
**Information technology —
Telecommunications and information
exchange between systems — MAC/PHY
standard for ad hoc wireless network to
support QoS in an industrial work
environment**

*Technologies de l'information — Télécommunications et échange
d'information entre systèmes — Norme MAC/PHY pour un réseau ad
hoc sans fil qui supporte QoS dans un environnement de travail
industriel*





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested 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

1	Scope	1
2	Normative references	1
3	Terms and definitions, and abbreviations	2
3.1	Terms and definitions.....	2
3.2	List of Abbreviations	3
4	Overview	7
4.1	Characteristics	7
4.1.1	Ad-hoc network	7
4.1.2	Quality of Service	7
4.1.3	Binary CDMA technology	7
4.2	Components of network	7
4.2.1	Station	8
4.2.2	Resources	8
4.3	Functional overview	8
4.3.1	Network synchronization	9
4.3.2	Data transmission	9
4.3.3	Security	10
4.3.4	Power management	11
4.3.5	Master handover	11
4.4	Summary of operations	11
4.4.1	Broadcasting during the beacon period.....	11
4.4.2	Random access during the contention period	11
4.4.3	Exclusive access during the allocation period.....	11
4.5	Summary of states	12
4.5.1	Establishing the network	12
4.5.2	Associating with the network	12
4.5.3	Security membership and key establishment.....	12
4.5.4	Data transfer.....	12
4.5.5	Master handover	12
4.5.6	Disassociating from the network	13
4.5.7	Terminating the network	13
5	Inter-layer interfaces	14
5.1	Summary	14
5.2	General format of management primitives.....	14
5.2.1	MLME-GET.request and PLME-GET.request.....	15
5.2.2	MLME-GET.confirm and PLME-GET.confirm	16
5.2.3	MLME-SET.request and PLME-SET.request	16
5.2.4	MLME-SET.confirm and PLME-SET.confirm	16
5.3	MLME SAP	17
5.3.1	Reset	18
5.3.2	Scan.....	19
5.3.3	Startup of network	21
5.3.4	Synchronization	22
5.3.5	Association.....	24
5.3.6	Disassociation.....	27
5.3.7	Key request.....	29
5.3.8	Key distribution.....	31
5.3.9	Security management.....	34
5.3.10	Master handover	38
5.3.11	Data request	40
5.3.12	Network node data probe.....	42
5.3.13	Stream creation, modification, termination.....	44

5.3.14	Channel state.....	48
5.3.15	Remote scan.....	50
5.3.16	Network parameter modification	53
5.3.17	Adjustment of power	55
5.3.18	Power saving	56
5.4	MAC management.....	58
5.4.1	MAC PIB master group.....	58
5.4.2	MAC PIB attributes group	59
5.4.3	MAC PIB authentication group.....	59
5.4.4	MAC PIB association group.....	59
5.4.5	MAC PIB network security group.....	60
5.5	MAC SAP.....	60
5.5.1	MAC-ASYNC-DATA.request.....	61
5.5.2	MAC-ASYNC-DATA.confirm.....	62
5.5.3	MAC-ASYNC-DATA.indication.....	62
5.5.4	MAC-ISOCH-DATA.request.....	63
5.5.5	MAC-ISOCH-DATA.confirm.....	63
5.5.6	MAC-ISOCH-DATA.indication.....	64
5.6	PHY specification.....	64
5.6.1	PD-SAP.....	64
5.6.2	PLME-SAP.....	74
5.6.3	Physical layer enumerated description	79
6	Mac frame format.....	81
6.1	Overview	81
6.2	General format of MAC frames	81
6.2.1	Frame header	82
6.2.2	Frame body.....	85
6.3	Frame formats	86
6.3.1	Beacon	86
6.3.2	Acknowledgement	88
6.3.3	Command.....	89
6.3.4	Data (stream or non-stream).....	90
6.3.5	RTS (Request To Send)	90
6.3.6	CTS (Clear To Send)	91
6.4	Information block.....	91
6.4.1	Station UID.....	92
6.4.2	Station name.....	92
6.4.3	Station type.....	92
6.4.4	Network synchronization	92
6.4.5	Capabilities.....	93
6.4.6	Maximum supported time slot.....	93
6.4.7	Maximum transmit power.....	94
6.4.8	Resource allocation	94
6.4.9	New master notification	95
6.4.10	Sleep state notification.....	95
6.4.11	Vendor specific	95
6.5	Command block	95
6.5.1	Network management.....	97
6.5.2	Stream management.....	99
6.5.3	Power management	103
6.5.4	Key management	104
6.5.5	Security management.....	105
6.5.6	Vendor specific	105
6.5.7	Other.....	106
7	MAC feature description	110
7.1	Network formation and association	110
7.1.1	Channel scanning	110
7.1.2	Network ID	111
7.1.3	Association.....	111

7.1.4	Disassociation	111
7.1.5	Master handover	112
7.2	Media access	112
7.2.1	Code assignment	112
7.2.2	Inter-frame space	112
7.2.3	Access during the contention period	113
7.2.4	Access during the allocation period	113
7.3	Synchronization	114
7.3.1	Superframe synchronization	114
7.3.2	Beacon generation	115
7.3.3	Beacon reception	115
7.3.4	Synchronization	115
7.4	Resource allocation	115
7.4.1	Transmission of synchronous data	115
7.4.2	Asynchronous data transmission	117
7.5	Fragmentation and defragmentation	117
7.6	Acknowledgement and retransmission	118
7.6.1	No acknowledgement	118
7.6.2	Immediate acknowledgement	118
7.6.3	Delayed acknowledgement	118
7.6.4	Implicit acknowledgement	118
7.6.5	Retransmission	118
7.7	Power saving	119
7.7.1	Saving power in a connected state	119
7.7.2	Sleep state	119
7.8	Dynamic channel management	119
7.8.1	Channel state probe	119
7.8.2	Remote Channel state probe	119
7.8.3	Frequency channel change	120
7.9	MAC parameters	120
8	Security	121
8.1	Security mechanisms	121
8.1.1	Security membership and key establishment	121
8.1.2	Key transport	121
8.1.3	Data encryption	121
8.1.4	Data integrity	121
8.1.5	Beacon integrity protection	122
8.1.6	Command integrity protection	122
8.1.7	Freshness protection	122
8.2	Security modes	122
8.2.1	Security mode 0	122
8.2.2	Security mode 1	122
8.2.3	Security mode 2	123
8.3	Security Support	123
8.3.1	Changes in the network group data key	123
8.3.2	Joining a secure network	123
8.3.3	Secure frame generation	124
8.3.4	Secure frame reception	124
8.3.5	Retransmission detect	125
8.3.6	Key selection	125
8.4	Key management protocol	128
8.4.1	Key distribution protocol	128
8.4.2	Key request protocol	130
8.5	CCM mode	131
8.5.1	Overview	131
8.5.2	Nonce	131
8.5.3	Inputs	132
9	General specifications	135
9.1	General requirements	135

9.1.1	Operating frequency range	135
9.1.2	PHY layer timing	136
9.1.3	Receive-to-transmit turnaround time	137
9.1.4	Transmit-to-receive turnaround time	137
9.1.5	Channel switch time	137
9.1.6	Maximum frame size	137
9.2	PHY Protocol Data Unit (PDU) format	137
9.2.1	General format	137
9.2.2	Preamble	138
9.2.3	PHY Header	139
9.2.4	PHY payload	140
9.3	Modulation and coding	141
9.3.1	Spreading code	141
9.3.2	QPSK modulation	142
9.3.3	Constant envelope coding	142
9.3.4	Modulation methods for PHY PDU	145
9.3.5	Data rate	146
9.3.6	QPSK Modulation and constellation	146
9.4	PHY layer constants and PHY PIB attribute	147
9.5	Transmitter specification	147
9.5.1	Error vector magnitude (EVM) definition	147
9.5.2	EVM calculated values	148
9.5.3	Transmitter power spectrum mask	148
9.5.4	Signal waveform filter	149
9.5.5	Error tolerance for carrier frequency	149
9.5.6	Transmitter data rate	149
9.5.7	Synchronization	149
9.5.8	Transmitter response time	150
9.5.9	RF carrier suppression	150
9.5.10	Transmit power	150
9.6	Receiver specifications	150
9.6.1	Error rate criteria	150
9.6.2	Receiver sensitivity	151
9.6.3	Maximum input power	151
9.6.4	Receiver Energy detection (ED)	151
9.6.5	Clear channel assessment (CCA)	151
9.6.6	Received CCA performance	151
9.6.7	Received Signal Strength Index	151
9.6.8	Link Quality Index (LQI)	152
Annex A (informative)	Example scheduler and admission control	153
A.1	Scheduling algorithm	153
A.2	Admission control Algorithm	154

List of Figures

FIGURE 1 - NETWORK	8
FIGURE 2 - SUPERFRAME.....	9
FIGURE 3 - PROTOCOL STACK CONFIGURATION.....	14
FIGURE 4 - TRANSMISSION ORDER.....	81
FIGURE 5 - FORMAT OF MAC FRAME	82
FIGURE 6 - NON-SECURE MAC FRAME BODY FORMAT	82
FIGURE 7 - SECURE MAC FRAME BODY FORMAT	82
FIGURE 8 - FORMAT OF FRAME CONTROL FIELDS	82
FIGURE 9 - FORMAT OF STREAM ID FIELD	84
FIGURE 10 - NON-SECURE BEACON FRAME FORMAT	86
FIGURE 11 - SECURE BEACON FRAME FORMAT	87
FIGURE 12 - IMMEDIATE ACKNOWLEDGEMENT FRAME FORMAT	88
FIGURE 13 - DELAYED ACKNOWLEDGEMENT FRAME PAYLOAD FORMAT	89
FIGURE 14 - FORMAT OF RECORD FOR STREAM-M	89
FIGURE 15 - NON-SECURE COMMAND FRAME FORMAT	89
FIGURE 16 - COMMAND BLOCK FORMAT	90
FIGURE 17 - FORMAT OF SECURE COMMAND FRAME.....	90
FIGURE 18 - NON-SECURE DATA FRAME FORMAT	90
FIGURE 19 - SECURE DATA FRAME FORMAT	90
FIGURE 20 - RTS FRAME FORMAT.....	91
FIGURE 21 - CTS FRAME FORMAT	91
FIGURE 22 - INFORMATION BLOCK FORMAT.....	92
FIGURE 23 - STATION UID INFORMATION BLOCK FORMAT	92
FIGURE 24 - STATION NAME INFORMATION BLOCK FORMAT.....	92
FIGURE 25 - STATION TYPE INFORMATION BLOCK FORMAT	92
FIGURE 26 - NETWORK SYNCHRONIZATION INFORMATION BLOCK FORMAT	92
FIGURE 27 - CAPABILITY INFORMATION BLOCK FORMAT	93
FIGURE 28 - CAPABILITY FIELD FORMAT.....	93
FIGURE 29 - MAXIMUM SUPPORT TIMESLOT INFORMATION BLOCK FORMAT	93
FIGURE 30 - MAXIMUM TRANSMIT POWER INFORMATION BLOCK FORMAT	94
FIGURE 31 - RESOURCE ALLOCATION INFORMATION BLOCK FORMAT	94
FIGURE 32 - RESOURCE ALLOCATION BLOCK FORMAT	94
FIGURE 33 - NEW MASTER NOTIFICATION INFORMATION BLOCK FORMAT	95
FIGURE 34 - SLEEP STATE NOTIFICATION INFORMATION BLOCK FORMAT.....	95
FIGURE 35 - VENDOR SPECIFIC INFORMATION ELEMENT FORMAT	95
FIGURE 36 - COMMAND BLOCK FORMAT	96
FIGURE 37 - ASSOCIATE REQUEST COMMAND BLOCK FORMAT.....	97
FIGURE 38 - ASSOCIATION RESPONSE COMMAND BLOCK FORMAT	97
FIGURE 39 - DISASSOCIATION REQUEST PAYLOAD FORMAT	98
FIGURE 40 - MASTER HANDOVER COMMAND BLOCK FORMAT	99
FIGURE 41 - RESOURCE ALLOCATION REQUEST COMMAND BLOCK FORMAT	100
FIGURE 42 - RESOURCE ALLOCATION REQUEST RECORD FORMAT	100
FIGURE 43 - RESOURCE ALLOCATION RESPONSE COMMAND BLOCK FORMAT.....	100
FIGURE 44 - RESOURCE ALLOCATION MODIFICATION COMMAND BLOCK FORMAT.....	101
FIGURE 45 - RESOURCE ALLOCATION MODIFICATION REQUEST RECORD FORMAT	101
FIGURE 46 - RESOURCE ALLOCATION TERMINATION COMMAND BLOCK FORMAT	102
FIGURE 47 - DELAYED ACKNOWLEDGEMENT RESYNCHRONIZATION COMMAND BLOCK FORMAT.....	102
FIGURE 48 - DELAYED ACKNOWLEDGEMENT RESYNCHRONIZATION COMMAND RECORD FORMAT.....	102
FIGURE 49 - SLEEP STATE REQUEST COMMAND BLOCK FORMAT	103
FIGURE 50 - SLEEP STATE RESPONSE COMMAND BLOCK FORMAT.....	103
FIGURE 51 - ACTIVATION INDICATION COMMAND BLOCK FORMAT	104
FIGURE 52 - TRANSMIT POWER ADJUSTMENT COMMAND BLOCK FORMAT	104
FIGURE 53 - KEY REQUEST COMMAND FORMAT	104
FIGURE 54 - REQUEST KEY RESPONSE COMMAND FORMAT	104

FIGURE 55 - REQUEST KEY RESPONSE COMMAND FORMAT	105
FIGURE 56 - REQUEST KEY RESPONSE COMMAND FORMAT	105
FIGURE 57 - VENDOR SPECIFIC SECURITY INFORMATION FORMAT	105
FIGURE 58 - VENDOR SPECIFIC INFORMATION ELEMENT FORMAT	106
FIGURE 59 - STATION INFORMATION REQUEST COMMAND BLOCK FORMAT	106
FIGURE 60 - STATION INFORMATION RESPONSE COMMAND BLOCK FORMAT	106
FIGURE 61 - STATION INFORMATION BLOCK FORMAT	106
FIGURE 62 - DATA QUERY COMMAND BLOCK FORMAT	107
FIGURE 63 - CHANNEL STATE REQUEST COMMAND BLOCK FORMAT	107
FIGURE 64 - CHANNEL STATE RESPONSE COMMAND BLOCK FORMAT	107
FIGURE 65 - REMOTE CHANNEL SCAN REQUEST COMMAND BLOCK FORMAT	108
FIGURE 66 - REMOTE CHANNEL SCAN RESPONSE COMMAND BLOCK FORMAT	108
FIGURE 67 - CHANNEL INFORMATION BLOCK FORMAT	108
FIGURE 68 - APPLICATION SPECIFIC COMMAND FORMAT	109
FIGURE 69 - ASSOCIATION PROCESS	111
FIGURE 70 - INTER-FRAME SPACE IN THE ALLOCATED TIME SLOTS	114
FIGURE 71 - SUPERFRAME SYNCHRONIZATION	114
FIGURE 72 - STREAM CONNECTION PROCESS FOR SYNCHRONIZED DATA TRANSMISSION	116
FIGURE 73 - MESSAGE FLOW OF KEY DISTRIBUTION BETWEEN THE MASTER AND A STATION	129
FIGURE 74 - MESSAGE FLOW OF THE KEY DISTRIBUTION BETWEEN STATIONS	130
FIGURE 75 - MESSAGE FLOW OF KEY REQUEST BETWEEN A STATION AND A KEY ORIGINATOR	131
FIGURE 76 - CCM NONCE FORMAT	132
FIGURE 77 - SECURE BEACON FRAME FORMAT	132
FIGURE 78 - FORMAT OF SECURE COMMAND FRAME	132
FIGURE 79 - SECURE DATA FRAME FORMAT	133
FIGURE 80 - CCM INTEGRITY CODE GENERATION BLOCK	133
FIGURE 81 - INTEGRITY BLOCK B_0	133
FIGURE 82 - INTEGRITY BLOCK B_1	133
FIGURE 83 - INTEGRITY BLOCK B_2, ..., B_N	134
FIGURE 84 - DATA ENCRYPTION BLOCK	134
FIGURE 85 - ENCRYPTION BLOCK	134
FIGURE 86 - OPERATING FREQUENCY CHANNELS AT 2.4–2.4835GHz AND 5.725–5.825GHz	135
FIGURE 87 - PHY PROTOCOL DATA UNIT (PDU) FORMAT	137
FIGURE 88 - PREAMBLE FORMAT	138
FIGURE 89 - PHY HEADER	139
FIGURE 90 - LFSR GENERATING THE (15,10) SHORTENED HAMMING CODE	139
FIGURE 91 - LFSR CIRCUIT GENERATING THE HEC	140
FIGURE 92 - SCRAMBLER BLOCK DIAGRAM	141
FIGURE 93 - QPSK MODULATION	142
FIGURE 94 - RATE1 BLOCK DIAGRAM	143
FIGURE 95 - RATE2 BLOCK DIAGRAM	143
FIGURE 96 - RATE3 BLOCK DIAGRAM	144
FIGURE 97 - RATE4 BLOCK DIAGRAM	145
FIGURE 98 - PREAMBLE MODULATION	145
FIGURE 99 - HEADER MODULATION	145
FIGURE 100 - PAYLOAD MODULATION	146
FIGURE 101 - SIGNAL CONSTELLATION- OF QPSK	146
FIGURE 102 - ERROR VECTOR CALCULATION	148
FIGURE 103 - TRANSMIT POWER SPECTRUM MASK	149
FIGURE 104 - TRANSMITTER RF RESPONSE TIME	150

List of Tables

TABLE 1 - GENERAL MANAGEMENT PRIMITIVE OVERVIEW	15
TABLE 2 - MLME/PLME GENERAL MANAGEMENT PRIMITIVE PARAMETERS	15
TABLE 3 - MLME PRIMITIVE SUMMARY	17
TABLE 4 - MLME-RESET PRIMITIVE PARAMETERS	18
TABLE 5 - MLME-SCAN PRIMITIVE PARAMETERS	19
TABLE 6 - PICONETDESCRIPTION ELEMENTS	19
TABLE 7 - MLME-START PRIMITIVE PARAMETERS	21
TABLE 8 - MLME-SYNCH PRIMITIVE PARAMETERS	22
TABLE 9 - MLME-ASSOCIATE.PRIMITIVE PARAMETERS	24
TABLE 10 - MLME-DISASSOCIATE PRIMITIVE PARAMETERS	27
TABLE 11 - MLME-REQUEST-KEY PRIMITIVE PARAMETERS	29
TABLE 12 - MLME-DISTRIBUTE-KEY PRIMITIVE PARAMETERS	31
TABLE 13 - MLME-MEMBERSHIP-UPDATE PRIMITIVE PARAMETERS	34
TABLE 14 - MLME-SECURITY-ERROR PRIMITIVE PARAMETERS	34
TABLE 15 - MLME-SECURITY-MESSAGE PRIMITIVE PARAMETERS	35
TABLE 16 - MLME-MASTER-HANDOVER PRIMITIVE PARAMETERS	38
TABLE 17 - MLME-MASTER-INFO PRIMITIVE PARAMETERS	40
TABLE 18 - MLME-PROBE PRIMITIVE PARAMETERS	42
TABLE 19 - MLME-CREATE-STREAM, MLME-MODIFY-STREAM, MLME-TERMINATE-STREAM PRIMITIVE PARAMETERS	44
TABLE 20 - MLME-CHANNEL-STATUS PRIMITIVE PARAMETERS	48
TABLE 21 - MLME-REMOTE-SCAN PRIMITIVE PARAMETERS	50
TABLE 22 - REMOTE PICONETDESCRIPTION ELEMENTS	51
TABLE 23 - MLME-NETWORK-PARM-CHANGE PRIMITIVE PARAMETERS	53
TABLE 24 - MLME-TX-POWER-CHANGE PRIMITIVE PARAMETERS	55
TABLE 25 - MLME-SLEEP PRIMITIVE PARAMETERS	56
TABLE 26 - MAC PIB MASTER GROUP PARAMETERS	58
TABLE 27 - MAC PIB ATTRIBUTE GROUP PARAMETERS	59
TABLE 28 - MAC PIB AUTHENTICATION GROUP PARAMETERS	59
TABLE 29 - MAC PIB ASSOCIATION GROUP PARAMETERS	60
TABLE 30 - MAC PIB NETWORK SECURITY GROUP PARAMETERS	60
TABLE 31 - MAC SAP PRIMITIVE SUMMARY	61
TABLE 32 - MAC-ASYNC-DATA AND MAC-ISOCH-DATA PRIMITIVE PARAMETERS	61
TABLE 33 - PD-SAP PRIMITIVES	64
TABLE 34 - PD-SAP PARAMETERS	65
TABLE 35 - PLME-SAP PRIMITIVES	74
TABLE 36 - PLME-SAP PRIMITIVE PARAMETERS	74
TABLE 37 - PHYSICAL LAYER ENUMERATED VALUES	79
TABLE 38 - FRAME TYPES	83
TABLE 39 - USAGE CODES BY FRAME TYPE	86
TABLE 40 - BEACON FRAME BODY	87
TABLE 41 - SETTING THE CONTROL FIELD OF THE NON-SECURE BEACON FRAME	87
TABLE 42 - SETTING THE CONTROL FIELD OF THE SECURE BEACON FRAME	88
TABLE 43 - SETTING THE CONTROL FIELD OF THE BEACON FRAME	88
TABLE 44 - INFORMATION BLOCKS	91
TABLE 45 - COMMAND TYPES	96
TABLE 46 - ORDER OF PREFERENCE WHEN COMPARING CAPABILITY	99
TABLE 47 - MAC LAYER PARAMETERS	120
TABLE 48 - KEY SELECTION	125
TABLE 49 - CENTER FREQUENCIES OF CHANNELS AT 2.4GHZ AND 5.8GHZ	136
TABLE 50 - PHY LAYER TIMING PARAMETERS AT 2.4GHZ AND 5.8GHZ	136
TABLE 51 - INTERFRAME SPACE PARAMETER	136
TABLE 52 - CAZAC SEQUENCE	138

TABLE 53 - FORWARD ERROR CORRECTION 139

TABLE 54 - CONSTANT ENVELOPE CODING 140

TABLE 55 - DATA RATE ACCORDING TO MODULATION TYPE 146

TABLE 56 - PHY LAYER CONSTANTS 147

TABLE 57 - PIB CHARACTERISTICS GROUP PARAMETERS..... 147

TABLE 58 - TRANSMIT PSD LIMITS..... 149

TABLE 59 - TRANSMIT POWER 150

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 6, *Telecommunications and information exchange between systems*.

This second edition cancels and replaces the first edition (ISO/IEC 24771:2009), which has been technically revised.

Information technology — Telecommunications and information exchange between systems — MAC/PHY standard for ad hoc wireless network to support QoS in an industrial work environment

1 Scope

This International Standard defines a protocol for the physical layer (PHY) and the data link layer in order to construct a reliable and high-speed data transmission network between devices on industrial sites such as factories and plants. This network specification provides a standardized protocol to provide a framework for various industrial devices to establish a simple, low-cost, energy-efficient, and high-speed network between them. In order to fulfil the service requirements of the factories and large plants, this network specification is designed to enable devices to establish a network by themselves without help of any infrastructure and reliably exchange various kinds of data, including real-time audio and video data, between them. In addition to high transmission rates, Quality of Service (QoS) for multimedia data - such as video - is also provided.

The devices mentioned in this International Standard refer to equipment that is and can be used in industrial sites such as factories and automated assembly lines. Such devices include PLC (Programmable Logic Controller), and CNC (Computerized Numerical Controller) and manufacturing robots. However, beyond such conventional devices, devices mentioned in this International Standard include personal IT devices that workers may carry and use while working, including cellular phones, personal industrial digital assistants (PDA), and laptop PCs.

2 Normative references

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

ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

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

3 Terms and definitions, and abbreviations

3.1 Terms and definitions

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

3.1.1

Access control

control process to prevent unauthorized use of resources or bandwidth

3.1.2

Ad-hoc network

network that is spontaneously formed usually without system installation

NOTE Such networks are mainly characterized by time and space limitations.

3.1.3

Association

service used to connect authorized devices in the network

3.1.4

Authentication

device verification process allowing devices within the network to connect to one another

3.1.5

Camellia

128-bits secure block algorithm defined in the ISO/IEC 18033-3 standard

3.1.6

Coverage area

territory over which two devices can achieve acceptable quality and performance while exchanging data

3.1.7

Dissociation

service used in an established network

3.1.8

Frame

format of bits in a data exchange

3.1.9

K

prefix indicating multiplication by 1024

3.1.10

K μ s

unit of 1024 μ s

3.1.11

k

prefix indicating multiplication by 1000

3.1.12

Logical Channel

data link channel sitting distinctly above the physical layer

3.1.13

Master

station that manages the network by periodically transmitting a beacon frame

3.1.14**MAC Management Protocol data Unit****MMPDU**

data unit exchanged between two media access control apparatuses in order to implement the media access control management protocol

3.1.15**MAC Protocol data Unit****MPDU**

data unit exchanged between two media access control apparatuses by means of utilizing the physical layer services

3.1.16**MAC Service data Unit****MSDU**

data unit transmitted between media access control service access points

3.1.17**Mobile Device**

device that utilizes communication networks while in motion

3.1.18**Portable Device**

station that is normally portable but must be in a fixed location in order to link to the communication network

3.1.19**SEED**

128-bits secure block algorithm defined in the ISO/IEC 18033-3 standard

3.1.20**Slave**

station in the network other than the master

3.1.21**Station**

device that can operate according to this International Standard

3.2 List of Abbreviations

AES	advanced encryption standard
ARQ	automatic repeat request
ARQN	automatic repeat request N
ASN.1	abstract symbol notation 1
BER	bit error rate
CAP	contention access period
CBC	cipher block chaining
CBC-MAC	cipher block chaining-message authentication code
CCA	clear channel assessment

CCM	counter mode encryption and cipher block chaining message authentication code
CDMA	code division multiple access
CODEC	coder/decoder
CRC	cyclic redundancy check
CTS	clear to send
DA	destination address
DBPSK	differential binary phase shift keying
DCE	data communication equipment
DLL	data link layer
DOQPSK	differential offset quadrature phase shift keying
DQPSK	differential quadrature phase shift keying
FCS	frame check sequence
FEC	forward error correction
FER	frame error rate
HCS	header check sequence
IETF	internet engineering task force
IDU	interface data unit
IP	internet protocol
ISM	industrial scientific medicine
IWN	industrial wireless network
LAN	local area network
LFSR	linear feedback shift register
LLC	logical link control
LM	link manager
LME	layer management entity
LMP	link manager protocol
LSB	least significant bit
MAC	medium access control
Master	network coordinator
MC-CDMA	multi-code CDMA

MCDU	MAC command data unit
MCPDU	MAC command protocol data unit
MDF	management-defined field
MIB	management information base
MIC	message integrity code
MLME	MAC layer management entity
MPDU	MAC protocol data unit
MSB	most significant bit
MSC	message sequence chart
MSDU	MAC service data unit
MTU	maximum transmission unit
NID	network ID
PAN	personal area network
PAR	project authorization request
PDU	protocol data unit
PHY	physical layer
PIB	PAN information base
PLME	physical layer management entity
PN	pseudo noise
PPDU	PHY protocol data unit
PPM	parts per million
PRNG	pseudo random number generator
PSDU	PHY service data unit
QAM	quadrature amplitude modulation
QoS	quality of service
QPSK	quadrature phase shift keying
OQPSK	offset quadrature phase shift keying
RF	radio frequency
RFC	request for comments
RSSI	received signal strength indication

RTS	request to send
RTX	response timeout expired
RX	receive or receiver
SAP	service access point
SDP	service discovery protocol
SDU	service data unit
SEC	security
SECID	security identifier
SEQN	sequential numbering scheme
SFC	security frame counter
SME	station management entity
SQ	signal quality
SRC	short retry count
SRES	signed response
SS	station service
STN	station
TA	transmitter address
TCM	trellis coded modulation
TDD	time division duplex
TDMA	time division multiple access
TX	transmit or transmitter
TXE	transmit enable
WAN	wide area network
WLAN	wireless local area network
WM	wireless medium

4 Overview

This section defines the general attributes of the industrial wireless network and describes the attributes of the physical layer and data link layer. The physical layer is built upon a binary CDMA, and the data link layer is composed of the media access control (MAC) layer.

4.1 Characteristics

This International Standard is designed for the construction and management of an optimal network for industrial use applications.

4.1.1 Ad-hoc network

This International Standard is based upon an ad-hoc network that can be established even without a network infrastructure. A network is made up of two kinds of devices - a master and a slave, which are differentiated according to their functions. All stations can function as a master or a slave and one of them is selected as a master based on the device layout and its capabilities. An independent network structure is feasible without requiring infrastructure.

4.1.2 Quality of Service

The number of devices participating in an industrial wireless network changes vastly over time due to the channel conditions and industrial mobile device operation characteristics of a wireless environment. The bandwidth allocated to each device and the transmission delay time also have a significant effect, making it difficult to support real-time multimedia traffic services that require a certain quality of service.

This document requires one station in the network to be the master, which allocates and controls resources and thereby manages the connection quality of each network traffic.

4.1.3 Binary CDMA technology

This International Standard uses Binary-CDMA technology so that it has strong noise resistance, inherent advantage of CDMA, and has another good capability of changing bandwidth finely,

and thereby has the advantages of noise resistance and finely tuned and flexible resource allocation.

First, Binary-CDMA possesses superior noise resistance that is characteristic of CDMA technology, and this is an outstanding attribute in a wireless network environment which, unlike a wire-line network, has a high noise factor. In addition, the nature of Binary CDMA makes it possible to adjust the bandwidth by changing the number of codes used, thereby allowing flexible and finely-tuned resource allocation.

4.2 Components of network

The components of a network can be roughly depicted as shown in Figure 1. The primary component is the station. The first station trying to connect or establish a network becomes the master of the network and helps other stations to associate with it by periodically transmitting beacons. It also takes responsibilities such as quality of service and power management. The network is made up of two or more stations operating on the same wireless frequency channel in an industrial activity area.

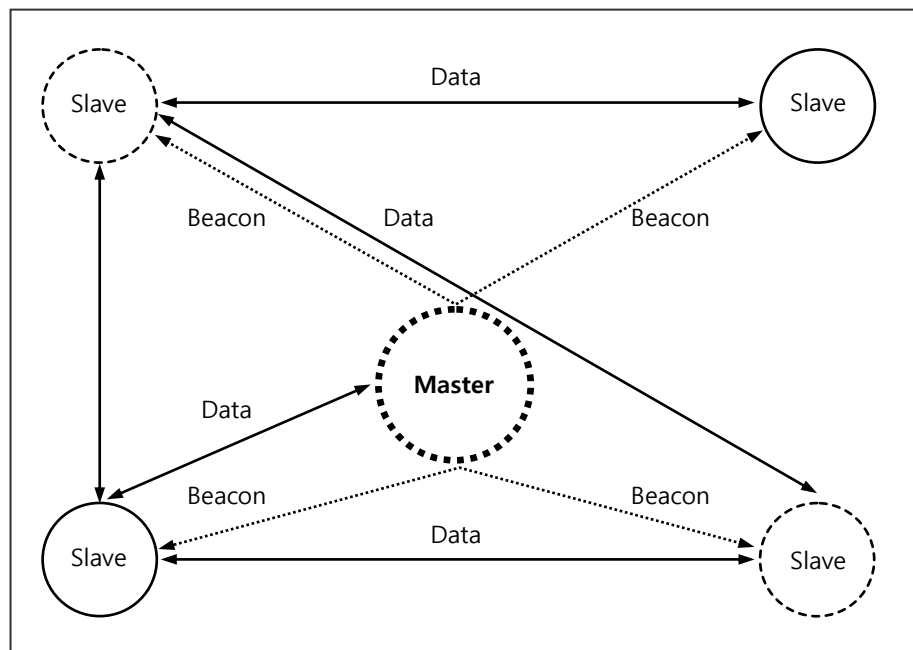


Figure 1- Network

4.2.1 Station

The station is the primary component of the network and is classified as either master or slave depending on its role. The master assumes full management, and no more than one can exist in a particular network. The master controls slaves by broadcasting beacons. Slaves send or receive data as directed by the master. To acquire time slots for data transfer, slaves make resource allocation requests to the master during the contention period.

4.2.2 Resources

Stations in the network should acquire time slots from master to perform their aimed job – exchanging data. After a station acquired rights to use some time slots from master, it can transmit frames exclusively during assigned time slots. In this sense, this International Standard depicts time slots as resources, which can be shared and/or competed among stations in the network. Time slots are supervised by the master and are distributed according to requests from slaves at the discretion of the master.

4.3 Functional overview

The media access control layer provides the following services:

- Network synchronization
- Data transmission
- Power management
- Master handover
- Security
- Data transport with quality of service (QoS)

Data transmission and reception between stations are possible under different standards of quality of service.

4.3.1 Network synchronization

The network is established once the master transmits the beacon frame. The beacon frame contains the status information of the network, and all slaves in the network use this information to sync with the network. The superframe is roughly composed of three parts as shown in Figure 2, and each period has a variable length. (The allocation period must be a multiple of the timeslot length.)

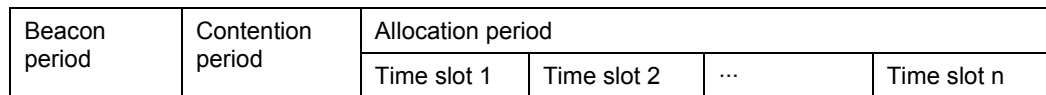


Figure 2 - Superframe

- a) beacon period: the master transmits the beacon frame containing the network status information to the slaves.
- b) contention period: the slaves and master send command frames such as associate/disassociate/grant frames, resource request/grant frames, and connect request/grant frames in a random access fashion.
- c) allocation period: this is divided into multiple time slots, each allotted for one station. The station receiving the time slot can send synchronous/asynchronous data or command frames during that interval.

4.3.2 Data transmission

For data transmission, two types of connections – synchronous and asynchronous - are supported. Asynchronous connections, which have minimal overhead when establishing connections but do not have a guaranteed bandwidth, are primarily used when transmitting general data that is relatively insensitive to delays. Synchronous connections, which carry a large overhead when establishing connections but have a guaranteed bandwidth, are used to transmit data for real-time services such as audio and video.

This International Standard manages communication quality in three characteristics – delay, data rate, BER. Each device defines the communication quality of data stream to send in these three parameters and sends the defined quality parameters to master to get channel time allocation. Master collects communication request from slaves and allocate time slots to streams in order that each stream can be transmitted satisfying each one's needed communication quality. Afterward a master monitors quality of communication of stream to check whether it meets initial QoS request. If the communication quality deteriorates below initial request quality, master changes time slot allocation to meet initial QoS request.

This International Standard covers MAC-to-MAC QoS within 1-hop network that MAC layer can control.

4.3.2.1 QoS parameter

Data transfers in this International Standard are differentiated as streams which are largely divided into synchronous stream and asynchronous stream, depending on whether a stream has QoS characteristic or not. Synchronous stream has 3 QoS parameter – Period, Data size to transmit per each period, BER, while asynchronous stream have only data size as a parameter.

Synchronous stream in this International Standard manages QoS with the following three parameters.

- Period: the period with which master allocates time slot. Each device is assigned at least a time slot within this period so that this value is equal to maximum delay.
- Data size to transmit per each period: the size of data that a slave will send during each period. Combined with period, this value decides data rate.
- BER: This value defines quality of communication in Bit Error Rate

Using above QoS parameters, devices can define their communication request with detail characteristics.

4.3.2.2 Maintenance of QoS

A master of a network manages communication resource (time slots) centrally. Master collects network information (usage status of allocated time slots, channel quality of each channel) and communication request by itself or from slaves and allocates time slots to slaves in order that each communication can meet its QoS request. After allocating time slots, a master checks whether each communication meets its initial QoS request. If communication does not meet its QoS requirements, a master makes communication to meet its initial requirements by using the following actions.

4.3.2.2.1 Check and estimation of wireless channel environment

Master continuously monitors BER and SNR value of current wireless channel environment. When it detects the serious change of channel environment, a master takes an action to counterpart the change such as data rate change or frequency channel change

4.3.2.2.2 Dynamic link quality control

A master continuously monitors actual communication status of data streams in a network. When a communication quality of a stream goes worse than its pre-determined level, a master changes resource allocations in order that the communication quality should meet its pre-determined level. To increase communication quality of a stream, a master decreases data rate of the stream and allocates more time slots to compensate reduced data rate through resource allocation and change mechanism.

4.3.2.2.3 Dynamic channel selection and change

When a master estimates that the network-wide communication quality of the current frequency channel goes worse than the acceptable level, it decides to change a frequency channel. Master notifies the new channel where network will be re-established to slaves, slaves leave current frequency channel and rejoin at the notified new channel. This function provides not only the ability to maintain the certain network-wide communication quality, but also interoperability to avoid collision with other kinds of wireless network.

4.3.3 Security

This standard use 128-bits secure block algorithms such as ISO/IEC18033-3 encryption algorithms and regional regulated secure block algorithms. Security for the network is one of three modes as follows:

a) Mode 0—open

Security membership is not required and payload protection (both data integrity and data encryption) is not used by the MAC. The master is allowed to use a list of slaves' addresses to admit or deny entry to the network.

b) Mode 1— inclusive CCM secure membership and payload protection

Stations establish secure membership with the master before they have access to the network's resources. Data sent in the network is allowed to use payload protection (data integrity and/or data encryption). Data integrity is required for most of the frames that are sent in the network through the inclusive CCM security mode based on secure block algorithms. Non-secure frames shall be used to communicate between a station using security mode 0 and a station using security mode 1.

c) Mode 2—exclusive CCM secure membership and payload protection

A device operating in security mode 2 shall not establish a secure relationship with devices operating in either security mode 0 or security mode 1. Stations establish secure membership with the master before they have access to the network's resources. Data sent in the network is allowed to use payload protection (data integrity and/or data encryption). When security mode 2 is enabled (the network adopts security mode 2), the exclusive CCM security mode based on secure block algorithms shall be used to communicate among the stations using security mode 2.

When security is enabled, stations that wish to join the network are required to establish secure membership with the master. The stations are also allowed to establish a secure relationship with other stations for secure communications. A station has established a secure membership or a secure relationship when it gets a management key for the security relationship. The process of establishing secure membership or a secure relationship is outside of the scope of this standard. The master or station that generates and distributes the key is called the key originator.

The payload protection protocol, as described in 8.5, uses a symmetric key that is generated by the key originator and is securely distributed to stations that have established secure membership or a secure relationship with the key originator, as described in 8.4.

4.3.4 Power management

In order to support mobile devices, efficient power management is critical. Each station is notified of the presence and timing of the incoming data during the corresponding superframe by means of the beacon frame, and can reduce power consumption by disabling the physical layer when not transmitting data. During a particular superframe, stations that are not transmitting data can be disabled until the next superframe period starts. Stations receiving data are enabled only during beacon periods and intervals during which they receive frames. Stations sending data or making requests are enabled during intervals when there is data to transmit.

4.3.5 Master handover

The master can decide whether to appoint another slave as the master based on the information it possesses about each slave's capabilities. If a newly connected station is determined to be better for the master, the master role may be handed over. Also, due to the nature of an ad-hoc network, the master may unexpectedly cease operating or depart from the established service area. In such an event, one of the remaining slaves which is most suitable for the master is selected to manage the network.

4.4 Summary of operations

The superframe is divided into the beacon period, contention period, and allocation period, and the stations operate in different modes depending on the period.

4.4.1 Broadcasting during the beacon period

During the beacon period the master broadcasts a beacon frame to all slaves. The beacon frame includes information about the status and resource availability of the network, and the slaves receiving the beacon frame use this information to verify the correctness of the corresponding superframe as well as the allocated resources.

The master places network status information into the beacon frame and sends it out to all slaves.

4.4.2 Random access during the contention period

During the contention period the slave and master communicate via the CSMA/CA scheme. Slave sends command frames such as resource allocation requests to the master during this period, and the master sends back an acknowledgement or response frame.

4.4.3 Exclusive access during the allocation period

During the allocation period, only the stations permitted by the master can communicate using the time slot and code assigned to them in the beacon frame. The master evaluates the currently available resources and decides whether or not to grant the slave's service request and allocate the resources. Data services that use asynchronous connections receive acknowledgements for the dispatched frames by default, and synchronous connections receive acknowledgements selectively.

4.5 Summary of states

A station has the following operational states.

- establishing the network
- associating with the network
- security membership and key establishment
- data transfer
- master handover
- disassociating from the network
- terminating the network

4.5.1 Establishing the network

The master establishes the network by filling a beacon frame with synchronization information such as the length of the superframe, contention period, and allocation period, and sending it out. The beacon frame includes the network ID as well as synchronization information, enabling the stations to identify the network they will connect with.

4.5.2 Associating with the network

Stations attempting to associate with the network periodically scan each frequency channel to listen for the beacon frame from the master. If the received frame is the beacon frame for the desired network, the process of associating with the relevant network's master is started, and if this succeeds, the link to the network is established.

When the station associates with the network, it sends its own capability information to the master. This capability information contains such information as the physical layer data transfer rate that can be supported, power management status, ability to function as the master, and size of memory, and based on this information the master may decide to initiate the process of changing the master.

4.5.3 Security membership and key establishment

Security mechanisms provided by this standard allow security services to be implemented to control the admission of stations into a security relationship between the master and a station or between two ordinary stations and protect the information and integrity of communications between stations in a security relationship. This standard also provides a symmetric cryptography mechanism to assist in providing security services. Additional security services need to be provided by the higher layers to ensure proper management and establishment of the symmetric keys used in this standard.

4.5.4 Data transfer

A slave to send data first requests resources for the transmission from the master during the contention period, and once it is allocated to the resources it uses them to send the data. Data transfer is possible between any stations – not only between master and slave, but also between slaves themselves. The master is involved only during the initial resource allocation process, thus enabling the stations to exchange data freely afterwards.

4.5.5 Master handover

The nature of an ad-hoc network entails frequent changes of the master. The following cases are the two most likely scenarios.

- The current master is no longer able to service requests. (For example, it cannot meet the decided quality of service.)
- The master abruptly vanishes from the network. (It loses power or moves out of the network.)

4.5.6 Disassociating from the network

Stations currently associated with the network can disassociate from the network either spontaneously or at the will of the master.

In the case of spontaneous disassociation, the station sends a disassociate request to the master. If the master wants to disassociate from the network, it first hands over the master role to the most capable slave among the stations before disassociating.

If a certain slave is having trouble in receiving service due to network conditions, the master can forcibly disassociate it by sending a disassociate command.

4.5.7 Terminating the network

Terminating of the network can be categorized in two ways: normal termination by station request and abnormal termination due to unexpected events.

Normal termination refers to the case where the master receives the request from a slave, decides whether or not to terminate, then broadcasts this decision to all slaves, thereby dissolving the network. The master can also initiate this request.

Abnormal termination of the network refers to cases where the network is dissolved due to situations such as a network-wide power outage or exodus out of the industrial coverage area. However, such occurrences are highly unlikely.

5 Inter-layer interfaces

5.1 Summary

Both the MAC layer and the physical layer conceptually have management entities, called the MAC Layer Management Entity (MLME) and the Physical Layer Management Entity (PLME) respectively. These entities provide a service interface for layer management functions.

The physical layer provides an interface between the MAC sublayer and the wireless channel by means of the PHY firmware and the PHY hardware. The physical layer includes a conceptual management entity called a PLME. This entity provides a service interface by means of layer management functions. The PLME maintains a database for managed objects in the physical layer, also called the PAN information base (PIB). The Device Management Entity (DME) is a layer independent from the other management entities and its functionality is beyond the scope of this International Standard. Simply stated, however, it is responsible for the inter-layer interfaces providing device management functions. The physical layer provides services through two Service Access Points (SAP). Data services are provided through the PD-SAP and management services are provided through the PLME-SAP. In addition, the physical layer provides DME-PLME-SAP interface, which is equivalent to the PLME-SAP interface except that it operates through DME rather than MLME.

In order for the MAC to operate correctly, each station must possess a Device Management Entity (DME). DME exists in each layer and is layer-independent. The functions of DME are beyond the scope of this International Standard and vary depending on implementation, but in general they carry out tasks such as receiving data from a layer or initializing another layer. Generally DME acts under the direction of a higher-level management application. Figure 3 shows the relationships between the various management entities.

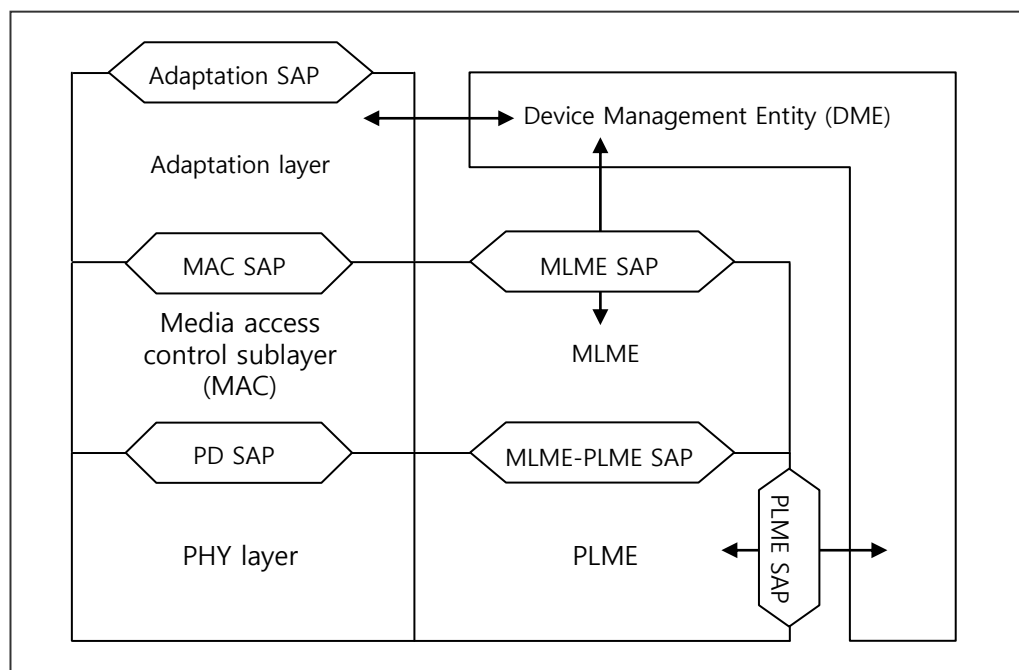


Figure 3 - Protocol stack configuration

5.2 General format of management primitives

Each sublayer's specific management information is organized into the relevant PAN information base (PIB). Corresponding to the PIB of the PAN, the LAN/MAN contains the management Information Base (MIB) that operates according to the Simple Network Management Protocol (SNMP). However, since management within Network is restricted to an individual network (i.e. one network does not interfere in the management of another) the PIB is used to define the specifications of each sublayer.

MLME and PLME are assumed to have a PIB for each sublayer, and the management primitives of the PIB are exchanged by means of management SAPs. The manager can “GET” or “SET” the value of the PIB attribute via the primitives. The “SET” request primitive can also trigger certain actions within the relevant layer.

A “GET” or “SET” primitive may be expressed in the form of a request accompanying a confirm primitive. Such primitives have the prefix MLME or PLME depending on whether the point of exchange is the MAC SAP or the PD SAP. DME utilizes the services provided by MLME through the MLME SAP.

In Table 1, “XX” stands for “MLME” or “PLME”, and the parameters of the primitives are defined in Table 2.

Table 1 - General management primitive overview

Name	Request	Confirm
XX-GET	Refer to 5.2.1	Refer to 5.2.2
XX-SET	Refer to 5.2.3	Refer to 5.2.4

Table 2 - MLME/PLME general management primitive parameters

Name	Type	Valid range	Description
PIBAttribute	octet string	Any PIB attribute	PIB attribute name
PIBValue	variable		PIB value
ResultCode	enumeration	SUCCESS, INVALID_PIB_ATTRIBUTE, READ_ONLY_PIB_ATTRIBUTE, WRITE_ONLY_PIB_ATTRIBUTE	Result of MLME or PLME request

5.2.1 MLME-GET.request and PLME-GET.request

These primitives request information about the relevant MAC PIB or PHY PIB. The semantics of these primitives are as follows.

XX-GET.request (

PIBAttribute

)

The primitive parameters are defined in Table 2.

5.2.1.1 Time of creation

DME and MLME (in the case of a PLME-GET.request) create these primitives to retrieve information from the MAC or PHY PIB.

5.2.1.2 Effect

The relevant management entity fetches the requested PIB attribute from the database and returns the value as the result of XX-GET.confirm.

5.2.2 MLME-GET.confirm and PLME-GET.confirm

These primitives return the result of an information request to the relevant MAC PIB or PHY PIB. The semantics of these primitives are as follows.

```
XX-GET.confirm (
    Status,
    PIBattribute,
    PIBattributevalue
)
```

The primitive parameters are defined in Table 2.

5.2.2.1 Time of creation

DME or MLME (in the case of a PLME-GET.confirm) create these primitives in response to an XX-GET.request.

5.2.2.2 Effect

If the status is SUCCESS, these primitives return the value of the relevant PIB attribute, otherwise they return the error code in the status field. Valid error status values include INVALID_PIB_ATTRIBUTE and WRITE_ONLY_PIB_ATTRIBUTE.

5.2.3 MLME-SET.request and PLME-SET.request

These primitives attempt to set the value of the relevant MAC PIB or PHY PIB attribute to the specified parameter. The semantics of these primitives is as follows.

```
XX-SET.request (
    PIBattribute,
    PIBattributevalue
)
```

The primitive parameters are defined in Table 2.

5.2.3.1 Time of creation

These primitives are created when DME or MLME (in the case of PLME-SET.request) tries to set the relevant MAC/PHY PIB attribute.

5.2.3.2 Effect

The relevant management entity tries to alter the value of the PIB attribute in the database. If the PIB is a reference to certain actions, this is interpreted as a request to execute the action. The management entity that receives this command responds by returning the result through a call to XX-SET.confirm.

5.2.4 MLME-SET.confirm and PLME-SET.confirm

These primitives return the result of the attempt to set the MAC PIB or PHY PIB attribute. The semantics of this primitive are as follows.

```

XX-SET.confirm (
    Status,
    PIBattribute
)

```

The primitive parameters are defined in Table 2.

5.2.4.1 Time of creation

DME or MLME (in the case of PLME-SET.confirm) create these primitives in order to respond to the XX-SET.request.

5.2.4.2 Effect

If the Status is SUCCESS, this means that the PIB attribute was set to the requested value. Otherwise, the Status field shows the error description. If the specified PIB attribute refers to a certain action, the primitive represents the success or failure of the execution of that action. Possible error status values include INVALID_PIB_ATTRIBUTE and READ_ONLY_PIB_ATTRIBUTE.

5.3 MLME SAP

In this subclause, the services that MLME provides to DME are defined. These definitions are conceptual and do not specify a certain implementation or external interface.

The MLME SAP primitive generally follows the format of an ACTION.confirm in response to an ACTION.request. The ACTION.indication is used to inform DME of events from other stations, and the station selectively sends an ACTION.response to the indication. DME uses the services provided by MLME through MLME SAP, and those primitives are outlined in Table 3.

Table 3 - MLME primitive summary

Name	Request	Indication	Response	Confirm
MLME-RESET	5.3.1.1			
MLME-SCAN	5.3.2.1			5.3.2.2
MLME-START	5.3.3.1			5.3.3.2
MLME-SYNCH	5.3.4.1			5.3.4.2
MLME-ATP-EXPIRED		5.3.4.3		
MLME-ASSOCIATE	5.3.5.1	5.3.5.2	5.3.5.3	5.3.5.4
MLME-STN-ASSOCIATION-INFO		5.3.5.5		
MLME-DISASSOCIATE	5.3.6.1	5.3.6.2		5.3.6.3
MLME-MASER-HANDOVER	5.3.10.1	5.3.10.2	5.3.10.3	5.3.10.4
MLME-MASTER-INFO	5.3.11.1	5.3.11.2	5.3.11.3	5.3.11.4
MLME-PROBE	5.3.12.1	5.3.12.2	5.3.12.3	5.3.12.4
MLME-CREATE-STREAM	5.3.13.10			5.3.13.2
MLME-MODIFY-STREAM	5.3.13.3			5.3.13.4
MLME-TERMINATE-STREAM	5.3.13.5	5.3.13.6		5.3.13.7

MLME-CHANNEL-STATUS	5.3.14.1	5.3.14.2	5.3.14.3	5.3.14.4
MLME-REMOTE-SCAN	5.3.15.1	5.3.15.2	5.3.15.3	5.3.15.4
MLME-NETWORK-PARM-CHANGE	5.3.16.1			5.3.16.2
MLME-TX-POWER-CHANGE	5.3.17.1	5.3.17.2		5.3.17.3
MLME-SLEEP	5.3.18.1	5.3.18.2	5.3.18.3	5.3.18.4

5.3.1 Reset

This mechanism describes the process of resetting the MAC. The parameters of this primitive are defined in Table 4.

Table 4 - MLME-RESET primitive parameters

Name	Type	Valid range	Description
SetDefaultPIB	boolean	TRUE, FALSE	If TRUE, all PIB attributes are reset to their default values. If FALSE, the MAC is reset but all PIB values remain what they were prior to the execution of the MLME-RESET.request primitive
ResetTimeout	duration	0 ~ 65535	The time in which the reset process must be completed, in msec

5.3.1.1 MLME-RESET.request

This primitive requests a reset of the MAC entity. The semantics are as follows.

```
MLME-RESET.request  (
                        SetDefaultPIB,
                        ResetTimeout
                      )
```

The primitive parameters are defined in Table 4.

5.3.1.1.1 Time of creation

DME sends this message to MLME to restore the MAC to its initial state.

5.3.1.1.2 Effect

When the primitive is received, if the station is associated with the current network, MLME sends a disassociate request command to the master (see 6.5.1.3). In all cases, the slave MLME sets the MAC to its initial state, and resets all variables but is still consistent with the SetDefaultPIB (see Table 4).

When the master MLME receives this primitive, it behaves the same way as a slave MLME, except for cases when it has been disassociated from the network after transferring the master role or is performing a shutdown of network.

If the ResetTimeout occurs while MLME is still executing network disassociations, master handover, or network shutdown, MLME resets the MAC and cancels the interrupted process.

5.3.2 Scan

This mechanism determines the existence of the network in the communication channel. The parameters of this primitive are defined in Table 5.

PiconetDescriptionSet is the set of PiconetDescriptions, and a PiconetDescription is composed of the elements in Table 6.

Table 5 - MLME-SCAN primitive parameters

Name	Type	Valid range	Description
OpenScan	boolean	TRUE, FALSE	Whether or not the scan is open (an open scan refers to search for any beacon frame)
NID	integer	0-65535	ID of the specific network to scan
ChannelList	Array of integers	0 – maximum channels supported by the physical layer	List of channels to search during a scan
Channel scanDuration	time	0-65535	The time it takes for the station to scan one channel
NumberOfNetworks	integer	0-255	Number of discovered networks (number of PiconetDescriptions in the PiconetDescriptionSet)
PiconetDescriptionSet	Network Description set	As defined in Table 6	The set of all attributes of the discovered networks, returned as the result of a scan request
NumberOfChannels	integer	0 - maximum channels supported by the physical layer	Number of channels to scan
ChannelRating List	Array of integers	0- maximum channels supported by the physical layer	List of channels sorted by quality (best to worst)
ResultCode	enumeration	SUCCESS, INVALID_PARAMETERS	Result of MLME request

Table 6 - PiconetDescription elements

Name	Type	Valid range	Description
MasterSTNAddress	MACAddress	all MACAddress	MACAddress of the master of the discovered network
NID	As defined in Table 5	As defined in Table 5	NID of the discovered network
ScannedFrameType	enumeration	BEACON, NON-BEACON	Type of the discovered frame
ChannelIndex	integer	0-255	Index of frequency channel on which the network was discovered
SuperframeDuration	time	0-65536	Length (msec) of the superframe of the discovered

ration			network
CPEndTime	integer	0-65525	The end time of the contention period of the discovered network

5.3.2.1 MLME-SCAN.request

This primitive requests a scan of the MAC entity. The semantics are as follows.

```
MLME-SCAN.request    (
    OpenScan,
    NID,
    ChannelList
    Channel scanDuration
)
```

The primitive parameters are defined in Table 5.

5.3.2.1.1 Time of creation

When a manual SCAN is initiated for a search of a specified NID or an arbitrary NID of a network, DME sends this message to MLME.

5.3.2.1.2 Effect

When MLME receives this primitive from DME, it executes a manual SCAN of the channels in the Channel List. When this SCAN is completed, MLME responds to DME with the result of the SCAN through a call to MLME-SCAN.confirm.

5.3.2.2 MLME-SCAN.confirm

This primitive and its parameters are collected during the SCAN and sent back upon the completion of the SCAN. The semantics are as follows.

```
MLME-SCAN.confirm    (
    NumberOfNetworks,
    PiconetDescriptionSet,
    NumberOfChannels,
    ChannelRatingList,
    ResultCode
)
```

The primitive parameters are defined in Table 5.

5.3.2.2.1 Time of creation

This message is sent to DME when MLME completes the requested SCAN or when the parameters of MLME-request are incorrect.

5.3.2.2.2 Effect

DME sends a notification of the result of the SCAN process.

5.3.3 Startup of network

This mechanism supports the process of creating a new network. The parameters used in this primitive are outlined in Table 7.

Table 7 - MLME-START primitive parameters

Name	Type	Valid range	Description
NID	As defined in Table 5	As defined in Table 5	new network NID
ChannelIndex	As defined in Table 6	As defined in Table 6	Index of frequency channel on which to create network
SuperframeDuration	As defined in Table 6	As defined in Table 6	As defined in Table 6
PiconetMaxTxPower	As defined in 6.4.7	As defined in 6.4.7	As defined in 6.4.7
ResultCode	enumeration	SUCCESS, ALREADY_STARTED, NETWORK_DETECTED, INVALID_PARAMETER, CHANNEL_INTERFERENCE	Result of MLME request

5.3.3.1 MLME-START.request

This primitive requests the creation of a new network to the MAC entity. The semantics are as follows.

```
MLME-START.request  (
    NID,
    ChannelIndex,
    SuperframeDuration,
    PiconetMaxTXPower
)
```

The primitive parameters are defined in Table 7.

5.3.3.1.1 Time of creation

This is created when DME requests that a station become the master and startup a new network.

5.3.3.1.2 Effect

MLME begins the creation process described in 7.1, and invokes MLME-START.confirm to report the result.

5.3.3.2 MLME-START.confirm

This primitive reports the result of the network creation.

```
MLME-START.confirm    (
                        ResultCode
                        )
```

The primitive parameters are defined in Table 7.

5.3.3.2.1 Time of creation

This is created as a result of an MLME-START.request from DLME.

5.3.3.2.2 Effect

DME reports the result of the creation process of network. A ResultCode of SUCCESS indicates that the station is now the master. If all channels have already been taken by another Network, the ResultCode is set to NETWORK_DETECTED. If network is already started, ResultCode is set to ALREADY_STARTED. If network cannot be started because the noise on the frequency channel indicated for the startup is too severe, the ResultCode is set to CHANNEL_INTERFERENCE. If there is an error in a parameter, the ResultCode is set to INVALID_PARAMETERS.

MLME begins the creation process described in 7.1, then calls MLME-START.confirm to report the result.

5.3.4 Synchronization

This mechanism is a preparatory step for a station to network. This primitive also notifies DME when a station has gone out-of-sync. The primitive parameters are defined in Table 8.

Table 8 - MLME-SYNCH primitive parameters

Name	Type	Valid range	Description
NID	As defined in Table 5	As defined in Table 5	ID of network to sync
ChannelIndex	As defined in Table 6	As defined in Table 6	The frequency channel on which to search network
Channel scan-Duration	As defined in Table 5	As defined in Table 5	Time to scan network
ResultCode	enumeration	SUCCESS, TIMEOUT, INVALID_PARAMETER	Result of MLME-SYNCH.request

5.3.4.1 MLME-SYNCH.request

This primitive initiates the process of synchronizing with a network. The semantics are as follows.

```
MLME-SYNCH.request    (
```

```

        NID,
        ChannelIndex,
        ChannelScanDuration
    )

```

The primitive parameters are defined in Table 8.

5.3.4.1.1 Time of creation

DME creates this when initiating the process of synchronizing with a specific beacon.

5.3.4.1.2 Effect

When MLME receives this primitive from DME, MLME scans until it finds the beacon corresponding to the specific channel or the channel scan duration time is exceeded. If the desired beacon is found, an MLME-SYNCH.confirm is sent to DME with the ResultCode set to SUCCESS. If the channel scan duration time limit is exceeded the ResultCode is set to TIMEOUT.

5.3.4.2 MLME-SYNCH.confirm

This primitive notifies DME of the success or failure of the requested network synchronization. The semantics are as follows.

```

MLME-SYNCH.confirm    (
                        ResultCode
                        )

```

The primitive parameters are defined in Table 8.

5.3.4.2.1 Time of creation

MLME creates this when the requested network synchronization task is completed.

5.3.4.2.2 Effect

DME is notified of the result of the synchronization task.

5.3.4.3 MLME-ATP-EXPIRED.indication

This primitive indicates that the station is no longer able to hear the beacon. The semantics are as follows.

```

MLME-ATP-EXPIRED.indication    ()

```

5.3.4.3.1 Time of creation

An MLME other than the master creates this when it has been unable to receive a beacon for longer than the Association Timeout Period (ATP).

5.3.4.3.2 Effect

DME receives notice that the ATP has timed out.

5.3.5 Association

The following primitives support the association of stations to network. The primitive parameters are defined in Table 9.

Table 9 - MLME-ASSOCIATE.primitive parameters

Name	Type	Valid range	Description
OrigID	integer	Valid addresses as defined in 6.2.1.3	The address to associate or the address assigned by the master
STNAddress	MACaddress	Valid MACaddress	The MACaddress of the station sending the associate request
CapabilityField	As defined in 6.4.5	As defined in 6.4.5	The capability of the station sending the associate request to the master
Association-TimeoutPeriod	duration	As defined in 6.5.1.1	Maximum association time as defined in 6.5.1.1
Max-Associations	integer	0-255	Maximum number of stations that the master can manage
MaxRRBs	integer	0-255	The maximum number of resource request blocks that the master can manage
TxPowerLevel	As defined in 6.4.7	As defined in 6.4.7	As defined in 6.4.7
STNID	integer	Valid address as defined in 6.2.1.3	If the association is successful, the assigned address of the station, otherwise the assigned association address
Association-Status	enumeration	DISASSOCIATED, ASSOCIATED	Indication of whether the station is newly associating or disassociating
AssocTimeout	time	0-65535	The time in which MLME must receive a reply to the associate request
ReasonCode	integer	As defined in 6.5.1.2	The explanation for the reply to the associate request
ResultCode	enumeration	SUCCESS, DENIED, NEIGHBOR_UNSUPPORTED, TIMEOUT	Indication of whether or not the request was granted or denied, or whether the timeout was exceeded

5.3.5.1 MLME-ASSOCIATE.request

This primitive initiates the association process with a network. The semantics are as follows.

```
MLME-ASSOCIATE.request      (
                                PiconetType,
                                CapabilityField,
                                AssociationTimeoutPeriod,
                                MAXRRBs,
                                TxPowerLevel,
                                NetworkserviceInquiry,
```

AssocTimeout

)

The primitive parameters are defined in Table 9.

5.3.5.1.1 Time of creation

This is created when DME attempts to associate with network.

5.3.5.1.2 Effect

When DME receives this primitive through the MLME-SAP, it creates an associate request command frame and sends it to the master MLME.

5.3.5.2 MLME-ASSOCIATE.indication

This primitive reports that an associate request frame has been received.

```
MLME-ASSOCIATE.indication    (
                                OrigID,
                                STNAddress,
                                CapabilityField,
                                AssociationTimeoutPeriod,
                                MaxAssociations
                                )
```

The primitive parameters are defined in Table 9.

5.3.5.2.1 Time of creation

This is created to notify DME that the master MLME has received an associate request frame from a currently unassociated station.

5.3.5.2.2 Effect

When DME receives this primitive, if the OrigID is the UnassocID, DME determines whether to grant the associate request of the station, and sends back the result via MLME-ASSOCIATE.response through MLME-SAP.

When DME receives this primitive, if OrigID is the STNID that has just been assigned to the station desiring association, the master is being notified that the station has successfully received the assigned STNID, and does not reply with MLME-ASSOCIATE.response.

5.3.5.3 MLME-ASSOCIATE.response

This primitive is created as a response to an MLME-ASSOCIATE.indication. The semantics are as follows.

```
MLME-ASSOCIATE.response    (
                                OrigID,
                                STNAddress,
```

```

        AssociationTimeoutPeriod,
        ReasonCode
    )

```

The primitive parameters are defined in Table 9.

5.3.5.3.1 Time of creation

This is created when the master MLME receives an MLME-ASSOCIATE.indication.

5.3.5.3.2 Effect

When the master MLME receives this primitive from DME, it creates an association response frame and sends it back.

5.3.5.4 MLME-ASSOCIATE.confirm

This primitive informs DME that initiated the association whether the associate request was successfully carried out. The semantics are as follows.

```

MLME-ASSOCIATE.confirm    (
        STNID,
        AssociationTimeoutPeriod,
        ReasonCode,
        ResultCode
    )

```

The primitive parameters are defined in Table 9.

5.3.5.4.1 Time of creation

MLME sends this to DME when the association is completed or the timeout is exceeded.

5.3.5.4.2 Effect

The DME that initiated the association receives this primitive and determines whether the associate request was successfully carried out. If successful, it receives a unique STNID, otherwise it remains in an unassociated state with no unique STNID.

5.3.5.5 MLME-STN-ASSOCIATION-INFO.indication

This primitive informs all associated stations in network of the station association information in the beacon. The semantics are as follows.

```

MLME-STN-ASSOCIATION-INFO.indication (
        STNAddress,
        STNID,
        AssociationStatus
    )

```

)

The primitive parameters are defined in Table 9.

5.3.5.5.1 Time of creation

MLME sends this to DME when it receives the beacon containing the association information of other stations.

5.3.5.5.2 Effect

DME collects information about the station that has just been associated or disassociated from network through this primitive.

5.3.6 Disassociation

The following primitives are used when a station is disassociated from network or when the master is trying to disassociate a station. The primitive parameters are defined in Table 10.

Table 10 - MLME-DISASSOCIATE primitive parameters

Name	Type	Valid range	Description
TrgtID	integer	Valid addresses as defined in 6.2.1.3	Address of destination station of MLME request
OrigID	integer	Valid addresses as defined in 6.2.1.3	Address of station initiating the MLME request
DisassocTimeout	time	0-65535	Time in which the task must be completed once the MLME disassociate request is made
ReasonCode	integer	As defined in 6.5.1.2	Reason for disassociate request
ResultCode	enumeration	SUCCESS, ACK_TIMEOUT	Result of MLME request

5.3.6.1 MLME-DISASSOCIATE.request

This primitive initiates the disassociate request. The semantics are as follows.

```
MLME-DISASSOCIATE.request  (
                                TrgtID,
                                ReasonCode,
                                DisassocTimeout
                              )
```

The primitive parameters are defined in Table 10

5.3.6.1.1 Time of creation

DME sends this to MLME when attempting to start the disassociation process.

5.3.6.1.2 Effect

When the slave MLME receives this primitive, the slave MLME sends a disassociate request command to the master DME.

When the master MLME receives this primitive, it sends a disassociate request command to the DME of the station to disassociate.

5.3.6.2 MLME-DISASSOCIATE.indication

This primitive reports that a disassociate request frame has been received. The semantics are as follows.

```
MLME-DISASSOCIATE.indication (
    OrigID,
    ReasonCode
)
```

The primitive parameters are defined in Table 10.

5.3.6.2.1 Time of creation

MLME sends this to DME when the master or a station receives a disassociate request frame.

5.3.6.2.2 Effect

The target DME is notified of the reason for the disassociate request.

5.3.6.3 MLME-DISASSOCIATE.confirm

This primitive reports the result of the disassociate request. The master MLME receives notification of the station to disassociate by means of this primitive. The semantics are as follows.

```
MLME-DISASSOCIATE.request (
    TrgtID,
    ResultCode,
)
```

The primitive parameters are defined in Table 10.

5.3.6.3.1 Time of creation

After the disassociate request command is sent, once the acknowledgement frame is received or the acknowledgement timeout is exceeded, MLME sends this to DME. If the MLME initiating the disassociate process receives the acknowledgement frame, it considers the disassociate process to have been successfully carried out, and if the acknowledgement time limit has been exceeded, it considers the process to have failed.

5.3.6.3.2 Effect

The result of the disassociation is reported through this primitive which initiated the disassociation.

5.3.7 Key request

The following primitives are used when a station is requesting and receiving a key from the key originator. The parameters used for these primitives are defined in Table 11.

Table 11 - MLME-REQUEST-KEY primitive parameters

Name	Type	Valid range	Description
TrgtID	integer	Any valid STNID as defined in 6.2.1.3	Specifies the STNID of the target of the MLME request.
OrigID	integer	Any valid STNID as defined in 6.2.1.3	Specifies the STNID of the station that initiated the MLME request.
SECID	2 octets	As defined in 6.2.2.2	As defined in 6.2.2.2
Key	octet string	Any valid key as defined by the symmetric key security operations,	The key to be used as the current payload protection key for this security relationship. The MAC/MLME encrypts the key before it is placed in the Encrypted Key field and decrypts the field before passing the received key to the DME.
KeyRequestTime-out	duration	0-65535	The time in milliseconds in which the operation initiated by the MLME request needs to be completed before responding with a ResultCode of TIMEOUT.
ResultCode	enumeration	SUCCESS, FAILURE, TIMEOUT	Indicates the result of the MLME request.

5.3.7.1 MLME-REQUEST-KEY.request

This primitive requests the transmission of a key from the key originator by a station. The semantics are as follows.

```
MLME-REQUEST-KEY.request    (
                                TrgtID,
                                KeyRequestTimeout
                              )
```

The primitive parameters are defined in Table 11.

5.3.7.1.1 Time of creation

DME generates this for a station to obtain the designated key from the key originator.

5.3.7.1.2 Effect

The MLME creates a Request Key command, as described in 6.5.4.1, and sends it to the indicated station.

5.3.7.2 MLME-REQUEST-KEY.indication

This primitive reports the request of a key from a station. The semantics are as follows.

```
MLME-REQUEST-KEY.indication (
    OrigID,
    TrgtID,
    ResultCode
)
```

The primitive parameters are defined in Table 11.

5.3.7.2.1 Time of creation

The MLME generates this after receiving a Request Key command, as described in 6.5.4.2. If the integrity code is valid, then the ResultCode is set to SUCCESS. Otherwise, the ResultCode is FAILURE.

5.3.7.2.2 Effect

The DME issues an MLME-REQUEST-KEY.response to the MLME if it receives the MLME-REQUEST-KEY.indication with the ResultCode set to SUCCESS.

5.3.7.3 MLME-REQUEST-KEY.response

This primitive responds to a key request from a station with the requested key by a station. The semantics are as follows.

```
MLME-REQUEST-KEY.response (
    OrigID,
    SECID,
    Key
)
```

The primitive parameters are defined in Table 11.

5.3.7.3.1 Time of creation

The DME generates this after receiving an MLME-REQUEST-KEY.indication primitive with ResultCode equal to SUCCESS where the OrigID corresponds to a station that has established secure membership or a secure relationship with the key originator.

5.3.7.3.2 Effect

The MLME generates a Request Key Response command, as described in 6.5.4.2, and sends it to the specified station. The MLME encrypts the key before transmission.

5.3.7.4 MLME-REQUEST-KEY.confirm

This primitive reports the results of a key request and, if the response was received, the requested key to the DME. The semantics are as follows.

```

MLME-REQUEST-KEY.confirm    (
                                TrgtID,
                                SECID,
                                Key,
                                ResultCode
                              )

```

The primitive parameters are defined in Table 11.

5.3.7.4.1 Time of creation

The MLME generates this after receiving a Request Key Response command, as described in 6.5.4.2, from the key originator of this relationship or due to a timeout. If there is no response from the key originator within KeyRequestTimeout, the ResultCode is set to TIMEOUT. If the integrity code is not valid, then the ResultCode is set to FAILURE. Otherwise, the ResultCode is SUCCESS and the MLME decrypts the key.

5.3.7.4.2 Effect

The DME is informed of the results of a previously issued key request and, if successful, obtains the requested key. The MLME generates MLME-MEMBERSHIP-UPDATE.request.

5.3.8 Key distribution

The following primitives are used when a station is acting as key originator sending a key to another station. The parameters used for these primitives are defined in Table 12.

Table 12 - MLME-DISTRIBUTE-KEY primitive parameters

Name	Type	Valid range	Description
TrgtID	integer	Any valid STNID as defined in 6.2.1.3	Specifies the STNID of the target of the MLME request.
OrigID	integer	Any valid STNID as defined in 6.2.1.3	Specifies the STNID of the station that initiated the MLME request.
SECID	2 octets	As defined in 6.2.2.2	As defined in 6.2.2.2
Key	octet string	Any valid key as defined by the symmetric key security operations,	The key to be used as the current payload protection key for this security relationship. The MAC/MLME encrypts the key before it is placed in the Encrypted Key field and decrypts the field before passing the received key to the DME.
DistributeKeyTime-out	duration	0-65535	The time in milliseconds in which the operation initiated by the MLME request needs to be completed before responding with a ResultCode of TIMEOUT.
ResultCode	enumeration	SUCCESS,	Indicates the result of the MLME request.

		FAILURE, TIMEOUT	
--	--	---------------------	--

5.3.8.1 MLME-DISTRIBUTE-KEY.request

This primitive distribute a key to another station by a station. The semantics are as follows.

```
MLME-DISTRIBUTE-KEY.request (
    TrgtID,
    SECID,
    Key,
    DistributeKeyTimeout
)
```

The primitive parameters are defined in Table 12.

5.3.8.1.1 Time of creation

The DME generates this to distribute a key to a station that has established secure membership or a secure relationship with the key originator.

5.3.8.1.2 Effect

The MLME creates a Distribute Key Request command, as described in 6.5.4.3, and sends it to the indicated station. The MLME encrypts the key before transmission.

5.3.8.2 MLME-DISTRIBUTE-KEY.indication

This primitive reports the reception of a key from a key originator. The semantics are as follows.

```
MLME-DISTRIBUTE-KEY.indication (
    OrigID,
    SECID,
    Key,
    ResultCode
)
```

The primitive parameters are defined in Table 12.

5.3.8.2.1 Time of creation

The MLME generates this after receiving a Distribute Key Request command, as described in 6.5.4.3. If the integrity code is not valid, then the ResultCode is set to FAILURE. Otherwise, the ResultCode is SUCCESS and the MLME decrypts the key.

5.3.8.2.2 Effect

If the ResultCode is SUCCESS, the DME will save the designated key and generate an MLME-DISTRIBUTE-KEY.response to acknowledge successful receipt of the key.

5.3.8.3 MLME-DISTRIBUTE-KEY.response

This primitive responds to a key distribution from a key originator with an acknowledgement of successful receipt of the key by a station. The semantics are as follows.

```
MLME-DISTRIBUTE-KEY.response      (
                                    OrigID,
                                    SECID
                                    )
```

The primitive parameters are defined in Table 12.

5.3.8.3.1 Time of creation

The DME generates this after receiving an MLME-DISTRIBUTE-KEY.indication primitive from a peer station. It is not generated by the DME as a result of the receipt of an MLME-DISTRIBUTE-KEY.indication primitive from the master.

5.3.8.3.2 Effect

The MLME generates a Distribute Key Response command, as described in 6.5.4.4, and sends it to the specified station.

5.3.8.4 MLME-DISTRIBUTE-KEY.confirm

This primitive reports the results of a distribute key process with a station. The semantics are as follows.

```
MLME-DISTRIBUTE-KEY.confirm      (
                                    TrgtID,
                                    SECID,
                                    ResultCode
                                    )
```

The primitive parameters are defined in Table 12.

5.3.8.4.1 Time of creation

The MLME generates this after receiving a Distribute Key Response command, as described in 6.5.4.4, from another station. If there is no response from the station within DistributeKeyTimeout, the ResultCode is set to TIMEOUT. If the integrity code is not valid, then the ResultCode is set to FAILURE. Otherwise, the ResultCode is SUCCESS.

5.3.8.4.2 Effect

The DME is informed of the results of a previously issued key distribution.

5.3.9 Security management

These primitives initialize, update or delete the security information of a membership or key change process or a security event. Primitives are also provided to transfer security messages. These primitives can be used in an authentication process.

The parameters used for the MLME-MEMBERSHIP-UPDATE are defined in Table 13 and MLME-SECURITY-ERROR primitives are defined in Table 14, MLME-SECURITY-MESSAGE primitive are defined in Table 15.

Table 13 - MLME-MEMBERSHIP-UPDATE primitive parameters

Name	Type	Valid range	Description
SecID	2 octets	As defined in 6.2.2.2	As defined in 6.2.2.2
KeyType	enumeration	MANAGEMENT, DATA, GROUP	Specifies the type of key that is being updated.
TrgtID	integer	Any valid STNID as defined in 6.2.1.3 except for the BcstID, the McstID or the UnassocID	The STNID of the target station for this relationship.
MembershipStatus	enumeration	MEMBER, NON-MEMBER	Indicates the membership status of the TrgtID for the provided SECID.
KeyOriginator	boolean	TRUE, FALSE	This station is the key originator for this relationship.
KeyDelete	boolean	TRUE, FALSE	This key is deleted or installed.
Key	octet string	Any valid key as defined by the symmetric key security operations,	The key used for protecting frames between this station and the TrgtID station.

Table 14 - MLME-SECURITY-ERROR primitive parameters

Name	Type	Valid range	Description
ReceivedMACHeader	octet string	Any valid MAC header, Figure 5.	The MAC header of the received frame that induced a failed security check or for which the station is unable to find the designated key.
ReceivedFramePayload	octet string	Any valid Frame Payload, Figure 7	The received Frame Payload that induces a failed security check or for which the station is unable to find the designated key.
ReasonCode	enumeration	INVALID-MODE, UNAVAILABLE-KEY, FAILED-SECURITY-CHECK, BAD-TIME-TOKEN,	The reason for the security error.

		REPLAYED-FRAME	
--	--	----------------	--

Table 15 - MLME-SECURITY-MESSAGE primitive parameters

Name	Type	Valid range	Description
TrgtID	integer	Any valid STNID as defined in 6.2.1.3	Specifies the STNID of the target of the MLME request.
OrigID	integer	Any valid STNID as defined in 6.2.1.3	Specifies the STNID of the originator of the MLME request.
VendorOUI	As defined in 6.5.6	As defined in 6.5.6	As defined in 6.5.6
SecurityInformation	octet string	Any valid octet string	Security information that will be passed from one DME to another peer DME in the network.
SecMsgTimeout	integer	0-65535	The time in milliseconds in which the operation initiated by the MLME request needs to be completed before responding with a ResultCode of TIMEOUT.
ReasonCode	enumeration	COMPLETED, TIMEOUT	Indicated if the MAC/MLME was successful in sending the security message.

5.3.9.1 MLME-MEMBERSHIP-UPDATE.request

This primitive requests the membership status, SECID and keying information associated with a security relationship to be included or updated. The semantics are as follows.

```
MLME-MEMBERSHIP-UPDATE.request  (
    TrgtID,
    MembershipStatus,
    SECID,
    KeyType,
    KeyOriginator,
    KeyDelete,
    Key
)
```

The primitive parameters are defined in Table 14.

5.3.9.1.1 Time of creation

The DME sends this request to the MLME after completing a membership change or key update process with the master or a station.

5.3.9.1.2 Effect

This primitive initiates the membership update procedure defined in 8.4.

5.3.9.2 MLME-SECURITY-ERROR.indication

This primitive allows the MLME of any station to indicate a failed security processing operation to the DME. The semantics are as follows.

```
MLME-SECURITY-ERROR.indication      (
                                     ReceivedMACHeader,
                                     Received FramePayload,
                                     ReasonCode
                                     )
```

The primitive parameters are defined in Table 14.

5.3.9.2.1 Time of creation

The MLME issues this when it receives a frame, but security mode is not correct or it is unable to find an appropriate key or fails the security check according to the symmetric key security operations. This primitive is also issued if the time token in the beacon was not within the range of valid time tokens, or replayed frame was received.

5.3.9.2.2 Effect

When a station receives this primitive, the DME is promptly notified of a security error and the reason for the security error and then analyze the reason for the security error.

5.3.9.3 MLME-SECURITY-MESSAGE.request

This primitive sends a security message to a station in the network. The semantics are as follows.

```
MLME-SECURITY-MESSAGE.request      (
                                     TrgtID,
                                     VendorOUI,
                                     SecurityInformation,
                                     SecMsgTimeout
                                     )
```

The primitive parameters are defined in Table 15.

5.3.9.3.1 Time of creation

The DME generates this to send security related information to another station in the network.

5.3.9.3.2 Effect

The MLME creates a Security Message command, as described in 6.5.5.1, and sends it to the appropriate station.

5.3.9.4 MLME-SECURITY-MESSAGE.indication

This primitive reports the reception of a Security Message command, as described in 6.5.5.1 from a station. The semantics are as follows.

```
MLME-SECURITY-MESSAGE.indication  (
                                     TrgtID,
                                     TrgtID,
                                     OrigID,
                                     VendorOUI,
                                     SecurityInformation
                                     )
```

The primitive parameters are defined in Table 15.

5.3.9.4.1 Time of creation

The MLME generates this after receiving a valid Security Message command from a station.

5.3.9.4.2 Effect

The DME receives the security related information. The use of this information is outside of the scope of this standard.

5.3.9.5 MLME-SECURITY-MESSAGE.confirm

This primitive reports the result of an attempt send security information to another station. The semantics are as follows.

```
MLME-SECURITY-MESSAGE.confirm      (
                                     ResultCode
                                     )
```

The primitive parameters are defined in Table 15.

5.3.9.5.1 Time of creation

The MLME generates this after receiving an Imm-ACK for the Security Message command or due to a timeout. If the Imm-ACK is not received within SecMsgTimeout, the ResultCode is TIMEOUT. Otherwise, the ResultCode is COMPLETED.

5.3.9.5.2 Effect

The DME is informed of whether the message was successfully sent and ACKed or not.

5.3.10 Master handover

The following primitives are used when the current master transfers its authority to the most capable station within network. The primitive parameters are defined in Table 16.

Table 16 - MLME-Master-HANDOVER primitive parameters

Name	Type	Valid range	Description
MasterCapable-STNID	integer	Valid STNID as defined in 6.2.1.3	STNID of station to which the master wants to handover its authority
NumberOfSTNs	integer	0-255	Number of stations in network
NmbrHndOvrBcns	integer	(1+maximum beacon loss)-255	Number of times that a beacon containing the relevant information blocks must be broadcasted prior to the actual handover of master authority
HandoverTimeout	time	0-65535	Time limit in which the MLME request must be actually executed
HandoverStatus	enumeration	STARTED, CANCELLED	Indicates whether the handover of the master role to another station has been started or cancelled
ResultCode	enumeration	SUCCESS, TIMEOUT	Result of MLME request

5.3.10.1 MLME-MASTER-HANDOVER.request

This primitive requests the start of the handover of the master authority to another station. The semantics are as follows.

```
MLME-MASTER-HANDOVER.request      (
                                     MasterCapableSTNID
                                     NmbrHdnOvrBcns,
                                     HandoverStatus,
                                     HandoverTimeout
                                     )
```

The primitive parameters are defined in Table 16.

5.3.10.1.1 Time of creation

This primitive is sent to MLME when the master DME tries to handover its authority to another station or cancels the handover operation.

5.3.10.1.2 Effect

When MLME receives this primitive, it sends a master handover command frame to the destination station.