

1



2

3

4 **ZigBee Document 074855r05**

5 **ZigBee-PRO Stack Profile: Platform**  
6 **restrictions for compliant platform testing**  
7 **and interoperability**

8

9 **Revision 05**

10

11 January 2008

12 **Sponsored by:**  
13 ZigBee Alliance

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

16 **Abstract:**  
17 This document defines the ZigBee-PRO stack profile as applied to the ZigBee Specification r17.

18 **Keywords:**  
19 ZigBee, ZigBee-PRO, Stack profile, Architecture.

1 *Copyright © ZigBee Alliance, Inc. (2007). All rights Reserved. This information within*  
2 *this document is the property of the ZigBee Alliance and its use and disclosure are*  
3 *restricted.*  
4 *Elements of ZigBee Alliance specifications may be subject to third party intellectual*  
5 *property rights, including without limitation, patent, copyright or trademark rights (such*  
6 *a third party may or may not be a member of ZigBee). ZigBee is not responsible and*  
7 *shall not be held responsible in any manner for identifying or failing to identify any or all*  
8 *such third party intellectual property rights.*  
9 *This document and the information contained herein are provided on an “AS IS” basis*  
10 *and ZigBee DISCLAIMS ALL WARRANTIES EXPRESS OR IMPLIED, INCLUDING*  
11 *BUT NOT LIMITED TO (A) ANY WARRANTY THAT THE USE OF THE*  
12 *INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OF THIRD PARTIES*  
13 *(INCLUDING WITHOUT LIMITATION ANY INTELLECTUAL PROPERTY RIGHTS*  
14 *INCLUDING PATENT, COPYRIGHT OR TRADEMARK RIGHTS) OR (B) ANY*  
15 *IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR*  
16 *PURPOSE, TITLE OR NON-INFRINGEMENT. IN NO EVENT WILL ZIGBEE BE*  
17 *LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA,*  
18 *INTERRUPTION OF BUSINESS, OR FOR ANY OTHER DIRECT, INDIRECT, SPECIAL*  
19 *OR EXEMPLARY, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF*  
20 *ANY KIND, IN CONTRACT OR IN TORT, IN CONNECTION WITH THIS DOCUMENT*  
21 *OR THE INFORMATION CONTAINED HEREIN, EVEN IF ADVISED OF THE*  
22 *POSSIBILITY OF SUCH LOSS OR DAMAGE. All Company, brand and product names*  
23 *may be trademarks that are the sole property of their respective owners.*  
24 *The above notice and this paragraph must be included on all copies of this document that*  
25 *are made.*  
26

27 ZigBee Alliance, Inc.  
28 2400 Camino Ramon, Suite 375  
29 San Ramon, CA 94583, USA  
30

## 1 **Contact information**

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

5 Don Sturek,  
6 Texas Instruments,  
7 1455 Frazee Road, Suite 800  
8 San Diego, CA 92108  
9 E-Mail: [dsturek@ti.com](mailto:dsturek@ti.com)  
10 Phone: +1-619-497-3814  
11 Fax: +1-619-497-3840  
12  
13

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

15 [www.zigbee.org](http://www.zigbee.org)

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

## 1 **Participants**

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

4 **Don Sturek:** *Chair*

5 **Zachary Smith:** *Vice Chair*

6  
7  
8 When the document was released, the ZigBee-PRO Stack Profile Task Group was composed of the  
9 following members:

10 **Phil Rudland:** **Chair**

11 **Phil Jamieson**

12 **Zachary Smith**

13 **Don Sturek**

14  
15 The editing team was composed of the following members:

16 **Phil Rudland**

17 **Zachary Smith**

18 **Don Sturek**

19

20

21

# 1 Table of Contents

2	1	Introduction .....	1
3	1.1	Scope .....	1
4	1.2	Purpose .....	1
5	2	References .....	2
6	2.1	ZigBee Alliance documents .....	2
7	2.2	IEEE documents .....	2
8	3	Definitions .....	3
9	4	Acronyms and abbreviations .....	4
10	5	General description .....	5
11	6	Knob settings .....	6
12	6.1	Introduction .....	6
13	6.2	Network settings .....	6
14	6.3	Application settings .....	6
15	6.4	Security settings .....	7
16	7	Functional description .....	8
17	7.1	Device roles .....	8
18	7.2	Compatibility with Other Stack Profiles .....	8
19	7.3	Binding tables .....	9
20	7.4	Multicast mechanism and groups .....	9
21	7.5	Trust Center Policies and Security Settings .....	9
22	7.6	Battery powered devices .....	9
23	7.7	Mains powered devices .....	10
24	7.8	Persistent storage .....	10
25	7.9	Address Reuse .....	10
26	7.10	Duty cycle limitations and fragmentation .....	10
27	7.10.1	Vulnerability join .....	10
28	7.10.2	Pre-installation .....	10
29	7.11	Security .....	11
30	7.11.1	Security Modes within PRO Networks .....	11
31	8	Protocol implementation conformance statement (PICS) proforma .....	13
32	8.1	Abbreviations and special symbols .....	13
33	8.2	IEEE 802.15.4 PICS .....	14
34	8.3	Network layer PICS .....	15
35	8.4	Security PICS .....	20
36	8.5	Application layer PICS .....	24

37

1 **List of Figures**

1 **List of Tables**

2 Table 1 – Document revision change history .....viii  
3 Table 2 – Network settings for this stack profile..... 6  
4 Table 3 – Application settings for this stack profile..... 6  
5 Table 4 – Security settings for this stack profile ..... 7  
6 Table 5 – IEEE 802.15.4 PICS for this stack profile..... 14  
7 Table 6 – Network PICS for this stack profile ..... 15  
8 Table 7 – Security PICS for this stack profile .....20  
9 Table 8 – Application framework PICS for this stack profile .....24  
10



## 1 Change history

2 Table 1 shows the change history for this specification.

3 **Table 1 – Document revision change history**

Revision	Description
04	Merger of 053646r03 and 064321r05, plus incorporation of all comments to date.
05	Updated following revisions to referenced PICS documents, and revision to r15.
06	Removed all of the Track Changes notes (by accepting all).
074855r00	Renamed Stack Profile to ZigBee PRO and restarted numbering. Incorporated comments from initial review.
r01	Reworked security section following discussions in SWG. Made use of the service permissions table optional. Updated various minor notes elsewhere.
r02	Errata and clarifications per 074942
r03	Errata and clarifications per 075115
r04	Addressed CCBs: 859, 860, 861, 862, 863, 864, 865, 851, 847, 789, 766, 767, 768, 730 and 686
R05	Address CCBs: 884, 873, 872,

4

5

# 1 Introduction

## 2 1.1 Scope

3 This document covers the ZigBee PRO stack profile for the 2007 release of the ZigBee specification.  
4 The ZigBee PRO stack profile allows for networks of small to moderately large size, a fair degree of  
5 autonomous self-configuration on the part of the network devices, and a flexible security model. The  
6 PRO stack profile is intended to support application profiles targeted to building automation plus  
7 sensing and control in commercial, industrial and institutional environments. It can also support other  
8 lightweight applications for ZigBee technology that do not require low-power routers.

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

## 14 1.2 Purpose

15 This document defines the knobs settings, functional description and PICS for devices conforming to  
16 this stack profile, and is intended as the foundation for the platform compliance test plan that stack  
17 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 053474r16, ZigBee specification release 16, ZigBee Technical Steering Committee
- [R2] ZigBee 04140r05, ZigBee Protocol Stack Settable Values (knobs) release 05, ZigBee Architecture Working Group
- [R3] ZigBee document 04319r01, 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

### 2.2 IEEE documents

- [R7] 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.

### 1 3 Definitions

<b>Stack profile</b>	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.
<b>ZigBee coordinator</b>	An IEEE 802.15.4-2003 PAN coordinator operating in a ZigBee network.
<b>ZigBee end device</b>	An IEEE 802.15.4-2003 RFD or FFD participating in a ZigBee network, which is neither the ZigBee coordinator nor a ZigBee router.
<b>ZigBee router</b>	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.

2

## 1 **4 Acronyms and abbreviations**

AODV	Ad-Hoc On-Demand Distance Vector
FFD	IEEE 802.15.4 Full Function Device
IEEE	Institute of Electrical and Electronic Engineers
PICS	Protocol Implementation Conformance Statement
RFD	IEEE 802.15.4 Reduced Function Device

2

## 1 **5 General description**

2 This document is the stack profile specification for the ZigBee-PRO stack profile.

3 The sections in this document are:

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

11 These requirements aim to allow a designer to make necessary assumptions about what settings,  
12 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-PRO stack.

### 6.2 Network settings

The network settings for the ZigBee-PRO 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
<i>nwkTransactionPersistenceTime</i>	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 <i>aBaseSuperframeDuration</i> . The value here yields a persistence time of 7.68 seconds using the 2.4Ghz symbol rate from [R7] in a non-beaconed network.
<i>nwkReportConstantCost</i>	FALSE	The NWK layer in PRO shall always calculate routing cost on the basis of neighbor link cost and never report constant cost.

### 6.3 Application settings

The application settings for the ZigBee-PRO 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)	-	As the responsibility to arrange for caching of service discovery information lies with the end device itself, this parameter is not restricted.
Config_NWK_Leave_removeChildren	FALSE	

1 **6.4 Security settings**

2 The security settings for the ZigBee-PRO stack profile are listed in Table 4.

3 **Table 4 – Security settings for this stack profile**

Parameter Name	Setting	Comments
apsSecurityTimeoutPeriod	50ms * (2*NWK Maximum Depth) + (AES Encrypt/Decrypt times)	<p>Where AES Encrypt/Decrypt times = 200ms, and</p> <p>Where NWK Maximum Depth is assumed to be 15, meaning every device in the network can be reached in not more than 30 hops.</p> <p>ie: 1.7 seconds. Note that this timeout assumes worst case AES engine speeds and is not indicative of expected performance for most devices.</p>

4

## 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-PRO 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-PRO 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 also perform the roles of trust center and Network Channel Manager. 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** 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. Since end devices may sleep, ZigBee routers and ZigBee coordinators in their role of ZigBee routers may cache discovery information on behalf of their sleeping end-device children. A ZigBee router may perform the role of trust center and Network Channel Manager.
- **ZigBee end devices** are joined to and managed by ZigBee routers or the ZigBee coordinator. Because ZigBee-PRO 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. End devices that wish to have their discovery information cached by their parent or some other device are responsible for using the discovery cache commands to achieve this.

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

### 7.2 Compatibility with Other Stack Profiles

Devices implementing the ZigBee-PRO stack profile will advertise a stack profile identifier of 2 in their beacon payloads as stated below in the additional restrictions for PICS item NLF4. In general, such devices will seek out and join networks in which the ZigBee coordinator and all ZigBee routers implement the ZigBee-PRO stack profile and advertise this fact by placing a stack profile identifier of 2 in their beacon payloads.

In order to provide compatibility with devices implemented according to the ZigBee stack profile, ZigBee-PRO devices shall additionally be able to join networks which advertise a stack profile identifier of 1 in their beacon payloads but the device must join the ZigBee networks as end devices.

If a ZigBee PRO network is to allow ZigBee devices to join as end devices, it shall use the standard network security. If high security is used, ZigBee devices will not be able to be authenticated on the network.

### 1 **7.3 Binding tables**

2 Binding tables, if used, shall be located on the source device. While binding is optional, devices that  
3 choose to use binding tables should allocate enough binding table entries to handle their own  
4 communications needs. This suggests that binding table size should be flexible enough that it can be  
5 set, at least at compile time, with some awareness of the actual intended usage of the device.

### 6 **7.4 Multicast mechanism and groups**

7 Support for APS level multicasts is mandatory to support compatibility with ZigBee 2006 devices. The  
8 multicast groups are then established using the application level mechanisms. Support for network  
9 level multicasts is optional in this stack profile.

### 10 **7.5 Trust Center Policies and Security Settings**

11 A ZigBee PRO network shall have a trust center uniquely pointed to by each device in the network  
12 through `apsTrustCenterAddress` within each network member device. It is beyond the scope of the  
13 PRO Stack Profile to describe how this value is set or whether it is changed and the Trust Center  
14 relocated to another device during operation. The only requirement of the PRO Stack Profile is that all  
15 devices in the network point to the one unique Trust Center and that the device pointed to as the Trust  
16 Center supplies the security services described by this document.

17 The trust center dictates the security parameters of the network, such as which network key type to use,  
18 settings of the service permissions table, when, if at all, to allow devices to use unsecured association  
19 to the network, and when, if at all, to allow an application master or link key to be set up between two  
20 devices. For interoperability, there are two distinct security settings that can be used within the ZigBee  
21 PRO stack profile – a standard and a high security.

22 Networks can exist for periods without a trust center. There are some operations where it is necessary  
23 for the trust center to be operational in the network. These include initial network setup, key changes,  
24 and when joining and rejoining devices require updated keys.

25 A wide range of implementations are possible, depending on the requirements of the application. A  
26 high security trust center may allow the user to install devices “out-of-band”, keep separate link keys  
27 for different devices, optionally ignore `Mgmt_Permit_Joining_req` commands from other nodes, and  
28 configure application trust policies between devices or groups of devices, etc. A standard security trust  
29 center would not offer these advantages, but would not be required to carry the associated costs.

### 30 **7.6 Battery powered devices**

31 ZigBee-PRO networks may, of course, contain battery-powered devices. ZigBee routers are required to  
32 have their receivers enabled whenever they are not transmitting.

33 As mentioned above, ZigBee-PRO networks are beaconless networks and, in the absence of an explicit  
34 mechanism for synchronization and indirect transmission, sleeping devices must set their own duty  
35 cycles and use polling, under ZDO control, if they expect to receive frames that are directed to them  
36 when they are asleep. The stack profile provides that parent devices, i.e. ZigBee routers and the ZigBee  
37 coordinator, hold frames for 7.5 seconds on behalf of sleeping end devices and this is also, roughly  
38 speaking, the maximum polling rate prescribed here. Devices may implement a polling interval longer  
39 than 7.5 seconds, however the application will then have to handle the potential loss of messages  
40 during longer sleep cycles.

## 1 **7.7 Mains powered devices**

2 It is assumed that for most ZigBee-PRO networks, the ZigBee coordinator and ZigBee routers will be  
3 mains-powered and always on in order to properly perform their required roles with respect to the  
4 operation of the network.

## 5 **7.8 Persistent storage**

6 The ZigBee-PRO stack profile does not support devices without persistent storage. Devices have  
7 information required to be saved between unintentional restarts and power failures. See [R1] sections  
8 2.2.8 and 3.6.8 for details of persistent data in the application and NWK layers. Various security  
9 material shall additionally be stored across power failures. All attributes in sections 4.3.3 and 4.4.10  
10 shall be stored, except that it is not mandatory to store those values which can safely be recovered  
11 using other stored information, or other methods.

## 12 **7.9 Address Reuse**

13 Re-use of previously assigned network short addresses in ZigBee-PRO devices is permitted subject to  
14 execution of the address conflict procedure by the device on the re-used address.

## 15 **7.10 Duty cycle limitations and fragmentation**

16 No mandatory restrictions are defined for intermittent, low channel usage data, although developers are  
17 encouraged to minimise bandwidth usage wherever possible.

18 Large acknowledged unicast transmissions should generally use the APS fragmentation mechanism,  
19 where supported, as this handles retransmissions, duplicate rejection, flow control and congestion  
20 control automatically. Use of the fragmentation mechanism is as specified in the application profile  
21 documents.

### 22 **7.10.1 Vulnerability join**

23 Vulnerability join shall be optional for networked devices, but support for it shall be mandatory for  
24 trust centers. The default for networks is permit joining is off. Permit joining is allowed for  
25 established time periods based on application requirements and specific instructions based on the  
26 system design.

27 Devices that join but do not successfully acquire and use the relevant security keys within the specified  
28 security timeout period shall disassociate themselves from the network, and their short address may be  
29 reused.

### 30 **7.10.2 Pre-installation**

31 Pre-installation is acceptable. Pre-installed devices are not exempt from the other requirements in this  
32 document. For example, a device certified as a trust center for this stack profile shall support  
33 vulnerability installation of new devices, even if it is initially pre-installed.

## 1 7.11 Security

2 This stack profile is designed to allow the efficient deployment of low cost devices, while also  
3 supporting the security requirements of highly sensitive applications. Installation and network  
4 maintenance procedures and administration are defined with the goal of satisfying the requirements of  
5 a range of applications within a single network infrastructure.

6 To achieve this, two security modes are specified: Standard mode and High Security mode. By default  
7 all applications will use the network key for communications. However, where confidentiality from  
8 other network nodes is required an application shall be permitted to use application link keys. Where  
9 link keys are required by specific application profiles, commands not secured with a link key shall be  
10 processed according to the rules established by the application profile.

11 The trust center plays a key role in determining the security settings in use in the network, and can  
12 optionally be implemented to apply further restrictions on the network. Please see section **Error!**  
13 **Reference source not found.** for details.

14 It is recommended that the trust center change the network key if it is discovered that any device has  
15 been stolen or otherwise compromised, and in order to avoid deadlock if all frame counter records  
16 become filled up. It is an application responsibility within the Trust Center to effect the change to the  
17 network key. There is no expectation that the network key be changed when adding a new device.

18 All devices may implement a service permissions table, which they may use to determine which  
19 devices are authorized to issue which commands. Unauthorized commands should not be carried out.

20 The trust center should be implemented to make appropriate choices about when to initiate an  
21 application master/link key shared between two devices. Where restrictions between devices are  
22 required it is the responsibility of the system installer/administrator to deploy a suitably intelligent trust  
23 center and configure it to make relevant checks before initiating sharing of application link keys  
24 between two devices. For example, it might facilitate policies based on certain times, certain  
25 manufacturers or device types, or when the trust center is configured in a certain way, etc. By default a  
26 simple trust center should always allow requests for link keys.

27 Devices may perform the relevant in or out of band authentication or key exchange before acquiring or  
28 using a link key with a new target.

### 29 7.11.1 Security Modes within PRO Networks

30 The stack profile shall use two security modes: Standard mode and High Security mode.

31 With the Standard mode, network keys and application link keys are permitted for all devices. The  
32 network key type shall be the “standard” network key. It shall not be required that devices perform  
33 entity authentication with their parent on joining nor shall it be required to perform entity  
34 authentication between neighbors. If end devices wish to have a trust center link key, this should be  
35 requested using the request key command. Note that it is optional for the trust center to support link  
36 keys.

37 With the High Security mode, all three key types are permitted and shall be supported by all devices.  
38 The network key type shall be the “high security” network key. It shall be required that devices shall  
39 perform entity authentication with their parent on joining and it shall be required to perform entity  
40 authentication between neighbors. Frames from devices not in the neighbor table shall not be accepted.

41 When a “standard” type network key is in use, devices shall be permitted to update the network key  
42 when requested to do so by a command appropriately secured with the current network key. When a  
43 “high security” type of network key is in use this shall not be permitted. Additionally, in “high  
44 security”, new trust center link keys may be deployed by SKKE only, ie: they shall not be sent using  
45 key transport.

1 Bit 6 of the capabilities field (security bit) shall be used to indicate whether or not a joining (or  
2 rejoining) device supports High Security mode. It shall be set to 0 if the joining or rejoining device  
3 does not support High Security mode (i.e. supports Standard mode), and shall be set to 1 if it does  
4 support High Security mode. The trust center may optionally make use of this information as part of its  
5 policy settings, for example when determining whether or not to allow the device onto the network, or  
6 when determining whether to initiate SKKE with a new joiner or send a link key and/or network key in  
7 the clear to the new device.

8 The above specifications are as currently described in the ZigBee specification.. Standard mode and  
9 High Security mode allow implementation of two different strengths of security depending on the  
10 application requirements and the specification supports a device indicating its security capabilities as it  
11 joins the network, thus giving the Trust Center the means to be able to accept or reject the device based  
12 on its policy.

13

14

## 1 **8 Protocol implementation conformance statement (PICS)** 2 **proforma**

### 3 **8.1 Abbreviations and special symbols**

4 *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

5

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

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

## 1 8.2 IEEE 802.15.4 PICS

2 The restricted IEEE 802.15.4 PICS items for the ZigBee stack profile are listed in Table 5. For the  
3 general PICS, including a description of each PICS item, see [R3].

4 **Table 5 – IEEE 802.15.4 PICS for this stack profile**

Item number [R3]	Status	Additional Constraints	Support
JN1	FDT1:X FDT2:O FDT3:O		
JN2	FDT1:X FDT2:M FDT3:M		
CA1	X		
CA2	M	All devices shall set their MIB values as follows: <i>macBeaconOrder=0x0f, macSuperframeOrder=0x0f.</i>	
CA3	X		
CA4	X		
S1	M	All devices shall be able to perform at least an active scan.	
S2	M	The coordinator shall perform an energy detection scan on each available channel in the active channel mask before starting a network.  Network devices shall perform an energy detection scan on request from the next higher layer.	
S3	M	All devices shall perform an active scan on each available channel in the active channel mask.	
S6	FDT1:M FDT2:M	Network rejoin is the preferred mechanism for devices to use, however, orphan scan may be used and the parent devices shall support orphan scan.	
S7	FDT1: M FDT2: M		
A1	FDT1: M FDT2: M		
A2	FDT1:X FDT2:O FDT3:O		
A3	FDT1: M FDT2: M		
A4	FDT1:X FDT2:O FDT3:O		
D2	FDT2: O FDT3: O		

Item number [R3]	Status	Additional Constraints	Support
D3	FDT1: O FDT2: O		
T1	M		
T2	M		
R1	M		
R3	M		
TH1	FDT1: M FDT2: M	The server shall be able to handle at least one transaction.	
TH2	FDT3: M		
TH3	FDT1: M FDT2: M		
TH5	FDT3: M		
AS1	M		
AS2	M		
AS3	M		
AS4	M		
MM1	M		
MM2	M		
MM3	M		
MS1	X		
MS2	X		
DR1	O		

1

### 2 8.3 Network layer PICS

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

5

**Table 6 – Network PICS for this stack profile**

Item number [R4]	Status	Additional Constraints	Support
NLF4	FDT1:M, FDT2:X, FDT3, X	Devices using the ZigBee-PRO stack profile shall set:  Stack profile = 2  <i>nwkcProtocolVersion</i> = 2  and shall advertise these values in their beacon payload in response to MAC beacon requests.	

Item number [R4]	Status	Additional Constraints	Support
		Devices using the ZigBee-PRO stack profile shall also set:  <i>nwkSecurityLevel</i> = 5	
NLF60	FDT1:M FDT2:M FDT3:X	NLME-ED-SCAN is mandatory for the coordinator and all routers on a PRO network	
NLF71	FDT2:M, FDT3:M		
NLF72	M	The network layer can be directed by the next higher layer to change the operating channel of the network of which it is currently part.	
NLF9	X		
NLF90	FDT1:M, FDT2:M FDT3:X	The ZigBee-PRO stack profile employs stochastic address allocation.  The follow parameter values are defined:  <i>nwkAddrAlloc</i> = 2 <i>nwkUseTreeRouting</i> = FALSE <i>nwkMaxDepth</i> = 15  Note that <i>nwkMaxDepth</i> above is only used to compute timeouts and shall not limit the actual network radius, as this stack profile does not use tree-based addressing.  The parameter <i>nwkMaxChildren</i> is not restricted in this stack profile.	
NLF14	FDT1:M	The ZigBee coordinator shall change the logical channel and PAN ID when directed to by the Network Channel Manager.	
NLF15	FDT2:M	The ZigBee router shall change the logical channel and PAN ID when directed to by the Network Channel Manager.	
NLF17	FDT2:X 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.  Additionally, the polling rate established to meet this requirement shall have a maximum value less than	

Item number [R4]	Status	Additional Constraints	Support
		<p><i>nwkTransactionPersistenceTime</i> to ensure that child devices can poll frequently enough to retrieve messages prior to expiration in the indirect message queue of their parent.</p> <p>The polling rate established here also does not consider APS acknowledgement timeout (which is much shorter than <i>nwkTransactionPersistenceTime</i>). If APS acknowledged messages are directed to sleeping end devices, then the polling rate of those destination devices may be adjusted to occur more frequently than the APS acknowledgement timeout.</p>	
NLF18	FDT2:X		
NLF110	FDT1:M FDT2:M FDT3:X	NWK report command frame generation is mandatory for the coordinator and all routers on a PRO network	
NLF111	FDT1:M FDT2:M		
NLF112	FDT1:O FDT2:O	Initiation of a Many-to-One route discovery is optional, and should be used in cases where there are relatively few concentrators in the network. Application developers should weigh the trade-offs between Many-to-One discovery and unicast discovery before deploying.	
NLF113	FDT1:O FDT2:O FDT3:X	Initiation of route discovery commands where <i>DstAddrMode</i> is 0x01 (Multicast Group Discovery) is optional.	
NLF114	FDT1:O FDT2:O FDT3:X	<p>Initiation of route discovery commands where <i>DstAddrMode</i> is 0x02 (Unicast) is optional.</p> <p>ZigBee coordinators and ZigBee routers shall support reception and correct handling of unicast discovery commands.</p>	
NLF115	X	<p>Devices using the ZigBee-PRO stack profile shall set:</p> <p><i>nwkUseTreeRouting</i> = FALSE</p>	
NLF21	FDT1:M, FDT2:M FDT3:N/ A		
NLF22	FDT1:M FDT2:M	ZigBee coordinators and ZigBee routers shall maintain a routing table and a route discovery table as follows:	

Item number [R4]	Status	Additional Constraints	Support
	FDT3:X	<p>Routing table (minimum): 10 entries</p> <p>An aging algorithm is recommended but is beyond the scope of this specification.</p> <p>Route discovery table entries (minimum): 4 entries</p> <p>The Route discovery table entries shall be managed as described in [R1] Section 3.6.3.6.</p>	
NLF24	N/A		
NLF26	M	<p>Devices using the ZigBee-PRO stack profile shall set:</p> <p><i>nwkSymLink</i> = TRUE</p>	
NLF27	FDT1:M FDT2:M FDT3:M	<p>ZigBee coordinators and ZigBee routers shall maintain a neighbor table or tables as follows:</p> <p>ZigBee coordinator (minimum): (Number of child end devices accepted) plus 16</p> <p>ZigBee router (minimum): (Number of child end devices accepted) plus 16</p> <p>ZigBee end device: 1 (Note: End Device shall only support only a single neighbor table entry and that entry shall be for their parent)</p> <p>Where (Number of child end devices accepted) is the maximum number of end device children that a particular router or coordinator in the network is configured to accept.</p>	
NLF29	M	<p>Devices using the ZigBee-PRO stack profile shall set:</p> <p>Number of frames buffered on behalf of sleeping end devices (minimum): 1</p> <p>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.</p>	
NLF30	X	<p>On invocation of the NLME-NETWORK-FORMATION.request or NLME-START-ROUTER.request primitives, devices using the ZigBee-PRO stack profile shall employ:</p> <p>BeaconOrder = 0x0f</p> <p>SuperframeOrder = 0x0f</p>	

Item number [R4]	Status	Additional Constraints	Support
NLF31	FDT1:M FDT2:M FDT3:X	Address conflict detection is mandatory for this stack profile ( <code>nwkUniqueAddr = FALSE</code> ). The coordinator and all routers shall implement the Address Conflict procedure in [R1] Section 3.6.1.9.	
NLF32	FDT1:M FDT2:M FDT3:X	Address conflict resolution is mandatory for this stack profile ( <code>nwkUniqueAddr = FALSE</code> ). The coordinator and all routers shall implement the Address Conflict procedure in [R1] Section 3.6.1.9.	
NLF33 NLF34	FDT1:M FDT2:M FDT3:X	PAN ID conflict resolution is mandatory for the coordinator and routers. Notification of a PAN ID conflict via the NWK Status command frame directed to the <code>nwkManagerAddr</code> is mandatory for all routers and the coordinator. The <code>nwkManagerAddr</code> is required to process all NWK Status command frames directed to it by the coordinator and routers.	
NDF4	FDT1:M FDT2:M FDT3:X	Devices using the ZigBee-PRO stack profile shall set:  Broadcast Transaction Table size: 9 (minimum)  <i>nwkBroadcastDeliveryTime</i> = 9 <sup>1</sup>  <i>nwkPassiveAckTimeout</i> = 0.5 (maximum)  <i>nwkMaxBroadcastRetries</i> = 2  Application designers should take care to use multicast and broadcast sparingly due to the limitations of the broadcast bandwidth of a network.	
NDF100	FDT1:M FDT2:M FDT3:N/ A	The coordinator and all routers in a PRO network shall be able to relay member mode <sup>2</sup> multicast network data frames.	
NDF101	FDT1:M FDT2:M FDT3:N/ A		
NCF1	FDT1:M FDT2:M		
NCF5	FDT1:M FDT2:M		

<sup>1</sup> CCB 884<sup>2</sup> CCB 872

Item number [R4]	Status	Additional Constraints	Support
NCF105	FDT1:M FDT2:M		
NCF106, NCF109	FDT1:X FDT2:M FDT3:M		
NCF107, NCF108	FDT1:M FDT2:M FDT3:X		
NCF114  NCF115	FDT1:M  FDT2:M  FDT3:X	The coordinator and all routers shall generate and receive link status command frames in PRO. End devices shall not either generate or receive link status commands.	

## 1 8.4 Security PICS

2 The security PICS for the ZigBee-PRO stack profile are listed in Table 7. For the general PICS,  
3 including a description of each PICS item, see [R5].

4 **Table 7 – Security PICS for this stack profile**

Item number [R5]	Status	Additional Constraints	Support
SR1	FDT1:M FDT2:O	Upon initial network formation, the coordinator must at least temporarily serve as the trust center. After formation, at least one of the routers or the coordinator must be capable of acting in the role of the trust center. It is an application responsibility to transition the trust center from the coordinator to another router device pointed to by apsTrustCenterAddress within all devices in the network if desired. For the device whose address is apsTrustCenterAddress, it is mandatory to act in the role of the trust center. All devices in the network shall maintain a single consistent definition of apsTrustCenterAddress. It is possible, under application control, to change apsTrustCenterAddress during later network operation, however, it is the application's responsibility to ensure that all devices in the network are notified of the change.	
TCC1	SR1:O.1	Every PRO network shall have a Trust Center either running in Standard or High Security mode  The device designated as the Trust Center shall be declared a concentrator in a PRO network and a Many to One route shall be created to the Trust Center.	

Item number [R5]	Status	Additional Constraints	Support
TCC2	SR1:O.1	<p>Every PRO network shall have a Trust Center either running in Standard or High Security mode</p> <p>The device designated as the Trust Center shall be declared a concentrator in a PRO network and a Many to One route shall be created to the Trust Center.</p>	
MOO1	O.2	A PRO device shall join a PRO network either running in Standard or High Security mode.	
MOO2	O.2	A PRO device shall join a PRO network either running in Standard or High Security mode.	
SL1, SL2, SL3, SL4, SL6, SL7	X	The device shall not apply security to outgoing frames or accept secured incoming frames using any level other than level 0x05.	
SL5	M	The device shall apply security to outgoing frames or accept secured incoming frames using only level 0x05 (i.e., ENC-MIC-32)	
NLS5	M	<p>All devices shall maintain at least 2 NWK keys with the frame counters consistent with the security mode of the network (Standard or High).</p> <p>A NWK key of all zero's shall be treated as reserved. Due to the fact that a NWK key of all zero's was used as a "dummy key" and employed in the trust center exchange where pre-configured keys are used, a NWK key of all zero's is indistinguishable from transport of a dummy key.</p>	
NLS7	M	Devices using this stack profile in Standard Security and High Security mode shall store a single frame counter per neighbor table entry associated with the current NWK Key.	
NLS9	M	Devices using the ZigBee-PRO stack profile shall set: nwkSecureAllFrames = TRUE	
NLS10	O	Coordinator and Router devices employing PRO Standard Mode security shall not reject frames from neighbors which have not been properly authenticated. Coordinator and Router devices employing PRO High Security shall reject frames from neighbors which have not been properly authenticated.	
ASLS4	O	In ZigBee PRO Standard Mode security, trust center master keys are optional for all devices. In ZigBee PRO High Security, trust center master keys mandatory for all devices.	
ASLS5	O	In ZigBee PRO Standard and High security modes, application master keys are optional for all devices.	

Item number [R5]	Status	Additional Constraints	Support
ASLS6	O	Use of application link keys is optional.	
ASLS7	X	ZigBee PRO Standard Mode or High Mode security use <code>nwkSecureAllFrames=TRUE</code> , the APS security header is not employed when the network key is used for incoming APS layer frames.	
ASLS8	O	In ZigBee PRO Standard Mode security, SKKE is optional for all devices. In ZigBee PRO High Security, SKKE is mandatory for all devices.	
ASLS10	M	A newly joined device in ZigBee PRO Standard and High Security shall be capable of receiving the NWK key from the trust center via transport-key commands.	
ASLS11	FDT1:M FDT2:M		
ASLS14	FDT1:M FDT2:M	The trust center shall be able to ask a ZigBee router or the ZigBee coordinator to request that a child device leave the network.	
ASLS18	M		
ASLS19	O	In ZigBee PRO Standard security, the ability to originate tunnel commands from the Trust Center is optional. In ZigBee PRO High Security, it is mandatory.	
ASLS20	FDT1:M FDT2:M FDT3:X	In ZigBee PRO Standard and High security, the ability for the coordinator and all routers to receive tunnel commands is mandatory.	
ASLS21	O	In ZigBee PRO Standard security, the ability to support the authentication service using the entity authentication protocol is optional. In ZigBee PRO High Security, it is mandatory.	
ALS1	M		
ALS2	FDT1:M FDT2:M		
ALS3	FDT2:M FDT3:M		
ALS4	SR1:M		
ALS5	FDT1:M FDT2:M		
ALS6	O	For devices implementing ZigBee PRO Standard Security, following the “authentication procedure” in the role of joining device with a pre-configured network key is optional. For devices implementing ZigBee PRO High Security, it is prohibited.	

Item number [R5]	Status	Additional Constraints	Support
ALS7	O	For devices implementing ZigBee PRO Standard Security, following the “authentication procedure” in the role of joining device with a pre-configured trust center key is optional. For devices implementing ZigBee PRO High Security, it is mandatory unless the ZigBee PRO High Security Trust Center policy permits in the clear delivery of the trust center key.	
ALS8	O	For devices implementing ZigBee PRO Standard Security, following the “authentication procedure” in the role of joining device without a pre-configured trust center key is optional and supported by default due to the requirement to permit ZigBee-2006 Residential Security Mode devices onto PRO Standard Security networks as end devices. For devices implementing ZigBee PRO High Security, it is optional and supported only if the ZigBee PRO High Security Trust Center policy permits in the clear delivery of the trust center key.	
ALS9	SR1:M		
ALS10	FDT2:M FDT3:M		
ALS11	X	This procedure was removed between ZigBee Specification R13 and R16	
ALS12	X	This procedure was removed between ZigBee Specification R13 and R16	
ALS13	SR1:O	For ZigBee PRO Standard Security, it is optional for the trust center to perform the “end-to-end application key establishment” procedure. For ZigBee PRO High Security, it is mandatory.	
ALS14	O	For ZigBee PRO Standard and High Security, it is optional for the network devices to perform the “end-to-end application key establishment” procedure.	
ALS16	SR1:M		
ALS17	FDT2:M		
ALS18	M		
ALS19	FDT2:M		
ALS20	FDT3:M		
ALS21	SR1:O	For ZigBee PRO High Security, the command tunneling procedure in the role of a trust center device is mandatory. For ZigBee PRO Standard Security, it is optional.	
ALS22	FDT1:O FDT2:O	For ZigBee PRO High Security, the command tunneling procedure in the role of a router device is mandatory. For ZigBee PRO Standard Security, it is optional.	

Item number [R5]	Status	Additional Constraints	Support
ALS23	O	The Permissions Configuration Table is optional for all devices.	

1

## 2 8.5 Application layer PICS

3 The application framework PICS for the ZigBee-PRO stack profile are listed in Table 8. For the  
4 general PICS, including a description of each PICS item, see [R6].

5

**Table 8 – Application framework PICS for this stack profile**

Item number [R6]	Status	Additional Constraints	Support
SDT1	SR1:M FDT3:X		
SDT2	SR1:X FDT2:M, FDT3:M		
AFF3	M		
ALF200	O	APS transmissions with DstAddrMode set to 0x00 (indirect) are supported if source binding is supported on the device.	
ALF300	X	APS receptions with DstAddrMode set to 0x00 (indirect) are no longer supported in specification [R1].	
ALF3, AZD24, AZD26, AZD28, AZD29, AZD44, AZD52	O	Binding support is optional for all devices, except that: <ul style="list-style-type: none"> <li>• Source binding only is supported (coordinator based binding is disallowed)</li> <li>• All devices shall minimally respond with NOT_IMPLEMENTED</li> <li>• The ZigBee Coordinator shall implement the mechanism for matching end device bind requests (AZD24;FDT1:M).</li> </ul>	
ALF100	M	The group table in the APS shall contain a minimum of 16 group addresses.	
ADF3 ADF4 ACF500 ACF501	O	Use of the auxiliary APS security header is optional for all devices. The application profiles shall determine requirements for use of the auxiliary APS security header.	

Item number [R6]	Status	Additional Constraints	Support
ADF5 ADF6	O	Use of the extended APS fragmentation/re-assembly header is optional, but in all cases the parameters shall be set by agreement within specific application profiles.  Devices using the ZigBee-PRO stack profile shall set:  <i>Config_Max_ZDO_Payload = 0</i> (ie: for compatibility with the ZigBee stack profile, ZDO messages shall not be fragmented)	
ACF1	SR1:M		
ACF100	SR1:O	In ZigBee PRO Standard Security Mode, it is optional to originate Key Establishment command frames from the Trust Center. In ZigBee PRO High Security, it is mandatory.	
ACF101	SR1:M	In ZigBee PRO Standard Security Mode, it is mandatory to originate Transport Key command frames from the Trust Center for Key Type 1 (Network Key Standard Mode). In ZigBee PRO High Security Mode, it is mandatory to originate Transport Key command frames from the Trust Center for Key Type 0 (Trust Center Master Key) and Key Type 5 (Network Key High Security Mode). It is optional in either ZigBee PRO Standard Security or High Security to originate Transport Key command frames for Key Types 4 (Trust Center Link Key), Key Type 2 (Application Master Key) and Key Type 3 (Application Link Key).	
ACF103	SR1:M		
ACF2	SR1:M		
ACF200	O	In ZigBee PRO Standard Security Mode, it is optional to receive Key Establishment command frames from the Trust Center. In ZigBee PRO High Security, it is mandatory.	
ACF201	M	In ZigBee PRO Standard Security Mode, it is mandatory to receive Transport Key command frames from the Trust Center for Key Type 1 (Network Key Standard Mode). In ZigBee PRO High Security Mode, it is mandatory to receive Transport Key command frames from the Trust Center for Key Type 0 (Trust Center Master Key) and Key Type 5 (Network Key High Security Mode). It is optional in ZigBee PRO Standard Security to receive Transport Key command frames for Key Types 4 (Trust Center Link Key), Key Type 2 (Application Master Key) and Key Type 3 (Application Link Key). It is prohibited in ZigBee PRO High Security to receive Transport Key command frames for Key Types 4 (Trust Center Link Key) and optional to receive Transport Key command frames for Key Type 2 (Application Master Key) and Key Type 3 (Application Link Key). <sup>3</sup>	

<sup>3</sup> CCB 873

Item number [R6]	Status	Additional Constraints	Support
ACF202	SR1:M		
ACF3	FDT1:M FDT2:M FDT3:O	In ZigBee PRO Standard Security, non Trust Center devices may optionally originate application command frames. In ZigBee PRO High Security, all non Trust Center routers and the coordinator shall originate application command frames and end devices may originate application command frames.	
ACF300	O	In ZigBee PRO Standard Security, it is optional for all devices to support origination of Key Establishment command frames from a non Trust Center device. In ZigBee PRO High Security, it is mandatory for all devices to support origination of Key Establishment command frames from a non Trust Center device.	
ACF301	O		
ACF302	FDT1:M FDT2:M FDT3:O		
ACF303	O		
ACF4	SR1:M FDT1:M FDT2:M FDT3:O	In all ZigBee PRO security modes, the Trust Center shall receive application command frames from non Trust Center devices. In ZigBee PRO Standard Security, all non Trust Center routers and the coordinator shall receive application command frames. In ZigBee PRO High Security, all non Trust Center devices shall receive application command frames.	
ACF400	FDT1:M FDT2:M FDT3:O	For all devices in ZigBee PRO Standard Security, receipt of Key Establishment application command frames from a non Trust Center device is optional. In ZigBee PRO High Security, receipt of Key Establishment application command frames from non Trust Center devices is mandatory in all devices.	
ACF402	SR1:M		
ACF403	SR1:M		
AZD707	M	Support of the rejoin mechanism for recovering from a missed network update (of any kind) is mandatory ([R1] Section 2.5.5.5.4).  The length of time between hearing from its parent, or from the ZigBee coordinator, beyond which a ZigBee router shall initiate steps to rejoin the "fragment" of the network which has the ZigBee coordinator in it, is left up to the application designer.	
AZD603	M	Does the device support the Configuration Parameters,	

Item number [R6]	Status	Additional Constraints	Support
		Startup Procedures and Additional Configuration Parameters (references [R1] Sections 2.5.5.5.6.1, 2.5.5.5.6.2, 2.5.5.5.6.3). For the ChannelMask parameter, in the 2.4 Ghz band, channel 26 shall either not be used or else a special provision for limited transmission power shall be imposed to permit U.S. FCC operations.	
AZD17	M		
AZD18	M		
AZD101	SR1:M		
AZD103	FDT1:O FDT2:O FDT3:X		
AZD650	O	Does the device support the Extended Simple Descriptor client service of the Device and Service Discovery Object?	
AZD651	M	Does the device support the Extended Simple Descriptor server service of the Device and Service Discovery Object?	
AZD652	O	Does the device support the Extended Active Endpoint client service of the Device and Service Discovery Object?	
AZD653	M	Does the device support the Extended Active Endpoint server service of the Device and Service Discovery Object?	
AZD19	M		
AZD20	SR1:M		
AZD22	FDT1:M	End_Device_Bind_req server processing in the coordinator is required.	
AZD35	FDT1:X FDT2:X FDT3:M	See sub-clause 8.3 NLF17	
AZD36	FDT1:M  FDT2:M  FDT3:O		
AZD38	FDT1:M FDT2:M		
AZD40	FDT1:M FDT2:M		

Item number [R6]	Status	Additional Constraints	Support
AZD42	FDT1:M FDT2:M		
AZD46	FDT2:M		
AZD400	FDT1:M FDT2:M FDT3:X		
AZD800	O	The ability to send the Mgmt_NWK_Update_req command in order to request the target to perform an energy scan is mandatory for the Network Channel Manager, and optional for all non Network Channel Manager routers and the coordinator.	
AZD801	FDT1:M FDT2:M FDT3:O	The ability for a non Network Channel Manager to receive and process the Mgmt_NWK_Update_req command is mandatory for the coordinator and all routers and optional for end devices.	
AZD503	FDT3:M	See sub-clause 8.3 NLF17	

1

2