

IEEE Standard for Wireless Smart Utility Network Field Area Network (FAN)

Developed by the
IEEE SA Board of Governors Corporate Advisory Group (CAG)

IEEE Std 2857™-2021

IEEE Standard for Wireless Smart Utility Network Field Area Network (FAN)

Developed by the

Corporate Advisory Group (CAG)
of the
IEEE SA Board of Governors

Approved 16 June 2021

IEEE SA Standards Board

Abstract: This document describes a complete communications specification, encompassing layers 1 to 4 of the Open Systems Integration (OSI) network model, for a secure, wireless mesh communications network, using open standards communications and cybersecurity standards from standards organizations including Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force (IETF). The specification describes the functionality of the physical (PHY layer), medium access control (MAC layer), the network layer, transport layer and security parameters including certificate format for a highly scaleable and secure wireless mesh network for critical infrastructure ipv6 wireless communications networks.

Keywords: adoption, FAN, field area network, IEEE 2857, Internet of Things, IoT, OSI, smart city, smart utility network, Wi-SUN, wireless mesh

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 25 June 2021. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-7696-6 STD24793
Print: ISBN 978-1-5044-7697-3 STDPD24793

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE-SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#). An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#). For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#). Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant

has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

This IEEE standard is based on a technical specification developed by a consortium. Patent declarations may have been provided to the consortium as a membership requirement, or in compliance with the consortium's intellectual property rights (IPR) policies and procedures. Normative references in this standard may contain material subject to patent claims that are also subject to the consortium's or other organizations' IPR policies and procedures. Additional information about declarations may be available from the consortium's website:

Wi-SUN Alliance—<https://wi-sun.org>

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this IEEE standard was completed, the BOG/CAG/Wi-SUN Working Group had the following entity membership:

Gary Stuebing, *Chair*
Hiroshi Harada, *Vice Chair*
Philip E. Beecher, *Editor*
Thomas Herbst, *Secretary*

<i>Organization Represented</i>	<i>Name of Representative</i>
Wi-SUN Alliance.....	Philip E. Beecher
Cisco Systems, Inc.....	Paul Duffy
Itron Inc.....	Ed Eckert
Wi-SUN Alliance.....	Hiroshi Harada
Arm Ltd.	Thomas Herbst
Landis+Gyr AG	Ruben E Salazar Cardozo
Landis+Gyr AG	Jeff Scheb
Itron Inc.	Kunal Shah
Cisco Systems, Inc.....	Gary Stuebing
Itron Inc.	Don Sturek

The following members of the entity balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

OxSenses Corporation	Landis+Gyr AG
Anhubao Corporation	ON Semiconductor
Beckhoff Automation	Qingdao Eastsoft Communication Technology Co., Ltd.
Cisco Systems, Inc.	Wi-SUN Alliance
Itron Inc.	

When the IEEE SA Standards Board approved this standard on 16 June 2021, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy	Howard Li	Mehmet Ulema
Doug Edwards	Daozhuang Lin	Lei Wang
Ramy Ahmed Fathy	Kevin Lu	F. Keith Waters
J. Travis Griffith	Daleep C. Mohla	Karl Weber
Thomas Koshy	Chenhui Niu	Sha Wei
Joseph L. Koepfinger*	Damir Novosel	Howard Wolfman
David J. Law	Annette Reilly	Daidi Zhong
	Dorothy Stanley	

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2857-2021, IEEE Standard for Wireless Smart Utility Network Field Area Network (FAN).

This IEEE standard is based on a technical specification developed by a consortium. Patent declarations may have been provided to the consortium as a membership requirement, or in compliance with the consortium's intellectual property rights (IPR) policies and procedures. Normative references in this standard may contain material subject to patent claims that are also subject to the consortium's or other organizations' IPR policies and procedures. Additional information about declarations may be available from the consortium's website:

Wi-SUN Alliance—<https://wi-sun.org>

This specification has been provided “as-is” to the IEEE as a proposed adoption standard. This specification has been fully implemented by a number of industry entities and is being used commercially by more than 96 million devices. The Wi-SUN Field Area Network (FAN) specification has been adopted by certain governmental agencies, regulatory authorities, cities and large utility companies. The specification is based on several IEEE 802® standards including IEEE Std 802.15.4™, IEEE Std 802.1™, and IEEE Std 802.11™. The Wi-SUN Board of Directors has offered this specification to the IEEE as a standard offering “as-is” given that the time to market for mesh wireless solutions in the Utility, Smart City, and Internet of Things (IoT) environments is critical. As such, the initial offering is provided without change to the IEEE.

Users should be aware that within the adopted specification, a statement of “must” shall be interpreted as “shall.”



Field Area Network Working Group (FANWG)

Technical Profile Specification Field Area Network

Version Released for IEEE Std 2857

(Date of Release: November 26, 2020)

Field Area Network Working Group

Field Area Network Technical Profile Specification

This document is provided under the terms of the agreement (18 Nov 2019) between Wi-SUN Alliance and IEEE. The contents of this document are Copyright © Wi-SUN Alliance™.

Table of Contents

1	INTRODUCTION	18
1.1	Scope	18
1.2	Requirements Language	18
1.3	Structure of This Document.....	18
1.4	Acknowledgements	19
2	REFERENCES	21
2.1	Wi-SUN.....	21
2.2	IEEE	22
2.3	ANSI/TIA.....	22
2.4	IETF	22
3	DEFINITIONS AND ACRONYMS	24
3.1	Definitions.....	24
3.2	Acronyms	24
4	TECHNICAL REQUIREMENTS.....	27
4.1	General	27
4.2	Reliability Targets	27
4.3	Adjacent Node Time Synchronization.....	27
4.4	PHY Layer	27
4.4.1	Regional Requirements.....	27
4.4.2	Data Rates.....	27
4.5	Data Link Layer.....	27
4.5.1	Frequency Hopping.....	27
4.5.2	Routing and Forwarding	28
4.6	Network Layer.....	28
4.7	Transport Layer.....	28
4.8	Security	28
5	ARCHITECTURE.....	30



5.1	Overview	30
5.2	Upper Layer Considerations	32
5.3	Transport Service	32
5.3.1	General Principles	32
5.3.2	Node Behavior	32
5.4	Network Service	32
5.4.1	General Principles	32
5.4.2	Node Behavior	33
5.5	Data Link Service	33
5.5.1	General Principles	33
5.5.2	Node Behavior	33
5.6	PHY Service	39
5.6.1	General Principles	39
5.6.2	Node Behavior	40
5.7	Security	40
6	SPECIFICATION	41
6.1	Transport Layer	41
6.1.1	Operation	41
6.2	Network Layer	41
6.2.1	Constants	41
6.2.2	Data Structures	41
6.2.3	Operation	42
6.3	Data Link Layer	51
6.3.1	Constants	51
6.3.2	Data Structures	54
6.3.3	LLC Operation	75
6.3.4	MAC Operation	79
6.3.5	Service Access Points	93
6.4	PHY Layer	98
6.4.1	Operating Modes	99
6.4.2	Preamble Length	99
6.4.3	Radio Specifications	99
6.5	Security	99
6.5.1	Public Key Infrastructure	100
6.5.2	FAN Access Control and Group Key Placement	101
6.5.3	Node to Node Pairwise (N2NP) Authentication and Key Generation	110
6.5.4	Frame Security	143
6.5.5	Node Hardening	147
6.5.6	State Maintenance Through Power Cycling	147
7	APPENDIX A – TR51 CHANNEL FUNCTION	148

7.1	Random Number Generation	148
7.2	Channel Table Calculation	148
7.3	Calculating the First Element and Step Size.....	150
7.4	Computation of Hopping Sequence Channel Table.....	150
8	APPENDIX B - UNICAST FRAME EXCHANGE EXAMPLES.....	153
8.1	Directed Frame Exchange:.....	153
8.1.1	Unacknowledged Data.....	153
8.1.2	Acknowledged Data	153
8.2	Extended Directed Frame Exchange:.....	154
8.2.1	Qualified Frame Exchange	154
8.2.2	Multi-Packet Frame Exchange	155
8.2.3	Frame Exchange with Initial Data	156
8.2.4	Bi Directional Frame Exchange	157
9	APPENDIX C DIRECT HASH CHANNEL FUNCTION	158
9.1	Example Usage of Jenkins Hash	158
9.2	The Jenkins Hash.....	159
9.3	Examples	163
10	APPENDIX D FAN IPV6 ADDRESSING ARCHITECTURE.....	165
11	APPENDIX E UNICAST / BROADCAST / DISCOVERY EXAMPLE.....	166
12	APPENDIX F IPV6 NEIGHBOR DISCOVERY OPTIMIZATIONS.....	169
13	APPENDIX G FRAME COUNTER, FRAME SEQUENCE NUMBER, AND MPX-IE TRANSACTION ID	170
14	APPENDIX H UNICAST TIMING CALCULATION EXAMPLE	171
14.1	Node1 Timing Calculations	171
14.2	Node2 Timing Calculations	171
15	APPENDIX J FAN NODE BOOTSTRAP MESSAGING FLOW	173
16	APPENDIX K EAPOL TARGET SELECTION.....	174
17	APPENDIX L KEY REINSTALLATION ATTACK (KRACK)	175

18	APPENDIX M PHYSICAL LAYER	177
18.1	PHY Specification	177
18.1.1	PPDU Format	177
18.1.2	Modulation and Coding	177
18.1.3	Symbol rate and Modulation Index	177
18.1.4	Frequency Bands and Channel Parameters	178
18.1.5	FEC	180
18.1.6	Data Whitening	180
18.2	PHY RF Requirements	180
18.2.1	Transmit Spectral Mask	180
18.3	Regional Considerations	180
18.3.1	Brazil Region	180
18.4	PHY Test Mode Requirements	180

Table of Figures

FIGURE 5-1 COMMUNICATIONS REFERENCE MODEL.....	30
FIGURE 5-2 SAMPLE LAYER 3 ROUTED FAN	31
FIGURE 5-3 SAMPLE LAYER 2 ROUTED FAN	32
FIGURE 5-4 UPPER LAYER PROTOCOL DISPATCH.....	34
FIGURE 5-5 UNICAST FREQUENCY HOPPING	37
FIGURE 5-6 BROADCAST FREQUENCY HOPPING	38
FIGURE 5-7 BROADCAST AND UNICAST SCHEDULES	39
FIGURE 6-1 EAPOL RELAY DATAGRAM	41
FIGURE 6-2 ADDRESS REGISTRATION	50
FIGURE 6-3 PA FRAME FORMAT	55
FIGURE 6-4 PA FRAME CONTROL FORMAT	55
FIGURE 6-5 PAS FRAME FORMAT	56
FIGURE 6-6 PAS FRAME CONTROL FORMAT.....	56
FIGURE 6-7 PC FRAME FORMAT	56
FIGURE 6-8 PC FRAME CONTROL FORMAT.....	57
FIGURE 6-9 PCS FRAME FORMAT	57
FIGURE 6-10 PCS FRAME CONTROL FORMAT.....	57
FIGURE 6-11 ULAD FORMAT.....	57
FIGURE 6-12 ULAD FRAME CONTROL FORMAT.....	58
FIGURE 6-13 ACKNOWLEDGEMENT FRAME FORMAT	59
FIGURE 6-14 ACKNOWLEDGEMENT FRAME CONTROL FORMAT	59
FIGURE 6-15 EAPOL FRAME FORMAT.....	59
FIGURE 6-16 EAPOL FRAME CONTROL FORMAT	60
FIGURE 6-17 WI-SUN HEADER IE	61
FIGURE 6-18 UNICAST TIMING IE.....	62
FIGURE 6-19 FRAME TYPES.....	62
FIGURE 6-20 BROADCAST TIMING IE	63
FIGURE 6-21 FLOW CONTROL IE	63
FIGURE 6-22 RSL IE.....	63
FIGURE 6-23 MHDS-IE.....	64
FIGURE 6-24 VENDOR EXTENSION IE.....	64
FIGURE 6-25 WI-SUN PAYLOAD IE	65
FIGURE 6-26 UNICAST SCHEDULE IE	65
FIGURE 6-27 BROADCAST SCHEDULE IE	66
FIGURE 6-28 CHANNEL INFORMATION FIELDS.....	66
FIGURE 6-29 EXCLUDED CHANNEL RANGES FIELD	68
FIGURE 6-30 CHANNEL MASK BIT ORDER ILLUSTRATION (TRANSMIT ORDER ... LEFT TO RIGHT).....	68
FIGURE 6-31 VENDOR EXTENSION IE	69
FIGURE 6-32 PAN IE	69
FIGURE 6-33 NETWORK NAME IE	70
FIGURE 6-34 PAN VERSION IE	70
FIGURE 6-35 GTK HASH IE.....	71
FIGURE 6-36 L2 MESH PDU STRUCTURE AND FORMAT.....	74
FIGURE 6-37 L2 MESH PDU HEADER STRUCTURE AND FORMAT	74
FIGURE 6-38 L2 MESH PDU HEADER MHD-CONTROL FIELD FORMAT	74
FIGURE 6-39 L2 MESH PDU HEADER ADDRESS LIST STRUCTURE AND FORMAT	74
FIGURE 6-40 L2 MESH PDU DATA STRUCTURE AND FORMAT.....	74
FIGURE 6-41 L2 MESH PDU DATA ELEMENT STRUCTURE AND FORMAT	74
FIGURE 6-42 STATE TRANSITION DIAGRAM FOR DFE.....	81
FIGURE 6-43 STATE TRANSITION DIAGRAM FOR EDFE.....	82

FIGURE 6-44 FAN JOIN STATES	90
FIGURE 6-45 SERVICE ACCESS POINTS (SAP)	94
FIGURE 6-46 AUTHENTICATION AND GROUP KEY ACQUISITION FLOWS	102
FIGURE 6-47 SHARED SECRET INITIATION	111
FIGURE 6-48 - UML ASSOCIATION MANAGEMENT STATE MACHINE	115
FIGURE 6-49 - STATE MACHINE SHAPES KEY	115
FIGURE 6-50 - START STATE TRANSITIONS	117
FIGURE 6-51 - ASSOCIATIONWAIT STATE TRANSITIONS.....	118
FIGURE 6-52 - ACKWAIT STATE TRANSITIONS	119
FIGURE 6-53 - SESSIONVALID STATE TRANSITIONS	119
FIGURE 6-54 - COMMON TRANSITIONS.....	120
FIGURE 6-55 ESTKEYTRUST PROCEDURE FLOW.....	121
FIGURE 6-56 START STATE TRANSITIONS PART 1	124
FIGURE 6-57 START STATE TRANSITIONS - PART 2	125
FIGURE 6-58 SESSIONPENDING1 STATE TRANSITIONS.....	126
FIGURE 6-59 SESSIONPENDING2 STATE TRANSITIONS.....	128
FIGURE 6-60 SESSIONVALID STATE TRANSITIONS	129
FIGURE 6-61 SESSIONOPEN STATE TRANSITIONS.....	130
FIGURE 6-62 COMMON TRANSITIONS.....	131
FIGURE 6-63 NEWASSOCIATION MESSAGE	133
FIGURE 6-64 ASSOCIATIONRESPONSE MESSAGE	134
FIGURE 6-65 ASSOCIATIONACK MESSAGE.....	135
FIGURE 6-66 GETCERTS MESSAGE	136
FIGURE 6-67 SENDCERTS MESSAGE.....	136
FIGURE 6-68 CLOSEASSOCIATION MESSAGE	137
FIGURE 6-69 NS SHARED SECRET INITIATION	137
FIGURE 6-70 NS SHARED SECRET RESPONSE	138
FIGURE 6-71 SM SPECIFIC ERROR MESSAGE	140
FIGURE 6-72 GTK CYCLING.....	146
FIGURE 8-1 DFE NON-ACKNOWLEDGED EXCHANGE	153
FIGURE 8-2 DFE ACKNOWLEDGED EXCHANGE	154
FIGURE 8-3 EDFE QUALIFIED FRAME EXCHANGE	155
FIGURE 8-4 EDFE 2 MULTI-PACKET DATA EXCHANGE	156
FIGURE 8-5 EDFE FRAME EXCHANGE WITH INITIAL DATA.....	156
FIGURE 8-6 EDFE BI-DIRECTIONAL FRAME EXCHANGE.....	157
FIGURE 15-1 JOINING NODE BOOTSTRAP MESSAGING FLOW (L3 ROUTING)	173

Table of Tables

TABLE 6-1 NETWORK LAYER CONSTANTS	41
TABLE 6-2 DATA LINK LAYER CONSTANTS	51
TABLE 6-3 MULTIPLEX IDS	71
TABLE 6-4 INFORMATION ELEMENT REQUIREMENTS FOR FRAMES	73
TABLE 6-5 MLME-WS-ASYNC-FRAME.REQUEST PARAMETERS	97
TABLE 6-6 MLME-WS-ASYNC-FRAME.CONFIRM PARAMETERS	98
TABLE 6-7 MLME-WS-ASYNC-FRAME.INDICATION PARAMETERS	98
TABLE 6-8 - PREAMBLE LENGTHS PER OPERATING MODES	99
TABLE 6-9 - RADIO SPECIFICATION	99
TABLE 6-10 AUTHENTICATION AND PMK INSTALLATION FLOW	105
TABLE 6-11 PTK AND GTK INSTALLATION FLOW	107
TABLE 6-12 GROUP KEY UPDATE FLOW	109
TABLE 18-1 - PHY OPERATING MODES AND SYMBOL RATES	178
TABLE 18-2: SUPPORTED FREQUENCY BANDS AND CHANNEL PARAMETERS	178

1 Introduction

1.1 Scope

This document defines the technical implementation and behavior of a Wi-SUN Field Area Network which fulfills the marketing requirements specified in [MRD]. With the details presented in this document, an implementer is enabled to construct an interoperable and certifiable implementation of the Wi-SUN FAN.

1.2 Requirements Language

Requirements are specified using the terminology and conventions as described in [RFC2119]. Requirements key words described in [RFC2119] must be capitalized.

1.3 Structure of This Document

The FAN Technical Profile Specification is developed in an iterative process as described in [FWGDP]. A brief overview of each TPS section is provided below. Unless noted otherwise, all sections are informative.

1. Introduction. Self-explanatory.
2. References. Self-explanatory.
3. Definitions and Acronyms. Self-explanatory.
4. Technical Requirements (normative). This section defines the requirements which must be met by the Specification section. It defines what functionality must be provided by the TPS. It does not define the technical specifics of how the Technical Requirements are met, nor test cases required to verify that functionality.
5. Architecture. Overview of the design and operation of the FAN.
6. Specification (normative). The technical specifics of how the mechanisms of the FAN are to be implemented. Normative clauses within this section require corresponding test case coverage be incorporated into the Wi-SUN FAN Compliance and Interoperability Test Plans.
7. Appendix A. (normative). Description of the TR51 Channel Function.
8. Appendix B. Unicast Frame Exchange examples.
9. Appendix C. (normative). Description of the Direct Hash Channel Function.
10. Appendix D. Guidance for FAN IPv6 Addressing Architecture.
11. Appendix E. Unicast / Broadcast / Discovery Example.
12. Appendix F. Description of IPv6 Neighbor Discovery Optimizations.
13. Appendix G. Description of Frame Counter, Frame Sequence Number, and MPX-IE Transaction ID interaction.
14. Appendix H. Unicast Timing Calculation Example.
15. Appendix J. FAN Node Bootstrap Messaging Flow.
16. Appendix K. EAPOL Target Selection.
17. Appendix L. Key Reinstallation Attack.

1.4 Acknowledgements

The Wi-SUN Alliance acknowledges the substantial efforts of the following individuals who contributed to the production of this document.

- Keith Barnes, Itron
- Paul Dietrich, Silver Spring Networks
- Paul Duffy, Cisco Systems (Co-Chair and Technical Editor)
- Gene Falendysz, Itron
- Veselin Ganev, Cisco Systems
- Elad Gottlib, Silver Spring Networks
- Thomas Herbst, Silver Spring Networks
- Chris Hett, Landis+Gyr
- Jonathan Hui, Cisco Systems
- Thomas Joyce, Analog Devices Inc.
- Amarjeet Kumar, Procubed Inc.
- Rakesh Kumar, Procubed Inc.
- Anand M, Procubed Inc.
- Ben Rolfe, Electric Power Research Institute
- Ryota Yamada, Omron
- Anders Grauballe, Kamstrup
- Ankush Sabharwal, Landis+Gyr
- Will San Filippo, Silver Spring Networks
- Koichi Sato, Renesas
- Cristina Seibert, Silver Spring Networks
- Kunal Shah, Itron (PHYWG Chair and Technical Editor)
- Huimin She, Cisco Systems
- Shobhit Singh, Landis+Gyr
- Michael St Johns, Silver Spring Networks
- Don Sturek, Itron (Co-Chair)
- Larry Taylor, Discrete Time Communications
- Kumaran Vijayasankar, Texas Instruments
- Hans Waldmann, Analog Devices Inc.
- Lu Wang, Cisco Systems
- Zhanglong Xia, Cisco Systems

2 References

- [SGNSRS] “Smart Grid Networks System Requirements Specification, Release Version 5, Final”, http://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Latest_Release_Deliverables/SG%20Network%20SRS%20Version%20V5%20Final.pdf
- [FCC-Part-15.247] “Code of Federal Regulations, Title 47 - Telecommunications, Section 15.247 - Operation within the bands 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz”, <http://www.gpo.gov/fdsys/pkg/CFR-2005-title47-vol1/xml/CFR-2005-title47-vol1-sec15-247.xml>
- [OSIRM] ITU X.200 / ISO/IEC 7498-1 OSI Basic Reference Model, <http://www.ecma-international.org/activities/Communications/TG11/s020269e.pdf>
- [ETSI-TS-102-887-1]: “Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices; Smart Metering Wireless Access Protocol; Part 1: PHY layer”
https://www.etsi.org/deliver/etsi_ts/102800_102899/10288701/01.01.01_60/ts_10288701v010101p.pdf
- [ETSI-TS-102-887-2] “Smart Metering Wireless Access Protocol; Part 2: Data Link Layer (MAC Sub-layer)”, http://www.etsi.org/deliver/etsi_ts/102800_102899/10288702/01.01.01_60/ts_10288702v010101p.pdf
- [CEPT ERC/REC 70-03] “ERC Recommendation 70-03 Relating to the use of Short Range Devices (SRD)”, <http://www.erodocdb.dk/Docs/doc98/official/pdf/REC7003E.PDF>
- [NFAP-WPC] “Government of India, Ministry of Telecommunications National Frequency Allocation Plan”, <https://dot.gov.in/sites/default/files/NFAP%202018.pdf>
- [WBXCF] “WAP Binary XML Content Format”, <http://www.w3.org/TR/wbxm1/>
- [SP800-108] “NIST Special Publication 800-108 Recommendation for Key Derivation Using Pseudorandom Function”, <http://csrc.nist.gov/publications/nistpubs/800-108/sp800-108.pdf>
- [SP800-38A] “Recommendation for Block Cipher Modes of Operation”, <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>
- [SP800-38C], “Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality”, http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf
- [SP800-38D], “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC”, <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>
- [FIPS197] “Advanced Encryption Standard”, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- [FIPS198-1] “The Keyed-Hash Message Authentication Code (HMAC)”, http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

2.1 Wi-SUN

- [FWGDP] “FAN Working Group Development Process”, <https://dms.wi-sun.org/htcomnet/Handlers/Download.ashx?action=download&file=FAN%20Profile%2FProcess%20Documents%2F20130618-FANWG-iterative%20process%20description-0v04.pdf>
- [MACREQ] “FAN TPS Frequency Hopping Proposal”, <https://www.wi-sun.org/index.php/fan1v0-refs/30-fan-fh-requirements/file>
- [MRD] “Marketing Requirements Document Field Area Network”, Wi-SUN Alliance Marketing Working Group, <https://dms.wi-sun.org/htcomnet/Handlers/Download.ashx?action=download&file=FAN%20Profile%2FMarketing%20Requirements%20Documents%20-%20FAN%201.0%2F20130130-MWG-FAN%20MRD%200V12.pdf>
- [WVIMP] “Wi-SUN Number Registry”, <https://dms.wi-sun.org/htcomnet/Handlers/Download.ashx?action=download&file=TSC%2FWi-SUN%20Number%20Registry%2F20150630-Wi-SUN-Number-Registry-0v07.docx>

2.2 IEEE

[IEEE802.15.4] “IEEE Standard for Low-Rate Wireless Personal Area Networks (WPANs)”, IEEE Std 802.15.4-2015, <https://standards.ieee.org/findstds/standard/802.15.4-2015.html>

[IEEE802.15.4v] “IEEE Standard for Low-Rate Wireless Networks, Amendment 5: Enabling/Updating the Use of Regional Sub-GHz Bands”, IEEE Std 802.15.4v-2017 https://standards.ieee.org/standard/802_15_4v-2017.html

[EUI64] “Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority”, <https://ccie.lol/wp-content/uploads/2016/10/eui64.pdf>

[IEEE802.1X] “IEEE Standard for Local and Metropolitan Area Networks – Port Based Network Access Control”, IEEE Std 802.1X-2010, <https://standards.ieee.org/findstds/standard/802.1X-2010.html>

[IEEE802.11] “IEEE Standard for Information Technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE Std 802.11-2012, <https://standards.ieee.org/findstds/standard/802.11-2012.html>

[IEEE802.15.9] “IEEE Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams”, 802.15.9-2016, <https://standards.ieee.org/findstds/standard/802.15.9-2016.html>

[IEEE802.1AR] “IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identity”, IEEE Std 802.1AR-2009, <https://standards.ieee.org/findstds/standard/802.1AR-2009.html>

2.3 ANSI/TIA

[ANSITIA-4957.200] “Layer 2 Standard Specification for the Smart Utility Network”, <https://standards.tiaonline.org/all-standards/committees/tr-51>

[ANSITIA-4957.210] “Multi-hop Delivery Specification of a Data Link Sub-Layer”, <https://standards.tiaonline.org/all-standards/committees/tr-51>

2.4 IETF

[ARP] “Address Resolution Protocol (ARP) Parameters <http://www.iana.org/assignments/arp-parameters/arp-parameters.xhtml>

[MPL] “Multicast Protocol for Low power and Lossy Networks (MPL)”, <https://tools.ietf.org/html/rfc7731>.

[RFC768] “User Datagram Protocol”, <http://tools.ietf.org/search/rfc768>

[RFC793] “Transmission Control Protocol”, <https://www.ietf.org/rfc/rfc793.txt>

[RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, <http://www.ietf.org/rfc/rfc2119.txt>

[RFC2460] “Internet Protocol, Version 6”, <http://tools.ietf.org/html/rfc2460>

[RFC2473] “Generic Packet Tunneling in IPv6 Specification”, <http://tools.ietf.org/html/rfc2473>

[RFC3280] “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, <https://www.ietf.org/rfc/rfc3280.txt>

[RFC3315] “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, <http://www.ietf.org/rfc/rfc3315.txt>

[RFC4108] “Using Cryptographic Message Syntax (CMS) to Protect Firmware Package”, <https://tools.ietf.org/html/rfc4108>

[RFC4443] “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, <http://tools.ietf.org/html/rfc4443>

[RFC4861] “Neighbor Discovery for IP version 6 (IPv6)”, <http://tools.ietf.org/html/rfc4861>

[RFC4862] “IPv6 Stateless Address Autoconfiguration”, <http://tools.ietf.org/html/rfc4862>

- [RFC5216] “The EAP-TLS Authentication Protocol”, <http://tools.ietf.org/html/rfc5216>.
- [RFC5480] “Elliptic Curve Cryptography Subject Public Key Information”, <https://tools.ietf.org/html/rfc5480>.
- [RFC6206] “The Trickle Algorithm”, <http://tools.ietf.org/search/rfc6206>
- [RFC6282] “Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks”, <http://tools.ietf.org/search/rfc6282>
- [RFC6550] “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks”, <http://tools.ietf.org/html/rfc6550>
- [RFC6551] “Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks”, <https://tools.ietf.org/html/rfc6551>
- [RFC6553] “RPL Option for Carrying RPL Information in Data-Plane Datagrams”, <http://tools.ietf.org/html/rfc6553>
- [RFC6554] “An IPv6 Routing Header for Source Routes with RPL”, <http://tools.ietf.org/html/rfc6554>
- [RFC6655] “AES-CCM Cipher Suites for Transport Layer Security (TLS)”, <https://tools.ietf.org/html/rfc6655>
- [RFC6719] “The Minimum Rank with Hysteresis Objective Function”, <http://tools.ietf.org/search/rfc6719>
- [RFC6775] “Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)”, <http://tools.ietf.org/search/rfc6775>
- [RFC7251] “AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS”, <https://tools.ietf.org/html/rfc7251>
- [RFC 7973] “Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation”, <https://tools.ietf.org/html/rfc7973>

3 Definitions and Acronyms

3.1 Definitions

Authenticator	See [IEEE802.1X].
Asynchronous frame	A frame that is transmitted using the MLME-WS-ASYNC-FRAME mechanism.
Broadcast frame	A frame transmitted by a node to the layer 2 broadcast address using the node's broadcast schedule.
Directed frame	A frame transmitted to a specific layer 2 unicast address using the target node's unicast schedule.
Dwell Interval	Time (duration) that a node has designated for frame exchange on a given channel when frequency hopping.
Exponentially Weighted Moving Average.	Given a sequence of values $X(t=0, 1, 2, 3, \dots)$, $EWMA(t)$ is defined as $S(X(t)) + (1-S)(EWMA(t-1))$ where ... Smoothing Factor $0 < S < 1$ $EWMA(0) = X(0)$.
Floor	$\text{floor}(x)$ returns the largest number not greater than x whose number is an integer.
Target (verb)	The action of transmitting a frame on a neighbor node's unicast listening schedule at a specific time. The neighbor node is known as the targeted node.

3.2 Acronyms

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks.
AEAD	Authenticated Encryption with Associated Data.
AR	Acknowledge Request. See [IEEE802.15.4].
BR	Border Router. Synonymous with 6LBR. See [RFC6775].
BSI	Broadcast Schedule Identifier.
CA	Certificate Authority
CBC	Cipher Block Chaining.
CCA	Clear Channel Assessment.
CCM	Counter with CBC-MAC.
CMAC	Cipher based MAC.
CRC	Cyclic Redundancy Check.
CSMA	Carrier Sense Multiple Access.
DAO	Destination Advertisement Object. See [RFC6550].
DIO	DODAG Information Object. See [RFC6550].

DIS	DODAG Information Solicitation. See [RFC6550].
DL	Data Link.
DODAG	Destination Oriented Directed Acyclic Graph. See [RFC6550].
DUID	DHCP Unique Identifier. See [RFC3315].
DUID-LL	DUID based on Link Local Address. See [RFC3315].
EWMA	Exponentially Weighted Moving Average.
ETX	Expected Transmission Count. Number of expected packet transmissions required for error free reception at destination.
FAN	Field Area Network.
GCM	Galois/Counter Mode.
GTK	Group Transient Key.
GUA	Global Unicast Address. See [RFC4291].
HMAC	Keyed Hash Message Authentication Code.
IA_NA	Identity Association for Non-temporary Address. See [RFC3315].
IAADDR	Identity Association Address option. See [RFC3315].
IDeVID	Initial Device Identifier. See [IEEE802.1AR].
IE	Information Element.
IV	Initialization Vector.
LDeVID	Locally significant Device Identifier. See [IEEE802.1AR].
LLA	Link Local Address. See [RFC4291].
LLC	Logical Link Layer.
LLN	Low Power and Lossy Network.
KDF	Key Derivation Function.
MAC	Medium Access and Control.
MHDS	Multi-Hop Delivery Service.
MPDU	MAC Protocol Data Unit.
MPL	Multicast Protocol for Low power and Lossy Network. See [MPL].
MSDU	MAC Service Data Unit.
NUD	Neighbor Unreachability Detection as described in [RFC6775].
PHR	PHY Header.
PA	PAN Advertisement
PAS	PAN Advertisement Solicit
PC	PAN Configuration

PCS	PAN Configuration Solicit
PIB	Personal area network Information Base.
PMK	Pairwise Master Key. See [IEEE802.15.4].
PPDU	PHY Protocol Data Unit.
PRF	Pseudo Random Function.
PTK	Pairwise Transient Key
RAMP	Route Advertisement and Management Protocol. See [ANSITIA-4957.210]
RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks. See [RFC6550].
RSSI	Received Signal Strength Indication. Unit less indication of the power level measured at a receiver's antenna.
RSL	Received Signal Level
RTA	Route Advertisement.
SAP	Service Access Point.
SDU	Service Data Unit.
SHR	Synchronization Header. See [IEEE802.15.4].
SM	Session Management. See [ETSI-TS-102-887-2].
SREG	Service Registration. See [ANSI/TIA-4957.210].
SREG-ACK	Service Registration Acknowledgement. See [ANSI/TIA-4957.210]
SRH	Source Routing Header. See [RFC6554].
SUP	Supplicant. See [IEEE802.1X].
TPS	Technical Profile Specification.
TR51CF	TR51 Channel Function. Defined in section 7.1 of [ANSITIA-4957.200].
UDI	Unicast Dwell Interval
ULA	Unique Local IPv6 Unicast Address. See [RFC4193].
ULAD	Upper Layer Application Data.

4 Technical Requirements

This section details the technical requirements intended to address the marketing requirements provided in [MRD].

4.1 General

The FAN MUST comply with all applicable local regulations.

The FAN MUST support mesh networking with FAN nodes being up to 24 hops from the root of the mesh tree.

4.2 Reliability Targets

The FAN must comply with the following reliability targets.

1. The FAN MUST provide overall application layer message delivery reliability as specified in [SGNSRS] for the use cases enumerated in [MRD].
2. The FAN MUST provide an undetected frame error rate, delivered by the MAC to the higher layer, of no more than 10^{-6} .

4.3 Adjacent Node Time Synchronization

1. Neighboring FAN nodes MUST exchange timing information adequate to support frequency hopping.
2. The MAC protocol MUST support synchronization of channel hop schedule timing with a resolution of better than 1 ms.

4.4 PHY Layer

A FAN node MUST be capable to send/receive PPDU's on different channels such that the time from the end of the last symbol of the first packet to the beginning part of the first symbol of the subsequent packet is no sooner than 1 ms and no greater than 3 ms (as measured at the RF interface).

4.4.1 Regional Requirements

A FAN node MUST adhere to the regional frequency band requirements of 18.16.4.

4.4.2 Data Rates

A FAN node MUST adhere to the operating mode requirements of 6.4.

FAN nodes are not required to dynamically change data rates.

4.5 Data Link Layer

4.5.1 Frequency Hopping

The following section presents the technical requirements for FAN frequency hopping. Informative discussion of these requirements can be found in section 5 of [MACREQ].

1. Frequency hopping in the FAN MAC MAY be used to meet the regulatory requirements for the regions specified in section 4.4.1.
2. The MAC protocol MUST implement frequency hopping mechanisms.
3. By default the FAN frequency hopping MUST equally (on average) use all available channels (excepting those explicitly excluded from the channel hopping sequence) in a pseudo-random sequence. See [FCC-Part-15.247] for further details.
4. The FAN MAC MUST support a hop dwell interval of between 15 msec and 255 msec (inclusive).
5. The MAC protocol MUST support exclusion of a subset of available channels.



6. The FAN MAC MUST allow re-transmissions of failed unicast transmission attempts. Re-transmissions MAY occur on the same or on different channels. The FAN frequency hopping MUST support at least 20 attempts over the available channels within 5 seconds.
7. A 'Poll-Response' mechanism SHOULD be employed to mitigate interference (such as hidden terminals) and to ensure the destination is listening before sending long data packets on the radio medium (definition of long is implementation specific).
8. The Poll-Response duration SHOULD be short compared to typical packet lengths to minimize transaction overhead (typical packet length is defined to be 128 octets).
9. The MAC protocol MUST implement a receiver directed frequency-hopping mechanism for unicast transmissions.
10. The exchange of MAC frames in a unicast transmission (including acknowledgements as defined in this specification) MUST take place on the channel on which the transmission was initiated and complete within regulatory limits. After completion the nodes MUST continue their hop sequence and timing as if no unicast exchange had ever occurred.
11. The frequency hopping mechanism MUST NOT require global synchronization for unicast traffic.
12. The percentage of a node's data transmission dedicated to frequency hopping synchronization should be small compared to its total data transmission.

4.5.2 Routing and Forwarding

1. Data Link layer routing and forwarding of unicast IPv6 packets MAY be supported.
2. Data Link layer routing and forwarding of multicast IPv6 packets MAY be supported.

4.6 Network Layer

The following section presents the technical requirements of the FAN network layer.

1. The Network layer MUST be based on IPv6 with 6LoWPAN adaptation.
2. Network layer routing and forwarding of unicast IPv6 packets MUST be supported.
3. Network layer routing and forwarding of multicast IPv6 packets MUST be supported.
4. Automated assignment of link-local IPv6 addresses MUST be supported.

4.7 Transport Layer

The following section presents the technical requirements of the FAN transport layer.

1. The Transport layer MUST provide a mechanism for connection-less data transmission between FAN nodes.
2. The Transport layer MAY provide a mechanism for connection oriented, reliable transmission of data between FAN nodes.

4.8 Security

The following section presents the technical requirements related to FAN security.

1. Mutual authentication of a FAN node and the FAN to which the node connects MUST be supported.
2. The FAN MUST provide a means to restrict traffic from non-authenticated nodes.
3. The FAN MUST support establishment, refresh, and revocation of pairwise keys between Border Routers and non Border Router nodes.
4. The FAN MUST support establishment, refresh, and revocation of group keys to FAN nodes.
5. The FAN MAY support establishment, refresh, and revocation of pairwise keys between any two FAN nodes.

6. The FAN MUST support encryption of transmitted frames and decryption of received frames.
7. The FAN MUST support integrity checking of transmitted frames.

5 Architecture

5.1 Overview

Figure 5-1 describes the architecture of the Wi-SUN Field Area Network (FAN) in terms of the layered OSI Reference Model [OSIRM].

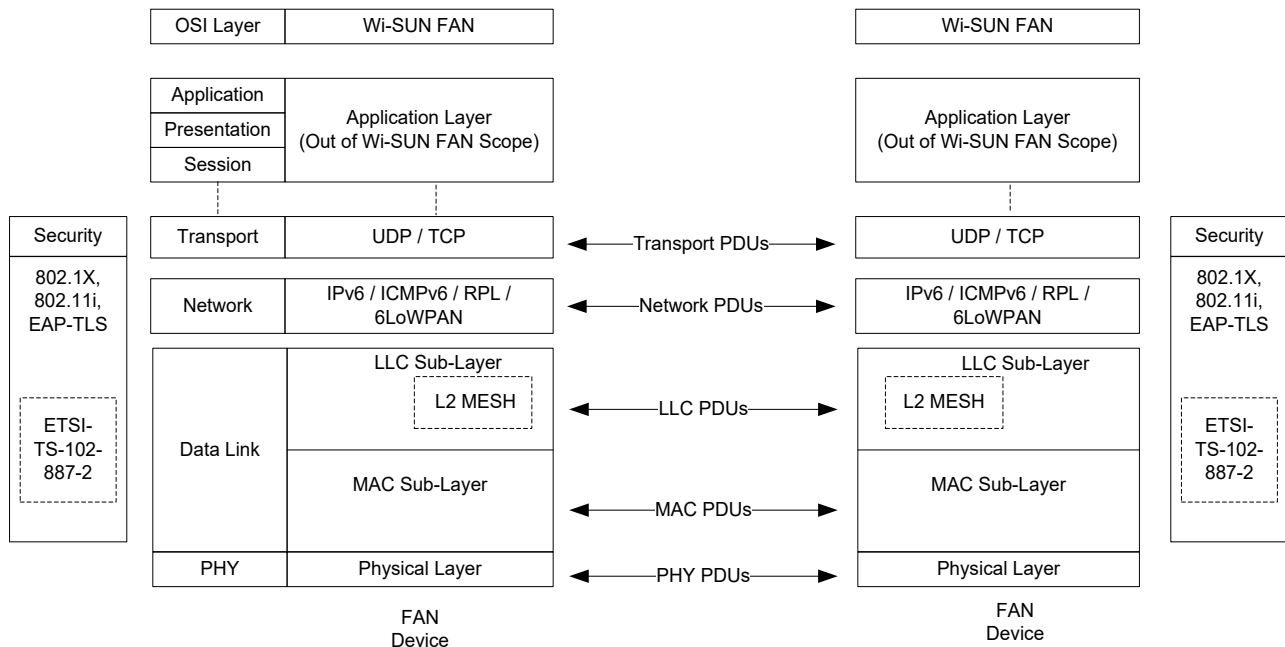


Figure 5-1 Communications Reference Model

The FAN specification is based upon various IETF, IEEE, and ANSI/TIA standards supporting Low Power and Lossy Networks. The complete FAN specification provides an application independent IPv6-based transport service for both connectionless (UDP) and connection-oriented (TCP) services.

The FAN is defined as having two possible methods for establishing IPv6 packet routing: mandatory RPL at layer 3 or optional MHDS at layer 2. The determination of routing method to be used by a node is administratively set prior to node deployment. The routing algorithm for which a node is configured is indicated in the PAN advertisement process and nodes will only join networks that match their configured routing algorithm.

The layer 3 routed FAN contains one or more PANs. Within a PAN, nodes assume one of three operational roles (set via local administrative policy):

1. Each PAN contains a Border Router providing WAN connectivity to the PAN. The Border Router maintains source routing tables for all nodes within its PAN, provides node authentication and key management services, and disseminates PAN wide information such as broadcast schedules.
2. Router nodes, which provide upward and downward packet forwarding (within a PAN). A Router also provides services for relaying security and address management protocols.
3. Leaf nodes provide minimum capabilities: discovering and joining a PAN, send/receive IPv6 packets, etc.

A sample deployment for the layer 3 routed FAN is depicted in Figure 5-2.

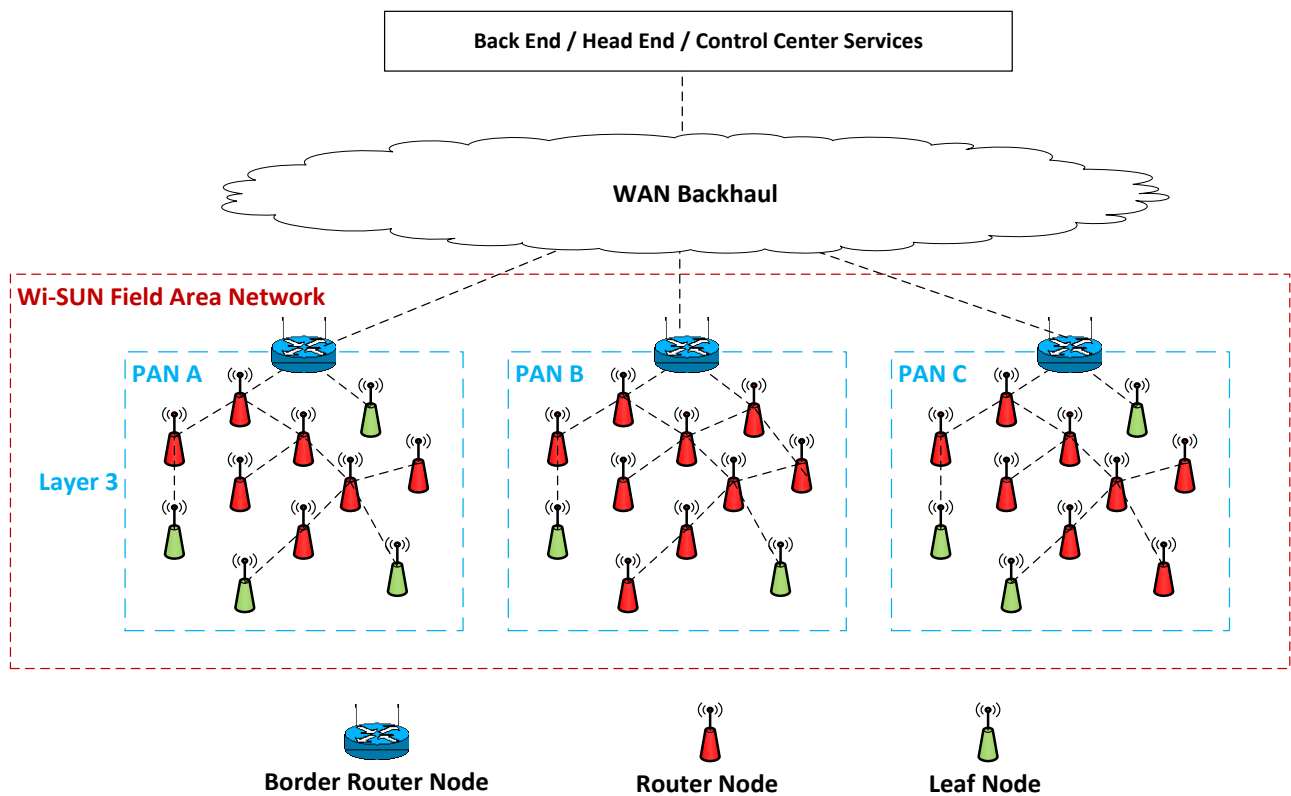


Figure 5-2 Sample Layer 3 Routed FAN

The topology for the layer 2 MHDS FAN is similar to the layer 3 routed FAN. Each PAN has exactly one layer 2 Access Point providing WAN connectivity. MHDS provides Leaf and Forwarding node roles equivalent to the layer 3 Leaf and Router roles. The AP node maps directly to the Border Router at layer 3.

The main difference between the two configurations is that, viewed from layer 3, all members of an MHDS PAN that need to communicate with the Border Router are neighbors of the Border Router. The connectivity for nodes which are not neighbors at layer 2 is provided by MHDS in much the same way that routing for non-neighbor layer 3 routed nodes is provided by RPL.

A sample deployment for the layer 2 MHDS FAN is depicted in Figure 5-3.

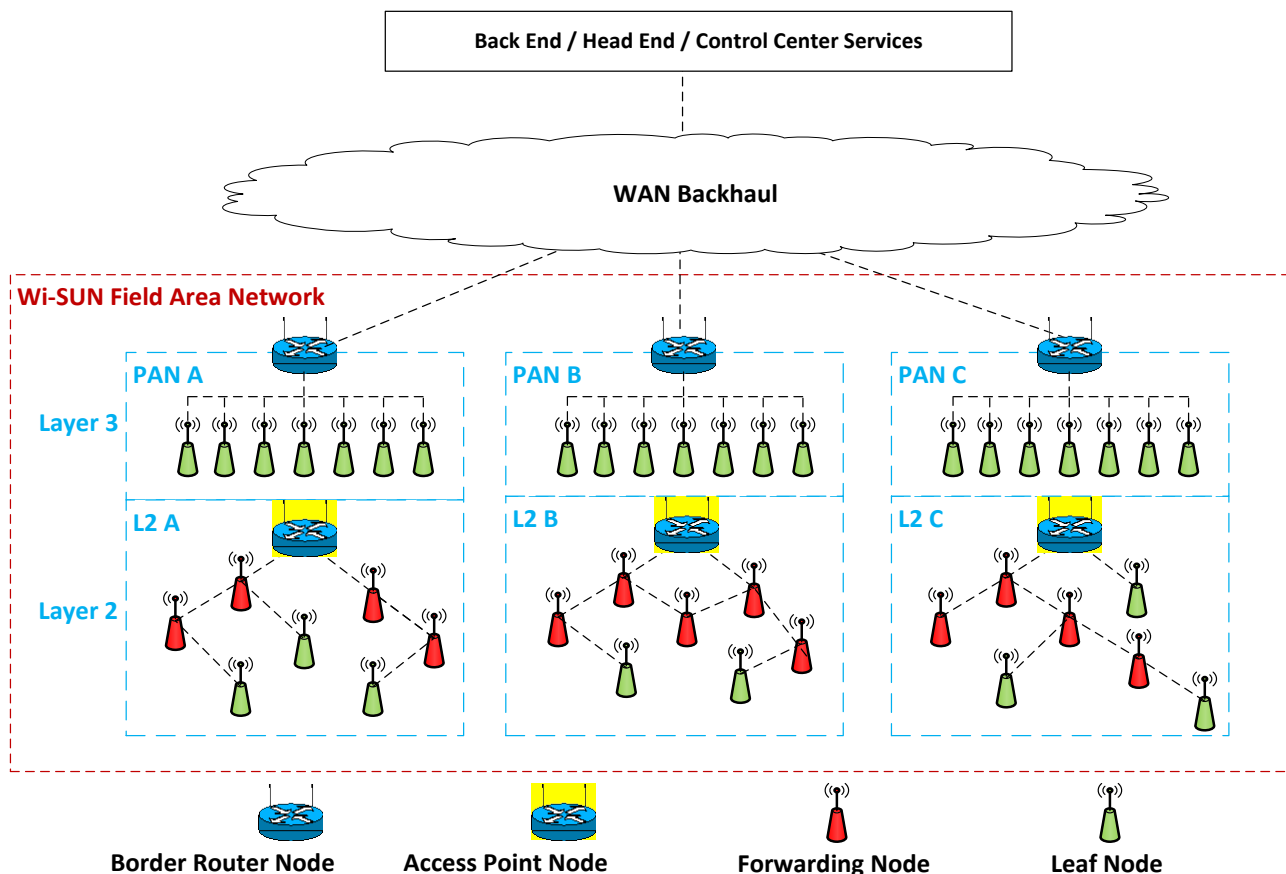


Figure 5-3 Sample Layer 2 Routed FAN

5.2 Upper Layer Considerations

The Wi-SUN FAN specifications do not define layers above the Transport Layer.

5.3 Transport Service

5.3.1 General Principles

The Transport Service is provided by UDP [RFC768] or TCP [RFC793]. No modifications to the protocols specified in these RFCs are required for use over the FAN Network Service.

5.3.2 Node Behavior

No specific node behavior is specified for the Transport Service.

5.4 Network Service

5.4.1 General Principles

The Network Service is provided by IPv6 as defined in RFC2460 with 6LoWPAN adaptation as defined in RFC4944 and RFC6282. ICMPv6, as defined in RFC4443, is used for control plane information exchange.

Though the underlying MAC/PHY services provide support for more than the IPv6 packet length requirement, 6LoWPAN dispatch values for uncompressed IPv6 Headers, Header Compression and Fragmentation may be used.

As the Wi-SUN FAN specifications include Layer 3 routing and optional Layer 2 multi-hop delivery, the 6LoWPAN Mesh Headers are not required and are not used.

Layer 3 routing is supported by RPL [RFC6550] using the non-storing mode. IPv6 packets are routed hop-by-hop “upwards” toward the RPL root. IPv6 packets are source routed “downward” from the RPL root.

If the optional Layer 2 multihop delivery service is present, Layer 3 routing is not used and a Layer 2 multi-hop forwarding path to the destination is determined for the Layer 2 frame.

5.4.2 Node Behavior

5.4.2.1 Neighbor Discovery

FAN nodes use the techniques described in [RFC6775] and [RFC6550] to optimize IPv6 Neighbor Discovery.

5.4.2.2 RPL

RPL is a control plane protocol for construction and maintenance of Layer 3 routing domains called Destination Oriented Directed Acyclic Graphs (DODAGs). In a Wi-SUN FAN, a DODAG originates (has its root) at a Border Router connecting a PAN to an external network.

The FAN implements the non-storing mode of RPL in which the Border Router is the single node maintaining downward routing information for a DODAG.

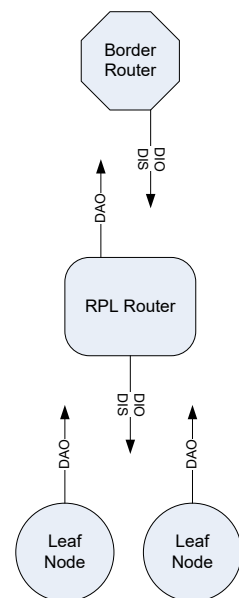
IPv6 packets are forwarded from a source node up the DODAG to the root using next hop routing. Packets are forwarded down the DODAG to a destination node using source routing determined by the root.

A Router node collects DIO RPL messages from one or more candidate neighbor parent nodes. The DIO messages contain various DODAG metadata and the rank (relative position within the DODAG) of the transmitting candidate. A set of routable parents is selected from the candidate set, one of which is determined to be the preferred parent, providing the default upward route from the child node. The child node itself calculates its rank within the DODAG, then transmits its version of DIO messages to listening neighbors. DIOs may further be explicitly requested by neighbors using DIS messages.

A Border Router is a special case of a Router which has no parents, starts the dissemination of DIO messages downward into the DODAG, and maintains all downward source routing information.

A Leaf node differs from a Router in that it does not transmit DIO messages. It does not provide any routing capability.

All DODAG nodes, except the Border Router, transmit DAO RPL messages to the Border Router announcing a node's routes to its parents. The entire set of DAO information received by the Border Router enables it to construct downward source routes to any node within the DODAG.



5.5 Data Link Service

5.5.1 General Principles

The Data Link layer (DL) provides both control and management of the Physical layer and data transfer and management services to the Network layer. These services are sub-divided into Media Access Control (MAC) and Logical Link Control (LLC) sub-layers.

5.5.2 Node Behavior

5.5.2.1 LLC sub-layer

The LLC sub-layer provides a protocol dispatch service which supports 6LoWPAN and an optional L2 MESH service.

5.5.2.1.1 Protocol Dispatch

The LLC layer protocol dispatch function provides support for multiple Data Link Clients, either a 6LoWPAN client or a client depending on the use of the MHDS. The general overview of upper layer protocol dispatch can be viewed in Figure 5-4.

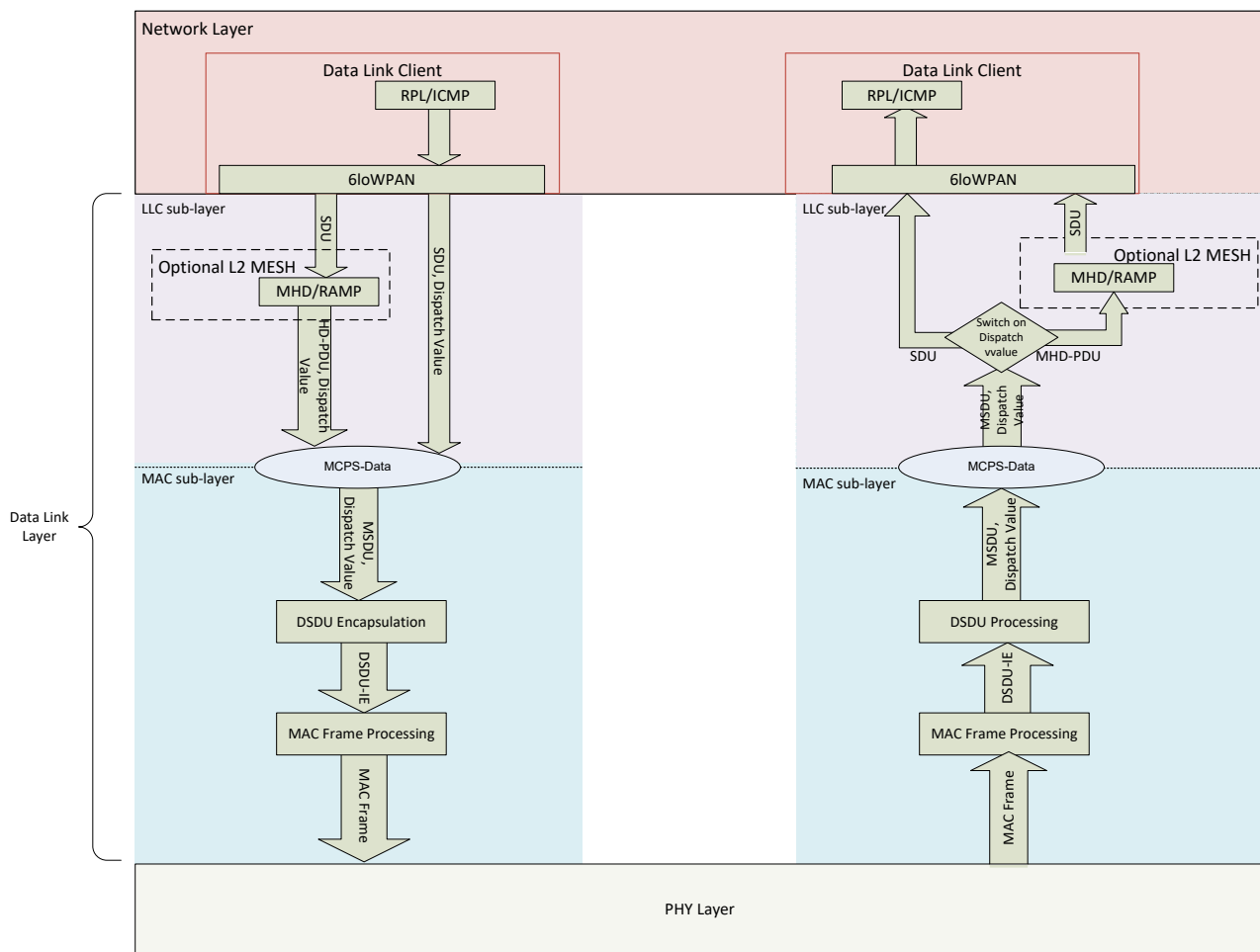


Figure 5-4 Upper Layer Protocol Dispatch

5.5.2.1.2 L2 MESH

A FAN node may implement the optional MESH-under service based on the MHDS defined in [ANSITIA-4957.210] Clause 4 as an alternative to RPL. The MHDS protocol defines a packet structure to carry multi-hop address information and a protocol identifier field to indicate the originating and destination protocol entity. The MHDS Client corresponds to a FAN Node.

MHDS provides similar functionality to RPL with both announcement and maintenance of routes between a Service and Nodes. In a FAN, the MHDS Service is equivalent to the RPL Border Router. MHDS nodes may provide forwarding for packets from a Service to downstream neighbor nodes and for packets from downstream neighbors towards a Service. As in RPL, the downstream transmissions are source routed and the upstream transmissions are hop-by-hop. In MHDS, upstream transmissions may also be source routed.

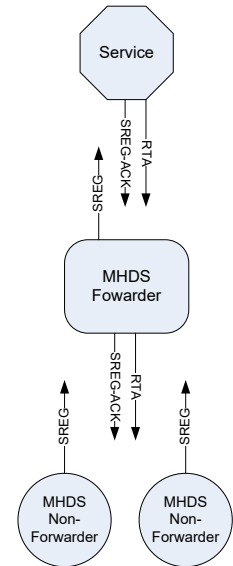
The route to a Service is identified by a Route Tag which is equivalent to an RPL Instance ID.

A Service is advertised by the service providing node issuing a RAMP Route Advertisement (RTA) packet. As in RPL, the root is identified as having a hop distance (equivalent to the RPL rank) of zero. Neighboring MHDS forwarders re-issue the RTA packets with incremented hop distance after having registered with the Service by exchanging SREG and SREG-ACK packets.

The extent of the route is limited by a maximum hop distance determined by the root node when the route is created.

A node selects a route by sending an SREG packet to the Service. SREG packets accumulate hop-by-hop node addresses enabling the Service to use source routing in replies to the destination node. If the SREG request is accepted by the Service responding with an SREG-ACK the node has a path to the Service and vice versa.

The MHDS Provider corresponds to a Wi-SUN FAN Access Point (AP) which acts as the source of one or more routes and provides the Network Point of Attachment for the FAN to a Wide Area Network.



5.5.2.1.2.1 Addressing

Addressing is as described in [ANSI/TIA-4957.210] Clause 4.3.

5.5.2.1.2.2 Protocol Identifier

The Protocol Identifier in data structures and parameter lists is as described in [ANSI/TIA-4957.210] Clause 4.4.

Vendor specific formats identified by Vendor Specific Protocol identifier ranges are not defined in this specification.

5.5.2.1.2.3 Multi-Hop Delivery

Multi-hop delivery constructs and principles are as described in [ANSI/TIA-4957.210] Clause 4.5.

1. Sequence Number principles are as described in [ANSI/TIA-4957.210] Clause 4.5.1.
2. MHD-PDU handling for broadcast and multicast destinations is as described in [ANSI/TIA-4957.210] Clause 4.5.2. The Broadcast Data Service is not supported in this specification and MHD-PDUs destined for broadcast or multicast destinations are transmitted to each neighbor using the FAN TPS unicast frame transfer services.
3. Neighbor information maintained by the local node is as described in [ANSI/TIA-4957.210] Clause 4.5.3.
4. A Route and the information a local node maintains for each active route is as described in [ANSI/TIA-4957.210] Clause 4.5.4.

5.5.2.1.2.4 Route Advertisement and Maintenance Protocol

RAMP principles and services are as described in [ANSI/TIA-4957.210] Clause 4.6.

1. The principles of Service Announcement used to advertise routes are as described in [ANSI/TIA-4957.210] Clause 4.6.1.
2. The principles of Service Registration used to join a collection of nodes advertising a route to an AP is as described in [ANSI/TIA-4957.210] Clause 4.6.2.
3. The principles used in maintaining route information are as described in [ANSI/TIA-4957.210] Clause 4.6.3.
4. The means to remove information used to identify an active route are as described in [ANSI/TIA-4957.210] Clause 4.6.3.1.
5. The principles to be followed to consider an active route to no longer be active, and the means to re-establish an active route are as defined in [ANSI/TIA-4957.210] Clause 4.6.3.2.
6. Periodic route updates are as described in [ANSI/TIA-4957.210] Clause 4.6.3.3.
7. A neighbor node may be requested to directly transmit its route information as described in [ANSI/TIA-4957.210] Clause 4.6.3.4.

8. Loops and their avoidance are as described in [ANSI/TIA-4957.210] Clause 4.6.4.
9. The timers maintained by a node to support L2 MESH are as described in [ANSI/TIA-4957.210] Clause 4.6.5.
10. The Link Cost metric computation for Expected Transmission count is as described in [ANSI/TIA-4957.210] Clause 4.6.6.
11. The expression of Link Quality used in RAMP data structures is as described in [ANSI/TIA-4957.210] Clause 4.6.7.

5.5.2.2 MAC Sub-layer

The MAC sub-layer is constructed using data structures defined in [IEEE802.15.4]. Multiple modes of frequency hopping are defined.

The MAC sub-layer operates in non-beacon enabled mode (no periodic beacon frames are defined) and hence no contention free period exists. All channel access operates using contention access mode. The [IEEE802.15.4] association procedures are not used. Short addressing is not within scope of this specification.

Nodes use EUI-64 based MAC address as defined in [IEEE802.15.4]. The Data and Enhanced Acknowledge frames are used and extended with a set of Wi-SUN defined Information Elements. Further, all MAC payload is encapsulated in an [IEEE802.15.9] MPX-IE, which enables LLC protocol dispatch and L2 fragmentation.

L2 Mesh supports transfer of large payloads as a sequence of multiple frames as described in [IEEE802.15.9].

5.5.2.2.1 PAN Discovery and Joining

The MAC sub-layer supports PAN discovery and joining functions with two mechanisms:

1. A Trickle based PAN Advertisement transmission which provides bare minimum cleartext information enabling a joining node to discover and choose from one of potentially several available PANs.
2. A Trickle based, secured PAN Configuration transmission which contains full information about the PAN: active security keys, broadcast schedule, change detection, etc.

5.5.2.2.2 Frequency Hopping

The MAC sub-layer supports neighbor synchronized channel hopping for both unicast and broadcast frame transmissions.

Multiple frequency bands are defined for operation in different regions and regulatory domains. The total number of PHY channels available depends on the selected regional band and channel spacing, which is determined by the PHY configuration (see 6.4). A node may additionally advertise a set of channels to be excluded from its hopping sequence.

A “channel function” defines a method used to determine, from the list of available PHY channels, the specific channel upon which a node is operating at a given time. Multiple channel functions are supported at the MAC sub-layer, each supporting unicast and broadcast operation.

Each node advertises its channel schedules with information necessary for a neighbor node to determine on which channel a node will be operating at any given time. A node is required to listen on its advertised unicast channel schedule when a node is not transmitting or listening for broadcast messages.

Unicast and broadcast synchronization information is also exchanged between neighbors, but note that there is no dependency upon PAN-wide time synchronization.

A fixed channel mode of operation is supported for situations in which channel hopping is not desired.

5.5.2.2.3 Unicast Frame Exchange

The MAC defines two unicast frame exchange patterns:

1. A Directed Frame Exchange pattern supporting exchange of a single frame between two nodes on a single channel with or without acknowledgement.
2. An Extended Directed Frame Exchange pattern supporting exchange of multiple frames between two nodes on a single channel using Flow Control.

Unicast frequency hopping is receiver directed, with the unicast hopping sequence derived from the node's EUI-64 address and the set of available channels. A node learns its neighbor's unicast listening schedule by receiving the unicast schedule information advertised by that neighbor.

The unicast listening schedule defines when a node will be able to receive on each channel in sequence. The duration during which the node will be listening is the dwell interval. The unicast hopping sequence can be thought of as a repeating sequence of dwell intervals or "slots" where the "slot number" identifies a particular place in the sequence.

The relationship between the Unicast Slot, Unicast Dwell Interval, channel function $C(t)$, and Sequence Duration is shown in Figure 5-5.

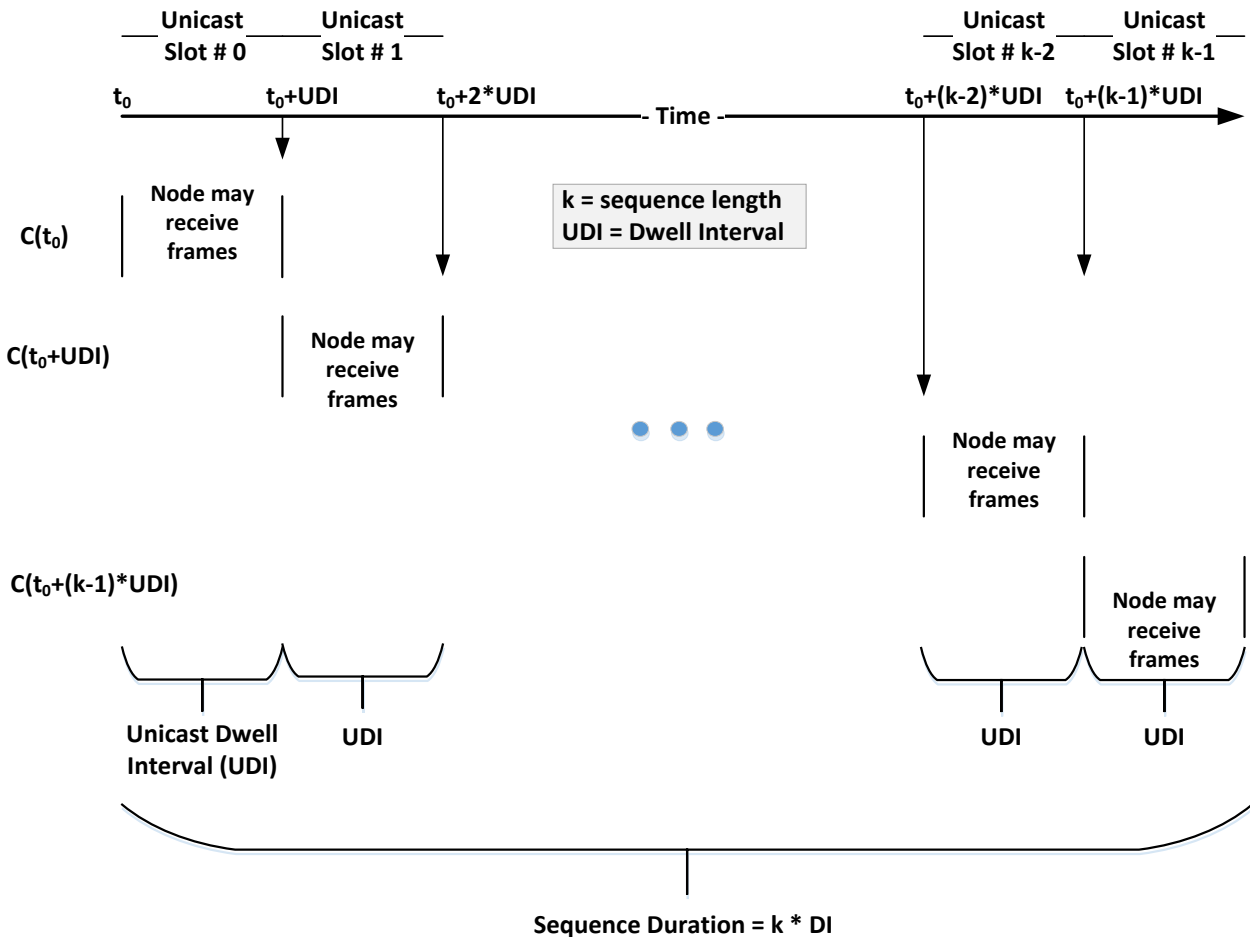


Figure 5-5 Unicast Frequency Hopping

5.5.2.2.3.1 Retransmission

Both the Directed and Extended Directed frame exchange patterns support bounded retransmission.

5.5.2.2.4 Broadcast Frame Exchange

Received discovery information (see 6.3.4.6) includes a Broadcast Schedule IE (BS IE) defining a broadcast schedule identifier (BSI), channel plan and hopping function designation, broadcast interval (BI), and broadcast dwell interval (BDI).

The broadcast interval is the duration between consecutive broadcast dwell intervals. A node transmits its broadcast schedule synchronization timing in a BT IE included in all Data frames.

A node of rank (distance from the root in hops) "n" (where n ranges from 1 to the maximum number of hops supported minus one) follows the BS-IE and BT-IE from its preferred parent at rank "n-1".

The initial BS-IE and BT-IE are created by the DODAG root when using layer 3 routing. A node at rank 'n' may advertise the same BS IE values, and a derived BT IE identifying the same active BDI, as those of its preferred parent or it may advertise a different, non-overlapping broadcast schedule and timing intended for its rank 'n+1' neighbors.

Upper layer IP multicast use of broadcast (RPL control messages, MPL, etc.) is based upon Trickle, whose consistency and suppression features are used to implement PAN wide data dissemination with a minimum amount of broadcast frame exchange.

Because [IEEE802.15.4] does not support multicast at the link layer, all IPv6 multicast transmissions are translated into link-layer broadcast. When forwarding multicast traffic, a node must transmit the broadcast data in each broadcast schedule it is tracking (if its advertised schedule is different from that of its preferred parent). Such repetition is transparent to the operation of its higher layer protocols.

The broadcast dwell interval is typically much shorter than the broadcast interval to minimize the impact of broadcast listening on unicast data transmission. This active/passive ratio (BDI/BI) reduces the efficacy of the Trickle randomization of broadcast data.

The broadcast hopping sequence can be thought of as a repeating sequence of broadcast intervals or “slots” where the “slot number” identifies a particular place in the sequence. The relationship between the Broadcast Slot, Broadcast Dwell Interval, Broadcast Interval, and Sequence Duration is depicted in Figure 5-6.

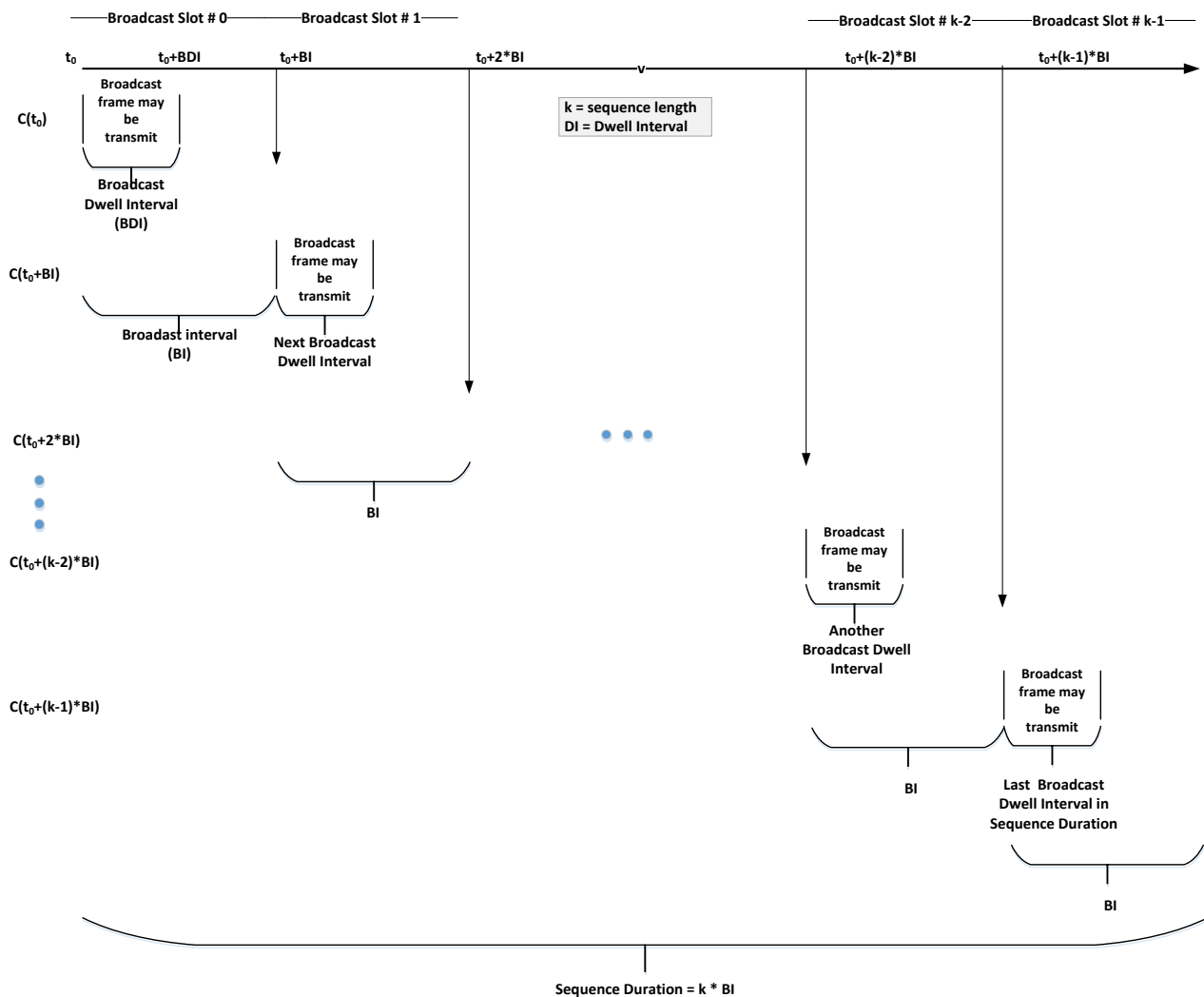


Figure 5-6 Broadcast Frequency Hopping

5.5.2.2.5 Interaction of Unicast and Broadcast

Figure 5-7 depicts the interaction of a node’s broadcast dwell intervals with the unicast channel listening schedule of several of its neighbor nodes.

1. Neighbors 1, 2, and 3 have each advertised their unicast schedules/timing to Node X. Nodes 1, 2, and 3 are listening for broadcast messaging per the broadcast schedule and timing received from Node X.

2. Note that Node X's broadcast dwell interval overlays the unicast schedules of itself and its neighbors. Also note that the unicast schedule is receiver directed, with the broadcast schedule being transmitter directed.
3. Node X will normally be listening for unicast frame transmissions on its own unicast schedule (not shown).
4. Node X transmits a unicast frame to a specific neighbor using that neighbor's unicast schedule to determine the appropriate channel.
5. When Node X has a broadcast frame ready for transmission, it will hold that frame until the start of its next Broadcast Dwell Interval, divert from its unicast listening schedule, transmit the broadcast frame, then return to its unicast listening schedule. Any node listening to the Node X broadcast transmission will receive the frame (in this example ... Nodes 1, 2, and 3).

Note that the Broadcast Interval must be adequately long versus its Broadcast Dwell Interval to allow adequate time for unicast listening.

The ratio of Unicast to Broadcast slots is highly application specific. For AMI applications, a ratio of 4:1 may be sufficient, but this ratio is highly dependent upon the application messaging patterns of the deployment architecture.

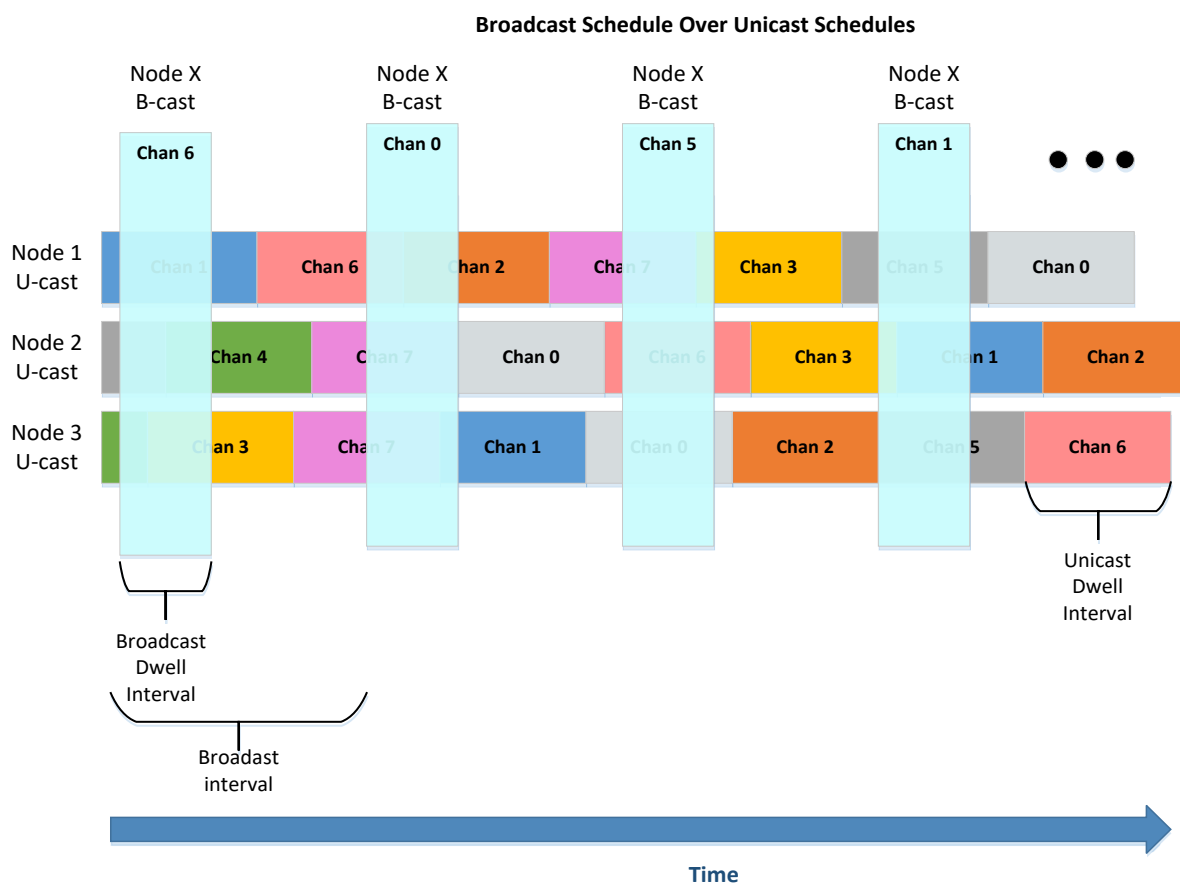


Figure 5-7 Broadcast and Unicast Schedules

5.6 PHY Service

5.6.1 General Principles

The PHY layer is derived from a sub-set of [IEEE802.15.4] as specified in Section 18

2-FSK modulation schemes, with channel spacing range from 100 to 600 kHz, are defined to provide uncoded data rates from 50 to 300 kbps. FEC is optional and based upon NRNSC code.

The PHY Protocol Data Unit (PPDU) structure is as defined in [IEEE802.15.4]. Coded and uncoded transmissions are discriminated by separate Start Words. Preamble lengths are defined based on interoperability requirements agreed by

Wi-SUN members. PHY header options are simplified by enforcing no Mode Switch, Data Whitening enabled and use of 4-octet FCS.

Radio specifications are similarly derived from [IEEE802.15.4] and specified in Section 18.

5.6.2 Node Behavior

There is limited behavior specified by the PHY Service. Control of the PHY transmit configuration is a local matter expressed in terms of PIB Attributes, but these are not exposed nor negotiated in any defined PHY layer protocol.

Interpretation of received bit-streams is as defined in the SUN FSK PHY clause of [IEEE 802.15.4].

5.7 Security

The FAN supports the following set of security mechanisms:

1. Layer 2 network access control, mutual authentication, and establishment of a secure pairwise link between a FAN node and its PAN Border Router is implemented with an adaptation of [IEEE802.1X] and [RFC5216] for [IEEE802.15.4].
 - a. Joining nodes assume the role of SUP, Border Routers assume the role of Authenticator, and a AAA service (such as RADIUS) fulfills the role of the Authentication Service.
 - b. An EAPOL Relay mechanism is defined to provide EAPOL messaging between SUP and Authenticator when the two are not within radio range of each another.
 - c. Mutual authentication is based on [IEEE802.1AR] secure device identity, with specific requirements made for the format of the FAN IDDevID (aka the device certificate).
 - d. The FAN will support both Wi-SUN approved vendor specific PKIs and a Wi-SUN PKI (provided for those vendors not desiring to operate a Certificate Authority).
2. An adaptation of the [IEEE802.11] 4-Way Handshake establishes a shorter-lived secure pairwise link between the joining node and the PAN Border Router; the 4-Way Handshake also establishes the PAN group security between all nodes of the PAN.
3. Secure node to node (pairwise) links are supported between one-hop FAN neighbors using an adaptation of [ETSI-TS-102-887-2].
4. FAN nodes implement frame Security as specified in section 9 of [IEEE802.15.4], using either the group or node to node pairwise keys previously established.
5. Misbehaving nodes are removed from a PAN by the Border Router revoking the node's pairwise keys, followed by distribution of new group keys to the remaining PAN nodes.

6 Specification

6.1 Transport Layer

6.1.1 Operation

6.1.1.1 UDP

FAN nodes MUST implement the User Datagram Protocol as defined in [RFC768].

6.1.1.2 TCP

FAN nodes MAY implement the Transport Control Protocol as defined in [RFC793].

6.2 Network Layer

6.2.1 Constants

Table 6-1 contains definitions of constants used for the FAN Network Layer.

Name	Description	Value
EAPOL_RELAY_PORT	UDP port assignment for the EAPOL Relay function.	10253
CAND_PARENT_THRESHOLD	Threshold (referenced to DEVICE_MIN_SENS) above which a neighbor node may be considered for inclusion into candidate parent set.	10 dB
CAND_PARENT_HYSTERESIS	Hysteresis factor to be applied to CAND_PARENT_THRESHOLD when admitting or dropping nodes from the candidate parent set.	3 dB
DEVICE_MIN_SENS	The vendor specific minimum receiver sensitivity level.	This value is vendor specific.

Table 6-1 Network Layer Constants

6.2.2 Data Structures.

Data structures unique to the FAN Network layer are described in this section.

6.2.2.1 EAPOL Relay Datagram.

An EAPOL Relay Datagram is a UDP datagram used by a Router's EAPOL Relay Agent to transport EAP messaging over IP between a SUP and Authenticator when they are unable to communicate directly at the MAC layer. The EAPOL Relay Datagram's payload is formatted as shown in Figure 6-1.

Octets: 8	1	Variable
SUP EUI-64	KMP ID	EAPOL PDU

Figure 6-1 EAPOL Relay Datagram

The SUP EUI-64 field MUST be set to the EUI-64 of the SUP from which or to which EAP messaging is being relayed.

The KMP ID field MUST be set to the KMP ID value obtained from the first MPX fragment of the EAPOL messaging exchange, and MUST remain set at this value for any subsequent MPX fragments relayed between the SUP and Authenticator. See section 6.3.2.3.3 for MPX Information Element (MPX-IE) details.

The EAPOL PDU field MUST contain a valid EAPOL PDU as defined in [IEEE802.1X] section 11.3.

The UDP destination port MUST be set to EAPOL_RELAY_PORT.

6.2.3 Operation

FAN nodes MUST implement Internet Protocol Version 6 as described in [RFC2460].

A Border Router's WAN interface MUST support an IPv6 MTU of 1280 bytes. A FAN node's MPX-IE upper layer fragment MUST support an MTU of 1576 bytes. The difference in the Border Router's WAN interface MTU and mesh interface MTU is due to the additional overhead required for mesh routing. The value 1576 is derived as follows:

1. IPv6 MTU: 1280 bytes.
2. Additional IPv6 header supporting IP-in-IP tunnel for packets routed into or out of the DAG: 40 bytes.
3. Routing Header supporting 24 hops: $24 \times 8 = 192$ bytes.
4. Allowance for possible use of Hop-by-Hop Options, Destination Options, etc.: 64 bytes.

FAN nodes MUST implement the L3 Routing Network Layer (section 6.2.3.1)

FAN nodes MAY implement the L2 Mesh Network Layer (section 6.2.3.2)

FAN nodes MUST NOT simultaneously operate the L3 Routing and L2 Mesh Network Layers, and the choice of L3 Routing or L2 Mesh Network operation is determined administratively via means out-of-scope of this specification.

6.2.3.1 L3 Routing Network Layer

6.2.3.1.1 6LoWPAN

FAN nodes support transmission and reception of IPv6 packets over IEEE 802.15.4 networks as described in [RFC4944] and amended by [RFC 6282]. Specifically:

1. FAN nodes MUST implement reception for the NALP Header Type as defined in [RFC4944].
2. FAN nodes MUST implement generation and reception for the IPv6 Header Type as defined in [RFC4944].
3. FAN nodes MUST implement generation and reception for IPv6 Header Compression (LOWPAN_IPHC) as defined in [RFC6282]. Stateful context based source, destination, or multicast address compression MUST NOT be used.
4. FAN nodes MUST implement generation and reception of IPv6 Extension Header Compression (LOWPAN_NHC) as defined in [RFC6282] (supporting IP-in-IP tunneling for packet forwarding).
5. FAN nodes MUST implement reception of UDP header compression as defined in [RFC6282].
6. FAN nodes MUST implement support for the FRAG1 and FRAGN Header Types as described in [RFC4944] (regardless of the FAN's minimum IPv6 MTU size, fragmentation support is desirable for high noise environments). Fragmentation and re-assembly MUST be performed on a hop-by-hop basis. Fragments MUST be transmitted in order, and indication of successful fragment delivery MUST be received before the next fragment is transmitted.
7. Multicast packets SHOULD not be fragmented. Fragmented multicast packets MUST be ignored on receipt (as layer 2 broadcast frames are unacknowledged).
8. FAN nodes MUST drop any frame containing an unknown 6LoWPAN Header Type.

6.2.3.1.2 IPv6 Addressing

This specification makes no normative requirements regarding a specific IPv6 addressing architecture, but informative guidance is presented in Appendix D.

6.2.3.1.2.1 Unicast Addresses

Unicast address mapping as specified in [RFC4944] MUST be supported. Short addressing (16 bit) is not used.

6.2.3.1.2.1.1 Link Local Addresses

FAN nodes MUST auto configure a link-local IPv6 address as described in [RFC4862].

The Interface Identifier (IID) MUST be of the modified EUI-64 format described [RFC4291], with the EUI-64 being that of the 802.15.4 FAN interface.

6.2.3.1.2.1.2 Global and Unique Local Addresses

FAN nodes implement DHCPv6 [RFC3315] to provide automated management of IPv6 GUA and ULA address assignments. DHCPv6 is used for several reasons:

1. To provide explicit control of the FAN address pool, thereby enabling maximum elision of source routing addresses in RPL Source Routing Headers.
2. To provide for delivery of additional configuration via DHCPv6 options.

Rapid Commit, using a Solicit/Reply message exchange, is the only DHCPv6 operating mode used by the FAN.

FAN Router nodes SHOULD NOT generate and MAY ignore receipt of Advertise, Rebind, Request, Renew, Release, Decline, Confirm, Reconfigure, and Information messages.

FAN Router nodes MUST implement Client behavior as defined in section 17 of [RFC3315] modified as follows:

1. A Rapid Commit Option MUST be included in the Solicit message.
2. An IA_NA option for the node's FAN interface MUST be included in the Solicit message. Temporary addresses are not used.
3. A Client Identifier option MUST be included in the Solicit message.
4. An Option Request option MAY be included in the Solicit message. Content of this option is out of scope of this specification. A Vendor Information option MAY be included in the Option Request option.
5. An Elapsed Time option MUST be included in the Solicit message.
6. Solicit messages MUST be unicast to a node's RPL preferred parent.
7. The Reply message MUST be processed as directed by section 17 of [RFC3315].
8. Client reliability mechanisms described in section 14 of [RFC3315] MUST be implemented.

Reply messages must be formatted as follows:

1. A Rapid Commit option MUST be included in the Reply message.
2. A Client Identifier option MUST be included in the Reply message.
3. A Server Identifier option MUST be included in the Reply message.
4. An IA_NA option MUST be included in the Reply message, and the IA_NA MUST contain the IAADDR for the IA_NA and/or relevant Status Code option(s).
5. A Status Code option MAY be included in the Reply message. Omission of the Status Code option indicates Success (see [RFC3315] section 22.13).
6. Vendor-specific Information options MAY be included in the Reply message. Content of this option is out of scope of this specification.

Upon expiration of an IA_NA's T1, the Router node MUST again execute the Solicit/Reply messaging exchange (this in lieu of Renew messaging). The IA_NA's value of T2 is not used. If a Router node had previously requested and received the Server Unicast Option, the node MAY unicast subsequent Solicit messaging directly to the DHCPv6 server.

A Router node MUST support the DHCPv6 Relay Agent mechanism as described in [RFC3315]. Upon receipt of a Solicit message, a Router MUST relay the Solicit message to the Border Router and relay the subsequent Reply message to the soliciting node.

A Border Router MUST support either the DHCPv6 Relay Agent mechanism or implement the Server behavior described section 17 of [RFC3315] to support the limited client exchange described above. This flexibility allows the DHCPv6 service instance to reside on the Border Router, or the Border Router may relay the DHCPv6 messaging to a remote DHCPv6 service.

The DUID-LL format MUST be used for all DHCPv6 client DUIDs, with the hardware type code set to 6 (as specified in [ARP] for IEEE 802 Networks).

DHCP server initiated configuration exchanges are not supported and MAY be ignored

DHCP authentication messaging SHOULD NOT be generated and MAY be ignored on receipt.

The following changes are made to default Transmission and Retransmission Parameters (section 5.5 of [RFC3315])

1. SOL_MAX_DELAY SHOULD default to 1 min.
2. SOL_TIMEOUT SHOULD default to 1 min.
3. SOL_MAX_RT SHOULD default to 1 hour.

FAN Router nodes MUST support a total assignment of at least 1 GUA and/or ULA, and MAY support additional GUA/ULA assignments.

6.2.3.1.2.2 Multicast Addresses

FAN nodes MAY originate multicast ICMPv6 or UDP messaging.

FAN nodes must join their FAN interface to the following IPv6 multicast groups.

Link scope:

1. A FAN node MUST join to the link-local-scope all-nodes group (ff02::1) [RFC4291].
2. A FAN node MUST join to the link-local-scope all-routers group (ff02::2) [RFC4291].
3. A FAN node MUST join to the link-local-scope all-RPL-nodes group (ff02::1a) [RFC6550].

Realm scope:

4. A FAN node MUST join to the realm-scope all-nodes group (ff03::1).
5. A FAN node MUST join to the realm-scope all-routers group (ff03::2).
6. A FAN node MUST join to the realm-scope all-mpl-forwarders group (ff03::fc).

Site and Global scope:

7. For each GUA/ULA acquired, a FAN node SHOULD subscribe to the equivalent unicast-prefix-based IPv6 multicast group (as described in [RFC3306]) supporting a MPL domain on that multicast address.

6.2.3.1.3 Duplicate Address Detection

Per [RFC6775] guidance, a FAN node's EUI-64 address is assumed to be globally unique. Duplicate Address Detection, as described in [RFC4861], is not performed.

6.2.3.1.4 Neighbor Discovery

FAN nodes MUST implement Neighbor Cache Management as described in [RFC6775].

FAN nodes MUST implement [RFC6775] Neighbor Solicitation with Address Registration Option (ARO) to resolve link layer addresses for GUAs and ULAs (to register or refresh an address registration with a neighbor). However,

once a RPL DODAG parent / child relationship has been established between nodes, a parent node SHOULD NOT use Neighbor Solicitation with ARO to register their GUAs/ULAs with their child nodes (this is unnecessary overhead, the function is fulfilled by the Prefix Information Option within DIO messaging).

A FAN node MUST NOT implement Neighbor Solicitation with the Source Link-Layer Address Option (SLLAO) [RFC 4861] (this is unnecessary as the EUI-64 within the ARO provides the node's link layer address ... see Appendix F for discussion).

If unicast IP traffic is transmitted within the lifetime of the address registration and a MAC-layer acknowledgement is received on the interface using the registered address, it is not necessary to perform the Neighbor Solicitation with ARO to refresh the lifetime of the registered address. A node that receives this unicast IP traffic shall refresh the lifetime of the registered address in its Neighbor Cache to the maximum value of the lifetime. If a node with a registered address does not receive any unicast IP traffic or Neighbor Solicitation with ARO with non-zero lifetime within the lifetime of Neighbor Cache then the device shall be removed from the Neighbor Cache.

FAN nodes MUST use Neighbor Solicitation to support Neighbor Unreachability Detection (NUD) as described in [RFC6775]. Note that Neighbor Solicitation messages issued for NUD using a link-local source address MUST NOT include the ARO (this is unnecessary overhead; link-local addresses do not require registration) and therefore do not update the lifetime of any registered GUA or ULA address.

Usage of Neighbor Advertisement, as described in [RFC6775], is modified. Neighbor Advertisement MUST NOT be transmitted in response to successful Neighbor Solicitation (address registrations or NUD). A Neighbor Advertisement MUST be transmitted only in response to a Neighbor Solicitation/Address Registration resulting in an ARO status code other than Success. See Appendix F for further informative detail.

[RFC6775] address registration/refresh, NUD, and metrics refresh operations may be combined within a single Neighbor Discovery exchange.

A FAN node MAY ignore potential neighbors which do not support the node's channel function.

The Router Solicitation/Router Advertisement exchange described RFC [6775] is not used. Router discovery is performed using [RFC6550] DIO and DIS messaging. See section 6.2.3.1.6.3 for further details. Router Solicitation/Router Advertisement as described in RFC [6775] MUST NOT be transmitted and MUST be silently discarded if received.

See Appendix F for discussion of Neighbor Discovery optimizations.

See Appendix J for an overview of a joining node's bootstrap messaging flow.

6.2.3.1.5 ICMPv6

FAN nodes MUST implement ICMPv6 message processing as described in [RFC4443] with the exception that Path MTU calculation and Packet Too Big error reporting between PAN nodes is OPTIONAL.

FAN nodes also implement several ICMPv6 message types supporting LLNs (mentioned here for completeness, normative details discussed elsewhere in this specification):

1. [RFC6775] Neighbor Solicitation w/ Address Registration Option (for resolution of GUAs and ULAs).
2. [RFC 6775] Neighbor Solicitation for Neighbor Unreachability Detection.
3. [RFC6550] RPL Control Messages (DIS, DIO, DAO, etc.).

6.2.3.1.6 Routing

FAN nodes MUST implement the non-storing downward mode of RPL as described in [RFC6550]. The routing mode in which a node operates (layer 3 RPL or layer 2 Mesh) is administratively assigned prior to node deployment.

Note that [RFC6550] normatively references Trickle [RFC6206], used for dissemination of DIOs to FAN nodes.

A FAN MUST support a single RPL instance, containing a single DODAG rooted at the FAN Border Router.

The DODAG MUST be grounded (see [RFC6550]).

6.2.3.1.6.1 Link Metrics

FAN Router nodes maintain three link metrics for each link neighbor.

1. FAN Router nodes MUST maintain an EWMA of the RSL for the node-to-neighbor direction of each neighbor link.
2. FAN Router nodes MUST maintain an EWMA of the RSL metric for the neighbor-to-node direction of each neighbor link. Neighbor-to-node RSL is maintained via reception of the RSL-IEs from the neighbor.
3. FAN Router nodes MUST maintain an EWMA of the ETX for each neighbor link.

RSL MUST be calculated as the received signal level relative to standard thermal noise (290°K) at 1 Hz bandwidth or -174 dBm. This provides a range of -174 (0) to +80 (254) dBm. (255 is reserved, see section 6.3.2.3.1.4). The RSL calculation is subsequently fed into an EWMA using a smoothing factor of 1/8.

ETX MUST be calculated as (frame transmission attempts)/(received frame acknowledgements) *128 with a maximum value of 1024, where 0 received frame acknowledgements sets ETX to the maximum value. Note this differs from [RFC6551], whose larger maximum value (65535) enables sharp increases in ETX and therefore instability in the DODAG topology.

The ETX calculation is performed at a defined epoch, with the ETX result fed into an EWMA using smoothing factor of 1/8. The ETX calculation epoch is triggered when both the following conditions are satisfied:

1. At least 4 transmissions have occurred since the last ETX calculation.
2. At least 1 minute has expired since the last ETX calculation.

At node start up, 1 transmission attempts will trigger the ETX calculation epoch (to speed boot time).

A Router node MUST calculate RSL and ETX EWMA across all acknowledged ULAD frames occurring between the node and neighbor. A Router node SHOULD refresh its neighbor link metrics at least every 30 minutes. In the absence of other messaging, a Router node SHOULD initiate NUD messaging to refresh its neighbor link metrics.

6.2.3.1.6.2 Objective Function

FAN Router nodes MUST implement the Minimum Rank Objective Function with Hysteresis (MRHOF) defined in [RFC6719].

The ETX metric (smoothed via an EWMA) MUST be used. If encountered in DIO messages, metric containers MUST be ignored.

Using the ETX metric, the neighbor path cost SHOULD be calculated per the schedule guidance provided in [RFC6719] section 3.1.

MRHOF variable and parameter defaults specified in section 5 of [RFC6719] MUST be used.

6.2.3.1.6.3 Upward Route Formation

FAN nodes MUST advertise their presence, DODAG affiliation, and routing related metrics by sending DIO messages to the link-local all-RPL-nodes multicast address. Configuration and initiation of DIO messaging is controlled by the DODAG root.

The scheduling of DIO transmission MUST be performed as described in section 8.3 of [RFC6550]. Recommended values for DEFAULT_DIO_INTERVAL_MIN, DEFAULT_DIO_INTERVAL_DOUBLINGS, and DEFAULT_DIO_REDUNDANCY_CONSTANT are provided in Table 6-2.

The specific DIO trickle settings used ultimately will depend on deployment specifics: RF environment, physical node topology, tradeoff between DODAG convergence time versus DIO messaging overhead, etc.

DIO messages MUST be populated per the defaults described in [RFC6550], with the following additional requirements:

1. The RPLInstanceID MUST be of the global form.
2. The G flag MUST be set to 1 (the DODAG is grounded).

3. The MOP field MUST be set to 1 (Non-Storing mode of RPL).
4. The DODAGID MUST be set to the routable IPv6 address of the DODAG root.
5. A Prefix Information Option MUST be included for each routable IPv6 address intended by the parent to be used by the child for upward DODAG routing (a full GUA and/or ULA). These addresses will be later reported by the child to the DODAG root (within Transit Information Options contained within a DAO message).
6. Prefix Information Options MAY be included to provide an IPv6 address prefix for each Global and/or Unique Local prefix active within the DODAG (potentially supporting auto configuration for GUAs and ULAs). The prefix is intended for use by an optional automatic address formation mechanism whose details are out of scope of this specification.
7. A DODAG Configuration Option MUST be included and MUST be populated per the defaults specified in [RFC6550], with following additional requirements:
 - a. The Authentication Enabled flag MUST be set to 0.
 - b. The MaxRankIncrease field MUST be set to 0 (for loop avoidance).
 - c. The OCP field MUST be set to 1 to indicate usage of the MRHOF objective function.
 - d. The Default Lifetime field MUST be set to 120.
 - e. The Lifetime Unit field MUST be set to 60.
 - f. The PCS field MUST be set to 7 (meaning 8 bits are used for DAO Transit Information Option / Path Control field).
 - g. The MinHopRankIncrease field MUST be set to 128.

A FAN Router node MAY wait for DIO messages, MAY solicit a DIO by issuing a unicast DIS to a likely neighbor, or MAY solicit a DIO by issuing a multicast DIS (as described in [RFC6550]). It is RECOMMENDED that multicast DIS be used only when necessary (in situations where a node believes itself to have a limited number of neighbors). A FAN node MUST respond to unicast or multicast DIS messages with an appropriate DIO (see [RFC6550] section 8.3).

A FAN Router node determines its upward routes as follows.

1. It is RECOMMENDED that a FAN node determine a set of candidate parents as the set of all neighbor nodes, from which a DIO has been received, whose node-to-neighbor and neighbor-to-node RSL EWMA values both exceed the minimum threshold of CAND_PARENT_THRESHOLD using a hysteresis factor of CAND_PARENT_HYSTERESIS.
 - a. For a node to be admitted to the candidate parent set, both its node-to-neighbor and neighbor-to-node RSL EWMA values should exceed (DEVICE_MIN_SENS + CAND_PARENT_THRESHOLD + CAND_PARENT_HYSTERESIS).
 - b. For a node to be removed from the candidate parent set, both its node-to-neighbor and neighbor-to-node RSL EWMA values should fall below (DEVICE_MIN_SENS + CAND_PARENT_THRESHOLD - CAND_PARENT_HYSTERESIS).
2. A FAN node MUST apply the Objective Function to its set of available candidate parents to rank parent/route selections to the DAG root thereby determining its parent set. The parent set MUST contain the preferred parent (as determined by the Objective Function) and MUST contain at least one alternate parent (when available).
3. The preferred parent MUST be configured as the node's default upward route to the DAG root.
4. A FAN node MUST be capable to maintain at least two upward routes to the DAG route and MUST do so when more than one parent is available.

6.2.3.1.6.4 Downward Route Formation

FAN Router nodes MUST establish downward routes by unicasting DAO messages, containing the node's GUA/ULA addresses and the GUA/ULA of all the node's parents, directly to the DODAG root. Prior to issuance of DAO messaging, the Router node MUST execute Neighbor Solicitation (with ARO) to register its GUA/ULA addresses with each parent that will be included in the DAO messaging (enabling routing of DAO Acknowledgements back to the node).

The DODAG root uses this information to determine source routes to be used for delivery of IPv6 datagrams downward from the root to individual FAN nodes (all downward routing is based on source routes maintained at the DODAG root).

The DAO message transmission schedule MUST adhere to the guidance provided in [RFC6550]. DAO transmission typically occurs with a change in a node's reachability (e.g. establishing first DAG parent, significant change in DAG parent set, etc.).

DAO messages MUST be populated per the defaults described in [RFC6550], with the following additional requirements:

1. The RPLInstanceID MUST be of the global form.
2. The K flag MUST be set to 1.
3. The D flag MUST be set to 0 when the DODAGID field is not included.
4. A RPL Target option MUST be included and populated for each GUA/ULA to be advertised to the DODAG root.
5. A Transit Information Option MUST be included for each member of the parent set, populated with the parent's GUA/ULA. The Path Control field MUST be populated to correctly rank the priority of each Transit Information Option (i.e. the preferred parent is indicated as the single member of PC1, the first alternate parent set as the single member of PC2, etc.).

Note that DAOs are acknowledged. FAN Router nodes SHOULD implement a binary exponential retransmission mechanism (as described in section 14 of [RFC3315]) until either the corresponding DAO-ACK is received or the retry mechanism has exhausted its maximum attempts.

6.2.3.1.7 Unicast Forwarding

Upward forwarding of unicast packets MUST adhere to the guidance provided in section 11 of [RFC6550], which describes the usage of the RPL Option [RFC6553] with IPv6-in-IPv6 tunneling [RFC2473] (outer header contains the parent link-local address).

Downward forwarding of unicast packets MUST adhere to the guidance provided in section 11 of [RFC6550], which describes the usage of the Source Routing Header [RFC6554] with IPv6-in-IPv6 tunneling [RFC2473] (outer header contains the SRH). Datagrams containing a RPL Source Routing Header MUST be forwarded to the next hop as specified by the Source Routing Header.

In both the upward and downward forwarding case, the inner packet of the tunnel contains the original IPv6 packet (source and destination addresses, etc.).

6.2.3.1.8 Multicast Forwarding

FAN nodes MUST implement [MPL] to support dissemination of IPv6 multicast packets. Because [IEEE802.15.4] does not directly support multicast at the link layer, all IPv6 multicast transmissions utilize the Broadcast Frame Exchange described in section 6.3.4.4.

The Proactive Forwarding mode of MPL MUST be used. The Reactive Forwarding mode of MPL and related MPL Control messages MUST NOT be used. MPL behavior is driven entirely via MPL data messages.

A FAN node MUST join its FAN interface to the realm-scope all-mpl-forwarders multicast group (the default MPL domain).

A FAN node MAY join its FAN interface to other realm-scope multicast groups.

Each IPv6 multicast message transmitted in the FAN MUST contain a MPL Option populated as described in [MPL] with the following additional requirements:

1. A MPL Seed MUST implement the MPL Data Message with MPL Option S field value set to 3 and the seed-id field set to the GUA\ULA of the message seed.
2. It is RECOMMENDED that MPL Forwarders support the MPL Option with S field value set to 0, 1, 2, or 3.

FAN nodes must configure MPL Parameters to the defaults specified in section 5.4 of [MPL], with DATA_MESSAGE_IMIN and DATA_MESSAGE_IMAX set according to Table 6-2a.

6.2.3.2 L2 Mesh Network Layer

This sub-clause applies when a node implements Layer 2 Mesh using Multi-Hop Delivery Service.

6.2.3.2.1 6LoWPAN

FAN nodes MUST implement Uncompressed IPv6 Headers as defined in [RFC 4944]

6.2.3.2.2 IPv6 Addressing

6.2.3.2.2.1 Unicast Addresses

6.2.3.2.2.1.1 Link Local Addresses

FAN nodes MUST auto configure a link-local IPv6 address as described in [RFC4862].

6.2.3.2.2.1.2 Global and Unique Local Addresses

FAN nodes MUST acquire the prefix information from the MHDS-IE to provide automated generation of IPv6 GUA and ULA addresses.

FAN nodes MUST support a total assignment of at least 2 GUA and/or ULA.

6.2.3.2.3 Duplicate Address Detection

Per [RFC6775], a FAN node's EUI-64 address is assumed to be globally unique. Duplicate Address Detection, as described in [RFC4861], must not be used for any address types.

6.2.3.2.4 IPv6 Neighbor Discovery

Neighbor Discovery, as described in Section 6.2.3.1.4, MUST be implemented with the following modification:

1. Router Discovery using [RFC6550] DIO and DIS messaging is not performed.

The message flow for Address Registration is depicted in Figure 6-2 Address Registration. Note that Address De-registration is optional.