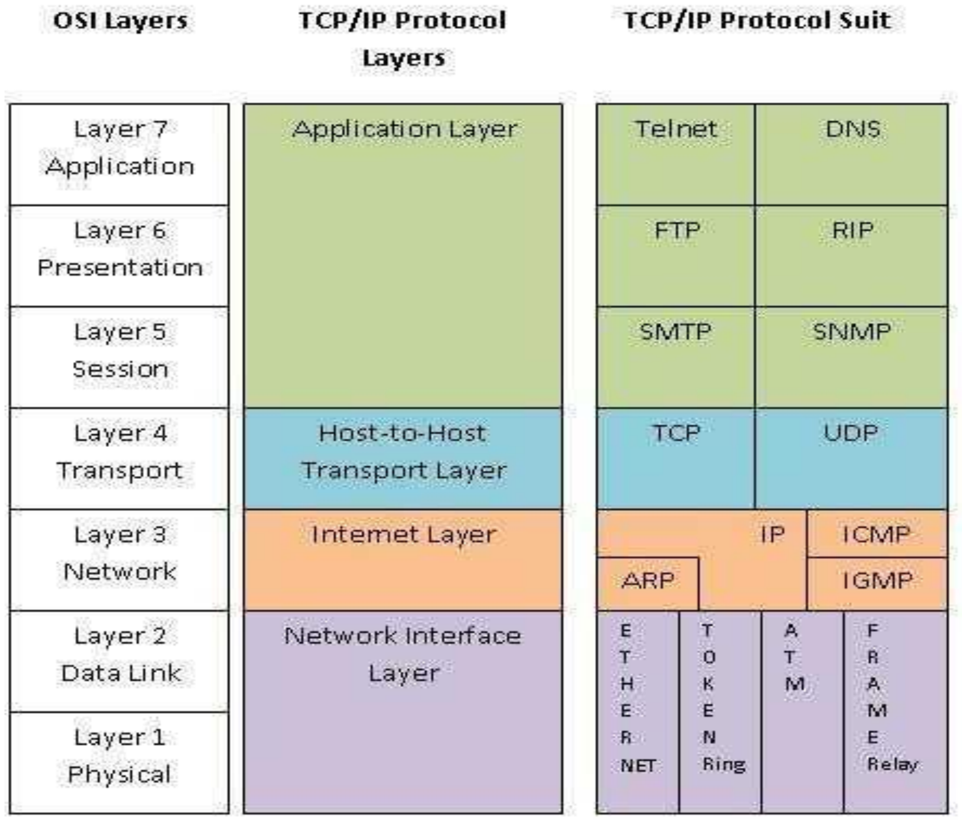
Lecture 2 - IoT stack and Web stack

Content

OSI and TCP/IP



OSI Layers	TCP/IP Protocol Layers	TCP/IP Protocol Suit	
Layer 7 Application	Application Layer	Telnet	DNS
Layer 6 Presentation		FTP	RIP
Layer 5 Session		SMTP	SNMP
Layer 4 Transport	Host-to-Host Transport Layer	TCP	UDP
Layer 3 Network	Internet Layer	IP, ARP	ICMP, IGMP
Layer 2 Data Link	Network Interface Layer	ETHERNET, TOKEN Ring	ATM, FRAME Relay
Layer 1 Physical			

www.rfwireless-world.com

Functions of OSI layers

- • **Application**: The data to be transmitted is obtained from this layer with the help of various applications such as web, ftp, telnet etc. These applications will have data in different formats such as binary, ASCII, EBCDIC etc.
  • **Presentation**: It does syntax conversion (such as binary to ascii) as well as performs encryption/decryption of the data.
  • **Session**: It takes care of session management which is very useful for operators to charge the subscribers as per their billing period.
  • **Transport**: It does flow control, fragmentation, reassembly of the data to be transmitted or received.
  • **Network**: It takes care of routing of the packets as per logical addressing (i.e. as per IPv4 and IPv6 assignments). Various routing protocols exist in different technologies such as RIP, OSPF, AODV etc.
  • **Datalink**: It takes care of error control and flow control. It provides retransmission capabilities in case of faulty received packets with the help of ARQ protocol. The other main job of datalink layer is to provide medium access control and management of the medium (wired or wireless) supported by physical layer interface. Hence it is known as MAC layer also.
  • **Physical**: This layer is responsible for transmission of data over physical layer medium (wired or wireless). The layer will have functionalities such as modulation-demodulation, FEC (forward error correction) etc. The most common FEC modules are convolution encoder at Tx side and viterbi decoder at Rx side. Advanced modulation schemes such as OFDM, OFDMA are also used to obtain high data rates

Data flow across TCP IP model layers

- As mentioned above all the hosts receive the packets and each will compare destination address in the Ethernet header with its' own Ethernet or MAC address of 6 bytes and accept the same if it matches otherwise does not pay attention.

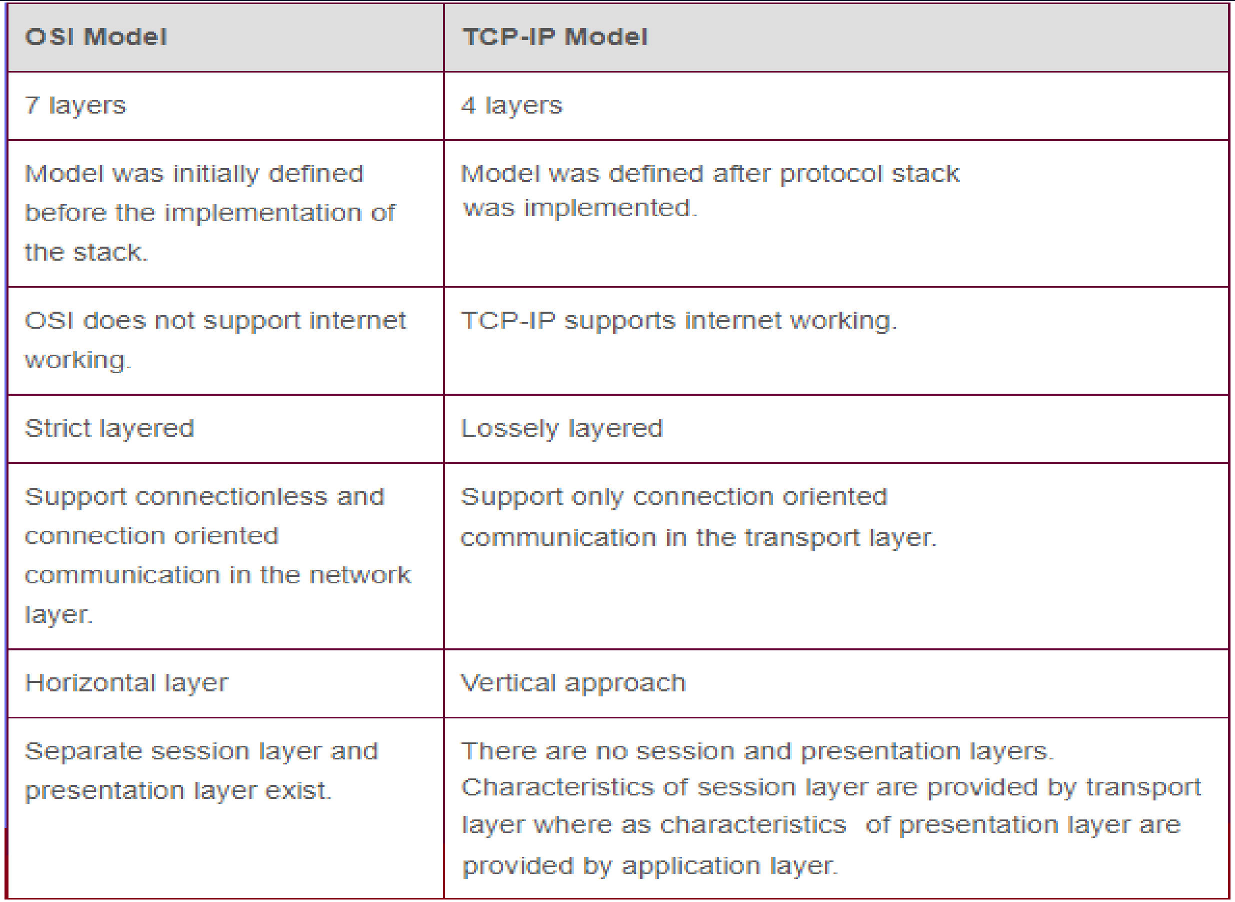
• Next it will check for type field(2 byte long), if it is 0x806 then the packet will be passed to ARP module and if it is 0x800 it will be passed to IP module. ARP module responds to hosts seeking for Ethernet address based on their logical (IP) address.

• After packet is received by IP layer it will decide where the packet need to be routed based on routing table and destination IP address embedded in received packet's IP header. IP header is usually 20 bytes.

• If the host is the final end system then IP module checks for protocol field (1 byte long) in the IP header. If it is 0x06 then the packet is passed to the TCP module and if it is 0x11 then the packet is passed to the UDP module.

• Above the TCP or UDP there is application layer, where so many applications will be usually running. Information to each application will be passed based on 'destination port number' field (16 bit long) embedded inside the TCP or UDP header. TCP utilizes 'sequence number field' (32 bit long) for reassembly of all the IP data grams received at irregular time instants in irregular orders. For example FTP has dedicated port address 23 and Telnet has dedicated port address 21, which is used to deliver the data to each.

Comparison between OSI layers vs TCP IP networking layer

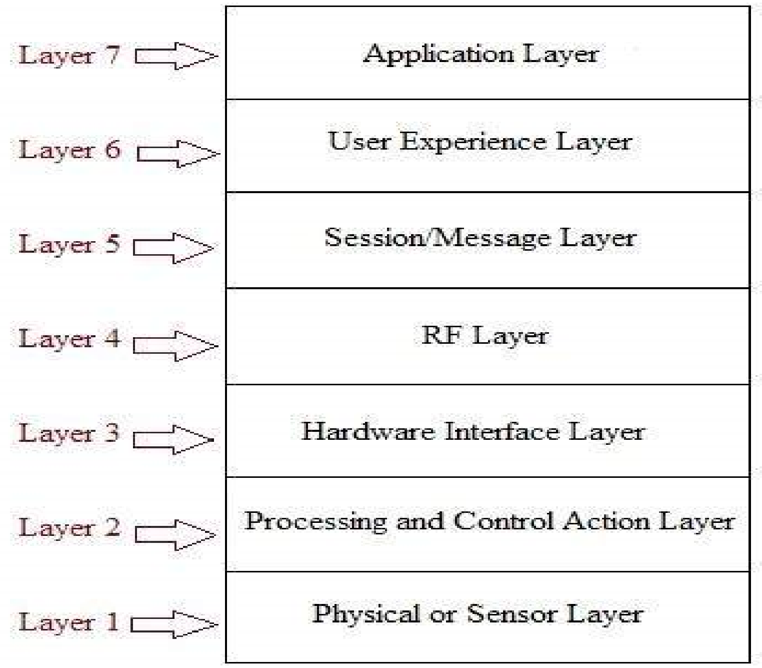


OSI Model	TCP-IP Model
7 layers	4 layers
Model was initially defined before the implementation of the stack.	Model was defined after protocol stack was implemented.
OSI does not support internet working.	TCP-IP supports internet working.
Strict layered	Lossely layered
Support connectionless and connection oriented communication in the network layer.	Support only connection oriented communication in the transport layer.
Horizontal layer	Vertical approach
Separate session layer and presentation layer exist.	There are no session and presentation layers. Characteristics of session layer are provided by transport layer where as characteristics of presentation layer are provided by application layer.

Vishwakarma Institute of Technology

IoT protocol stack

- Functional description of 7 layers of IoT protocol stack



IoT Protocol Stack Layers

Seven Layers of IoT Stack

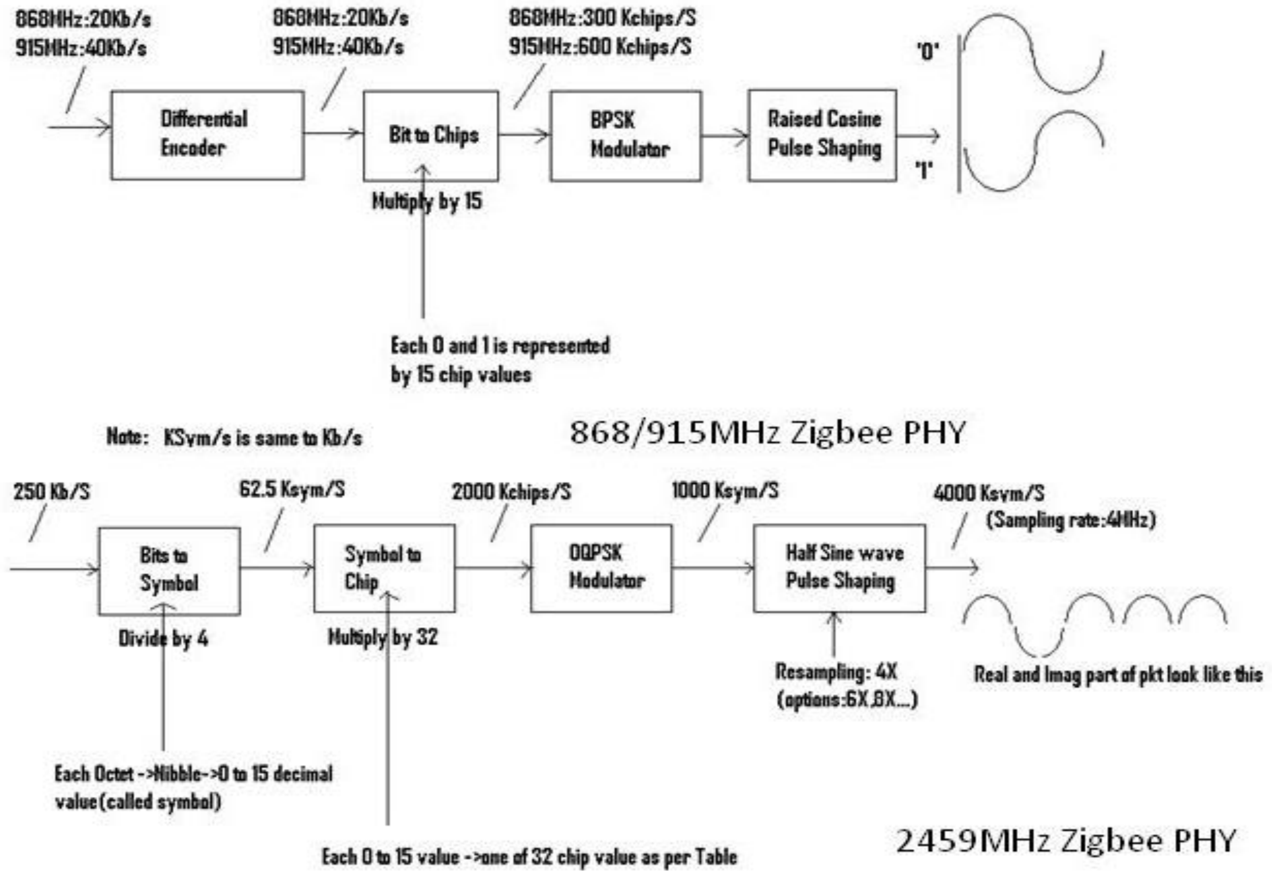
IoT stack consists of following seven layers –

- Sensor layer,
- processing/control layer,
- hardware interface layer,
- RF layer,
- session/message layer,
- user experience layer
- application layer.

IoT Stack Layer 1

- **Physical or sensor layer:**
  Similar to OSI physical layer, this IoT layer 1 interfaces with physical components. The physical components are mainly sensors such as humidity sensor, temperature sensor, pressure sensor, heartrate sensor, pH sensor, odour sensor etc. The sensors are used for sensing of various parameters as per application of use. There are plenty of sensors available for same functionality and hence appropriate selection of sensor is done based on cost and quality. It is this layer-1 which provides sensed data to IoT stack for further processing.

Zigbee Physical Layer


868MHz:20Kb/s
915MHz:40Kb/s
Differential Encoder
868MHz:20Kb/s
915MHz:40Kb/s
Bit to Chips
Multiply by 15
868MHz:300 Kchips/S
915MHz:600 Kchips/S
BPSK Modulator
Raised Cosine Pulse Shaping
'0'
'1'
Each 0 and 1 is represented by 15 chip values
Note: KSym/s is same to Kb/s
868/915MHz Zigbee PHY
250 Kb/S
Bits to Symbol
Divide by 4
62.5 Ksym/S
Symbol to Chip
Multiply by 32
2000 Kchips/S
OQPSK Modulator
1000 Ksym/S
Half Sine wave Pulse Shaping
Resampling: 4X (options:6X,8X...)
4000 Ksym/S (Sampling rate:4MHz)
Real and Imag part of pkt look like this
Each Octet ->Nibble->0 to 15 decimal value(called symbol)
Each 0 to 15 value ->one of 32 chip value as per Table
2459MHz Zigbee PHY

There are two physical layer version in zigbee. These are categorized based on frequency band of use viz. 868/915MHz and 2450MHz.

IoT Stack Layer 2

- **Processing and control layer :**

  The data provided by layer-1 using sensors are processed at this layer. Microcontroller/Processor and operating system play vital role at this layer. Various development kits can be used for this purpose such as Arduino, NodeMCU (based on ESP32 or ESP8266) , ARM, PIC etc. Typical operating systems used are Android, Linux, IOS etc.

IoT Stack Layer 3

- **Hardware Interface layer :**

  This layer include components or interfaces used for communication such as RS232, RS485, SPI, I2C, CAN, SCI etc. These interfaces are used for serial or parallel communication at various baud rates in synchronous/asynchronous modes. The above mentioned interface protocols ensure flawless communication.

IoT Stack Layer 4

- **RF layer :**

  This radio frequency layer houses RF technologies based on short range or long range and data rate desired by the application of use. The common indoor RF/wireless technologies include Wifi, Bluetooth, Zigbee, Zwave, NFC, RFID etc. The common outdoor RF cellular technologies include GSM/GPRS, CDMA, LTE-M, NB-IoT, 5G etc. RF layer does communication of data using radio frequency based EM waves. There is another technology which uses light waves for data communication. This light based data communication is referred as LiFi.

IoT Stack Layer 5

- **Session/Message Layer :**

  This layer deals with various messaging protocols such as MQTT, CoAP, HTTP, FTP (or Secured FTP), SSH etc. It defines how messages are broadcasted to the cloud. Refer architectures of MQTT protocol and CoAP protocol.

IoT Stack Layer 6

- **User experience layer :**

  This layer deals with providing best experience to the end users of IoT products. To fulfill this, this layer takes care of rich UI designs with lots of features. Various languages and tools are developed for the design of GUI interface softwares. These include objected oriented and procedure oriented technologies as well database languages (DBMS, SQL) in addition to analytics tools.

Vishwakarma Institute of Technology

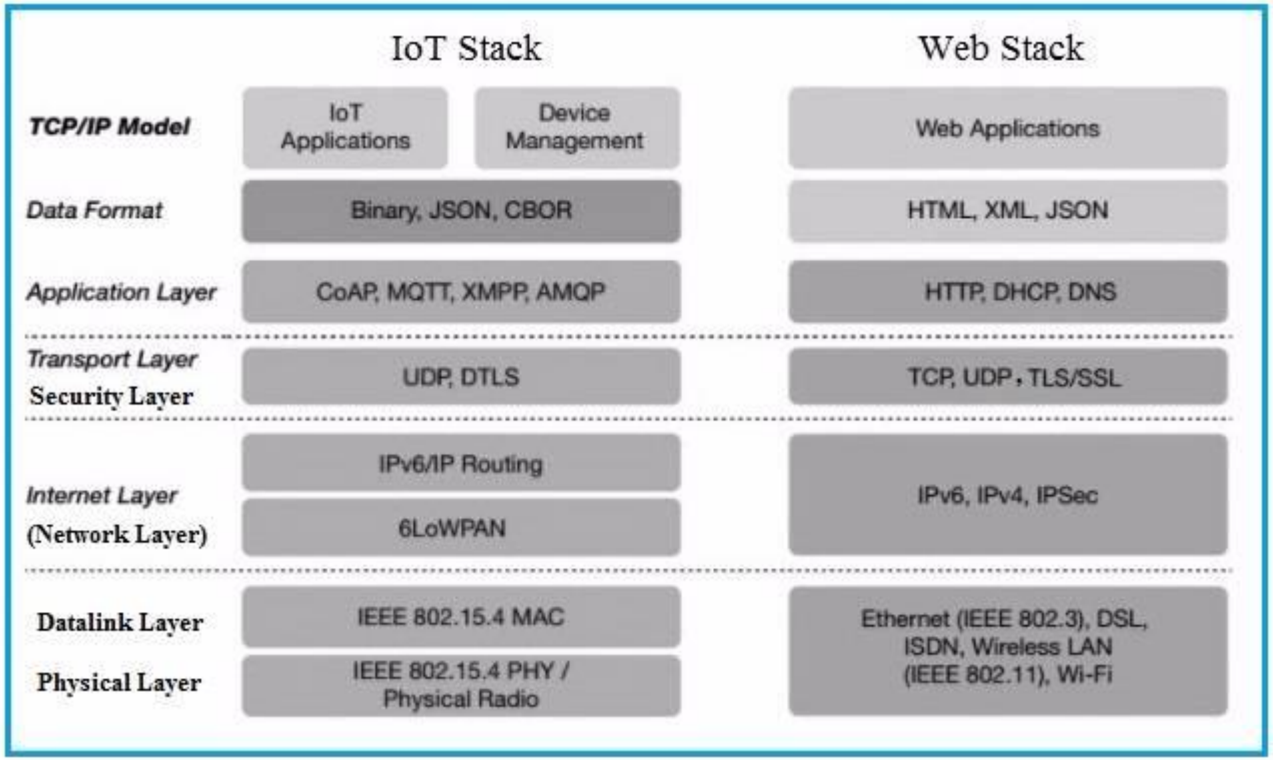
IoT Stack Layer 7

Application layer :

This layer utilizes rest of the six layers in order to develop desired application. The typical case studies or applications of IoT are as follows.

- Smart Home
- Smart Parking System based on zigbee, LoRaWAN and other wireless technologies.
- Smart Energy System, Refer Smart Grid Architecture.
- Smart City
- Smart lighting system based on zigbee standard
- Smart Retail
- Smart Agriculture farming
- Smart Waste Management

IoT Stack VS Web Stack



	IoT Stack	Web Stack
TCP/IP Model	IoT Applications; Device Management	Web Applications
Data Format	Binary, JSON, CBOR	HTML, XML, JSON
Application Layer	CoAP, MQTT, XMPP, AMQP	HTTP, DHCP, DNS
Transport Layer / Security Layer	UDP, DTLS	TCP, UDP, TLS/SSL
Internet Layer (Network Layer)	IPv6/IP Routing; 6LoWPAN	IPv6, IPv4, IPSec
Datalink Layer	IEEE 802.15.4 MAC	Ethernet (IEEE 802.3), DSL, ISDN, Wireless LAN (IEEE 802.11), Wi-Fi
Physical Layer	IEEE 802.15.4 PHY / Physical Radio	

Comparison

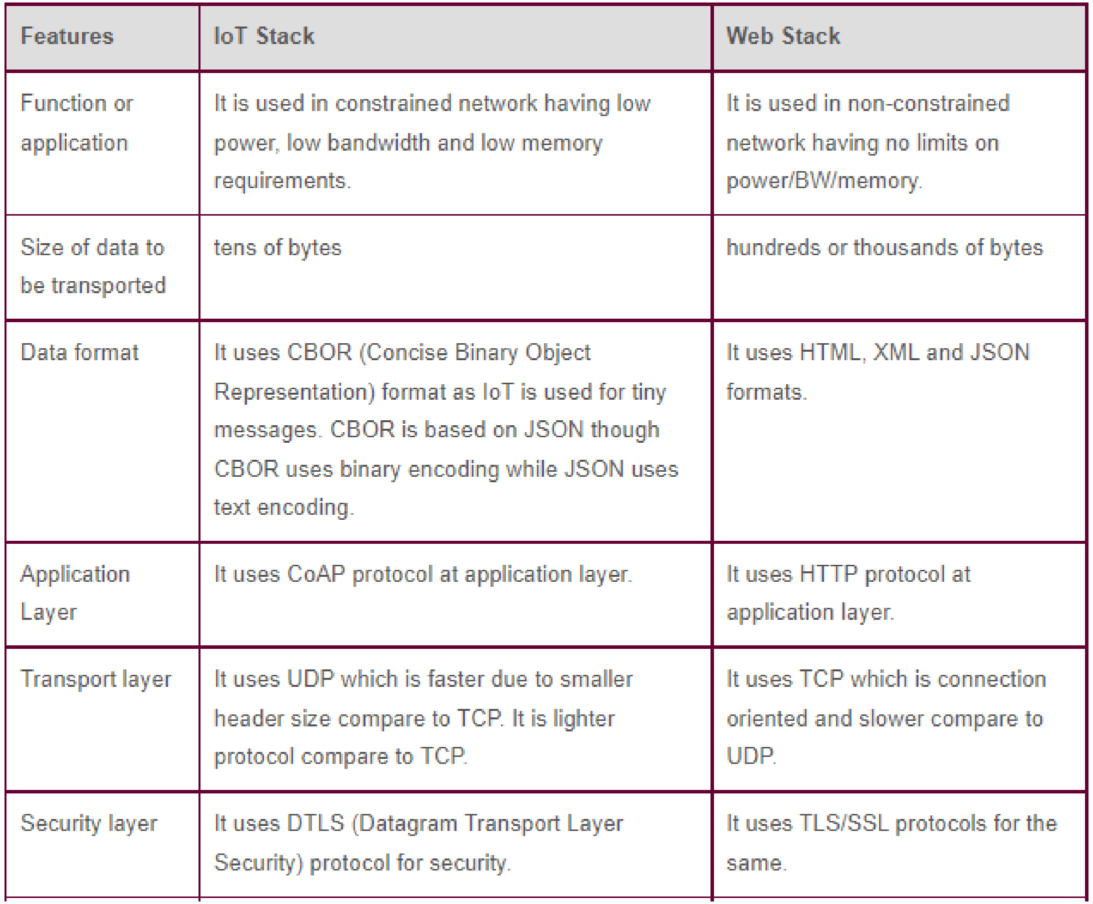
IoT Stack Protocol

- Efficient Devices
- Efficient web services applications
- Optimized IP Access
- Packets of Tens of bytes

Web Stack Protocol

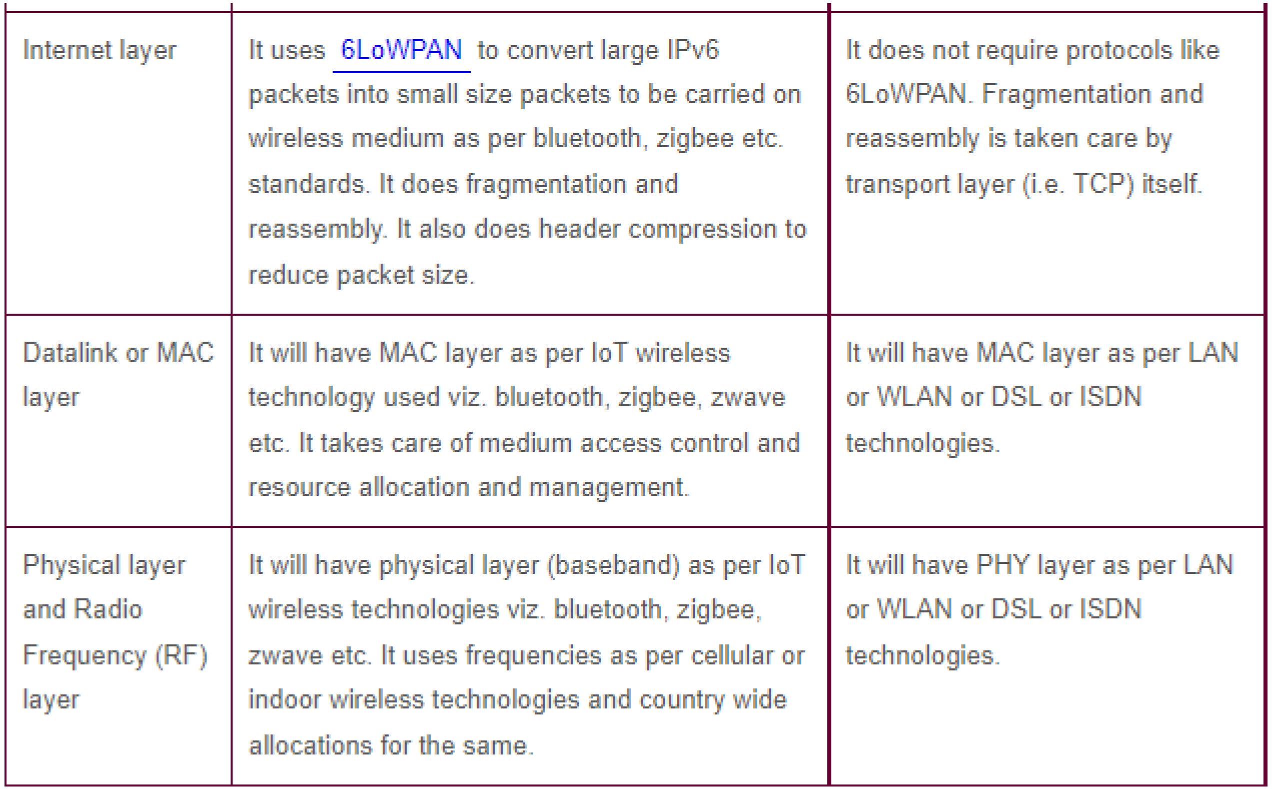
- Huge overhead
- Requres lots of internet devices
- Sometimes inefficient, content encoding
- Packets of hundred and thousands of bytes

Difference between IoT Stack and Web Stack



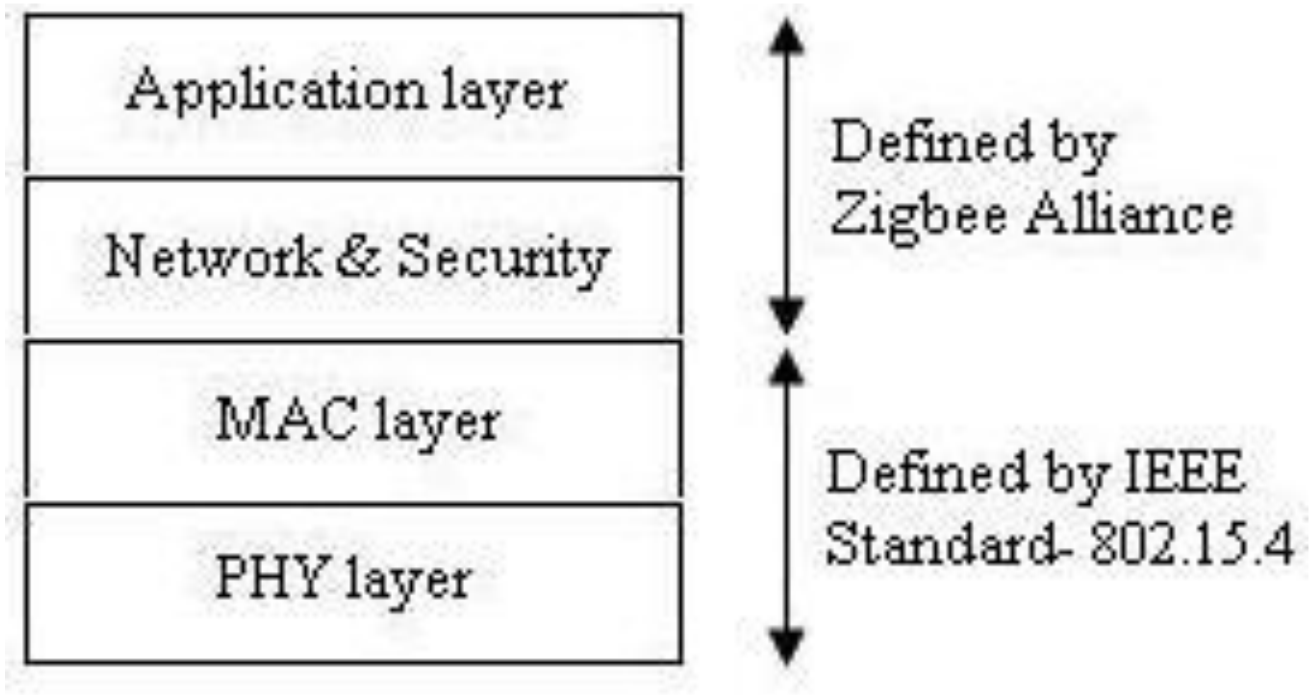
Features	IoT Stack	Web Stack
Function or application	It is used in constrained network having low power, low bandwidth and low memory requirements.	It is used in non-constrained network having no limits on power/BW/memory.
Size of data to be transported	tens of bytes	hundreds or thousands of bytes
Data format	It uses CBOR (Concise Binary Object Representation) format as IoT is used for tiny messages. CBOR is based on JSON though CBOR uses binary encoding while JSON uses text encoding.	It uses HTML, XML and JSON formats.
Application Layer	It uses CoAP protocol at application layer.	It uses HTTP protocol at application layer.
Transport layer	It uses UDP which is faster due to smaller header size compare to TCP. It is lighter protocol compare to TCP.	It uses TCP which is connection oriented and slower compare to UDP.
Security layer	It uses DTLS (Datagram Transport Layer Security) protocol for security.	It uses TLS/SSL protocols for the same.

Cont….



Internet layer	It uses 6LoWPAN to convert large IPv6 packets into small size packets to be carried on wireless medium as per bluetooth, zigbee etc. standards. It does fragmentation and reassembly. It also does header compression to reduce packet size.	It does not require protocols like 6LoWPAN. Fragmentation and reassembly is taken care by transport layer (i.e. TCP) itself.
Datalink or MAC layer	It will have MAC layer as per IoT wireless technology used viz. bluetooth, zigbee, zwave etc. It takes care of medium access control and resource allocation and management.	It will have MAC layer as per LAN or WLAN or DSL or ISDN technologies.
Physical layer and Radio Frequency (RF) layer	It will have physical layer (baseband) as per IoT wireless technologies viz. bluetooth, zigbee, zwave etc. It uses frequencies as per cellular or indoor wireless technologies and country wide allocations for the same.	It will have PHY layer as per LAN or WLAN or DSL or ISDN technologies.

zigbee protocol layers


Application layer
Network & Security
MAC layer
PHY layer
Defined by Zigbee Alliance
Defined by IEEE Standard- 802.15.4

Zigbee Protocol Stack

Zigbee Protocol Stack

Application Layer:

There are two profiles at this layer.

1. **Manufacturer specific application profile-**

Operate as closed systems and also ensure that they can coexist with other zigbee systems.

2. Public application profile-

For this to work interoperability between various zigbee devices is a must. A single zigbee node supports up to 240 application objects called end points. An end point specifies specific application, for example, 0 dedicated to ZDO (Zigbee device object), provides control and management commands. 6 used for control of light. 8 used for managing heating and air conditioning.

Zigbee Protocol Stack

- **Network Layer:**

Ad-hoc on-demand Distance Vector Routing protocol (AODV) is used at network layer.

- **Security Layer:**

If security is enabled, zigbee device will start up using a 128 bit AES encryption key. Devices having same security key can communicate on PAN.

How to obtain this key?

1. Pre-installation
2. Key is received over the air during joining.

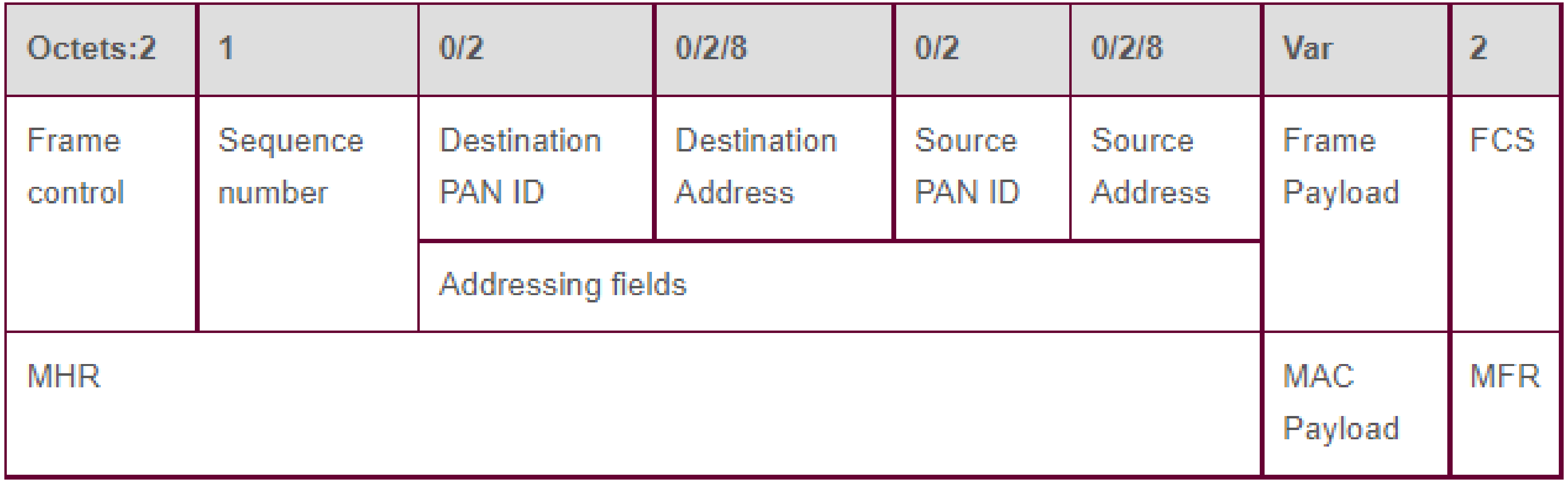
Zigbee Protocol Stack

MAC Layer

- Each MAC frame consists of three fields MAC header, MAC payload and MFR (FCS).
- Each MAC frame will contain Frame control field (16 bit), which carry frame type, addressing fields and other control flags.
- This MAC control field contain frame type field, which is the main differentiating factor in identifying one MAC frame with the other. It is 3 bit in length.
- The MAC frames are divided into following four major categories, which is used by zigbee devices to establish connection to the PAN by exchanging system information.

  1. Beacon
  2. Data
  3. Acknowledgement
  4. MAC command

Generic MAC Frame Format



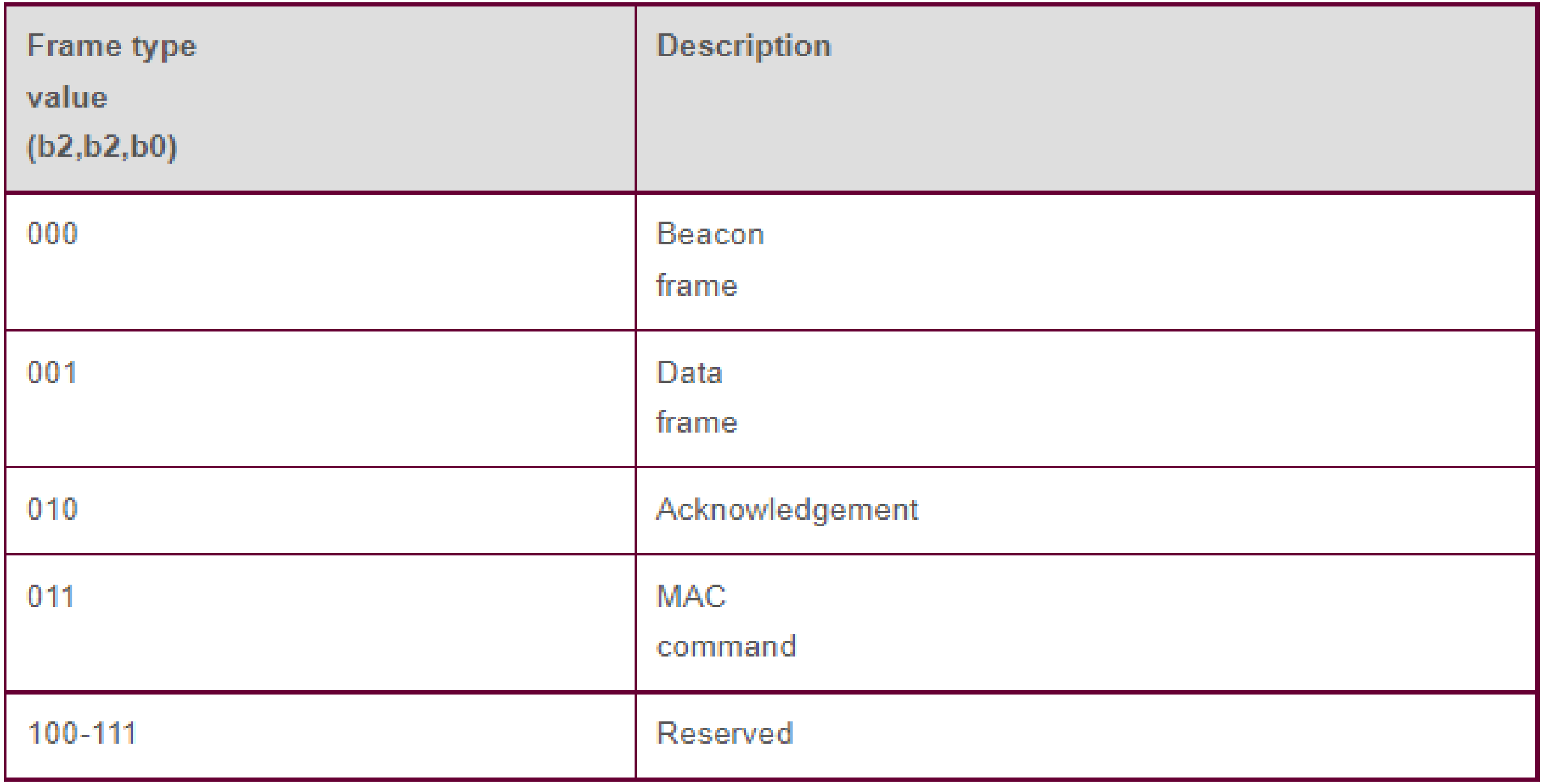
Octets:2	1	0/2	0/2/8	0/2	0/2/8	Var	2
Frame control	Sequence number	Destination PAN ID	Destination Address	Source PAN ID	Source Address	Frame Payload	FCS
		Addressing fields					
MHR						MAC Payload	MFR

Generic MAC layer frame has frame control field of 2 octets. It carries useful information such as frame type, source and destination addressing modes. Frame type specifies whether the frame is beacon frame,data frame, ACK of data, MAC command frame etc.

Frame Control Field

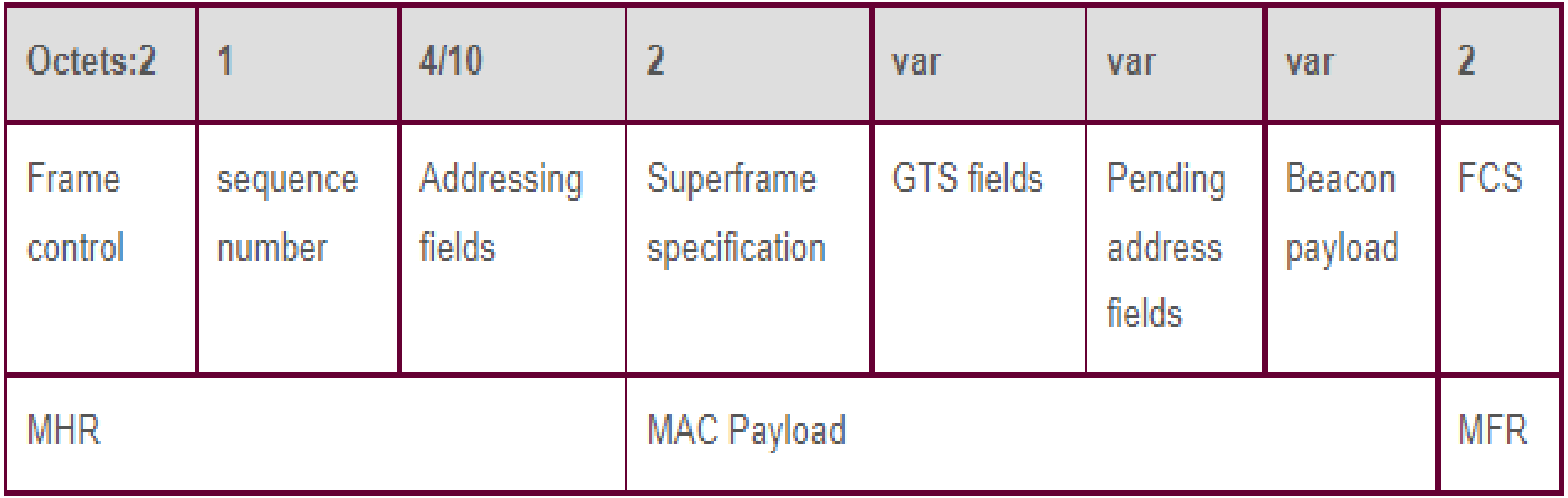
Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	security enabled	Frame pending	Ack. Request	Intra PAN	Reserved	Dest. Addre-ssing mode	Reserved	Source Addre-ssing mode

Frame Type Subfield



Frame type value (b2,b2,b0)	Description
000	Beacon frame
001	Data frame
010	Acknowledgement
011	MAC command
100-111	Reserved

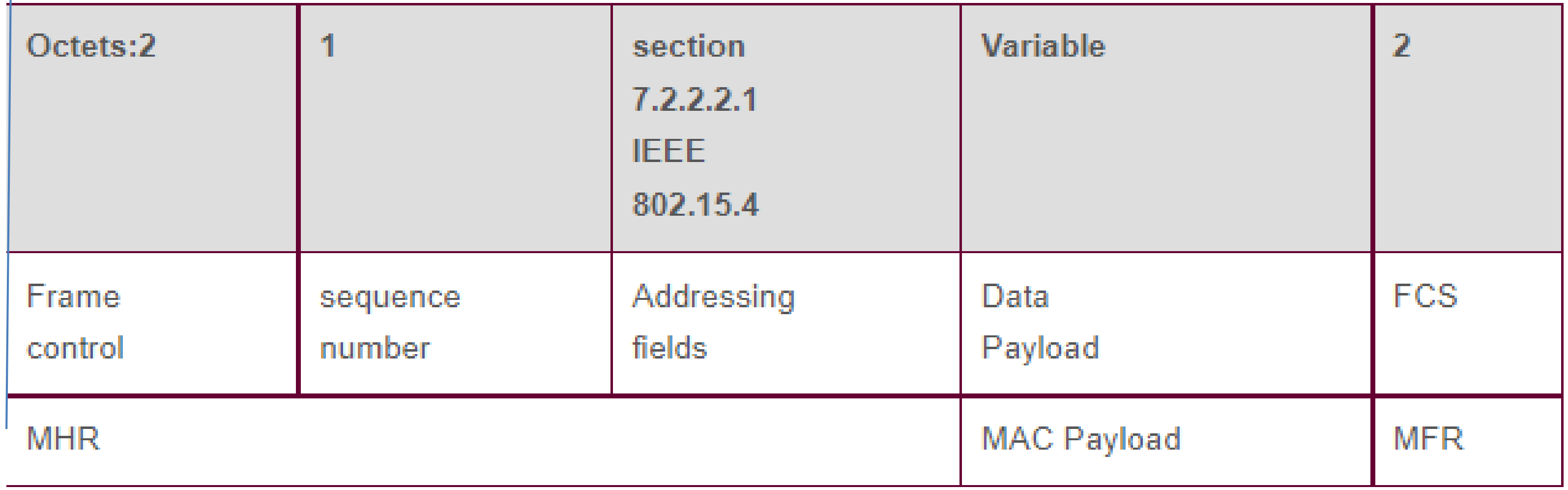
Beacon Frame Format



Octets:2	1	4/10	2	var	var	var	2
Frame control	sequence number	Addressing fields	Superframe specification	GTS fields	Pending address fields	Beacon payload	FCS
MHR			MAC Payload				MFR

- Beacon frame carries frame control field and addressing fields along with sequence number.
- It is broadcasted to obtain PAN ID of nearby zigbee devices.

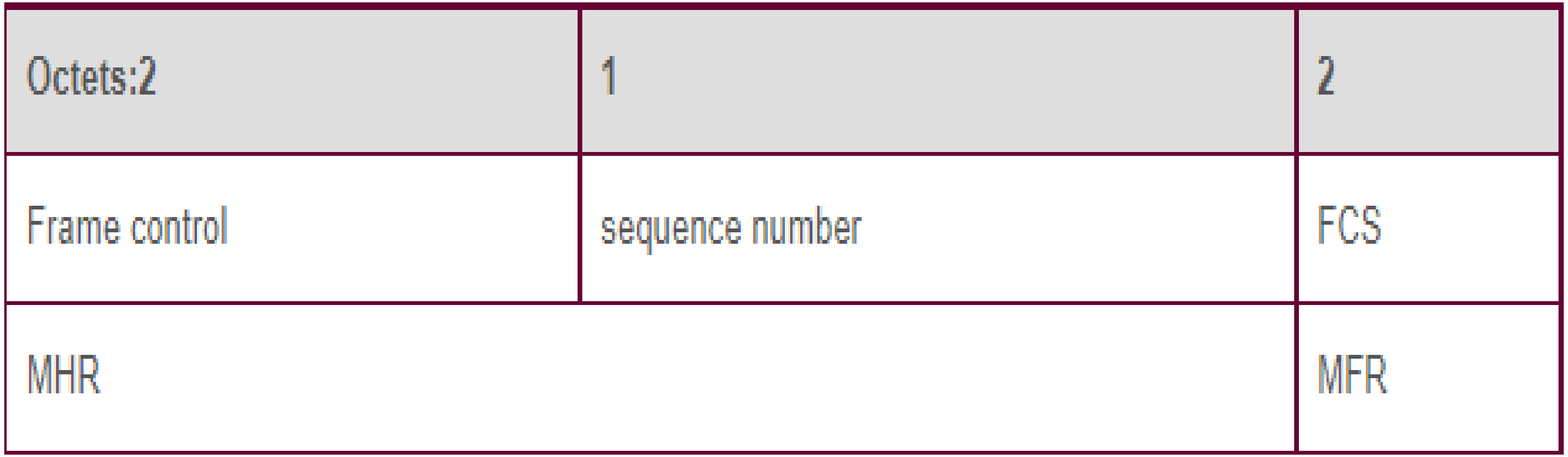
Data Frame Format



Octets:2	1	section 7.2.2.2.1 IEEE 802.15.4	Variable	2
Frame control	sequence number	Addressing fields	Data Payload	FCS
MHR			MAC Payload	MFR

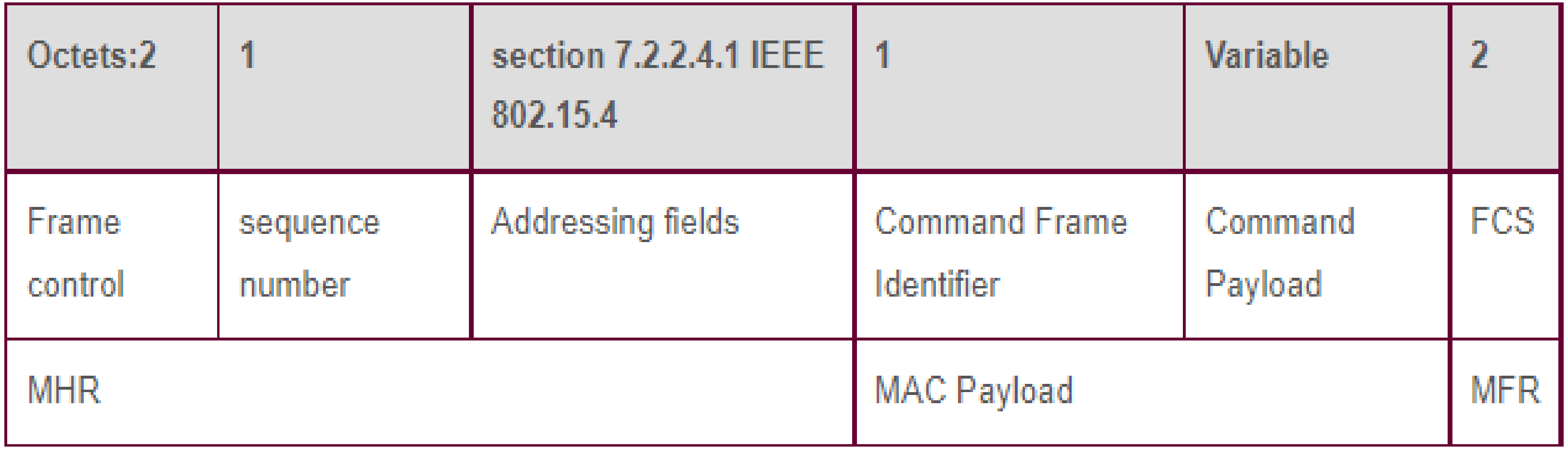
- Once connection is established data frame carry data.
- The format of data frame is similar to generic mac frame format

Acknowledgement Frame Format



Octets:2	1	2
Frame control	sequence number	FCS
MHR		MFR

MAC Command Frame Format



Octets:2	1	section 7.2.2.4.1 IEEE 802.15.4	1	Variable	2
Frame control	sequence number	Addressing fields	Command Frame Identifier	Command Payload	FCS
MHR			MAC Payload		MFR

MAC Command Frames

Command Frame ID	Command frame
0x01	Association request(Tx)
0x02	Association response(Rx)
0x03	Disassociation notification(Tx,Rx)
0x04	Data request(Tx)
0x05	PAN ID conflict notification(Tx)
0x06	Orphan notification(Tx)
0x07	Beacon request(Tx)
0x08	coordinator realignment(Rx)
0x09	GTS Request
0x0a-0xFF	Reserved

Zigbee protocol supports different command frames for different use cases