SEVENTH FRAMEWORK PROGRAMME
THEME 3
Information & Communication Technologies (ICT)

ICT-213311
OMEGA

Deliverable D4.3

Optical Wireless MAC Specification

Contractual Date of Delivery:	**Month 22**
Actual Date of Delivery:	*16/11/2009*
Editor:	*Olivier Bouchet*
Author:	*Porcon Pascal*
Work package:	*WP4*
Estimated person months:	*10*
Security:	*PU*
Nature:	Report
Version:	*1.0*
Total number of pages:	*85*

Abstract

This document defines a MAC and LLC protocol for Infra Red Communication (IRC) and Visible Light Communication (VLC). This protocol is based on TDMA (Time division multiple access), and Multi-sector transmission, each 67 ms superframe contains 1024 Time Slots (TSs) and each TS duration is 65µs. This protocol defines half duplex transmission (one wave length for transmission and reception) and full duplex transmission (two wavelengths: one wave length for transmission and one for reception for a point to point communication). This protocol handles meshed or star topology, unicast, broadcast and multicast traffic and emergency traffic. This document doesn't define any security mechanism. The switching function is not in the scope of this document.

Keyword list

Optical Wireless MAC, MAC LLC, Optical Wireless, VLC (Visible Light Communication), IRC (Infra Red Communication)

Executive Summary

This document defines a MAC and LLC protocol for Infra Red Communication (IRC) and Visible Light Communication (VLC). This protocol is based on TDMA (Time division multiple access, §1.6), and Multi-sector transmission with one or several transmitter(s) (Tx) and receiver(s) (Rx) and multiple (§1.7). The OWMAC is an adaptation of the Distributed Medium Access Control defined in [5] and the OWLLC is an adaptation of the Wimedia Logical Link Control Protocol defined in [6]. Modifications have been made due to medium and data rate requirements.

Each 67 ms superframe contains 1024 Time Slots (TSs) and each TS duration is 65µs. This protocol defines half duplex transmission (one wave length for transmission and reception) and full duplex transmission (two wavelengths: one wave length for transmission and one for reception for a point to point communication, § 1.8).

The OW-MAC protocol offers an adaptive data rate (the Time slots duration have been chosen for data rates varying from 128 to 1024 Mbit/s, § 8.4) to cope with medium quality changes (§ 2.11). The Link adaptation is based on feedback information which is included in the MAC header (§2.5.11).

A superframe (§ 2.1.1) starts with a BP (Beacon Period) followed by a DP (Data Period). If there is no data to send or receive, a device can switch to power save mode for the rest of the super frame, which means that a device can remain in power save mode 98% of the time for one given superframe.

During the Beacon Period (BP) each device broadcast a Beacon frame to advertise the reserved time slots and to reserve some time slots (or refuse a reservation from a neighbour).

An 8 µs SIFS (Short InterFrame Space) is used between a Frame and an Ack and a Guard Time of 16 µs (2 SIFS) is used for the last TS (§ 2.4.2).

The PHY (PHYsical) layer (§ 1.2) starts with a preamble, which is a synchronisation sequence, followed by a PLCP (Physical Layer Convergence Procedure) Header.

This PLCP Header includes the PHY header (§ 1.4), the MAC header (§ 2.5.1) and the PLCP header code correction field (Reed Solomon), followed by the Frame Payload and the FCS (Frame Check Sequence - § 2.5.13).

This protocol uses the same MAC frame format (§ 2.5) for every frame type, with a fixed-length MAC Header and a variable-length MAC frame body. As mentioned above, the Beacon frame (§ 2.6) is mainly used to reserve Time slots (or refuse a reservation) and to advertise the time slots reserved by its neighbours. Once a device has reserved some Time Slots with a neighbour (with MAC frames), the device can discover (§ 3.4.1), enroll (§ 3.4.2) and connect (§ 3.4.3) to this neighbour with OWLLC frames. Once connected to another neighbour, the device can send data in the reserved Time Slots.

To gain in efficiency in terms of time processing, a device can use a tunnel mode (§ 2.13), the Ethernet frames are directly encapsulated in OWMAC Frame, thus, with this mode there is no need to remove the Ethernet header when receiving an Ethernet frame, before sending the corresponding OWMAC frame. Note that we could encapsulate any other layer two protocol in OWMAC frames, other Protocol ID value would then have to be defined.

Finally, this protocol handles meshed or star topology. The first section is a general description of the OWMAC layer (Optical wireless MAC) and OWLLC layer (Optical wireless LLC). The second section describes the MAC layer: the MAC service functionality, the multiplexing sublayer, the Service Access Points, the MAC frame formats, the Beacon frames, the control frames, the Beacon period and the reservation protocol. The third section describes the OWLLC layer: the OWLLC frame format, the attribute fields and the functions handled by the OWLLC protocol.

List of Authors

First name	Last name	Beneficiary	Email address
Pascal	Porcon	FT&RD	pascal.porcon@orange-ftgroup.com

History

Version	Date	Comments
V0.1	1/11/2008	First release
V0.2	22/12/2008	Length field of MAC IE set to 2 octets. Beacon transmission procedure updated.
V0.3	15/01/2009	OWLLC attribute type updated
V0.4	14/05/2009	SDMA function & multi-rate added
V0.5	28/05/2009	Multicast and broadcast multi-sector transmission description
V0.6	24/062009	Multi-sector transmission. Full duplex transmission.
V0.7	04/06/2009	Abstract & miscellaneous errors, correction
V0.8	04/10/2009	PHY Header description removed, multi-sector transmission updated
V1.0	13/11/2009	Typo and final edition

List of Acronyms

Acronym	Meaning
AC	Access Category
ACK	Acknowledgment
Block-Ack	Block Acknowledgment
BP	Beacon Period
BPST	Beacon Period Start Time
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
EUI	Extended Unique Identifier
HCS	Header Check Sequence
IE	Information Element
IFS	Inter-Frame Space
IP	Internet Protocol
IRC	Infra Red Communication
MAC	Medium Access Control
TS	Time Slot
MCDU	MAC command data unit
MLME MAC	Sublayer Management Entity
MPDU	MAC protocol data unit
MSDU	MAC Service Data Unit
MTU	Maximum Transmission Unit
NAV	Network Allocation Vector
OUI	Organizationally Unique Identifier
OWLLC	Optical Wireless Logical link Control
OWSS	Optical Wireless service set
OWSSID	Optical Wireless service set identifier
PHY	Physical Layer
PLCP	Physical Layer Convergence Protocol
PLME	Physical Layer Management Entity
PPDU	PHY Protocol Data Unit
PSDU	PHY Service Data Unit
QoS	Quality of Service
RP	Reservation protocol

RSSI	Received Signal Strength Indicator
RTS	Ready to Send
SAP	Service Access Point
SDMA	Space Division Multiple Access
SIFS	Short Inter-Frame Space
SNR	Signal to Noise Ratio
TDMA	Time Division Multiple Access
TIM	Traffic Indication Map
TSPEC	Traffic Specification
UUID	Universally Unique Identifier
VLAN	Virtual Local Area Network
VLC	Visible Light Communication

Table of contents

List of Tables

List of Figures

1 General Description

1.1 General description of the architecture

This document defines a MAC and LLC service and protocol. As shown in Figure 1, the MAC sublayer corresponds to the MAC sublayer of the standard ISO/OSI-IEEE 802 reference model [3]. The MAC service is provided by means of the MAC service access point (MAC SAP) to the LLC sublayer.

The LLC corresponds to the logical link control sublayer of the standard ISO/OSI IEEE 802 reference model [3] and is called Optical Wireless Logical Link Control Protocol (OWLLC). The OWLLC service is provided by means of the OWLLC service access point (OWLLC SAP) to a higher layer protocol.

The MAC sublayer in turn relies on the service provided by the PHY layer via the PHY service access point (PHY SAP). The MAC protocol applies between peer MAC entities and the OWLLC protocol applies between peer OWLLC entities. The MAC layer uses volatile abbreviated address called a DevAddr, whereas the OWLLC layer uses EUI-48 [2] to connect two devices.

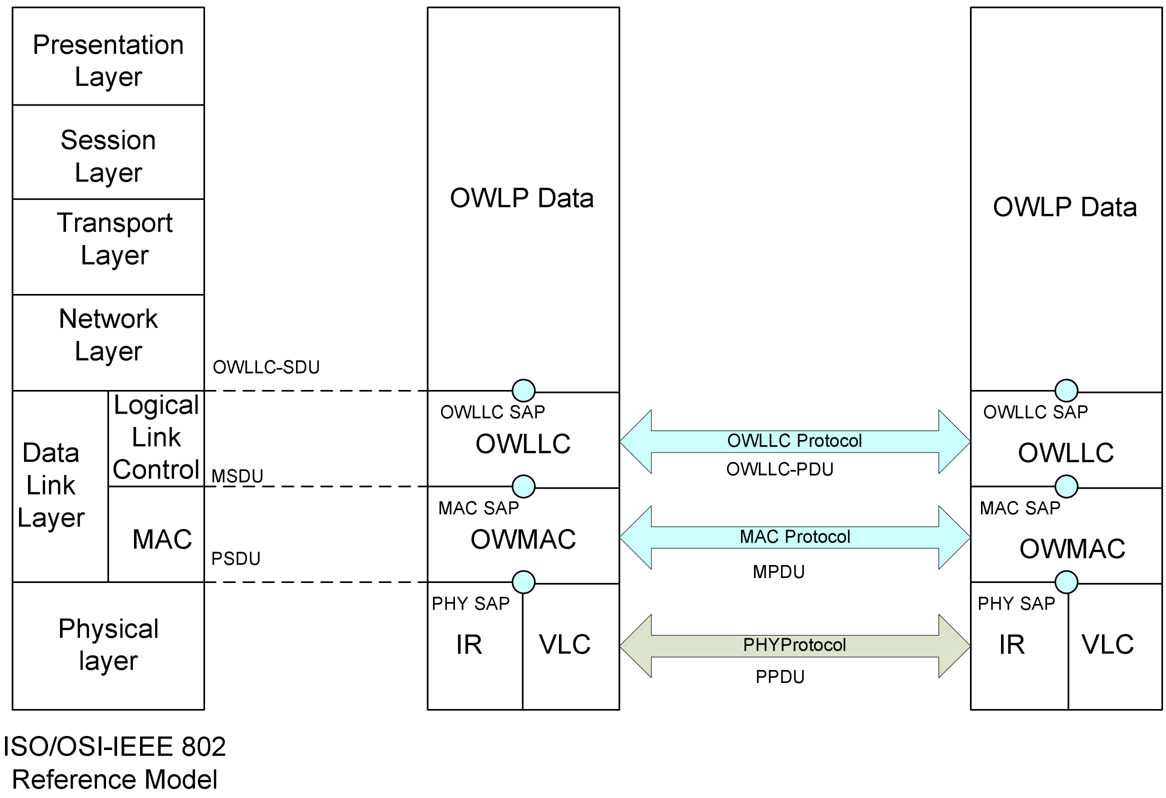


Figure 1: Architectural reference model

The MAC layer uses volatile abbreviated 2 octets address called a DevAddr. The destination DevAddr changes on a hop by hop basis. The OWLLC layer uses EUI-48 [2] to connect two devices as, the destination OWLLC address is therefore not modified. When the OWLLC destination address and the destination MAC address are the same, a device can send an abbreviated frame with no OWLLC address as described in Figure 2.

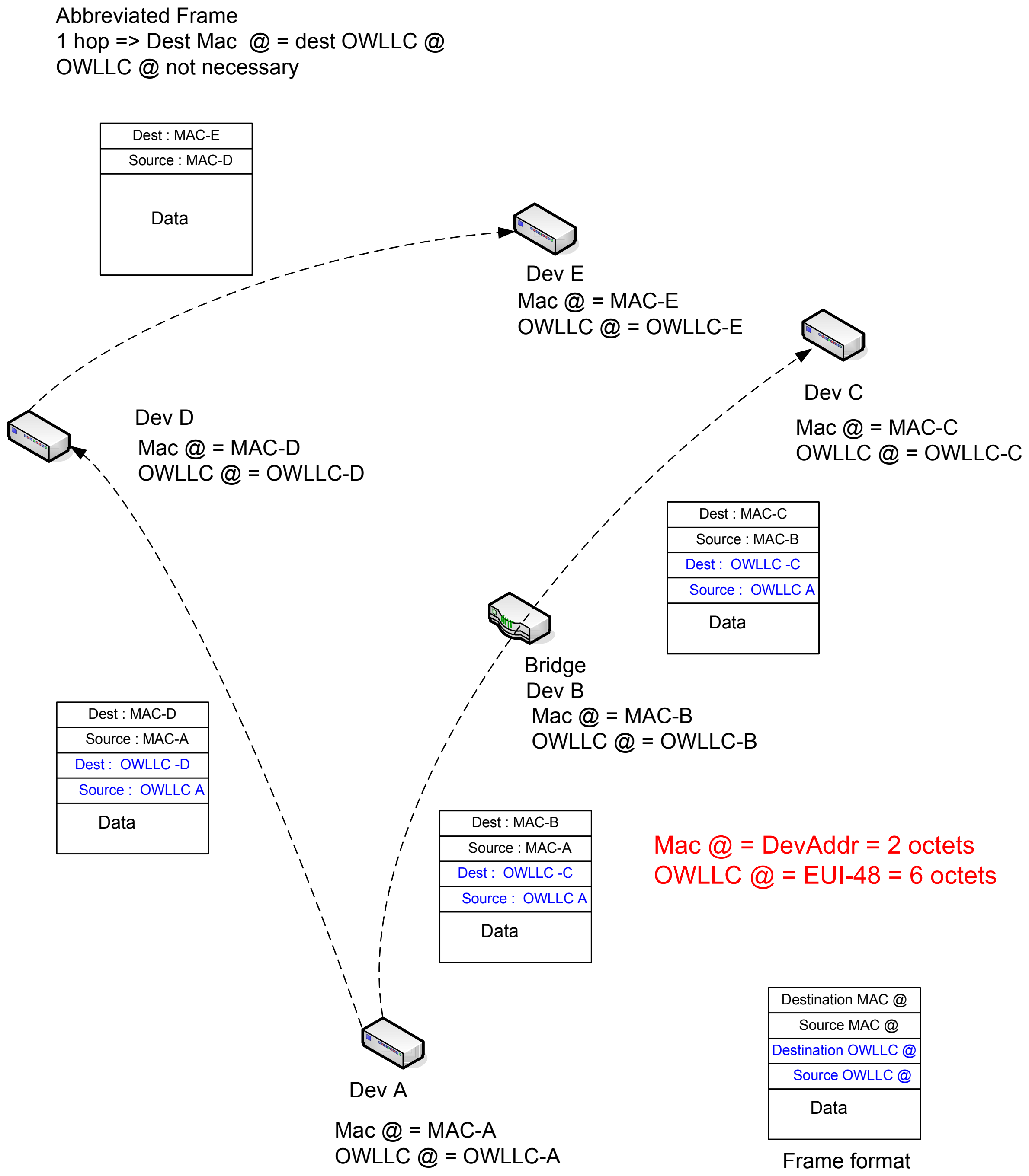


Figure 2: Data exchange example

1.2 Features assumed from the PHY

A MAC entity is associated with a single PHY entity via that entity's PHY SAP. The PHY SAP is not defined in this document.

The MAC sublayer requires the following features provided by the PHY:

- Frame transmission
- Frame reception
- PLCP header error indication (or correction) for both PHY and MAC header structures
- Clear channel assessment for estimation of medium activity
- The PHY preamble.
- The PLCP header including MAC and PHY Headers and is protected by a 16 octets Reed Solomon error correction code.
- The Frame Payload is followed by its frame check sequence (FCS).

Figure 3 shows the structure of a PHY frame.

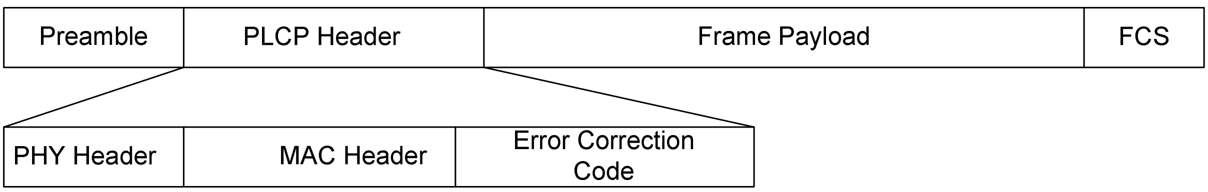


Figure 3: PHY Frame Structure

Frames are transmitted by the PHY from the source device and delivered to the destination device in identical bit order. The IRC Preamble or training sequence is defined in OMEGA Document D4.2 [7] and should be used for Line Clock recovery. The preamble is defined in Document D4.2 [7]. The IRC Preamble or training sequence should be 100 bytes and should be used for Line Clock recovery. No preamble is needed for VLC as OFDM is used. The error correction code field is a 16 octets Reed Solomon error correction code.

1.3 Data format convention

MAC frames are described as a sequence of fields in a specific order Figure 4 depict fields in the order they are delivered to the PHY SAP, from top to bottom, where the least-significant bit is transmitted first in time. In field figures, bits within the field are numbered from the least-significant bit on the left to the most-significant bit on the right.

Unless otherwise noted, fields longer than a single octet are delivered to the PHY SAP in order from the octet containing the least-significant bits to the octet containing the most-significant bits. And for each octet the least-significant bit is transmitted first in time.

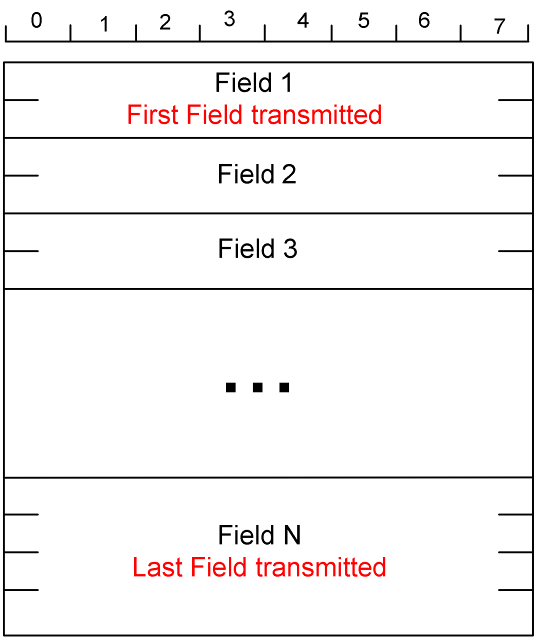


Figure 4: Example sequence of field

1.4 MAC Header protection

Why do we need to protect the MAC header with an error correction code, while the rest of the payload is not protected? Simply because we want to protect the Acknowledgement frames, to make sure that when a station receives a frame with no error, the corresponding acknowledgement sent by the station, will be correctly decoded or corrected if necessary, avoiding retransmission as much as possible. That's why the PLCP header includes the MAC header.

1.5 TDMA (Time Division Multiple Access)

We use TDMA because this is the only way to avoid collision and retransmission. Each device can reserve a time slot, and advertise the reservation in a Beacon frame, preventing other stations to use the medium during the reserved time slot. TDMA also prevents stations from using admission control mechanisms and RTS/CTS frames that consume bandwidth. Thus, all the times slots (apart from the Beacon period) can be used to send traffic.

1.6 Multi-sector transmission

We use Multi-sector transmission to be able to send data in a wider area (see Figure 5). The covered area, where equipment can send and receive data, is divided n sectors (seven in the example below). As we use TDMA, two devices cannot send data at the same time (except in full duplex mode if the two devices exchange data). If for instance, 4 equipments can connect to each other, but if two equipments exchange data in one sector and the other two equipments exchange data in another sector, they won't send data at the same time, they should use different time slots. The sectors should overlap, to allow seamless changes between sectors. For transmission, a device shall send the Beacons in n sectors with n LEDs. It shall transmit the same Beacon in each sector at the same time. For Data transmission, it's up to the implementation, to transmit the frame in one selected sector (the sector with the best received signal) or in all sectors. The choice of the method to select the best sector for transmission and reception is beyond the scope of this specification.

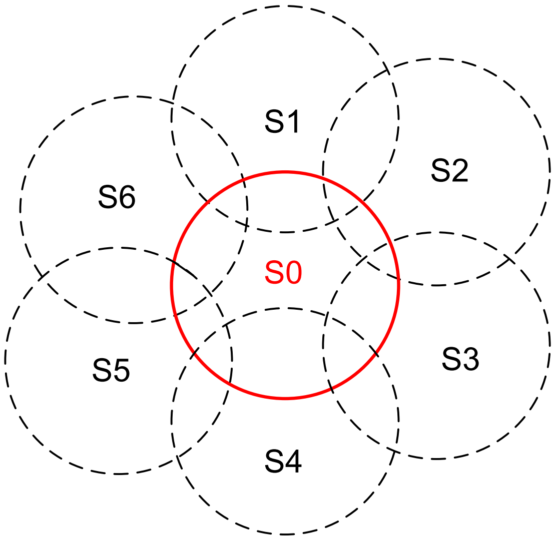


Figure 5: Multi-sector transmission with 7 sectors

The limit of the sectors shown in the figure above is the limit where you receive enough signal to be able to receive a proper frame that means that the actual sector where you transmit signal is larger.

1.7 Half duplex and full duplex transmission

This protocol defines half duplex transmission and full duplex transmission. In half duplex mode, the same wave length is used for transmission and reception, each device must reserve its own time slots to be able to send data, but they can't reserve the same time slots, you can't therefore receive and send data at the same time. In full duplex mode, two wavelengths are used, one wave length for transmission and one for reception. Each device must reserve its own time slots to be able to send data, but they can reserve the same time slots, you can therefore receive and send data at the same time. Note that you can reserve time slots that are already reserved, only if these time slots are used to send data to the device which has already reserved these timeslots.

2 MAC Layer description

2.1 Overview of MAC service functionality

The MAC service defined in this specification provides:

- Communication between cooperating devices within optical range on a single channel using the PHY;
- A distributed, reservation-based channel access mechanism;
- Multi-sector transmission
- A synchronization facility for coordinated applications;

The architecture of this MAC service is fully distributed. All devices provide all required MAC functions and optional functions as determined by the application. No device acts as a central coordinator.

Coordination of devices within optical range is achieved by the exchange of beacon frames. Periodic beacon transmission enables device discovery, supports dynamic network organization, and provides support for mobility. Beacons provide the basic timing for the network and carry reservation and scheduling information for accessing the medium.

2.1.1 The superframe

The basic timing structure for frame exchange is a superframe. The superframe duration is 67,108864 ms.The superframe is composed of 1024 Time Slots (TSs), where each TS duration is 65,536 µs.

Each superframe starts with a Beacon Period (BP), which extends over one or more contiguous Beacon slot. The duration of one Beacon slot is 2xTSs. The start of the first TS in the BP, and the superframe, is called the beacon period start time (BPST).

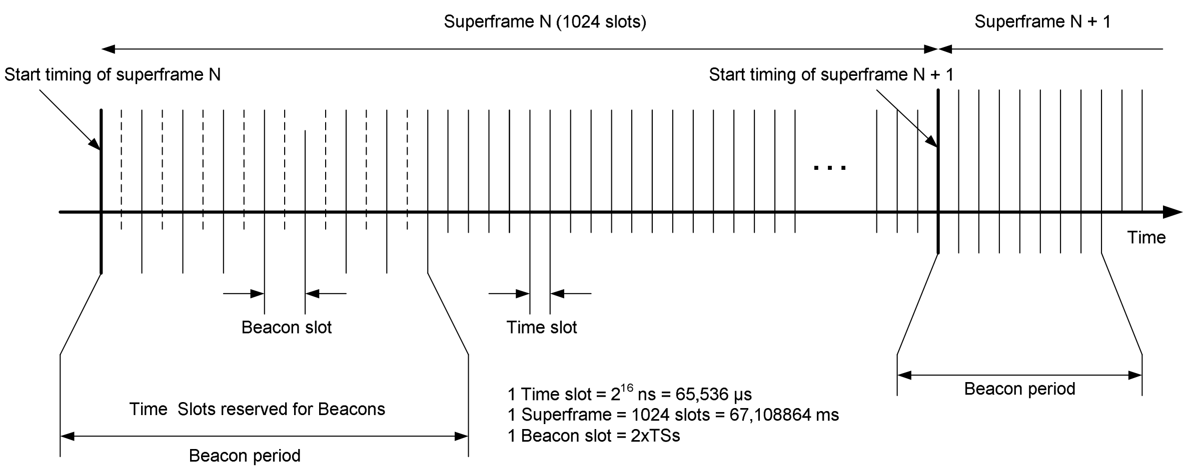


Figure 6: MAC SuperFrame Structure

2.1.2 Beacon period protection

Each device protects its and its neighbours' BPs for exclusive use of the beacon protocol. No transmissions other than beacons are attempted during the BP of any device. Protection of the device's BP is implicit.

2.1.3 Medium access

The medium is accessed in one of two ways:

- During the BP, devices send only beacon frames.
- During reservations, devices participating in the reservation send frames in half duplex or full duplex mode.

2.1.4 Data communication between devices

Data is passed between the MAC entity and its client in MSDUs. MSDUs are transported between devices in data frames. To reduce the frame error rate of a marginal link, data frames can be fragmented and reassembled. Fragments are numbered with an MSDU sequence number and a fragment number.

If the source device wishes to verify the delivery of a frame, then one of the acknowledgement policies is used. This specification provides for three types of acknowledgements to enable different applications. The No-ACK policy, is appropriate for frames that do not require guaranteed delivery, or are delay sensitive and a retransmitted frame would arrive too late. The ACK policy, provides an acknowledgement process in which each frame is individually acknowledged following the reception of the frame. The BLOCK-ACK policy, lets the source send multiple frames without intervening ACK frames. Instead, the acknowledgements of the individual frames are grouped into a single response frame that is sent when requested by the source device. The BLOCK-ACK process decreases the overhead of the ACK process while allowing the source device to verify the delivery of frames to the destination.

If the source device does not receive the requested acknowledgement, then it may retransmit the frame, or it may discard the frame. The decision to retransmit or discard the frame depends on the type of data or command that is being sent, the number of times that the source device has attempted to send the frame, the length of time it has attempted to send the frame, and other implementation-dependent factors.

2.1.5 MAC frame data rates

MAC beacon frames are intended to be received and interpreted by all devices and hence their frame payloads are transmitted at the lowest available data rate (the lowest data rate should be defined in Document D4.2 [7], depending on the required and available range), which can be decoded by all recipients. Other frames are exchanged in a more restricted context and their frame payloads may be transmitted at higher data rates if possible (the available data rates should be defined in OMEGA internal Document D4.2 [7], depending on the required and available range). The choice of the data rate could be based on the received BER, RSSI, packet loss or other information regarding the channel condition. This information should be included in the MAC Header in the Feedback information field. Frame headers are always transmitted at the lowest data rate supported by the PHY.

2.1.6 Information discovery

The protocols and facilities of this specification are supported by the exchange of information between devices. Information can be broadcast in beacon frames or requested in Probe commands. For each type of information, an Information Element (IE) is defined. IEs can be included by a device in its beacon at any time and may optionally be requested or provided using the Probe command.

A device uses the MAC Capabilities IE and PHY Capabilities IE to announce information about its support of variable or optional facilities. Declaration of capabilities is especially useful when a device detects changes in its immediate neighbourhood.

2.2 Multiplexing sublayer

In order to enable the coexistence of concurrently active higher layer protocols within a single device, a multiplexing sublayer is defined. This sublayer routes outgoing and incoming MSDUs to and from their corresponding higher layers.

2.2.1 Multiplexing service

The MULTIPLEXING sublayer is expressed in terms of the MULTIPLEXING SAP, the MULTIPLEXING service, and the MULTIPLEXING client. Each MULTIPLEXING client is associated with a unique protocol. Service data units presented at the MULTIPLEXING SAP by the MULTIPLEXING client are therefore associated with that protocol.

The protocol is encoded in a MULTIPLEXING header as either:

- A protocol identifier and an OUI; or
- An IEEE Ethernet type value [1].

The MULTIPLEXING service adds a MULTIPLEXING header to the MULTIPLEXING service data unit to construct a MULTIPLEXING protocol data unit. The MULTIPLEXING sublayer makes use of the service provided by the MAC sublayer for the transfer of its protocol data units.

On receipt of a MULTIPLEXING protocol data unit from the MAC sublayer, the MULTIPLEXING service removes the MULTIPLEXING header and delivers the transported service data unit to the appropriate MULTIPLEXING client based on the identified protocol.

2.2.2 Multiplexing protocol data unit format

A MULTIPLEXING protocol data unit consists of a MULTIPLEXING Header and a MULTIPLEXING Payload and is illustrated in Figure 7.

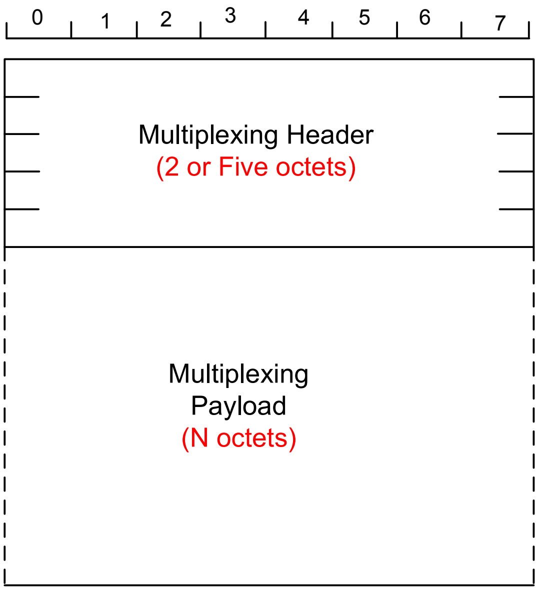


Figure 7: MULTIPLEXING protocol data unit format

The MULTIPLEXING Payload field contains the MULTIPLEXING service data unit that is a payload data unit of the protocol identified in the MULTIPLEXING Header.

The first two octets of the MULTIPLEXING Header are encoded as unsigned binary values, and are delivered to the MAC sublayer in order from the octet containing the most-significant bits to the octet containing the least-significant bits. The octet order for this field is the reverse of that for most fields in this specification.

There are three versions of the MULTIPLEXING Header, which are distinguished based on the value of the first two octets of the header.

2.2.2.1 MULTIPLEXING Header—OUI version

The first version has a length of five octets and is illustrated in Figure 8.

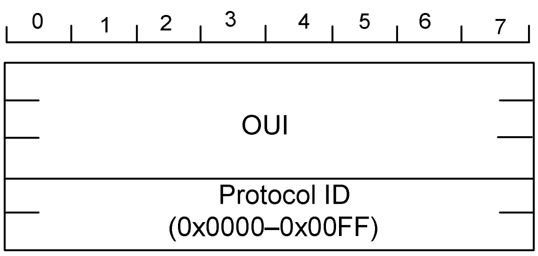


Figure 8: Format of first version of MULTIPLEXING Header

The OUI is a sequence of 3 octets.

The Protocol ID field is restricted to values from 0 through 255 and is set to a value that identifies a protocol defined by the owner of the OUI specified in the OUI field.

2.2.2.2 *MULTIPLEXING Header—reserved version*

The second version of the MULTIPLEXING Header has a length of 2 octets and is illustrated in Figure 9.

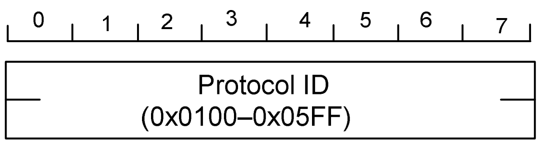


Figure 9: Format of second version of MULTIPLEXING Header

The Protocol ID field is restricted to values from 256 through 1535. These values identify the protocol that defines the MULTIPLEXING Payload format.

2.2.2.3 *MULTIPLEXING Header—Ethernet type version*

The third version of the MULTIPLEXING Header has a length of two octets and is illustrated in Figure 10.

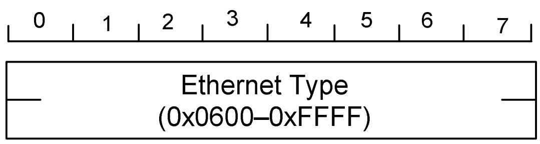


Figure 10: Format of third version of MULTIPLEXING Header

The Ethernet Type field is restricted to values from 1536 through 65535 and is set to the value of an Ethernet type [1] identifying a protocol.

2.3 Service access points

Service access points (SAPs) are provided for both data transfer as well as management of the MAC sublayer. Data transfer for the MAC sublayer is through the MAC SAP.

Both the MAC sublayer and the PHY layer conceptually include management entities, called the MAC sublayer management entity (MLME) and physical layer management entity (PLME). These entities provide the layer management service interfaces for the layer management functions. In order to provide correct MAC protocol operation, a device management entity (DME) should be present within each device. The DME is a layer-independent entity that may be viewed as residing in a separate management plane or as residing “off to the side.” The functionality of the DME may be viewed as being responsible for such functions as the gathering of layer-dependent status from the various layer management entities, and similarly setting the value of layer-specific parameters. The DME typically performs such functions on behalf of the general system management entities and implements standard management protocols. Figure 11 depicts the relationship among the management entities.

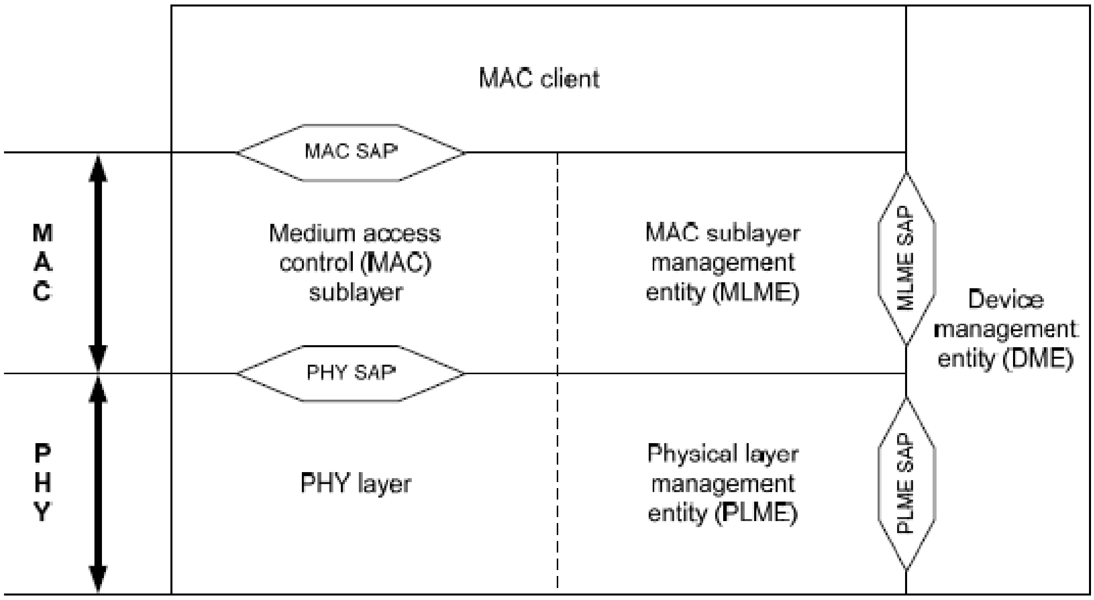


Figure 11: The SAP reference model

2.4 MAC sublayer functional description

Channel time is divided into superframes, with each superframe composed of two major parts, the beacon period (BP) and the data period.

During the data period devices send and receive data using reservations established using the reservation protocol (RP).The RP enables a device to gain scheduled access to the medium within a negotiated reservation. In full duplex mode, a device can reserve time slots that are already reserved, only if these time slots are used to send data to the device which has already reserved these timeslots.

2.4.1 Frame reception

Unless otherwise indicated, a frame is considered to be received by the device if it has a valid header check sequence (HCS) and frame check sequence (FCS) and indicates a protocol version that is supported by the device. The HCS is validated by the PHY, which indicates whether or not a header error occurred.

A frame header is considered to be received by the device if it has a valid HCS and indicates a protocol version supported by the device, regardless of the FCS validation.

2.4.2 Frame transaction

A frame transaction consists of a single frame, and the associated acknowledgement frame if requested by the ACK policy.

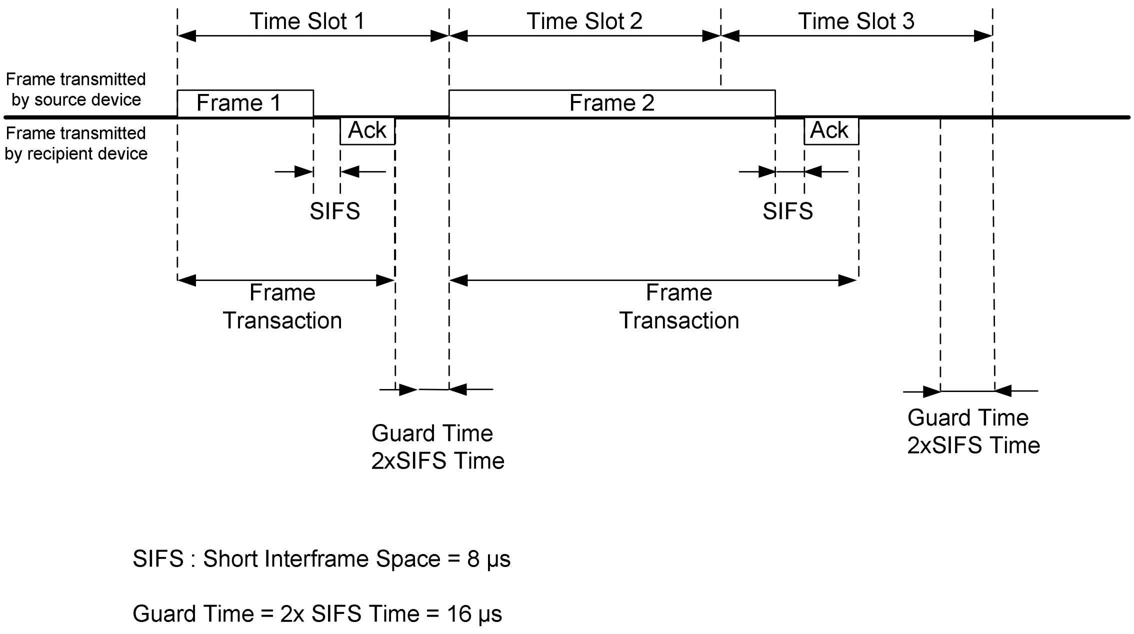


Figure 12: Frame transaction

2.4.3 Frame transfer

A source device shall transmit MSDUs associated with the same Delivery ID and addressed to the same destination EUI-48 in the order in which they arrived at the local MAC SAP. The device shall transmit fragments of an MSDU or MCDU in order of increasing fragment number.

The MAC entity shall translate the EUI-48 provided by the OWLLC layer along with an MSDU to the DevAddr of the target for use in the transmission of the MSDU over the medium. A source device may reorder MSDUs for transmission if their associated Delivery IDs or destination EUI-48s are different. A recipient device shall release MSDUs to the OWLLC layer that was transmitted by the same source device with the same Delivery ID in order of increasing sequence number values.

2.4.4 Frame retry

A frame retry is a retransmission of a previously transmitted frame from the same source device to the same recipient device. In a frame that is retransmitted, the source device shall set the Retry bit to one.

The device will retry transmission of a MPDU until the retry limit is reached. The retry limit is 6.

After transmitting an MPDU that requires an ACK frame as a response, the device shall wait for an ACKTimeout interval=2x8µs, If the device hasn't received an ACK during the ACKTimeout interval, the

Device concludes that the transmission of the MPDU has failed, and this device shall retransmit the MPDU. The recognition of a valid ACK frame sent by the recipient of the MPDU requiring acknowledgment shall be interpreted as successful acknowledgment, permitting the frame sequence to continue, or to end without retries, as appropriate for the particular frame sequence in progress. The recognition of anything else, including any other valid frame, shall be interpreted as failure of the MPDU transmission.

2.4.5 Inter-frame space (IFS)

Only one type of IFS is used in this specification: the short inter-frame space (SIFS)

A device shall not start transmission of a frame on the medium with non-zero length payload earlier than SIFS, after the end of a frame it transmitted previously on the medium. A device shall not start transmission of a frame on the medium earlier than SIFS duration after the end of a previously received frame on the medium.

2.4.6 Synchronization of devices

Each device shall maintain a beacon period start time (BPST). The device shall derive all times for communication with its neighbours based on the current BPST. The device shall adjust its BPST in order to maintain superframe synchronization with its slowest neighbour. Hence all devices synchronise with the slowest neighbour. A device shall synchronize with such a device before it sends its first beacon.

When a device receives a beacon from a neighbour, the device determines the difference between the beacon's actual reception time and the expected reception time. The beacon's actual reception time is an estimate of the time that the start of the beacon preamble arrived at the receiving device's antenna. The expected reception time is determined from the Beacon Slot Number field of the received beacon and the receiving device's BPST. If the difference is positive, then the neighbour is slower. In order to maintain superframe synchronization with a slower neighbour, the device shall delay its BPST by the difference, but shall limit the adjustment to a maximum of 4 µs per superframe. This might require adjustment of its BPST in multiple superframes, based on the latest BPST observed via any beacon received from a neighbour in the last 4 superframes.

A device must consider its own sampling and round-off error in calculating the BPST difference, and shall ensure that the BPST it indicates via its beacons is not later than the known or estimated BPST of its slowest neighbour in the previous superframe. The adjustment to BPST may occur at any time following the detection of a slower device, but shall be done before the end of the superframe.

A device shall not use a beacon with the Signalling Slot bit set, for synchronization.

If a device does not receive a beacon from a neighbour, the device may use historical measurements to estimate the impact on superframe synchronization and increment its BPST accordingly. This estimate may be applied for up to 3 consecutive superframes.

Beacon transmit time and measured beacon receive time shall be accurate to at least 1 µs.

2.4.7 Clock accuracy

A device shall maintain a clock at least as accurate as 1 µs. All time measurements, such as TS boundary and frame reception time measurements, shall be measured with a minimum resolution of 1 µs.

2.4.8 Guard times

Due to inaccuracies in superframe synchronization and drift between synchronization events, TS start times for different devices are not synchronized perfectly. To ensure a full SIFS interval between transmissions in adjacent TSs, the devices shall maintain two SIFS interval as guard interval at the end of a reservation block.

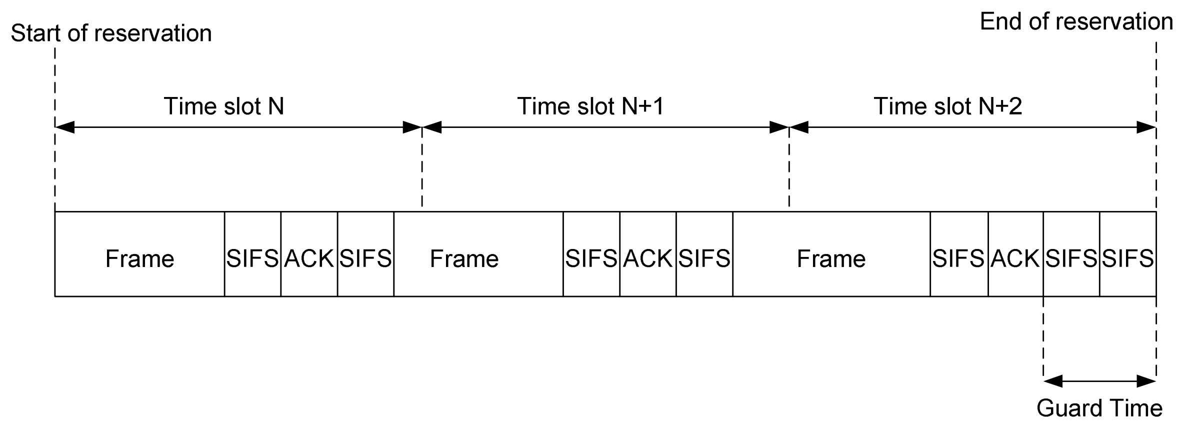


Figure 13: Guard Time description

2.5 MAC Frame Formats

2.5.1 General MAC frame format

A MAC frame consists of a fixed-length MAC Header and an optional variable-length MAC Frame Body.

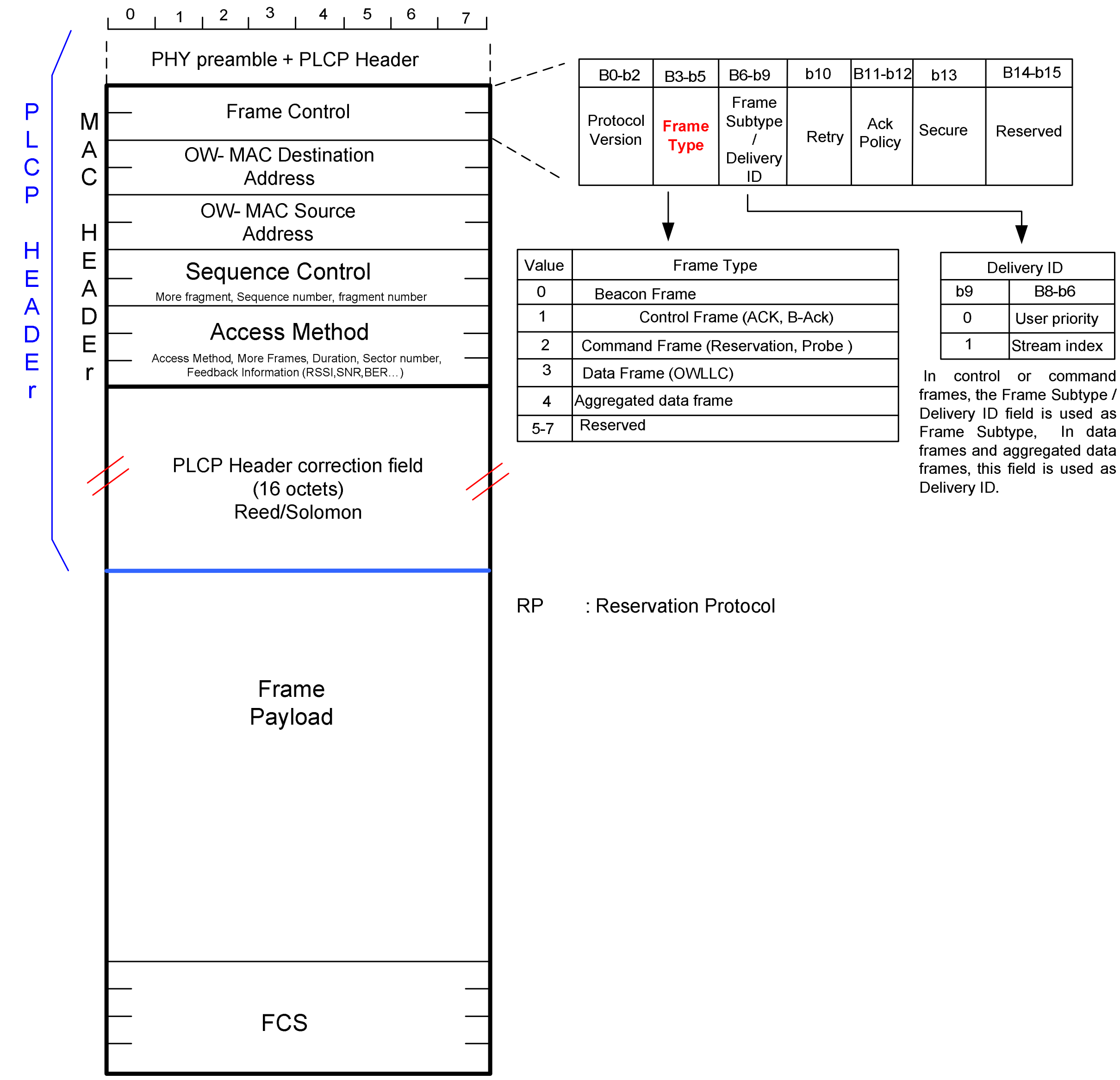


Figure 14: General MAC Frame format

The Frame Payload length ranges from zero to **MaxFramePayloadSize= 4095 octets**. If the Frame Payload length is zero, the FCS field is not included, and there is no MAC Frame Body. The Frame Payload length includes the length of the security fields for a secure frame.

The user priority bits in the delivery ID field (in the MAC header), won't be used until a CSMA/CA solution is specified.

2.5.2 Protocol Version

For this revision of the specification, the Protocol Version is set to zero. All other values are reserved.

2.5.3 Secure

The Secure bit is set to one in a secure frame, which is protected using a temporal key (to be defined). The Secure bit is set to zero otherwise. For the prototype, the frames should be sent with the Secure bit is set to zero.

2.5.4 ACK Policy

The ACK Policy field is set to the type of acknowledgement requested by the transmitter. The allowed values for the ACK Policy field are defined in Table 1 - ACK Policy field encoding.

Table 1 - ACK Policy field encoding

Value	ACK policy type	Description
0	No-ACK (undefined)	The recipient(s) do not acknowledge the transmission, and the sender treats the transmission as successful without regard for the actual result.
1	ACK	The addressed recipient returns an ACK frame after correct reception.
2	BLOCK-ACK (undefined)	The addressed recipient keeps track of the frames received with this policy until requested to respond with a BLOCK-ACK frame.
3	BLOCK-ACK Request (undefined)	The addressed recipient returns a BLOCK-ACK frame after reception.

2.5.5 Frame Type

The Frame Type field is set to the type of frame that is being sent. Table 2 lists the valid frame type values, descriptions, and the subclauses that describe the format and use of each of the individual frame types.

Table 2 - Frame Type field encoding

Value	Frame type
0	Beacon frame
1	Control frame
2	Command frame (undefined)
3	Data frame
4	Aggregated data frame (undefined)
5–7	Reserved

2.5.6 Frame Subtype / Delivery ID

The Frame Subtype / Delivery ID field is used to assist a receiver in the proper processing of received frames. In control or command frames, this field is used as Frame Subtype. In data frames and aggregated data frames, this field is used as Delivery ID as defined in Table 3.

Table 3- Delivery ID encoding in Frame Control

Delivery ID	
b9	B8-b6
0	User priority
1	Stream index

The user priority bits in the delivery ID field (in the MAC header), won't be used until a CSMA/CA solution is specified.

2.5.7 Retry

The Retry bit is set to one in any data, aggregated data, or command frame that is a retransmission of an earlier frame. It is reserved in all other frame types.

2.5.8 DestAddr

The DestAddr field is set to the DevAddr of the intended recipient(s) of the frame. The DevAddr specifies a single device for a unicast frame, a group of devices for a multicast frame, or all devices for a broadcast frame.

Frames are addressed using DevAddrs. There are four types of DevAddrs; Private, Generated, Multicast, and Broadcast. Table 4 shows the range for each type of DevAddr, it follows the address range defined by the WiMedia Alliance [5].

Table 4 - DevAddr types and ranges

Type	Range
Private	0x0000–0x00FF
Generated	0x0100–0xFEFF
Multicast (McstAddr)	0xFF00–0xFFFE
Broadcast (BcstAddr)	0xFFFF

A device shall associate a Generated DevAddr with its local MAC entity and use that DevAddr in its beacon. A device shall select a Generated DevAddr from the Generated DevAddr range at random with equal probability and should ensure that the generated value is unique among all devices.

Except in Private reservations, in all frames transmitted, a device shall set the SrcAddr field to its own DevAddr. In unicast frames, the DestAddr field shall be set to the DevAddr of the recipient. In multicast frames, the DestAddr field shall be set to an address from the Multicast DevAddr range.

In broadcast frames, the DestAddr field shall be set to the Broadcast DevAddr.

A device shall not transmit frames addressed with a Private DevAddr at any time outside a Private reservation.

2.5.9 SrcAddr

The SrcAddr field is set to the DevAddr of the transmitter of the frame.

2.5.10 Sequence Control

The Sequence Control field identifies the order of MSDUs/MCDUs and their fragments. The Sequence Control field is illustrated in Figure 15. The Sequence Control field is reserved in control frames.

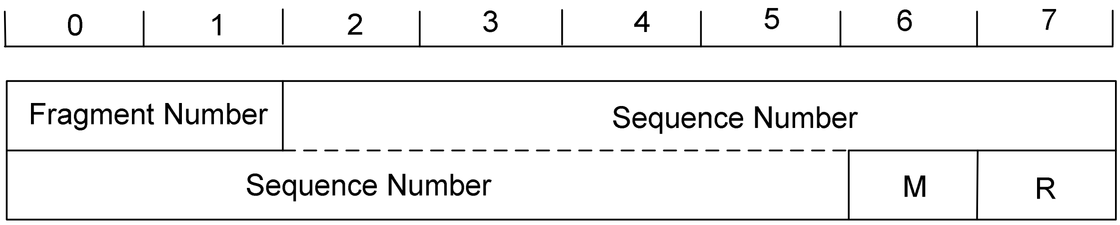


Figure 15: Sequence Control field format

Bit M : More Fragment

Bit R : reserved

2.5.10.1 Fragment Number

The Fragment Number field is set to the number of the fragment within the MSDU or MCDU. The fragment number is zero in the first or only fragment of an MSDU or MCDU and is incremented by one for each successive fragment of that MSDU or MCDU.

2.5.10.2 *Sequence Number*

The Sequence Number field value is used for duplicate detection for frames sent using the ACK acknowledgement policy. It is used for both duplicate detection and reordering for frames sent using the BLOCK-ACK mechanism.

A device shall assign each MSDU or MCDU transmitted a sequence number from a modulo 4096 counter.

A device shall assign the same sequence number to each fragment of an MSDU or MCDU.

A single sequence number applies to all MSDUs contained in an aggregated data frame. A device shall increment the sequence number counter by one for each transmitted aggregated data frame.

A device shall use a dedicated counter for MCDUs.

A device shall use a dedicated counter for each sequence of MSDUs addressed to the same DestAddr with the same Delivery ID using BLOCK-ACK acknowledgement policy.

A device may use a dedicated counter for MSDUs with the same Delivery ID field value addressed to the same DestAddr.

In each beacon frame transmitted in a superframe, a device shall set the Sequence Number field from a dedicated counter that increments once per superframe, modulo 2048, or shall set it to zero.

2.5.10.3 *More Fragments*

The More Fragments field is set to zero to indicate that the current fragment is the sole or final fragment of the current MSDU or MCDU; otherwise the field is set to one.

2.5.11 Access & Feedback Information

The Access Information field is illustrated in Figure 16.

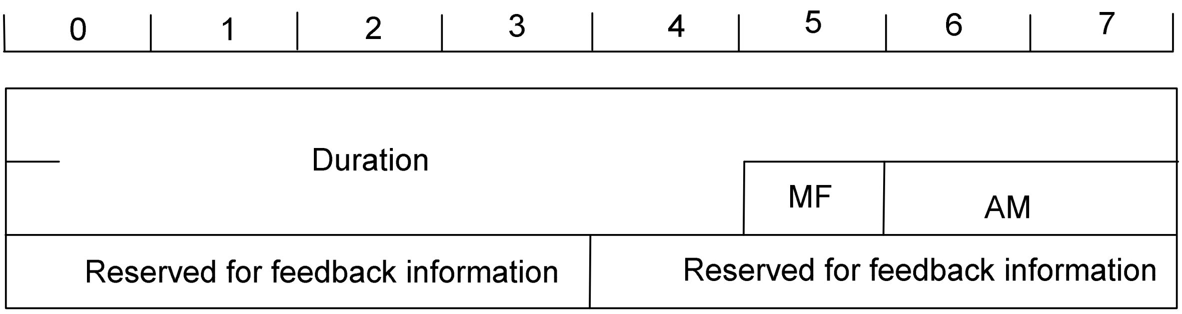


Figure 16 : Access & feedback Information field format

2.5.11.1 *Duration*

The Duration field is 13 bits in length and is set to an expected medium busy interval after the end of the PLCP header of the current frame in units of microseconds (max duration = 8191 µs). The duration value is used to update the network allocation vector (NAV). **Note that it takes 93 µs to send 1500 octets at 128 MegaBits/s,as the maxDuration = 8191 µs, we could use only 11 bits for the duration field and use the remaining 2 bits if necessary.**

A device shall set the Duration field in beacon frames to one of the following:

- If there are more than one Beacon in the Beacon period, it shoud be set to the time remaining in the BP measured from the end of the PLCP header of the beacon frame, as determined by the largest BP length announced by neighbours of the device in the previous superframe;
- If there is only one Beacon in the Beacon period, it should be set to the transmission time of the frame body (Mac Frame payload + FCS) of the beacon frame;

A device shall set the Duration field in data frames to the sum of:

- The transmission time of the frame body (Mac Frame payload + FCS) of the current frame;
- The transmission time of the expected response frame for the current frame (ACK frame), if any;
- The transmission time of subsequent frames, if any, to be sent to the same recipient up to and including next frame with ACK Policy set to ACK

All the IFSs separating the frames included in the Duration calculation. The calculated value for Duration has a required accuracy of +/- one microsecond per frame included in the calculation.

A device shall set the Duration field in ACK frames to the ceiling of zero or a value equal to the duration value contained in the previous frame minus one SIFS time, minus the transmission time of the frame body of the received frame to which the ACK is responding, minus the transmission time up to the end of the PLCP header of this ACK frame.

2.5.11.2 More Frames

The More Frames bit is set to zero if the transmitter will not send further frames to the same recipient during the current superframe; otherwise it is set to one. The More Frames bit is reserved in beacon and control frames.

2.5.11.3 Access Method

The access method must be set for each packet and must be updated for each time slot.

The Access Method bits are set to 0x00, for each packet sent in the time slots working in half duplex transmission. For these time slots, a reservation has been made by only one device

The Access Method bits are set to 0x01, for each packet sent in the time slots working in full duplex transmission. For these time slots, a reservation has been made by each device involved in the reservations process.

2.5.11.4 Feedback information

The Feedback information field is 8 bits, and should be used by the receiver of the frame to assess the channel condition. The Feedback information value could be based on RSSI, BER, Packets Loss or any other information allowing channel condition assessment.

2.5.12 Frame Payload

The Frame Payload field is a variable length field that carries the information that is to be transferred to a device or group of devices.

2.5.13 FCS

The FCS field contains a 32-bit value that represents a CRC polynomial of degree 31.

The CRC is calculated over a calculation field, which is the entire Frame Payload field for this specification. The calculation field is mapped to a message polynomial M(x) of degree k-1, where k is the number of bits in the calculation field. The least-significant bit of the first octet presented to the PHY SAP is the coefficient of the x^{k-1} term, and the most-significant bit of the last octet transmitted is the coefficient of the x^0 term.

The CRC is calculated using the following standard generator polynomial of degree 32:

$$\mathbf{G(x)} = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

The CRC polynomial is the one's complement of the modulo 2 sum of the following remainders:

- The remainder resulting from $x^k \times (x^{31} + x^{30} + ... + x + 1)$ divided (modulo 2) by **G(x)**.
- The remainder resulting from $x^{32} \times M(x)$, divided (modulo 2) by **G(x)**.

The FCS field value is derived from the CRC polynomial such that the least-significant bit is the coefficient of the x^{31} term and the most-significant bit is the coefficient of the x^0 term. Figure 17 illustrates the encoding of the FCS field for the CRC polynomial:

$a_{31}x^{31} + a_{30}x^{30} + a_{29}x^{29} + \ldots + a_2x^2 + a_1x + a_0$

b0	b1	b2	....	b29	b30	b31
a_0	a_1	a_2	....	a_{29}	a_{30}	a_{31}

Figure 17 - FCS field encoding

In a common implementation, at the transmitter, the initial remainder of the division is preset to all ones and is then modified via division of the calculation field by the generator polynomial G(x). The one's complement of this remainder is the FCS field. At the receiver, the initial remainder is preset to all ones. The serial incoming bits of the calculation field and FCS, when divided by G(x) in the absence of transmission errors, results in a unique non-zero remainder value. The unique remainder value is the polynomial:

$$x^{31} + x^{30} + x^{26} + x^{25} + x^{24} + x^{18} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^{8} + x^{6} + x^{5} + x^{4} + x^{3} + x + 1$$

2.5.14 Information elements

This section defines the information elements (IEs) that can appear in beacons and certain command frames. The general format of all IEs is illustrated in Figure 18: Information Element general format.

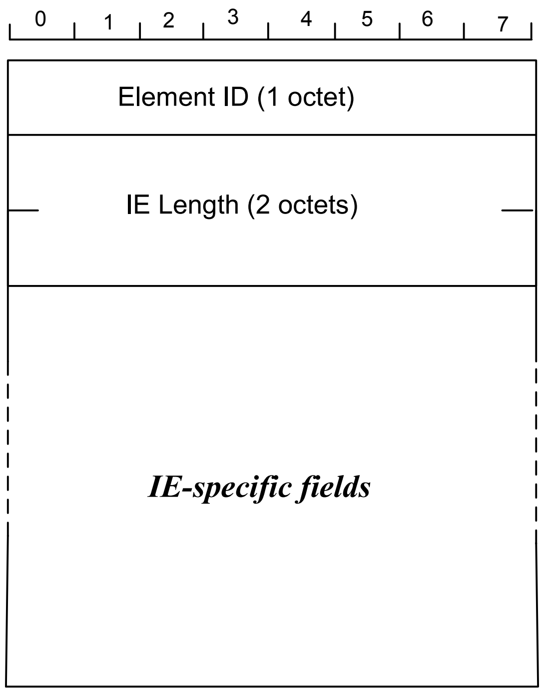


Figure 18: Information Element general format

The Element ID field is set to the value as listed in Table 5 that identifies the information element. The Length field is set to the length, in octets, of the IE-specific fields that follow. The IE-specific fields contain information specific to the IE.

Table 5: Information Elements

Element ID	Information element	Description
0	Emergency traffic	The emergency traffic IE allows a device to send an emergency message in a Beacon.
1	Beacon Period Occupancy	The Beacon Period Occupancy IE provides information on the BP observed by the device sending the IE.
2	Time Slot Availability	The Time Slot Availability IE is used by a device to indicate its view of the current utilization of Time Slots.
3	Reservation Protocol	A RP IE is used to negotiate a reservation or part of a reservation for certain TSs and to announce the reserved TSs.
4	MAC Capability	The MAC Capability Bitmap field indicates capabilities supported by the MAC entity.
5	Identification	The Identification IE provides identifying information about the device, including a name string.
6	Multicast Binding	The Multicast Binding IE binds a multicast EUI-48 and the McstAddr that the device will use when transmitting frames destined for that multicast EUI-48.
240	OWLLCP	The OWLLCP IE is included in beacons by all devices. It provides information about the device and its participation in OWSSs.

2.6 Beacon frames

The Beacon frame is described in Figure 19.

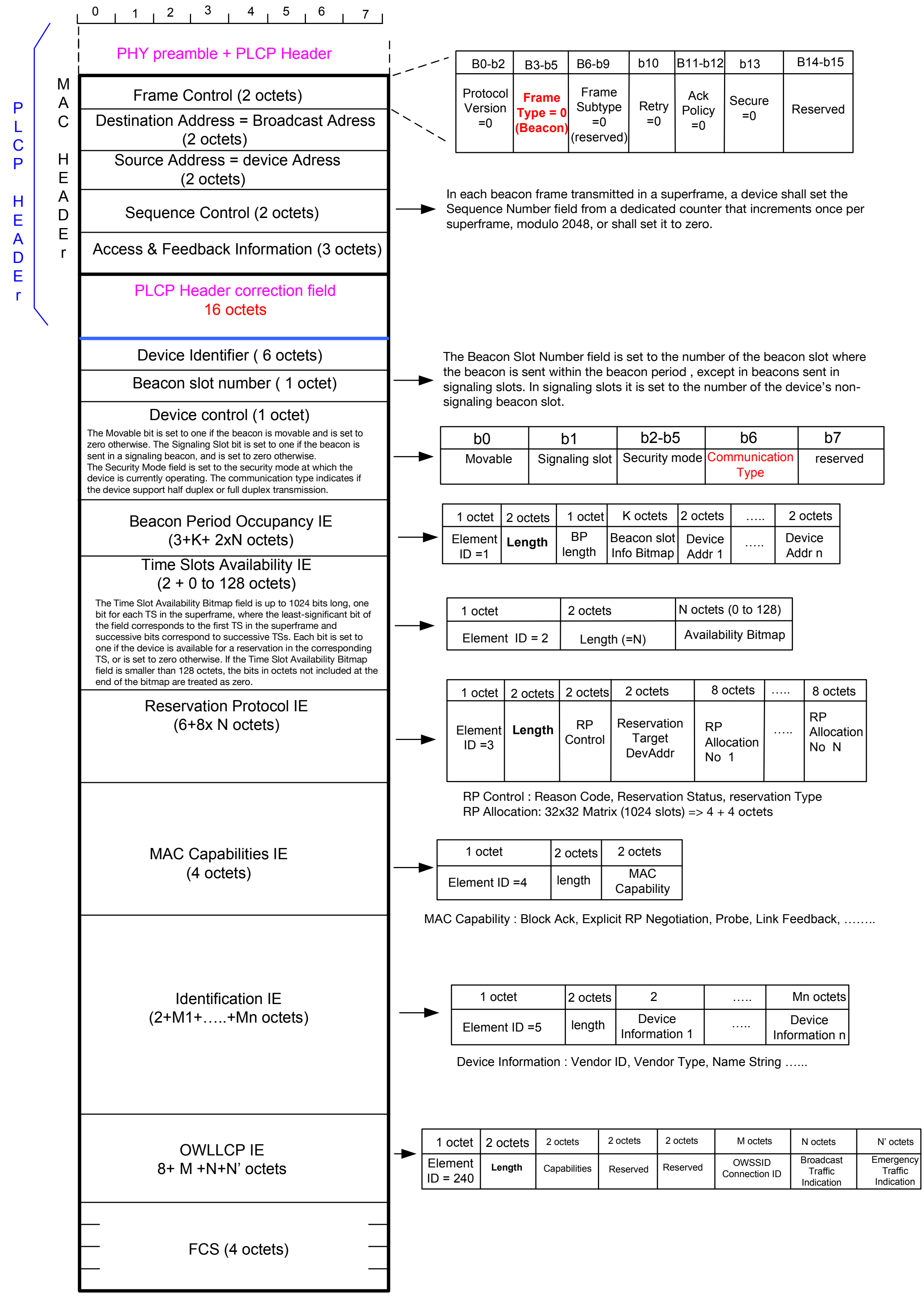


Figure 19: Beacon Frame format

2.6.1 Beacon Parameters

The Beacon parameters are described in Figure 20.

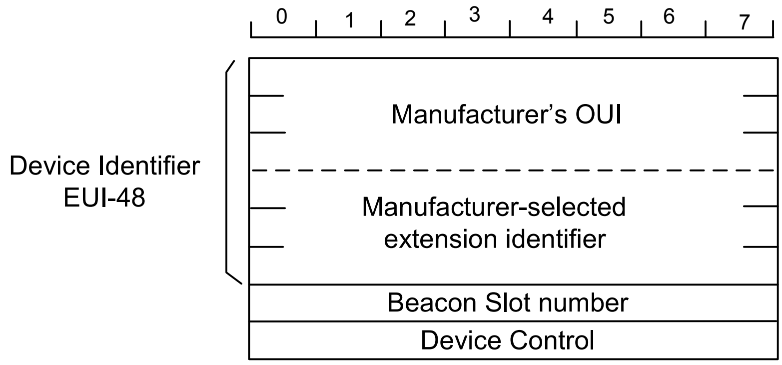


Figure 20: BEACON parameters

The Device Identifier field is set to the EUI-48 [2] of the device sending the beacon. A device may use a NULL EUI-48 value (all bits set to one) to indicate it does not have a unique EUI-48 value. The EUI is a sequence of 6 octets. The first three octets are the manufacturer's OUI, and the last three octets are the manufacturer-selected extension identifier. Octets of the EUI are passed to the PHY SAP in ascending index-value order.

The Beacon Slot Number field is set to the number of the beacon slot where the beacon is sent within the beacon period (BP), in the range of 0 -63 except in beacons sent in signalling slots. In signalling slots it is set to the number of the device's non-signalling beacon slot.

The Device Control field is illustrated in Figure 21.

b0	b1	b2-b5	b6	b7
Movable	Signaling slot	Security mode	Communication Type	reserved

Figure 21 - Device Control field format

The Movable bit is set to one if the beacon is movable, and is set to zero otherwise. The Signalling Slot bit is set to one if the beacon is sent in a signalling beacon slot, and is set to zero otherwise. The Security Mode field is set to the security mode at which the device is currently operating. There is only one security mode defined 0x00 : open mode

The communication type indicates if the device can support half duplex or full duplex transmission. If the bit is set to zero, the device supports half duplex mode only, if the bit is set to one, the device supports full duplex and half duplex mode.

2.6.2 Beacon Period Occupancy IE

The Beacon Period Occupancy IE provides information on the BP observed by the device sending the IE. The Beacon Period Occupancy IE is illustrated in Figure 22.

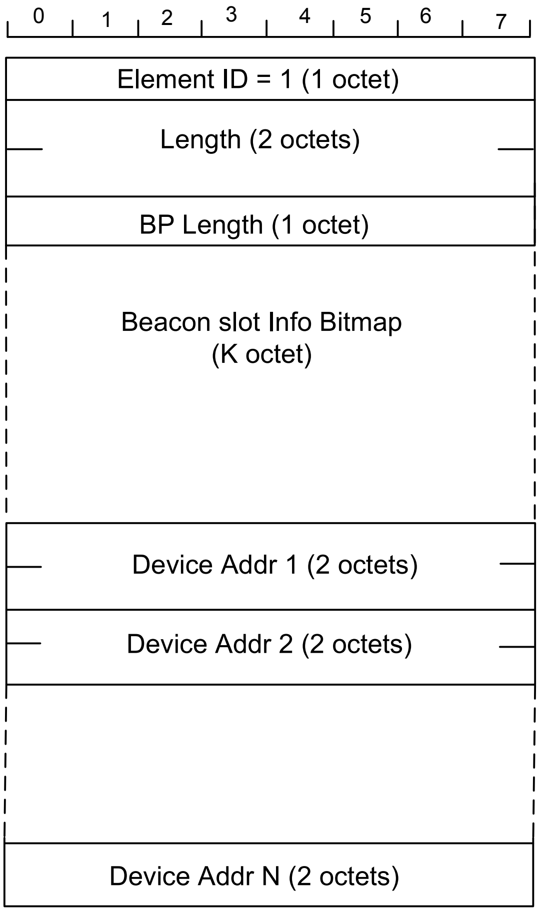


Figure 22: Beacon Period Occupancy IE

2.6.2.1 BP Length field

The BP Length field is set to the length of the BP, measured in Beacon Slots.

2.6.2.2 Beacon Slot Info Bitmap field

The Beacon Slot Info Bitmap field consists of K octets of 2-bit elements to indicate the beacon slot occupancy and movability in the BP. Each octet contains 4 elements, and each element represents 1 Beacon slot, therefore K = Ceiling (BP_Length/4). Each element n, numbered from 0 to 4×K-1, corresponds to beacon slot n and is encoded as shown in Table 6. Element zero is the least-significant two bits of the field. Unused elements, if any, are set to zero.

Table 6- Beacon Slot Info Bitmap element encoding

Element value	Beacon slot status	DevAddr encoding
0	Unoccupied (non-movable) No PHY indication of medium activity was received in the corresponding beacon slot in the last superframe.	No DevAddr is included in the DevAddr fields for this beacon slot.
1	Occupied & non-movable A beacon frame aligned to the device's BPST was received in the corresponding beacon slot in the last superframe, and the Movable bit in that beacon was set to zero.	The corresponding DevAddr field is set to the SrcAddr in the MAC header of the received beacon frame.
2	Occupied & movable A PHY indication of medium activity was received in the corresponding beacon slot in the last superframe, but did not result in reception of a beacon frame aligned to the device's BPST.	If a beacon frame header was received within a time slot boundary, but the frame had an FCS error, the DevAddr field is set to the SrcAddr in the MAC header of the beacon frame. In all other cases, the DevAddr field is set to BcstAddr.
3	Occupied & movable A beacon frame aligned to the device's BPST was received in the corresponding beacon slot in the last superframe, and the Movable bit in that beacon was set to one.	The corresponding DevAddr field is set to the SrcAddr in the MAC header of the received beacon frame.

2.6.2.3 DevAddr fields

The DevAddr fields correspond to beacon slots encoded as specified in the Beacon Slot Info Bitmap. They are included in ascending beacon slot order.

2.6.3 Time Slot Availability IE

The Time Slot Availability IE is used by a device to indicate its view of the current utilization of Time Slots. The Time Slot Availability IE is illustrated in Figure 23.

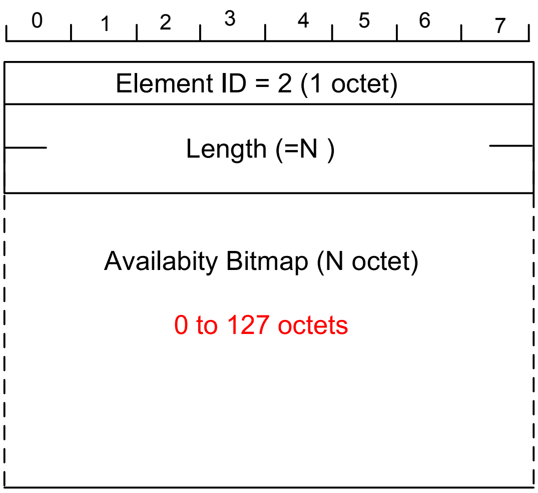


Figure 23: Time Slot Availability IE format

The Time Slot Availability Bitmap field is up to 1024 bits long, one bit for each TS in the superframe, where the least-significant bit of the field corresponds to the first TS in the superframe and successive bits correspond to successive TSs. Each bit is set to one if the device is available for a reservation in the corresponding TS, or is set to zero otherwise. If the Time Slot Availability Bitmap field is smaller than 128 octets, the bits in octets not included at the end of the bitmap are treated as zero.

2.6.4 Reservation Protocol (RP) IE

A RP IE is used to negotiate a reservation or part of a reservation for certain TSs and to announce the reserved TSs. The RP IE is illustrated in Figure 24. **Note that a device, can include several RP IE in the same Beacon, one for each target.**

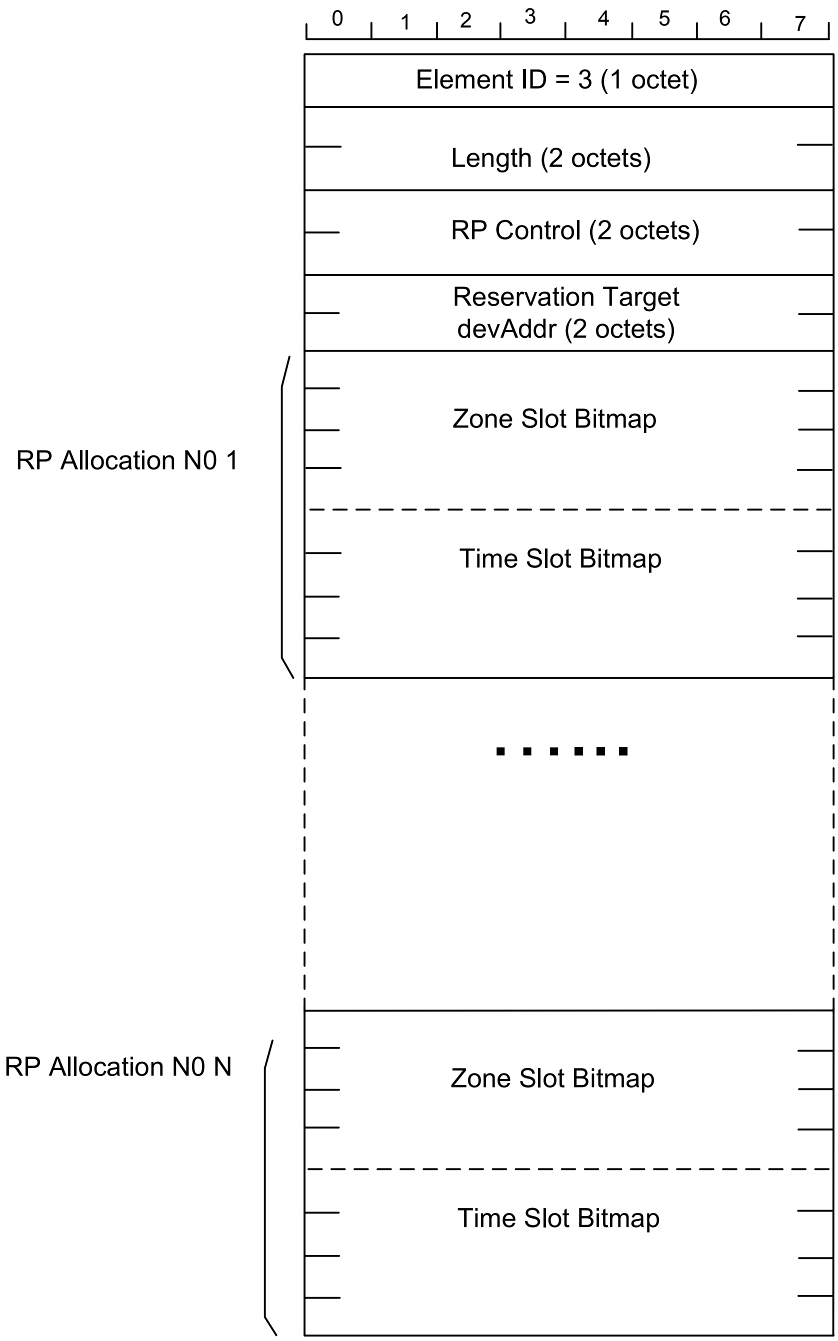


Figure 24: RP IE format

2.6.4.1 RP Control field

The RP Control field is illustrated in Figure 25.

b0-b2	b3-b5	b6-b8	b9	b10	b11	b12	b13	b14-b15
Réservation type	Stream index	Reason Code	Reservation status	Owner	Conflict Tie-Breaker	Unsafe	Transmission type	Reserved

Figure 25: RP control field encoding

The Reservation Type field is set to the type of the reservation, as there is only one reservation type, the reservation type should be set to zero.

The Reason Code is used by a reservation target to indicate whether a reservation request was successful and is encoded as shown in Table 7. The Reason Code is set to zero in a RP IE sent during negotiation by a reservation owner and by a device maintaining an established reservation. The Reason Code is set to Modified by a device if some of the Time Slots claimed in the reservation have been removed or if RP IEs have been combined, split, or both.

Table 7 - Reason Code field encoding

Value	Code	Meaning
0	Accepted	The RP reservation request is granted
1	Conflict	The RP reservation request or existing reservation is in conflict with one or more existing RP reservations
2	Pending	The RP reservation request is being processed
3	Denied	The RP reservation request is rejected or existing RP reservation can no longer be accepted
4	Modified	The RP reservation is still maintained but has been reduced in size or multiple RP IEs for the same reservation have been combined
5	Cancelled	The RP reservation has been cancelled.
6–7	Reserved	Reserved

The Reservation Status bit indicates the status of the RP negotiation process. The Reservation Status bit is set to zero in a RP IE for a reservation that is under negotiation or in conflict. It is set to one by a device granting or maintaining a reservation, which is then referred to as an established reservation.

The Owner bit is set to one if the device transmitting the RP IE is the reservation owner, or to zero if the device transmitting the RP IE is a reservation target.

The Conflict Tie-breaker bit is set to a random value of zero or one when a reservation request is made. The same value selected is used as long as the reservation is in effect. For all RP IEs that represent the same reservation, the Conflict Tie-breaker bit is set to the same value.

The Target/Owner DevAddr field is set to the DevAddr of the reservation target if the device transmitting this RP IE is the reservation owner. The reservation target may be a unicast or multicast DevAddr. The field is set to the DevAddr of the reservation owner if the device transmitting the RP IE is a reservation target.

The Unsafe bit is set to one if any of the Time Slots identified in the RP Allocation fields is considered in excess of reservation limits.

The transmission type it set to zero, if there is no full duplex transmission for any of the reserved time slots. The transmission type it set to one, if there is at least one time slot working in full duplex transmission.

A RP IE contains one or more RP Allocation fields. Each RP Allocation field is encoded using a zone structure. The superframe is split into 32 zones numbered from 0 to 31 starting from the BPST. Each zone contains 32 consecutive time slots, which are numbered from 0 to 32 within the zone.

The format of a RP Allocation field is illustrated in Figure 26.

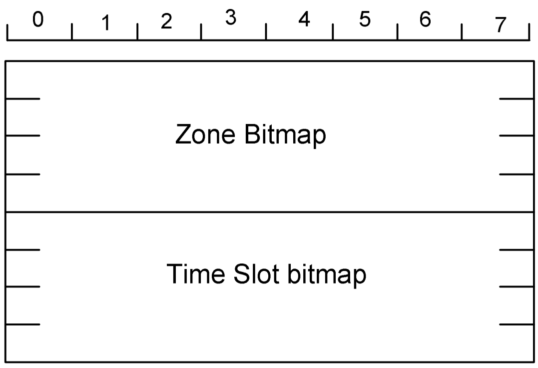


Figure 26: RP Allocation field format

The Zone Bitmap field identifies the zones that contain reserved time slots. If a bit in the field is set to one, the corresponding zone contains reserved Time Slots, where bit zero corresponds to zone zero.

The Time Slot Bitmap specifies which Time Slots in the zones identified by the Zone Bitmap field are part of the reservation. If a bit in the field is set to one, the corresponding Time Slot within each zone identified by the Zone Bitmap is included in the reservation, where bit zero corresponds to Time Slot zero within the zone.

Note that with this method you cannot reserve the diagonal of the 32x32 matrix.

Example:

If the Zone Bimap is : 00000000000000001000000000000000 = 0x8000 =(32768)dec

If the TS Bimap is : 00000000000000001111111100000000 = 0xFF00 =(65280)dec

In the above example, the device is reserving 8 timeslots (TS 8-16) in zone number 15 (timeslot 448-479). So the TSs reserved are the TSs : 456<->463

2.6.5 MAC Capabilities IE

The MAC Capabilities IE is illustrated in Figure 27.

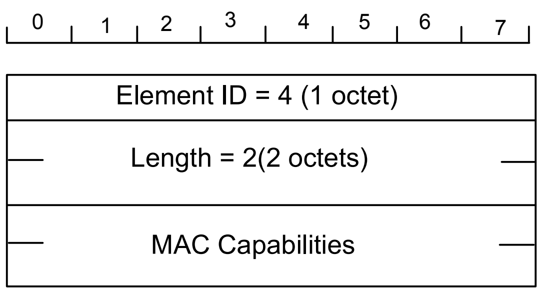


Figure 27: MAC Capabilities IE format

The MAC Capability Bitmap field indicates capabilities supported by the MAC entity. A bit is set to one if the corresponding attribute is supported, or is set to zero otherwise. This field is encoded as described in Table 8..

Table 8: MAC Capability Bitmap

Octet	Bit	Attribute	Description
0	0	Block ACK	Capable of transmitting and acknowledging frames using the B-ACK mechanism
	1	Explicit RP negotiation	Capable of negotiating reservation using command frames
	2	Reserved	Reserved
	3	Reserved	Reserved

	4	Reserved	Reserved
	5	Reserved	Reserved
	6	Reserved	Reserved
	7	Reserved	Reserved
1	0	Reserved	Reserved
	1–7	Reserved	Reserved

2.6.6 Identification IE

The Identification IE provides identifying information about the device, including a name string. The Identification IE is illustrated in Figure 28.

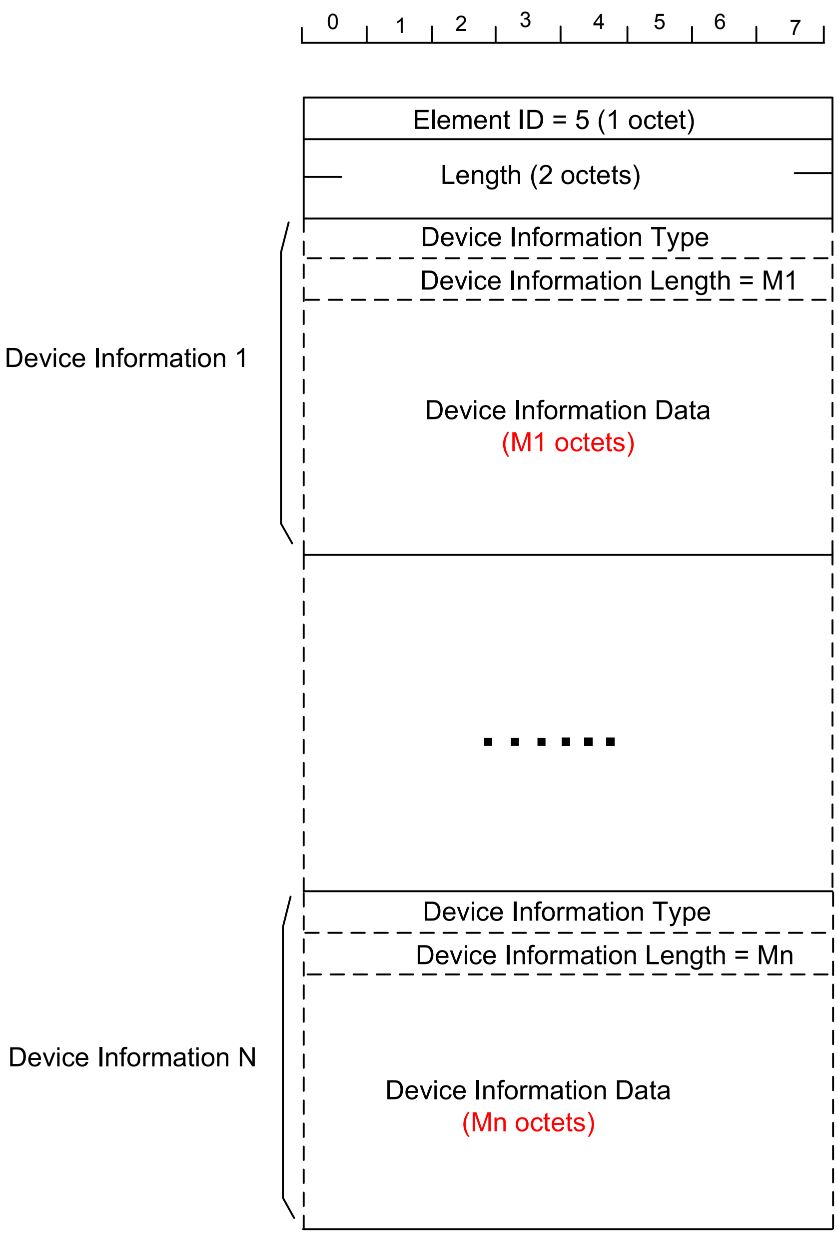


Figure 28: Identification IE format

2.6.6.1 *Device Information field*

The general format of the Device Information field is illustrated in Figure 29.

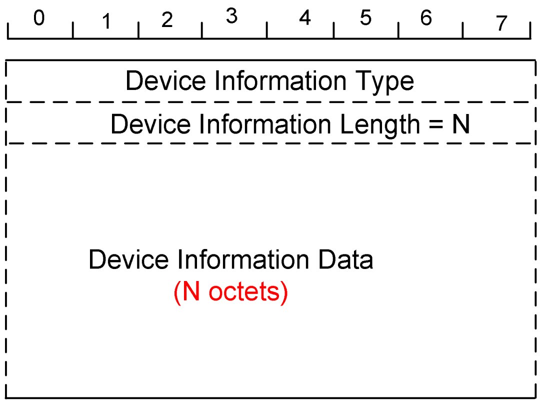


Figure 29- Device Information field format

The Device Information Length field indicates the length, in octets, of the Device Information Data Field that follows. The encoding for the Device Information Type field is shown in Table 9.

Table 9: Device Information Type field encoding

Value	Device Information Data field contents
0	Vendor ID
1	Vendor Type
2	Name String
3–255	Reserved

The Device Information Data field, if Device Information Type is Vendor ID, is illustrated in Figure 30. The Vendor ID is set to an OUI that indicates the vendor of the device.

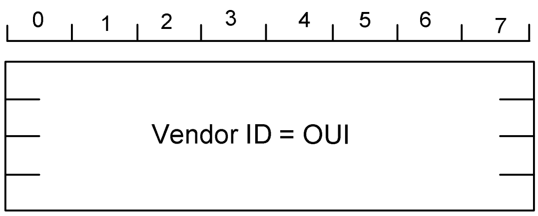


Figure 30: Vendor ID field format

The Device Information Data field, if Device Information Type is Vendor Type, is illustrated in Figure 31.The Vendor ID field is set to an OUI that indicates the entity that assigns the values used in the Device Type ID field. The Device Type ID field indicates the type of device.

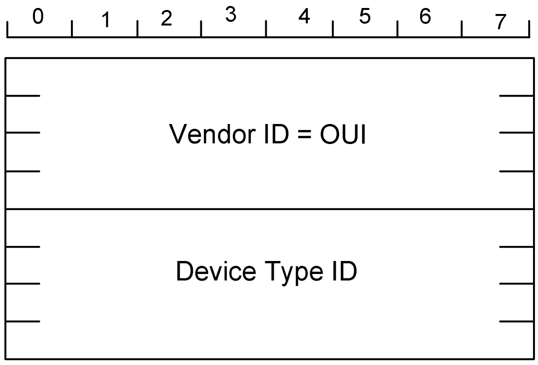


Figure 31: Vendor Type field format

The Device Information Data field, if Device Information Type is Name String, contains the name of the device encoded in Unicode UTF-16LE format, and is illustrated in Figure 32..

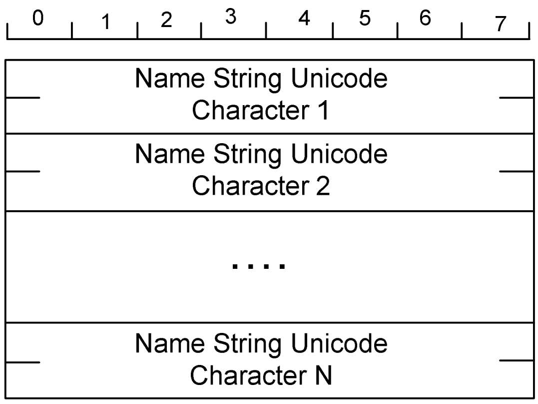


Figure 32: Name string field format

2.6.7 Multicast Binding Information Element

As shown in Figure 33, Each device maps multicast EUI-48s to McstAddrs in the 16-bit DevAddr address range. The Multicast Binding IE binds a multicast EUI-48 and the McstAddr that the device will use when transmitting frames destined for that multicast EUI-48.

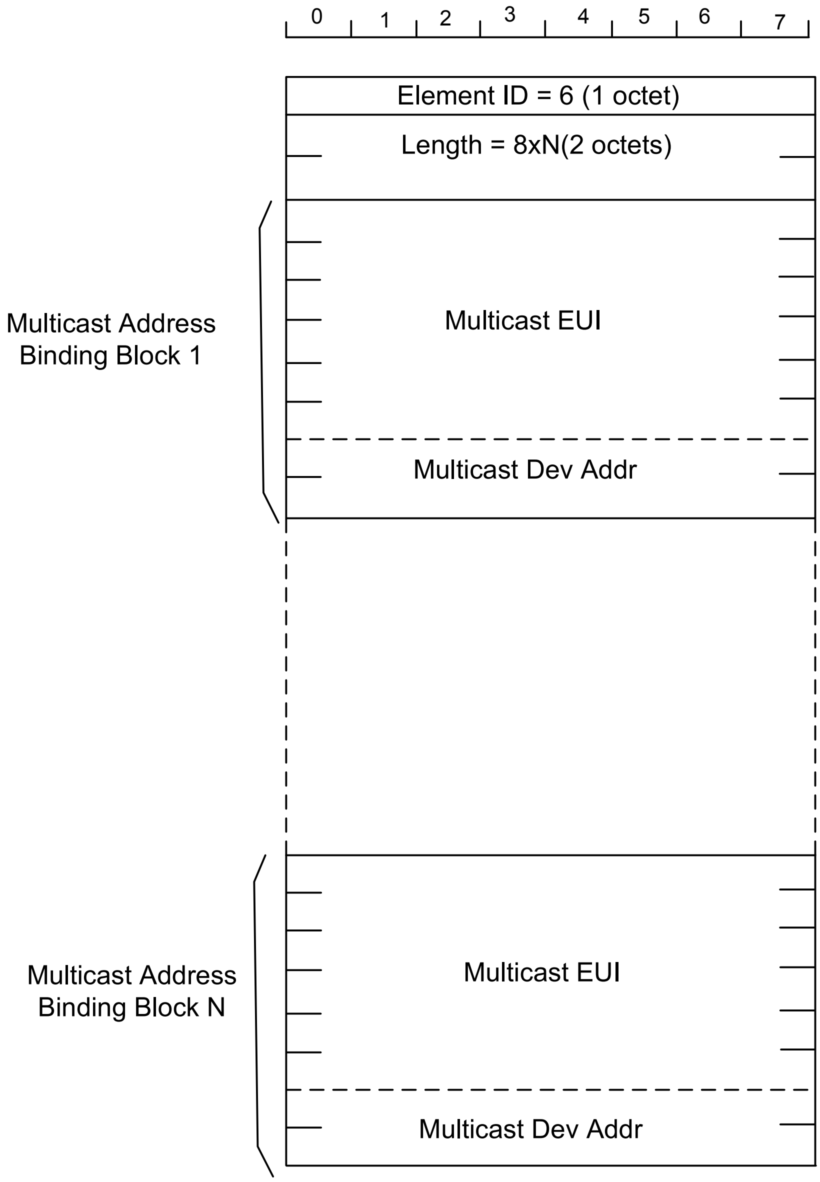


Figure 33: Multicast address Binding IE

2.6.8 OWLLCP IE

The OWLLCP IE is included in beacons by all devices. It provides information about the device and its participation in OWSSs. The format of the IE is illustrated in Figure 34.

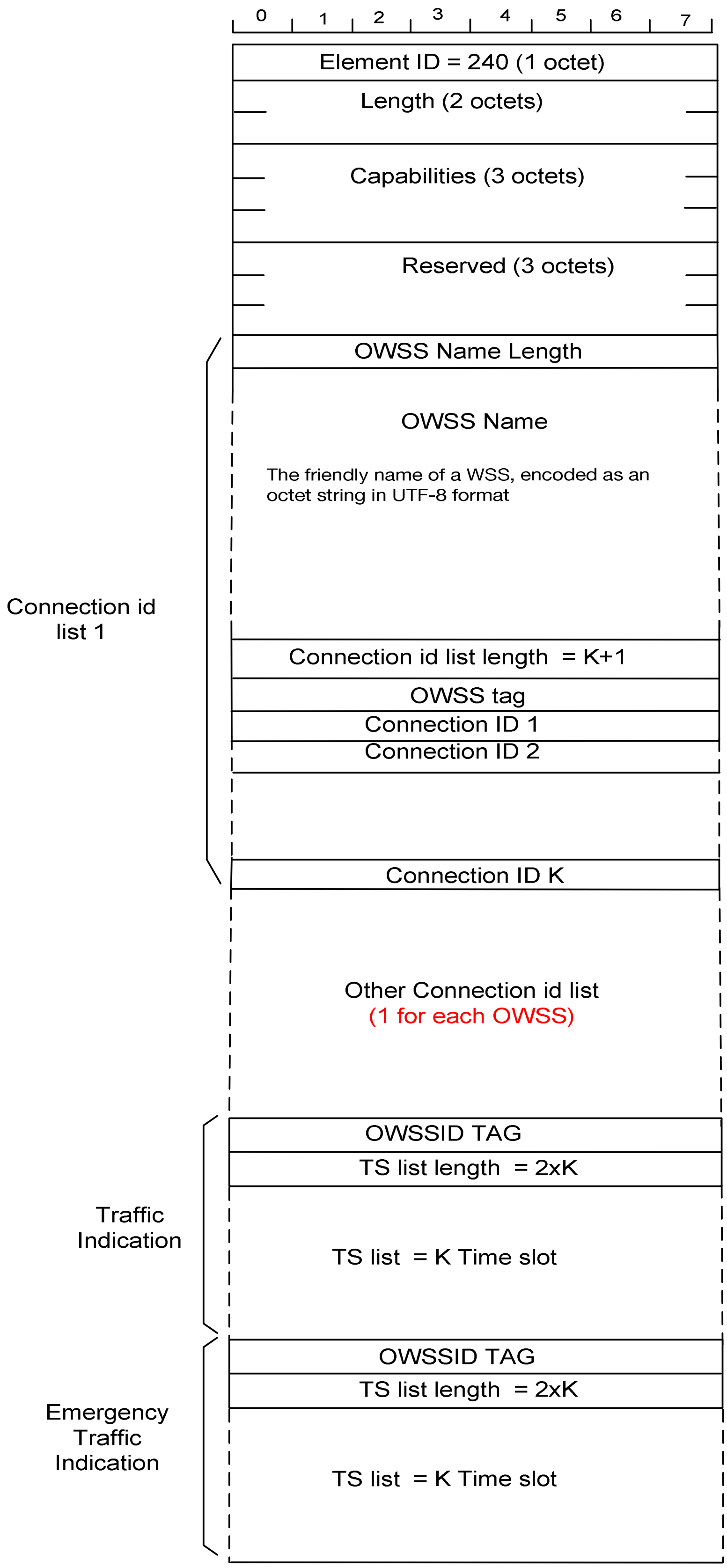


Figure 34: OWLLCP IE format

2.6.8.1 Capabilities field

The Capabilities field format is illustrated in Figure 35.

b0	b1-b2	b3	b4	b5-b7	b8-b11	b12-b15	b16-b19	b19-b23
Bridge device	Reserved	Reservation	Enrollment	Reserved	Broadcast Traffic indication Count	Emergency Traffic indication	Number of Connection ID	Reserved

Figure 35: Capabilities field format

The Bridge device bit is set to one if the device can provide bridge services to client devices. The RP Establishment bit is set to one if the device is a bridge and is capable of accepting a RP reservation request from a client device, or is set to zero otherwise. The Enrollment bit is set to one if the device has been enabled by the user to accept a new enrollment, or is set to zero otherwise. The Broadcast Traffic Indications Count field is set to the number of Traffic Indication fields in the Broadcast Traffic Indications field. The Emergency Traffic Indications is set to the number of Emergency Traffic Indication fields in the Broadcast Traffic Indications field. The number of connection ID list is set to the number of OWSS connection ID field included in the OWSSID List field.

2.6.8.2 Connection ID list

The OWSSID connection ID list field contains the OWSS connection ID's that indicate which OWSSs a device has activated, and how many connection are active per OWSS. An OWSS connection ID is one octet, identifying a connection for a given OWSS. OWSS connections ID are transmitted in ascending order. **The connection ID has a local significance only.**

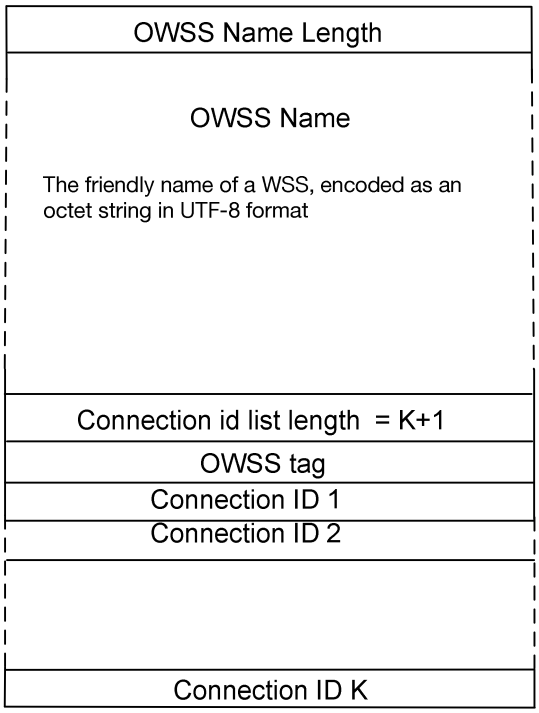


Figure 36- Connection id list field format

As shown in Figure 36 an OWSS is identified by a name, a tag (see section 3.5.7).

2.6.8.3 Broadcast Traffic Indications

The Broadcast Traffic Indications field contains zero or more Traffic Indication fields, an example of which is illustrated in Figure 37. Each Traffic Indication field informs neighbours of the device of its intent to transmit frames carrying OWLLCP broadcast or multicast traffic. An OWLLCP device includes one Traffic Indication field for each OWSS to which it intends to transmit broadcast or multicast frames in the current superframe.

The format of a Broadcast Traffic Indication field is illustrated in Figure 37.

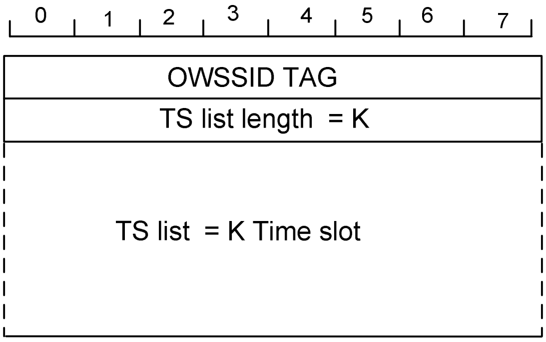


Figure 37: Traffic Indication field format

The OWSS Tag field identifies the OWSS to which the device intends to transmit multicast or broadcast traffic; it's the first octet of the **OWSSID connection ID**. The TS List Length field is set to the number of TS numbers included in the TS List field.

The TS List field contains one or more TS numbers in the current superframe in which the device intends to send broadcast or multicast traffic. A TS number is two octets. The TS numbers are transmitted in increasing value order.

2.6.8.4 Emergency Traffic Indications

The Emergency Traffic Indications field contains zero or more Emergency Traffic Indication fields, an example of which is illustrated in Figure 36. Each Emergency Traffic Indication field informs neighbours of the device of its intent to transmit frames carrying Emergency traffic. A OWLLCP device includes one Emergency Traffic Indication field for each OWSS to which it intends to transmit Emergency frames in the current superframe. The format of a Emergency Traffic Indication field is illustrated in Figure 38.

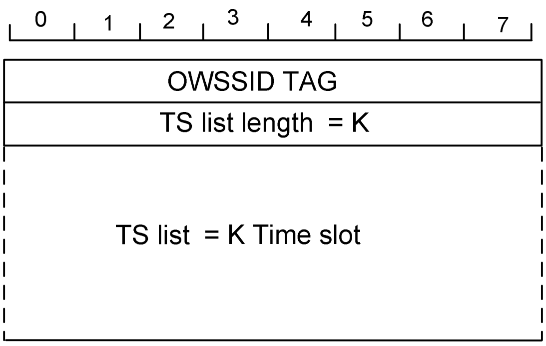


Figure 38: Emergency Traffic Indication field format

The OWSS Tag field identifies the OWSS to which the device intends to transmit emergency traffic, it's the first octet of the **OWSSID connection ID**. The TS List Length field is set to the number of TS numbers included in the TS List field. The TS List field contains one or more TS numbers in the current superframe in which the device intends to send emergency traffic. A TS number is two octets. The TS numbers are transmitted in increasing value order.

2.6.9 Emergency Traffic IE format

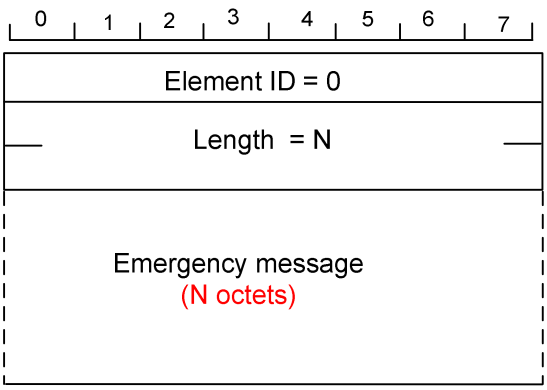


Figure 39: Emergency Traffic IE format

The emergency traffic IE described in Figure 39, allows a device to send an emergency message in a Beacon. The size of the message is limited to PHYdataRate *(0,000049). For longer emergency messages, a device can reserve some TSs with the OWLLC IE (see section 2.6.8). The emergency message is encoded in Unicode UTF-16LE format.

2.7 Control Frames

The control frame format is described in Figure 40.

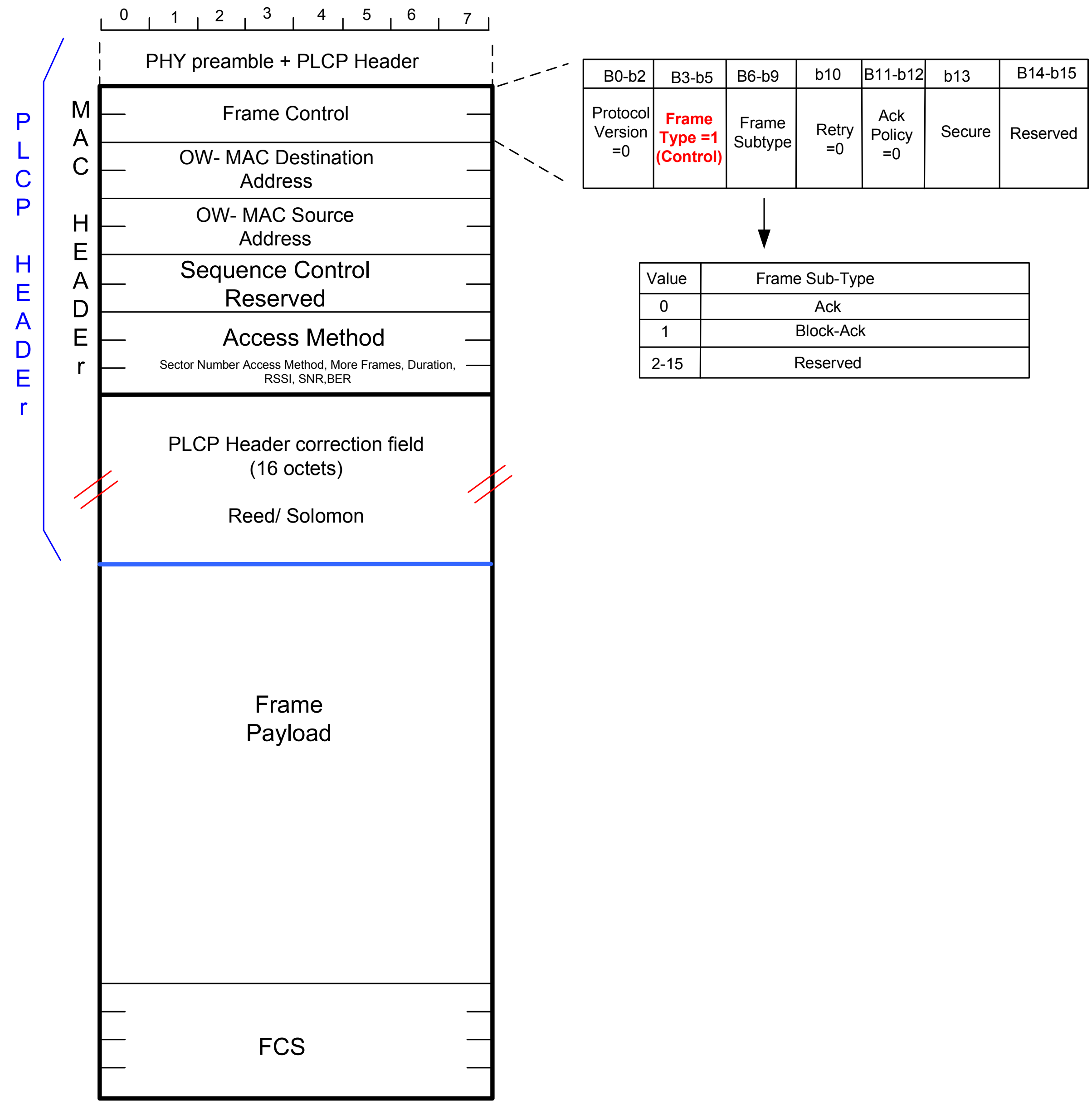


Figure 40: Control Frame format

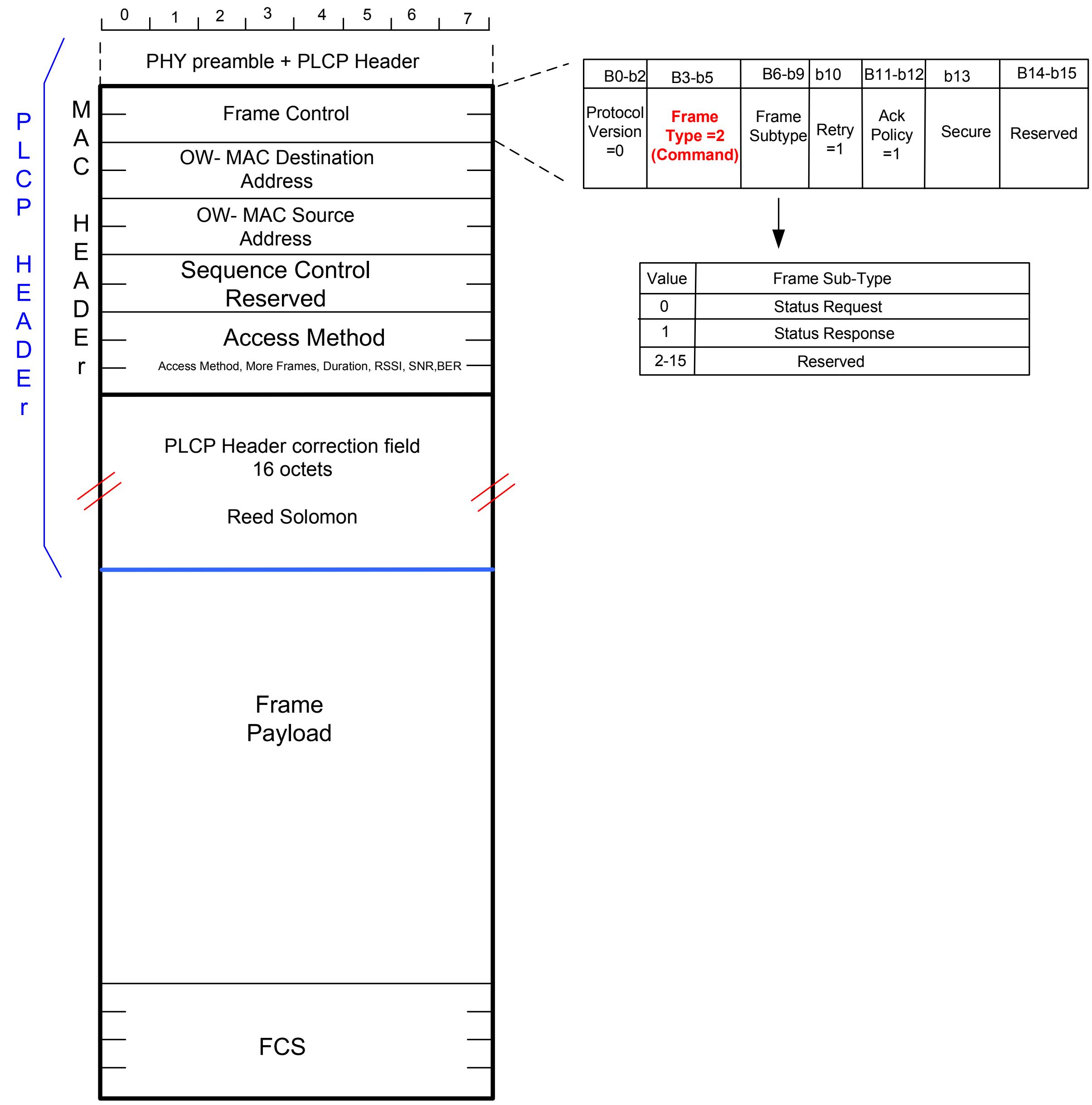
2.7.1 Acknowledgement (ACK)

In ACK frames, the DestAddr field is set to the SrcAddr of the received frame that is acknowledged. ACK frames have no frame payload. As the Ack frame is a control frame, the Sequence Number field is reserved. As we use TDMA, we don't need to indicate which frame you acknowledge.

2.8 Command Frame

2.8.1 General Format

The command frame format is described in Figure 41.



Value	Frame Sub-Type
0	Status Request
1	Status Response
2-15	Reserved

Figure 41: Command Frame format

As shown in the above figure, a command frame can be status request (Subtype = 0) or Status response (Subtype = 0).

2.9 Beacon Period

Figure 42 illustrates an example of a BP observed by a device in a given superframe.

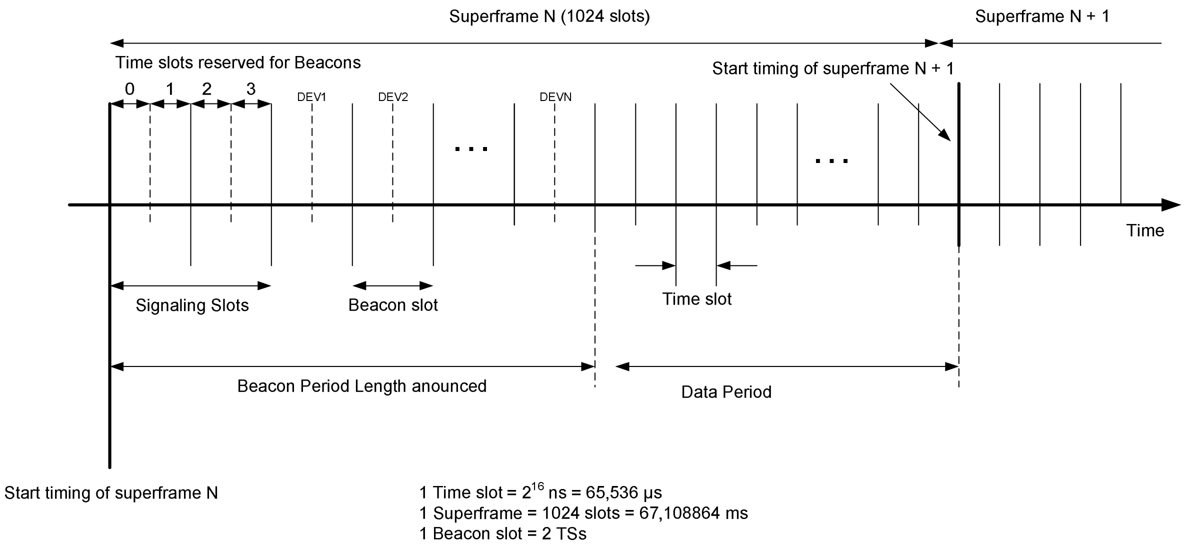


Figure 42: Beacon Period (BP) description

Each superframe starts with a Beacon Period (BP), which extends over one or more contiguous Beacon slots. The duration of a Beacon slot is 2xTSs. The start of the first TS in the BP, and the superframe, is called the beacon period start time (BPST). Each superframe starts with a BP, which has a maximum length of 64 time slots. Beacon slots in the BP are numbered in sequence, starting at zero. The first 2 beacon slots of a BP are referred to as signalling slots and are used to extend the BP length of neighbours.

When transmitting in a beacon slot, a device shall start transmission of the frame on the medium at the beginning of that beacon slot.

A device shall transmit beacons at 150 Megabits/s. The transmission time of beacon frames shall not exceed BeaconSlotDuration – 2xSIFS Time = 2x65,536 -2x8µs= 115,072µs. This allows for a guard time of at least 2xSIFS Time between the end of a beacon and the start of the next beacon slot.

A device shall announce its BP length in its beacon as a count of beacon slots starting from the BPST. The announced BP length shall include a) the device's own beacon slots in the current superframe, b) all monitored beacon slots in the BP of the prior superframe, and c) the beacon slot indicated in any beacon received in a signalling slot in the prior superframe.

2.9.1 Beacon transmission

Before a device transmits any frames, it shall scan for beacons for at least two superframes, or at least two superframes if no beacon frame is received. If the device receives no frame headers during the scan, it shall create a new BP and send a beacon in the first beacon slot after the signalling slots. If the device receives one or more frame headers, but no beacon frames with a valid FCS during the scan, the device should scan for an additional superframe.

If the device receives one or more beacons during the scan, it shall not create a new BP. Instead, prior to communicating with another device, the device shall transmit a beacon in a beacon slot selected from up to 8 beacon slots located after the highest-numbered unavailable beacon slot in the last superframe and within 64 after the BPST.

A device shall not transmit frames in the current superframe during the BP length indicated in the most recent beacon received from any neighbour in the previous 4 superframes.

A device shall consider another device to be a neighbour if it has received a beacon from that device within the last 4 superframes, and the latest beacon from the device indicated a BPST aligned with its own. If a device has not received a beacon from another device for the last 4 superframes, it shall not consider the device a neighbour.

A device shall not consider a received beacon with the Signalling Slot bit set to one as received from a neighbour.

2.9.2 Beacon slot collision

A device shall consider itself involved in a beacon slot collision with another device if one of the following events occurs:

- Its beacon slot is reported as occupied in the Beacon Period Occupancy IE in any beacon it receives in the current superframe, but the corresponding DevAddr is neither BcstAddr nor its own DevAddr used in the previous superframe.
- After skipping beacon transmission in the previous superframe, its beacon slot is reported as occupied in the Beacon Period Occupancy IE in any beacon it receives in the current superframe, and the corresponding DevAddr is not BcstAddr.
- When skipping beacon transmission in the current superframe, it receives a MAC header of type beacon frame in its beacon slot.
- It receives a signalling slot beacon aligned with one of its own signalling slots, with the Beacon Slot Number field set to its own beacon slot.

Certain events indicate a potential beacon slot collision. A device should consider the possibility of a beacon slot collision and take appropriate action if one or more of the following anomalous events occurs, or occurs consistently over multiple superframes:

- The device’s beacon slot was reported as occupied and the corresponding DevAddr was BcstAddr in the Beacon Period Occupancy IE of a beacon it received in the current superframe, and it sent a beacon in its beacon slot in the previous superframe.
- After skipping beacon transmission in the previous superframe, its beacon slot is reported as occupied in the Beacon Period Occupancy IE in any beacon it receives in the current superframe and the corresponding DevAddr is BcstAddr.
- When skipping beacon transmission in the current superframe, it receives a PHY indication of medium activity in its beacon slot that does not result in correct reception of a frame header.

If a device detects a beacon slot collision, it shall select a different beacon slot for its subsequent beacon transmissions from up to 8 beacon slots located after the highest-numbered unavailable beacon slot in the last superframe and within 64 after the BPST.

2.9.3 Use of signalling slots

If the beacon slot in which a device will transmit its beacon in the current superframe is located beyond the BP length indicated in any beacon the device received from a neighbour in the previous superframe, the device shall also transmit the same beacon, except with the Signalling Slot bit set to one, in a randomly selected signalling slot, except as follows:

- it should wait for a random number of superframes before sending a beacon in a signalling slot
- If a device transmits a beacon in a signalling slot for 4 consecutive superframes, it shall not transmit a beacon in a signalling slot in the next 4 superframes, and it should not transmit a signalling slot beacon for an additional aperiodic interval that does not exceed 128 superframes.

A device also may send a beacon in a signalling slot in response to abnormal conditions, such as failure to receive a beacon from a neighbour that previously did not include the device's beacon slot in its BP Length, or failure of a neighbour to report reception of the device's beacon in its Beacon Period Occupancy IE.

2.9.4 Required reception interval

An active mode device shall listen for neighbours’ beacons in the first N beacon slots in each superframe, where N is the greater of its BP Length values for the current and previous superframes. At a minimum, the device shall listen for intervals such that it would receive a frame with a reception time within GuardTime of the start of any of the N beacon slots.

If a device received a beacon with invalid FCS, or detected a medium activity that did not result in reception of a frame with valid HCS in a signalling slot in the previous superframe, no BP Length adjustment is required, but it shall listen for beacons for an additional 8 beacon slots after its BP length indicated in the current superframe, but not more than 64 beacon slots.

2.9.5 Skipping beacon transmission

An active mode device shall transmit a beacon sequence in each superframe, except as follows: In order to detect beacon slot collisions with neighbours, a device shall skip beacon transmission aperiodically, and listen for a potential neighbour in its beacon slot. A device shall skip beacon transmission, but not any associated signalling slot beacon, at least every 128. When a device skips beacon transmission, it shall act as if the skipped beacon were transmitted.

2.10 Reservation Protocol (RP)

The RP enables devices to reserve one or more TSs that the device can use to communicate with one or more neighbours. A device shall announce its reservations by including RP IEs in its Beacons. A reservation is the set of TSs identified by RP IEs with the same values in the Target/Owner DevAddr, Owner, Reservation Type, and Stream Index fields.

Reservation negotiation is always initiated by the device that will initiate frame transactions in the reservation, referred to as the reservation owner. The device that will receive information is referred to as the reservation target. In a reservation, devices other than the reservation owner and target(s) shall not transmit frames. Devices other than the reservation owner shall not initiate frame transactions.

In full duplex mode, a device can reserve time slots that are already reserved, only if these time slots are used to send data to the device which has already reserved these timeslots.

The transmission type in the Reservation protocol Information Element, must be set to zero, if there is no full duplex transmission for any of the reserved time slots with a given device. The transmission type must be set to one, if there is at least one time slot working in full duplex transmission for a given reservation.

A device shall not transmit a data frame unless the Delivery ID field is set to a Stream Index that is the same as the Stream Index for the reservation and the DestAddr of the frame is the same as the Target DevAddr for the reservation. A device may transmit any command or control frame in a reservation.

That's why the user priority bits in the delivery ID field (in the MAC header), won't be used until a CSMA/CA solution is specified.

A device shall not negotiate for TSs that are included in a RP IE received from a neighbour or any other DRP IE included in the device's beacon, unless the TSs are referenced only in a RP IE with Reason Code set to Denied.

Implicit negotiation is carried out by transmitting RP IE(s) in beacon frames. A device that supports the RP shall parse all beacons received from neighbours for RP IE(s) whose Target/Owner DevAddr field matches either the device's DevAddr or a multicast DevAddr for which the device has activated multicast reception. From this initial selection, the device shall process the RP IE(s) that are new with respect to RP IE(s) included in the most recently received beacon from the same device as a RP reservation request or a RP reservation response.

To start implicit negotiation, a reservation owner shall include a RP IE that describes the proposed reservation in its beacon. The device should continue to include the RP IE for at least 4 consecutive superframes or until a response is received.

On reception of a unicast RP reservation request in a beacon, the reservation target shall include a RP reservation response in its beacon no later than the next superframe, with fields set as described as follows:

- If a unicast reservation is granted, it shall set the Reservation Status bit to one and the Reason Code to Accepted.
- If a multicast reservation is granted, it shall set the Reservation Status bit to the same value included in the RP IE by the reservation owner, and shall set the Reason Code to Accepted.
- If the reservation is not granted, it shall set the Reservation Status bit to zero.
- If the reservation cannot be granted due to a conflict with its own or its neighbours' reservations, the reservation target shall set the Reason Code to Conflict.
- If the reservation is not granted, it shall set the Reason Code to Denied. If the reservation target cannot grant the reservation immediately, it may set the Reason Code to Pending, and deliver a final response later. For a unicast reservation, the reservation target shall set the RP Allocation fields to match those in the request. For a multicast reservation, it shall set the RP Allocation fields to match the request, or to include a subset of the TSs included in the request.

If the Reason Code indicates Conflict, the reservation target shall include a RP Availability IE in its beacon.

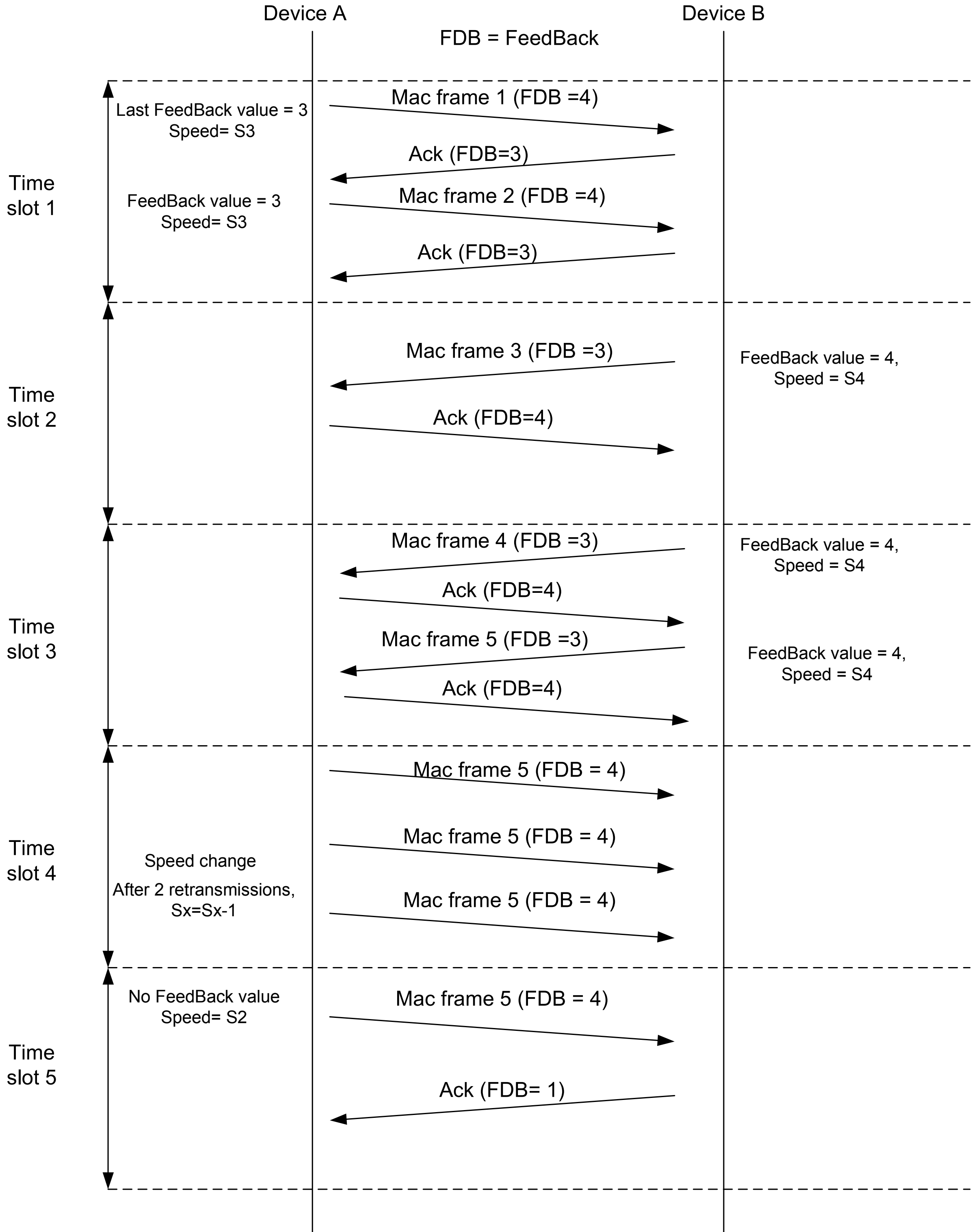
As long as the reservation owner includes a unicast RP reservation request in its beacon, the reservation target shall continue to include the RP reservation response in its beacon. The reservation target shall not change the Reservation Status bit to one if there is a reservation conflict with its neighbours.

On reception of a multicast RP reservation request, a reservation target shall include a reservation response RP IE in its beacon no later than the next superframe if it is a member of the targeted multicast group. The fields in the RP IE shall be set as described above. If the Reservation Status bit in the response is zero, the reservation target shall include a RP Availability IE in its beacon unless the Reason Code is set to Denied.

A device that elects to receive traffic in an already established multicast reservation does not negotiate the reservation. To join an established multicast reservation that does not conflict with other existing reservations, a device shall include corresponding RP IE(s) in its beacon with Reservation Status bit set to one and Reason Code set to Accepted.

A device that cannot join an established multicast reservation because of an availability conflict may inform the source by including the corresponding RP IE(s) in its beacon with Reservation Status bit set to zero, and the Reason Code set to Conflict. The device shall also include the RP Availability IE in the beacon.

2.11 Link adaptation (Half duplex mode example)



FDB	Speed
1	S1=128 Mbits/s
2	S2=256 Mbits/s
3	S3= 512 Mbits/s
4	S4=1024 Mbits/s

After 2 retransmissions a device must adapt its speed, Sx=Sx-1

Figure 43 : Link adaptation example

Depending on the medium conditions and retransmissions, a device should be able to adapt his throughput as shown in Figure 43. Let's assume that there are N data rate available (N=4 in the above figure). Each data rate corresponding to a predefined medium condition (based on BER, RSSI, SNR….). When device A receives a frame from device B (Figure 43 : Link adaptation example, Time slot 3), device A will assess (based on BER, RSSI, SNR….) the uplink medium conditions (B=>A) and send the result to device B, in the Access & feedback MAC header field of the ACK frame. When device B receives the link feedback from device A, it will adapt his data rate accordingly, if the medium condition hasn't changed, device B won't change his data rate, if the Link feedback is x, device A should change his data rate to Sx megabits/s (see table Figure 43 : Link adaptation example).

The link adaptation algorithm should also check the number of retransmissions. If the data rate is Sx megabits/s ($x \geq 2$), and if device A has sent a MAC frame twice, and hasn't received any acknowledgment, it should change his data rate to Sx-1 or to another lower data rate (Figure 43 : Link adaptation example, Time slot 4 & 5).

2.12 Emergency traffic

Emergency traffic can be either sent in Beacons (see 2.6.9) or in reserved time slots (see 2.6.8.4). Beacons are always sent at the lowest data rate (defined in the D4.2 [7] document), moreover two Beacons frames are separated by a guard interval (2xSIFS time= 2x8s) , that's why a device can sent a maximum of 792 bytes (Phy preamble and PLCP header included) in a Beacon slot. If the emergency message is too long, a device will have to reserve some Time Slots to be able to send his emergency message. If all the time slots are reserved, the device will indicate in his Beacon which time slot he wants to use to send his emergency message (the time slots preempted for emergency traffic must be taken from all the devices, to make sure all devices release time slots if needed). After two super frame, each device should have updated his Beacon accordingly. The device wishing to send an emergency message, should then send his emergency message in the released time slots.

To make sure that a device can always include an Emergency IE (4 bytes) in a beacon, the length of the beacon (excluding the Emergency IE) shouldn't exceed 788 bytes.

2.13 Tunnel Mode – Ethernet over OWMAC

To gain in efficiency in terms of time processing, a device can use a tunnel mode, the Ethernet frames are directly encapsulated in OWMAC Frame, thus, with this mode there is no need to remove the Ethernet header when receiving an Ethernet frame, before sending the corresponding OWMAC frame.

Ethernet over OWMAC uses protocol ID value 0x0103. Note that we could encapsulate any other layer two protocol , in OWMAC frames, other Protocol ID value would then have to be defined.

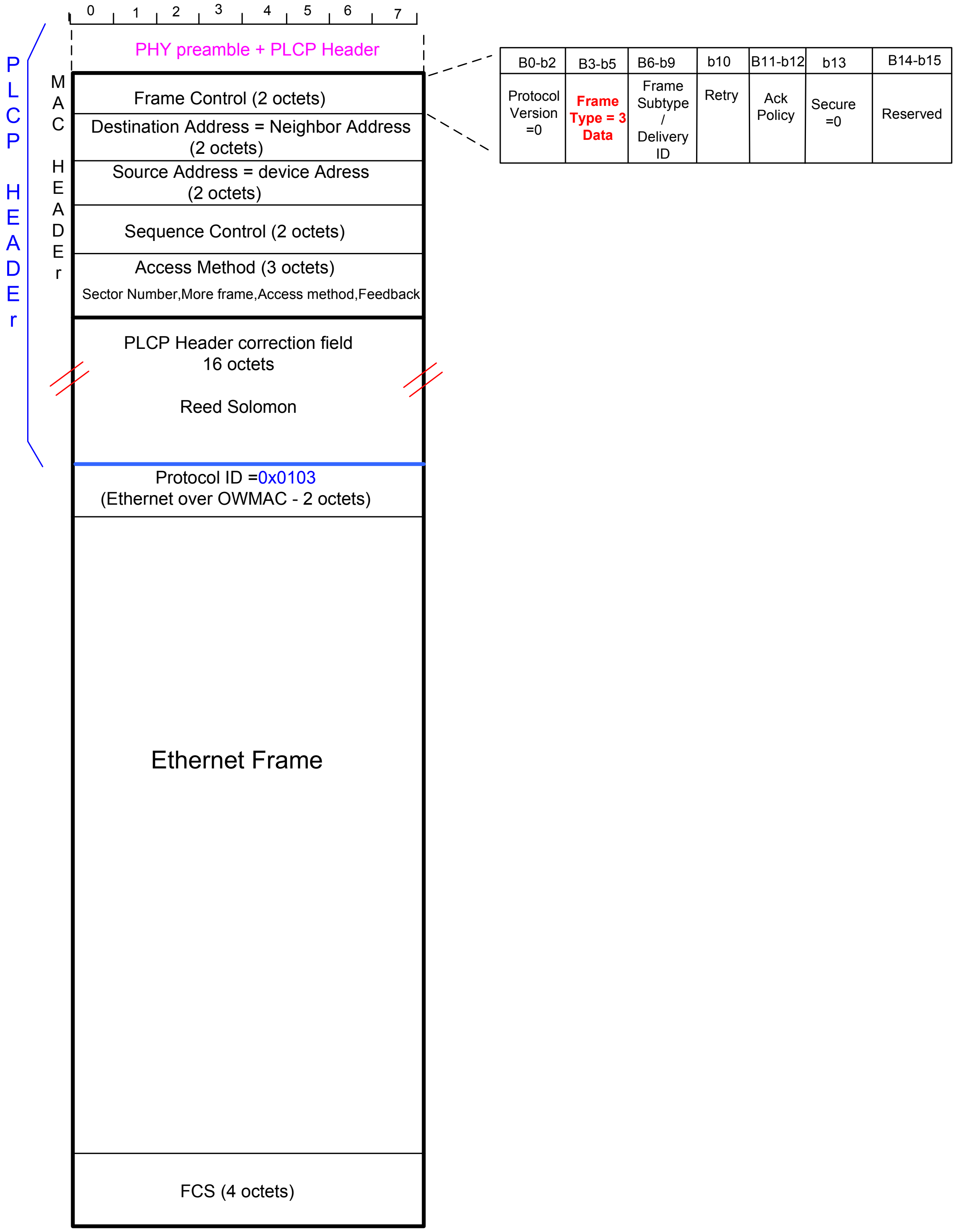


Figure 44- Ethernet over OWMAC frame

3 OWLLC description

3.1 OWLLC frame format

The OWLLC frame format is described in Figure 45.

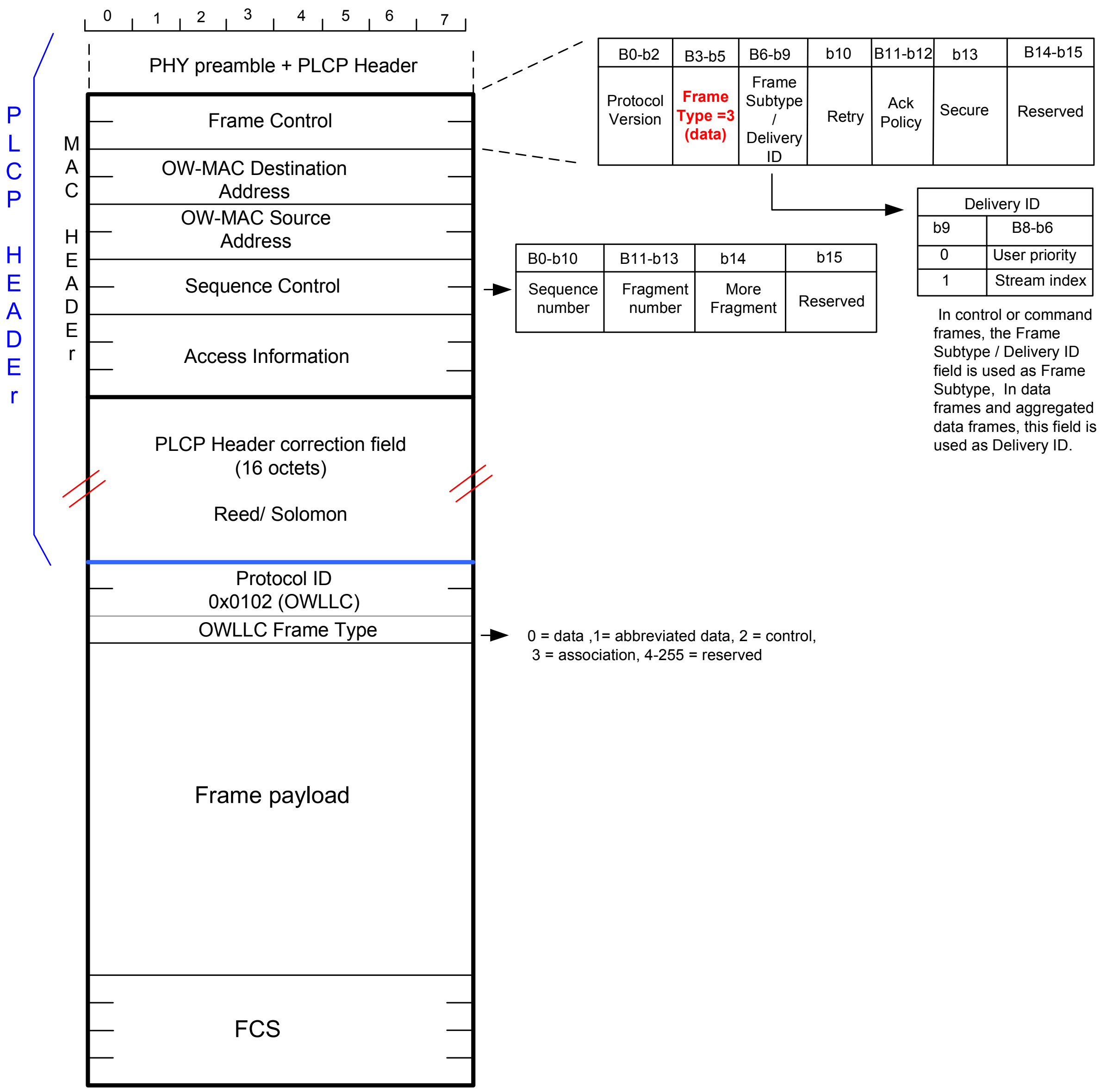


Figure 45: OWLLC Frame format

An OWLLC Frame, is a OWMAC data frame. The multiplexing MAC header is used to specify the type of OWMAC dataframe. The multiplexing header for all OWLLC Frame is the OWLLC Protocol ID 0X0102.

The OWLLC Frame Type field is set to a value from Table 10, which contains a list of OWLLC Frame Types, the names of the frame types, and the subclauses that describe the frame format for each of the frame types.

Table 10- OWLLC Frame Type field encoding

Value	OWLLCP Frame Type	Subclause
0	Standard Data	
1	Abbreviated Data	
2	Control	
3	Association	
4–255	Reserved	

3.2 Standard Data frame

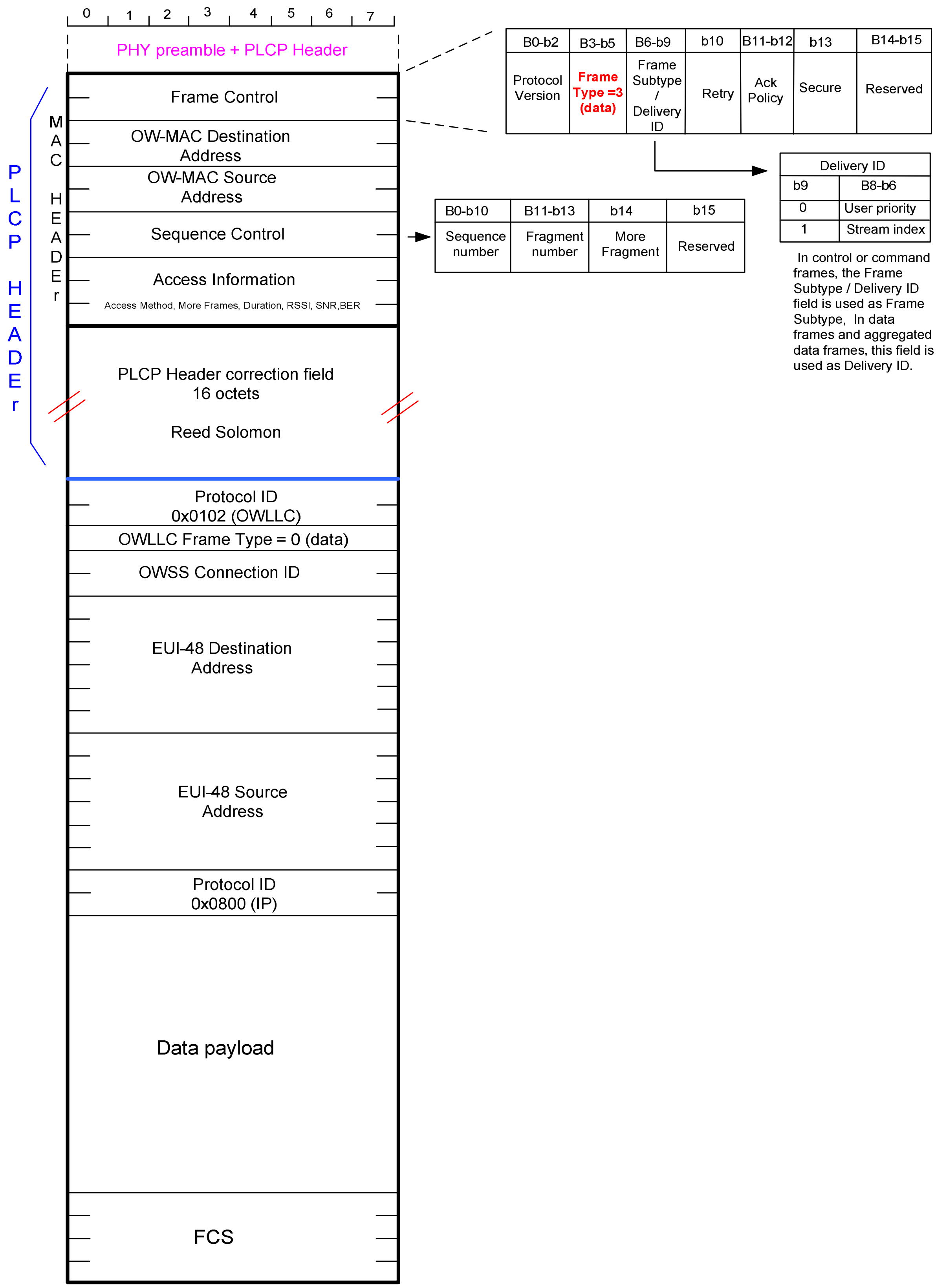


Figure 46- OWLLC Standard format Example

The OWLLC Frame Type field is set to zero. The OWSSID connection ID field is set to a value used by the transmitting device to identify the OWSS for the data frame, as described in 2.6.8.2. The Destination Address field is set to the EUI-48 [2] of the ultimate destination of the frame. The EUI-48 is a sequence of 6 octets. The Source Address field is set to the EUI-48 of the original source of the frame. The Type/Length field is set to a type or length value as described in section 2.2.

This two-octet field takes one of two meanings, depending on its numeric value. For numerical evaluation, the first octet is the most significant octet of this field.

- If the value of this field is less than or equal to the value of maxValidFrame = 1500 octets then the Length/Type field indicates the number of OWLLC layer (or other higher layer) data octets contained in the subsequent data field of the frame (Length interpretation).
- If the value of this field is greater than or equal to 1536 decimal (equal to 0600 hexadecimal), then the Length/Type field indicates the nature of the MAC client protocol (Type interpretation) as defined in section 2.2.2.3

The Data field contains the payload of the frame as received from the OWLLC client. The format is defined according to the value in the Type/Length field. In Figure 43 the protocol ID is 0x800, the data payload is therefore an IP packet.

3.3 Abbreviated data frame

An abbreviated data frame is a shorter version of the standard data frame that assumes that the original source and ultimate destination of the frame are the transmitting and recipient devices, respectively. The format of an abbreviated data frame is illustrated in Figure 47, note that there is no EUI destination or source address in the OWLLC header.

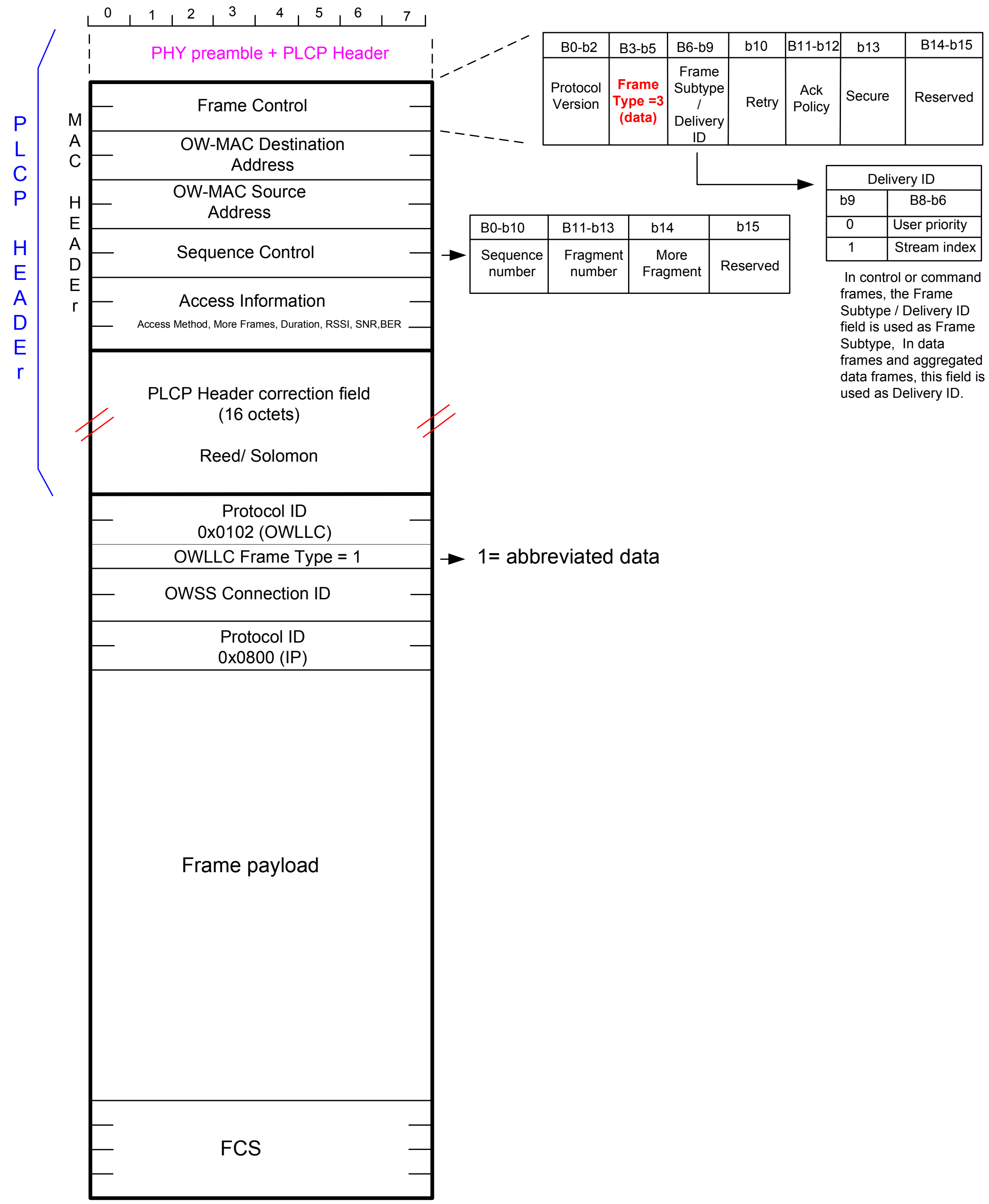


Figure 47: Abbreviated data frame

3.4 Association Frame

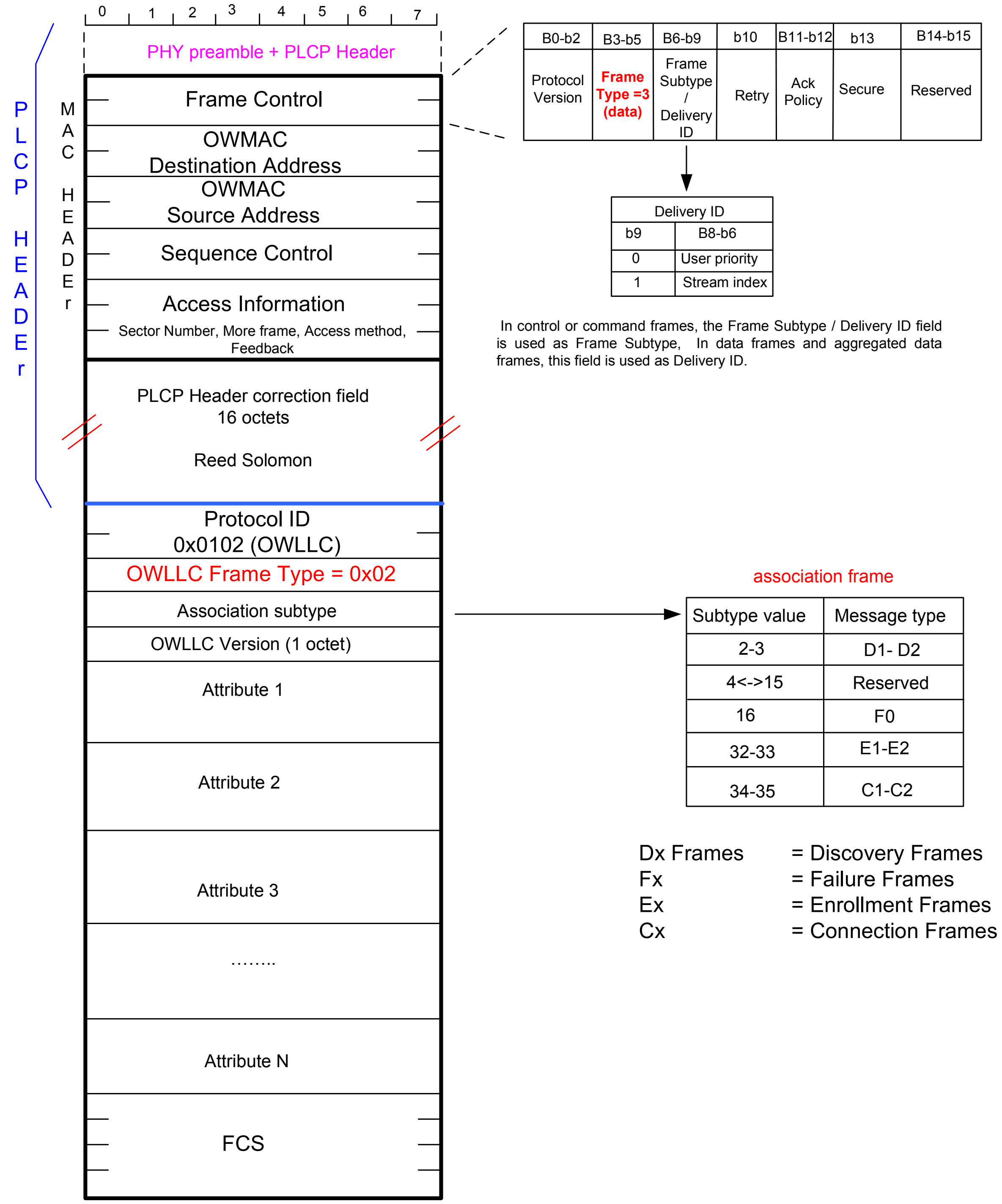


Figure 48: OWLLC Association Frame format

Association frames are encoded as a list of attributes, each of which contains a specific piece of information relevant for the particular association subtype. The general format of an association frame is illustrated in Figure 48.

The association subtype field defines the message type: Discovery, Enrollment, Failure or Connection. The Attribute Type field is illustrated in Figure 48. It determines the contents of the Attribute Value field. The Attribute Length field is set to the length of the Attribute Value field, in octets.

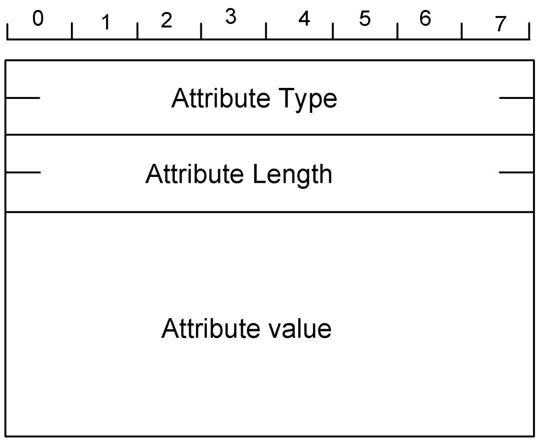


Figure 49: OWLLC Attribute field format

3.4.1 Discovery frame

*3.4.1.1 **D1 Frame***

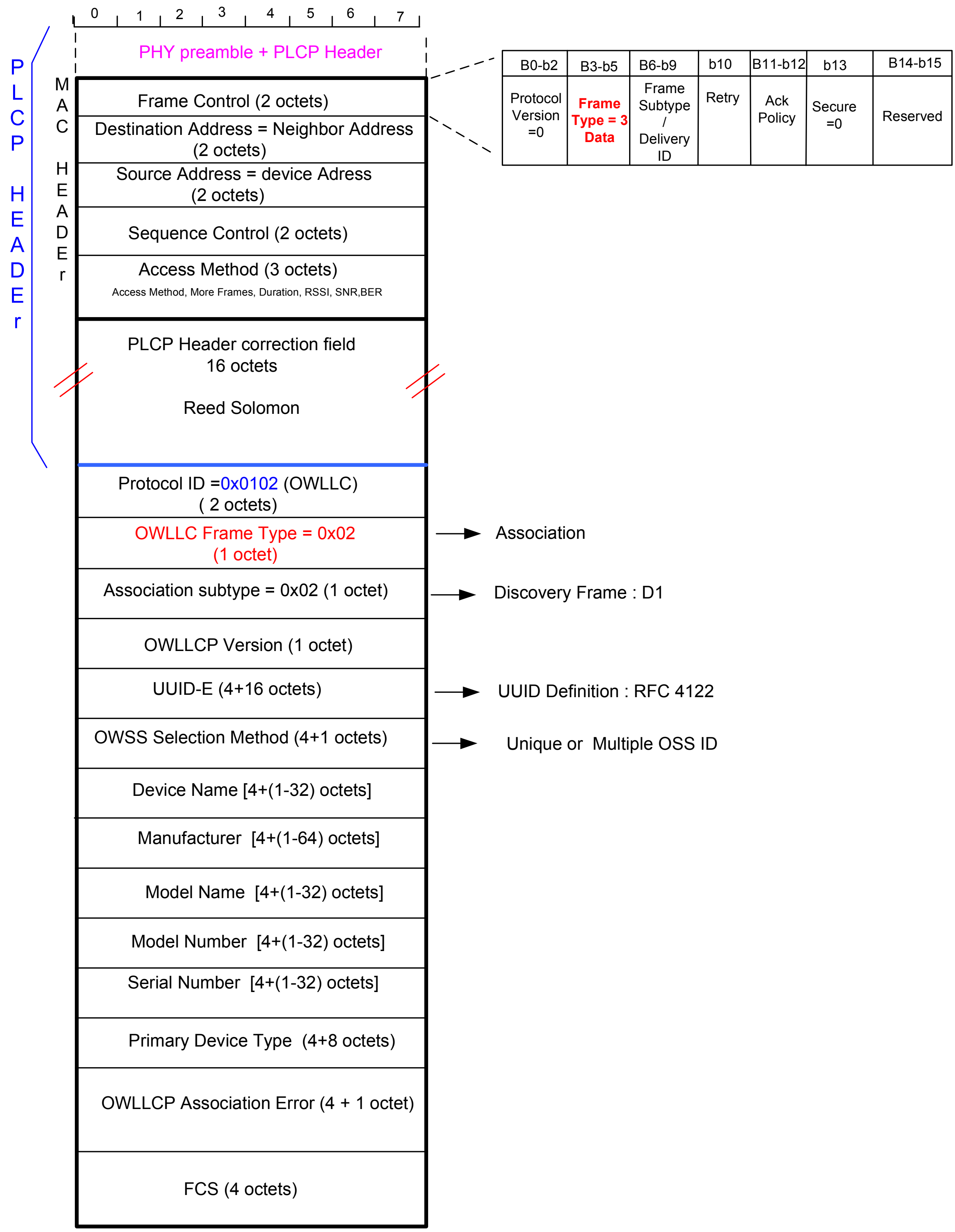


Figure 50: D1 frame description

3.4.1.2 D2 Frame

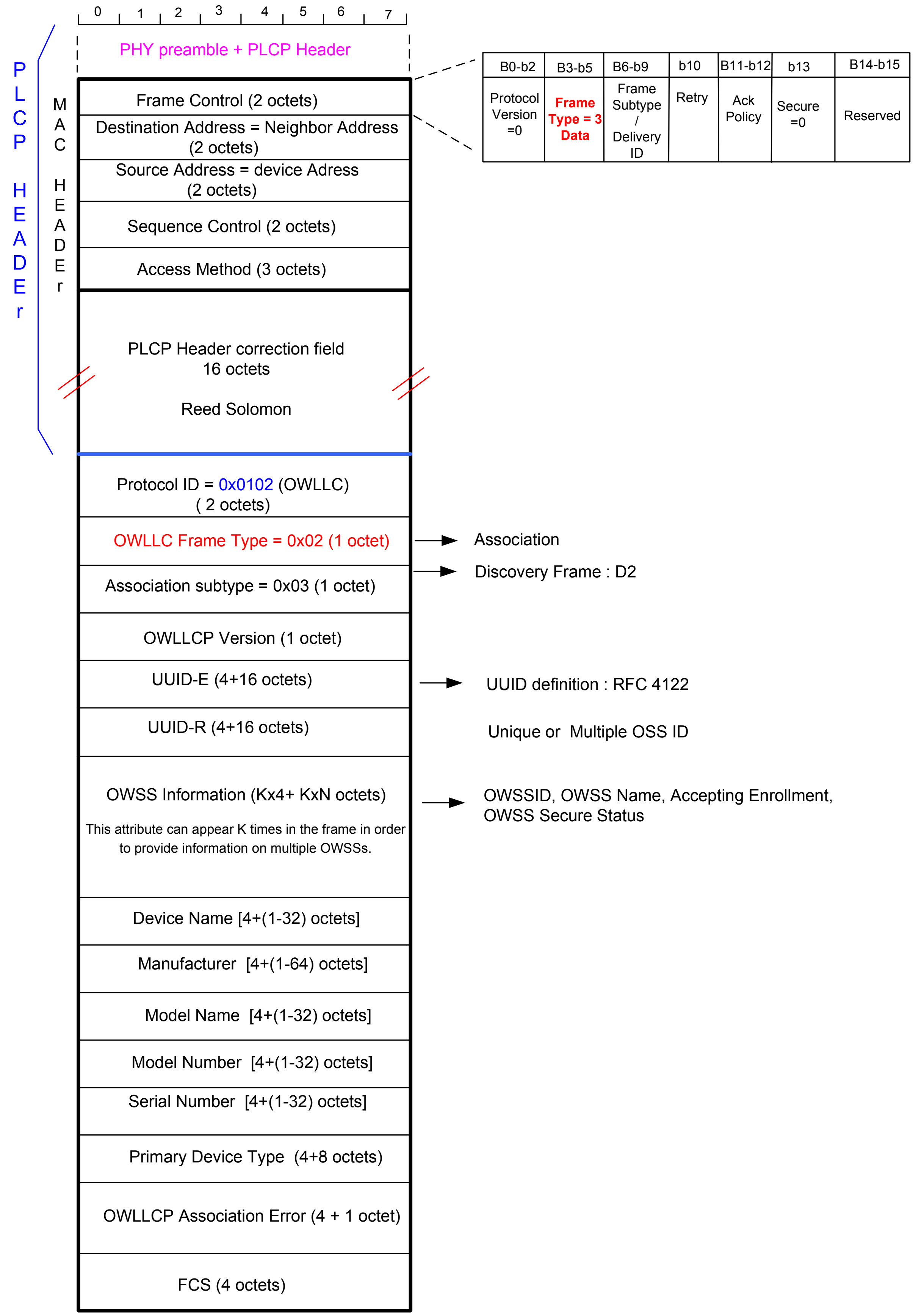


Figure 51: D2 frame description

3.4.2 Enrollment frames

3.4.2.1 E1 Frame

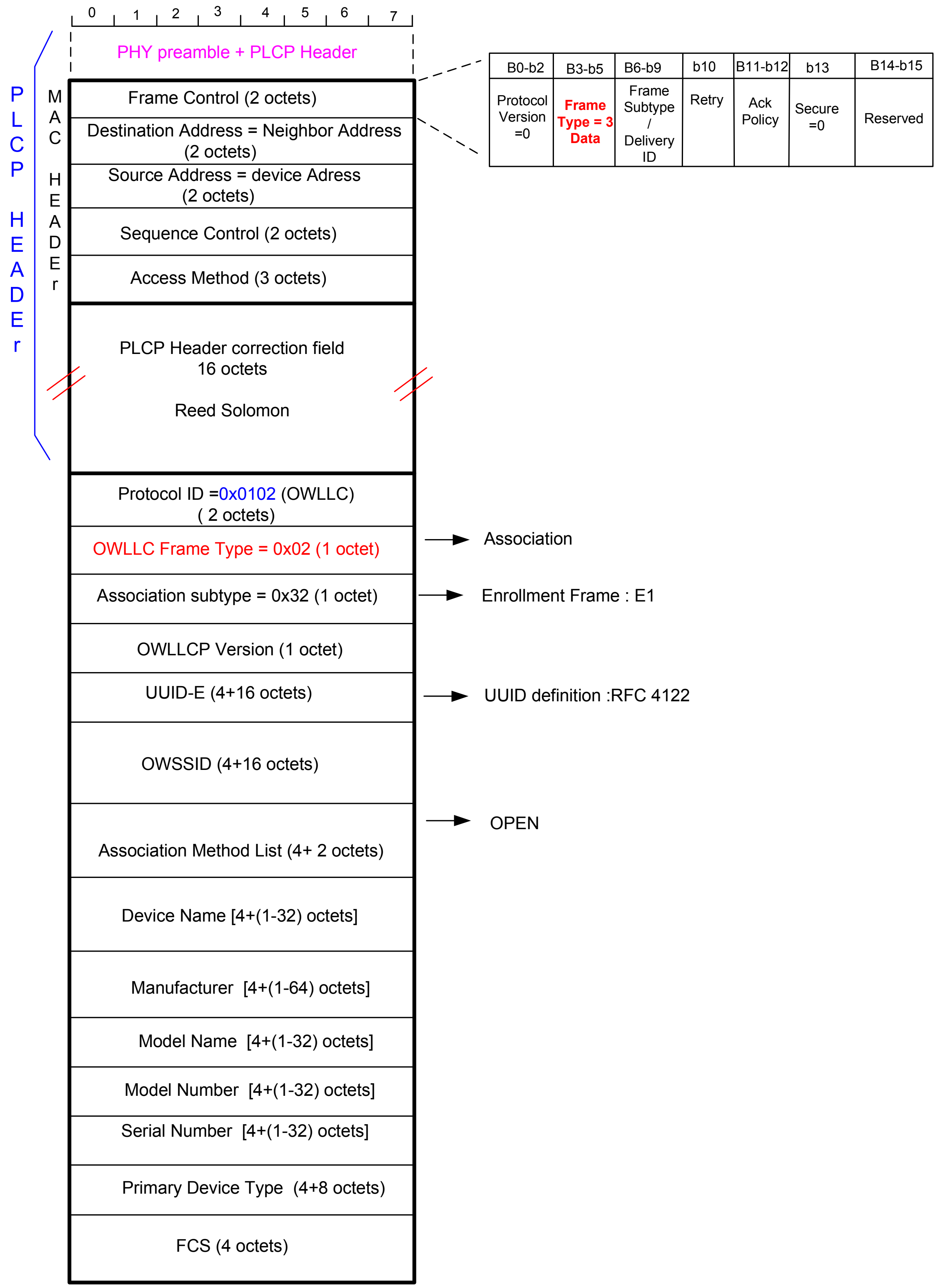


Figure 52: E1 frame description

3.4.2.2 *E2 Frame*

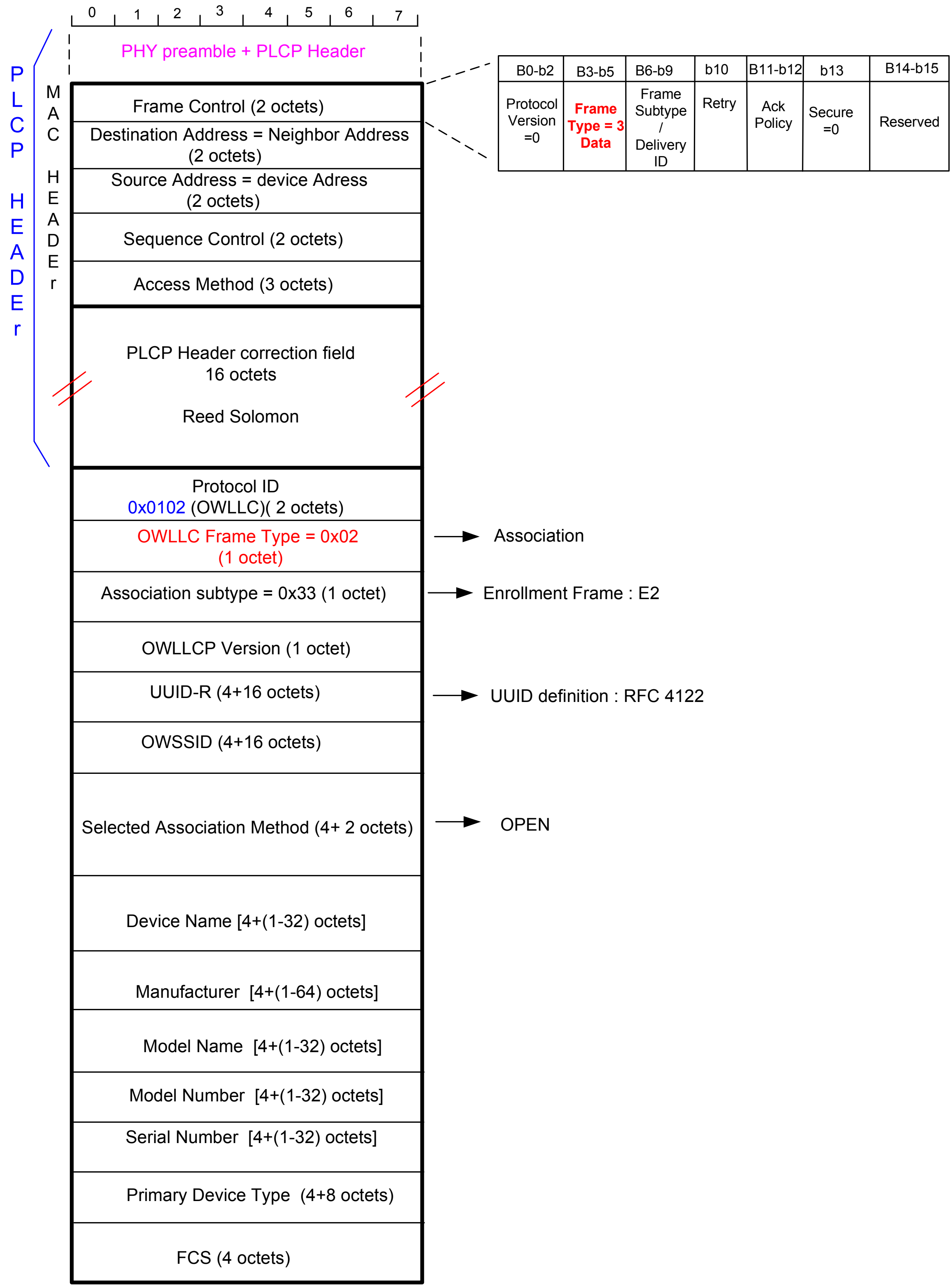


Figure 53: E2 frame description

3.4.3 Connection Frames

3.4.3.1 C1 frame

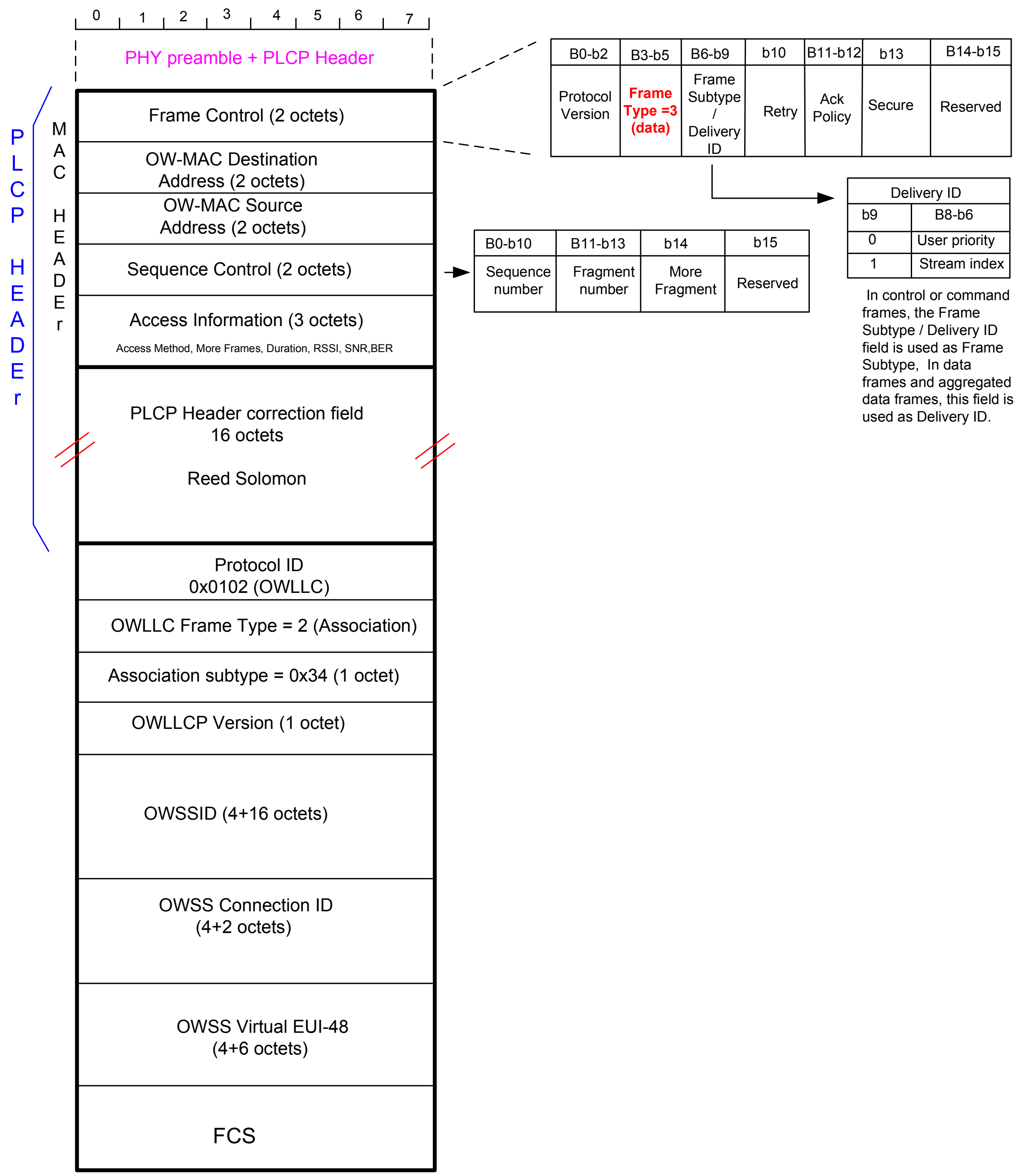


Figure 54: C1 frame description

The OWSS Virtual EUI-48 is a unicast EUI-48 used as by the device as its virtual local address for communication within the OWSS.

3.4.3.2 *C2 frame*

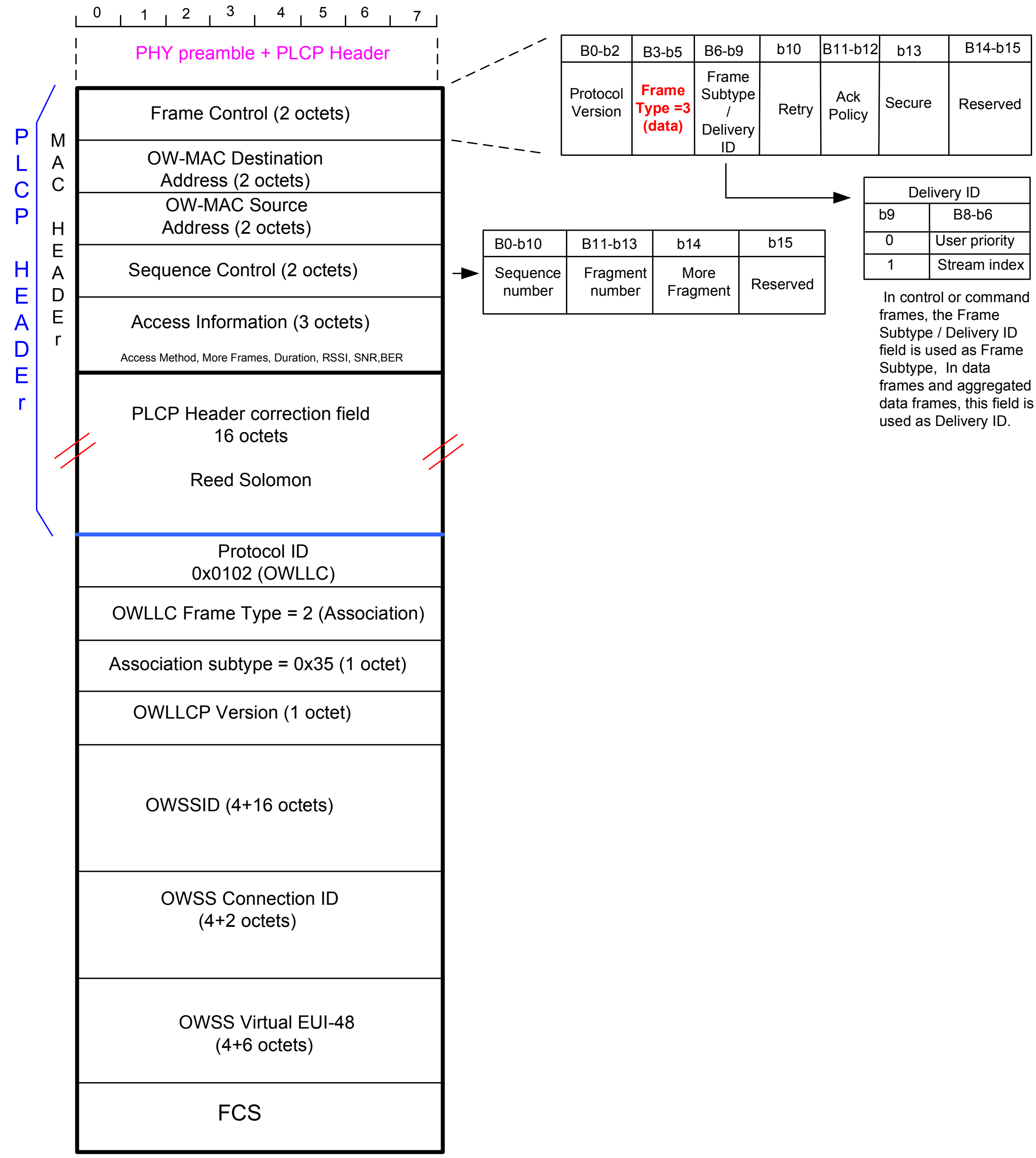


Figure 55 –C2 frame description

The OWSS Virtual EUI-48 is a unicast EUI-48 used as by the device as its virtual local address for communication within the OWSS.

3.4.3.3 *F0 Frame*

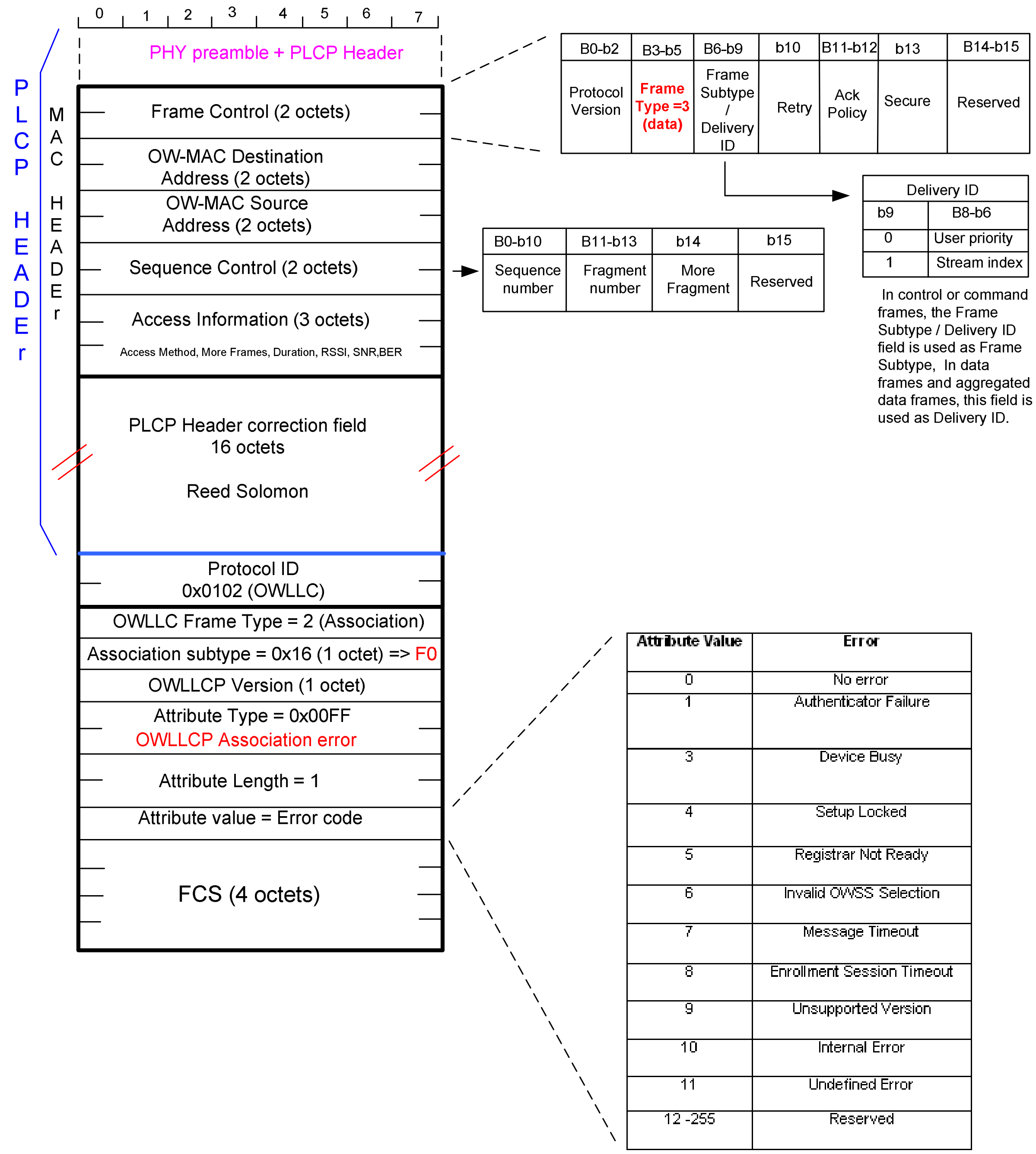


Figure 56: F0 frame description

3.5 Attribute fields description

3.5.1 Attribute fields

This section defines the attributes fields that can appear in association frames. The general format of all attributes fields is illustrated in Figure 56.

The attribute type field is set to the value as listed in Table 11 that identifies the attribute. The Length field is set to the length, in octets, of the attribute-specific fields that follow. The attribute-specific fields contain information specific to the attribute.

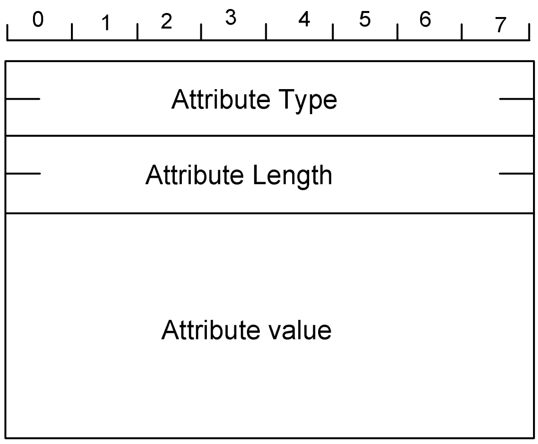


Figure 57 : Attribute field general format

Table 11 - Attribute type

Attribute value	Attribute type	Description
0x0001	OWSS Information Attribute	The OWSS Information Atttribute contains 4 attributes defining each OWSS dvertised by the Registrar : the OWSSID identifying the Service Set, the OWSS Name, the Accepting Enrollment Status, and the OWSS Secure Status.
0x0002	OWSSID	OWLLC service set identifier. The value is a UUID (Universally Unique Identifier) encoded as an octet string in the order the octets are shown in string representation in RFC 4122.
0x0003	Universally Unique Identifier (UUID)- Enrollee	Universally unique identifier (UUID) assigned to the enrollee.
0x0004	Universally Unique Identifier (UUID)- Registrar	Universally unique identifier (UUID) assigned to the registrar.
0x0005	OWSS Selection Method Attribute	If the Enrollee select method is used, the registrar is requested to provide information on all OWSSs for which it is currently accepting enrollment.
0x0006	Association Methods List attribute	For the prototype, only one method is defined, the OPEN method. The registrar admits any Enrollee to the OWSS. The value for the OPEN method is zero.
0x0007	OWSS Name	The friendly name of a OWSS, encoded as an octet string in UTF-8 format
0x0008	Accepting Enrolment	Set to one if the registrar is accepting enrollment in this WSS, or zero otherwise.
0x0009	OWSS Secure Status	Set to one if the WSS is secure or zero if it is not secure.
0x000A	OWSS connection ID	The connection id is a unique number identifying a connection in a given OWWS.
0x000B	OWSS EUI-48	An EUI-48, encoded as an octet string, that identifies the sending device within a OWSS
0x00FF	OWLLCP Association Error Attribute	The result of an OWLLC association.

3.5.2 OWSSID Attribute

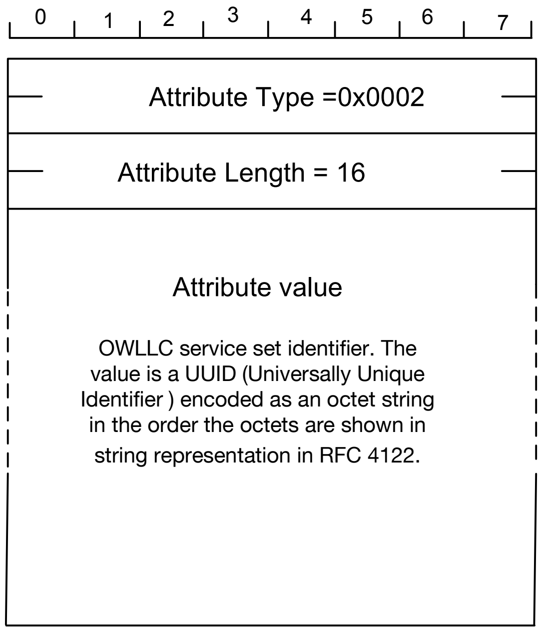


Figure 58- OWSSID attribute format

3.5.3 OWSS Information Attribute

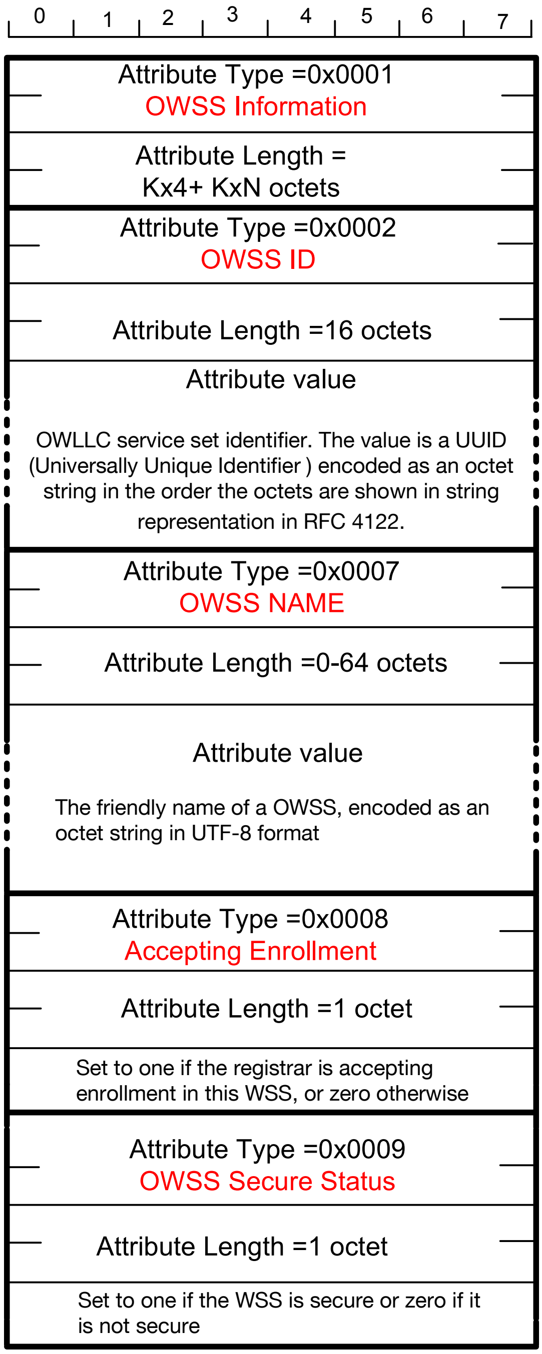


Figure 59: OWSS information attribute format

As shown in Figure 59, the OWSS Information Atttribute contains 4 attributes defining each OWSS advertised by the Registrar: the OWSSID identifying the Service Set, the OWSS Name, the Accepting Enrollment Status, and the OWSS Secure Status. This attribute can appear zero or more times in the frame in order to provide information on multiple OWSSs.

3.5.4 Universally Unique Identifier (UUID) Attributes

3.5.4.1 UUID-E

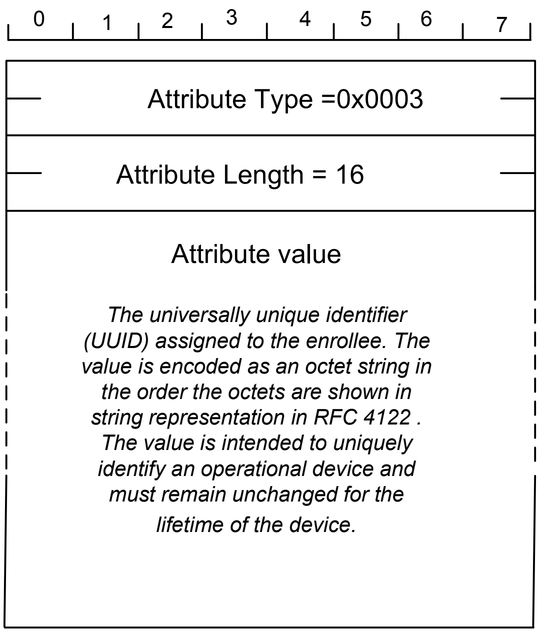


Figure 60: UUID-E attribute format

3.5.4.2 UUID-R

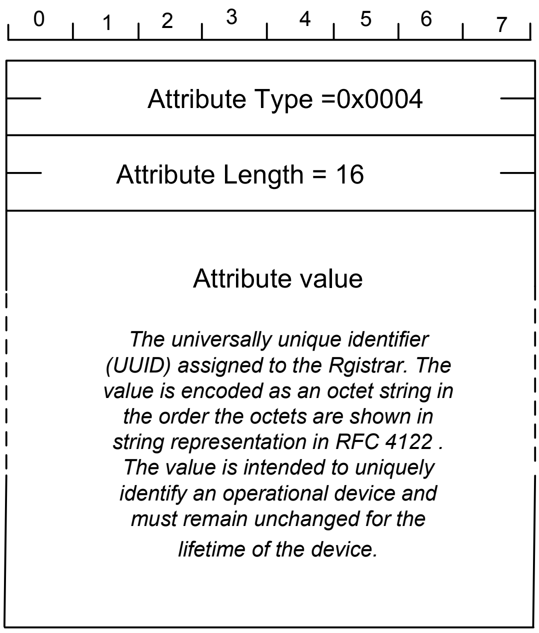


Figure 61: UUID-R attribute format

3.5.5 OWSS Selection Method Attribute

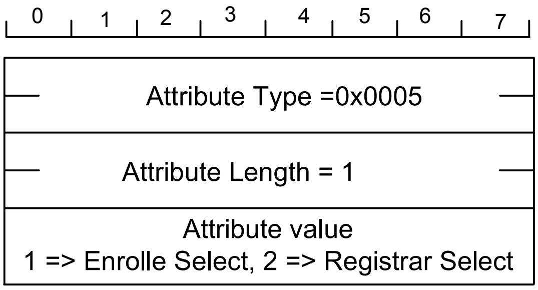


Figure 62: OWSS Selection Method Attribute format

If the Enrollee select method is used, the registrar is requested to provide information on all OWSSs for which it is currently accepting enrollment. The enrollee will select the OWSS in which it will seek to enroll. If this Registrar select method is used, the registrar is requested to provide information about only a single OWSS. The enrollee is not capable of selecting between multiple OWSSs.

3.5.6 Association Methods List attribute

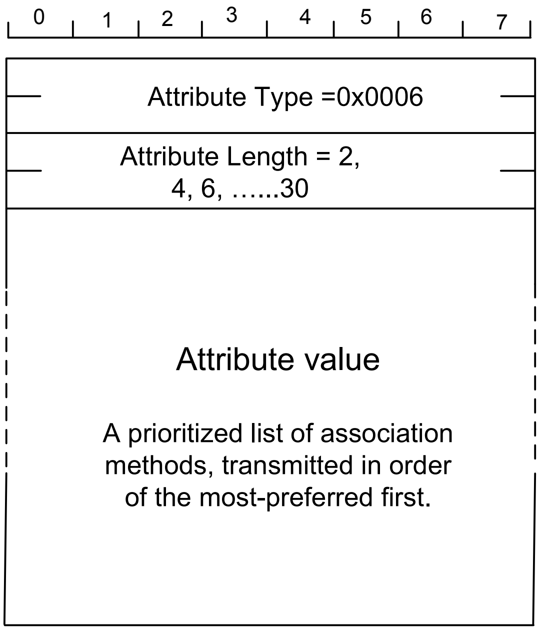


Figure 63: Association Method attribute format

For the prototype, only one method is defined, the OPEN method. The registrar admits any Enrollee to the OWSS. The value for the OPEN method is zero.

3.5.7 OWSS connection ID attribute

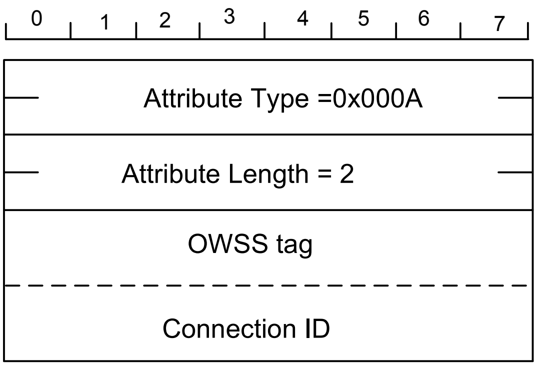


Figure 64: OWSS connection ID attribute

The first octet is the OWSS tag, a random number identifying the OWSS. The following octet is the OWSS connection ID; the connection id should be a unique number identifying a connection in a given OWSS.

3.5.8 OWSS Virtual EUI-48

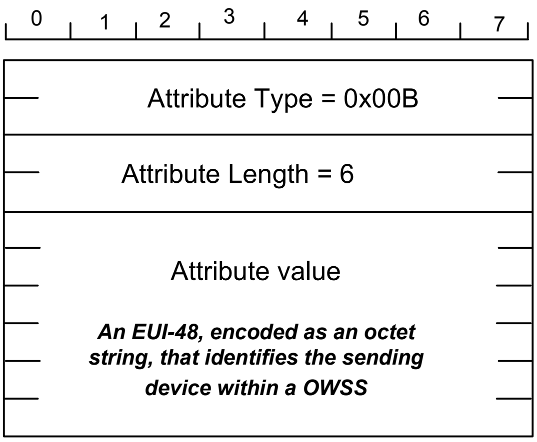


Figure 65: OWSS EUI-48 Attribute format

3.5.9 OWLLCP Association Error Attribute

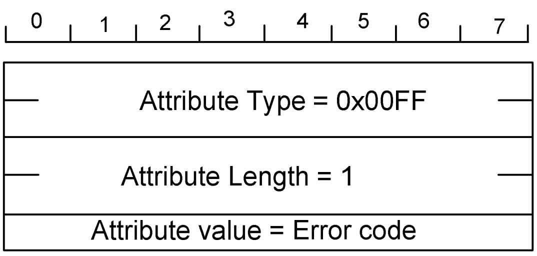


Figure 66: OWLLCP Association Error attribute format

Table 12: Error Attribute list

Attribute Value	Error	Description
0	No error	
1	Authenticator Failure	The device determined that an Authenticator or Key Wrap Authenticator attribute did not match that expected for the contents of a frame, and has abandoned the enrollment session.
3	Device Busy	The device was unable to process the request, for example, because it received multiple requests but can only participate in one enrollment session at a time. The device has abandoned the enrollment session.
4	Setup Locked	The registrar was not accepting enrollment requests because of too many recent enrollment failures.
5	Registrar Not Ready	The registrar is not ready to continue enrollment, and has abandoned the enrollment session.
6	Invalid OWSS Selection	The OWSSID requested for enrollment or connection is not valid.
7	Message Timeout	The device reached a timeout waiting for the next association frame in the sequence, and has abandoned the enrollment session.
8	Enrollment Session Timeout	The device reached a timeout on completing the entire enrollment session, and has abandoned the enrollment session.
9	Unsupported Version	The device received a frame that indicated an O WLLCP version not supported by the recipient, and has abandoned the enrollment session.

10	Internal Error	An unexpected error specific to the device occurred. The device has abandoned any enrollment session in progress.
11	Undefined Error	An error not defined in this table occurred. The device has abandoned any enrollment session in progress.
12	Waiting for response	The device is not ready to send the next association frame in a sequence because it is waiting for an association response.
13 -255	Reserved	

3.5.10 Other attributes

Table 13: Other Attribute list

Attribute Name	Attribute Type	Attribute Length (octets)	Attribute Value
Device Name	0x0010	1–32	The friendly name of the sending device, encoded as an octet string in UTF-8 format
Manufacturer	0x0011	0–64	The name of the manufacturer of the sending device, encoded as an octet string in UTF-8 format
Model Name	0x0012	0–32	The model name of the sending device, encoded as an octet string in UTF-8 format
Model Number	0x0013	0–32	The model number of the sending device, encoded as an octet string in UTF-8 format
Serial Number	0x0014	0–32	The serial number of the sending device, encoded as an octet string in UTF-8 format
Primary Device Type	0x0015	8	The primary type or function of the sending device.

3.5.10.1 Device Type attribute

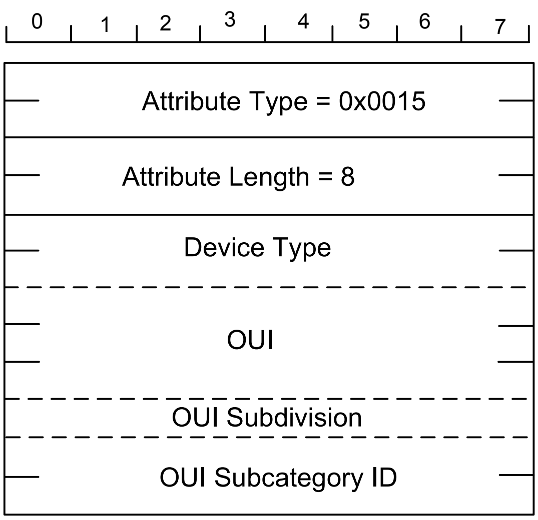


Figure 67: Device Type attribute format

The OUI field is set to the OUI of the organization that defines valid values for the OUI Subdivision and Subcategory ID fields. The OUI is encoded as an octet string. The OUI Subdivision field is defined by the OUI owner, and is used by the OUI owner to support multiple subcategory definition sets. The Subcategory ID is defined by the OUI owner, and identifies the specific device function.

Table 14- Device type list

Value	Device Type
1	Computer
2	Printer
3	scanner
4	FAX
5	copier
6	Telephone
7	Camera
8	Storage Network
9	Telephone
10	Router
11	Switch
12	Bridge
13	Infrastructure
14	Multimedia device
15	Gaming device
16	Multimedia device

3.6 OWLLC sublayer functional description

3.6.1 Association

A device shall send association frames to unicast addresses only. A device shall use the ACK acknowledgment policy at the MAC sublayer to send association frames. A device shall retransmit any association frame for which an ACK frame was not received. If a response is required, a registrar or enrollee shall respond to an association frame within 4 seconds of receiving the association frame.

3.6.2 OWSS discovery

If there is no OWSS advertised, a device can create a new OWSS, in which case it is automatically enrolled in the OWSS, but can only communicate with other devices that subsequently enroll in the OWSS. If there is an OWSS advertised by another device, the new device can enroll in the existing OWSS, in which case it can communicate with the device advertising the OWSS and any other devices also enrolled in that OWSS.

Discovery mechanisms could be based on a scan of the PHY channel for available and activated OWSSs. During discovery and a subsequent enrollment session, a device that is already enrolled in an existing OWSS is referred to as a registrar, and a device seeking to enroll in the OWSS is referred to as an enrollee. These roles are temporary and last only for the duration of the enrollment session.

A device shall be capable of acting as a registrar. A device shall be capable of acting as an enrollee. To check the OWSS properties of an OWSS activated by a neighbour, a device shall send a D1 association frame to the neighbour. A device shall not send a D1 frame to a neighbour unless the Discoverable bit is set to one in the latest OWLLC IE received from the neighbour.

A device that receives a D1 association frame shall respond with a D2 association frame that contains device information and OWSS information, or an F0 association frame that indicates why the discovery request is not accepted or OWSS information is not available. A registrar may respond with a D2 frame that includes partial information and a non-zero error code. A registrar should not send a D2 frame with a non-zero error code if the frame contains OWSS information with the Accepting Enrollment attribute value set to one. If an enrollee receives a D2 or F0 frame with the Association Error attribute value set to a non-zero value, it shall not respond with an E1 frame, and shall not send another D1 frame to the same registrar for at least one second. In a D2 frame, a registrar may respond with zero or more OWSS Information fields. If the OWSS Selection Method attribute value in the preceding D1 frame was set to Registrar Selects, the registrar shall not set the Accepting Enrollment attribute value to one in more than one OWSS Information field in the D2 frame.

3.6.3 OWSS activation

In order to enable connection to other devices in an OWSS, a device must activate the OWSS. Prior to activating a OWSS, a device must be enrolled in the OWSS. To activate a OWSS, a device shall include the OWSS tag and connection ID and OWSS name in the OWLLCP IE in its beacon in each superframe. A device may deactivate an OWSS by removing the OWSS tag, connection ID and OWSS name from its beacon. A device may activate multiple OWSSs simultaneously.

When a device activates an OWSS, it shall select an OWSS tag to identify the OWSS in frames that it transmits. The device shall not use the same OWSS tag value for more than one activated OWSS. In the event of conflict, the device should use the first unused value higher than the OWSSID tag, modulo 256.

3.6.4 Connection

Prior to exchanging data frames with a neighbour within an OWSS, a device shall connect to the neighbour. Prior to connecting, both devices must have activated the OWSS to be used for the communication context.

A device seeking to establish a connection shall transmit a C1 association frame to a target device. If a device receives a C1 frame that identifies an OWSS it has activated, it shall transmit a corresponding C2 association frame. Otherwise, it shall transmit an F0 association frame to indicate the connection failure. In a C1 or C2 frame, a device shall include the OWSS tag value selected when the device activated the OWSS. The tag is included in the Connection ID List attribute (see section 3.4.7)

3.6.5 Flow chart example (Half duplex example)

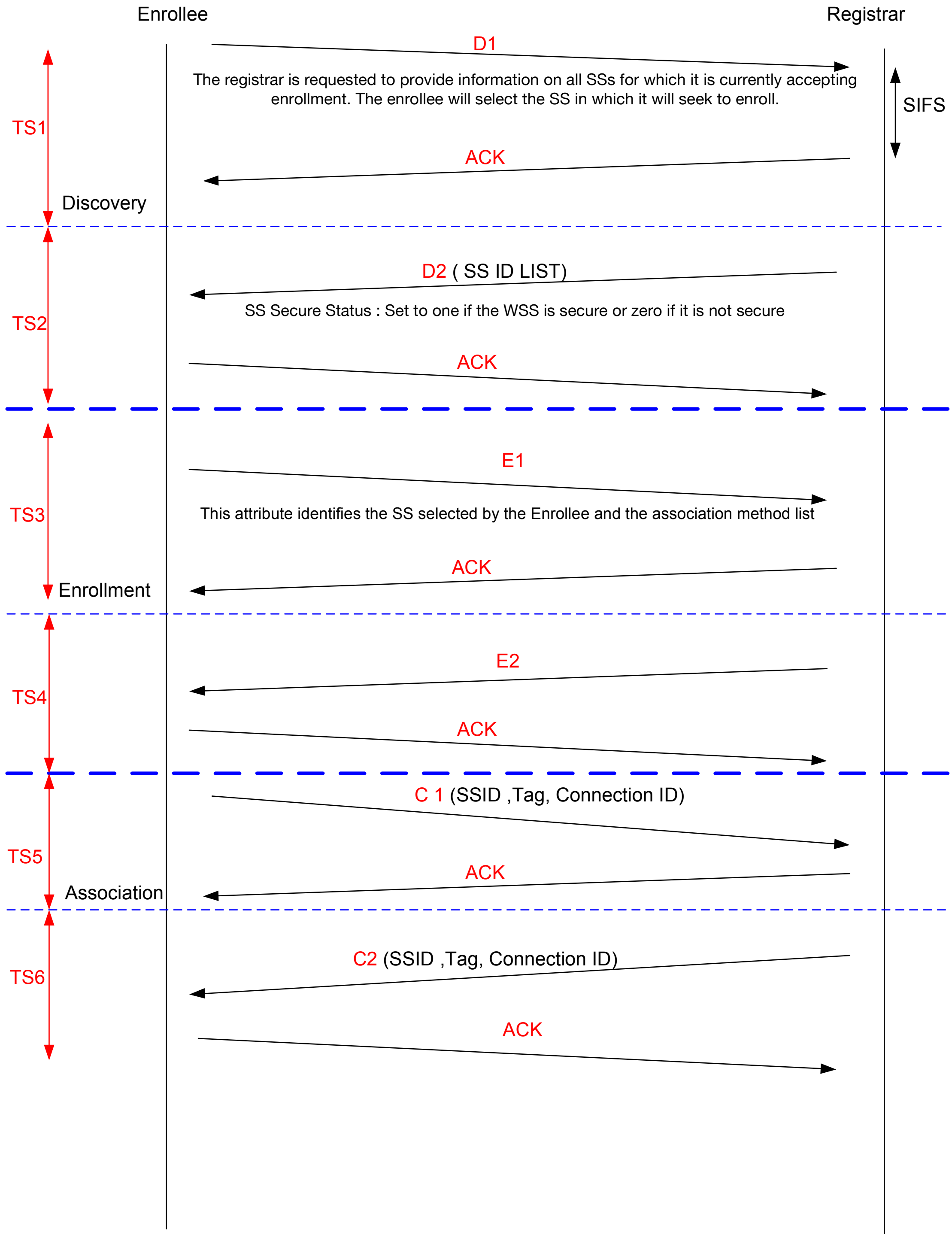


Figure 68: Flow chart example

4 Broadcast MAC frame used for VLC

An abbreviated data frame is a shorter version of the standard data frame that assumes that the original source and ultimate destination of the frame are the transmitting and recipient devices, respectively. The format of an abbreviated data frame is illustrated in Figure 69, note that there is no EUI destination or source address in the OWLLC header.

As there is only downlink traffic in VLC, the destination address is the broadcast address 0xFFFF.

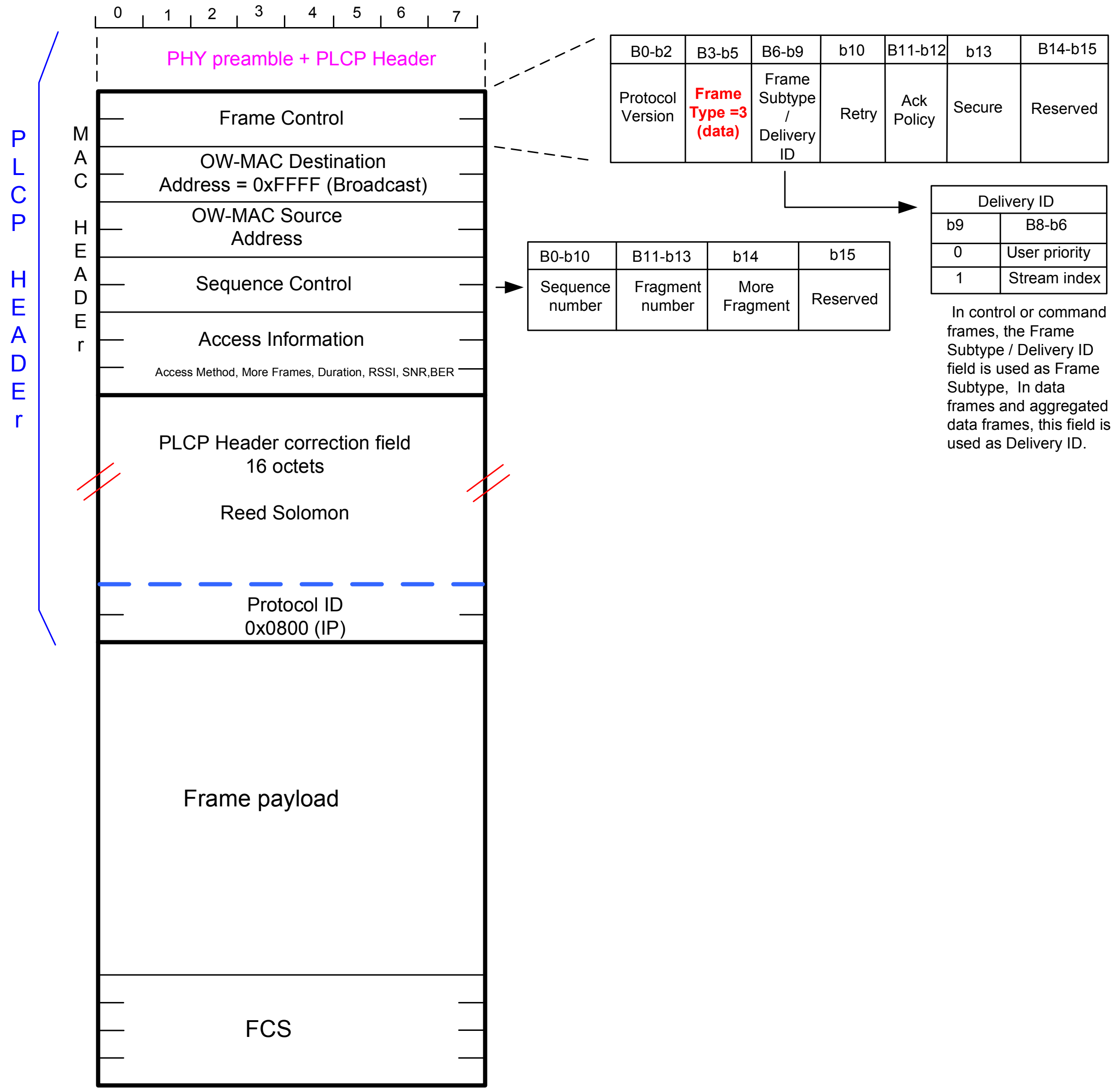


Figure 69: Abbreviated data example used for VLC

5 Power Save Mode recommendation

A device doesn't need to be awake during the whole superframe, it should be awake during the Beacon period and during the reserved time slots (for transmission and reception). In the other time slots the device can stay in power save mode.

6 Conclusion

This is the first public version for the specification of the OWMAC and the OWLLC layers; it includes TDMA, Multi-sector transmission, and Multi-rate function and full or half duplex communication. This specification also defines how a device chooses a sector, how it changes from one sector to another.

7 References

[1] IEEE STD 802.3™-2005 IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications. 2005. New York: Institute of Electrical and Electronics Engineers, Inc.

[2] "Guidelines for use of a 48-bit Extended Unique Identifier (EUI-48™)", http://standards.ieee.org/regauth/oui/tutorials/EUI48.html. 2005. New York: Institute of Electrical and Electronics Engineers, Inc.

[3] ISO/IEC 7498-1:1994, Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model. 1994. Geneva: ISO/IEC

[4] RFC 4122, A Universally Unique IDentifier (UUID) URN Namespace, P. Leach, M. Mealling, and R. Salz. July 2005. Internet Engineering Task Force.

[5] WiMedia ALLIANCE – MAC Specification – Draft 1.2 RC2 DISTRIBUTED MEDIUM ACCESS CONTROL (MAC) FOR WIRELESS NETWORKS

[6] WIMEDIA LOGICAL LINK CONTROL PROTOCOL, WLP SPECIFICATION: APPROVED DRAFT 1.0, AUGUST 13, 2007

[7] ICT-OMEGA Deliverable D4.2 "Final links specification design DEMO1", February 2010, http://www.ict-omega.eu/publications/deliverables.html

8 Annex

8.1 Technical choices explanation

TDMA (Time Division Multiple Access)

We use TDMA because this is the only way to avoid collision and retransmission. Each device can reserve a time slot, and advertise the reservation in a Beacon frame, preventing other stations to use the medium during the reserved time slot. TDMA also prevents stations from using admission control mechanisms and RTS/CTS frames that consume bandwidth. Thus, all the times slots (apart from the Beacon period) can be used to send traffic.

Multi-sector transmission

We use Multi-sector transmission to be able to send data in a wider area (see Figure 5). The covered area, where equipment can send and receive data, is divided n sectors (seven in the example below). As we use TDMA, two devices cannot send data at the same time (except in full duplex mode if the two devices exchange data). If for instance, 4 equipments can connect to each other, but if two equipments exchange data in one sector and the other two equipments exchange data in another sector, they won't send data at the same time, they should use different time slots. The sectors should overlap, to allow seamless changes between sectors. For transmission, a device shall send the Beacons in n sectors with n LEDs. It shall transmit the same Beacon in each sector at the same time. For Data transmission, it's up to the implementation, to transmit the frame in one selected sector (the sector with the best received signal) or in all sectors. The choice of the method to select the best sector for transmission and reception is beyond the scope of this specification.

MAC Header protection

Why do we need to protect the MAC header with an error correction code, while the rest of the payload is not protected? Simply because we want to protect the Acknowledgement frames, to make sure that when a station receives a frame with no error, the corresponding acknowledgement sent by the station, will be correctly decoded or corrected if necessary, avoiding retransmission as much as possible. That's why the PLCP header includes the MAC header.

Data rate and adaptive data rate

The OW-MAC protocol offers various data rate. The Time slots duration have been chosen for data rates varying from 128 to 1024 Mbit/s, this is to be in accordance with the serialisation delay (See annexe 8.2). Also, the OW-MAC protocol offers an adaptive data rate to cope with medium quality changes. This Link adaptation is based on feedback information which is included in the MAC header.

8.2 Serialisation Delay example

Throughput	Serialization delay for 1600 bytes packets (12800 bits)	Serialization delay for 1100 bytes packets (8800 bits)	Serialization delay for 200 bytes packets (1600 bits)
10 mega bits/s	1,28 ms	888 µs	160 µs
100 mega bits/s	128 µs	88 µs	16 µs
1000 mega bits/s	12,8 µs	8,8 µs	1,6 µs

We can see from the above table, that the minimum value for a Time slot should be : 12,µs + a SIFS Time = 20,8 µs, as we should be able to transmit one 1600 bytes packet in one time slot at the highest data rate.

Throughput	Number of slots per second if 1600 bytes packets (12800 bits) = 1 slot	Number of slots per second if 1100 bytes packets (8800 bits) = 1 slot	Number of slots per second if 200 bytes packets (1600 bits) = 1 slot
10 mega bits/s	780	1130	6250
100 mega bits/s	7800	11300	62500
1000 mega bits/s	78000	113000	625000

8.3 64 ms Superframe Example

Number of slots per 64 ms frame	Number of 1600 bytes packets sent in one slot time (Throughput = 100 meg bits/s)	Number of 1100 bytes packets sent in one slot time (Throughput = 100 meg bits/s)	Number of 200 bytes packets sent in one slot time (Throughput = 100 meg bits/s)
16x16 = 256 TS = 250 µs	1 packet = 1 slots	1 slot = 2 packets	1 slot = 15 packets
32x32 = 1024 TS = 62,5 µs	1 packet = 4 slots	1 packet = 2 slots	1slot = 3 packets
64x64 = 4096 TS = 15,6 µs	1 packet = 16 slots	1 packet = 8 slots	1 packet = 2 slots
128x128 = 16384 TS = 3,9 µs	1 packet = 64 slots	1 packet = 32 slots	1 packet = 8 slots

Note that we want to use a power of two, for the number of time-slots in a super-frame. We can see from the above table; that the maximum number of time slots in a super-frame should be 1024 slots. With 4096 TS's in a super-frame, one TS= 15,6 µs, as a TS should be greater than 20,8 µs we cannot use 4096 TS's.

Number of slots per 64 ms frame	**Number of 1600 bytes packets sent in one slot time (Throughput = 1000 meg bits/s)**	**Number of 1100 bytes packets sent in one slot time (Throughput = 1000 meg bits/s)**	**Number of 200 bytes packets sent in one slot time (Throughput = 1000 meg bits/s)**
16x16 = 256 TS = 250 µs	1 slot = 19 packets	1 slot = 28 packets	1 slot = 156 packets
32x32 = 1024 TS = 62,5 µs	1 slot = 4 packets	1 slot = 7 packets	1slot = 39 packets
64x64 = 4096 TS = 15,6 µs	1 packet = 1 slot	1 slot = 1 packet	1 slot = 9 packets
128x128 = 16384 TS = 3,9 µs	1 packet = 4 slots	1 packet = 3 slots	1 slot = 2 packets

We can see from the above table, that at 1Gbits/s, if we use 256 a TS's super-frame, we can send 19 1600 bytes packets in one time slot, which is unlikely to happen, that's why we can't choose this value, the TS wouldn't be fully used, and we would therefore loose loads of bandwidth. AT 1Gbits/s and with 128 µs TS's we would still waste loads of bandwidth. The only value we can use for a time slot is therefore 62,5µs.

8.4 32 ms Superframe Example

Number of slots per 32 ms frame	Number of 1600 bytes packets sent in one slot time (Throughput = 100 meg bits/s)	Number of 1100 bytes packets sent in one slot time (Throughput = 100 meg bits/s)	Number of 200 bytes packets sent in one slot time (Throughput = 100 meg bits/s)
16x16 = 256 TS = 125 µs	1 packet = 2 slots	1 slot = 1 packets	1 slot = 7 packets
32x32 = 1024 TS = 31 µs	1 packet = 8 lots	1 packet = 4 slots	1 packet = 1 slot
64x64 = 4096 TS = 7,8 µs	1 packet = 32 slots	1 packet = 16 slots	1 packet = 4 slots
128x128 = 16384 TS = 1,9 µs	1 packet = 128 slots	1 packet =64 slots	1 packet = 16 slots

We can see from the above table, that if we use a 32 ms Super-frame, and 31µs TS's, at 100 Megabits/s (which is roughly the data rate used for Beacons and association frames) we can only send 400 bytes in one TS. It's not enough data for a Beacon, that's why we can't use 32 ms Super-frame, and 31µs TS's (and therefore 16 ms super-frame).

For all the previous reasons, a 64 ms super-frame and 1024 TS's, is the best solution.

Number of slots per 32 ms frame	Number of 1600 bytes packets sent in one slot time (Throughput = 1000 meg bits/s)	Number of 1100 bytes packets sent in one slot time (Throughput = 1000 meg bits/s)	Number of 200 bytes packets sent in one slot time (Throughput = 1000 meg bits/s)
16x16 = 256 TS = 125 µs	1 slot = 9 packets	1 slot = 14 packets	1 slot = 78 packets
32x32 = 1024 TS = 31 µs	1 slot = 2 packets	1 slot = 3 packets	1 slot = 19 packets
64x64 = 4096 TS = 7,8 µs	1 packet = 2 slots	1 packet = 1 slot	1 slot = 4 packets
128x128 = 16384 TS = 1,9 µs	1 packet = 7 slots	1 packet = 5 slots	1 slot = 1 packets

8.5 16 ms Superframe Example

Number of slots per 16 ms frame	**Number of 1600 bytes packets sent in one slot time (Throughput = 100 meg bits/s)**	**Number of 1100 bytes packets sent in one slot time (Throughput = 100 meg bits/s)**	**Number of 200 bytes packets sent in one slot time (Throughput = 100 meg bits/s)**
16x16 = 256 TS = 62,5 µs	1 packet = 3 slots	1 packet = 2 slots	1 slot = 4 packets
32x32 = 1024 TS = 15,6 µs	1 packet = 12 lots	1 packet = 8 slots	1 packet = 2 slots
64x64 = 4096 TS = 3,9 µs	1 packet = 48 slots	1 packet = 32 slots	1 packet =8 slots
128x128 = 16384 TS = 0,9 µs	1 packet = 192 slots	1 packet =128 slots	1 packet = 32slots

Number of slots per 16 ms frame	**Number of 1600 bytes packets sent in one slot time (Throughput = 1000 meg bits/s)**	**Number of 1100 bytes packets sent in one slot time (Throughput = 1000 meg bits/s)**	**Number of 200 bytes packets sent in one slot time (Throughput = 1000 meg bits/s)**
16x16 = 256 TS = 62,5 µs	1 slot = 4 packets	1 slot = 7 packets	1 slot = 39 packets
32x32 = 1024 TS = 15,6 µs	1 slot = 1 packets	1 slot = 1 packet	1 slot = 9 packets
64x64 = 4096 TS = 3,9 µs	1 packet = 4 slots	1 packet = 4 slots	1 slot = 2 packets
128x128 = 16384 TS = 0,9 µs	1 packet = 16 slots	1 packet = 16 slots	2 slots = 1 packets

8.6 PHY Header examples

8.6.1 VLC PHY Header example

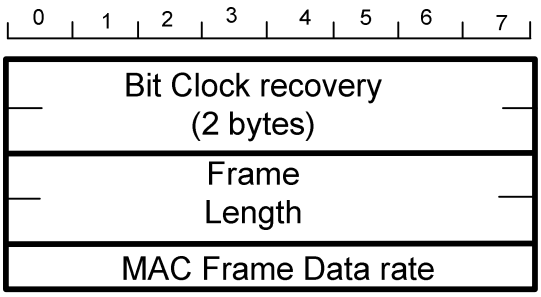


Figure 70 : VLC PHY HEADER

The PHY header is defined in Document ID4.2. Figure 70 is a VLC PHY header example, It contains 2 bytes for bit clock recovery, 2 bytes for the frame length (PLCP Header + Frame Payload + FCS) and one byte for the MAC Frame data rate.

8.6.2 IRC PHY Header example

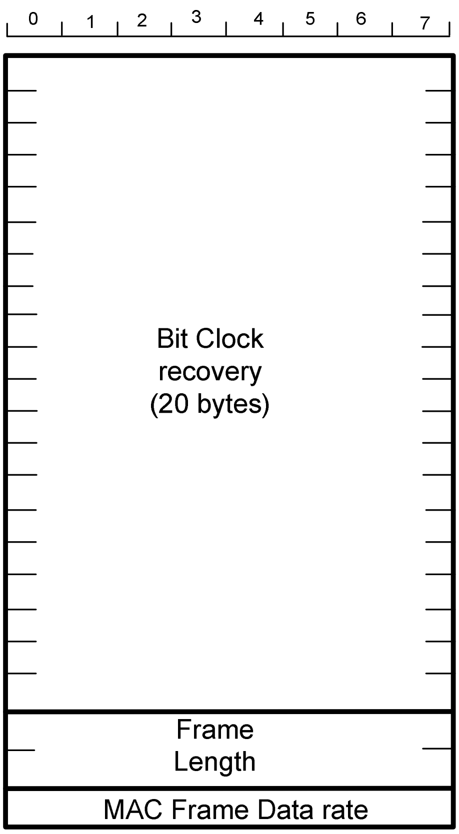


Figure 71: IRC PHY HEADER

The PHY header is defined in Document ID4.2. Figure 71 is an IRC PHY header example, It contains 20 bytes for bit clock recovery, 2 bytes for the frame length (PLCP Header + Frame Payload + FCS) and one byte for the MAC Frame data rate.