Contents

Communication Technologies in IoT

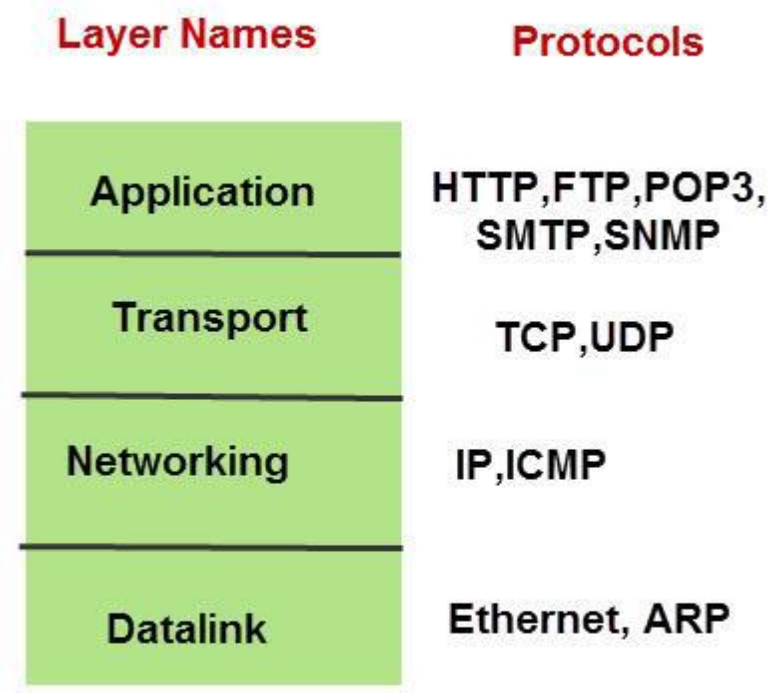
Communication technology, also known as information technology, refers to all equipment and programs that are used to process and communicate information.

Perhaps to understand how all these communication technologies fit together, we need to start of from a familiar communication technology that we all understand, which is the TCP/IP protocol.

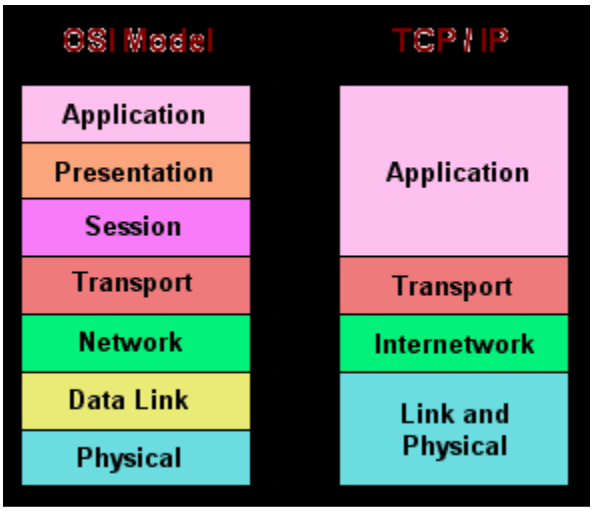
Transmission Control Protocol/Internet Protocol (TCP/IP) is the language a computer uses to access the internet. It consists of a suite of protocols designed to establish a network of networks to provide a host with access to the internet.

TCP/IP is responsible for full-fledged data connectivity and transmitting the data end to end by providing other functions, including addressing, mapping and acknowledgment. TCP/IP contains four layers, which differ slightly from the OSI model.

The technology is so common that one would rarely use the full name. In other words, in common usage the acronym is now the term itself.



TCP/IP Networking Model



Link layer: This layer is also known as the network access layer and is the equivalent of both the physical and data link layers of the OSI model. It deals with components such as cables, connectors, and network cards, like OSI Layer 1. Like Layer 2 of the OSI model, the link layer of the TCP/IP model is concerned with hardware addresses.

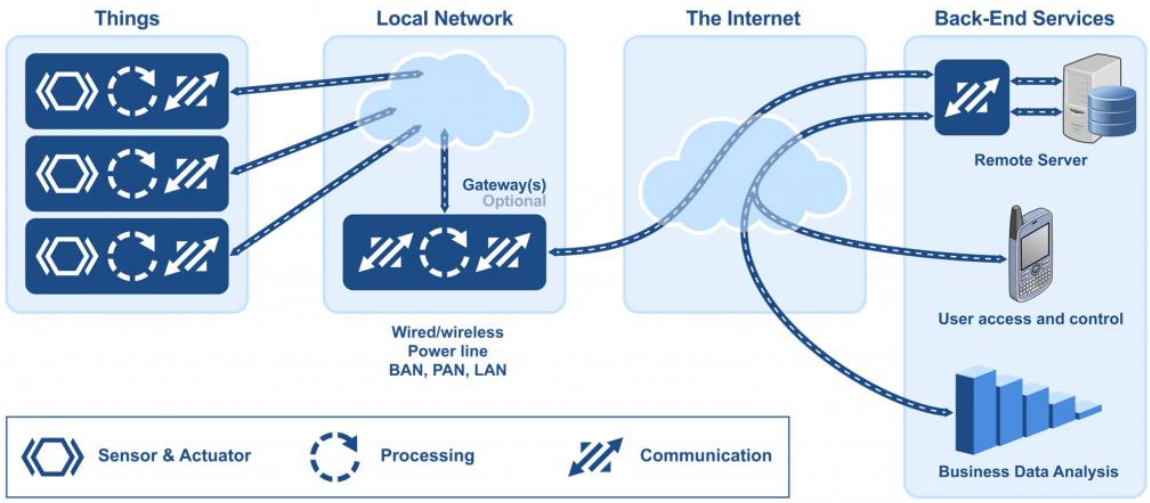
Internet layer: This layer aligns directly with Layer 3 of the OSI model. You may also know this layer as the network layer. It routes data from the source to the destination by defining the packet and the addressing scheme, moving data between the link and transport layers, routing packets of data to remote hosts, and performing fragmentation and reassembly of data packets. The Internet layer is where IP operates.

Transport layer: This layer is directly aligned with Layer 4 of the OSI model: It is the core of the TCP/IP architecture. It is the layer where TCP and UDP operate. This layer provides communication services directly to the application processes that are running on network hosts.

Application layer: This layer corresponds to Layers 5, 6, and 7 of the OSI model. It provides applications for file transfer, network troubleshooting, and Internet activities. It also supports network APIs, which allow programs that have been created for a particular operating system to access the network. An application layer protocol defines how application processes (clients and servers) running on different end systems pass messages to each other

- The types of messages e.g. request messages and response messages
- The syntax of the various message types i.e. the fields in the messages
- The semantics of the field i.e. the meaning of the information that the field is supposed to contain.
- Rules determining when and how a process sends messages and responds to messages.

Let’s take a look at an IoT system to get a clear picture of where communication fits



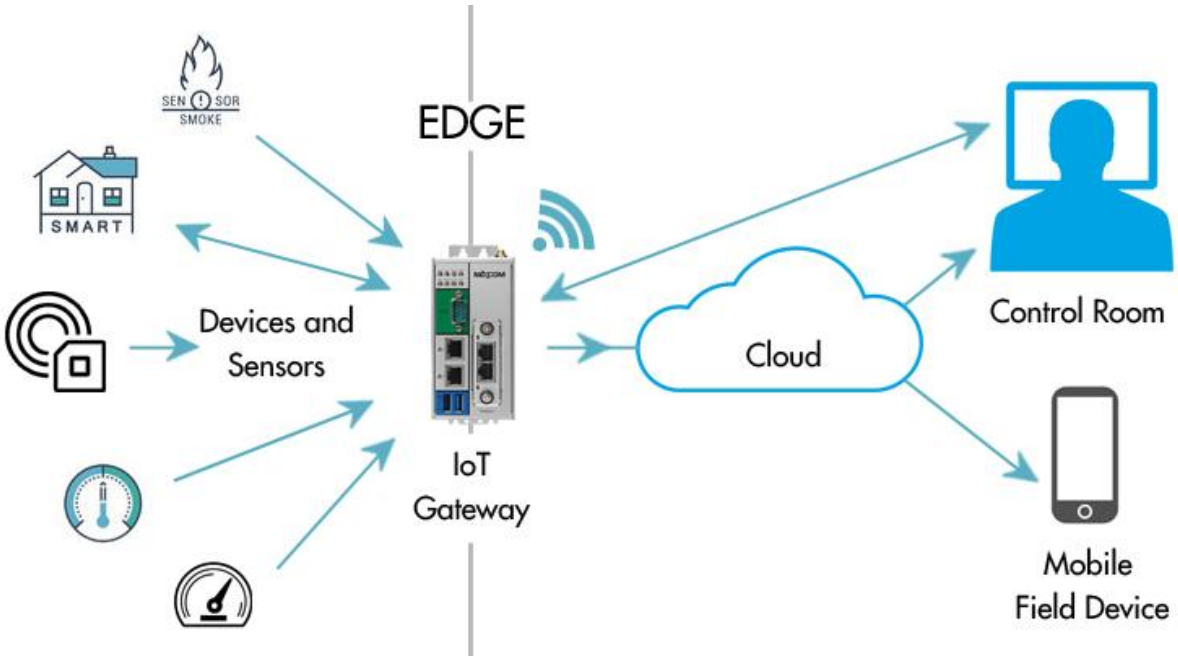
- The Thing itself (the device)
- The Local Network; this can include a gateway, which translates proprietary communication protocols to Internet Protocol
- The Internet
- Back-End Services; enterprise data systems, or PCs and mobile devices

The Gateway

An Internet of Things (IoT) gateway is a physical device or software program that serves as the connection point between the cloud and controllers, sensors and intelligent devices. All data moving to the cloud, or vice versa, goes through the gateway, which can be either a dedicated hardware appliance or software program. An IoT gateway may also be referred to as an intelligent gateway or a control tier.

Some sensors generate tens of thousands of data points per second. A gateway provides a place to preprocess that data locally at the edge before sending it on to the cloud. When data is aggregated, summarized and tactically analyzed at the edge, it minimizes the volume of data that needs to be forwarded on to the cloud, which can have a big impact on response times and network transmission costs.

Another benefit of an IoT gateway is that it can provide additional security for the IoT network and the data it transports. Because the gateway manages information moving in both directions, it can protect data moving to the cloud from leaks and IoT devices from being compromised by malicious outside attacks with features such as tamper detection, encryption, hardware random number generators and crypto engines.



A *gateway* manages traffic between networks that use different protocols. A gateway is responsible for protocol translation and other interoperability tasks. An IoT gateway device is sometimes employed to provide the connection and translation between devices and the cloud. Because some devices don't contain the network stack required for Internet connectivity, a gateway device acts as a proxy, receiving data from devices and packaging it for transmission over TCP/IP.

A dedicated gateway device might be a requirement if devices in the deployment:

- Don’t have routable connectivity to the Internet, for example, Bluetooth devices.
- Don’t have processing capability needed for transport-layer security (TLS).
- Don't have the electrical power to perform required network transmission.

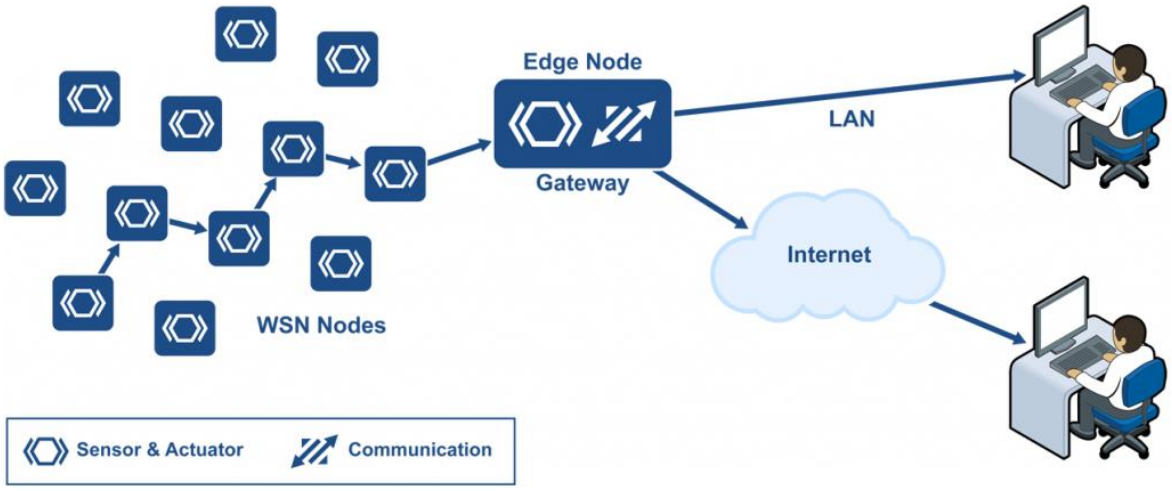
A gateway device might be used even when the participating devices are capable of communicating without one. In this scenario, the gateway adds value because it provides processing of the data across multiple devices before it is sent to the cloud. In that case, the direct inputs would be other devices, not individual sensors. The following tasks would likely be relegated to a gateway device:

- Condensing data to maximize the amount that can be sent to the cloud over a single link
- Storing data in a local database, and then forwarding it on when the connection to cloud is intermittent
- Providing a real-time clock, with a battery backup, used to provide a consistent timestamp for devices that can't manage timestamps well or keep them well synchronized
- Performing IPV6 to IPV4 translation
- Ingesting and uploading other flat-file-based data from the local network that is relevant and associated with the IoT data
- Acting as a local cache for firmware updates

The Local Network

Your choice of communication technology directly affects your device's hardware requirements and costs. Which networking technology is the best choice? IoT devices are deployed in so many different ways — in clothing, houses, buildings, campuses, factories, and even in your body — that no single networking technology can fit all bills.

Let's take a factory as a typical case for an IoT system. A factory would need a large number of connected sensors and actuators scattered over a wide area, and a wireless technology would be the best fit.



Wireless sensor network installed in a factory, connected to the Internet via a gateway

A *wireless sensor network* (WSN) is a collection of distributed sensors that monitor physical or environmental conditions, such as temperature, sound, and pressure. Data from each sensor passes through the network node-to-node.

WSN Nodes

WSN nodes are low cost devices, so they can be deployed in high volume. They also operate at low power so that they can run on battery, or even use *energy harvesting*. A WSN node is an embedded system that typically performs a single function (such as measuring temperature or pressure, or turning on a light or a motor).

Energy harvesting is a new technology that derives energy from external sources (for example, solar power, thermal energy, wind energy, electromagnetic radiation, kinetic energy, and more). The energy is captured and stored for use by small, low-power wireless autonomous devices, like the nodes on a WSN.

WSN Edge Nodes

A WSN edge node is a WSN node that includes Internet Protocol connectivity. It acts as a gateway between the WSN and the IP network. It can also perform local processing, provide local storage, and can have a user interface.

Link Layer Communication

Bluetooth

An important short-range communications technology is of course Bluetooth, which has become very important in computing and many consumer product markets. It is expected to be key for wearable products in particular, again connecting to the IoT albeit probably via a smartphone in many cases. The new Bluetooth Low-Energy (BLE) – or Bluetooth Smart, as it is now branded – is a significant protocol for IoT applications. Importantly, while it offers similar range to Bluetooth it has been designed to offer significantly reduced power consumption. However, Smart/BLE is not really designed for file transfer and is more suitable for small chunks of data. It has a major advantage certainly in a more personal device context over many competing technologies given its widespread integration in smartphones and many other mobile devices. According to the Bluetooth SIG, more than 90 percent of Bluetooth-enabled smartphones, including iOS, Android and Windows based models, are expected to be 'Smart Ready' by 2018. Devices that employ Bluetooth Smart features incorporate the Bluetooth Core Specification Version 4.0 (or higher – the latest is version 4.2 announced in late 2014) with a combined basic-data-rate and low-energy core configuration for a RF transceiver, baseband and protocol stack. Importantly, version 4.2 via its Internet Protocol Support Profile will allow Bluetooth Smart sensors to access the Internet directly via 6LoWPAN connectivity (more on this below). This IP connectivity makes it possible to use existing IP infrastructure to manage Bluetooth Smart 'edge' devices. More information on Bluetooth 4.2 is available here and a wide range of Bluetooth modules are available from RS.

- Standard: Bluetooth 4.2 core specification
- Frequency: 2.4GHz (ISM)
- Range: 50-150m (Smart/BLE)
- Data Rates: 1Mbps (Smart/BLE)

Zigbee

ZigBee, like Bluetooth, has a large installed base of operation, although perhaps traditionally more in industrial settings. ZigBee PRO and ZigBee Remote Control (RF4CE), among other available ZigBee profiles, are based on the IEEE802.15.4 protocol, which is an industry-standard wireless networking technology operating at 2.4GHz targeting applications that require relatively infrequent data exchanges at low data-rates over a restricted area and within a 100m range such as in a home or building. ZigBee/RF4CE has some significant advantages in complex systems offering low-power operation, high security, robustness and high scalability with high node counts and is well positioned to take advantage of wireless control and sensor networks in M2M and IoT applications. The latest version of ZigBee is the recently launched 3.0, which is essentially the unification of the various ZigBee wireless standards into a single standard.

- Standard: ZigBee 3.0 based on IEEE802.15.4
- Frequency: 2.4GHz
- Range: 10-100m

- Data Rates: 250kbps

Z-Wave

Z-Wave is a low-power RF communications technology that is primarily designed for home automation for products such as lamp controllers and sensors among many others. Optimized for reliable and low-latency communication of small data packets with data rates up to 100kbit/s, it operates in the sub-1GHz band and is impervious to interference from WiFi and other wireless technologies in the 2.4-GHz range such as Bluetooth or ZigBee. It supports full mesh networks without the need for a coordinator node and is very scalable, enabling control of up to 232 devices. Z-Wave uses a simpler protocol than some others, which can enable faster and simpler development, but the only maker of chips is Sigma Designs compared to multiple sources for other wireless technologies such as ZigBee and others.

- Standard: Z-Wave Alliance ZAD12837 / ITU-T G.9959
- Frequency: 900MHz (ISM)
- Range: 30m
- Data Rates: 9.6/40/100kbit/s

6LowPAN

A key IP (Internet Protocol)-based technology is 6LowPAN (IPv6 Low-power wireless Personal Area Network). Unlike Bluetooth or ZigBee, 6LowPAN is a network protocol that defines encapsulation and header compression mechanisms. The standard has the freedom of frequency band and physical layer and can also be used across multiple communications platforms, including Ethernet, Wi-Fi, 802.15.4 and sub-1GHz ISM. A key attribute is the IPv6 (Internet Protocol version 6) stack, which has been a very important introduction in recent

years to enable the IoT. IPv6 is the successor to IPv4 and offers approximately 5 x 1028addresses for every person in the world, enabling any embedded object or device in the world to have its own unique IP address and connect to the Internet. Especially designed for home or building automation, for example, IPv6 provides a basic transport mechanism to produce complex control systems and to communicate with devices in a cost-effective manner via a low-power wireless network.

Designed to send IPv6 packets over IEEE802.15.4-based networks and implementing open IP standards including TCP, UDP, HTTP, COAP, MQTT, and websockets, the standard offers end-to-end addressable nodes, allowing a router to connect the network to IP. 6LowPAN is a mesh network that is robust, scalable and self-healing. Mesh router devices can route data destined for other devices, while hosts are able to sleep for long periods of time.

- Standard: RFC6282
- Frequency: (adapted and used over a variety of other networking media including Bluetooth Smart (2.4GHz) or ZigBee or low-power RF (sub-1GHz)
- Range: N/A

- Data Rates: N/A

WiFi

WiFi connectivity is often an obvious choice for many developers, especially given the pervasiveness of WiFi within the home environment within LANs. It requires little further explanation except to state the obvious that clearly there is a wide existing infrastructure as well as offering fast data transfer and the ability to handle high quantities of data.
A wireless network uses radio waves to communicate with portable devices, granting them access to other connected devices and to the Internet. Depending on the specific type of wireless network you use, Wi-Fi signals travel in two distinct frequency ranges. The 802.11b and g networks use the 2.4 GHz band, while 802.11a networks use 5 GHz and 802.11n networks broadcast on both frequencies to increase throughput.
Currently, the most common WiFi standard used in homes and many businesses is 802.11n, which offers serious throughput in the range of hundreds of megabit per second, which is fine for file transfers, but may be too power-consuming for many IoT applications.

- Standard: Based on 802.11n (most common usage in homes today)
- Frequencies: 2.4GHz and 5GHz bands
- Range: Approximately 50m
- Data Rates: 600 Mbps maximum, but 150-200Mbps is more typical, depending on channel frequency used and number of antennas (latest 802.11-ac standard should offer 500Mbps to 1Gbps)

Cellular

Any IoT application that requires operation over longer distances can take advantage of GSM/3G/4G cellular communication capabilities. While cellular is clearly capable of sending high quantities of data, especially for 4G, the expense and also power consumption will be too high for many applications, but it can be ideal for sensor-based low-bandwidth-data projects that will send very low amounts of data over the Internet.

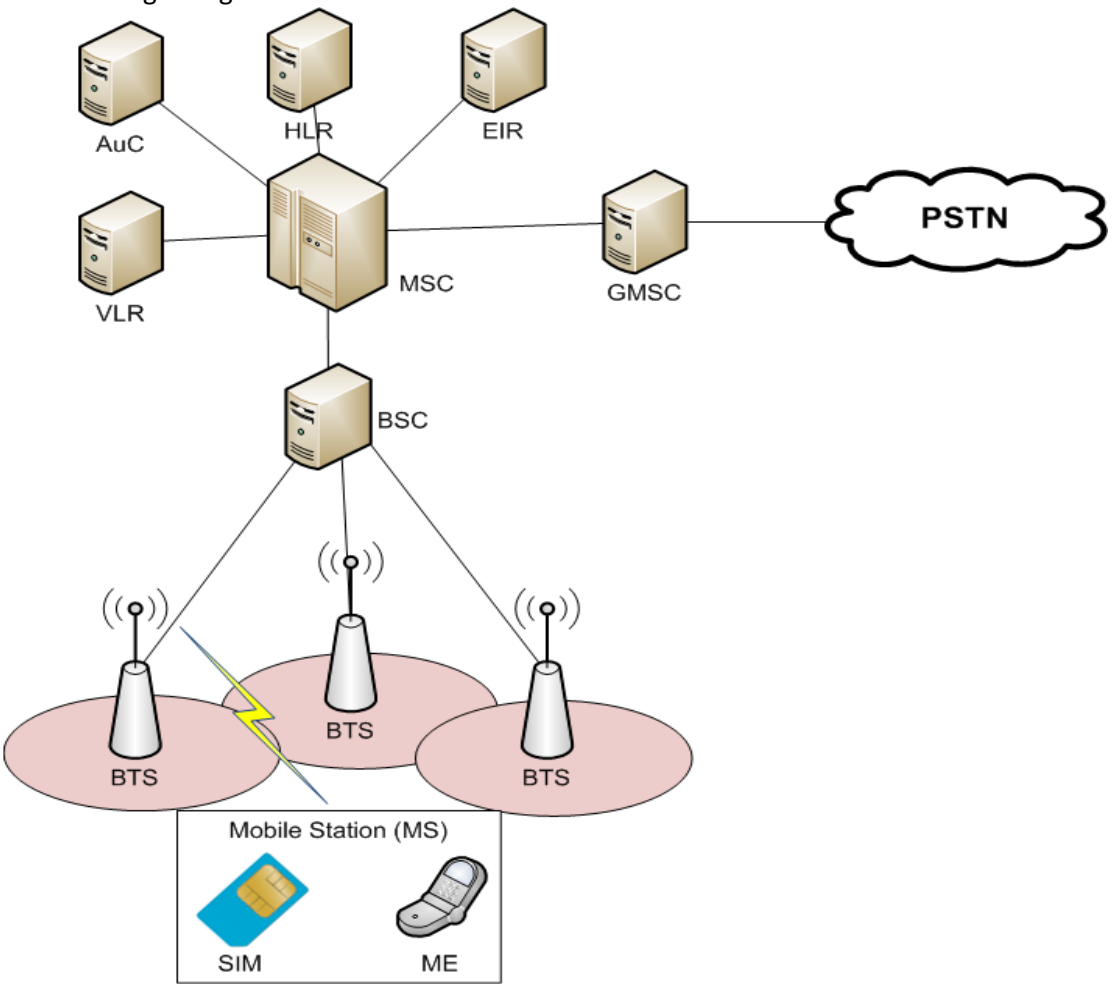
- Standard: GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)
- Frequencies: 900/1800/1900/2100MHz
- Range: 35km max for GSM; 200km max for HSPA
- Data Rates (typical download): 35-170kps (GPRS), 120-384kbps (EDGE), 384Kbps-2Mbps (UMTS), 600kbps-10Mbps (HSPA), 3-10Mbps (LTE)

A Closer Look at GSM

GSM or **Global System for Mobile Communications** is the most popular wireless cellular communication technique, used for public communication. The GSM standard was developed for setting protocols for second generation (2G) digital cellular networks.
It initially started as a circuit switching network, but later packet switching was implemented after integration General Packet Radio Service (GPRS) technology as well. The widely-used GSM frequency bands are 900 MHz and 1800 MHz
In the Europe and Asia, the GSM operates in 900 to 1800 MHz frequency range, whereas in United States and other American countries, it operates in the 850 to 1900 MHz frequency range. It uses the digital air interface wherein the analog signals are converted to digital signals before transmission. The transmission speed is 270 Kbps.

GSM Architecture

The GSM architecture is divided into Radio Subsystem, Network and Switching Subsystem and the Operation Subsystem. The radio sub system consists of the Mobile Station and Base Station Subsystem.
The mobile station is generally the mobile phone which consists of a transceiver, display and a processor. Each handheld or portable mobile station consists of a unique identity stored in a module known as SIM (Subscriber Identity Chip). It is a small microchip which is inserted in the mobile phone and contains the database regarding the mobile station.



The base station subsystem

It connects the mobile station with the network subsystem via the air interface.
It consists of the below given elements**:**

Base Transceiver Station*:* One or more Base Transceiver Station provides physical connection of a mobile station to the network in form of air interface. Depending on load, subscriber behavior and morph structure, it can have different configurations – Standard configuration (Each BTS is assigned a different cell identity (CI) and several BTS forms a location area).
Umbrella Cell configuration (One BTS with high transmission power installed at a higher altitude, acting as an umbrella to the lower transmission power Base Transmitter Stations), Collocated configurations (several BTSs collocated at one site, but antennas cover only area of 120 or 180 degrees). It is a network of neighboring radio cells which provide a complete coverage of the service area.

Base Station Controller*:* It controls operation of one more Base Transceiver Stations, basically the handover or power control. It consists of a database comprising the whole maintenance status of the BTS, quality of radio and terrestrial resources and BTS operations software).

Transcoding Rate and Adaption Unit*:* It is located between a Base Station Controller and a Mobile Switching Centre. It compresses or decompresses speech from the mobile station. However, it is not used for data connections.

Network Switching Subsystem

It provides the complete set of control and database functions needed to set up a call using encryption, authentication and roaming features. It basically provides network connection to the Mobile Station. It consists of the below given elements

Mobile Switching Centre*:* It is the main element within the overall GSM network. It is like a Public Switched Telephone Network (PSTN) exchange or Integrated Services Digital Network (ISDN) exchange. Apart from the normal functionary, it supports additional functionality like registration, authentication, call location and call routing to the subscriber.
It provides interfaces to Public Switched Telephone Network (PSTN) for connection with landline or interface to another Mobile Switching Centre (MSC) for connection to another mobile phone.

Home Location Register*:* It is a repository which stores data belonging to large number of subscribers. It is basically a large database which administers data of each subscriber. For security purposes, it maintains subscriber specific parameter such as parameter Ki, known only to the HLR and the SIM.

Virtual Location Register*:* It is similar to Home Location Register (HLR) , but differs in the fact that it stores dynamic information regarding the subscriber data. It comes to act in case of roaming where a subscriber moves from one location to another. The information is stored in the Equipment Identity Register that maintains account of all mobile stations, each identified by their International Mobile Equipment Identity (IMEI) number.

NFC

NFC (Near Field Communication) is a technology that enables simple and safe two-way interactions between electronic devices, and especially applicable for smartphones, allowing consumers to perform contactless payment transactions, access digital content and connect electronic devices. Essentially it extends the capability of contactless card technology and enables devices to share information at a distance that is less than 4cm.

- Standard: ISO/IEC 18000-3
- Frequency: 13.56MHz (ISM)
- Range: 10cm
- Data Rates: 100–420kbps

Sigfox

An alternative wide-range technology is Sigfox, which in terms of range comes between WiFi and cellular. It uses the ISM bands, which are free to use without the need to acquire licenses, to transmit data over a very narrow spectrum to and from connected objects. The idea for Sigfox is that for many M2M applications that run on a small battery and only require low levels of data transfer, then WiFi's range is too short while cellular is too expensive and also consumes too much power. Sigfox uses a technology called Ultra Narrow Band (UNB) and is only designed to handle low data-transfer speeds of 10 to 1,000 bits per second. It consumes only 50 microwatts compared to 5000 microwatts for cellular communication, or can deliver a typical stand-by time 20 years with a 2.5Ah battery while it is only 0.2 years for cellular.
Already deployed in tens of thousands of connected objects, the network is currently being rolled out in major cities across Europe, including ten cities in the UK for example. The network offers a robust, power-efficient and scalable network that can communicate with millions of battery-operated devices across areas of several square kilometres, making it suitable for various M2M applications that are expected to include smart meters, patient monitors, security devices, street lighting and environmental sensors. The Sigfox system uses silicon such as the EZRadioPro wireless transceivers from Silicon Labs, which deliver industry-leading wireless performance, extended range and ultra-low power consumption for wireless networking applications operating in the sub-1GHz band.

- Standard: Sigfox
- Frequency: 900MHz
- Range: 30-50km (rural environments), 3-10km (urban environments)
- Data Rates: 10-1000bps

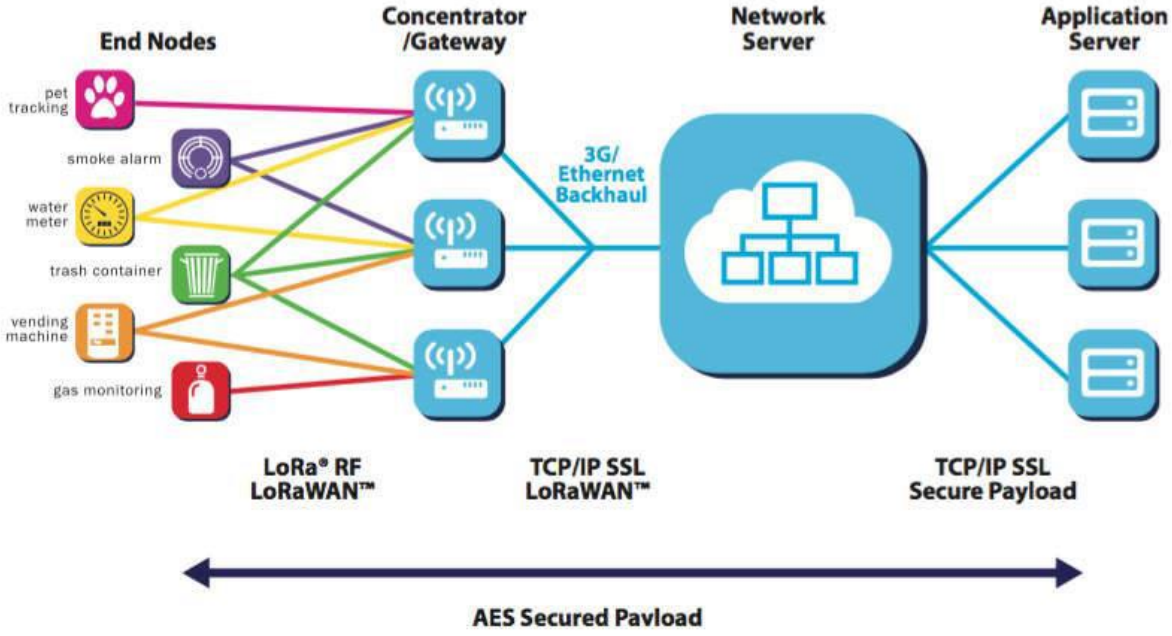
LoRaWAN

LoRaWAN is a media access control (MAC) protocol for wide area networks. It is designed to allow low-powered devices to communicate with Internet-connected applications over long range wireless connections. LoRaWAN can be mapped to the second and third layer of the OSI model. It is implemented on top of LoRa or FSK modulation in industrial, scientific and medical (ISM) radio bands. The LoRaWAN

protocols are defined by the LoRa Alliance and formalized in the LoRaWAN Specification which can be requested on the LoRa Alliance website.

Terminology

- **End Device, Node, Mote** - an object with an embedded low-power communication device.
- **Gateway** - antennas that receive broadcasts from End Devices and send data back to End Devices.
- **Network Server** - servers that route messages from End Devices to the right Application, and back.
- **Application** - a piece of software, running on a server.
- **Uplink Message** - a message from a Device to an Application.
- **Downlink Message** - a message from an Application to a Device



Again, similar in some respects to Sigfox and Neul, LoRaWAN targets wide-area network (WAN) applications and is designed to provide low-power WANs with features specifically needed to support low-cost mobile secure bi-directional communication in IoT, M2M and smart city and industrial applications. Optimized for low-power consumption and supporting large networks with millions and millions of devices, data rates range from 0.3 kbps to 50 kbps.

- Standard: LoRaWAN
- Frequency: Various
- Range: 2-5km (urban environment), 15km (suburban environment)
- Data Rates: 0.3-50 kbps.

Application Layer Protocols in IoT

Remember that an application layer protocol defines how application processes (clients and servers) running on different end systems pass messages to each other.

- The types of messages e.g. request messages and response messages
- The syntax of the various message types i.e. the fields in the messages
- The semantics of the field i.e. the meaning of the information that the field is supposed to contain.
- Rules determining when and how a process sends messages and responds to messages.

Some of the common application layer protocols employed in IoT include MQTT, COAP, AMQP and HTTP.

MQTT

MQTT is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium. MQ Telemetry Transport

It was, and is, designed for small, constrained devices and makes design decisions based on those constraints. Concepts which are important in the IoT world, such as memory, bandwidth, latency, power consumption, and network reliability. Let's focus in on one of the main MQTT concepts, the publish/subscribe pattern.

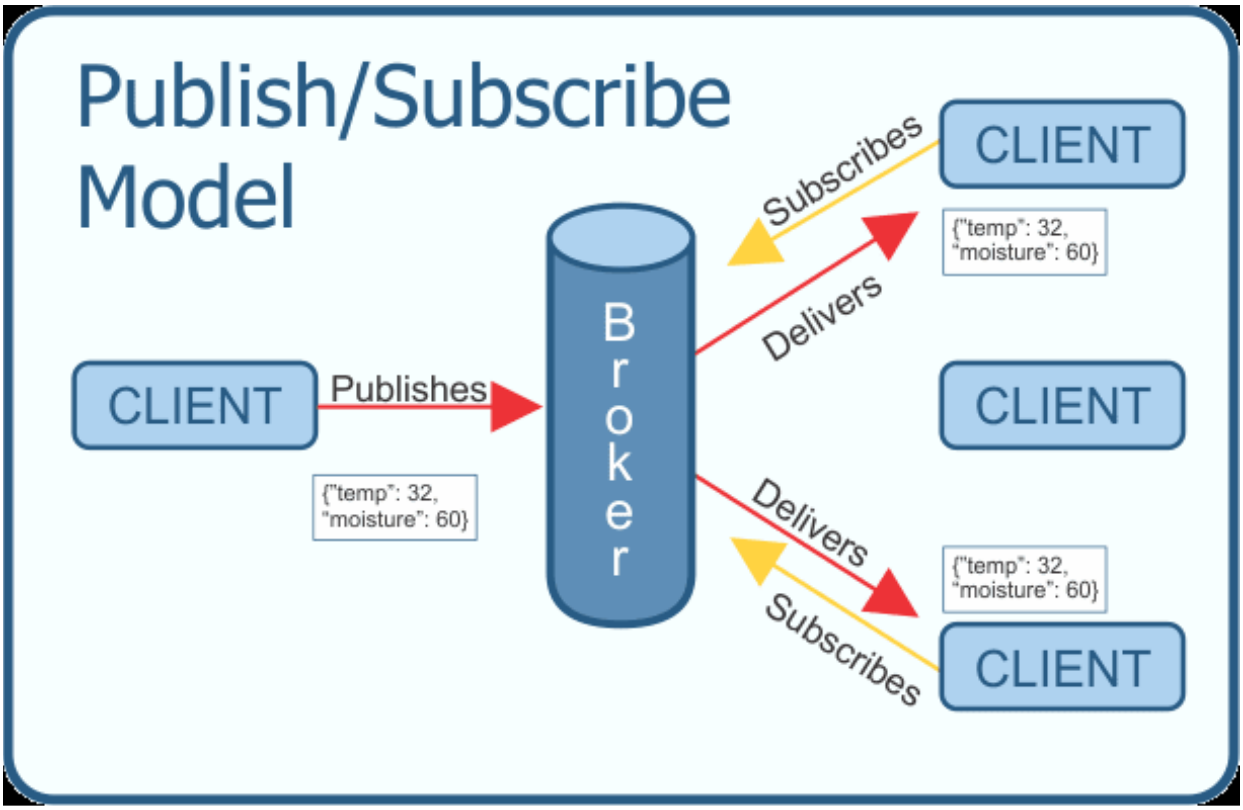
MQTT Publish/Subscribe Pattern

In a publish/subscribe pattern a client publishes information and another client can *subscribe* to the information it wants. In many cases there is a broker between the clients who facilitates and/or filters the information. This allows for a loose coupling between entities.

The decoupling can occur in a few different ways, space, time, and synchronization.

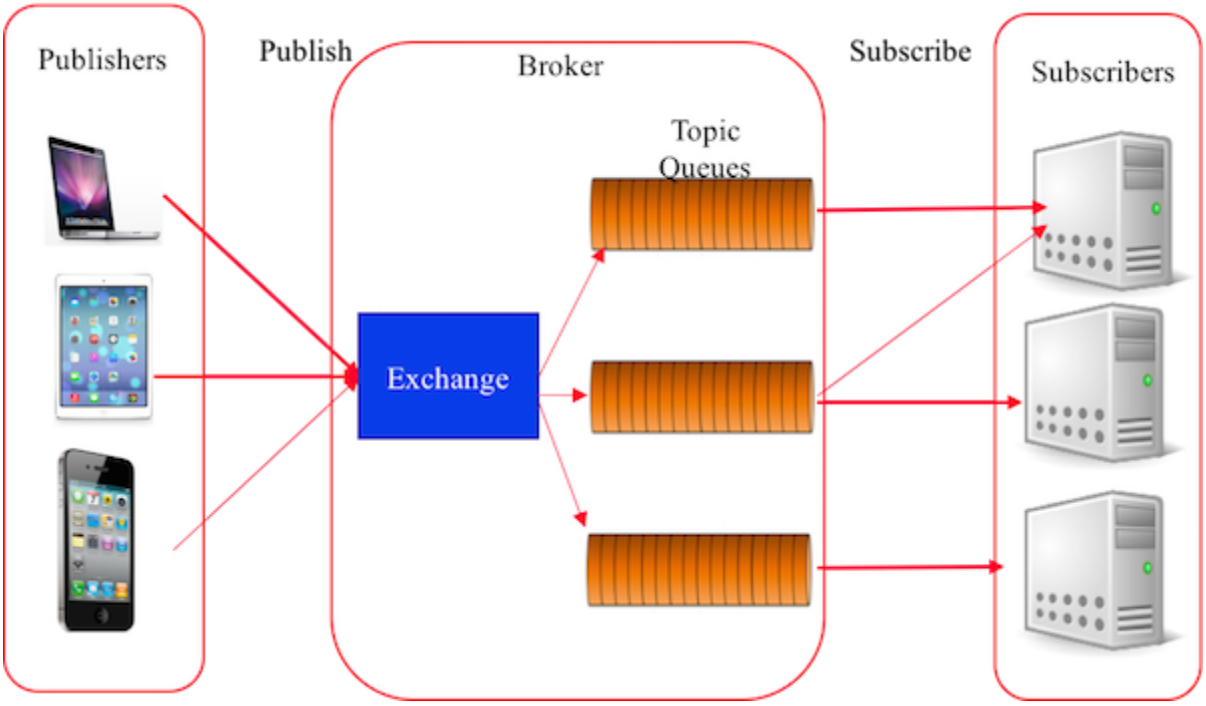
1. Space - the subscriber doesn't need to know who the publisher is, for example by IP address, and vice-versa
2. Time - the two clients don't have to be running at the same time
3. Synchronization - Publishing and receiving doesn't halt operations

Through the filtering done on the broker not all subscribers have to get the same messages. The broker can filter on subject, content, or type of message. A client, therefore could subscribe to only messages about temperate data. Or only messages with content about centrifuge machines. Or, perhaps, we only want to receive information about specific types of errors.



AMQP

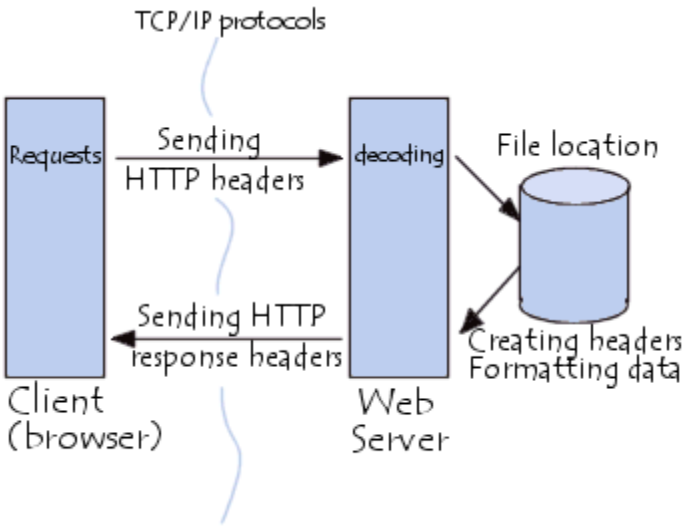
The Advanced Message Queuing Protocol (AMQP) is another session layer protocol that was designed for financial industry. It runs over TCP and provides a publish/ subscribe architecture which is similar to that of MQTT. The difference is that the broker is divided into two main components: exchange and queues. The exchange is responsible for receiving publisher messages and distributing them to queues based on pre-defined roles and conditions. Queues basically represent the topics and subscribed by subscribers which will get the sensory data whenever they are available in the queue.



HTTP

HTTP is still a widely used protocol in IoT. HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

HTTP concepts include (as the Hypertext part of the name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests. Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. Your Web browser is an HTTP client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator or URL) or clicking on a hypertext link, the browser builds an HTTP request and sends it to the Internet Protocol address (IP address) indicated by the URL. The HTTP daemon in the destination server machine receives the request and sends back the requested file or files associated with the request. (A Web page often consists of more than one file.)



HTTP is not really ideal for many of IoT's special needs, such as:

- Emitting information from one to many
- Listening for events whenever they may happen
- Distributing small packets of data in huge volumes
- Pushing information over unreliable networks
- High sensitivity to
    - Volume (cost) of data being transmitted
    - Power consumption (battery-powered devices)
    - Responsiveness (near real-time delivery of information)
- Security and privacy
- Scalability

HTTP versus MQTT

The table below offers a quick summary comparison of results from tests done between HTTPS and Message Queue Telemetry Transport (MQTT). The tests were done by sending and receiving 1024 messages of 1 byte each.

Characteristics		3G		WiFi	
		HTTPS	***MQTT***	***HTTPS***	***MQTT***
Receive Messages	**Messages / Hour**	1,708	160,278	3,628	263,314
	Percent Battery / Hour	18.43%	16.13%	3.45%	4.23%
	Percent Battery / Message	0.01709	0.00010	0.00095	0.00002
	Messages Received (Note the losses)	240 / 1024	1024 / 1024	524 / 1024	1024 / 1024
Send Messages	**Messages / Hour**	1,926	21,685	5,229	23,184
	Percent Battery / Hour	18.79%	17.80%	5.44%	3.66%
	Percent Battery / Message	0.00975	0.00082	0.00104	0.00016

As the above sample data shows, HTTP:

- Uses more battery (percent battery/hour and percent battery/message)
- Is less reliable—note that only 240 (3G) / 524 (WiFi) messages were received out of a total of 1024 messages in the case of HTTP versus receiving all of the 1024 messages in the case of MQTT
- Is a lot slower (for example 1,708 messages/hour for HTTP versus 160,278 messages/hour for MQTT)

From this as well as other comparisons, it is quite clear that the search for the right protocol in the IoT is still an open topic. There are plenty of indications that there is a possibility to overcome many of the limitations of HTTP by adopting or creating a more suited solution for the IoT.

Notable Mentions

1. ***The Constrained Application Protocol (CoAP***) is a specialized web transfer protocol for use with constrained networks and nodes for machine-to-machine applications such as smart energy and building automation.
2. ***Extensible Messaging and Presence Protocol (XMPP)*** is an open technology for real-time communication, which powers a wide range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication and generalized routing of XML data.
3. ***Representational State Transfer (REST) or RESTful HTTP*** is a style to use the existing features and capabilities of the web. REST does not invent new technologies, components or services. RESTful HTTP defines the principles and constraints to use the existing web standards in a better way.

IPV6

The IPv4 address space provides approximately 4.3 billion addresses. Of that address space, approximately 3.7 billion addresses are actually assignable; the other addresses are reserved for special purposes, such as multicasting, private address space, loopback testing, and research.

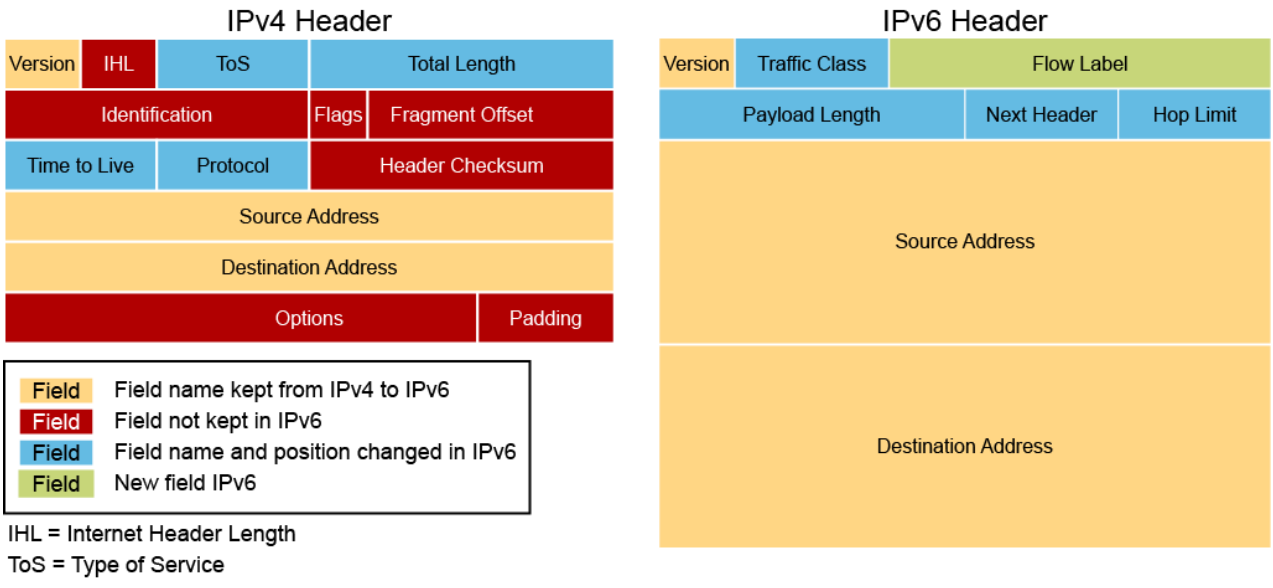
The IPv4 public address space has now been exhausted. Many enterprises have sufficient address space (public or private) to manage their intranet needs for the next few years. However, the length of time that is needed to transition to IPv6 demands that administrators and managers consider the issue well in advance. The largest enterprises may need to act sooner rather than later to ensure sufficient enterprise connectivity.

A simplified IPv6 header architecture and protocol operation translates into reduced operational expenses. Built-in security features mean easier security practices that are sorely lacking in many current networks. However, perhaps the most significant IPv6 improvement is the address autoconfiguration features.

The Internet is rapidly evolving from a collection of stationary devices to a fluid network of mobile devices. IPv6 allows mobile devices to quickly acquire and transition between addresses as they move among foreign networks, with no need for a foreign agent. A foreign agent is a router that can function as the point of attachment for a mobile device when it roams from its home network to a foreign network.

IPv6 address auto configuration also means more robust plug-and-play network connectivity. Auto configuration supports consumers who can have any combination of computers, printers, digital cameras, digital radios, IP phones, Internet-enabled household appliances, and robotic toys that are connected to their home networks. Many manufacturers already integrate IPv6 into their products.

The figure below compares the fields of an IPv6 header to the fields of an IPv4 header.



The IPv6 header fields are the following:

- **Version (4-bit):** Contains the value 6 rather than the value 4 contained in an IPv4 packet

- **Traffic class (8 bits):** This field and its functions are similar to the ToS field in IPv4.
- **Flow label (20 bits):** Used to tag a flow for IPv6 packets, which is new in the IPv6 protocol. The current IETF standard does not specify the details about how to manage and process the flow label.
- **Payload length (16 bits):** The size of the payload in octets, including any extension headers.
- **Next header (8 bits):** Specifies the type of the next header. This field usually specifies the transport layer protocol that is used by a packet's payload. When extension headers are present in the packet, this field indicates which extension header follows. IPv6 extension headers are optional headers that may follow the basic IPv6 header. Several types of extension headers are defined in the RFC 2460, Internet Protocol, Version 6 (IPv6) Specification.
- **Hop limit (8 bits):** Replaces the time to live field of IPv4. This value is decremented by one at each intermediate node visited by the packet. When the counter reaches 0, the packet is discarded.
- **Source address (128 bits):** The IPv6 address of the sending node.
- **Destination address (128 bits):** The IPv6 address of the destination node or nodes.

  Extension headers, if any, follow these eight fields. The number of extension headers is not fixed, so the total length of the extension header chain is variable.

  An IPv6 address is a 128-bit binary value, which can be displayed as 32 hexadecimal characters. IPv6 offers a virtually unlimited supply of IP addresses, due to its generous 128-bit address space. With IPv6, there are enough addresses to allocate more than the entire IPv4 Internet address space to everyone on the planet.

  IPv6 address format:

- x:x:x:x:x:x:x:x, where x is a 16-bit hexadecimal field (case-insensitive for hexadecimal A, B, C, D, E, and F)
- Leading zeros in a field are optional
- Successive fields of zeros can be represented as :: only once per address

  IPv6 address examples:

- Unicast: 2001:0000:130F:0000:0000:09C0:876A:130B or 2001:0:130f::9c0:876a:130b
- Multicast: FF01:0:0:0:0:0:0:1 or FF01::1
- Loopback: 0:0:0:0:0:0:0:1 or ::1
- Unspecified: 0:0:0:0:0:0:0:0 or ::

Why should the Internet of Things care about IPv6? Many answers can be given to such question, and thus, there are several arguments that show IPv6 will be (and actually it is already) a key enabler for the future Internet of Things:

1. *Adoption is just a matter of time*

The Internet Protocol is a must and a requirement for any Internet connection. It is the addressing scheme for any data transfer on the web. The limited size of its predecessor, IPv4, has made the transition to IPv6 unavoidable. The Google's figures are revealing an IPv6 adoption rate following an exponential curve, doubling every 9 months about.

2. *Scalability*

IPv6 offers a highly scalable address scheme. It provides 2^{128} unique addresses, which represents 3.4×10^{38} addresses. In other words, more than 2 Billions of Billions addresses per square millimetre of the Earth surface. It is quite sufficient to address the needs of any present and future communicating device.

3. *Solving the NAT barrier*

Due to the limits of the IPv4 address space, the current Internet had to adopt a trick to face its unplanned expansion: The Network Address Translation (NAT). It enables several users and devices to share the same public IP address. This solution is working but with two main trades-off:

- The NAT users are borrowing and sharing IP addresses with others. Hence, they do not have their own public IP address, which turns them into homeless Internet users. They can access the Internet, but they cannot be directly accessed from the Internet.
- It breaks the original end-to-end connection and dramatically weakens any authentication process.

4. *Strong Security enablers*

IPv6 provides end-to-end connectivity, with a more distributed routing mechanism. Moreover, IPv6 is supported by a very large community of users and researchers supporting an on-going improvement of its security features, including IPsec.

5. *Tiny stacks available*

IPv6 application to the Internet of Things has been being researched since many years. The research community has developed a compressed version of IPv6 named 6LoWPAN. It is a simple and efficient mechanism to shorten the IPv6 address size for constrained devices, while border routers can translate those compressed addresses into regular IPv6 addresses.

6. *Enabling the extension of the Internet to the web of things*

Thanks to its large address space, IPv6 enables the extension of the Internet to any device and service. Experiments have demonstrated the successful use of IPv6 addresses to large scale deployments of sensors in smart buildings, smart cities and even with cattle. Moreover, the CoAP protocol enables the

constrained devices to behave as web services easily accessible and fully compliant with REST architecture.

7. *Mobility*

IPv6 provides strong features and solutions to support mobility of end-nodes, as well as mobility of the routing nodes of the network.

8. *Address self-configuration*

IPv6 provides an address self-configuration mechanism (Stateless mechanism). The nodes can define their addresses in very autonomous manner. This enables to reduce drastically the configuration effort and cost.

9. *Fully Internet compliant*

IPv6 is fully Internet compliant. In other words, it is possible to use a global network to develop one's own network of smart things or to interconnect one's own smart things with the rest of the World.