SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

AN AUTONOMOUS INSTITUTION

Accredited by NBA–AICTE and Accredited by NAAC–UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

Department of Information Technology

19IT503 – Internet of Things

UNIT 3 - EVOLVING IoT STANDARDS & PROTOCOLS

IETF IPv6 Routing Protocol for RPL Roll

Low power and lossy networks (LLNs) are1 a class of networks in which both the routers and their interconnect are constrained. LLN routers typically operate with constraints on processing power, memory, and energy (battery power); their interconnects are characterized by high loss rates, low data rates, and instability.

The IPv6 Routing Protocol for LLNs (RPL) is a mechanism proposed by the IETF to support multipoint-to-point traffic from devices inside the LLN toward a central control point, as well as point to- multipoint traffic from the central control point to the devices inside the LLN.

Challenges in LLNs are low processing power, memory and energy constrained operation and it must also support point to point, point to multipoint and multipoint to point traffic. To address these issues, the IETF ROLL Working Group has defined application-specific routing requirements for an LLN routing protocol; it has also specified the RPL.

Existing routing protocols include

- OSPF/IS-IS (open shortest path first/ intermediate system to intermediate system),
- OLSRv2 (optimized link state routing protocol version 2),
- TBRPF (topology-based reverse path forwarding),
- RIP (routing information protocol),
- AODV (ad hoc on-demand distance vector),
- DYMO (dynamic MANET on-demand), and
- DSR (dynamic source routing).

Some of the metrics to be considered for IoT applications include the following:

- Routing state memory space—limited memory resources of low power nodes;
- Loss response—what happens in response to link failures;
- Control cost—constraints on control traffic;
- Link and node cost—link and node properties are considered when choosing routes.

The existing protocols all fail one or more of these goals for IoT applications.

RPL is designed to be able to operate over a variety of different link layers, including ones that are constrained, potentially lossy, or typically utilized in conjunction with highly constrained

host or router devices, such as but not limited to low power wireless or PLC (power line communication) technologies.

Some RPL Mechanisms and characteristics are

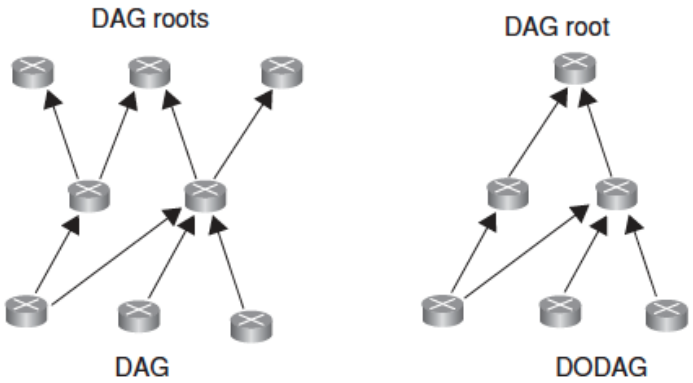
- RPL Packet Information and IPv6 Hop-by-Hop RPL
- RPL provides a mechanism to disseminate information over the dynamically formed network topology
- RPL also introduces the capability to bind a subnet together with a common prefix and to route within that subnet.
- RPL may, in particular, disseminate IPv6 neighbor discovery (ND) information prefix information option (PIO) and the route information option (RIO).

Some basic definitions in RPL are as follows

- Directed acyclic graph (DAG) is a directed graph with no cycles.
- Destination-oriented DAG (DODAG) is a DAG rooted at a single destination.

RPL defines a new ICMPv6 message with three possible types:

- DAG information object (DIO)—carries information that allows a node to discover an RPL instance, learn its configuration parameters, and select DODAG parents;
- DAG information solicitation (DIS)—solicit a DODAG information object from an RPL node;
- Destination advertisement object (DAO)—used to propagate destination information upward along the DODAG.



A node rank defines a node's relative position within a DODAG with respect to the DODAG root.

The approach in RPL is to build a topology (instance) where routes to these nodes are optimized (namely, DODAG(s) rooted at these nodes). DODAG construction proceeds as follows

- Nodes periodically send link-local multicast DIO messages;
- Stability or detection of routing inconsistencies influence the rate of DIO messages;
- Nodes listen for DIOs and use their information to join a new DODAG, or to maintain an existing DODAG;
- Nodes may use a DIS message to solicit a DIO;
- Based on information in the DIOs, the node chooses parents that minimize path cost to the DODAG root.

Constrained Application Protocol (CoAP)

CoAP is a simple application layer protocol targeted to simple electronic devices (e.g., IoT/M2M things) to allow them to communicate interactively over the Internet. CoAP is designed for low power sensors (especially wireless sensor network [WSN] nodes.

CoAP can be seen as a specialized web transfer protocol for use with constrained networks and nodes for M2M applications, such as smart energy and building automation.

CoAP operates with HTTP (hypertext transfer protocol) for basic support with the web, allowing proxies to be built providing access to CoAP resources via HTTP in a uniform way, while also supporting multicast and enjoying low overhead CoAP can run on most devices that support user datagram protocol (UDP) or a similar protocol.

Some key aspects of the protocol are as follows:
(i) minimal complexity for the mapping with HTTP;
(ii) low header overhead and low parsing complexity;
(iii) support for the discovery of resources;
(iv) simple resource subscription process; and
(v) simple caching based on max-age.

CoAP makes use of two message types, requests and responses, using a simple binary base header format. CoAP is by default bound to UDP and, optionally, to transmission control protocol (TCP).

One of the main goals of CoAP is to design a generic web protocol for the special requirements of this constrained environment, especially considering energy, building automation, and other M2M applications.

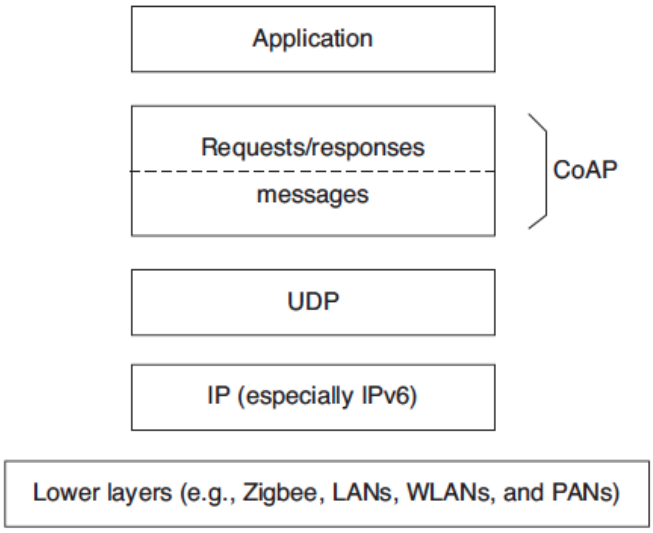
The objective of CoAP is not to statically compress HTTP, but rather to realize a subset of REST common with HTTP, but optimized for M2M applications.

CoAP has the following main features:

- Constrained web protocol fulfilling M2M requirements;
- UDP binding with optional reliability supporting unicast and multicast requests;
- Asynchronous message exchanges;
- Low header overhead and parsing complexity;
- URI and content-type support;
- Simple proxy and caching capabilities;
- A stateless HTTP mapping, allowing proxies to be built providing access toCoAP resources via HTTP in a uniform way or for HTTP simple interfaces tbe realized alternatively over CoAP; and
- Security binding to datagram transport layer security (DTLS).

The interaction model of CoAP is similar to the client/server model of HTTP. A CoAP request is equivalent to that of HTTP and is sent by a client to request an action (using a method code) on a

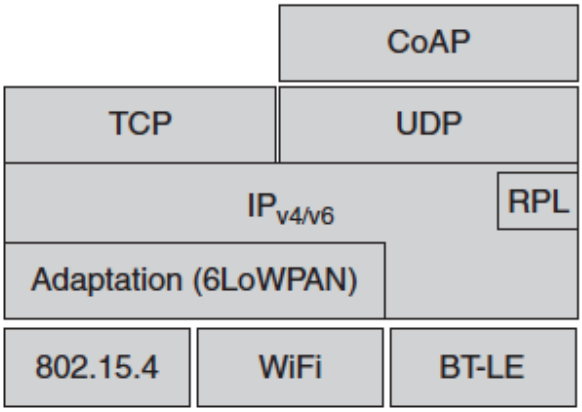
resource (identified by a URI) on a server. The server then sends a response with a response code; this response may include a resource representation.



CoAP defines four types of messages:

- confirmable (CON),
- non-confirmable (NON),
- acknowledgement,
- reset

Protocol Stack of CoAP



Messaging Model

- The CoAP messaging model is based on the exchange of messages over UDP between end-points.
- It uses a short fixed-length binary header (4 bytes) that may be followed by compact binary options and a payload.
- Each CoAP message contains a message ID used to detect duplicates and for optional reliability

- Reliability is provided by marking a message as CON. A CON message is retransmitted using a default timeout and exponential back-off between retransmissions, until the recipient sends an acknowledgement message (ACK) with the same message ID from the corresponding end-point.
- When a recipient is not able to process a CON message, it replies with a reset message (RST) instead of an ACK.
- A message that does not require reliable delivery, for example, each single measurement out of a stream of sensor data, can be sent as a NON message.

Request/Response Model

- CoAP request and response semantics are carried in CoAP messages, which include either a method code or response code, respectively
- A request is carried in a CON or NON message, and if immediately available, the response to a request carried in a CON message is carried in the resulting ACK message.
- If the server is not able to respond immediately to a request carried in a CON message, it simply responds with an empty ACK message so that the client can stop retransmitting the request.
- When the response is ready, the server sends it in a new CON message
- CoAP makes use of GET, PUT, POST, and DELETE methods in a similar manner to HTTP.

Intermediaries and Caching

The protocol supports the caching of responses in order to efficiently fulfill requests. Proxying is useful in constrained networks for several reasons, including

(i) Network traffic limiting,
(ii) to improve performance,
(iii) to access resources of sleeping devices, or
(iv) for security reasons

Representational State Transfer (REST)

REST was first described in 2000 by Roy Fielding in his University of California dissertation which analyzed a set of web focused software architecture principles for distributed computing.

It defines a set of architectural principles by which one can design WS. It focus on a system's resources, including how resource states are addressed and transferred over HTTP by a plethora of clients written in different languages.

REST is an architectural style of large-scale networked software that takes advantage of the technologies and protocols of the World Wide Web;

It describes how distributed data objects, or resources, can be defined and addressed, stressing the easy exchange of information and scalability.

A REST-based WS follows four basic design principles:

- Use HTTP methods explicitly.

- Be stateless.
- Expose directory structure-like URIs.
- Transfer XML, JavaScript Object Notation (JSON), or both.

A REST-based WS follows four basic design principles:

- Use HTTP methods explicitly.
- Be stateless.
- Expose directory structure-like URIs.
- Transfer XML, JavaScript Object Notation (JSON), or both.
- A web API that obeys the REST constraints is informally described as RESTful
- RESTful web APIs are typically loosely based on HTTP methods to access resources via URL-encoded parameters and the use of JSON or XML to transmit data

The REST architectural constraints are Client-Server, Stateless, Cache-able, Layered System, Uniform Interface, Code on Command.

Making Requests

REST requires that a client make a request to the server in order to retrieve or modify data on the server.

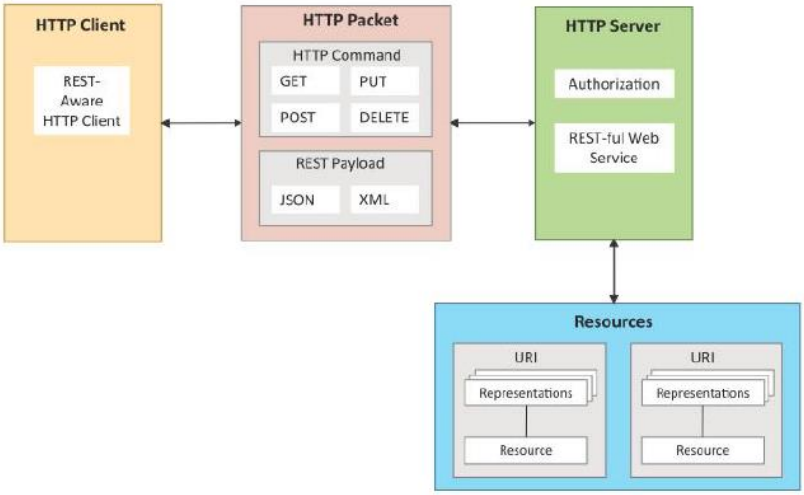
A request generally consists of:

- an HTTP verb, which defines what kind of operation to perform
- a header, which allows the client to pass along information about the request
- a path to a resource
- an optional message body containing data

HTTP Verbs

There are 4 basic HTTP verbs we use in requests to interact with resources in a REST system:

- GET — retrieve a specific resource (by id) or a collection of resources
- POST — create a new resource
- PUT — update a specific resource (by id)
- DELETE — remove a specific resource by id



- In the header of the request, the client sends the type of content that it is able to receive from the server.
- This is called the Accept field, and it ensures that the server does not send data that cannot be understood or processed by the client.
- MIME Types, used to specify the content types in the Accept field, consist of a type and a subtype. They are separated by a slash (/).
- For example, a text file containing HTML would be specified with the type text/html.
- If this text file contained CSS instead, it would be specified as text/css.
- A generic text file would be denoted as text/plain. This default value, text/plain

Other types and commonly used subtypes:
- image — image/png, image/jpeg, image/gif
- audio — audio/wav, audio/mpeg
- video — video/mp4, video/ogg
- application — application/json, application/pdf, application/xml, application/octet-stream

- For example, a client accessing a resource with id 23 in an articles resource on a server might send a GET request like this:
- GET /articles/23 Accept: text/html, application/xhtml
- The Accept header field in this case is saying that the client will accept the content in text/html or application/xhtml.

Paths
- Requests must contain a path to a resource that the operation should be performed on.
- In RESTful APIs, paths should be designed to help the client know what is going on.

Example
- GET flipkart.com/customers/223/MyOrders/12
- DELETE flipkart.com/customers/223/MyOrders/12

Content Type
- In cases where the server is sending a data payload to the client, the server must include a content-type in the header of the response.

- This content-type header field alerts the client to the type of data it is sending in the response body.

For example, when a client is accessing a resource with id 23 in a topic resource with this GET Request:
GET snscourseware/IT/IoT/Topic/23 HTTP/1.1
Accept: text/html, application/xhtml

The server might send back the content with the response header:
HTTP/1.1 200 (OK)
Content-Type: text/html

Response Codes
Responses from the server contain status codes to alert the client to information about the success of the operation.

Status code Meaning

- 200 (OK) This is the standard response for successful HTTP requests.
- 201 (CREATED) This is the standard response for an HTTP request that resulted in an item being successfully created.
- 204 (NO CONTENT) This is the standard response for successful HTTP requests, where nothing is being returned in the response body.
- 400 (BAD REQUEST) The request cannot be processed because of bad request syntax, excessive size, or another client error.
- 403 (FORBIDDEN) The client does not have permission to access this resource.
- 404 (NOT FOUND) The resource could not be found at this time. It is possible it was deleted, or does not exist yet.
- 500 (INTERNAL SERVER ERROR) The generic answer for an unexpected failure if there is no more specific information available.

Third Generation Partnership Project Service Requirements for Machine Type Communications

Current mobile networks are optimized for human-to-human (H2H) traffic and not for M2M/MTC interactions; hence, optimizations for MTC are advantageous.

3GPP has started work on M2Mspecification in 2010 for interoperable solutions, particularly in the 3G/4G/LTE context.

In M2M architecture, the interfaces are as follows:

- MTCu: provides MTC devices access to the 3GPP network for the transport of user traffic;
- MTCi: the reference point for MTC server to connect the 3GPP network via 3GPP bearer service; and
- MTCsms: the reference point for MTC server to connect the 3GPP network via 3GPP SMS.

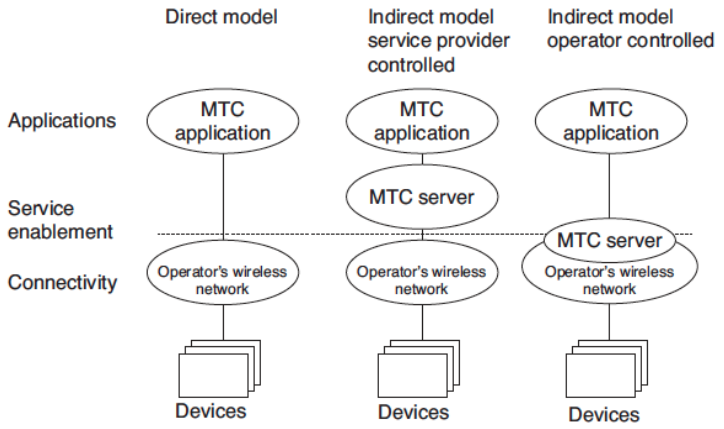
For MTC communication, the following communication scenarios are identified and described
(i) MTC devices communicating with one or more MTC server;
(ii) MTC devices communicating with each other.

For MTC devices communicating with one or more MTC servers, the following use cases exist:
(a) MTC server controlled by the network operator; namely the MTC server is located in the operator domain. Here

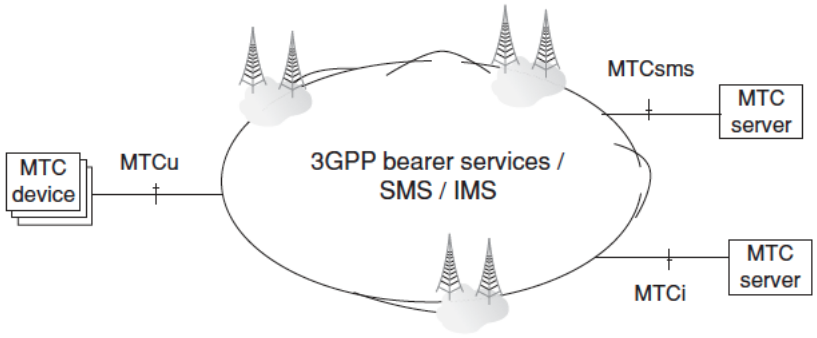
– The network operator offers API (e.g., Open Systems Architecture [OSA]) on its MTC server(s)
– MTC user accesses MTC server(s) of the network operator via API

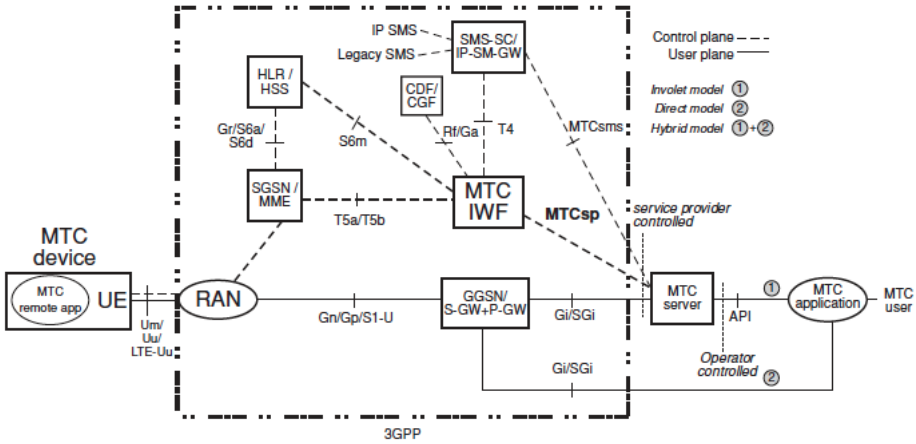
(b) MTC server not controlled by the network operator; namely MTC server is located outside the operator domain. Here

– The network operator offers the network connectivity to the MTC server(s) located outside of the network operator domain



M2M in 3GPP—service models





M2M in 3GPP—Architecture

Architectural Reference Model for MTC

The architecture encompasses a number of models as follows:

- **Direct model**—direct communication provided by the 3GPP operator: The MTC application connects directly to the operator network without the use of any MTC server;
- **Indirect model—MTC** service provider controlled communication: The MTC server is an entity outside of the operator domain. The MTCsp and MTCsms are external interfaces (i.e., to a third-party M2M service provider);
- **Indirect model—3GPP** operator controlled communication: The MTC server is an entity inside the operator domain. The MTCsp and MTCsms are internal to the public land mobile network (PLMN);
- **Hybrid model:** The direct and indirect models are used simultaneously in the hybrid model, for example, connecting the user plane using the direct model and doing control plane signalling using the indirect model.

IPv6 Over Low Power WPAN (6LoWPAN)

6LoWPAN is an IPv6 adaption layer for low power wireless PAN (LoWPAN). A link in a LoWPAN is characterized as lossy, low power, low bit-rate, short range, with many nodes saving energy with long sleep periods.

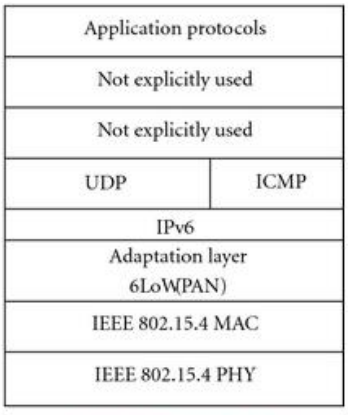
6LoWPAN provides a means of carrying packet data in the form of IPv6 over IEEE 802.15.4 and other networks. A LoWPAN is potentially composed of a large number of overlapping radio ranges works on 2.4 GHz

It uses AES-128 link layer security for authentication and encryption and TLS

6LoWPAN is a low power wireless mesh network where every node has its own IPv6 address. This allows the node to connect directly with the Internet using open standards.

It works great with open IP standard including TCP, UDP, HTTP, COAP, MATT and web-sockets. It offers end-to-end IP addressable nodes. There's no need for a gateway, only a router which can connect the 6LoWPAN network to IP.

In a 6LowPAN network, leaf nodes can sleep for a long duration of time.



6LoWPAN protocol stack

6LoWPAN Application Areas

- Automation: There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
- Industrial monitoring: Industrial plants and automated factories provide a great opportunity for 6LoWPAN. Major savings can be made by using automation in every day practices. Additionally, 6LoWPAN can connect to the cloud which opens up many different areas for data monitoring and analysis.
- Smart Grid: Smart grids enable smart meters and other devices to build a micro mesh network. They are able to send data back to the grid operator's monitoring and billing system using the IPv6.
- Smart Home: By connecting your home IoT devices using IPv6, it is possible to gain distinct advantages over other IoT systems.

6LoWPAN Security

- 6LoWPAN can use AES-128 link layer security which is defined in IEEE 802.15.4. This provides link authentication and encryption.

- Further security is provided by the transport layer security mechanisms.

Advantages of 6LoWPAN

- It works great with open IP standard including TCP, UDP, HTTP, COAP, MATT and web-sockets.
- It offers end-to-end IP addressable nodes. There's no need for a gateway, only a router which can connect the 6LoWPAN network to IP.
- It supports self-healing, robust and scalable mesh routing.
- Offers one-to-many & many-to-one routing.
- The 6LoWPAN mesh routers can route data to others nodes in the network.
- In a 6LowPAN network, leaf nodes can sleep for a long duration of time.
- It also offers thorough support for the PHY layer which gives freedom of frequency band & physical layer, which can be used across multiple communication platforms like Ethernet, WI-Fi, 802.15.4 or Sub-1GHz ISM with interoperability at the IP level.

6LoWPANS GOALS

LoWPANs in general and IEEE 802.15.4-2003-based systems in particular have design constraints that need to be taken into consideration when developing a protocol stack. These constraints fall into two categories:

- Communication constraints defined by the underlying personal area network (PAN): Small packet size, Support for both 16-bit short or IEEE 64-bit extended media access control addresses, Low bandwidth, Topologies include star and mesh operation

- System constraints driven by the intended application parameters: Characteristic examples include low/battery power, low cost, low processing capabilities, small memory size, large population of devices, ad-hoc locations/ logical topology, mobility, and unreliable nodal behaviors e.g., due to uncertain radio connectivity, interference, sleep state, battery drain, device, etc

IP in Small Objects (IPSO)

The IPSO Alliance is an advocate for IP-networked devices for use in energy, consumer, healthcare, and industrial applications.

The IPSO Alliance is a non-profit association of more than 60 members from leading technology, communications, and energy companies around the world.

The mission is to provide a foundation for industry growth through building stronger relationships, fostering awareness, providing education, promoting the industry, generating research, and creating a better understanding of IP and its role in connecting smart objects.

Goals include

- Promote IP as the premier solution for access and communication for smart objects.
- Promote the use of IP in smart objects by developing and publishing white papers and case studies and providing updates on standards progress from associations like IETF, among others, and through other supporting marketing activities.
- Understand the industries and markets where smart objects can have an effective role in growth when connected using the Internet protocol.
- Organize interoperability tests that will allow members and interested parties to show that products and services using IP for smart objects can work together and meet industry standards for communication.
- Support IETF and other standards development organizations in the development of standards for IP for smart objects.

WPAN Technologies for IoT/M2M

A PAN (Personal Area Networks also called WPAN) is a network used for communication among intelligent devices physically close to a person (including smart phones, tablets, body monitors, and so on)

PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network such as the Internet.

Some of the commonly used PAN are

- 3GPP2 – Cellular Technologies like – GSM, UMTS, LTE
- 6LoWPAN - IPv6 over low-power area network IEEE802.15.4
- ANT/ANT+ - low-power proprietary wireless technology introduced in 2004 by the sensor company Dynastream. ANT's goal is to allow sports and fitness sensors to communicate with a display unit

- Bluetooth - Bluetooth is a PAN technology based on IEEE 802.15.1. It is a specification for short-range wireless connectivity for portable personal devices initially developed by Ericsson.

- DASH7 - A long range low-power wireless networking technology from 10m to 10km, max-200kbps

- IEEE 802.15.4j (TG4j) MBAN – Medical body area network

- Infrared Data Association (IrDA) – used for very short range communication

- ISA100.11a - ISA SP100 standard for wireless industrial networks developed by the International Society of Automation (ISA) to address all aspects of wireless technologies in a plant.

- NFC (Near Field Communication) - A group of standards for devices such as PDAs, smartphones, and tablets that support the establishment of wireless communication when such devices are in immediate proximity of a few inches.

- NIKE+ Nike+R is a proprietary wireless technology developed by Nike and Apple to allow users to monitor their activity levels while exercising.

- RF4CE (Radio Frequency for Consumer Electronics) - RF4CE is based on ZigBee and was standardized in 2009 by four CE companies: Sony, Philips, Panasonic, and Samsung. RF4CE's intended use is as a device RC system, for example for television set-top boxes.

- Satellite systems Satellite communication plays a key role in commercial, TV/media, government, and military communications because of its intrinsic multicast/broadcast capabilities, mobility aspects, global reach, reliability, and ability to quickly support connectivity in open-space and/or hostile environments.

- WiMAX - WiMAX is defined as Worldwide Interoperability for Microwave Access by the WiMAX Forum, formed in June 2001 to promote conformance and interoperability of the IEEE 802.16 standard.

- Wireless Meter-Bus (M-BUS) - The Wireless M-Bus standard (EN 137514–4:2005) specifies communications between water, gas, heat, and electric meters and is becoming widely accepted in Europe for smart metering or AMI applications. Wireless M-Bus is targeted to operate in the 868 MHz band (from 868 MHz to 870 MHz).

- WSN (Wireless Sensor Network) - A sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives the administrator the ability to instrument, observe, and react to events and phenomena in a specified environment.

- WirelessHART (aka IEC 62591) – Wireless HART is a wireless sensor networking

technology based on the highway addressable remote transducer protocol (HART).

- Zigbee – The core ZigBee specification defines ZigBee's smart, cost-effective, and energy-efficient mesh network based on IEEE 802.15.4

- Z-wave - Z-wave is a wireless ecosystem that aims at supporting connectivity of home electronics, and the user, via Remote Control (RC). It uses low-power radio waves that easily travel through walls, floors, and cabinets.

Zigbee/IEEE 802.15.4

Zigbee is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks.

ZigBee is an open global standard for wireless technology designed to use low-power digital radio signals for personal area networks. ZigBee operates on the IEEE 802.15.4 specification and is used to create networks that require a low data transfer rate, energy efficiency and secure networking. It is employed in a number of applications such as building automation systems, heating and cooling control and in medical devices.

ZigBee is designed to be simpler and less expensive than other personal are network technologies such as Bluetooth. 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.

Physical Characteristics
Standard- Zigbee 3.0 based on IEEE802.15.4
Frequencies- 2.4 Ghz
Range- Approx. 10-100m
Data Rates – 250 kbps

ZigBee networks support star, mesh, and cluster-tree topologies. These capabilities enable a network to have over 65,000 devices on a single wireless network. ZigBee offers low-latency communication

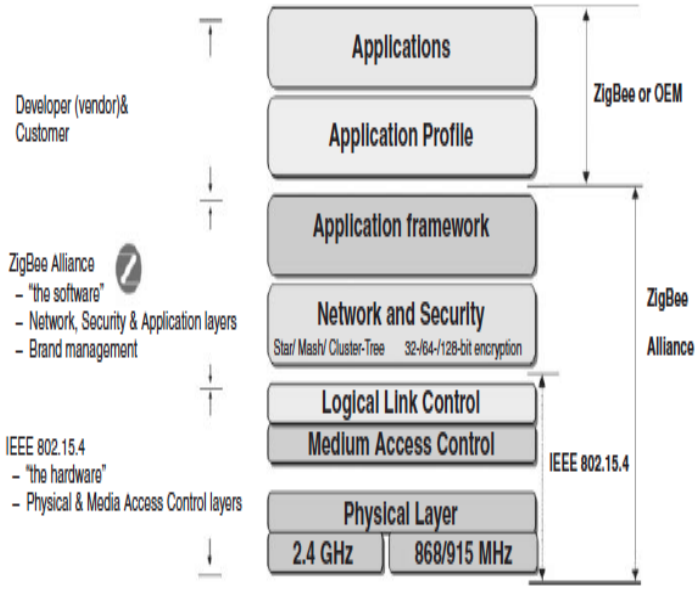
ZigBee can create robust self-forming, self-healing wireless mesh network. The ZigBee mesh network connects sensors and controllers without being restricted by distance or range limitations.

Variations of Technology
ZigBee is available as two feature sets, ZigBee PRO and ZigBee.

ZigBee PRO, the most widely used specification, is optimized for low-power consumption and to support large networks with thousands of devices ZigBee PRO adds some new application profiles such as automatic meter reading, commercial building automation, and home automation.
ZigBee PRO networks have the ability to aggregate routes through the use of "many-to-one" routing.

The ZigBee 802.15.4 spec defines a maximum packet size of 128 octets; this packet size is optimal for short control messages.

Protocol Stack
The following figure depicts the protocol stack of Zig Bee



Physical Layer
The PHY layer of the reference model specifies the network interface components, their parameters, and their operation. To support the operation of the MAC layer, the PHYlayer includes a variety of features, such as

- Receiver energy detection (RED)
- Link quality indicator (LQI), and
- Clear channel assessment (CCA)

The PHY layer is also specified with a number of operational low-power features, including low-duty cycle operations, strict power management, and low transmission overhead.

MAC Layer
MAC layer handles network association and disassociation. It also regulates access to the medium; this is achieved through two modes of operation, namely beaconing and nonbeaconing.

The beaconing mode is specified for environments where control and data forwarding is achieved by an always active device.

The non beaconing mode specifies the use of unslotted, nonpersistent CSMA-based MAC protocol.

IEEE 802.15.4 standard defines three physical media

- Direct sequence spread spectrum (DSSS) using binary phase shift keying (BPSK), operating in the 868 MHz at a data rate of 20 Kbps;
- DSSS using BPSK, operating in the 915 MHz at a data rate of 40 Kbps; and
- DSSS using offset quadrature phase shift keying (O-QPSK), operating in the 2.4 GHz at a data rate of 140 Kbps.

Network Layer

- The network layer provides the functionality required to support network routing capabilities, configuration and device discovery, association and disassociation, topology management, MAC layer management, and routing and security management.

- Three network topologies, namely star, mesh, and cluster tree, are supported.

Security Layer

The security layer leverages the basic security services specified by the IEEE 802.15.4 security model to provide support for infrastructure security and application data security.

Application Layer

The application layer consists of the application support sublayer (APS), the ZigBee device object (ZDO), and the manufacturer-defined application objects.

The responsibilities of the APS sublayer include maintaining tables for binding devices together, based on their services and their needs, and forwarding messages between bound devices.

Other Features

Network and MAC layer consist of physical devices, namely a **full function device (FFD)** and a **reduced function device (RFD).**

There are three categories of logical devices:

- Network coordinator: An FFD device responsible for network establishment and control.

- Router : An FFD device that supports the data routing functionality, including acting as an intermediate device to link different components of the network and forwarding message between remote devices across multihop paths.

- End Devices : An RFD device that contains (just) enough functionality to communicate with its parent node, namely the network coordinator or a router. An end device does not have the capability to relay data messages to other end devices.

- A PAN coordinator is the designated principal controller of the WPAN. Every network has exactly one PAN coordinator.

Topology Supported

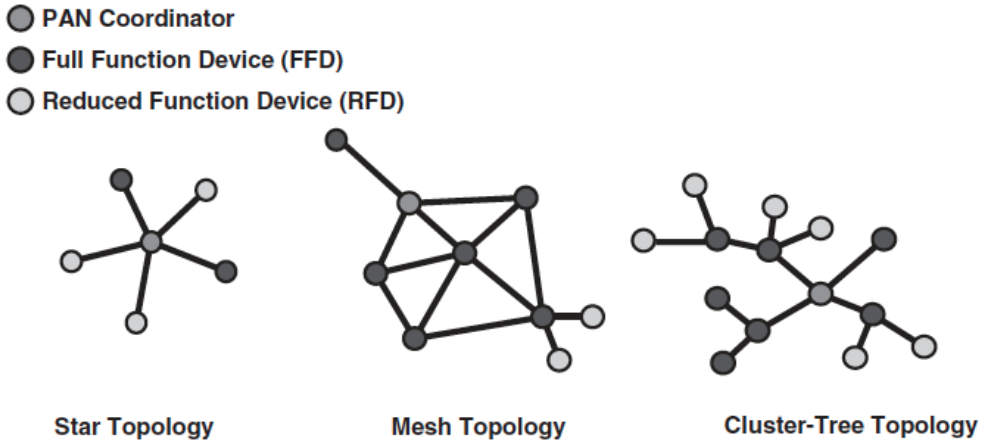
Based on these logical device types, a ZigBee WPAN can be organized into one of three possible topologies, namely a **star, a mesh (peer-to-peer), or a cluster tree**.

- The star network topology supports a single coordinator, with up to 65,536 devices. In this topology configuration, one of the FFD-type devices assumes the role of network coordinator. All other devices act as end devices.

- The mesh configuration allows path formation from any source device to any destination device, using tree- and table-driven routing algorithms.

- Cluster-tree networks enable a peer– peer network to be formed with a minimum of routing overhead, using multihop routing.

- The cluster can be rather large, comprising up to 255 clusters of up to 254 nodes each, for a total of 64,770 nodes.



Application Standards

- ZigBee Building Automation
- ZigBee Health Care
- ZigBee Home Automation
- ZigBee Input Device
- ZigBee Light Link
- ZigBee network devices (assist and expand ZigBee networks)
- ZigBee Remote Control (used for advanced RCs)
- ZigBee Retail Services (used for smarter shopping)
- ZigBee Smart Energy (SE) (used for home energy savings)
- ZigBee Telecom Services (used for value-added services)

RF4CE

Radio Frequency for Consumer Electronics (RF4CE)

ZigBee RF4CE protocol has been designed for simple, two-way device-to-device control applications that do not require the full-featured mesh networking capabilities offered by ZigBee 2007.

ZigBee RF4CE offers lower memory size requirements, thereby enabling lower cost

implementations. RF4CE is based on ZigBee and was standardized in 2009 by four consumer electronics (CE) companies: Sony, Philips, Panasonic, and Samsung.

The ZigBee RF4CE specification defines an RC network that defines a simple, robust, and low-cost communication network allowing wireless connectivity in applications for CE devices.

The ZigBee RF4CE specification enhances the IEEE 802.15.4 standard by providing a simple networking layer and standard application layer that can be used to create a multivendor interoperable solution for use within the home.

Some of the characteristics of ZigBee RF4CE include the following (16):

- Operation in the 2.4 GHz frequency band according to IEEE 802.15.4;
- Frequency agile solution operating over three channels;
- Incorporates power-saving mechanisms for all device classes;
- Discovery mechanism with full application confirmation;
- Pairing mechanism with full application confirmation;
- Multiple star topology with inter-PAN communication;
- Various transmission options including broadcast;
- Security key generation mechanism;
- Utilizes the industry standard AES-128 security scheme;
- Specifies a simple RC control profile for CE products;
- Support alliance-developed standards or manufacturer-specific profiles.

RF4CE's intended use is as a device RC system, for example for television settop boxes. The intention is that it overcomes the common problems associated with infrared (IR): interoperability, line-of-sight (LOS), and limited enhanced features.

At least wo-chip vendors supported RF4CE as of press time: Texas Instruments and Freescale Semiconductor, Inc.

Bluetooth

Bluetooth is a WPAN technology based on IEEE 802.15.1. It is a specification for short-range wireless connectivity for portable personal devices, including computer peripherals. It is now one of the most popular technologies in consumer electronics.

Bluetooth was initially developed by Ericsson; in the late 1990s, the Bluetooth Special Interest Group (SIG) made their specifications publicly available. Soon thereafter, the IEEE 802.15 Group took the Bluetooth work and developed a vendor-independent standard.

Bluetooth has evolved through five versions all versions of the Bluetooth standards maintain downward compatibility. Bluetooth is designed for a small variety of tasks, such as synchronization, voice headsets, cell-modem calls, and mouse and keyboard input

Bluetooth Versions

Bluetooth Version		Published Year	Description
Bluetooth v1	1.0 & 1.0B	1999	Original versions; had limited interoperability
	1.1	2002	This is original IEEE Standard 802.15.1
	1.2	2005	Ratified as IEEE Standard 802.15.1, enhancements compared with v1.1 including (i) faster connection and discovery; (ii) use of AFH spread spectrum; (iii) supports higher transmission speeds up to 721 Kbps; and (iv) adds flow control mechanisms
Bluetooth v2	2.0 + EDR (Enhanced Data Rate)	2004	Enhancements compared with v1.1 including faster data transfer of about 3 Mbps and lower power consumption
	2.1 + EDR	2007	Adds secure simple pairing (SSP), which improves the pairing process for Bluetooth devices while improving security; it also incorporates a subrating mechanism that reduces the power consumption in low-power mode
Bluetooth v3	3.0 + HS (High Speed)	2009	Data transfer speeds of up to 24 Mbps and data traffic carried over a collocated 802.11 link.(Wi-Fi). It adds alternate MAC/PHY (AMP) for the use of 802.11 as a HS transport.
Bluetooth v4	4.0 called Bluetooth Smart	2010	Classic Bluetooth, Bluetooth high speed, and BLE (Bluetooth Low Energy) protocols used. Bluetooth high speed is based on Wi-Fi and Classic Bluetooth consists of legacy Bluetooth protocols. Improvements include Generic Attribute Profile (GATT) and Security Manager (SM) services with AES Encryption.
	4.1	2013	Efficient data exchange and better co-existence with LTE frequencies, bulk data exchange rates.
	4.2	2014	Designed for the Internet of Things (IoT), Low Energy Secure Connection with Data Packet Length Extension (payload), Link Layer Privacy with Extended Scanner Filter Policies. 6LoWPAN is supported, which enables billions of devices to have a unique IPv6 address.
Bluetooth v5	5.0	2016	Improvements include double the speed (data rate) (2 Mbit/s burst) extended battery life, BT 5 increased the outdoor transmission range from 50 to 200 meters. Location services are enhanced. Increased message capacity. Dual Audio.
	5.1	2019	Angle of Arrival (AoA) and Angle of Departure (AoD) which are used for locating and tracking of devices Advertising Channel Index GATT Caching
	5.2	2020	Enhanced Attribute Protocol (EATT), an improved

			version of the Attribute Protocol (ATT), LE Power Control, LE Isochronous Channels, LE Audio
	5.3	2021	Connection Subrating, Periodic Advertisement Interval, Channel Classification Enhancement, Encryption Key Size Control Enhancements.

Bluetooth operates in the 2.4-GHz ISM band and has a bandwidth of approximately 1–5 Mbps. Bluetooth radios use a frequency-hopping spread spectrum, in full-duplex signal. Data transfer rate is upto 2 Mbps.

Bluetooth layers

The sublayers of IEEE 802.15 are as follows:
(i) RF layer;
(ii) baseband layer;
(iii) the link manager (an MAC-level protocol); and
(iv) the logical link control and adaptation protocol (L2CAP)

- **RF layer**: The air interface is based on antenna power range starting from 0 dBm up to 20 dBm, 2.4 GHz band, and the link range from 0.1 to 10 m.

- **Baseband layer**: The baseband layer establishes the Bluetooth piconet. The piconet is formed when two Bluetooth devices connect. In a piconet, one device acts as the master and the other devices act as slaves.

- **Link manager**: The link manager establishes the link between Bluetooth devices. Additional functions include security, negotiation of Baseband packet sizes, power mode and duty cycle control of the Bluetooth device, and the connection states of a Bluetooth device in a piconet.

- **L2CAP**: This sublayer provides the upper-layer protocols with connectionless and connection-oriented services. The services provided by this layer include protocol multiplexing capability, segmentation and reassembly of packets, and group abstractions.

Piconet and Scatternet

A Bluetooth device playing the role of "master" can communicate with up to seven devices playing the role of "slave" (these groups of up to eight devices are called **piconets**).

At any given instant in time, data can be transferred between the master and one slave; but the master switches rapidly from slave to slave in a round-robin fashion.

The Bluetooth specification also allows connecting two or more piconets together to form a **scatternet**, with some devices acting as a bridge by simultaneously playing the master role in one piconet and the slave role in another piconet.

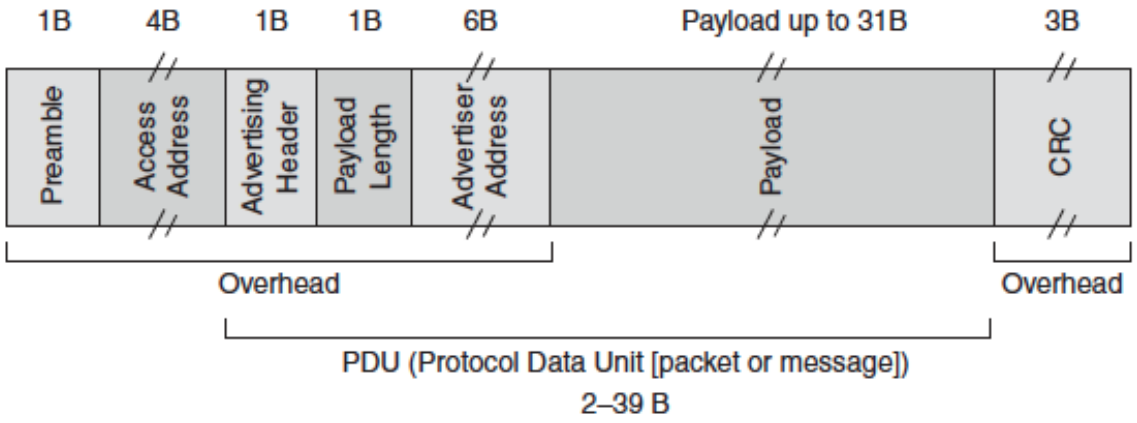
Bluetooth LE (Low Energy)

BLE (originally known as WiBree and/or Bluetooth ultra low power is a low-power subset to Bluetooth v4.0, with an entirely new protocol stack for rapidbuild-up of simple links. BLE is an alternative to the "power management" features that were introduced in Bluetooth v1.0 to v3.0 as part of the standard Bluetooth protocols.

BLE is aimed at very low-power applications running off a coin cell: it is capable of reporting data from a sensor for up to a year from a small button battery without recharging.

BLE sensor devices are typically required to operate for many years without needing a new battery; they commonly use a coin cell, for example, the popular CR2032. The aim of the BLE technology is to enable power-sensitive devices to be permanently connected to the Internet.

BLE per se is primarily aimed at mobile telephones, where it is envisaged that a star network topology, similar to Bluetooth, will often be created between the phone and an ecosystem of other devices.



BLE packet

Current chip designs allow for two types of implementation—dual mode and single mode.

- In a single-mode implementation, the BLE protocol stack is implemented solely.
- In a dual-mode implementation, BLE functionality is integrated into an existing Classic Bluetooth controller.

Bluetooth Health Device Profile

- Under Bluetooth, a profile defines the characteristics and features including function of a Bluetooth system.
- The HDP is used for connecting application data source devices such as blood pressure monitors, weight scales, glucose meters, thermometers, and pulse oximeters to application data sink devices such as mobile phones, laptops, desktop computers, and health appliances without the need for cables.

- This profile can be combined with BLE to make sure that medical devices can be in the operational conditions for many months and even years.

- HDP devices act as sinks and/or sources. A source is the small device that will act as the transmitter of the medical data (weight scale, glucose meter, thermometer, etc.).

- The sink is the feature-rich device that will act as the receiver of the medical data (mobile phone, desktop computer, health appliances, etc.).

- Other source devices such as pulse oximeter, EEG, or ECG transmit application data over a streaming data channel to a sink.

- This data can then be routed on to a physician through an alternate transport (e.g., the Internet or a mobile phone network) to a medical server application at a hospital.

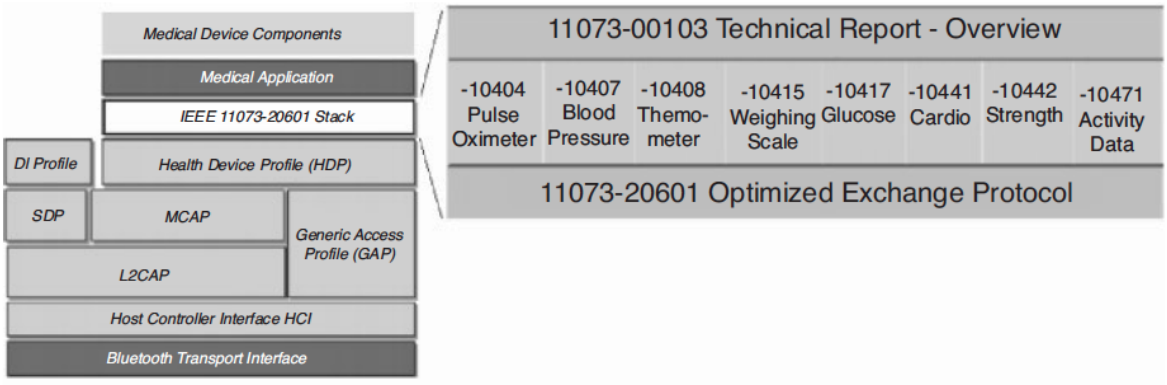


FIGURE 6.10 Bluetooth protocol and a HDP in a medical device application.

Cellular and Mobile Network Technologies for IoT/M2M

Universal Mobile Telecommunications System (UMTS)

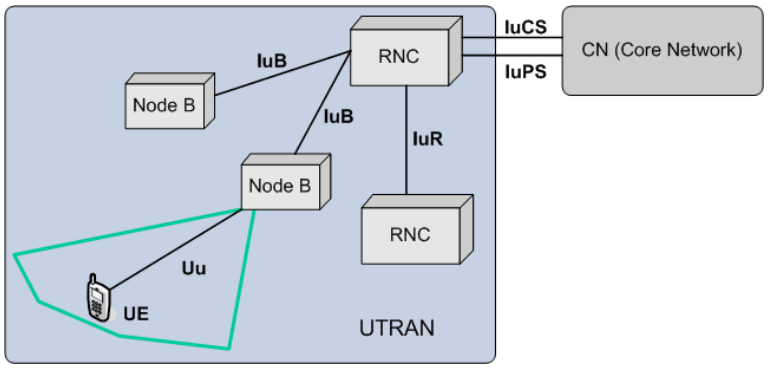
- UMTS is a 3G mobile cellular technology for networks supporting voice and data (IP) based on the GSM standard developed by the 3GPP (Third-Generation Partnership project).

- UMTS is a component of the ITU IMT-2000 standard set and is functionally comparable with the CDMA2000 standard set for networks based on the competing cdma One technology.

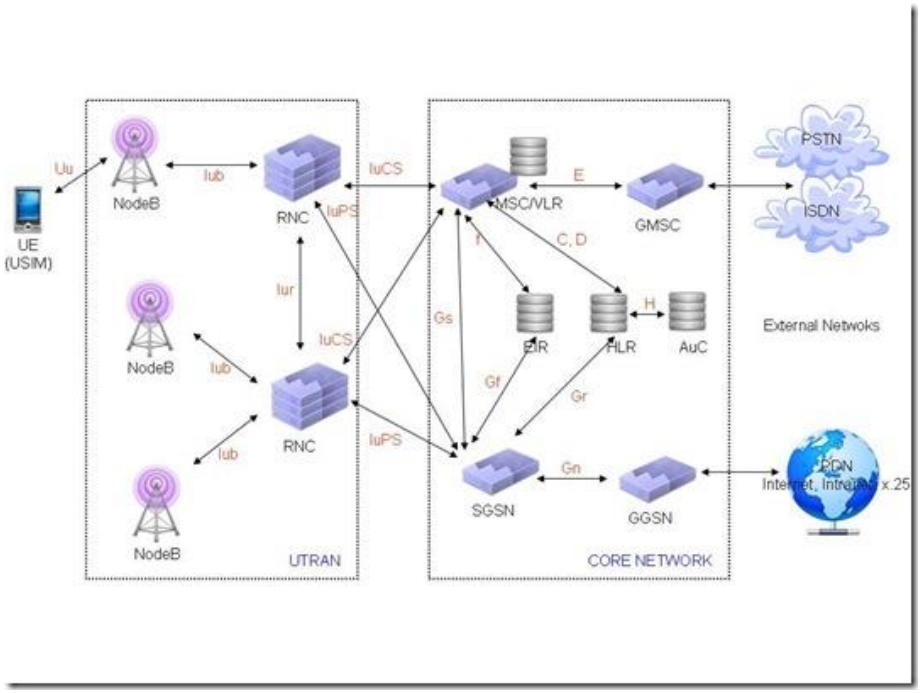
- UMTS can carry many traffic types from real-time circuit switched to IP-based packet switched.

- Universal terrestrial radio access network (UTRAN) is a collective term for the NodeBs (base stations) and radio network controllers (RNC) that comprise the UMTS RAN.

- NodeB is the equivalent to the base transceiver station (BTS) concept used in GSM. The UTRAN allows connectivity between the UE (User equipment) and the CN (Core network).



UMTS Architecture



Long Term Evolution (LTE)

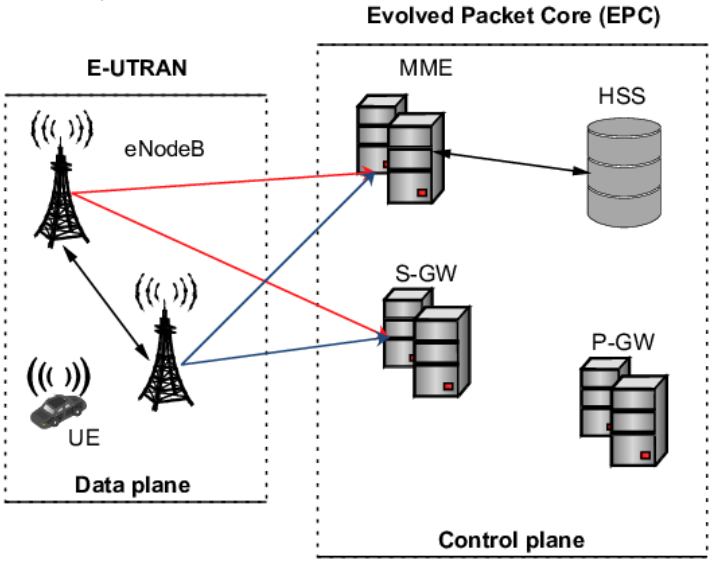
- LTE is the 3GPP initiative to evolve the UMTS technology toward a 4G.
- LTE can be viewed as an architecture framework and a set of ancillary mechanisms that aims at providing seamless IP connectivity between UE and the packet (IPv4, IPv6) data network without any disruption to the end-users' applications during mobility.
- In contrast to the circuit-switched model of previous-generation cellular systems, LTE has been designed to support only packet-switched services.

- System architecture evolution (SAE) is the corresponding evolution of the GPRS/3G packet CN evolution.
- The key element provided by LTE/SAE is the EPS (evolved packet system), that is, together LTE and SAE comprise the EPS.
- EPS provides the user with IP connectivity to a packet data network for accessing the Internet, as well as for supporting services such as streaming video.

The EPS consists of the:

- New air interface E-UTRAN (evolved UTRAN) and
- The evolved packet core (EPC) network

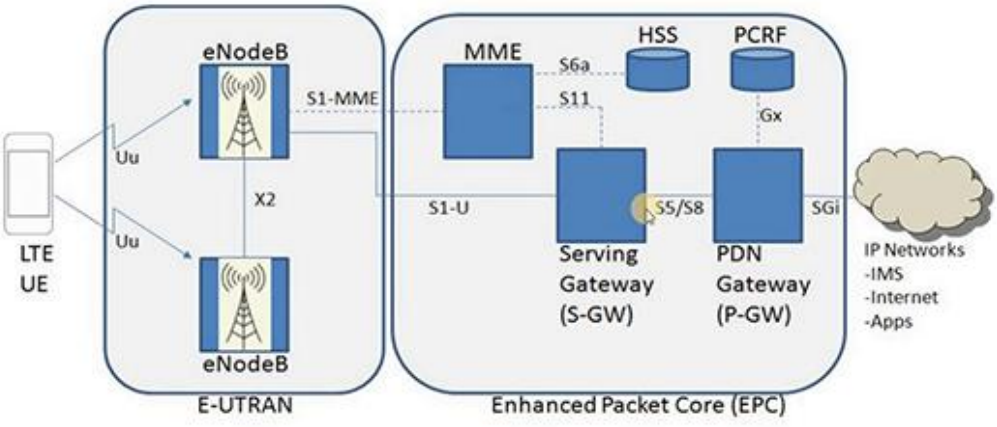
Hence, while the term "LTE" encompasses the evolution of the UMTS radio access through the E-UTRAN, it is accompanied by an evolution of the non-radio aspects under the term SAE, which includes, as just noted, the EPC network.



eNodeB: Evolved Node B
E-UTRAN: Evolved Universal Terrestrial Radio Access
HSS: Home Subscriber Server
UE: User Equipment
MME: Mobility Management Entity
P-GW: Packet data network GateWay
S-GW: Serving GateWay

In principle, LTE promises the following benefits:

- Simplified network architecture (Flat IP based);
- Efficient interworking;
- Robust QoS framework;
- Common evolution for multiple technologies;
- Real-time, interactive, low-latency true broadband;
- Multisession data;
- End-to-end enhanced QoS management (see below);
- Policy control and management;
- High level of security.



- The EPS uses the concept of bearers to route IP traffic from a gateway in the packet data network to the UE.
- A bearer is an IP packet flow with a defined QoS between the gateway and the UE.
- The E-UTRAN and EPC together set up and release bearers as required by applications.
- Multiple bearers can be established for an end-user in order to provide different QoS streams or connectivity to different packet data networks or applications reachable via that network.

Access Network

- The access network of LTE, E-UTRAN, consists of a network of eNodeB.
- The eNodeBs are normally interconnected with each other by means of an interface known as “X2” and to the EPC by means of the S1 interface.
- More specifically, to the MME by means of the S1–MME interface and to the S-GW by means of the S1–U interface.
- The protocols that run between the eNodeBs and the UE are known as the “AS protocols.” The E-UTRAN is responsible for all radio-related functions.

Core Network

- At a high level, the network is comprised of the CN (i.e., the EPC) and the access network E-UTRAN.
- While the CN consists of many logical nodes, the access network is comprised of essentially just one node, the evolved NodeB (eNodeB), which connects to the UE.
- The CN is responsible for the overall control of the UE and establishment of the bearers.

The main logical nodes of the CN are:

1. PDN gateway (P-GW);
2. Serving gateway (S-GW); and
3. Mobility management entity (MME)

- In addition to these nodes, the CN also includes other logical nodes and functions such as the Home Subscriber Server (HSS) and the Policy Control and Charging Rules Function

Evolution Paths to 4G/LTE

Mobile operators are evolving toward LTE/SAE using different evolution paths, as follows

- 3GPP environments: GSM, GPRS, EDGE, WCDMA, HSPA
- Non-3GPP environments: 1xRTT, EV-DO, 3xRTT, WLAN, WiMAX

Network element evolution from 2G/3G to LTE includes the following upgrades in the provider network:

- GERAN and UTRAN -> E-UTRAN
- SGSN/PDSN-FA ->S-GW
- GGSN/PDSN-HA ->PDN-GW
- HLR/AAA ->HSS
- VLR ->MME

In addition, the following signaling evolution from 2G/3G to LTE is needed:

- SS7-MAP/ANSI-41/RADIUS ->Diameter
- GTPc-v0 and v1 ->GTPc-v2
- MIP ->PMIP