ZigBee Document 08006r03

ZigBee-2007 Layer PICS and Stack Profiles

Revision 03

June 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:

Keywords:
ZigBee, ZigBee-Pro, Stack profile, Architecture.

Copyright © 1996-2008 by the ZigBee Alliance.
2400 Camino Ramon, Suite 375, San Ramon, CA 94583, USA
http://www.zigbee.org
All rights reserved.

Permission is granted to members of the ZigBee Alliance to reproduce this document for their own use or the use of other ZigBee Alliance members only, provided this notice is included. All other rights reserved. Duplication for sale, or for commercial or for-profit use is strictly prohibited without the prior written consent of the ZigBee Alliance.

Copyright © ZigBee Alliance, Inc. (2008). All rights Reserved. This information within this document is the property of the ZigBee Alliance and its use and disclosure are restricted.
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

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Contact information

Much of the information in this document is preliminary and subject to change. Members of the ZigBee 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.

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

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:

Phil Jamieson: *Chair*

Mads Westergreen: *Vice Chair*

Don Sturek: Chief *Technical Editor*

Tim Gilman: *Secretary*

The editing team was composed of the following members:

Robert Cragie

Phil Jamieson

Bob Old

Phil Rudland

Zachary Smith

Don Sturek

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Table of Contents

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

List of Figures

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

List of Tables

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Change history

Table 1 shows the change history for this specification.

Table 1 – Document revision change history

Revision	Description
00	Original version as a merge of 064321r08, 074855r04, 04319r01, 04300r08, 043171r04, 064147r07.
01	Snapshot version provided to Core Stack and Qualification Working Groups to validate format of the combined document
02	Major PICS update following many test events. Overhaul of the formatting.
03	Final updates during the June 2008 ZigBee members meeting in Atlanta.

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 Introduction

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented for a given standard. Such a statement is called a protocol implementation conformance statement (PICS).

1.1 Scope

This document provides the protocol implementation conformance statement (PICS) proforma for ZigBee specification (053474r17) in compliance with the relevant requirements, and in accordance with the relevant guidance, given in ISO/IEC 9646-7.

1.2 Purpose

The supplier of a protocol implementation claiming to conform to the ZigBee standard shall complete the following PICS proforma and accompany it with the information necessary to identify fully both the supplier and the implementation.

The protocol implementation conformance statement (PICS) of a protocol implementation is a statement of which capabilities and options of the protocol have been implemented. The statement is in the form of answers to a set of questions in the PICS proforma. The questions in a proforma consist of a systematic list of protocol capabilities and options as well as their implementation requirements. The implementation requirement indicates whether implementation of a capability is mandatory, optional, or conditional depending on options selected. When a protocol implementer answers questions in a PICS proforma, they would indicate whether an item is implemented or not, and provide explanations if an item is not implemented.

ZigBee™ Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

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 04319r01, ZigBee IEEE 802.15.4 PHY & MAC Layer Test Specification release r01, ZigBee Application Working Group

[R4] ZigBee document 084xxx, ZigBee Trust Centre Policies, ZigBee Security Task Group.

2.2 IEEE documents

[R5] 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.

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

3 Definitions

Feature set 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.

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.

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

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

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

5 General description

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 feature set 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.

For clarity, settings applied to the ZigBee feature set will be marked with the string **ZigBee** and settings applied to the ZigBee-PRO feature set will be marked with the string **ZigBee-PRO.**

ZigBee™ Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

6 Knob settings

6.1 Introduction

This section specifies values for parameters specified in the ZigBee specification for tuning the operation of the ZigBee and ZigBee-PRO stack. This section describes settings for both ZigBee and ZigBee-PRO feature sets applied to the ZigBee-2007 Specification ([R1])

6.2 Network settings

The network settings for the ZigBee and ZigBee-PRO feature sets are, for the most part, described in the restricted PICS captured in Section 8.4. Those setting not covered by the PICS are listed in Table 2.

Table 2 – Network settings for this feature set

Parameter Name	Setting		Comments
nwkTransactionPersistenceTime	0x01f4	ZigBee	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 [R5] in a non-beaconed network.
		ZigBee-PRO	
nwkReportConstantCost	FALSE	ZigBee	The NWK layer in PRO shall always calculate routing cost on the basis of neighbor link cost and never report constant cost.
		ZigBee-PRO	

6.3 Application settings

The application settings for the ZigBee and ZigBee-PRO feature sets are, for the most part, described in the restricted PICS captured in Section 8.6. Those setting not covered by the PICS are listed in Table 3.

Table 3 – Application settings for this feature set

Parameter Name	Setting		Comments
Number of active endpoints per sleeping ZigBee end device (maximum)	-	ZigBee	As the responsibility to arrange for caching of service discovery information lies with the end device itself, this parameter is not restricted.
		ZigBee-PRO	

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Parameter Name	Setting	Comments	
Config_NWK_Leave_removeChildren	FALSE	ZigBee	
		ZigBee-PRO	

6.4 Security settings

The security settings for the ZigBee and ZigBee-PRO feature sets are listed in Table 4.

Table 4 – Security settings for this feature set

Parameter Name	Setting	Comments	
apsSecurityTimeoutPeriod	50ms * (2*NWK Maximum Depth) + (AES Encrypt/Decrypt times)	ZigBee	Where AES Encrypt/Decrypt times = 200ms, and Where NWK Maximum Depth is assumed to be 5, meaning every device in the network can be reached in not more than 10 hops. I.e. 700 milliseconds. Note that this timeout assumes worst case AES engine speeds and is not indicative of expected performance for most devices.
		ZigBee-PRO	Where AES Encrypt/Decrypt times = 200ms, and Where NWK Maximum Depth is assumed to be 15, meaning every device in the network can be reached in not more than 30 hops. I.e. 1.7 seconds. Note that this timeout assumes worst case AES engine speeds and is not indicative of expected performance for most devices.

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

7 Functional description

For the most part, the functioning of ZigBee and ZigBee-PRO 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 and ZigBee-PRO feature sets lead to some special functional considerations, which are detailed here.

7.1 Device roles

The basic roles performed by ZigBee devices in ZigBee and 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 feature set. 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 and ZigBee-PRO feature sets, all devices are expected to manage their own binding tables if they use binding tables.

This section is valid for both the **ZigBee** and **ZigBee-PRO** feature sets.

7.2 ZigBee: Compatibility with Other Feature sets

Devices implementing the ZigBee feature set will advertise a feature set identifier of 1 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 feature set and advertise this fact by placing a feature set identifier of 1 in their beacon payloads.

In order to provide compatibility with devices implemented according to the ZigBee-PRO feature set, ZigBee devices shall additionally be able to join networks which advertise a feature set identifier of 2 in their beacon payloads but the device must join the ZigBee-PRO networks as end devices and only those ZigBee-PRO networks employing standard network security.

This section is valid for the **ZigBee** feature set.

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

7.3 ZigBee-PRO: Compatibility with Other Feature sets

Devices implementing the ZigBee-PRO feature set will advertise a feature set 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 feature set and advertise this fact by placing a feature set identifier of 2 in their beacon payloads.

In order to provide compatibility with devices implemented according to the ZigBee feature set, ZigBee-PRO devices shall additionally be able to join networks which advertise a feature set 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.

This section is valid for the **ZigBee-PRO** feature set.

7.4 Binding tables

Binding tables, if used, shall be 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 should be flexible enough that it can be set, at least at compile time, with some awareness of the actual intended usage of the device.

This section is valid for both the **ZigBee** and **ZigBee-PRO** feature sets.

7.5 Multicast mechanism and groups

Support for APS level multicasts is mandatory to support compatibility with ZigBee devices. The multicast groups are then established using the application level mechanisms. Support for routing of network level multicasts is mandatory in the ZigBee-Pro feature set.

ZigBee devices do not support network level multicasts.

7.6 Trust Center Policies and Security Settings

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

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

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

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

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

7.7 Battery powered devices

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

As mentioned above, ZigBee-PRO 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 feature set provides that parent devices, i.e. ZigBee routers and the ZigBee coordinator, hold frames for 7.5 seconds on behalf of sleeping end devices and this is also, roughly speaking, the maximum polling rate prescribed here. Devices may implement a polling interval longer than 7.5 seconds, however the application will then have to handle the potential loss of messages during longer sleep cycles.

7.8 Mains powered devices

It is assumed that for most ZigBee-PRO 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.

7.9 Persistent storage

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

7.10 Address Reuse

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

7.11 Duty cycle limitations and fragmentation

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

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

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

7.11.1 Vulnerability join

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

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

7.11.2 Pre-installation

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

7.12 Security

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

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

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

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

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

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

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

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

7.12.1 Security Modes within PRO Networks

The feature set shall use two security modes: Standard mode and High Security mode.

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

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

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

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

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

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

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, if FDT1 and FDT2 are both marked "O.1" this 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.

8.2 ZigBee device types

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
FDT1	Is this device capable of acting as a ZigBee coordinator?	[R1]/Preface (Definitions)		ZigBee	O.1		
				ZigBee-PRO	O.1		Y
FDT2	Is this device capable of acting as a ZigBee router?	[R1]/ Preface (Definitions)		ZigBee	O.1		
				ZigBee-PRO	O.1		Y
FDT3	Is this a ZigBee end device?	[R1]/ Preface (Definitions)		ZigBee	O.1		
				ZigBee-PRO	O.1		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

8.3 IEEE 802.15.4 PICS

8.3.1 FDT2 and FDT3 network join options

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
JN1	The device joins a network by scanning and then associating (client)	[R5] 7.3.1.1	FDT1:X FDT2:O FDT3:O	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
JN10	The device supports joining a network by associating (server)	[R5] 7.3.1.1	FDT1: O FDT2: O FDT3: N/A	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
JN2	The device joins a network by using an orphan scan (client)	[R5] 7.3.2.3	FDT1: N/A FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: O FDT3: O		
				ZigBee-PRO	FDT1: X FDT2: O FDT3: O		N
JN20	The device supports joining a network by using an orphan scan (server)	[R5] 7.3.2.3	FDT1: O FDT2: O FDT3: N/A	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 ### 8.3.2 IEEE 802.15.4 PHY

2 #### 8.3.2.1 Radio frequency of operation

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
RF1	The device operates at a frequency of 868 MHz.	[R5] 6.1.1, 6.1.2, 6.6	O^3	ZigBee	O^3		
				ZigBee-PRO	O^3		N
RF2	The device operates at a frequency of 915 MHz.	[R5] 6.1.1, 6.1.2, 6.6	O^3	ZigBee	O^3		
				ZigBee-PRO	O^3		N
RF3	The device operates at a frequency of 2.4 GHz.	[R5] 6.1.1, 6.1.2, 6.5	O^3	ZigBee	O^3		
				ZigBee-PRO	O^3		Y

3 O^3: at least one option must be selected.
4

5 #### 8.3.2.2 Clear channel assessment

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
CCA1	Mode 1: Energy above threshold is supported.	[R5] 6.7.9	O^4	ZigBee	O^4		
				ZigBee-PRO	O^4		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
CCA2	Mode 2: Carrier sense only is supported.	[R5] 6.7.9	O[4]	ZigBee	O[4]		
				ZigBee-PRO	O[4]		Y
CCA3	Mode 3: Carrier sense with energy above threshold is supported.	[R5] 6.7.9	O[4]	ZigBee	O[4]		
				ZigBee-PRO	O[4]		Y

1 O[4]: at least one option must be selected.
2

3 ### 8.3.3 IEEE 802.15.4 MAC

4 #### 8.3.3.1 Channel access

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
CA1	A super-frame structure is supported.	[R5] 7.5.1.1	O	ZigBee	X		
				ZigBee-PRO	X		
CA2	Un-slotted CSMA-CA is supported.	[R5] 7.5.1.1	M	ZigBee	M	All devices shall set their MIB values as follows: *macBeaconOrder* = 0x0f, *macSuperframeOrder* = 0x0f.	
				ZigBee-PRO	M	All devices shall set their MIB values as follows: *macBeaconOrder* = 0x0f, *macSuperframeOrder* = 0x0f.	Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
CA3	Slotted CSMA-CA is supported.	[R5] 7.5.1.1	CA1: M	ZigBee	X		
				ZigBee-PRO	X		
CA4	Super-frame timing is supported.	[R5] 7.5.1.1	CA1: M	ZigBee	X		
				ZigBee-PRO	X		

1

2 ### 8.3.3.2 Guaranteed time slots

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
GTS1	Guaranteed time slots are supported (*server*).	[R5] 7.5.7	FDT1: O	ZigBee	X		
				ZigBee-PRO	X		
GTS2	Guaranteed time slots are supported (*client*).	[R5] 7.5.7	FDT2: O FDT3: O	ZigBee	X		
				ZigBee-PRO	X		

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
GTS3	The client device has the ability to request a GTS. Operations include: • Allocation requests • De-allocation requests • [MLME-GTS.request primitive] • [MLME-GTS.confirm primitive] • Transmission of the GTS request command.	[R5] 7.1.7.1, 7.1.7.2, 7.3.3.1, 7.5.7.2, 7.5.7.4	GTS2: M	ZigBee	X		
				ZigBee-PRO	X		
GTS4	The server has the ability to process GTS requests. Operations include: • Allocation requests • De-allocation requests • Re-allocation requests • [MLME-GTS.indication primitive] • Reception and processing of the GTS request command.	[R5] 7.1.7.3, 7.3.3.1, 7.5.7.2, 7.5.7.4, 7.5.7.5	GTS1: M	ZigBee	X		
				ZigBee-PRO	X		
GTS5	The server can manage the GTSs.	[R5] 7.5.7	GTS1: M	ZigBee	X		
				ZigBee-PRO	X		

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
GTS6	The server can perform CAP maintenance.	[R5] 7.5.7.1	GTS1: M	ZigBee	X		
				ZigBee-PRO	X		
GTS7	The device can transmit and/or receive data within a GTS.	[R5] 7.5.7.3	GTS1: M GTS2: M	ZigBee	X		
				ZigBee-PRO	X		

1

2 ### 8.3.3.3 Scanning

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
S1	The device can perform some form of channel scan. Operations include: • Scanning mechanism • [MLME-SCAN.request primitive] • [MLME-SCAN.confirm primitive]	[R5] 7.1.11.1, 7.1.11.2, 7.5.2.1	M	ZigBee	M	All devices shall be able to perform at least an active scan.	
				ZigBee-PRO	M	All devices shall be able to perform at least an active scan.	Y
S2	The device can perform an energy detection scan.	[R5] 7.5.2.1.1	FDT1: M	ZigBee	FDT1: M FDT2: M FDT3: X	Network devices shall perform an energy detection scan on request from the next higher layer.	
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X	The coordinator shall perform an energy detection scan on each available channel in the active channel mask before starting a network.	Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
S3	The device can perform an active scan. Operations include: • Transmission of the beacon request command.	[R5] 7.3.2.4, 7.5.2.1.2	FDT1: M JN1: M	ZigBee	M	All devices shall perform an active scan on each available channel in the active channel mask.	
				ZigBee-PRO	M	All devices shall perform an active scan on each available channel in the active channel mask.	Y
S4	The device can perform a passive scan.	[R5] 7.5.2.1.3	O	ZigBee	X		
				ZigBee-PRO	X		
S5	The client can perform an orphan scan. Operations include: • Orphan device realignment. • Transmission of the orphan notify command. • Reception and processing of the coordinator realignment command.	[R5] 7.3.2.3, 7.3.2.5, 7.5.2.1.4	JN2: M	ZigBee	JN2:M		
				ZigBee-PRO	JN2:M		Y
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.	[R5] 7.1.8.1, 7.1.8.2, 7.3.2.3, 7.3.2.5, 7.5.2.1.4	FDT1: O FDT2: O	ZigBee	FDT1: M FDT2: M FDT3: X	Network rejoin is the preferred mechanism for devices to use, however, orphan scan may be used and the parent devices shall support orphan scan.	
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X	Network rejoin is the preferred mechanism for devices to use, however, orphan scan may be used and the parent devices shall support orphan scan.	Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
S7	The server can receive and process a beacon request command.	[R5] 7.3.2.4	S3 & FDT1: M	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

1

2 ### 8.3.3.4 PAN identifier conflict resolution

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
PICR1	PAN identifier conflict resolution is supported (*server*). Operations include: • Reception and processing of the PAN identifier conflict notification command. • Transmission of the coordinator realignment command.	[R5] 7.3.2.2, 7.3.2.5, 7.5.2.2	FDT1: O	ZigBee	FDT1: X FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: X		
PICR2	PAN identifier conflict resolution is supported (*client*). Operations include: • Transmission of the PAN identifier conflict notification command. • Reception and processing of the coordinator realignment command.	[R5] 7.3.2.2, 7.3.2.5, 7.5.2.2	FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: X		

3

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 **8.3.3.5 PAN start**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
PS1	Starting a PAN is supported. Operations include: • [MLME-START.request primitive] • [MLME-START.confirm primitive]	[R5] 7.1.14.1, 7.1.14.2, 7.5.2.3	FDT1: M FDT2: M FDT3: O	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

2

3 **8.3.3.6 Association**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
A1	Association is supported (*server*).	[R5] 7.5.3.1	FDT1: O FDT2: O	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
A2	Association is supported (*client*).	[R5] 7.5.3.1	FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
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.	[R5] 7.1.3.2, 7.1.3.3, 7.3.1.1, 7.3.1.2	A1: M	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
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.	[R5] 7.1.3.1, 7.1.3.4, 7.3.1.1, 7.3.1.2	A2: M	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y

1

ZigBee™ Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 **8.3.3.7 Disassociation**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
D1	The device can request a disassociation. Operations include: • [MLME-DISASSOCIATE.request primitive] • [MLME-DISASSOCIATE.confirm primitive] • Transmission of the disassociation notify command.	[R5] 7.1.4.1, 7.1.4.3, 7.3.1.3	O	ZigBee	FDT1: X FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: X		
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.	[R5] 7.1.4.2, 7.3.1.3	O	ZigBee	FDT1: X FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: X		
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.	[R5] 7.1.4.2, 7.3.1.3	O	ZigBee	FDT1: X FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: X		

2

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 **8.3.3.8 Beacon synchronization**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
BS1	Beacon notification is supported. Operations include: • [MLME-BEACON-NOTIFY.indication primitive]	[R5] 7.1.5.1	O	ZigBee	FDT1: M FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: M		Y
BS2	The client can synchronize to a beacon. Operations include: • (Tracking only for beacon networks) • [MLME-SYNC.request primitive] • [MLME-SYNC-LOSS.indication primitive]	[R5] 7.1.15.1, 7.1.15.2, 7.5.4	O	ZigBee	FDT1: X FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: X		

2

3 **8.3.3.9 Transmission**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
T1	Frame transmission is supported. Operations include: • Frame construction • [MCPS-DATA.request primitive] • [MCPS-DATA.confirm primitive] • Transmission of data frames.	[R5] 7.1.1.1, 7.1.1.2, 7.2.1, 7.2.2.2, 7.5.6.1	M	ZigBee	M		
				ZigBee-PRO	M		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
T2	Implicit (command frame) transmission confirmation is supported. Operations include: • [MLME-COMM-STATUS.indication primitive]	[R5] 7.1.12.1	M	ZigBee	M		
				ZigBee-PRO	M		Y

1

2 **8.3.3.10 Reception**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
R1	Frame reception is supported. Operations include: • Data frame de-construction • [MCPS-DATA.indication primitive] • Reception of data frames.	[R5] 7.1.1.3, 7.2.1, 7.2.2.2	M	ZigBee	M		
				ZigBee-PRO	M		Y
R2	Receiver control is supported. Operations include: • [MLME-RX-ENABLE.request primitive] • [MLME-RX-ENABLE.confirm primitive]	[R5] 7.1.10.1, 7.1.10.2	O	ZigBee	O		
				ZigBee-PRO	O		Y
R3	Filtering and rejection is supported.	[R5] 7.5.6.2	M	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
R4	Promiscuous mode is supported.	[R5] 7.5.6.6	O	ZigBee	O		
				ZigBee-PRO	O		N

1

2 **8.3.3.11 Transaction handling**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
TH1	Transaction handling is supported (*server*).	[R5] 7.5.5	FDT1: O FDT2: O	ZigBee	FDT1: M FDT2: M FDT3: X	The server shall be able to handle at least one transaction.	
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X	The server shall be able to handle at least one transaction.	Y
TH2	Transaction handling is supported (*client*).	[R5] 7.5.5	FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: X FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: M		
TH3	The server can manage transactions to its devices. Operations include: • Transaction queuing • Reception and processing of the data request command.	[R5] 7.5.5, 7.1.1.4, 7.1.1.5, 7.3.2.1	TH1: M	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
TH30	The server can manage transaction purging operations: • [MCPS-PURGE.request primitive] • [MCPS-PURGE.confirm primitive]	[R5] 7.1.1.4, 7.1.1.5, 7.3.2.1	TH1: M	ZigBee	O		
				ZigBee-PRO	O		N
TH4	The client can extract data from the coordinator following an indication of data in a beacon.	[R5] 7.5.6.3	TH2: O[5]	ZigBee	FDT1: X FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: X		
TH5	The client can poll for data. Operations include: • [MLME-POLL.request primitive] • [MLME-POLL.confirm primitive] • Transmission of the data request command.	[R5] 7.1.16.1, 7.1.16.2, 7.3.2.1	TH2: O[5]	ZigBee	FDT1: X FDT2: X FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: M		

1 O[5]: At least one of these options must be supported.

2 ### 8.3.3.12 Acknowledgement service

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AS1	The acknowledgement service is supported.	[R5] 7.5.6.4	O	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AS2	The device can transmit, receive and process acknowledgement frames.	[R5] 7.2.2.3	AS1: M	ZigBee	M		
				ZigBee-PRO	M		Y
AS3	Deprecated	[R5] 7.5.6.4.2, 7.5.6.5	AS1: M	ZigBee	X		
				ZigBee-PRO	X		
AS4	Retransmissions are supported.	[R5] 7.5.6.5	AS1: M	ZigBee	M		
				ZigBee-PRO	M		Y

1

2 ### 8.3.3.13 MIB management

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
MM1	MIB management is supported. Operations include: • MIB attribute storage	[R5] 7.4.2	O	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
MM2	The device supports the reading of MIB attributes. Operations include: • [MLME-GET.request primitive] • [MLME-GET.confirm primitive]	[R5] 7.1.6.1, 7.1.6.2, 7.4.2	MM1: O	ZigBee	M		
				ZigBee-PRO	M		Y
MM3	The device supports the writing of MIB attributes. Operations include: • MIB attribute verification • [MLME-SET.request primitive] • [MLME-SET.confirm primitive]	[R5] 7.1.13.1, 7.1.13.2, 7.4.2	MM1: O	ZigBee	M		
				ZigBee-PRO	M		Y

1

2 **8.3.3.14 MAC security**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
MS1	The device supports ACL mode. Operations include: • ACL storage • ACL mode usage	[R5] 7.4.2, 7.5.8.1, 7.5.8.3	O	ZigBee	X		
				ZigBee-PRO	X		
MS2	The device supports secured mode.	[R5] 7.5.8.4	O	ZigBee	X		
				ZigBee-PRO	X		

3

4

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

8.3.3.15 Device reset

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
DR1	The device is able to reset. Operations include: • [MLME-RESET.request primitive] • [MLME-RESET.confirm primitive]	[R5] 7.1.9.1, 7.1.9.2	O	ZigBee	O		
				ZigBee-PRO	O		Y

8.4 Network layer PICS

8.4.1 ZigBee network frame format

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
GFF1	Does the device support the general ZigBee network frame format?	[R1]/3.3.1		ZigBee	M		
				ZigBee-PRO	M		Y

8.4.2 Major capabilities of the ZigBee network layer

Tables in the following sub-clauses detail the capabilities of NWK layer for ZigBee devices.

8.4.2.1 Network layer functions

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF1	Does the network layer support transmission of data by the next higher layer?	[R1]/3.2.1.1, 3.2.1.2, 3.6.2.1	M	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF2	Does the network layer support reception of data by the next higher layer?	[R1]/3.2.1.3, 3.6.2.2	M	ZigBee	M		
				ZigBee-PRO	M		Y
NLF3	Does the network layer support discovery of existing ZigBee networks?	[R1]/3.2.2.1, 3.2.2.2	M	ZigBee	M		
				ZigBee-PRO	M		Y
NLF4	Does the network layer support formation of ZigBee networks?	[R1]/3.2.2.3, 3.2.2.4, 3.6.1.1	FDT1:M, FDT2:X, FDT3:X	ZigBee	FDT1: M FDT2: X FDT3: X	Devices using the ZigBee feature set shall set: Feature set = 1 *nwkcProtocolVersion* = 2 and shall advertise these values in their beacon payload in response to MAC beacon requests. Devices using the ZigBee feature set shall also set: *nwkSecurityLevel* = 5	
				ZigBee-PRO	FDT1: M FDT2: X FDT3: X	Devices using the ZigBee-PRO feature set shall set: Feature set = 2 *nwkcProtocolVersion* = 2 and shall advertise these values in their beacon payload in response to MAC beacon requests. Devices using the ZigBee-PRO feature set shall also set: *nwkSecurityLevel* = 5	Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF5	Can the network layer permit other devices to join the network of which it is a part (and also deny such permission)?	[R1]/3.2.2.5, 3.2.2.6, 3.6.1.2	FDT1:M, FDT2:M, FDT3:X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NLF6	Can the device start as a router?	[R1]/3.2.2.7, 3.2.2.8	FDT1:X, FDT2:M, FDT3:X	ZigBee	FDT1: X FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: X		Y
NLF60	Can the network layer perform energy detection scans at the request of the next higher layer?	[R1]/3.2.2.9, 3.2.2.10	M	ZigBee	FDT1: M FDT2: M FDT3: X	NLME-ED-SCAN is mandatory for the coordinator and optional for all routers on a ZigBee network.	
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X	NLME-ED-SCAN is mandatory for the coordinator and all routers on a PRO network.	Y
NLF7	Can the device request membership in a ZigBee network?	[R1]/3.2.2.11, 3.2.2.13, 3.6.1.4	FDT1: N/A FDT2: M FDT3: M	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
NLF70	Can the device request to join or rejoin a network using the orphaning procedure?	[R1]/3.2.2.14, 3.2.2.15, 3.6.1.4.3.1	FDT1: N/A FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: O FDT3: O		
				ZigBee-PRO	FDT1: X FDT2: O FDT3: O		N

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF71	Can the device request to join / rejoin a network using the rejoin command frame and associated procedure?	[R1]/3.2.2.11, 3.2.2.13, 3.6.1.4.2.1	FDT1: N/A FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
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?	[R1]/3.2.2.11, 3.2.2.13	O	ZigBee	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.	
				ZigBee-PRO	M		Y
NLF8	Can the device respond to requests to join the network of which it is a part?	[R1]/3.6.1.4.1 .2, 3.6.1.4.2.2	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NLF81	Does the network layer of a device inform the next higher layer when a second device has joined or rejoined its network as a child?	[R1]/3.2.2.12	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NLF9	Does the network layer employ the Distributed Address Mechanism to generate a unique network address to assign to a joining device?	[R1]/3.6.1.6	FDT1: O FDT2: O FDT3: N/A	ZigBee	FDT1: M FDT2: M FDT3: X	The ZigBee feature set always employs the distributed addressing scheme with: nwkMaxDepth = 5 nwkMaxChildren = 20 nwkMaxRouters = 6	
				ZigBee-PRO	FDT1: X FDT2: X FDT3: X		

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF90	Does the network layer employ the Stochastic Addressing Scheme to generate a unique network address to assign to a joining or rejoining device?	[R1]/3.6.1.7	FDT1: O FDT2: O FDT3: N/A	ZigBee	FDT1: X FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X	The ZigBee-PRO feature set employs stochastic address allocation. The follow parameter values are defined: *nwkAddrAlloc* = 2 *nwkUseTreeRouting* = FALSE *nwkMaxDepth* = 15 Note that nwkMaxDepth above is only used to compute timeouts and shall not limit the actual network radius, as this feature set does not use tree-based addressing. The parameter *nwkMaxChildren* is not restricted in this feature set.	Y
NLF100	Does the network layer employ the Higher Layer Address Assignment Mechanism to generate a unique network address to assign to a joining device?	Deprecated	X	ZigBee	X		
				ZigBee-PRO	X		
NLF10	Can the next higher layer request that a particular device be “pre-joined” to it using the DIRECT-JOIN procedure?	[R1]/3.2.2.14, 3.2.2.15, 3.6.1.4.3	FDT1: O FDT2: O FDT3: X	ZigBee	X	This service is useful for testing and may be allowed as a part of test procedures at the option of the stack developer.	
				ZigBee-PRO	X	This service is useful for testing and may be allowed as a part of test procedures at the option of the stack developer.	

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF11	Can the device make a request to leave the network?	[R1]/3.2.2.16, 3.2.2.18, 3.6.1.10.1	O	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
NLF12	Can the device make a request that one of its child devices leave the network?	[R1]/3.2.2.16, 3.2.2.18, 3.6.1.10.2	FDT1: O FDT2: O FDT3: N/A	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NLF13	Can the network layer process network leave commands from child devices?	[R1]/3.6.1.10.3	FDT1: M FDT2: M FDT3: N/A	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NLF130	Can the network layer process network leave commands from parent devices?	[R1]/3.6.1.10.3	FDT1: N/A FDT2: M FDT3: M	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
NLF131	Does the network layer inform the next higher layer if the device itself has left the network?	[R1]/3.2.2.17	M	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF14	Does the device support changing of the ZigBee coordinator configuration in an operating network?	[R1]/3.2.2.3, 3.2.2.4, 3.6.1.11	FDT1: O FDT2: X FDT3: X	ZigBee	FDT1: M FDT2: X FDT3: X	The ZigBee coordinator shall change the logical channel and PAN ID when directed to by the Network Channel Manager.	
				ZigBee-PRO	FDT1: M FDT2: X FDT3: X		Y
NLF15	Does the device support changing of the ZigBee router configuration in an operating network?	[R1]/3.2.2.7, 3.2.2.8	FDT1: X FDT2: O FDT3: X	ZigBee	FDT1: X FDT2: M FDT3: X	The ZigBee router shall change the logical channel and PAN ID when directed to by the Network Channel Manager.	
				ZigBee-PRO	FDT1: X FDT2: M FDT3: X		Y
NLF16	Does the network layer support reset?	[R1]/3.2.2.19, 3.2.2.20, 3.6.1.12	M	ZigBee	M		
				ZigBee-PRO	M		Y

ZigBee™ Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF17	Does the network layer allow the next higher layer to synchronize with or extract data from the device's ZigBee coordinator or router?	[R1]/3.2.2.22, 3.2.2.23	FDT1: X FDT2: O FDT3: M	ZigBee	FDT1: X FDT2: X FDT3: M	Recommended polling rates for end devices using this feature set: 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 *nwkTransactionPersistenceTime* to ensure that child devices can poll frequently enough to retrieve messages prior to expiration in the indirect message queue of their parent. The polling rate established here also does not consider APS acknowledgement timeout (which is much shorter than *nwkTransaction-PersistenceTime).* 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.	
				ZigBee-PRO	FDT1: X FDT2: X FDT3: M		
NLF18	Does the network layer report a loss of synchronization with the device's ZigBee router or ZigBee coordinator to the next higher layer?	[R1]/3.2.2.23	FDT1: X FDT2: O FDT3: M	ZigBee	X		
				ZigBee-PRO	X		

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF19	Does the network layer offer the next higher layer the ability to retrieve network information base (NIB) attributes?	[R1]/3.2.2.26, 3.2.2.27	M	ZigBee	M		
				ZigBee-PRO	M		Y
NLF20	Does the network layer offer the next higher layer the ability to set network information base (NIB) attributes?	[R1]/3.2.2.28, 3.2.2.29	M	ZigBee	M		
				ZigBee-PRO	M		Y
NLF110	Does the network layer support network status reporting to the next higher layer?	[R1]/3.2.2.30	M	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NLF111	Does the network layer support Route Discovery?	[R1]/3.2.2.31, 3.2.2.32, 3.6.3.5	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF112	Does the network layer support Route Discovery requests with DstAddrMode of 0x00 in support of Many-to-One discovery?	[R1]/3.2.2.31, 3.2.2.32, 3.6.3.5	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X	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.	N
NLF113	Does the network layer support Route Discovery requests with DstAddrMode of 0x01 in support of Multicast Group Discovery?	[R1]/3.2.2.31, 3.2.2.32, 3.6.3.5, 3.6.6	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X	Initiation of route discovery commands where DstAddrMode is 0x01 (Multicast Group Discovery) is optional.	Y
NLF114	Does the network layer support Route Discovery requests with DstAddrMode of 0x02 in support of the discovery of Unicast routes?	[R1]/3.2.2.31, 3.2.2.32, 3.6.3.5	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: O FDT2: O FDT3: X	Initiation of route discovery commands where DstAddrMode is 0x02 (Unicast) is optional. ZigBee coordinators and ZigBee routers shall support reception and correct handling of unicast discovery commands.	
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF115	Does the network layer employ tree routing?	3.6.3.3	O	ZigBee	M	Devices using the ZigBee stack profile must set: *nwkUseTreeRouting* = TRUE	
				ZigBee-PRO	X	Devices using the ZigBee-PRO stack profile shall set: *nwkUseTreeRouting* = FALSE	
NLF21	Does the network layer calculate routing cost based on probability of reception?	3.6.3.1	O	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NLF22	Does the network layer maintain a routing table and route discovery table?	[R1]/3.6.3.2	FDT1: O FDT2: O FDT3: X	ZigBee	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	
				ZigBee-PRO	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): 10 entries An aging algorithm is recommended but is beyond the scope of this specification. Route discovery table entries (minimum): 4 entries The Route discovery table entries shall be managed as described in [R1] sub-clause 3.6.3.6.	Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF220	Does the network layer maintain a route record table?	[R1]/3.5.2, 3.6.3.2	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		N
NLF221	Does the network layer maintain a multicast group ID table?	[R1]/3.6.6.1	FDT1:O, FDT2:O, FDT3:X	ZigBee	X	ZigBee coordinators and ZigBee routers that use this stack profile shall set *nwkUseMulticast* to FALSE.	
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		Y
NLF23	Does the network layer reserve routing capacity for route repair operations? (Note: This capability has been removed from the ZigBee specification as of r08).	None	X	ZigBee	X		
				ZigBee-PRO	X		
NLF24	Does the device implement beacon collision-avoidance measures?	[R1]/3.6.4	O	ZigBee	X		
				ZigBee-PRO	X		
NLF25	Does the network layer support router re-enumeration as a route repair method? (Note: This capability has been removed from the ZigBee specification as of r10).	None	X	ZigBee	X		
				ZigBee-PRO	X		

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF26	Does the network layer assume that links are symmetrical and establish forward and reverse routes at the same time?	[R1]/3.5.2, 3.6.3.5.2	O	ZigBee	X	Devices using the ZigBee stack profile must set: *nwkSymLink* = FALSE	
				ZigBee-PRO	M	Devices using the ZigBee-PRO stack profile shall set: *nwkSymLink* = TRUE	Y
NLF27	Does the network layer maintain a neighbor table or tables in order to store information about nearby devices?	[R1]/3.6.1.5	M	ZigBee	M	ZigBee coordinators and ZigBee routers shall maintain a neighbor table or tables as follows: ZigBee coordinator (minimum): 24 entries[1] ZigBee router (minimum): 25 entries ZigBee end device (minimum): 1 entry	
				ZigBee-PRO	M	ZigBee coordinators and ZigBee routers shall maintain a neighbor table or tables as follows: ZigBee coordinator (minimum): (Number of child end devices accepted) plus 16 ZigBee router (minimum): (Number of child end devices accepted) plus 16 ZigBee end device: 1 (Note: End Device shall only support only a single neighbor table entry and that entry shall be for their parent) 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.	Y

[1] LB #047

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF28	Does the network layer buffer frames pending route discovery or route repair operations?	[R1]/3.6.3.5.1	O	ZigBee	O		
				ZigBee-PRO	O		N
NLF29	Does the network layer buffer data frames on behalf of end device that are its children?	[R1]/3.6.5	FDT1:M FDT2:M FDT3:X	ZigBee	FDT1: M FDT2: M FDT3: X	ZigBee router and coordinator devices shall 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.	
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NLF30	Is the device capable of participating in a beacon-oriented network?	[R1]/Preface Definitions and Network Topology sections	O	ZigBee	X	On invocation of the NLME-NETWORK-FORMATION.request or NLME-START-ROUTER.request primitives, devices shall employ: BeaconOrder = 0x0f SuperframeOrder = 0x0f	
				ZigBee-PRO	X		
NLF31	Does the network layer support the detection of address conflicts?	[R1]/3.6.1.9	O	ZigBee	X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X	Address conflict detection is mandatory for this stack profile (nwkUniqueAddr = FALSE). The coordinator and all routers shall implement the Address Conflict procedure.	Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLF32	Does the network layer support resolving address conflicts?	[R1]/3.6.1.9.3	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X	Address conflict resolution is mandatory for this stack profile (nwkUniqueAddr = FALSE). The coordinator and all routers shall implement the Address Conflict procedure.	Y
NLF33	Does the network layer support the detection of PAN ID conflicts?	[R1]/3.6.1.13	O	ZigBee	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 nwkManagerAddr is mandatory for all routers and the coordinator. The nwkManagerAddr is required to process all NWK Status command frames directed to it by the coordinator and routers.	
				ZigBee-PRO	FDT1:M FDT2:M FDT3:X		Y
NLF34	Does the device support resolving PAN ID conflicts?	[R1]/3.6.1.13	O	ZigBee	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 nwkManagerAddr is mandatory for all routers and the coordinator. The nwkManagerAddr is required to process all NWK Status command frames directed to it by the coordinator and routers.	
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

1

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

8.4.2.2 Network layer frames

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NDF1	Does the device support the origination of network data frames?	[R1]/3.3.2.1, 3.6.2.1	M	ZigBee	M		
				ZigBee-PRO	M		Y
NDF2	Does the device support the receipt of network data frames?	[R1]/3.3.2.1, 3.6.2.2	M	ZigBee	M		
				ZigBee-PRO	M		Y
NDF3	Does the device support the relaying of unicast network data frames?	[R1]/3.3.2.1, 3.6.3.3	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NDF4	Does the device support relaying of broadcast network data frames?	[R1]/3.3.2.1, 3.6.5	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X	Devices using the ZigBee stack profile must set: Broadcast Transaction Table size: 9 (minimum) nwkBroadcastDeliveryTime = 9 nwkPassiveAckTimeout = 0.5 (maximum) nwkMaxBroadcastRetries = 2	
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X	Devices using the ZigBee-PRO stack profile shall set: Broadcast Transaction Table size: 9 (minimum) *nwkBroadcastDeliveryTime* = 9[2] *nwkPassiveAckTimeout* = 0.5 (maximum) *nwkMaxBroadcastRetries* = 2 Application designers should take care to use multicast and broadcast sparingly due to the limitations of the broadcast bandwidth of a network.	Y
NDF100	Does the device support relaying of multicast network data frames?	[R2]/3.3.2.1, 3.6.6	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X	The coordinator and all routers in a PRO network shall be able to relay member mode[3] multicast network data frames.	Y
NDF101	Does the device support the relaying of source routed network data frames?	[R2]/3.3.2.1, 3.6.3.3.2	FDT1:O, FDT2:O, FDT3:X	ZigBee	X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

[2] CCB 884
[3] CCB 872

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 **8.4.2.3 Network command frames**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NCF1	Does the device support the origination of route request command frames?	[R1]/3.4.1, 3.6.3.5.1	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF2	Does the device support the receipt of route request command frames?	[R1]/3.4.1, 3.6.3.5.2	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF3	Does the device support the relaying of route request command frames?	[R1]/3.4.1, 3.6.3.5.2	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF4	Does the device support the origination of route reply command frames?	[R1]/3.4.2, 3.6.3.5.2	FDT1:M, FDT2:M, FDT3:X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF5	Does the device support the receipt of route reply command frames?	[R1]/3.4.2, 3.6.3.5.3	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NCF6	Does the device support the relaying of route reply command frames?	[R1]/3.4.2, 3.6.3.5.3	FDT1:M, FDT2:M, FDT3:X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF7	Does the device support the transmission of network status command frames?	[R1]/3.4.3, 3.6.1.9.3, 3.6.3.3, 3.6.3.7.1	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF8	Does the device support the receipt of network status command frames?	[R1]/3.4.3, 3.6.1.9.3, 3.6.3.7.1	M	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF9	Does the device support the relaying of network command frames? In particular, does it support the relaying of those command frames, specifically network status, network report and network update, which require relaying but for which there are no special per-hop processing requirements?	[R1]/3.4.3, 3.4.9, 3.4.10	FDT1:M, FDT2:M, FDT3:X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NCF100	Does the device support the origination of leave command frames?	[R1]/3.4.4, 3.6.1.10	FDT1:O, FDT2:O, FDT3:O	ZigBee	FDT1: M FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: M		Y
NCF101	Does the device support the receipt of leave command frames?	[R1]/3.4.4, 3.6.1.10	M	ZigBee	M		
				ZigBee-PRO	M		Y
NCF103	Does the device support the origination of route record command frames?	[R1]/3.4.5, 3.6.3.5.4	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF104	Does the device support the receipt of route record command frames?	[R1]/3.4.5, 3.6.3.5.4	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF105	Does the device support the relaying of route record command frames?	[R1]/3.4.5, 3.6.3.5.4	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NCF106	Does the device support the transmission of rejoin request command frames?	[R1]/3.4.6, 3.7.1.3.2.1	FDT1:X FDT2:M FDT3:M	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
NCF107	Does the device support the reception of rejoin request command frames?	[R1]/3.4.6, 3.7.1.3.2.2	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF108	Does the device support the transmission of rejoin response command frames?	[R1]/3.4.7, 3.7.1.3.2.2	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
NCF109	Does the device support the reception of rejoin response command frames?	[R1]/3.4.7, 3.7.1.3.2.1	FDT1: X FDT2: M FDT3: M	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y

ZigBee™ Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NCF110	Does the device support the generation of a network report command frame.	[R1]/3.4.9, 3.6.1.13.1	O	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
NCF111	Does the device support the reception of a network report command frame	[R1]/3.4.9, 3.6.1.13.2	O	ZigBee	FDT1: O FDT2: O FDT3: X	While this feature is optional, one device in the network must be designated as the network manager and for that device this feature is mandatory.	
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		Y
NCF112	Does the device support the generation of a network update command frame.	[R1]/3.4.10, 3.6.1.13.2	O	ZigBee	FDT1: O FDT2: O FDT3: X	While this feature is optional, one device in the network must be designated as the network manager and for that device this feature is mandatory.	
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		Y
NCF113	Does the device support the reception of a network update command frame	[R1]/3.4.10, 3.6.1.13.3	O	ZigBee	FDT1: M FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: M		Y
NCF114	Does the device support the generation of a link status command frame.	[R1]/3.4.8, 3.6.3.4.1	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NCF115	Does the device support the reception of a link status command frame.	[R1]/3.4.8, 3.6.1.5, 3.6.3.4.2	FDT1: O FDT2: O FDT3: X	ZigBee	X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

8.5 Security PICS

8.5.1 ZigBee security roles

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
SR1	Is this device capable of acting in the role of a trust center?	[R1]/1.4, 4.6.2	FDT1: M FDT2: O FDT3: X	ZigBee	FDT1: M FDT2: O FDT3: X	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 apsTrust-CenterAddress 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 apsTrust-CenterAddress. It is possible, under application control, to change apsTrustCenter-Address during later network operation, however, it is the application's responsibility to ensure that all devices in the network are notified of the change.	
				ZigBee-PRO	FDT1: M FDT2: O FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 ### 8.5.2 ZigBee trust center capabilities

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
TCC1	Is this device capable of acting as a ZigBee trust center in high security mode?	[R1]/1.4.1.2, 4.6.2.1	SR1:O.2	ZigBee	X		
				ZigBee-PRO	SR1: O.2	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. At least one of TCC1 or TCC2 must be supported if the device supports SR1.	N
TCC2	Is this device capable of acting as a ZigBee trust center in standard mode?	[R1]/1.4.1.2, 4.6.2.2	SR1:O.2	ZigBee	M		
				ZigBee-PRO	SR1: O.2	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. At least one of TCC1 or TCC2 must be supported if the device supports SR1.	Y

2

3

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 **8.5.3 Modes of operation**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
MOO1	Is this device capable of operating in a network secured with a trust center running in high security mode?	[R1]/1.4.1.2, 4.6.2.1	O.3	ZigBee	X		
				ZigBee-PRO	O.3	A PRO device shall join a PRO network either running in Standard or High Security mode. At least one of MOO1 or MOO2 must be supported.	N
MOO2	Is this device capable of operating in a network secured with a trust center running in standard mode?	[R1]/1.4.1.2,	O.3	ZigBee	M		
				ZigBee-PRO	O.3	A PRO device shall join a PRO network either running in Standard or High Security mode. At least one of MOO1 or MOO2 must be supported.	Y

2

3 **8.5.4 Security levels**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
SL1	Is this device capable of supporting security level 0x01?	[R1]/4.5.1.1.1	O.4	ZigBee	X	The device shall not apply security to outgoing frames or accept secured incoming frames using any level other than level 0x05.	
				ZigBee-PRO	X		
SL2	Is this device capable of supporting security level 0x02?	[R1]/4.5.1.1.1	O.4	ZigBee	X	The device shall not apply security to outgoing frames or accept secured incoming frames using any level other than level 0x05.	
				ZigBee-PRO	X		

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
SL3	Is this device capable of supporting security level 0x03?	[R1]/4.5.1.1.1	O.4	ZigBee	X	The device shall not apply security to outgoing frames or accept secured incoming frames using any level other than level 0x05.	
				ZigBee-PRO	X		
SL4	Is this device capable of supporting security level 0x04?	[R1]/4.5.1.1.1	O.4	ZigBee	X	The device shall not apply security to outgoing frames or accept secured incoming frames using any level other than level 0x05.	
				ZigBee-PRO	X		
SL5	Is this device capable of supporting security level 0x05?	[R1]/4.5.1.1.1	O.4	ZigBee	M	The device shall apply security to outgoing frames or accept secured incoming frames using only level 0x05 (i.e., ENC-MIC-32)	
				ZigBee-PRO	M		Y
SL6	Is this device capable of supporting security level 0x06?	[R1]/4.5.1.1.1	O.4	ZigBee	X	The device shall not apply security to outgoing frames or accept secured incoming frames using any level other than level 0x05.	
				ZigBee-PRO	X		
SL7	Is this device capable of supporting security level 0x07?	[R1]/4.5.1.1.1	O.4	ZigBee	X	The device shall not apply security to outgoing frames or accept secured incoming frames using any level other than level 0x05.	
				ZigBee-PRO	X		

1

2

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 **8.5.5 NWK layer security**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLS1	Does the device support the security processing of NWK layer outgoing frames?	[R1]/4.3.1.1	M	ZigBee	M		
				ZigBee-PRO	M		Y
NLS2	Does the device support the security processing of NWK layer incoming frames?	[R1]/4.3.1.2	M	ZigBee	M		
				ZigBee-PRO	M		Y
NLS3	Does the device support the ZigBee secured NWK layer frame format?	[R1]/4.3.1	M	ZigBee	M		
				ZigBee-PRO	M		Y
NLS4	Does the device support the ability to manage at least one network key and corresponding outgoing frame counter?	[R1]/4.2.1.3, 4.3.3	M	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLS5	Does the device support the ability to manage two network keys and corresponding outgoing frame counter?	[R1]/4.2.1.3, 4.3.1, 4.3.3	O	ZigBee	M	All devices shall maintain at least 2 NWK keys with the frame counters consistent with the security mode of the network (Standard or High). 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.	
				ZigBee-PRO	M		Y
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)?	[R1]/4.2.1.3, 4.3.1, 4.3.3	O	ZigBee	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.	
				ZigBee-PRO	M		Y
NLS8	Does the device support a setting to indicate that all incoming NWK frames must be checked for freshness (i.e., *nwkAllFresh*).	[R1]/4.4.1.2, 4.6.2.1, 4.6.2.2	MOO1: M MOO2: O	ZigBee	MOO1: M MOO2: O	See also the trust centre policies document [R4].	
				ZigBee-PRO	MOO1: M MOO2: O		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
NLS9	Does the device support the ability to secure all incoming and outgoing NWK frames (i.e., the *nwkSecureAllFrames* attribute of the NIB)?	[R1]/4.2.3, 4.6	O	ZigBee	M	Devices using the ZigBee and ZigBee-PRO feature sets shall set: nwkSecureAllFrames = TRUE	
				ZigBee-PRO	M		Y
NLS10	Does the device support the ability to reject frames from neighbors which have not been properly authenticated?	[R1]/4.2.3, 4.6	O	ZigBee	MOO1: M MOO2: O	Coordinator and Router devices employing ZigBee and ZigBee PRO Standard Mode security shall not reject frames from neighbors which have not been properly authenticated. Coordinator and Router devices employing ZigBee PRO High Security shall reject frames from neighbors which have not been properly authenticated.	
				ZigBee-PRO	MOO1: M MOO2: O		Y

1

2 ### 8.5.6 APS layer security

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ASLS1	Does the device support the security processing of APS layer outgoing frames?	[R1]/4.4.1.1	M	ZigBee	M		
				ZigBee-PRO	M		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ASLS2	Does the device support the security processing of APS layer incoming frames?	[R1]/4.4.1.2	M	ZigBee	M		
				ZigBee-PRO	M		Y
ASLS3	Does the device support the ZigBee secured APS layer frame format?	[R1]/4.4.7.3	M	ZigBee	M		
				ZigBee-PRO	M		Y
ASLS4	Does the device support the ability to manage trust center master keys?	[R1]/4.4.3, 4.4.10, 4.6.3	O	ZigBee	MOO1: M MOO2: O	In ZigBee and 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.	
				ZigBee-PRO	MOO1: M MOO2: O		N
ASLS5	Does the device support the ability to manage application master keys?	[R1]/4.2.3.5, 4.4.3, 4.4.6, 4.4.10, 4.6.3.5	O	ZigBee	O	In ZigBee and ZigBee PRO Standard and ZigBee PRO High security modes, application master keys are optional for all devices.	
				ZigBee-PRO	O		N
ASLS6	Does the device support the ability to manage application data keys and corresponding security material (e.g., the incoming and outgoing frame counters)?	[R1]/4.2.1.3, 4.4.1, 4.4.10	O	ZigBee	O		
				ZigBee-PRO	O		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ASLS7	Does the device support network key incoming frame counters for incoming APS layer frames secured with the network key?	[R1]/4.4.1.2, 4.3.3	O	ZigBee	X	ZigBee and ZigBee PRO Standard Mode or ZigBee-PRO High Mode security use nwkSecure-AllFrames=TRUE, the APS security header is not employed when the network key is used for incoming APS layer frames.	
				ZigBee-PRO	X		
ASLS8	Does the device support establish-key service using the Symmetric-Key Key Establishment (SKKE) protocol?	[R1]/4.2.3.1, 4.4.2, 4.4.9.1	O	ZigBee	MOO1: M MOO2: O	In ZigBee and ZigBee PRO Standard Mode security, SKKE is optional for all devices. In ZigBee PRO High Security, SKKE is mandatory for all devices.	
				ZigBee-PRO	MOO1: M MOO2: O		N
ASLS9	Does the device support the origination of transport-key commands?	[R1]/4.2.3.2, 4.4.3, 4.4.9.2	SR1: M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ASLS10	Does the device support the receipt of transport-key commands?	[R1]/4.2.3.2, 4.4.3, 4.4.9.2	O	ZigBee	M	A newly joined device in ZigBee or ZigBee PRO Standard and ZigBee PRO High Security shall be capable of receiving the NWK key from the trust center via transport-key commands.	
				ZigBee-PRO	M		Y
ASLS11	Does the device support the origination of update-device commands?	[R1]/4.2.3.3, 4.4.4, 4.4.9.3	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ASLS12	Does the device support the receipt of update-device commands?	[R1]/4.2.3.3, 4.4.4, 4.4.9.3	SR1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ASLS13	Does the device support the origination of remove-device commands?	[R1]/4.2.3.4, 4.4.5, 4.4.9.4	SR1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ASLS14	Does the device support the receipt of remove-device commands?	[R1]/4.2.3.4, 4.4.5, 4.4.9.4	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X	The trust center shall be able to ask a ZigBee router or the ZigBee coordinator to request that a child device leave the network.	
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
ASLS15	Does the device support the origination of request-key commands?	[R1]/4.2.3.5, 4.4.6, 4.4.9.5	O	ZigBee	O		
				ZigBee-PRO	O		N
ASLS16	Does the device support the receipt of request-key commands?	[R1]/4.2.3.5, 4.4.6, 4.4.9.5	SR1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ASLS17	Does the device support origination of switch-key commands?	[R1]/4.2.3.6, 4.4.7, 4.4.9.6	SR1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ASLS18	Does the device support receipt of switch-key commands?	[R1]/4.2.3.6, 4.4.7, 4.4.9.6	O	ZigBee	M		
				ZigBee-PRO	M		Y
ASLS19	Does the device support origination of tunnel commands?	[R1]/4.4.3.1, 4.4.9.8	SR1:M	ZigBee	MOO1: M MOO2: O	In ZigBee and ZigBee PRO Standard security, the ability to originate tunnel commands from the Trust Center is optional unless using link keys. In ZigBee PRO High Security, it is mandatory.	
				ZigBee-PRO	MOO1: M MOO2: O		Y
ASLS20	Does the device support receipt of tunnel commands?	[R1]/4.4.3.1, 4.4.9.8	O	ZigBee	MOO2: FDT1: O FDT2: O FDT3: X	In ZigBee and ZigBee PRO Standard and High security, the ability for the coordinator and all routers to receive tunnel commands is mandatory.	
				ZigBee-PRO	MOO1: FDT1: M FDT2: M FDT3: X MOO2: FDT1: O FDT2: O FDT3: X		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ASLS21	Does the device support the authentication service using the entity authentication protocol?	[R1]/4.2.3.7, 4.4.8, 4.4.9.7	O	ZigBee	MOO2: FDT1: O FDT2: O FDT3: X	In ZigBee and 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.	
				ZigBee-PRO	MOO1: FDT1: M FDT2: M FDT3: X MOO2: FDT1: O FDT2: O FDT3: X		N

1 ### 8.5.7 Application layer security

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALS1	Is this device capable of learning and maintaining knowledge of its trust center using the *apsTrust-CenterAddress* attribute in the AIB?	[R1]/4.4.10, 4.6.1	O	ZigBee	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.	
				ZigBee-PRO	M		Y
ALS2	Is this device capable of following the “joining a secure network procedure” in the role of a router?	[R1]/4.6.3.1	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALS3	Is this device capable of following the "joining a secure network procedure" in the role of a joining device?	[R1]/4.6.3.1	O	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
ALS4	Is this device capable of following the "authentication procedure" in the role of a trust center?	[R1]/4.6.3.2, 4.6.3.2.2.1	TCC1: O TCC2: O	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ALS5	Is this device capable of following the "authentication procedure" in the role of a router?	[R1]/4.6.3.2, 4.6.3.2.1	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
ALS6	Is this device capable of following the "authentication procedure" in the role of a joining device with a preconfigured network key?	[R1]/4.6.3.2, 4.6.3.2.3.1	O	ZigBee	O	For devices implementing ZigBee and 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.	
				ZigBee-PRO	O		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALS7	Is this device capable of following the "authentication procedure" in the role of a joining device with a preconfigured trust center link key?	[R1]/4.6.3.2, 4.6.3.2.3.2	O	ZigBee	O	For devices implementing ZigBee and ZigBee PRO Standard Security, following the "authentication procedure" in the role of joining device with a pre-configured trust center link 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 master key.	
				ZigBee-PRO	O		N
ALS8	Is this device capable of following the "authentication procedure" in the role of a joining device without preconfigured network or trust center link keys?	[R1]/4.6.3.2, 4.6.3.2.3.3	O	ZigBee	O	For devices implementing ZigBee and ZigBee PRO Standard Security, following the "authentication procedure" in the role of joining device without a pre-configured trust center link key is optional and supported by default due to the requirement to permit ZigBee 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 master key.	
				ZigBee-PRO	O		N
ALS9	Is this device capable of following the "network key update procedure" in the role of a trust center?	[R1]/4.6.3.4, 4.6.3.4.1	TCC1: O TCC2: O	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALS10	Is this device capable of following the “network key update procedure” in the role of a network device?	[R1]/4.6.3.4, 4.6.3.4.2	O	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
ALS11	Is this device capable of following the “network key recovery procedure” in the role of a trust center?		TCC1:O.1 TCC2:O.1	ZigBee	X	This item was deprecated.	
				ZigBee-PRO	X		
ALS12	Is this device capable of following the “network key recovery procedure” in the role of a network device?		O	ZigBee	X	This item was deprecated.	
				ZigBee-PRO	X		
ALS13	Is this device capable of following the “end-to-end application key establishment procedure” in the role of a trust center?	[R1]/4.6.3.5, 4.6.3.5.2	TCC1: O TCC2: O	ZigBee	SR1: O	For ZigBee and 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.	
				ZigBee-PRO	SR1: O		N
ALS14	Is this device capable of following the "end-to-end application key establishment procedure" in the role of a device receiving a master key for use with the SKKE protocol?	[R1]/4.6.3.5, 4.6.3.5.1, 4.6.3.5.1.2	O	ZigBee	O	For ZigBee and ZigBee PRO Standard Security and ZigBee PRO High Security, it is optional for the network devices to perform the “end-to-end application key establishment” procedure.	
				ZigBee-PRO	O		N
ALS15	Is this device capable of following the “end-to-end application key establishment procedure” in the role of a device directly receiving a link key?	[R1]/4.6.3.5, 4.6.3.5.1, 4.6.3.5.1.1	O	ZigBee	O	For ZigBee and ZigBee PRO Standard Security and ZigBee PRO High Security, it is optional for the network devices to perform the “end-to-end application key establishment” procedure.	
				ZigBee-PRO	O		N

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALS16	Is this device capable of following the "network leave procedure" in the role of a trust center?	[R1]/4.6.3.6, 4.6.3.6.1	TCC1: O TCC2: O	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ALS17	Is this device capable of following the "network leave procedure" in the role of a router?	[R1]/4.6.3.6, 4.6.3.6.2	FDT1:O, FDT2:O, FDT3:X	ZigBee	FDT1: X FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: X		Y
ALS18	Is this device capable of following the "network leave procedure" in the role of a leaving device?	[R1]/4.6.3.6, 4.6.3.6.3	O	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
ALS19	Is this device capable of following the "intra-PAN portability procedure" in the role of a parent?	[R1]/4.6.3.3, 4.6.3.3.1	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
ALS20	Is this device capable of following the "intra-PAN portability procedure" in the role of an end device?	[R1]/4.6.3.3, 4.6.3.3.2	O	ZigBee	FDT1: X FDT2: X FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: M		Y
ALS21	Is this device capable of following the "command tunneling procedure" in the role of a trust center device?	[R1]/4.6.3.8, 4.6.3.8.1	TCC1: O TCC2: O	ZigBee	SR1: O	For ZigBee PRO High Security, the command tunneling procedure in the role of a trust center device is mandatory. For ZigBee and ZigBee PRO Standard Security, it is optional.	
				ZigBee-PRO	SR1: O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALS22	Is this device capable of following the "command tunneling procedure" in the role of a router?	[R1]/4.6.3.8, 4.6.3.8.2	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: O FDT2: O FDT3: X	For ZigBee PRO High Security, the command tunneling procedure in the role of a router device is mandatory. For ZigBee and ZigBee PRO Standard Security, it is optional.	
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		N
ALS23	Does the device support the permissions configuration table?	[R1]/4.2.3.8, 4.6.3.8	O	ZigBee	O	The Permissions Configuration Table is optional for all devices.	
				ZigBee-PRO	O		Y

1

2 8.6 Application layer PICS

3 8.6.1 ZigBee security device types

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
SDT1	Is this device capable of acting as a ZigBee Trust Center?	[R1]/4.2.4, 4.6.2	O.2	ZigBee	FDT1: M FDT2: O FDT3: X	This item was deprecated in favor of SR1.	
				ZigBee-PRO	FDT1: M FDT2: O FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
SDT2	Is this device capable of joining a secure ZigBee network only as a device?	[R1]/4.6.3	O.2	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y

1

2 ### 8.6.2 ZigBee APS frame format

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AFF1	Does the device support the general ZigBee APS frame format?	[R1]/2.2.5.1	M	ZigBee	M		
				ZigBee-PRO	M		Y
AFF2	Does the device support the ZigBee APS data frame format?	[R1]/2.2.5.2.1	M	ZigBee	M		
				ZigBee-PRO	M		Y
AFF3	Does the device support the ZigBee APS command frame format?	[R1]/2.2.5.2.2, 2.2.6	O	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AFF4	Does the device support the ZigBee APS acknowledgement frame format?	[R1]/2.2.5.2.3	M	ZigBee	M		
				ZigBee-PRO	M		Y

1

2 **8.6.3 Major capabilities of the ZigBee application layer**

3 *Tables in the following subclauses detail the capabilities of the APL layer for ZigBee devices.*

4 **8.6.3.1 Application layer functions**

5 **8.6.3.1.1 Application Support Sub-layer functions**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALF1	Does the application support sub-layer support transmission of data by the next higher layer?	[R1]/2.2.4.1.1 , 2.2.4.1.2	M	ZigBee	M		
				ZigBee-PRO	M		Y
ALF200	Does the device support transmission of outgoing APS frames within APSDE with the DstAddrMode set to 0x00 (indirect)	[R1]/2.2.4.1.1	O	ZigBee	X	This must be handled by the application.	
				ZigBee-PRO	X		
ALF201	Does the device support transmission of outgoing APS frames within APSDE with the DstAddrMode set to 0x01 (group addressed)	[R1]/2.2.4.1.1	M	ZigBee	M		
				ZigBee-PRO	M		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALF202	Does the device support transmission of outgoing APS frames within APSDE with the DstAddrMode set to 0x02 (unicast using NWK address and Destination Endpoint)	[R1]/2.2.4.1.1	M	ZigBee	M		
				ZigBee-PRO	M		Y
ALF203	Does the device support transmission of outgoing APS frames within APSDE with the DstAddrMode set to 0x03 (unicast using IEEE address and Destination Endpoint)	[R1]/2.2.4.1.1	O	ZigBee	O		
				ZigBee-PRO	O		Y
ALF2	Does the application support sub-layer support reception of data by the next higher layer at the endpoint supplied by the incoming packet?	[R1]/2.2.4.1.3	M	ZigBee	M		
				ZigBee-PRO	M		Y
ALF300	Does the device support reception of incoming APS frames within APSDE with the DstAddrMode set to 0x00 (indirect)	[R1]/2.2.4.1.3	O	ZigBee	X		
				ZigBee-PRO	X		
ALF301	Does the device support reception of incoming APS frames within APSDE with the DstAddrMode set to 0x01 (group addressed)	[R1]/2.2.4.1.3	M	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALF302	Does the device support reception of incoming APS frames within APSDE with the DstAddrMode set to 0x02 (unicast using NWK address and Destination Endpoint)	[R1]/2.2.4.1.3	M	ZigBee	M		
				ZigBee-PRO	M		Y
ALF3	Does the application support sub-layer support BIND and UNBIND requests and confirms?	[R1]/2.2.4.3.1, 2.2.4.3.2, 2.2.4.3.3, 2.2.4.3.4	O	ZigBee	O	Binding support is optional for all devices, except that: • Source binding only is supported (coordinator based binding is disallowed) • All devices shall minimally respond with NOT_IMPLEMENTED	
				ZigBee-PRO	O	The ZigBee Coordinator shall implement the mechanism for matching end device bind requests (AZD24; FDT1: M).	N
ALF4	Does the device's application support sub- layer offer the next higher layer the ability to get application information base (AIB) attributes.	[R1]/2.2.4.4.1, 2.2.4.4.2	M	ZigBee	M		
				ZigBee-PRO	M		Y
ALF5	Does the device's application support sub- layer offer the next higher layer the ability to set application information base (AIB) attributes.	[R1]/2.2.4.4.3, 2.2.4.4.4	M	ZigBee	M		
				ZigBee-PRO	M		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ALF100	Does the application support sub-layer support ADD GROUP requests and confirms?	[R1]/2.2.4.5.1, 2.2.4.5.2	M	ZigBee	O	If supported, the group table in the APS shall contain a minimum of 16 group addresses.	
				ZigBee-PRO	O		Y
ALF101	Does the application support sub-layer support REMOVE GROUP requests and confirms?	[R1]/ 2.2.4.5.3, 2.2.4.5.4	M	ZigBee	O		
				ZigBee-PRO	O		Y
ALF102	Does the application support sub-layer support REMOVE ALL GROUPS requests and confirms?	[R1]/ 2.2.4.5.5, 2.2.4.5.6	M	ZigBee	O		
				ZigBee-PRO	O		Y

1

2 ### 8.6.3.1.2 Application layer frames

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ADF1	Does the device support the origination of application data frames.	[R1]/2.2.5.1, 2.2.5.2.1, 2.2.8.4.1	M	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ADF2	Does the device support the receipt of application data frames.	[R1]/2.2.5.1 2.2.5.2.1, 2.2.8.3.2, 2.2.8.3.3	M	ZigBee	M		
				ZigBee-PRO	M		Y
ADF3	Does the device support the origination of application data frames with the auxiliary APS security header?	[R1]/ 2.2.5.1, 2.2.5.2.1, 2.2.8.4.1, 4.4.1.1	O	ZigBee	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.	
				ZigBee-PRO	O		N
ADF4	Does the device support the receipt of application data frames with the auxiliary APS security header?	[R1]/ 2.2.5.1 2.2.5.2.1, 2.2.8.3.2, 2.2.8.3.3, 4.4.1.2	O	ZigBee	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.	
				ZigBee-PRO	O		N
ADF5	Does the device support the origination of application data frames with the extended APS fragmentation/re-assembly header?	[R1]/ 2.2.5.1, 2.2.5.2.1, 2.2.8.4.1, 2.2.5.1.8, 2.2.8.4.5.1	O	ZigBee	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.	
				ZigBee-PRO	O	Devices using the ZigBee and ZigBee-PRO feature sets shall set: *Config_Max_ZDO-_Payload = 0* (i.e. for compatibility with the earlier ZigBee feature set, ZDO messages shall not be fragmented)	Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ADF6	Does the device support the receipt of application data frames with the extended APS fragmentation/re-assembly header?	[R1]/ 2.2.5.1 2.2.5.2.1, 2.2.8.3.2, 2.2.8.3.3, 2.2.5.1.8, 2.2.8.4.5.2	O	ZigBee	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 and ZigBee-PRO feature sets shall set: *Config_Max_ZDO-_Payload = 0* (i.e. for compatibility with the earlier ZigBee feature set, ZDO messages shall not be fragmented)	
				ZigBee-PRO	O		Y

1 ### 8.6.3.1.3 Application layer command frames

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ACF500	Does the device support the origination of command frames with the auxiliary APS security header?	[R1]/ 2.2.5.1, 2.2.5.2.2, 2.2.6, 4.4.1.1	O	ZigBee	O		
				ZigBee-PRO	O		N
ACF501	Does the device support the receipt of command frames with the auxiliary APS security header?	[R1]/ 2.2.5.1 2.2.5.2.1, 2.2.6, 2.2.8.3.3, 4.4.1.2	O	ZigBee	O		
				ZigBee-PRO	O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ACF1	Does the device support the origination of application command frames from the Trust Center.	[R1]/4.4.9, 4.6.2, 4.6.3.2, 4.6.3.3, 4.6.3.4, 4.6.3.5, 4.6.3.6, 4.6.3.7	SDT1: M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ACF100	Does the device support the origination of Key Establishment application command frames from the Trust Center?	[R1]/4.4.9.1	SDT1:M	ZigBee	SR1: O	In ZigBee and 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.	
				ZigBee-PRO	SR1: O		N
ACF101	Does the device support the origination of Transport Key application command frames from the Trust Center?	[R1]/4.4.9.2	SDT1:M	ZigBee	SR1: M	In ZigBee and 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 and 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).	
				ZigBee-PRO	SR1: M		Y

ZigBee™ Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ACF102	Does the device support the origination of Remove Device application command frames from the Trust Center?	[R1]/4.4.9.4	SDT1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ACF103	Does the device support the origination of Switch Key application command frames from the Trust Center?	[R1]/4.4.9.6	SDT1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ACF104	Does the device support the origination of entity authentication application command frames?	[R1]/4.4.9.7	SDT1:M	ZigBee	SR1: O		
				ZigBee-PRO	MOO2: O MOO1: M		N
ACF2	Does the device support the receipt of application command frames at the Trust Center	[R1]/4.4.9, 4.6.2, 4.6.3.2, 4.6.3.3, 4.6.3.4, 4.6.3.5, 4.6.3.6, 4.6.3.7	SDT1:M	ZigBee	SR1: M	Mandatory for the trust centre and optional for other devices.	
				ZigBee-PRO	SR1: M		Y
ACF200	Does the device support the receipt of Key Establishment application command frames at the Trust Center?	[R1]/4.4.9.1	SDT1:M	ZigBee	SR1: O	In ZigBee and 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.	
				ZigBee-PRO	SR1: O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ACF201	Does the device support the receipt of Transport Key application command frames at the Trust Center?	[R1]/4.4.9.2	SDT1:M	ZigBee	SR1: M	In ZigBee and 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 and 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).[4]	
				ZigBee-PRO	SR1: M		Y
ACF202	Does the device support the receipt of Update Device application command frames at the Trust Center?	[R1]/4.4.9.3	SDT1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ACF203	Does the device support the receipt of Request Key application command frames at the Trust Center?	[R1]/4.4.9.5	SDT1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y

[4] CCB 873

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ACF204	Does the device support the receipt of entity authentication application command frames?	[R1]/4.4.9.7	SDT1:M	ZigBee	X		
				ZigBee-PRO	MOO1: M MOO2: O		N
ACF3	Does the device support the origination of application command frames from a non-Trust Center device.	[R1]/4.4.9, 4.6.3	SDT2:M	ZigBee	FDT1: X FDT2: M FDT3: O	In ZigBee and 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.	
				ZigBee-PRO	MOO1: FDT1: X FDT2: M FDT3: M MOO2: FDT1: X FDT2: M FDT3: O		Y
ACF300	Does the device support the origination of Key Establishment application command frames from a non-Trust Center device?	[R1]/4.4.9.1, 4.6.3.5	SDT2:M	ZigBee	O	In ZigBee and 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.	
				ZigBee-PRO	O		N
ACF301	Does the device support the origination of Transport Key application command frames from a non-Trust Center device?	[R1]/4.4.9.2	SDT2:M	ZigBee	O		
				ZigBee-PRO	O		N
ACF302	Does the device support the origination of Update Device application command frames from a non-Trust Center device?	[R1]/4.4.9.3, 4.6.3.4	SDT2:M	ZigBee	FDT1: M FDT2: M FDT3: O	Assumes it is legal to have the Trust Center on a non-ZigBee Coordinator device for the ZigBee feature set via ZigBee-2007	
				ZigBee-PRO	FDT1: M FDT2: M FDT3: O		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ACF303	Does the device support the origination of Request Key application command frames from a non-Trust Center device?	[R1]/4.4.9.5	SDT2:M	ZigBee	O		
				ZigBee-PRO	O		Y
ACF304	Does the device support the origination of Authenticate application command frames from a non-Trust Center device?	[R1]/4.4.9.7, 4.6.3.2	SDT2:M	ZigBee	O		
				ZigBee-PRO	O		N
ACF4	Does the device support the receipt of application command frames from a non-Trust Center device.	[R1]/4.4.9, 4.6.3	SDT1:M, SDT2:M	ZigBee	SR1: FDT1: M FDT2: M FDT3: O	In all ZigBee and ZigBee PRO security modes, the Trust Center shall receive application command frames from non Trust Center devices. In ZigBee and 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.	
				ZigBee-PRO	SR1: FDT1: M FDT2: M FDT3: O		Y
ACF400	Does the device support the receipt of Key Establishment application command frames from a non-Trust Center device?	[R1]/4.4.9.1, 4.6.3.5	SDT1:M, SDT2:M	ZigBee	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.	
				ZigBee-PRO	O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
ACF401	Does the device support the receipt of Transport Key application command frames from a non-Trust Center device?	[R1]/4.4.9.2	SDT1:M, SDT2:M	ZigBee	SR1: M SDT2: M		
				ZigBee-PRO	SR1: M SDT2: M		Y
ACF402	Does the device support the receipt of Update Device application command frames from a non-Trust Center device?	[R1]/4.4.9.3, 4.6.3.4	SDT1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ACF403	Does the device support the receipt of Request Key application command frames from a non-Trust Center device?	[R1]/4.4.9.5	SDT1:M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
ACF404	Does the device support the receipt of entity authenticate application command frames from a non-Trust Center device?	[R1]/4.4.9.7, 4.6.3.2	SDT1:M SDT2:M	ZigBee	O	Need a comment that this feature is optional in ZigBee and ZigBee PRO Standard Security and mandatory for all devices in ZigBee PRO High Security.	
				ZigBee-PRO	O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

1 **8.6.3.1.4 Application acknowledgement frames**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AFR1	Does the device support the origination of application acknowledgement frames.	[R1]/2.2.8.3.1, 2.2.8.3.3	M	ZigBee	M		
				ZigBee-PRO	M		Y
AFR2	Does the device support the receipt of application acknowledgement frames?	[R1]/2.2.8.3.2, 2.2.8.3.3	M	ZigBee	M		
				ZigBee-PRO	M		Y

2 **8.6.3.1.5 ZigBee Device Objects functions**

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD700	Does the device support the permissions configuration table?	[R1]/4.6.3.8	O	ZigBee	O		
				ZigBee-PRO	O		Y
AZD701	Does the device support the ModifyPermissionsCapabilityTable element of the permissions configuration table?	[R1]/4.6.3.8	AZD700: O	ZigBee	AZD700: O		
				ZigBee-PRO	AZD700: O		N

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD702	Does the device support the NetworkSettings element of the permissions configuration table?	[R1]/4.6.3.8	AZD700: O	ZigBee	AZD700: O		
				ZigBee-PRO	AZD700: O		N
AZD703	Does the device support the Application-Settings element of the permissions configuration table?	[R1]/4.6.3.8	AZD700: O	ZigBee	AZD700: O		
				ZigBee-PRO	AZD700: O		N
AZD704	Does the device support the SecuritySettings element of the permissions configuration table?	[R1]/4.6.3.8	AZD700: O	ZigBee	AZD700: O		
				ZigBee-PRO	AZD700: O		N
AZD705	Does the device support the Application-Commands element of the permissions configuration table?	[R1]/4.6.3.8	AZD700: O	ZigBee	AZD700: O		
				ZigBee-PRO	AZD700: O		N
AZD706	Does the device support the SKKEWith-MasterKey element of the permissions configuration table?	[R1]/4.6.3.8	AZD700: O	ZigBee	AZD700: O		
				ZigBee-PRO	AZD700: O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD707	Does the device support the NWK rejoin procedure?	[R1]/ 3.6.1.4.2	M	ZigBee	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.	
				ZigBee-PRO	M		Y
AZD600	Does the device act as a Binding Table Cache?	[R1]/2.5.5.5.3	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: O FDT2: O FDT3: X		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		N
AZD601	Does the device perform the Intra-PAN portability parent procedure?	[R1]/2.5.5.5.4	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
AZD602	Does the device perform the Intra-PAN portability child procedure?	[R1]/2.5.5.5.4	FDT1: X FDT2: X FDT3: M	ZigBee	FDT1: X FDT2: X FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: M		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD603	Does the device support the Configuration Parameters, Startup Procedures and Additional Configuration Parameters?	[R1]/2.5.5.5.6.1, 2.5.5.5.6.2, 2.5.5.5.6.3	O	ZigBee	O	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.	
				ZigBee-PRO	M		Y
AZD1	Does the device support the mandatory Device and Service Discovery Object?	[R1]/2.5.5.6.1	M	ZigBee	M		
				ZigBee-PRO	M		Y
AZD2	Does the device support the mandatory attributes of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	M	ZigBee	M		
				ZigBee-PRO	M		Y
AZD3	Does the device support the optional attributes of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	O	ZigBee	O		
				ZigBee-PRO	O		Y
AZD4	Does the device support the optional NWK address client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD5	Does the device support the optional IEEE address client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD6	Does the device support the optional Node Descriptor client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD7	Does the device support the optional Power Descriptor client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD8	Does the device support the optional Simple Descriptor client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD9	Does the device support the optional Active Endpoint client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD10	Does the device support the optional Match Descriptor client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD11	Does the device support the optional Complex Descriptor client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD12	Does the device support the optional Complex Descriptor server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD13	Does the device support the optional User Descriptor client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD14	Does the device support the optional User Descriptor server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD17	Does the device support the mandatory Device Announce client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD1: M	ZigBee	M		
				ZigBee-PRO	M		Y
AZD18	Does the device support the Device Announce server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD1: M	ZigBee	M		
				ZigBee-PRO	M		Y
AZD100	Does the device support the optional System Server Discovery client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		Y
AZD101	Does the device support the optional System Server Discovery server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	SR1: M		Y
AZD102	Does the device support the optional Discovery Cache client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD103	Does the device support the optional Discovery Cache server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: FDT1: O FDT2: O FDT3: X		
				ZigBee-PRO	AZD3: FDT1: O FDT2: O FDT3: X		N
AZD104	Does the device support the optional Discovery Store client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD105	Does the device support the optional Discovery Store server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD103: M	ZigBee	AZD103: M		
				ZigBee-PRO	AZD103: M		Y
AZD106	Does the device support the optional Node Descriptor Store client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD107	Does the device support the optional Node Descriptor Store server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD103: M	ZigBee	AZD103: M		
				ZigBee-PRO	AZD103: M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD108	Does the device support the optional Power Descriptor Store client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD109	Does the device support the optional Power Descriptor Store server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD103: M	ZigBee	AZD103: M		
				ZigBee-PRO	AZD103: M		Y
AZD110	Does the device support the optional Active Endpoint Store client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD111	Does the device support the optional Active Endpoint Store server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD103: M	ZigBee	AZD103: M		
				ZigBee-PRO	AZD103: M		Y
AZD112	Does the device support the optional Simple Descriptor Store client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD113	Does the device support the optional Simple Descriptor Store server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD103: M	ZigBee	AZD103: M		
				ZigBee-PRO	AZD103: M		Y
AZD114	Does the device support the optional Remove Node Cache client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD115	Does the device support the optional Remove Node Cache server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD103: M	ZigBee	AZD103: M		
				ZigBee-PRO	AZD103: M		Y
AZD116	Does the device support the optional Find Node Cache client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD117	Does the device support the optional Find Node Cache server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD103: M	ZigBee	AZD103: M		
				ZigBee-PRO	AZD103: M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD650	Does the device support the optional Extended Simple Descriptor client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD651	Does the device support the optional Extended Simple Descriptor server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD103: M	ZigBee	AZD103: M		
				ZigBee-PRO	AZD103: M		Y
AZD652	Does the device support the optional Extended Active Endpoint client service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD3: O	ZigBee	AZD3: O		
				ZigBee-PRO	AZD3: O		N
AZD653	Does the device support the optional Extended Active Endpoint server service of the Device and Service Discovery Object?	[R1]/2.5.5.6.1	AZD103: M	ZigBee	AZD103: M		
				ZigBee-PRO	AZD103: M		Y
AZD19	Does the device support the optional Security Manager Object?	[R1]/2.5.5.7.1	O	ZigBee	M		
				ZigBee-PRO	M		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD20	Does the device support the mandatory attributes of the Security Manager Object with the device in a Trust Center role?	[R1]/2.5.5.7.1	AZD19: SDT1: M	ZigBee	SR1: M		
				ZigBee-PRO	SR1: M		Y
AZD21	Does the device support the mandatory attributes of the Security Manager Object with the device in a non-Trust Center role?	[R1]/2.5.5.7.1	AZD19: SDT2: M	ZigBee	SDT2: M		
				ZigBee-PRO	SDT2: M		Y
AZD22	Does the device support the optional Binding Manager Object?	[R1]/2.5.5.8.1	O	ZigBee	FDT1: M FDT2: O FDT3: O	End_Device_Bind_req server processing in the coordinator is required. 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.	
				ZigBee-PRO	FDT1: M FDT2: O FDT3: O		Y
AZD23	Does the device support the optional End Device Bind client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.1	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD24	Does the device support the optional End Device Bind server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.1	AZD22: FDT1: M FDT2: X FDT3: X	ZigBee	AZD22: FDT1: M FDT2: X FDT3: X		
				ZigBee-PRO	AZD22: FDT1: M FDT2: X FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD25	Does the device support the optional Bind client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.2	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD26	Does the device support the optional Bind server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.2	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD27	Does the device support the optional Unbind client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.3	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD28	Does the device support the optional Unbind server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.3	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD200	Does the device support the optional Bind Register client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.4	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD201	Does the device support the optional Bind Register server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.4	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD202	Does the device support the optional Replace Device client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.5	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD203	Does the device support the optional Replace Device server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.5	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD204	Does the device support the optional Store Backup Bind Entry client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.6	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD205	Does the device support the optional Store Backup Bind Entry server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.6	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD206	Does the device support the optional Remove Backup Bind Entry client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.7	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD207	Does the device support the optional Remove Backup Bind Entry server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.7	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD208	Does the device support the optional Backup Bind Table client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.8	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD209	Does the device support the optional Backup Bind Table server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.8	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD210	Does the device support the optional Recover Bind Table client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.9	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD211	Does the device support the optional Recover Bind Table server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.9	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD212	Does the device support the optional Backup Source Bind client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.10	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD213	Does the device support the optional Backup Source Bind server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.10	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD214	Does the device support the optional Recover Source Bind client service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.3.2.11	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N
AZD215	Does the device support the optional Recover Source Bind server service of the Binding Manager Object?	[R1]/2.5.5.8.1 [R1]/2.4.4.2.11	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD29	Does the device support the optional APSME BIND and UNBIND service of the Binding Manager Object?	[R1]/2.5.5.8.1	AZD22: FDT1: O FDT2: O FDT3: O	ZigBee	AZD22: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD22: FDT1: O FDT2: O FDT3: O		Y
AZD30	Does the device support the mandatory NLME GET, SET and NETWORK DISCOVERY services of the Network Manager Object?	[R1]/2.5.5.9.1	M	ZigBee	M		
				ZigBee-PRO	M		Y
AZD31	Does the device support the optional NLME NETWORK FORMATION service of the Network Manager Object?	[R1]/2.5.5.9.1	FDT1: M FDT2: X FDT3: X	ZigBee	FDT1: M FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: X FDT3: X		Y
AZD32	Does the device support the optional NLME JOIN service of the Network Manager Object?	[R1]/2.5.5.9.1	FDT1: X FDT2: M FDT3: M	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
AZD300	Does the device support the optional NLME START ROUTER service of the Network Manager Object?	[R1]/2.5.5.9.1	FDT1: X FDT2: M FDT3: X	ZigBee	FDT1: X FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: X		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD33	Does the device support the mandatory NLME LEAVE service of the Network Manager Object?	[R1]/2.5.5.9.1	FDT1: X FDT2: M FDT3: M	ZigBee	FDT1: X FDT2: M FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: M FDT3: M		Y
AZD301	Does the device support the optional NLME PERMIT JOINING service of the Network Manager Object?	[R1]/2.5.5.9.1	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
AZD34	Does the device support the optional NLME RESET service of the Network Manager Object?	[R1]/2.5.5.9.1	FDT1: O FDT2: O FDT3: O	ZigBee	FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: O		Y
AZD35	Does the device support the optional NLME SYNC service of the Network Manager Object?	[R1]/2.5.5.9.1	FDT1: O FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: X FDT3: M	See clause 8.4.2.1 in this document, Network layer functions, Item number NLF17.	
				ZigBee-PRO	FDT1: X FDT2: X FDT3: M		N
AZD302	Does the device support the mandatory NLME NWK_STATUS service of the Network Manager Object?	[R1]/2.5.5.9.1	M	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD303	Does the device support the optional NLME ROUTE DISCOVERY service of the Network Manager Object?	[R1]/2.5.5.9.1	FDT1: O FDT2: O FDT3: O	ZigBee	FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: O		Y
AZD36	Does the device support the optional Node Manager Object?	[R1]/2.5.5.10.1	FDT1: O FDT2: O FDT3: O	ZigBee	FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: O		Y
AZD37	Does the device support the optional Node Manager NWK Discovery client service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		N
AZD38	Does the device support the optional Node Manager NWK Discovery server service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: M FDT2: M FDT3: O		
				ZigBee-PRO	AZD36: FDT1: M FDT2: M FDT3: O		Y
AZD39	Does the device support the optional Node Manager LQI client service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		N

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD40	Does the device support the optional Node Manager LQI server service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: M FDT2: M FDT3: O		
				ZigBee-PRO	AZD36: FDT1: M FDT2: M FDT3: O		Y
AZD41	Does the device support the optional Node Manager RTG client service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		N
AZD42	Does the device support the optional Node Manager RTG server service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: M FDT2: M FDT3: O		Y
AZD43	Does the device support the optional Node Manager Bind client service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		N
AZD44	Does the device support the optional Node Manager Bind server service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD45	Does the device support the optional Node Manager Leave client service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		N
AZD46	Does the device support the optional Node Manager Leave server service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: M FDT2: M FDT3: O		
				ZigBee-PRO	AZD36: FDT1: M FDT2: M FDT3: O		Y
AZD47	Does the device support the optional Node Manager Direct Join client service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		N
AZD48	Does the device support the optional Node Manager Direct Join server service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	X		
				ZigBee-PRO	X		N
AZD400	Does the device support the optional Node Manager Permit Joining client service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	AZD36: FDT1: M FDT2: M FDT3: X		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD401	Does the device support the optional Node Manager Discovery Cache client service?	[R1]/2.5.5.10.1	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		N
AZD402	Does the device support the optional Node Manager Discovery Cache server service?	[R1]/2.5.5.10.2	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O		
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		N
AZD800	Does the device support the optional Node Manager NWK update client service?	[R1]/2.4.3.3.9	AZD36: FDT1: O FDT2: O FDT3: X	ZigBee	AZD36: FDT1: O FDT2: O FDT3: 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.	
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		Y
AZD801	Does the device support the optional Node Manager NWK update server service?	[R1]/2.4.4.3.9	AZD36: FDT1: O FDT2: O FDT3: O	ZigBee	AZD36: FDT1: O FDT2: O FDT3: O	The ability for a non Network Channel Manager to receive and process the Mgmt_NWK_Update_-req command is mandatory for the network manager and all routers and optional for end devices.	
				ZigBee-PRO	AZD36: FDT1: O FDT2: O FDT3: O		Y
AZD49	Does the device support the mandatory Configuration Attributes?	[R1]/2.5.6	M	ZigBee	M		
				ZigBee-PRO	M		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD50	Does the device support the optional Complex Descriptor configuration attribute?	[R1]/2.5.6	O	ZigBee	O		
				ZigBee-PRO	O		N
AZD51	Does the device support the optional User Descriptor configuration attribute?	[R1]/2.5.6	O	ZigBee	O		
				ZigBee-PRO	O		N
AZD52	Does the device support the optional Max Bind configuration attribute?	[R1]/2.5.6	O	ZigBee	O		
				ZigBee-PRO	O		N
AZD53	Does the device support the optional Master Key configuration attribute?	[R1]/2.5.6	O	ZigBee	O		
				ZigBee-PRO	O		N
AZD54	Does the device support the optional End Device Bind Timeout configuration attribute?	[R1]/2.5.6	FDT1: M FDT2: X FDT3: X	ZigBee	FDT1: M FDT2: X FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: X FDT3: X		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD55	Does the device support the optional Permit Join Duration configuration attribute?	[R1]/2.5.6	FDT1: M FDT2: M FDT3: X	ZigBee	FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	FDT1: M FDT2: M FDT3: X		Y
AZD56	Does the device support the optional NWK Security Level configuration attribute?	[R1]/2.5.6	AZD19: O	ZigBee	AZD19: O		
				ZigBee-PRO	AZD19: O		Y
AZD57	Does the device support the optional NWK Secure All Frames configuration attribute?	[R1]/2.5.6	AZD19: O	ZigBee	AZD19: O		
				ZigBee-PRO	AZD19: O		Y
AZD500	Does the device support the optional NWK Leave Remove Children configuration attribute?	[R1]/2.5.6	AZD19: FDT1: M FDT2: M FDT3: X	ZigBee	AZD19: FDT1: M FDT2: M FDT3: X		
				ZigBee-PRO	AZD19: FDT1: M FDT2: M FDT3: X		Y
AZD501	Does the device support the optional NWK Broadcast Delivery configuration attribute?	[R1]/2.5.6	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: O FDT2: O FDT3: X		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		Y

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD502	Does the device support the optional NWK Transaction Persistence Time configuration attribute?	[R1]/2.5.6	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: O FDT2: O FDT3: X		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		Y
AZD503	Does the device support the optional NWK Indirect Poll Rate configuration attribute?	[R1]/2.5.6	FDT1: X FDT2: X FDT3: M	ZigBee	FDT1: X FDT2: X FDT3: M		
				ZigBee-PRO	FDT1: X FDT2: X FDT3: M		N
AZD504	Does the device support the optional Max Associations configuration attribute?	[R1]/2.5.6	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: O FDT2: O FDT3: X		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		Y
AZD505	Does the device support the optional NWK Direct Join Addresses configuration attribute?	[R1]/2.5.6	FDT1: O FDT2: O FDT3: X	ZigBee	FDT1: O FDT2: O FDT3: X		
				ZigBee-PRO	FDT1: O FDT2: O FDT3: X		Y
AZD506	Does the device support the optional Parent Link Retry Threshold configuration attribute?	[R1]/2.5.6	FDT1: X FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: O FDT3: O		
				ZigBee-PRO	FDT1: X FDT2: O FDT3: O		Y

ZigBee Alliance
Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AZD507	Does the device support the optional Orphan Rejoin Interval configuration attribute?	[R1]/2.5.6	FDT1: X FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: O FDT3: O		
				ZigBee-PRO	FDT1: X FDT2: O FDT3: O		N
AZD508	Does the device support the optional Max Orphan Rejoin Interval configuration attribute?	[R1]/2.5.6	FDT1: X FDT2: O FDT3: O	ZigBee	FDT1: X FDT2: O FDT3: O		
				ZigBee-PRO	FDT1: X FDT2: O FDT3: O		N

1 ### 8.6.3.1.6 ZigBee Application Framework functions

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AAF2	Does the device support the mandatory ZigBee Descriptor structures?	[R1]/2.3.2	M	ZigBee	M		
				ZigBee-PRO	M		Y
AAF3	Does the device support the optional ZigBee Complex Descriptor structure?	[R1]/2.3.2	O	ZigBee	O		
				ZigBee-PRO	O		N
AAF4	Does the device support the optional ZigBee User Descriptor structure?	[R1]/2.3.2	O	ZigBee	O		
				ZigBee-PRO	O		N

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.

Item number	Item description	Reference	ZigBee Status	Feature set Support		Additional Constraints	Platform Support
AAF5	Does the device support the transmission of descriptors?	[R1]/2.3.2.1	M	ZigBee	M		
				ZigBee-PRO	M		Y

1

Copyright © 2008, The ZigBee Alliance. All rights reserved.
This is an unaccepted ZigBee specification draft, subject to change.