

# Z-Stack Monitor and Test API

Document Number: SWRA198

Texas Instruments, Inc.

Dallas, Texas USA

Version	Description	Date
1.0	Initial Release	09/06/2008
1.1	Update address type for AUTOPEND	04/02/2009
1.2	Add MT_AF command and MT_ZDO callback for source routing	06/25/2009
	Add MT_AF commands to support inter-pan	
	Add MT_ZDO commands to support link key configuration	
1.3	Add MT_ZDO commands to MSG callback register/remove/indicate	01/17/2010
	Add MT_UTIL commands for link key establishment	
	Increase 'Length' field from uint8 to uint16 in: MT_AF_DATA_REQUEST_EXT and MT_AF_INCOMING_MSG_EXT	
	Add MT_AF_DATA_STORE and MT_AF_DATA_RETRIEVE	
	Add MT_UTIL_DATA_REQ and UTIL_TEST_LOOPBACK	
1.4	Move MT_MAC_SRC_MATCH commands to MT_UTIL	07/08/2010
	Add MT_ZDO commands to support manual joining procedure:	
	<ul> <li>MT_ZDO_NWK_DISCOVERY_REQ</li> </ul>	
	<ul><li>MT_ZDO_JOIN_REQ</li></ul>	
	<ul> <li>MT_ZDO_NWK_DISCOVERY_CNF</li> </ul>	
	<ul><li>MT_ZDO_BEACON_NOTIFY_IND</li></ul>	
	<ul><li>MT_JOIN_CNF</li></ul>	
1.5	Add UTIL_APSME_LINK_KEY_NV_ID_GET command	07/27/2010
	Add MT_SYS commands for handling system date and time:	
	<ul><li>MT_SYS_GET_TIME</li></ul>	
	<ul><li>MT_SYS_SET_TIME</li></ul>	
	Corrections to SYS_VERSION and ZDO_NODE_DESC_RSP commands	
	Add UTIL_APSME_REQUEST_KEY_CMD command.	
	Changed command name from ZDO_NETWORK_DISCOVERY_REQ to ZDO_NWK_DISCOVERY_REQ	
	Fixed Cmd0 for ZDO_NWK_DISCOVERY_REQ and ZDO_JOIN_REQ.	
	Add AF_APSF_CONFIG_SET, SYS_OSAL_NV_ITEM_INIT, SYS_OSAL_NV_ITEM_LENGTH, SYS_OSAL_NV_ITEM_DELETE	
1.6	commands.	07/16/2011
1.7	Add ZDO_LEAVE_IND callback	03/10/2012

	Add SYS_SET_TX_POWER command	
	Fixed parameter info for UTIL_ADDRMGR_EXT_ADDR_LOOKUP	
	Add Wildcard Profile ID bit definition in AF_DATA_REQUEST and AF_DATA_REQUEST_EXT	
	Add AF_REFLECT_ERROR message	
	Clarify RemoveChildren_Rejoin parameter for ZDO_MGMT_LEAVE_REQ	
1.8	command	11/14/2012
1.9	Add UTIL_SRNG_GEN and UTIL_BIND_ADD_ENTRY commands  Modify ZDO_MGMT_PERMIT_JOIN_REQ command, added AddrMode field.	11/23/2013
	Add MT_SYS commands for statistics:  SYS_ZDIAGS_INIT_STATS	
	<ul> <li>SYS_ZDIAGS_CLEAR_STATS</li> </ul>	
	<ul> <li>SYS_ZDIAGS_GET_STATS</li> </ul>	
	<ul> <li>SYS_ZDIAGS_RESTORE_STATS_NV</li> </ul>	
1.10	<ul> <li>SYS_ZDIAGS_SAVE_STATS_TO_NV</li> </ul>	03/13/2014
1.11	Correction to UTIL_KEY_EVENT command	12/09/2014
	Added NV MT commands	
	SYS_NV_CREATE	
	SYS_NV_DELETE	
	SYS_NV_READ	
	SYS_NV_WRITE	
	SYS_NV_UPDATE	
	SYS_NV_COMPACT	
	Added ZDO command for new rejoin parameter ZDO_SET_REJOIN_PARAMETERS_REQ	
	Added MT_ZDO extension commands	
	MT_ZDO_SEC_ADD_LINK_KEY	
	MT_ZDO_SEC_ENTRY_LOOKUP_EXT	
	MT_ZDO_SEC_DEVICE_REMOVE	
	MT_ZDO_EXT_ROUTE_DISC	
	MT_ZDO_EXT_ROUTE_CHECK	
	MT_ZDO_EXT_REMOVE_GROUP	
	MT_ZDO_EXT_REMOVE_ALL_GROUP	
	MT_ZDO_EXT_FIND_ALL_GROUPS_ENDPOINT	
	MT_ZDO_EXT_FIND_GROUP	
1.12	MT_ZDO_EXT_ADD_GROUP	02/19/2015

	MT_ZDO_EXT_COUNT_ALL_GROUPS	
	MT_ZDO_EXT_RX_IDLE	
	<ul> <li>MT_ZDO_EXT_UPDATE_NWK_KEY</li> </ul>	
	<ul> <li>MT_ZDO_EXT_SWITCH_NWK_KEY</li> </ul>	
	MT_ZDO_EXT_NWK_INFO	
	<ul> <li>MT_ZDO_EXT_SEC_APS_REMOVE_REQ</li> </ul>	
	MT_ZDO_FORCE_CONCENTRATOR_CHANGE	
	MT_ZDO_EXT_SET_PARAMS	
1.13	Added MT_ZDO_TC_DEVICE_IND, MT_ZDO_PERMIT_JOIN_IND, MT_ZDO_NWK_ADDR_OF_INTEREST_REQ commands	03/09/2015
	Addition of new MT commands for the Z3 stack update	
	New ZDO command ZDO_STARTUP_FROM_APP_EX	
	Added MT_APP_CNF commands	
	APP_CNF_SET_NWK_FRAME_COUNTER	
	APP_CNF_SET_DEFAULT_REMOTE_ENDDEVICE _TIMEOUT	
	APP_CNF_SET_ENDDEVICETIMEOUT	
	APP_CNF_SET_ALLOWREJOIN_TC_POLICY	
	APP_CNF_BDB_START_COMMISSIONING	
	APP_CNF_BDB_SET_CHANNEL	
	APP_CNF_BDB_ADD_INSTALLCODE	
	APP_CNF_BDB_SET_TC_REQUIRE_KEY_EXCHANGE	
	APP_CNF_BDB_SET_JOINUSESINSTALLCODEKEY	
	APP_CNF_BDB_SET_ACTIVE_DEFAULT_CENTRALIZED	
	APP_CNF_BDB_COMMISSIONING_NOTIFICATION	
	APP_CNF_BDB_ZED_ATTEMPT_RECOVER_NWK	
	Added MT_GREENPOWER commands	
	GP_DATA_REQ	
	GP_SEC_RSP	
	GP_DATA_CNF	
	GP_SEC_REQ	
1.14	GP_DATA_IND	10/25/2016
	MT_APP_CNF	
	ZDO_STARTUP_FROM_APP_EX deprecated.	
	ZDO_STARTUP_FROM_APP fixed to be backward compatible.	
	BDB_COMMISSIONING_NOTIFICATION remaining methods     parameter now returns the right value.	
	parameter now returns the right value.  MT_UTIL	
1.15	UTIL_GET_DEVICE_INFO now returns Reduce Function Devices associated to the local device instead of	5/10/2017
	i diletion Devices associated to the focal device instead of	

	all devices in the association table.	
	MT_APP_CNF	
	APP_CNF_BDB_SET_ACTIVE_DEFAULT_CENTRALIZED_KE     Y updated to support fallback to default global centralized key and	
1.16	text plain key modes.	6/21/2018
	Update to GP_DATA_IND command	
1.17	Update SYS_SET_TX_POWER SRSP attribute	5/23/2019
1.18	Removed MT_SAPI	9/1/2020

# **Table of Contents**

1.		INTRO	DUCTION	1
	1.1	l Scoi	PE	1
	1.2	2 OVE	RVIEW	1
	1.3	REQ	UIREMENTS	2
	1.4	4 Acr	ONYMS	2
	1.5	5 Refe	RENCE DOCUMENTS	2
2.		MONI	FOR AND TEST TRANSPORT PROTOCOL	3
	2.1	I Form	MAT	3
		2.1.1	General Serial Packet	3
		2.1.2	MT CMD	4
	2.2	2 Exa	MPLE	6
3.		MONI	TOR AND TEST COMMANDS	7
	3.1	l Intr	ODUCTION	7
	3.2	2 MT_	AF	7
		3.2.1	MT_AF Commands	7
		3.2.1.1	AF_REGISTER	7
		3.2.1.2	AF_DATA_REQUEST	8
		3.2.1.3	AF_DATA_REQUEST_EXT	9
		3.2.1.4	AF_DATA_REQUEST_SRC_RTG	11
		3.2.1.5	AF_INTER_PAN_CTL	13
		3.2.1.6	AF_ DATA_STORE	14
		3.2.1.7	AF_ DATA_RETRIEVE	15
		3.2.1.8	AF_APSF_CONFIG_SET	16
		3.2.2	MT_AF Callbacks	17
		3.2.1.1	AF_DATA_CONFIRM	17
		3.2.1.2	AF_REFLECT_ERROR	17
		3.2.1.3	AF_INCOMING_MSG	18
		3.2.1.4	AF_INCOMING_MSG_EXT	18
	3.3	3 MT_	APP	20
		2 2 1	MT APP Commands	20

3.3.1.1	APP_MSG	20
3.3.1.2	APP_USER_TEST	21
3.3.2	MT_APP Callbacks	22
3.4 MT_D	DEBUG	22
3.4.1	MT_DEBUG Commands	22
3.4.1.1	DEBUG_SET_THRESHOLD	22
3.4.1.2	DEBUG_MSG	23
3.4.2	MT_DEBUG Callbacks	23
3.5 MT_M	1AC	24
3.5.1	MT_MAC Commands	24
3.5.1.1	MAC_RESET_REQ	24
3.5.1.2	MAC_INIT	25
3.5.1.3	MAC_START_REQ	26
3.5.1.4	MAC_SYNC_REQ	29
3.5.1.5	MAC_DATA_REQ	30
3.5.1.6	MAC_ASSOCIATE_REQ	33
3.5.1.7	MAC_ASSOCIATE_RSP	36
3.5.1.8	MAC_DISASSOCIATE_REQ	37
3.5.1.9	MAC_GET_REQ	39
3.5.1.10	MAC_SET_REQ	42
3.5.1.11	MAC_SCAN_REQ	44
3.5.1.12	MAC_ORPHAN_RSP	46
3.5.1.13	MAC_POLL_REQ	47
3.5.1.14	MAC_PURGE_REQ	49
3.5.1.15	MAC_SET_RX_GAIN_REQ	49
3.5.2	MT_MAC Callbacks	50
3.5.2.1	MAC_SYNC_LOSS_IND	50
3.5.2.2	MAC_ASSOCIATE_IND	51
3.5.2.3	MAC_ASSOCIATE_CNF	53
3.5.2.4	MAC_BEACON_NOTIFY_IND	54
3.5.2.5	MAC DATA CNF	56

3.5.2.6	MAC_DATA_IND	56
3.5.2.7	MAC_DISASSOCIATE_IND	58
3.5.2.8	MAC_DISASSOCIATE_CNF	59
3.5.2.9	MAC_ORPHAN_IND	60
3.5.2.10	MAC_POLL_CNF	61
3.5.2.11	MAC_SCAN_CNF	62
3.5.2.12	MAC_COMM_STATUS_IND	62
3.5.2.13	MAC_START_CNF	64
3.5.2.14	MAC_RX_ENABLE_CNF	64
3.5.2.15	MAC_PURGE_CNF	65
3.6 MT_N	NWK	65
3.7 MT_S	SAPI	65
3.8 MT_S	SYS	65
3.8.1	MT_SYS Commands	66
3.8.1.1	SYS_RESET_REQ	66
3.8.1.2	SYS_PING	66
3.8.1.3	SYS_VERSION	67
3.8.1.4	SYS_SET_EXTADDR	68
3.8.1.5	SYS_GET_EXTADDR	68
3.8.1.6	SYS_RAM_READ	69
3.8.1.7	SYS_RAM_WRITE	70
3.8.1.8	SYS_OSAL_NV_READ	71
3.8.1.9	SYS_OSAL_NV_WRITE	72
3.8.1.10	SYS_OSAL_NV_ITEM_INIT	73
3.8.1.11	SYS_OSAL_NV_DELETE	74
3.8.1.12	SYS_OSAL_NV_LENGTH	75
3.8.1.13	SYS_OSAL_START_TIMER	75
3.8.1.14	SYS_OSAL_STOP_TIMER	76
3.8.1.15	SYS_RANDOM	77
3.8.1.16	SYS_ADC_READ	77
3.8.1.17	SYS_GPIO	<i>7</i> 9

3.8.1.18	SYS_STACK_TUNE	80
3.8.1.19	SYS_SET_TIME	81
3.8.1.20	SYS_GET_TIME	82
3.8.1.21	SYS_SET_TX_POWER	82
3.8.1.22	SYS_ZDIAGS_INIT_STATS	83
3.8.1.23	SYS_ZDIAGS_CLEAR_STATS	84
3.8.1.24	SYS_ZDIAGS_GET_STATS	85
3.8.1.25	SYS_ZDIAGS_RESTORE_STATS_NV	85
3.8.1.26	SYS_ZDIAGS_SAVE_STATS_TO_NV	86
3.8.1.27	SYS_NV_CREATE	87
3.8.1.28	SYS_NV_DELETE	87
3.8.1.29	SYS_NV_LENGTH	88
3.8.1.30	SYS_NV_READ	89
3.8.1.31	SYS_NV_WRITE	90
3.8.1.32	SYS_NV_UPDATE	91
3.8.1.33	SYS_NV_COMPACT	91
3.8.1.34	SYS_OSAL_NV_READ_EXT	92
3.8.1.35	SYS_OSAL_NV_WRITE_EXT	93
3.8.2 N	AT_SYS Callbacks	94
3.8.2.1	SYS_RESET_IND	94
3.8.2.2	SYS_OSAL_TIMER_EXPIRED	94
3.9 MT_U	ART	95
3.10 MT_	_UTIL	95
3.10.1	MT_UTIL Commands	95
3.10.1.1	UTIL_GET_DEVICE_INFO	95
3.10.1.2	UTIL_GET_NV_INFO	96
3.10.1.3	UTIL_SET_PANID	97
3.10.1.4	UTIL_SET_CHANNELS	98
3.10.1.5	UTIL_SET_SECLEVEL	99
3.10.1.6	UTIL_SET_PRECFGKEY	99
3.10.1.7	UTIL_CALLBACK_SUB_CMD	100

	3.10.1.8	UTIL_KEY_EVENT	101
	3.10.1.9	UTIL_TIME_ALIVE	102
	3.10.1.10	UTIL_LED_CONTROL	103
	3.10.1.11	UTIL_LOOPBACK	104
	3.10.1.12	UTIL_DATA_REQ	104
	3.10.1.13	UTIL_SRC_MATCH_ENABLE	105
	3.10.1.14	UTIL_SRC_MATCH_ADD_ENTRY	105
	3.10.1.15	UTIL_SRC_MATCH_DEL_ENTRY	106
	3.10.1.16	UTIL_SRC_MATCH_CHECK_SRC_ADDR	107
	3.10.1.17	UTIL_SRC_MATCH_ACK_ALL_PENDING	108
	3.10.1.18	UTIL_SRC_MATCH_CHECK_ALL_PENDING	109
	3.10.1.19	UTIL_ADDRMGR_EXT_ADDR_LOOKUP	109
	3.10.1.20	UTIL_ADDRMGR_NWK_ADDR_LOOKUP	110
	3.10.1.21	UTIL_APSME_LINK_KEY_DATA_GET	111
	3.10.1.22	UTIL_APSME_LINK_KEY_NV_ID_GET	112
	3.10.1.23	UTIL_APSME_REQUEST_KEY_CMD	113
	3.10.1.24	UTIL_ASSOC_COUNT	113
	3.10.1.25	UTIL_ASSOC_FIND_DEVICE	114
	3.10.1.26	UTIL_ASSOC_GET_WITH_ADDRESS	115
	3.10.1.27	UTIL_BIND_ADD_ENTRY	116
	3.10.1.28	UTIL_ZCL_KEY_EST_INIT_EST	116
	3.10.1.29	UTIL_ZCL_KEY_EST_SIGN	117
	3.10.1.30	UTIL_SRNG_GEN	118
	3.10.2	MT_UTIL Callbacks	119
	3.10.2.1	UTIL_SYNC_REQ	119
	3.10.2.2	UTIL_ZCL_KEY_ESTABLISH_IND	119
3.	11 MT_	VERSION	119
3.	12 MT_	ZDO	120
	3.12.1	MT_ZDO Commands	120
	3.12.1.1	ZDO_NWK_ADDR_REQ	120
	3 12 1 2	ZDO IFFF ADDR RFO	121

3.12.1.3	ZDO_NODE_DESC_REQ	122
3.12.1.4	ZDO_POWER_DESC_REQ	122
3.12.1.5	ZDO_SIMPLE_DESC_REQ	123
3.12.1.6	ZDO_ACTIVE_EP_REQ	124
3.12.1.7	ZDO_MATCH_DESC_REQ	125
3.12.1.8	ZDO_COMPLEX_DESC_REQ	126
3.12.1.9	ZDO_USER_DESC_REQ	126
3.12.1.10	ZDO_END_DEVICE_ANNCE	127
3.12.1.11	ZDO_USER_DESC_SET	128
3.12.1.12	ZDO_SERVER_DISC_REQ	129
3.12.1.13	ZDO_END_DEVICE_BIND_REQ	129
3.12.1.14	ZDO_BIND_REQ	130
3.12.1.15	ZDO_UNBIND_REQ	132
3.12.1.16	ZDO_MGMT_NWK_DISC_REQ	133
3.12.1.17	ZDO_MGMT_LQI_REQ	134
3.12.1.18	ZDO_MGMT_RTG_REQ	135
3.12.1.19	ZDO_MGMT_BIND_REQ	136
3.12.1.20	ZDO_MGMT_LEAVE_REQ	137
3.12.1.21	ZDO_MGMT_DIRECT_JOIN_REQ	138
3.12.1.22	ZDO_MGMT_PERMIT_JOIN_REQ	139
3.12.1.23	ZDO_MGMT_NWK_UPDATE_REQ	140
3.12.1.24	ZDO_MSG_CB_REGISTER	142
3.12.1.25	ZDO_MSG_CB_REMOVE	143
3.12.1.26	ZDO_STARTUP_FROM_APP	143
3.12.1.27	ZDO_STARTUP_FROM_APP_EX	144
3.12.1.28	ZDO_SET_LINK_KEY	145
3.12.1.29	ZDO_REMOVE_LINK_KEY	146
3.12.1.30	ZDO_GET_LINK_KEY	146
3.12.1.31	ZDO_NWK_DISCOVERY_REQ	147
3.12.1.32	ZDO_JOIN_REQ	149
3.12.1.33	ZDO_SET_REJOIN_PARAMETERS	150

3.12.1.34	ZDO_SEC_ADD_LINK_KEY	150
3.12.1.35	ZDO_SEC_ENTRY_LOOKUP_EXT	151
3.12.1.36	ZDO_SEC_DEVICE_REMOVE	152
3.12.1.37	ZDO_EXT_ROUTE_DISC	153
3.12.1.38	ZDO_EXT_ROUTE_CHECK	154
3.12.1.39	ZDO_EXT_REMOVE_GROUP	155
3.12.1.40	ZDO_EXT_REMOVE_ALL_GROUP	155
3.12.1.41	ZDO_EXT_FIND_ALL_GROUPS_ENDPOINT	156
3.12.1.42	ZDO_EXT_FIND_GROUP	157
3.12.1.43	ZDO_EXT_ADD_GROUP	158
3.12.1.44	ZDO_EXT_COUNT_ALL_GROUPS	158
3.12.1.45	ZDO_EXT_RX_IDLE	159
3.12.1.46	ZDO_EXT_UPDATE_NWK_KEY	160
3.12.1.47	ZDO_EXT_SWITCH_NWK_KEY	160
3.12.1.48	ZDO_EXT_NWK_INFO	161
3.12.1.49	ZDO_EXT_SEC_APS_REMOVE_REQ	162
3.12.1.50	ZDO_FORCE_CONCENTRATOR_CHANGE	163
3.12.1.51	ZDO_EXT_SET_PARAMS	163
3.12.1.52	ZDO_NWK_ADDR_OF_INTEREST_REQ	164
3.12.2	MT_ZDO Callbacks	165
3.12.2.1	ZDO_NWK_ADDR_RSP	165
3.12.2.2	ZDO_IEEE_ADDR_RSP	166
3.12.2.3	ZDO_NODE_DESC_RSP	167
3.12.2.4	ZDO_POWER_DESC_RSP	169
3.12.2.5	ZDO_SIMPLE_DESC_RSP	170
3.12.2.6	ZDO_ACTIVE_EP_RSP	171
3.12.2.7	ZDO_MATCH_DESC_RSP	172
3.12.2.8	ZDO_COMPLEX_DESC_RSP	172
3.12.2.9	ZDO_USER_DESC_RSP	173
3.12.2.10	ZDO_USER_DESC_CONF	173
3.12.2.11	ZDO_SERVER_DISC_RSP	174

3.12.2.12	ZDO_END_DEVICE_BIND_RSP	175
3.12.2.13	ZDO_BIND_RSP	175
3.12.2.14	ZDO_UNBIND_RSP	176
3.12.2.15	ZDO_MGMT_NWK_DISC_RSP	176
3.12.2.16	ZDO_MGMT_LQI_RSP	177
3.12.2.17	ZDO_MGMT_RTG_RSP	178
3.12.2.18	ZDO_MGMT_BIND_RSP	179
3.12.2.19	ZDO_MGMT_LEAVE_RSP	180
3.12.2.20	ZDO_MGMT_DIRECT_JOIN_RSP	180
3.12.2.21	ZDO_MGMT_PERMIT_JOIN_RSP	181
3.12.2.22	ZDO_STATE_CHANGE_IND	181
3.12.2.23	ZDO_END_DEVICE_ANNCE_IND	182
3.12.2.24	ZDO_MATCH_DESC_RSP_SENT	183
3.12.2.25	ZDO_STATUS_ERROR_RSP	183
3.12.2.26	ZDO_SRC_RTG_IND	184
3.12.2.27	ZDO_BEACON_NOTIFY_IND	184
3.12.2.28	ZDO_JOIN_CNF	186
3.12.2.29	ZDO_NWK_DISCOVERY_CNF	186
3.12.2.30	ZDO_LEAVE_IND	187
3.12.2.31	ZDO_MSG_CB_INCOMING	187
3.12.2.32	ZDO_TC_DEV_IND	188
3.12.2.33	ZDO_PERMIT_JOIN_IND	189
3.13 MT	_APP_CONFIG	189
3.13.1	MT_APP_CONFIG Commands	189
3.13.1.1	APP_CNF_SET_NWK_FRAME_COUNTER	189
3.13.1.2	APP_CNF_SET_DEFAULT_REMOTE_ENDDEVICE _TIMEOUT	190
3.13.1.3	APP_CNF_SET_ENDDEVICETIMEOUT	191
3.13.1.4	APP_CNF_SET_ALLOWREJOIN_TC_POLICY	192
3.13.1.5	APP_CNF_BDB_START_COMMISSIONING	193
3.13.1.6	APP_CNF_BDB_SET_CHANNEL	194
3.13.1.7	APP CNF BDB ADD INSTALLCODE	195

3.13.1.8	APP_CNF_BDB_SET_TC_REQUIRE_KEY_EXCHANGE	196
3.13.1.9	APP_CNF_BDB_SET_JOINUSESINSTALLCODEKEY	197
3.13.1.10	APP_CNF_BDB_SET_ACTIVE_DEFAULT_CENTRALIZED_KEY	198
3.13.1.11	APP_CNF_BDB_ZED_ATTEMPT_RECOVER_NWK	200
3.13.2	MT_APP_CONFIG Callbacks	201
3.13.2.1	APP_CNF_BDB_COMMISSIONING_NOTIFICATION	201
3.14 MT	_GREENPOWER	202
3.14.1	MT_GP Commands	202
3.14.1.1	GP_DATA_REQ	202
3.14.1.2	GP_SEC_RSP	204
3.14.2	MT_GP Callbacks	206
3.14.2.1	GP_DATA_CNF	206
3.14.2.2	GP_SEC_REQ	207
3.14.2.3	GP_DATA_IND	208

## 1. Introduction

# 1.1 Scope

This document describes the Monitor and Test (MT) interface that is used for communication between the host tester and a ZigBee device through RS-232 serial port. Tester can issue MT commands to the ZigBee target through a PC application called Z-Tool. The target must be programmed with the latest Texas Instruments Z-Stack<sup>TM</sup>.

## 1.2 Overview

MT interfaces are divided into categories, shown in the table below. Most interfaces can be disabled or enabled by a compile flag. Depending on the desired interfaces, certain flags need to be enabled during compilation. For a list of supported compile flags, check the "**Z-Stack Compile Option**" document.

Interface	Description	Compile flags
MT_AF	This interface allows tester to interact with AF layer of the target.	MT_AF_FUNC
_	of the target.	MT_AF_CB_FUNC
MT_APP	This interface allows tester to interact with APP layer of the target to control custom tests such as test profile or user-defined test.	MT_APP_FUNC
MT_DEBUG	This interface allows tester to control the debug- messaging mechanism such as debug threshold, debug messages, etc.	MT_DEBUG_FUNC
MT NIXIZ	This interface allows tester to interact with NWK	MT_NWK_FUNC
MT_NWK	layer of the target.	MT_NWK_CB_FUNC
MT_SYS	This interface allows the tester to interact with the target at system level such as reset, read/write memory, read/write extended address, etc.	MT_SYS_FUNC
MT_TASK	This interface handles communication between the Monitor Test interface and Z-Stack. Tester has no control direct over this interface.	MT_TASK
MT_UART	This interface handles communication between the target and Z-Tool. Tester has no direct control over this interface.	N/A
MT_UTIL	This interface provides tester supporting functionalities such as setting PanID, getting device info, getting NV info, subscribing callbacks, etc.	MT_UTIL_FUNC
MT_VERSION	This interface contains information about the release version of the software.	N/A
MT_ZDO	This interface allows tester to interact with the ZDO	MT_ZDO_FUNC
MII_ZDU	layer of the target.	MT_ZDO_CB_FUNC

This interface allows to interact with the commands introduced by Z3.0 Base Device Behavior.

MT\_APP\_CNF\_FUNC

This interface allows to interact with GP stubs.

MT\_GP\_CB\_FUNC

# 1.3 Requirements

There are several requirements for a tester to interact with the ZigBee target through the MT interface:

- ZigBee target is programmed with Texas Instruments Z-Stack<sup>TM</sup> (ZStack-2.1.0 or newer).
- Z-Tool 2.0 or newer installed on the tester PC.

Analog to Digital Conversion

• PC is connected to ZigBee target though RS-232 serial port.

# 1.4 Acronyms

ADC

#### Table 1

1 6 6	
Application Framework	
Asynchronous Request	
Frame Check Sequence	
Monitor and Test	
Remote Procedure Call	
Simple API	
Start of Frame	
Synchronous Request	
Synchronous Response	
Texas Instruments ZigBee protocol stack	
Texas Instruments ZigBee PC-based test tool	

#### 1.5 Reference Documents

- [1] Z-Stack Compile Options (SWRA188).
- [2] Z-Stack User's Guides (SWRA161, SWRA162, SWRA163, SWRA164, SWRA165)
- [3] Z-Stack Developer's Guide (SWRA176)
- [4] Z-Stack Application Programming Interface (SWRA195)

#### 2. Monitor and Test Transport Protocol

- A transport protocol is necessary so that messages can be exchanged between the tester and target over an RS-232 serial link. The purpose of the transport protocol is to frame the messages in packets for proper transmission and reception and to ensure message integrity.
- The physical transmission uses: no Parity; 8 data bits and 1 stop bits for each byte.
- The transmission rate will be 38.4 kbps, 57.6kbps and 115.2kbps
- The Z-Tool program must send one message at a time and wait for either the expected response message to a timeout before sending the next message or resending the current message.
- Fields that are multi-byte fields are transmitted Least Significant byte first (LSB). There is no provision for retransmission of lost packets

#### 2.1 Format

#### 2.1.1 General Serial Packet

- Serial packets are sent between the Z-Tool PC application and the target ZigBee device.
   They contain an SOF (Start of Frame), followed by a variable-length MT packet, and terminated by an FCS (Frame Check Sequence).
- Building of the serial packets is handled by MT\_TransportSend() where the SOF is
  inserted at the beginning of the packet and FCS is computed and appended to the end of
  the packet.

SOF	MT CMD	FCS
Byte: 1	3-256	1

**SOF** (Start of Frame): This is a one byte field with value equal to **0xFE** that defines the start of each general serial packet.

**MT CMD** (Monitor Test Command): This contains 1 byte for the length of the actual data, 2 bytes for the MT command Id, and the data ranging from 0-250 bytes. Check 2.1.2 for more details.

FCS (Frame Check Sequence): This is a one byte field that is used to ensure packet integrity. This field is computed as an XOR of all the bytes in the message starting with LEN field and through the last byte of data. The receiver XORs all the received data bytes as indicated above and then XORs the received FCS field. If the sum is not equal to zero, the received packet is in error.

#### 2.1.2 MT CMD

- MT CMD is the actually Monitor and Test command. It contains information that Z-Tool and Z-Stack need to control the target.
- It contains 1 byte for the length of the actual data, 2 bytes for the command, and data ranging from 0-250 bytes.

LEN	CMD	DATA
Byte: 1	2	0-250

**LEN** (Length): This one byte field is the number of bytes in the **DATA** field. If the **DATA** field contains no information this LEN field has a value of 0 and the total length of the **MT CMD** is 3 bytes (0 data message).

**CMD** (Command Id): This is a two byte field with a value denoting the Command Identification (Id) for this message. This field is described in detail below.

	CMD0	CMD1	
Bit: 7-5	4-0	7-0	
Type	Subsystem	Id	

**Type**: Type for the command is described by bit 5, 6, 7 of CMD0 byte. The command type has one of the following values:

Type	CMD0Value
POLL	0x00
SREQ	0x20
AREQ	0x40
SRSP	0x60

0: POLL. A POLL command is used to retrieve queued data. This
command is only applicable to SPI transport. For a POLL command the
subsystem and Id are set to zero and data length is zero.

- 1: SREQ: A synchronous request that requires an immediate response. For example, a function call with a return value would use an SREQ command.
- 2: AREQ: An asynchronous request. For example, a callback event or a function call with no return value would use an AREQ command.
- 3: SRSP: A synchronous response. This type of command is only sent in response to a SREQ command. For an SRSP command the subsystem and Id are set to the same values as the corresponding SREQ. The length of an SRSP is generally nonzero, so an SRSP with length=0 can be used to indicate an error.
- 4-7: Reserved.

**Subsystem**: The subsystem of the command is described by bit 0, 1, 2, 3, 4 of CMD0. The command subsystem has one of the following values:

Subsystem	<b>Subsystem Value</b>
Reserved	0x00
SYS interface	0x01
MAC interface	0x02
NWK interface	0x03
AF interface	0x04
ZDO interface	0x05
SAPI interface	0x06
UTIL interface	0x07
DEBUG interface	0x08
APP interface	0x09
APP config	0x0F
GreenPower	0x15

**Id**: The command Id. The Id maps to a particular interface message. Range: 0-250.

**DATA**: This field contains the actual data to be transmitted. This is a field which varies in size according to the command. It can be 0 to 250.

# 2.2 Example

 $SYS\_PING \text{ command will look like } 0xFE \text{ } 0x00 \text{ } 0x21 \text{ } 0x01 \text{ } 0x20$ 

SOF	LEN	CMD0	CMD1	DATA	FCS
Byte: 1	1	1	1	0	1
0xFE	0x00	0x21	0x01	N/A	0x20

SYS\_PING response will look like 0xFE 0x02 0x61 0x01 0x11 0x00 0x73

SOF	LEN	CMD0	CMD1	DATA0	DATA1	FCS
Byte: 1	1	1	1	1	1	1
0xFE	0x02	0x61	0x01	0x11	0x00	0x73

#### 3. Monitor and Test Commands

#### 3.1 Introduction

Monitor and Test commands (MT commands) exchanged between the target and the tester via a supported H/W medium (i.e.RS-232 or USB.) The tester controls the target using Z-Tool 2.0. In order for the target to communicate with Z-Tool 2.0, Z-Stack must be compiled with MT\_SYS\_FUNC. This enables the MT\_SYS interface so Z-Tool 2.0 can communicate to establish the connection. Some MT interfaces support callbacks. This requires MT\_UTIL\_FUNC to be compiled with Z-Stack in order for the tester to subscribe callback. The corresponding MT interface must also be complied with the correct flag in order for the callbacks to be received and processed correctly by Z-Stack and Z-Tool 2.0. For the complete details on MT flags, check section 1.2 or "Z-Stack Compile Option" document (SWRA188).

#### Summary:

- Z-Tool 2.0 installed and connected to target using the supported H/W interface.
- Z-Stack must be compiled with MT\_SYS\_FUNC and MT\_UTIL\_FUNC.
- Z-Stack must be compiled with MT interface what tester will use.
- Z-Stack and Z-Tool must be set at the same baud rate, no Parity, 8 data-bits and 1 stop-bit for each byte.
- If the target supports flow control, this must be set correctly as well in Z-Tool 2.0

#### 3.2 MT AF

This interface allows the tester to interact with the Application Framework layer (AF).

#### 3.2.1 MT AF Commands

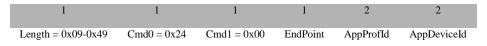
## 3.2.1.1 AF\_REGISTER

#### **Description**:

This command enables the tester to register an application's endpoint description.

#### Usage:

#### **SREQ:**

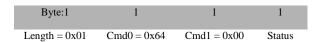




## **Attributes:**

Attribute	Length (byte)	Description
EndPoint	1	Specifies the endpoint of the device
AppProfId	2	Specifies the profile Id of the application
AppDeviceId	2	Specifies the device description Id for this endpoint
AddDevVer	1	Specifies the device version number
		Specifies latency.
LaterrayDag	1	0x00-No latency
LatencyReq		0x01-fast beacons
		0x02-slow beacons
AppNumInClusters	1	the number of Input cluster Id's following in the AppInClusterList
AppInClusterList	32	Specifies the list of Input Cluster Id's
AppNumOutClusters	1	Specifies the number of Output cluster Id's following in the AppOutClusterList
AppOutClusterList	32	Specifies the list of Output Cluster Id's

## **SRSP:**



# **Attributes**:

Attribute	Length (byte)	Description	
Status	1	Status is either Success (0) or Failure (1).	

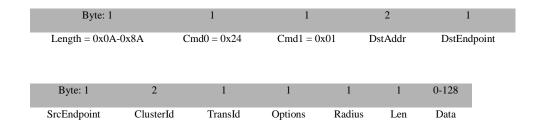
# 3.2.1.2 AF\_DATA\_REQUEST

# **Description**:

This command is used by the tester to build and send a message through AF layer.

Usage:

**SREQ:** 



#### **Attributes**:

Attribute	Length (byte)	Description
DstAddr	2	Short address of the destination device
DstEndpoint	1	Endpoint of the destination device
SrcEndpoint	1	Endpoint of the source device
ClusterId	2	Specifies the cluster ID
TransId	1	Specifies the transaction sequence number of the message.
Options	1	Transmit options bit mask according to the following defines from AF.h: bit 1: sets 'Wildcard Profile ID'; bit 4: turns on/off 'APS ACK'; bit 5 sets 'discover route'; bit 6 sets 'APS security'; bit 7 sets 'skip routing'.
Radius	1	Specifies the number of hops allowed delivering the message (see AF_DEFAULT_RADIUS.)
Len	1	Length of the data.
Data	0-128	0-128 bytes data

#### **SRSP:**



#### **Attributes:**

ı	Attribute	Length (byte)	Description
_	Status	1	Status is either Success (0) or Failure (1).

# 3.2.1.3 AF\_DATA\_REQUEST\_EXT

#### **Description**:

This extended form of the AF\_DATA\_REQUEST must be used to send an inter-pan message (note that the target code must be compiled with the INTER\_PAN flag defined.) This extended data request must also be used when making a request with a huge data byte count which is defined to be a size that would cause the RPC request to exceed the maximum allowed size:

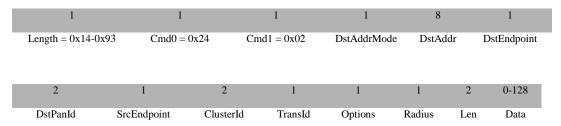
```
MT_RPC_DATA_MAX - sizeof(AF_DATA_REQUEST_EXT)
```

Where <code>sizeof(AF\_DATA\_REQUEST\_EXT)</code> counts everything but the data bytes and now stands at 20. When making an AF\_DATA\_REQUEST\_EXT with a huge data byte count, the request shall not contain any data bytes. The huge data buffer is sent over separately as a sequence of one or more AF\_DATA\_STORE requests. Note that the outgoing huge message is timed-out in 15 seconds; thus all AF\_DATA\_STORE requests must be completed within 15 seconds of an AF\_DATA\_REQUEST\_EXT with a huge data byte count. And any AF\_DATA\_REQUEST\_EXT with a huge data byte count must be completed (or timed-out) before another will be started. The default timeout can be changed by defining the following to other values:

```
#if !defined MT_AF_EXEC_CNT
#define MT_AF_EXEC_CNT 15
#endif
#if !defined MT_AF_EXEC_DLY
#define MT_AF_EXEC_DLY 1000
#endif
```

#### Usage:

#### **SREQ:**



Attribute	Length (byte)	Description	
DstAddrMode	1	A value of 3 (the enumeration value for 'afAddr64Bit') indicates 8-byte (64-bit) address mode; otherwise a value of 2 indicates 2-byte (16-bit) address mode, using only the 2 LSB's of the DstAddr field to form a 2-byte short address.	
DstAddr	8	LSB to MSB for the long or short address of the destination device (upper 6 by are don't care when short address.)	
DstEndpoint	1	Endpoint of the destination device (but don't care if the DstPanId is non-zero, which indicates an inter-pan message.)	
DstPanId	2	PanId of the destination device: 0x0000=Intra-Pan; otherwise, Inter-Pan.	
SrcEndpoint	1	Endpoint of the source device.	
ClusterId	2	Specifies the cluster ID	
TransId	1	Specifies the transaction sequence number of the message.	
Options	1	Transmit options bit mask according to the following defines from AF.h: bit 1: sets 'Wildcard Profile ID'; bit 4: turns on/off 'APS ACK'; bit 5 sets 'discover route'; bit 6 sets 'APS security'; bit 7 sets 'skip routing'. (This doesn't apply for	

an inter-pan message.)

Radius 1 Specifies the number of hops allowed delivering the message (reference DEF\_NWK\_RADIUS.)

Length of the data. If a large data length causes the MT command to exceed MT\_RPC\_DATA\_MAX, then zero bytes of the data shall be sent with this request and the data shall be transferred in as many MT\_AF\_DATA\_STORE requests as necessary.

Data 0-128 0-128 bytes data

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x64	Cmd1 = 0x02	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.2.1.4 AF\_DATA\_REQUEST\_SRC\_RTG

## **Description**:

This command is used by the tester to build and send a message through AF layer using source routing.

## Usage:

#### **SREQ:**



Byte: 1	2	1	1	1	1	2N	1	0-128
SrcEndpoint	ClusterId	TransId	Options	Radius	Relay Count (N)	RelayList	Len	Data

# **Attributes**:

Attribute	Length (byte)	Description
DstAddr	2	Short address of the destination device
DstEndpoint	1	Endpoint of the destination device
SrcEndpoint	1	Endpoint of the source device
ClusterId	2	Specifies the cluster ID
TransId	1	Specifies the transaction sequence number of the message.
Options	1	Transmit options bit mask: Bit 0: turns on/off 'APS ACK'; bit 2 sets 'APS security'; bit 3 sets 'skip routing'.
Radius	1	Specifies the number of hops allowed delivering the message (reference DEF_NWK_RADIUS.)
Relay Count	1	Specifies the number of devices in the relay list for source routing
Relay List	2N	List of relay devices on the source routing path. For each device, it contains 2 bytes short address for each device.
Len	1	Length of the data.
Data	0-128	0-128 bytes data

# **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x64	Cmd1 = 0x03	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Memory Failure (0x01).

# 3.2.1.5 AF\_INTER\_PAN\_CTL

# **Description**:

Inter-Pan control command and data. The data content depends upon the command and the available commands are enumerated as InterPanCtl\_t.

# Usage:

## **SREQ:**

Byte: 1	1	1	1	0-3
Length = 0x01-0x04	Cmd0 = 0x24	Cmd1 = 0x10	Command	Data

#### Data:

Command	Data Length (byte)	Description
0: InterPanClr	0	Proxy call to StubAPS_SetIntraPanChannel() to switch channel back to the NIB-specified channel.
1: InterPanSet	1	Proxy call to StubAPS_SetInterPanChannel() with the 1-byte channel specified.
2: InterPanReg	1	If the 1-byte Endpoint specified by the data argument is found by invoking afFindEndPointDesc(), then proxy a call to StubAPS_AppRegister () with the pointer to the endPointDesc_t found (i.e. the Endpoint must already be registered with AF).
3: InterPanChk	3	Proxy a call to StubAPS_InterPan() with the 2-byte PanId (LSB:MSB) and 1-byte EndPoint data.

## **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x64	Cmd1 = 0x10	Status

Attribute	Length (byte)	Description
		Success (0)
Chatana	1	Failure (0x01) if a channel change is in progress
Status	1	Invalid_Parameter (0x02).
		ZApsNotAllowed (0xBA) if MAC is not in an Idle state.

# 3.2.1.6 AF\_ DATA\_STORE

# **Description**:

Huge AF data request data buffer store command and data.

## Usage:

# **SREQ:**

Byte: 1	1	1	2	1	0-252
Length = $0x03-0xFA$	Cmd0 = 0x24	Cmd1 = 0x11	Index	Length	Data

## **Attributes**:

Command	Length (byte)	Description
Index	2	Specifies the index into the outgoing data request data buffer to start the storing of this chunk of data.
		Specifies the length of this data chunk to store.
Length	1	A length of zero is special and triggers the actually sending of the data request OTA.
Data	0-252	Contains 0 to 252 bytes of data.

## **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x64	Cmd1 = 0x11	AF-Status

Attribute	Length (byte)	Descript	ion
		afStatus_SUCCESS	0x00
		afStatus_FAILED	0x01
		afStatus_MEM_FAIL	0x10
Status	1	afStatus_INVALID_PARAMETER	0x02
		Note that the status is for of data when Length is not return value of the AF_Data is zero.	zero and the

# 3.2.1.7 AF\_ DATA\_RETRIEVE

# **Description**:

Huge AF incoming message data buffer retrieve command.

## Usage:

# **SREQ:**

Byte: 1	1	1	4	2	1
Length = $0x07$	Cmd0 = 0x24	Cmd1 = 0x12	Timestamp	Index	Length

## **Attributes**:

Command	Length	Description
Timestamp	4	The timestamp of the incoming message in order to uniquely Identify it in a queue of incoming huge messages.
Index	2	Specifies the index into the incoming message data buffer to start the retrieving of this chunk of data.
		Specifies the length of this data chunk to retrieve.
Length	1	A length of zero is special and triggers the freeing of the corresponding incoming message.

## **SRSP:**

Byte: 1	1	1	1	1	0-253
Length = $0x02-0xFA$	Cmd0 = 0x64	Cmd1 = 0x12	AF-Status	Length	Data

Attribute	Length (byte)	Description
		afStatus_SUCCESS 0x00
Status		afStatus_FAILED 0x01
Status	1	afStatus_MEM_FAIL 0x10
		afStatus_INVALID_PARAMETER 0x02
Length	1	Specifies the length of this data chunk retrieved.
Data	0-253	The length of data bytes requested from the specified index into the huge incoming message data buffer.

# 3.2.1.8 AF\_APSF\_CONFIG\_SET

# **Description**:

 $MT\ proxy\ for\ af APSF\_ConfigSet().$ 

# Usage:

# **SREQ:**

Byte: 1	1	1	1	1	1
Length = $0x03$	Cmd0 = 0x24	Cmd1 = 0x13	endPoint	frameDelay	windowSize

## **Attributes**:

Command	Length	Description
endpoint	1	The specific EndPoint for which to set the fragmentation configuration.
frameDelay	1	The APS Fragmentation inter-frame delay in milliseconds (delay between frame fragments within the window).
windowSize	1	The APS Fragmentation window size (number of frames between APS acknowledge from receiving node).

# **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x64	Cmd1 = 0x13	AF-Status

Attribute	Length (byte)		Description
Status	1	afStatus_SUCCESS	0x00
Status	1	afStatus_INVALID_PARAMETER	0x02

# 3.2.2 MT\_AF Callbacks

# 3.2.1.1 AF\_DATA\_CONFIRM

## **Description:**

This command is sent by the device to the user after it receives a data request.

#### Usage:

## **AREQ:**

Byte: 1	1	1	1	1	1
Length = $0x03$	Cmd0 = 0x44	Cmd1 = 0x80	Status	Endpoint	TransId

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).
Endpoint	1	Endpoint of the device
TransId	1	Specified the transaction sequence number of the message

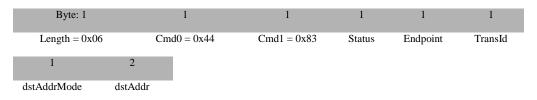
# 3.2.1.2 AF\_REFLECT\_ERROR

## **Description:**

This command is sent by the device to the user when it determines that an error occurred during a reflected message.

## **Usage:**

#### **AREQ:**



Attribute	Length (byte)	Description
Status	1	Contains the error indication (ie. ZApsNoAck)
Endpoint	1	Endpoint of the device
TransId	1	Specified the transaction sequence number of the message
dstAddrMode	1	Destination address type: 0 - short address, 1 - group address
dstAddr	2	Destination address - depends on dstAddrMode

# 3.2.1.3 AF\_INCOMING\_MSG

WasBroadcast

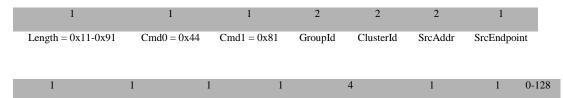
LinkQuality

#### **Description:**

This callback message is in response to incoming data to any of the registered endpoints on this device.

#### Usage:

#### AREQ:



SecurityUse

Timestamp

TransSeqNumber

Len

Data

#### Attributes:

DstEndpoint

Attribute	Length (byte)	Description	
GroupId	2	Specifies the group ID of the device	
ClusterId	2	Specifies the cluster Id (only the LSB is used in V1.0 networks.)	
SrcAddr	2	Specifies the ZigBee network address of the source device sending the message.	
SrcEndpoint	1	Specifies the source endpoint of the message	
DstEndpoint	1	Specifies the destination endpoint of the message	
WasBroadcast	1	Specifies if the message was a broadcast or not	
LinkQuality	1	Indicates the link quality measured during reception	
SecurityUse	1	Specifies if the security is used or not	
TimeStamp	4	Specifies the timestamp of the message	
TransSeqNumber	1	Specifies transaction sequence number of the message	
Len 1 Specifies the length of the data.		Specifies the length of the data.	
Data	0-128	Contains 0 to 128 bytes of data.	

# 3.2.1.4 AF\_INCOMING\_MSG\_EXT

#### **Description:**

This callback message is in response to incoming data to any of the registered endpoints on this device when the code is compiled with the INTER\_PAN flag defined. This extended incoming message indication must also be used when handling an incoming message with a huge data byte count which is defined to be a size that would cause the RPC request to exceed the maximum allowed size:

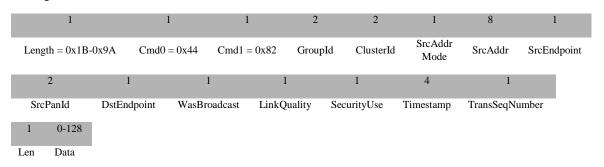
```
MT_RPC_DATA_MAX - sizeof(AF_INCOMING_MSG_EXT)
```

Where sizeof (AF\_ INCOMING\_MSG\_EXT) counts everything but the data bytes and now stands at 27. An AF\_INCOMING\_MSG\_EXT with a huge data byte count indication shall not contain any data bytes. The huge data buffer must be retrieved separately as a sequence of one or more AF\_DATA\_RETRIEVE requests. Note that the incoming huge message is timed-out in 15 seconds after receiving it; thus all AF\_DATA\_ RETRIEVE requests must be completed within 15 seconds of an AF\_INCOMING\_MSG\_EXT with a huge data byte count. Note that multiple AF\_INCOMING\_MSG\_EXT indications with huge data byte counts may be queued, and each will be timed-out separately. The default timeout can be changed by defining the following to other values:

```
#if !defined MT_AF_EXEC_CNT
#define MT_AF_EXEC_CNT 15
#endif
#if !defined MT_AF_EXEC_DLY
#define MT_AF_EXEC_DLY 1000
#endif
```

#### **Usage:**

#### AREO:



Attribute	Length (byte)	Description
GroupId	2	Specifies the group ID of the device
ClusterId	2	Specifies the cluster Id (only the LSB is used in V1.0 networks.)
SrcAddrMode	1	A value of 3 (i.e. the enumeration value for 'afAddr64Bit') indicates 8-byte/64-bit address mode; otherwise, only the 2 LSB's of the 8 bytes are used to form a 2-byte short address.
SrcAddr	8	LSB to MSB for the long or short address of the destination device (upper 6 bytes are don't care when short address.)
SrcEndpoint	1	Specifies the source endpoint of the message
SrcPanId	2	Specifies the source PanID of the message.
DstEndpoint	1	Specifies the destination endpoint of the message

WasBroadcast 1 Specifies if the		Specifies if the message was a broadcast or not	
LinkQuality 1 Indicates		ndicates the link quality measured during reception	
SecurityUse 1 Specifies if the security is used or not		Specifies if the security is used or not	
TimeStamp 4		Specifies the timestamp of the message	
TransSeqNumber 1		Specifies transaction sequence number of the message	
Len	2	Specifies the length of the data. If a large data length causes the MT command to exceed MT_RPC_DATA_MAX, then zero bytes of the data shall be sent with this request and the host shall retrieve the data with as many MT_AF_DATA_RETRIEVE requests as necessary.	
Data	0-128	Contains 0 to 128 bytes of data.	

# 3.3 MT\_APP

This interface allows tester to interact with APP layer of the target to control custom tests such as test profile or user-defined test.

# 3.3.1 MT\_APP Commands

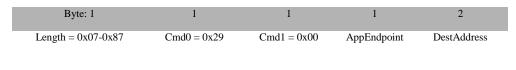
# **3.3.1.1 APP\_MSG**

#### **Description:**

This command is sent to the target in order to test the functions defined for individual applications. This command sends a raw data to an application.

## **Usage:**

## **SREQ:**



1	2	1	0-128
DestEndpoint	ClusterId	MsgLen	Message

#### **Attributes**:

Attribute	Length (byte)	Description
AppEndpoint	1	Application endpoint of the outgoing message
DestAddress	2	Destination address of the outgoing message
DestEndpoint	1	Destination endpoint of the outgoing message
ClusterId	2	Cluster Id of the outgoing message
MsgLen	1	Length of the outgoing message
Message	0-128	Raw data packet to send to the application

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x69	Cmd1 = 0x00	Status

#### **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.3.1.2 APP\_USER\_TEST

# **Description:**

This command is used by tester to issue user's defined commands to the application.

# Usage:

# **SREQ:**

Byte: 1	1	1	1	2	2	2
Length = $0x07$	Cmd0 = 0x29	Cmd1 = 0x01	SrcEP	CommandId	Parameter1	Parameter2

Attribute	Length (byte)	Description
SrcEP	1	Source Endpoint of the user-defined command
CommandId	2	Command Id of the user-defined command
Parameter1	2	Parameter #1 of the command
Parameter2	2	Parameter #2 of the command

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x69	Cmd1 = 0x01	Status

#### **Attributes:**

Attribute	Length (byte)	Description	
Status	1	Status is either Success (0) or Failure (1).	

## 3.3.2 MT\_APP Callbacks

NONE

# 3.4 MT\_DEBUG

This interface allows tester to control the debug-messaging mechanism such as debug threshold, debug messages, etc.

# 3.4.1 MT\_DEBUG Commands

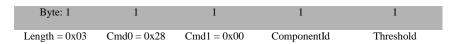
# 3.4.1.1 DEBUG\_SET\_THRESHOLD

## **Description**:

This command allows the user to set the threshold for the debug message.

## Usage:

#### **SREQ:**



#### **Attributes**:

Attribute	Length (byte)	Description
ComponentId	1	Uniquely Identifies a particular software component on the target
Threshold	1	Specifies the threshold value for reporting debug messages by that software component

#### SRSP:

Byte: 1	1	1	1

 $Length = 0x01 \qquad \qquad Cmd0 = 0x68 \qquad \qquad Cmd1 = 0x00 \qquad \qquad Status$ 

#### **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# **3.4.1.2 DEBUG\_MSG**

## **Description:**

This command sends a debug string to Z-Tool. The content of the string is defined by the application.

## **Usage:**

## **AREQ:**

Byte: 1	1	1	1	0-254
Length = $0x01-0xFA$	Cmd0 = 0x48	Cmd1 = 0x00	Length	String

#### **Attributes:**

Attribute	Length (byte)	Description
Length	1	Length of the string
String	0-254	String to be displayed by Z-Tool 2.0

# 3.4.2 MT\_DEBUG Callbacks

**NONE** 

# 3.5 MT\_MAC

This interface allows tester to interact with the TI-MAC

# 3.5.1 MT\_MAC Commands

# 3.5.1.1 MAC\_RESET\_REQ

# **Description:**

This command is used to send a MAC Reset command to reset MAC state machine.

## **Usage:**

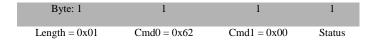
## **SREQ:**

Byte: 1	1	1	1
Length = $0x02$	Cmd0 = 0x22	Cmd1 = 0x01	SetDefault

#### **Attributes:**

Attribute	Length (byte)	Description
SetDefault	1	TRUE – Set the MAC PIB values to default values.

## SRSP:



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.5.1.2 **MAC\_INIT**

# **Description:**

This command is used to initialize the MAC.

# Usage:

# **SREQ:**

Byte: 1	1	1
Length = $0x00$	Cmd0 = 0x22	Cmd1 = 0x02

## **Attributes**:

None

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x02	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.5.1.3 MAC\_START\_REQ

## **Description:**

This command is used to start the MAC as a coordinator or end device.

## Usage:

## **SREQ:**



BeaconOrder	SuperFrameOrder	PanCoordinator	BatteryLifeExt	CoordRealignment	RealignKeySource

Byte: 1	1	1	8	1
RealignSecurityLevel	RealignKeyIdMode	RealignKeyIndex	BeaconKeySource	BeaconSecurityLevel

Byte: 1

BeaconKeyIdMode BeaconKeyIndex

# Attribute

Attributes:				
Attribute	Length (byte)	Description		
StartTime	4	The time to begin transmitting beacons relative to the received beacon		
PanId	2	The PAN Id to use. This parameter is ignored if Pan Coordinator is FALSE		
LogicalChannel	1	The logical channel to use. This parameter is ignored if Pan Coordinator is FALSE		
ChannelPage	1	The channel page to use. This parameter is ignored if Pan Coordinator is FALSE		
BeaconOrder	1	The exponent used to calculate the beacon interval		
SuperFrameOrder	1	The exponent used to calculate the superframe duration		
PanCoordinator	1	Set to TRUE to start a network as PAN coordinator		
BatteryLifeExt	1	If this value is TRUE, the receiver is disabled after MAC_BATT_LIFE_EXT_PERIODS full backoff periods following the interframe spacing period of the beacon frame		
CoordRealignment	1	Coordinator Realignment		
RealignKeySource	8	Key Source of this data frame		
		Security Level of this data frame:		
		Security Level Value		
		NO_SECURITY 0x00		

RealignSecurityLevel

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

RealignKeyIdMode	1
------------------	---

Key Id Mode	Value
NOT_USED	0x00
KEY_1BYTE_INDEX	0x01
KEY_4BYTE_INDEX	0x02
KEY_8BYTE_INDEX	0x03

Realign Key Index1 Key Index of this data frame

BeaconKeySource 8

Key Source of this data frame

#### Security Level of this data frame:

BeaconSecurityLevel 1

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

BeaconKeyIdMode 1

Key Id Mode of this data frame

BeaconKeyIndex 1

Key Index of this data frame

## SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x03	Status

#### **Attributes**:

Attrib	ute Length	(byte)	Description
Stati	is 1	Status is either S	Success (0) or Failure (1).

# 3.5.1.4 MAC\_SYNC\_REQ

## **Description:**

This command is used to request synchronization to the current network beacon

# Usage:

# **SREQ:**

Byte: 1	1	1	1	1	1
Length = $0x03$	Cmd0 = 0x22	Cmd1 = 0x04	LogicalChannel	ChannelPage	TrackBeacon

#### **Attributes**:

Attribute	Length (byte)	Description
LogicalChannel	1	The logical channel to use.
ChannelPage	1	The channel page to use.
TrackBeacon	1	Set to TRUE to continue tracking beacons after synchronizing with the first beacon. Set to FALSE to only synchronize with the first beacon

## SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x04	Status

Attribute	Length (byte)	Description	
Status	1	Status is either Success (0) or Failure (1).	

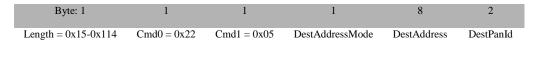
# 3.5.1.5 MAC\_DATA\_REQ

# **Description:**

This command is used to send (on behalf of the next higher layer) MAC Data Frame packet.

# Usage:

# **SREQ:**



Byte: 1	1	1	1	1	8	1	1
SrcAddressMode	Handle	TxOption	LogicalChannel	Power	KeySource	SecurityLevel	KeyIdMode

Byte: 1	1	0-250
KevIndex	MSDULength	MSDU

#### **Attributes:**

Handle

Attribute	Length (byte)	Description
		Specifies the format of the destination address.

Mode Value Description ADDRESS\_NOT\_PRESENT 0x00Address Not Present DestAddressMode 1 GROUP\_ADDRESS 0x01Group address ADDRESS\_16\_BIT 0x02 Address 16 bit ADDRESS\_64\_BIT Address 64 bit 0x03 BROADCAST 0xFF Broadcast DestAddress 8 Address of the destination. DestPanId PAN Id of the destination. 2 Specifies the format of the source address. Mode Value Description ADDRESS\_NOT\_PRESENT 0x00 Address Not Present SrcAddressModeGROUP\_ADDRESS 0x01 Group address ADDRESS\_16\_BIT Address 16 bit 0x02 ADDRESS\_64\_BIT Address 64 bit 0x03 BROADCAST 0xFF Broadcast

Handle of the packet.

#### Transmitting options:

Option	Value	Description
MAC_TXOPTION_ACK	0x01	Acknowledged transmission. The MAC will attempt to retransmit the frame until it is acknowledged
MAC_TXOPTION_GTS	0x02	GTS transmission (unused)
MAC_TXOPTION_INDIRECT	0x04	Indirect transmission. The MAC will queue the data and wait for the destination device to poll for it. This can only be used by a coordinator device
MAC_TXOPTION_NO_RETRANS	0x10	This proprietary option prevents the frame from being retransmitted
MAC_TXOPTION_NO_CNF	0x20	This proprietary option prevents a MAC_MCPS_DATA_CNF event from being sent for this frame
MAC_TXOPTION_ALT_BE	0x40	Use PIB value MAC_ALT_BE for the minimum backoff exponent
MAC_TXOPTION_PWR_CHAN	0x80	Use the power and channel values in macDataReq_t instead of the PIB values

TxOption 1

LogicalChannel 1

Channel that data frame will be transmitted.

Power 1

Power level that data frame will be transmitted.

KeySource 8

Key Source of this data frame.

Security Level of this data frame:

SecurityLevel 1

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

		Key Id Mode	Value
KeyIdMode	1	NOT_USED	0x00
		KEY_1BYTE_INDEX	0x01
		KEY_4BYTE_INDEX	0x02
		KEY_8BYTE_INDEX	0x03
KeyIndex	1	Key Index of this data frame.	
MSDULength	1	Length of the data.	
MSDU	0-250	Actual data that will be sent.	

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x05	Status

#### **Attributes:**

Attribute	Length (byte)	Description	
Status	1	Status is either Success (0) or Failure (1).	

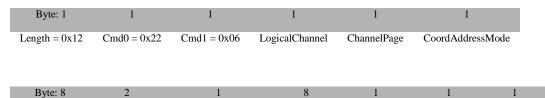
# 3.5.1.6 MAC\_ASSOCIATE\_REQ

## **Description:**

This command is used to request (on behalf of the next higher layer) an association with a coordinator

## **Usage:**

#### **SREQ:**



KeySource

SecurityLevel

KeyIdMode

KeyIndex

CapabilityInformation

Attribute	Length (byte)	Description					
LogicalChannel	1	Channel that data frame will be transmitted.					
ChannelPage	1	The channel page to be used.					
		Specifies the format of the coordin	Specifies the format of the coordinator address.				
		Mode	Value	Description			
CoordAddressMode	1	ADDRESS_NOT_PRESENT	0x00	Address Not Present			
2007411441255271042	•	GROUP_ADDRESS	0x01	Group address			
		ADDRESS_16_BIT	0x02	Address 16 bit			
		ADDRESS_64_BIT	0x03	Address 64 bit			
		BROADCAST	0xFF	Broadcast			
CoordAddress	8	Address of the Coordinator.		<u> </u>			
CoordPanId	2	PAN Id of the coordinator.					
		Bit map which specifies the operat	tional capa	bilities of the device.			
		Bit: 0 – Alternate PAN Coordinate	or				
		1 – Device type: 1- ZigBee Router; 0 – End Device					
2 – Power Source: 1 Main powered							
CapabilityInformation 1 3 – Receiver on when Idle							
		4 – Reserved					
		5 – Reserved					
		6 – Security capability					
		7 – Reserved					
KeySource	8	Key Source of this data frame					
		Security Level of this data frame:					
		Security Level	Value	1			
		NO_SECURITY	0x00	-			
SecurityLevel 1		MIC_32_AUTH	0x01	_			
		MIC_64_AUTH	0x02	_			
		MIC_128_AUTH 0x03					
		AES_ENCRYPTION	0x04	-			

AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

KeyIdMode

Key Id Mode	Value
NOT_USED	0x00
KEY_1BYTE_INDEX	0x01
KEY_4BYTE_INDEX	0x02
KEY_8BYTE_INDEX	0x03

KeyIndex

Key Index of this data frame.

## SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x06	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.5.1.7 MAC\_ASSOCIATE\_RSP

# **Description:**

This command is sent by the host to response to the MAC\_ASSOCIATE\_IND.

## **Usage:**

## **SREQ:**

Byte: 1	1	1	8	2	1
Length = $0x0B$	Cmd0 = 0x42	Cmd1 = 0x50	ExtAddr	AssocShortAddress	AssocStatus

#### **Attributes:**

Attribute	Length (byte)	Descript	tion
ExtAddr	8	Extended Address of the device reque	sting association
AssocShortAddress	2	Short address for the associated device	e. Allocated by the coordinator.
		Status of the association:	
AssocStatus	1	Status	Value
		SUCCESSFUL_ASSOCIATION	0x00

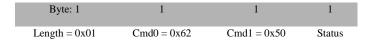
PAN\_AT\_CAPACITY

PAN\_ACCESS\_DENIED

0x01

0x02

## SRSP:



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.5.1.8 MAC\_DISASSOCIATE\_REQ

## **Description:**

This command is used to request (on behalf of the next higher layer) a disassociation of the device from the coordinator.

# Usage:

## **SREQ:**

Byte: 1	1	1	1	8	2
Length = 0x18	Cmd0 = 0x22	Cmd1 = 0x07	DeviceAddressMode	DeviceAddress	DevicePanId
Byte: 1	1	8	1	1	1
DisassociateReaso	n TxIndirect	KeySource	SecurityLevel	KeyIdMode	KeyIndex

Attribute	Length (byte)	Descri	iption	
		Specifies the format of the device a	ddress.	
		Mode	Value	Description
		ADDRESS_NOT_PRESENT	0x00	Address Not Present
DeviceAddressMode	1	GROUP_ADDRESS	0x01	Group address
		ADDRESS_16_BIT	0x02	Address 16 bit
		ADDRESS_64_BIT	0x03	Address 64 bit
		BROADCAST	0xFF	Broadcast
DeviceAddress	8	Device Address.		
DevicePanId	2	Network PAN Id of device.		
		Reason of disassociation:		
DisassociateReason	1	Reason	Value	1
DisassociateReason	1	RESERVED	0x00	1
		COOR_WISHES_DEV_LEAVE	0x01	1
		DEV_WISHES_LEAVE	0x02	
TxIndirect	1	Tx indirect		
KeySource	8	Key Source of this data frame.		

SecurityLevel

#### Security Level of this data frame:

Value Security Level NO\_SECURITY 0x00 MIC\_32\_AUTH 0x01 MIC\_64\_AUTH 0x02 1 MIC\_128\_AUTH 0x03 AES\_ENCRYPTION 0x04 AES\_ENCRYPTION\_MIC\_32 0x05 AES\_ENCRYPTION\_MIC\_64 0x06 AES\_ENCRYPTION\_MIC\_128 0x07

Key Id Mode of this data frame:

KeyIdMode 1

Key Id Mode	Value
NOT_USED	0x00
KEY_1BYTE_INDEX	0x01
KEY_4BYTE_INDEX	0x02
KEY_8BYTE_INDEX	0x03

KeyIndex 1

Key Index of this data frame.

#### SRSP:



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# **3.5.1.9 MAC\_GET\_REQ**

# **Description:**

This command is used to read (on behalf of the next higher layer) a MAC PIB attribute.

#### Usage:

#### **SREQ:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x22	Cmd1 = 0x08	Attribute

#### **Attributes:**

Attribute Length (byte) Description

Specifies the MAC PIB Attributes:

MAC PIB Attribute Value ZMAC\_ACK\_WAIT\_DURATION 0x40 ZMAC\_ASSOCIATION\_PERMIT 0x41 ZMAC\_AUTO\_REQUEST 0x42 ZMAC\_BATT\_LIFE\_EXT 0x43 ZMAC\_BATT\_LEFT\_EXT\_PERIODS 0x44 ZMAC\_BEACON\_MSDU 0x45 ZMAC\_BEACON\_MSDU\_LENGTH 0x46 ZMAC\_BEACON\_ORDER 0x47 ZMAC\_BEACON\_TX\_TIME 0x48 ZMAC\_BSN 0x49 ZMAC\_COORD\_EXTENDED\_ADDRESS 0x4A ZMAC\_COORD\_SHORT\_ADDRESS 0x4B ZMAC\_DSN 0x4C ZMAC\_GTS\_PERMIT 0x4D ZMAC\_MAX\_CSMA\_BACKOFFS 0x4E ZMAC\_MIN\_BE 0x4F ZMAC\_PANID 0x50 ZMAC\_PROMISCUOUS\_MODE 0x51

Attribute 1

ZMAC_RX_ON_IDLE	0x52
ZMAC_SHORT_ADDRESS	0x53
ZMAC_SUPERFRAME_ORDER	0x54
ZMAC_TRANSACTION_PERSISTENCE_TIME	0x55
ZMAC_ASSOCIATED_PAN_COORD	0x56
ZMAC_MAX_BE	0x57
ZMAC_FRAME_TOTAL_WAIT_TIME	0x58
ZMAC_MAC_FRAME_RETRIES	0x59
ZMAC_RESPONSE_WAIT_TIME	0x5A
ZMAC_SYNC_SYMBOL_OFFSET	0x5B
ZMAC_TIMESTAMP_SUPPORTED	0x5C
ZMAC_SECURITY_ENABLED	0x5D
ZMAC_PHY_TRANSMIT_POWER	0xE0
ZMAC_LOGICAL_CHANNEL	0xE1
ZMAC_EXTENDED_ADDRESS	0xE2
ZMAC_ALT_BE	0xE3

## SRSP:

ı	Byte: 1	1	1	1	16
ľ	Length = $0x11$	Cmd0 = 0x62	Cmd1 = 0x08	Status	Data

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).
Data	16	1-16 bytes value of the PIB attribute.

# **3.5.1.10** MAC\_SET\_REQ

# **Description:**

This command is used to request the device to write a MAC PIB value.

# Usage:

# **SREQ:**

Byte: 1	1	1	1	16
Length = $0x11$	Cmd0 = 0x22	Cmd1 = 0x09	Attribute	AttributeValue

## **Attributes:**

Attribute Length (byte)	Description
-------------------------	-------------

Specified the MAC PIB Attribute:

MAC PIB Attribute

WINC TIB FAUTOUC	varae
ZMAC_ACK_WAIT_DURATION	0x40
ZMAC_ASSOCIATION_PERMIT	0x41
ZMAC_AUTO_REQUEST	0x42
ZMAC_BATT_LIFE_EXT	0x43
ZMAC_BATT_LEFT_EXT_PERIODS	0x44
ZMAC_BEACON_MSDU	0x45
ZMAC_BEACON_MSDU_LENGTH	0x46
ZMAC_BEACON_ORDER	0x47
ZMAC_BEACON_TX_TIME	0x48
ZMAC_BSN	0x49
ZMAC_COORD_EXTENDED_ADDRESS	0x4A
ZMAC_COORD_SHORT_ADDRESS	0x4B
ZMAC_DSN	0x4C
ZMAC_GTS_PERMIT	0x4D
ZMAC_MAX_CSMA_BACKOFFS	0x4E
ZMAC_MIN_BE	0x4F
ZMAC_PANID	0x50
ZMAC_PROMISCUOUS_MODE	0x51

Attribute 1

ZMAC_RX_ON_IDLE	0x52
ZMAC_SHORT_ADDRESS	0x53
ZMAC_SUPERFRAME_ORDER	0x54
ZMAC_TRANSACTION_PERSISTENCE_TIME	0x55
ZMAC_ASSOCIATED_PAN_COORD	0x56
ZMAC_MAX_BE	0x57
ZMAC_FRAME_TOTAL_WAIT_TIME	0x58
ZMACMAC_FRAME_RETRIES	0x59
ZMAC_RESPONSE_WAIT_TIME	0x5A
ZMAC_SYNC_SYMBOL_OFFSET	0x5B
ZMAC_TIMESTAMP_SUPPORTED	0x5C
ZMAC_SECURITY_ENABLED	0x5D
ZMAC_PHY_TRANSMIT_POWER	0xE0
ZMAC_LOGICAL_CHANNEL	0xE1
ZMAC_EXTENDED_ADDRESS	0xE2
ZMAC_ALT_BE	0xE3

AttributeValue

16

1-16 bytes of the PIB attribute value.

# SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x09	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.5.1.11 MAC\_SCAN\_REQ

# **Description:**

This command is used to send a request to the device to perform a network scan.

## Usage:

## **SREQ:**

Byte: 1	1	1	4	1	1
Length = $0x13$	Cmd0 = 0x22	Cmd1 = 0	x0C ScanChar	nnels ScanTy	pe ScanDuration
Byte: 1	1	8	1	1	1
ChannelPage	MaxResults	KeySource	SecurityLevel	KeyIdMode	KeyIndex

## **Attributes:**

Attribute	Length (byte)	Description	

This represents a bit-mask of channels to be scanned when starting the device:

Channel	Value	channe starting
NONE	0x00000000	
ALL_CHANNELS	0x07FFF800	
CHANNEL 11	0x00000800	
CHANNEL 12	0x00001000	
CHANNEL 13	0x00002000	
CHANNEL 14	0x00004000	
CHANNEL 15	0x00008000	
CHANNEL 16	0x00010000	
CHANNEL 17	0x00020000	
CHANNEL 18	0x00040000	
CHANNEL 19	0x00080000	
CHANNEL 20	0x00100000	
CHANNEL 21	0x00200000	
CHANNEL 22	0x00400000	
CHANNEL 23	0x00800000	
CHANNEL 24	0x01000000	
CHANNEL 25	0x02000000	

ScanChannels 4

CHANNEL 26	0x04000000

ScanType 1

Scan Type	Value
ENERGY_DETECT	0x00
ACTIVE	0x01
PASSIVE	0x02
ORPHAN	0x03

ScanDuration 1

Duration of the scan - The exponent used in the scan duration calculation.

ChannelPage 1

The channel page on which to perform the scan.

KeySource 8

Key Source of this data frame.

Security Level of this data frame:

SecurityLevel

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

 Key Id Mode
 Value

 KeyIdMode
 1

 NOT\_USED
 0x00

 KEY\_1BYTE\_INDEX
 0x01

 KEY\_4BYTE\_INDEX
 0x02

 KEY\_8BYTE\_INDEX
 0x03

 KeyIndex
 1

 Key Index of this data frame.

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x0C	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

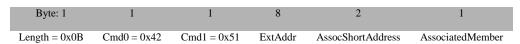
# 3.5.1.12 MAC\_ORPHAN\_RSP

## **Description:**

This command is sent by the host to response to the ORPHAN\_IND.

#### Usage:

# **SREQ:**



Attribute	Length (byte)	Description
ExtAddr	8	Extended Address of the device sending the orphan notification
AssocShortAddress	2	Short address of the orphan device
AssociatedMember	1	TRUE if the orphan is an associated member. FALSE otherwise.

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x51	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

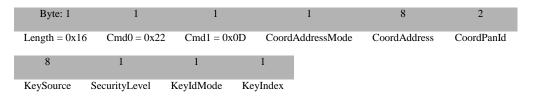
# 3.5.1.13 MAC\_POLL\_REQ

# **Description:**

This command is used to send a MAC data request poll.

## **Usage:**

# **SREQ:**



Attribute	Length (byte)	Description		
		Mode	Value	Description
		ADDRESS_NOT_PRESENT	0x00	Address Not Present
CoordAddressMode	1	GROUP_ADDRESS	0x01	Group address
		ADDRESS_16_BIT	0x02	Address 16 bit
		ADDRESS_64_BIT	0x03	Address 64 bit

BROADCAST	0xFF	Broadcast

CoordAddress 8 64-bit Coordinator Address

CoordPanId 2 Coordinator PanId

KeySource 8 Key Source of this data frame.

Security Level of this data frame:

SecurityLevel 1

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

KeyIdMode 1

Key Id Mode	Value
NOT_USED	0x00
KEY_1BYTE_INDEX	0x01
KEY_4BYTE_INDEX	0x02
KEY_8BYTE_INDEX	0x03

KeyIndex 1

Key Index of this data frame.

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x0D	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.5.1.14 MAC\_PURGE\_REQ

# **Description:**

This command is used to send a request to the device to purge a data frame

# Usage:

#### **SREQ:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x22	Cmd1 = 0x0E	MsduHandle

#### **Attributes:**

Attribute	Length (byte)	Description
MsduHandle	1	Msdu Handle

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x62	Cmd1 = 0x0E	Status

#### **Attributes:**

	Attribute	Length (byte)	Description
_	Status	1	Status is either Success (0) or Failure (1).

# 3.5.1.15 MAC\_SET\_RX\_GAIN\_REQ

## **Description:**

This command is used to send a request to the device to set Rx gain.

## **Usage:**

## **SREQ:**



## **Attributes:**

Attribute	Length (byte)	Description
Mode	1	PA/PNA mode – TRUE/FALSE

## SRSP:



## **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.5.2 MT\_MAC Callbacks

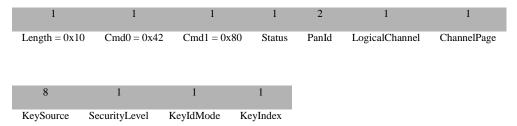
# 3.5.2.1 MAC\_SYNC\_LOSS\_IND

## **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) an indication of the synchronization loss.

## Usage:

## AREQ:



Attribute	Length (byte)	Description

Status	1	This field indicates either SUCCESS (0) or FAILURE (1).
PanId	2	PAN Id of the device
LogicalChannel	1	Logical Channel of the device where the synchronization is lost
ChannelPage	1	Channel Page of the device where the synchronization is lost
KeySource	8	Key Source of this data frame.
		Security Level of this data frame:

SecurityLevel 1

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

KeyIdMode 1

Key Id Mode	Value
NOT_USED	0x00
KEY_1BYTE_INDEX	0x01
KEY_4BYTE_INDEX	0x02
KEY_8BYTE_INDEX	0x03

KeyIndex 1 Key Index of this data frame.

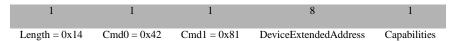
# 3.5.2.2 MAC\_ASSOCIATE\_IND

# **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) an association indication message.

## **Usage:**

## **AREQ:**





Attributes.	<b>Y</b>		
Attribute	Length (byte)		ription
DeviceExtendedAddress	8	Extended address of the device	
		Specifies the operating capabilities of Bit weighted values follow:	of the device being directly joined.
		Bit: 0 – Alternate PAN Coordinator	
		1 – Device type: 1- ZigBee Rou	ter; 0 – End Device
		2 – Power Source: 1 Main power	ered
Capabilities	1	3 – Receiver on when Idle	
		4 – Reserved	
		5 – Reserved	
		6 – Security capability	
		7 – Reserved	
KeySource	8	Key Source of this data frame.	
		Security Level of this data frame:	
		Security Level	Value
		NO_SECURITY	0x00
		MIC_32_AUTH	0x01
SecurityLevel	1	MIC_64_AUTH	0x02
SecurityLever	1	MIC_128_AUTH	0x03
		AES_ENCRYPTION	0x04
		AES_ENCRYPTION_MIC_32	0x05
		AES_ENCRYPTION_MIC_64	0x06
		AES_ENCRYPTION_MIC_128	0x07
		Key Id Mode of this data frame:	
		Key Id Mode	Value
KeyIdMode	1	NOT_USED	0x00
		KEY_1BYTE_INDEX	0x01
		KEY_4BYTE_INDEX	0x02
		KEY_8BYTE_INDEX	0x03

KeyIndex 1 Key Index of this data frame.

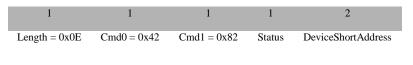
# 3.5.2.3 MAC\_ASSOCIATE\_CNF

## **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) an association confirmation message.

#### Usage:

## **AREQ:**



8	1	1	1
KeySource	SecurityLevel	KeyIdMode	KeyIndex

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).
DeviceShortAddress	2	Short address of the device
KeySource	8	Key Source of this data frame.
		Security Level of this data frame:

SecurityLevel 1

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

		Key Id Mode	Value
KeyIdMode	1	NOT_USED	0x00
		KEY_1BYTE_INDEX	0x01
		KEY_4BYTE_INDEX	0x02
		KEY_8BYTE_INDEX	0x03
KeyIndex	1	Key Index of this data frame.	II.

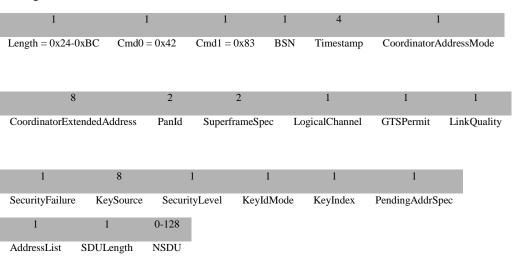
# 3.5.2.4 MAC\_BEACON\_NOTIFY\_IND

## **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC beacon notify indication.

## **Usage:**

#### AREQ:



Attribute	Length (byte)	Description
BSN	1	BSN
Timestamp	4	Timestamp of the message

#### Address mode of the coordinator

		Mode	Value	Description
		ADDRESS_NOT_PRESENT	0x00	Address Not Present
CoordinatorAddressMode	1	GROUP_ADDRESS	0x01	Group address
		ADDRESS_16_BIT	0x02	Address 16 bit
		ADDRESS_64_BIT	0x03	Address 64 bit
		BROADCAST	0xFF	Broadcast
Coordinator Extended Address	8	Extended address of the coordinate	or	
PanId	2	Pan Id of the device		
SuperframeSpec	2			
LogicalChannel	1	Current logical channel		

LinkQuality 1 Link quality of the message SecurityFailure

1

1

KeySource 8 Key Source of this data frame.

Security Level of this data frame:

TRUE/FALSE - Permit/Not permit GTS

SecurityLevel

GTSPermit

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

KeyIdMode

Key Id Mode	Value
NOT_USED	0x00
KEY_1BYTE_INDEX	0x01
KEY_4BYTE_INDEX	0x02
KEY_8BYTE_INDEX	0x03

KeyIndex

Key Index of this data frame.

Pending Addr Spec

AddressList	1	List of address associate with the device
SDULength	1	Beacon Length
NSDU	0-128	Beacon payload

# 3.5.2.5 MAC\_DATA\_CNF

## **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC data confirmation.

#### **Usage:**

#### AREQ:



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).
Handle	1	Handle of the message
Timestamp	4	64bit timestamp of the message
Timestamp2	2	16bit timestamp of the message

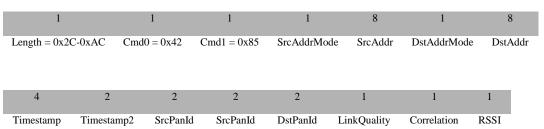
# **3.5.2.6** MAC\_DATA\_IND

#### **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC data indication.

## Usage:

#### AREQ:



1	8	1	1	1	1	0-128
DSN	KevSource	SecurityLevel	KevIdMode	KeyIndex	Length	Data

Attribute	Length (byte)	Descr	ription	
		Source address mode		
		Mode	Value	Description
		ADDRESS_NOT_PRESENT	0x00	Address Not Present
SrcAddrMode	1	GROUP_ADDRESS	0x01	Group address
		ADDRESS_16_BIT	0x02	Address 16 bit
		ADDRESS_64_BIT	0x03	Address 64 bit
		BROADCAST	0xFF	Broadcast
SrcAddr	8	Source address		
DstAddrMode	1	Destination address mode		
DstAddr	8	Destination address		
Timestamp	4	32bit timestamp of the message		
Timestamp2	2	16bit timestamp of the message		
SrcPanId	2	Pan Id of the source address		
DstPanId	2	Pan Id of the destination address		
LinkQuality	1	Link quality		
Correlation	1	Correlation		
RSSI	1	RSSI		
DSN	1	DSN		
KeySource	8	Key Source of this data frame.		
		Security Level of this data frame:		
		Security Level	Value	1
		NO_SECURITY	0x00	1
SecurityLevel	1	MIC_32_AUTH	0x01	
SecurityLever	1	MIC_64_AUTH	0x02	
		MIC_128_AUTH	0x03	1
		AES_ENCRYPTION	0x04	1
		AES_ENCRYPTION_MIC_32	0x05	
		AES_ENCRYPTION_MIC_64	0x06	
		L		_

AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

		Key Id Mode	Value
KeyIdMode	1	NOT_USED	0x00
		KEY_1BYTE_INDEX	0x01
		KEY_4BYTE_INDEX	0x02
		KEY_8BYTE_INDEX	0x03
KeyIndex	1	Key Index of this data frame.	
Length	1	Data length	
Data	0-128	Data	

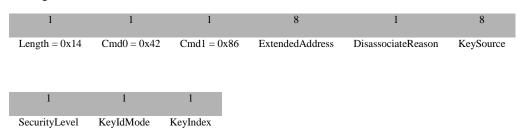
# 3.5.2.7 MAC\_DISASSOCIATE\_IND

## **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC disassociation indication.

## **Usage:**

## AREQ:



Attribute	Length (byte)	Description
ExtendedAddress	8	Extended address of the device leaving the network

Reason of the disassociation:

DisassociateReason	1	Reason	Value
		Coordinator wishes the device to disassociate	0x01
		Device itself wishes to disassociate	0x02
KeySource	8	Key Source of this data frame.	

Security Level of this data frame:

Security Level Value NO\_SECURITY 0x00 MIC\_32\_AUTH 0x01 SecurityLevel 1 MIC\_64\_AUTH 0x02 MIC\_128\_AUTH 0x03 AES\_ENCRYPTION 0x04 AES\_ENCRYPTION\_MIC\_32 0x05 AES\_ENCRYPTION\_MIC\_64 0x06 AES\_ENCRYPTION\_MIC\_128 0x07

Key Id Mode of this data frame:

		Key Id Mode	Value
KeyIdMode	1	NOT_USED	0x00
		KEY_1BYTE_INDEX	0x01
		KEY_4BYTE_INDEX	0x02
		KEY_8BYTE_INDEX	0x03
KeyIndex	1	Key Index of this data frame.	•

# 3.5.2.8 MAC\_DISASSOCIATE\_CNF

#### **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC disassociate confirm.

# Usage: AREQ:

Attribute	Length (byte)	Desc	ription	
Status	1	This field indicates either SUCCE	SS (0) or I	FAILURE (1).
		Address mode of the device		
		Mode	Value	Description
		ADDRESS_NOT_PRESENT	0x00	Address Not Present
DeviceAddrMode	1	GROUP_ADDRESS	0x01	Group address
		ADDRESS_16_BIT	0x02	Address 16 bit
		ADDRESS_64_BIT	0x03	Address 64 bit
		BROADCAST	0xFF	Broadcast
DeviceAddr	8	Address of the device		
DevicePanId	2	Pan Id of the device		

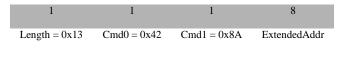
# 3.5.2.9 MAC\_ORPHAN\_IND

### **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC orphan indication.

### **Usage:**

### **AREQ:**





Attribute	Length (byte)	Description
ExtendedAddr	8	Extended address of the orphan device
KeySource	8	Key Source of this data frame.

Security Level of this data frame:

SecurityLevel 1

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:

KeyIdMode 1

Key Id Mode	Value
NOT_USED	0x00
KEY_1BYTE_INDEX	0x01
KEY_4BYTE_INDEX	0x02
KEY_8BYTE_INDEX	0x03

KeyIndex

Key Index of this data frame.

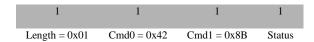
# 3.5.2.10 MAC\_POLL\_CNF

### **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC poll confirmation.

### Usage:

# **AREQ:**



Attribute	Length (byte)	Description
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).

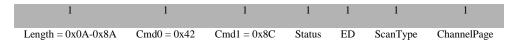
# 3.5.2.11 **MAC\_SCAN\_CNF**

#### **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC scan confirmation.

### **Usage:**

#### AREQ:



4	1	1	0-128
UnscannedChannelList	ResultListCount	ResultListMaxLength	ResultList

#### **Attributes:**

Attribute	Length (byte)	I	Description	
Status	1	This field indicates either	r SUCCESS	S (0) or FAILURE (1).
ED	1	ED max energy.		
		Scan Type	Value	Specifies the scan type:
		ENERGY_DETECT	0x00	
ScanType	1	ACTIVE	0x01	
		PASSIVE	0x02	
		ORPHAN	0x03	
ChannelPage	1	Channel Page		
UnscannedChannelList	4	List of un-scanned chann	nels	
ResultListCount	1	Number of item in the re	sult list	
ResultListMaxLength	1	Max length of the result	list in bytes	
ResultList	0-128	Result list		

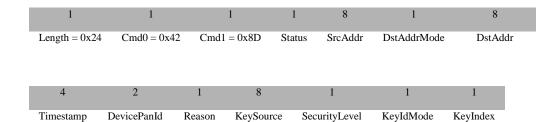
# 3.5.2.12 MAC\_COMM\_STATUS\_IND

### **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC communication indicator.

#### **Usage:**

### **AREQ:**

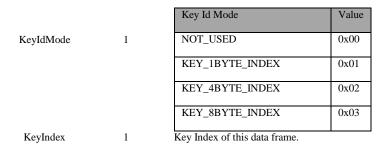


Attribute	Length (byte)	Desc	ription	
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).		
		Destination address mode		
		Mode	Value	Description
		ADDRESS_NOT_PRESENT	0x00	Address Not Present
DstAddrMode	1	GROUP_ADDRESS	0x01	Group address
		ADDRESS_16_BIT	0x02	Address 16 bit
		ADDRESS_64_BIT	0x03	Address 64 bit
		BROADCAST	0xFF	Broadcast
SrcAddr	8	Source address		1
DstAddr	8	Destination address		
Timestamp	4	Timestamp of the message		
DevicePanId	2	Pan Id of the device that generate	the indicat	ion
Reason	1	Reason for this communication in	dication.	
KeySource	8	Key Source of this data frame.		
		Security Level of this data frame:		

SecurityLevel 1

Security Level	Value
NO_SECURITY	0x00
MIC_32_AUTH	0x01
MIC_64_AUTH	0x02
MIC_128_AUTH	0x03
AES_ENCRYPTION	0x04
AES_ENCRYPTION_MIC_32	0x05
AES_ENCRYPTION_MIC_64	0x06
AES_ENCRYPTION_MIC_128	0x07

Key Id Mode of this data frame:



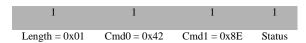
# 3.5.2.13 MAC\_START\_CNF

### **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC start confirmation.

#### Usage:

#### **AREQ:**



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).

# 3.5.2.14 MAC\_RX\_ENABLE\_CNF

### **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC Rx enable confirmation.

#### Usage:

### **AREQ:**



Attribute	Length (byte)	Description
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).

# 3.5.2.15 MAC\_PURGE\_CNF

### **Description:**

This callback is called by the MAC to send (on behalf of the next higher layer) a MAC purge confirmation.

#### Usage:

#### AREQ:



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).
Handle	1	Handle of this message

# **3.6** MT\_NWK

Not supported.

# **3.7** MT\_SAPI

Not supported

# 3.8 MT\_SYS

This interface allows the tester to interact with the target at system level such as reset, read/write memory, read/write extended address, etc.

# 3.8.1 MT\_SYS Commands

# 3.8.1.1 SYS\_RESET\_REQ

### **Description:**

This command is sent by the tester to reset the target device

#### Usage:

### **AREQ:**

1	1	1	1
Length = 0x01	Cmd0 = 0x41	Cmd1 = 0x00	Туре

#### **Attributes:**

Attribute	Length (byte)	Description
Туре	1	This command will reset the device by using a hardware reset (i.e. watchdog reset) if 'Type' is zero. Otherwise a soft reset (i.e. a jump to the reset vector) is done. This is especially useful in the CC2531, for instance, so that the USB host does not have to contend with the USB H/W resetting (and thus causing the USB host to re-enumerate the device which can cause an open virtual serial port to hang.)

# **3.8.1.2 SYS\_PING**

### **Description:**

This command issues PING requests to verify if a device is active and check the capability of the device.

### Usage:

#### **SREQ:**

1	1	1
Length = $0x00$	Cmd0 = 0x21	Cmd1 = 0x01

### **Attributes:**

None

### SRSP:

1	1	1	2
Length = $0x02$	Cmd0 = 0x61	Cmd1 = 0x01	Capabilities

Attribute	Length (byte)	Description

This field represents the interfaces that this device can handle (compiled into the device). Bit weighted and defined as:

Capabilities

Capability	Value
MT_CAP_SYS	0x0001
MT_CAP_MAC	0x0002
MT_CAP_NWK	0x0004
MT_CAP_AF	0x0008
MT_CAP_ZDO	0x0010
MT_CAP_SAPI	0x0020
MT_CAP_UTIL	0x0040
MT_CAP_DEBUG	0x0080
MT_CAP_APP	0x0100
MT_CAP_ZOAD	0x1000

# 3.8.1.3 SYS\_VERSION

### **Description:**

This command is used to request for the device's version string.

# Usage:

### **SREQ:**

1	1	1
Length = 0x00	Cmd0 = 0x21	Cmd1 = 0x02

#### **Attributes:**

None

#### SRSP:

1	1	1	1	1	1	1	1
Length = $0x05$	Cmd0 = 0x61	Cmd1 = 0x02	TransportRev	Product	MajorRel	MinorRel	MaintRel

Attribute	Length (byte)	Description
TransportRev	1	Transport protocol revision
Product	1	Product Id
MajorRel	1	Software major release number
MinorRel	1	Software minor release number
MaintRel	1	Software maintenance release number

# 3.8.1.4 SYS\_SET\_EXTADDR

### **Description:**

This command is used to set the extended address of the device.

#### Usage:

### **SREQ:**

1	1	1	8
Length = 0x08	Cmd0 = 0x21	Cmd1 = 0x03	ExtAddress

#### **Attributes:**

Attribute	Length (byte)	Description
ExtAddres	s 8	The device's extended address.

#### **SRSP:**

1	1	1	1
Length = 0x01	Cmd0 = 0x61	Cmd1 = 0x03	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (1) or Failure (0)

# 3.8.1.5 SYS\_GET\_EXTADDR

### **Description:**

This command is used to get the extended address of the device.

### **Usage:**

### **SREQ:**

1	1	1
Length = $0x00$	Cmd0 = 0x21	Cmd1 = 0x04

Attribute	Length (byte)	Description
Status	1	Status is either Success (1) or Failure (0)

#### SRSP:

1	1	1	8
Length = $0x08$	Cmd0 = 0x61	Cmd1 = 0x04	ExtAddress

#### **Attributes:**

Attribute	Length (byte)	Description
ExtAddress	8	The device's extended address.

# 3.8.1.6 SYS\_RAM\_READ

### **Description:**

This command is used by the tester to read a single memory location in the target RAM. The command accepts an address value and returns the memory value present in the target RAM at that address.

### **Usage:**

# **SREQ:**

1	1	1	2	1
Length = $0x03$	Cmd0 = 0x21	Cmd1 = 0x05	Address	Len

Attribute	Length (byte)	Description
Address	2	Address of the memory that will be read.
Len	1	The number of bytes that will be read from the target RAM.

#### **SRSP:**

1	1	1	1	1	0-128
Length = 0x02-0x82	Cmd0 = 0x61	Cmd1 = 0x05	Status	Len	Value

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).
Len	1	The number of bytes that will be read from the target RAM.
Value	0-128	The value read from the target RAM.

# 3.8.1.7 SYS\_RAM\_WRITE

# **Description:**

This command is used by the tester to write to a particular location in the target RAM. The command accepts an address location and a memory value. The memory value is written to the address location in the target RAM.

### **Usage:**

### SREQ:

1	1	1	2	1	1-128
Length = 0x04-0x84	Cmd0 = 0x21	Cmd1 = 0x06	Address	Len	Value

#### **Attributes:**

Attribute	Length (byte)	Description		
Address	2	Address of the memory that will be read.		
Len	1	The number of bytes that will be read from the target RAM.		
Value	1-128	The value written to the target RAMS.		

### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x06	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.8.1.8 SYS\_OSAL\_NV\_READ

# **Description:**

This command is used by the tester to read a single memory item from the target non-volatile memory. The command accepts an attribute Id value and data offset and returns the memory value present in the target for the specified attribute Id.

### **Usage:**

### **SREQ:**

1	1	1	2	1
Length = $0x03$	Cmd0 = 0x21	Cmd1 = 0x08	Id	Offset

#### **Attributes:**

Attribute	Length (byte)	Description
Id	2	The Id of the NV item.
Offset	1	Number of bytes offset from the beginning or the NV value.

#### SRSP:

1	1	1	1	1	0-248
Length = $0x02-0xFA$	Cmd0 = 0x61	Cmd1 = 0x08	Status	Len	Value

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).
Len	1	Length of the NV value.
Value	0-248	Value of the NV item.

# 3.8.1.9 SYS\_OSAL\_NV\_WRITE

### **Description:**

This command is used by the tester to write to a particular item in non-volatile memory. The command accepts an attribute Id, data offset, data length, and attribute value. The attribute value is written to the location specified for the attribute Id in the target.

### **Usage:**

# **SREQ:**

1	1	1	2	1	1	1-246
Length = $0x04-0xFA$	Cmd0 = 0x21	Cmd1 = 0x09	Id	Offset	Len	Value

#### **Attributes:**

Attribute	Length (byte)	Description		
Id	2	The Id of the NV item.		
Offset	1	Number of bytes offset from the beginning or the NV value.		
Len	1	Length of the NV value.		
Value	0-246	Value of the NV item.		

### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x09	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.8.1.10 SYS\_OSAL\_NV\_ITEM\_INIT

#### **Description**

This command is used by the tester to create and initialize an item in non-volatile memory. The NV item will be created if it does not already exist. The data for the new NV item will be left uninitialized if the *InitLen* parameter is zero. When *InitLen* is non-zero, the data for the NV item will be initialized (starting at offset of zero) with the values from *InitData*. Note that it is not necessary to initialize the entire NV item (*InitLen* < *ItemLen*). It is also possible to create an NV item that is larger than the maximum length *InitData* – use the SYS\_OSAL\_NV\_WRITE command to finish the initialization.

### Usage

#### **SREQ:**

1	1	1	2	2	1	0-245
Length = 0x04-0xFA	Cmd0 = 0x21	Cmd1 = 0x07	Id	ItemLen	InitLen	InitData

#### **Attributes:**

Attribute	Length (byte)	Description
Id	2	The Id of the NV item.
ItemLen	2	Number of bytes in the NV item.
InitLen	1	Number of bytes in the initialization data.
InitData	0-245	Value of the initialization data.

#### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x07	Status

Attribute	Length (byte)	Description
Status	1	0x00 = Item already exists, no action taken
		0x09 = Success, item created and initialized
		0x0A = Initialization failed, item not created

# 3.8.1.11 SYS\_OSAL\_NV\_DELETE

# Description

This command is used by the tester to delete an item from the non-volatile memory. The *ItemLen* parameter must match the length of the NV item or the command will fail. Use this command with caution – deleted items cannot be recovered.

#### Usage

### **SREQ:**

1	1	1	2	2
Length = $0x04$	Cmd0 = 0x21	Cmd1 = 0x12	Id	ItemLen

#### **Attributes:**

Attribute	Length (byte)	Description
Id	2	The Id of the NV item.
ItemLen	2	Length of the NV item.

### SRSP:

1 1		1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x12	Status

Attribute	Length (byte)	Description
Status	1	0x00 = Success, the item was deleted
Status	1	0x09 = No action taken, item did not exist
		0x0A = Failure, item was not deleted
		0x0C = Bad length, item was not deleted

# 3.8.1.12 SYS\_OSAL\_NV\_LENGTH

#### **Description**

This command is used by the tester to get the length of an item in non-volatile memory. A returned length of zero indicates that the NV item does not exist.

### Usage

# **SREQ:**

1	1	1	2
Length = 0x02	Cmd0 = 0x21	Cmd1 = 0x13	Id

#### **Attributes:**

Attribute	Length (byte)	Description
Id	2	The Id of the NV item.

#### **SRSP:**

1	1	1	2
Length = 0x01	Cmd0 = 0x61	Cmd1 = 0x13	Length

#### **Attributes:**

Attribute	Length (byte)	Description
Length	2	0x0000 = item does not exist
		0x0001-0xNNNN = number of bytes in NV item

# 3.8.1.13 SYS\_OSAL\_START\_TIMER

### **Description**

This command is used by the tester to start a timer event. The event will expired after the indicated amount of time and a notification will be sent back to the tester.

#### Usage

### **SREQ:**

1	1	1	1	2
Length = $0x03$	Cmd0 = 0x21	Cmd1 = 0x0A	Id	Timeout

Attribute	Length (byte)	Description
Id	1	The Id of the timer event (0-3)
Timeout	2	Amount of time it will take before the event expired in milliseconds.

### SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x61	Cmd1 = 0x0A	Status

### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.8.1.14 SYS\_OSAL\_STOP\_TIMER

### **Description:**

This command is used by the tester to stop a timer event.

### **Usage:**

### **SREQ:**

1	1	1	1
Length = $0x01$	Cmd0 = 0x21	Cmd1 = 0x0B	Id

### **Attributes:**

Attribute	Length (byte)	Description
Id	1	The Id of the timer event (0-3).

#### SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x61	Cmd1 = 0x0B	Status

Attribute	Length (byte)	Description

Status 1 Status is either Success (0) or Failure (1).

# 3.8.1.15 **SYS\_RANDOM**

#### **Description:**

This command is used by the tester to get a random 16-bit number.

#### **Usage:**

### **SREQ:**

1	1	1
Length = 0x00	Cmd0 = 0x21	Cmd1 = 0x0C

#### **Attributes:**

None

#### SRSP:

1	1	1	2
Length = $0x02$	Cmd0 = 0x61	Cmd1 = 0x0C	Value

#### **Attributes:**

Attribute	Length (byte)	Description
Value	2	The random value.

# 3.8.1.16 **SYS\_ADC\_READ**

# Description

This command reads a value from the ADC based on specified channel and resolution.

### Usage

### **SREQ:**

1	1	1	1	1
Length = $0x02$	Cmd0 = 0x21	Cmd1 = 0x0D	Channel	Resolution

Attribute	Length (byte)	Description

The channel of the ADC that will be used.

Channel

Channel	Value
AIN0	0x00
AIN1	0x01
AIN2	0x02
AIN3	0x03
AIN4	0x04
AIN5	0x05
AIN6	0x06
AIN7	0x07
Temperature Sensor	0x0E
Voltage Reading	0x0F

Resolution of the reading. This can be 8-bit, 10-bit, 12-bit or 14-bit.

Resolution 1

Resolution	Value
8-bit	0x00
10-bit	0x01
12-bit	0x02
14-bit	0x03

# SRSP:

1	1	1	2
Length = $0x02$	Cmd0 = 0x61	Cmd1 = 0x0D	Value

Attribute	Length (byte)	Description
Value	2	Value of the ADC reading based on the specified information.

# 3.8.1.17 SYS\_GPIO

### **Description**

This command is used by the tester to control the 4 GPIO pins on the CC2530-ZNP build.

### Usage

### **SREQ:**

1	1	1	1	1
Length = $0x02$	Cmd0 = 0x21	Cmd1 = 0x0E	Operation	Value

Operation -1 byte - specifies the type of operation to perform on the GPIO pins. It can take the values, shown in the table below, with effects dictated by the bit values of the value parameter:

#### **Attributes:**

Operation	Description
Set direction (0x00)	Configure the direction of the GPIO pins. A value of 0 in a bit position configures the corresponding GPIO pin as an Input while a value of 1 configures it as Output.
Set Input mode ( 0x01 )	Configure the Input mode of the GPIO pins. A value of 0 in a bit position configures it as pull-up mode while a 1 configures it in tri-state Input mode. ( <i>Note: P1_0 and P1_1 of the CC2530 can only be set in tri-state input mode</i> ).
Set ( 0x02 )	A value of 1 in a bit position will set the corresponding GPIO pin ( writes a $1$ ).
Clear ( 0x03 )	A value of $\boldsymbol{0}$ in a bit position will clear the corresponding GPIO pin ( writes a $\boldsymbol{0}$ ).
Toggle ( 0x04 )	A value of 1 in a bit position will toggle the corresponding GPIO pin.
Read ( 0x05 )	Reads the GPIO pins.

#### SRSP:

1	1	1	2
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x0E	Value

A	Attribute	Length (byte)	Description
V	<sup>7</sup> alue	1	The value read from the GPIO pins.

# 3.8.1.18 SYS\_STACK\_TUNE

# Description

This command is used by the tester to tune stack parameters and adjust performance at runtime.

### Usage

# **SREQ:**

1	1	1	1	1
Length = 0x02	Cmd0 = 0x21	Cmd1 = 0x0F	Operation	Value

### **Attributes:**

The tuning operation to be executed according to the STK\_Tune\_t enumeration:

Operation	Value
Set the transmitter power level according to the value of the Value parameter which should correspond to the valid values specified by the $ZMacTransmitPower\_t\ enumeration\ (0xFD-0x16)$	0x00
Set RxOnWhenIdle off/on if the value of Value is 0/1; otherwise return the current setting of RxOnWhenIdle.	0x01

### SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x61	Cmd1 = 0x0F	Value

Attribute	Length (byte)	Description
Value	1	Applicable status of the tuning operation.

# **3.8.1.19 SYS\_SET\_TIME**

# Description

This command is used by the tester to set the target system date and time. The time can be specified in "seconds since 00:00:00 on January 1, 2000" or in parsed date/time components.

### Usage

# **SREQ:**

1	1	1	4	1	1	1
Length = 0x0B	Cmd0 = 0x21	Cmd1 = 0x10	UTCTime	Hour	Minute	Second

1	1	2
Month	Day	Year

### **Attributes:**

Attribute	Length (bytes)	Description
UTCTime	4	Number of seconds since 00:00:00 on January 1, 2000.
		Set this parameter to zero to use date/time attributes below.
Hour	1	Hour of the day (0-23)
Minute	1	Minute of the hour (0-59)
Second	1	Second of the minute (0-59)
Month	1	Month of the year (1-12)
Day	1	Day of the month (1-31)
Year	2	Year (2000-)

### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x10	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# **3.8.1.20 SYS\_GET\_TIME**

#### **Description:**

This command is used by the tester to get the target system date and time. The time is returned in "seconds since 00:00:00 on January 1, 2000" and parsed date/time components.

### **Usage:**

# **SREQ:**

1	1	1
Length = $0x00$	Cmd0 = 0x21	Cmd1 = 0x11

#### **Attributes:**

None

#### SRSP:

1	1	1	4	1	1	1
Length = $0x0B$	Cmd0 = 0x61	Cmd1 = 0x11	UTCTime	Hour	Minute	Second

1	1	2
Month	Day	Year

#### **Attributes:**

Attribute	Length (bytes)	Description
UTCTime	4	Number of seconds since 00:00:00 on January 1, 2000.
Hour	1	Hour of the day (0-23)
Minute	1	Minute of the hour (0-59)
Second	1	Second of the minute (0-59)
Month	1	Month of the year (1-12)
Day	1	Day of the month (1-31)
Year	2	Year (2000-)

# 3.8.1.21 SYS\_SET\_TX\_POWER

### **Description:**

This command is used by the tester to set the target system radio transmit power. The returned TX power is the actual setting applied to the radio – nearest characterized value for the specific radio.

### **Usage:**

# **SREQ:**

1	1	1	1
Length = 0x01	Cmd0 = 0x21	Cmd1 = 0x14	TX Power

### **Attributes:**

Attribute	Length (bytes)	Description
TX Power	1	Requested TX power setting, in dBm.

### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x14	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.8.1.22 SYS\_ZDIAGS\_INIT\_STATS

### **Description:**

This command is used to initialize the statistics table in NV memory.

# Usage:

# **SREQ:**

1	1	1
Length = $0x00$	Cmd0 = 0x21	Cmd1 = 0x17

# **Attributes:**

None

### SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x61	Cmd1 = 0x17	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.8.1.23 SYS\_ZDIAGS\_CLEAR\_STATS

### **Description:**

This command is used to clear the statistics table. To clear data in NV (including the Boot Counter) the clearNV flag shall be set to TRUE.

#### **Usage:**

### **SREQ:**

1	1	1	1
Length = $0x01$	Cmd0 = 0x21	Cmd1 = 0x18	clearNV

# **Attributes:**

Attribute	Length (bytes)	Description
clearNV	1	TRUE – Clears statistics in NV memory including Boot Counter.
clearNV	1	FALSE – Clears statistics in RAM only. Boot Counter is preserved.

### SRSP:

1	1	1	4
Length = $0x04$	Cmd0 = 0x61	Cmd1 = 0x18	SysClock

Attribute	Length (byte)	Description	
SysClock	4	Milliseconds since last reset.	

# 3.8.1.24 SYS\_ZDIAGS\_GET\_STATS

### **Description:**

This command is used to read a specific system (attribute) ID statistics and/or metrics value.

### **Usage:**

#### **SREQ:**

1	1	1	2
Length = 0x02	Cmd0 = 0x21	Cmd1 = 0x19	AttributeID

#### **Attributes:**

Attribute	Length (bytes)	Description
AttributeID	2	System Diagnostics (ZDiags) attribute ID, as defined in ZDiags.h module.

#### SRSP:

1	1	1	4
Length = 0x04	Cmd0 = 0x61	Cmd1 = 0x19	AttributeValue

#### **Attributes:**

Attribute	Length (byte)	Description
AttributeValue	4	Value of the requested attribute.

# 3.8.1.25 SYS\_ZDIAGS\_RESTORE\_STATS\_NV

### **Description:**

This command is used to restore the statistics table from NV into the RAM table.

#### **Usage:**

# **SREQ:**

1	1	1
Length = $0x00$	Cmd0 = 0x21	Cmd1 = 0x1A

#### **Attributes:**

None

### SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x61	Cmd1 = 0x1A	Status

### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.8.1.26 SYS\_ZDIAGS\_SAVE\_STATS\_TO\_NV

# **Description:**

This command is used to save the statistics table from RAM to NV.

# Usage:

# **SREQ:**

1	1	1
Length = $0x00$	Cmd0 = 0x21	Cmd1 = 0x1B

#### **Attributes:**

None

#### SRSP:

1	1	1	4
Langth - Ov04	Cmd0 = 0v61	Cmd1 = 0v1D	CraCleals
Length = $0x04$	Cmd0 = 0x61	Cmd1 = 0x1B	SysClock

Attribute	Length (byte)	Description
SysClock	4	Milliseconds since last reset.

# **3.8.1.27 SYS\_NV\_CREATE**

### **Description:**

This command is used to attempt to create an item in non-volatile memory.

### **Usage:**

# **SREQ:**

1	1	1	1	2	2	4
Length = $0x09$	Cmd0 = 0x21	Cmd1 = 0x30	SysID	ItemID	SubID	Length

#### **Attributes:**

Attribute	Length (bytes)	Description
SysID	1	System ID of the NV item
ItemID	2	Item ID of the NV item
SubID	2	Sub ID of the NV item
Length	4	Number of bytes in the NV item

#### SRSP:

1	1	1	1
T 1 0 01	G 10 0 61	G 11 0 20	G
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x30	Status

#### **Attributes:**

Attribute	Length (byte)		Description	
Status	1	Status of NV create		

# **3.8.1.28 SYS\_NV\_DELETE**

### **Description:**

This command is used to attempt to delete an item in non-volatile memory.

### Usage:

# **SREQ:**

1	1	1	1	2	2
Length = 0x05	Cmd0 = 0x21	Cmd1 = 0x31	SysID	ItemID	SubID

Attribute	Length (bytes)	Description
SysID	1	System ID of the NV item
ItemID	2	Item ID of the NV item
SubID	2	Sub ID of the NV item

### SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x61	Cmd1 = 0x31	Status

### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status of NV delete

# 3.8.1.29 **SYS\_NV\_LENGTH**

# **Description:**

This command is used to get the length of an item in non-volatile memory.

# Usage:

# **SREQ:**

1	1	1	1	2	2
Length = $0x05$	Cmd0 = 0x21	Cmd1 = 0x32	SysID	ItemID	SubID

### **Attributes:**

Attribute	Length (bytes)	Description
SysID	1	System ID of the NV item
ItemID	2	Item ID of the NV item
SubID	2	Sub ID of the NV item

# **SRSP:**

1	1	1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x32	Length

Attribute	Length (byte)	Description	
Length	1	Length of NV Item	

# 3.8.1.30 **SYS\_NV\_READ**

# **Description:**

This command is used to read an item in non-volatile memory.

# Usage:

# **SREQ:**

1	1	1	1	2	2	2	1
Length = 0x08	Cmd0 = 0x21	Cmd1 = 0x33	SysID	ItemID	SubID	Offset	Length

# **Attributes:**

Attribute	Length (bytes)	Description
SysID	1	System ID of the NV item
ItemID	2	Item ID of the NV item
SubID	2	Sub ID of the NV item
Offset	2	Offset into NV
Length	1	Length of data to read

### **SRSP:**

1	1	1	1	1	0-240
Length = $0x02$ - $0xF2$	Cmd0 = 0x61	Cmd1 = 0x33	Status	Length	Value

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).
Length	1	Length of NV Item
Value	0-240	Value of the NV Item read

# **3.8.1.31 SYS\_NV\_WRITE**

# **Description:**

This command is used to write an item in non-volatile memory

# Usage:

# **SREQ:**

1	1	1	1	2	2	2	1	0-240
Length = 0x08-0xF8	Cmd0 = 0x21	Cmd1 = 0x34	SysID	ItemID	SubID	Offset	Length	Value

### **Attributes:**

Attribute	Length (bytes)	Description
SysID	1	System ID of the NV item
ItemID	2	Item ID of the NV item
SubID	2	Sub ID of the NV item
Offset	2	Offset into NV
Length	1	Length of data to read
Value	0-240	Data Bytes to be written to NV item

# **SRSP:**

1	1	1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x34	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.8.1.32 SYS\_NV\_UPDATE

# **Description:**

This command is used to update an item in non-volatile memory

### Usage:

### **SREQ:**

1	1	1	1	2	2	1	0-240
Length = 0x06- 0xF6	Cmd0 = 0x21	Cmd1 = 0x35	SysID	ItemID	SubID	Length	Value

#### **Attributes:**

Attribute	Length (bytes)	Description
SysID	1	System ID of the NV item
ItemID	2	Item ID of the NV item
SubID	2	Sub ID of the NV item
Length	1	Length of data to read
Value	0-240	Data Bytes to be written to NV item

### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x35	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.8.1.33 SYS\_NV\_COMPACT

### **Description:**

This command is used to compact the active page in non-volatile memory

# Usage:

### **SREQ:**

1	1	1	2
Length = 0x02	Cmd0 = 0x21	Cmd1 = 0x36	Threshold

Attribute	Length (bytes)	Description
Threshold	2	Compaction occurs when NV bytes are less than this value

#### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x61	Cmd1 = 0x36	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status of compaction of active page

# 3.8.1.34 SYS\_OSAL\_NV\_READ\_EXT

#### **Description:**

This command is used by the tester to read a single memory item from the target non-volatile memory. The command accepts an attribute Id value and data offset and returns the memory value present in the target for the specified attribute Id.

### **Usage:**

# **SREQ:**

1	1	1	2	2
Length = $0x03$	Cmd0 = 0x21	Cmd1 = 0x08	Id	Offset

### **Attributes:**

Attribute	Length (byte)	Description
Id	2	The Id of the NV item.
Offset	2	Number of bytes offset from the beginning or the NV value.

#### SRSP:

1	1	1	1	1	0-248
Length = 0x02-0xFA	Cmd0 = 0x61	Cmd1 = 0x08	Status	Len	Value

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).
Len	1	Length of the NV value.
Value	0-248	Value of the NV item.

# 3.8.1.35 SYS\_OSAL\_NV\_WRITE\_EXT

### **Description:**

This command is used by the tester to write to a particular item in non-volatile memory. The command accepts an attribute Id, data offset, data length, and attribute value. The attribute value is written to the location specified for the attribute Id in the target.

### **Usage:**

# **SREQ:**

1	1	1	2	2	1	1-246
Length = $0x04-0xFA$	Cmd0 = 0x21	Cmd1 = 0x09	Id	Offset	Len	Value

#### **Attributes:**

Attribute	Length (byte)	Description	
Id	2	The Id of the NV item.	
Offset	2	Number of bytes offset from the beginning or the NV value.	
Len	1	Length of the NV value.	
Value	0-246	Value of the NV item.	

### SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x61	Cmd1 = 0x09	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.8.2 MT\_SYS Callbacks

# 3.8.2.1 SYS\_RESET\_IND

#### **Description**

This callback is sent by the device to indicate that a reset has occurred.

#### Usage

#### **AREQ:**

1	1	1	1	1	1
Length = $0x06$	Cmd0 = 0x41	Cmd1 = 0x80	Reason	TransportRev	ProductId

1	1	1
MajorRel	MinorRel	HwRev

#### **Attributes:**

Attribute	Length (byte)		Description	

Reason for the reset.

Reason	1

Resolution	Value
Power-up	0x00
External	0x01
Watch-dog	0x02

TransportRev 1 Transport protocol revision.

Product 1 Major release number.

MinorRel 1 Minor release number.

HwRev 1 Hardware revision number.

# 3.8.2.2 SYS\_OSAL\_TIMER\_EXPIRED

### **Description:**

This callback is sent by the device to indicate that a specific timer has been expired.

### Usage:

#### **AREQ:**

1	1	1	1
Length = $0x01$	Cmd0 = 0x41	Cmd1 = 0x81	Id

Attribute	Length (byte)	Description
Id	1	The Id of the timer event (0-3)

# 3.9 MT\_UART

This interface handles communication between the target and Z-Tool. Tester has no direct control over this interface. There is no direct command for the tester to interact with this interface.

# **3.10** MT\_UTIL

This interface provides tester supporting functionalities such as setting PanId, getting device info, getting NV info, subscribing callbacks...etc.

# 3.10.1 MT\_UTIL Commands

# 3.10.1.1 UTIL\_GET\_DEVICE\_INFO

#### **Description:**

This command is sent by the tester to retrieve the device info.

#### **Usage:**

#### **SREQ:**

1	1	1
Length = 0x00	Cmd0 = 0x27	Cmd1 = 0x00

# **Attributes:**

None

#### SRSP:

1	1	1	1	8	2	1
Length = $0x02$	Cmd0 = 0x67	Cmd1 = 0x00	Status	IEEEAddr	ShortAddr	DeviceType

1	1	0-128
DeviceState	NumAssocDevices	AssocDeviceList

Attribute	Length (byte)	Description
		-

Status	1	Status is a one byte field and is either success (0) or fail (1). The fail status is returned if the address value in the command message was not within the valid range.
IEEEAddr	8	IEEE address of the device
ShortAddr	2	Short address of the device
DeviceType	1	Indicates device type, where bits 0 to 2 indicate the capability for the device to operate as a coordinator, router, or end device, respectively.
		Indicates the state of the device with different possible states as shown below:
		0x00: Initialized - not started automatically
		0x01: Initialized - not connected to anything
		0x02: Discovering PAN's to join
		0x03: Joining a PAN
DeviceState	1	0x04: Rejoining a PAN, only for end devices
		0x05: Joined but not yet authenticated by trust center
		0x06: Started as device after authentication
		0x07: Device joined, authenticated and is a router
		0x08: Starting as ZigBee Coordinator
		0x09: Started as ZigBee Coordinator
		0x0A: Device has lost information about its parent
NumAssocDevices	1	Specifies the number of Reduce Function Devices being associated to the target device.
AssocDevicesList	Array	Array of 16-bits of network addresses of Reduce Function Devices associated to the local device.

# 3.10.1.2 UTIL\_GET\_NV\_INFO

# **Description:**

This command is used by the tester to read a block of parameters from non-volatile storage of the target device.

# Usage:

# **SREQ:**

1	1	1
Length = $0x00$	Cmd0 = 0x27	Cmd1 = 0x01

# **Attributes:**

None

1	1	1	1	8	4	2
Length = 0x20	Cmd0 = 0x67	Cmd1 = 0x01	Status	IEEEAddr	ScanChannels	PanId

1	16
SecurityLevel	PreConfigKey

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	A value of zero indicates success. Failure is indicated by a non-zero value, representing a bit mask of each item that failed to be retrieved from NV memory. Bit0 is used for the first item (IEEEAddress), bit1 for the second item (ScanChannels), and so forth. Data values for failed items are returned as one or more bytes of 0xFF, the typical value read from erased NV memory.
IEEEAddr	8	IEEE address of the device
ScanChannels	4	This represents a bit-mask of channels to be scanned when starting the device.
PanId	2	Specifies the Pan Id to start or join. Set to 0xFFFF to select a PAN after scanning.
SecurityLevel	1	This specifies the network messaging security level, zero disables security.
PreConfigKey	16	This specifies the pre-configured security key.

# 3.10.1.3 UTIL\_SET\_PANID

# **Description:**

Store a PanId value into non-volatile memory to be used the next time the target device resets.

# **Usage:**

# **SREQ:**

1	1	1	2
Length = $0x02$	Cmd0 = 0x27	Cmd1 = 0x02	PanId

Attribute	Length (byte)	Description
PanId	2	PanId that will be set

1	1	1	1
Length = 0x01	Cmd0 = 0x67	Cmd1 = 0x02	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.4 UTIL\_SET\_CHANNELS

# **Description:**

This command is used to store a channel select bit-mask into non-volatile memory to be used the next time the target device resets.

# Usage:

# **SREQ:**

1	1	1	4
Length = 0x04	Cmd0 = 0x27	Cmd1 = 0x03	Channels

### **Attributes:**

Attribute	Length (byte)	Description
Channels	4	A bit-mask representing the channel(s) to scan the next time the target device resets.

# SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x67	Cmd1 = 0x03	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.5 UTIL\_SET\_SECLEVEL

#### **Description:**

This command is used to store a security level value into non-volatile memory to be used the next time the target device resets

# **Usage:**

#### **SREQ:**

1	1	1	1
Length = 0x01	Cmd0 = 0x27	Cmd1 = 0x04	SecLevel

#### **Attributes:**

Attribute	Length (byte)	Description
SecLevel	1	Security level to use the next time the target device resets. Zero is used to disable security.

#### SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x67	Cmd1 = 0x04	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.6 UTIL\_SET\_PRECFGKEY

# **Description:**

This command is used to store a pre-configured key array into non-volatile memory to be used the next time the target device resets.

### **Usage:**

#### **SREQ:**

1	1	1	16
Length = 0x10	Cmd0 = 0x27	Cmd1 = 0x05	PreCfgKey

Attribute	Length (byte)	Description
PreCfgKey	16	An array representing the pre-configured key to use the next time the target device resets.

1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x05	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.7 UTIL\_CALLBACK\_SUB\_CMD

#### **Description:**

This command subscribes/unsubscribes to layer callbacks. For particular subsystem callbacks to work, the software must be compiled with a special flag that is unique to that subsystem to enable the callback mechanism. For example to enable ZDO callbacks, MT\_ZDO\_CB\_FUNC flag must be compiled when the software is built. For complete list of callback compile flags, check section 1.2 or "**Z-Stack Compile Options**" document.

# **Usage:**

1	1	1	2	1
Length = $0x03$	Cmd0 = 0x27	Cmd1 = 0x06	SubsystemId	Action

Attribute	Length (byte)	Description
		Cubaratam Id of the armented large

Subsystem Id of the expected layer

SubsystemId 2

Subsystem	Id
MT_SYS	0x0100
MT_MAC	0x0200
MT_NWK	0x0300
MT_AF	0x0400
MT_ZDO	0x0500
MT_SAPI	0x0600
MT_UTIL	0x0700
MT_DEBUG	0x0800
MT_APP	0x0900
ALL SUBSYSTEM	0xFFFF
sabla 1: Enabla	1

Action

0: Disable, 1: Enable

#### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x06	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.8 UTIL\_KEY\_EVENT

# **Description:**

Sends key and shift codes to the application that registered for key events. The keys parameter is a bit mask, allowing for multiple keys in a single command. The return status indicates success if the command is processed by a registered key handler, not whether the key code was used. Not all applications support all key or shift codes but there is no indication when a key code is dropped.

# **Usage:**

1	1	1	1	1
Length = $0x02$	Cmd0 = 0x27	Cmd1 = 0x07	Keys	Shift

Attribute	Length (byte)	Description
Keys	1	Key code bit mask:
		0x01: key 1
		0x02: key 2
		0x04: key 3
		0x08: key 4
		0x10: key 5
		0x20: key 6
		0x40: key 7
		0x80: key 8
Shift	1	0: No shift, 1: Shift

#### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x07	Status

# **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.9 UTIL\_TIME\_ALIVE

# **Description:**

This command is used by the tester to get the board's time alive.

# Usage:

# **SREQ:**

1	1	1
Length = $0x00$	Cmd0 = 0x27	Cmd1 = 0x09

#### **Attributes:**

None

1	1	1	4
Length = $0x04$	Cmd0 = 0x67	Cmd1 = 0x09	Seconds

# **Attributes:**

Attribute	Length (byte)	Description
Seconds	4	The time of the board's live in seconds

# 3.10.1.10 UTIL\_LED\_CONTROL

# **Description:**

This command is used by the tester to control the LEDs on the board.

# **Usage:**

# **SREQ:**

1	1	1	1	1
Length = $0x02$	Cmd0 = 0x27	Cmd1 = 0x0A	LedId	Mode

# **Attributes:**

Attribute	Length (byte)	Description
Laded	1	The LED number
Mode	1	0: OFF, 1: ON

#### SRSP:

1	1	1	1
Length = 0x01	Cmd0 = 0x67	Cmd1 = 0x0A	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.11 UTIL\_LOOPBACK

# **Description:**

This command is used by the tester to test data buffer loopback.

# **Usage:**

# **SREQ:**

1	1	1	0 - 250
Length = 0x00 - 0xFA	Cmd0 = 0x27	Cmd1 = 0x10	Data

#### **Attributes:**

Attribute	Length (byte)	Description
Data	0 - 250	The data bytes to be looped back.

# SRSP:

1	1	1	0 - 250
Length = 0x00 - 0xFA	Cmd0 = 0x67	Cmd1 = 0x10	Data

# **Attributes:**

A	ttribute	Length (byte)	Description
	Data	0 - 250	The looped back data bytes.

# 3.10.1.12 **UTIL\_DATA\_REQ**

# **Description:**

This command is used by the tester to effect a MAC MLME Poll Request.

# **Usage:**

# **SREQ:**

1	1	1	1
Length = 0x01	Cmd0 = 0x27	Cmd1 = 0x11	SecurityUse

Attribute	Length	Description
SecurityUse	1	TRUE to request MAC security, but not used for now.

1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x11	Status

# **Attributes:**

Attribute	Length	Description
Status	1	A MAC status value from ZComDef.h, but only ZMacSuccess for now.

# 3.10.1.13 UTIL\_SRC\_MATCH\_ENABLE

# **Description:**

This command is used to enable AUTOPEND and source address matching.

# Usage:

# **SREQ:**

Byte: 1	1	1	
Length = $0x00$	Cmd0 = 0x27	Cmd1 = 0x20	

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x20	Status

# **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.14 UTIL\_SRC\_MATCH\_ADD\_ENTRY

# **Description:**

This command is used to add a short or extended address to the source address table.

# Usage:

# **SREQ:**

Byte: 1	1	1	1	8
Length = $0x0B$	Cmd0 = 0x27	Cmd1 = 0x21	AddressMode	Address

# **Attributes:**

Attribute	Length (byte)	)	Descriptio	n
		Mode	Value	Description
AddressMode	1	ADDRESS_16_BIT	0x02	Address 16 bit
		ADDRESS_64_BIT	0x03	Address 64 bit
Address	8	Address of the device that will be the address mode.	added - Ca	nn be short or extended depends on
PanId	2	PAN Id of the device. Only use wh	hen the add	dress is a short address.

### SRSP:



#### **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.15 UTIL\_SRC\_MATCH\_DEL\_ENTRY

# **Description:**

This command is used to delete a short or extended address from the source address table.

# Usage:

Byte: 1	1	1	1	8	2
Length = $0x0B$	Cmd0 = 0x27	Cmd1 = 0x22	AddressMode	Address	PanId

Attribute	Length (byte)		Descript	tion	
		Mode	Value	Description	
AddressMode	1	ADDRESS_16_BIT	0x02	Address 16 bit	
		ADDRESS_64_BIT	0x03	Address 64 bit	
Address	8	Address of the device that will be address mode.	deleted - C	Can be short or extended depe	ends on the
PanId	2	PAN Id of the device. Only use when	hen the add	dress is a short address.	

# SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x22	Status

# **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

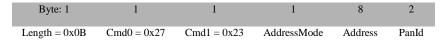
# 3.10.1.16 UTIL\_SRC\_MATCH\_CHECK\_SRC\_ADDR

# **Description:**

This command is used to check if a short or extended address is in the source address table.

# Usage:

# **SREQ:**



Attribute	Length (byte)	Description			
		Mode	Value	Description	
AddressMode	1	ADDRESS_16_BIT	0x02	Address 16 bit	
		ADDRESS_64_BIT	0x03	Address 64 bit	
Address	8	Address of the device that will b address mode.	e checked -	Can be short or extended	depends on the
PanId	2	PAN Id of the device. Only use	when the ad	dress is a short address.	

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x23	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.17 UTIL\_SRC\_MATCH\_ACK\_ALL\_PENDING

# **Description:**

This command is used to enable/disable acknowledging all packets with pending bit set.

# Usage:

# **SREQ:**



Attribute	Length (byte)	Description
Option	1	TRUE - acknowledging all packets with pending field set. FALSE - Otherwise

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x24	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

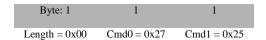
# 3.10.1.18 UTIL\_SRC\_MATCH\_CHECK\_ALL\_PENDING

#### **Description:**

This command is used to check if acknowledging all packets with pending bit set is enabled.

# Usage:

#### **SREQ:**



Attributes: None

#### SRSP:



#### **Attributes:**

Attribute	Length (byte)	Description	
Status	1	Status is either Success (0) or Failure (1).	
Value	1	TRUE - acknowledging all packets with pending bit set is enabled. FALSE – otherwise.	

# 3.10.1.19 UTIL\_ADDRMGR\_EXT\_ADDR\_LOOKUP

# **Description:**

This command is a proxy call to the AddrMgrEntryLookupExt() function.

# **Usage:**

# **SREQ:**

1	1	1	8
Length = 0x08	Cmd0 = 0x27	Cmd1 = 0x40	ExtAddr

# **Attributes:**

Attribute	Length (byte)	Description
ExtAddr	8	Extended Address (LSB-MSB) of the device for which to lookup the Network Address.

#### SRSP:

1	1	1	2
Length = $0x02$	Cmd0 = 0x67	Cmd1 = 0x40	NwkAddr

# **Attributes:**

Attribute	Length (byte)	Description
NwkAddr	2	Network Address (LSB-MSB) of the device that corresponds to the Extended Address sent as a parameter in the request.

# 3.10.1.20 UTIL\_ADDRMGR\_NWK\_ADDR\_LOOKUP

# **Description:**

This command is a proxy call to the AddrMgrEntryLookupNwk() function.

# **Usage:**

1	1	1	2
Length = $0x02$	Cmd0 = 0x27	Cmd1 = 0x41	NwkAddr

Attribute	Length (byte)	Description
NwkAddr	2	Network Address (LSB-MSB) of the device for which to lookup the Extended Address.

#### SRSP:

1	1	1	8
Length = 0x08	Cmd0 = 0x67	Cmd1 = 0x41	ExtAddr

#### **Attributes:**

Attribute	Length (byte)	Description
ExtAddr	8	Extended Address (LSB-MSB) of the device that corresponds to the Network Address sent as a parameter in the request.

# 3.10.1.21 UTIL\_APSME\_LINK\_KEY\_DATA\_GET

# **Description:**

This command retrieves APS link key data, Tx and Rx frame counters.

# Usage:

# **SREQ:**

1	1	1	8
Length = $0x08$	Cmd0 = 0x27	Cmd1 = 0x44	ExtAddr

# **Attributes:**

Attribute	Length (byte)	Description
ExtAddr	8	The extended address for which to get the link key data.

# **SRSP:**

1	1	1	1	16	4	4
Length = 0x19	Cmd0 = 0x67	Cmd1 = 0x44	Status	SecKey	TxFrmCntr	RxFrmCntr

Attribute	Length (byte)	Description
Status	1	The ZStatus_t returned by the proxy call to APSME_LinkKeyNVIdGet().
SecKey	16	On success, the security key looked up; otherwise N/A.
TxFrmCntr	4	On success, the TX frame counter; otherwise N/A.
RxFrmCntr	4	On success, the RX frame counter, otherwise N/A.

# 3.10.1.22 UTIL\_APSME\_LINK\_KEY\_NV\_ID\_GET

# **Description:**

This command is a proxy call to the APSME\_LinkKeyNvIdGet() function.

# Usage:

# **SREQ:**

1	1	1	8
Length = $0x08$	Cmd0 = 0x27	Cmd1 = 0x45	ExtAddr

# **Attributes:**

Attribute	Length (byte)	Description
ExtAddr	8	The extended address for which to get the link key NV Id.

# SRSP:

1	1	1	1	2
Length = $0x03$	Cmd0 = 0x67	Cmd1 = 0x45	Status	LinkKeyNvId

Attribute	Length (byte)	Description
Status	1	Status of proxy call to APSME_LinkKeyNvIdGet().
LinkKeyNvId	2	On success, link key NV ID. Otherwise 0xFFFF

# 3.10.1.23 UTIL\_APSME\_REQUEST\_KEY\_CMD

#### **Description:**

This command is used to send a request key to the Trust Center from an originator device who wants to exchange messages with a partner device.

# Usage:

#### **SREQ:**

1	1	1	2
Length = $0x02$	Cmd0 = 0x27	Cmd1 = 0x4B	PartnerAddr

#### **Attributes:**

Attribute	Length (byte)	Description
PartnerAddr	8	Specifies the extended address of the partner device the originator wants to exchange messages with.

#### **SRSP:**

1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x4B	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.10.1.24 UTIL\_ASSOC\_COUNT

# **Description:**

This command is a proxy call to the AssocCount() function.

#### Usage:

1	1	1	1	1
Length = 0x02	Cmd0 = 0x27	Cmd1 = 0x48	StartRelation	EndRelation

Attribute	Length (byte)	Description	on
		A valid node relation from AssocList.h:	
		// Node Relations	
		#define PARENT	0
		#define CHILD_RFD	1
	1	#define CHILD_RFD_RX_IDLE	2
StartRelation	1	#define CHILD_FFD	3
		#define CHILD_FFD_RX_IDLE	4
		#define NEIGHBOR	5
		#define OTHER	6
		The node relation at which to start counting.	
EndRelation	1	Same as StartRelation, but the node rela	tion at which to stop counting.

# **SRSP:**

1	1	1	2
Length = $0x02$	Cmd0 = 0x67	Cmd1 = 0x48	Count

#### **Attributes:**

Attribute	Length (byte)	Description
Count	2	The count returned by the proxy call to AssocCount().

# 3.10.1.25 UTIL\_ASSOC\_FIND\_DEVICE

# **Description:**

This command is a proxy call to the AssocFindDevice() function.

# **Usage:**

# **SREQ:**

1	1	1	1
Length = 0x01	Cmd0 = 0x27	Cmd1 = 0x49	Number

Attribute	Length (byte)	Description
Number	1	Nth active entry in the device list.

1	1	1	18
Length = $0x12$	Cmd0 = 0x67	Cmd1 = 0x49	Device

# **Attributes:**

Attribute	Length (byte)	Description
Device	18	The packed (LSB-MSB) associated_devices_t structure returned by the proxy call to AssocFindDevice().The device short address is set to INVALID_NODE_ADDR to indicate failure.

# 3.10.1.26 UTIL\_ASSOC\_GET\_WITH\_ADDRESS

# **Description:**

This command is a proxy call to the AssocGetWithAddress() function.

#### Usage:

# **SREQ:**

1	1	1	8	2
Length = 0x0A	Cmd0 = 0x27	Cmd1 = 0x4A	ExtAddr	NwkAddr

# **Attributes:**

Attribute	Length (byte)	Description
ExtAddr	8	The extended address to use for the lookup or all zeroes to use the NwkAddr for the lookup.
NwkAddr	2	Network Address (LSB-MSB) to use for the lookup if the ExtAddr is all zeroes.

# **SRSP:**

1	1	1	18
Length = $0x12$	Cmd0 = 0x67	Cmd1 = 0x4A	Device

Attribute	Length (byte)	Description
Device	18	The packed (LSB-MSB) associated_devices_t structure returned by the proxy call to AssocGetWithAddress (). The device short address is set to INVALID NODE ADDR to indicate failure.

# 3.10.1.27 UTIL\_BIND\_ADD\_ENTRY

# **Description:**

This command is a proxy call to the bindAddEntry() function.

# **Usage:**

# **SREQ:**

1	1	1	1	8
Length = $0x0D-0x13$	Cmd0 = 0x27	Cmd1 = 0x4D	AddrMode	DstAddr

1	1	2-8
DstEndpoint	NumClusterIds	ClusterIds

# **Attributes:**

Attribute	Length (byte)	Description
AddrMode	1	The destination address mode according to the afAddrMode_t enumeration in AF.h.
DstAddr	8	If AddrMode is afAddr64Bit, the 8-byte extended destination address; otherwise the 2-byte network destination address.
DstEndpoint	1	Binding entry destination endpoint.
NumClusterIds	1	Specifies the number of IDs in the ClusterIds list.
ClusterIds	2-8	Contains the cluster IDs.

#### SRSP:

1	1	1	14
Length = $0x0E$	Cmd0 = 0x67	Cmd1 = 0x4D	BindEntry

#### **Attributes:**

Attribute	Length (byte)	Description
BindEntry	14	The packed (LSB-MSB) BindingEntry_t structure returned by the proxy call to bindAddEntry(). The dstIdx in the BindEntry is set to INVALID_NODE_ADDR to indicate failure.

# 3.10.1.28 UTIL\_ZCL\_KEY\_EST\_INIT\_EST

# **Description:**

This command is a proxy call to zclGeneral\_KeyEstablish\_InitiateKeyEstablishment().

# **Usage:**

# **SREQ:**

1	1	1	1	1	1	1	8
Length = 0x0C	Cmd0 = 0x27	Cmd1 = 0x80	TaskId	SeqNum	EndPoint	AddrMode	Addr

# **Attributes:**

Attribute	Length (byte)	Description
TaskId	1	The OSAL Task Id making the request.
SeqNum	1	The sequence number of the request.
EndPoint	1	The endpoint on the partner.
AddrMode	1	The address mode to the partner according to the afAddrMode_t enumeration in AF.h.
Addr	8	If AddrMode is afAddr64Bit, the 8-byte extended address of the partner; otherwise the 2-byte network address of the partner.

# SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x67	Cmd1 = 0x80	Status

# **Attributes:**

Attribute	Length (byte)	Description
Status	1	The ZStatus_t returned by the proxy call to zclGeneral_KeyEstablish_InitiateKeyEstablishment().

# 3.10.1.29 UTIL\_ZCL\_KEY\_EST\_SIGN

# **Description:**

This command is a proxy call to zclGeneral\_KeyEstablishment\_ECDSASign().

# **Usage:**

1	1	1	1	1
Length = 0x0C	Cmd0 = 0x27	Cmd1 = 0x81	InputLen	Input

Attribute	Length (byte)	Description	
InputLen	1	The length of the input data.	
Input	InputLen	The input data.	

# SRSP:

1	1	1	1	42
Length = $0x2B$	Cmd0 = 0x67	Cmd1 = 0x81	Status	Key

# **Attributes:**

Attribute	Length (byte)	Description
Status	1	The ZStatus_t returned by the proxy call to zclGeneral_KeyEstablishment_ECDSASign ().
Key	42	The output key on success.

# 3.10.1.30 UTIL\_SRNG\_GEN

# **Description:**

This command is used to generate Secure Random Number. It generates 1,000,000 bits in sets of 100 bytes. As in 100 bytes of secure random numbers are generated until 1,000,000 bits are generated. 100 bytes are generated 1250 times. So 1250 SRSPs are generated. MT\_SRNG has to be defined to include this API.

#### **Usage:**

# **SREQ:**

1	1	1
Length = 0x00	Cmd0 = 0x27	Cmd1 = 0x4C

#### SRSP:

1	1	1	0x64
Length = 0x64	Cmd0 = 0x67	Cmd1 = 0x4C	Secure Random Numbers

# 3.10.2 MT\_UTIL Callbacks

# 3.10.2.1 UTIL\_SYNC\_REQ

# **Description:**

This is an asynchronous request/response handshake.

#### **Usage:**

# **AREQ:**

1	1	1
Length = $0x00$	Cmd0 = 0x47	Cmd1 = 0xE0

# 3.10.2.2 UTIL\_ZCL\_KEY\_ESTABLISH\_IND

#### **Description:**

This is the RPC proxy indication for a ZCL\_KEY\_ESTABLISH\_IND.

#### Usage:

#### **AREQ:**

1	1	1	1	1	1	1	2
Length = 0x06	Cmd0 = 0x47	Cmd1 = 0xE1	TaskId	Event	Status	WaitTime	Suite

# **Attributes:**

Attribute	Length (byte)	Description
TaskId	1	The OSAL Task Id registered to receive this indication (see UTIL_ZCL_KEY_EST_INIT_EST).
Event	1	The OSAL message event.
Status	1	The OSAL message status.
WaitTime	1	The wait time.
Suite	2	The key establishment suite.

# 3.11 MT\_VERSION

This interface contains information about the release version of the software. There is no direct command for tester to interact with this interface.

# 3.12 MT\_ZDO

This interface allows the tester to issue commands to the ZDO layer in the target and receive responses. Each of these messages has a corresponding message that is returned by the target. The response message only indicates that the command message was received and executed. The result of the command execution will be conveyed to the tester via a callback message interface.

# 3.12.1 MT\_ZDO Commands

# 3.12.1.1 ZDO\_NWK\_ADDR\_REQ

#### **Description:**

This message will request the device to send a "Network Address Request". This message sends a broadcast message looking for a 16 bit address with a known 64 bit IEEE address. You must subscribe to "ZDO Network Address Response" to receive the response to this message. Check section 3.0.1.7 for more details on callback subscription. The response message listed below only indicates whether or not the message was received properly.

#### **Usage:**

#### **SREQ:**

Byte: 1	1	1	8	1	1
Length = $0x0A$	Cmd0 = 0x25	Cmd1 = 0x00	IEEEAddress	ReqType	StartIndex

#### **Attributes:**

Attribute	Length (byte)	Desc	ription
IEEEAddress	8	64 bit IEEE address of the device.	
		Value that the search was executed on.	
ReqType	1	Туре	Value
		Single Device response	0x00
		Extended, include associated devices	0x01
StartIndex	1	Starting index into the list of children. The too large for one message.	ais is used to get more of the list if the list is

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x00	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.2 ZDO\_IEEE\_ADDR\_REQ

# **Description:**

This command will request a device's IEEE 64-bit address. You must subscribe to "ZDO IEEE Address Response" to receive the data response to this message. The response message listed below only indicates whether or not the message was received properly.

#### **Usage:**

# **SREQ:**

Byte: 1	1	1	2	1	1
Length = $0x04$	Cmd0 = 0x25	Cmd1 = 0x01	ShortAddr	ReqType	StartIndex

#### **Attributes:**

Attribute	Length (byte)	Desc	ription	
ShortAddr	2	Specifies the short address of the device.		
		Value that the search was executed on.		
ReqType	1	Type	Value	
ReqType	1			
		Single Device response	0x00	
		Extended, include associated devices	0x01	
StartIndex	1	Starting index into the list of children. The too large for one message.	nis is used t	to get more of the list if the list is

#### **SRSP:**



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

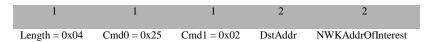
# 3.12.1.3 ZDO\_NODE\_DESC\_REQ

#### **Description:**

This command is generated to inquire about the Node Descriptor information of the destination device.

#### Usage

#### **SREQ:**



# **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Specifies NWK address of the device to route the inquiry.
NWKAddrOfInterest	2	Specifies NWK address of the destination device being queried.

#### **SRSP:**



#### **Attributes:**

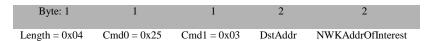
Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.4 ZDO\_POWER\_DESC\_REQ

# **Description:**

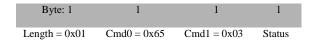
This command is generated to inquire about the Power Descriptor information of the destination device.

#### Usage:



Attribute	Length (byte)	Description
DstAddr	2	Specifies NWK address of the device to route the inquiry.
NWKAddrOfInterest	2	Specifies NWK address of the destination device being queried.

#### **SRSP:**



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.5 ZDO\_SIMPLE\_DESC\_REQ

# **Description:**

This command is generated to inquire as to the Simple Descriptor of the destination device's Endpoint.

# **Usage:**

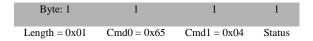
# **SREQ:**



# **Attributes**:

Attribute	Length (byte)	Description
DstAddr	2	Specifies NWK address of the device to route the inquiry.
NWKAddrOfInterest	2	Specifies NWK address of the destination device being queried.
Endpoint	1	Specifies the application endpoint the data is from.

#### **SRSP:**



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

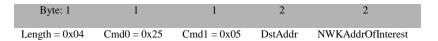
# 3.12.1.6 ZDO\_ACTIVE\_EP\_REQ

# **Description:**

This command is generated to request a list of active endpoint from the destination device.

#### **Usage:**

# **SREQ:**



# **Attributes**:

Attribute	Length (byte)	Description
DstAddr	2	Specifies NWK address of the device to route the inquiry.
NWKAddrOfInterest	2	Specifies NWK address of the destination device being queried.

# **SRSP:**



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

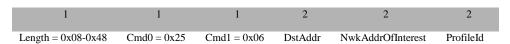
# 3.12.1.7 ZDO\_MATCH\_DESC\_REQ

# **Description:**

This command is generated to request the device match descriptor.

# **Usage:**

# **SREQ:**



1	0-32	1	0-32
NumInClusters	InClusterList	NumOutClusters	OutClusterList

# **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Specifies NWK address of the device to route the inquiry.
NWKAddrOfInterest	2	Specifies NWK address of the destination device being queried.
ProfileId	2	Specifies the profile Id of the device
NumInClusters	1	Specifies the number of Id's in the InClusterList.
InClusterList	0-32	Contains the input cluster Id's.
NumOutClusters	1	Specifies the number of Id's in the OutClusterList.
OutClusterList	0-32	Contains the output cluster Id's.

#### SRSP:



ı	Attribute	Length (byte)	Description
	Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.8 ZDO\_COMPLEX\_DESC\_REQ

#### **Description:**

This command is generated to request for the destination device's complex descriptor.

#### Usage:

#### **SREQ:**

Byte: 1	1	1	2	2
Length = $0x04$	Cmd0 = 0x25	Cmd1 = 0x07	DstAddr	NWKAddrOfInterest

#### **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Specifies NWK address of the device to route the inquiry.
NWKAddrOfInterest	2	Specifies NWK address of the destination device being queried.

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x07	Status

# **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

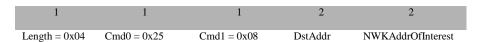
# 3.12.1.9 ZDO\_USER\_DESC\_REQ

#### **Description:**

This command is generated to request for the destination device's user descriptor.

#### **Usage:**

#### **SREQ:**



Attribute	Length (byte)	Description

NWKAddrOfInterest

2 DstAddr Specifies NWK address of the device to process the inquiry. 2

Specifies NWK address of the destination device being queried.

# **SRSP:**



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.10 ZDO\_END\_DEVICE\_ANNCE

# **Description:**

This command will cause the device to issue an "End device announce" broadcast packet to the network. This is typically used by an end-device to announce itself to the network.

#### Usage:

# **SREQ:**

1	1	1	2	8	1
Length = $0x0B$	Cmd0 = 0x25	Cmd1 = 0x0A	NwkAddr	IEEEAddr	Capabilites

Attribute	Length (byte)	Description
NwkAddr	2	Specifies network address of the device generating the request.
IEEEAddr	8	Specifies the 64 bit IEEE Address of the device being announced.
		Specifies MAC capabilities
		Bit: 0 – Alternate PAN Coordinator
		1 – Device type: 1- ZigBee Router; 0 – End Device
Capabilites	1	2 – Power Source: 1 Main powered
Capabilities	1	3 – Receiver on when Idle
		4 – Reserved
		5 – Reserved
		6 – Security capability

#### 7 - Reserved

# **SRSP:**



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.11 ZDO\_USER\_DESC\_SET

# **Description:**

This command is generated to write a User Descriptor value to the targeted device.

# **Usage:**

# **SREQ:**

1	1	1	2	2	1	0-16
Length = 0x05-0x15	Cmd0 = 0x25	Cmd1 = 0x0B	DstAddr	NWKAddrOfInterest	Len	UserDescriptor

#### **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Specifies network address of the device to route the set request.
NWKAddrOfInterest	2	Specifies NWK address of the destination device being queried.
Len	1	Specifies the length of the user descriptor.
UserDescriptor	0-16	User descriptor array (can be up to 16 bytes).

# **SRSP:**



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.12 ZDO\_SERVER\_DISC\_REQ

# **Description:**

The command is used for local device to discover the location of a particular system server or servers as indicated by the ServerMask parameter. The destination addressing on this request is 'broadcast to all RxOnWhenIdle devices'.

#### Usage:

#### **SREQ:**



#### **Attributes:**

Attribute	Length (byte)	Description
ServerMask	2	Specifies the system server capabilities of the device.

#### **SRSP:**



#### **Attributes:**

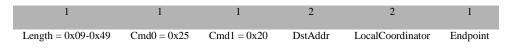
Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.13 ZDO\_END\_DEVICE\_BIND\_REQ

# **Description:**

This command is generated to request an End Device Bind with the destination device.

### **Usage:**





Attribute	Length (byte)	Description
DstAddr	2	Specifies NWK address of the target device for binding.
LocalCoordinator	2	Specifies Specifies local coordinator's short address. In the case of source binding, it's the short address of the source address
IEEE	8	Local coordinator's IEEE address
Endpoint	1	Device's endpoint.
ProfileId	2	Specifies the profile Id of the device.
NumInClusters	1	Specifies the number of Id's in the InClusterList.
InClusterList	0-32	Contains the input cluster Id's.
NumOutClusters	1	Specifies the number of Id's in the OutClusterList.
OutClusterList	0-32	Contains the output cluster Id's.

### **SRSP:**



# **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# **3.12.1.14 ZDO\_BIND\_REQ**

# **Description:**

This command is generated to request a Bind.

# Usage:

1	1	1	2	8	1	2



#### **Attributes:**

Attribute	Length (byte)	Description	
DstAddr	2	Specifies the destination address of the device to process the bind request	
SrcAddress	8	64 bit Binding source IEEE address	
SrcEndpoint	1	Specifies the binding source endpoint.	
ClusterId	2	Specifies the cluster Id to match in messages.	
		Specifies destination address mode	

Mode Value Description ADDRESS\_NOT\_PRESENT 0x00 Address Not Present DstAddrMode GROUP\_ADDRESS 0x01 Group address ADDRESS\_16\_BIT 0x02 Address 16 bit ADDRESS\_64\_BIT 0x03 Address 64 bit BROADCAST 0xFF Broadcast DstAddress 8/2 Binding destination IEEE address. Not to be confused with DstAddr. Specifies the binding destination endpoint. It is used only when DstAddrMode is DstEndpoint 1/0

64 bits extended address

#### **SRSP:**



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# **3.12.1.15 ZDO\_UNBIND\_REQ**

# **Description:**

This command is generated to request a un-bind.

## **Usage:**

# **SREQ:**

1	1	1	2	8	1	2
Length = 0x10-0x17	Cmd0 = 0x25	Cmd1 = 0x22	DstAddr	SrcAddress	SrcEndpoint	ClusterId

1	2/8	0/1
DstAddrMode	DstAddress	DstEndpoint

Attribute	Length (byte)	Description	
DstAddr	2	Specifies destination address of the device to process the unbind request.	
SrcAddress	8	Specifies 64 bit Binding source IEEE address.	
SrcEndpoint	1	Specifies the binding source endpoint.	
ClusterI	2	Specifies cluster Id to match in messages.	
		Specifies 64 bit Binding destination address mode:	

		Mode	Value	Description	
		ADDRESS_NOT_PRESENT	0x00	Address Not Present	
DstAddrMode	1				
		GROUP_ADDRESS	0x01	Group address	
		ADDRESS_16_BIT	0x02	Address 16 bit	
		ADDRESS_64_BIT	0x03	Address 64 bit	
		BROADCAST	0xFF	Broadcast	
DstAddress	8	Specifies 64 bit Binding destination IEEE address. Not to be confused with DstAddr.			
DstEndpoint	1	Specifies the binding destination endpoint			

#### SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x22	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.16 ZDO\_MGMT\_NWK\_DISC\_REQ

## **Description:**

This command is generated to request the destination device to perform a network discovery.

## Usage:

# **SREQ:**

1	1	1	2	4	1	1
Length = $0x08$	Cmd0 = 0x25	Cmd1 = 0x30	DstAddr	ScanChannels	ScanDuration	StartIndex

#### **Attributes:**

Attribute	Length (byte)	Description	
DstAddr	2	Specifies the network address of the device performing the discovery.	

Specifies the Bit Mask for channels to scan:

		Channel	Value
		NONE	0x00000000
		ALL_CHANNELS	0x07FFF800
		CHANNEL 11	0x00000800
		CHANNEL 12	0x00001000
ScanChannels	4	CHANNEL 13	0x00002000
		CHANNEL 14	0x00004000
		CHANNEL 15	0x00008000
		CHANNEL 16	0x00010000
		CHANNEL 17	0x00020000
		CHANNEL 18	0x00040000
		CHANNEL 19	0x00080000

CHANNEL 20	0x00100000
CHANNEL 21	0x00200000
CHANNEL 22	0x00400000
CHANNEL 23	0x00800000
CHANNEL 24	0x01000000
CHANNEL 25	0x02000000
CHANNEL 26	0x04000000

ScanDuration 1 Specifies the scanning time.

Specifies where to start in the response array list. The result may contain more StartIndex 1 entries than can be reported, so this field allows the user to retrieve the responses

anywhere in the array list.

## **SRSP:**



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.17 ZDO\_MGMT\_LQI\_REQ

## **Description:**

This command is generated to request the destination device to perform a LQI query of other devices in the network.

## **Usage:**

## **SREQ:**

Byte: 1	1	1	2	1
Length = $0x03$	Cmd0 = 0x25	Cmd1 = 0x31	DstAddr	StartIndex

#### **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Specifies the network address of the device to process the query.
StartIndex	1	Specifies where to start in the response array list. The result may contain more entries than can be reported, so this field allows the user to retrieve the responses anywhere in the array list.

## SRSP:



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

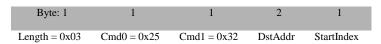
# 3.12.1.18 ZDO\_MGMT\_RTG\_REQ

## **Description:**

This command is generated to request the Routing Table of the destination device.

#### **Usage:**

# **SREQ:**



## **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Specifies the network address of the device to process the query.
StartIndex	1	Specifies where to start in the response array list. The result may contain more entries than can be reported, so this field allows the user to retrieve the responses anywhere in the array list.

## **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x32	Status

## **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.19 ZDO\_MGMT\_BIND\_REQ

# Description

This command is generated to request the Binding Table of the destination device.

## Usage

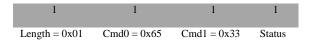
# **SREQ:**

Byte: 1	1	1	2	1
Length = $0x03$	Cmd0 = 0x25	Cmd1 = 0x33	DstAddr	StartIndex

# **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Specifies the network address of the device being queried.
StartIndex	1	Specifies where to start in the response array list. The result may contain more entries than can be reported, so this field allows the user to retrieve the responses anywhere in the array list.

## SRSP:



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.20 ZDO\_MGMT\_LEAVE\_REQ

# **Description:**

This command is generated to request a Management Leave Request for the target device.

## **Usage:**

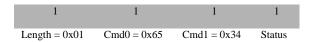
# **SREQ:**

1	1	1	2	8	1
Length = $0x0B$	Cmd0 = 0x25	Cmd1 = 0x34	DstAddr	DeviceAddr	RemoveChildren_Rejoin

## **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Short address of the device that will process the mgmt leave (remote or self)
DeviceAddress	8	The 64-bit IEEE address of the entity to be removed from the network or 0x00000000000000000 if the device removes itself from the network.
		Specifies actions to be performed by device when leaving the network:
RemoveChildren Rejoin	1	Bit 0: rejoin
	-	Bit 1: remove children

# SRSP:



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.21 ZDO\_MGMT\_DIRECT\_JOIN\_REQ

# **Description:**

This command is generated to request the Management Direct Join Request of a designated device.

# Usage:

# **SREQ:**

Byte: 1	1	1	2	8	1
Length = $0x0B$	Cmd0 = 0x25	Cmd1 = 0x35	DstAddr	DeviceAddr	CapInfo

## **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Network address of the device to which the device specified in DeviceAddress is to join.
DeviceAddress	8	The 64 bit IEEE Address of the device you want to be joined to the device at DstAddr.
		Specifies the operating capabilities of the device being directly joined. Bit weighted values follow:
		Bit: 0 – Alternate PAN Coordinator
		1 – Device type: 1- ZigBee Router; 0 – End Device
		2 – Power Source: 1 Main powered
CapInfo	1	3 – Receiver on when Idle
		4 – Reserved
		5 – Reserved
		6 – Security capability
		7 – Reserved

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x35	Status

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.22 ZDO\_MGMT\_PERMIT\_JOIN\_REQ

# **Description:**

This command is generated to set the Permit Join for the destination device.

## **Usage:**

## **SREQ:**



#### **Attributes:**

Attribute	Length (byte)	Description
AddrMode		Destination address type: 0x02 – Address 16 bit, 0xFF – Broadcast.
DstAddr	2	Specifies the network address of the destination device whose Permit Join information is to be modified.
Duration	1	Specifies the duration to permit joining. $0 = \text{join disabled}$ . $0xff = \text{join enabled}$ . $0x01-0xfe = \text{number of seconds to permit joining}$ .
TCSignificance	1	Trust Center Significance.

#### **SRSP:**



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.23 ZDO\_MGMT\_NWK\_UPDATE\_REQ

# **Description:**

This command is provided to allow updating of network configuration parameters or to request information from devices on network conditions in the local operating environment.

# Usage:

# **SREQ:**



#### **Attributes:**

ı	Attribute	Length (byte)	Description
	DstAddr	2	Short address of the destination device(s). The destination addressing on this primitive can be unicast or broadcast to all devices for which macRxOnWhenIdle=TRUE (i.e., 0xFFFD)
			Destination address mode:

DstAddrMode 1

Mode	Value	Description
ADDRESS_NOT_PRESENT	0x00	Address Not Present
GROUP_ADDRESS	0x01	Group address
ADDRESS_16_BIT	0x02	Address 16 bit
ADDRESS_64_BIT	0x03	Address 64 bit
BROADCAST	0xFF	Broadcast

A bitmap indicating which channels are to be scanned:

Channel	Value
NONE	0x00000000
ALL_CHANNELS	0x07FFF800
CHANNEL 11	0x00000800
CHANNEL 12	0x00001000
CHANNEL 13	0x00002000
CHANNEL 14	0x00004000
CHANNEL 15	0x00008000
CHANNEL 16	0x00010000
CHANNEL 17	0x00020000
CHANNEL 18	0x00040000
CHANNEL 19	0x00080000
CHANNEL 20	0x00100000
CHANNEL 21	0x00200000
CHANNEL 22	0x00400000
CHANNEL 23	0x00800000
CHANNEL 24	0x01000000
CHANNEL 25	0x02000000
CHANNEL 26	0x04000000

ChannelMask 4

ScanDuration 1 A value used to calculate the length of time to spend scanning each channel

ScanCount 1 This field represents the number of energy scans to be conducted and reported

NwkManagerAddr 2 Indicates the NWK address for the device with the Network Manager bit set in its Node Descriptor

## **SRSP:**



Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.12.1.24 ZDO\_MSG\_CB\_REGISTER

# **Description:**

This command registers for a ZDO callback (see reference [3], "6. ZDO Message Requests" for example usage).

# Usage:

# **SREQ:**



#### **Attributes:**

Attribute	Length (byte)	Description
ClusterId	2	Specifies the ZDO Cluster Id for which to receive a ZDO callback.

## **SRSP:**



Attribute	Length (byte)	Description
Status	1	Return value of the call to ZDO_RegisterForZDOMsg().

# 3.12.1.25 ZDO\_MSG\_CB\_REMOVE

#### **Description:**

This command removes a registration for a ZDO callback (see reference [3], "6. ZDO Message Requests" for example usage).

## **Usage:**

# **SREQ:**

1	1	1	2
Length = $0x02$	Cmd0 = 0x25	Cmd1 = 0x3F	ClusterId

#### **Attributes:**

Attribute	Length (byte)	Description
ClusterId	2	Specifies the ZDO Cluster Id for which to receive a ZDO callback.

## **SRSP:**



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Return value of the call to ZDO_RemoveRegisteredCB ().

# 3.12.1.26 ZDO\_STARTUP\_FROM\_APP

#### **Description:**

This command starts the device in the network.

## Usage:

#### **SREQ:**



Attribute	Length (byte)	Description
StartDelay	2	Specifies the time delay before the device starts.

#### SRSP:



#### **Attributes:**

Attribute	Length (byte)	Description
		0x00 - Restored network state
Status	1	0x01 - New network state
		0x02 – Leave and not Started

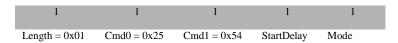
# 3.12.1.27 ZDO\_STARTUP\_FROM\_APP\_EX

## **Description:**

Extended version of ZDO to indicate to router devices to create a distributed network.

#### **Usage:**

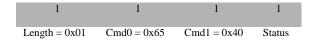
## **SREQ:**



## **Attributes:**

Attribute	Length (byte)	Description
StartDelay	1	Specifies the time delay before the device starts.
Mode	1	Flag for ZR devices to indicate to create a distributed network if set to TRUE, if set to FALSE or send to ZC or ZED has the same effect as non-extended interface.

# SRSP:



Attribute	Length (byte)	Description
Status	1	0x00 - Restored network state
Status	1	0x01 – New network state

# 3.12.1.28 ZDO\_SET\_LINK\_KEY

# **Description:**

This command sets the application link key for a given device.

# Usage:

# **SREQ:**

1	1	1	2	8	16
Length = $0x1A$	Cmd0 = 0x25	Cmd1 = 0x23	ShortAddr	IEEEAddr	LinkKeyData

#### **Attributes:**

Attribute	Length (byte)	Description
ShortAddr	2	Specifies the short address of the pair device of the link key.
IEEEAddr	8	Specifies the IEEE address of the pair device of the link key
LinkKeyData	16	128 bit link key data of the device.

## SRSP:

1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x23	Status

Attribute	Length (byte)	Description
		0x00 – Success
Status	1	0x01 - Fail to add to address manager.
		0x11 - Security manager key table full

# 3.12.1.29 ZDO\_REMOVE\_LINK\_KEY

#### **Description:**

This command removes the application link key of a given device.

## **Usage:**

#### **SREQ:**



#### **Attributes:**

Attribute	Length (byte)	Description
IEEEAddr	8	Specifies the IEEE address of the pair device of the link key

#### **SRSP:**



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	0x00 – Success
Status	•	0xC8 – Unknown device.

# 3.12.1.30 ZDO\_GET\_LINK\_KEY

#### **Description:**

This command retrieves the application link key of a given device.

## **Usage:**

#### **SREQ:**



#### **Attributes:**

Attribute	Length (byte)	Description
IEEEAddr	8	Specifies the IEEE address of the pair device of the link key

#### SRSP:

1	1	1	1	8	16
Length = $0x19$	Cmd0 = 0x65	Cmd1 = 0x25	Status	IEEEAddr	LinkKeyData

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	0x00 – Success
Status	1	0xC8 – Unknown device.
IEEEAddr	8	IEEE address of the device
LinkKeyData	16	Link key data of the device.

# 3.12.1.31 ZDO\_NWK\_DISCOVERY\_REQ

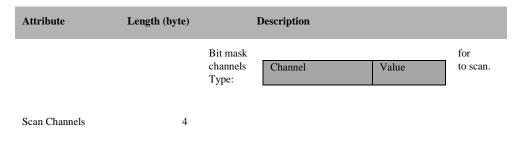
## **Description:**

This command is used to initiate a network discovery (active scan).

#### Usage:

## **SREQ:**

Byte: 1	1	1	4	1
Length = $0x05$	Cmd0 = 0x25	Cmd1 = 0x26	Scan Channels	Scan Duration



ZIGBEE\_CHANNELS

NONE	0x00000000
ALL_CHANNELS	0x07FFF800
CHANNEL 11	0x00000800
CHANNEL 12	0x00001000
CHANNEL 13	0x00002000
CHANNEL 14	0x00004000
CHANNEL 15	0x00008000
CHANNEL 16	0x00010000
CHANNEL 17	0x00020000
CHANNEL 18	0x00040000
CHANNEL 19	0x00080000
CHANNEL 20	0x00100000
CHANNEL 21	0x00200000
CHANNEL 22	0x00400000
CHANNEL 23	0x00800000
CHANNEL 24	0x01000000
CHANNEL 25	0x02000000
CHANNEL 26	0x04000000

Scan Duration

A value used to calculate the length of time to spend scanning each channel

## **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x26	Status

Attribute	Length (byte)	Description
		Success (0)
		Invalid_Parameter (0x02).
Status	1	ZNwkInvalidRequest (0xC2) if the device is already on a network. User ZDO_MGMT_NWK_DISC_REQ instead. Or leave the network first, then initiate the request.
		MAC_SCAN_IN_PROGRESS (0xFC) if a channel change is in progress.

 $MAC\_NO\_RESOURCE \ (0x1A) \ if \ the \ operation \ could \ not complete because no memory resource were available.$ 

# **3.12.1.32 ZDO\_JOIN\_REQ**

# **Description**:

This command is used to request the device to join itself to a parent device on a network.

## Usage:

# **SREQ:**

Byte: 1	1	1	1	2
Length = $0x0F$	Cmd0 = 0x25	Cmd1 = 0x27	Logical Channel	Pan ID
8	2	1	1	
Extended Pan ID	Chosen Parent	Parent Depth	Stack Profile	

#### **Attributes:**

Attribute	Length (byte)	Description
Logical Channel	1	Channel where the PAN is located
Pan ID	2	Id of PAN to join
Extended Pan ID	8	64-bit extended PAN ID (ver. 1.1 only). If not v1.1 or don't care, use all $0xFF$
Chosen Parent	2	Short address of the parent device chosen to join
Parent Depth	1	Depth of the parent
Stack Profile	1	Stack profile of the network to join

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x27	Status

Attribute	Length (byte)	Description
		Success (0)
Status	1	ZNwkInvalIdRequest (0xC2) if device is already on a network. Leave the network first, then try to join again.
		ZNwkNotPermitted (0xC3) if chosen router is not a valid short address.

# 3.12.1.33 ZDO\_SET\_REJOIN\_PARAMETERS

# **Description:**

This command is used to set rejoin backoff duration and rejoin scan duration for an end device

## Usage:

## **SREQ:**

Byte: 1	1	1	4	4
Length = $0x08$	Cmd0 = 0x25	Cmd1 = 0x26	Backoff Duration	Scan Duration

## **Attributes**:

Attribute	Length (byte)	Description
Backoff Duration	4	Rejoin backoff duration for end device
Scan Duration	4	Rejoin scan duration for end device

## **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x27	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Success (0)

# 3.12.1.34 ZDO\_SEC\_ADD\_LINK\_KEY

# **Description:**

This command handles the ZDO security add link key extension message.

## Usage:

# **SREQ:**

Byte: 1	1	1	2	8	16
Length = $0x1A$	Cmd0 = 0x25	Cmd1 = 0x42	Short Address	Extended Adress	Key

#### **Attributes:**

Attribute	Length (byte)	Description
Short Address	2	short address of the partner device
Extended Address	8	extended address of the partner device
Key	16	Link key

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x42	Status

## **Attributes**:

Attribute	Length (byte)	Description	
Status	1	Success (0) or Failure(1)	

# 3.12.1.35 ZDO\_SEC\_ENTRY\_LOOKUP\_EXT

# **Description:**

This command handles the ZDO security entry lookup extended extension message.

## Usage:

# **SREQ:**

Byte: 1	1	1	8	5
Length = $0x013$	Cmd0 = 0x25	Cmd1 = 0x43	Extended Adress	Entry

## **Attributes**:

Attribute	Length (byte)	Description
Extended Address	8	extended address
entry	5	Valid entry

## **SRSP:**

Byte: 1	1	1	2	2	1
Length = 0x05	Cmd0 = 0x65	Cmd1 = 0x42	AMI	KeyNVID	Authentication option

## **Attributes:**

Attribute	Length (byte)	Description
AMI	2	Address manager index
KeyNVID	2	Index to link key table in NV
Authentication option	1	Authentication option for device

# 3.12.1.36 ZDO\_SEC\_DEVICE\_REMOVE

# **Description:**

This command handles the ZDO security remove device extended extension message.

## **Usage:**

## **SREQ:**

Byte: 1	1	1	8
Length = 0x08	Cmd0 = 0x25	Cmd1 = 0x44	Extended Adress

Attribute Length (byte) Description
-------------------------------------

Extended Address 8 extended address

#### **SRSP:**



## **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status of device remove

# 3.12.1.37 ZDO\_EXT\_ROUTE\_DISC

## **Description:**

This command handles the ZDO route discovery extension message.

# Usage:

## **SREQ:**

Byte: 1	1	1	2	1	1
Length = $0x04$	Cmd0 = 0x25	Cmd1 = 0x45	Destination Address	Options	Radius

## **Attributes:**

Attribute	Length (byte)	Description
Destination Address	2	Destination address
Options	1	Route options
Radius	1	Broadcast radius

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x45	Status

## **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status of route discovery

# 3.12.1.38 ZDO\_EXT\_ROUTE\_CHECK

# **Description:**

This command handles the ZDO route check extension message.

# Usage:

# **SREQ:**

Byte: 1	1	1	2	1	1
Length = $0x04$	Cmd0 = 0x25	Cmd1 = 0x46	Destination Address	RTStatus	Options

#### **Attributes**:

Attribute	Length (byte)	Description
Destination Address	2	Destination address
RtStatus	1	Status value for routing entries
Options	1	Route options

## **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x46	Status

Attribute	Length (byte)	Description	
Status	1	Status of route check	

# 3.12.1.39 ZDO\_EXT\_REMOVE\_GROUP

## **Description:**

This command handles the ZDO extended remove group extension message.

# Usage:

# **SREQ:**

Byte: 1	1	1	1	2
Length = $0x03$	Cmd0 = 0x25	Cmd1 = 0x47	Endpoint	GroupID

#### **Attributes:**

Attribute	Length (byte)	Description	
Endpoint	1	Endpoint to look for	
GroupID	2	ID to look for group	

#### **SRSP:**

Byte: 1	1	1	1
Length = 0x01	Cmd0 = 0x65	Cmd1 = 0x47	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status of remove group

# 3.12.1.40 ZDO\_EXT\_REMOVE\_ALL\_GROUP

# **Description:**

This command handles the ZDO extended remove all group extension message.

## Usage:

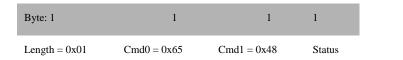
## **SREQ:**

Byte: 1	1	1	1	
Length = $0x01$	Cmd0 = 0x25	Cmd1 = 0x48	Endpoint	

#### **Attributes**:

Attribute	Length (byte)	Description	
Endpoint	1	Endpoint to look for	

## **SRSP:**



#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status of remove all groups

# 3.12.1.41 ZDO\_EXT\_FIND\_ALL\_GROUPS\_ENDPOINT

# **Description:**

This command handles the ZDO extension find all groups for endpoint message

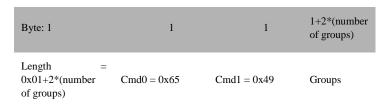
## Usage:

## **SREQ:**

Byte: 1	1	1	1	2
Length = $0x03$	Cmd0 = 0x25	Cmd1 = 0x49	Endpoint	GroupList

Attribute	Length (byte)	Description	
Endpoint	1	Endpoint to look for	
GroupList	2	List to hold group IDs	

## **SRSP:**



## **Attributes**:

Attribute	Length (byte)	Description
Groups	1+2*(number of groups)	Number of groups copied to group list

# 3.12.1.42 ZDO\_EXT\_FIND\_GROUP

# **Description:**

This command handles the ZDO extension find group message

# Usage:

# **SREQ:**

Byte: 1	1	1	1	2
Length = $0x03$	Cmd0 = 0x25	Cmd1 = 0x4A	Endpoint	GroupID

#### **Attributes:**

Attribute	Length (byte)	Description	
Endpoint	1	Endpoint to look for	
GroupID	2	Group ID	

## **SRSP:**

Byte: 1	1	1	0-18
Length = 0x01-0x13	Cmd0 = 0x65	Cmd1 = 0x4A	Group

Attribute	Length (byte)	Description
Group	0-18	Group information

# 3.12.1.43 ZDO\_EXT\_ADD\_GROUP

## **Description:**

This command handles the ZDO extension add group message.

# Usage:

## **SREQ:**

Byte: 1	1	1	1	2	16
Length = $0x013$	Cmd0 = 0x25	Cmd1 = 0x4B	Endpoint	GroupID	GroupName

#### **Attributes:**

Attribute	Length (byte)	Description	
Endpoint	1	Endpoint to look for	
GroupID	2	Group ID	
GroupName	16	Group name	

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x4B	Status

#### **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status of adding group

# 3.12.1.44 ZDO\_EXT\_COUNT\_ALL\_GROUPS

## **Description:**

This command handles the ZDO extension count all groups message.

# Usage:

# **SREQ:**

Byte: 1	1	1
Length = $0x00$	Cmd0 = 0x25	Cmd1 = 0x4C

Attribute	Length (byte)	Description	
None			

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x4C	Status

#### **Attributes**:

Attribute	Length (byte)	Description
Status	1	Total number of groups

# **3.12.1.45 ZDO\_EXT\_RX\_IDLE**

## **Description:**

This command handles the ZDO extension Get/Set RxOnIdle to ZMac message

# Usage:

## **SREQ:**

Byte: 1	1	1	1	1
Length = $0x02$	Cmd0 = 0x25	Cmd1 = 0x4D	SetFlag	SetValue

#### **Attributes**:

Attribute	Length (byte)	Description
SetFlag	1	Set or get the value
SetValue	1	Value to be set to ZMac message

## SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x4D	Status

Attribute	Length (byte)	Description
Status	1	Status of get or set value

# 3.12.1.46 ZDO\_EXT\_UPDATE\_NWK\_KEY

## **Description:**

This command handles the ZDO security update network key extension message.

# Usage:

## **SREQ:**

Byte: 1	1	1	2	1	128
Length = $0x083$	Cmd0 = 0x25	Cmd1 = 0x4E	Destination Address	KeySeqNum	Key

#### **Attributes:**

Attribute	Length (byte)	Description
DestinationAddress	2	Destination address
KeySeqNum	1	Key Sequence number
Key	128	Network key

## **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x4E	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status of key update

# 3.12.1.47 ZDO\_EXT\_SWITCH\_NWK\_KEY

## **Description:**

This command handles the ZDO security switch network key extension message.

## **Usage:**

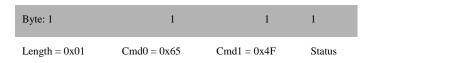
## **SREQ:**

Byte: 1	1	1	2	1
Length = $0x03$	Cmd0 = 0x25	Cmd1 = 0x4F	Destination Address	KeySeqNum

#### **Attributes**:

Attribute	Length (byte)	Description
DestinationAddress	2	Destination address
KeySeqNum	1	Key Sequence number

## SRSP:



#### **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status of key switch

# 3.12.1.48 ZDO\_EXT\_NWK\_INFO

# **Description:**

This command handles the ZDO extension network message.

# Usage:

# **SREQ:**

Byte: 1	1	1
Length = $0x00$	Cmd0 = 0x25	Cmd1 = 0x50

#### **Attributes:**

Attribute	Length (byte)	Description
None		

## **SRSP:**

Byte: 1		1	1	2	2	2	8	8	2
Length 0x18	=	Cmd0 = 0x65	Cmd1 = 0x50	Short Address	PAN ID	Parent address	Extended PAN ID	Extended Parent Address	Channel

te Length (byte) Description
------------------------------

Short Address	2	Short address
PAN ID	2	PAN ID
Parent Address	2	Parent address
Extended PAN ID	8	Extended PAN ID
Extended Parent Address	8	IEEE address of parent
Channel	2	Current channel

# 3.12.1.49 ZDO\_EXT\_SEC\_APS\_REMOVE\_REQ

# **Description:**

This command handles the ZDO extension Security Manager APS Remove Request message.

## Usage:

# **SREQ:**

Byte: 1	1	1	2	8	2
Length = $0x0c$	Cmd0 = 0x25	Cmd1 = 0x51	NWK Address	Extended Address	Parent address

#### **Attributes:**

Attribute	Length (byte)	Description
NWK Address	2	Device's network address
Extended Address	8	IEEE address of device
Parent Address	2	Parent's network address

## **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x65	Cmd1 = 0x51	Status

Status 1 Status of removing device from the network

# 3.12.1.50 ZDO\_FORCE\_CONCENTRATOR\_CHANGE

#### **Description:**

This command forces a network concentrator change by resetting zgConcentratorEnable and zgConcentratorDiscoveryTime from NV and set nwk event.

**Usage:** 

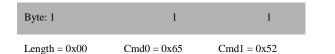
#### **SREQ:**

Byte: 1	1	1
Length = $0x00$	Cmd0 = 0x25	Cmd1 = 0x52

#### **Attributes:**

Attribute	Length (byte)	Description
None		

#### **SRSP:**



#### **Attributes:**

None

# 3.12.1.51 ZDO\_EXT\_SET\_PARAMS

## **Description:**

This command set parameters not settable through NV.

**Usage:** 

## **SREQ:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x25	Cmd1 = 0x53	useMulticast

Attribute Length (byte) Description
-------------------------------------

useMulticast 1 Set or reset the use of multicast

#### SRSP:



## **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status of use of multicast

# 3.12.1.52 ZDO\_NWK\_ADDR\_OF\_INTEREST\_REQ

## **Description:**

This command handles ZDO network address of interest request.

## **Usage:**

## **SREQ:**

Byte: 1	1	1	2	2	1
Length = $0x05$	Cmd0 = 0x25	Cmd1 = 0x29	destAddr	nwkAddrofIntere st	cmd

## **Attributes:**

Attribute	Length (byte)	Description
destAddr	2	Destination Address
nwkAddrofInterest	2	16 bit network address of interest
cmd	1	A valid cluster ID as specified by the Profile

# **SRSP:**

Byte: 1	1	1	1
Length = 0x01	Cmd0 = 0x65	Cmd1 = 0x29	Status

|--|

Status 1 AF status

# 3.12.2 MT\_ZDO Callbacks

# 3.12.2.1 ZDO\_NWK\_ADDR\_RSP

## **Description:**

This command is issued by the tester to return the results from a  ${\tt ZDO}$  NWK  ${\tt ADDR}$   ${\tt REQ}$ .

#### Usage

## **AREQ:**





Attribute	Length (byte)	Description
Status	1	This field indicates either SUCCESS or FAILURE.
IEEEAddr	8	64 bit IEEE address of source device.
NwkAddr	2	Specifies the short network address of responding device.
StartIndex	1	Specifies the starting index into the list of associated devices for this report.
NumAssocDev	1	Specifies the number of associated devices.
AssocDevList	0-70	Contains the list of network address for associated devices. This list can be a partial list if the entire list doesn't fit into a packet. If it is a partial list, the starting index is StartIndex.

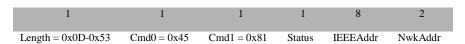
# 3.12.2.2 ZDO\_IEEE\_ADDR\_RSP

# **Description:**

This callback message is in response to the ZDO IEEE Address Request.

Usage:

## **AREQ:**



1	1	0-70
StartIndex	NumAssocDev	AssocDevList

Attribute	Length (byte)	Description
Status	1	This field indicates either SUCCESS or FAILURE.
IEEEAddr	8	64 bit IEEE address of source device.
NwkAddr	2	Specifies the short network address of responding device.
StartIndex	1	Specifies the starting index into the list of associated devices for this report.
NumAssocDev	1	Specifies the number of associated devices.
AssocDevList	0-70	Contains the list of network address for associated devices. This list can be a partial list if the entire list doesn't fit into a packet. If it is a partial list, the starting index is StartIndex.

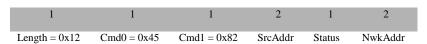
# 3.12.2.3 ZDO\_NODE\_DESC\_RSP

# **Description:**

This callback message is in response to the ZDO Node Descriptor Request.

# **Usage:**

# **AREQ:**



1	1	1	2
LogicalType/	APSFlags/	MACCapabilityFlags	ManufacturerCode
ComplexDescAvailable/	FrequencyBand		
UserDescAvailable			

1	2	2	2	1
MaxBufferSize	MaxTransferSize	ServerMask	MaxOutTransferSize	DescriptorCapabilities

Attribute	Length (byte)	Description
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS or FAILURE.
NWKAddrOfInterest	2	Device's short address of this Node descriptor
		Logical Type: Bit 0-2 –
		Description Value
		ZigBee Coordinator 0
LogicalType/		ZigBee Router 1
ComplexDescriptorAvailable/ UserDescriptorAvailable	1	ZigBee End Device 2
		ComplexDescriptorAvailable: Bit 3 – Indicates if complex descriptor is available for the node UserDescriptorAvailable: Bit 4 – Indicates if user descriptor is available for the node
		Reserved: Bit 5-7 – Reserved for future use
APSFlags/FrequencyBand	1	eq:APSFlags-Bit 0-4-Node Flags assigned for APS. For V1.0 all bits are reserved.
		NodeFrequencyBand – Bit 5-7 – Identifies node frequency band capabilities

# Capability flags stored for the MAC:

		Description	Value
		CAPINFO_DEVICETYPE_RFD	0x00
		CAPINFO_ALTPANCOORD	0x01
MacCapabilitiesFlags	1	CAPINFO_DEVICETYPE_FFD	0x02
		CAPINFO_POWER_AC	0x04
		CAPINFO_RCVR_ON_IDLE	0x08
		CAPINFO_SECURITY_CAPABLE	0x40
		CAPINFO_ALLOC_ADDR	0x80
ManufacturerCode	2	Specifies a manufacturer code that is allocated	
manufacturer Code 2	2	ZigBee Alliance, relating to the manufacture device.	r to tne
MaxBufferSize	1	Indicates size of maximum NPDU. This field a high level indication for management.	l is used as
MaxInTransferSize	2	Indicates maximum size of Transfer up to 0x field is reserved in version 1.0 and shall be so	,
		Bit 0 - Primary Trust Center	
		1 - Backup Trust Center	
C M 1	2	2 - Primary Binding Table Cache	
ServerMask	2	3 - Backup Binding Table Cache	
		4 - Primary Discovery Cache	
		5 - Backup Discovery Cache	
MaxOutTransferSize	2	Indicates maximum size of Transfer up to 0x field is reserved in version 1.0 and shall be so	
DescriptorCapabilities	1	Specifies the Descriptor capabilities	

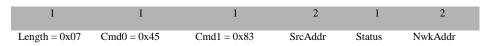
# 3.12.2.4 ZDO\_POWER\_DESC\_RSP

# **Description:**

This callback message is in response to the ZDO Power Descriptor Request.

# **Usage:**

# **AREQ:**



1 CurrentPowerMode/AvailablePowerSources CurrentPowerSource/CurrentPowerSourceLevel

Attribute	Length (byte)	Description
SrcAddr	2	Specifies the message's source network address.
Status	1	This field indicates either SUCCESS or FAILURE.
NWKAddr	2	Specifies Device's short address that this response describes.
		- CurrentPowerMode: bits 3-0
CurrentPowerMode/AvailablePowerSources	1	- AvailablePowerSources: bits 7-4
		- CurrentPowerSource: bits 3-0
CurrentPowerSource/CurrentPowerSourceLevel	1	- CurrentPowerSourceLevel: bits 7-4

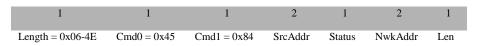
# ${\bf 3.12.2.5} \quad {\bf ZDO\_SIMPLE\_DESC\_RSP}$

# **Description:**

This callback message is in response to the ZDO Simple Descriptor Request

# **Usage:**

# **AREQ:**







Attribute	Length (byte)	Description
SrcAddr	2	Specifies the message's source network address.
Status	1	This field indicates either SUCCESS or FAILURE.
NWKAddr	2	Specifies Device's short address that this response describes.
Len	1	Specifies the length of the simple descriptor
Endpoint	1	Specifies Endpoint of the device
ProfileId	2	The profile Id for this endpoint.
DeviceId	2	The Device Description Id for this endpoint.
		Defined as the following format
DeviceVersion	1	0 – Version 1.00
		0x01-0x0F – Reserved.
NumInClusters	1	The number of input clusters in the InClusterList.
InClusterList	0-32	List of input cluster Id's supported.
NumOutClusters	1	The number of output clusters in the OutClusterList.
OutClusterList	0-32	List of output cluster Id's supported.

# 3.12.2.6 ZDO\_ACTIVE\_EP\_RSP

# **Description:**

This callback message is in response to the ZDO Active Endpoint Request.

# **Usage:**

# **AREQ:**



0-77

ActiveEPList

Attribute	Length (byte)	Description
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS or FAILURE.
NWKAddr	2	Device's short address that this response describes.
ActiveEPCount	1	Number of active endpoint in the list
ActiveEPList	0-77	Array of active endpoints on this device.

# 3.12.2.7 ZDO\_MATCH\_DESC\_RSP

# **Description:**

This callback message is in response to the ZDO Match Descriptor Request.

Usage:

# **AREQ:**



0-77

MatchList

#### **Attributes:**

Attribute	Length (byte)	Description
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS or FAILURE.
NWKAddr	2	Device's short address that this response describes.
MatchLength	1	The count of endpoints on the remote device that match the request criteria
MatchList	0-77	List of bytes, each represents an 8 bit endpoint

# 3.12.2.8 ZDO\_COMPLEX\_DESC\_RSP

#### **Description:**

This callback message is in response to the ZDO Complex Descriptor Request.

#### Usage:

#### **AREQ:**



0-77

ComplexList

#### **Attributes:**

Attribute	Length (byte)	Description
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS or FAILURE.
NWKAddr	2	Device's short address that this response describes.
ComplexLength	1	Length of the complex descriptor.
ComplexDescriptor	0-77	Array of bytes contains the complex descriptor.

# 3.12.2.9 ZDO\_USER\_DESC\_RSP

# **Description:**

This callback message is in response to the ZDO User Descriptor Request.

#### **Usage:**

# **AREQ:**

1	1	1	2	1	2	1	0-77
Length = $0x06-0x16$	Cmd0 = 0x45	Cmd1 = 0x88	SrcAddr	Status	NwkAddr	Len	UserDescriptor

#### **Attributes:**

Attribute	Length (byte)	Description
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS or FAILURE.
NWKAddr	2	Device's short address that this response describes.
UserLength	1	Length of the complex descriptor.
UserDescriptor	0-77	Array of bytes contains user descriptor.

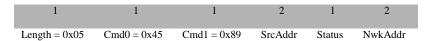
# 3.12.2.10 ZDO\_USER\_DESC\_CONF

# **Description:**

This confirmation notifies the user when the device receives a user descriptor.

# Usage:

# **AREQ:**



#### **Attributes:**

Attribute	Length (byte)	Description
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS or FAILURE.
NWKAddr	2	Device's short address that this response describes.

# 3.12.2.11 ZDO\_SERVER\_DISC\_RSP

# **Description:**

This callback message is in response to the ZDO System Service Discovery Request. Upon receiving the request, remote devices shall compare the ServerMask parameter to the Server Mask field in their own Node descriptor. If no bits are found to match, no action is taken.

# **Usage:**

# **AREQ:**

1	1	1	2	1	2
Length = $0x05$	Cmd0 = 0x45	Cmd1 = 0x8A	SrcAddr	Status	ServerMask

Attribute	Length (byte)	Description
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).
		Each bit signifies one system server capability of the node. The bit setting is defined in the following table:

		Bit Number	Assignment
		0	Primary Trust Center
		1	Backup Trust Center
Server Mask	2	2	Primary Binding Table Cache
		3	Backup Binding Table Cache
		4	Primary Discovery Cache
		5	Backup Discovery Cache
		6–15	Reserved

# 3.12.2.12 ZDO\_END\_DEVICE\_BIND\_RSP

# **Description:**

This callback message is in response to the ZDO End Device Bind Request.

# Usage:

# **AREQ:**

1	1	1	2	1
Length = $0x03$	Cmd0 = 0x45	Cmd1 = 0xA0	SrcAddr	Status

# **Attributes:**

Attribute	Length (byte)	Description
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).

# **3.12.2.13 ZDO\_BIND\_RSP**

#### **Description:**

This callback message is in response to the ZDO Bind Request.

# **Usage:**

# **AREQ:**



Attribute	Length (byte)	Description
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).

# 3.12.2.14 ZDO\_UNBIND\_RSP

# **Description:**

This callback message is in response to the ZDO Unbind Request.

#### Usage:

#### **AREQ:**

Byte: 1	1	1	2	1
Length = $0x03$	Cmd0 = 0x45	Cmd1 = 0xA2	SrcAddr	Status

#### **Attributes:**

Attribute	Length (byte) Description	
SrcAddr	2	The message's source network address.
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).

# 3.12.2.15 ZDO\_MGMT\_NWK\_DISC\_RSP

# **Description:**

This callback message is in response to the ZDO Management Network Discovery Request.

#### Usage:

# **AREQ:**





Attribute	Lengt h (byte)	Description
SrcAddr	2	Source address of the message.
Status	1	This field indicates either SUCCESS or FAILURE.
NetworkCount	1	Total number of entries available in the device.
StartIndex	1	Where in the total number of entries this response starts.
NetworkListCou nt	1	Number of entries in this response.

An array of NetworkList items. NetworkListCount contains the number of items in this table

Name Size Description PAN ID/Extended PAN 2 bytes PAN ID of the neighbor device Logical Channel 1 byte The current logical channel occupied by the network. Stack Profile / ZigBee 1 byte StackProfile: bits 3-0 Version ZigBeeVersion: bits 7-4 A ZigBee stack profile Identifier indicating stack profile in use in the discovered networ The version of the ZigBee protocol in use in the discovered network. Beacon Order / Super BeaconOrder: bits 3-0 1 byte frame Order SuperframeOrder: bits 7-4 Permit Joining 1 byte Permit joining flag

NetworkList List

# 3.12.2.16 ZDO\_MGMT\_LQI\_RSP

# **Description:**

This callback message is in response to the ZDO Management LQI Request.

#### Usage:

#### **AREQ:**





Attribute	Length (byte)	Description	
SrcAddr	2	Source address of the message.	
Status	1	This field indicates either SUCCESS or FAILURE.	
NeighborTableEntries	1	Total number of entries available in the device.	
StartIndex	1	Where in the total number of entries this response starts.	

NeighborLqiListCount

Number of entries in this response.

1

0-66

An array of NeighborLqiList items. NeighborLQICount contains the number of items in this table.

Name Size Description ExtendedPanID 8 bytes Extended PAN ID of the neighbor device ExtendedAddress 8 bytes Network extended address NetworkAddress 2 bytes Device short address DeviceType/ 1 byte DeviceType: bits 1-0 RxOnWhenIdle/ RxOnWhenIdle: bits 3-2 Relationship Relationship: bits 6-4 PermitJoining 1 byte PermitJoining: bits 1-0 Depth 1 byte LQI 1 byte

NeighborLqiList

# 3.12.2.17 ZDO\_MGMT\_RTG\_RSP

#### **Description:**

This callback message is in response to the ZDO Management Routing Table Request.

#### Usage:

#### **AREQ:**



1 0-75

RoutingTableListCount RoutingTableListRecords

Attribute	Length (byte)	Description	
SrcAddr	2	Source address of the message.	
Status	1	This field indicates either SUCCESS or FAILURE.	
RoutingTableEntries	1	Total number of entries available in the device.	

StartIndex 1 Where in the total number of entries this response starts.

RoutingTableListCount 1 Number of entries in this response.

An array of RtgList items. RtgListCount contains the number

of items in this table.

Name	Size	Description
Destination Address	2 bytes	Network destination address
Status	1 byte	Route status: bits 2-0  0x00 Active 0x01 Discovery Underway 0x02 Discovery Failed 0x03 Inactive 0x04 – 0x07 Reserved
Next Hop	2 bytes	Next hop network address

RoutingTableList 0-75

# 3.12.2.18 ZDO\_MGMT\_BIND\_RSP

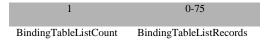
# **Description:**

This callback message is in response to the ZDO Management Binding Table Request.

#### Usage:

#### **AREQ:**





Attribute	Length (byte)	Description
SrcAddr	2	Source address of the message
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).
BindTableEntries	1	Total number of entries available in the device.
StartIndex	1	Where in the total number of entries this response starts.

BindTableListCount

Number of entries in this response.

An array of BindList items. BindListCount contains the number of items in this table.

Name	Size	Description
SrcAddr	8 bytes	Binding Entry's source IEEE address
SrcEndpoint	1 byte	Binding Entry's source endpoint
ClusterId	1 byte	Message Id in binding table
DstAddrMode	1 byte	Address mode for binding entry's destination address
DstAddr	8 bytes	Binding Entry's destination IEEE address
DstEndpoint	1 byte	Binding Entry's destination endpoint. For V1.1, this field is only present when the DestAddrMode is 64-bits extended address.

BindTableList List

# 3.12.2.19 ZDO\_MGMT\_LEAVE\_RSP

# **Description:**

This callback message is in response to the ZDO Management Leave Request.

#### **Usage:**

#### **AREQ:**

Byte: 1	1	1	2	1
Length = $0x03$	Cmd0 = 0x45	Cmd1 = 0xB4	SrcAddr	Status

#### **Attributes:**

Attribute	Length (byte)	Description
SrcAddr	2	Source address of the message
Status	1	This field indicates either SUCCESS (0) or FAILURE (1)

# ${\bf 3.12.2.20\ ZDO\_MGMT\_DIRECT\_JOIN\_RSP}$

# **Description:**

This callback message is in response to the ZDO Management Direct Join Request.

#### **Usage:**

#### **AREQ:**



 $Length = 0x03 \qquad Cmd0 = 0x45 \qquad Cmd1 = 0xB5 \qquad SrcAddr \qquad Status$ 

#### **Attributes:**

Attribute	Length (byte)	Description
SrcAddr	2	Source address of the message
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).

# 3.12.2.21 ZDO\_MGMT\_PERMIT\_JOIN\_RSP

# **Description:**

This callback message is in response to the ZDO Management Permit Join Request.

#### **Usage:**

# **AREQ:**



#### **Attributes:**

Attribute	Length (byte)	Description
SrcAddr	2	Source address of the message.
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).

# 3.12.2.22 ZDO\_STATE\_CHANGE\_IND

#### **Description:**

This callback message indicates the ZDO state change.

#### Usage:

# **AREQ:**



Attribute	Length (byte)	Description
State	1	Specifies the changed ZDO state.

# 3.12.2.23 ZDO\_END\_DEVICE\_ANNCE\_IND

# **Description:**

This callback indicates the ZDO End Device Announce.

# Usage:

# **AREQ:**

Byte: 1	1	1	2	2	8	1
Length = 0x0D	Cmd0 = 0x45	Cmd1 = 0xC1	SrcAddr	NwkAddr	IEEEAddr	Capabilites

Attribute	Length (byte)	Description
SrcAddr	2	Source address of the message.
NwkAddr	2	Specifies the device's short address.
IEEEAddr	8	Specifies the 64 bit IEEE address of source device.
		Specifies the MAC capabilities of the device.
		Bit: 0 – Alternate PAN Coordinator
		1- Device type: $1-$ ZigBee Router; $0-$ End Device
		2 – Power Source: 1 Main powered
Capabilites	1	3 – Receiver on when Idle
		4 – Reserved
		5 – Reserved
		6 – Security capability
		7 – Reserved

# 3.12.2.24 ZDO\_MATCH\_DESC\_RSP\_SENT

# **Description:**

This callback indicates that Match Descriptor Response has been sent.

# **Usage:**

# **AREQ:**

Byte: 1	1	1	2
Length = 0x04-0x44	Cmd0 = 0x45	Cmd1 = 0xC2	NwkAddr

1	0-32	1	0-32
NumInClusters	InClusterList	NumOutClusters	OutClusterList

# **Attributes:**

Attribute	Length (byte)	Description
NwkAddr	2	Specifies the device's short address
NumInClusters	1	The number of input clusters in the InClusterList.
InClusterList	0-32	List of input cluster Id's supported.
NumOutClusters	1	The number of output clusters in the OutClusterList.
OutClusterList	0-32	List of output cluster Id's supported.

# 3.12.2.25 ZDO\_STATUS\_ERROR\_RSP

# **Description:**

This message is the default message for error status.

# **Usage:**

# **AREQ:**

Byte: 1	1	1	2	1
Length = $0x04-0x44$	Cmd0 = 0x45	Cmd1 = 0xC3	SrcAddr	Status

Attribute	Length (byte)	Description
SrcAddr	2	Source address of the message
Status	1	This field indicates either SUCCESS (0) or FAILURE (1).

# 3.12.2.26 ZDO\_SRC\_RTG\_IND

# **Description:**

This message is an indication to inform host device the receipt of a source route to a given device.

# **Usage:**

#### **AREQ:**

Byte: 1	1	1	2	1	2N
Length = 0x04-0x44	Cmd0 = 0x45	Cmd1 = 0xC4	dstAddr	Relay Count (N)	Relay List

#### **Attributes:**

Attribute	Length (byte)	Description
DstAddr	2	Short address of the destination of the source route
Relay Count	1	This field indicates number of devices in the relay list of the source route.
Relay List	2N	This field contains the list of devices in the relay list of the source route. It includes a two bytes short address for each device.

# 3.12.2.27 ZDO\_BEACON\_NOTIFY\_IND

# **Description:**

This message is an indication to inform host device the receipt of a beacon notification.

# Usage:

# **AREQ:**

Byte: 1	1	1	1	N*21
Length = 21	Cmd0 = 0x45	Cmd1 = 0xC5	BeaconCount	BeaconList

Attribute	Length (byte)	Description
BeaconCount	1	Number of beacons in the packet.

An array of BeaconList items. BeaconCount contains the number of items in this table.

Name	Size	Description
Source Address	2	Short address of the source device of the beacon
Pan ID	2	ID of the PAN
Logical Channel	1	Channel where the PAN is located.
Permit Joining	1	Flag to indicate whether the device accept association.
Router Capacity	1	Flag to indicate whether the device accept other router to associate
Device Capacity	1	Flag to indicate whether the device accept other device to associate
Protocol Version	1	Version of the ZigBee protocol. Value '1' represents ZigBee 2004. Value '2' represents ZigBee 2006/2007
Stack Profile	1	Stack profile of the PAN: Stack Profile 1 for ZigBee and Stack Profile 2 for ZigBee Pro.
LQI	1	LQI (Link quality indicator) measurement of the beacon.
Depth	1	Depth of the source device, i.e. number of hops from the device to the ZigBee coordinator.
Update ID	1	Update ID of the device.
Extended Pan ID	8	64 bit extended Pan ID of the Pan.

# **3.12.2.28 ZDO\_JOIN\_CNF**

# **Description:**

This message is an indication to inform host device the result of a ZDO join request.

# **Usage:**

#### **AREQ:**

Byte: 1	1	1	1	2	2
Length = 0x05	Cmd0 = 0x45	Cmd1 = 0xC6	status	Device Address	Parent Address

#### **Attributes:**

Attribute	Length (byte)	Description
		Return status of the join request:
Status	1	Success (0)
		ZMAC_NO_ACK (0xE9) if the chosen parent device dId
		not respond to the association request.
Device Address	2	Short address of the device.
Parent Address	2	Short address of the parent device

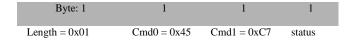
# 3.12.2.29 ZDO\_NWK\_DISCOVERY\_CNF

# **Description:**

This message is an indication to inform host device the completion of network discovery scan.

# Usage:

# **AREQ:**



Attribute	Length (byte)	Description
		Return status of the network discovery.
		Success (0)
Status	1	ZMAC_NO_BEACON (0xEA)
		ZMAC_INVALID_PARAMETER (0xE8) if input parameter is out of valid range.

# 3.12.2.30 ZDO\_LEAVE\_IND

#### **Description:**

This message is an indication to inform the host of a device leaving the network.

#### Usage:

#### **AREQ:**

Byte: 1	1	1	2	8	1	1	1
Length=0x0D	Cmd0=0x45	Cmd1=0xC9	SrcAddr	ExtAddr	Request	Remove	Rejoin

#### **Attributes:**

Attribute	Length (byte)	Description
SrcAddr	2	Short address (LSB-MSB) of the source of the leave indication.
ExtAddr	8	Extended address (LSB-MSB) of the source of the leave indication.
Request	1	Boolean, TRUE = request, FALSE = indication.
Remove	1	Boolean, TRUE = remove children.
Rejoin	1	Boolean, TRUE = rejoin.

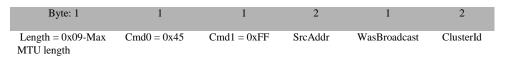
# 3.12.2.31 ZDO\_MSG\_CB\_INCOMING

# **Description:**

This message is a ZDO callback for a Cluster Id that the host requested to receive with a ZDO\_MSG\_CB\_REGISTER request.

#### **Usage:**

# **AREQ:**



1	1	2	0-Max MTU length
SecurityUse	SeqNum	MacDstAddr	Data

Attribute	Length (byte)	Description
SrcAddr	2	Short address (LSB-MSB) of the source of the ZDO message.
WasBroadcast	1	This field indicates whether or not this ZDO message was broadcast.

ClusterId	2	The ZDO Cluster Id of this message.
SecurityUse	1	N/A – not used.
SeqNum	1	The sequence number of this ZDO message.
MacDstAddr	2	The MAC destination short address (LSB-MSB) of the ZDO message.
Data	0-Max MTU length.	The data that corresponds to the Cluster Id of the message (see reference [4], "ZDO Parsing Functions" for information on parsing the data that corresponds to each ZDO Cluster Id).

# 3.12.2.32 ZDO\_TC\_DEV\_IND

# **Description:**

This message is a ZDO callback for TC Device Indication.

# Usage:

# **AREQ:**

Byte: 1	1	1	2	8	2
Length = $0x0C$	Cmd0 = 0x45	Cmd1 = 0xCA	SrcNwkA ddr	SrcIEEEAddr	Parent Nwk Addr

Attribute	Length (byte)	Description
SrcNwkAddr	2	Source network Address.
WasBroadcast	8	IEEE Address of the source
ParentNwkAddr	2	Network address of the parent

# 3.12.2.33 ZDO\_PERMIT\_JOIN\_IND

#### **Description:**

This message is a ZDO callback for Permit Join Indication.

#### **Usage:**

#### **AREQ:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x45	Cmd1 = 0xCB	PermitJoinDuration

#### **Attributes:**

Attribute	Length (byte)	Description
Permit Join Duration	1	Duration for which joining is permitted

# 3.13 MT\_APP\_CONFIG

This interface allows the tester to issue commands to configure some parameters of the device, trust center and BDB subsystem.

# 3.13.1 MT\_APP\_CONFIG Commands

#### 3.13.1.1 APP\_CNF\_SET\_NWK\_FRAME\_COUNTER

# **Description:**

This message sets the network frame counter to the value specified in the Frame Counter Value. For projects with multiple instances of frame counter, the message sets the frame counter of the current network.

#### **Usage:**

This message should only be use for debugging purposes. Changing the network frame counter in a production device, may cause the failures in the authentication process with other devices in the network.

#### **SREQ:**



#### **Attributes:**

Attribute	Length (byte)	Description
Frame Counter Value	4	Set the network frame counter to the specified value

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x6F	Cmd1 = 0xFF	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.13.1.2 APP\_CNF\_SET\_DEFAULT\_REMOTE\_ENDDEVICE \_TIMEOUT

# **Description:**

Sets the default value used by parent device to expire legacy child devices.

# Usage:

# **SREQ:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x2F	Cmd1 = 0x01	Timeout Index

Attribute	Length (byte)		Description
Timeout Index	1	-	e number of seconds until the timeout ording to the next list:
		0x00	10 seconds
		0x01	2 minutes
		0x02	4 minutes
		0x03	8 minutes
		0x04	16 minutes
		0x05	32 minutes

0x06	64 minutes
0x07	128 minutes
0x08	256 minutes (Default)
0x09	512 minutes
0x0A	1024 minutes
0x0B	2048 minutes
0x0C	4096 minutes
0x0D	8192 minutes
0x0E	16384 minutes

#### **SRSP:**

Byte: 1	1	1	1
Length = 0x01	Cmd0 = 0x6F	Cmd1 = 0x01	Status

# **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Invalid Parameter (2).

# 3.13.1.3 APP\_CNF\_SET\_ENDDEVICETIMEOUT

# **Description:**

Sets in ZED the timeout value to be send to parent device for child expiring.

# Usage:

# **SREQ:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x2F	Cmd1 = 0x02	Timeout Index

Attribute	Length (byte)		Description
Timeout Index	1		the number of seconds until the timeout according to the next list:
		0x00	10 seconds
		0x01	2 minutes

0x02	4 minutes
0x03	8 minutes
0x04	16 minutes
0x05	32 minutes
0x06	64 minutes
0x07	128 minutes
0x08	256 minutes (Default)
0x09	512 minutes
0x0A	1024 minutes
0x0B	2048 minutes
0x0C	4096 minutes
0x0D	8192 minutes
0x0E	16384 minutes

# **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x6F	Cmd1 = 0x02	Status

# **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Invalid Parameter (2).

# 3.13.1.4 APP\_CNF\_SET\_ALLOWREJOIN\_TC\_POLICY

# **Description:**

Sets the AllowRejoin TC policy.

# Usage:

# **SREQ:**

Byte: 1	1	1	1
Length = 0x01	Cmd0 = 0x2F	Cmd1 = 0x03	Allow Rejoin

Attribute	Length (byte)	Description

Allow Rejoin 1 This value specifies whether or not the Trust Center allows devices to rejoin.

# **SRSP:**



# **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.13.1.5 APP\_CNF\_BDB\_START\_COMMISSIONING

#### **Description:**

Set the commissioning methods to be executed. Initialization of BDB is executed with this call, regardless of its parameters.

# **Usage:**

#### **SREQ:**

Length = $0x01$ Cmd0 = $0$	x2F Cmd1 = 0	0x05 Commissioning mode

Attribute	Length (byte)		Description
Commissioning Mode	1		lue specifies the commissioning mode ng to this list:
Wode		0x00	Initialization
		0x01	TouchLink
		0x02	Network Steering
		0x04	Network Formation
		0x08	Finding and Binding

# **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x6F	Cmd1 = 0x05	Status

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.13.1.6 APP\_CNF\_BDB\_SET\_CHANNEL

# **Description:**

Sets BDB primary or secondary channel masks.

# Usage:

# **SREQ:**

Byte: 1	1	1	1
Length = $0x05$	Cmd0 = 0x2F	Cmd1 = 0x08	isPrimary
4			
Channel			

Attribute	Length (byte)	Desc	ription
isPrimary	1	This value specifies if the either primary or secondar	
Channel	4	This is the value of the ch following list of masks.	annel set according to the
		Channel 11	0x00000800
		Channel 12	0x00001000
		Channel 13	0x00002000
		Channel 14	0x00004000
		Channel 15	0x00008000
		Channel 16	0x00010000
		Channel 17	0x00020000

Ch	nannel 18	0x00040000
Ch	nannel 19	0x00080000
Ch	nannel 20	0x00100000
Ch	nannel 21	0x00200000
Ch	nannel 22	0x00400000
Ch	nannel 23	0x00800000
Ch	nannel 24	0x01000000
Ch	nannel 25	0x02000000
Ch	nannel 26	0x04000000

# **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x6F	Cmd1 = 0x08	Status

# **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.13.1.7 APP\_CNF\_BDB\_ADD\_INSTALLCODE

# **Description:**

Add a preconfigured key (plain key or IC) to Trust Center device.

# Usage:

# **SREQ:**

Byte: 1	1	1	1
Length = $0x19-0x1B$	Cmd0 = 0x2F	Cmd1 = 0x04	installCodeFormat
8	16-18	_	
IEEEAddress	installCode		

Attribute	Length (byte)	Description
installCodeFormat	1	This value specifies the format in which the install code is being added. The following list contains the values

corresponding to the supported formats:

0x01 Install Code + CRC

0x02 Key derived from Install Code

IEEEAddress 8 Full IEEE address for the device joining the network

installCode 16-18 16 Bytes for the Key derived from the IC

18 Bytes for the Install Code +CRC

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x6F	Cmd1 = 0x04	Status

#### **Attributes:**

Attribute	Length (byte)	Description
		Status values:
Status 1	0x00 Success	
	0x01 Failure (IC not supported)	
	0x02 Invalid parameter (bad CRC)	

# 3.13.1.8 APP\_CNF\_BDB\_SET\_TC\_REQUIRE\_KEY\_EXCHANGE

# **Description:**

Sets the policy flag on Trust Center device to mandate or not the TCLK exchange procedure.

#### Usage:

# **SREQ:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x2F	Cmd1 = 0x09	bdbTrustCenterRequireKeyExchange

Attribute	Length	Description	
-----------	--------	-------------	--

	(byte)	
bdbTrustCenterRequireKeyExchange	1	The bdbTrustCenterRequireKeyExchange attribute specifies whether the Trust Center requires a joining device to exchange its initial link key with a new link key generated by the Trust Center. If bdbTrustCenterRequireKeyExchange is equal to TRUE, the joining node must undergo the link key exchange procedure; failure to exchange the link key will result in the node being removed from the network. If bdbTrustCenterRequireKeyExchange is equal to FALSE, the Trust Center will permit the joining node to remain on the network without exchanging its initial link key. This attribute is used by ZigBee coordinator nodes.

#### SRSP:

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x6F	Cmd1 = 0x09	Status

# **Attributes**:

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

# 3.13.1.9 APP\_CNF\_BDB\_SET\_JOINUSESINSTALLCODEKEY

# **Description:**

Sets the policy to mandate or not the usage of an Install Code upon joining.

# Usage:

# **SREQ:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x2F	Cmd1 = 0x06	bdbJoinUsesInstallCodeKey

Attribute Length (byte)	Description
-------------------------	-------------

If it is equal to TRUE and the installation code derived link key is not stored, the Trust Center SHALL terminate the procedure for adding a new node into the network. If bdbJoinUsesInstall-CodeKey is equal to TRUE and the installation code derived link key is stored, the Trust Center SHALL first find the entry in apsDeviceKeyPairSet that corresponds to the joining node and then overwrite the LinkKey entry with the installation code derived link key and set the KeyAttributes field to PROVISIONAL\_KEY. The Trust Center MAY then set OutgoingFrame-Counter to 0 and SHALL set IncomingFrameCounter to 0. If bdbJoinUsesInstallCodeKey is equal to FALSE, the Trust Center SHALL first find the entry in

bdbJoinUsesInstallCodeKey

set OutgoingFrame-Counter to 0 and SHALL set IncomingFrameCounter to 0. If bdbJoinUsesInstallCodeKey is equal to FALSE, the Trust Center SHALL first find the entry in apsDeviceKeyPairSet that corresponds to the joining node and then overwrite the LinkKey entry with the default global Trust Center link key and set the KeyAttributes field to PROVISIONAL\_KEY. The Trust Center MAY then set OutgoingFrameCounter to 0 and SHALL set IncomingFrameCounter to 0.

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x6F	Cmd1 = 0x06	Status

1

#### **Attributes:**

Attribute	Length (byte)	Description
Status	1	Status is either Success (0) or Failure (1).

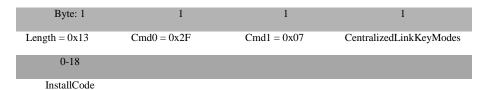
# 3.13.1.10 APP\_CNF\_BDB\_SET\_ACTIVE\_DEFAULT\_CENTRALIZED\_K EY

#### **Description:**

On joining devices, set the default key or an install code to attempt to join the network.

#### **Usage:**

#### **SREQ:**



# **Attributes:**

Attribute	Length (byte)		Description
			neter controls which key will be used when g association to a centralized network.
	KeyModes 1	0x00	Instruct joining node to use Default Global Trust Center link key. No key buffer requiered
		0x01	Instruct the joining node to use the provided install code (16 bytes + 2 CRC bytes) to derive APS Link key to be used during joining
CentralizedLinkKeyModes		0x02	Instruct the joining node to use the provided install code (16 bytes + 2 CRC bytes) to derive APS Link key to be used during joining.
			If it fails to decrypt Transport Key, it will automatically try Default Global Trust Center Link Key
		0x03	Instruct the joining node to use the provided APS Link key to be used during joining (key size is 16 bytes)
		0x04	Instruct the joining node to use the provided APS Link key to be used during joining (key size is 16 bytes). If it fails to decrypt Transport Key, it will automatically try Default Global Trust Center Link Key
InstallCode	0-18	Buffer with	n the key in any of its formtats.

# **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x6F	Cmd1 = 0x07	Status

Attribute	Length (byte)	Description
		Status values:
Status	Status 1	0x00 Success
Status		0x01 Failure (IC not supported)
		0x02 Invalid Parameters (bad CRC)

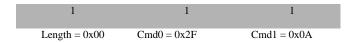
# 3.13.1.11 APP\_CNF\_BDB\_ZED\_ATTEMPT\_RECOVER\_NWK

# **Description:**

Instruct the ZED to try to rejoin its previews network. Use only in ZED devices.

# Usage:

# **SREQ:**



#### **Attributes:**

# **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x6F	Cmd1 = 0x0A	Status

Attribute	Length (byte)	Description
	Status 1	Status values:
Status		0x00 Success
		0x01 Failure (Device not ZED or doesn't
		have network parameters)

# 3.13.2 MT\_APP\_CONFIG Callbacks

# 3.13.2.1 APP\_CNF\_BDB\_COMMISSIONING\_NOTIFICATION

# **Description:**

Callback to receive notifications from BDB process.

# Usage:

# **AREQ:**

Byte: 1	1	1	1	1	1
Length = $0x03$	Cmd0 = 0x4F	Cmd1 = 0x80	Status	Commissioning mode	Remaining commissioning modes

Attribute	Length (byte)	Description
		Status of the commissioning mode being notified:
		0x00 BDB_COMMISSIONING_SUCCESS
		0x01 BDB_COMMISSIONING_IN_PROGRESS
		0x02 BDB_COMMISSIONING_NO_NETWORK
		0x03 BDB_COMMISSIONING_TL_TARGET_FAILURE
		0x04 BDB_COMMISSIONING_TL_NOT_AA_CAPABLE
		0x05 BDB_COMMISSIONING_TL_NO_SCAN_RESPONSE
G: ·	4	0x06 BDB_COMMISSIONING_TL_NOT_PERMITTED
Status	1	0x07 BDB_COMMISSIONING_TCLK_EX_FAILURE
		0x08 BDB_COMMISSIONING_FORMATION_FAILURE
		0x09 BDB_COMMISSIONING_FB_TARGET_IN_PROGRESS
		0x0A BDB_COMMISSIONING_FB_INITIATOR_IN_PROGRESS
		0x0B BDB_COMMISSIONING_FB_NO_IDENTIFY_QUERY_RESPONSE
		0x0C BDB_COMMISSIONING_FB_BINDING_TABLE_FULL
		0x0D BDB_COMMISSIONING_NETWORK_RESTORED
		0x0E BDB_COMMISSIONING_FAILURE
Commissioning	g 1	Commissioning mode for which the notification is done and to which the status is related:
mode		0x00 BDB_COMMISSIONING_INITIALIZATION

Lifetime

0x01 BDB\_COMMISSIONING\_NWK\_STEERING

0x02 BDB\_COMMISSIONING\_FORMATION

0x03 BDB\_COMMISSIONING\_FINDING\_BINDING

0x04 BDB\_COMMISSIONING\_TOUCHLINK

0x05 BDB\_COMMISSIONING\_PARENT\_LOST

Bitmask of the remaining commissioning modes after this notification:

0x01 BDB\_COMMISSIONING\_MODE\_INITIATOR\_TL

0x02 BDB\_COMMISSIONING\_MODE\_NWK\_STEERING

Remaining
commissioning

1 0x04 BDB\_COMMISSIONING\_MODE\_NWK\_FORMATION

0x08 BDB\_COMMISSIONING\_MODE\_FINDING\_BINDING

0x10 BDB\_COMMISSIONING\_MODE\_INITIALIZATION

# 3.14 MT\_GREENPOWER

This interface allows a host processor to interact with Green Power devices and Green Power infrastructure.

0x20 BDB\_COMMISSIONING\_MODE\_PARENT\_LOST

# 3.14.1 MT\_GP Commands

# **3.14.1.1 GP\_DATA\_REQ**

#### **Description:**

Callback to receive notifications from BDB process.

#### **Usage:**

#### **SREQ**



ASU

Length

Command ID

Attribute	Length (byte)	Range	Description
Action	1	TRUE/FALSE	TRUE: add GPDF into the queue
rector	1	TROE,TTESE	FALSE: remove GPDF from queue
			The transmission options for this GPDF. These are a
			bitwise OR of one or more of the following:
			b0 = Use gpTxQueue
			b1 = Use CSMA/CA
m o .:			b2 = Use MAC ACK
TxOptions	1	AnyValid	b3-b4 = GPDF frame type for Tx (can take non-reserved
			values as defined in Table 10)
			b5 = Tx on matching endpoint
			b6 – b7 – reserved
			ApplicationID of the GPD to which the ASDU will be sent;
			ApplicationID 0x00 indicates the usage of the SrcID;
Application ID	1	0x00, 0x02	ApplicationID 0x02 indicates the usage of the GPD IEEE
ID			address.
			The identifier of the GPD entity to which the ASDU will be
SrcID	4	0x00000000 - 0xffffffff	sent if ApplicationID = $0b000$ .
			The identifier of the GPD entity to which the ASDU will be
GPD IEEE address	8	Any valid	sent if ApplicationID = $0b010$ .
			The identifier of the GPD endpoint used in combination with the GPD IEEE address if ApplicationID = 0b010.
Endpoint	1	0x00 - 0xf0, 0xff	If ApplicationID = 0b000 this parameter is ignored.
F		0	ii Applicationii) – 00000 tilis parameter is ignored.
GPD Command ID	1	0x00- 0xff	The identifier of the command, within the GP specification, which defines the application semantics of the ASDU.
		0x00 -	which dornes are appreciation semantics of the ABB C.
GPD ASDU Length	1	(aMaxMACFrameSize -	The number of octets in the transmitted GPD ASDU.
-	CDD	9)	
GPD ASDU	GPD ASU	-	The sequence of octets forming the transmitted GPD ASDU.
	Length		

GPEP handle	1	0x00-0xff	The handle used between Green Power EndPoint and dGP stub, to match the request with the confirmation.
gpTxQueueE			The lifetime of this packet in the gpTxQueue, in milliseconds.
ntry-			0x000000 indicates immediate transmission.
Lifetime	3	0x000000-0xffffff	Oxffffff indicates infinity.
			In a Basic Proxy/Sink, the default lifetime MAY be 0xffffff.

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x75	Cmd1 = 0x01	Status

#### **Attributes:**

Attribute	Length (byte)	Description
		Status values:
Status	1	0x00 Success
		0x01 Failure (Out of memory)
		0x02 Invalid Parameters (Invalid App ID)

# **3.14.1.2 GP\_SEC\_RSP**

# **Description:**

This message provides a mechanism for the Green Power EndPoint to provide security data into the dGP stub.

# **Usage:**

# **SREQ**



8	1	1	1	16	4
GPD IEEE address	EndPoint	GPDFScurityLevel	GPDFKeyType	GPDKey	GPDSecurityFrameCounter

Attribute	Length (byte)	Range	Description
			The status code, as returned by the Green Power EndPoint.
			The following are supported:
Status	1	Any valid	MATCH
Status	1	Any vand	DROP_FRAME
			PASS_UNPROCESSED
			TX_THEN_DROP
dGP stub handle	1	0x00-0xff	The handle used between dGP stub and the higher layers, to match the request with the response.
Application ID	1	0x00, 0x02	ApplicationID of the GPD entity from which the ASDU was received. ApplicationID 0x00 indicates the usage of the SrcID; ApplicationID 0x02 indicates the usage of the GPD IEEE address.
SrcID	4	0x00000001 - 0xfffffffe	The identifier of the GPD entity from which the ASDU was received if ApplicationID = 0b000.
GPD IEEE address	8	Any valid	The identifier of the GPD entity from which the ASDU was received if ApplicationID = 0b010.
Endpoint	1	0x00 - 0xf0, 0xff	The identifier of the GPD endpoint used in combination with the GPD IEEE address if ApplicationID = 0b010.
			If Application $ID = 0b000$ this parameter is ignored.
GPDFSecurityL evel	1	0x00 - 0x07	The security level to be used for GPDF security processing.
GPDFKeyType	1	Any valid	The security key type to be used for GPDF security processing.
GPD Key	16	Any valid	The security key to be used for GPDF security processing.
GPD security frame counter	4	Any valid	The security frame counter value to be used for GPDF security processing.

#### **SRSP:**

Byte: 1	1	1	1
Length = $0x01$	Cmd0 = 0x75	Cmd1 = 0x02	Status

#### **Attributes:**

Attribute	Length (byte)	Description
	tatus 1	Status values:
Status		0x00 Success
		0x01 Failure (Out of memory)
		0x02 Invalid Parameters (Invalid App ID)

# **3.14.2** MT\_GP Callbacks

# **3.14.2.1 GP\_DATA\_CNF**

# **Description:**

Green power confirm is a message that provides a mechanism for the Green Power EndPoint in the host processor to understand the status of a previous request to send a GPDF.

# Usage:

# **AREQ**

Byte: 1	1	1	1	1
Length = $0x02$	Cmd0 = 0x55	Cmd1 = 0x05	Status	GP MPDU handle

Attribute	Length (byte)	Range	Description
Status	1	Any valid	Status code, as returned by the MAC layer (see Table 28 of [15]).
GP MPDU	1	0x00 - 0xff	The handle used between dGP/dLPED stub and cGP stub, to match the request with the confirmation.

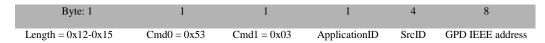
# **3.14.2.2 GP\_SEC\_REQ**

# **Description:**

This message provides a mechanism for dGP stub to request security data from the Green Power EndPoint in the host processor.

# **Usage:**

# **AREQ**





Attribute	Length (byte)	Range	Description
ApplicationID	1	0x00, 0x02	ApplicationID of the GPD entity from which the ASDU was received.
			ApplicationID 0x00 indicates the usage of the SrcID; ApplicationID 0x02 indicates the usage of the GPD IEEE address.
SrcID	4	0x00000001 - 0xfffffffe	The identifier of the GPD entity from which the ASDU was received if ApplicationID = $0b000$ .
GPD IEEE address	8	Any valid	The identifier of the GPD entity from which the ASDU was received if Application $ID = 0b010$ .
EndPoint	1	0x00 - 0xf0, 0xff	The identifier of the GPD endpoint used in combination with the GPD IEEE address if ApplicationID = 0b010. If ApplicationID = 0b000 this parameter is ignored.
GPDFSecurity Level	1	0x00, 0x02 - 0x03	The security level, corresponding to the received MPDU.
GPDFKey Type	1	0x00 - 0x01	The security key type, corresponding to the received MPDU.
GPD Security Frame Counter	1, 4	As specified by the GPDF Security Level parameter	The security frame counter value corresponding to the received MPDU.
dGP stub handle	1	0x00-0xff	The handle used between dGP stub and the higher layers, to match the request with the response.

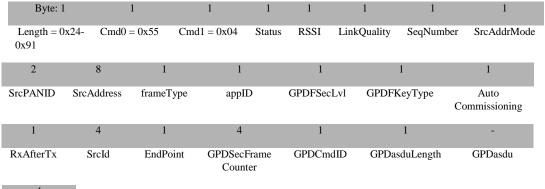
# 3.14.2.3 **GP\_DATA\_IND**

# **Description:**

This message provides a mechanism for identifying and conveying a received GPDF to the Green Power EndPoint in the host processor.

# Usage:

# AREQ



4 MIC

Attribute	Length (byte)	Range	Description
Status	1	Any Valid	Status code, as returned by dGP stub. It can have the following values: SECURITY_SUCCESS NO_SECURITY COUNTER_FAILURE AUTH_FAILURE UNPROCESSED
RSSI	1	0x00 - 0xff	The RSSI delivered by the MAC on receipt of this frame.
Link Quality	1	0x00 - 0xff	The LQI delivered by the MAC on receipt of this frame.
C N 1	1	0x00 - 0xff	The sequence number from MAC header of the received
SeqNumber	1		MPDU.
			The source addressing mode for this primitive corresponding
SrcAddrMode			to the received MPDU. This value can take one of the following
			values:
	1	0x00 - 0x03	$0 \times 00 = \text{no}$ address (SrcPANId and SrcAddress omitted).
			$0 \times 01 = \text{reserved}.$
			$0 \times 02 = 16$ bit short address.
			$0 \times 03 = 64$ bit extended address.

SrcPANId	2	0x0000 - 0xffff	The 16-bit PAN identifier of the GPD entity from which the ASDU was received.
SrcAddress	8	As specified by the SrcAddrMode parameter	The device address of the GPD entity from which the ASDU was received. Always sent as uint64.
frameType	1	0x00, 0x01	The number of octets in the received GP MPDU.
appID	1	0x00, 0x02	Application ID of the GPD entity from which the ASDU was received.
GPDFSecLvl	1	0x00, 0x02 - 0x03	The security level, corresponding to the received MPDU.
GPDFKeyType	1	0x00 - 0x01	The security key type, corresponding to the received MPDU.
Auto Commissioning	1	0x00, 0x01	Auto commissioning value received from GPD.
RxAfterTx	1	0x00, 0x01	If the value of this field is $0x01$ , then it indicates that the GPD will enter the receive mode.
SrcId	4	0x00000001 - 0xffffffe	The identifier of the GPD entity from which the ASDU was received if Application $ID = 0b000$ .
EndPoint	1	0x00 - 0xf0, 0xff	The identifier of the GPD endpoint used in combination with the GPD IEEE address if ApplicationID = 0b010. If ApplicationID = 0b000 this parameter is ignored.
GPDSecFrame Counter	4	Any valid	The security frame counter value to be used for GPDF security processing.
GPDCmdID	1	0x00- 0xff	The identifier of the command, within the GP specification, which defines the application semantics of the ASDU.
GPDasduLength	1	0x00 - (aMaxMACFrameSi ze - 9)	The number of octets in the transmitted GPD ASDU.
GPDasdu	GPD ASU Length	-	The sequence of octets forming the transmitted GPD ASDU.
MIC	4	Any valid	The sequence of octets forming the MIC for the received GPD MPDU.