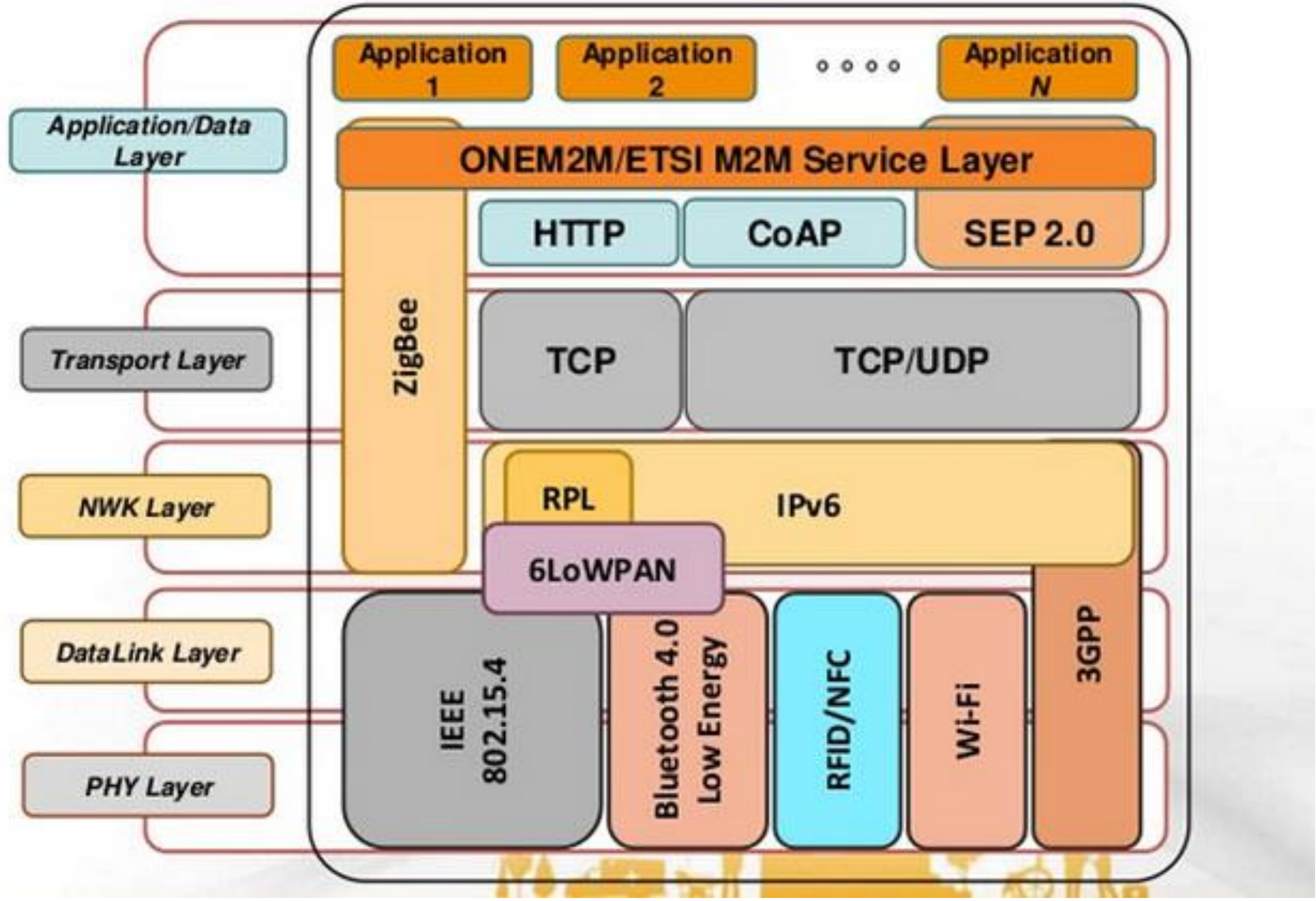
Internet of Things
IO 4041
6LoWPAN

IoT Protocol 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, TLS/SSL
Transport Layer	UDP, DTLS		TCP, UDP
Internet Layer	IPv6/IP Routing		IPv6, IPv4, IPSec
	6LoWPAN		
Network/Link Layer	IEEE 802.15.4 MAC		Ethernet (IEEE 802.3), DSL, ISDN, Wireless LAN (IEEE 802.11), Wi-Fi
	IEEE 802.15.4 PHY / Physical Radio		

IoT Protocol stack



Link layer and physical layer protocol

- The bottom two networking layers are defined by the IEEE **802.15.4** standard.

- This standard is developed by the IEEE 802 standards committee and was initially released in 2003.

- IEEE 802.15.4 defines the specifications for PHY and MAC layers of wireless networking,
  - but it does not specify any requirements for higher networking layers.
- The **ZigBee** standard defines only the networking, application, and security layers of the protocol and
  - adopts IEEE 802.15.4 PHY and MAC layers as part of the ZigBee networking protocol

Zigbee

- ZigBee is a standard that defines a set of communication protocols for **low-data-rate short-range** wireless networking
- ZigBee-based wireless devices operate in 868 MHz, 915 MHz, and 2.4 GHz frequency bands
  - The 868 MHz band is used in Europe,
  - the 915 MHz frequency band is used mainly in North America,
  - whereas the 2.4 GHz band is used worldwide.
- The maximum data rate is 250 K bits per second
- ZigBee is targeted mainly for battery-powered applications where low data rate, low cost, and long battery life are main requirements

Zigbee

In many ZigBee applications

- the total time the wireless device is engaged in any type of activity is very limited;
- the device spends most of its time in a power-saving mode, also known as **sleep mode**.

As a result,

- ZigBee enabled devices are capable of being operational for several years before their batteries need to be replaced.
- Design for wireless controls and sensors networking
- ZigBee provides the most power and the most cost efficient solution compared to Bluetooth and IEEE 802.11b

Bluetooth

- Creating personal area networks(PANs) with high levels of security with a medium data rate of 1 to 3Mbps
- Its indoor range is typically 2–10 meters
- Communicating on a frequency between 2.402 and 2.480
- 100+KB memory
- Created by telecom vender Ericsson in 1994
- Transmitting data via low-power radio waves
- Using a radio technology called **frequency-hopping spread spectrum**
- It is wireless, inexpensive and automatic
- Connection happen when device come within range of one another the electronic conversation happens automatically

Bluetooth

- Use Point-to-multipoint(Star topology)

- Bluetooth systems create a Personal Area Network(PAN) after conversation occurred and this called **Piconet**.

- A master Bluetooth device can communicate with up to seven devices in a Piconet

- Devices can switch roles, by agreement, the slave can become the master at any time

Wi-Fi

- It is a wireless technology that uses radio frequency to transmit data through the air.
- Wi-Fi is based on the 802.11 standard
- 802.11 is primarily concerned with the lower layers of the OSI model.
- Physical Layer
  - to map the MAC frames onto the medium
  - to transmit those frames.
- Data Link Layer
  - Logical Link Control (LLC).
  - Medium Access Control (MAC)

802.11 standards

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

IEEE 802.15.4 Characteristics

- Small packet size (Max MTU is 127 bytes)
  - Less room for data when including other headers
- MTU size of links was purposely small
  - to cope with limited buffering capabilities and
  - to limit the packet error rate since the bit error rate (BER) is relatively high

- Support for both 16-bit short or IEEE 64-bit extended **MAC addresses**
  - 24 for Organization unique Identifier + 40 bits assigned by the chipset manufacturer

Device Types: FFDs vs RFDs

Two types of devices in an IEEE 802.15.4 wireless network:

- Full-function devices (FFDs)
  - Any topology
  - PAN coordinator capable
  - Talks to any other device
  - Implements complete protocol set
- Reduced-function devices (RFDs)
  - Limited to star topology or end-device in a peer-to-peer network.
  - Cannot become a PAN coordinator
  - Very simple implementation
  - Reduced protocol set

Device Types: FFDs vs RFDs

Different roles of a device in an In an IEEE 802.15.4 network

- **Coordinator:** an FFD device that is capable of relaying messages, providing coordination and other services to the network

- **PAN coordinator:** If the coordinator is also the principal controller of a PAN, then called a PAN coordinator. A network has exactly one PAN coordinator

- **Network Device:** An FFD or RFD is simply called a device if not acting as a coordinator

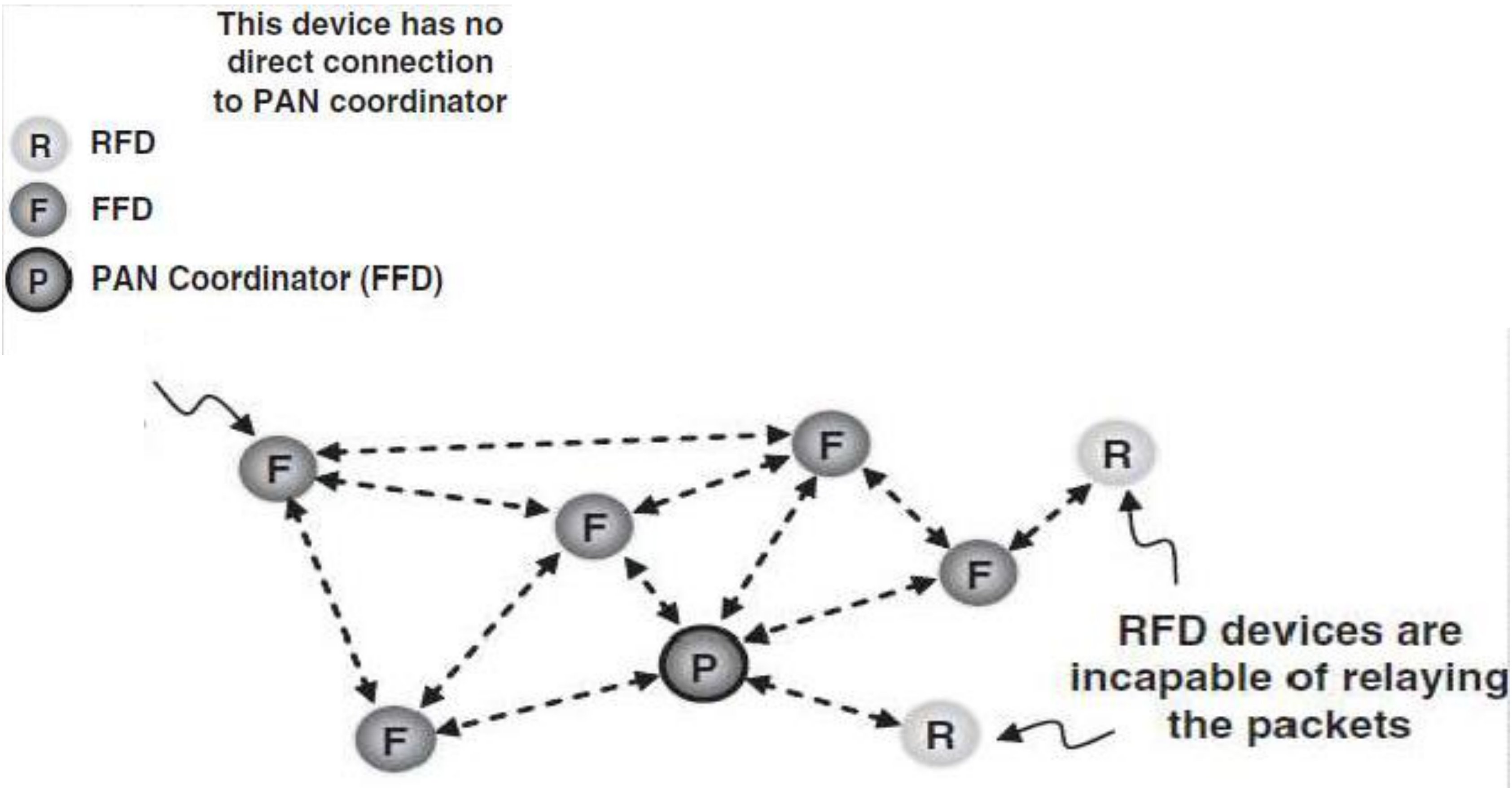
Topology

- In the star topology(point to multi points), every device in the network can communicate only with the PAN coordinator.
- In a peer-to-peer topology (mesh topology), each device can communicate directly with any other device
  - if the devices are placed close enough together to establish a successful communication link.
- Any FFD in a peer-to-peer network can play the role of the PAN coordinator
- One way to decide which device will be the PAN coordinator is to pick the first FFD device that starts communicating as the PAN coordinator

Coordinator

- FFDs can become coordinator and can also route messages to other nodes
- RFDs cannot become coordinator and can only be a leaf
- FFD that starts a PAN becomes the coordinator
- In star topology, all communication is to/from the coordinator
- In P2P topology, FFDs can communicate directly also. ‰
- Each piconet has a PAN ID and is called a cluster.
- Nodes join a cluster by sending association request to the coordinator.
- Coordinator assigns a 16-bit short address to the device. Devices can use either the short address or EUI-64 address.

Mesh Topology

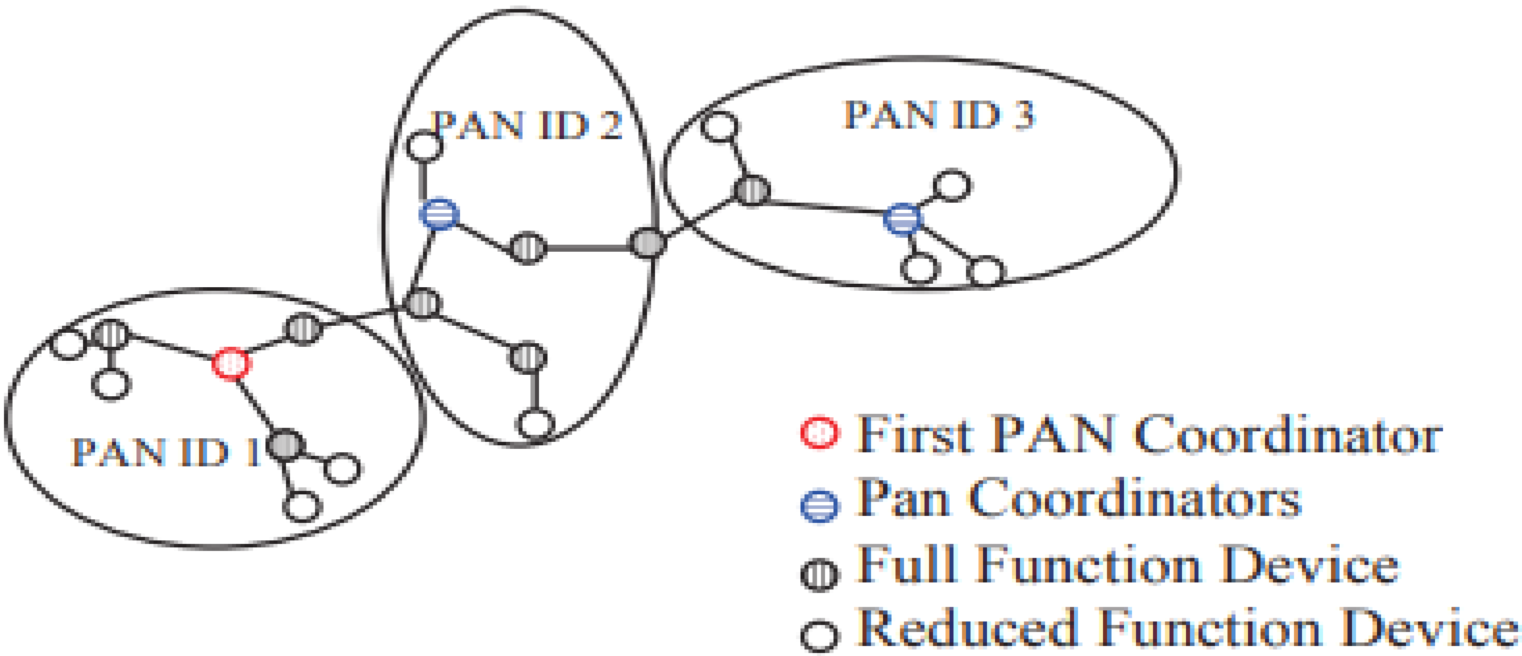


A Mesh Networking Topology

Cluster Tree Network

A coordinator can ask another FFD to become a coordinator for a subset of nodes.

Tree → No loops



IEEE 802.15.4 Characteristics

- Constrained devices regarding power, memory, and CPU.
  - Most of the time these devices are low cost.
- Large number of deployed devices in the network requiring scalable technologies.
- Networks are usually ad hoc networks since their location is usually not predetermined.
  - Some locations may be moving devices
- Low **data rates**: specification allows various data rates from 20 Kbits/s (868 MHz) to 250 Kbits/s (2.45 GHz).
- Support of star and mesh **topologies**

IEEE 802.15.4 Characteristics

- The nodes within a LoWPAN are interconnected by IEEE 802.15.4 links
  - which are usually unreliable, especially when compared to wired links such as Ethernet or fiber-optic links

- very common for nodes to be in sleep mode for long periods of time
  - Depending on the device, it can be in various sleep mode states that have a different impact
    - on the energy consumption in sleep mode and
    - the speed at which the node can wake up

IEEE 802.15.4 Characteristics

- Used by several link layer protocols
- ZigBee, 6LoWPAN, Wireless HART, MiWi, and ISA 100.11a

IEEE 802.15.4: The Header size problem

Worst-case scenario calculations

- Maximum frame size in IEEE 802.15.4: 127 byte

- Reduced by the max. frame header (25 byte): 102 byte
- Reduced by highest link-layer security (21 byte): 81 byte [AES-CCM-128]

- Reduced by standard IPv6 header (40 byte): 41 byte
- Reduced by standard UDP header (8 byte): 33 byte

- This leaves only 33 byte for actual payload
- The rest of the space is used by headers

The 6LoWPAN Adaptation Layer

Since IPv6 mandates supporting links with an MTU (Maximum Transmission Unit) of 1280 bytes

- it was necessary for IEEE 802.15.4 links that have an MTU of 127 bytes to specify an **adaptation layer below IP**
  - responsible for handling packet fragmentation and reassembly

- 6LoWPAN implements an adaptation layer between network and data link layers
  - to support transmission of IPv6 packets over LoWPAN [Low-power Wireless Personal Area Networks]

The 6LoWPAN Adaptation Layer

- A LoWPAN is composed of devices conforming to the **IEEE 802.15.4 standard**

- It effectively becomes part of the Network layer, but only on the specified Data-Link layers

TCP/IP Protocol Stack			6LoWPAN Protocol Stack
HTTP / RTP		Application	Application
TCP / UDP / ICMP		Transport	UDP / ICMP
IP		Network	IPv6 with LoWPAN
Ethernet MAC		Data Link	IEEE 802.15.4 MAC
Ethernet PHY		Physical	IEEE 802.15.4 PHY

After the implementation of the adaptation layer

- it is possible to take routing/forwarding decisions either in
  - the traditional network layer or
  - the adaptation layer.

- **route-over**: If the routing decision is taken in the network layer
- **mesh-under**: if the decision is taken in the adaptation layer

Three main services of 6LoWPAN

The 6LoWPAN adaptation layer provides three main services:

- Packet fragmentation and reassembly
- Header compression
- Link layer (layer 2) forwarding when multi-hop is used by the link layer

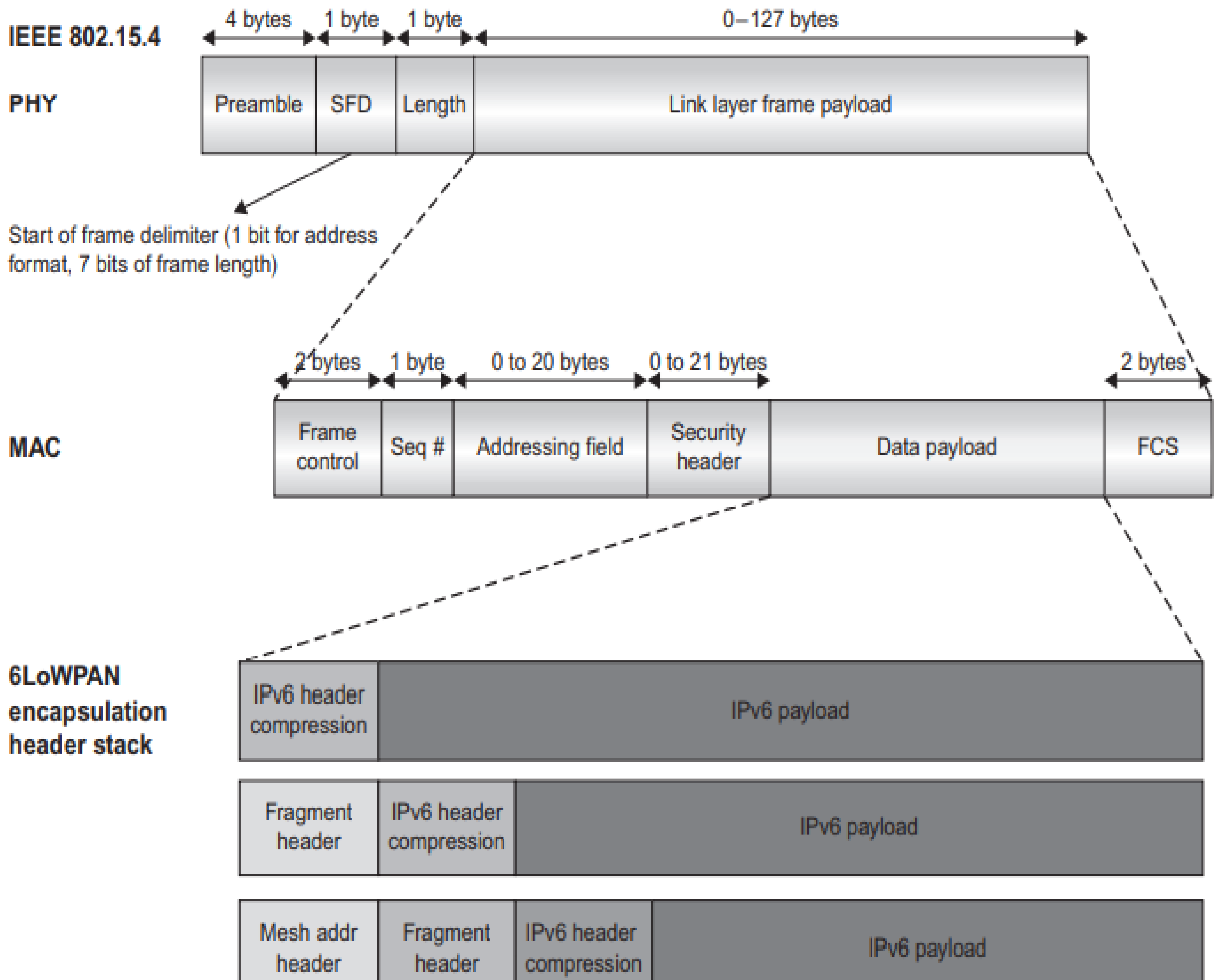
6LoWPAN encapsulation header stack

- Similar to IPv6, The 6LoWPAN adaptation layer defines what is called the "**encapsulation header stack**"
  - headers are added only when needed.
  - precedes each IPv6 datagram
- Mostly the use of efficient compression techniques allows most applications to send their data within a single IPv6 pack

The 6LoWPAN adaptation currently supports three headers

- A mesh addressing header,
- The fragment header, and
- The IPv6 header compression header

6LoWPAN encapsulation header stack



1. Mesh Addressing Header

It is used in **conjunction** with a **mesh-under** "routing" approach where

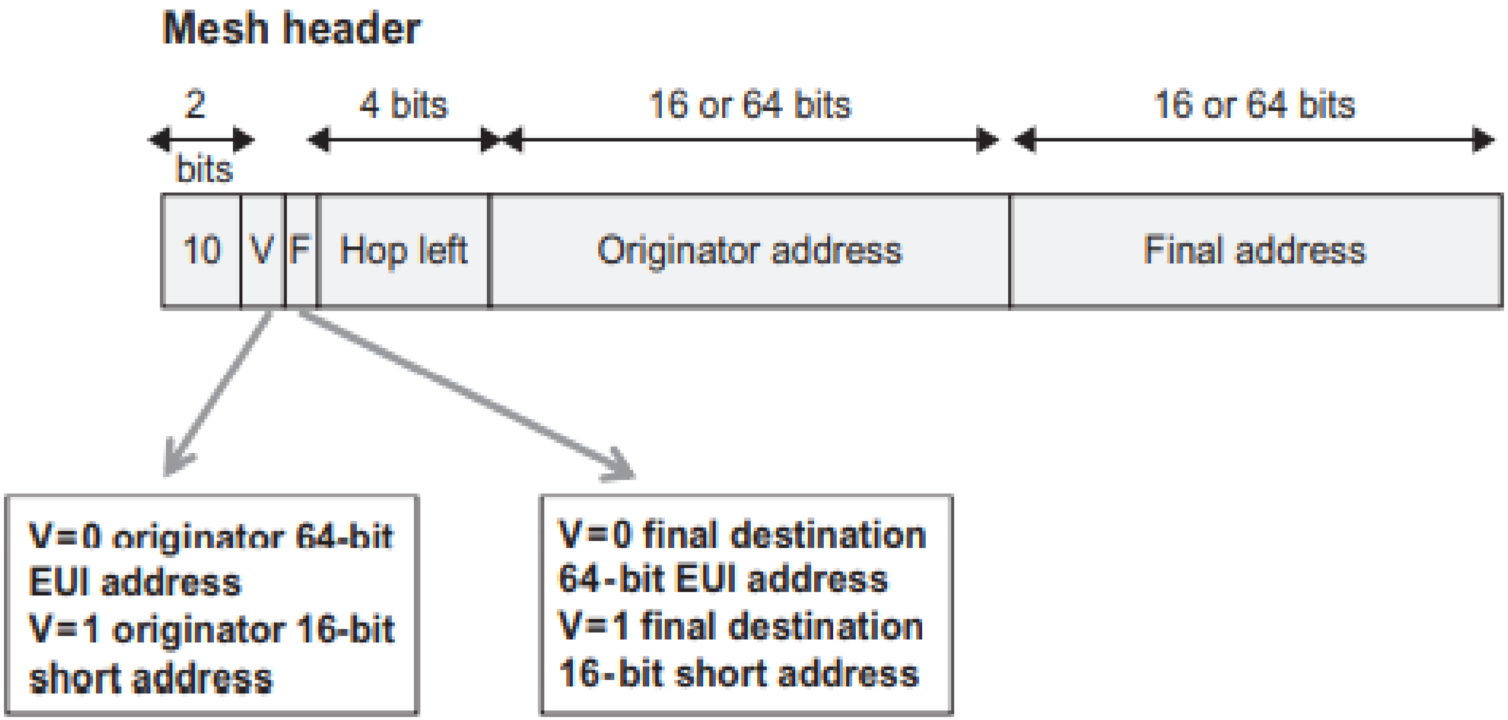
- According to IEEE 802.15.4, only full function devices (FFDs) perform mesh-under operation.

- Reduced function devices (RFDs) systematically send all of their traffic to FFDs.

- With mesh-under routing it is necessary to provide
  - the originator and final destination as well as
  - the hop-by-hop source and destination addresses

1. Mesh Addressing Header

- The first 2 bits (**equal to 10**) of the dispatch byte identify the presence of a mesh header
- possible to use short 16-bit addresses for broadcast and 64-bit addresses as a source address



1. Mesh Addressing Header

- The first 2 bits (equal to 10) of the dispatch byte identify the presence of a mesh header
- When a node A sends a frame to a final destination C via the node B
  - the set of link layer addresses is as follows:

Mesh Header

- The originator address is set to the link layer address of A.
- The final destination address is set to the link layer address of C

IEEE 802.15.4 frame

- The source address is of the node sending the frame (A).
- The destination address is the link layer address of the next-hop node as determined by the mesh-under routing protocol (B in this case).

1. Mesh Addressing Header

Upon receiving the frame, B performs the following process:

- The hop left field is decremented.
- If the hop left field is
  - equal to 0, the frame is discarded
  - not equal to 0, then B determines that the next hop is C.

Mesh Header

- The originator and final destination address are unchanged.

IEEE 802.15.4 frame

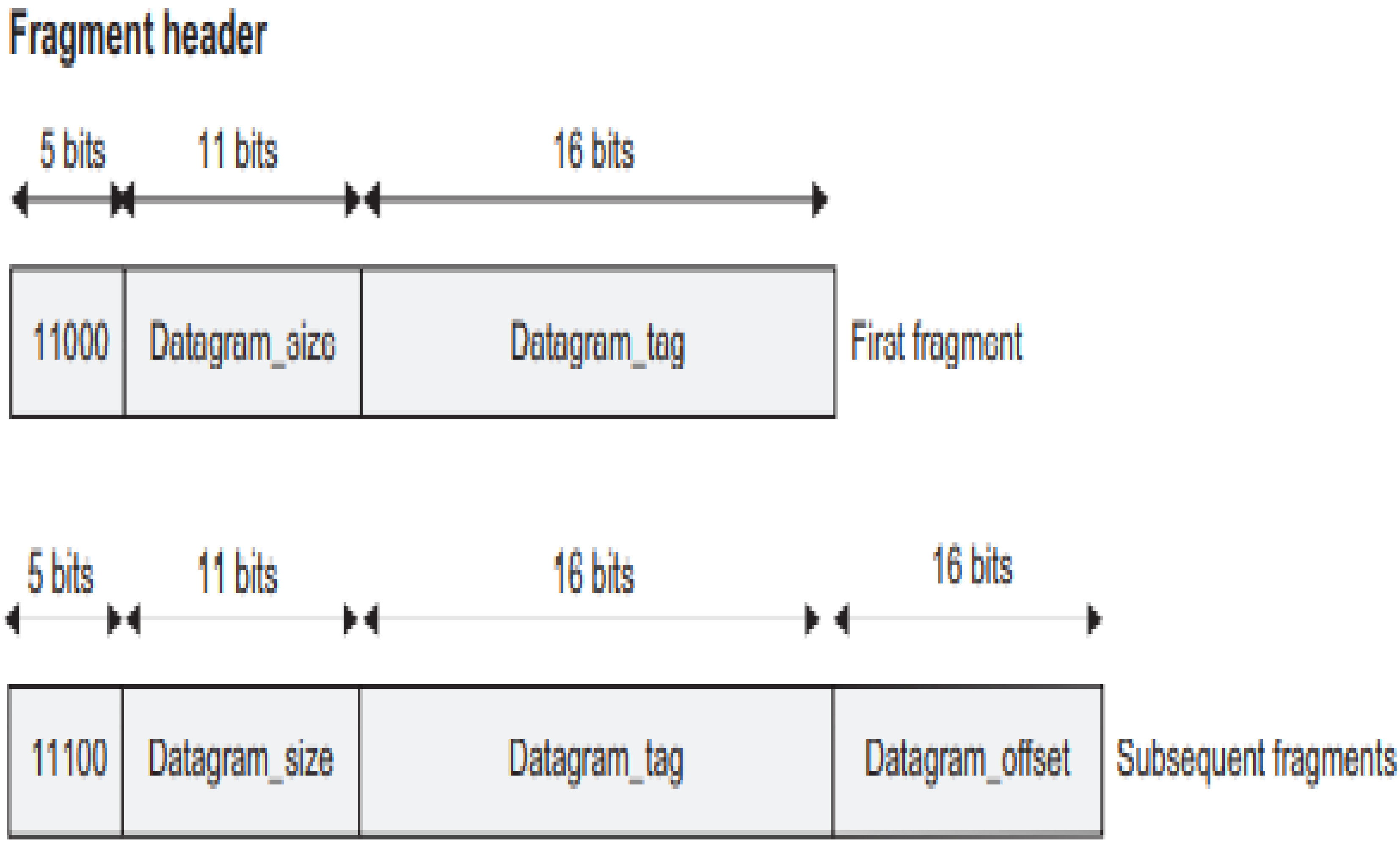
- The source address is set to the link layer address of B.
- The destination address is set to link layer address of C.

2. Fragmentation

When the IPv6 payload cannot be carried within a single IEEE 802.15.4 frame because of MTU size

- Then, fragmentation may be required at the 6LoWPAN adaptation layer
- So, the link frame is broken into multiple link fragments using the fragment header
- All fragment sizes are expressed in units of 8 bytes.

2. Fragmentation



2. Fragmentation

- **Datagram size:** This 11-bit field is used to encode the size in 8-byte units of the original IPv6 packet before link layer fragmentation
- Link layer fragmentation supports a 1280-byte packet as mandated by the IPv6 specification
- The datagram_size may only be needed in the first link fragment and then omitted in other link fragments.
  - **Drawback**: subsequent link fragments may arrive first, especially in the presence of multi-hop routing.
  - Then the receiver would not know how much memory should be allocated for the entire frame.

2. Fragmentation

Datagram_tag:

- The recipients will use this field in conjunction with the
  - IEEE 802.15.4 source address (or originator address if a mesh header is present),
  - the IEEE 802.15.4 destination address (or the final destination address if a mesh header is present),
  - the datagram_size and
  - Datagram_tag
- In order to uniquely identify the fragments of the same IPv6 datagram

- It is recommended to increment the datagram_tag for successive fragmented frames.

2. Fragmentation

Datagram_offset:

- This 8-bit field is present in all link fragments except the first fragment
  - which makes it slightly different from the subsequent fragment

- This indicates the offset in 8-byte units from the beginning of the payload datagram.

3. 6LoWPAN Header Compression

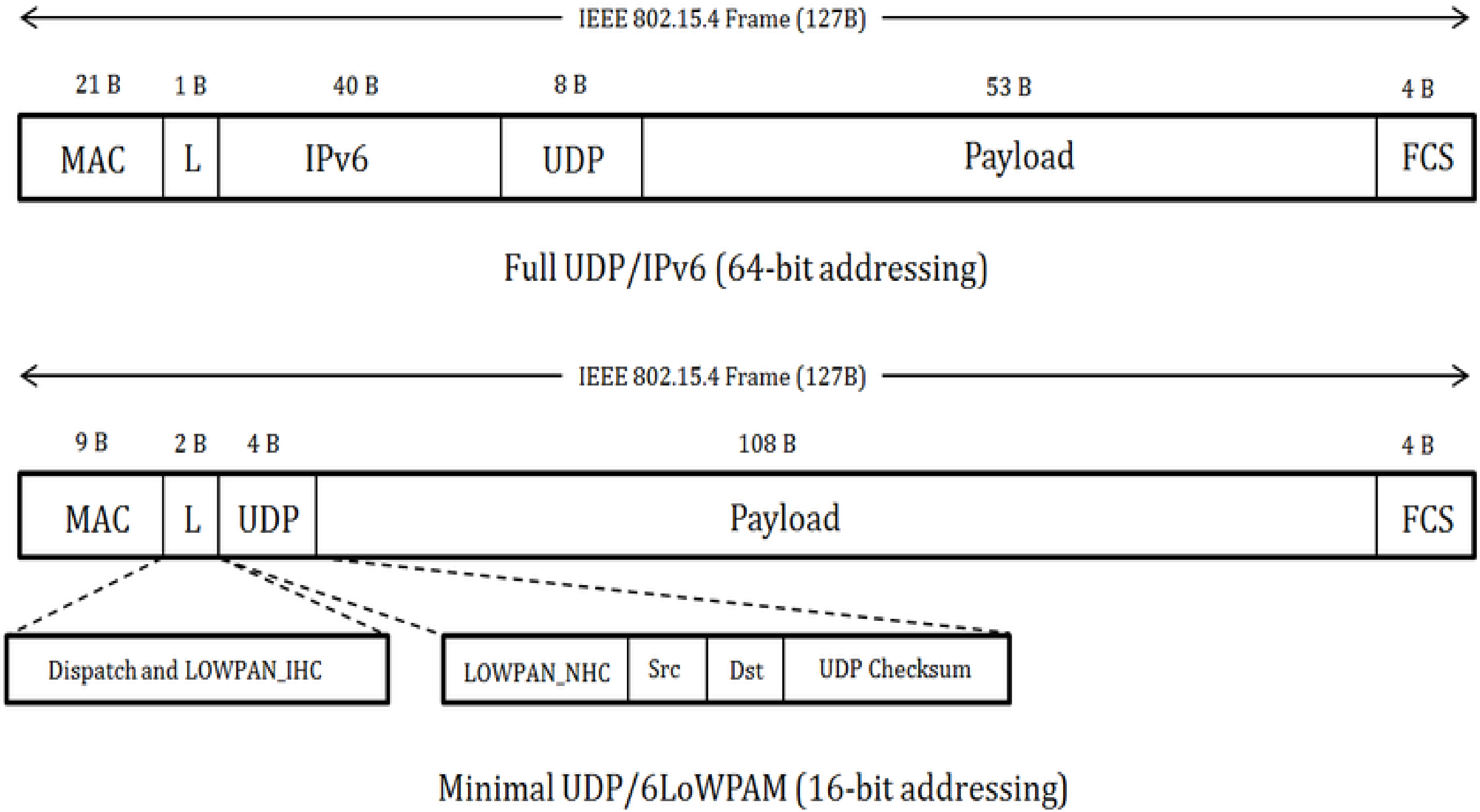
Header Compression (6LoWpANto 6Lo)

- Defined initially in RFC 4944 and updated in RFC 6282
- Reduces the size of IPv6 (40 byte header) and UDP (8 byte header)
  - As low as 6 bytes combined in some cases
- Only defined for an IPv6 header

- 6LowPAN does not support IPv4, and
- There is no standardization IPv4 adoption layer for IEEE 802.15.4

3. 6LoWPAN Header Compression

Header Compression (6LoWpANto 6Lo)



3. 6LoWPAN Header Compression

- Existing IP compression techniques were not suitable for short-lived flows of 6LoWPAN
- so 6LoWPAN developed special header compression methods with a focus on **avoiding information redundancy across layers**
- The general idea is to derive the IP address from link layer addresses
  - to avoid information duplication and suppression of IPv6 headers that have common values
- The use of shared contexts such as the use of a common network prefix allows address compression of IPv6 global addresses
- IPv6 interface ID can be derived from the link layer frame when using extended 64-bit 802.15.4 addresses