
**Information technology —
Telecommunications and information
exchange between systems — MAC and
PHY for operation in TV white space**

*Technologies de l'information — Télécommunications et échange
d'information entre systèmes — MAC et PHY pour opération en espace
blanc TV*





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	vii
Introduction.....	viii
1 Scope	1
2 Conformance	1
3 Normative references	1
4 Terms and definitions	1
5 Abbreviations and Acronyms	4
6 General description.....	7
6.1 Network components	7
6.2 Network formation	7
6.3 Protocol architecture	8
6.4 Addressing	9
6.5 PHY features	9
6.6 Overview of MAC service functionality	10
6.6.1 Logical groups	11
6.6.2 Control algorithms	11
6.6.3 Channel selection	11
6.6.4 The superframe.....	11
6.6.5 Beaconing	12
6.6.6 Medium access	13
6.6.7 Data communication between devices	13
6.6.8 MAC frame data rates.....	13
6.6.9 Security	13
6.6.10 Information discovery	14
6.6.11 Support for higher-layer timer synchronization.....	14
6.6.12 Protection of incumbent users	14
6.6.13 Self-coexistence	14
6.6.14 Rate adaptation.....	15
6.6.15 Power management.....	15
7 MAC common part sublayer.....	15
7.1 MAC Frame Format	15
7.1.1 Frame format conventions	16
7.1.2 General MAC frame format	16
7.1.3 Beacon frames	22
7.1.4 Control frames	24
7.1.5 Command frames	27
7.1.6 Data frames	35
7.1.7 Aggregated data frames	35
7.1.8 Information elements	35
7.2 Frame processing.....	63
7.2.1 Frame addresses	63
7.2.2 Frame reception.....	64
7.2.3 Frame transaction	64
7.2.4 Frame transfer	65
7.2.5 Frame retry	65
7.2.6 Inter-frame space (IFS).....	65
7.2.7 Duplicate detection	66
7.2.8 RTS/CTS use	66

7.2.9	MAC header fields.....	67
7.2.10	Information elements	69
7.3	MAC Structure and Beaconing.....	73
7.3.1	Beacon Period.....	74
7.3.2	Beacon slot state	74
7.3.3	BP length	74
7.3.4	Beacon transmission and reception.....	75
7.3.5	Beacon collision detection	76
7.3.6	BP contraction	76
7.3.7	Merger of multiple beacon groups.....	77
7.3.8	Signalling window.....	79
7.4	Device Synchronization	80
7.4.1	Clock accuracy.....	80
7.4.2	Synchronization for devices in hibernation mode	80
7.4.3	Guard times	80
7.5	Data Transfer Period	82
7.5.1	Prioritized Contention Access (PCA).....	83
7.5.2	Channel Reservation Access (CRA)	89
7.6	Fragmentation and Aggregation	96
7.6.1	Fragmentation and reassembly.....	96
7.6.2	Aggregation.....	97
7.7	ARQ, Multirate Support and Power Control	98
7.7.1	ARQ Policies	98
7.7.2	Multi-rate Support.....	100
7.7.3	Transmit Power Control	100
7.8	Dynamic Channel Selection.....	100
7.9	Power Management Mechanisms	101
7.9.1	Power management modes	101
7.9.2	Device power states	101
7.9.3	Power state transitions	101
7.9.4	Hibernation mode operation.....	103
7.9.5	Hibernation anchor operation	103
7.10	Probe	104
7.11	Protection of incumbents	104
7.11.1	Channel Measurement	104
7.11.2	Channel Classification	107
7.11.3	Channel Evacuation	108
7.12	Self-coexistence.....	109
7.12.1	Self-coexistence scenarios.....	109
7.12.2	Distributed self-coexistence mechanisms.....	109
7.12.3	Centralized self-coexistence mechanisms	110
7.13	Network Entry and Initialization	111
7.13.1	Initial Channel SCAN and Device Discovery.....	113
7.13.2	Master-Slave Association	114
7.13.3	Pair discovery	115
7.13.4	Create/join a beacon group	116
7.13.5	Pairing.....	116
7.13.6	Setup connections.....	117
7.14	MAC sublayer parameters	118
8	Security.....	120
8.1	Security mechanisms.....	120
8.1.1	Security operation	120
8.1.2	4-way handshake	121
8.1.3	Key transport.....	121
8.1.4	Freshness protection	121
8.1.5	Data encryption.....	121
8.1.6	Frame integrity protection	121
8.2	Security modes	121
8.2.1	Security mode 0	123

8.2.2	Security mode 1	123
8.2.3	Security mode 2	123
8.3	Temporal keys	123
8.3.1	Mutual authentication and PTK derivation	124
8.3.2	GTK exchange	125
8.3.3	Pseudo-random function (PRF) definition	126
8.3.4	PTK and KCK derivation	127
8.3.5	PTK MIC generation	127
8.3.6	Random number generation	128
8.4	Frame reception steps and replay prevention measures	128
8.4.1	Frame reception	128
8.4.2	Replay prevention	129
8.4.3	Implications on GTKs	129
8.5	AES-128 CCM Inputs	129
8.5.1	Overview	129
8.5.2	Nonce	130
8.5.3	CCM blocks	130
9	PHY	132
9.1	Introduction	132
9.2	Symbol description	132
9.2.1	OFDM symbol description	132
9.2.2	Symbol parameters	134
9.3	PPDU	134
9.3.1	PLCP preamble	135
9.3.2	PLCP header	137
9.3.3	PSDU	142
9.4	Constellation mapping and modulation	148
9.4.1	Data modulation	148
9.4.2	Pilot modulation	150
9.5	OFDM modulation	150
9.5.1	Data subcarriers	151
9.5.2	Pilot subcarriers	151
9.5.3	Null subcarriers	153
9.5.4	Implementation of Fourier transform	153
9.6	General block diagram for the OFDM PHY	154
9.7	General requirements	154
9.7.1	Operating frequency range	154
9.7.2	Channel bandwidth and numbering	155
9.7.3	PHY layer timing	155
9.8	Transmitter requirements	155
9.8.1	Transmit center frequency tolerance	155
9.8.2	Symbol clock frequency tolerance	155
9.8.3	Clock synchronization	155
9.8.4	Transmitter constellation error	156
9.9	Receiver requirements	157
9.9.1	Receiver sensitivity	157
9.9.2	Maximum received signal level	158
9.9.3	Center frequency and symbol clock frequency tolerance	158
9.9.4	Link quality estimate	158
9.10	Control mechanisms	159
9.10.1	Device synchronization	159
9.10.2	Transmit power control	159
9.11	Multiple antennae (optional)	160
9.11.1	Multiple antennae normal preamble and burst preamble specification	160
9.11.2	Multiple antennae PLCP header specification	161
9.11.3	Pilot subcarriers for all multiple antennae modes	163
9.11.4	Frequency interleaved transmit diversity (FITD)	163
9.11.5	Alamouti space time block coding (STBC)	163
9.11.6	Spatial multiplexing (SM) mode	164

Annex A (normative) **MUX sublayer** 165

Annex B (normative) **OFDM parameters for 7 MHz and 8 MHz channel bandwidths** 167

Annex C (normative) **Data rates for 7 MHz and 8 MHz channel bandwidths**..... 169

Annex D (normative) **MAC policies** 170

Annex E (informative) **FFT-based pilot sensing algorithms** 173

Annex F (informative) **An example of TPC algorithm** 175

Bibliography..... 178

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 16504 was prepared by Ecma International (as ECMA-392) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Introduction

Analogue broadcasting systems have been or are being upgraded to digital technology, which frees up channels in the TV frequency bands. This International Standard specifies a physical layer and a medium access sub-layer for wireless devices to operate in the TV frequency bands.

Applications include high speed video streaming and internet access on personal/portable electronics, home electronics equipment, and computers and peripherals.

Information technology — Telecommunications and information exchange between systems — MAC and PHY for operation in TV white space

1 Scope

This International Standard specifies a medium access control (MAC) sub-layer and a physical (PHY) layer for personal/portable cognitive wireless networks operating in TV bands. This International Standard also specifies a MUX sublayer for higher layer protocols.

This International Standard specifies a number of incumbent protection mechanisms which may be used to meet regulatory requirements.

2 Conformance

Conforming devices implement the MUX sub-layer, MAC sub-layer and the PHY layer as specified herein and support at least one of the device types (master, peer, or slave) and at least one of bandwidths (6 MHz, 7 MHz, 8 MHz), and may support multiple antennae modes.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10646:2003, *Information technology — Universal Multiple-Octet Coded Character Set (UCS)*

ISO/IEC 18033-3:2005, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

4.1

alien beacon group

group of devices for which the beacon period (BP) is not aligned with the BP of the current device

4.2

alien device

member of an alien beacon group

- 4.3**
Access Category
AC
common set of prioritized contention access (PCA) parameters to contend for the medium to transmit MAC protocol data units (MPDUs) with certain priorities
- 4.4**
beacon group
BG
set of devices that share the same beacon period start time (BPST)
- 4.5**
beacon period
BP
time during which a device sends or listens for beacons
- 4.6**
beacon period start time
BPST
start of the beacon period
- 4.7**
channel reservation protocol
CRP
protocol to support negotiation and maintenance of channel time reservations
- 4.8**
contention signalling window
time window for exchanging control or management information in the slotted aloha based manner
- 4.9**
data integrity
assurance that the data has not been modified from its original form
- 4.10**
data transfer period
DTP
time period within a superframe used mainly for data transfer via prioritized contention access (PCA) or in reservations established using the channel reservation protocol (CRP)
- 4.11**
device
entity conforming to this International Standard
- 4.12**
extended beacon group
union of a device's beacon group and the beacon groups of all devices in the device's beacon group
- 4.13**
incumbents
regulatory protected transmission systems operating in the TV bands
- 4.14**
incumbent protection mechanisms
mechanisms including DFS, TPC, geo-location/database access, and spectrum sensing
- 4.15**
MPDU
MAC PDU

4.16**MSDU**

MAC SDU

4.17**master****master device**

device acting as a centralized coordinator of medium access on behalf of at least one slave device

4.18**master-slave group**

group of devices with a master device and its slave devices

4.19**message integrity code****MIC**

cryptographic checksum generated using a symmetric key

NOTE A MIC is typically appended to data for data integrity and source authentication similar to a digital signature.

4.20**neighbour**

member of a beacon group

4.21**network allocation vector****NAV**

remaining time a neighbour device has indicated it will access the medium

4.22**outband channel**

channel other than the one being used for data transmission

4.23**peer****peer device**

device coordinating medium access with other devices without a centralized coordinator

4.24**peer-to-peer group**

group of peer devices

4.25**prioritized contention access****PCA**

prioritized CSMA/CA access mechanism

4.26**proxy**

peer device that coordinates outband channel measurement

4.27**quiet period**

time period scheduled to detect incumbents

4.28**reservation**

one or more medium access slots (MASs) within a superframe during which a device has preferential access to the medium

4.29

reservation signalling window

time window used for exchanging control or management information in the reservation based manner

4.30

slave

slave device

device associated with and coordinated by a master device for medium access

4.31

stream

logical flow of MSDUs from one device to one or more other devices

4.32

superframe

periodic time interval to coordinate frame transmissions between devices

4.33

transmission opportunity

TXOP

time interval for prioritized contention access (PCA) to initiate transmissions

4.34

TXOP holder

device that has successfully contended for a TXOP

5 Abbreviations and Acronyms

AC	access category
ACK	acknowledgment
A/D	analog-to-digital
AES	advanced encryption standard
AGC	automatic gain control
AIFS	arbitration inter-frame space
ASIE	application-specific information element
AWGN	additive white Gaussian noise
BPOIE	beacon period occupancy information element
BPSK	binary phase-shift keying
BcstAddr	broadcast device address
BP	beacon period
BPST	beacon period start time
B-ACK	block acknowledgment
BW	bandwidth
CBC-MAC	cipher block chaining-message authentication code
CCA	clear channel assessment
CCM	counter mode encryption and cipher block chaining message authentication code
CE	channel estimation
CINR	carrier-to-interference and noise ratio

CP	cyclic prefix
CRC	cyclic redundancy check
CRP	channel reservation protocol
CSMA/CA	carrier sense multiple access with collision avoidance
CTS	clear to send
D/A	digital-to-analog
DC	direct current
DestAddr	destination device address
DevAddr	device address
DME	device management entity
DTP	Data transfer period
EO	encryption offset
EUI	extended unique identifier
FCS	frame check sequence
FEC	forward error correction
FFT	fast Fourier transform
FITD	frequency interleaved transmit diversity
GF	Galois field
GTK	group temporal key
HDR	header
HEI	header error indicator
I	inphase
ICI	inter-carrier interference
ID	identifier
IE	information element
IFFT	inverse FFT
IFS	inter-frame space
Imm-ACK	immediate acknowledgment
ISI	inter-symbol interference
KCK	key confirmation key
LQE	link quality estimate
LSB	least significant bit
M2S	Master-to-Slave
MAC	medium access control
MAS	medium access slot
MCDU	MAC command data unit
McstAddr	multicast device address
MIB	management information base
MIC	message integrity code
MIFS	minimum inter-frame space

MKID	master key identifier
MLME	MAC sublayer management entity
MPDU	MAC protocol data unit
MSB	most significant bit
MSDU	MAC service data unit
NAV	network allocation vector
No-ACK	no acknowledgement
OFDM	orthogonal frequency division multiplexing
OUI	organizationally unique identifier
P2P	Peer-to-Peer
PCA	prioritized contention access
PER	packet error rate
PHY	physical layer
PLCP	physical layer convergence protocol
PLME	physical layer management entity
PMK	pair-wise master key
PPDU	PHY protocol data unit
ppm	parts per million
PRBS	pseudo-random binary sequence
PRF	pseudo-random function
PSDU	PHY service data unit
PTK	pair-wise temporal key
Q	quadrature
QAM	quadrature amplitude modulation
QP	quiet period
QPSK	quadrature phase-shift keying
RF	radio frequency
RMS	root mean square
RS	Reed-Solomon
RSSI	received signal strength indication
RTG	receive-to-transmit transition gap
RTS	request to send
SAP	service access point
SFC	secure frame counter
SFN	secure frame number
SIFS	short inter-frame space
SM	spatial multiplexing
SNR	signal-to-noise ratio
SrcAddr	source device address
STBC	space time block code

TKID	temporal key identifier
TPC	transmit power control
TTG	transmit-to-receive transition gap
TV	television
TXOP	transmission opportunity
UCA	unused CRP reservation announcement
UCR	unused CRP reservation response
UHF	ultra high frequency
VHF	very high frequency
WM	wireless microphone

6 General description

6.1 Network components

A basic component of a network is a device. Two or more devices communicating on the same physical channel constitute a network. There are three types of devices, master device, slave device, and peer device. The device type of a device is preconfigured. The autonomous transition of device type is not supported in this International Standard, although the device type may be reconfigurable by DME which is out of scope of this International Standard.

6.2 Network formation

A basic network operates in one of two basic network formation modes: the master-slave mode or the peer-to-peer mode. Both are shown in Figure 1. In the master-slave mode, a device is designated as master and others are associated with the master as slaves. The master coordinates channel access in the master-slave mode. Communication is normally established between slave devices and the master device. A slave device may also directly communicate with another slave device under the coordination of the master.

A peer-to-peer network differs from a master-slave based network mainly in that devices can form a network in the peer-to-peer way and coordinate channel access with distributed beaconing and channel reservation. A peer-to-peer network comprises of peer devices. A peer device is able to access channel via distributed reservation and directly communicate with any other peer device as long as they are in range of one another. In other words, a peer-to-peer network can be ad hoc, self-organizing, and self-healing.

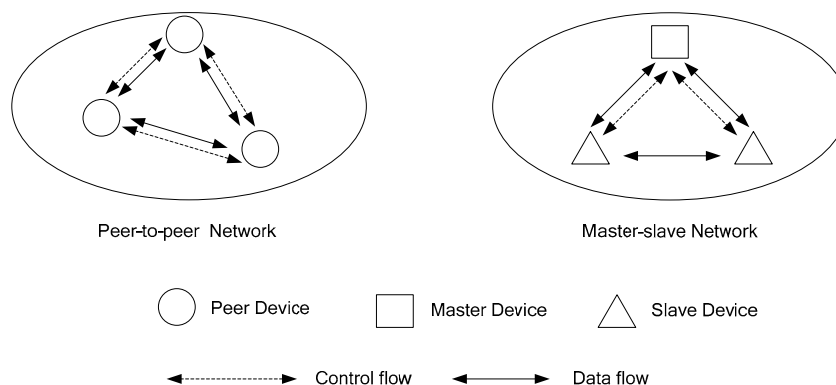


Figure 1 — Basic Network Formation

Two or more networks can share the same channel and may also communicate with each other in a coordinated way.

A number of networks may also form a large-scale network such as a mesh network or a cluster tree network. It allows multiple hops to route messages from any device to any other device in the network. Such functions can be added at the higher layer, but are not part of this International Standard.

6.3 Protocol architecture

This International Standard specifies a PHY layer and a MAC sublayer. As shown in Figure 2, the PHY layer and the MAC sublayer correspond to the PHY layer and the MAC sublayer of the OSI basic reference model [5] respectively. In this International Standard the MAC entity is represented by a device address.

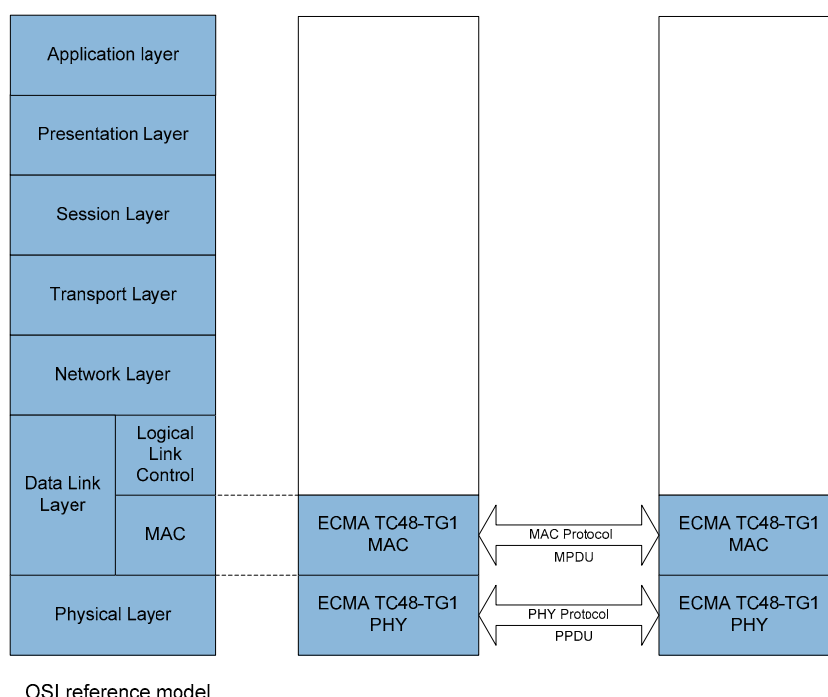


Figure 2 — Architectural reference model

Service access points (SAPs) interaction with PHY and MAC sublayers are illustrated in Figure 3. As a reference, 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. 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.” 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 3 depicts the relationship among the management entities. The specification of SAPs and management entities, as shaded parts of Figure 3, is out of the scope of this International Standard.

In order to enable the coexistence of concurrently active higher layer protocols within a single device, a MUX sublayer is specified. This sublayer routes outgoing and incoming MSDUs to and from their corresponding higher layers. The MUX sublayer is described in Annex A.

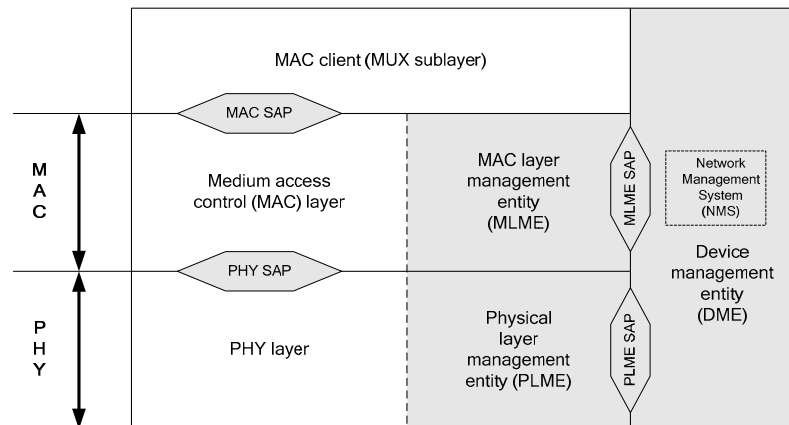


Figure 3 — The reference model for this International Standard

6.4 Addressing

Individual MAC entities are addressed via an EUI-48 [1], and are associated with a volatile abbreviated address called a DevAddr. MAC address is included in beacon and/or control messages for global identification.

Data frames normally use abbreviated DevAddr that identifies a single MAC entity for reducing overhead. DevAddrs are 16-bit values, generated locally within the device. Consequently, it is possible for a single value to ambiguously identify two or more MAC entities. This International Standard provides mechanisms for resolving ambiguous DevAddrs.

The MAC addressing scheme includes multicast and broadcast address values. A multicast address identifies a group of MAC entities. The broadcast address identifies all MAC entities.

Device name string may be used for helping user to identify a device, as specified in 7.1.8.16. Device name string can be assigned and changed by DME. Device name string should be included in beacons for assisting device discovery.

A stream ID may be determined locally by device to identify stream originating from itself.

6.5 PHY features

A MAC entity is associated with a single PHY entity.

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

- Frame transmission for both normal and burst modes;
- Frame reception for both normal and burst modes;
- Header error indication for PHY and MAC header;
- Clear channel assessment for estimation of medium activity.

Figure 4 shows the structure of a PHY frame.

- There are two types of preamble: normal and burst.
- The PLCP header including MAC and PHY Headers is protected by RS parity.
- The Frame Payload is followed by its frame check sequence (FCS).

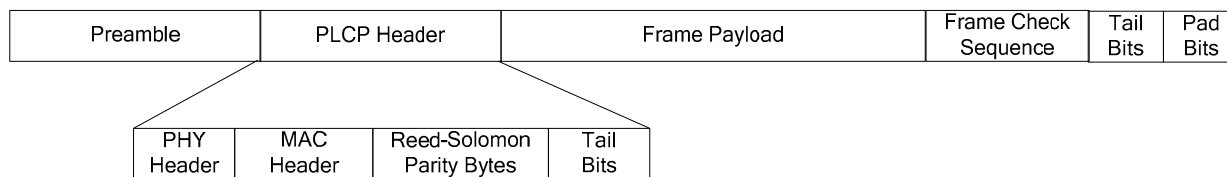


Figure 4 — PHY Frame Structure

Frames are transmitted by the PHY from the source device and delivered to the destination device in identical bit order. Throughout this specification reference to the start of a frame refers to the leading edge of the first symbol of the PHY frame at the local antenna and end of a frame refers to the trailing edge of the last symbol of the PHY frame.

Frame transmission and reception are supported by the exchange of parameters between the MAC sublayer and the PHY layer. These parameters allow the MAC entity to control, and be informed of, the frame transmission mode, the frame payload data rate and length, the frame preamble, the PHY channel and other PHY-related parameters.

In normal mode transmission, the MAC entity has full control of frame timing. In burst mode transmission, the MAC entity has control of the first frame timing and the PHY provides accurate timing for the remaining frames in the burst.

6.6 Overview of MAC service functionality

The MAC service specified in this International Standard provides:

- Communication between devices within radio range on a single channel using the PHY;
- A reservation-based channel access mechanism;
- A prioritized, contention-based channel access mechanism;
- A synchronization facility for coordinated applications;
- Mechanisms for protection of incumbent user;
- Master-slave operation;
- Peer-to-peer operation;
- Mechanisms for handling mobility and interference situations;
- Device power management by scheduling of frame transmission and reception;
- Secure communication with data authentication and encryption using cryptographic algorithms.

The architecture of this MAC service is either master-coordinated or fully distributed. A device provides required MAC functions and optional functions according to its device type.

Coordination of devices within radio range is achieved by the exchange of beacon frames and/or command 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.

6.6.1 Logical groups

The MAC protocol is specified with respect to an individual device, which has its own individual neighbourhood. All MAC protocol facilities are expressed with respect to this individual neighbourhood.

In a peer-to-peer network formed with fully distributed medium access coordination, logical groups are formed around each device to facilitate contention-free frame exchanges while exploring medium reuse over different spatial regions. In this International Standard, these logical groups are a beacon group and an extended beacon group, both of which are determined with respect to an individual device.

In a master-slave based network formed under the coordination of a master, logical groups are formed with master-slave operation to facilitate contention-free frame exchanges. A master must be a beaconing device. A slave device could be either a beaconing device or nonbeaconing device.

6.6.2 Control algorithms

MAC protocol algorithms attempt to ensure that no member of the extended beacon group transmits a beacon frame at the same time as the device. Information included in beacon frames facilitates contention-free frame exchanges by ensuring that a device does not transmit frames while a neighbour is transmitting or receiving frames.

To permit correct frame reception, MAC protocol algorithms attempt to ensure that a device's DevAddr is unique within the device's extended beacon group.

6.6.3 Channel selection

A device chooses a channel without incumbent presence. If no beacon is detected in the selected channel and no incumbent user is found, a master device or a peer device creates its beacon period (BP) by sending a beacon. If one or more beacons are detected in the selected channel, the device synchronizes its BP to existing beacons in the selected channel. The device exchanges data with members of its beacon group using the same channel the device selected for beacons.

When a slave device is enabled, it scans one or more channels for master beacon. A slave device selects the channel used by its intended master.

Each device operates in a dynamic environment and under unlicensed operation rules. Thus, it is subject to interference from licensed users, other networks, and other unlicensed wireless entities in its channel. To enable the device to continue operation in this type of environment, each device has the capability to dynamically change the channel in which it operates.

If at any time a device determines that the current channel is unsuitable, it uses the dynamic channel selection procedure, as described in 7.8, to move to a new channel.

6.6.4 The superframe

The basic timing structure for frame exchange is a superframe. The superframe duration is specified as mSuperframeLength. The superframe is composed of 256 medium access slots (MASs), where each MAS duration is mMASLength.

Each superframe starts with a BP, which extends over one or more contiguous MASs. The start of the first MAS in the BP, and the superframe, is called the beacon period start time (BPST).

A recurring superframe consists of a beacon period (BP), data transfer period (DTP) and a contention signalling window (CSW). A reservation based signalling window (RSW) could be appended right after BP to support signal exchange between a master and slave devices in the master-slave mode. RSW is not needed for a peer-to-peer network. The signalling windows and beacon period are used for sending and receiving control/management information.

The BP length is adjustable and depends on how many regular beaconing devices participate in the same BP. In the master-slave mode, BP length can be kept as minimum as 1 beacon slot if the master is the only device that does regular beaconing. In the peer-to-peer mode, the number of beacon slots can be as many as the number of peer devices. The beaconing policy is specified in 6.6.5.

All devices which share the same channel shall follow the same superframe structure. Superframe merging is necessary if two networks follow different superframe structures and share the same channel.

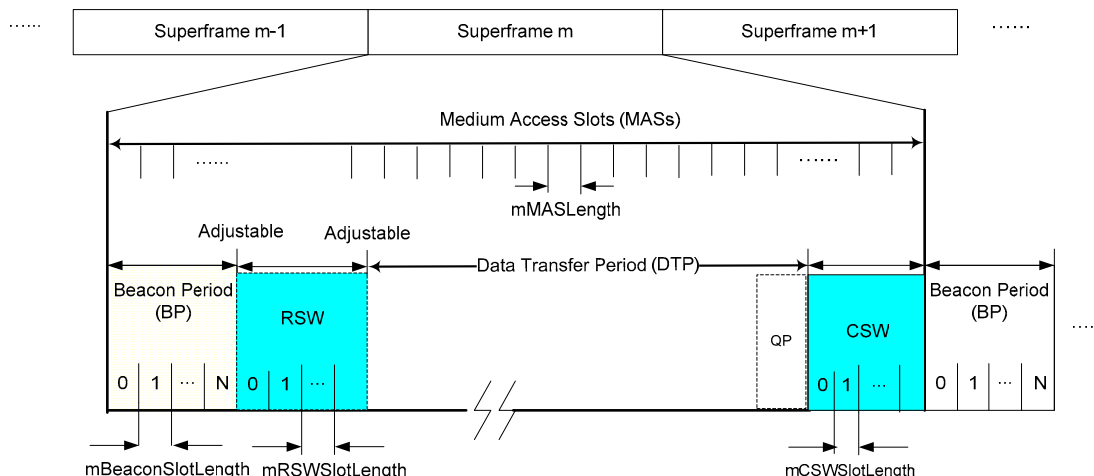


Figure 5 — MAC superframe structure

6.6.5 Beacons

A device is defined as a beaconing device if it owns a beacon slot in BP and regularly transmits beacons. A peer device or a master device is by default a beaconing device. A slave device is normally a non-beaconing device unless promoted to be a beaconing device. All slave devices must be capable to transmit regular beacons, if the master device so decides.

All the devices shall keep awake during beacon period and CSW in order to capture all the control/management information which might be relevant to every device. A device may exchange data, monitor channel status, or go to sleep mode during data transfer period (DTP).

A beacon packet contains the following important information for network operation, but not limited to:

- Device identification information
 - Important for device discovery and self-coexistence
- Beacon slot occupation information
- Medium reservation information
 - Necessary for QoS provisioning
- TIM (Traffic indication map)
- Quiet period schedule
 - Necessary for in-service channel monitoring (sensing)
- Channel Measurement Report
- Channel classification and change information.

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.

A device should protect an alien BP, detected by reception of a beacon frame unaligned with the device's own BP, by announcing a reservation covering the alien BP in its beacon.

6.6.6 Medium access

The medium is accessed in one of three ways:

- During the BP, devices send only beacon frames, according to the rules specified in 7.3.
- During reservations, devices participating in the reservation send frames according to rules specified in 7.5.2.
- During quiet period, all devices keep silent.
- Outside the BP and reservations, devices may send frames using a prioritized contention-based access method, as described in 7.5.1.

6.6.7 Data communication between devices

Data is passed between the MAC entity and its client in MSDUs qualified by certain parameters. 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, as described in 7.6.1. 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, as described in 7.7.1. This International Standard provides for three types of acknowledgements to enable different applications. The No-ACK policy, described in 7.7.1.1, is appropriate for frames that do not require guaranteed delivery, or are delay sensitive and a retransmitted frame would arrive too late. The Imm-ACK policy, described in 7.7.1.2, provides an acknowledgement process in which each frame is individually acknowledged following the reception of the frame. The B-ACK policy, described in 7.7.1.3, 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 B-ACK process decreases the overhead of the Imm-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, as described in 7.5.1.7 and 7.5.2.9, 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.

6.6.8 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 pBeaconTransmitRate, 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. MAC headers are always transmitted at the most robust data rate supported by the PHY.

6.6.9 Security

Wireless networks present unique security challenges due to the loss of protection provided by wires and shielding. Personal/portable wireless networks present additional challenges due to the wide range of applications and use models that they must support. To name a few, eavesdroppers can overhear data exchanges not intended for them, whereas imposters can send forged data not using its own identity, can replay previously transmitted data, and can transmit modified data captured from a previous transmission.

This International Standard specifies two levels of security: no security and strong security protection. Security protection includes data encryption, message integrity, and replay attack protection. Secure frames are used to provide security protection to data and aggregated data frames as well as selected control and command frames.

Three security modes are defined to control the level of security for devices in their communications. This International Standard allows for a device to use one of the two security levels or a combination of them in communicating with other devices by selecting the appropriate security mode.

This International Standard further specifies a 4-way handshake mechanism to enable two devices to derive their pair-wise temporal keys (PTKs) while authenticating their identity to each other. A secure relationship is established following a successful 4-way handshake between two devices. A 4-way handshake between two devices is conducted based on a shared master key. How two devices obtain their shared master keys is outside the scope of this International Standard.

In addition, this International Standard provides means for the solicitation and distribution of group temporal keys (GTKs). While PTKs are used for protecting unicast frames exchanged between two devices, GTKs are employed for protecting multicast and broadcast frames transmitted from a source device to a multicast or broadcast group of recipient devices.

A pseudo-random function is defined based on the MIC generation by CCM using AES-128.

Secure frame counters and replay counters are set up on a per-temporal key basis to guarantee message freshness. No specific mechanisms are created in this International Standard to address denial of service attacks given the open nature of the wireless medium.

In this International Standard, 128-bit symmetric temporal keys are employed based on AES-128 with CCM to provide payload encryption and message integrity code (MIC) generation.

In general, this International Standard specifies security mechanisms, not security policies.

6.6.10 Information discovery

The protocols and facilities of this International Standard are supported by the exchange of information between devices. Information may be broadcasted in beacon frames or requested in Probe commands. For each type of information, an Information Element (IE) is defined. IEs may 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.

6.6.11 Support for higher-layer timer synchronization

Some applications, for example, the transport and rendering of audio or video streams, require synchronization of timers located at different devices. Greater accuracy (in terms of jitter bounds) or finer timer granularity than that provided by the synchronization mechanism described in 7.4.

6.6.12 Protection of incumbent users

This International Standard provides protocols for detecting incumbent users, protecting incumbent users and enabling seamless device operation, which include coordinated channel measurement, channel management, and TPC as specified in 7.7.3, 7.8 and 7.11.

6.6.13 Self-coexistence

This International Standard provides self-coexistence protocol and mechanisms in 7.12 that allow neighbouring networks to share the same channel in the coordinated manner if desired. A master-slave based

network can share the same channel with another co-located master-slave network or peer-to-peer network. Similarly, a peer-to-peer network can share the same channel with another peer-to-peer network or master-slave network.

6.6.14 Rate adaptation

A mechanism for data rate adaptation is provided in 7.7.2. A receiver may use this mechanism to inform a transmitter of the optimal data rate to increase throughput and/or reduce the frame error rate (FER).

6.6.15 Power management

A complementary goal of this International Standard is to enable long operation time for battery powered devices. An effective method to extend battery life is to enable devices to turn off completely or reduce power for long periods of time, where a long period is relative to the superframe duration.

This International Standard provides two power management modes in which a device can operate: active and hibernation. Devices in active mode transmit and receive beacons in every superframe. Devices in hibernation mode hibernate for multiple superframes and do not transmit or receive in those superframes.

In addition, this International Standard provides facilities to support devices that sleep for portions of each superframe in order to save power.

To coordinate with neighbours, a device indicates its intention to hibernate by including a Hibernation Mode IE in its beacon. The Hibernation Mode IE specifies the number of superframes in which the device will sleep and will not send or receive beacons or any other frames.

Power management mechanisms are described in 7.9.

7 MAC common part sublayer

This clause specifies the format of MAC frames and MAC sublayer functionality.

The format of MAC frame which includes descriptions of common fields, each frame type and subtype, and information elements is specified in 7.1.

The rules for transmission and reception of MAC frames, including setting and processing MAC header fields and information elements, are specified in 7.2. The MAC superframe structure and beaconing policies are specified in 7.3.

During the data period devices send and receive data using prioritized contention access (PCA) or in reservations established using the channel reservation protocol (CRP), specified in 7.5. PCA permits multiple devices to contend for access to the medium based on traffic priority, and is specified in 7.5.1. The CRP enables a device to gain scheduled access to the medium within a negotiated reservation, and is specified in 7.5.2.

Device synchronization is specified in 7.4. The fragmentation and aggregation of MSDUs is specified in 7.6. 7.7 through 7.10 specify ARQ, probe commands, dynamic channel selection, multi-rate support, transmit power control, power management mechanisms. 7.11 specifies incumbent protections. 7.12 specifies self-coexistence. 7.13 specifies network entry and initialization. 7.14 specifies values for all MAC sublayer parameters.

7.1 MAC Frame Format

This Clause specifies the format of MAC frames. An overview of the MAC frame with descriptions of common fields is followed by Clauses for each frame type and subtype.

7.1.1 Frame format conventions

The following conventions and definitions apply throughout this clause.

7.1.1.1 Figures and Tables

MAC frames are described as a sequence of fields in a specific order. Tables in clause 7 depict fields in the order they are delivered to the PHY SAP from top to bottom, where the top-most field is transmitted first in time, as illustrated in Table 1. In field tables, bits within the field are numbered from the least-significant bit on the top to the most-significant bit on the bottom, as illustrated in Table 2.

Table 1 — Example sequence of fields

Syntax	Size	Notes
Example_MAC_frame_Format {		
First field	2 bytes	First transmitted
Second field	2 bytes	Second transmitted
...	...	...
Last field	2 bytes	Last transmitted
}		

Table 2 — Example bitmap of a field

Syntax	Size	Notes
Example_Field_Format {		
Protocol Version	2 bits	Least significant bits, b1-b0
Secure	1 bit	
ACK Policy	2 bits	
Frame Type	3 bits	
Frame Subtype/Delivery ID	4 bits	
Retry	1 bit	
Reserved	3 bits	Most significant bits, b15-b13
}		

7.1.1.2 Octet order

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.

7.1.1.3 Encoding

Values specified in decimal are encoded in unsigned binary unless otherwise stated.

A bitmap is a sequence of bits, labeled as bit[0] through bit[N-1]. A bitmap is encoded in a field such that bit[0] corresponds to the least-significant bit of the field and subsequent bitmap elements correspond to subsequent significant bits of the field. Octets of the field are presented to the PHY SAP in order from least-significant octet to most-significant octet.

Reserved fields and subfields are set to ZERO on transmission and ignored on reception.

7.1.2 General MAC frame format

A MAC frame consists of a fixed-length MAC Header and an optional variable-length MAC Frame Body. The MAC Header is specified in Table 3.

Table 3 — MAC header format

Syntax	Size	Notes
MAC_Header_Format {		
Frame Control	16 bits	Refer to 7.1.2.1
DestAddr	16 bits	Destination Address
SrcAddr	16 bits	Source Address
Sequence Control	16 bits	The Sequence Control field identifies the order of MSDUs/MCDUs and their fragments; refer to 7.1.2.4
Access Control	16 bits	Access method, duration, and more frames flag; refer to 7.1.2.5
}		

The MAC frame body, when present, contains a Frame Payload and Frame Check Sequence (FCS) as shown in Table 4.

Table 4 — MAC frame body format

Syntax	Size	Notes
MAC_Frame_Body_Format {		
Frame Payload	<i>variable</i>	Refer to 7.1.2.6
FCS	32 bits	Refer to 7.1.2.7
}		

The Frame Payload length ranges from zero to mMaxFramePayloadSize. 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. In secure frames, the Frame Payload includes security fields, as specified in Table 5.

Table 5 — Frame Payload field format for secure frames

Syntax	Size	Notes
Secure_Frame_Payload_Field_Format {		
Temporal Identifier (TKID)	24 bits	Refer to 7.1.2.6.1
Secure Payload	<i>variable</i>	Refer to 7.1.2.6.2
Message Integrity Code (MIC)	64 bits	Refer to 7.1.2.6.3
}		

7.1.2.1 Frame Control

The Frame Control field is specified in Table 6.

Table 6 — Frame Control field format

Syntax	Size	Notes
Frame_Control_Field_Format {		
Protocol Version	2 bits	Refer to 7.1.2.1.1
Secure	1 bit	Refer to 7.1.2.1.2
ACK Policy	2 bits	Refer to 7.1.2.1.3
Frame Type	3 bits	Refer to 7.1.2.1.4
Frame Subtype/Delivery ID	4 bits	Refer to 7.1.2.1.5
Retry	1 bit	Refer to 7.1.2.1.6
Reserved	3 bits	
}		

7.1.2.1.1 Protocol Version

The Protocol Version field is invariant in size and placement across all revisions of this International Standard. For this revision of the standard, the Protocol Version is set to zero. All other values are reserved.

7.1.2.1.2 Secure

The Secure bit is set to ONE in a secure frame, ZERO otherwise. Frames with the Secure bit set to ONE use the Frame Payload format for secure frames as specified in Table 5.

7.1.2.1.3 ACK Policy

The ACK Policy field is specified in Table 7.

Table 7 — ACK Policy field encoding

Value	ACK policy type	Description
0	No-ACK	The recipient(s) do not acknowledge the transmission, and the sender treats the transmission as successful without retransmission. The use of this policy is specified in 7.7.1.1.
1	Imm-ACK	The addressed recipient returns an Imm-ACK frame after correct reception, according to the procedures specified in 7.7.1.2.
2	B-ACK	The addressed recipient keeps track of the frames received with this policy until requested to respond with a B-ACK frame, according to the procedures specified in 7.7.1.3.
3	B-ACK Request	The addressed recipient returns a B-ACK frame after reception, according to the procedures specified in 7.7.1.3.

7.1.2.1.4 Frame Type

The Frame Type field is specified in Table 8.

Table 8 — Frame Type field encoding

Value	Frame type	Subclause
0	Beacon frame	Refer to 7.1.3
1	Control frame	Refer to 7.1.4
2	Command frame	Refer to 7.1.5
3	Data frame	Refer to 7.1.6
4	Aggregated data frame	Refer to 7.1.7
5-7	Reserved	

7.1.2.1.5 Frame Subtype/ Delivery ID

The Frame Subtype / Delivery ID field is used to assist a receiver in the proper processing of received frames. In beacon, control or command frames, this field is used as Frame Subtype, as specified in Table 14, Table 21 and Table 25, respectively. In data frames and aggregated data frames, this field is used as Delivery ID as specified in Table 9.

Table 9 — Delivery ID encoding in Frame Control

Bit b12	Bits b11-b9
0	User Priority
1	Stream Index

This field is reserved in all other frame types.

7.1.2.1.6 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 for all other frame types.

7.1.2.2 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.

7.1.2.3 SrcAddr

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

7.1.2.4 Sequence Control

Table 10 — Sequence Control field format

Syntax	Size	Notes
Sequence_Control_Field_Format {		
Fragment Number	3 bits	Refer to 7.1.2.4.1
Sequence Number	11 bits	Refer to 7.1.2.4.3
More Fragments	1 bit	Refer to 7.1.2.4.2
Reserved	1 bit	
}		

The Sequence Control field identifies the order of MSDUs/MCDUs and their fragments. The Sequence Control field is specified in Table 10. The Sequence Control field is reserved in control frames.

7.1.2.4.1 Fragment Number

The Fragment Number field is set to the number of the fragment within the MSDU or MCDU. The fragment number is set zero if the current fragment is the first fragment of an MSDU or MCDU, or if there is no fragmentation applied in the MSDU or MCDU. The fragment number is incremented by one for each successive fragment of that MSDU or MCDU.

7.1.2.4.2 More Fragments

The More Fragments field is set to ZERO if the current fragment is the final fragment of the current MSDU or MCDU, or if there is no fragmentation applied in the MSDU or MCDU. Otherwise, the field is set to ONE.

7.1.2.4.3 Sequence Number

The sequence number is derived from a modulo 2048 counter.

If frame type is beacon frame, the sequence number represents the current superframe number. Superframe number is set zero if the current superframe is the first superframe for the beacon group. The superframe number is incremented by one for each successive superframe. A device shall use a dedicated counter for beacon frame. In addition, all the devices in the same beacon group shall use the same superframe number.

If frame type is command frame, the Sequence Number is set to the sequence number of the MCDU. A device shall increment the sequence number by one for each transmitted MCDU. A device shall use a dedicated counter for MCDUs.

The Sequence Number field for MSDU and MCDU is specified in 7.2.9.3.

The Sequence Number field is reserved in control frames.

The Sequence Number field is used for duplicate frame detection, as described in 7.2.7, and to preserve frame order when using the B-ACK mechanism, as described in 7.7.1.3.

7.1.2.5 Access Control

The Access Control field is specified in Table 11.

Table 11 — Access Control field encoding

Syntax	Size	Notes
Access_Control_Field_Format {		
Duration	14 bits	Refer to 7.1.2.5.1
More frames	1 bit	Refer to 7.1.2.5.2
Access method	1 bit	Refer to 7.1.2.5.3
}		

7.1.2.5.1 Duration

The Duration field is 14 bits in length and is set to an expected medium busy interval after the end of the PLCP header of the current frame. The unit of duration is 4 microseconds. The duration value is set as specified in 7.2.9.1 and used to update the network allocation vector (NAV) according to the procedures specified in 7.5.1.2.

7.1.2.5.2 More frames

In frames sent with the Access Method bit set to ONE, the More Frames bit is set to ZERO if the transmitter will not send further frames to the same recipient during the current reservation block; otherwise it is set to ONE.

In frames sent with the Access Method bit set to ZERO, 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. Additional rules regarding the More Frames field are specified in 7.2.9.2.

7.1.2.5.3 Access method

The Access Method bit shall be set to ONE in all frames transmitted within a hard or private CRP reservation block by the reservation owner or target prior to the release of the reservation block, including the UCA and UCR control frames that release the reservation block.

The Access Method bit may be set to ONE in frames transmitted within a Soft CRP reservation block without backoff by the reservation owner.

The Access Method bit in an Imm-ACK, B-ACK or CTS control frame is set to the same value as the Access Method bit in the corresponding received frame.

The Access Method bit is set to ZERO in frames transmitted at all other times, other than in beacon frames.

The Access Method bit is reserved in beacon frames.

7.1.2.6 Frame Payload

The Frame Payload field is a variable length field that carries the information. In a secure frame, it includes the required security fields as shown in Table 5 and specified below.

7.1.2.6.1 Temporal Key Identifier (TKID)

The TKID field is an identifier for the temporal key used to protect the frame. The TKID uniquely identifies this key from any other temporal keys held by the sender and the recipient(s) of the frame. It does not need to uniquely identify the key for devices not holding the key.

7.1.2.6.2 Secure Payload

The Secure Payload field in the secure frames is the counterpart of the Frame Payload field in non-secure frames. It contains the information specific to individual frame types and protected by the symmetric key identified in the TKID field of the same frame.

7.1.2.6.3 Message Integrity Code (MIC)

The MIC field contains an 8-octet cryptographic checksum used to protect the integrity of the MAC Header and Frame Payload.

7.1.2.7 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:

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

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

- The remainder resulting from $x^k \times (x^{31} + x^{30} + \dots + x + 1)$ 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. Table 12 specifies the encoding of the FCS field for the CRC polynomial:

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

Table 12 — FCS field encoding

bits: b_{31}	b_{30}	b_{29}	...	b_2	b_1	b_0
a_0	a_1	a_2	...	a_{29}	a_{30}	a_{31}

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:

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

7.1.3 Beacon frames

MAC Header field settings for beacon frames are described in Table 13. Beacon frames are also referred to as beacons throughout this specification.

Table 13 — MAC header field values for beacon frames

MAC header field	Value
Protocol version	0
Secure	0
ACK Policy	0 (No-ACK)
Frame Type	0 (beacon frame)
Frame Subtype	As specified in Table 14
Retry	Reserved
DestAddr	BcstAddr
SrcAddr	DevAddr of the transmitter
Sequence Control	As specified in 7.1.2.4 and 7.2.9.3. The sequence number contained in sequence control represents the superframe number
Duration	As specified in 7.1.2.5.1 and 7.2.9.1
More Frames	Reserved
Access Method	Reserved

Frame subtype specified in Table 14 indicates four beacon types: regular, signalling, echo beacon.

Table 14 — Frame subtype for beacon frames

Value	Beacon frame subtype	Description
0	Regular	Regular beaconing
1	Signalling	Signalling beacon for network entry
2	Echo	Help coverage extension or coexistence operation during master/slave mode
3 – 15	Reserved	Reserved

As specified in 7.1.2.4, the sequence number contained in sequence control represents the superframe number. The superframe number increments once per superframe, following a modulo counter. The device first establishing beacon group initializes the superframe number. Each device includes the superframe number in its beacon frame. Through beacon, a device knows the superframe number of its neighbours. Each device shall align its superframe number to the largest superframe number it observes in the beacon group. Therefore, all the devices in a network can quickly converge to the same superframe number even in the multi-hop case.

7.1.3.1 Regular beacon frame

The beacon frame payload is specified in Table 15.

Table 15 — Regular Beacon frame payload format

Syntax	Size	Notes
Regular_Beacon_Frame_Payload_Format {		
Device Identifier	6 bytes	
Beacon Slot Descriptor	1 byte	Refer to Table 16
Device type	1 byte	Refer to Table 17
For(i=1, i<=N, i++){		
IE _i	<i>variable</i>	Information element, as specified in 7.1.8
}		
}		

The information elements (IEs) are listed in Table 45 in 7.1.8. IEs are included in order of increasing Element ID. CRP IEs that have the same Target DevAddr and Stream Index are adjacent to each other in the beacon. Each beacon frame shall include at least the following IEs: BPOIE, CRP Availability IE, and Regular QP schedule IE.

The Device Identifier field is set to the EUI-48 [1] of the device sending the beacon.

The Beacon Slot Descriptor field format is specified in Table 16.

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, mMaxBPLength-1].

The Movable bit is set to one if the beacon is movable according to 7.3.6 and is set to ZERO otherwise.

Device type is specified in Table 17.

The operation mode field is set to 00 if the device is peer device, 01 if the device is master device, 10 if the device is nonbeaconing slave device, and 11 if the device is beaconing slave device.

The Security Mode field is set to the security mode at which the device is currently operating.

Table 16 — Beacon Slot Descriptor field format

Syntax	Size	Notes
Beacon_Slot_Descriptor_Field_Format {		
Reserved	2 bits	
Movable	1 bit	
Beacon Slot Num	5 bits	
}		

Table 17 — Device Type

Syntax	Size	Notes
Device_Type_Field_Format {		
Operation mode	2 bits	00: peer 01: master 10: nonbeaconing slave 11: beaconing slave
Security mode	2 bits	00: security mode 0 01: security mode 1 10: security mode 2 11: reserved Specified in 8
Reserved	4 bits	
}		

7.1.3.2 Signalling beacon frame

The signalling beacon frame payload is specified in Table 18. The signalling beacon is transmitted in the contention signalling window (CSW) only when a device performs network entry. More description of the use of the signalling beacon is specified in 7.3.

Table 18 — Signalling Beacon Frame Payload Format

Syntax	Size	Notes
Signalling_Beacon_Frame_Payload_Format {		
Device Identifier	6 bytes	
Device type	1 byte	As specified in Table 17
For(i=1, i<=N, i++){		
IE _i	<i>variable</i>	Information element, as specified in 7.1.8. Information elements are optional.
}		
}		

7.1.3.3 Echo beacon frame

During master/slave operation mode, to help beacon coverage extension or to collect coexistence information among the networks, echo beacons could be transmitted as a relay of the mater beacon. The echo beacon frame payload is specified in Table 19.

Table 19 — Echo Beacon Frame Payload Format

Syntax	Size	Notes
Echo_Beacon_Frame_Payload_Format {		
Device Identifier	6 bytes	Address of echo beacon transmitter
Master Identifier	6 bytes	Address of master device
Device type	1 byte	As defined in Table 17
For(i=1, i<=N, i++){		N is the number of including IEs
IE _i	<i>variable</i>	Information element, as defined in 7.1.8. Information elements are optional.
}		
}		

The Master Identifier field is set to the EUI-48 [1] of the master device sending the regular beacon. Others are the same as regular beacon frame payload format.

The size of echo beacon slot equals to one MAS.

7.1.4 Control frames

Default MAC Header field settings for control frames are listed in Table 20. Specific MAC Header field settings and payload descriptions for each of the control frames are shown in the following subclauses.

Table 20 — MAC Header field values for control frames

Header field	Value
Protocol Version	0
Secure	As specified in 7.1.2.1.2
ACK Policy	0 (No-ACK)
Frame Type	1 (control frame)
Frame Subtype	Value from Table 21
Retry	Reserved
DestAddr	DevAddr of the recipient
SrcAddr	DevAddr of the transmitter
Sequence Control	Reserved
Duration	As described in 7.1.2.5.1 and 7.2.9.1
More Frames	Reserved
Access Method	As described in 7.1.2.5.3

Table 21 lists valid values for the Frame Subtype field for control frames.

Table 21 — Frame Subtype field encoding for control frames

Value	Control frame subtype	Description
0	Imm-ACK	Acknowledges correct receipt of the previously-received frame
1	B-ACK	Acknowledges correct or incorrect receipt of one or more preceding frames
2	RTS	Announces to a recipient device that a frame is ready for transmission and requests confirmation of ability to receive
3	CTS	Responds to an RTS control frame that the recipient is able to receive
4	UCA	Announces to neighbours of the transmitting device that the remainder of a reservation block it owns is available for use by other devices via PCA
5	UCR	Announces to neighbours of the transmitting device that the remainder of a reservation block of which it is the target is available for use by other devices via PCA
6 – 13	Reserved	Reserved
14	Application-specific	At discretion of application owner
15	Reserved	Reserved

7.1.4.1 Immediate Acknowledgement (Imm-ACK)

In Imm-ACK frames, the DestAddr field is set to the SrcAddr of the received frame that is acknowledged. Imm-ACK frames have no frame payload.

7.1.4.2 Block Acknowledgement (B-ACK)

The B-ACK frame acknowledges correct or incorrect receipt of the previous sequence of frames and provides information for the transmission of the next sequence of frames as described in 7.7.1.3. The B-ACK frame payload is specified in Table 22.

In B-ACK frames, the DestAddr field is set to the SrcAddr of the frame that requested the B-ACK. The Buffer Size field specifies the maximum number of octets in the sum of the frame payloads of all frames in the next B-ACK sequence.

The Frame Count Field specifies the maximum number of frames in the next B-ACK sequence.

The Sequence Control and Frame Bitmap fields together specify an acknowledgement window of MSDU fragments and their reception status. The Sequence Control field specifies the Sequence Number and Fragment Number that start the acknowledgement window.

Table 22 — B-ACK frame payload

Syntax	Size	Notes
B-ACK_Frame_Payload_Format {		
Buffer Size	2 bytes	
Frame Count	1 byte	
Reserved	1 byte	
Sequence Control	2 bytes	
Frame Bitmap	variable	
}		

The Frame Bitmap field varies in length. A zero-length Frame Bitmap field indicates an acknowledgement window of length ZERO. Otherwise, the least-significant octet of the Frame Bitmap field corresponds to the MSDU indicated by the Sequence Control field, and each bit of the octet corresponds to a fragment of that MSDU. The least-significant bit in each octet corresponds to the first fragment and successive bits correspond to successive fragments. Successive octets present in the Frame Bitmap field correspond to successive MSDUs, and each bit corresponds to a fragment of the MSDU. The acknowledgement window ends at fragment seven of the MSDU that corresponds to the most-significant octet in the Frame Bitmap.

For all bits within the Frame Bitmap, a value of one indicates that the corresponding fragment was received in either the current sequence or an earlier one. A value of ZERO indicates that the corresponding fragment was not received in the current sequence (although it might have been received in an earlier one). Bits of the least-significant octet of the Frame Bitmap field corresponding to fragments prior to the start of the acknowledgement window are undefined. Frames with a Sequence Number earlier than the Sequence Number indicated in the Sequence Control field were not received in the last B-ACK sequence. Such frames were previously received or are no longer expected.

7.1.4.3 Request To Send (RTS)

In RTS frames, the DestAddr field is set to the DevAddr of the device to receive the following frame from the transmitter. RTS frames have no frame payload.

7.1.4.4 Clear To Send (CTS)

In CTS frames, the DestAddr field is set to the SrcAddr of the received RTS frame. CTS frames have no frame payload.

7.1.4.5 Unused CRP Reservation Announcement (UCA)

The UCA frame is used to explicitly release the remaining time of the current Hard or Private CRP reservation block. The DestAddr field is set to BcstAddr.

The UCA frame payload includes a list of DevAddrs of the devices that are expected to respond with a UCR frame, as shown in Table 23.

Table 23 — Payload format for UCA frames

Syntax	Size	Notes
UCA_Frame_Payload_Format {		
For (i=0; i<N; i++){		
DevAddr _i	2 bytes	
}		
}		

7.1.4.6 Unused CRP Reservation Response (UCR)

The UCR frame is used to respond to UCA frames to explicitly release the remaining time of the current Hard or Private CRP reservation block. The DestAddr field is set to the SrcAddr of the received UCA frame. UCR frames have no frame payload.

7.1.4.7 Application-specific

The payload format for Application-specific control frames is specified in Table 24.

Table 24 — Payload format for Application-specific control frames

Syntax	Size	Notes
Application_Specific_Control_Frame_Payload_Format {		
Specifier ID	2 bytes	Identification of a company or organization
Data		Format and use of the Data field defined by the owner of the Specifier ID
}		

The Specifier ID field is set to a 16-bit value that identifies a company or organization, as listed in [4]. The owner of the Specifier ID defines the format and use of the Data field.

7.1.5 Command frames

Default MAC Header settings for command frames are shown in Table 25.

Table 25 — Default MAC Header field values for command frames

Header field	Value
Protocol Version	0
Secure	As specified in 7.1.2.1.2
ACK Policy	0 (No-ACK) or 1 (Imm-ACK)
Frame Type	2 (command frame)
Frame Subtype	Value from Table 26
Retry	As specified in 7.1.2.1.6
DestAddr	DevAddr of the recipient
SrcAddr	DevAddr of the transmitter
Sequence Control	As specified in 7.1.2.4 and 7.2.9.3
Duration	As described in 7.1.2.5.1 and 7.2.9.1

Table 26 contains a list of valid values for the Frame Subtype field for command frames.

Table 26 — Frame Subtype field encoding for Command frames

Value	Command frame subtype	Description
0	CRP Reservation Request	Used to request creation or modification of a CRP reservation
1	CRP Reservation Response	Used to respond to a CRP reservation request command
2	Probe	Used to request for, or respond with, information elements
3	Pair-wise Temporal Key (PTK)	Used to derive a PTK via a 4-way handshake between two devices
4	Group Temporal Key (GTK)	Used to solicit or distribute a GTK within a secure relationship
5	Beaconing Promotion Request	Used from a nonbeaconing slave device to master to request being promoted as a regular beaconing slave device.
6	Channel Measurement Request	Used to request channel measurement by other devices
7	Channel Measurement Response	Used to respond to channel measurement request
8	Channel Measurement Report	Used to report channel measurement results
9	Channel Measurement Report Acknowledgement	Used to confirm the reception of channel measurement reports
10	Channel Switch Command	Used to request channel switch
11	Channel Switch Response	Used to respond to channel switch request
12	RSW Slot Request	Used by slave devices to request an RSW slot allocated by Master device. The command frame is transmitted in CSW.
13	Application-specific	At discretion of application owner
14	Association Request	Used by a slave device to request association with a master device or used by a peer device to request association with another peer device
15	Reserved	Reserved

7.1.5.1 CRP Reservation Request

The CRP Reservation Request command frame is used to create or modify a CRP reservation. The CRP Reservation Request command frame payload is specified in Table 27.

Table 27 — Payload format for CRP Reservation Request command frames

Syntax	Size	Notes
CRP_Reservation_Request_Frame_Payload_Format		
{		
For (i=0; i<N; i++){		
CRP IE _i	variable	
}		
}		

Each CRP IE field included in the command frame corresponds to a reservation request identified by the Owner DevAddr, Target DevAddr, Stream Index, and Reservation Type in the IE. The CRP IE is defined in Table 48.

7.1.5.2 CRP Reservation Response

The CRP Reservation Response command frame is used to respond to a CRP Reservation Request command frame. The CRP Reservation Response command frame payload is specified in Table 28.

Table 28 — Payload format for CRP Reservation Response command frames

Syntax	Size	Notes
CRP_Reservation_Response_Frame_Payload_Format {		
For (i=0; i<N; i++){		
CRP IE _i	variable	
}		
CRP Availability IE	2-34 bytes	
}		

The CRP Reservation Response command frame includes all the CRP IEs from the reservation request. The CRP Availability IE is included according to the rules specified in 7.5.2.

7.1.5.3 Probe

The Probe command frame is used to request information from a device or respond to a Probe request. The payload format is specified in Table 29.

Table 29 — Payload format for Probe command frames

Syntax	Size	Notes
Probe_Command_frame_Format {		
For(i=0; i < N; i++){		
IE _i	<i>variable</i>	
}		
}		

If the payload includes a Probe IE, the command requests information from the recipient. Each Information Element field contains one information element.

7.1.5.4 Channel Measurement Request

The Channel Measurement Request frame is used to request information from a device of channel measurement, including the presence of incumbents and alien devices. The payload format is specified in Table 30.

Table 30 — Format for Channel Measurement Request Frame Payload

Syntax	Size	Notes
Channel_Measurement_Request_Frame_Payload_Format {		
For(i=0; i < N; i++){		
IE _i	Variable	Channel Measurement Request IEs only, as defined in Table 59
}		
}		

7.1.5.5 Channel Measurement Response

Channel Measurement Response frame is used to confirm the reception of channel measurement request. The payload format is specified in Table 31.

Table 31 — Format for Channel Measurement Response Frame Payload

Syntax	Size	Notes
Channel_Measurement_Response_Frame_Payload_Format {		
For(i=0; i < N; i++){		
IE _i	Variable	Channel Measurement Response IEs only, as defined in Table 61
}		
}		

7.1.5.6 Channel Measurement Report

The Channel Measurement Report frame is used to report channel measurement results. The payload format is specified in Table 32.

Table 32 — Format for Channel Measurement Report Frame Payload

Syntax	Size	Notes
Channel_Measurement_Report_Frame_Payload_Format {		
For(i=0; i < N; i++){		
IE _i	Variable	Channel Measurement Report IE, as defined Table 62
}		
}		

7.1.5.7 Channel Measurement Report Acknowledgement

The Channel Measurement Report Acknowledgement frame is used to confirm the reception of channel measurement reports. The payload format is specified in Table 33.

Table 33 — Format for Channel Measurement Report Acknowledgement Frame Payload

Syntax	Size	Notes
Channel_Measurement_Report_Acknowledgement_Frame_Payload_Format {		
For(i=0; i < N; i++){		
IE _i	Variable	Channel Measurement Report Acknowledgement IE, as defined in Table 65
}		
}		

7.1.5.8 Channel Switch Command

The Channel Switch Command frame is used to request channel switch of other devices. The payload format is specified in Table 34.

Table 34 — Format for Channel Switch Command Frame Payload

Syntax	Size	Notes
Channel_Switch_Command_Payload_Format {		
For(i=0; i < N; i++){		
IE _i	Variable	Channel Change IE, as defined in Table 66
}		
}		

7.1.5.9 Channel Switch Response

The Channel Switch Response frame is used to respond to the Channel Switch Request command. The payload format is specified in Table 35.

Table 35 — Payload format for Channel Switch Response command frame

Syntax	Size	Notes
Channel_Switch_Command_Payload_Format {		
Channel Change Response IE	4 bytes	Refer to Table 68
}		

7.1.5.10 RSW Slot Request command frame

The command frame is used by nonbeaconing slave devices and sent in CSW slot. The payload of the RSW Slot Request command frame is specified in Table 36.

Table 36 — Payload format for RSW Slot Request command frame

Syntax	Size	Notes
RSW_Slot_Request_Payload_Format {		
Device Identifier	6 bytes	MAC address of current device
Reservation Target DevAddr	2 bytes	
}		

The Reservation Target DevAddr is set to the DevAddr of the reservation target of the requested RSW slot(s) which will be used for channel reservation negotiation. If the reservation target is Master device, it shall be set to Master DevAddr. If the reservation target is another slave device, it shall be set to the DevAddr of the slave device.

7.1.5.11 Beaconing Promotion Request

The Beaconing Promotion Request command frame is sent from a nonbeaconing slave device to its master to request to be promoted as a regular beaconing slave device. The format of payload is specified in Table 37.

Table 37 — Payload format for Beaconing Promotion Request frame

Syntax	Size	Notes
Beaconing_Promotion_Request_Payload_Format {		
Reason code	1 byte	0 – CRA by a slave device 1 – Self-coexistence 2 – unspecified 3 – 255 - reserved
}		

7.1.5.12 Association Request

The Association Request command frame is sent from a slave device to a master device, or from a peer device to another peer device, to request association. The format of payload is specified in Table 38.

Table 38 — Payload format for Association Request

Syntax	Size	Notes
Association_Request_Payload_Format {		
MAC address	6 bytes	The MAC address of the device requesting association
Identification IE	variable	It at least includes the Regulation ID (see Table 78).
}		

7.1.5.13 Pairwise Temporal Key (PTK)

The PTK command frame is used in a 4-way handshake by a pair of devices, as described in 8.3.1, to authenticate each other and to derive a shared symmetric PTK for securing certain unicast traffic between the two devices. The PTK command frame is specified in Table 39.

Table 39 — Payload format for PTK command frame

Syntax	Size	Notes
PTK_Payload_Format {		
Message Number	1 byte	
Status Code	1 byte	
PTKID	3 bytes	
Reserved	11 bytes	
MKID	16 bytes	
I-Nonce / R-Nonce	16 bytes	
PTK MIC	8 bytes	
}		

The Message Number is set to 1, 2, 3, or 4, respectively, in the PTK command containing the first, second, third, or fourth message of the 4-way handshake. The other values of this field are reserved.

The Status Code in a PTK command indicates the current status of the 4-way handshake at the device sending this command. It is encoded as shown in Table 40.

Table 40 — Status Code field encoding in PTK commands

Value	Meaning
0	Normal—the 4-way handshake proceeds.
1	Aborted—the 4-way handshake is aborted per security policy.
2	Aborted—the 4-way handshake is aborted in order to yield to a concurrent 4-way handshake using the same master key.
3	PTKID not accepted—it is the TKID of a PTK or GTK being possessed by this device.
4 – 255	Reserved

The PTKID is set to a non-zero number as the TKID of the PTK to be derived from this 4-way handshake procedure. The initiator of the 4-way handshake chooses this value after determining that this value is different from the TKID of the PTK, if any, that is to be replaced by the new PTK, and the TKID of any PTK or GTK it currently possesses.

The MKID identifies the master key used in this 4-way handshake as described 8.3.1.

The I-Nonce/R-Nonce is a random number generated by the initiator or responder for this 4-way handshake. This field is set to I-Nonce, the random number generated by the initiator in the command containing a Message Number of 1 or 3, and is set to R-Nonce, the random number generated by the responder in the command containing a Message Number of 2 or 4.

The PTK MIC in the PTK command containing a Message Number of 1 is set to zero on transmission and is ignored on reception.

The PTK MIC in the PTK command containing a Message Number of 2, 3, or 4 is set to the MIC that protects the fields in the Frame Payload of this command using the PTK MIC key generated from the first two messages of the 4-way handshake as specified in 8.3.1.

The MAC Header for the PTK command frame is set as indicated in Table 25, with the ACK Policy set to Imm-ACK.

7.1.5.14 Group Temporal Key (GTK)

The GTK command frame is used to solicit or distribute a GTK following a PTK update. The GTK is used to secure certain multicast traffic from a sending device to a group of recipient devices, and is chosen by the sending device. The GTK command frame is always in secure form, and the Secure Payload field is specified in Table 41.

Table 41 — Payload format for GTK command frame

Syntax	Size	Notes
GTK_Payload_Format {		
Message Number	1 byte	
Status Code	1 byte	
GTKID	3 bytes	
Reserved	3 bytes	
GroupAddr	2 bytes	
GTK SFC	6 bytes	
GTK	16 bytes	
}		

The TKID identifies the PTK used to secure this frame and to generate the GTK being solicited or distributed.

The EO is set to zero, indicating that the secure payload which starts with the Message Number field is encrypted with the PTK indicated in the TKID field.

The SFN is set in the same way as for any secure frame. It is one plus the SFN value used in the last secure frame transmitted with the protection of the PTK indicated in the TKID field.

The Message Number is set to 0 in the GTK command transmitted by a multicast recipient device to solicit a new GTK from a multicast sender. The Message Number is set to 1 in the GTK command transmitted by a multicast sender to distribute a new GTK to a multicast recipient. The Message Number is set to 2 in the GTK command transmitted by a multicast recipient device to respond to the distribution of a new GTK command.

The Status Code in a GTK command indicates the current status of the GTK solicitation or distribution at the device sending this command. It is encoded as shown in Table 42.

Table 42 — Status Code field encoding in GTK commands

Value	Meaning
0	Normal—GTK solicitation or distribution proceeds.
1	Rejected—GTK solicitation or distribution is rejected per security policy.
2	GTKID not accepted—it is the TKID of a PTK or GTK being possessed by this device.
3 – 255	Reserved

The GTKID in the GTK command containing a Message Number of 0 is set to the TKID of the GTK being solicited. It is set to zero if the soliciting device does not know the TKID of the GTK it is soliciting.

The GTKID in the GTK command containing a Message Number of 1 is set to a non-zero number as the TKID of the GTK being distributed. The distributor chooses this value after determining that this value is different from the TKID of the GTK, if any, that is to be replaced by the new GTK, and the TKID of any PTK or GTK the distributor or recipient currently possesses.

The GTKID in the GTK command containing a Message Number of 2 is set to the GTKID in the last received GTK command containing a Message Number of 1.

The GroupAddr is set to the McstAddr or BcstAddr for which the GTK is being solicited or distributed. It is set to 0x0001 if the GTK is applied to all broadcast and multicast traffic from the device distributing this GTK.

The GTK SFC in the GTK command containing a Message Number of 0 is set to zero on transmission and ignored on reception.

The GTK SFC in the GTK command containing a Message Number of 1 is set to the current value of the secure frame counter set up for the GTK being distributed.

The GTK SFC in the GTK command containing a Message Number of 2 is set to the GTK SFC in the last received GTK command containing a Message Number of 1.

The GTK is the GTK distributed by the multicast sender for the McstAddr. In a GTK command soliciting a GTK, the GTK is set to zero prior to encryption.

The MIC is calculated as for any secure frame, using the PTK indicated in the TKID field.

The MAC Header for the GTK command frame is set as indicated in Table 25, with the ACK Policy set to Imm-ACK.

7.1.5.15 Application-specific

The payload format for Application-specific command frames is specified in Table 43.

Table 43 — Payload format for Application-specific command frame

Syntax	Size	Notes
Application-specific Command Payload Format {		
Specifier ID	2 bytes	
Data	variable	
}		

The Specifier ID field is set to a 16-bit value that identifies a company or organization, as listed in [4]. The owner of the Specifier ID defines the format and use of the Data field.

7.1.6 Data frames

MAC Header and Frame Payload fields for data frames are set as described in 7.1.2.

7.1.7 Aggregated data frames

MAC header and frame payload field format for aggregated data frames is defined in 7.6.2.

7.1.8 Information elements

This subclause defines the information elements (IEs) that may appear in beacons and certain command frames.

The general format of all IEs is specified in Table 44.

Table 44 — General IE format

Syntax	Size	Notes
General IE Format {		
Element ID	1 byte	Set to the value as listed in Table 45 that identifies the information element
Length	1 byte	Set to the length, in bytes, of the IE-specific fields
IE-specific fields	As indicated in Length field	Contain information specific to the IE
}		

Table Information elements contains a list of IEs defined in this draft.

Table 45 — Information elements

Element ID	Information element	Description
0	Traffic Indication Map (TIM) IE	Indicates that a device has data buffered for transmission via PCA
1	Beacon Period Occupancy IE (BPOIE)	Provides information on neighbours' BP occupancy in the previous superframe
2	PCA Availability IE	Indicates the MASs that a device is available to receive PCA frames and transmit the required response
3 – 7	Reserved	Reserved
8	CRP Availability IE	Indicates a device's availability for new CRP reservations
9	Channel Reservation Protocol (CRP) IE	Indicates a reservation with another device
10	Hibernation Mode IE	Indicates the device will go to hibernation mode for one or more superframes but intends to wake at a specified time in the future
11	BP Switch IE	Indicates the device will change its BPST at a specified future time
12	MAC Capabilities IE	Indicates which MAC capabilities a device supports
13	PHY Capabilities IE	Indicates which PHY Capabilities a device supports
14	Probe IE	Indicates a device is requesting one or more IEs from another device or/and responding with requested IEs
15	Application-specific Probe IE	Indicates a device is requesting an Application-specific IE from another device
16	Link Feedback IE	Provides data rate and power control feedback
17	Hibernation Anchor IE	Provides information on devices in hibernation mode
18	Identification IE	Provides identifying information about the

		device, including a name string.
19	Master Key Identifier (MKID) IE	Identifies some or all of the master keys held by the transmitting device
20	Relinquish Request IE	Indicates that a neighbour requests that a device release one or more MASs from its reservations.
21	Multicast Address Binding (MAB) IE	Indicates an address binding between a multicast EUI-48 and a McstAddr
22	Regular QP Schedule IE	Indicates the regular quiet period schedule
23	On-demand QP Schedule IE	Indicates the on-demand quiet period schedule
24	Channel Measurement Request IE	Asks a device to measure an outband channel
25	Channel Measurement Response IE	Confirms receiving Channel Measurement Request IE
26	Channel Measurement Report IE	Report Channel Measurement Report to other devices
27	Channel Measurement Report Acknowledgement IE	Acknowledge the reception of Channel Measurement Report IE
28	On-leave IE	Announces the temporary on-leave schedule
29	Proxy Assignment IE	Assigns the next proxy
30	Channel Change IE	Advise a group of device to move to a new available channel
31	Slave device list IE	Used by a master to indicate the list of slave devices associated with itself
32	Channel change response IE	Respond to channel switch request
33	Channel Classification IE	
34	RSW Schedule IE	Indicates the RSW schedule
35	Echo Beacon Position IE	Indicates both MAS position of echo beacon and transmission owner of echo beacon
36	Beaconing Promotion Indication IE	Indicate nonbeaconing slave devices to become regular beaconing slave devices
37	Association Response IE	Used by a device to confirm the association request by another device
38	On-demand QP Negotiation Request IE	To request On-demand QP
39	On-demand QP Negotiation Response IE	To respond to On-demand QP request
40	Device Feature IE	Provides information of device's feature
41	Link Quality Estimate IE	Report link quality estimate
42	Transmit Power Control IE	Provide the recommended transmit power for other devices
43	Disassociation IE	Used by a master or peer device to disassociate a group of slave devices or peer devices, respectively
44	Contact Verification Signal IE	Transmitted from a master device to slave devices or from a peer device to peer devices. A slave device must either receive a contact verification signal from the master device that provided its current list of available channels or contact the master device to re-verify/re-establish channel availability. A peer device must either receive a contact verification signal from the peer device that provided its current list of available channels or contact the peer device to re-verify/re-establish channel availability.
45 – 254	Reserved	Reserved
255	Application-Specific IE (ASIE)	Use varies depending on the application

7.1.8.1 Beacon Period Occupancy IE (BPOIE)

A device shall always include a BPOIE in its beacon. In the BPOIE the device shall reflect beacons received from neighbours in the recent superframes, as well as information retained based on hibernation mode rules.

The BPOIE provides information on the BP observed by the device sending the IE. The BPOIE is specified in Table 46.

Table 46 — BPOIE format

Syntax	Size	Notes
BPOIE_Format {		
Element ID	1 byte	Set to the value as listed in Table 45 that identifies the information element
Length (= 1+K+2×N)	1 byte	N is the total number of devices that occupy beacon slot(s).
BP Length	1 byte	For a master device, BP length ≥ 1 ; For a peer device, BP length ≥ 2 .
Beacon Slot Info Bitmap	K bytes	$K = \text{Ceiling}(\text{BP_Length}/4)$
For(i=1; i<=N; i++){		
DevAddr _i	2 bytes	The device address of the slot owner
}		
}		

The BP Length field is set to the length of the BP, measured in beacon slots, as defined in 7.3.3.

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, where $K = \text{Ceiling}(\text{BP_Length}/4)$. Each element n, numbered from 0 to $4 \times K - 1$, corresponds to beacon slot n and is encoded as shown in Table 47. Element zero is the least-significant two bits of the field. Unused elements, if any, are set to zero.

Table 47 — Beacon Slot Info Bitmap element encoding

Element value	Beacon slot status
0	Unoccupied (non-movable) No PHY indication of medium activity was received in the corresponding beacon slot in the last superframe, or any frame header received with a valid HEI was not a beacon frame.
1	Occupied & non-movable A beacon frame was received with a valid HEI and FCS in the corresponding beacon slot in the last superframe, and the Movable bit in that beacon was set to zero, or a beacon frame was received in the corresponding beacon slot in a previous superframe that indicated a hibernation period that has not expired, as described in 7.9.
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 frame with valid HEI and FCS.
3	Occupied & movable A beacon frame was received with a valid HEI and FCS in the corresponding beacon slot in the last superframe, and the Movable bit in that beacon was set to one.

The DevAddr fields correspond to beacon slots encoded as occupied in the Beacon Slot Info Bitmap. They are included in ascending beacon slot order. If a beacon was received with a valid HEI at a beacon slot in the last superframe, the corresponding DevAddr field is set to the SrcAddr in the MAC header of that received beacon. If a frame was received with an invalid HEI from a beacon slot in the last superframe, the corresponding DevAddr field is set to BcstAddr. If a neighbour of the device is in hibernation mode, the DevAddr field that corresponds to the hibernating neighbour's beacon slot is set to the DevAddr of that neighbour.

7.1.8.2 Channel Reservation Protocol (CRP) IE

A CRP IE is used to negotiate a reservation or part of a reservation for certain MASs and to announce the reserved MASs. The CRP IE is specified in Table 48.

Table 48 — CRP IE format

Syntax	Size	Notes
CRP IE Format {		
Element ID	1 byte	Set to the value as listed in Table 45 that identifies the information element
Length (= 6+4×N)	1 byte	
CRP Control	2 bytes	Defined in Table 49
Owner DevAddr	2 bytes	DevAddr of reservation owner
Target DevAddr	2 bytes	DevAddr of reservation target
For(i=0; i < N; i++){		
CRP Allocation	4 bytes	Defined in Table 52
}		

The CRP Control field is specified in Table 49.

Table 49 — CRP Control field format

Syntax	Size	Notes
CRP_Control_field {		
Reservation Type	3 bits	
Stream Index	3 bits	
Reason Code	3 bits	
Reservation Status	1 bit	
Conflict Tie-breaker	1 bit	
Unsafe	1 bit	
Reserved	4 bits	
}		

The Reservation Type field is set to the type of the reservation and is encoded as shown in Table 50.

Table 50 — Reservation Type field encoding

Value	Reservation Type
0	Alien BP
1	Hard
2	Soft
3	Private
4	PCA
5 – 7	Reserved

The Stream Index field identifies the stream of data to be sent in the reservation. This field is reserved if the Reservation Type is PCA and Alien BP.

The Reason Code is used by a reservation target to indicate whether a CRP reservation request was successful and is encoded as shown in Table 51. The Reason Code is set to ZERO in a CRP 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 MASs claimed in the reservation have been removed or if CRP IEs have been combined. The field is reserved if the Reservation Type is PCA.

Table 51 — Reason Code field encoding

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

The Reservation Status bit indicates the status of the CRP negotiation process. The Reservation Status bit is set to ZERO in a CRP 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 bit is set to ONE if Reservation Type is Alien BP or PCA.

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 CRP IEs that represent the same reservation, the Conflict Tie-breaker bit is set to the same value.

The Owner DevAddr field and Target DevAddr field are set to the DevAddr of the reservation owner and the DevAddr of the reservation target, respectively. These two fields are reserved if the Reservation Type is PCA.

The Unsafe bit is set to ONE if any of the MASs identified in the CRP Allocation fields is considered in excess of reservation limits.

A CRP IE contains one or more CRP Allocation fields. Each CRP Allocation field is encoded using a zone structure. The superframe is split into 16 zones numbered from 0 to 15 starting from the BPST. Each zone contains 16 consecutive MASs, which are numbered from 0 to 15 within the zone.

The format of a CRP Allocation field is specified in Table 52.

Table 52 — CRP Allocation field format

Syntax	Size	Notes
CRP_Allocation_field {		
Zone Bitmap	2 bytes	
MAS Bitmap	2 bytes	
}		

The Zone Bitmap field identifies the zones that contain reserved MASs. If a bit in the field is set to ONE, the corresponding zone contains reserved MASs, where bit zero corresponds to zone zero.

The MAS Bitmap specifies which MASs 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 MAS within each zone identified by the Zone Bitmap is included in the reservation, where bit zero corresponds to MAS zero within the zone.

7.1.8.3 CRP Availability IE

The CRP Availability IE is used by a device to indicate its view of the current utilization of MASs in the current superframe.

The CRP Availability IE is specified in Table 53.

Table 53 — CRP Availability IE format

Syntax	Size	Notes
CRP_Availability_IE_Format {		
Element ID	1 byte	Set to the value as listed in Table 45 that identifies the information element
Length (= N)	1 byte	
CRP Availability Bitmap	N (0-32)	variable
}		

The CRP Availability Bitmap field is up to 256 bits long, one bit for each MAS in the superframe, where the least-significant bit of the field corresponds to the first MAS in the superframe and successive bits correspond to successive MASs. Each bit is set to ONE if the device is available for a CRP reservation in the corresponding MAS, or is set to ZERO otherwise. If the CRP Availability Bitmap field is smaller than 32 octets, the bits in octets not included at the end of the bitmap are treated as zero.

7.1.8.4 Link Feedback IE

The Link Feedback IE contains information on the recommended change to the data rate and transmit power level by a recipient device for one or more source devices. The Link Feedback IE is specified in Table 54.

Table 54 — Link Feedback IE format

Syntax	Size	Notes
Link_Feedback_IE_Format {		
Element ID	1 byte	
Length (= 1+3xN)	1 byte	
N	1 byte	Num of Link fields
For (i=1, i <=N, i++) {		
Link _i	3 bytes	Defined in Table 55
}		
}		

The Link field is specified in Table 55.

Table 55 — Link field format

Syntax	Size	Notes
Link_Field_Format {		
DevAddr	16 bits	
Transmit Power Level Change	4 bits	Specified in Table 56
Data rate	4 bits	Specified in Table 140
}		

The DevAddr field is set to the DevAddr of the source device for which the feedback is provided.

The Transmit Power Level Change field is set to the change in transmit power level that the recipient recommends to the source device. The Transmit Power Level Change field encoding is shown in Table 56.

Table 56 — Transmit Power Level Change field encoding

Value	dB
1000 – 1101	Reserved
1110	-2
1111	-1
0000	no change
0001	+1
0010	+2
0011 – 0111	Reserved

The Data Rate field is set to the data rate that the recipient device recommends that the source device use. The Data Rate field is encoded as shown in Table 140.

7.1.8.5 Regular QP Schedule IE

Regular QP Schedule IE, defined in Table 57, shall be included in each beacon frame in order to make sure every device in the beacon group knows the sensing schedule. All the devices in the beacon group should participate in service monitoring.

Table 57 — Regular QP Schedule IE format

Syntax	Size	Notes
Operating_Channel_Monitor_IE_Format {		
Element ID	1 byte	Set to the value as listed in Table 45 that identifies the information element
Length (=3)	1 byte	
Countdown	1 byte	In the number of superframe. If it equals zero, the regular QP is scheduled in the current superframe.
Sensing cycle	1 byte	In the unit of superframe. Set as mQPfrequency
QP duration	1 byte	In the unit of MAS. Set as mQPD
}		

NOTE if sensing cycle is set as zero, no regular QP is scheduled.

7.1.8.6 On-demand QP Schedule IE

A device may schedule QP on demand as described in 7.11.1.1.2. An on-demand QP schedule IE should be included in beacons. Other devices hearing on-demand QP schedule IE shall keep quiet during QP and may participate in sensing. The format of on-demand QP schedule IE is defined in Table 58.

Table 58 — On-demand QP Schedule IE format

Syntax	Size	Notes
Operating_Channel_Monitor_IE_Format {		
Element ID	1 byte	Set to the value as listed in Table 45 that identifies the information element
Length (= 3)	1 byte	
Superframe count down	1 byte	The number of superframe left before On-demand QP is enabled. When the value is set to 0, On-demand QP is enabled in current superframe.
QP starting time	1 byte	Starting MAS to perform monitoring
Duration	1 byte	Channel monitoring period, in the unit of MAS
}		

7.1.8.7 Channel Measurement Request IE

A peer device or a master device may ask another device to measure a channel for the detection of incumbents or alien devices. The device shall include channel measurement request IE, defined in Table 59, in its beacon frame or corresponding command frame for such request.

In addition, a peer device or a master device may ask another device to check the availability of a outband channel for backup purpose by using this IE.

Table 59 — Channel Measurement Request IE

Syntax	Size	Notes
Channel_Measurement_Request_IE_Format {		
Element ID	1 byte	Set to the value as listed in Table 45 that identifies the information element
Length (= 4+2xN)	1 byte	N is the total number of devices invited to monitor outband channel
Channel number	1 byte	Target Channel for measurement. Refer to 9.7.2.
Monitor countdown	1 byte	The starting MAS to perform monitoring
Action code	1 byte	Measurement requirements, as defined in Table 60
Duration	1 byte	The channel monitoring period, in the unit of MAS
For(i=0; i<N; i++){		
DevAddr _i	2 bytes	Invited device
}		
}		

Table 60 — Field Format for Action Code of Channel Measurement

Syntax	Size	Notes
Action_Code_Field_Format {	bit	
TV	1 bit	1 – TV detection required; 0 otherwise
WM	1 bit	1 – WM detection required; 0 otherwise
Alien device	1 bit	1 – Alien device detection required; 0 otherwise
Measured signal strength	1 bit	1 – Need to report measured signal strength; 0 otherwise
Reserved	4 bits	
}		