UNIT IV

IOT TECHNOLOGIES, STANDARDS, TOOLS & M2M NETWORK

SYLLABUS

- Fundamental characteristics and high level requirements of IoT, IoT Reference models; Introduction to Communication Technologies & Protocols of IoT: BLE, Wi-Fi, LoRA, 3G/4G Technologies and HTTP, MQTT, CoAP protocols; Relevant Practicals on above technologies, M2M Network, SDN (Software Defined Networking) & NFV (Network Function Virtualization) for IoT .

Internet of Things

- **Internet of Things** refers to the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and network connectivity, allowing them to collect and exchange data.
- The IoT enables these devices to interact with each other and with the environment and enables the creation of smart systems and services.

Internet of Things

- IoT development involves a wide range of technologies, including wireless communication protocols, cloud computing, big data analytics, machine learning, and security technologies.
- IoT can be used to build applications for agriculture, assets tracking, energy sector, safety and security sector, defense, embedded applications, education, waste management, healthcare product, telemedicine, smart city applications, etc.

- Connectivity
- Intelligence and identity
- Scalability
- Dynamic and self adapting
- Architecture
- Safety
- Self configuring
- Automation and control

Characteristics of the Internet of Things

1. Connectivity

Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times.

For example, the connection between people through Internet devices like mobile phones, and other gadgets, also a connection between Internet devices such as routers, gateways, sensors, etc.

2. Intelligence and Identity

- The extraction of knowledge from the generated data is very important.
- For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

3. Scalability

- The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

4. Dynamic and Self-Adapting (Complexity)

- IoT devices should dynamically adapt themselves to changing contexts and scenarios.
- Assume a camera meant for surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, and night).

5. Architecture

- IoT Architecture cannot be homogeneous in nature.
- It should be hybrid, supporting different manufacturers ' products to function in the IoT network.
- IoT is not owned by anyone engineering branch.
- IoT is a reality when multiple domains come together.

6. Safety

- There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet.
- This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge.
- IoT networks may also be at risk. Therefore, equipment safety is also critical.

7. Self Configuring

- This is one of the most important characteristics of IoT.
- IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation.
- Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

Automation & Control:

- IoT enables autonomous operation, allowing devices to act without human intervention, such as automated lighting or industrial maintenance.

High-Level Requirements of IoT

- **Security & Privacy:** Robust encryption, authentication, and firewalls are critical to protect data and prevent unauthorized access.
- **Interoperable Communication Protocols:** Devices must communicate seamlessly across different platforms and networks using standardized protocols (e.g., MQTT, CoAP).
- **Energy Efficiency:** Many IoT devices are battery-operated, necessitating low-power consumption and efficient communication protocols (e.g., BLE, LoRaWAN).

High-Level Requirements of IoT

- **Data Management & Processing:** High-volume data requires efficient, secure storage (cloud/edge) and real-time processing capabilities.
- **Reliable Infrastructure:** Constant network availability is crucial for functional, uninterrupted IoT operations.
- **Architecture Hybridization:** The system architecture must be flexible enough to allow different manufacturers' products to coexist and function together.

Layers of IoT Reference Architecture

- IoT reference architectures typically consist of multiple layers that work together to enable the functioning of an IoT system.
- **Perception Layer:** This layer comprises the physical devices or sensors that collect data from the environment or interact with the physical world. These devices can include temperature sensors, motion detectors, cameras, and other IoT enabled devices.

Layers of IoT Reference Architecture

- **Network Layer:** The network layer facilitates the connectivity and communication between the IoT devices and the cloud or other data processing components. It includes protocols, gateways, routers, and other networking infrastructure to ensure seamless data transfer and reliable connections.
- **Data Processing Layer:** This layer involves processing and analyzing the data collected from IoT devices. It may include edge computing devices or cloud based platforms where data is aggregated, filtered, transformed, and analyzed to derive valuable insights.

Layers of IoT Reference Architecture

- **Application Layer:** The application layer encompasses the software applications or services that utilize the processed IoT data to provide specific functionalities or address specific use cases. These applications can range from realtime monitoring and control systems to predictive analytics, machine learning algorithms, and automation

Benefits of Using IoT Reference Architecture

- **Common Framework:** IoT reference architecture provides a standardized framework for designing and implementing IoT solutions, ensuring consistency and interoperability across systems.
- **Security and Scalability:** The architecture serves as a foundation for implementing robust security and scalability measures, safeguarding IoT systems against threats and enabling future growth.
- **Cost Efficiency:** By leveraging a reference architecture, organizations can avoid reinventing the wheel and utilize existing technologies and expertise, reducing the cost of development and deployment.

Benefits of Using IoT Reference Architecture

- **Faster Time to Market:** Utilizing a reference architecture accelerates the implementation of IoT solutions, enabling organizations to get their systems up and running more quickly and efficiently.

Types of Communications in IOT

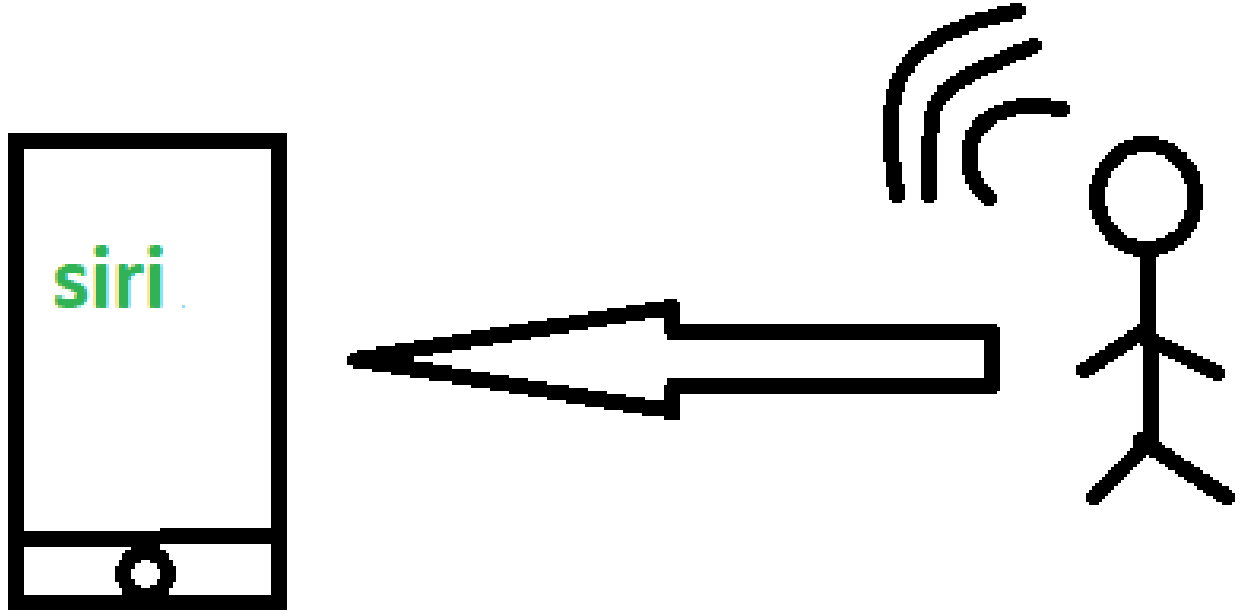
- **IoT Communication:** IoT is the connection of devices over the internet, where these smart devices communicate with each other , exchange data , perform some tasks without any human involvement. These devices are embedded with electronics, software, network and sensors which help in communication. Communication between smart devices is very important in IOT as it enables these devices to gather, exchange data which contribute in success of that IOT product/project.

Types of Communications in IOT

- **1. Human to Machine (H2M):**

In this human gives input to IOT device i.e as speech/text/image etc. IOT device (Machine) like sensors and actuators then understands input, analyses it and responds back to human by means of text or Visual Display.

This is very useful as these machines assist humans in every everyday tasks. It is a combo of software and hardware that includes human interaction with a machine to perform a task.



Merits: This **H2M** has a user-friendly interface that can be quickly accessed by following the instructions. It responds more quickly to any fault or failure. Its features and functions can be customized.

Examples:

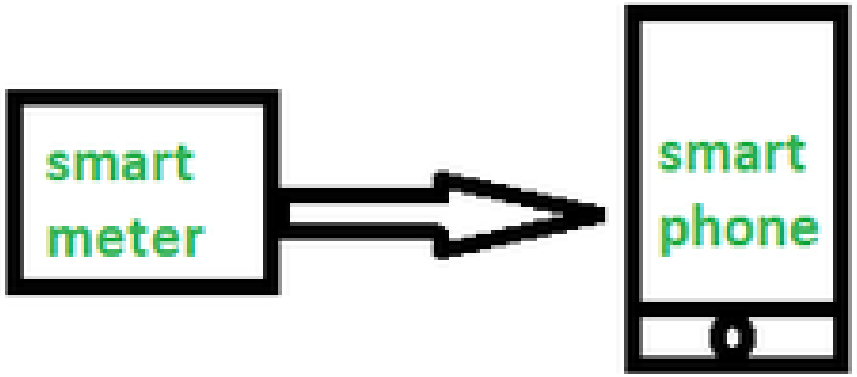
- Facial recognition.
- Bio-metric Attendance system.
- Speech or voice recognition.

2. Machine to Machine (M2M):

- The process of exchanging information or messages between two or more machines or devices is known as Machine to Machine (M2M) communication.
- It is the communication among the physical things which do not need human intervention.
- M2M communication is also named as Machine Type communication in 3GPP(3rd Generation Partnership Project). In this the interaction or communication takes place between machines by automating data/programs. In this machine level instructions are required for communication.

2. Machine to Machine (M2M):

- Here communication takes place without human interaction. The machines may be either connected through wires or by wireless connection.
- An M2M connection is a point-to-point connection between two network devices that helps in transmitting information using public networking technologies like Ethernet and cellular networks.
- IoT uses the basic concepts of M2M and expands by creating large “cloud” networks of devices that communicate with one another through cloud networking platforms.



Advantages -

This M2M can operate over cellular networks and is simple to manage. It can be used both indoors and outdoors and aids in the communication of smart objects without the need for human interaction. The M2M contact facility is used to address security and privacy problems in IoT networks. Large-scale data collection, processing, and security are all feasible.

Machine to Machine (M2M):

- **Disadvantages** -

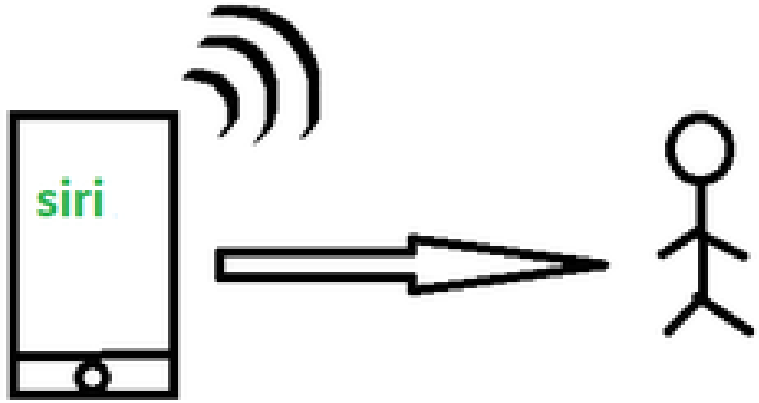
  However, in M2M, use of cloud computing restricts versatility and creativity. Data security and ownership are major concerns here. The challenge of achieving interoperability between cloud/M2M IoT systems is daunting. M2M connectivity necessitates the existence of a reliable internet connection.

Examples:

- Smart Washing machine sends alerts to the owners' smart devices after completion of washing or drying of clothes.
- Smart meters tracks amount of energy used in household or in companies and automatically alert the owner.

3. Machine to Human (M2H) :

- In this machine interacts with Humans. Machine triggers information(text messages/images/voice/signals) respective / irrespective of any human presence. This type of communication is most commonly used where machines guide humans in their daily life. It is way of interaction in which humans co-work with smart systems and other machines by using tools or devices to finish a task.



Examples:

- Fire Alarms
- Traffic Light
- Fitness bands
- Health monitoring devices

4. Human to Human (H2H) :

- This is generally how humans communicate with each other to exchange information by speech, writing, drawing, facial expressions, body language etc. Without H2H, M2M applications cannot produce the expected benefits unless humans can immediately fix issues, solve challenges, and manage scenarios.
- The process of exchanging information or messages between two or more people is known as human to human (H2H) communication. This can be done through various means such as verbal, non-verbal, or written communication.

IoT communication technologies and protocols

- It enable connected devices to exchange data efficiently over networks, ranging from short-range sensors to long-distance, low-power applications.

IOT Communication Technologies (**Physical/Link Layers**):

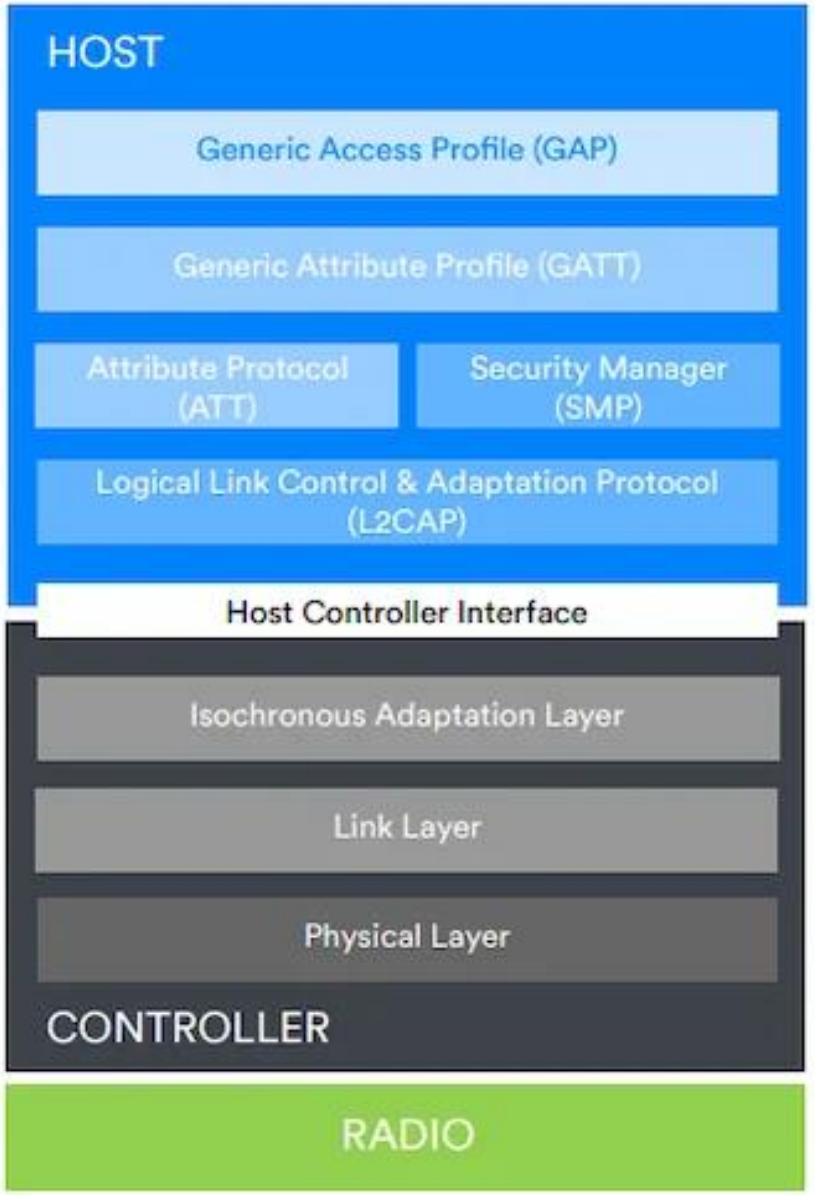
- These technologies define how devices physically connect to a network. BLE, Wi-Fi, LoRA, 3G/4G Technologies.

IoT Communication Protocols (**Network/Application Layers**)

- These protocols define the rules for data exchange.

IOT Communication Technologies (Physical/Link Layers):

- **BLE** designed for **ultra-low power applications**. short-range connectivity technology that uses radio waves as a communication medium.
- The first standard or specification for this technology is called **Bluetooth Classic**.
- It was primarily designed to replace wires and provide wireless connectivity between mobile phones and other portable devices.
- Bluetooth employs Radio Frequency (RF) for communication. It makes use of **frequency modulation** to generate radio waves in the **ISM** band.



Two Main Ways BLE-enabled Devices Communicate:

1. Connectionless communication: Broadcasts its data to any listening device.

2. Connection-oriented communication: It forms a dedicated connection with another device and communicates with it using the **client-server mechanism.**

Connectionless Communication: One device has to be the **broadcaster**, and the other device(s) has to be the **observer(s**)

Step 1: The broadcaster device instructs its link layer to be an advertiser. A link layer that is an advertiser controls the LE radio to move from the stand-by or idle state to the advertising state and vice versa.

Step 2: When the LE radio is in an **advertising state**, the advertiser (link layer) can send out advertising packets on the **three dedicated advertising channels**, RF37, RF38, and RF39. The advertising packets can contain data such as the name and the address of the broadcasting device.

Step 3: On the other hand, the observer(s) instructs its link layer to be a scanner. A link layer that is a scanner controls the LE radio to move from a stand-by state (idle) to the scanning state and vice versa.

Step 4: When the LE radio is in the scanning state, the scanner tunes in and listens for data on the primary advertising channels (RF37, RF38, and RF39).

Connection-oriented Communication Here, you must be clear about two main concepts: device discovery and the client-server relationship between connected devices.

LE devices that want to participate in connection-oriented communication are given two roles defined by the GAP layer. One device has to be central, and the other has to be peripheral.

Step 1: The broadcaster device instructs its link layer to be an advertiser. A link layer that is an advertiser controls the LE radio to move from the stand-by or idle state to the advertising state and vice versa.

Step 2: When the LE radio is in an advertising state, the advertiser (link layer) can send out advertising packets on the three dedicated advertising channels, RF37, RF38, and RF39. The advertising packets can contain data such as the name and the address of the broadcasting device.

Step 3: On the other hand, the observer(s) instructs its link layer to be a scanner. A link layer that is a scanner controls the LE radio to move from a stand-by state (idle) to the scanning state and vice versa.

Step 4: When the LE radio is in the scanning state, the scanner tunes in and listens for data on the primary advertising channels (RF37, RF38, and RF39).

Wi-Fi is a high-speed internet connection and network connection without the use of any cables or wires. The wireless network is operating three essential elements that are radio signals, **antenna**, and router.

Wi-Fi is the acronym for **Wireless Fidelity**. **Wi-Fi technology** is used to achieve connection to the Internet without a direct cable between device and Internet Service Provider. Wi-Fi enabled device and wireless router are required for setting up a Wi-Fi connection. These are some characteristics of wireless Internet connection −

- Range of 100 yards
- Insecure connection
- Throughput of 10-12 Mbps

Types of WiFi Technologies Currently, they are the four major types of WIFI technologies.

- Wi-Fi-802.11a
- Wi-Fi-802.11b
- Wi-Fi-802.11g
- Wi-Fi-802.11n

- **802.11a** is one of a series of wireless technology. That defines the format and structure of the radio signals sent out by WI-FI networking routers and antennas.

- **802.11b** is one of a series of wireless technology. 802. 11b support bandwidth 11mbps. The signal in the unregulated frequency spectrum around 2.4 GHz.

- **Wi-Fi-802.11g**
- It is the best technology of 802.11a and 802.11b. The 802.11 b support bandwidth upto 54mbps and it use a 2.4 GHz frequency for greater range

- **802.11n** is the newest WIFI technology. It was designed to improve on 802.11g. The amount of bandwidth supported by utilizing multiple wireless signals and antennas instead of one. It supports 100 Mbps bandwidth and increased signal intensity.

Limitations of WiFi

The limitations of WiFi include the following.

- Range is limited
- Interference from other devices like microwave ovens, telephones, etc
- Power consumption is high
- Risks of data security.

Applications of WiFi Technology

The applications of WiFi include the following.

- Mobile applications
- Business applications
- Home applications
- Computerized application
- Automotive segment
- Browsing internet
- Video conference

WiMax: To overcome the drawback of **Wi-Fi** connections, **WiMax (Worldwide Interoperability for Microwave Access)** was developed. WiMax is a collection of wireless communication standards based on **IEEE 802.16**. WiMax provides multiple **physical layer** and **media access control** (MAC) options.

WiMax Forum, established in 2001, is the principal body responsible to ensure conformity and interoperability among various commercial vendors. These are some of the characteristics of WiMax −

- Broadband wireless access
- Range of 6 miles
- Multilevel encryption available
- Throughput of 72 Mbps

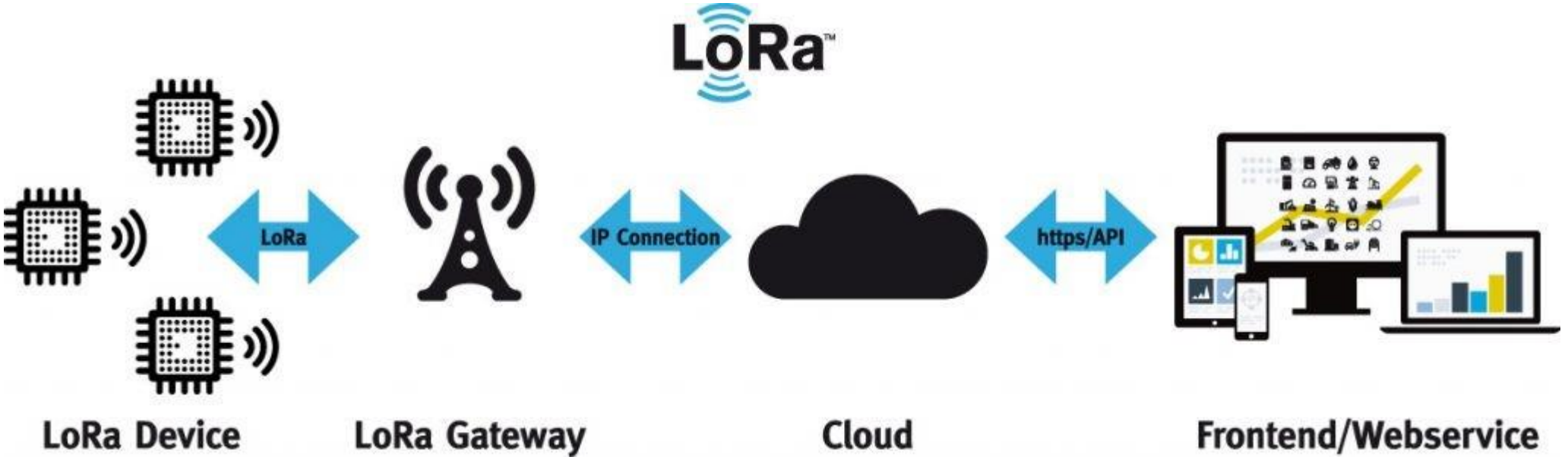
The main components of a WiMax unit are −

- **WiMax Base Station** − It is a tower similar to mobile towers and connected to Internet through high speed wired connection.
- **WiMax Subscriber Unit (SU)** − It is a WiMax version of wireless modem. The only difference is that modem is connected to the Internet through cable connection whereas WiMax SU receives Internet connection wirelessly through microwaves.

LoRA

Long distance, low power consumption, large number of connections and other characteristics, it has been widely used in the field of Internet of Things.

- **Principle: It** is a spread spectrum modulation technology, and its basic principle is to **convert information data into spread spectrum signals** for transmission through spread spectrum coding.
- Spread spectrum modulation is a technique for spreading the spectrum of information data by widening the bandwidth of the information data, The resistance of the signal to noise and interference in the transmission process is enhanced.

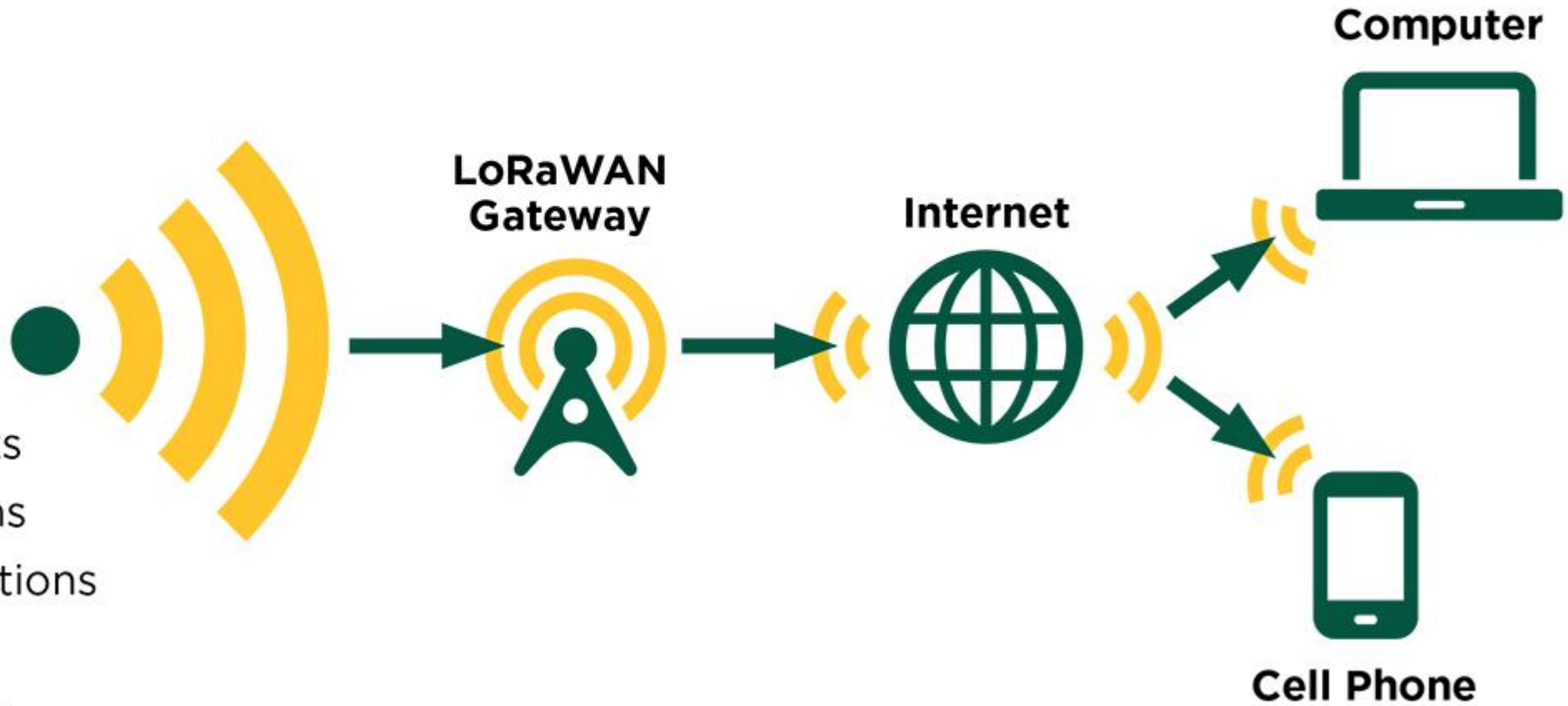


LoRaWAN Wireless Technology

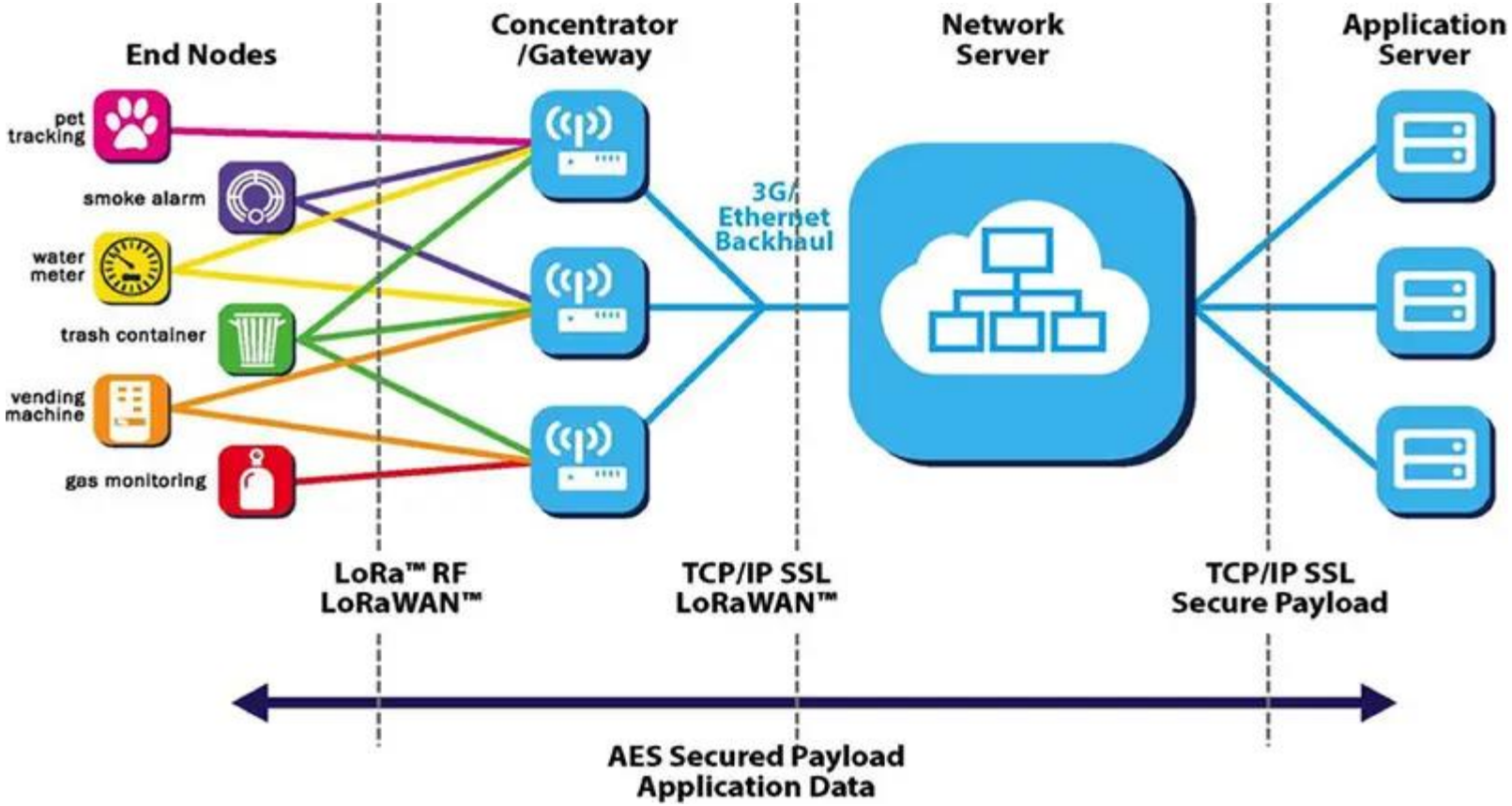
Nodes

LoRaWAN (Long Range Wide Area network)

Air temperature
Relative humidity
Soil moisture
Rainfall
Wind speed
Wind direction
CO_2 emissions
Liquid level in tanks
Machinery locations
Stored grain conditions
Building security
Livestock locations



It consists of LoRa nodes, LoRa gateways, the network server and the application server. In a LoRaWAN architecture, the nodes are typically in a star topology with gateways forming a transparent bridge. Communication to end nodes is generally bidirectional, which means the gateway can collect data from the end nodes, but it can also send commands to the end nodes.



LoRa nodes: The end nodes are the elements of the LoRa network where the control or sensing is undertaken. They are normally battery-powered and remotely located. End nodes send data to every gateway in their vicinity and they transmit data in periodic not 24×7.

LoRa gateway: The gateway receives the data from the LoRa end nodes and then channels it to a network server. A LoRa gateway usually consists of a LoRa radio module, a microprocessor, and an Internet connectivity medium.
The gateway converts the data received from the LoRa nodes into TCP/IP format via the backhaul network (Ethernet, 3G, 4G, WiFi, etc.) and sends it to the network server. LoRa gateway supports multi-channel, multi-modulation transceivers, and even simultaneous demodulation of signals on the same channel. They **do not store any data and act only as packet forwarders to the network** server.

Network Server: The network server manages the network. It filters duplicate packets caused by multiple gateways receiving the same data, performs security checks, manages gateway traffic and routing, control adaptive rate, and forwards messages to the application server.

Application Server: The application server processes data from the network server, analyzes sensor data, supports functions like status display and real-time alerts, and can optionally send responses back to the end node.

Benefits and disadvantages of LoRa technology

•**Long range:** Connects devices up to 15-20 km in rural settings and 2-5 km in urban areas. Permits city-scale coverage, and good penetration of buildings is achieved.

•**Low power and long lifespan:** Designed for low power use with prolonged battery life up to 10 years. For example, MOKOSmart LW009 LoRaWAN Parking Sensor can operate up to 5 years.

•**High capacity:** A single LoRa gateway can handle millions of messages from thousands of end nodes.

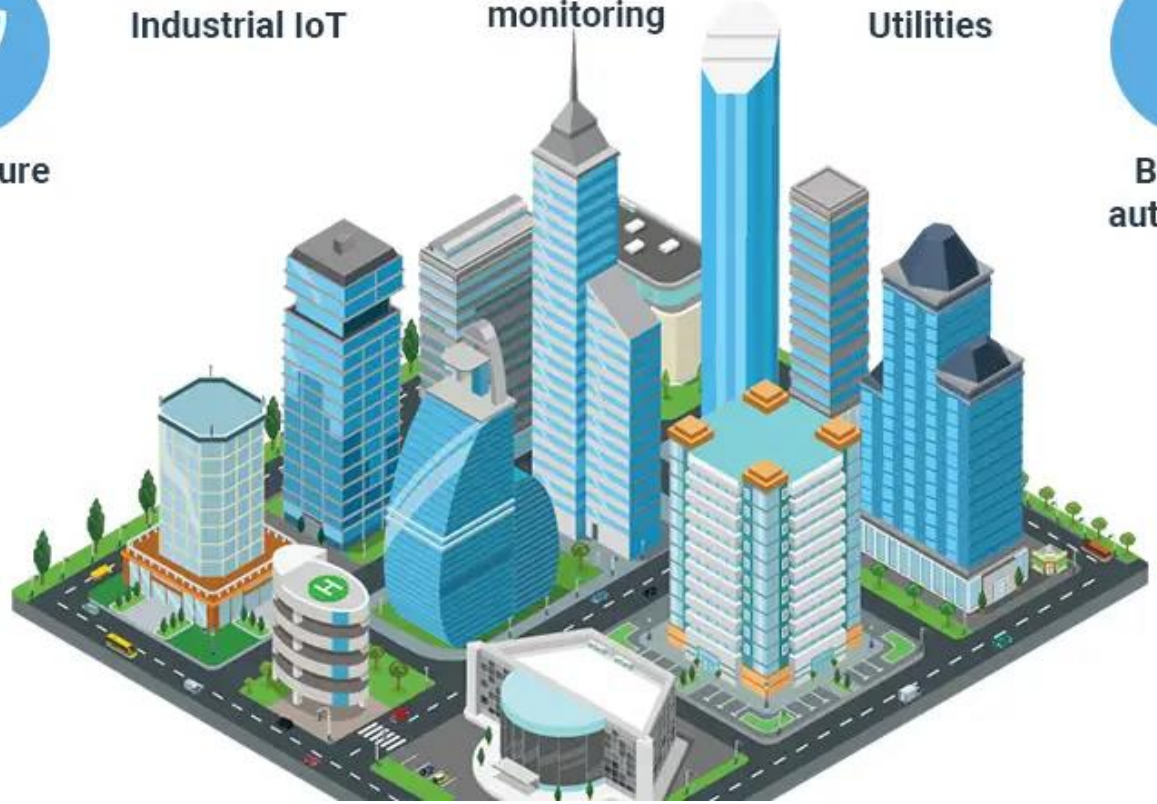
•**Low cost:** Low initial infrastructure investment

Disadvantages of LoRa:

Low transmission speed: LoRa has a relatively narrow bandwidth and its ability to transmit over long distances comes at the cost of lower data rates, making it suitable for sensor networks not high-data applications.

Limited payload: LoRa supports only small data packets, with a maximum data capacity of about 242 bytes per transmission. This makes it less suitable for use cases that need large data transfers.

Applications of LoRa technology



Industrial IoT

Infrastructure monitoring

Utilities

Agriculture

Building automation

Supply chain/ logistics

Healthcare

Smart cities

Retail

3G/4G Technologies

Mobile communication enables you to talk to people who are far away from you without having to be connected physically. It becomes possible to transfer audio and multimedia files between mobiles and computers without the need for any physical connection. A cell phone or a mobile phone is one form of mobile communication.

3G/4G Technologies

Specifications	3G	4G
Full form	Third Generation	Fourth Generation
Switching	Circuit and Packet Switching	All digital with packetized voice
RF Frequency Band	About 1.8 to 2.5GHz	About 2-8 GHz
RF Bandwidth	5-20 MHz	100 MHz and more.
Data rate	384 kbps- 2 Mbps	20-100Mbps in mobile
Applications	Mainly Voice along with data	Converged Data and VOIP
Technologies supported	EGDE, EGPRS, WCDMA, HSPA, HSPA+, CDMA2000	Mobile WiMAX, LTE, LTE-Advanced
Network architecture	Wide area cell based	Integration of wireless LAN and Wide Area Network
Forward Error Correction	turbo codes	Concatenated codes
Video Access	Provides video access to users	Provides HD video access to users
Virtual presence	Not available	It is possible
Navigation	Digital navigation provided	Virtual navigation provided

•**Speed:** 4G offers significantly faster data speeds compared to 3G. This makes it ideal for streaming HD video, online gaming, and other data-intensive applications. Think about downloading a large file on your phone – it will be much faster on 4G.

•**Technology:** 3G uses a combination of circuit and packet switching, while 4G utilizes an all-digital, packet-switched network. This allows for more efficient data transfer and improved performance.

•**Applications:** While 3G focused on voice calls and basic data services, 4G is designed for converged data and VoIP (Voice over Internet Protocol) technologies. This means 4G is better suited for services like video conferencing and online collaboration.

•**Video Access:** 4G networks allow for High Definition video access whereas 3G provides standard video access to the users.

•**Virtual Presence:** 4G technology makes virtual presence possible, a feature unavailable in 3G networks.

•**Bandwidth:** 4G networks support much wider bandwidth than 3G networks

HTTP (Hypertext Transfer Protocol) is a set of rules that govern how information will be transferred between networked devices, specifically web servers and client browsers.

HTTP is an application layer protocol whose older versions (prior to HTTP/3) ran on top of the TCP/IP (transmission control protocol/internet protocol) suite of protocols. HTTP, TCP and IP form the foundation of the modern-day internet.

information requested by the browser may include many kinds of files or resources, such as text, images, sound, video and other multimedia files, all of which are transferred by HTTP over the web and displayed in the user's web browser. HTTP facilitates communications between web browsers and web servers in a standardized way, thus providing the foundation for information exchange on the world wide web.

Method

Developers often implement RESTful APIs by using the **Hypertext Transfer Protocol (HTTP).** An HTTP method tells the server what it needs to do to the resource. The following are four common HTTP methods:

Clients use **GET** to access resources that are located at the specified URL on the server. They can cache GET requests and send parameters in the RESTful API request to instruct the server to filter data before sending.

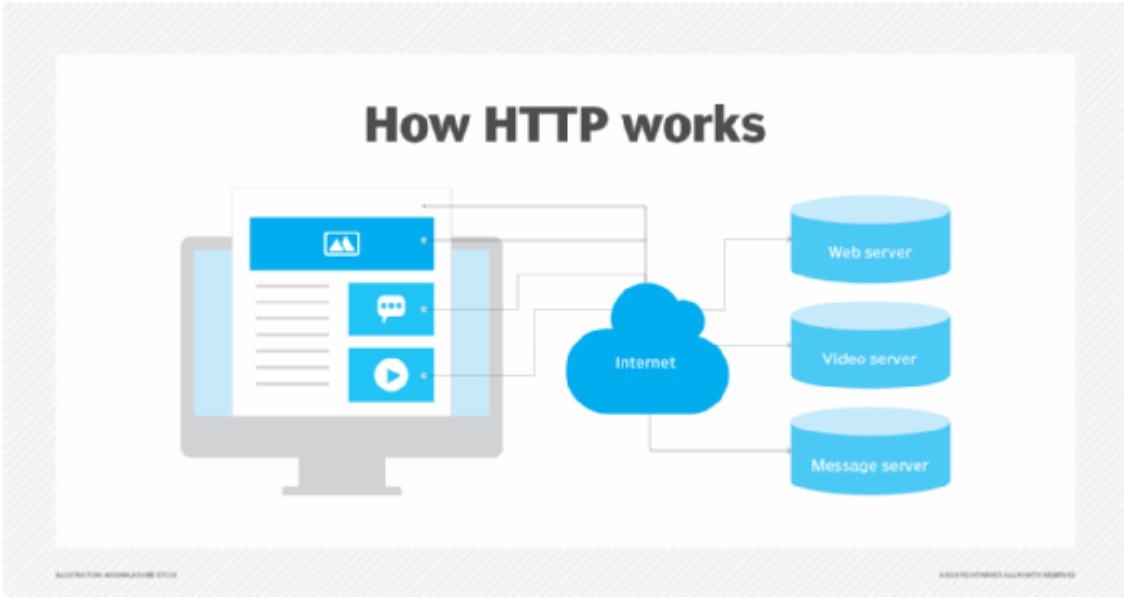
Clients use **POST** to send data to the server. They include the data representation with the request. Sending the same POST request multiple times has the side effect of creating the same resource multiple times.

Clients use **PUT** to update existing resources on the server. Unlike POST, sending the same PUT request multiple times in a RESTful web service gives the same result.

Clients use the **DELETE** request to remove the resource. A DELETE request can change the server state. However, if the user does not have appropriate authentication, the request fails.

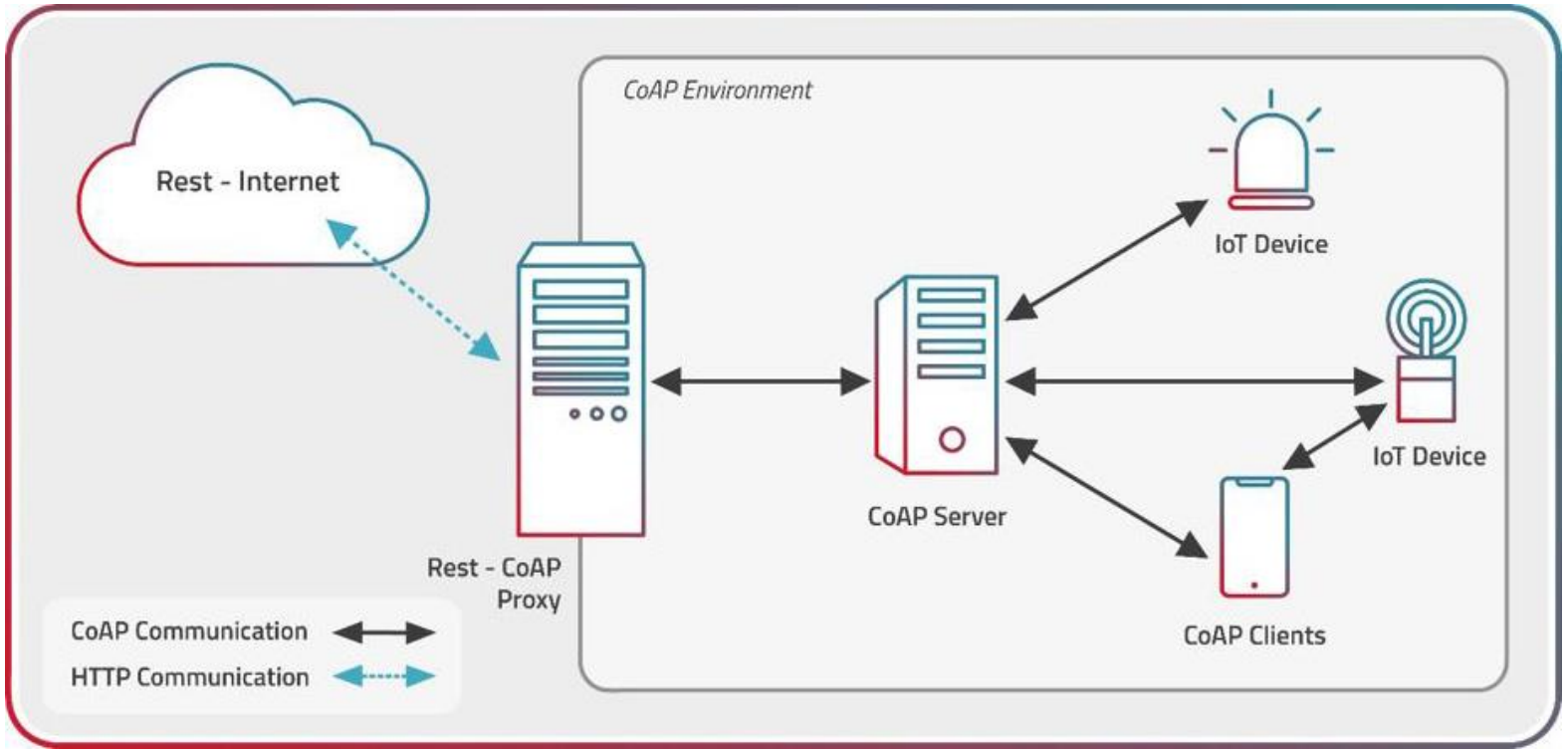
HTTP headers: Request headers are the metadata exchanged between the client and server. For instance, the request header indicates the format of the request and response, provides information about request status, and so on.

Data: REST API requests might include data for the POST, PUT, and other HTTP methods to work successfully.


How HTTP works
Internet
Web server
Video server
Message server

Constrained Application Protocol

- Internet Engineering Task Force in the year 2014
  - It created for limited devices, like sensors.



- CoAP allows devices like sensors and actuators to communicate across the Internet of Things by acting as a sort of HTTP for limited devices.

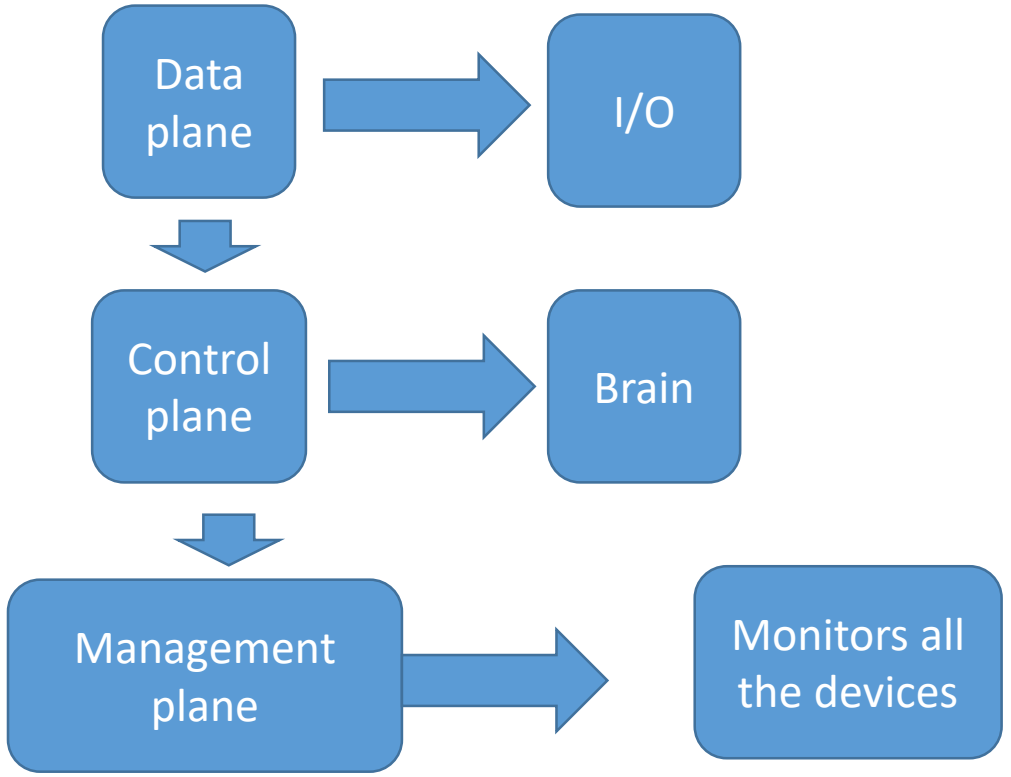
- The protocol's low power consumption and little network overhead are designed to ensure resilience in situations with limited bandwidth and high congestion. **CoAP can function on a network** where TCP-based protocols, like MQTT, are unable to share data and interact efficiently because of high congestion or poor connectivity.

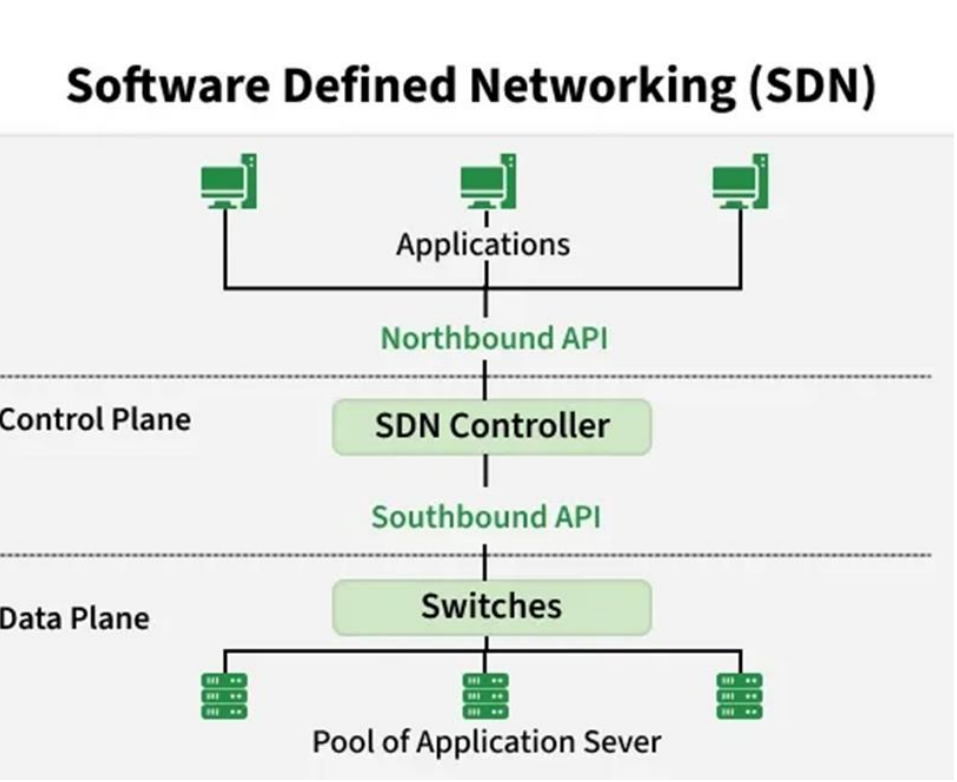
- Furthermore, devices working in **low signal quality** may communicate data consistently, and an orbiting satellite can successfully sustain its distant communication. Moreover, billion-node networks are supported by CoAPs. The DTLS parameters that are used by default are similar to 128 bit RSA keys in terms of security.

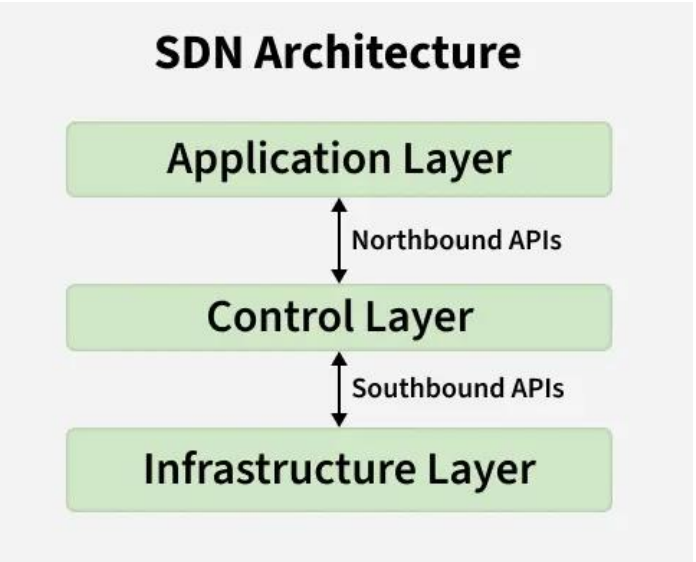
- UDP is the fundamental network protocol used by CoAP. In simple terms, CoAP is a **client-server Internet of Things protocol**, like HTTP, in which a request is made by the client and a response is sent by the server. HTTP and CoAP both use the same techniques.

Software defined network is a network management approach that utilizes software-based controllers to dynamically and centrally control network behavior, enhancing flexibility, performance, and monitoring capabilities.

1. It separates the control plane (decision-making) from the data plane (packet forwarding).
2. Network intelligence is centralized in an SDN controller instead of being distributed across devices.
3. Network devices like switches become simple forwarding elements that follow controller instructions.
4. It enables programmability and automation, making networks easier to manage and adapt.







Organized into three logical layers, each with a specific role. This layered design simplifies network management and enables centralized control.

Application Layer

•Contains network applications such as traffic management, security, and monitoring tools.
•Allows administrators to define network policies and requirements.
•Communicates with the SDN controller through northbound APIs.

2. Control Layer

•Hosts the SDN controller, which acts as the brain of the network.
•Translates application requirements into forwarding rules.
•Maintains a global view of the network and makes routing decisions.

3. Infrastructure Layer (Data Plane)

•Consists of physical or virtual switches and routers.
•Forwards packets based on rules received from the controller.
•Does not make independent decisions, ensuring simple and efficient forwarding.

1. Northbound APIs

- Northbound APIs allow communication between the Application Layer and the SDN Controller.

- They enable network applications to define high-level policies, such as routing, load balancing, and security rules, without dealing with low-level network details.

- These APIs simplify network management and support automation

Example: **REST APIs** are commonly used as northbound interfaces to allow applications to interact with the SDN controller using standard web-based methods.

2. Southbound APIs

- Southbound APIs enable communication between the SDN Controller and the Infrastructure Layer (switches and routers).

- They allow the controller to install forwarding rules and manage packet flow in the data plane.

- Through southbound APIs, network devices follow instructions from the centralized controller instead of making independent decisions.

Example: **OpenFlow** is a widely used southbound protocol that allows the SDN controller to directly program flow tables in switches.

Benefits : Flexibility, Scalability, Automation and network programmability

Process of Virtualizing Network Functions?

Network Functions Virtualization (NFV) runs as software and relies on general-purpose computing resources, like those found in servers and switches, in contrast to dedicated hardware devices like traditional switches, routers, firewalls, and load balancers that perform these network functions. Such base network functionalities are virtualized in software-based network functions (VNFs) that can be deployed on standard servers, storage, and switches.

The Network Functions Virt

Virtualization layer:

Virtual network functions

NFV infrastructure (NFVI

Management and orchestration (MANO)