Unit IV – IOT Systems, Network and Protocols 7 Hr

Syllabus:

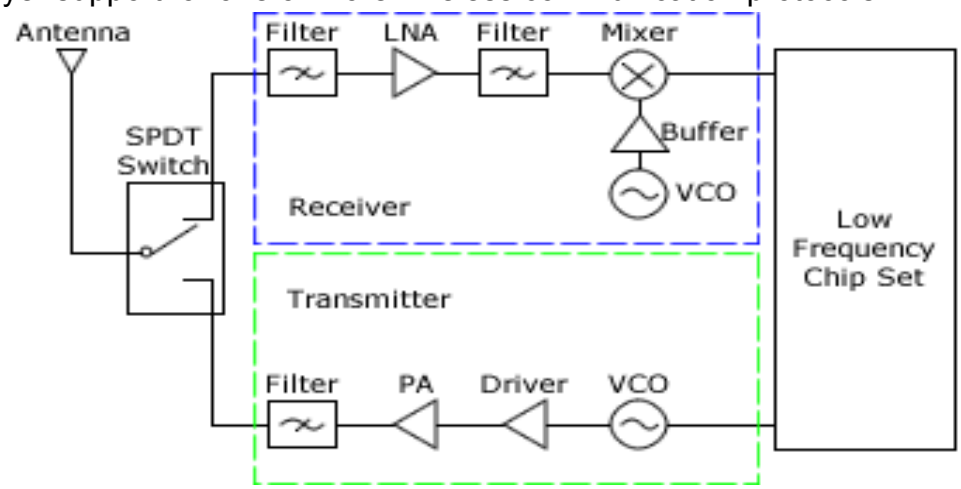
Study of RF Wireless Sensors, Wireless networks; Wireless Sensor Networking (WSN), Cellular Machine-to- Machine (M2M) application networks, Computer Connected to Internet, Network Devices; Device configuration and management, Exchange information in real time without human intervention, IoT Protocols

WHAT IS A WIRELESS SENSOR?

A wireless sensor is a device that can gather sensory information and detect changes in local environments. Wireless sensors are designed to measure specific parameters about their physical surroundings and produce outputs, often electrical signals, for further processing. These parameters include many different types of stimuli, including air temperature, lighting levels, movements, and liquid leakages.

RF Wireless Sensors:

RF wireless sensors are devices that use radio frequency (RF) signals refer to a wireless electromagnetic signal to communicate wirelessly with a central hub or controller. Radio waves are a form of electromagnetic radiation with identified radio frequencies that range from 3 kHz to 300 GHz. Frequency refers to the rate of oscillation (of the radio waves.) RF propagation occurs at the speed of light and does not need a medium like air in order to travel. RF waves occur naturally from sun flares, lightning, and from stars in space that radiate RF waves as they age. Humankind communicates with artificially created radio waves that oscillate at various chosen frequencies. RF communication is used in many industries including television broadcasting, radar systems, computer and mobile platform networks, remote control, remote metering/monitoring, and many more. While individual radio components such as mixers, filters, and power amplifiers can be classified according to operating frequency range, they cannot be strictly categorized by wireless standard (e.g. Wi-Fi, Bluetooth, etc.) because these devices only provide physical layer (PHY) support. In contrast, RF modules, transceivers, and SoCs often include data link layer support for one or more wireless communication protocols.



These sensors are typically used in applications where it is difficult or impractical to run wires or cables, such as in industrial automation, building automation, and

environmental monitoring. RF wireless sensors can measure a variety of parameters, including temperature, humidity, pressure, flow rate, and level. They typically include a sensor element, a radio transmitter, and a power source, such as a battery or energy-harvesting system.

One of the advantages of RF wireless sensors is their flexibility in installation and placement, as they can be placed in hard-to-reach or hazardous locations without requiring the installation of cabling. They also allow for easy scalability, as additional sensors can be added to the network without significant infrastructure changes.

However, RF wireless sensors can also have limitations, such as limited battery life, susceptibility to interference, and limited range depending on the frequency band and power output. These limitations can be mitigated through careful system design and selection of appropriate wireless protocols and components.

RF wireless sensors offer several advantages over wired sensors, including:

1. Flexibility: RF wireless sensors are easy to install and can be placed in difficult to reach or hazardous locations without the need for cables or wiring. This flexibility allows for easy reconfiguration and scalability of the system.
2. Reduced installation costs: Without the need for wiring and cabling, the installation costs of RF wireless sensors are significantly reduced, making them a more cost-effective option.
3. Increased reliability: With fewer cables and wires to maintain, RF wireless sensors can provide a more reliable solution for monitoring and control systems.
4. Improved accessibility: RF wireless sensors can be placed in locations that are difficult to access, such as underground or in hard-to-reach areas.
5. Lower maintenance costs: RF wireless sensors require less maintenance than wired sensors, reducing ongoing maintenance costs.
6. Real-time monitoring: RF wireless sensors can provide real-time data, allowing for immediate identification and response to changes in the monitored environment.
7. Reduced power consumption: With the use of energy harvesting or low-power consumption technologies, RF wireless sensors can operate for extended periods on battery power, reducing the need for frequent battery replacement or recharging.

Overall, RF wireless sensors offer a more flexible, cost-effective, and reliable solution for monitoring and control applications.

While RF wireless sensors offer several advantages over wired sensors, there are also some disadvantages to consider. These include:

1. Limited range: RF wireless sensors have a limited range, and obstacles like walls or other obstructions can reduce their effective range even further. This can limit the scope and scale of the sensor network.
2. Interference: RF wireless sensors are vulnerable to interference from other wireless devices operating on the same frequency band. This can cause signal loss or corruption, reducing the accuracy and reliability of the sensor readings.

3. Security concerns: Wireless sensor networks can be vulnerable to security breaches, as the signals can potentially be intercepted or hacked, allowing unauthorized access to the data.
4. Battery life: RF wireless sensors are typically battery-powered, and battery life can be limited, depending on the frequency of transmission and the power requirements of the sensor. This can result in more frequent battery replacement or recharging, adding to the maintenance costs.
5. Cost: While RF wireless sensors may offer reduced installation costs, the initial cost of the sensors and associated network infrastructure can be higher than wired solutions.
6. Data rate: RF wireless sensors typically have lower data rates compared to wired solutions, which can limit the amount of data that can be transmitted and processed in real-time.

Overall, while RF wireless sensors offer many advantages, they may not be suitable for all applications, and the disadvantages outlined above should be carefully considered when selecting a monitoring or control system.

Wireless networks

As an alternative to traditional cable and fibre optic networks, wireless networks have become crucial for enabling mobility.

A Wireless network is a type of the computer network that uses the wireless connections for connecting network nodes for data transfer. The wireless networks are very useful, inexpensive, popular and widely used. They are easy setup and do not require the cables installation. The wireless networks are usually realized and administered using the radio communications. The examples of the wireless networks are Wi-Fi local networks, cell phone networks, communications satellites, terrestrial microwave networks, and many others.

Dozens of wireless technologies exist to meet the needs each with its unique performance characteristics and optimization for specialized tasks and context be it WiFi, Bluetooth, ZigBee, NFC, WiMax, LTE, HSPA, EV-DO , earlier 3G standards, satellite services and many more.

Types of wireless networks

A group of devices connected to one another is collectively referred to as a network. For wireless networks, the medium of choice is usually radio communication.

However, there are several different technologies designed for use at different scales, topologies, and for dramatically different use cases. One way to differentiate the technologies is by using their “geographic range”.

Types of Wireless Networks

Let’s look at four different types of wireless networks and understand their characteristics:

1. Wireless Local Area Networks (LAN)
2. Wireless Metropolitan Area Networks (MAN)
3. Wireless Personal Area Networks (PAN)
4. Wireless Wide Area Networks (WAN)

The table below provides an overview of several different types of wireless networks, along with their ranges and typical use:

Type	Geographic Range	Usage	Standards
Wireless Personal Area Network (WPAN)	Within reach of an individual	Alternative, or replacement, to cables for peripherals	Bluetooth, ZigBee, NFC
Wireless Local Area Network (WLAN)	Within a building or campus	Wireless extension of wired network	IEEE 802.11(Wi-Fi)
Wireless ad hoc network (Also referred to as a wireless mesh network or mobile ad hoc network, or MANET)	Typically 100m which can be extended by multihop communication of nodes	Variety of applications where central nodes can't be relied upon, i.e. field operations, surveillance network, home and street lighting networks	Not restricted to any one technology or protocol
Wireless Metropolitan Area Network (Wireless MAN)	Citywide	Allows several WLANs to interconnect to cover a metropolitan area and provide a connection to a WAN	IEEE 802.16 (WiMAX)
Wireless Wide Area Network (Wireless WAN or WWAN)	Regional, national, or global	Typically delivered to smartphones and other handheld devices	GSM/UMTS, CDMA One/CDMA2000 and WiMAX
Cellular network	Regional, national, or global	Voice and data cellular networks	Cellular(UMTS, LTE, 0G-5G, etc.)

Wireless networks have penetrated all spheres of society, from research and development, through to businesses and personal lives.

Examples of wireless network usage include cellular or mobile phones which enable personal communications, intercontinental network systems, which rely on radio satellites to communicate globally, and the emergency services, which depend on wireless networks to communicate effectively.

Advantages of Wireless Network

1. Accessibility: Wireless networks do not require any wires or cables, and hence the users can communicate even when they are moving. It allows users to roam around without getting disconnected. As a result, there is a productivity improvement.
2. Easy installation: Installing a wireless network is faster and easier compared to a wired network. It also reduces the usage of cables that are difficult to set up and imposes the risk of safety since the user can trip on the wires and fall. If users want to change the network, they have to update the wireless network to meet the new configurations.
3. Wider reach: Wireless networks have a wider reach than wired networks. They can be easily extended to places where wires and cables are not accessible.
4. Flexibility: Setting up a wireless network helps the user to do work from home easily. Due to this network, users can work more productively and also have accessibility to customer data.
5. Efficiency: Wireless networks allow improved and better communication of data. With a wireless network, the transfer of information between users is much faster.

6. Cost-effective: Wireless networks are cost-effective since they are cheaper and easier to install. Even though their initial investment is high, with time, the overall expenses become lower.

Disadvantages of Wireless Network

1. Security: Security is a big issue while using wireless networks. If a wireless network is not installed correctly or maintained correctly, it may cause severe security threats. Connecting physical components such as wires is not required by a wireless network. They only need a wireless adapter which automatically increases the risk of hacking since hackers can have easy accessibility of the network. If there is password protection for the network, then situations may take a turn for the worse.
2. Limited bandwidth: Wireless networks cannot support VTC or Video Teleconferencing since they have minimal bandwidth. It also has limited expandability since there is an absence of a wireless spectrum for occupying. The bandwidth can also get stolen by neighbors if the network is not password protected.
3. Speed: The speed of the wireless network is slower than the speed of wired networks. Transferring or sharing files is much slower in a wireless network. The speed also depends on the location of the user concerning the network. The farther the user is from the network, the worse the connection becomes. This is a huge problem for large spaces or buildings.
4. Cost: Wireless networks are usually inexpensive, but the cost of installation is very high. Setting up a wireless network is very costly, and sometimes there are extra costs along with it. A wireless network may require the setting up of specific equipment, which can be costly.
5. Prone to interference: Due to external factors like dust storms or fog, there are high chances of interference and jamming in wireless networks. Wireless networks are highly prone to interference; therefore, fog, radiation, radio signals, or any similar interference may cause a malfunction in a wireless network. Again, when there are too many users in the same area, the air band using which the signals are transmitted can get overloaded.
6. Coverage: The coverage area of a wireless network is minimal. A typical wireless router allows users within the range of 150 to 300 feet to use the network.
7. Requires basic computer knowledge: Setting up a wireless network requires minimum knowledge of computers. People who are inexperienced in the computer field may face trouble installing a wireless network. There is a high risk of security, and hackers can easily hack those networks.

Wireless Sensor Networking (WSN)

The wireless sensor network is an intelligent and comprehensive information system that integrates information collection, information transmission, and information processing. Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. A Wireless Sensor Network is a self-configuring network of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world. Wireless Sensor nodes are called motes Provide a bridge between the real physical and virtual world's .Allow the ability to observe the previously unobservable at a fine resolution over large spatio-temporal scales. Have a wide range of potential applications to industry, science, transportation, civil infrastructure, and security.

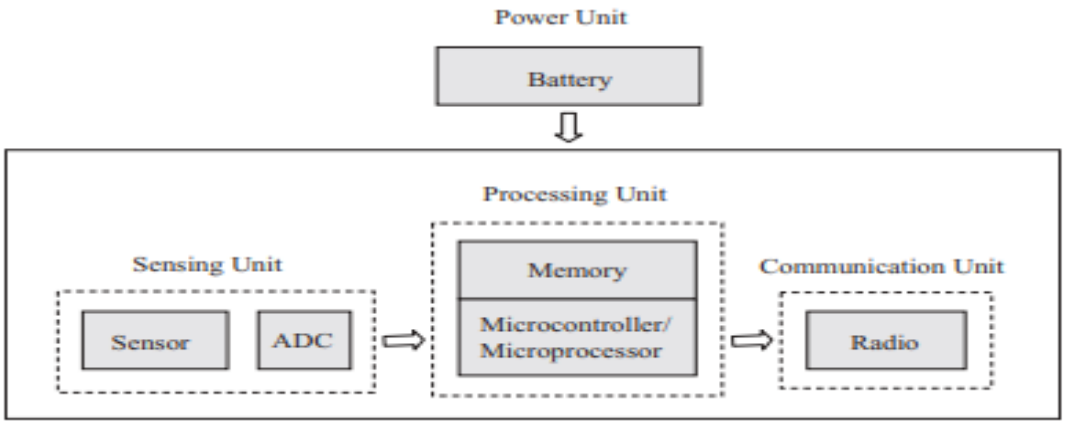
NETWORK ARCHITECTURES FOR WIRELESS SENSOR NETWORKS

A typical wireless sensor network can be divided into two elements. They are: 1. Sensor Node and 2. Network Architecture

First we see the structure of a sensor node and then describe typical network architectures for WSNs.

Sensor Node Structure

A sensor node typically consists of four basic components: a sensing unit, a processing unit, a communication unit, and a power unit, which is show in the following figure



The sensing unit usually consists of one or more sensors and analog - to – digital converters (ADCs). The sensors observe the physical phenomenon and generate analog signals based on the observed phenomenon. The ADCs convert the analog signals into digital signals, which are then fed to the processing unit.

The processing unit usually consists of a microcontroller or microprocessor with memory (e.g., Intel ' s StrongARM microprocessor and Atmel ' s AVR microprocessor), which provides intelligent control to the sensor node.

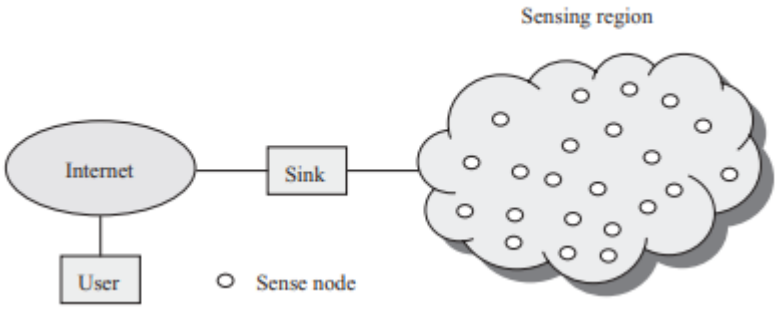
The communication unit consists of a short - range radio for performing data transmission and reception over a radio channel.

The power unit consists of a battery for supplying power to drive all other components in the system. In addition, a sensor node can also be equipped with some other units, depending on specific applications.

For example, a global positioning system (GPS) may be needed in some applications that require location information for network operation. A motor may be needed to move sensor nodes in some sensing tasks. All these units should be built into a small module with low power consumption and low production cost.

Network Architectures

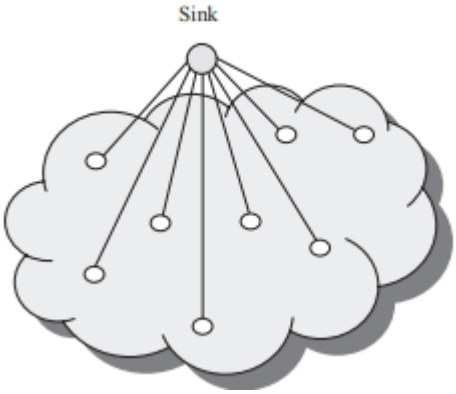
A sensor network typically consists of a large number of sensor nodes densely deployed in a region of interest, and one or more data sinks or base stations that are located close to or inside the sensing region, as shown in Fig



The sink(s) sends queries or commands to the sensor nodes in the sensing region while the sensor nodes collaborate to accomplish the sensing task and send the sensed data to the sink(s). Meanwhile, the sink(s) also serves as a gateway to outside networks, for example, the Internet. It collects data from the sensor nodes, performs simple processing on the collected data, and then sends relevant information (or the processed data) via the Internet to the users who requested it or use the information.

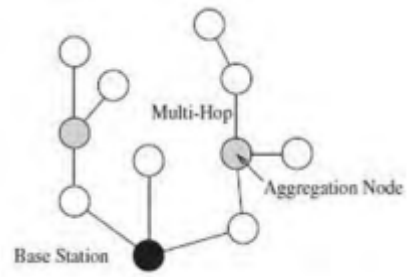
• The base station sends commands to the sensor nodes and the sensor node perform the task by collaborating with each other. The sensor nodes in turn send the data back to the base station. A base station also acts as a gateway to other networks through the internet. After receiving the data from the sensor nodes, a base station performs simple data processing and sends the updated information to the user using internet. If each sensor node is connected to the base station, it is known as Single-hop network architecture. Although long distance transmission is possible, the energy consumption for communication will be significantly higher than data collection and computation.

To send data to the sink, each sensor node can use single - hop long – distance transmission, which leads to the single - hop network architecture, as shown in Fig.



However, long - distance transmission is costly in terms of energy consumption. In sensor networks, the energy consumed for communication is much higher than that for sensing and computation. For example, the energy consumed for transferring one bit of data to a receiver at 100m away is equal to that needed to execute 3,000 instructions. In this network, each sensor node communicates directly with the base station using a single hop

However, sensor networks often cover large geographic areas and radio transmission power should be kept at a minimum in order to conserve energy; consequently, multi-hop communication is the more common case for sensor networks (shown in Figure). In this mesh topology, sensor nodes must not only capture and disseminate their own data, but also serve as relays for other sensor nodes, that is, they must collaborate to propagate sensor data towards the base station.



This can be implemented in two ways. Flat network architecture and Hierarchical network architecture.

Flat Architecture: In a fl at network, each node plays the same role in performing a sensing task and all sensor nodes are peers. Due to the large number of sensor nodes, it is not feasible to assign a global identifier to each node in a sensor network. For this reason, data gathering is usually accomplished by using data - centric routing, where the data sink transmits a query to all nodes in the sensing region via flooding and only the sensor nodes that have the data matching the query will respond to the sink. Each sensor node communicates with the sink via a multihop path and uses its peer nodes as relays. Figure 2.4 illustrates the typical architecture of a flat network.

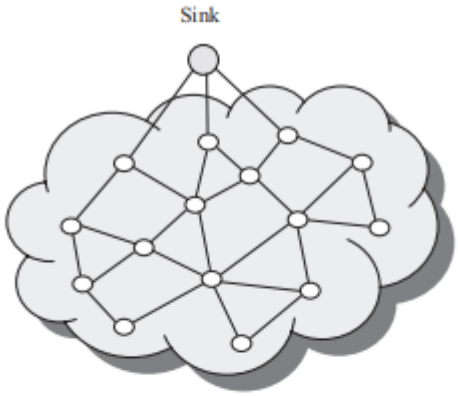


Fig. 2.4 Flat network architecture.

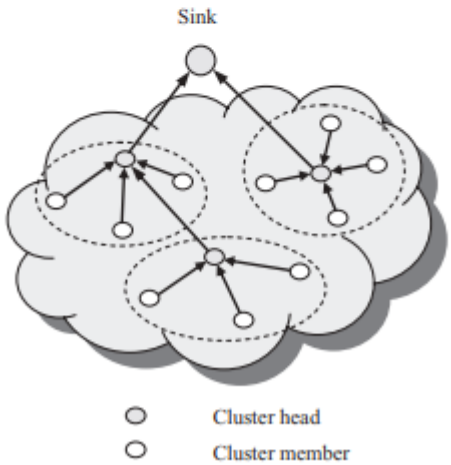


Fig. 2.5 Single-hop clustering architecture.

Hierarchical Architecture: In a hierarchical network, sensor nodes are organized into clusters, where the cluster members send their data to the cluster heads while the cluster heads serve as relays for transmitting the data to the sink. A node with lower energy can be used to perform the sensing task and send the sensed data to its cluster head at short distance, while a node with higher energy can be selected as a cluster head to process the data from its cluster members and transmit the processed data to the sink. This process can not only reduce the energy consumption for communication, but also balance traffic load and improve scalability when the network size grows. Since all sensor nodes have the same transmission capability, clustering must be periodically performed in order to balance the traffic load among all sensor nodes. Moreover, data aggregation can be performed at cluster heads to reduce the amount of data transmitted to the sink and improve the energy efficiency of the network

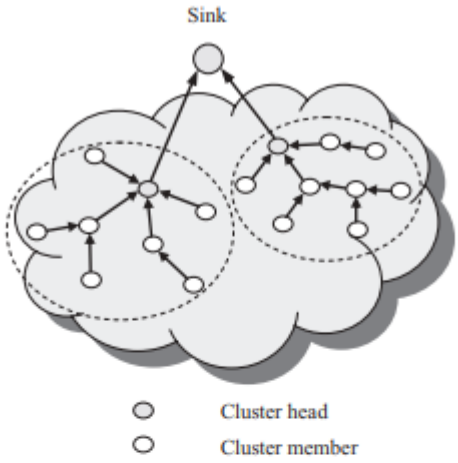


Fig. 2.6 Multihop clustering architectures.

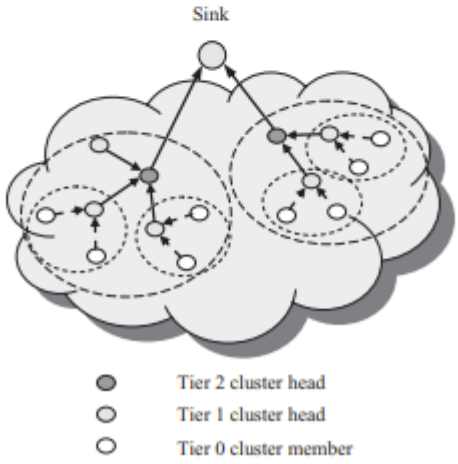


Fig. 2.7 Multitier clustering architectures.

Applications of Wireless Sensor Networks

- Habitat and Ecosystem Monitoring
- Seismic Monitoring
- Civil Structural Health Monitoring
- Monitoring Groundwater Contamination
- Rapid Emergency Response
- Industrial Process Monitoring
- Perimeter Security and Surveillance
- Automated Building Climate Control

Machine to Machine

M2M, the acronym for Machine-to-Machine communication is an emerging area in the field of telecom technologies. Machine to machine (M2M) refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability. M2M uses a device (such as a sensor or meter) to capture an event, which is relayed through a network (wireless, wired or hybrid) to an application, that translates the captured event into meaningful information.

In M2M communication, machines can be interconnected through host of media depending on the specific requirements i.e. Indoor Electrical Wiring, Wired Networks (IEEE 802.3 Ethernets), WPANs (Bluetooth, Dash7, ZigBeeetc.), Wi-Fi (IEEE 802.11), PLC, PSTN/ DSL, 2G/3G/4G or even satellites.

Machines are having capability of communication with other machines for decades. But availability of Inexpensive electronics, use of Internet Protocol (IP) along with ubiquitous network availability and cloud computing has vastly enhanced the possibility of devices equipped with communication module capable of providing their status and other information, which can be aggregated, interpreted and can be in turn used to control these devices or can be used in more meaningful ways.

With traditional revenue streams getting saturated in most markets around the world, M2M holds the promise of generating new avenues for revenue generation for TSPs/ ISPs as well as opening new business opportunities for new service providers.

Applications of M2M:

M2M Ecosystem comprises of telecom service providers, M2M application service providers, Sensors, hardware OEMs, supply chain, middleware, deployment and asset management. Varying requirement of mobility and dispersion level in different applications of M2M and Network Technology used can be explained as per the following diagram:

		NEED OF MOBILITY →	
		FIXED	**MOBILE**
GEOGRAPHICAL SPREAD →	DISPERSED	**Applications** Smart Grid, Smart Meters, Smart City Remote Monitoring **Technology** PSTN Broadband 2G/3G/4G Power Line Communication	**Applications** Car Automation eHealth Logistics Portable Consumer electronics **Technology** 2G/3G/4G Satellite
	CONCENTRATED	**Applications** Smart Home/ Smart Building Factory Automation eHealth **Technology** Wireless Personal Area Network Wired Network Indoor Electrical Wiring Wi-Fi	**Applications** On Site Logistics **Technology** Wi-Fi WPAN

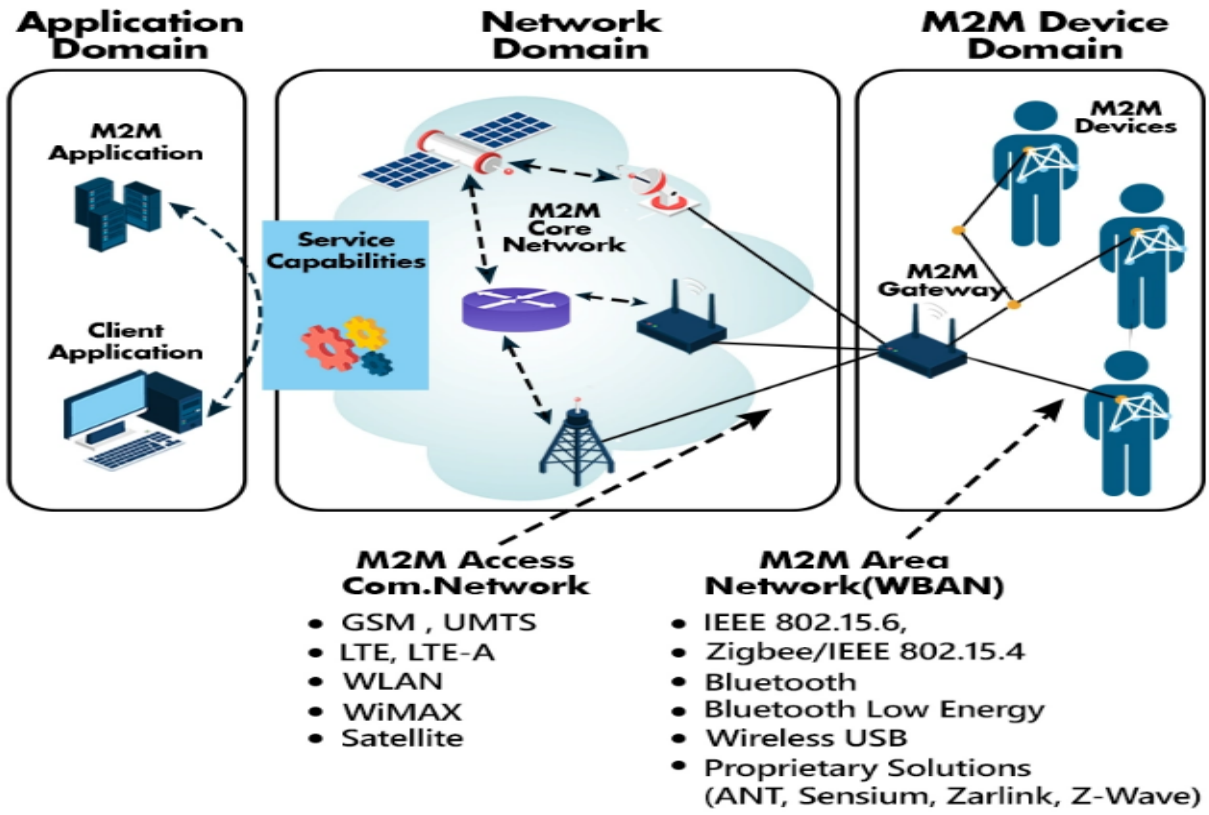
M2M is driving an increasingly complex relationship between networks, service providers and an exploding number of devices in real time. These devices will be

powered and connected by a complicated convergence of networks. Different types of applications have different needs in terms of network resources leading to requirement of different regulatory treatment to them. DoT endeavors to tackle the regulatory implications of usage of digital communication technologies, including wireless, wireline, MPLS, Ethernet, Private Line, etc. in M2M applications.

M2M architecture

M2M enables machines to communicate with other machines and pass small amounts of information. Some examples could include smoke detectors that detect smoke and send the information to various other digital devices.

In order to develop and deploy an M2M architecture, we follow the latest standards such as ETSI, ANSI C12, and so on. The three main domains of M2M architecture are:



1. **M2M application**: As the name suggests, the M2M application domain offers applications to use M2M technology conveniently. Examples include server and end-user applications.

2. **M2M network domain**: M2M network domain acts as a bridge between the M2M application domain and the M2M device domain. It is made of two parts called the M2M core and M2M service capabilities.

3. **M2M device domain**: M2M device domain contains all the devices that can connect to the M2M network easily. The device domain can also be called the M2M area network. The M2M device domain includes devices that can connect directly over a

network, devices that cannot directly connect to a network and may perhaps require an M2M gateway and proprietary devices.

Working of M2M

M2M devices send data across a network by sensing information. In order to send the data the machines use public networks such as cellular and ethernet.

M2M comprises components such as RFID, sensors, Wi-Fi communication links and automated computer software programs that translate the incoming data to generate responses or actions.

Telemetry is one of the most renowned M2M communication. It has been in use since the beginning of the last century to transmit data. Developers used telephone lines for communication and later moved to radio wave transmission signals in order to monitor the performance of the data that is gathered from remote locations.

The arrival of the internet improved the standards of wireless technology and now wireless communication is used in everyday real life applications such as hospitals, cities, stations, roads and so on.

Application of M2M

1. SMART CITIES
2. AUTOMOTIVE
3. POWER
4. SMART WATER

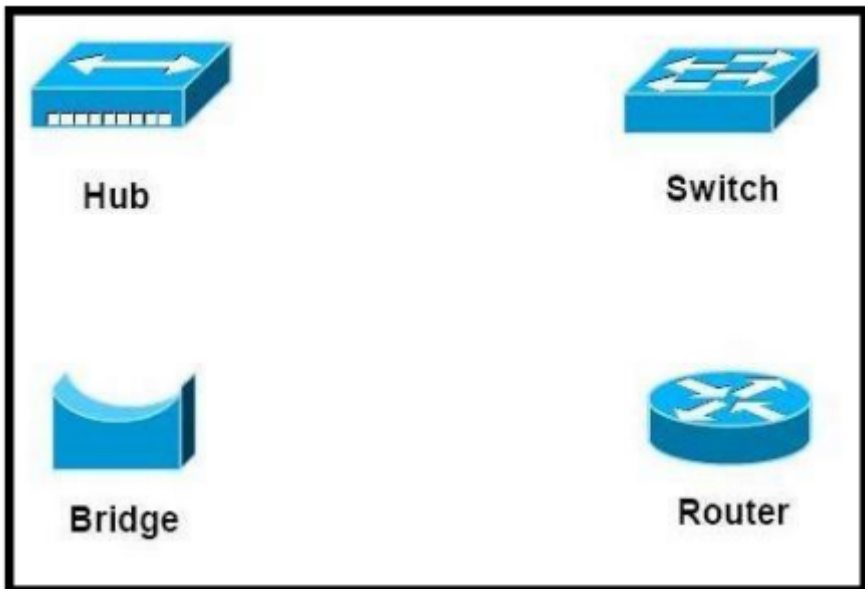
Network Devices; Device configuration and management

Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.
Network devices are called hardware devices that link computers, printers, faxes, and other electronic devices to the network. Such devices easily, safely, and correctly transfer data over one or other networks. Inter-network or intra-network devices may be available. Some devices, such as the NIC card or the connector RJ45, are mounted on the device, while others are network components such as a router, switch, etc. Let's look more closely at some of these phones. The modem is a system that can send and receive data through phone or cable lines from a computer.

The data stored on the device is digital, while a phone line or cable wire can transmit only analog data. Digital signal is converted to analog and vice versa, which is important in the modem. The modulator transforms digital data into analog. When the processor sends the data, the demodulator is translated into digital data.

Here is the common network device list:

1. Hub
2. Switch
3. Router
4. Bridge
5. Gateway
6. Modem
7. Repeater
8. Access Point



1. **Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do no amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.
   A single Ethernet segment can have a maximum length of 500 meters with a maximum of 100 stations (in a cheapernet segment it is 185m). To extend the length of the network, a repeater may be used as shown in Fig. 1. Functionally, a repeater can be considered as two transceivers joined together and connected to two different segments of coaxial cable. The repeater passes the digital signal bit-by-bit in both directions between the two segments. As the signal passes through a repeater, it is amplified and regenerated at the other end. The repeater does not

isolate one segment from the other, if there is a collision on one segment, it is regenerated on the other segment. Therefore, the two segments form a single LAN and it is transparent to rest of the system. Ethernet allows five segments to be used in cascade to have a maximum network span of 2.5 km. With reference of the ISO model, a repeater is considered as a level-1 relay as depicted in Fig..2. It simply repeats, retimes and amplifies the bits it receives. The repeater is merely used to extend the span of a single LAN. Important features of a repeater are as follows:

- A repeater connects different segments of a LAN
- A repeater forwards every frame it receives
- A repeater is a regenerator, not an amplifier
- It can be used to create a single extended LAN

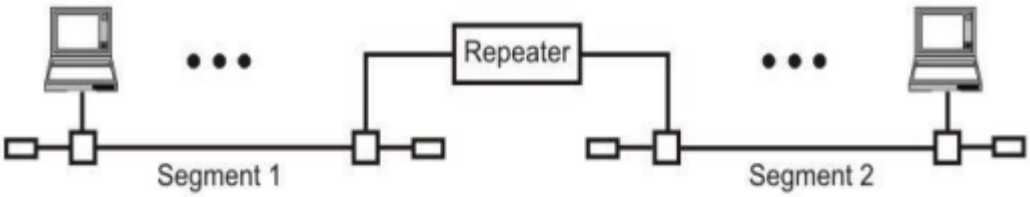


Figure Repeater connecting two LAN segments

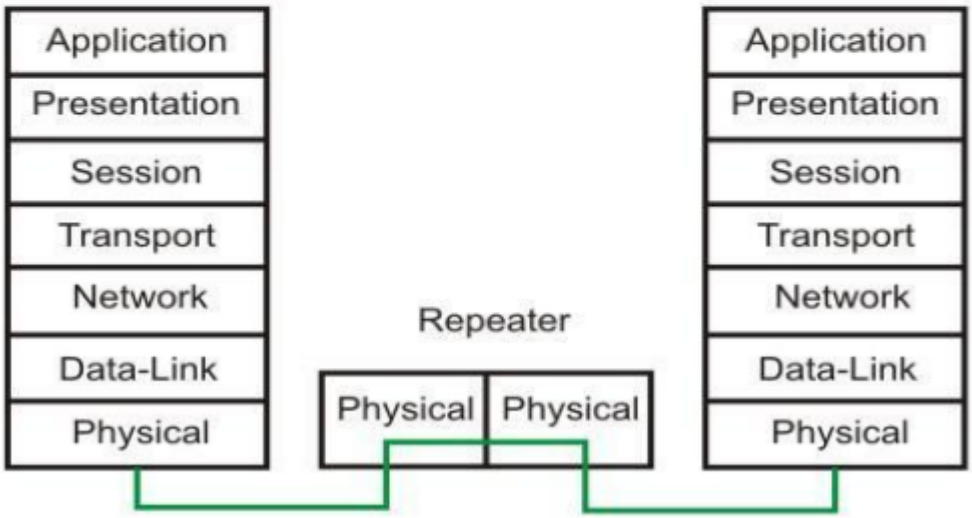


Figure Operation of a repeater as a level-1 relay

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage. Hub is a generic term, but commonly refers to a multiport repeater. It can be used to create multiple levels of hierarchy of stations. The stations connect to the hub with RJ-45 connector having

maximum segment length is 100 meters. This type of interconnected set of stations is easy to maintain and diagnose. Figure shows how several hubs can be connected in a hierarchical manner to realize a single LAN of bigger size with a large number of nodes.

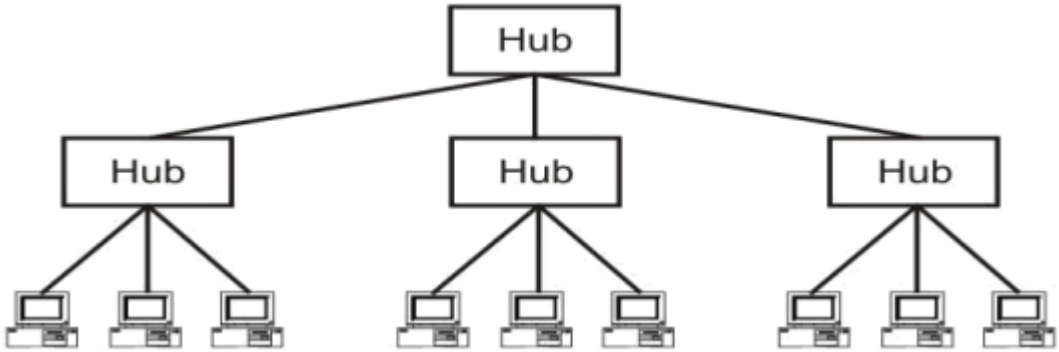


Figure Hub as a multi-port repeater can be connected in a hierarchical manner to form a single LAN with many nodes

3. **Bridge** – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.
   The device that can be used to interconnect two separate LANs is known as a bridge. It is commonly used to connect two similar or dissimilar LANs as shown in Fig. 1 the Bridge operates in layer 2, that is data-link layer and that is why it is called level-2 relay with reference to the OSI model. It links similar or dissimilar LANs, designed to store and forward frames, it is protocol independent and transparent to the end stations. The flow of information through a bridge is shown in Fig.2. Use of bridges offers a number of advantages, such as higher reliability, performance, security, convenience and larger geographic coverage. But, it is desirable that the quality of service (QOS) offered by a bridge should match that of a single LAN. The parameters that define the QOS include availability, frame mishaps, transit delay, frame lifetime, undetected bit errors, frame size and priority.

   Key features of a bridge are mentioned below:
   • A bridge operates both in physical and data-link layer
   • A bridge uses a table for filtering/routing
   • A bridge does not change the physical (MAC) addresses in a frame

   • Types of bridges: o Transparent Bridges and o Source routing bridges

   A bridge must contain addressing and routing capability. Two routing algorithms have been proposed for a bridged LAN environment. The first, produced as an extension of IEEE 802.1 and applicable to all IEEE 802 LANs, is known as transparent bridge. And the other, developed for the IEEE 802.5 token rings, is based on source routing approach. It applies to many types of LAN including token ring, token bus and CSMA/CD bus

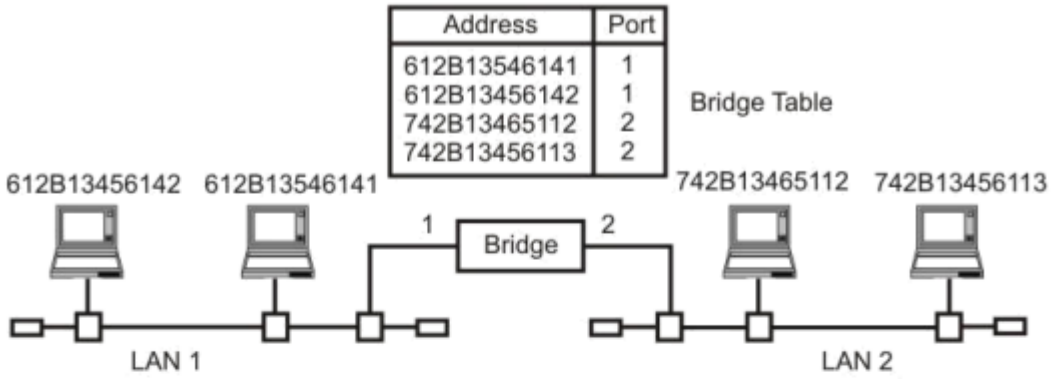


Figure A bridge connecting two separate LANs

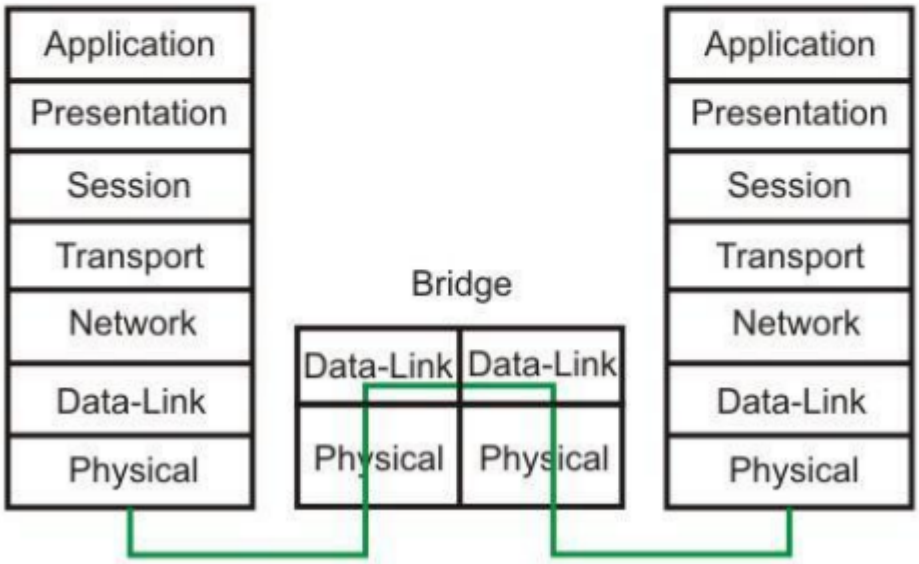


Figure Information flow through a bridge

4. Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency (large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

A switch is essentially a fast bridge having additional sophistication that allows faster processing of frames. Some of important functionalities are:

• Ports are provided with buffer
• Switch maintains a directory: #address - port#
• Each frame is forwarded after examining the #address and forwarded to the proper port#

Three possible forwarding approaches: Cut-through, Collision-free and Fullybuffered as briefly explained below.

1. Cut-through: A switch forwards a frame immediately after receiving the destination address. As a consequence, the switch forwards the frame without collision and error detection.
2. Collision-free: In this case, the switch forwards the frame after receiving 64 bytes, which allows detection of collision. However, error detection is not possible because switch is yet to receive the entire frame.
3. Fully buffered: In this case, the switch forwards the frame only after receiving the entire frame. So, the switch can detect both collision and error free frames are forwarded.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

A router is used to route data packets between two networks. It reads the information in each packet to tell where it is going. If it is destined for an immediate network it has access to, it will strip the outer packet (IP packet for example), readdress the packet to the proper ethernet address, and transmit it on that network. If it is destined for another network and must be sent to another router, it will re-package the outer packet to be received by the next router and send it to the next router. Routing occurs at the network layer of the OSI model. They can connect networks with different architectures such as Token Ring and Ethernet. Although they can transform information at the data link level, routers cannot transform information from one data format such as TCP/IP to another such as IPX/SPX. Routers do not send broadcast packets or corrupted packets. If the routing table does not indicate the proper address of a packet, the packet is discarded.

There are two types of routers:
1. Static routers - Are configured manually and route data packets based on information in a router table.
2. Dynamic routers - Use dynamic routing algorithms.

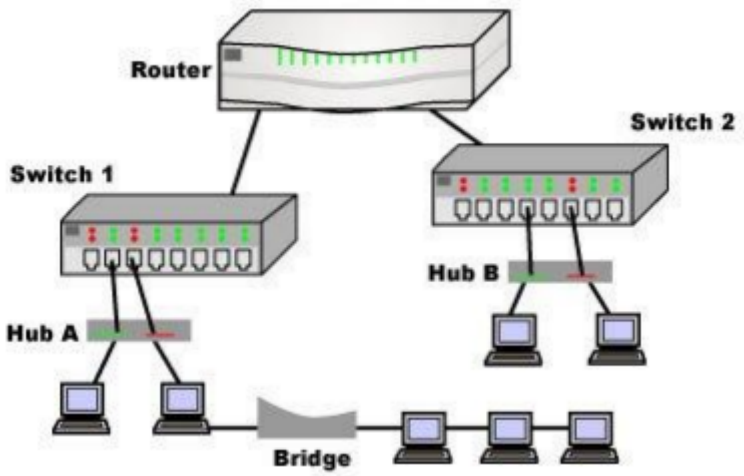
There are two types of algorithms:
o Distance vector - Based on hop count, and periodically broadcasts the routing table to other routers which takes more network bandwidth especially with more routers. RIP uses distance vectoring. Does not work on WANs as well as it does on LANs.
o Link state - Routing tables are broadcast at startup and then only when they change. The open shortest path first (OSPF) protocol uses the link state routing method to configure routes or distance vector algorithm (DVA).

Common routing protocols include:

1. IS-IS -Intermediate system to intermediate system which is a routing protocol for the OSI suite of protocols.

2. IPX - Internet Packet Exchange. Used on Netware systems.
3. NLSP - Netware Link Services protocol - Uses OSPF algorithm and is replacing IPX to provide internet capability.
4. RIP - Routing information protocol uses a distance vector algorithm.

There is a device called a brouter which will function similar to a bridge for network transport protocols that are not routable, and will function as a router for routable protocols. It functions at the network and data link layers of the OSI network model.



A router is considered as a layer-3 relay that operates in the network layer, that is it acts on network layer frames. It can be used to link two dissimilar LANs. A router isolates LANs in to subnets to manage and control network traffic. However, unlike bridges it is not transparent to end stations. A schematic diagram of the router is shown on Fig. A router has four basic components: Input ports, output ports, the routing processor and the switching fabric. The functions of the four components are briefly mentioned below.

• Input port performs physical and data-link layer functions of the router. As shown in Fig. 1 (a), the ports are also provided with buffer to hold the packet before forwarding to the switching fabric.
• Output ports, as shown in Fig., perform the same functions as the input ports, but in the reverse order.
• The routing processor performs the function of the network layer. The process involves table lookup.
• The switching fabric, shown in Fig. moves the packet from the input queue to the output queue by using specialized mechanisms. The switching fabric is realized with the help of multistage interconnection networks.

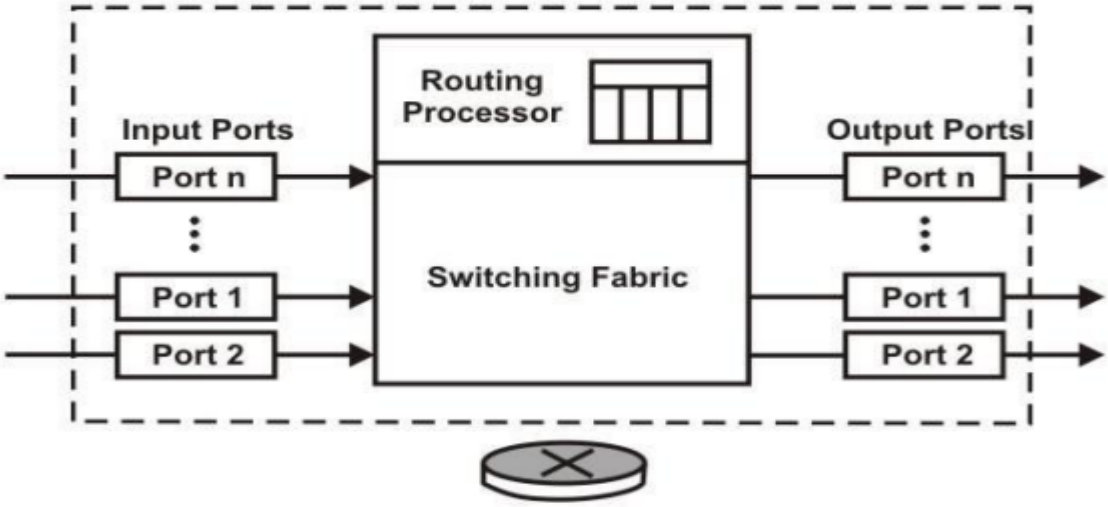
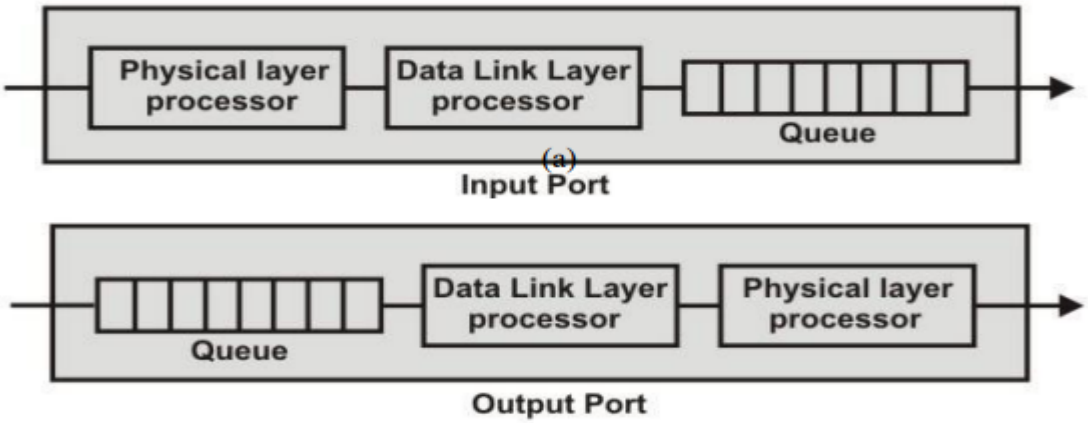


Figure Schematic diagram of a router



• Communication of a frame through a router is shown in Fig.2

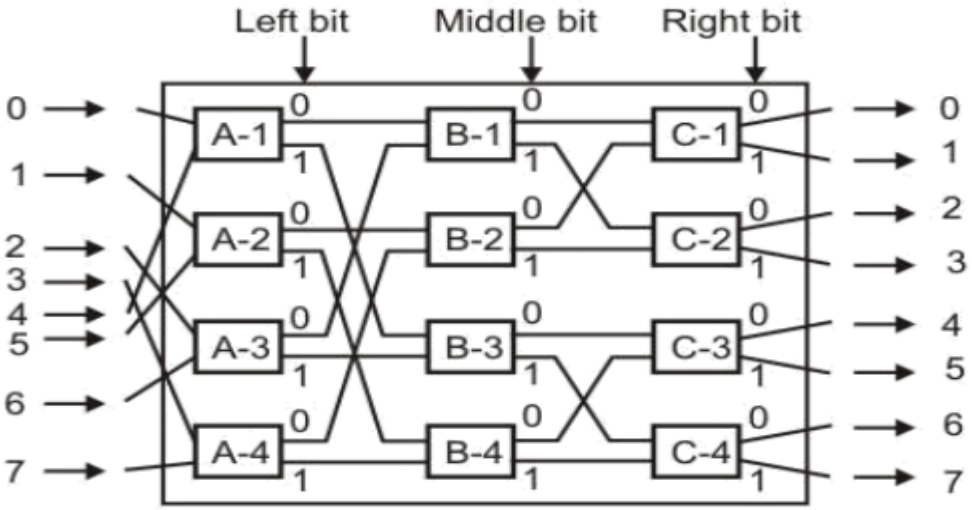


Figure Switching fabric of a router

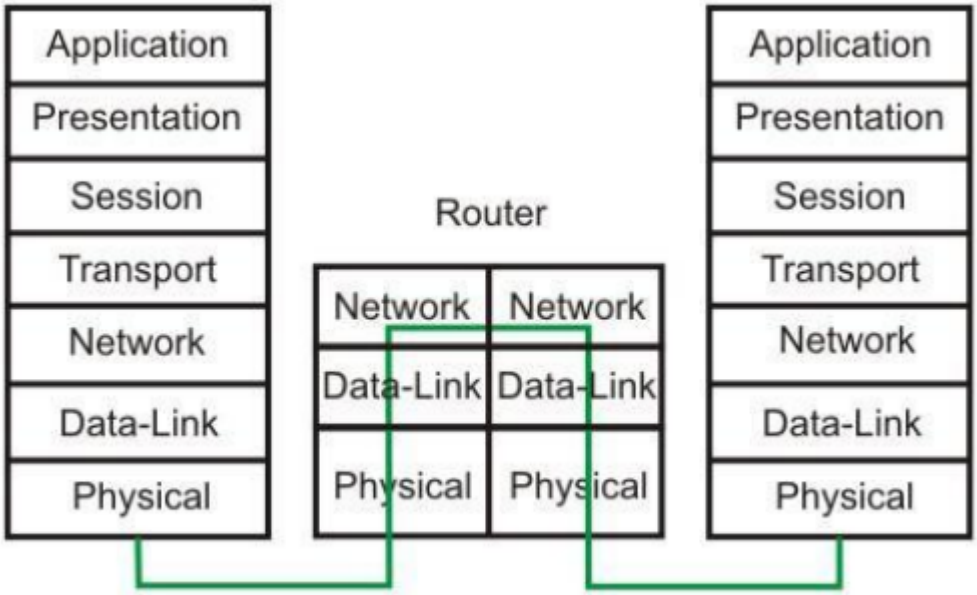


Figure Communication through a router

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

A gateway can translate information between different network data formats or network architectures. It can translate TCP/IP to AppleTalk so computers supporting TCP/IP can communicate with Apple brand computers. Most gateways operate at the application layer, but can operate at the network or session layer of the OSI model. Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model. To confuse issues, when talking about a router that is used to interface to another network, the word gateway is often used. This does not mean the routing machine is a gateway as defined here, although it could be.

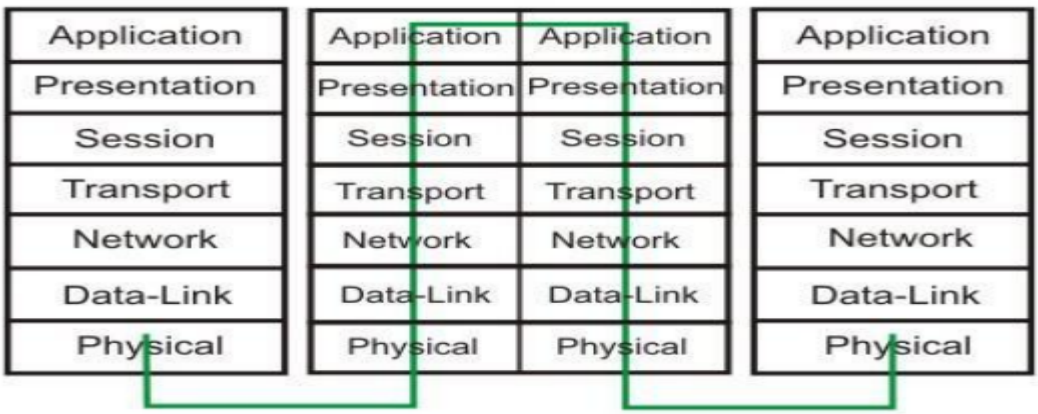


Figure Communication through a gateway

Network Device Configuration

Network configuration focuses on managing a network and its devices by applying the right set of policies, controls, and configurations. It encompasses activities from device discovery to configuration backups for efficient network administration.

Network configuration can also be automated and managed via a centralized configuration manager network configuration manager, further reducing manual IT workload and making it easier to: Maintain a network, Make configuration changes, Relaunch devices and Track and report data

Some network configuration basics include switch/router configuration, host configuration, software and firewall configuration, and network topology which can be controlled through rest APIs.

Network configuration allows a system administrator to set up a network to meet communication objectives. The process involves the following tasks::

1. Router configuration: Specifies the correct IP addresses and route settings, etc.
2. Host configuration: Sets up a network connection on a host computer/laptop by logging the default network settings, such as IP addressing, proxy, network name and ID/password, to enable network connection and communication.
3. Software configuration: Any network-based software, like an intrusion detection system (IDS), is allowed access and provided with the appropriate credentials to monitor network traffic..

In a command-line environment, the commands **ipconfig** (for Windows network configuration) and **ifconfig** (for Linux network configuration, as well as Mac OSX and other Linux-like environments) allow you to view information about your network configuration and to configure your networsk interface.

With a network configuration manager or with APIs, you can check and set up the network configuration in a centralized software interface, allowing you to more easily configure, monitor and administer your network. A network configuration manager also enables the use of automation to make policy changes and updates.

Why is network configuration important?

The right network configuration is essential to supporting the flow of traffic through a network, and it can also support and enhance network security and improve network stability. In addition, the use of network configuration management manager and or configuration tools can provide a number of benefits, including:

1. Automated data tracking and reporting, allowing administrators to spot any configuration changes and potential threats or issues
2. An easy way to make bulk changes, such as a blanket password change in a situation where passwords are compromised
3. The means to swiftly roll back network settings to a previous configuration
4. Reduced downtime, thanks to increased visibility and the ability to quickly identify changes
5. Streamlined maintenance and repair of network devices (physical or virtual) and connections

6. The ability to relaunch a device when it fails, thanks to centralized storage management of device configurations

Computer Connected to Internet

Internet connection options vary by Internet Service Provider and by region. Customers should consider some of the following factors before selecting an Internet package and Internet connection type: connection speed or bandwidth, cost, availability, reliability and convenience. In order to determine what Internet plan is right for you, we recommend you review the different types of Internet connections and connection speeds available on the market today.

Understanding The Differences Between Internet Connections

When determining which type of Internet speed and Internet connection type is right for you or your family, it's important to understand the distinction between each connection. In today's age, there are numerous ways to connect laptops, desktops, mobile phones, gaming consoles, e-readers and tablets to the Internet. Some of the most widely used Internet connections are described below.

1. MOBILE

Many cell phone and smartphone providers offer voice plans with Internet access. Mobile Internet connections provide good speeds and allow you to access the Internet.

2. WIFI HOTSPOTS

Wifi Hotspots are sites that offer Internet access over a wireless local area network (WLAN) by way of a router that then connects to an Internet service provider. Hotspots utilize WiFi technology, which allows electronic devices to connect to the Internet or exchange data wirelessly through radio waves. Hotspots can be phone-based or free-standing, commercial or free to the public.

3. DIAL-UP

Dial-up connections require users to link their phone line to a computer in order to access the Internet. This particular type of connection—also referred to as analog—does not permit users to make or receive phone calls through their home phone service while using the Internet. Now more outdated, a dial-up connection used to be among the most common Internet connection type.

4. BROADBAND

This high-speed Internet connection is provided through either cable or telephone companies. One of the fastest options available, broadband Internet uses multiple data channels to send large quantities of information. The term broadband is shorthand for broad bandwidth. Broadband Internet connections such as DSL and cable are considered high-bandwidth connections. Although many DSL connections can be considered broadband, not all broadband connections are DSL.

5. DSL

DSL, which stands for Digital Subscriber Line, uses existing 2-wire copper telephone line connected to one's home so service is delivered at the same time as landline telephone service. Customers can still place calls while surfing the Internet.

6. CABLE

Cable Internet connection is a form of broadband access. Through use of a cable modem, users can access the Internet over cable TV lines. Cable modems can provide extremely fast access to the Internet, making a cable connection a viable option for many.

7. SATELLITE

In certain areas where broadband connection is not yet offered, a satellite Internet option may be available. Similar to wireless access, satellite connection utilizes a modem.

8. ISDN

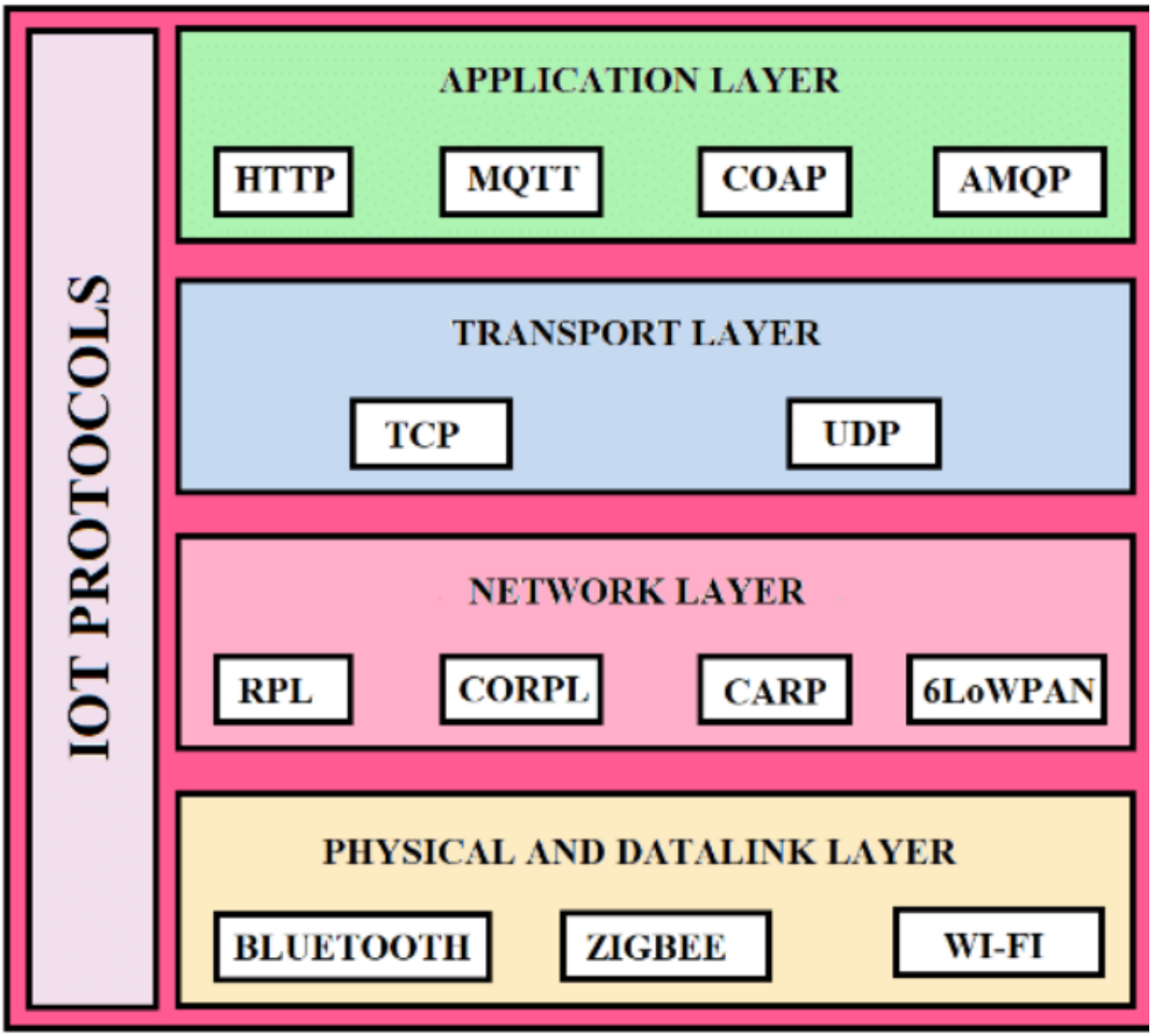
ISDN (Integrated Services Digital Network) allows users to send data, voice and video content over digital telephone lines or standard telephone wires. The installation of an ISDN adapter is required at both ends of the transmission—on the part of the user as well as the Internet access provider.

There are quite a few other Internet connection options available, including T-1 lines, T-3 lines, OC (Optical Carrier) and other DSL technologies. Read more about how new technologies like 5g home internet compares to cable.
As you decide what Internet connection is the best fit for your needs, you may wish to narrow down your selection based on your preferred download and upload speeds, or based on deals and pricing options. Reliably fast speeds and comprehensive coverage make it easier than ever to stream your favorite TV shows and movies, share photos, chat with friends and play games online.

IoT Protocols

IoT devices communicate using IoT protocols. Internet protocol (IP) is a set of rules that dictates how data gets sent to the internet. IoT protocols ensure that information from one device or sensor gets read and understood by another device, a gateway, a service. Different IoT protocols have been designed and optimized for different scenarios and usage. Given the diverse array of IoT devices available, using the right protocol in the right context is important.

Fig showing the different protocol support with all OSI Model



Besides HTTP, other protocols that are optimal and suitable for communication in IoT are Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), WebSocket, Extensible Messaging and Presence Protocol (XMPP), and Advanced Message Queuing Protocol (AMQP).

REST connectivity over the internet is used as the communication architecture for the IoT devices. Typically, the IoT devices are resource constrained, and there may be data loss or a high memory requirement in this type of communication. Alternatively, a few protocols that are effective are MQTT, CoAP, XMPP, WebSocket, and AMQP.

Name	Description	Security	Use Case
MQTT	Simple and lightweight IoT protocol designed for constrained devices and low network bandwidth. See mqtt.org.	In an MQTT packet, you can pass an user name and password, but it doesn't support additional security. You can use SSL in the network for encryption, independent from the MQTT protocol.	Small medical devices with limited network connectivity, mobile apps in mobile devices, sensors in remote locations that communicate with a gateway.
CoAP	Protocol based on the REST model and is suitable for constrained devices such as a microcontroller or a constrained network because it functions with minimum resources in the device or the network.	CoAP applies datagram transport layer security (DTLS) that's equivalent to 3072-bit RSA keys.	Smart energy applications and building automation applications.
WebSocket	A full-duplex communication channel over a TCP connection.	WebSocket protocol defines a `ws://` and `wss://` prefixes indicate a WebSocket and a WebSocket secure connection, respectively.	Implement WebSocket in runtime environments or libraries that act as servers or clients. You can apply WebSockets in an IoT network where chunks of data are transmitted continuously within multiple devices.
XMPP	Uses the XML text format for communication and runs over TCP. It's not fast and uses polling to check for updates when needed. See https://xmpp.org	XMPP uses a security mechanism based on Transport Layer Security (TLS) and Simple Authentication and Security Layer (SASL).	Use XMPP to connect your home thermostat to a web server so that you can access it from your phone. It's used in consumer-oriented IoT applications.
AMQP	The message queue asynchronous protocol is for communication of transactional messages between servers. See https://www.amqp.org/	AMQP provides TLS/SSL and SASL for security.	AMQP is best used in sever-based analytical functions. It's effectively used in the banking industry.