IoT/M2M Area Network

國立交通大學資訊工程系
Department of Computer Science
National Chiao Tung University
September 28, 2018

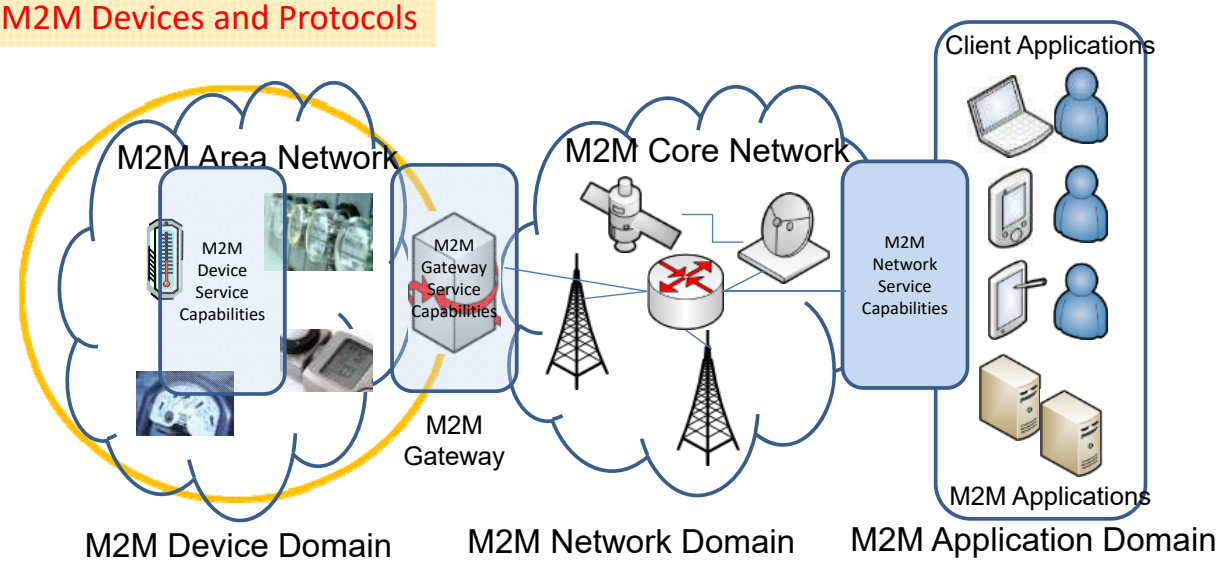
Outline

- Introduction to M2M Area Networks
- Example M2M Area Protocols
  - ANSI C12 Suite
  - Zigbee (IEEE 802.15.4)
  - Bluetooth Low Energy (BLE)
- Appendix (IoT Devices)

INTRODUCTION TO M2M AREA NETWORKS

M2M Area Networks

M2M Devices and Protocols



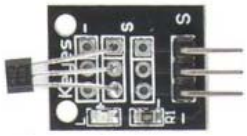
IoT/M2M Area Network

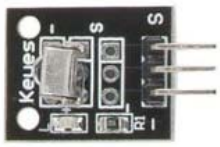
- IoT/M2M Sensors and Devices
  - Under fast development!
- IoT/M2M Area Network Protocols
  - **ANSI C12 Suite**
  - **Zigbee (IEEE 802.15.4)**
  - **Bluetooth Low Energy (BLE)**
  - WiFi
  - Power Line Communication
  - BACnet
  - KNX
  - **6LoWPAN/RPL/CoAP**
  - Etc.

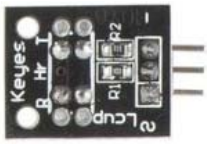
Catalog of IoT/M2M Sensors (1)

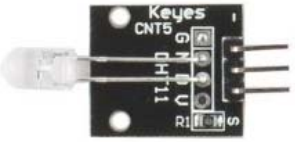
- Embedded in Smart Phones
  - Accelerometer : Measure the three-axis acceleration
  - Magnetic : Measure the magnetic potential vector
  - Orientation : Measure the direction
  - Gyroscope : Measure the orientation, based on angular momentum
  - Temperature :Measure the temperature
  - Light: Measure the luminosity
  - Pressure : Measure the pressure
  - Proximity : Measure whether any object is closing
  - GPS : Positioning the current latitude and longitude
  - NFC : Allow smartphones to transfer data to each other within 10 cm
  - Etc.

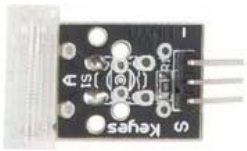
Catalog of IoT/M2M Sensors (2)


Analogy-hall sensor

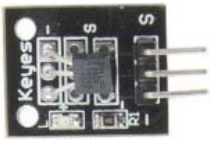

Infrared-receiver

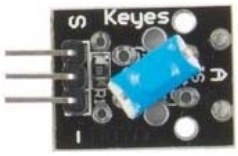

Light break sensor


Colorful Auto-flash

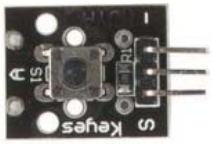

Knock sensor


Passive buzzer

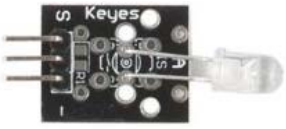

18B20 Temperature Sensor


Tilt-Switch

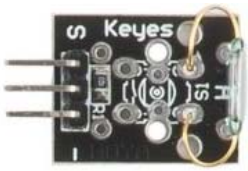

Laser-transmit


Push button

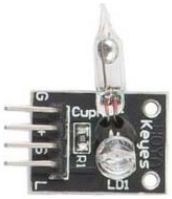

Active buzzer

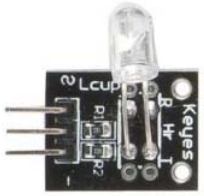

Infrared-transmitter

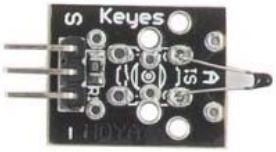
Catalog of IoT/M2M Sensors (3)

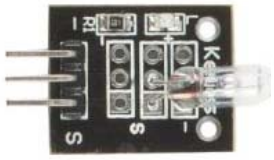

Magnet-ring sensor


Rotate-encode


Magic-ring


Finger-Pulse sensor


Analog-temperature sensor


Hydrargyrum-switch sensor


Two-color Common Cathode (陰極) LED

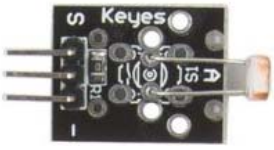
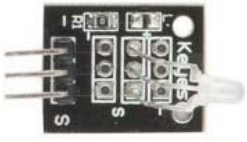
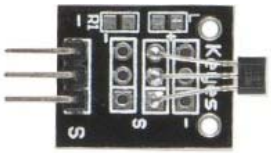
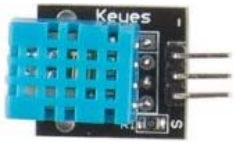


Photo resistor sensor


Common-Cathode Red & Green LED


Hall sensor


Humiture sensor


Shock-switch sensor

Catalog of IoT/M2M Sensors (4)

Obstacle avoidance sensor

Line Tracking sensor

Metal touch sensor

Microphone sensor

Digital-Temperature sensor

Flame sensor

Linear-Hall sensor

High-Sensitive voice sensor

Magnetic spring

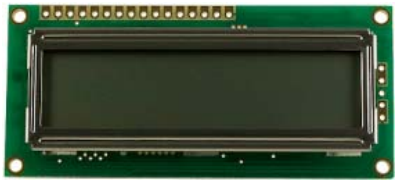
Catalog of IoT/M2M Sensors (5)

Ultrasound Sensor

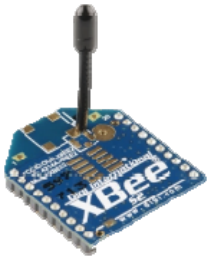
Graphic LCD 5110

Gas sensor

PIR* sensor
*Passive infrared



16 pin LCD module



Xbee S2 wire antenna

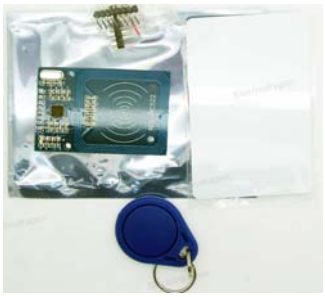
9 gram Plastic Servo Motor
(伺服馬達)

Catalog of IoT/M2M Sensors (6)

Relay module

Joystick PS2

LED Digitial Indicator



RFID
Card-Reader-Detector
Module

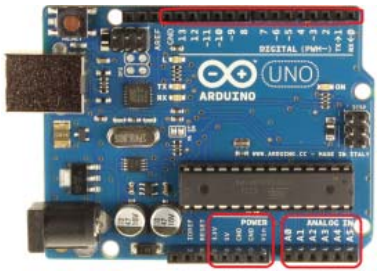
Water level sensor

Stepper motor
(步進馬達)

Category of Sensor Platforms

Mediatek Linkit

Raspberry Pi



Arduino UNO

Intel Edison

NXP JN516x-EK001

Intel Galileo

Catalog of IoT/M2M Devices

- Type of IoT/M2M Devices
  - Smartphone
  - IP camera
  - Robot
  - Smart Bulb
  - E-Lock
  - Thermostat
  - Smart Watch
  - Activity Tracker
  - Healthcare
  - Etc.


Jawbone UP24


Dropcam


iPhone


Parrot Ar. Drone


Sony Smart Watch


WowWee Rovio


Kwikset Kevo E-Lock


Philips Hue Smart Bulb


iRobot Roomba 830


Bluetooth Blood Pressure Monitor

NEST

Honeywell Lyric Thermostat

Catalog of M2M Area Network Protocols (1)

- CoAP/6LoWPAN/RPL
- RFID
- **Bluetooth Low Energy**
- WiFi
- **Zigbee (based on IEEE 802.15.4)**
- Zigbee Smart Energy 2.0
- M-Bus – Utility metering
- **ANSI C12 – Electricity metering**
- KNX – HVAC, lighting and building automation

Catalog of M2M Area Network Protocols (2)

- LonWorks – Control and automation
- ModBus – Industry automation and metering
- Power Line Communications
- BACnet – Building automation and control
- Insteon – Smart Home
- DLMS/COSEM - Multi utility metering
- Z-Wave – Home automation
- Dali – Lighting control
- X10 - Home automation
- DLNA/UPnP – home multimedia sharing
- Etc.

EXAMPLE M2M AREA PROTOCOLS

C12.19
C12.18
C12.21
C12.22
RFC 6142

ANSI C12 SUITE

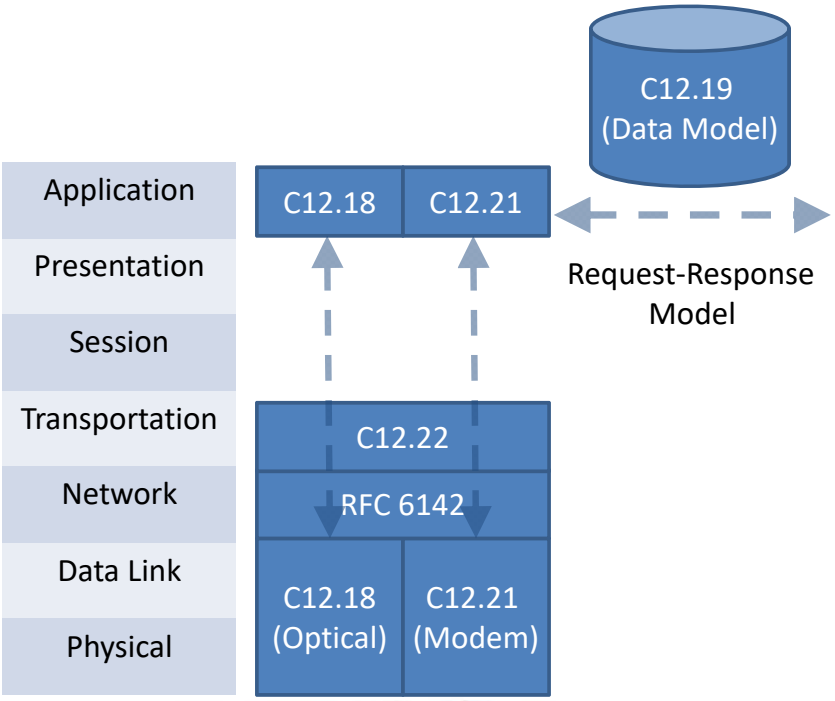
ANSI C12 Suite

- Provide an interoperable solution for data formats, data structures, and communication protocols used in Automatic Metering Infrastructure (AMI) projects and specified by the American National Standards Institute (ANSI).
  - C12.01: Code for Electricity Metering
  - C12.10: Physical Aspects of Watthour Meters – Safety Standard
  - C12.18: Protocol Specification for ANSI Type 2 Optical Port
  - C12.19: American National Standard for Utility Industry End Device Data Tables
  - C12.20: Electricity Meters – 0.2 and 0.5 Accuracy Classes
  - C12.21: Protocol Specification for Telephone Modem Communication
  - C12.22: Protocol Specification for Interfacing to Data Communication Networks
  - RFC 6142: ANSI C12.22, IEEE 1703, and MC12.22 Transport over IP

A Brief History

- C12.19 (1990s published ,2007 revised)
  - The standard data structure is specified in the ANSI C12.19 document.
- C12.18 (First release published in 1996 then revised in 2006)
  - The first standardized protocol that was specified to interact with ANSI C12.19 Data Tables
  - Define the communications between a C12.18 meter and a C12.18 client by means of an optical port
- C12.21 (1999)
  - Specify the communications between a C12 device and C12 client via a modem
  - The first solution for AMI projects
- C12.22 (2007)
  - Allow interactions with C12.19 table data over any networking communications system
- RFC 6142 (2011)
  - Propose a framework for transporting ANSI C12.22 Application Layer messages on an IP network

Network Protocol Stack



C12.19: The Data Model

- Defines a data structure for representing metering data and metering functions exposed by a metering equipment to a client machine.
  - The data structure is defined as a set of standard tables.
  - Besides standard tables, C12.19 also provides a standard way to add proprietary tables called manufacturer tables.
- Does not contain any protocol for the transport of the data.

Decade

- Tables that share a common purpose or are relative to a common feature are called a “decade”.
  - There are 17 decades in the version published in 2007.

Decade number	Name of the Decade	# of Tables in the Decade	Decade number	Name of the Decade	# of Tables in the Decade	Decade number	Name of the Decade	# of Tables in the Decade
0	Configuration Tables	9	6	Load Profile Tables	8	12	Network Control Tables	Defined in ANSI C12.22
1	Data Source Tables	9	7	History & Events Logs	10	13	Relay Control Tables	Defined in ANSI C12.22
2	Register Tables	9	8	User-Defined Tables	10	14	Extended User Defined Tables	4
3	Local Display Tables	5	9	Telephone Control Tables	9	15	Quality of Service Tables	9
4	Security Tables	7	10	Extended Source Tables	4	16	One-Way Tables	5
5	Time-of-Use Tables	7	11	Load Control & Pricing Tables	9			

Read/Write Services

- The read service request allows the transfer of table data from a sending party to a receiving party.
  - Full table read: specified by Table_Identifier
  - Partial table read
    - Index-based: specified by up to 5 indexes and optionally an element count
    - Offset-based: specified by an offset and optionally a count
- The write service allows nonsolicited data to be sent to a receiving party.
  - Support both full and partial table write

Three Remarkable Tables in Decade 0

- Table 00 (GEN_CONFIG_TBL)
  - The information related to the configuration of the end device
  - E.g., the list of supported tables and procedures
- Table 07 and Table 08 are designed for enabling the execution of commands
  - Procedure Initiate Table: an initiator writes parameters in the Table 07 to execute a command in a meter
  - Procedure Response Table: the result is placed in Table 08 to be read by the initiator
  - No buffering: only one command at a time

    "If a procedure initiate request is followed by another procedure initiate request, the procedure response for the first procedure initiate request may be lost."

C12.18: Basic Point-to-Point Communication over an Optical Port

- The communications between an electric metering equipment and another client device via an optical port
  - The first standardized protocol that was specified to interact with ANSI C12.19 Data Tables
  - Focuses on the physical, data link and application layers
- Three main functionalities
  - Modification of the communication channel;
  - Transport of information to and from the metering device;
  - Closure of the communication channel when communications are complete.

Protocol Specifications for Electric Metering (PSEM)

- The application layer defines the PSEM language
  - Provide basic services for channel configuration and information retrieval
  - Use request–response scheme
- Provides settings for Layer-2 and Layer-1 establishment
  - E.g., baud rate, number of packets, packet size channel traffic time-out, data type, data format and data polarity
- Nine services are defined in PSEM, including
  1. Identification service
  2. Read service
  3. Write service
  4. Logon service
  5. Security service
  6. Logoff service
  7. Negotiate service
  8. Wait service
  9. Terminate service

C12.21: An Extension of C12.18 for Modem Communication

- Allows remote interactions with ANSI C12.19 tables over a telephone network.
- The three main functional areas specified in the C12.18 are not modified.
- Instead of 9 services specified in the C12.18, the PSEM provides 12 services.
  - 7 services are identical: read, write, logon, security, logoff, negotiate, wait.
  - 2 services are modified: identification and terminate.
  - 3 new services are provided: timing setup, disconnect, and authenticate.

Interactions with the Data-Link Layer

- The communication channel of the modem is established with a set of default parameters.
- After calling the identification service and before calling the logon service, the service layer can
  - Call either the negotiate service or the Timing_ Setup service
  - Modify packet size, packet number for reassembly, timers, or retry attempts number.

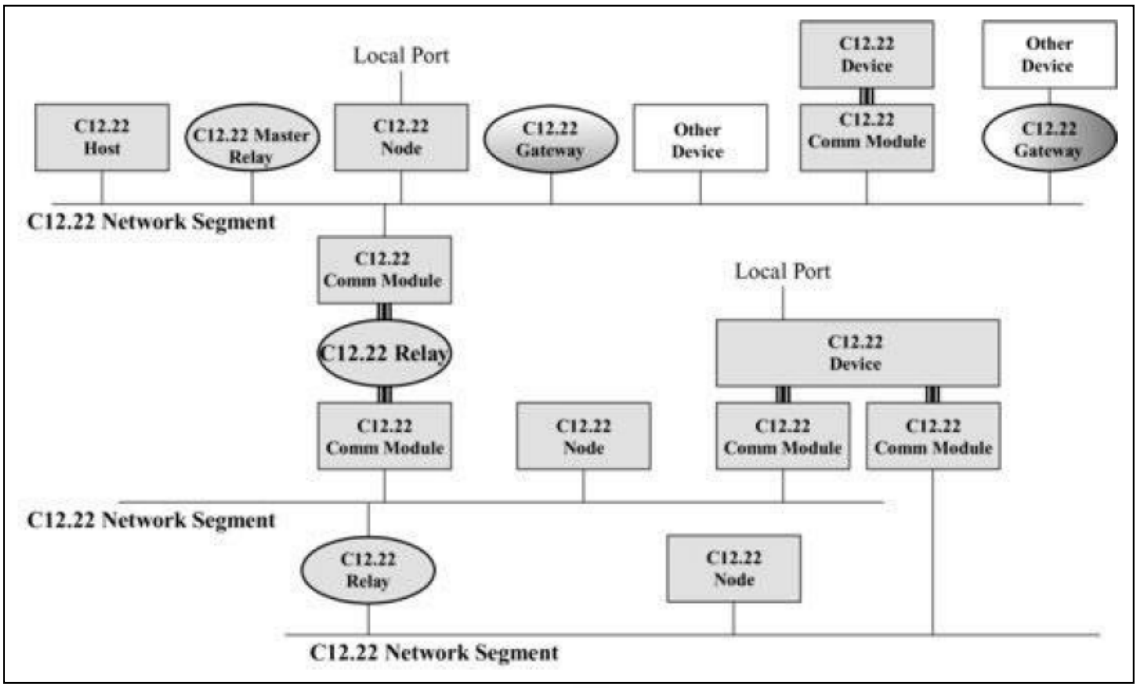
Modifications and Additions to C12.19 Tables

- The most significant changes to C12.19 tables includes
  - The Procedure Initiate Table (Table 07) was modified to add a new standard procedure in order to trigger an immediate call establishment with a phone number specified as a procedure parameter
  - A new decade (no. 9) that contains 7 new tables associated with the use of a telephone modem.

C12.22: Enable Transportation over any Networking Communication System

- Defines several types of network elements that are used in a reference topology
- Describes interfaces between different types of network elements
- New data tables are added and some existing tables are also modified

C12.22 Reference Topology



Source: ANSI C12.22, Chapter 5, Figure 5.1; *The Internet of Things*

Network Elements in C12.22 (1/2)

- C12.22 Host: this is a termination point in a C12.22 network. It may be an authentication host or/and notification host.
- C12.22 Device: this is a network element that contains a C12.22 application.
- C12.22 Communication Module: this is a hardware device that allows communications between a C12.22 Device and a C12.22 network.
- C12.22 Node: it is a combined C12.22 communication-module/device network element.

Network Elements in C12.22 (2/2)

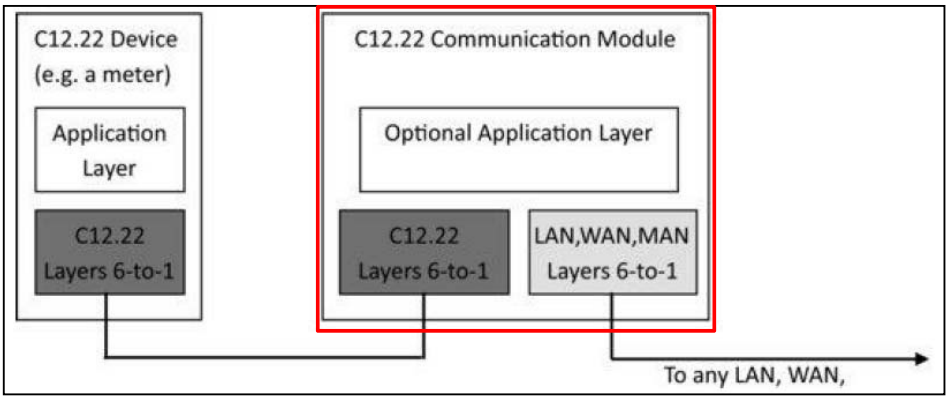
- C12.22 Master Relay:
- C12.22 Relay:
  - This layer 7 address is called ApTitle (application process title)
- C12.22 Gateway: this is a protocol converter from the C12.22 protocol to any other protocol.

C12.22 Node to C12.22 Network Communications

- The protocol stack between a C12.22 node and a C12.22 network is only defined at layer 7.
- The new version of the PSEM protocol contains 13 services:
  - Three services are unchanged: the read, write and security services.
  - Six services are modified (compared to C12.21): identification, logon, logoff, terminate, disconnect, and wait services.
  - Four new services are provided: registration, deregistration, resolve, and trace services.
- The extended PSEM (EPSEM) is specified to allow sending multiple requests and receiving multiple responses simultaneously.
- C12.22 security mechanism supports both authentication and encryption

C12.22 Communication Module

- The concept of C12.22 communication modules is introduced to model the communication ports of C12.22 meters.
  - Connects to the C12.22 Device through an interface defined in the C12.22 standard.
  - Connects to any LAN (e.g., ZigBee, …), WAN (DSL, GPRS, …), or MAN (Ethernet, …).



Source: The Internet of Things, Chapter 10, Figure 10.1.

C12.22 Protocol Stack and Services

Layer 7 : same as Node Layer 7
Layer 6 : empty
Layer 5 : empty
Layer 4 : Transport Layer Services
Layer 3 : empty
Layer 2 : 8 asynchronous data bits, 1 start bit, 1 stop bit, 1 start of packet character, CRC at end of packet
Layer 1 : 6-pins RJ11 Jack

Transport Layer Service

- Negotiate service
- Get-Configuration service
- Link-Control service
- Send-Message service
- Get-Status service
- Get-Registration-Status service

Source: The Internet of Things, Chapter 10, Figure 10.3.

C12.19 Updates

- Decade 12 “Node Network Control Tables” is added, modeling the C12.22 node access to a C12.22 network
- Decade 13 “Relay Control Tables” is added, related with the management of a C12.22 relay.
- The content of the Procedure Initiate Table is augmented with 4 new procedures (Registration, Deregistration, Network Interface Control, and Exception Report), related to the newly added Decade 12

RFC 6142: C12.22 Transport Over an IP Network

- Transport C12.22 messages by using TCP and UDP transports over an IP network.
  - Specifies an encoding for the native IP address in the appropriate fields of ANSI C12.19 Tables.
    - IPv4 and IPv6 are two possible options.
  - Port number 1153 was assigned by *IANA** for both TCP and UDP.
- Since C12.22 has its own security mechanism, transport layer security is not mandated. RFC 6142 allows the use of a transport layer security mechanism as an enhancement.

*IANA: Internet Assigned Number Authority

RFC 6142: C12.22 Transport Over an IP Network (Cont.)

- To facilitate the reading of numerous C12.22 meters, the support of IP multicast is required in all C12.22 hosts, relays and master relays and recommended in the C12.22 nodes.
  - Meters with a common C12.22 multicast group ApTitle can be reached by sending a single EPSEM read request.
  - 224.0.2.4 for IPv4 and FF0X::24 for IPv6 have been assigned by IANA to a newly created “All C1222 Nodes” multicast group.
  - TTL (Time To Live) attribute in an IP packet header is used to limiting the propagation of C12.22 IP multicast messages.

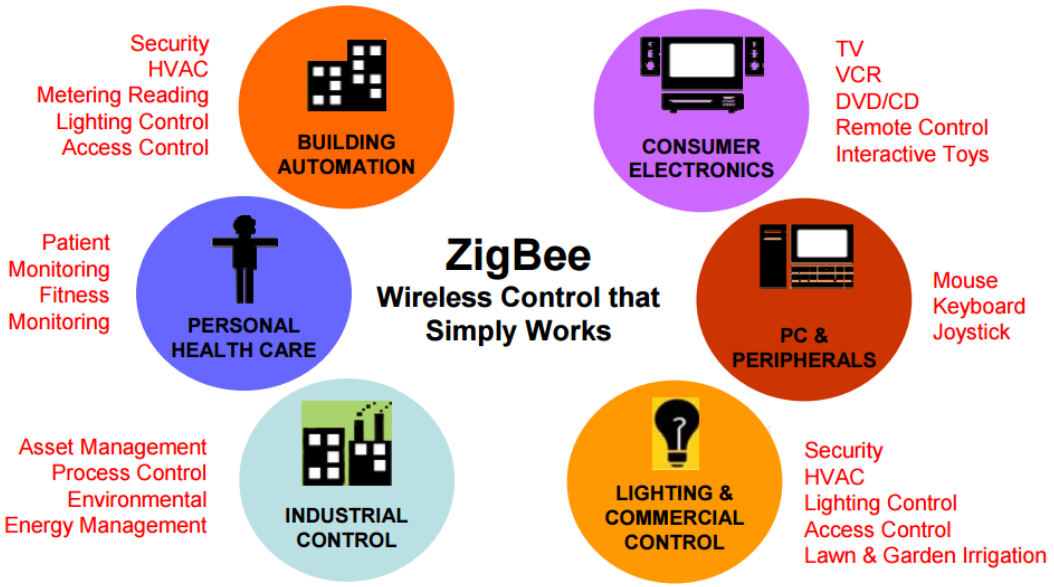
ZIGBEE

ZigBee®
Control your world

ZigBee

- ZigBee is a standardized wireless protocol for personal area networking, or “WPAN.”
- The protocol is the work and property of the ZigBee Alliance, a consortium that creates and promotes this WPAN standard
- Zigbee is built on IEEE 802.15.4 standard that defines physical (PHY) and Medium Access Control (MAC) layers of a WPAN.
- The ZigBee Alliance defines Network (NWK) and Application (APL) layer specifications to complete what is called the ZigBee stack.
- Designed for low cost, low power, low data rate, low duty cycle wireless connectivity.

ZigBee Applications



Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

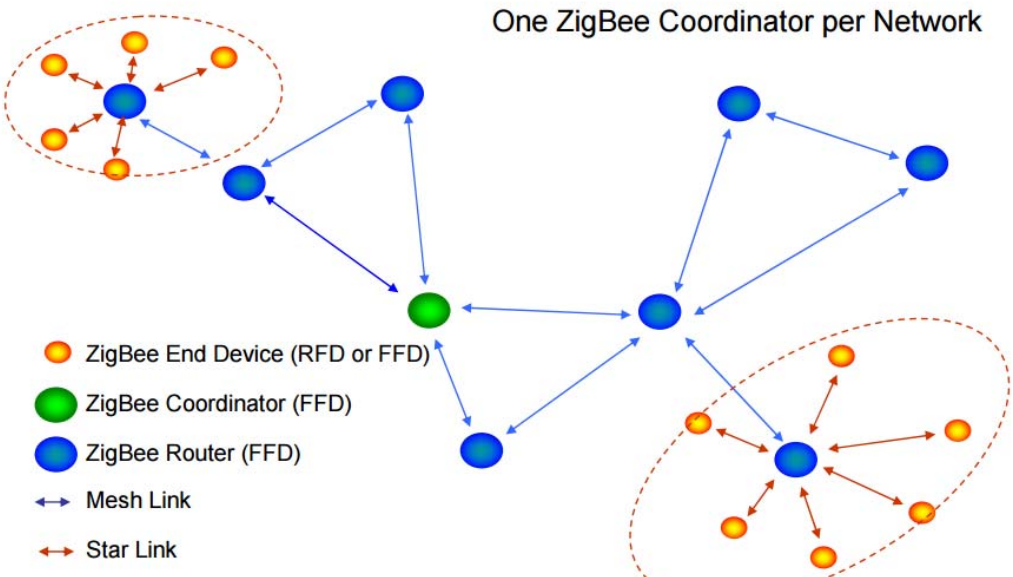
ZigBee Market Goals

- Global band operation, 2.4 GHz unlicensed band or one of the 900MHz regional bands
- Unrestricted geographic use
- RF penetration through walls and ceilings
- Automatic or semi-automatic installation
- Easy to add or remove devices
- Low cost

ZigBee Technical Specs

- Data throughput: 10 kbps to 115 kbps
- Range: 10 to 75 m coverage
- Scalability: Up to 100 collocated networks
- Low power: Up to 2 years of battery life on standard alkaline batteries

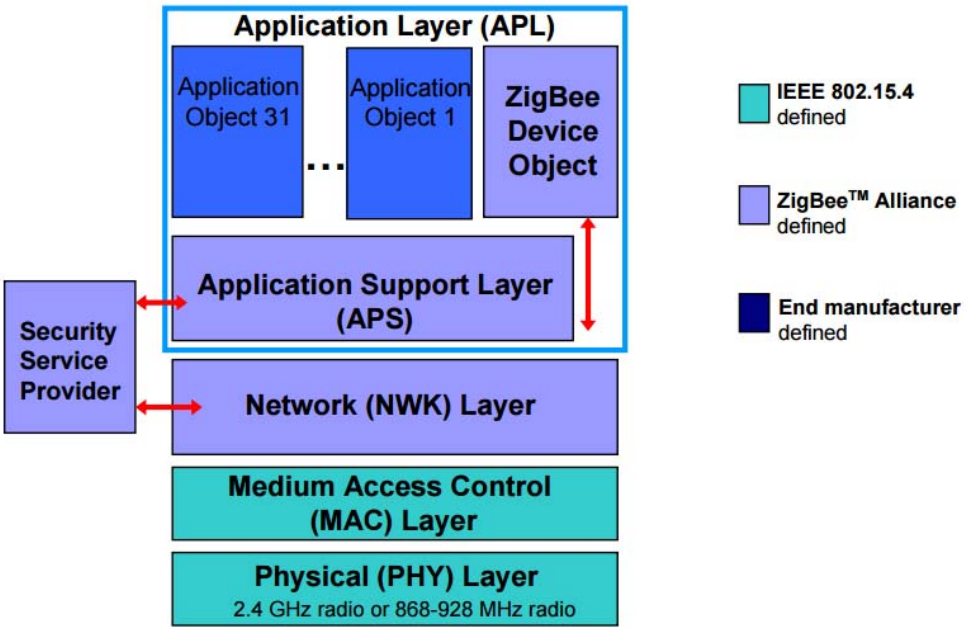
Zigbee Network Models



RFD: Reduced Function Device
FFD: Full Function Device
Coordinator: A full function device that manages the network.

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

Zigbee Protocol Stack



Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

IEEE 802.15.4 Standard Basics

- CSMA (Carrier Sense Multiple Access) channel access with collision avoidance and optional time slotting
- Three bands, 27 channels specified
  - 2.4 GHz: 16 channels, 250 kbps
  - 868.3 MHz : 1 channel, 20 kbps
  - 902-928 MHz: 10 channels, 40 kbps
- Message acknowledgment for improved data delivery reliability
- Beacon structures to improve latency.
- Multi-level security
- Designed for monitoring and control applications where battery life is important. 802.15.4 is the source of ZigBee's excellent battery life.

IEEE 802.15.4 MAC Features

- Employs 64-bit IEEE & 16-bit short addresses
  - Ultimate network size can be 2^{64} nodes (more than probably needed)
  - Using local addressing, simple networks of more than 65,000 (2^{16}) nodes can be configured, with reduced address overhead
- Simple frame structure
- Reliable delivery of data
- Supports AES-128 security
- Employs CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) channel access for better coexistence
- Offers optional superframe structure for improved latency

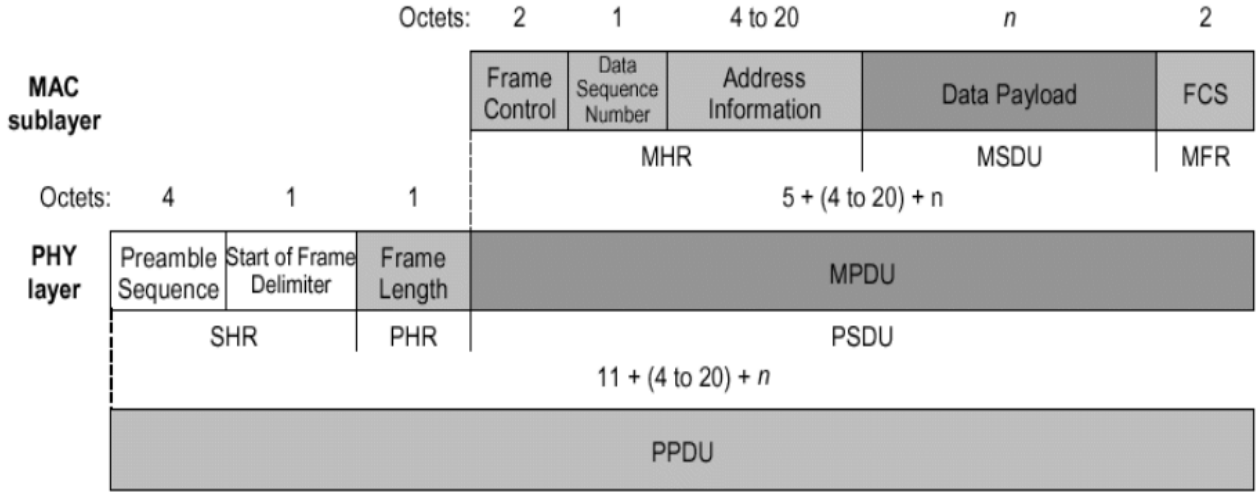
IEEE 802.15.4 MAC Options

- Non-beacon network
  - Standard ALOHA CSMA-CA communications
  - Positive acknowledgment for successfully received packets
- Optional beacon-enabled network
  - Superframe structure
    - For dedicated bandwidth and low latency
    - Set up by network coordinator to transmit beacons at predetermined intervals
      - » 15ms to 252sec (15.38ms ∗ 2n where 0 ≤ n ≤ 14)
      - » 16 equal-width time slots between beacons
      - » Channel access in each time slot is contention free

IEEE 802.15.4 Device Types

- Network Coordinator
  - Maintains overall network knowledge; most sophisticated of the three types; requires most memory and computing power
- Full Function Device (FFD)
  - Carries full 802.15.4 functionality and all features specified by the standard
  - Additional memory, computing power make it ideal for a network router function
  - Could also be used in network edge devices where the network touches other networks or devices that are not IEEE 802.15.4 compliant
- Reduced Function Device (RFD)
  - Carriers limited (as specified by the standard) functionality to control cost and complexity
  - General usage will be in network edge devices

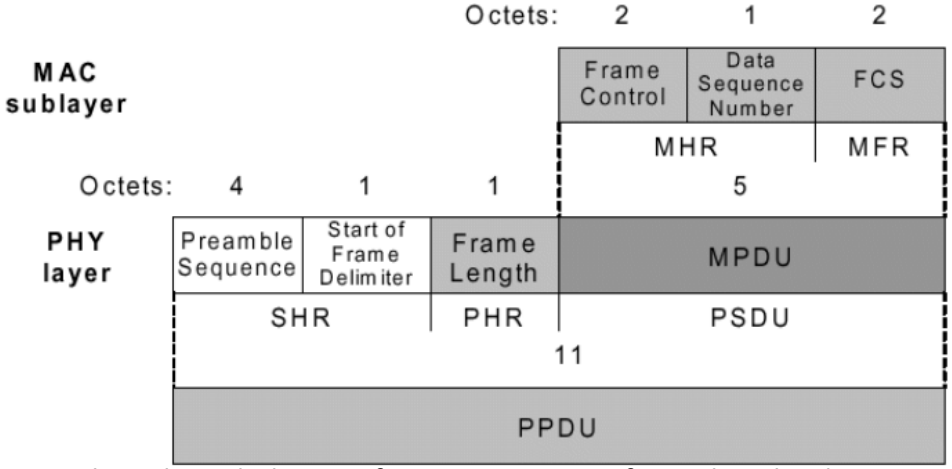
802.15.4 Data Frame Packet



- Provides up to 104 byte data payload capacity
- PHY Service Data Unit (PSDU) is a maximum of 127 bytes in length
- Data sequence numbering ensures that packets are tracked
- Robust structure improves reception in difficult conditions
- Frame Check Sequence (FCS) validates error-free data

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

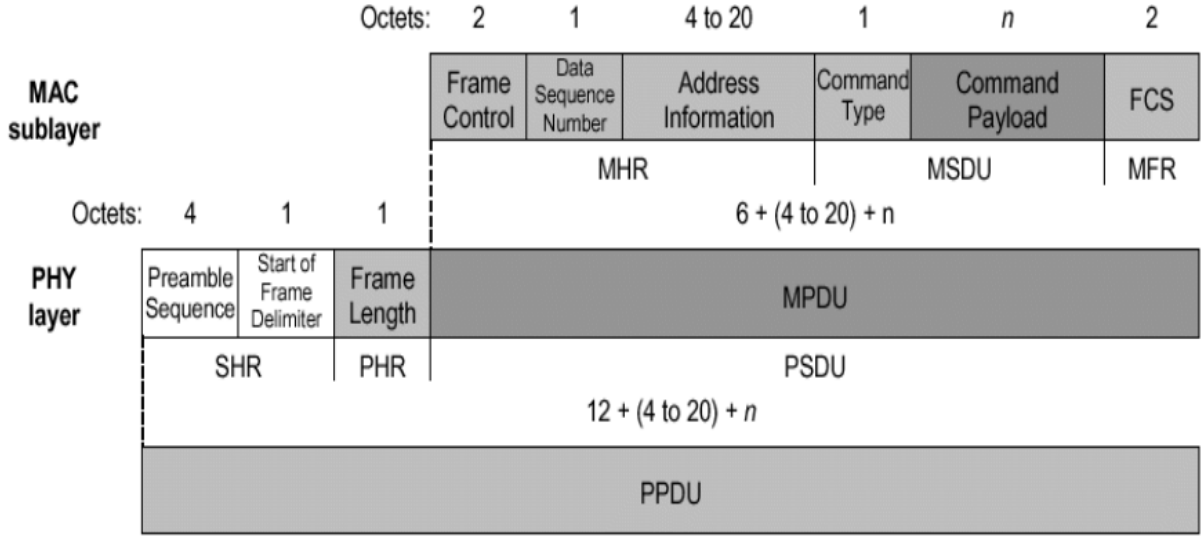
802.15.4 Acknowledgment Frame Format



- The acknowledgment frame, or ACK, confirms that the data is received successfully.
- Frame control and Data sequence are taken from the original packet.
- A transmission is considered successful if the ACK frame contains the same sequence number as the transmitted frame.

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

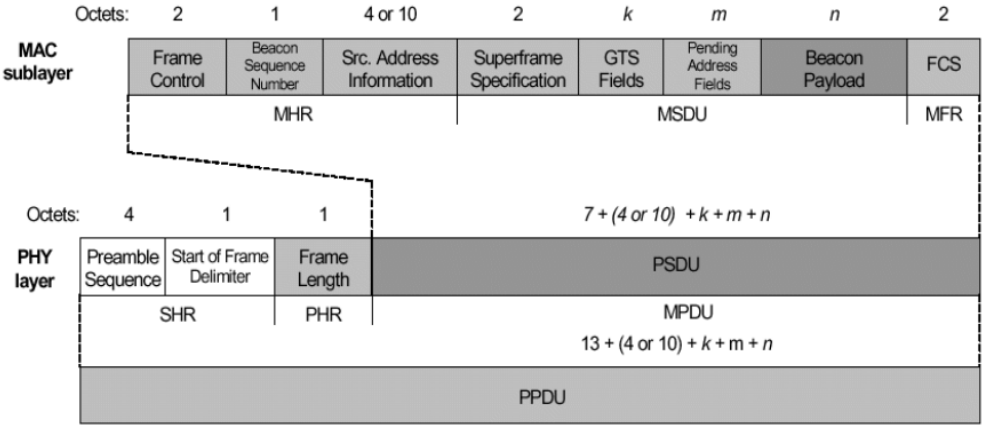
802.15.4 Command Frame Format



The command frame is used for remote control. Instead of data as the payload, this frame contains command information. A command type byte is added as well. The MPDU must still be 127 bytes or less as with the Data frame.

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

802.15.4 Beacon Frame Format



- The beacon frame is much more complex as it must convey the synchronization and guaranteed time slot (GTS) information to all of the devices in the network.
- Beacons add a new level of functionality to a network. Client devices can wake up only when a beacon is to be broadcast, listen for their address, and if hear nothing, return to sleep.
- Beacons are important for mesh and cluster tree networks to keep all of the nodes synchronized without requiring nodes to consume precious battery energy listening for long periods of time.

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

ZigBee Architecture Objectives

- Support all target environments and applications that are in the scope of ZigBee:
  - Ensure that devices are efficient in their use of the available bandwidth
- Provide a platform and implementation for wirelessly networked devices:
  - Make it easy to design and develop ZigBee devices
  - Reduce today's cost of building wireless solutions
- Ensure interoperability through the definition of application profiles
  - Enable out-of-the-box interoperable devices where desired by manufacturers
- Define the ZigBee network and stack models
  - Define ZigBee device types and core functions
  - Define layers and modules with their interfaces, and services
- Provide the framework to allow a separation of concerns for the specification, design, and implementation of ZigBee devices
  - Help to create and coordinate consistent use of terms in ZigBee
- Allow future extension of ZigBee
  - Enable both extension of the basic ZigBee platform as well as ZigBee application profiles

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

Wireless Networking Basics

- **Network scan**: the ability of a device to detect active channels within its communications range. This range is often called, in personal area networking, the Personal Operating Space (POS).
- **Creating/Joining a PAN**: the ability to form a network on unused channels within the POS. In the case of ZigBee, the network is a PAN. Joining is the ability to join a network within the POS.
- **Device discovery**: the ability to identify the devices on active channels in the PAN.
- **Service discovery**: the ability to determine what features or services are supported on devices within a network.
- **Binding**: the ability to communicate at the application level with other devices in the network.

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

Zigbee Networking Assumptions

- Devices are pre-programmed for their network function:
  - Coordinator scans to find an unused channel to start a network.
  - Router (mesh device within a network) scans to find an active channel to join, then permits other devices to join.
  - End device will always try to join an existing network.
- Devices discover other devices in the network providing complementary services:
  - Service discovery can be initiated from any device within the network or performed via Gateways from devices outside the network
- Devices can be bound to other devices offering complementary services:
  - Binding provides a command and control feature for specially identified sets of devices.

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

Zigbee Routing Architecture

Star Network	Cluster Tree	Mesh Network Routing
• Supports a single ZigBee coordinator with one or more ZigBee end devices (up to 65,536 in theory)	• Permits "netmask" style message routing down or up the tree based on the destination address	• Employs a simplified version of Ad Hoc On Demand Distance Vector Routing (AODV). This is an Internet Engineering Task Force (IETF) Mobile Ad Hoc Networking (MANET) submission • Flooding is used to determine paths from source to destination in the mesh • Route Replies determine viable paths in the mesh • Routing tables record known paths.

- Star Network - one coordinator networked with one or more end devices
- Cluster Tree - where devices branch off of a tree, the network backbone.
- Mesh network - Routing paths are not as constrained as in the cluster tree topology. Mesh networking permits path formation from any source to any destination device.

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

Application Support Features

- Profile: Profiles are used to define a device's application capability and drive the application details. An example of a profile would be Home Control—Lighting.
- Endpoint: Endpoints are the physical dimensions added to a ZigBee device which permit multiple application support, addressed by the Endpoint number (0-31).
- Interface: Interfaces are defined per endpoint and allow such things as extra proprietary capability extensions and backward compatibility.
- Key Relationships:
  - Maximum of 30 Endpoints per ZigBee device (0 is reserved to describe the device itself and 31 is reserved for broadcast messaging to all endpoints)
  - Maximum of 8 Interfaces per Endpoint
  - One Profile described per Interface

Source: https://www.nxp.com/files/training_pdf/28081_ZIGBEE_OVERVIEW_WBT.pdf

BLUETOOTH LOW ENERGY

Bluetooth SMART

Bluetooth Low Energy (BLE)

- Bluetooth is a wireless technology standard for building personal area networks (PANs).
- It is based on short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz for fixed and mobile devices.
- Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables.
- Bluetooth Low Energy (BLE) is a light-weight subset of classic Bluetooth and was introduced as part of the Bluetooth 4.0 core specification.
- While there is some overlap with classic Bluetooth, BLE actually has a completely different lineage and was started by Nokia as an in-house project called 'Wibree' before being adopted by the Bluetooth SIG.

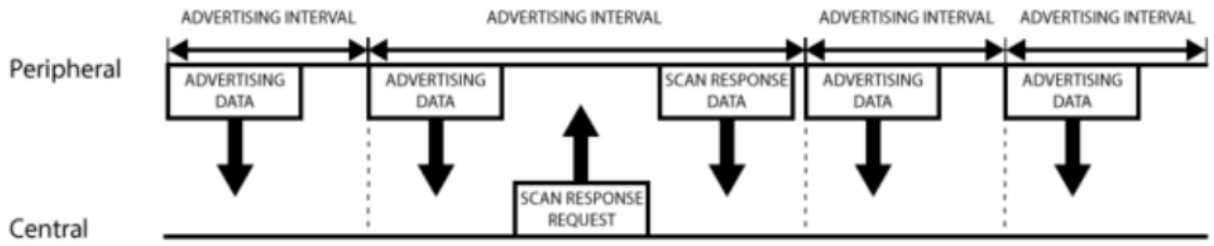
Generic Access Profile (GAP)

- GAP governs connections and advertising in Bluetooth.
- GAP defines various roles for devices, but the two key concepts to keep in mind are Central Devices and Peripheral Devices.
  - Peripheral devices are small, low power, resource constrained devices that can connect to a much more powerful central device. Peripheral devices are things like a heart rate monitor, a BLE enabled proximity tag, etc.
  - Central devices are usually the mobile phone or tablet that you connect to with far more processing power and memory.

Advertising and Scan Response Data

- Two ways to send advertising out with GAP. Both payloads are identical and can contain up to 31 bytes of data.
- The Advertising Data payload (mandatory): that is constantly transmitted out from the device to let central devices in range know that it exists.
- The Scan Response payload (optional): that central devices can request, and allows more information fit in the advertising payload such as strings for a device name, etc.

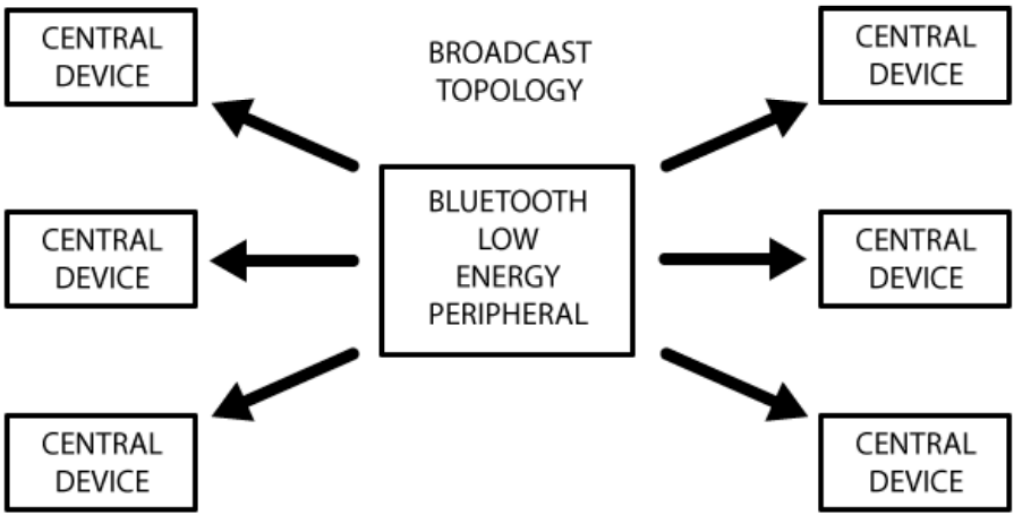
Advertising Process



A peripheral will set a specific advertising interval, and every time this interval passes, it will retransmit it's main advertising packet. If a listening device is interested in the scan response payload (and it is available on the peripheral) it can optionally request the scan response payload, and the peripheral will respond with the additional data.

Source: https://learn.adafruit.com/introduction-to-bluetooth-low-energy/introduction

Advertising via Broadcast



Once you establish a connection between your peripheral and a central device, the advertising process will generally stop and you will typically no longer be able to send advertising packets out anymore, and you will use GATT services and characteristics to communicate in both directions.

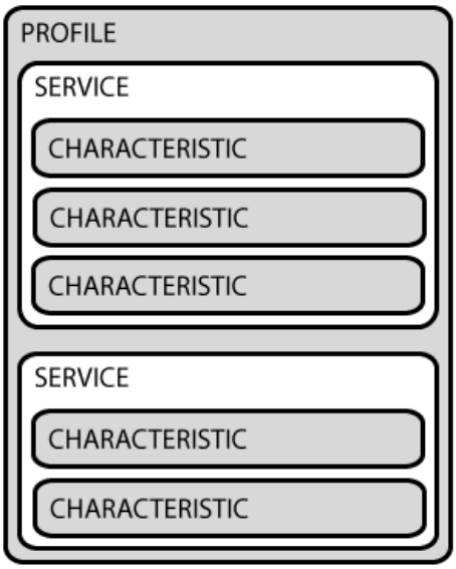
https://learn.adafruit.com/introduction-to-bluetooth-low-energy/introduction

GATT Services and Characteristics

- GATT is an acronym for the **Generic Attribute Profile**.
- It defines the way that two Bluetooth Low Energy devices transfer data back and forth using concepts called **Services** and **Characteristics**.
- It makes use of a generic data protocol called the **Attribute Protocol (ATT)**, which is used to store Services, Characteristics and related data in a simple lookup table using 16-bit IDs for each entry in the table.

Services and Characteristics

- GATT transactions in BLE are based on high-level, nested objects called **Profiles**, **Services** and **Characteristics**.



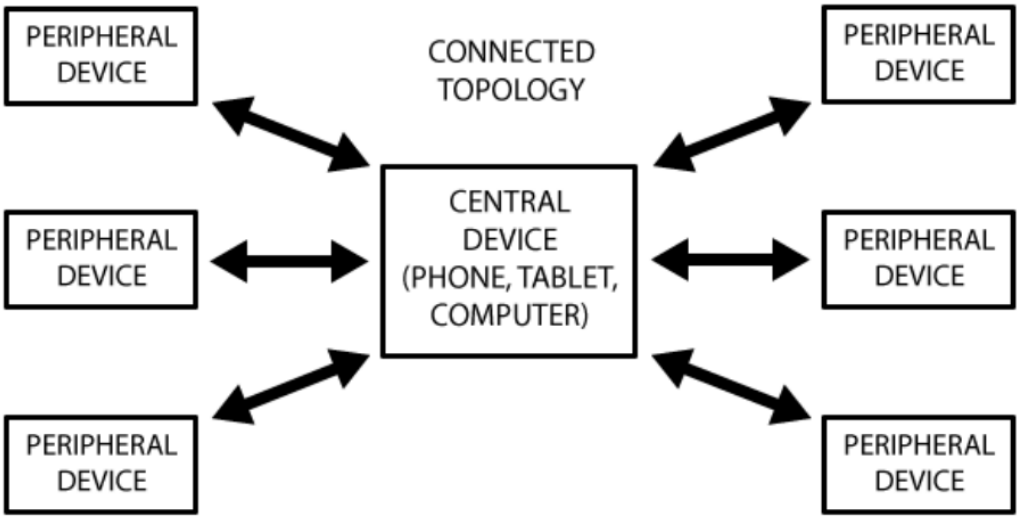
- **Profile**: This is simply a pre-defined collection of Services compiled by either the Bluetooth SIG or by the peripheral designers.
- **Service**: contains specific chunks of data called characteristics. A service can have one or more characteristics, and each service distinguishes itself from other services by means of a unique numeric ID called a UUID.
- **Characteristic**: encapsulates as single data point. Similarly to Services, each Characteristic has a pre-defined UUID. Used to send data back to the BLE peripheral.

https://learn.adafruit.com/introduction-to-bluetooth-low-energy/introduction

Exclusive Connection of GATT

- With GATT, connections are exclusive. This means that a BLE peripheral can only be connected to one central device (a mobile phone, etc.) at a time!
- As soon as a peripheral connects to a central device, it will stop advertising itself and other devices will no longer be able to see it or connect to it until the existing connection is broken.

Connected Topology



A peripheral can only connect to a central device but a central device can connect up To 7 peripherals. Once a connection is established between a peripheral and a central device, communication can take place in both directions.

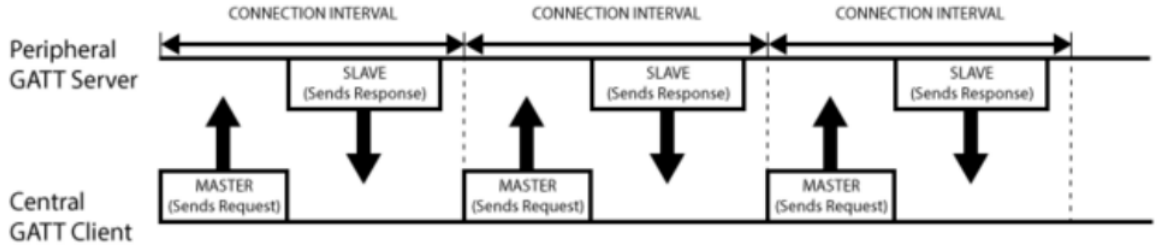
https://learn.adafruit.com/introduction-to-bluetooth-low-energy/introduction

Server-Client in GATT Transactions

- Client: Typically sends a request to the GATT server. The client can read and/or write attributes found in the server.
- Server: One of the main roles of the server is to store attributes. Once the client makes a request, the server must make the attributes available.
- The IoT device is known as the GATT Server, which holds the ATT lookup data and service and characteristic definitions, and the GATT Client (smart phone/tablet) sends requests to this server.

GATT Transactions

- All transactions are started by the master device, the GATT Client, which receives response from the slave device, the GATT Server.
- When establishing a connection, the peripheral will suggest a 'Connection Interval' to the central device, and the central device will try to reconnect every connection interval to see if any new data is available, etc.
- The following diagram illustrates the data exchange process between a peripheral (the GATT Server) and a central device (the GATT Client), with the master device initiating every transaction:



https://learn.adafruit.com/introduction-to-bluetooth-low-energy/introduction

A Comparison between Zigbee, BT and BLE

Feature	ZigBee	Bluetooth Classic (BT)	Bluetooth Smart
Design Focus	Wireless networking among sensors	Wireless keyboards, mouse, headsets	Wireless sensor and fitness devices
IEEE Standard	802.15.4	802.15.1	802.15.1
Network Type	Mesh, ZigBee PRO	Piconet, Master/Slave; Scatternet	Scatternet
Distance	75-100m line of sight	10m (33ft) min	>10m >(33ft)
Nodes Connected, max	65000	8	N/A
Operating Band	2.400 Ghz-2.4835 GHz ISM band 16 channels, 5MHz apart, 2MHz used Direct Spread Spectrum	2.400 Ghz-2.4835 GHz ISM band 79 1-MHz channels Frequency Spread Spectrum	2.400 Ghz-2.4835 GHz ISM band 40 2-MHz channels Frequency Spread Spectrum
Throughput	0.03Mbps	1-3Mbps	0.27Mbps
Latency with Connect	15ms	100ms - 3sec	3-6ms
Type of Data	Operational instructions Low data rate	Continuous streaming All types of data; text, multimedia Relatively high speeds	Burst
Voice	No	Yes	No
Security	EAP (Extensible Authentication Protocol)	56/128-bit and application layer user defined	128-bit AES (Advanced Encryption Standard) with Counter Mode CBC-MAC and application layer user defined
Power Consumed (dependent on application)	30mW	100 mW	0.01-0.5W
Modulation	Direct Sequence Spread Spectrum	Frequency Hopping Spread Spectrum	Gaussian Frequency Shift Keying

Source: http://www.allaboutcircuits.com/technical-articles/zigbee-vs-bluetooth-and-bluetooth-smart/

Summary

- An M2M area network consists of many types of sensors/actuators/devices and (wireless) communication protocols.
- We show many examples of those sensors/ actuators/devices.
- We cover three examples of M2M area protocols: ANSI C12 Suite, Zigbee (IEEE 802.15.4), Bluetooth Low Energy (BLE).
- Sensor platforms such as Arduino and Raspberry Pi are important tools for connecting and enabling sensors/actuators.

Appendix

Example IoT Devices

Game Drone – Parrot Ar. Drone (1)

- http://ardrone.parrot.com/parrot-ar-drone/usa/
- With its own generated WiFi network, players can create a game party where others players can join and play against each other (e.g., AR.FlyingAce)
- A quadricopter made in carbon fiber and high resistance PA66 plastic
- MEMS (Micro-Electro-Mechanical Systems) and video processing to ensure an intuitive piloting of a radio controlled object
- WiFi and video streaming for a modern interface with an iPhone™ or iPod touch®
- Images processing software for augmented reality
- One front camera (wide angle), one vertical camera (high speed), one ultrasound altimeter

Game Drone – Parrot Ar. Drone (2)

*** Embedded Computer System

- ARM9 468 MHz processor
- DDR 128 Mbyte at 200MHz
- WiFi – 802.11 b/g
- USB high speed
- Linux OS

*** Development tool

- Download-able Software Development Kit to develop innovative video games
- Open Game API enabling projects changing the way video games are played, both indoor and outdoor

Surveillance Robot – WowWee Rovio (1)

- http://www.wowwee.com/en/products/tech/telepresence/rovio
- Wi-Fi enabled mobile robot with webcam that lets you view and interact with its environment through streaming video and audio, wherever you are, via a browser with IP connection
- Free iPhone and Android APP enables to move your Rovio by simply tiling the smartphone in the direction you want to travel.
- requires some setting adjustment or firmware update to get good video quality or play back paths accurately, or docking in time

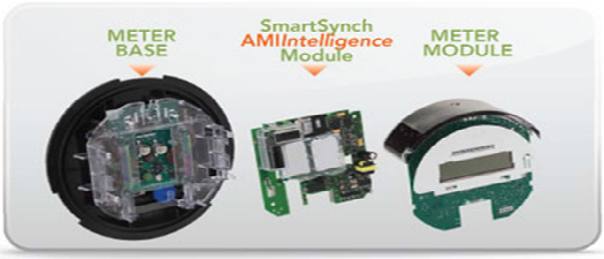
Surveillance Robot – WowWee Rovio (2)

- Detect the computer setting and guides the user through the setup process
- Its head-mounted, moveable VGA camera and wide range of vision enable you to see and hear (via 1 x Speaker and 1 x microphone for 2-way audio) exactly what Rovio sees and hears, on your screen, anywhere.
- Set waypoints so that Rovio can navigate itself (with 3 x Omni-directional wheels) around your home, without having to control each step yourself
- At the click of a button, send Rovio back to the charging dock (with built-in TrueTrack Beacon**) using its self-docking capabilities - even when you are not at home
- Guide Rovio through dimly lit locations with the aid of its built-in LED headlight.
- USB connectivity
- Rechargeable NiMH battery

- ** Rovio requires additional TrueTrack Room Beacons to navigate or self-dock across multiple rooms.

Smart Meter – Elster A3 ALPHA SmartMeter (1)

- SmartSynch's C&I metering solution features a communications module that is integrated into the Elster A3 ALPHA electricity meter
- http://www.smartsynch.com/SmartSynch_elster_a3.htm
- This solution delivers actionable intelligence (critical usage and rate data) over secure public GSM/GPRS wireless networks and the Internet—in lieu of cumbersome & expensive private networks.



Smart Meter – Elster A3 ALPHA SmartMeter (2)

Features a host of key monitoring and communication functionalities, including

- Flexible Two-Way Data Retrieval
- Scheduled and On-Demand Reads
- Automated Interval Read Retrieval
- Real-Time Interval Reads
- Automated Register, Self-Read and TOU (Total Ozone Unit) Retrieval
- Instrumentation Profiling
- Current and Voltage Profiling
- Critical Peak Pricing
- Demand Resets
- Real-Time Meter Event and Alarm Retrieval

Smart Meter – Elster A3 ALPHA SmartMeter (3)

- Real-Time Power Outage and Power Restoration Alarms
- Power Quality Monitoring and Alarms
- Demand Threshold Monitoring and Alarms
- Service Diagnostics and Tamper Detection
- Meter Clock Synchronization
- SmartMeter Status Display
- Automated Meter Registration
- Secure and Encrypted Data Transmissions
- Supports Reads from Itron MV-90 Software
- Supports Reads from Elster MAS Software
- Remote Meter Programming
- Over-The-Air SmartMeter Module Firmware Upgrade

Cleaning Robot with IP Camera – Ankaka G182 (1)

- Robot vacuum cleaner
- WiFi IP camera
- Virtual wall and charging station
- Proprietary software
- http://www.ankaka.com/intelligent-robot-vacuum-cleaner-with-wireless-ip-camera-wifi-ip-camera_p1165.html

Cleaning Robot with IP Camera – Ankaka G182 (2)

- Applications include:
  - DVS application (Designed to identify IP addresses and Modify IP Addresses)
  - IP Camera Center (View, record, control, and access multiple functions and features of the robot vacuum cleaner with the WiFi IP camera)
  - IP Camera Player - Plays back recorded video footage
- Program it to clean while away from home
- Auto Charging station, meaning it will recharge when it is low on power automatically
- Use the virtual wall unit to prevent the robot vacuum cleaner from venturing into areas you do not wish it to go
- As with all vacuum cleaners, the robot vacuum cleaner does not empty itself, so you will need to clean out the units dust bin after every cleaning cycle
- For best results it is recommend that you observe the robot vacuum cleaner operate in each room of your house the first time so you can make sure the room layout and furnishings do not interfere with the units navigation

Cleaning Robot with IP Camera – Ankaka G182 (3)

- Moulded ABS body, pressure sensitive front bumper, two castor style front wheels, large traction grip rear wheels
- Height From Floor: 1 inch (approx 2.5cm)
- Movement: 360 degrees
- Working Time Per Charge: 70 Minutes
- Usual Charging Time: 3.5 hours
- Noise Level:<50db

iRobot Create (1)

- Create is preassembled and ready to use right out of the box.
- Beginners can observe the robot's behavior in any of the 10 demonstration modes or program the robot by downloading scripts with any basic terminal program.
- Advanced users can write custom software using a variety of methods that take advantage of the robot's "streaming sensor data" mode for more control of the robot.
- Highly advanced users can write programs for completely autonomous operations.
- Create accessories include a Bluetooth Access Module (BAM) for wireless communication
- http://store.irobot.com/shop/index.jsp?categoryId=3311368

iRobot Create (2)

- Bluetooth Adaptor Module (BAM)
  - Up to 300ft (100m) range in a typical residential home (attainable range will depend on the environment)
  - Wireless control of the iRobot Createý from any Windows or Linux PC or Macintosh computer
  - 20 pin I/O connector for adding your own hardware and sensors to the robot in addition to the wireless connection
  - High power Class 1 Bluetooth radio
  - Bluetooth Serial Port Profile (SPP)
  - DB-25 male connector plugs into the Createýs expansion port
  - Providing a virtual serial port connection between the computer and the Create robot

iRobot Create (3)

iRobot Create Open Interface

- The Create Open Interface (OI) consists of an electronic interface and a software interface for controlling Create's behavior and reading its sensors. The electronic interface includes a 7 pin Mini-DIN connector and a DB-25 connector in the Cargo Bay for connecting hardware and electronics for sensors and actuators such as a robotic arm or light sensor to Create.

- The software interface lets you manipulate Create's behavior and read its sensors through a series of commands including start commands, mode commands, actuator commands, demo commands, song commands, input commands, script commands, and wait commands that you send to Create's serial port by way of a PC or microcontroller that is connected to the Mini-DIN connector or Cargo Bay.