ZigBee Document 064321r09

ZigBee Stack Profile: Platform restrictions for compliant platform testing and interoperability

Revision 09

January 23. 2008

Sponsored by:
ZigBee Alliance

Accepted for release by:
This document has not yet been accepted for release by the ZigBee Alliance Board of Directors.

Abstract:
This document defines the ZigBee stack profile as applied to the ZigBee Specification r17.

Keywords:
ZigBee, Stack profile, Architecture.

Elements of ZigBee Alliance specifications may be subject to third party intellectual property rights, including without limitation, patent, copyright or trademark rights (such a third party may or may not be a member of ZigBee). ZigBee is not responsible and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

This document and the information contained herein are provided on an "AS IS" basis and ZigBee DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO (A) ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OF THIRD PARTIES (INCLUDING WITHOUT LIMITATION ANY INTELLECTUAL PROPERTY RIGHTS INCLUDING PATENT, COPYRIGHT OR TRADEMARK RIGHTS) OR (B) ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT. IN NO EVENT WILL ZIGBEE BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, IN CONTRACT OR IN TORT, IN CONNECTION WITH THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. All Company, brand and product names may be trademarks that are the sole property of their respective owners.

The above notice and this paragraph must be included on all copies of this document that are made.

ZigBee Alliance, Inc.
2400 Camino Ramon, Suite 375
San Ramon, CA 94583, USA

Contact information

Much of the information in this document is preliminary and subject to change. Members of the ZigBee Core Stack Working Group are encouraged to review and provide inputs for this proposal. For document status updates, please contact:

Don Sturek,
Texas Instruments,
1455 Frazee Road, Suite 800
San Diego, CA 92108
E-Mail: dsturek@ti.com
Phone: +1-619-497-3814
Fax: +1-619-497-3840

You can also submit comments using the ZigBee Alliance reflector. Its web site address is:

www.zigbee.org

The information on this page should be removed when this document is accepted.

Participants

The following is a list of those who were members of the ZigBee Alliance Core Stack Working Group leadership when this document was released:

Skip Ashton: *Chair*

Open: *Vice Chair*

When the document was released, the ZigBee Stack Profile Task Group was composed of the following members:

Zachary Smith: *Chair*

The editing team was composed of the following members:

Zachary Smith

Don Sturek

Christopher Leidigh

Table of Contents

List of Figures

List of Tables

Change history

Table 1 shows the change history for this specification.

Table 1 – Document revision change history

Revision	Description
00	Original version derived from document 064023r03, the ZigBee stack profile) and references [R1]… [R6]. Includes updated terminology, e.g. ZigBee/ZigBee Pro vs. HC/CII. Also includes results of comment resolution for TAG LB9.
01	Removed items RF3 and S5 from MAC PICS table in response to review comments. Also, cleaned up document header format.
02	Addressed CCB items #589, #586, #593, #596
03	Spurious upload?
04	Fixed ALF100 to reflect mandatory status of group addressing. Addressed CCB items #608, #625
05	Added changes for CCB items from Oct. ’06 test event – 666, 671, 675, 676 + related items 647 and 641, and editorial 646.
06	Changed to reflect document #053474r16 and the associated PICS – 04300r06, 04317r04 and 064147r05.
07	Modified to include NWK Group ID Table. Fixed NLF4 based on review comment. Added description column from PICS.
08	Added Fragmentation and Frequency Agility features into the ZigBee-2007 stack profile
09	Comment resolution from TAG LB16. Comment resolution database is 075159r02

1 Introduction

1.1 Scope

This document covers the Q4 2007 release of the ZigBee specification, which allows for networks of modest size, a fair degree of autonomous self-configuration on the part of network devices, and a simple security model. It is intended to support application profiles targeted to home control and monitoring, SOHO applications and other lightweight applications for ZigBee technology that do not require low-power routers.

The ZigBee specification has a number of options, which, if exercised in different ways by different vendors, will hamper both compliance testing activities and future product interoperability. This document, which is, for the most part, a set of restrictions on the Protocol Implementation Conformance Statement (PICS) documents corresponding to the three main sub-clauses of the specification, further restricts those options so as to promote interoperability and testability.

1.2 Purpose

This document defines the knobs settings, functional description and PICS for devices conforming to this stack profile, and is intended as the foundation for the platform compliance test plan that stack providers must pass in order to certify their products as ZigBee compliant.

2 References

The following standards and specifications contain provisions, which through reference in this document constitute provisions of this specification. All the standards and specifications listed are normative references. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this specification are encouraged to investigate the possibility of applying the most recent editions of the standards and specifications indicated below.

2.1 ZigBee Alliance documents

[R1] ZigBee document 053474r17, ZigBee specification release 17, ZigBee Technical Steering Committee

[R2] ZigBee 04140r05, ZigBee Protocol Stack Settable Values (knobs) release 05, ZigBee Architecture Working Group

[R3] ZigBee document 05319r01, ZigBee IEEE 802.15.4 PHY & MAC Layer Test Specification release r01, ZigBee Application Working Group

[R4] ZigBee document 04300r08, ZigBee Network Layer PICS release 08, ZigBee Network Layer Working Group

[R5] ZigBee document 04317r04, ZigBee Security Layer PICS release 04, ZigBee Security Working Group

[R6] ZigBee document 064147r07, ZigBee Application Layer PICS, release 07, ZigBee Application Working Group

[R7] ZigBee document 075098r01, Frequency Agility Full Text, ZigBee Application Working Group

2.2 IEEE documents

[R8] IEEE Standards 802, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), IEEE, April 2003.

3 Definitions

NWK Channel Manager A device on each PAN responsible for resolving PAN ID conflicts and processing frequency agility reports.[1]

Stack profile A collection of parameter values and configuration settings, collectively and loosely referred to as “knobs” in [R2], that determine the specific performance of a ZigBee stack variant and govern interoperability between stacks provided by different vendors.

Trust Center The device trusted by devices within a ZigBee network to distribute keys for the purpose of network and end-to-end application configuration management.[2]

ZigBee coordinator An IEEE 802.15.4-2003 PAN coordinator operating in a ZigBee network.

ZigBee end device An IEEE 802.15.4-2003 RFD or FFD participating in a ZigBee network, which is neither the ZigBee coordinator nor a ZigBee router.

ZigBee router An IEEE 802.15.4-2003 FFD participating in a ZigBee network, which is not the ZigBee coordinator but may act as an IEEE 802.15.4-2003 coordinator within its personal operating space, that is capable of routing messages between devices and supporting associations.

[1] LB #053

[2] LB #051

4 Acronyms and abbreviations

AODV	Ad-Hoc On-Demand Distance Vector
PICS	Protocol Implementation Conformance Statement

5 General description

This document is the stack profile specification for the ZigBee stack profile.

The sections in this document are:

- Knob settings – details of values to be used for parameters specified in the ZigBee specification for tuning the operation of the ZigBee stack, including network, application and security settings.
- Functional description – further operational restrictions to be applied to all devices in this stack profile where various approaches are otherwise supported by the ZigBee specification.
- Protocol implementation conformance statement (PICS) – a formal definition of functionality to be implemented in these devices.

These requirements aim to allow a designer to make necessary assumptions about what settings, features and safeguards will be in place in the networks in which a device will be deployed.

6 Knob settings

6.1 Introduction

This section specifies values for parameters specified in the ZigBee specification for tuning the operation of the ZigBee stack.

6.2 Network settings

The network settings for the ZigBee stack profile are, for the most part, described in the restricted PICS captured in Table 6. Those setting not covered by the PICS are listed in Table 2.

Table 2 – Network settings for this stack profile

Parameter Name	Setting	Comments
nwkTransactionPersistenceTime	0x01f4	Note that this value essentially “covers” the MAC attribute of the same name. Note also that, while [R1] implies that this quantity has meaning only in beacon-enabled networks, it may actually be used in beaconless networks as well and, in that case, is a multiplier for *aBaseSuperframeDuration* The value here yields a persistence time of 7.68 seconds using the 2.4Ghz symbol rate from [R8].

6.3 Application settings

The application settings for the ZigBee stack profile are, for the most part, described in the restricted PICS captured in Table 8. Those setting not covered by the PICS are listed in Table 3.

Table 3 – Application settings for this stack profile

Parameter Name	Setting	Comments
Number of active endpoints per sleeping ZigBee end device (maximum)	1	Note that this restriction only applies to sleeping end devices that make use of the Network Discovery Cache service provided by their parent router or ZigBee coordinator.
Config_NWK_Leave_removeChildren	FALSE	

7 Functional description

For the most part, the functioning of ZigBee with respect to the NWK layer, the APS layer and the ZDO is described in [R1]. However, the configuration details and operational requirements for devices operating under the ZigBee stack profile lead to some special functional considerations, which are detailed here.

7.1 Device roles

The basic roles performed by ZigBee devices in ZigBee networks are determined by their device type:

- The **ZigBee coordinator** initiates network formation, choosing the network channel, PAN ID and extended PAN ID in the process, and thereafter should act as a ZigBee router. It may[3] also perform the role of trust center. With respect to binding, the ZigBee coordinator is expected to handle end device bind request on behalf of all end devices in the network but is not expected to be a global binding repository for the network.

- **ZigBee routers** in ZigBee networks may accept up to 20 children of which 6 may be routers and the rest must be end devices, at least from a functional perspective. ZigBee routers are called upon to relay traffic on behalf of other devices in the network and, in particular, are required to act as routing agents on behalf of their end device children, which will typically not have the neighbor tables, routing tables, route discovery tables or broadcast transaction tables required to perform routing. [4]

- **ZigBee end devices** are joined to and managed by ZigBee routers or the ZigBee coordinator. Because ZigBee networks are beaconless, there is no built-in synchronization mechanism between sleeping end devices and their router parents. End devices are free to set their own duty cycles within the broad polling limits defined by this stack profile.

Under the ZigBee stack profile, all devices are expected to manage their own binding tables if they use binding tables.

7.1.1 Forward Compatibility

Devices implementing the ZigBee stack profile will advertise a stack profile identifier of 1 in their beacon payloads as stated below in the additional restrictions for PICS item NLF4. In general, it is expected that such devices will seek out and join networks in which the ZigBee coordinator and all ZigBee routers implement the ZigBee stack profile and advertise this fact by placing a stack profile identifier of 1 in their beacon payloads. However, for purposes of forward compatibility, a device that implements the ZigBee stack profile may also join networks that implement other stack profiles and advertise other stack profile identifiers in their beacon payloads as long as they are end devices or, if they are ZigBee routers or ZigBee coordinator-capable devices, they join the network as end devices and behave strictly as end devices, i.e. by not accepting beacon requests or allowing other devices to join the network, not participating in any form of routing etc. ZigBee devices should not join networks with a stack profile of 0x00 (network specific).[5]

[3] LB #024
[4] LB #026
[5] LB #001

7.1.2 Binding tables

Centralized binding and indirect addressing are disallowed in the ZigBee stack profile. If binding tables are used, they are located on the source device. While binding is optional, devices that choose to use binding tables should allocate enough binding table entries to handle their own communications needs. This suggests that binding table size be flexible enough that it can be set, at least at compile time, with some awareness of the actual intended usage of the device.

7.1.3 Trust center

The trust center function maintains and controls the security policies of the network. It is responsible for key deployment, trust relationships and network authorization. The trust center in the ZigBee stack profile operates in the residential mode.

7.1.4 Non-trust center installation tool

No installation tools are mandated under the ZigBee stack profile although application developers may supply them as they deem necessary.

7.2 Battery powered devices

ZigBee networks may, of course, contain battery-powered devices. Unless the network is to be very short-lived, however, battery-powered devices should not act as ZigBee routers under the ZigBee stack profile since ZigBee routers are required to have their receivers enabled whenever they are not transmitting, and while there is any possibility that they may be asked to relay traffic on behalf of other devices in the network. Thus, for most ZigBee networks, battery-powered devices should be ZigBee end devices and should be on or awake for only a fraction of their operating lives.

As mentioned above, ZigBee networks are beaconless networks and, in the absence of an explicit mechanism for synchronization and indirect transmission, sleeping devices must set their own duty cycles and use polling, under ZDO control, if they expect to receive frames that are directed to them when they are asleep. The stack profile provides that parent devices, i.e. Zigbee routers and the ZigBee coordinator, should hold frames for 7.5 seconds on behalf of sleeping end devices and this is also, roughly speaking, the maximum polling rate prescribed here.

7.3 Mains powered devices

It is assumed that for most ZigBee networks, the ZigBee coordinator and ZigBee routers will be mains-powered and always on in order to properly perform their required roles with respect to the operation of the network. Because hierarchical routing may be used in ZigBee networks, the ZigBee coordinator has a central role in routing and should be both present and operating as a router in the network.[6]

7.4 Considerations for devices without persistent storage

The ZigBee stack profile provides minimal support for devices without persistent storage. Devices are expected to remember information between unintentional restarts and power failures. At a minimum the PAN ID, EPAN, ID and short address and channel should be saved to insure proper operation through reboots or power cycles.

[6] LB #0033

7.5 Address Reuse

Network addresses under the ZigBee stack profile are assigned using a distributed tree-structured scheme. Assigning an address to a router presumes that the router will manage a block of addresses with the given address as a root address.[7] In view of this, the address of a ZigBee router that has been removed from the network should not be reassigned to another device that joins later except in the case where a ZigBee router fails authentication on joining and is removed from the network before invoking NLME-START-ROUTER.request, since there is no way for the device doing the reassignment to know how routers have assigned and managed addresses further down the tree.

The addresses of ZigBee end devices that have similarly failed authentication may be reused. The addresses of ZigBee end devices that are known to have been removed forever from the network may also reused but the implementer is warned that, if another device on the network is not informed of the replacement, the new device may receive application frames that are intended for the device it is replacing.

7.6 Additional Features for ZigBee-2007

The ZigBee-2007 stack profile employs 2 additional features beyond the feature-set for ZigBee-2006:

- Fragmentation ([R1], Section 2.2.8.4.5)
- Frequency Agility ([R7])

7.6.1 Fragmentation

Fragmentation is an optional feature both for client and server within the ZigBee-2007 stack profile. Application profiles shall indicate whether the feature is used and for which clusters. Clients and servers employing fragmentation shall agree on employment of the feature based on their deployment of a specific application profile employing a particular set of clusters designated to use the feature.

Fragmentation within the ZigBee-2007 specification was designed to permit intervening routing devices to not need fragmentation nor know whether particular routed packets employ fragmentation. In this regard, the deployment of fragmentation within ZigBee-2007 devices does not present backward compatibility issues with ZigBee-2006 devices.

7.6.2 Frequency Agility

Frequency agility is a mandatory feature for the device designated as the NWK Channel Manager (pointed to by the NWK IB value nwkChannelManager) as well as other ZigBee-2007 router devices. Since frequency agility was not a feature deployed in ZigBee-2006, here are the requirements for deployment of this feature in ZigBee-2007:

1) ZigBee-2006 and ZigBee-2007 end devices shall not need to implement any additional features. There are existing provisions for an end device in both the 2006 and 2007 versions of the specification to locate its PAN or parent (orphan scan, NWK rejoin, etc.)

[7] LB #036

2) ZigBee-2006 routers shall interoperate in a network with ZigBee-2007 devices including those deploying Frequency Agility. It shall be the responsibility of the ZigBee-2007 NWK Channel Manager to identify the ZigBee-2006 routers in their PAN and ensure they are transitioned to the new channel in the event of a channel change. The NWK Channel Manager is not addressed in the ZigBee specification ([R1]) or the Frequency Agility text ([R7]) in anything but general detail (much like the Trust Center) so details are left to the implementer. The following generally describes the responsibilities of the NWK Channel Manager in a network with both ZigBee-2006 and ZigBee-2007 devices:

   a. Determine the topology of the network and the identity of router devices in the topology. The IEEE_addr_req and NWK_addr_req ZDO commands (extended versions) can be used.

   b. Determine the identity of ZigBee-2006 router devices. The Mgmt_NWK_Update_req ZDO command (mandatory in ZigBee-2007 and not defined in ZigBee-2006) can be used.

   c. ZigBee-2006 routers must be managed separately by the NWK Channel Manager on a channel change event. Since the ZigBee-2006 routers do not support the Mgmt_NWK_update-req ZDO command, the NWK Channel Manager must employ either the leave command or cluster library commands such as Restart (if supported) to effect the channel change on the ZigBee-2006 routers.

   d. A frequency agility enabled network needs a NWK Channel Manager if it is being upgraded from ZigBee-2006. The NWK Channel Manager shall be deployed on a ZigBee-2007 device to enable a channel change if network conditions warrant.

3) A Stack version number on all devices that enables software to determine the functionality of a device.

8 Protocol implementation conformance statement (PICS) proforma

8.1 Abbreviations and special symbols

Notations for requirement status:

M	Mandatory
O	Optional
O.n	Optional, but support of at least one of the group of options labeled O.n is required.
N/A	Not applicable
X	Prohibited

“item”: Conditional, status dependent upon the support marked for the “item”.

For example, FDT1: O.1 indicates that the status is optional but at least one of the features described in FDT1 and FDT2 is required to be implemented, if this implementation is to follow the standard of which this PICS Proforma is a part.

Table 4 - Functional device types

Item number	Item description	Reference	Stack Profile Support	Support
FDT1	Is this device capable of acting as a ZigBee coordinator?	[R1]/1.4	O.1	
FDT2	Is this device capable of acting as a ZigBee router?	[R1]/ 1.4	O.1	
FDT3	Is this a ZigBee end device?	[R1]/ 1.4	O.1	

O^1: one option must be selected. [8]

[8] LB #0002

8.2 IEEE 802.15.4 PICS

The restricted IEEE 802.15.4 PICS items for the ZigBee stack profile are listed in Table 5.

Table 5 – IEEE 802.15.4 PICS for this stack profile

Item number [R2]	Item Description	Status	Additional Constraints	Support
JN1	The device joins a network by scanning and then associating.	FDT1:X FDT2:M FDT3:M[9]		
JN2	The device joins a network by using an orphan scan.	X	Direct join is disallowed.	
CA1	A super-frame structure is supported.	X		
CA2	Un-slotted CSMA-CA is supported.	M	All devices shall set their MIB values as follows: *macBeaconOrder* = 0x0f, *macSuperframeOrder* = 0x0f.	
CA3	Slotted CSMA-CA is supported.	X		
CA4	Super-frame timing is supported.	X		
S1	The device can perform some form of channel scan. Operations include: Scanning mechanism [MLME-SCAN.request primitive] [MLME-SCAN.confirm primitive]	M	All devices shall be able to perform at least an active scan.	

[9] LB #061

Item number [R2]	Item Description	Status	Additional Constraints	Support
S6	The server can perform orphan scan processing. Operations include: [MLME-ORPHAN.indicate primitive] [MLME-ORPHAN.response primitive] Reception and processing of the orphan notify command. Transmission of the coordinator realignment command.	FDT1: M FDT2: M		
A1	Association is supported (*server*).	FDT1: M FDT2: M		
A2	Association is supported (*client*).	JN1: M		
A3	The server can process association requests. Operations include: [MLME-ASSOCIATE.indicate primitive] [MLME-ASSOCIATE.response primitive] Reception and processing of the association request command. Transmission of the association response command.	FDT1: M FDT2: M		

Item number [R2]	Item Description	Status	Additional Constraints	Support
A4	The client can perform association. Operations include: [MLME-ASSOCIATE.request primitive] [MLME-ASSOCIATE.confirm primitive] Transmission of the association request command. Reception and processing of the association response command.	JN1: M		
D2	The client can react to a disassociation from the server. Operations include: [MLME-DISASSOCIATE.indicate primitive] Reception and processing of the disassociation notify command.	FDT2: O FDT3: O		
D3	The server can react to a disassociation from a client device. Operations include: [MLME-DISASSOCIATE.indicate primitive] Reception and processing of the disassociation notify command.	FDT1: O FDT2: O		
T1	Frame transmission is supported. Operations include: Frame construction [MCPS-DATA.request primitive] [MCPS-DATA.confirm primitive] Transmission of data frames.	M		

Item number [R2]	Item Description	Status	Additional Constraints	Support
T2	Implicit (command frame) transmission confirmation is supported. Operations include: [MLME-COMM-STATUS.indication primitive]	M		
R1	Frame reception is supported. Operations include: Data frame de-construction [MCPS-DATA.indication primitive] Reception of data frames.	M		
R3	Filtering and rejection is supported.	M		
TH1	Transaction handling is supported (*server*).	FDT1: M FDT2: M	The server shall be able to handle at least one transaction.	
TH2	Transaction handling is supported (*client*).	FDT3: M		
TH3	The server can manage transactions to its devices. Operations include: Transaction queuing [MCPS-PURGE.request primitive] [MCPS-PURGE.confirm primitive] Reception and processing of the data request command.	FDT1: M FDT2: M		
TH5	The client can poll for data. Operations include: [MLME-POLL.request primitive] [MLME-POLL.confirm primitive] Transmission of the data request command.	FDT3: M		
AS1	The acknowledgement service is supported.	M		

Item number [R2]	Item Description	Status	Additional Constraints	Support
MM1	MIB management is supported. Operations include: MIB attribute storage	M		
MM2	The device supports the reading of MIB attributes. Operations include: [MLME-GET.request primitive] [MLME-GET.confirm primitive]	M		
MM3	The device supports the writing of MIB attributes. Operations include: MIB attribute verification [MLME-SET.request primitive] [MLME-SET.confirm primitive]	M		
DR1	The device is able to reset. Operations include: [MLME-RESET.request primitive] [MLME-RESET.confirm primitive]	M		

8.3 Network layer PICS

The restricted network PICS items for the ZigBee stack profile are listed in Table 6. For the general PICS, including a description of each PICS item, see [R4].

Table 6 – Network PICS for this stack profile

Item number [R4]	Item Description	Status	Additional Constraints	Support
NLF4	Does the network layer support formation of ZigBee networks?	FDT1:M, FDT2:X, FDT3, X	Devices using the ZigBee stack profile must set: Stack profile = 1	

Item number [R4]	Item Description	Status	Additional Constraints	Support
			nwkcProtocolVersion = 2 *nwkSecurityLevel* = 5 and must advertise these values in their beacon payload in response to MAC beacon requests during network formation.	
NLF72	Can the network layer be directed by the next higher layer to change the operating channel of the network of which it is currently a part?	FDT1:M, FDT2:M, FDT3:M[10]		
NLF9	Does the network layer employ the Distributed Address Mechanism to generate a unique network address to assign to a joining device?	FDT1:M, FDT2:M, FDT:N/A	The ZigBee stack profile always employs the distributed addressing scheme with: *nwkMaxDepth* = 5 *nwkMaxChildren* = 20 *nwkMaxRouters* = 6	
NLF90	Does the network layer employ the Stochastic Addressing Scheme to generate a unique network address to assign to a joining or rejoining device?	FDT1:X, FDT2:X, FDT3:N/A		
NLF10	Can the next higher layer request that a particular device be “pre-joined” to it using the DIRECT-JOIN procedure?	X	This service is useful for testing and may be allowed as a part of test procedures at the option of the stack developer.	
NLF11	Can the device make a request to leave the network?	FDT1:X, FDT2:M, FDT3:M[11]		
NLF12	Can the device make a request that one of its child devices leave the network?	FDT1:M, FDT2:M, FDT3: N/A		

[10] LB #062

[11] LB #006

Item number [R4]	Item Description	Status	Additional Constraints	Support
NLF14	Does the device support changing of the ZigBee coordinator configuration in an operating network?	FDT1:M, FDT2:X, FDT3:X		
NLF15	Does the device support changing of the ZigBee router configuration in an operating network?	FDT1:X, FDT2:M, FDT3:X		
NLF17	Does the network layer allow the next higher layer to synchronize with or extract data from the device's ZigBee coordinator or router?	FDT1:X, FDT2:O, FDT3:M	Recommended polling rates for end devices using this stack profile: Maximum: once per 7.5s Minimum: once per hour Note that these values represent the (rather loose) recommended boundaries on polling rate for normal operation only.[12] Additionally, the polling rate established to meet this requirement should have a maximum value less than *nwkTransactionPersistenceTime* to ensure that child devices can poll frequently enough to retrieve messages prior to expiration in the indirect message queue of their parent.	
NLF112	Does the network layer support Route Discovery requests with DstAddrMode of 0x00 in support of Many-to-One discovery?	X		

[12] The desired polling rate during commissioning and maintenance may be different. Also, it is assumed that each device will have its own reasons for waking and sleeping based on application considerations, e.g. battery-powered alarm devices in security systems, and that these operational considerations take precedence over the polling boundaries described here. Profile designers wishing to use higher or lower polling rates should justify those rates, both to themselves and to the reviewers of the profile, in terms of network density and loading, security, maintenance, and other operational factors.

Item number [R4]	Item Description	Status	Additional Constraints	Support
NLF113	Does the network layer support Route Discovery requests with DstAddrMode of 0x01 in support of Multicast Group Discovery?	X		
NLF115	Does the network layer employ tree routing?	M	Devices using the ZigBee stack profile must set: *nwkUseTreeRouting* = TRUE	
NLF21	Does the network layer calculate routing cost based on probability of reception?	FDT1:M, FDT2:M, FDT3:N/A		
NLF22	Does the network layer maintain a routing table and route discovery table?	FDT1:M, FDT2:M, FDT3:X	ZigBee coordinators and ZigBee routers shall maintain a routing table and a route discovery table as follows: Routing table (minimum): 8 entries Route discovery table (minimum): 4 entries	
NLF220	Does the network layer maintain a route record table?	X		
NLF221	Does the network layer maintain a multicast group ID table?	X	ZigBee coordinators and ZigBee routers that use this stack profile shall set *nwkUseMulticast* to FALSE:	
NLF24	Does the device implement beacon collision-avoidance measures?	N/A		
NLF26	Does the network layer assume that links are symmetrical and establish forward and reverse routes at the same time?	X	Devices using the ZigBee stack profile must set: *nwkSymLink* = FALSE	
NLF27	Does the network layer maintain a neighbor table or	M	ZigBee coordinators and ZigBee routers shall	

[13] LB #047

Item number [R4]	Item Description	Status	Additional Constraints	Support
	tables in order to store information about nearby devices?		maintain a neighbor table or tables as follows: ZigBee coordinator (minimum): 24 entries[13] ZigBee router (minimum): 25 entries ZigBee end device (minimum): 1 entry	
NLF29	Does the network layer buffer data frames on behalf of end devices that are its children?	FDT1:M, FDT2:M, FDT3:X	Devices using the ZigBee stack profile must set: Number of frames buffered on behalf of sleeping end devices (minimum): 1 Note that this means 1 frame TOTAL not 1 frame for each end device. In other words, it is up to the implementer to put in some buffering but routers should not be overburdened with, possibly unnecessary, buffering.	

NLF30	Is the device capable of participating in a beacon-oriented network?	X	On invocation of the NLME-NETWORK-FORMATION.request or NLME-START-ROUTER.request primitives, devices using the ZigBee stack profile must employ:
			BeaconOrder = 0x0f
			SuperframeOrder = 0x0f	

NLF31	Does the network layer support the detection of address conflicts?	X		
NLF32	Does the network layer support resolving address conflicts?	X		
NLF33	Does the network layer support the detection of	FDT1:M, FDT2:X,	Only the ZigBee Coordinator detects	

Item number [R4]	Item Description	Status	Additional Constraints	Support
	PAN ID conflicts?	FDT3:X	PANID conflicts in ZigBee networks and only at network startup time.	
NLF34	Does the device support resolving PAN ID conflicts?	FDT1:M, FDT2:X, FDT3:X	Only the ZigBee Coordinator detects PANID conflicts in ZigBee networks and only at network startup time. (see [R1], sub-clause 3.2.2.3.3)	
NDF4	Does the device support relaying of broadcast network data frames?	FDT1:M, FDT2:M, FDT3:X	Devices using the ZigBee stack profile must set: Broadcast Transaction Table size: 9 (minimum) *nwkBroadcastDeliveryTime* = 3 *nwkPassiveAckTimeout* = 0.5 (maximum) *nwkMaxBroadcastRetries* = 2	
NDF100	Does the device support relaying of multicast network data frames?	X		
NDF101	Does the device support the relaying of source routed network data frames?	X		
NCF100	Does the device support the origination of leave command frames?	M		
NCF103	Does the device support the origination of route record command frames?	X		
NCF104	Does the device support the receipt of route record command frames?	X		
NCF105	Does the device support the relaying of route record command frames?	X		
NCF110	Does the device support the generation of a network	X		

Item number [R4]	Item Description	Status	Additional Constraints	Support
	report command frame.			
NCF111	Does the device support the reception of a network report command frame	X		
NCF112	Does the device support the generation of a network update command frame.	X		
NCF113	Does the device support the reception of a network update command frame	X		
NCF114	Does the device support the generation of a link status command frame.	X		
NCF115	Does the device support the reception of a link status command frame.	X		

8.4 Security PICS

The security PICS for the ZigBee stack profile are listed in Table 7.

Table 7 – Security PICS for this stack profile

Item number [R5]	Item Description	Status	Additional Constraints	Support
SR1	Is this device capable of acting in the role of a trust center?	FDT1:M, FDT2:O[14], FDT3:X		
TCC1	Is this device capable of acting as a ZigBee trust center in high security mode?	X		
TCC2	Is this device capable of acting as a ZigBee trust center in standard mode?	SR1:M		

[14] LB #063

Item number [R5]	Item Description	Status	Additional Constraints	Support
MOO1	Is this device capable of operating in a network secured with a trust center running in high security mode?	X		
MOO2	Is this device capable of operating in a network secured with a trust center running in standard mode?	M		
SL5	Is this device capable of supporting security level 0x05?	M		
NLS5	Does the device support the ability to manage two network keys and corresponding outgoing frame counter?	FDT1: M, FDT2: M, FDT3: O	ZigBee routers and coordinators shall maintain at least 2 NWK keys with the full complement of incoming and outgoing frame counters.	
NLS6, NLS7	Does the device support at least one frame counter for incoming NWK layer frames for each potential source of incoming frames (e.g., a coordinator or router should support the same number of counters per network key as the maximum number of neighbor table entries and an end device should support one counter per network key)?	M	Devices using this stack profile shall, for purposes of NWK security, store a frame counter for every neighbor, i.e. device listed in their neighbor table, from which they expect to receive traffic. See NLF27 in Table 6 for neighbor table sizes.	
NLS9	Does the device support the ability to secure all incoming and outgoing NWK frames (i.e., the *nwkSecureAllFrames* attribute of the NIB)?	M		

Item number [R5]	Item Description	Status	Additional Constraints	Support
ASLS4	Does the device support the ability to manage trust center master keys?	X	Devices using this stack profile shall not employ a KeyType parameter value of 0x00 when invoking the APSME security primitives. Nor shall they respond to or process APS transport key or request key command frames with a key type field value of 0x00[15].	
ASLS5[16]	Does the device support the ability to manage application [17]master keys?	O	Devices using this stack profile may employ a KeyType parameter value of 0x02 when invoking the APSME security primitives. Agreement on the use of KeyType parameter value of 0x02 shall be established by the Application Profiles deployed on the devices employing the security primitives.[18]	
ASLS11	Does the device support the origination of update-device commands?	FDT1:M FDT2:M, FDT3:X		
ASLS14	Does the device support the receipt of remove-device commands?	FDT1:M, FDT2:M, FDT3:X		
ALS1	Is this device capable of learning and maintaining knowledge of its trust center using the *apsTrustCenterAddress* attribute in the AIB?	O	Trust Center must initially reside on the ZigBee coordinator but may, under application control, move to any router on the PAN as long as all devices in the PAN have their apsTrustCenterAddress attribute updated appropriately by the application.[19]	
ALS2	Is this device capable of following the “joining a secure network procedure” in the role of a router?	FDT1:M, FDT2:M, FDT3:X		

[15] LB #065
[16] LB #065
[17] LB #065
[18] LB #065
[19] LB #063

Item number [R5]	Item Description	Status	Additional Constraints	Support
ALS3	Is this device capable of following the “joining a secure network procedure” in the role of a joining device?	FDT1:N/A, FDT2:M, FDT3:M		
ALS4	Is this device capable of following the “authentication procedure” in the role of a trust center?	SR1:M		
ALS5	Is this device capable of following the “authentication procedure” in the role of a router?	FDT1:X, FDT2:M, FDT3:X		
ALS6	Is this device capable of following the “authentication procedure” in the role of a joining device with a preconfigured network key?	FDT1:X, FDT2:M, FDT3:M		
ALS9	Is this device capable of following the “network key update procedure” in the role of a trust center?	SR1:M		
ALS10	Is this device capable of following the “network key update procedure” in the role of a network device?	FDT1:X, FDT2:M, FDT3:M		
ALS13	Is this device capable of following the “end-to-end application key establishment procedure” in the role of a trust center?	SR1:X		
ALS16	Is this device capable of following the “network leave procedure” in the role of a trust center?	SR1:M		
ALS17	Is this device capable of following the “network leave procedure” in the role of a router?	FDT1:X, FDT2:M, FDT3:X		
ALS18	Is this device capable of following the “network leave procedure” in the role of a leaving device?	FDT1:X, FDT2:M, FDT3:M		

8.5 Application layer PICS

The application framework PICS for the ZigBee stack profile are listed in Table 8.

Table 8 – Application framework PICS for this stack profile

Item number [R6]	Item Description	Status	Additional Constraints	Support
AFF3	Does the device support the ZigBee APS command frame format?	M		
ALF200	Does the device support transmission of outgoing APS frames within APSDE with the DstAddrMode set to 0x00 (indirect)?	X		
ALF100	Does the application support sub-layer support ADD GROUP requests and confirms?	O[20]	The group table in APS, shall contain a minimum of 16 group addresses if supported.[21]	
ALF101	Does the application support the REMOVE GROUP request and confirms?	O[22]	See above	
ALF102	Does the application support REMOVE ALL GROUPS request and confirms?	O[23]	See above	
ALF300	Does the device support reception of incoming APS frames within APSDE with the DstAddrMode set to 0x00 (indirect)	X		
ADF3	Does the device support the origination of application data frames with the auxiliary APS security header?	M		
ADF4	Does the device support the receipt of application data frames with the auxiliary APS security header?	M		
ACF101	Does the device support the origination of Transport Key application command frames	SR1:M		

[20] LB #069
[21] LB #070
[22] LB #069
[23] LB #069

Item number [R6]	Item Description	Status	Additional Constraints	Support
	from the Trust Center?			
ACF102	Does the device support the origination of Remove Device application command frames from the Trust Center?	SR1:M		
ACF103	Does the device support the origination of Switch Key application command frames from the Trust Center?	SR1:M		
ACF104	Does the device support the origination of Update Device application command frames from the Trust Center?	SR1:M		
ACF2	Does the device support the receipt of application command frames at the Trust Center	SR1:M		
ACF302	Does the device support the origination of Update Device application command frames from a non-Trust Center device?	FDT1:N/A, FDT2: M, FDT2:M		
ACF303	Does the device support the origination of Request Key application command frames from a non-Trust Center device?	FDT1:N/A, FDT2: M, FDT2:M		
ACF402	Does the device support the receipt of Update Device application command frames from a non-Trust Center device?	SR1:M		
ACF500	Does the device support the origination of command frames with the auxiliary APS security header?	M		
ACF501	Does the device support the receipt of command frames with the auxiliary APS security header?	M		
AZD103	Does the device support the optional Discovery Cache	FDT1:O, FDT2:O,	The ZigBee coordinator and each ZigBee router in networks using this stack	

Item number [R6]	Item Description	Status	Additional Constraints	Support
	server service of the Device and Service Discovery Object?	FDT3:X	profile should set aside a recommended cache size of 476 bytes reflecting node descriptor, power descriptor and 1 endpoint per child with 8 clusters for each end device child.	
AZD19	Does the device support the optional Security Manager Object?	M		
AZD22	Does the device support the optional Binding Manager Object?	FDT1:M	The ZigBee coordinator must process end device bind requests and supply Bind_req commands to the source of matched clusters in the paired end device bind requests.[24]	
AZD35	Does the device support the optional NLME SYNC service of the Network Manager Object?	FDT3:M	See sub-clause 8.3 NLF17	
AZD38	Does the device support the optional Node Manager NWK Discovery server service?	FDT1:M FDT2:M		
AZD40	Does the device support the optional Node Manager LQI server service?	FDT1:M FDT2:M		
AZD42	Does the device support the optional Node Manager RTG server service?[25]	FDT1:O FDT2:O		
AZD46	Does the device support the Management Leave server service?	M[26]		
AZD48	Does the device support the optional Node Manager Direct Join server service?	X		
AZD800	Does the device support the optional Node Manager NWK Update client service?	FDT1:M, FDT2:M,		

[24] LB #067
[25] LB #072
[26] LB #073

Item number [R6]	Item Description	Status	Additional Constraints	Support
		FDT3:X		
AZD801	Does the device support the optional Node Manager NWK Update server service?	FDT1:M, FDT2:O, FDT3:X		
AZD503	Does the device support the optional NWK Indirect Poll Rate configuration attribute?	FDT3:M	See sub-clause 8.3 NLF17	
AZD700	Does the device support the permissions configuration table?	O[27]		

[27] LB #068