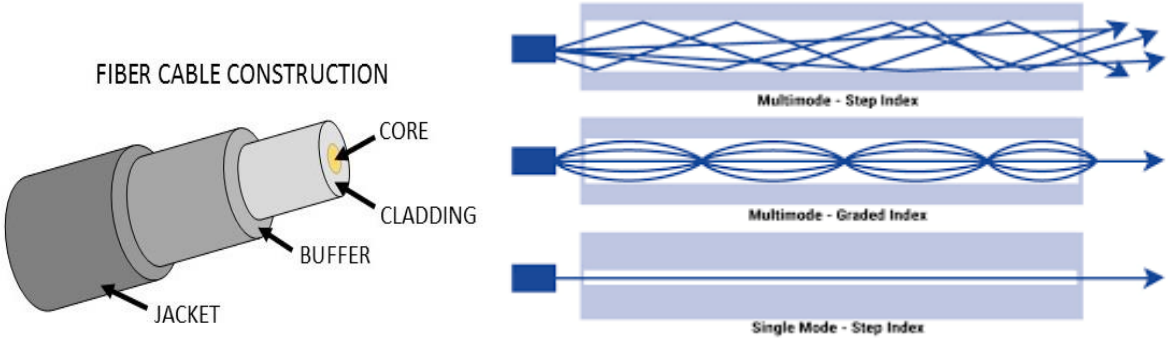
Consider these coaxial capabilities when making a decision on the type of cabling to use.

Use coaxial cable if you need:

- A medium that will transmit voice, video, and data.
- To transmit data longer distances than less expensive cabling can transmit.
- A familiar technology that offers reasonable data security.

3. Fiber Optic Cable

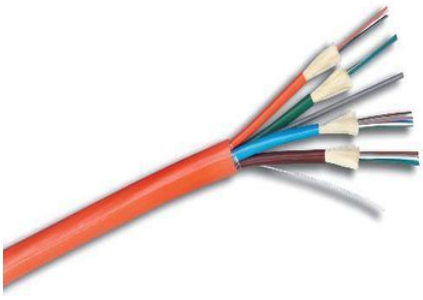
An optical fiber (or fibre in British English) is a flexible, transparent fiber made by drawing glass (silica) or plastic to a diameter slightly thicker than that of a human hair. Optical fibers are used most often as a means to transmit light[a] between the two ends of the fiber and find wide usage in fiber-optic communications, where they permit transmission over longer distances and at higher bandwidths (data transfer rates) than electrical cables. Fibers are used instead of metal wires because signals travel along them with less loss; in addition, fibers are immune to electromagnetic interference, a problem from which metal wires suffer. Fibers are also used for illumination and imaging and are often wrapped in bundles so they may be used to carry light into, or images out of confined spaces, as in the case of a fiberscope. Specially designed fibers are also used for a variety of other applications, some of them being fiber optic sensors and fiber lasers.



3.1 Multi Mode Fiber Optic Cable

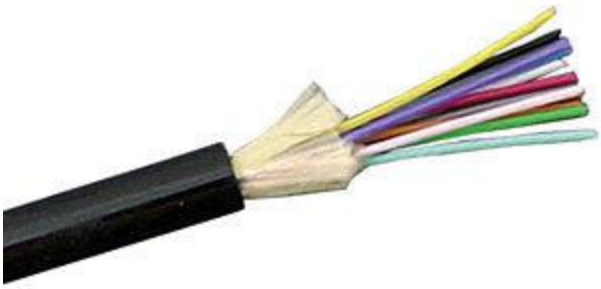
Fiber optic cable is sometimes called wave guide or light guide because it guides the light waves along the length of the cable. Multi mode fiber is used for short cable runs, usually 1.6 mi (approximately 2 km) or less.





3.2 Single Mode Fiber Optic Cable

Single mode fiber optic cable can operate over much longer distances. Because the fiber only allows one mode of light to propagate, light pulses put on the fiber keep their shape much longer. This allows the light pulses to travel much further without interfering with other pulses. Single mode fibre is recommended for cable runs in excess of 1.6 mi.



4. Wireless Network

To receive the signals from the access point, a PC or laptop must install a wireless adapter card (wireless NIC). Wireless signals are electromagnetic waves that can travel through the vacuum of outer space and through a medium such as air. Therefore, no physical medium is necessary for wireless signals, making them a very versatile way to build a network. Wireless signals use portions of the RF spectrum to transmit voice, video, and data. Wireless frequencies range from 3 kilohertz (kHz) to 300 gigahertz (GHz). The data-transmission rates range from 9 kilobits per second (kbps) to as high as 54 Mbps.

The primary difference between electromagnetic waves is their frequency. Low-frequency electromagnetic waves have a long wavelength (the distance from one peak to the next on the sine wave), while high-frequency electromagnetic waves have a short wavelength.

Some common applications of wireless data communication include the following:

- Accessing the Internet using a cellular phone
- Establishing a home or business Internet connection over satellite
- Beaming data between two hand-held computing devices
- Using a wireless keyboard and mouse for the PC

Another common application of wireless data communication is the wireless LAN (WLAN), which is built in accordance with Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards. WLANs typically use radio waves (for example, 902 megahertz [MHz]), microwaves (for example, 2.4 GHz), and IR waves (for example, 820 nanometers [nm]) for communication. Wireless technologies are a crucial part of the today's networking. See Chapter 28, "Wireless LANs," for a more detailed discuss on wireless networking.

Review questions

1.State the types of network media.

2.Describe the two basic types of twisted-pair cable.

3.With a sketch, demonstrate the two layer of coaxial cable construction.

4.Differanciate with specifications, the two modes of Fiber optic.

1

Learning Outcome 1.4: Prepare the working environment

CCTV Pole and Foundation Erection

1. Understanding methods of Erection
2. Understanding the field requirement
3. Excavation and Backfilling method
4. PCC
5. Pre Cast Foundation erection
6. Pole and cantilever Assembly
7. Pole erection
8. Leavling and Alignment of pole
9. Cable routing
10. HDPE Laying
11. Manual and HDD Trenching
12. Man hole
13. Safety
14. Site Tidiness

LEARNING UNIT 2- INSTALL CCTV CAMERA

Learning Outcomes:

2.1 Fix trunking and cables conduits

2.2 Fix and mount cameras

2.3 Connect cameras and controller devices

2.4 Configure the CCTV camera system

2.5 Test the CCTV camera system

Learning hours: **15 Hours**

Learning Outcome 2.1: Layout and fix trunking and cables conduits

- Understanding methods of Erection
- Understanding the field requirement
- Excavation and Backfilling method
- PCC
- Pre Cast Foundation erection
- Pole and cantilever Assembly
- Leavling and Alignment of pole
- Cable routing
- HDPE Laying
- Manual and HDD Trenching
- Man hole
- Safety
- Site Tidiness

Learning Outcome 2.2 : Fix and mount cameras

CCTV Camera Installation

1. Understanding types of CCTV Camera
2. Understanding the site sketches & drawings
3. Network Cable laying
4. RJ45 Connector Crimping
5. Camera Mounting Assembly
6. Camera Mounting Marking
7. Mounting and Camera fixing
8. Power supply unit Connection
9. Network Cable Connection
10. Lens Adjustment
11. Safety
12. Site tidiness

Learning Outcome 2.3: Connect cameras and controller devices

What Is an IP Camera

IP camera (Internet protocol camera) distinguishes itself with a direct connection to the Internet, which enables it to send and receive data via the Internet.

After proper IP camera configuration, you are able to access the CCTV camera via your network mobile devices (phone, PC or tablet). That's to say, you can watch camera live, receive push alerts, and check the camera recordings wherever you are (inside or outside home network).

IP camera data transmission is based on the IP camera address assigned by the router or the NVR. So typically, you will need to find the right IP camera address to access the camera on the Internet.

Network Video Recorder Installation

1. Understanding Installation Method
2. Interpretation of sketches & drawings
3. Network rack Installation

4. Hard disk Installation
5. Digital Video Recorder Mounting Assembly
6. Digital Video Recorder Mounting
7. Power Supply Adapter Connection
8. Network Cable connection

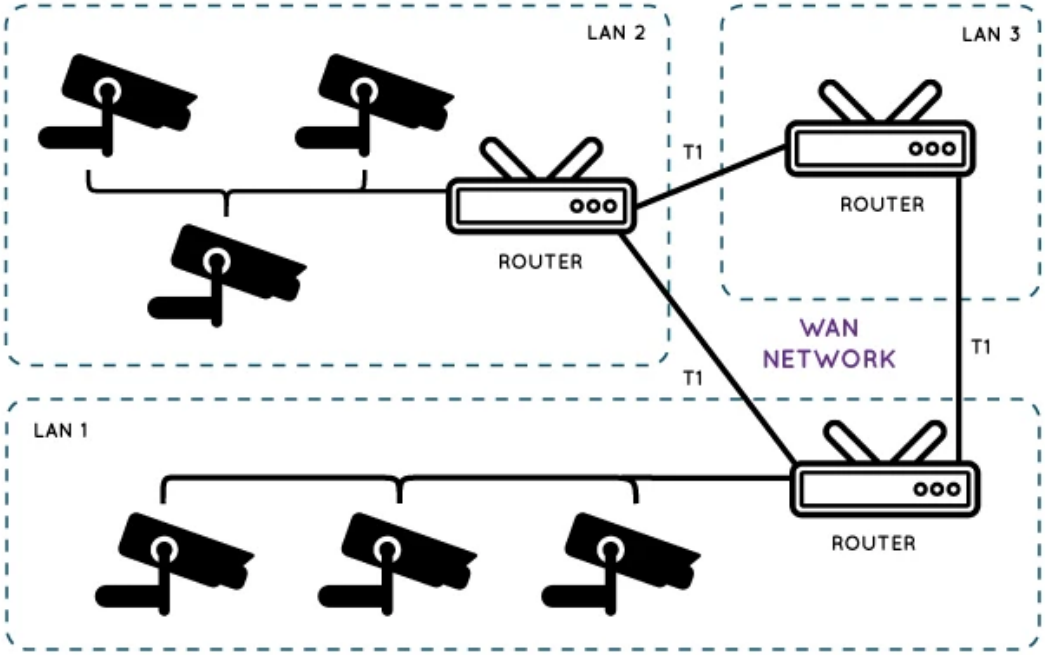
Network Switch Installation and Configuration

1. Understanding Installation and Configuration method
2. Network Switch Assembly
3. Network Switch Installation
4. Connect Console cable
5. Create User name and Password
6. Date and Time configuration
7. Create Management IP Address
8. Enabling Telnet
9. Creating VLAN
10. Port Security
11. Poe enabling and Power Budget
12. Create Access List
13. Routing configuration
14. Multicast Enabling

IP Camera Configuration Guide

Technically, the major task for IP camera configuration is to get the right IP address of your camera which serves as the only clue to find it among various devices attached to the same network. Note that the IP camera installation and configuration on the local area network (LAN) could be a little different from that in the wide area network (WAN). And whichever way you go with, the cameras should be on the network so that they can be accessed.

LAN vs WAN



Learning Outcome 2.4: Configure the CCTV camera system

The most general steps for different types of CCTV configuration are:

1. Set up a Camera
2. Set up a Monitor
3. Set up Network devices
4. Set up Encoder and Decoders
5. Set up recording devices (NVR & DVR, VMS)
6. Set up Server and Storage
7. Set up UPS/DCPS
8. Set up Pole and foundation
9. Connect up and test system elements
10. Adjust the Back Focus of a lens to prevent picture going out of focus from day to
11. night.
12. Setup For Wireless communication
13. Setup For Video Management Software

14. Perform Trouble shooting and maintenance
15. Perform Testing and Commissioning

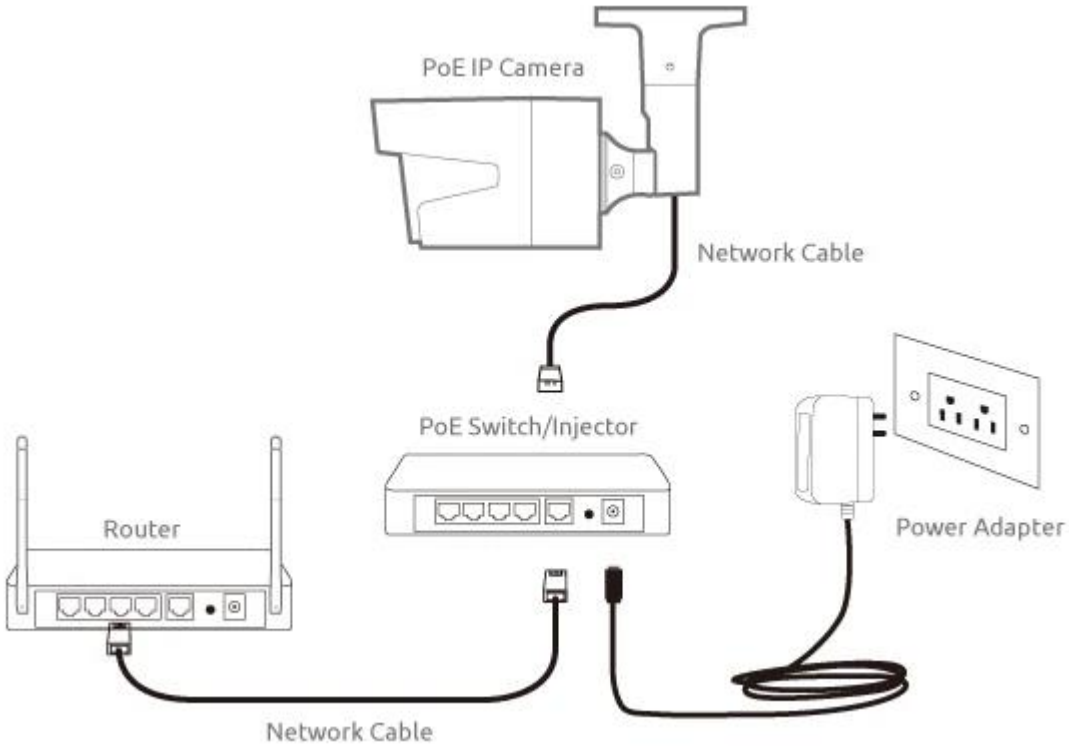
But here below are some example from them.

So we'll break the IP camera configuration with networking into three parts:

Step 1. Configure IP Camera Network

Before you start setting the IP camera configuration, make sure both your monitoring devices and CCTV cameras (and NVR) are connected to the home network. This could be done with or without router.

Here is a CCTV camera wire connection diagram for your reference:



PoE IP Camera Network

Reolink RLC-410 PoE IP camera network diagram

Step 2. IP Camera Configuration on LAN

To configure IP cameras on the LAN, like the typical home network, you need to find out the CCTV camera local IP address.

Previously we introduced 3 ways for you to do that.

And then you only need to input the IP address on the web search bar to get into the camera's web UI, and then everything will appear.

Step 3. CCTV Camera Configuration on WAN

As for IP camera configuration on the WAN, port forwarding is a typical way to go, which generally requires the camera local IP address, HTTP and RTMP port number, and the WAN IP address.

What is port forwarding?

Simply put, port forwarding transfers your local IP address into a public one which is used to access a specific camera in a wide area network (WAN), like crossing the neighborhoods or even countries.

Shortcut to IP Camera Configuration

Get confused by the technical terms on the IP camera configuration steps above?

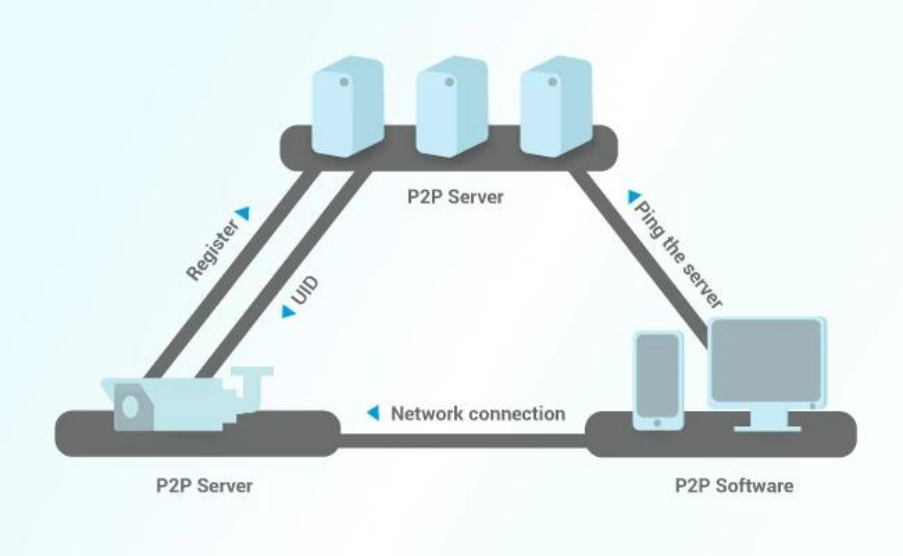
Is there any easy way to configure IP camera for people with the only basic understanding of the Internet?The answer is absolutely YES.

P2P technology makes the IP camera configuration easy enough for even beginners. Moreover, P2P security cameras (including both wireless cameras and wired PoE cameras) effectively save your trouble of fixing the IP address for stable remote viewing.

So what is P2P? How to configure IP camera on Internet with P2P?

Simply put, each P2P enabled security camera is registered at the P2P server at the developer level and identified with a unique ID number (UID). So every time you want to access the camera locally or remotely, you only need to ping the P2P server via the security camera software with the camera UID.

P2P



For P2P IP camera configuration, basically, only 3 simple steps are required:

#1. Download the IP camera configuration software Reolink App or Client to your phones or PC.

#2. Launch the Reolink App or Client and enter the UID to add the security camera.

Connect IP Camera Network via Mobile Phone

(CCTV camera mobile configuration screenshot)

#3. Click the camera on the software and the configuration of CCTV camera is done. You can then watch the live view inside and outside your home network.

Is the IP camera configuration secure via the P2P server?

Actually, P2P is not a new technology. It has been used maturely on many fields including the Skype. And reputable brands like Reolink have adopted many ways to keep the data transmission

absolutely secure, including using multiple servers and advanced encryptions.

So if you are looking for an IP camera with easy setup, the P2P camera will not let you down (Download the IP camera client manual for more detailed guide with screenshots of every setting step).

IP Camera Configuration Without Router

Generally speaking, the CCTV camera router configuration is indispensable for remote viewing. Yet the 4G P2P LTE camera makes it possible for you to set up wireless cameras without connecting to a router.

The trick is that 4G security cameras are running on the cellular network provided by a SIM card, and thereby its data transmission and the whole CCTV IP camera configuration are independent from the WiFi network.

But how could we do the IP camera configuration if it doesn't have an IP address (since it is not connected to the router)?

That's where the P2P technology comes in. P2P provides an easy exit for remote viewing with no need of an IP address: Simply entering the UID and password on the camera app or client, and then you can access the camera.

So the 4G LTE camera is your best choice if you don't want to mess around with the IP camera router configuration.

Reolink Go

100% Wire-Free 3G/4G LTE Mobile Camera

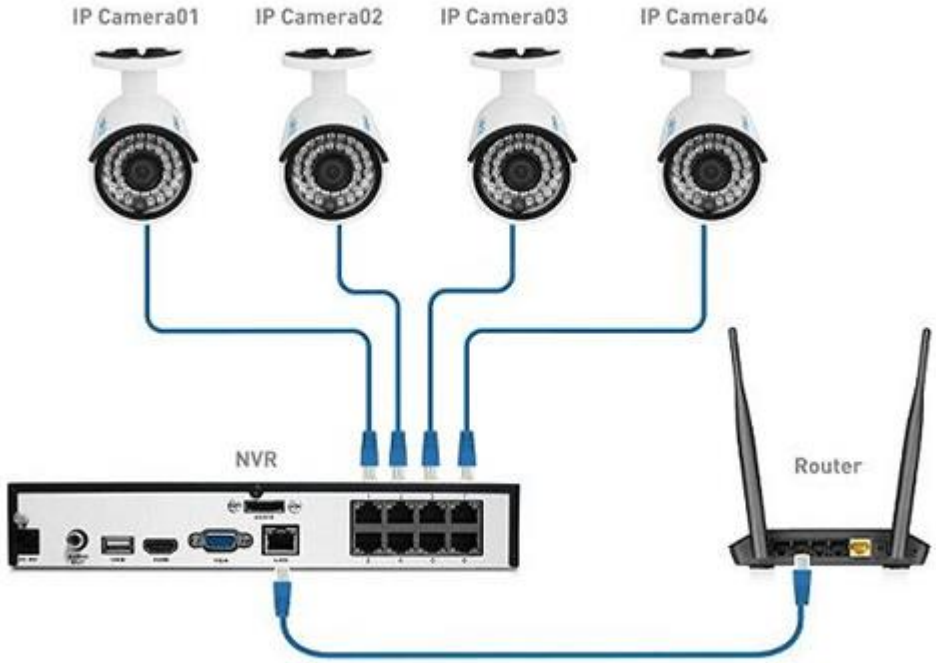
No WiFi & Power Needed; Rechargeable Battery or Solar Powered; 1080p Full HD; Starlight Night Vision; 2-Way Audio; Live View Anytime Anywhere.

CCTV Camera Without Configuration

To make IP camera configuration even easier, you can just skip the whole IP camera setup thing with an NVR security camera system.The configuration of DVR/NVR camera surveillance is a little bit different.

The point is you don't need to do the IP camera configuration with NVR if you only want the cameras to record and save on the network video recorder (NVR).That's because the NVR and cameras connected to it will automatically build a private network once powered up. Within the subnet, cameras and NVR could communicate with each other. So you don't need to connect it to a router or do any IP camera configuration.

For example, the Reolink RLK8-410B4 can save your trouble of IP camera NVR configuration and offer you 24/7 protection. Check the NVR CCTV camera setup with this diagram:



RLK8-410B4 Diagram

However, if you want remote viewing, say accessing the cameras on your phone or receiving push notifications, you still need the help of a router and add the cameras to the surveillance software. (Don't forget the P2P technology can simplify the CCTV camera system configuration.)

To Configure NVR for IP Camera with a PoE Switch

There are ethernet switches for IP surveillance in different configurations. The configuration starts with a hardware setup. Here is how you can proceed with the hardware setup:

Take the Ethernet cable from the router and connect it at the back of NVR. Ensure that NVR is connected to the Internet.

Use Ethernet cables to connect the IP cameras to PoE NVR. As the NVR is enabled with the PoE technology, it can easily power the IP cameras.

Take an HDMI cable or a VGA cable to connect NVR and TV or monitor. Ensure that you use the right input to connect the TV or the monitor— HDMI 1, HDMI 2, or VGA.

When these steps are performed properly then NVR and IP camera connection can be easily made. Software setup is the next step in the configuration, and this can be easily done by following the instruction manual provided by the manufacturer.

How to Configure NVR for IP Camera without PoE Switch?

As discussed before, NVR without PoE switch has no Ethernet ports at its back panel. It utilizes an external power adapter or an external PoE switch to power each IP camera. Like NVR with a PoE switch, the configuration of NVR for IP camera without a POE switch also begins with the hardware configuration. Here is how to proceed:

Take an Ethernet cable to connect the LAN port on the external PoE switch and the router. Then connect the router with the non-PoE NVR.

Use Ethernet cables to connect all IP cameras to the PoE switch RJ45 ports. The PoE switch will deliver power as well as support video transmission.

Use an HDMI cable or VGA cable to connect the monitor and the NVR. Always use the right input for making the connection.

Recording will be enabled only when users add the cameras to NVR. This can be easily done by referring to the steps in the instruction manual.

Important Questions on Setup of NVR with IP Camera Answered

Here is everything you may want to know about the configuration of NVR with IP Camera:

Why NVR must be connected to the Internet?

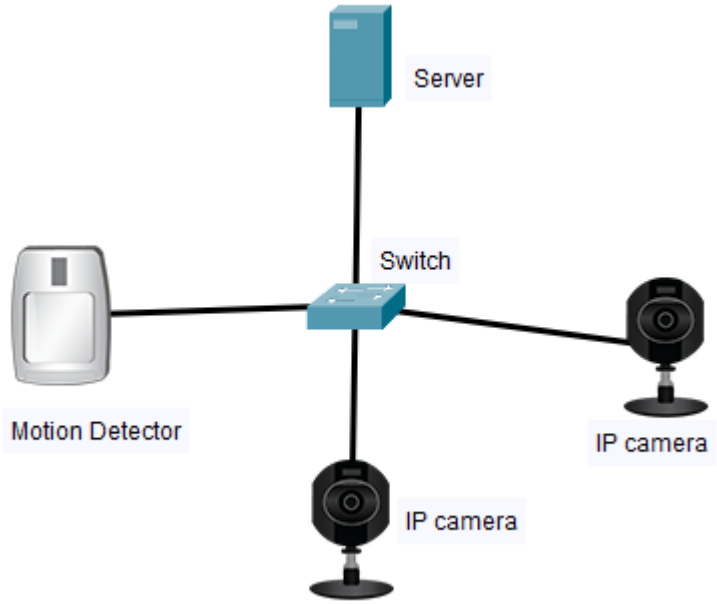
NVR when connected to the Internet provides easy remote access of the recordings. It sends alerts or notifications to users regularly and creates backup of the videos on cloud storage solutions. In

the absence of the Internet, NVR will record and stream the videos, but they will not be remotely accessible to users.

What is the maximum transmission distance of the camera from the NVR?

The maximum transmission distance of the Ethernet cable connecting the NVR and an IP camera is 100 meters. This distance limited due to the attenuation of signals. The Ethernet extender is used to extend the transmission distance beyond 100 meters.

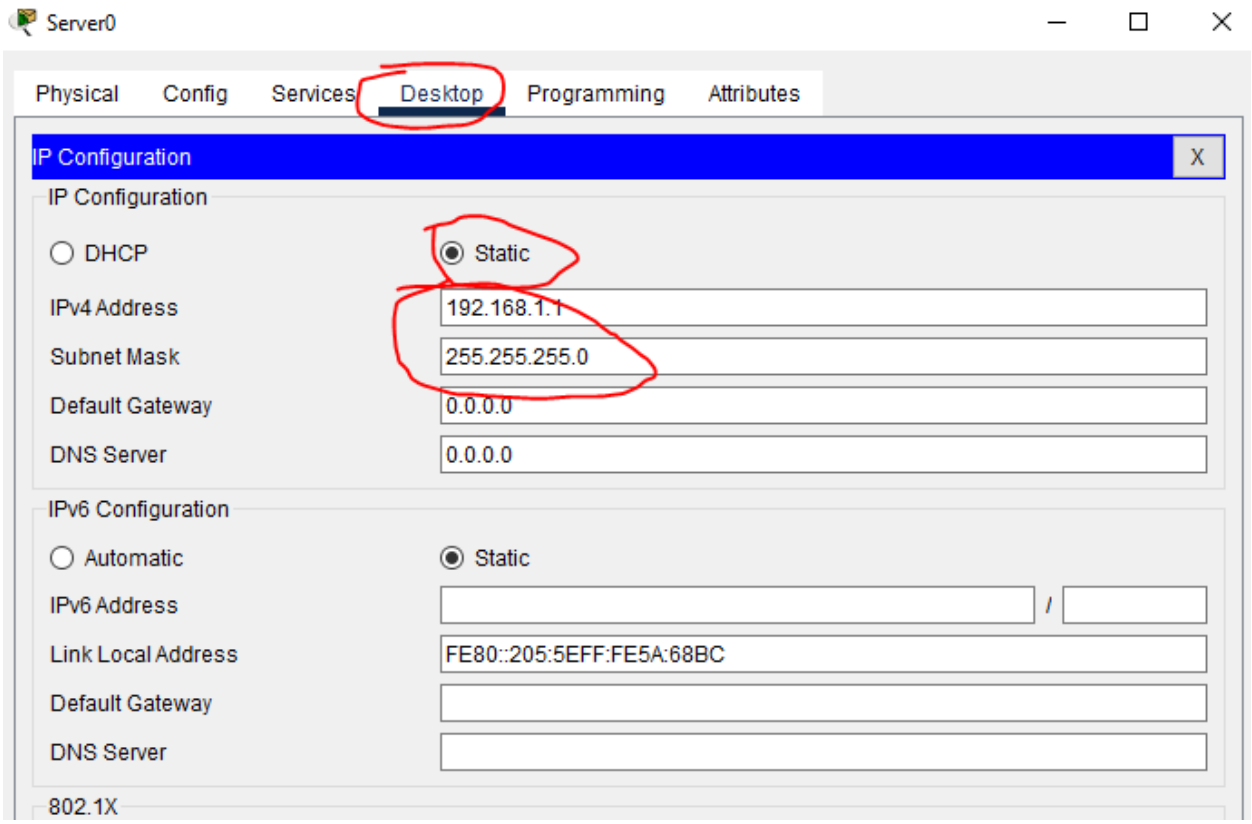
Example:



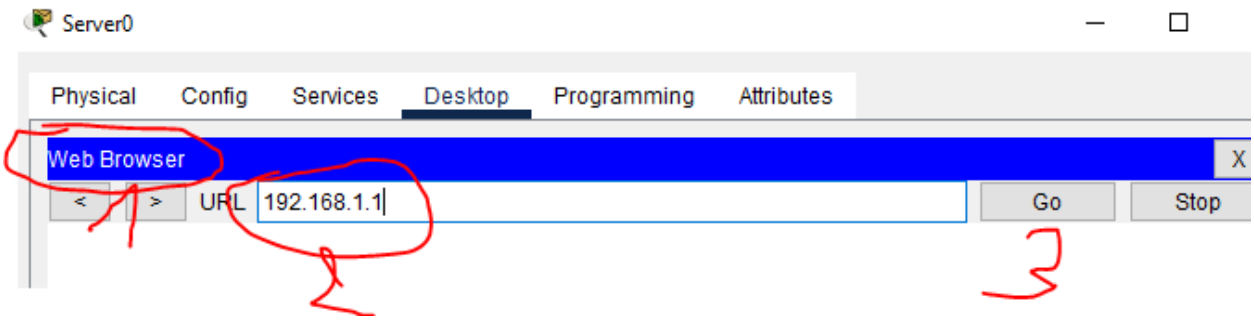
Let have some steps about configurations:

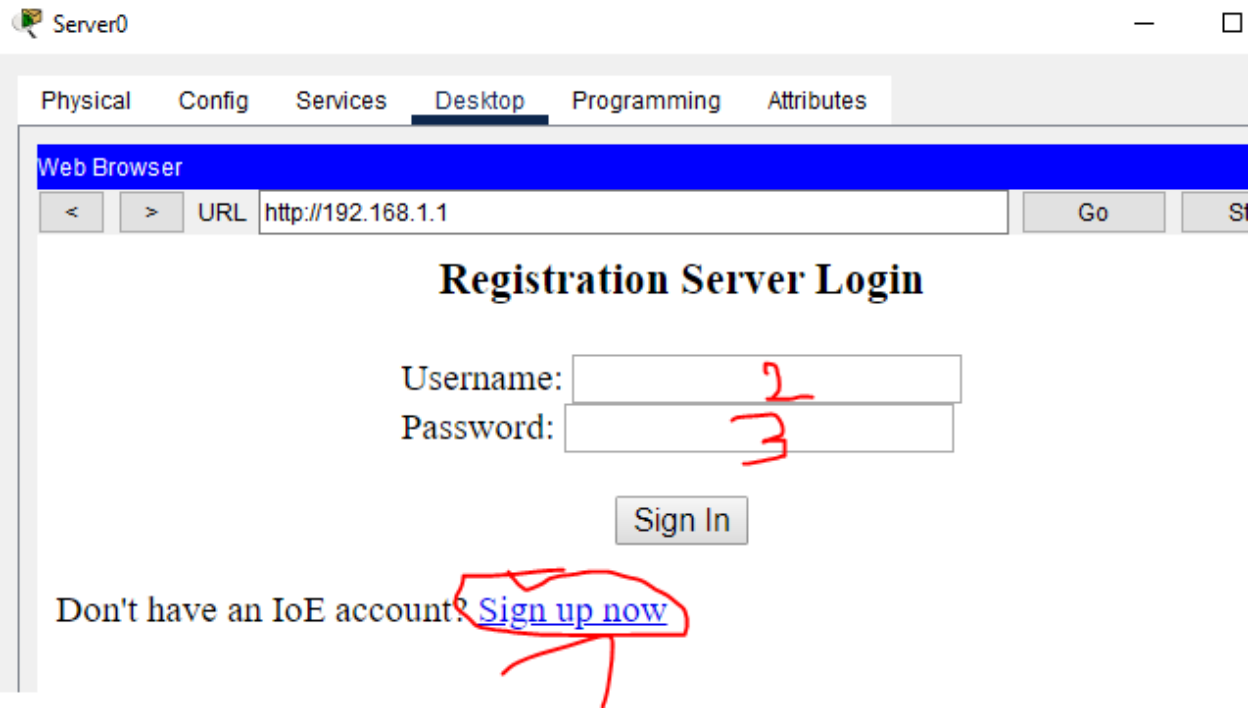
1. **server**

   set the static IP address to the server.

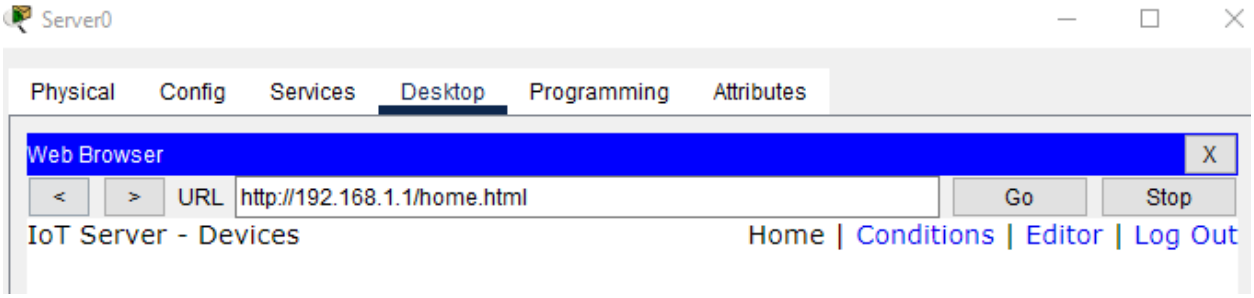


Go to the brouser/desktop of the server and set the new Username and password.





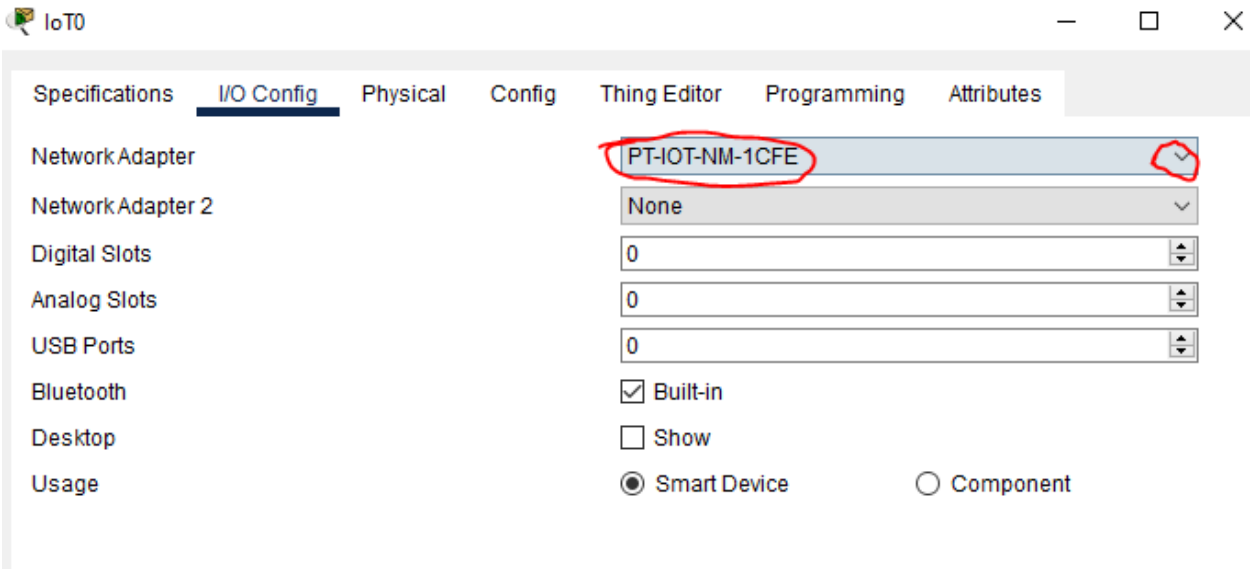
You will get the following screen

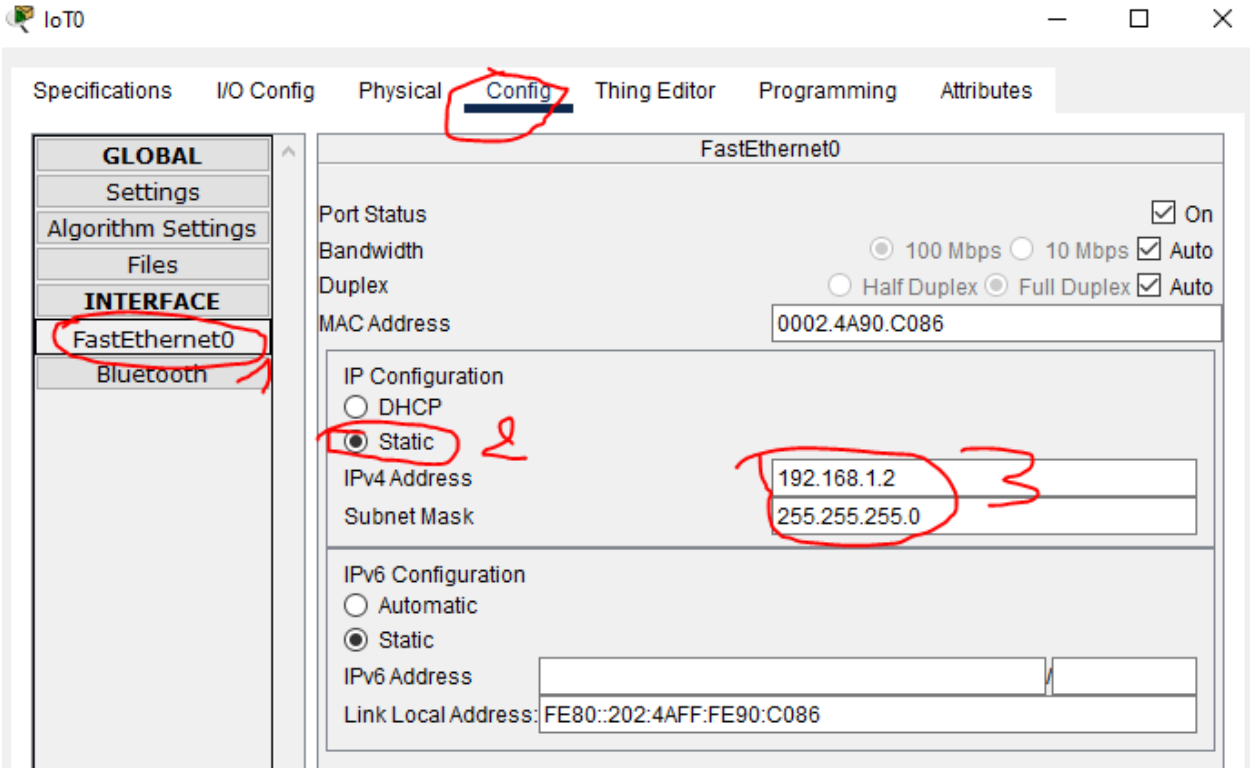


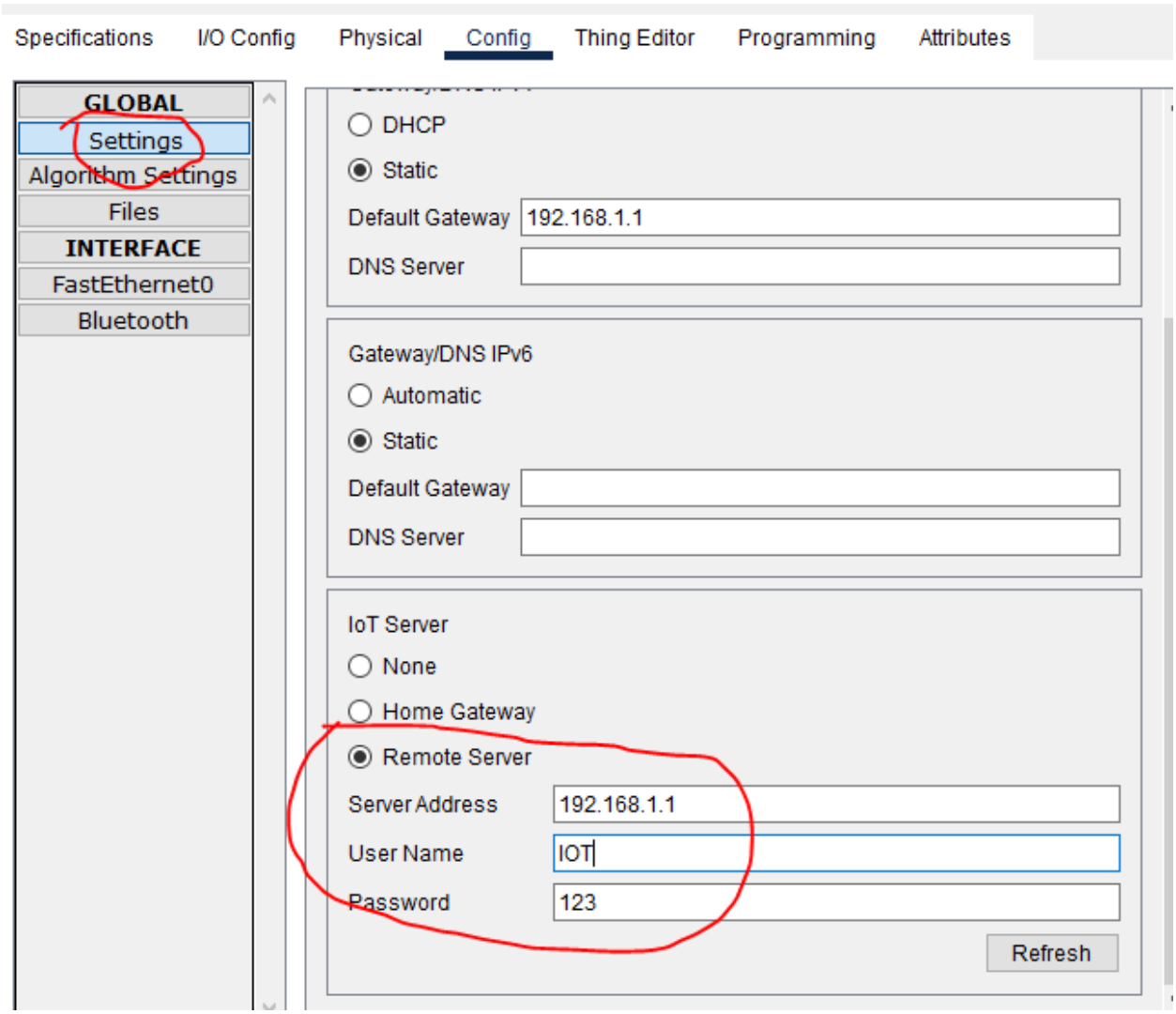
Once the other devices are connected, they will appear here.

2. Motion detector

Add wired NIC from the list of adapters via Advanced button if needed.


IoT0
Specifications
I/O Config
Physical
Config
Thing Editor
Programming
Attributes
Network Adapter
PT-IOT-NM-1CFE
Network Adapter 2
None
Digital Slots
0
Analog Slots
0
USB Ports
0
Bluetooth
Built-in
Desktop
Show
Usage
Smart Device
Component

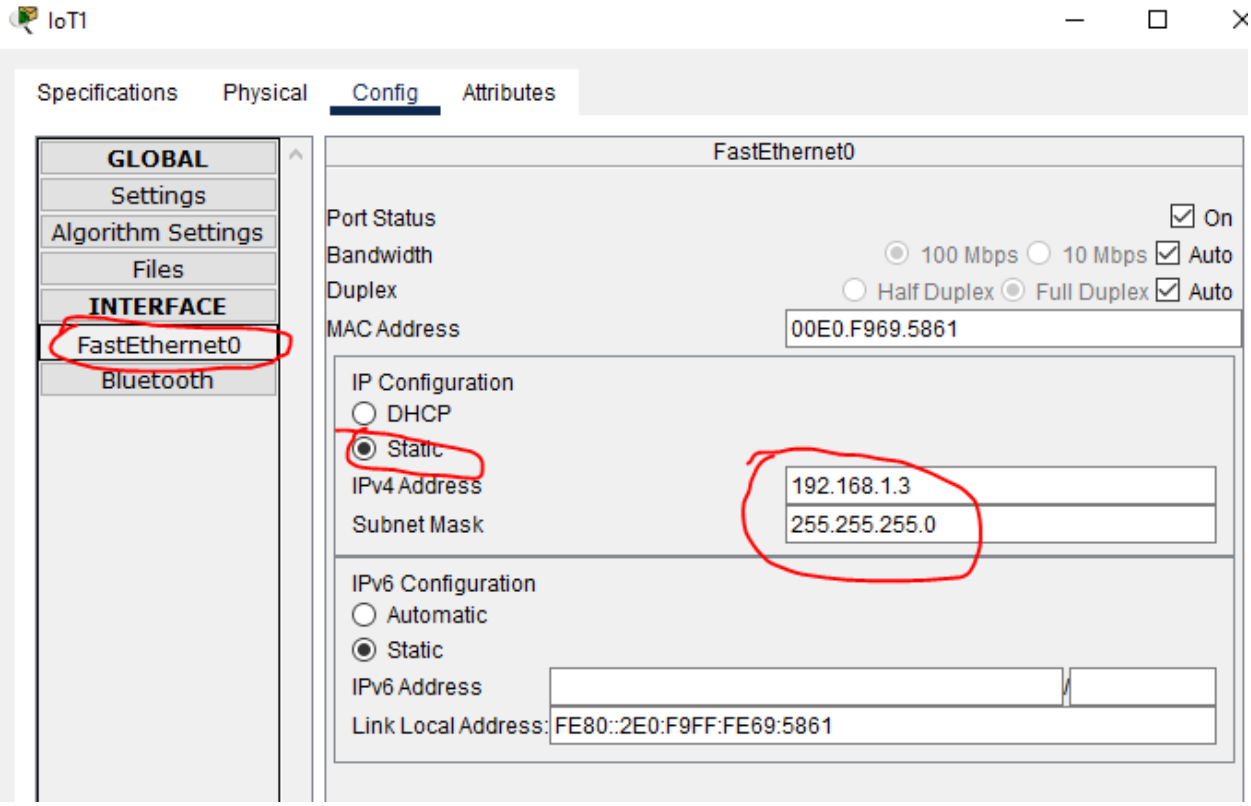

IoT0
Specifications
I/O Config
Physical
Config
Thing Editor
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
Files
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0002.4A90.C086
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::202:4AFF:FE90:C086

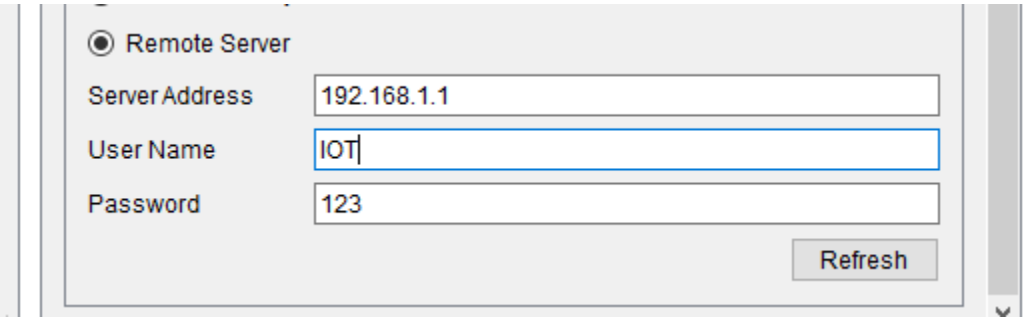


Then, connect to the server.

3. IP camera 1

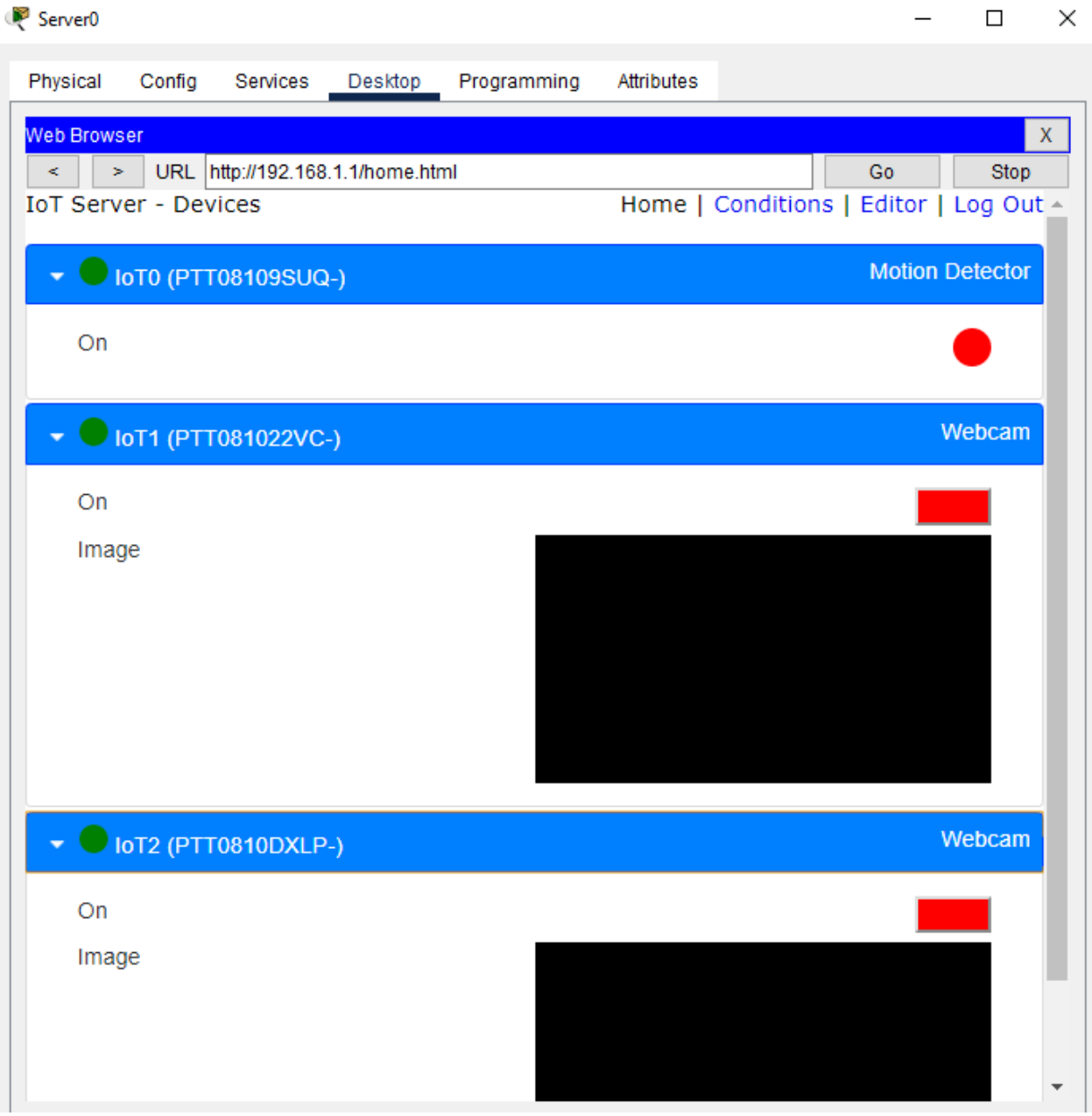
Same step as above to this IP camera for the configurations.





These will be applied to the all camera all other type of devices.

Then, back to the server and we will find the following:

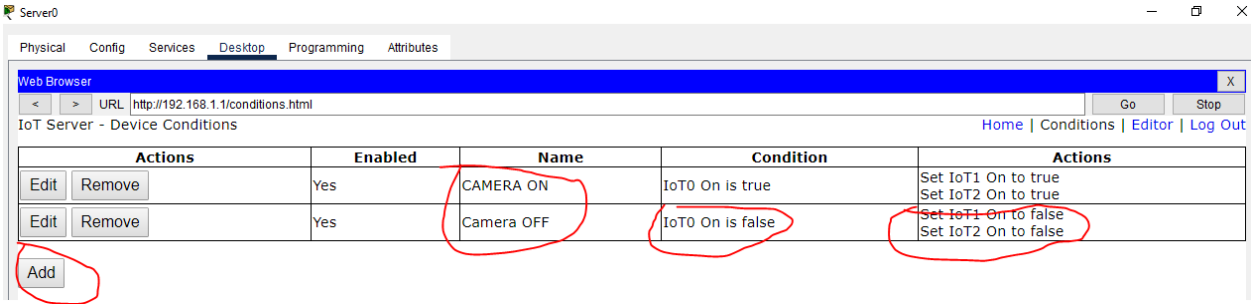


To record the motion in Cisco packet tracer, hold Alt key and move the cursor on the Motion the detector and watch on the server monitor. Nothing changes.

And, Go to the conditions/server and set the rules/condition to apply the surveillance conditions.

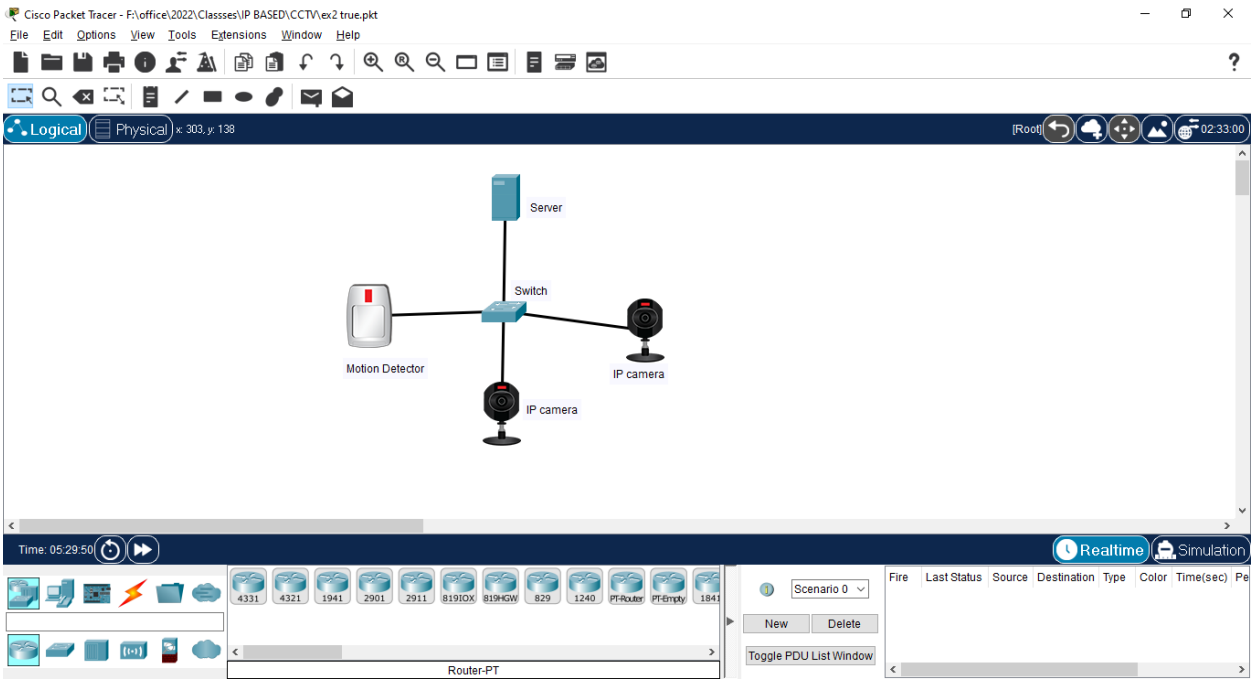
Then, click ok.

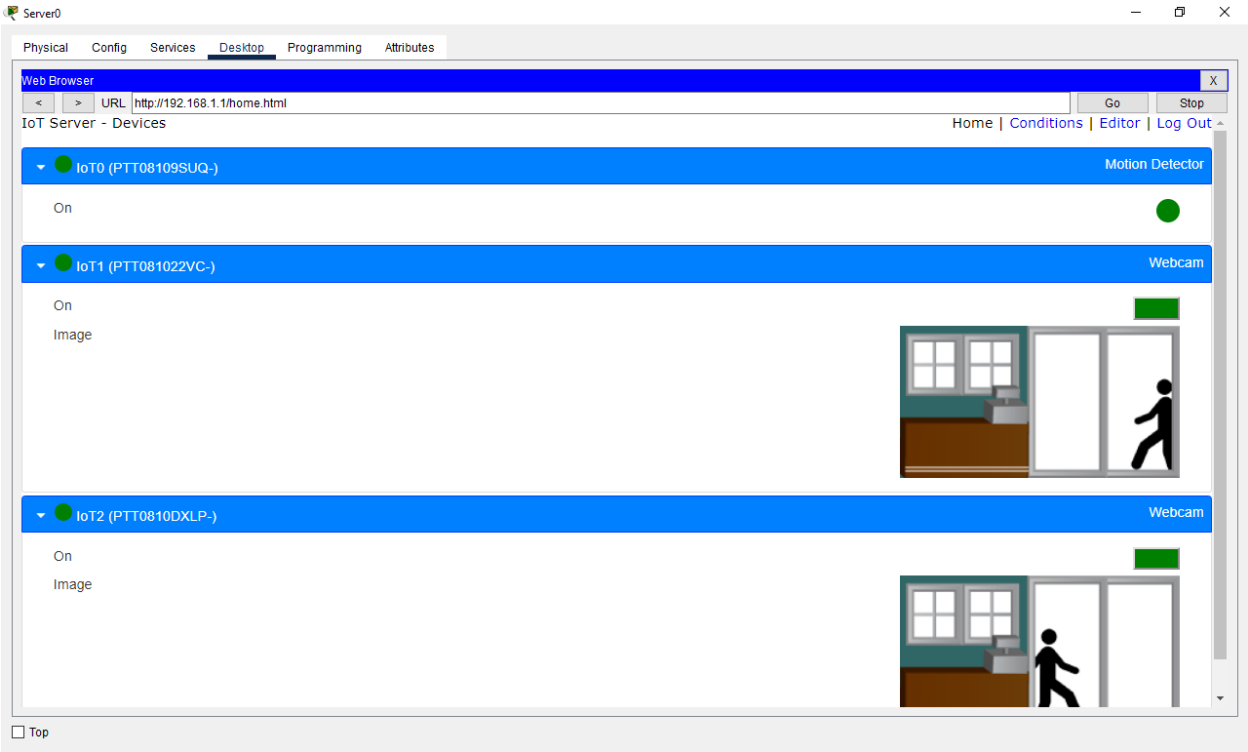
For Make them sleep mode while no motion, the next condition will be applied.



After the configuration, hold the Alt key and roll over the cursor to the motion detector,

The devices will be actives/red diode and in the server, the link will be green and there will be movement of person via window or door.




Server0
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
X
URL
http://192.168.1.1/home.html
Go
Stop
IoT Server - Devices
Home | Conditions | Editor | Log Out
IoT0 (PTT08109SUQ-)
Motion Detector
On
IoT1 (PTT081022VC-)
Webcam
On
Image
IoT2 (PTT0810DXLP-)
Webcam
On
Image
Top

Learning Outcome 2.5: Test and commission the CCTV camera system

- Understanding the Equipment
- Lan tester
- Multi Meter
- Electric Megger Meter
- OTDR
- Fiber Slicing machine
- RJ45 Crimping Tool
- Lug Punching Tool
- Lux Level Meter
- Flux Meter
- Hand tools
- Safety Site Tidiness

LEARNING UNIT 3 – ENABLE CONNECTION VIA WIRELESS TECHNOLOGY

Learning Outcomes:

3.1 Describe wireless technologies

3.2 Apply Wi-Fi technology

3.3 Apply Wimax technology

3.4 Configure voice of IP

Learning hours: 10 hours

Mobile handsets today come with GPRS technology, allowing users to gain Internet access directly via their cellular phones. Whether it's wireless gaming, audio and video capability or access to information and email, it can all be done with instant connectivity. The use of Wi-Fi technology is gathering speed, so users located within range of a Wi-Fi network or hotspot, can benefit from the higher data transmission speeds that are possible with Wi-Fi.

The convergence process is accelerating at an astonishing speed, thanks to the adaptability of the Internet protocol suite as a shared standard that lends itself with almost any service.

Learning Outcome 3.1: Describe wireless technologies

WLAN Concepts

1. **Introduction to Network**

Module Objectives

Topic Title	Topic Objective
Introduction to Wireless	Describe WLAN technology and standards.
Components of WLANs	Describe the components of a WLAN infrastructure.
WLAN Operation	Explain how wireless technology enables WLAN operation.
CAPWAP Operation	Explain how a WLC uses CAPWAP to manage multiple APs.
Channel Management	Describe channel management in a WLAN.
WLAN Threats	Describe threats to WLANs.
Secure WLANs	Describe WLAN security mechanisms.

1.1 Benefits of Wireless

- A Wireless LAN (WLAN) is a type of wireless network that is commonly used in homes, offices, and campus environments.
- WLANs make mobility possible within the home and business environments.
- Wireless infrastructures adapt to rapidly changing needs and technologies.

1.2 Types of Wireless Networks

- **Wireless Personal-Area Network (WPAN)** – Low power and short-range (20-30ft or 6-9 meters). Based on IEEE 802.15 standard and 2.4 GHz frequency. Bluetooth and Zigbee are WPAN examples.
- **Wireless LAN (WLAN)** – Medium sized networks up to about 300 feet. Based on IEEE 802.11 standard and 2.4 or 5.0 GHz frequency.

- **Wireless MAN (WMAN)** – Large geographic area such as city or district. Uses specific licensed frequencies.

- **Wireless WAN (WWAN)** – Extensive geographic area for national or global communication. Uses specific licensed frequencies.

Bluetooth – IEEE WPAN standard used for device pairing at up to 300ft (100m) distance.

- Bluetooth Low Energy (BLE) – Supports mesh topology to large scale network devices.
- Bluetooth Basic Rate/Enhanced Rate (BR/EDR) – Supports point-to-point topologies and is optimized for audio streaming.

WiMAX (Worldwide Interoperability for Microwave Access) – Alternative broadband wired internet connections. IEEE 802.16 WLAN standard for up 30 miles (50 km).

Cellular Broadband – Carry both voice and data. Used by phones, automobiles, tablets, and laptops.

- Global System of Mobile (GSM) – Internationally recognized
- Code Division Multiple Access (CDMA) – Primarily used on the US.

Satellite Broadband – Uses directional satellite dish aligned with satellite in geostationary orbit. Needs clear line of site. Typically used in rural locations where cable and DSL are unavailable.

1.4. 802.11 Standards

802.11 WLAN standards define how radio frequencies are used for wireless links.

IEEE Standard	Radio Frequency	Description
802.11	2.4 GHz	Data rates up to 2 Mb/s
802.11a	5 GHz	Data rates up to 54 Mb/s Not interoperable with 802.11b or 802.11g
802.11b	2.4 GHz	Data rates up to 11 Mb/s Longer range than 802.11a and better able to penetrate building structures

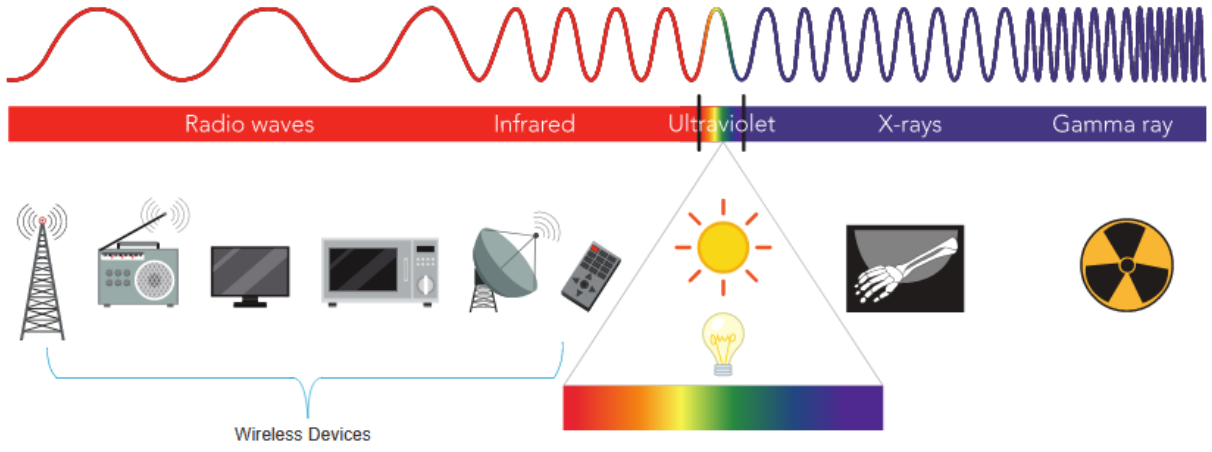
802.11g	2.4 GHz	Data rates up to 54 Mb/s Backward compatible with 802.11b
802.11n	2.4 and 5 GHz	Data rates 150 – 600 Mb/s Require multiple antennas with MIMO technology
802.11ac	5 GHz	Data rates 450 Mb/s – 1.3 Gb/s Supports up to eight antennas
802.11ax	2.4 and 5 GHz	High-Efficiency Wireless (HEW) Capable of using 1 GHz and 7 GHz frequencies

1.5 .Radio Frequencies

All wireless devices operate in the range of the electromagnetic spectrum. WLAN networks operate in the 2.4 and 5 GHz frequency bands.

2.4 GHz (UHF) – 802.11b/g/n/ax

5 GHz (SHF) – 802.11a/n/ac/ax



1.6. Wireless Standards Organizations

Standards ensure interoperability between devices that are made by different manufacturers. Internationally, the three organizations influencing WLAN standards:

International Telecommunication Union (ITU) – Regulates the allocation of radio spectrum and satellite orbits.

Institute of Electrical and Electronics Engineers (IEEE) – Specifies how a radio frequency is modulated to carry information. Maintains the standards for local and metropolitan area networks (MAN) with the IEEE 802 LAN/MAN family of standards.

Wi-Fi Alliance – Promotes the growth and acceptance of WLANs. It is an association of vendors whose objective is to improve the interoperability of products that are based on the 802.11 standard.

Review questions

1. what are the benefits of wireless
2. Describe the Types of Wireless Networks

Learning Outcome 3.2. WLAN COMPONENTS

1.1.Wireless NICs

To communicate wirelessly, laptops, tablets, smart phones, and even the latest automobiles include integrated wireless NICs that incorporate a radio transmitter/receiver.

If a device does not have an integrated wireless NIC, then a USB wireless adapter can be used.

2.2. Wireless Home Router

A home user typically interconnects wireless devices using a small, wireless router.

Wireless routers serve as the following:

Access point – To provide wires access

Switch – To interconnect wired devices

Router - To provide a default gateway to other networks and the Internet

2.3. Wireless Access Point

Wireless clients use their wireless NIC to discover nearby access points (APs).

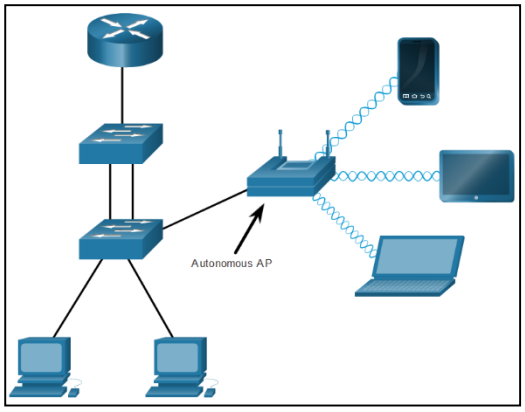
Clients then attempt to associate and authenticate with an AP.

After being authenticated, wireless users have access to network resources.

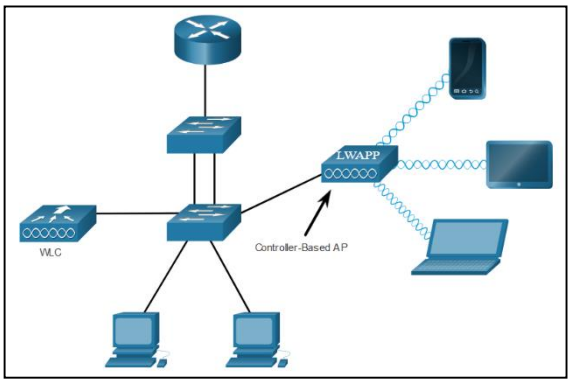
2.4. AP Categories

APs can be categorized as either autonomous APs or controller-based APs.

- **Autonomous APs** – Standalone devices configured through a command line interface or GUI. Each autonomous AP acts independently of the others and is configured and managed manually by an administrator.



- **Controller-based APs** – Also known as lightweight APs (LAPs). Use Lightweight Access Point Protocol (LWAPP) to communicate with a LWAN controller (WLC). Each LAP is automatically configured and managed by the WLC.



2.5. Wireless Antennas

Types of external antennas:

- **Omnidirectional** – Provide 360-degree coverage. Ideal in houses and office areas.

- **Directional** – Focus the radio signal in a specific direction. Examples are the Yagi and parabolic dish.

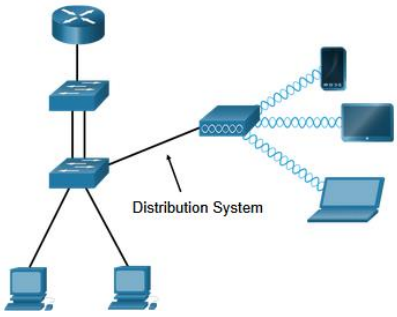
- **Multiple Input Multiple Output (MIMO)** – Uses multiple antennas (Up to eight) to increase bandwidth.

Learning outcome 3.3.: WLAN

3.1 802.11 Wireless Topology Modes

Ad hoc mode - Used to connect clients in peer-to-peer manner without an AP.

Infrastructure mode - Used to connect clients to the network using an AP.

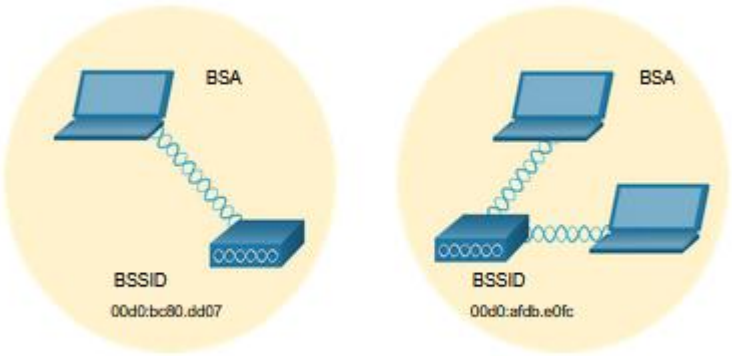


Tethering - Variation of the ad hoc topology is when a smart phone or tablet with cellular data access is enabled to create a personal hotspot.

3.2 BSS and ESS

Infrastructure mode defines two topology blocks:

Basic Service Set (BSS)



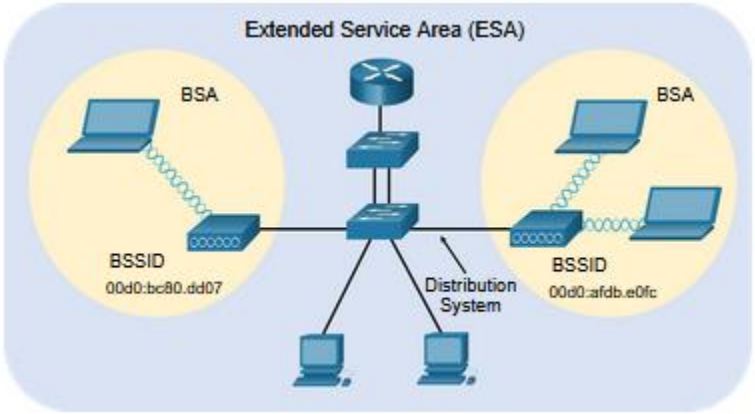
Uses single AP to interconnect all associated wireless clients.

Clients in different BSSs cannot communicate.

Extended Service Set (ESS)

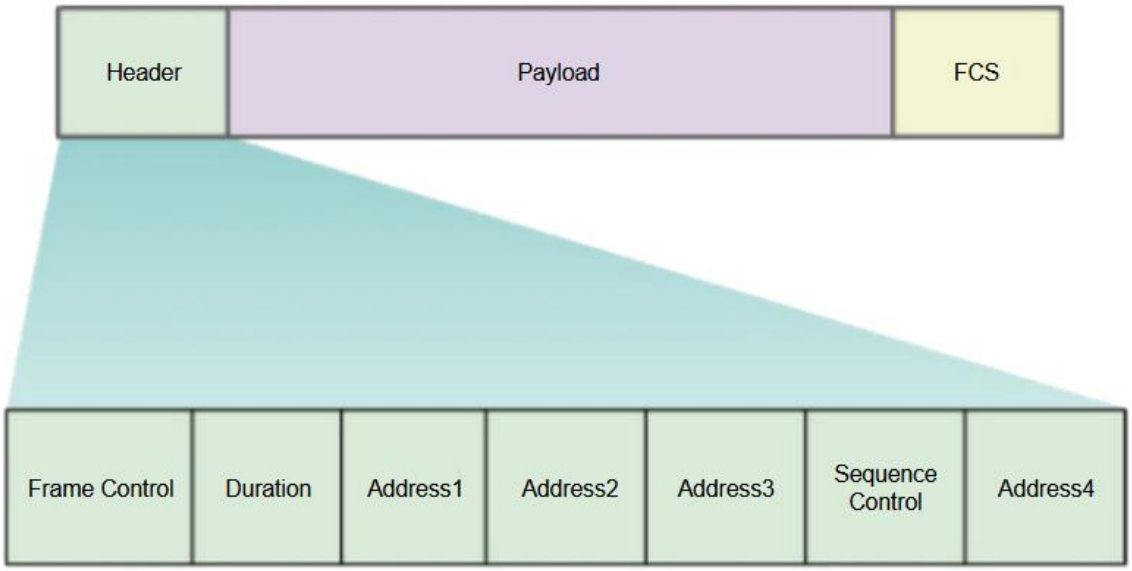
A union of two or more BSSs interconnected by a wired distribution system.

Clients in each BSS can communication through the ESS.



3.3 802.11 Frame Structure

The 802.11 frame format is similar to the Ethernet frame format, except that it contains more fields.



3.4 CSMA/CA

WLANs are half-duplex and a client cannot "hear" while it is sending, making it impossible to detect a collision.

WLANs use carrier sense multiple access with collision avoidance (CSMA/CA) to determine how and when to send data. A wireless client does the following:

- Listens to the channel to see if it is idle, i.e. no other traffic currently on the channel.
- Sends a ready to send (RTS) message the AP to request dedicated access to the network.
- Receives a clear to send (CTS) message from the AP granting access to send.
- Waits a random amount of time before restarting the process if no CTS message received.
- Transmits the data.
- Acknowledges all transmissions. If a wireless client does not receive an acknowledgment, it assumes a collision occurred and restarts the process

3.5 Wireless Client and AP Association

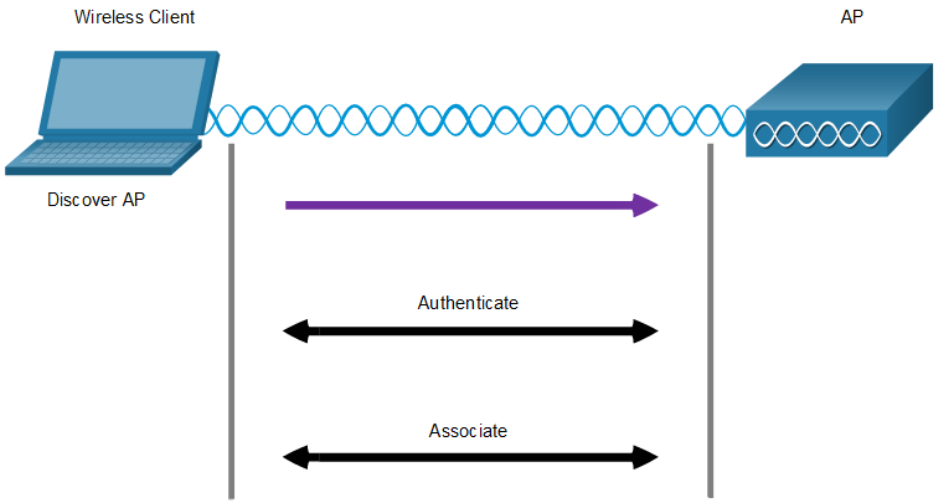
For wireless devices to communicate over a network, they must first associate with an AP or wireless router.

Wireless devices complete the following three stage process:

Discover a wireless AP

Authenticate with the AP

Associate with the AP



To achieve successful association, a wireless client and an AP must agree on specific parameters:

SSID – The client needs to know the name of the network to connect.

Password – This is required for the client to authenticate to the AP.

Network mode – The 802.11 standard in use.

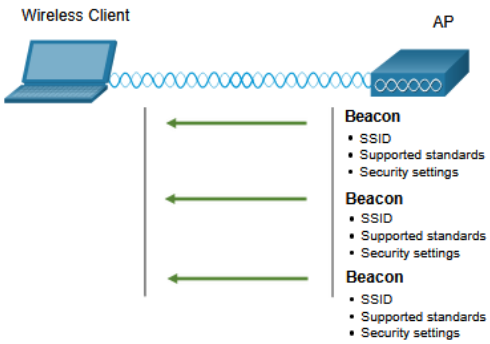
Security mode – The security parameter settings, i.e. WEP, WPA, or WPA2.

Channel settings – The frequency bands in use.

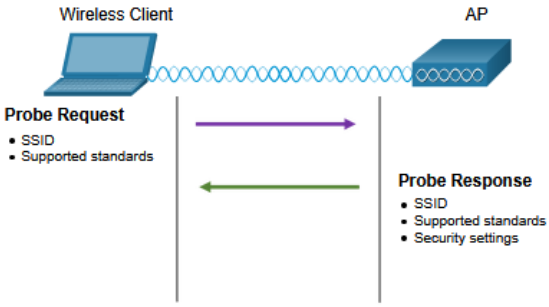
3.6 Passive and Active Discover Mode

Wireless clients connect to the AP using a passive or active scanning (probing) process.

- **Passive mode** – AP openly advertises its service by periodically sending broadcast beacon frames containing the SSID, supported standards, and security settings.



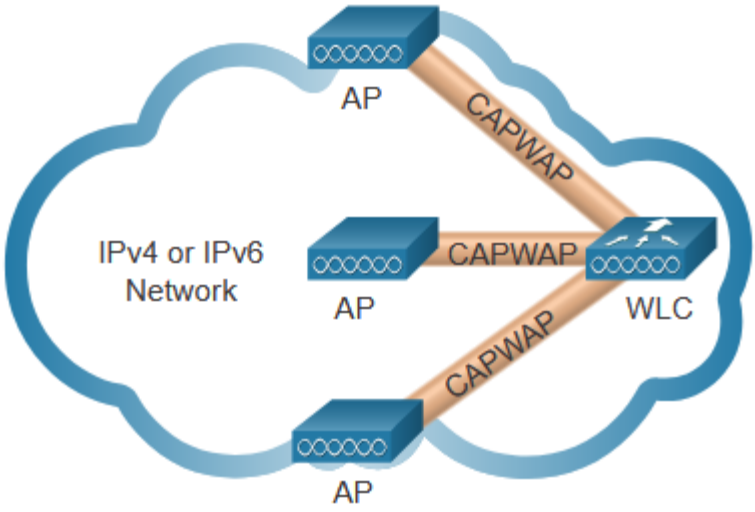
- **Active mode** – Wireless clients must know the name of the SSID. The wireless client initiates the process by broadcasting a probe request frame on multiple channels.



2. **CAPWAP Operation**

4.1 Introduction to CAPWAP

- CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs.
- Based on LWAPP but adds additional security with Datagram Transport Layer Security (DLTS).
- Encapsulates and forwards WLAN client traffic between an AP and a WLC over tunnels using UDP ports 5246 and 5247.
- Operates over both IPv4 and IPv6. IPv4 uses IP protocol 17 and IPv6 uses IP protocol 136.



4.2. Split MAC Architecture

The CAPWAP split MAC concept does all the functions normally performed by individual APs and distributes them between two functional components:

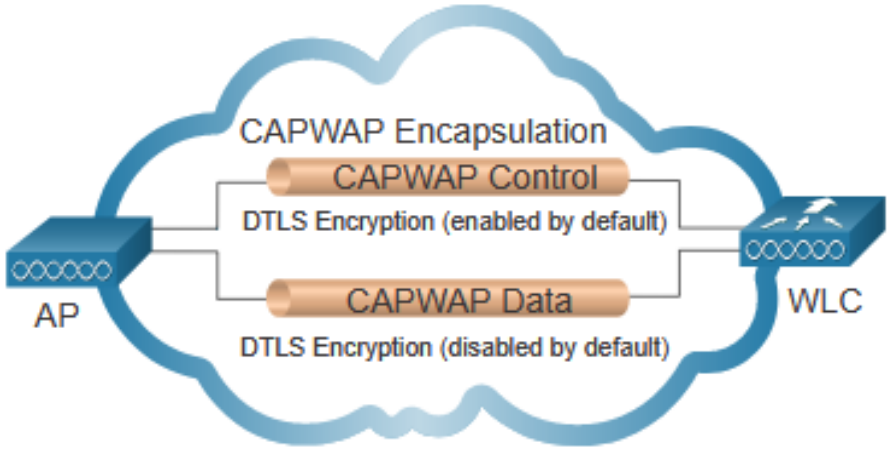
AP MAC Functions

WLC MAC Functions

AP MAC Functions	WLC MAC Functions
Beacons and probe responses	**Authentication**
Packet acknowledgements and retransmissions	**Association and re-association of roaming clients**
Frame queueing and packet prioritization	**Frame translation to other protocols**
MAC layer data encryption and decryption	**Termination of 802.11 traffic on a wired interface**

4.3. DTLS Encryption

- DTLS provides security between the AP and the WLC.
- It is enabled by default to secure the CAPWAP control channel and encrypt all management and control traffic between AP and WLC.
- Data encryption is disabled by default and requires a DTLS license to be installed on the WLC before it can be enabled on the AP.



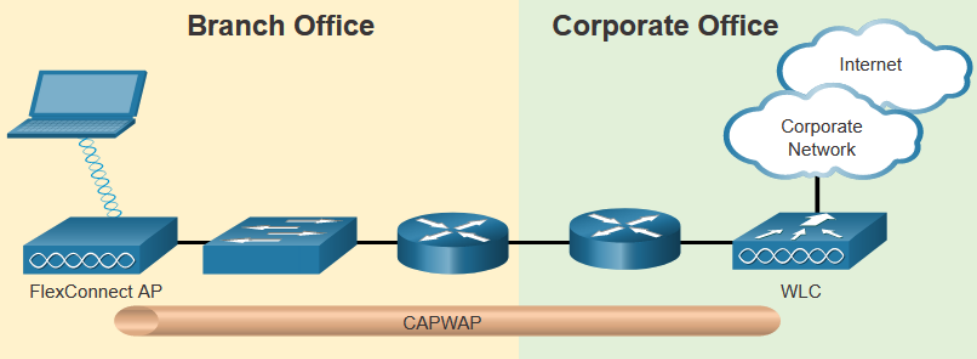
4.4. Flex Connect APs

FlexConnect enables the configuration and control of Aps over a WAN link.

There are two modes of option for the FlexConnect AP:

Connected mode – The WLC is reachable. The FlexConnect AP has CAPWAP connectivity with the WLC through the CAPWAP tunnel. The WLC performs all CAPWAP functions.

Standalone mode – The WLC is unreachable. The FlexConnect AP has lost CAPWAP connectivity with the WLC. The FlexConnect AP can assume some of the WLC functions such as switching client data traffic locally and performing client authentication locally.



3. **Channel Management**

5.1 Frequency Channel Saturation

If the demand for a specific wireless channel is too high, the channel may become oversaturated, degrading the quality of the communication.

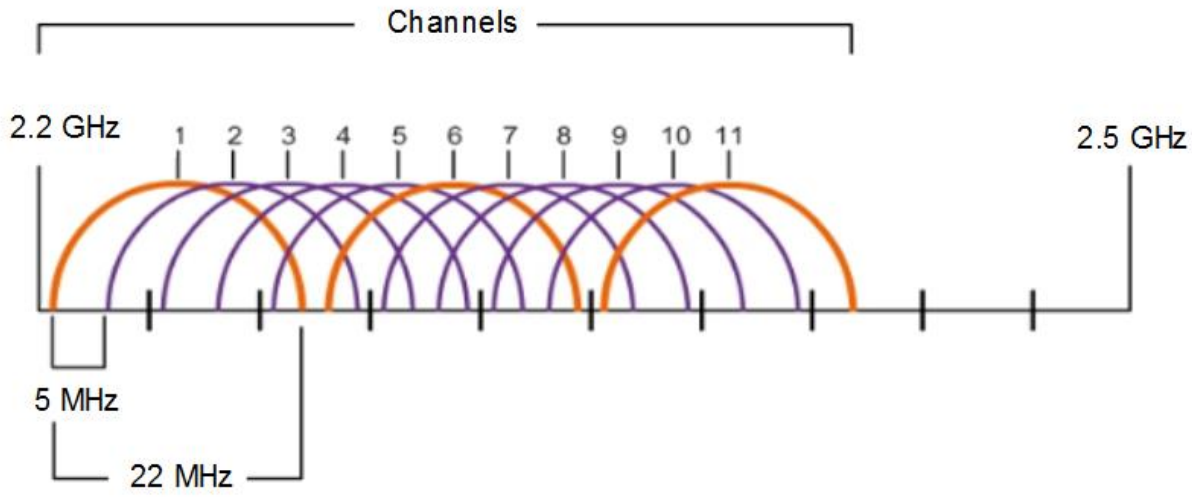
Channel saturation can be mitigated using techniques that use the channels more efficiently.

- **Direct-Sequence Spread Spectrum (DSSS)** - A modulation technique designed to spread a signal over a larger frequency band. Used by 802.11b devices to avoid interference from other devices using the same 2.4 GHz frequency.
- **Frequency-Hopping Spread Spectrum (FHSS)** - Transmits radio signals by rapidly switching a carrier signal among many frequency channels. Sender and receiver must be synchronized to "know" which channel to jump to. Used by the original 802.11 standard.

- **Orthogonal Frequency-Division Multiplexing (OFDM)** - A subset of frequency division multiplexing in which a single channel uses multiple sub-channels on adjacent frequencies. OFDM is used by a number of communication systems including 802.11a/g/n/ac.

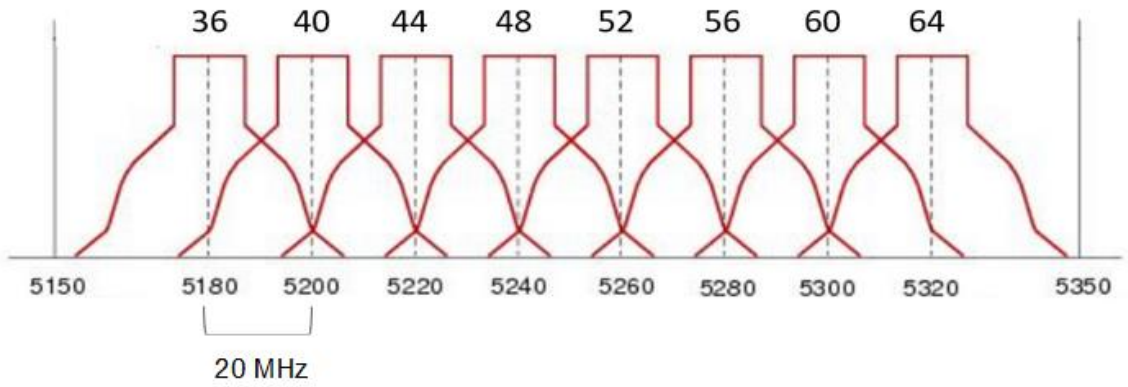
5.2. Channel Selection

- The 2.4 GHz band is subdivided into multiple channels each allotted 22 MHz bandwidth and separated from the next channel by 5 MHz.
- A best practice for 802.11b/g/n WLANs requiring multiple APs is to use non-overlapping channels such as 1, 6, and 11.



For the 5GHz standards 802.11a/n/ac, there are 24 channels. Each channel is separated from the next channel by 20 MHz.

- Non-overlapping channels are 36, 48, and 60.

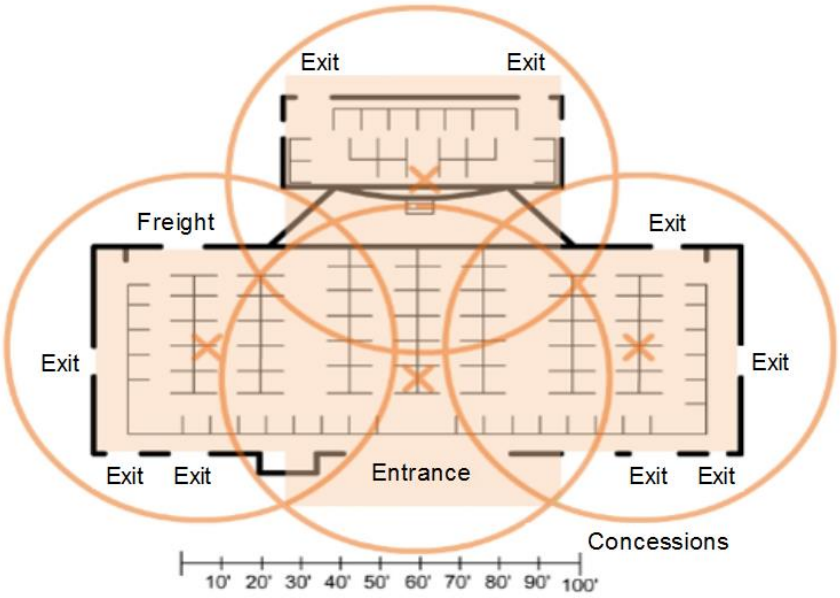


5.3. Plan a WLAN Deployment

The number of users supported by a WLAN depends on the following:

- The geographical layout of the facility
- The number of bodies and devices that can fit in a space
- The data rates users expect
- The use of non-overlapping channels by multiple APs and transmit power settings

When planning the location of APs, the approximate circular coverage area is important.



4. **WLAN Threats**

4.1.Wireless Security Overview

A WLAN is open to anyone within range of an AP and the appropriate credentials to associate to it.

Attacks can be generated by outsiders, disgruntled employees, and even unintentionally by employees. Wireless networks are specifically susceptible to several threats, including the following:

- Interception of data
- Wireless intruders
- Denial of Service (DoS) Attacks
- Rogue APs

6.2. DoS Attacks

Wireless DoS attacks can be the result of the following:

- Improperly configured devices
- A malicious user intentionally interfering with the wireless communication
- Accidental interference

To minimize the risk of a DoS attack due to improperly configured devices and malicious attacks, harden all devices, keep passwords secure, create backups, and ensure that all configuration changes are incorporated off-hours.

6.3 Rogue Access Points

- A rogue AP is an AP or wireless router that has been connected to a corporate network without explicit authorization and against corporate policy.
- Once connected, the rogue AP can be used by an attacker to capture MAC addresses, capture data packets, gain access to network resources, or launch a man-in-the-middle attack.
- A personal network hotspot could also be used as a rogue AP. For example, a user with secure network access enables their authorized Windows host to become a Wi-Fi AP.
- To prevent the installation of rogue APs, organizations must configure WLCs with rogue AP policies and use monitoring software to actively monitor the radio spectrum for unauthorized APs.

6.4 Man-in-the-Middle Attack

In a man-in-the-middle (MITM) attack, the hacker is positioned in between two legitimate entities in order to read or modify the data that passes between the two parties. A popular wireless MITM attack is called the “evil twin AP” attack, where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.

Defeating a MITM attack begins with identifying legitimate devices on the WLAN. To do this, users must be authenticated. After all of the legitimate devices are known, the network can be monitored for abnormal devices or traffic.

5. Secure WLANs

7.1. SSID Cloaking and MAC Address Filtering

To address the threats of keeping wireless intruders out and protecting data, two early security features were used and are still available on most routers and APs:

SSID Cloaking

- APs and some wireless routers allow the SSID beacon frame to be disabled. Wireless clients must be manually configured with the SSID to connect to the network.

MAC Address Filtering

- An administrator can manually permit or deny clients wireless access based on their physical MAC hardware address. In the figure, the router is configured to permit two MAC addresses. Devices with different MAC addresses will not be able to join the 2.4GHz WLAN.

7.2. 802.11 Original Authentication Methods

The best way to secure a wireless network is to use authentication and encryption systems. Two types of authentication were introduced with the original 802.11 standard:

Open system authentication

- No password required. Typically used to provide free internet access in public areas like cafes, airports, and hotels.
- Client is responsible for providing security such as through a VPN.

Shared key authentication

- Provides mechanisms, such as WEP, WPA, WPA2, and WPA3 to authenticate and encrypt data between a wireless client and AP. However, the password must be pre-shared between both parties to connect.

7.3. Shared Key Authentication Methods

There are currently four shared key authentication techniques available, as shown in the table.

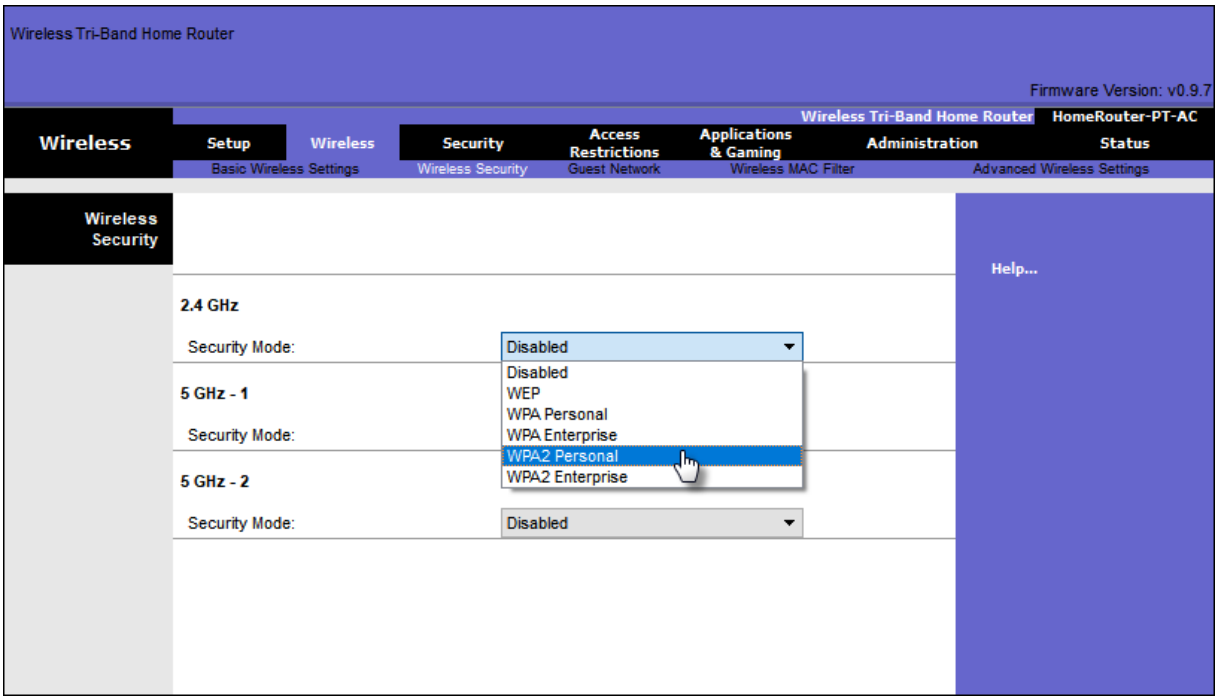
Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more

	difficult to hack.
WPA2	It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	This is the next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF).

7.4. Authenticating a Home User

Home routers typically have two choices for authentication: WPA and WPA2, with WPA 2 having two authentication methods.

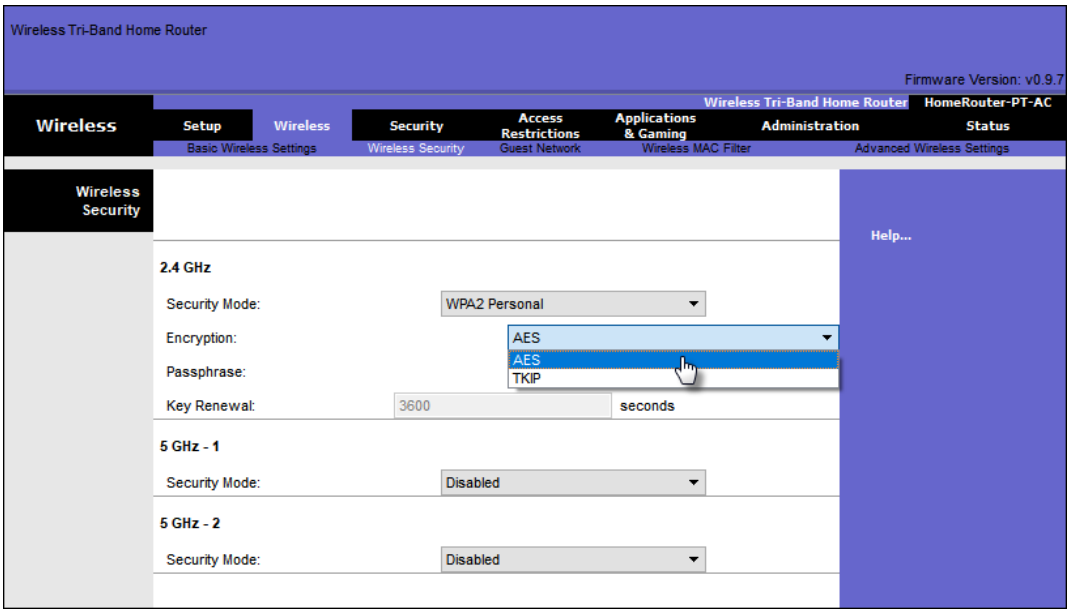
- **Personal** – Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.
- **Enterprise** – Intended for enterprise networks. Requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.



7.5 Encryption Methods

WPA and WPA2 include two encryption protocols:

- **Temporal Key Integrity Protocol (TKIP)** – Used by WPA and provides support for legacy WLAN equipment. Makes use of WEP but encrypts the Layer 2 payload using TKIP.
- **Advanced Encryption Standard (AES)** – Used by WPA2 and uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) that allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered.

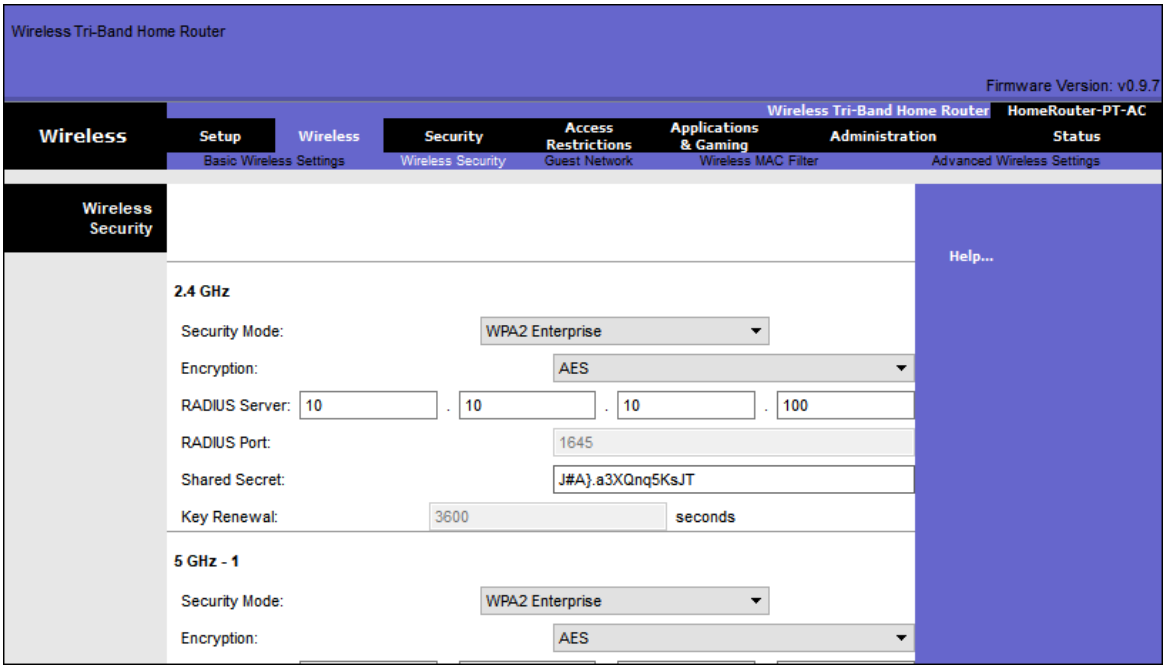


7.6. Authentication in the Enterprise

Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

There pieces of information are required:

- **RADIUS server IP address** – IP address of the server.
- **UDP port numbers** –UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646.
- **Shared key** – Used to authenticate the AP with the RADIUS server.



Note: User authentication and authorization is handled by the 802.1X standard, which provides a centralized, server-based authentication of end users.

7.7. WPA 3

Because WPA2 is no longer considered secure, WPA3 is recommended when available. WPA3 Includes four features:

- **WPA3 – Personal :** Thwarts brute force attacks by using Simultaneous Authentication of Equals (SAE).

- **WPA3 – Enterprise :** Uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards.
- **Open Networks :** Does not use any authentication. However, uses Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.
- **IoT Onboarding :** Uses Device Provisioning Protocol (DPP) to quickly onboard IoT devices.

Review questions

1.what are the Access points categories

2.Explain the types of external antennas

3.Describe briefly the 802.11 wireless topology modes

4.Identify the common wireless network threats.

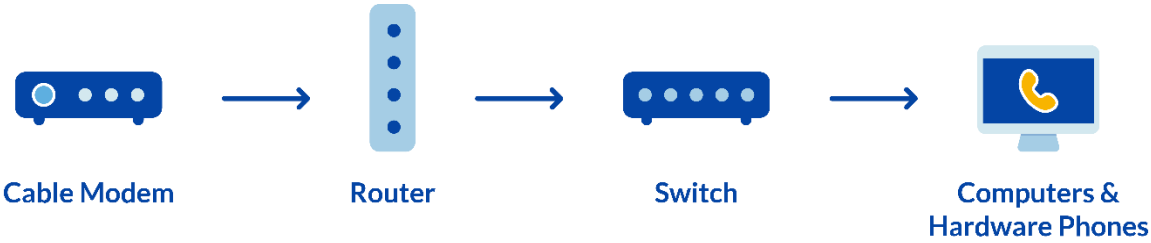
5. Demonstrate how to secure WLANs

Learning Outcome 3.4: Installation of VoIP

VoIP

VoIP is an acronym for Voice over Internet Protocol that describes the method to place and receive phone calls over the internet. Most people consider VoIP the alternative to the local telephone company.

If you've heard of an IP address, that's your Internet Protocol address. An IP address is how computers and devices communicate with each other on the internet. VoIP isn't actually all that new. Telephony has relied on digital lines to carry phone calls since the late 90s. VoIP is a cost-effective way to handle an unlimited number of calls.



If you have an internet connection, you call anyone without the need for local phone service. VoIP solutions work on any computer because it's built upon many years of open standards.

VoIP service providers do more than establishing calls. They perform routing of outgoing and incoming calls through existing telephone networks. Landlines and cell phones depend on the Public Switched Telephone Network (PSTN).

Traditional telephones use analog lines to carry voice signals. If you want to make calls, you have to have extra wiring installed. Many businesses rely on specialized hardware for phone service. This equipment is known as a Private Branch Exchange (PBX). It connects internal phone extensions to the public telephone network. PBXs are generally quite costly to set up and maintain. There's a better option.

A trusted VoIP provider can handle everything for you. Plug your IP phone in, and you're done. These digital phones use your high-speed internet connection to establish connectivity. VoIP converts your phone calls into data and is sent over the internet. You can use the Ethernet cables or skip them if you have a strong Wi-Fi signal. It does so at a much lower cost than older telephone systems. Voice over IP has many advantages over traditional phone service. We'll discuss later on.

Operation

Voice over IP uses Internet Protocol, an essential building block of the internet. IP telephony is a massive innovation from the century-old telecommunications system.

For phone calls, the conversation is exchanged using small data packets. The internet can send these data packets around the world in less than a second. For internet telephony, these packets travel between your phone and a VoIP provider.

A VoIP phone system facilitates calls between other phones or over to another telephone company. It also provides other useful functions like voicemail, call forwarding, call recording, and more.

In four steps, here's how VoIP works.

- Your phone connects to your switch or router in your Local Area Network (LAN).
- When you dial a telephone number, your IP phone tells your VoIP service provider to call the other party.
- Your VoIP service establishes the call and exchanges data packets from your IP phone.
- Your VoIP phone converts these digital signals back into the sound you can hear.

Voice over Internet Protocol bypasses the telephone company entirely. Wherever you have a broadband internet connection, you can use VoIP. It’s a significant upgrade from an analog phone system.

You used to need expensive, proprietary equipment to use VoIP — but that was over 20 years ago! Today, VoIP is built upon open standards such as Session Initiation Protocol (SIP). SIP provides complete interoperability between different desk phones, conference phones, and VoIP apps.

Cloud-based PBXs are responsible for features like voicemail, conferencing, and call routing. When you think about it, they act as their own full-service phone companies that you control.

All you need is a broadband internet connection (cable, DSL, or fiber) and you can reap all the benefits of VoIP.

Pros and cons of Voice over IP

Benefits of VoIP

Lower cost - Many consumers and businesses alike have realized substantial cost savings and lowered their phone bills by over 60%.

High-quality sound - There's a noticeable difference in the call quality, so the audio isn't muffled or fuzzy.

Advanced features - Leverage premium features to run your company such as auto attendants, call recording, and call queues. They're often included with business phone service plans.

Remote-ready - Use your phone service wherever you work. No technical setup is necessary if you work from home.

Call anyone worldwide - International long distance rates are as low as $0.04 per minute to call Mexico or $0.01 to reach the United Kingdom.

Downsides of VoIP

Needs a high-speed internet connection - VoIP doesn't work well on dial-up or satellite-based internet connections. You'll need at least 100 kbps (0.1 Mbps) per phone line.

Emergency services limitations - In the unlikely event you need to call 911 from your VoIP phone, you need to tell the operator your actual location. Voice over IP systems default to sending your company's mailing address to public safety operators.

Makes analog phones obsolete - Voice over IP uses new technology that doesn't rely on analog signals. You'll likely want to upgrade outdated phone handsets. Read our advice later to find out how you can get a free VoIP phone.

Top VoIP phone system features

What are the attractive features available with a cloud-based office phone system? Here are the most popular VoIP features that businesses will enjoy using.

These business phone features will matter more or less depending on your needs.

1) Auto attendant

Project a professional image with a phone menu that greets incoming calls. If you've called a company and had to press 1 for sales, 2 for support, you've used an auto attendant. An auto attendant helps you direct callers to the right person or department. You can forward calls to your voicemail or elsewhere outside of business hours.

2) Mobile and desktop apps

With cloud communications, you won't miss calls because you're not in the office. Several VoIP service providers now offer an app for your computer and mobile device.

It's more important than ever to equip your team with a VoIP solution to work from home. These apps let you make phone calls, join conference calls, exchange text messages, and more. You can use these telecommunications apps with or without a separate desk phone. It's your choice.

3) HD call quality

There's almost nothing worse than asking callers to repeat themselves. HD Voice increases the sound quality in your phone calls. This VoIP technology makes phone calls sound twice as clear as a standard phone call.

For even fuller sound, many VoIP headsets and phones provide noise-canceling capabilities. This high-definition sound quality is noticeable even for long-distance calls.

4) Unified Communications

VoIP elevates your team's workflow through a concept known as Unified Communications (UC). Instead of using several disparate apps, your company's communications platform is fully integrated. It's now even easier for employees to connect with each other and with customers. You can even flip calls between mobile devices, too.

Your team gets work done faster by meeting over video and screen sharing. UC makes real-time communication intuitive and well-organized.

Here are some of the key functions within a UC platform:

- Instant messaging
- Team chats
- Video meetings
- Screen sharing
- Conference calling
- Mobile and desktop apps

5) Call encryption and VoIP security

VoIP security is top of mind for business owners. Telephone calls carry confidential information like credit card numbers and HR conversations. You must protect these assets, or it could cost you. VoIP is safe and secure even as data packets travel through the internet. IP phone systems have built-in security to stop bad actors from tapping your calls.

Ask your VoIP service provider about call encryption. VoIP technologies like TLS and SRTP scramble call data making eavesdropping near impossible.

You should consider whether a VoIP provider is accredited and meets industry standards. It’s handy to have a requirements checklist when selecting a business phone service.

Useful questions to ask include:

- Are they accredited (PCI, SOC 2, ISO/IEC 27001)?
- How many data centers do they have?
- What is the uptime of their VoIP service?
- Do they provide HIPAA compliant IP telephony?
- Can you access real-time call logs?
- Related: An In-Depth Look at VoIP Security & Call Encryption

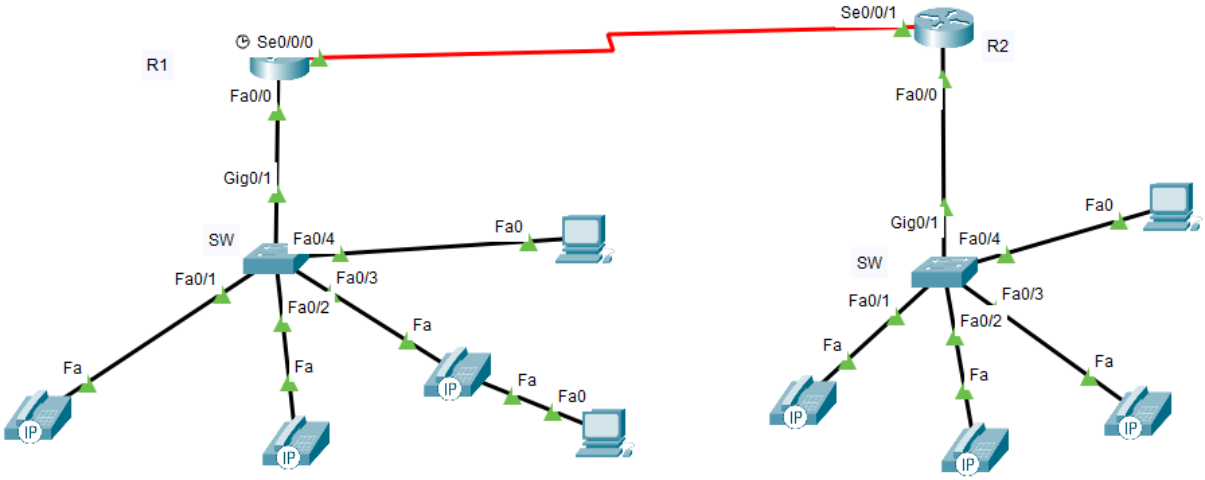
6) Call recording

Leverage your phone system to record phone calls between customers and your staff. Is your team handling calls with care and precision? Recording calls through your phone system reveals areas for your team to improve. Plus, it's secure, so only authorized personnel can access it. The advantage of VoIP call recording is that it's undetectable to all parties. It also requires no extra hardware, unlike landline PBX systems.

Review questions

1. What stands for VoIP?
2. Briefly, describe the operation of VoIP.
3. list some Pros and cons of Voice over IP

Configuration of VOIP using packet tracer



R1

========

hostname R_VOIP

!

!

ip dhcp pool voip

 network 192.168.1.0 255.255.255.0

 default-router 192.168.1.1

 option 150 ip 192.168.1.1

!

interface FastEthernet0/0

 ip address 192.168.1.1 255.255.255.0

 duplex auto

 speed auto

!

interface Serial0/0/0

 ip address 10.0.0.1 255.255.255.252

 clock rate 64000

interface Vlan1

 no ip address

```
 shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.1.0
!
dial-peer voice 1 voip
 destination-pattern 3...
 session target ipv4:192.168.2.1
!
telephony-service
 max-ephones 5
 max-dn 5
 ip source-address 192.168.1.1 port 2001
 auto assign 1 to 5
!
ephone-dn 1
 number 5555
!
ephone-dn 2
 number 5556
!
ephone-dn 3
 number 5557
!
ephone 1
 device-security-mode none
 mac-address 0009.7C11.C608
 type 7960
 button 1:1
```

```
!
ephone 2
 device-security-mode none
 mac-address 0001.6430.9CCD
 type 7960
 button 1:2
!
ephone 3
 device-security-mode none
 mac-address 00E0.F979.0495
 type 7960
 button 1:3
============================
R2
========
hostname VOICE
!
ip dhcp pool VOIP2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 option 150 ip 192.168.2.1
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/1
 ip address 10.0.0.2 255.255.255.252
!
router rip
```

```
 version 2
 network 10.0.0.0
 network 192.168.2.0
!
dial-peer voice 1 voip
 destination-pattern 5...
 session target ipv4:192.168.1.1
!
telephony-service
 max-ephones 4
 max-dn 4
 ip source-address 192.168.2.1 port 2001
 auto assign 1 to 5
!
ephone-dn 1
 number 3333
!
ephone-dn 2
 number 3334
!
ephone-dn 3
 number 3335
!
ephone 1
 device-security-mode none
 mac-address 0030.A381.C18A
 type 7960
 button 1:1
!
ephone 2
 device-security-mode none
```

```
 mac-address 0001.6430.9CCD
 type 7960
 button 1:2
!
ephone 3
 device-security-mode none
 mac-address 00E0.F979.0495
 type 7960
 button 1:3
!
==============================


switch
======
interface FastEthernet0/1
 switchport mode access
 switchport voice vlan 1
!
interface FastEthernet0/2
 switchport mode access
 switchport voice vlan 1
!
interface FastEthernet0/3
 switchport mode access
 switchport voice vlan 1.
```

LEARNING UNIT 4 - Operate mobile devices

Learning Outcomes:	4.1 Describe mobile phone parts
	4.2 Connect mobile phone
	4.3 Connect specialty mobile devices
Learning hours:	**12 Hours**

Learning Outcome 4.1: Describe mobile phone parts

Mobile Devices

The Rise of Mobile Devices

A mobile device (or handheld computer) is a computer small enough to hold and operate in the hand. Typically, any handheld computer device will have an LCD or OLED flat screen interface, providing a touchscreen interface with digital buttons and keyboard or physical buttons along with a physical keyboard. Many such devices can connect to the Internet and interconnect with other devices such as car entertainment systems or headsets via Wi-Fi, Bluetooth, cellular networks or near field communication (NFC). Integrated cameras, the ability to place and receive voice and video telephone calls, video games, and Global Positioning System (GPS) capabilities are common. Power is typically provided by a lithium-ion battery. Mobile devices may run mobile operating systems that allow third-party applications to be installed and run.

Characteristics

Device mobility can be viewed in the context of several qualities:

- Physical dimensions and weight
- Whether the device is mobile or some kind of host to which it is attached is mobile
- To what kind of host devices can it be bound
- How devices communicate with a host
- When the mobility occurs

Strictly speaking, many so-called mobile devices are not mobile. It is the host that is mobile, i.e., a mobile human host carries a non-mobile smartphone device. An example of a true mobile

computing device, where the device itself is mobile, is a robot. Another example is an autonomous vehicle. There are three basic ways mobile devices can be physically bound to mobile hosts: accompanied, surface-mounted or embedded into the fabric of a host, e.g., an embedded controller embedded in a host device. Accompanied refers to an object being loosely bound and accompanying a mobile host, e.g., a smartphone can be carried in a bag or pocket but can easily be misplaced. Hence, mobile hosts with embedded devices such as an autonomous vehicle can appear larger than pocket-sized.

As stated earlier, the most common size of mobile computing device is pocket-sized that can be hand-held, but other sizes for mobile devices exist, too. Mark Weiser, known[by whom?] as the father of ubiquitous computing, computing everywhere, referred to device sizes that are tab-sized, pad and board sized, where tabs are defined as accompanied or wearable centimeter-sized devices, e.g. smartphones, phablets and pads are defined as hand-held decimeter-sized devices. If one changes the form of the mobile devices in terms of being non-planar, one can also have skin devices and tiny dust-sized devices.

Dust refers to miniaturized devices without direct HCI interfaces, e.g., micro electro-mechanical systems (MEMS), ranging from nanometres through micrometers to millimeters. See also Smart dust. Skin: fabrics based upon light emitting and conductive polymers and organic computer devices. These can be formed into more flexible non-planar display surfaces and products such as clothes and curtains, see OLED display. Also see smart device.

Although mobility is often regarded [by whom?] as synonymous with having wireless connectivity, these terms are different. Not all network access by mobile users, applications and devices need be via wireless networks and vice versa. Wireless access devices can be static and mobile users can move in between wired and wireless hotspots such as in Internet cafés. Some mobile devices can be used as mobile Internet devices to access the Internet while moving but they do not need to do this and many phone functions or applications are still operational even while disconnected to the Internet.

What makes the mobile device unique compared to other technologies is the inherent flexibility in the hardware and also the software. Flexible applications include video chat, Web browsing, payment systems, NFC, audio recording etc. As mobile devices become ubiquitous there, will be a proliferation of services which include the use of the cloud. [citation needed] Although a common

form of mobile device, a smartphone, has a display, another perhaps even more common form of smart computing device, the smart card, e.g., used as a bank card or travel card, does not have a display. This mobile device often has a CPU and memory but needs to connect or be inserted into a reader in order to display its internal data or state.

Types of mobile devices

There are many kinds of mobile devices, designed for different applications. They include:

- Mobile computers
- Tablet computer
- Netbook
- Digital media player
- Enterprise digital assistant
- Graphing calculator
- Handheld game console
- Handheld PC
- Laptop
- Mobile Internet device (MID)
- Personal digital assistant (PDA)
- Pocket calculator
- Portable media player
- Ultra-mobile PC
- Mobile phones
- Camera phones
- Feature phones
- Smartphones
- Phablets
- Digital cameras
- Digital camcorder
- Digital still camera (DSC)
- Digital video camera (DVC)

- Front-facing camera
- Pagers
- Personal navigation device (PND)
- Wearable computers
- Calculator watch
- Smartwatch
- Head-mounted display
- Smart cards

Mobile Devices and Their Uses

Let's take a look at some of the most popular mobile devices and their uses.

With the rise of Android and iOS, smartphones are the most popular mobile device right now, and for a good reason. These devices are handheld, can fit in a pocket, have a million and one uses, and help keep us connected at all times thanks to a constant network connection from a wireless carrier. There are many different device choices, so it should be easy to find one that meets all of your needs.

Similarly to smartphones, tablets share many of the same benefits but in a larger form factor. A tablet really shines when performing tasks that would be more suitable for a larger display with more battery life. Some examples include work presentations, heavy gaming, or even live streaming of shows in high definition on Netflix.

Laptop computers have always been popular because they give us the functionality of a desktop computer that we can take anywhere. We can use the same operating system with the same programs, which means there's no device learning curve. Having a full-sized keyboard, the same input and output ports and the ability to connect an external display are some added benefits as well.

Smartwatches are relatively new and play in somewhat of a niche market at this point in time. The main benefits a smartwatch can provide us with are the ability to get notifications and necessary information on our wrist without having to pick up another device. With some of the new standalone models, we can take and receive phone calls just like our smartphones can.

E-readers have been around for many years, and they share some commonalities with a tablet, but their primary purpose is for reading. The Amazon Kindle and Barnes & Noble Nook have made

the e-reader a popular choice for people who enjoy reading books in a digital format. These devices changed the whole concept of reading and helped to bring books into a new era.

Handheld gaming consoles go way back to Nintendo's Gameboy and have forever changed how we think about mobile gaming. Some of the most well-known mobile gaming devices we have today include the Nintendo Switch and the Nintendo 3DS. Gaming is now one of the most popular forms of entertainment, and there will always be a need for such devices.

New Mobile Trends

With every passing year, new sets of trends in the world of technology emerge. We can expect quite a few mobile-based trends, specifically over the next few years. For example, we will see a more significant shift to progressive web applications, more websites that provide a mobile-first environment, and a continual focus on artificial intelligence-based apps and services. Let's take a closer look at each.

Mobile Operating System

Like desktops and laptops, mobile devices use an operating system (OS) to run software. This chapter focuses on the two most used mobile operating systems: Android and iOS. Android is developed by Google, and iOS is developed by Apple. Before users can analyze and modify software, they must be able to see the source code. Source code is the sequence of instructions that is written in human readable language, before it is turned into machine language (zeroes and ones). The source code is an important component of free software as it allows the user to analyze and eventually modify, he code. When the developer chooses to provide the source code, the software is said to be open source. If the program's source code is not published, the software is said to be closed source.

Figure is titled "Android GUI". Photograph shows a screenshot of an Android tablet screen.

Description

Android is an open source, Linux based smartphone/tablet operating system developed by the Open Hadset Alliance, primarily driven by Google. Released in 2008 on the HTC Dream, the Android OS has been customized for use on a wide range of electronic devices. Because Android is open and customizable, programmers can use it to operate devices like laptops, smart TV, and e-book readers. There have even been Android installations in devices like cameras, navigation systems, and portable media players. The figure shows Android running on a tablet.

Figure 3 is titled "iOS GUI". Photograph shows a screenshot of an Apple iPhone running iOS.

Description

iOS is a closed source Unix based operating systems for Apple's iPhone smartphone and iPad

tablet. Released in 2007 on the first iPhone, the Apple iOS source code was not released to the public. To copy, modify or redistribute iOS requires permission from Apple.

The figure shows iOS running on an iPhone.

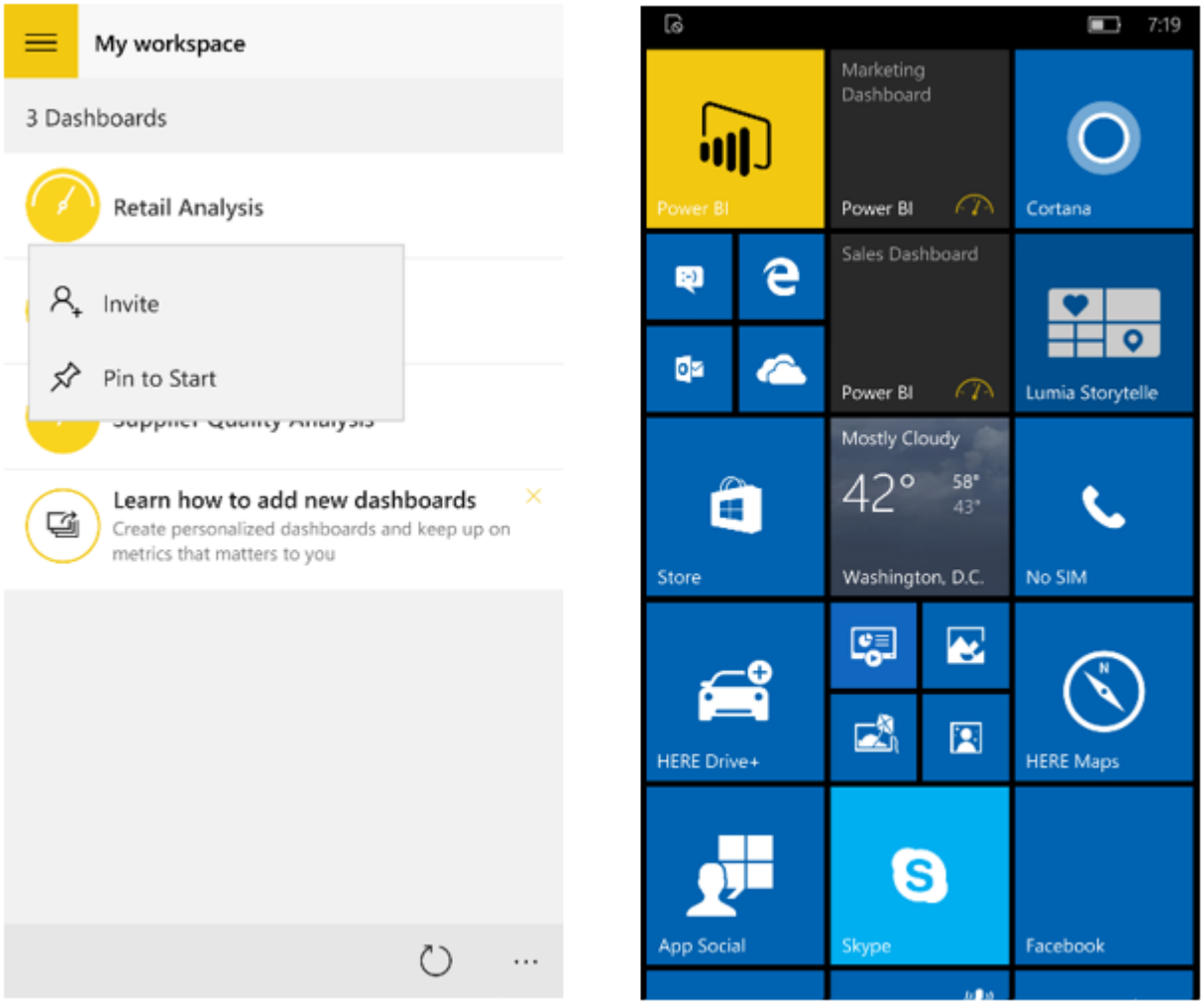


Figure 4 is titled "Windows 10 Mobile". The photograph shows a screenshot from a Windows smartphone.

Description: iOS is not the only closed source OS for mobile devices. Microsoft also created a version of Windows for their mobile devices.

Content source

Graphic consists of three figures. Each figure is represented by a screenshot of the apps installed on a device. Instructions:

Figure 1 is titled "Applications". The photograph is symbolic and shows a smartphone with application icons suspended above it.

Description: Apps are programs that are executed on mobile devices. Apps are written and compiled for a specific operating system, such as Apple iOS, Android, or Windows. Mobile devices come with a number of different apps preinstalled to provide basic functionality. There are apps to make phone calls, send and receive email, listen to music, take pictures and play video or video games. Apps are used on mobile devices the same way that programs are used on computers. Instead of being installed from an optical disk, apps are downloaded from a content source. Some apps can be downloaded for free, and others must be purchased.

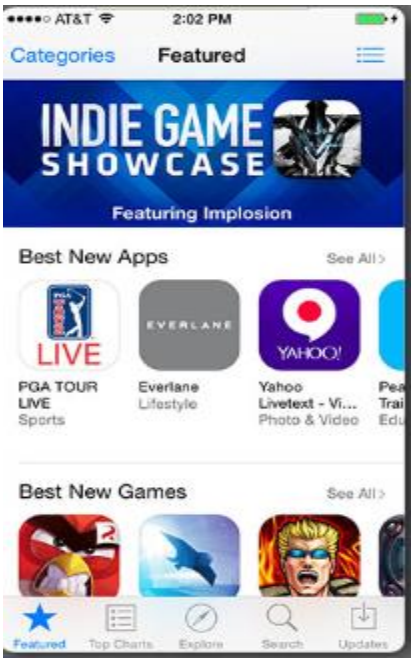


Figure 2 is titled "iOS Apps". Photograph shows a screenshot from an iPhone depicting the Apple

App Store Featured Apps screen.

Description: Apps for Apple iOS mobile devices are available for free or purchase from the App Store. Apple uses a walled garden model for their apps, meaning that the apps must be submitted to and approved by Apple before they are released to users. This helps prevent the spread of malware and malicious code. Third-party developers can create apps for iOS devices by using Apple's Software Development Kit (SDK) Xcode and the Swift programming language. Note that Xcode can only be installed on computers running OS X.

Figure 3 is titled "Android Apps". The photograph shows a screenshot from an Android tablet depicting the Google Play main screen.

Description: Android apps are available from both Google PlayTM and third-party sites, such as Amazon's App Store. Android Studio, a Java-based SDK, is available on Linux, Windows and OS X. Android apps run in a sandbox and have only the privileges enabled by the user. A prompt will appear if an app needs to obtain permissions. Permissions are granted via the app's Settings page. Third-party or custom programs areinstalled directly using an Android Application Package (apk) file. This gives the users the ability to directly install apps without going through the storefront interface. This is known as sideloading.

Android touch Interface

Graphic contains four figures. Each figure is represented by a screenshot of an Android tablet or portion of the tablet screen.

Figure 1 is titled "Icon and Widget Organization".

The photograph shows an Android smartphone positioned so that the home screen is visible. Description: Much like adesktop or laptop computer, mobile devices organize icons and widgets on multiple screens for easy access.

Figure 2 is titled "Android Main Home Screen" Photograph of Android tablet home screen is displayed, with sections highlighted.

The highlighted areas are: The background process and indicators at the top left of the screen, the system items and clock at the top right of the screen, the Google search bar at the top center of the screen, the main area in the center of the screen for applications and widget icons, the dock area near the bottom of the screen where active processes and frequently used apps are displayed, the navigation icons in the system bar at the bottom of the screen and the home screen indicator

centered above the dock area.

Description: One screen is designated as the home screen. Additional screens are access by sliding the home screen to the left or right. Each screen contains navigation icons, the main area where icons and widgets are accessed, and notification and system icons. The screen indicator displays which screen is currently active.

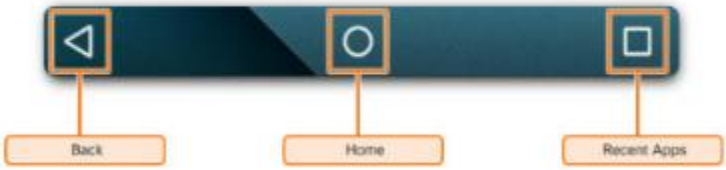


Figure 3 is titled "Navigation Icons". The photograph shows the portion of the Android home screen where the navigation buttons are located.

There are three buttons which are highlighted and labeled. The button to the far left is labeled "Back". The center button is labeled "Home" and the button to the far right is labeled "Recent Apps". Description: The Android OS uses the system bar to navigate apps and screens The system bar is always displayed at thebottom of every screen.

The system bar contains the following buttons: Back - returns to the previous screen. If the on-screen keyboard is displayed, this button closes it. Continuing to press the back button returns to the home screen. Home - Returns to the home screen. Recent Apps - Opens thumbnail images of recently used apps. To open an app, touch its thumbnail. Swipe a thumbnail to remove it from the list. Menu - If available, Menu shows additional options for the current screen.

Figure 4 is titled "Notification and System icons". Picture shows an Android tablet screen with

five areas highlighted.

First area is icon for Quick Access to User at top right of screen. Second area is the icon for Quick Access to Settings, which is located to the left of the Quick Access to User icon. Third highlighted area is the screen brightness setting bar, which appears when the notification area is open. Fourth area is the Toggle Often Used Settings area in the center of the screen. The fifth area is the Respond to Notifications area where notifications are listed and actions can be taken.

Description: To open the notification are on Android devices, swipe down from the top of the screen. You can do the following when notifications are open: respond to a notification by touching it, dismiss a notification by swiping it off the screen to either side, dismiss all notifications with the icon, toggle often-used settings, adjust the brightness of the screen, and open the settings menu with the Quick Settings icon.

Graphic contains three figures. Each figure is represented by a screenshot from a mobile device.

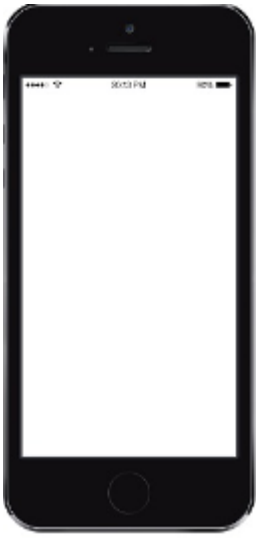


Figure 1 is titled "GPS". Picture shows a smartphone mounted on a dashboard of a car with a GPS app loaded.

Description: Another common feature of mobile devices is the Global Positioning System (GPS). GPS is a navigation system that determines the time and geographical location of the device by using messages from satellites in space and a receiver on Earth. A GPS radio receiver uses at least four satellites to calculate its position based on the messages. GPS is very accurate and can be used under most weather conditions. However, dense foliage, tunnels, and tall buildings can interrupt satellite signals. GPS receivers must have line-of-sight to GPS satellites and do not work well indoors. Indoor Positioning Systems (IPS) can determine device location by triangulating its

proximity to other radio signals, such as Wi-Fi access points.

Figure 2 is titled "Android location services". Picture is screenshot of Location Services setting on an Android tablet. Description:

To enable GPS on Android devices, use the following path: Settings > Location > Tap on the toggle to turn location services on. Figure 3 is titled "iOS location services". Picture is screenshot of iPhone Location Services settings.

Description: To enable GPS on iOS devices, use the following path: Settings > Privacy > Location Services > Turn location services on.

Review questions

1. With examples, explain the mobile devices

2.What are the characteristics if the mobile devices

3.Define the use of Mobile phones

Learning Outcome 4.2: Connect mobile phone

BLUETOOTH

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers,coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability.

A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos. Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology. Monitoring devices can communicate with sensor devices in a small health care center. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their laptop computers at a conference.

Bluetooth was originally started as a project by the Ericsson Company. It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway. Blaatand translates to Bluetooth in English. Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

Architecture

Bluetooth defines two types of networks: piconet and scatternet.

1. **Piconets**

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary and the secondary can be one-to-one or one-to-many.

Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state. A secondary in a parked state is synchronized with the primary but cannot take part in communication until it is moved from the parked state. Because only eight stations can

be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

2. **Scat/ernet**

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages. Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.

Bluetooth Devices

A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.

Bluetooth Layers

Bluetooth uses several layers that do not exactly match those of the Internet model we have defined in this book.

Radio Layer

The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

Band

Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

FHSS

Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to

avoid interference from other devices or other networks. Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second. A device uses a frequency for only 625 Ils (1/1600 s) before it hops to another frequency; the dwell time is 625 Ils.

Modulation

To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering; a discussion of this topic is beyond the scope of this book). GFSK has a can'ier frequency. Bit 1 is represented by a frequency deviation above the carrier; bit ais represented by a frequency deviation below the carrier. The frequencies, in megahertz, are defined according to the following formula for each channel:

fc=2402+n n =0, 1,2,3, ..., 78

For example, the first channel uses carrier frequency 2402 MHz (2.402 GHz), and the second channel uses carrier frequency 2403 MHz (2.403 GHz).

Baseband Layer

The baseband layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA (see Chapter 12). The primary and secondary communicate with each other using time slots. The length of a time slot is the same as the dwell time, 625 Ils. This means that during the time that one frequency is used, a sender sends a frame to a secondary, or a secondary sends a frame to the primary. Note that the communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.

TDMA

Bluetooth uses a form of TDMA (see Chapter 12) that is called TDD-TDMA (time division duplex TDMA). TDD-TDMA is a kind of half-duplex communication in which the secondary and receiver send and receive data, but not at the same time (half duplex); however, the communication for each direction uses different hops. This is similar to walkie-talkies using different carrier frequencies. Single-Secondary Communication If the piconet has only one secondary, the TDMA operation is very simple. The time is divided into slots of 625 Ils. The primary uses even numbered slots (0, 2, 4, ...); the secondary uses odd-numbered slots (1, 3, 5, ...). TDD-TDMA allows the primary and the secondary to communicate in half-duplex mode.

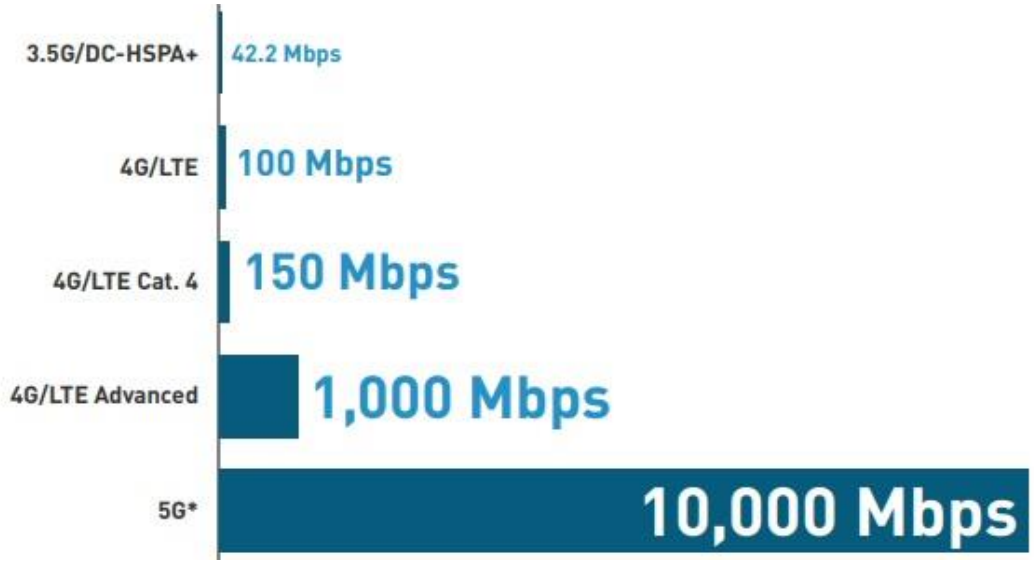
In slot 0, the primary sends, and the secondary receives; in slot 1, the secondary sends, and the primary receives.

CELLULAR COMMUNICATION

Description of Cellular communication generations

- ✓ 2G
- ✓ 2.5G
- ✓ 3G
- ✓ 4G
- ✓ 5G

The cellular communications networks are known by their numeric generation: 1G, 2G, 3G, 4G and 5G. We are currently fully deployed in 4G with 5G gaining ground. See also wireless LAN, wireless glossary and Wi-Fi vs. cellular.



5G

The 5G network is on its way and is widely anticipated by the mobile industry. Many experts claim that the network will change not just how we use our mobiles, but how we connect our devices to the internet. The improved speed and capacity of the network will signal new IoT trends, such as connected cars, smart cities and IoT in the home and office. The latest cellular generation began in 2018 and will take several years for nationwide adoption. 5G increases speed but at a cost of deploying many more cell towers when the high frequencies are used.

The next generation of telecom networks (fifth generation or 5G) has started hitting the market end of 2018 and will continue to expand worldwide.

Beyond speed improvement, the technology is expected to unleash a massive 5G IoT (Internet of Things) ecosystem where networks can serve communication needs for billions of connected

devices, with the right trade-offs between speed, latency, and cost.

- Up to 10Gbps data rate - > 10 to 100x speed improvement over 4G and 4.5G networks
- 1-millisecond latency
- 1000x bandwidth per unit area
- Up to 100x number of connected devices per unit area (compared with 4G LTE)
- 99.999% availability
- 100% coverage
- 90% reduction in network energy usage
- Up to 10-year battery life for low power IoT device
- 5G speed tops out at 10 gigabits per second (Gbps).
- 5G is 10 to x100 faster than what you can get with 4G.

4G

It's a worldwide standard for 4G wireless transmission data, the fourth generation of mobile network technology initiated in 2008. 4G LTE networks are the next generation from the existing 3G networks - Universal Mobile Telecommunications System UMTS or 3rd generation. The 3rd Generation Partnership Project (3GPP) standards group has developed and maintains LTE high-speed wireless technology.

3GGP unites telecom standard development organizations so that everybody uses the same technology.

And 4G LTE is a global success.Is 4G LTE the same as 3G?No. LTE means 4G, and the visible difference is speed!3G (third generation of mobile communications introduced in 2001) theoretically delivers 7.2Mbps and up to 3Mbps in practice.

3G HSPA+ (the advanced version - High-Speed Packet Access+) or 3G++ delivers up to 42Mps and up to 6Mbps in practice.4G LTE data rates with 100Mbps are 2,5 times faster than 3G HSPA+ and 15 times faster than 3G.LTE vs 4G: who's better?What's the difference between LTE and 4G?Well, they are not competing. LTE is the technology behind 4G (the fourth generation of mobile communications - an architecture).

All 4G phones utilize LTE technology in 2022. It brings high speed to mobile and broadband data.

How fast is 4G LTE?

In theory, LTE's maximum speed is 100Mbps. In practice, it tops at 15Mbps. Of course, it all

depends on where you're located. But what is LTE-A?LTE-A, LTE-Advanced, 4G+, and LTE+ LTE-A, LTE-Advanced, 4G+, and LTE+ are all acronyms for the same 4G service. It's a faster version of LTE. How fast is LTE-A? Again, in theory, LTE-A data rates are up to 300Mbps. In practice, you can expect between 40 to 90Mbps.LTE-A is three times faster than LTE.

4G - LTE

LTE stands for Long Term Evolution. Starting in the 2011 time frame, GSM and CDMA carriers embraced LTE, which offers higher speeds than 3G. 4G LTE integrates all communications (data, voice and video) using the IP protocol. See LTE and IP Multimedia Subsystem.

4G - WiMAX

The introduction of 4G went one step further than the revolutionary 3G. It's five times faster than the 3G network – and can in theory provide speeds of up to 100Mbps. All mobile models released from 2013 onwards should support this network, which can offer connectivity for tablets and laptops as well as smartphones. Under 4G, users can experience better latency (less buffering), higher voice quality, easy access to instant messaging services and social media, quality streaming and make faster downloads. Sprint was the first carrier to offer a 4G network in the U.S using the WiMAX technology. It was rolled out to major cities in 2009 but was eventually dropped in favor of LTE. See WiMAX.

4G - HSPA+

In late 2010, the ITU officially designated HSPA+ as a 4G technology, having previously defined it as 3G.

3G - WCDMA/HSDPA and CDMA2000

Launched after the turn of the century, the third generation features faster Internet access with downstream speeds up to 1 Mbps and more. The predominant 3G technologies on the GSM side are WCDMA and HSDPA with CDMA2000 on the CDMA side (see WCDMA, HSPA and CDMA2000). 3G also embraces worldwide roaming for travelers .

Third generation mobile networks are still in use today, but normally when the superior 4G signal fails. 3G revolutionised mobile connectivity and the capabilities of cell-phones. In comparison to 2G, 3G was much faster and could transmit greater amounts of data. This means that users could video call, share files, surf the internet, watch TV online and play online games on their mobiles for the first time. Under 3G, cell-phones where no longer just about calling and texting, they were

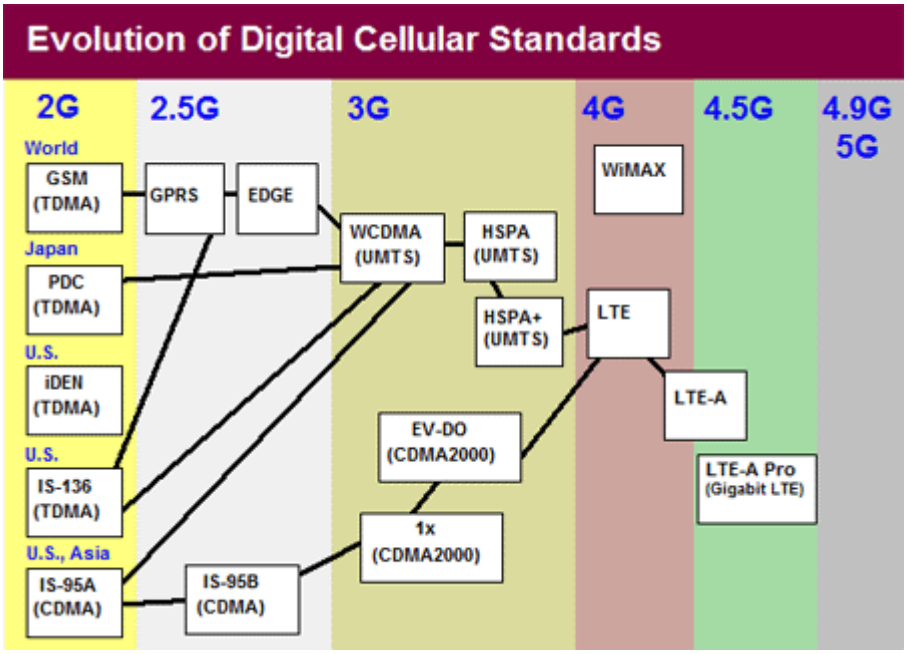
the hub of social connectivity.

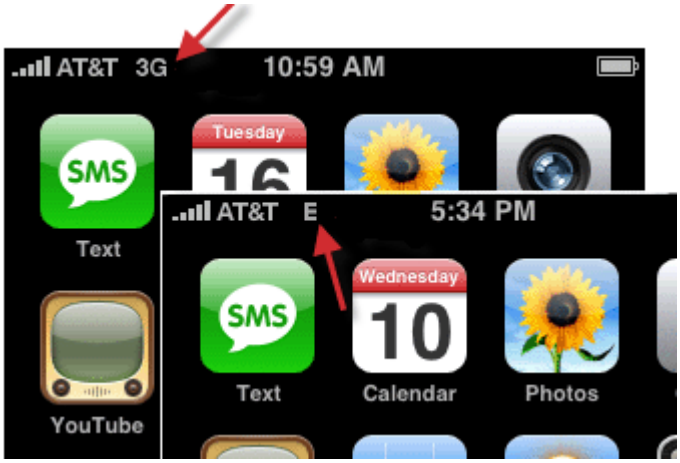
2G/2.5G - GSM/CDMA, GPRS/EDGE/IS95-B

The second generation refers to the digital voice systems of the 1990s, replacing analog phones and based on the TDMA and CDMA air interfaces. First deployed in Europe, GSM became the predominant TDMA system worldwide. Data networks were added (GPRS, EDGE, IS-95B), and these so-called 2.5G technologies enabled Internet access and email with slow downstream speeds in the Kbps range. See GSM, CDMA, GPRS, EDGE and IS-95. The 1G network was not perfect, but it remained until remained until 1991 when it was replaced with 2G. This new mobile network ran on digital signal, not analogue, which vastly improved its security but also its capacity. On 2G, users could send SMS and MMS messages (although slowly and often without success) and when GPRS was introduced in 1997, users could receive and send emails on the move.

1G - Analog Voice

Introduced in the late 1970s, the first cellular systems were analog voice. Years later, some 1G cellphones occasionally provided wireless data service to a laptop by connecting them to the laptop's dial-up modem, but hookups were precarious and the data transfer rate was minuscule. See AMPS, TACS and NMT. First generation mobile networks were reliant upon analogue radio systems which meant that users could only make phone calls, they couldn’t send or receive text messages. The 1G network was first introduced in Japan in 1979 before it was rolled out in other countries such as the USA in 1980. In order to make it work, cell towers were built around the country which meant that signal coverage could be obtained from greater distances. However, the network was unreliable and had some security issues. For instance, cell coverage would often drop, it would experience interference by other radio signals and due to a lack of encryption, it could easily be hacked. This means that with a few tools, conversations could be heard and recorded.





Cellphones generally support two technology generations. For example, if this earlier iPhone was in range of a 3G cell tower, it used the higher speed of HSDPA. However, it throttled down to the very low-speed EDGE (E) channel if 3G was not available. See HSPA.

Review questions

1. State the methods used to connect mobile phone to other devices

2.describe the Cellular communication generations

Learning Outcome 4.3: Connect specialty mobile devices

A. GPS RECEIVER

A GPS Receiver is a L-band radio processor capable of solving the navigation equations in order to determine the user position, velocity and precise time (PVT), by processing the signal broadcasted by GPS satellites.

Any navigation solution provided by a GNSS Receiver is based on the computation of its distance to a set of satellites, by means of extracting the propagation time of the incoming signals traveling through space at the speed of light, according to the satellite and receiver local clocks.

Notice that satellites are always in motion, so previous to obtaining the navigation message, the satellite's signal is detected and tracked. The receiver's functional blocks that perform these tasks are the antenna, the front-end and the baseband signal processing (in charge of acquiring and tracking the signal).

Once the signal is acquired and tracked, the receiver application decodes the navigation message and estimates the user position. The Navigation Message includes:

- Ephemeris parameters, needed to compute the satellite's coordinates.
- Time parameters and Clock Corrections, to compute satellite clock offsets and time conversions.
- Service Parameters with satellite health information.
- Ionospheric parameters model needed for single frequency receivers.
- Almanacs, that allow computing the position of all satellites but with a lower accuracy than the ephemeris.

The Global Positioning System (GPS)

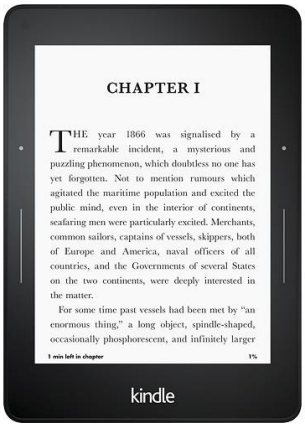
The Global Positioning System (GPS), originally Navstar GPS, is a satellite-based radionavigation system owned by the United States government and operated by the United States Space Force.[3] It is one of the global navigation satellite systems (GNSS) that provides geolocation and time information to a GPS receiver anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. Obstacles such as mountains and buildings can block the relatively weak GPS signals. The Global Positioning System (GPS), originally Navstar GPS, is a satellite-based radionavigation system owned by the United States government and operated by the United States Space Force. It is one of the global navigation satellite systems (GNSS) that

provides geolocation and time information to a GPS receiver anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. Obstacles such as mountains and buildings can block the relatively weak GPS signals.

B. E-READER

An e-reader, also called an e-book reader or e-book device, is a mobile electronic device that is designed primarily for the purpose of reading digital e-books and periodicals.

Any device that can display text on a screen may act as an e-reader; however, specialized e-reader devices may optimize portability, readability, and battery life for this purpose. Their main advantage over printed books is portability. This is because an e-reader is capable of holding thousands of books while weighing less than one book, and the convenience provided due to add-on features.



E-reader applications

Many of the major book retailers and third-party developers offer e-reader applications for desktops, tablets, and mobile devices, to allow the reading of e-books and other documents independent of dedicated e-book devices.[30] E-reader applications are available for Mac, Linux, and PC computers as well as for Android, iOS and Windows Phone devices.

C. SMARTWATCH

A smartwatch is a wearable computing device that closely resembles a wristwatch or other time-keeping device.

In addition to telling time, many smartwatches are Bluetooth-capable. The watch becomes a

wireless Bluetooth adaptor capable of extending the capabilities of the wearer's smartphone to the watch. The wearer can use the watch's interface to initiate and answer phone calls from their mobile phone, read email and text messages, get weather reports, listen to music, dictate email and text messages, and ask a digital assistant a question.
Smartwatches offer unique insights into users' location and health data that smartphones are less adept at collecting.

Other smartwatches are standalone devices with a specific purpose. For instance, some smartwatches collect data about the wearer's health, monitoring the wearer's heart rate, for instance. Others provide Global Positioning System (GPS) data, providing the wearer with walking or driving directions.

What features do smartwatches offer?

Smartwatches offer many features. Among them are the following:

health informatics, such as heart rate, blood oxygen level, blood pressure and temperature monitoring;

- contactless payment and digital wallet applications;
- messaging and calling features, similar to those on a smartphone;
- emergency calls for assistance if the watch detects the wearer has fallen;
- social media and other notifications from synchronized smartphone applications;
- games, music, photos and other entertainment options;
- location features, such as maps, a compass and an altimeter; and GPS tracking.

Smartwatches typically integrate with a user's smartphone. Many of the same features and applications available on the phone are available on the watch and can synchronize with it. Apple Watch requires that users also have an Apple iPhone.
Health and health-related parts are other features that many SmartWatch people are used. Many smart can work with fitness. This includes the following characteristics:

- Heart rate monitor
- Pedometer
- Body tracker game (running, swimming, cycling, etc.)

- High arterial pressure monitor
- look

Some smartwatches have features for special uses. For example, police officers and firefighters might use a smartwatch application to receive alerts from dispatch. Pilots in the U.S. Air Force have smartwatches with special satellite navigation features.

APPLE

Apple Watch Series 7 provides health information features, like ECG and electrical heart sensor applications.

Types of smartwatches

There are a number of general-purpose smartwatches on the market that provide a collection of features. Examples of these include the following:

Apple Watch is Apple's general-purpose smartwatch.Wear OS watches are available from multiple vendors that design and sell watches using Google's Wear operating system (OS).

Tizen watches use Samsung's proprietary smartwatch OS.

SAMSUNG

Samsung Galaxy Watch4 is a general-purpose watch that features a rotating bezel and a pseudo-analog display that mimics a traditional watch.

There are also several smartwatch options available for specific uses, such as the following:

Hiking and climbing. These watches are engineered for durability and are made to withstand drops, dust and water. They also collect basic vital signs and can forecast the weather.

Diving. These waterproof watches provide divers with important indicators such as depth, time remaining and temperature.

Aviation

Optimized for pilots, these watches have logbooks, GPS-powered maps and weather tracking. Visual assistance. Braille watches enable visually impaired users to tell time and receive notifications.

Top smartwatch products

The following are some examples of prominent smartwatches:

Apple Watch SE is a less expensive Apple Watch model.

Apple Watch Series 7 is a general-purpose smartwatch with a QWERTY keyboard and large display.

Fitbit Sense includes a comprehensive set of health and wellness features. Fitbit Versa 3 comes with custom training programs, sleep analysis and a fitness tracker. Garmin D2 Delta PX is a high-

end, general-purpose watch with GPS flight navigation for aviators and health tracking features.

Garmin Descent Mk2 Series is a specialty diving watch with Bluetooth. Garmin Vivoactive 4 has GPS, a built-in sports app, fitness tracking and contactless payment features.

Mobvoi TicWatch Pro 3 is a general-purpose smartwatch with 1 gigabyte of random access memory and sleep, heart rate and fitness tracking. Motorola Moto 360 is a fitness tracking watch that is waterproof to 30 meters.

Samsung Galaxy Watch4 is a general-purpose, Android-compatible smart digital watch with a rotating bezel. Suunto 9 Baro is a specialty hiking and outdoor sports watch.

Fitbit Sense is designed to collect and monitor health and fitness data.

History of smartwatches

Smartwatches can be traced back to the early 1970s. Hamilton Pulsar was one of the first digital watches, released in 1972. This marks the point in history when computers became small enough to fit in a wristwatch. Another early digital watch was the Calcron calculator watch, which featured a nine-digit display.

Another smartwatch predecessor was Seiko Data 2000, which came out in 1983. It could store two memos of 1,000 characters each and could be attached to a keyboard that came with the watch, which was used to type memos.

WORN & WOUND

The Seiko Data 2000 is a smartwatch predecessor that came with a separate keyboard.

Seiko RC 1000 was released in 1984. It connected to a personal computer. In 1990, Seiko released Receptor MessageWatch, a watch that received pager messages. Throughout the 1990s, wearable computers had increasingly complex data storage capabilities and battery lives.

Some of the first smartwatches were based on Microsoft's Smart Personal Objects Technology (SPOT). Fossil and Suunto introduced the first SPOT watches in 2004. The watches were able to receive news, weather and stock updates, as well as email and instant messages using frequency modulation transmitters.

Smartwatches gained popularity in the 2010s. Popular ones such as Apple Watch -- released in 2013 -- began to take on a role in the mobile computing market. Google developed Android Wear, a mobile OS, in 2014.

Future of smartwatches

Smartwatches have changed a lot in the last 50 years. They can now track, store and transmit complex data about the wearer.

One area that many smartwatch manufacturers are focusing on is biometric data. Smartwatches can monitor fitness information, like steps taken in the day and body composition. They can also monitor and spot potential medical conditions. Manufacturers are continually focusing on ways to include more health-related technologies in smartwatches.

The healthcare focus is in part related to the increase in chronic diseases that require constant

monitoring. Smartwatches are helpful in this area. In addition, with their combined GPS, health and portability features, smartwatches are useful for identifying exposure to COVID-19 and contact tracing.

Operating systems

AsteroidOS

AsteroidOS is an open source firmware replacement for some Android Wear devices.

Flyme OS

Flyme OS, firmware based on Android operating system by Meizu.

InfiniTime

InfiniTime is the default firmware for the PineTime smartwatch, produced by Pine64. It is a community project based on FreeRTOS, as well as being free software licensed under the GNU General Public License. It supports Android, desktop Linux, the PinePhone, and SailfishOS as companion devices for features such as music playback, call/text notifications, navigation instructions, and time synchronization.

LiteOS

LiteOS is a lightweight open source real-time operating system which is part of Huawei's "1+2+1" Internet of Things solution, which is similar to Google Android Things and Samsung Tizen. Currently LiteOS are introduce to the consumer market with the Huawei Watch GT series and their sub-brand Honor Magic Watch series.

Sailfish OS

Sailfish OS is a Linux-based operating system for various platforms, including Sailfish smartwatches.

Tizen

Tizen in a Samsung Gear2. Tizen is a Linux-based operating system for various platforms including smartwatches. Tizen is a project within the Linux Foundation and is governed by a Technical Steering Group (TSG) composed of Samsung and Intel among others. Samsung released the Samsung Gear 2, Gear 2 Neo, Samsung Gear S, Samsung Gear S2 and Samsung Gear S3 running Tizen.[103]

Ubuntu Touch

Ubuntu Touch is an OS developed by Canonical UK Ltd and Ubuntu Community for various mobile platforms including smartwatches.[104] It is designed primarily for touchscreen mobile

devices such as smartwatches and smartphones/tablets.

watchOS

watchOS is a proprietary mobile operating system developed by Apple Inc. to run on the Apple Watch.

Wear OS

Wear OS, previously known as Android Wear, is a smartwatch operating system developed by Google Inc.

D. AR/VR HEADSET (AUGMENTED REALITY/VIRTUAL REALITY HEADSET)

Virtual Reality (VR) is the use of computer technology to create a simulated environment. Virtual Reality's most immediately-recognizable component is the head-mounted display (HMD). Human beings are visual creatures, and display technology is often the single biggest difference between immersive Virtual Reality systems and traditional user interfaces. Major players in Virtual Reality include HTC Vive, Oculus Rift and PlayStation VR (PSVR).

Unlike traditional user interfaces, VR places the user inside an experience. Instead of viewing a screen in front of them, users are immersed and able to interact with 3D worlds. By simulating as many senses as possible, such as vision, hearing, touch, even smell, the computer is transformed into a gatekeeper to this artificial world. The only limits to near-real VR experiences are the availability of content and cheap computing power.

Virtual Reality and Augmented Reality are two sides of the same coin. You could think of Augmented Reality as VR with one foot in the real world: Augmented Reality simulates artificial objects in the real environment; Virtual Reality creates an artificial environment to inhabit.

In Augmented Reality, the computer uses sensors and algorithms to determine the position and orientation of a camera. AR technology then renders the 3D graphics as they would appear from the viewpoint of the camera, superimposing the computer-generated images over a user's view of the real world.

In Virtual Reality, the computer uses similar sensors and math. However, rather than locating a real camera within a physical environment, the position of the user's eyes are located within the simulated environment. If the user's head turns, the graphics react accordingly. Rather than compositing virtual objects and a real scene, VR technology creates a convincing, interactive world

for the user.

Virtual Reality's most immediately-recognizable component is the head-mounted display (HMD). Human beings are visual creatures, and display technology is often the single biggest difference between immersive Virtual Reality systems and traditional user interfaces. For instance, CAVE automatic virtual environments actively display virtual content onto room-sized screens. While they are fun for people in universities and big labs, consumer and industrial wearables are the wild west.

With a multiplicity of emerging hardware and software options, the future of wearables is unfolding but yet unknown. Concepts such as the HTC Vive Pro Eye, Oculus Quest and Playstation VR are leading the way, but there are also players like Google, Apple, Samsung, Lenovo and others who may surprise the industry with new levels of immersion and usability. Whomever comes out ahead, the simplicity of buying a helmet-sized device that can work in a living-room, office, or factory floor has made HMDs center stage when it comes to Virtual Reality technologies.

Types of VR headsets:

Oculus Rift - a computer-based system that reignited interest in virtual reality when the Oculus VR startup launched a successful Kickstarter campaign. Rift works with positioning technology that lets the user move physically through 3D space and has Touch controllers.

Microsoft's Hololens - a standalone VR headset. The system features 3D spatialized sound, Wi-Fi, a Kinect-like camera with a 120-degree spatial sensing system, a fleet of gyroscopes and accelerometers and a transparent screen for each eye.

HTC Vive - plugs into a powerful gaming PC for its performance. Dual base stations allow users to move freely through a 15' X 15' area. The system was developed collaboratively with Portal, a video game software company.

PlayStation VR - works with PlayStation 4 rather than a PC. The system duplicates the headset VR display on a TV.

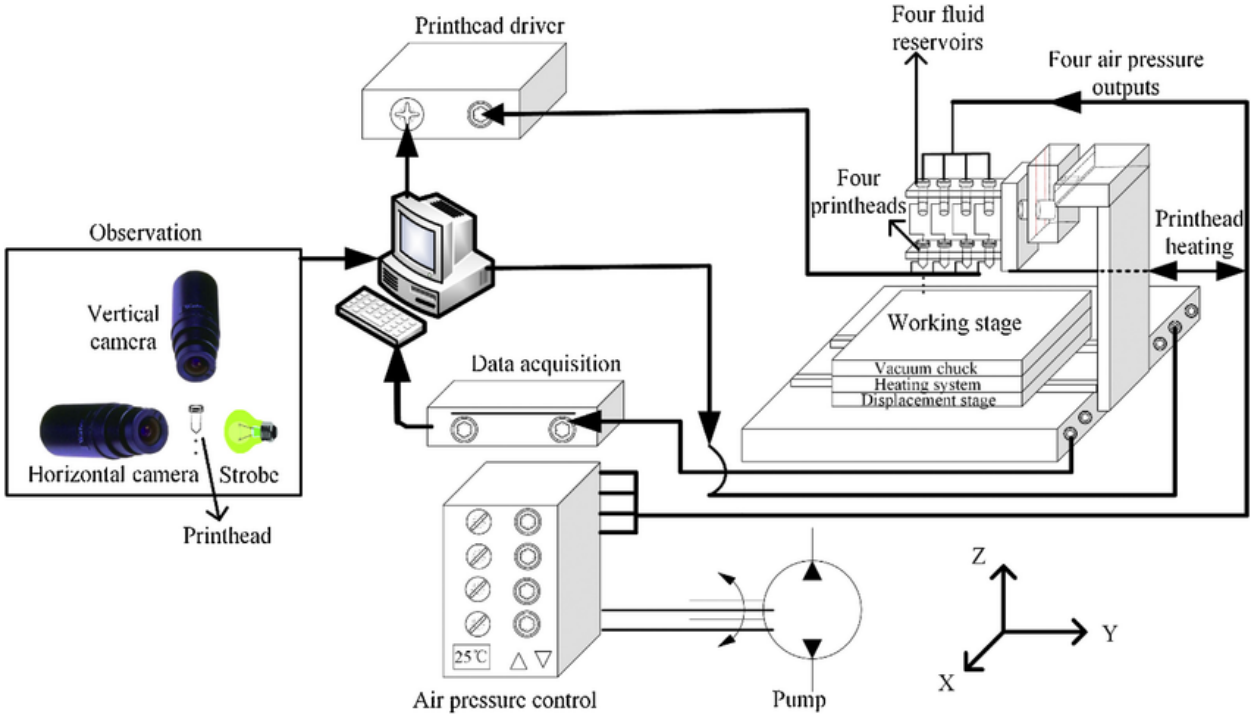
Samsung Gear VR - a smartphone container that uses the phone's processing power. The system, which works with high-end Samsung Galaxy models, was developed in collaboration with Oculus VR.

Google Cardboard - a low-cost, smartphone container made of plain cardboard. There are a number of inexpensive headsets based on the original open source model.

Learning Outcome 4.4 :PRINTER

A printer is an external hardware output device that takes the electronic data stored on a computer or other device and generates a hard copy. For example, if you created a report on your computer, you could print several copies to hand out at a staff meeting. Printers are one of the most popular computer peripherals and are commonly used to print text and photos. The picture is an example of an inkjet computer printer, the Lexmark Z605.

Schematic diagram of the Inkjet printing



Types of printers

Below is a list of all the different types of computer printers. Today, the most common printers are inkjet and laser printers.

- 3D printer
- AIO (all-in-one) printer
- Dot matrix printer
- Inkjet printer
- Laser printer
- LED printer
- MFP (multifunction printer)
- Plotter
- Thermal printer

Printer interfaces

There are a few different ways a printer can connect to and communicate with a computer (referred to as interfaces). Today, the most common connection types are by USB cable (wired) or via Wi-Fi (wireless). Below is a full list of cables and interfaces used to connect a computer to a printer.

- Cat 5
- Firewire
- MPP-1150
- Parallel port
- SCSI
- Serial port
- USB
- Wi-Fi

What are the benefits and uses of a printer?

Each type of printer has different types of uses. Examples of more frequent uses of printers include the following.

3D printer

- Print tools or parts needed to build something.
- Print replacement parts for something broken.
- Print toys for children.
- Print objects to be sold.

Inkjet printer

- Print copy of a document for school.
- Print a paper that can be physically signed.
- Print colored pictures that can be viewed without a monitor or mobile device.
- Print receipts for purchases made online.

Laser printer

- Quickly print hundreds of text documents or pages.
- Print hard copies of professional or legal documents.

Review questions

1. Briefly define the GPS connection.

2. How to use E-READER?

3. Is smartwatch mobile device? how is to connect it to the network?

4. Identify the benefits of AR/VR headset.

5. What is the purpose of printer?

6. Define the types of printers.

References:

[1] Katie T., H. (August 2021) *Printer. "Whatls.com"*. Retrieved on 20 December 2021 https://www.techtarget.com/whatis/definition/printer.

[2] Forouzan, Behrouz (2012-02-17). *Data Communications and Networking*. McGraw-Hill.p. 14. ISBN 9780073376226.

[3] Peassler "*CCTV "*. Retrieved 21 December 2022. https://www.paessler.com/it-explained/cctv

[4] Reuben Y. "what is a VoIP?" GETVoIP, 1st November 2021. Retrieved on 22nd Dec 2022. https://getvoip.com/library/what-is-an-ip-phone

[5] Dingle, Simon (5 September 2013). "A history of the smart watch and why nobody wants one". Medium. Medium. Retrieved 14 September 2013.