



IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats

IEEE Instrumentation and Measurement Society

Sponsored by the
Technical Committee on Sensor Technology (TC-9)

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

5 October 2007

IEEE Std 1451.5™-2007

IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats

Sponsor

Technical Committee on Sensor Technology (TC-9)
of the
IEEE Instrumentation and Measurement Society

Approved 22 March 2007

IEEE-SA Standards Board

Abstract: This standard defines a wireless interface for sensors. It specifies radio-specific protocols for this wireless interface. It defines communication modules that connect the wireless transducer interface module (WTIM) and the network-capable applications processor (NCAP) using the radio-specific protocols. It also defines the Transducer Electronic Data Sheets (TEDS) for the radio-specific protocols.

Keywords: network-capable applications processor, sensor, Transducer Electronic Data Sheet, wireless communication protocol, wireless sensor, wireless transducer interface module

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

Copyright © 2007 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 5 October 2007. Printed in the United States of America.

IEEE and ZigBee are registered trademarks in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

Bluetooth is a registered trademark in the U.S. Patent & Trademark Office, owned by Bluetooth SIG and used by the IEEE under license.

CORBA is a registered trademark in the U.S. Patent & Trademark Office, owned by the Object Management Group, Inc.

Print: ISBN 0-7381-5599-3 SH95685
PDF: ISBN 0-7381-5600-0 SS95685

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.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied **“AS IS.”**

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. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, 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 publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received 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 interpretation requests except in those cases where the matter has previously received formal consideration. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

This introduction is not part of IEEE Std 1451.5-2007, IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats.

The purpose of this document is to define an IEEE wireless interface standard for sensors. This standard specifies radio-specific protocols for achieving this wireless interface. Where appropriate, Transducer Electronic Data Sheets (TEDS) are also defined for the radio-specific protocols and OSI network layers.

Notice to users

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

Patents

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 with respect to the existence or validity of any patent rights in connection therewith. 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 are reasonable or non-discriminatory. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the Wireless Sensor Working Group had the following membership:

Steven Chen, Chair
Ryon K. Coleman, Editor/IEEE 802.11 Subgroup Chair
Peter Flittner, Bluetooth Subgroup Chair
Ken Cornett, IEEE 802.15.4 Subgroup Chair

Thurston Brooks
Jeff Burch
Matt Call
Lee H. Eccles
Robin Heydon

Jens Hult
Charles H. Jones
Kang Lee
Wayne Manges
Dan Maxwell
Jay J. Nemeth-Johannes

David B. Perrussel
Andy Segal
Victoria K. Sweetser
Darold Wobschall
Shang-Tae Yee

Other individuals who have contributed to this standard are as follows:

Wayne Catlin
Benga Erinle
Fernando Gen-Kuong
Pat Gonia
Chris Guo
Chris Herzog

Gerard Hill
Robert N. Johnson
Hesh Kagan
Alice Law
Ryan Maley

Mike Moore
Geoff Mulligan
Steve Smith
Charles Summey
Amos Young
Tiebing Zhang

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

William J. Ackerman
Chris B. Bagge
Jefferson B. Burch
Juan C. Carreon
Keith Chow
Ryon K. Coleman
Tommy P. Cooper
Matthew T. Davis
David B. Droste
Lee H. Eccles
Michael D. Geipel
Fernando Genkuong
Sergiu R. Goma
Patrick S. Gonia
Randall C. Groves
Werner Hoelzl

Dennis Horwitz
Jens Hult
Jose A. Jarque
Robert N. Johnson
Charles H. Jones
Innocent Kamwa
Piotr Karocki
James C. Kemerling
Edward Koch
Charles A. Lennon, Jr.
William Lumpkins
G. L. Luri
Gary L. Michel
Yinghua Min
Georges F. Montillet
Jerry R. Murphy
Jay J. Nemeth-Johannes

Michael S. Newman
Chris L. Osterloh
Howard W. Penrose
David B. Perrussel
Vikram Punj
Bogdan Seliger
Thomas M. Siep
Matthew L. Smith
Victoria K. Sweetser
Leroy O. Thielman
Stephen C. Webb
Darold Wobschall
Derek T. Woo
Eric V. Woods
Oren Yuen
Janusz Zalewski

When the IEEE-SA Standards Board approved this standard on 22 March 2007, it had the following membership:

Steve M. Mills, *Chair*
Robert M. Grow, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Richard DeBlasio
Alex Gelman
William R. Goldbach
Arnold M. Greenspan
Joanna N. Guenin
Julian Forster*
Kenneth S. Hanus
William B. Hopf

Richard H. Hulett
Hermann Koch
Joseph L. Koepfinger*
John Kulick
David J. Law
Glenn Parsons
Ronald C. Petersen
Tom A. Prevost

Narayanan Ramachandran
Greg Ratta
Robby Robson
Anne-Marie Sahazizian
Virginia C. Sulzberger
Malcolm V. Thaden
Richard L. Townsend
Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Alan H. Cookson, *NIST Representative*

Don Messina
IEEE Standards Program Manager, Document Development

Norma B. Davis
IEEE Standards Program Manager, Technical Program Development

Contents

1	Overview	1
1.3	Scope	1
1.4	Purpose	1
1.5	Conformance	2
2	Normative references.....	2
3	Definitions, acronyms, and abbreviations	4
3.1	Definitions	4
3.2	Acronyms and abbreviations	6
4	Data types.....	8
4.1	Unsigned octet integer.....	8
4.2	Unsigned 16 bit integer	8
4.3	Unsigned 32 bit integer	8
4.4	Boolean.....	8
4.5	String	9
4.6	Arbitrary octet array	9
5	Common IEEE 1451.5 Wireless Interface Definitions.....	9
5.1	General role definitions	10
5.2	General role configurations	10
5.3	PHY TEDS	12
5.4	NCAP radio state diagram.....	18
5.5	WTIM radio state diagram	19
5.6	Quality of service	20
5.7	Error codes	21
6	IEEE 802.11 radio sub-specification.....	22
6.1	Layered approach within IEEE 802.11 radio sub-specification	23
6.2	IEEE 802.11 MAC and PHY specifications.....	24
6.3	Internet Protocol Version 4 (IPv4) Specification (optional).....	29
6.4	Internet Protocol Version 6 (IPv6) Specification (optional).....	30
6.5	Transmission Control Protocol (TCP) Specification (optional)	30
6.6	User Datagram Protocol (UDP) Specification (optional).....	30
6.7	Discovery, communication, and group creation mechanics	30
6.8	Convergence layer.....	33
6.9	PHY TEDS.....	74
7	Bluetooth radio sub-specification.....	79
7.1	Introduction	79
7.2	Bluetooth IEEE 1451.5 stack	79
7.3	Profile fundamentals.....	80
7.4	Bluetooth NCAP functional specification	84
7.5	Bluetooth WTIM functional specification.....	89
7.6	Quality of service	94
7.7	Security.....	96
7.8	Convergence layer.....	96
7.9	PHY TEDS.....	131

8	ZigBee radio sub-specification.....	131
8.1	Introduction	131
8.2	ZigBee architecture	132
8.3	Application, profile, and cluster details.....	133
8.4	ZigBee NCAP functional specification	138
8.5	ZigBee WTIM functional specification.....	141
8.6	Quality of service	143
8.7	Security.....	143
8.8	Convergence layer	143
8.9	PHY TEDS	176
9	6LoWPAN Radio sub-specification	176
9.1	6LoWPAN architecture	176
9.2	Convergence layer	181
9.3	PHY TEDS	213
	Annex A (informative) IPv4 reference.....	214
	Annex B (informative) IPv6 reference.....	217
	Annex C (informative) TCP reference	221
	Annex D (informative) UDP reference	232
	Annex E (informative) TEDS read and write protocols.....	234
	Annex F (informative) Bibliography.....	235

IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats

1. Overview

This standard introduces the concept of a Wireless Transducer Interface Module (WTIM), connected wirelessly over an approved radio Communication Module to a Network-Capable Application Processor (NCAP) Service Module. The IEEE 1451.5 approved radios (Dot5AR) are IEEE 802.11™, IEEE 802.15.4™, IEEE Bluetooth™, and IEEE ZigBee™ technologies. A WTIM is a module that contains a Dot5ApprovedRadio, signal conditioning, analog-to-digital, and/or digital-to-analog conversion and in many cases the transducers (sensors and actuators). A WTIM may range in complexity from a single sensor or actuator plus radio to units containing many transducers plus radio. Although the WTIM contains a Dot5AR for wireless communication, the NCAP in-turn contains a similar radio to complete the wireless communication link between NCAP and WTIM. This specification for this standard focuses on the communication modules that connect the WTIM and NCAP using the Dot5AR protocols.

This standard is organized as follows: Clause 1: “Overview” provides the scope of this standard. Clause 2: “References” lists references to other standards and documents that are useful in applying this standard. Clause 3: “Definitions” provides definitions that are either not found in other standards or have been modified for use with this standard. Clause 4: “Data types” defines the data types used in the standard. Clause 5 defines the commonality section among the supported PHYs. Clause 6 through Clause 8 outline the details of each respective PHY. The annexes are included for completeness.

1.1 Scope

This project establishes a standard for wireless communication methods and data format for transducers (sensors and actuators). The standard defines a TEDS based on the IEEE 1451 concept and protocols to access TEDS and transducer data. It adopts necessary wireless interfaces and protocols to facilitate the use of technically differentiated, existing wireless technology solutions. It does not specify transducer design, signal conditioning, wireless system physical design or use, or use of TEDS.

1.2 Purpose

Many companies are developing various wireless communication interfaces and protocols for sensors. An openly defined wireless transducer communication standard, which may accommodate various existing

wireless technologies, will reduce risk for users, transducer manufacturers, and system integrators. It will enhance the acceptance of the wireless technology for transducers connectivity.

1.3 Conformance

Conformance to this IEEE 1451.5 specification requires that all nonoptional sections be implemented in the vendor device.

1.3.1 Conformance keywords

Several keywords are used to differentiate among various levels of requirements and optionality, as follows.

1.3.1.1 Shall

The key word “shall” indicates a mandatory requirement. Designers are required to implement all such mandatory requirements to ensure interoperability with other products that conform to the radio specification for this standard.

1.3.1.2 Recommended

Recommended is a keyword indicating flexibility of choice with a strong preference alternative. The word “should” has the same meaning.

1.3.1.3 Should

Should is a keyword indicating flexibility of choice with a strong preference alternative. The phrase *it is recommended* has the same meaning.

1.3.1.4 May

May is a keyword that indicates flexibility of choice with no implied preference.

2. Normative references

This standard shall be used in conjunction with the following standards publications. When the following standards are superseded by an approved revision, the revision shall apply.

Bluetooth Special Interest Group, “Core Specification Version 1.2,” Specification of the Bluetooth System, Nov. 5, 2003. [BT_Core_v1_2.PDF.]¹

Bluetooth Special Interest Group, “Core Specification Version 2.0 + EDR,” Specification of the Bluetooth System, Nov. 4, 2004. [Core v2.0 + EDR.PDF.]

Bluetooth Special Interest Group, “BNEP Specification,” Bluetooth Network Encapsulation Protocol (BNEP) Specification, Feb. 14, 2003. [BNEP Specification. PDF.]

¹Bluetooth publications are available from the Bluetooth Special Interest Group (SIG) on the World Wide Web at <http://www.gvinedesigns.com/shopping/bluetooth/>.

draft-ietf-6lowpan-problem-05, “6LoWPAN: Overview, Assumptions, Problem Statement and Goals,” Aug. 3, 2006.

draft-ietf-6lowpan-format-04, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks,” Aug. 3, 2006.

Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation, 6 October 2000.²

IEEE Std 802.11™-2007, 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 802.11a™-1999, Supplement to 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: High-Speed Physical Layer in the 5 GHz Band.

IEEE Std 802.11b™-1999, Supplement to 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: Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

IEEE Std 802.11b™-1999/Cor 1-2001, 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: Amendment 2: Higher-Speed Physical Layer (PHY) Extension in the 2.4 GHz Band—Corrigendum 1.

IEEE Std 802.11e™-2004, Supplement to 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: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements.

IEEE Std 802.11g™-2003, Supplement to 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: Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band.

IEEE Std 802.11i™-2004, Supplement to 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: Amendment 6: Medium Access Control (MAC) Security Enhancements.

IEEE Std 802.15.4™-2003, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs).

IEEE Std 1451.0™-2007, IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Common Functions, Communications Protocols, and Transducer Electronic Data Sheet (TEDS) Formats.

IEEE Std 1451.1™-1999, IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Network Capable Application Processor (NCAP) Information Model.

² Documents on the eXtensible Markup language can be downloaded from <http://www.w3.org/TR/2000/REC-xml-20001006> or ordered from the World Wide Web Consortium, c/o MIT, 32 Vassar Street, Room 32-G515, Cambridge, MA 02139, USA.

IEEE Std 1451.2™-1997, IEEE Standard for a Smart Transducer Interface for Sensors and Actuators—Transducer to Microprocessor Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats.

IETF RFC 768, User Datagram Protocol (UDP), Aug. 1980.³

IETF RFC 791, Internet Protocol, DARPA Internet Program, Protocol Specification (IPv4), Sept. 1981.

IETF RFC 793, Transmission Control Protocol, DARPA Internet Program, Protocol Specification (TCP), Sept. 1981.

IETF RFC 1752, The Recommendation for the IP Next Generation Protocol (IPv6), Jan. 1995.

IETF RFC 2460, The Recommendation for the IP Next Generation Protocol, Internet Protocol, Version 6 (IPv6) Specification, Dec. 1998.

ISO 639: 1988-04-01 (E/F), Codes for the Representation of Names of Languages.⁴

ISO/IEC 14750: 1999-03-15, Information technology—Open Distributed Processing—Interface Definition Language.⁵

ITU Recommendation G.989.2, Phoneline networking transceivers—Payload format and link layer requirements.⁶

Taylor, B. N., and Kuyatt, C. E., *Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results*, National Institute of Standards and Technology Technical Note 1297, National Institute of Standards and Technology, Gaithersburg, MD, 1994 edition.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms* [B6]⁷ should be referenced for terms not defined in this clause.

3.1.1 acknowledge: A reply message used to indicate that a command or trigger message was received.

3.1.2 actuator: A transducer that accepts a data sample or samples and converts them into physical action.

3.1.3 address: A character or group of characters that identifies a register, a particular part of storage, or some other data source or destination.

3.1.4 AddressGroup: A collection of TransducerChannels that respond to a single address.

³ IETF publications are available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112, USA (<http://global.ihs.com/>).

⁴ ISO publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembe, CH-1211, Genève 20, Switzerland/ Suisse (<http://www.iso.ch/>). ISO publications are also available in the United States from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

⁵ ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse (<http://www.iso.ch/>). ISO/IEC publications are also available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112, USA (<http://global.ihs.com/>). Electronic copies are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

⁶ ITU-T publications are available from the International Telecommunications Union, Place des Nations, CH-1211, Geneva 20, Switzerland/Suisse (<http://www.itu.int/>).

⁷ The numbers in brackets correspond to those in the bibliography in Annex A.

3.1.5 buffer: An intermediate data storage location used to compensate for the difference in rate of flow of data or time of occurrence of events when transmitting information from one device to another.

3.1.6 byte: A group of 8 bits. *Syn:* **octet**.

3.1.7 controller: A device, possibly an network-capable applications processor (NCAP), which acts as the master to control all of the devices on a transducer network.

3.1.8 data sheet: A set of information on a device that defines the parameters of operation and conditions of usage (usually produced by the device's manufacturer).

3.1.9 electronic data sheet: A data sheet stored in some form of electrically readable memory (as opposed to a piece of paper).

3.1.10 enumeration: The assignment of a numeric value to a specific meaning within the context of a specific data field. Binary numbers are usually expressed in decimal terms for human convenience. Not all possible numeric values need to have a specific meaning. Values without meaning are declared to be unused or reserved for future use. Enumeration is the process of declaring the encoding of human interpretable information in a manner convenient for digital electronic machine storage and interchange. Any subclause that defines a Transducer Electronic Data Sheet data field to be enumerated shall contain a table that defines the meaning of the data field for each numeric value possible. The meanings encoded in each data field shall be specific and unique to that data field and only to that data field. The value becomes meaningless if not associated with the data field and its defining table.

3.1.11 event sensor: A sensor that detects a change of state in the physical world. The fact that a change of state has occurred and/or instant in time of the change of state, not the state value, is the “measurement.”

3.1.12 hot swap: The act of connecting or disconnecting a transducer interface module (TIM) from a transducer interface medium without first turning off the power that is supplied to the TIM over the medium.

3.1.13 message: Information that is to be passed between devices as a single logical entity. A message may occupy one or more packets.

3.1.14 network-capable application processor (NCAP): A device between the transducer modules and the network. The NCAP performs network communications, transducer interface module communications, and data conversion or other processing functions.

3.1.15 octet: A group of 8 bits. *Syn.:* **byte**.

3.1.16 packet: A block of information that is to be passed by the physical layer between devices in a single transmission.

3.1.17 sensor: A transducer that converts a physical, biological, or chemical parameter into an electrical signal.

3.1.18 signal conditioning: The transducer signal processing that involves operations such as amplification, compensation, filtering, and normalization.

3.1.19 smart transducer: A transducer that provides functions beyond those necessary for generating a correct representation of a sensed or controlled quantity. This functionality typically simplifies the integration of the transducer into applications in a networked environment.

3.1.20 transducer: A device that converts energy from one domain into another. The device may be either a sensor or an actuator.

3.1.21 transducer interface module (TIM): A module that contains the Transducer Electronic Data Sheet, logic to implement the transducer interface, the transducer(s) or connection to the transducer(s), and any signal conversion or signal conditioning.

3.1.22 TransducerChannel: A transducer and all of the signal conditioning and conversion components associated with that transducer.

3.1.23 Transducer Electronic Data Sheet (TEDS): An electronic data sheet describing a transducer interface module or a TransducerChannel. The structures of multiple TEDS are described in this standard.

3.1.24 transfer: The act or process of moving information from one digital device to another.

3.1.25 trigger: A signal or message that is used to start an action.

3.2.26 Wireless Transducer Interface Module (WTIM): A module that contains the radio communication module, Transducer Electronic Data Sheet, logic to implement the Transducer interface, the transducer(s) or connection to the transducer(s) and any signal conversion or signal conditioning.

3.2.27 ZigBee™: A meshed, low-power, wireless network standard built atop IEEE Std 802.15.4-2003.

3.2 Acronyms and abbreviations

6LoWPAN	wireless personal area network utilizing mesh networking and IPv6
ACK	acknowledgment
ACL	asynchronous connectionless link
AES	advanced encryption standard
AP	access point
API	application programming interface
BB	Bluetooth baseband
BD_ADDR	Bluetooth MAC-sublayer address
BNP	Bluetooth network encapsulation protocol
BSS	basic service set
CAPI	communications application program interface
CCMP	counter mode encryption with cipher-block-chaining message-authenticate-code authentication
CDMA	code-division multiple access
CM	connection manager
Comm	communication
CORBA®	common object request broker architecture, reference <i>OMG Common Object Request Broker Architecture (CORBA/IIOP)</i> [B13]
CRC	cyclic redundancy check
DARPA	Defense Advanced Research Projects Agency
DCF	distributed coordination function
DHCP	dynamic host configuration protocol
DNS	domain name server
Dot5AR	An IEEE 1451.5 approved radio
DS	distribution system
DSM	distribution system medium
DSSS	direct sequence spread spectrum
DTIM	delivery traffic indication message
EAP	extensible authentication protocol (RFC 2284)
EAPOL	EAP over LANs (IEEE 802.1X)
EMT	emulator trap
ERP	extended rate PHY
eSCO	extended Synchronous Connections
ESS	extended service set
FHSS	frequency hopping spread spectrum
FIN	finished control flag (No more data from sender) in TCP
GAP	generic access profile
HCI	host controller interface

HTML	Hypertext markup language
HRDSSS	high-rate direct sequence spread spectrum
IBSS	independent basic service set
ID	identifier
IE	Information Element
IETF	Internet Engineering Task Force
IHV	independent hardware vendor
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
L2CAP	logical link control and adaptation layer protocol
LAN	local area network
LM	link manager
LLC	logical link control
LoWPAN	low-power, low-cost, low-data-rate wireless personal area network
MAC	medium access control
MIB	management information base
MIC	message integrity code
MLME	MAC sublayer management entity
MMPDU	MAC management protocol data unit
MSDU	MAC service data unit
NCAP	network-capable applications processor
OFDM	orthogonal frequency division multiplexing
OMG	Object Management Group, consortium committed to developing technically excellent, commercially viable and vendor-independent specifications for software industry
PAN	personal area network
PBCC	packet binary convolutional coding
PCF	point coordination function
PHY	physical layer
PLCP	physical layer convergence procedure
PLME	physical layer management entity
PMD	physical medium dependent
PMKID	pairwise master key identification
PSK	pre-shared keys
QoS	quality of service
RFC	request for comments (often used to define Internet protocols)
RSN	robust security network
RSNA	robust security network association
SAID	security association identifier
SAP	service access point
SCO	synchronous connected oriented
SDP	session description protocol
SDU	service data unit
SI	International System of Units, <i>The International System of Units (SI)</i> [B15]
SIG	special interest group
SME	station management entity
ST	Stream Protocol
STA	station
SVC	supervisor call
SYN	Synchronize sequence numbers control flag
TCB	transmission control block
TCP	transmission control protocol
TEDS	Transducer Electronic Data Sheet
TKIP	temporal key integrity protocol
TLV	type/length/value data structure
UDP	user datagram protocol

UML	unified modeling language, reference <i>The Unified Modeling Language User Guide</i> [B2], OMG Unified Modeling Language Specification [B12], <i>Doing Hard Time: Developing Real-Time Systems with UML, Objects, Frameworks and Patterns</i> [B14]
UUO	Unimplemented user operation
WEP	wired equivalent privacy
WM	wireless medium
WPA	wi-fi protected access
WTIM	wireless transducer interface module
XML	eXtensible Markup Language
ZD_ADDR	ZigBee™ network layer address

4. Data types

All data types used throughout the remainder of this standard are defined in subordinate subclauses.

4.1 Unsigned octet integer

Symbol: UInt8

Size: 1 octet

IDL: `typedef octet UInt8;`

This data type represents positive integers from 0 to 255.

4.2 Unsigned 16 bit integer

Symbol: UInt16

Size: 2 octets

IDL: `typedef unsigned short UInt16;`

This data type is used to represent positive integers from 0 to 65 535.

4.3 Unsigned 32 bit integer

Symbol: UInt32

Size: 4 octets

IDL: `typedef unsigned long UInt32;`

This data type is used to represent unsigned integers from 0 to 4 294 967 295. The value shall be interpreted as the length in octets of an associated field or data block.

When used to specify the length of a data block (more than one field), the length field shall not include the length of the length field itself.

4.4 Boolean

Symbol: `_Boolean`

Size: 1 octet

IDL: `typedef boolean _Boolean; // Leading '_' to escape reserved IDL keyword`

For the purposes of this standard, a bit or octet with a nonzero value is considered True. A zero value represents the False state of the variable.

4.5 String

The use of text strings as defined in IEEE Std 1451.2-1997 has been replaced with the use of the eXtensible Markup Language (XML) in this standard. The controlling document for XML is the W3C Recommendation *Extensible Markup Language (XML) 1.0 (Second Edition)*. All text strings in the TEDS shall conform to this recommendation or a future update to it.

4.6 Arbitrary octet array

Symbol: OctetArray

Size: varies

This data type comprises an arbitrary number of octets, treated as an aggregate entity that may or may not be interpreted as a number. An OctetArray may be a structure comprising one or more primitive data types, arrays of primitive data types, or smaller OctetArrays.

5. Common IEEE 1451.5 Wireless Interface Definitions

The purpose of this clause is to define the common features of the IEEE 1451.5 specification that shall apply to all the radio sub-specifications.

As shown in Figure 1, from left to right, the NCAP IEEE 1451.0 Services interface with the NCAP IEEE 1451.5 Communication Module through the IEEE 1451.0/5 Communications API. The NCAP IEEE 1451.5 Communication Module communicates with the WTIM IEEE 1451.5 Communication Module through the IEEE 1451.5 Radio wireless PHY. On the WTIM, the WTIM IEEE 1451.0 Services interfaces with the WTIM IEEE 1451.5 Communication Module through the IEEE 1451.0/5 Communications API. What is shown shaded in Figure 1 includes the logical and physical partitioning that is covered by the radio sub-specifications for IEEE 1451.5 services.

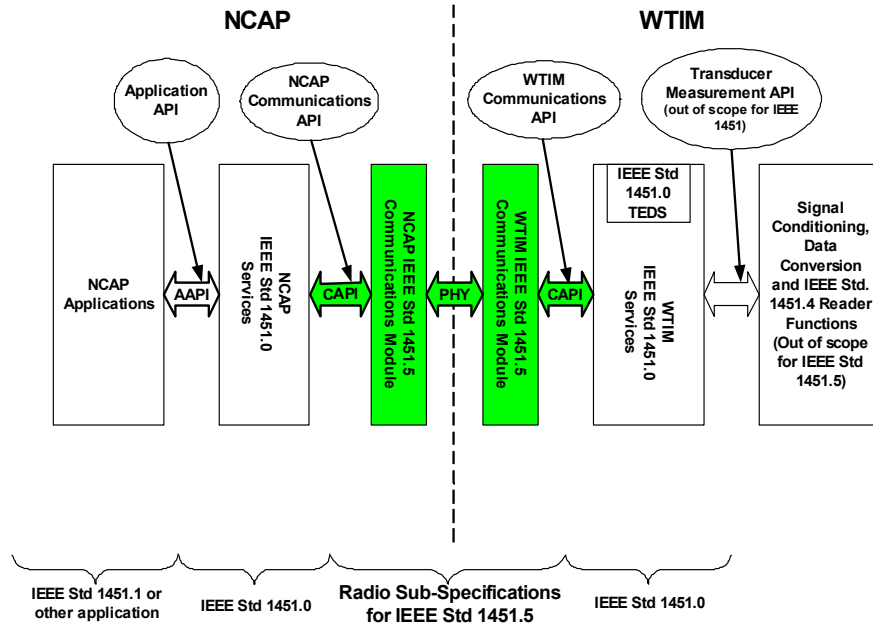


Figure 1—Functional context for the radio sub-specifications for IEEE 1451.5 services

5.1 General role definitions

An NCAP may route commands and data from an external network to/from a transducer connected to a WTIM.

An NCAP may register multiple WTIMs.

A WTIM shall only be registered with a single NCAP.

A WTIM may interface to multiple transducers.

WTIM-to-WTIM communication is allowed.

5.2 General role configurations

Figure 2 and Figure 3 show typical configurations of devices for which an IEEE 1451.5 configuration is applicable.

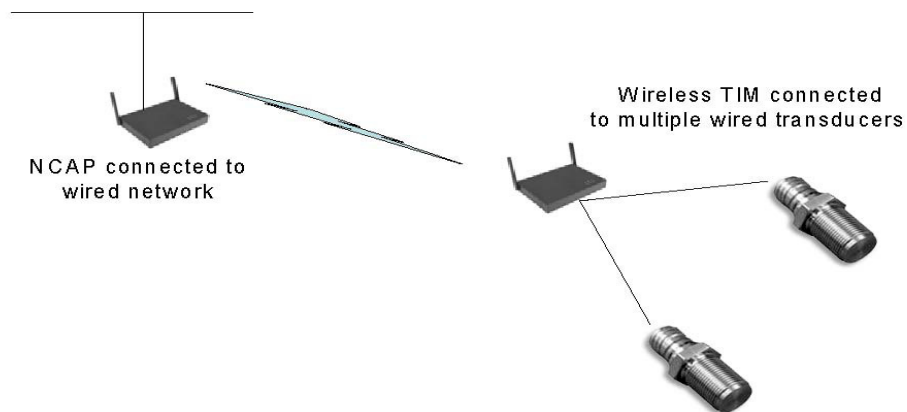


Figure 2—Gateway to WTIM

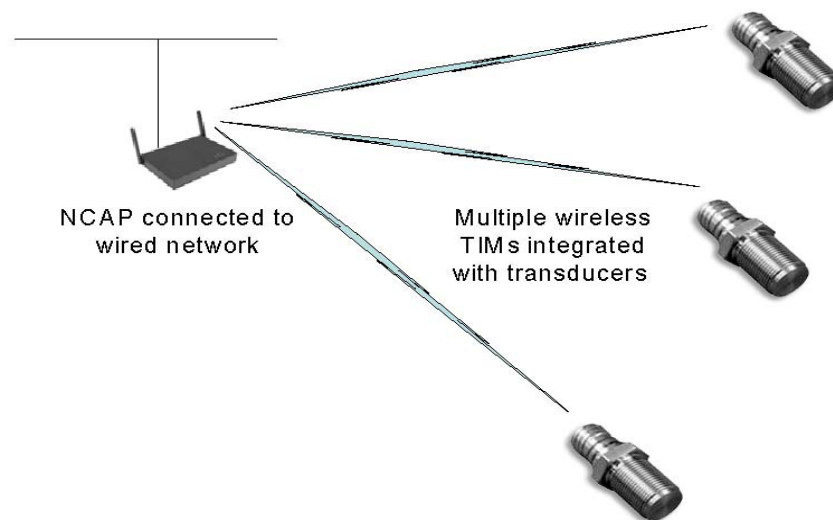


Figure 3—Gateway to Integrated WTIMs

The following roles are defined for a typical IEEE 1451.5 configuration:

NCAP—This device connects to one or more WTIMs via Dot5AR protocols and may be connected to a network.

WTIM—This device is connected to transducers and is connected via Dot5AR protocol(s) to an NCAP. A WTIM is a TIM, as defined in IEEE Std 1451.0-2007, including wireless communication to the NCAP.

5.3 PHY TEDS

The general structure for TEDS is defined in IEEE Std 1451.0-2007. All TEDS use a type/length/value (TLV) data structure. Using the TLV construct as shown in Table 1, each entry is stored as a TLV tuple. The “Type” field is one octet tag that identifies the TLV, which is similar in function to HTML or XML tags. The “Length” field specifies the number of octets of the value field, and the “Value” field is the actual data. Each entry may be composed of one or more TLVs. The structure, or data type, of the value field is defined in the specification for the TEDS.

Table 1—Definition of the TLV structure

Field	Description
Type	This code identifies the field in the TEDS that is contained within the value field. Except for types 2 and 3, the same number in the type field will have a different meaning in each different TEDS.
Length	The number in this field gives the number of octets in the value field. The number of octets in the length field is controlled by an entry in the TEDS Identification TLV.
Value	This field contains the TEDS information.

All fields in the PHY TEDS are required fields except for those with field types 32 and above. If any required field is omitted, the NCAP shall report a fatal TEDS error.

The field type entry in Table 2 is the “type” code in the TLV tuple used in the electronic copy of the TEDS. The “field name” entry is intended to be used as the argument name in any argument array used to pass all or parts of this TEDS to other software entities.

Table 2—PHY TEDS data block

Field type	Field name	Description	Type	# octets	Contents
—		TEDS length	UInt32	4	
3	TEDSID	TEDS Identification Header	UInt8	4	
4–9		Reserved			
10	Radio	Radio Type	UInt8	1	See Table 4
11	MaxBPS	Max data throughput	UInt32	4	Bits per second
12	MaxCDev	Max Connected Devices	UInt16	2	Maximum number of devices that may be simultaneously operational with this device
13	MaxRDev	Max Registered Devices	UInt16	2	Maximum number of devices that may be simultaneously registered with this device
14	Encrypt	Encryption	UInt16	2	Encryption type and key length
15	Authent	Authentication	Boolean	1	TRUE = Authentication supported FALSE = not supported
16	MinKeyL	Min Key Length	UInt16	2	Minimum key length for security functions
17	MaxKeyL	Max Key Length	UInt16	2	Maximum key length for security functions
18	MaxSDU	Max SDU Size	UInt16	2	Maximum payload size for transfer between devices
19	MinALat	Min Access Latency	UInt32	4	Minimum period for initiating a first transmission to an unconnected device
20	MinTLat	Min Transmit Latency	UInt32	4	The period for transmitting an N-octet payload, where N is the minimum payload size
21	MaxXact	Max Simultaneous Transactions	UInt8	1	Maximum number of queued, uncompleted commands
22	Battery	Device is battery powered	UInt 8	1	A nonzero value indicates battery power
23	RadioVer	Radio Version #	UInt16	2	A zero value indicates unknown
24	MaxRetry	Maximum Retries before Disconnect	UInt16	2	A zero value indicates never disconnect
25–31		Reserved			
32–41		Bluetooth Protocol Specific			See Table 7
42–47		Reserved			
48–54		802-11 Radio Specific			
55–63		Reserved			
64–80		ZigBee Protocol Specific			
81–95		Reserved			
96–103		6LoWPAN Protocol Specific			
104–127		Reserved			
128–255		Open to manufacturers			
—		Checksum	UInt16	2	

5.3.1 TEDS Identification Header

Field Type: 3

Field Name: TEDSID

This field is required in all TEDS.

The TEDS Identifier consists of the four fields shown in Table 3 and is standard for all TEDS. This field is always the first one in the TEDS. The Tuple Length for this field is assumed to be one.

The contents are as follows:

IEEE 1451 standards family number (5 for this standard)
TEDS class (13 for the PHY TEDS)
Version number
Tuple length (1 for this TEDS)

Table 3—TEDS Identifier structure

Field	Contents	Function
Type	03	Type field for the TEDS Identifier
Length	04	This field is always set to 04, indicating that the value field contains four octets. The four octets represent the “family,” “class,” “version,” and “tuple length” values shown in this table.
Family	05	This field identifies this TEDS as being defined in this standard.
Class	13	This field identifies the TEDS being accessed as the PHY TEDS.
Version	See Table 4	This field identifies the TEDS version. The value is the version number identified in the standard. A value of zero in this field indicates that the TEDS do not conform to any released standard. Table 2 lists the allowable values for this field.
Tuple length	01	This field gives the number of octets in the length field of all tuples in the TEDS except this tuple. NOTE—For the PHY TEDS, the number of octets in the length field of the tuples is “1,” meaning that there are 255 or less octets in the value field. ⁸

Table 4—Enumeration of TEDS version numbers

TEDS version	IEEE 1451.5 standard version
0	Reserved for prototype or other nonstandard TEDS versions
1	This will correspond to the original release of this standard.
2–255	Reserved for future releases of this standard.

5.3.2 Common PHY TEDS fields

Subclauses 5.3.2.1 through 5.3.2.15 define the information that is contained in all PHY TEDS.

5.3.2.1 IEEE1451.5 radio type

Field Type: 10

Field Name: Radio

Data type: UInt8

This field is required. If this field is omitted, the IEEE 1451.5 system shall report a fatal TEDS error.

⁸ Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the guide.

This field defines the IEEE 1451.5 radio (PHY) type. The values for PHY Id key are defined in Table 5.

Table 5—Enumeration of Phy ID

Value	Meaning
0	IEEE 802.11
1	Bluetooth
2	ZigBee
3	LoWPAN
4–254	Reserved for future expansion
255	Manufacturer specific

5.3.2.2 Maximum data throughput

Field type: 11

Field Name: MaxBPS

Data type: UInt32

This field contains the nominal maximum data throughput for the radio type in bits per second (bps).

5.3.2.3 Maximum number of connected devices

Field Type: 12

Field Name: MaxCDev

Data type: UInt16

This field contains the maximum number of devices that may be simultaneously operational with this device.

5.3.2.4 Maximum number of registered devices

Field type: 13

Field Name: MaxRDev

Data type: UInt16

This field contains the maximum number of devices that may be simultaneously registered to the radio node.

5.3.2.5 Encryption support

Field type: 14

Field Name: Encrypt

Data type: UInt16

This field contains two bytes. The first byte (MSB) indicates whether MAC level encryption is supported by the radio by enumeration of the encryption type as shown in Table 6.

The second byte (LSB) contains the encryption key length in bits.

Table 6—Enumeration of encryption

Value	Meaning
0	No encryption
1	AES
2	SAFER
3	3DES
4–254	Reserved for future expansion
255	Manufacturer specific

5.3.2.6 Authentication

Field type: 15

Field Name: Authent

Data type: Boolean

This field indicates whether MAC level authentication is supported by the radio.

5.3.2.7 Minimum key length

Field type: 16

Field Name: MinKeyL

Data type: UInt16

This field contains the minimum authentication or encryption key length supported by the radio.

5.3.2.8 Maximum key length

Field type: 17

Field Name: MaxKeyL

Data type: UInt16

This field contains the maximum authentication or encryption key length supported by the radio.

5.3.2.9 Maximum SDU size

Field type: 18

Field Name: MaxSDU

Data type: UInt16

This field contains the maximum service data unit (SDU) size in bytes accepted for transfer between this device and another device.

5.3.2.10 Minimum access latency

Field type: 19

Field Name: MinALat

Data type: UInt32

This field contains the minimum period for initiating a first transmission to an unconnected device, in nanoseconds.

5.3.2.11 Minimum transmit latency

Field type: 20

Field Name: MinTLat

Data type: UInt32

This field contains the minimum time to transmit the smallest complete data packet to/from the radio node, in nanoseconds.

5.3.2.12 Maximum number of simultaneous transactions

Field Type: 21

Field Name: MaxXact

Data type: UInt8

This field contains the maximum number of simultaneous transactions that may be pending across the WTIM IEEE 1451.0 API.

5.3.2.13 Battery powered

Field Type: 22

Field Name: Battery

Data type: unsigned octet integer (UInt8, 1 octet)

This field indicates whether the radio node is battery powered. A nonzero value indicates the device is battery powered.

5.3.2.14 Radio version

Field Type 23

Field Name: RadioVer

Data Type: UInt16

This field indicates the software version of the radio level code. A value of 0 is default and indicates that the radio version is unknown. A nonzero value is interpreted with the upper two digits indicating the major

radio version number and the lower two digits indicating the minor version number. For example, a radio with version number 1.2 would be indicated as 0x0102.

5.3.2.15 Maximum retries before disconnect

Field Type 24

Field Name: MaxRetry

Data Type UInt16

This field indicates the maximum number of retries the radio will attempt before automatically performing a disconnect operation to unbind the device link. A value of 0 is default and indicates that the radio will never disconnect without being instructed.

5.3.3 Bluetooth protocol-specific fields

This subclause specifies the contents of all of the TEDS fields defined in this standard for Bluetooth IEEE 1451.5 devices (Table 7).

Table 7—Protocol-specific fields for Bluetooth

Field type	Field name	Description	Type	# octets
		Protocol-specific (Bluetooth)		
40	Reconnect	Support for WTIM reconnection	UInt 8	1
41	Reserved			1

5.3.3.1 WTIM Reconnect

Field Type: 40

Field Name: Reconnect

Data type: unsigned octet integer (UInt8, 1 octet)

This field indicates whether the radio node supports the WTIM Reconnect feature of the Smart Transducer Profile.

5.4 NCAP radio state diagram

The Dot5AR of the NCAP supports connections to multiple WTIMs with the same type radio. There may be multiple Dot5ARs on an NCAP. The initial state for an NCAP Dot5AR at power up or after a reset is to state UNREGDOT5. After performing a registration process with a Dot5AR on the NCAP, that Dot5AR moves to state DOT5REG (Figure 4). This state means that the NCAP is associated with that Dot5AR but is not yet associated with a WTIM; therefore, it is not configured to perform transducer data exchange. The NCAP shall maintain separate status for each of its Dot5ARs.

Each of the NCAP's Dot5ARs shall maintain separate status for each of the WTIM's (Figure 5). When an NCAP's Dot5AR registers one or more WTIMs, it moves to state TIMREG for that NCAP's Dot5AR state machine. To perform data exchange the NCAP issues an open command and one or more write commands containing IEEE 1451.0 octet array payloads, and the NCAP moves to state OPEN for that WTIM. In the OPEN state, the NCAP may become involved in data exchange with the WTIM. The OPEN state is terminated with a close command. Since the NCAP has to maintain separate status for each NCAP Dot5ARs and WTIMs, the NCAP may initiate discoverable or connectable nodes at any time.

This state machine configuration is shown in Figure 4 and Figure 5.

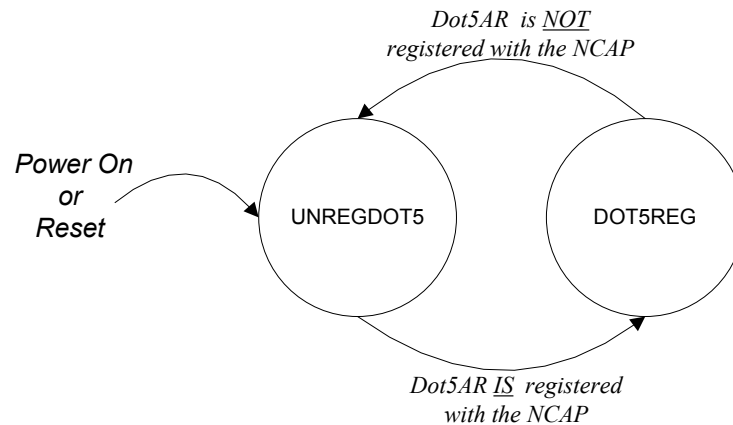


Figure 4—NCAP radio state diagram

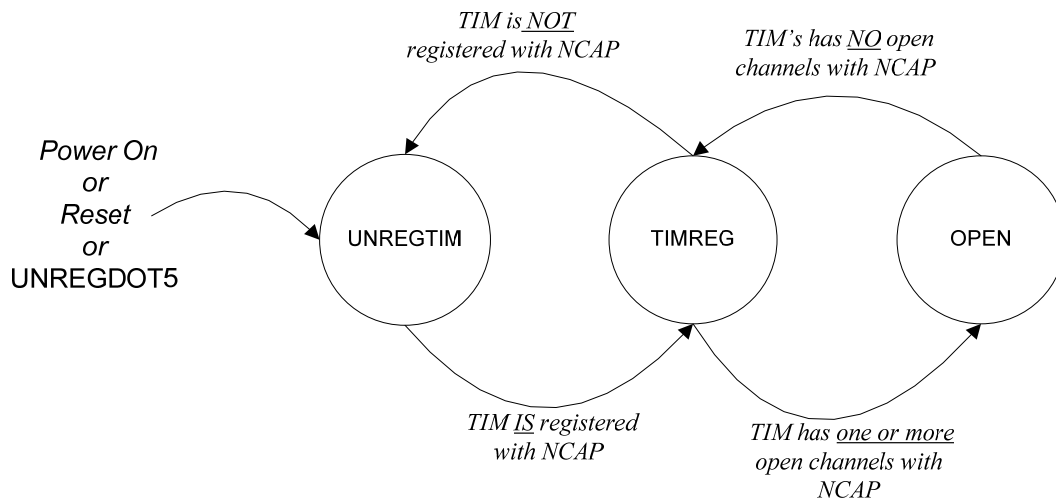


Figure 5—NCAP radio state diagram (one per WTIM)

5.5 WTIM radio state diagram

The WTIM Dot5AR is a dedicated, single-PHY as described in the state diagram. The initial state for a WTIM Dot5AR on first power up or after a reset is to state PREREG. After performing a registration process with an NCAP, the WTIM moves to state NCAPREG. This state means that the device is associated with a single NCAP but is not configured to perform transducer data exchange. When an NCAP configures a WTIM to perform data exchange, it issues an open command and one or more write commands containing IEEE 1451.0 octet array payloads, and the WTIM moves to state OPEN. In the OPEN state, the WTIM may become involved in data exchange with the NCAP. The OPEN state is terminated with a close command. If the number of consecutive communication failures exceeds the maximum retries before disconnect, the TIM shall move to the PREREG state. There is no DOTREG registration state in this machine, because the device is permanently preregistered.

This state machine configuration is shown in Figure 6.

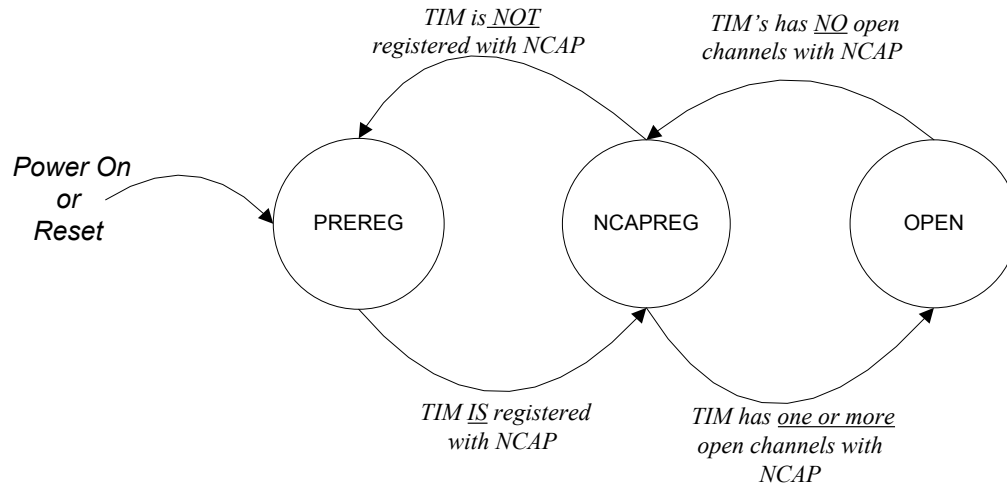


Figure 6—WTIM radio state diagram

5.6 Quality of service

The term “quality of service” (QoS) is used in different contexts with different meanings. In the context of an IEEE 1451.5 network, it means allocating sufficient resources for a link and choosing link configurations so the link meets the application requirements (see Figure 7). However, there are limitations on what any QoS implementation can achieve when using a wireless technology in an unlicensed band. These restrictions are as follows:

- No device can predict the affect of interference on link quality.
- No device can predict the requirements of other devices to which a peer device may be connected.
- A device may not be able to accurately predict its ability to meet QoS requirements.
- A device may not be able to accurately measure failure to meet a QoS requirement.
- A QoS failure at the MAC layer is notified to the transmitting entity, not to the peer device that should receive the data. This means the device to receive the data may not be notified of a QoS failure.

QoS Parameters

IDL: boolean setQoS(UInt16 commId, UInt16 mode, UInt16 period, UInt16 transmitSize, UInt16 receiveSize, UInt16 accessLatency UInt16 transmitLatency);

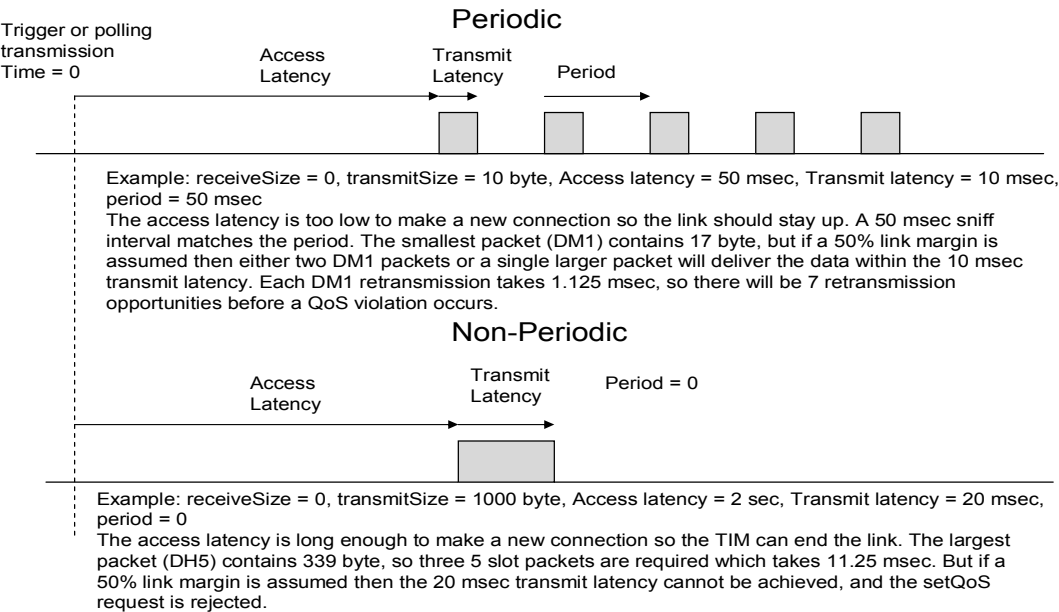


Figure 7—QoS parameter

5.7 Error codes

All error codes are represented as UInt16 quantities. Five entities are involved in a communication transaction: the local IEEE 1451.0 layer, the local IEEE 1451.5 layer, the remote IEEE 1451.5 layer, the remote IEEE 1451.0 layer, and the remote application layer. The error code source is encoded in the upper 3 bits. The error code enumeration is encoded in the lower bits. Bits are numbered from most significant (bit 15) to least significant (bit 0) as shown in Table 8.

Table 8—Bit assignments for error codes

Bits	Used by
Bits 15 through 13	(the 3 most significant bits) The error code source information is encoded in this location as described in Table 9.
Bits 12 through 0	Error code enumeration; see Table 10.

Error code source values are specified in Table 9. The value column contains the bits 15 through 13 evaluated as a 3 bit unsigned integer.

Table 9—Error code source enumeration

Value	Source of the error
0	No error
1	Error from the local IEEE 1451.0 layer
2	Error from the local IEEE 1451.5 layer
3	Error from the remote IEEE 1451.5 layer
4	Error from the remote IEEE 1451.0 layer
5	Error from the remote application layer
6	Reserved
7	Open to manufacturers

Error code values are specified in Table 10. In this case, bits 12 through 0 are evaluated as a 13 bit unsigned integer.

Table 10—Error code enumerations

Enumerations	Error code name	Description
0	NO_ERROR	No error, operation successful
1	INVALID_COMMID	Invalid “commId”
2	UNKNOWN_DESTID	Unknown “destId”
3	TIMEOUT	Operation timeout
4	NETWORK_FAILURE	Destination unreachable network failure
5	NETWORK_CORRUPTION	Corrupt Communication network failure
6	MEMORY	Local out-of-memory error
7	QOS_FAILURE	Network quality-of-service violation
8	MCAST_NOT_SUPPORTED	Multicast not supported
9	UNKNOWN_GROUPID	Unknown “groupId”
10	UNKNOWN_MODULEID	Unknown “moduleId”
11	UNKNOWN_MSGID	Unknown “msgId”
12	NOT_GROUP_MEMBER	destId not in the group
13	ILLEGAL_MODE	The mode parameter is not valid
14	LOCKED_RESOURCE	The resource being accessed is locked
15	FATAL_TEDS_ERROR	There is an error in the TEDS that makes the device unusable
16	NON-FATAL_TEDS_ERROR	The value in a field in the TEDS is unusable, but the device will still function.
17	CLOSE_ON_LOCKED_RESOURCE	A warning error code returned to signal that a close on a locked resource was performed
18	LOCK_BROKEN	If a non-blocking read or write, or measurement stream is in progress, the callback will be invoked with this error code
19	NETWORK_RESOURCE_EXCEEDED	The IEEE 1451.5 system has reached network resource limits
20	MEMORY_RESOURCE_EXCEEDED	The IEEE 1451.5 system has reached memory resource limits
21–4095	Reserved	
4096–8191	Open to manufacturers	

6. IEEE 802.11 radio sub-specification

This IEEE 802.11 radio specification for the IEEE 1451.5 system provides a description of the functions, protocols, and interfaces that are to be performed and provided by the IEEE 802.11 Communication Module between the Transducer Access Module, or WTIM, and the NCAP Service Module. The IEEE 802.11 radio specification for IEEE 1451.5 maps commands and messages from the IEEE 1451.5 higher convergence layer, bidirectionally through the IEEE 802.11 MAC and PHY for radio-based communication between the WTIM and the NCAP Service Module.

The IEEE 802.11 radio specification for the IEEE 1451.5 system shall support the use of IEEE 802.11 PHYs. Radio range is highly dependent on antenna design and transmit gain. It is therefore vendor-specific and outside the scope of this IEEE 802.11 radio specification for the IEEE 1451.5 system.

The main goal of the IEEE 802.11 radio specification for the IEEE 1451.5 system is to provide a complete mapping from the IEEE 1451.5 convergence layer through the IEEE 802.11 network stack down to the PHY, and vice versa. The specification is written to be inclusive of emerging IEEE 802.11 working groups/task groups, such as IEEE 802.11i security and IEEE 802.11e QoS. For IEEE 802.11, this specification shall support IEEE 802.11a/b/g radios and be compatible with IEEE 802.11e QoS and IEEE 802.11i security constructs. As such, the purpose is not to redefine IEEE 802.11a/b/g/e/i, but to support these existing drafts and standards for inclusion in the IEEE 1451.5 system.

A WTIM implementation shall be deemed in conformance with the IEEE 802.11 radio specification for the IEEE 1451.5 system provided one of the following three requirements are met:

- The WTIM provides IEEE 802.11a capability as per the Wi-Fi Alliance Certified Product Listing.
- The WTIM provides IEEE 802.11b capability as per the Wi-Fi Alliance Certified Product Listing.
- The WTIM provides IEEE 802.11g capability as per the Wi-Fi Alliance Certified Product Listing.

Support for IEEE 802.11e QoS and IEEE 802.11i security are both optional and shall be determined based on the vendor application. Secure Wi-Fi and advanced Wi-Fi guidelines may be followed and are described at <http://www.weca.net>.

This IEEE 802.11 radio specification for the IEEE 1451.5 system permits the use of DSSS and/or FHSS as defined within the IEEE 802.11a/b/g PHY specifications.

6.1 Layered approach within IEEE 802.11 radio sub-specification

The following IEEE 802.11 radio sub-specification shall be structured according to a layered network approach, as shown in Figure 8. IEEE 802.11 shall be specified at layers 1 and 2. The choice of either Internet Protocol (IP) version 4 or version 6 is supported at layer 3. The choice of either Transmission Control Protocol (TCP) for “connected” or User Datagram Protocol (UDP) for “connectionless” transport protocols are supported at layer 4. A thin “API Shim” fits between the IEEE 1451.0 and the IEEE 1451.5 layers.

	API SHIM		
Layer 4	TCP	UDP	Transport
Layer 3	IP (v4, v6)		Network
Layer 2	802.11 LLC / MAC		Datalink
Layer 1	802.11 PHY		Physical

Figure 8—Layers specified within IEEE 802.11 radio sub-specification for the IEEE 1451.5 system

The details of each layer shall be described in subsequent clauses within this functional specification. Either TCP or UDP at layer 4, and either IPv4 or IPv6 at layer 3, shall be implemented in compliance with this functional specification, respectively. The layered stack shown in Figure 9 embodies the

“IEEE 802.11 radio specification for the IEEE 1451.5 system” and logically resides at layers 1–4 of the networking stack within the NCAP communication module and within the WTIM communication module for an IEEE 1451.5–IEEE 802.11 compliant system. A thin “API Shim” fits between the IEEE 1451.0 and the IEEE 1451.5 layers.

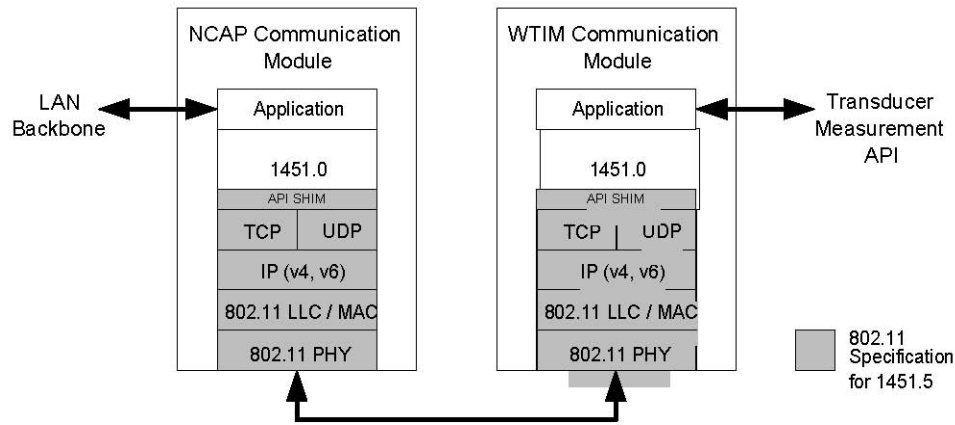


Figure 9—Layered framework within NCAP and WTIM

6.2 IEEE 802.11 MAC and PHY specifications

6.2.1 Multiple logical address spaces within IEEE 802.11 MAC and PHY

Just as the IEEE 802.11 architecture allows for the possibility that the WM, DSM, and an integrated wired LAN may all be different physical media, it also allows for the possibility that each of these components may be operating within different address spaces. IEEE 802.11 architecture only uses and specifies the use of the WM address space.

Each IEEE 802.11 PHY operates in a single medium—the WM. The IEEE 802.11 MAC operates in a single address space. MAC addresses are used on the WM in the IEEE 802.11 architecture. IEEE 802.11 architecture has chosen to use the IEEE 802 48-bit address space. Thus IEEE 802.11 addresses are compatible with the address space used by the IEEE 802 LAN family.

The IEEE 802.11 choice of address space implies that for many instantiations of the IEEE 802.11 architecture, the wired LAN MAC address space and the IEEE 802.11 MAC address space may be the same. In those situations where a DS that uses MAC level IEEE 802 addressing is appropriate, all three of the logical address spaces used within a system could be identical. Although this case is common, it is not the only combination allowed by the architecture. The IEEE 802.11 architecture allows for all three logical address spaces to be distinct.

A multiple address space example is one in which the DS implementation uses network layer addressing. In this case, the WM address space and the DS address space would be different.

The ability of the architecture to handle multiple logical media and address spaces is key to the ability of IEEE 802.11 architecture to be independent of the DS implementation and to interface cleanly with network layer mobility approaches.

6.2.2 General description of the IEEE 802.11 radio specification for the IEEE 1451.5 system

This subclause presents the concepts, terminology, and general description of the IEEE 802.11 radio architecture for the IEEE 1451.5 system. Refer to Clause 5 of IEEE Std 802.11-2007. The general description subclause includes (5.1) general description of the IEEE 802.11 architecture, (5.2) components of the IEEE 802.11 architecture, (5.3) logical service interfaces, (5.4) overview of the services, (5.5) relationships between services, (5.6) differences between ESS and IBSS LANs, (5.7) message information contents that support the services, and (5.8) 802.11 Reference Model.

IEEE Std 802.11-2007 uses an architecture to describe functional components of an IEEE 802.11 LAN. The architectural descriptions in this general description clause (Clause 5 of IEEE Std 802.11-2007) are not intended to represent any specific physical implementation of IEEE 802.11.

6.2.3 General description of the IEEE 802.11i security enhancements (optional)

(Optional) IEEE Std 802.11i-2004 provides fundamental security enhancements to IEEE Std 802.11-2007. If IEEE 802.11i security is utilized, refer to Clause 5 of IEEE Std 802.11i-2004. This security-enhanced general description subclause includes (5.1) general description of the IEEE 802.11 architecture; (5.2) components of the IEEE 802.11 architecture including the robust security network association; (5.3) association; (5.4) overview of the services including authentication, confidentiality, key management, data origin authenticity, replay detection; (5.6) differences between ESS and IBSS LANs; (5.7) message information contents that support the services including confidentiality, authentication, and deauthentication; (5.8) Security-enhanced IEEE 802.11 Reference Model; and (5.9) IEEE 802.11 and IEEE 802.1X, including introduction of the IBSS 4-Way Handshake.

6.2.4 MAC service definition

This subclause presents the MAC service definition for the IEEE 802.11 radio architecture for the IEEE 1451.5 system. Refer to Clause 6 of IEEE Std 802.11-2007. The MAC service definition includes (6.1.1) asynchronous data service, (6.1.2) security services, (6.1.3) MSDU ordering, and (6.2) detailed service specification consisting of MAC data services as defined in ISO/IEC 8802-2:1998, including

MA-UNITDATA.request
MA-UNITDATA.indication
MA-UNITDATA-STATUS.indication

Semantics, generation, and effect of reception of these service primitives.

6.2.5 MAC service definition for IEEE Std 802.11i (optional)

(Optional) IEEE Std 802.11i-2004 provides fundamental security enhancements to IEEE Std 802.11-2007. If IEEE 802.11i security is utilized, refer to Clause 6 of IEEE Std 802.11-2007. The MAC service definition includes (6.1.2) security services and (6.1.4) MAC data service architecture (informative).

6.2.6 Frame formats

The format of the IEEE 802.11 MAC frames is specified in this subclause. All wireless nodes (IEEE 802.11-compliant NCAPs and WTMs) shall be able to properly construct frames for transmission and decode frames upon reception, as specified in this subclause. Refer to Clause 7 of IEEE Std 802.11-2007. Frame formats include (7.1) MAC frame formats, (7.2) Format of individual frame types, and (7.3) Management frame body components.

6.2.7 Frame formats for IEEE Std 802.11b-1999 (optional)

(Optional) IEEE Std 802.11b-1999 provides a higher speed physical layer extension in the 2.4 GHz band. If IEEE 802.11b technology is utilized, refer to Clause 7 of IEEE Std 802.11b-1999. Frame formats include (7.2.3.1) Beacon frame format, (7.2.3.9) Probe Response frame format, (7.3.1.4) Capability Information field, (7.3.1.9) Status Code field, and (7.3.2.2) Supported Rates element.

6.2.8 Frame formats for IEEE Std 802.11g-2003 (optional)

(Optional) IEEE Std 802.11g-2003 provides a further higher data rate extension in the 2.4 GHz band. If IEEE 802.11g technology is utilized, refer to Clause 7 of IEEE Std 802.11g-2003. Frame formats include (7.2) Format of individual frame types, (7.2.1) Control frames, (7.2.3) Management frames, (7.3) Management frame body components, (7.3.1) Fixed fields, and (7.3.2) Information elements.

6.2.9 Frame formats for IEEE Std 802.11i-2004 (optional)

(Optional) IEEE Std 802.11i-2004 provides fundamental security enhancements to IEEE Std 802.11-2007. If IEEE 802.11i security is utilized, refer to Clause 7 of IEEE Std 802.11i-2004. Frame formats include protected frames, frame control field, format of individual frame types including data frames and management frames (with RSN Information Element), management frame body components with Capability Information fixed field, RSN Information Element, Cipher Suites, Authentication and Key Management Suites, RSN Capabilities, PMKID, and RSN IE Examples.

6.2.10 Security

The security, including authentication and privacy, of the IEEE 802.11 MAC frames is specified in this subclause. It should be noted that Clause 8 of IEEE Std 802.11-2007 is largely a defunct clause, with outdated WEP functionality, that should be replaced by Clause 8 of IEEE Std 802.11i-2004 (see 5.6.1) for real security utilization. Clause 8 of IEEE Std 802.11-2007 includes (8.1) Authentication services, (8.2) the Wired Equivalent Privacy (WEP) algorithm, and (8.3) Security-Related MIB attributes.

6.2.11 Security for IEEE Std 802.11i-2004 (optional)

(Optional) IEEE Std 802.11i-2004 provides fundamental security enhancements to IEEE Std 802.11-2007. If IEEE 802.11i security is utilized, refer to Clause 8 of IEEE Std 802.11i-2004. Security includes framework, pre-RSNA security methods, RSNA data confidentiality protocols including TKIP and CCMP, RSNA security association management, keys and key distribution including key hierarchy, EAPOL-KEY frames, 4-way handshake, group key handshake, RSNA supplicant key management state machine, RSNA authenticator key management state machine, and nonce generation (informative), mapping EAPOL keys to IEEE 802.11 keys, and per-frame pseudocode including WEP frame pseudocode and RSNA frame pseudocode.

6.2.12 MAC sublayer functional description

The MAC functional description is presented in this subclause. Refer to Clause 9 of IEEE Std 802.11-2007. The architecture of the MAC sublayer, including the distributed coordination function (DCF), the point coordination function (PCF), and their coexistence in an IEEE 802.11 LAN are introduced in (9.1). These functions are expanded on in (9.2) and (9.3), and a complete functional description of each is provided. Fragmentation and defragmentation are covered in (9.4) and (9.5). Multirate support is addressed in (9.6). The allowable frame exchange sequences are listed in (9.7). Finally, a number of additional restrictions to limit the cases in which MSDUs are reordered or discarded are described in 9.8.

6.2.13 MAC sublayer functional description for IEEE Std 802.11a-1999 (optional)

(Optional) IEEE Std 802.11a-1999 provides a high-speed physical layer in the 5 GHz band. If IEEE 802.11a technology is utilized, refer to Clause 9 of IEEE Std 802.11a-1999. This subclause includes modifications to (9.6) multirate support.

6.2.14 MAC sublayer functional description for IEEE Std 802.11b-1999 (optional)

(Optional) IEEE Std 802.11b-1999 provides a higher speed physical layer extension in the 2.4 GHz band. If IEEE 802.11b technology is utilized, refer to Clause 9 of IEEE Std 802.11b-1999. This subclause includes modifications to (9.2) DCF and (9.6) multirate support.

6.2.15 MAC sublayer functional description for IEEE Std 802.11g-2003 (optional)

(Optional) IEEE Std 802.11g-2003 provides a further higher data rate extension in the 2.4 GHz band. If IEEE 802.11g technology is utilized, refer to Clause 9 of IEEE Std 802.11g-2003. This subclause includes modifications to (9.2) DCF, (9.6) multirate support, (9.7) frame exchange sequences, and (9.10) protection mechanism.

6.2.16 Layer management

Both MAC and PHY layers conceptually include management entities, called MAC sublayer management and PHY layer management entities (MLME and PLME, respectively). These entities provide the layer management service interfaces through which layer management functions may be invoked. Certain of these interactions are defined explicitly via a service access point (SAP) across which defined primitives are exchanged. Refer to Clause 10 of IEEE Std 802.11-2007. This subclause includes (10.1) overview of management model, (10.2) generic management primitives, (10.3) MLME SAP interface, and (10.4) PLME SAP interface.

6.2.17 Layer management for IEEE Std 802.11a-1999 (optional)

(Optional) IEEE Std 802.11a-1999 provides a high-speed physical layer in the 5 GHz band. If IEEE 802.11a technology is utilized, refer to Clause 10 of IEEE Std 802.11a-1999. This subclause includes modifications to (10.4) PLME SAP interface.

6.2.18 Layer management for IEEE Std 802.11b-1999 (optional)

(Optional) IEEE Std 802.11b-1999 provides a higher speed physical layer extension in the 2.4 GHz band. If IEEE 802.11b technology is utilized, refer to Clause 10 of IEEE Std 802.11b-1999. This subclause includes modifications to (10.3.2.2) MLME_scan.confirm, (10.3.2.2.2) Semantics of the service primitive, (10.3.3.1.2) Semantics of the service primitive, (10.3.10) Start, (10.3.10.1.2) Semantics of the service primitive, and (10.4.4) PLME_DSSSTESTMODE.

6.2.19 Layer management for IEEE Std 802.11g-2003 (optional)

(Optional) IEEE Std 802.11g-2003 provides a further higher data rate extension in the 2.4 GHz band. If IEEE 802.11g technology is utilized, refer to Clause 10 of IEEE Std 802.11g-2003. This subclause includes modifications to (10.4) PLME SAP interface.

6.2.20 Layer management for IEEE Std 802.11i-2004 (optional)

(Optional) IEEE Std 802.11i-2004 provides fundamental security enhancements to IEEE Std 802.11-2007. If IEEE 802.11i security is utilized, refer to Clause 10 of IEEE Std 802.11i-2004. This subclause consists of modifications to the MLME SAP interface, including Scan, Associate, Reassociate, SetKeys, DeleteKeys, Michael MIC Failure Event, EAPOL (Michael MIC Failure Report), MLME-STAKEYESTABLISHED, SetProtection, and MLME-PROTECTEDFRAMEDROPPED.

6.2.21 MAC sublayer management entity

This subclause expands on the previous subclause by providing details of the MLME. Refer to Clause 11 of IEEE Std 802.11-2007. This subclause includes (11.1) Synchronization, (11.2) Power management, (11.3) Association and reassociation, and (11.4) Management information base (MIB) definitions.

6.2.22 MAC sublayer management entity for IEEE Std 802.11i-2004 (optional)

(Optional) IEEE Std 802.11i-2004 provides fundamental security enhancements to IEEE 802.11. If IEEE 802.11i security is utilized, refer to Clause 11 of IEEE Std 802.11i-2004. This subclause consists of modifications to Authentication, Deauthentication, Association, Reassociation, and Disassociation.

6.2.23 Physical layer (PHY) service specification

The PHY services provided to the IEEE 802.11 wireless LAN MAC are described in this subclause. Refer to Clause 12 of IEEE Std 802.11-2007. This subclause includes (12.1) Scope, (12.2) PHY functions, and (12.3) Detailed PHY service specifications.

6.2.24 PHY management

The MIB comprises the managed objects, attributes, actions, and notifications required to manage a station. The definition of these managed objects, attributes, actions, and notifications, as well as their structure, is referred to in Clause 13 and is presented in Annex D of IEEE Std 802.11-2007.

6.2.25 Frequency-Hopping spread spectrum (FHSS) PHY specification for the 2.4 GHz Industrial, Scientific, and Medical (ISM) band (optional)

(Optional) The PHY services provided to the IEEE 802.11 wireless LAN MAC for the 2.4 GHz FHSS system are described in this subclause. Refer to Clause 14 of IEEE Std 802.11-2007. This subclause includes (14.1) overview, (14.2) FHSS PHY-specific service parameters list, (14.3) FHSS PLCP sublayer, (14.4) PLME SAP layer management, (14.5) FHSS PMD sublayer services, (14.6) FHSS PMD sublayer, 1.0 Mbit/s, (14.7) FHSS PMD sublayer, 2.0 Mbit/s, (14.8) FHSS PHY management information base (MIB), and (14.9) FH PHY characteristics.

6.2.26 Direct sequence spread spectrum (DSSS) PHY specification for the 2.4 GHz band designated for ISM applications (optional)

(Optional) The PHY services provided to the IEEE 802.11 wireless LAN MAC for the 2.4 GHz DSSS system are described in this subclause. Refer to Clause 15 of IEEE Std 802.11-2007. This subclause includes (15.1) overview, (15.2) DSSS PLCP sublayer, (15.3) DSSS physical layer management entity (PLME), and (15.4) DSSS PMD sublayer.

6.2.27 Infrared (IR) PHY specification (optional)

(Optional) The PHY services provided to the IEEE 802.11 wireless LAN MAC for the infrared system are described in this subclause. Refer to Clause 16 of IEEE Std 802.11-2007. This subclause includes (16.1) overview, (16.2) IR PLCP sublayer, (16.3) IR PMD sublayer, and (16.4) PHY attributes.

6.2.28 Orthogonal Frequency Division Multiplexing (OFDM) PHY specification for the 5 GHz band (optional)

(Optional) This subclause specifies the PHY entity for an OFDM system and the additions that have to be made to the base standard to accommodate the OFDM PHY. Refer to Clause 17 of IEEE Std 802.11a-1999. This subclause includes (17.1) Introduction, (17.2) OFDM PHY specific service parameter list, (17.3) OFDM PLCP sublayer, (17.4) OFDM PLME, and (17.5) OFDM PMD sublayer.

6.2.29 High Rate, direct sequence spread spectrum PHY specification (optional)

(Optional) This subclause specifies the high rate extension of the PHY for the DSSS High Rate PHY for the 2.4 GHz band designated for ISM applications. Refer to Clause 18 of IEEE Std 802.11b-1999. This subclause includes (18.1) Overview, (18.2) High Rate PLCP sublayer, (18.3) High Rate PLME, and (18.4) High Rate PMD sublayer.

6.2.30 High Rate, direct sequence spread spectrum PHY specification for IEEE 802.11g (optional)

(Optional) IEEE Std 802.11g-2003 provides a further higher data rate extension in the 2.4 GHz band. If IEEE 802.11g technology is used, refer to Clause 18 of IEEE Std 802.11g-2003. This subclause includes modifications to (18.2) High Rate PLCP sublayer.

6.2.31 Extended Rate PHY specification for IEEE 802.11g (optional)

(Optional) IEEE Std 802.11g-2003 provides a further higher data rate extension in the 2.4 GHz band. If IEEE 802.11g technology is used, refer to Clause 19 of IEEE Std 802.11g-2003. This subclause includes specifications for an Extended Rate PHY (ERP) that operates in the 2.4 GHz ISM band. The subclause includes (19.1) Overview, (19.2) PHY-specific service parameter list, (19.3) Extended Rate PLCP sublayer, (19.4) ERP PMD sublayer general operating specifications, (19.5) ERP operation specifications, (19.6) ERP-PBCC operation specifications, (19.7) DSSS-OFDM operation specifications, (19.8) ERP PLME, and (19.9) Extended Rate PMD sublayer.

6.3 Internet Protocol Version 4 (IPv4) Specification (optional)

(Optional) IPv4 provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed-length addresses. The Internet Protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through “small packet” networks. If IPv4 at the network layer is used (see Figure 2), refer to IETF RFC 791. Explicit subclauses and sections from IETF RFC 791 shall be referenced within this clause. Support for IPv4 is optional; however, either IPv4 or IPv6 shall be used at the network layer to comply with this specification.

Refer to Annex A for an informative overview of IPv4.

6.4 Internet Protocol Version 6 (IPv6) Specification (optional)

(Optional) IPv6 includes a simplified header with a hierarchical address structure that permits rigorous route aggregation. IPv6 also includes packet-level authentication and encryption along with plug-and-play autoconfiguration. IPv6 changes the way IP header options are encoded to increase the flexibility of introducing new options in the future while improving performance. It also includes the ability to label traffic flows.

Support for IPv6 is optional; however, either IPv4 or IPv6 shall be used at the network layer to comply with this specification.

Refer to Annex B for an informative overview of IPv6.

6.5 Transmission Control Protocol (TCP) Specification (optional)

(Optional) Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host transport-layer protocol between NCAPs and WTIMs in the packet-switched “802.11 IEEE 1451.5” communication network and in interconnected systems of such networks. TCP is a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols that support multi-network applications. IETF RFC 793 describes TCP and provides references to additional supporting documents.

Refer to Annex C for an informative overview of TCP.

6.6 User Datagram Protocol (UDP) Specification (optional)

(Optional) The UDP is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. UDP at the transport-layer assumes that either IPv4 or IPv6 is used as the underlying protocol at the network-layer. Refer to IETF RFC 768 for complete specification of UDP. Support for UDP is optional; however, either TCP or UDP shall be used at the transport layer to comply with this specification.

Refer to Annex D for an informative overview of UDP.

6.7 Discovery, communication, and group creation mechanics

A discovery protocol, TCP unicast communication, and group creation process are specified in this subclause.

6.7.1 IP address and traffic management

IEEE 1451.5 802.11 nodes (either NCAP or WTIM) shall contain an IP address that is managed either by static assignment or via DHCP protocol.

Optionally, IEEE 1451.5 802.11 nodes (either NCAP or WTIM) may have a name that is managed by DNS.

The discovery protocol shall use UDP multicast address 224.0.1.179 port number 14515 (see 6.7.2).

Group communication between nodes shall use UDP multicast addresses in the following range:

224.0.1.180 to 224.0.1.183.

6.7.2 Discovery protocol

The purpose of the discovery protocol is to permit nodes in the local network to discover one another without reliance on preconfigured IP addresses. Also it is used to configure network addresses. It is based on a UDP multicast message mechanism on address 224.0.1.179 and port 14515. The time-to-live parameter in the IP header shall default to one, so that the multicast message traverses only the local subnet.

Following power-on, once a stable condition is reached, each IEEE 1451.5 802.11 node shall transmit an “announce” message. Upon reception of a “command” message, the node shall also issue an “announce” message.

On an NCAP, reception of an “announce” message from an unrecognized TIM shall result in an API call invoking the registerDest(UInt8 dotXId, UInt8 type) call (see 6.8). The following information shall be cached locally inside the IEEE 1451.5 802.11 convergence layer: “destId, remote IP address, and TCP server Port.” Note that the “destId” is returned by the IEEE 1451.0 system from the IEEE 1451.5 802.11 call to registerDest (UInt8 dotXId, UInt8 type).

The payload for these multicast messages is encoded in a simple ASCII scheme, using a “&” delimited “name=value” format. This format is patterned after typical URL parameter encoding mechanisms.

The “announce” message is generated at power-on as well as in response to “command” messages. Optionally, it may be generated on a periodic basis, as a status heartbeat. It contains the following information:

- The supported standard shall be IEEE Std 1451.5 encoding: STD=1451.5
- Version encoding: VER=1.0
- Announcement response encoding: RSP=BOOT, REPLY, HEARTBEAT
- TIM or NCAP indicator encoding: NODE=NCAP or TIM
- Device’s IP address encoding: IP=xxx.yyy.zzz.aaa
- Device’s MAC address encoding: MAC=01:23:45:67:89:AB
- Device’s TCP server port number encoding: TCP_port=1234
- Optional: device name encoding: NAME=”string”
- Optional: DHCP ON/OFF encoding: DHCP=ON or OFF

Three “command” messages are currently defined. The “Discover Request” command is used to trigger all devices to generate a “Reply” message. The “Discovery Request” command contains the following fields:

- The supported standard shall be IEEE Std 1451.5 encoding: STD=1451.5
- Version encoding: VER=1.0
- Command Flag Indicator encoding: CMD=DISCOVER

The “Setup Static IP Address” command is used to configure network address parameters. As the message is sent via multicast, the MAC address field is provided to specify the desired recipient. It contains the following fields:

- The supported standard shall be IEEE Std 1451.5 encoding: STD=1451.5
- Version encoding: VER=1.0
- Command Flag Indicator encoding: CMD=STATIC_ADDRESS
- IP address encoding: IP=xxx.yyy.zzz.aaa
- Subnet mask encoding: SM=255.255.255.0
- Gateway address encoding: GW=xxx.yyy.zzz.aaa
- Optional: DNS address encoding: DNS=xxx.yyy.zzz.aaa
- MAC address encoding: MAC=01:23:45:67:89:AB

The “Setup Dynamic IP Address” command is used to enable DHCP address configuration. As the message is sent via multicast, the MAC address field is provided to specify the desired recipient. It contains the following fields:

- The supported standard shall be P1451.5 encoding: STD=1451.5
- Version encoding: VER=1.0
- Command Flag Indicator encoding: CMD=DHCP

6.7.3 TCP unicast communication

Following power-on, once a stable condition is reached, each IEEE 1451.5 802.11 node within the convergence layer shall open a TCP “listen” socket on an arbitrary port; however, this port is provided as part of the discovery protocol discussed in 6.7.2. The IEEE 1451.5 802.11 node shall prepare to receive incoming TCP traffic on that socket.

During the registration phase, each destination is registered with the IEEE 1451.0 system.

In the open(...) call made by the IEEE 1451.0 system, the IEEE 1451.0 system shall pass the proper “destId” through the API to the IEEE 1451.5 802.11 convergence layer.

The IEEE 1451.5 802.11 convergence layer shall use “destId” to look up the IP address, hostname, and destination port in its local cache. This information is used to open a TCP socket to the remote device.

If the TCP “Open” is successful, a “commId” shall be created and cached with the appropriate socket descriptor. Also, the IEEE 1451.0 “Open” shall return true.

During the write(...) or read(...) call, the IEEE 1451.0 system shall pass back down the “commId,” which the IEEE 1451.5 802.11 layer shall use to retrieve the socket descriptor from the local cache.

6.7.4 Group creation process

The IEEE 1451.0 system shall invoke this method when it is trying to add a node to the group: boolean joinGroup(UInt16 groupId, UInt16 destId).

The IEEE 1451.5 802.11 layer shall decide what group multicast address and port to use for this group. The IEEE 1451.5 802.11 layer shall locally cache the information: groupId, multicast address, port. It is outside of the standard how the multicast addresses and ports are selected.

It is recommended that multicast addresses be selected using the following algorithm. This scheme provides a mechanism whereby NCAPs on the same subnet use a different block of multicast addresses. It is assumed that the time-to-live is set to one so the multicast messages do not traverse the gateway or router device and do not reach other subnets.

- The upper byte of the multicast address shall be 239.
- The next byte shall start with zero and be incremented for each new IEEE 1451.5 group. This allows each NCAP to configure up to 256 different multicast groups.
- The last two bytes shall be the same as the last two bytes of the NCAP's IP address. As IP addresses on the same subnet will differ in these locations, this will ensure that the multicast addresses selected by each NCAP will not conflict with addresses being used by other NCAPs.
- All nodes in the same group shall open a UDP listen socket on the designated multicast address and port. The appropriate IGMP message must also be generated to fully join the multicast group.

The IEEE 1451.5 802.11 layer shall look up the IP address associated with the “destId” passed by the IEEE 1451.0 system in the joinGroup(...) call.

Refer to 6.8.3.14 of IEEE 1451.5 802.11 for details on how to tell a destination to join the appropriate multicast group.

The receiving IEEE 1451.5 802.11 convergence layer shall join the designated multicast group by opening a “listen” socket with appropriate multicast address and port. The receiving IEEE 1451.5 802.11 convergence layer shall prepare itself to receive incoming multicast traffic.

6.8 Convergence layer

The IEEE 1451.5 802.11 layer shall interface directly with the API defined between the IEEE 1451.0 and IEEE 1451.5 systems, as shown in Figure 8. This subclause shall outline the mapping between the IEEE 1451.0 API at Layer 5 and the Layer 4 TCP commands outlined above.

NOTE—The IDL code and the description of the arguments are defined in IEEE Std 1451.0-2007 and repeated here for completeness. In case of differences IEEE Std 1451.0-2007 is the controlling document.

6.8.1 IEEE1451Dot0::ModuleCommunication::Comm

IDL: interface Comm { };

The Comm abstract interface is provided by the IEEE 1451.5 system and called by the IEEE 1451.0 system to provide a common mechanism to control the “life cycle” of an IEEE 1451.5 instance. The Comm methods are listed in Table 11.

Table 11—Comm Methods

<i>Ieee1451Dot0::ModuleCommunication::Comm</i>
Args::UInt16 init()
Args::UInt16 shutdown()
Args::UInt16 sleep(in Args::TimeDuration duration)
Args::UInt16 wakeup()
Args::UInt16 performOperation(in Args::UInt16 operationId, in Args::TimeDuration timeout, in Args::ArgumentArray inArgs, out Args::ArgumentArray outArgs)
Args::UInt16 describe(out Args::UInt8 logicalType, out Args::UInt8 physicalType, out Args::_String name)

6.8.1.1 init

IDL: Args::UInt16 init();

This method will be called at startup and when the IEEE 1451.0 system needs to reset this IEEE 1451.5 instance to the power-on state. In dynamic cases, each IEEE 1451.5 instance shall call the appropriate Registration::Register1451.5() method to register this instance with the IEEE 1451.0 system.

Parameters:

None.

Return result: Error code.

Mapping to the IEEE 1451.5 system:

The functionality of “Init” shall be achieved by the use of information from the PHY TEDS, followed by use of the TCP “Open” command as specified above.

6.8.1.2 shutdown

IDL: Args::UInt16 shutdown();

The following method is invoked by the IEEE 1451.0 system to shutdown this instance of the IEEE 1451.5 interface. This shall be called to coordinate an orderly shutdown of the IEEE 1451.5 interface. In dynamic cases, each IEEE 1451.5 instance shall call the Registration::unRegister1451.5() method to unregister this instance from the IEEE 1451.0 system.

Parameters:

None.

Return result: Error code.

Mapping to the IEEE 1451.5 system:

The functionality of “Shutdown” shall be achieved by the use of information from the PHY TEDS, followed by use of the TCP “Close” command as specified above.

6.8.1.3 sleep

IDL: Args::UInt16 sleep(in Args::TimeDuration duration);

The following method is invoked by the IEEE 1451.0 system to put this instance of the IEEE 1451.5 interface into the sleep (i.e., low-power) state. This shall be when the IEEE 1451.0 system does not intend to communicate through this IEEE P1451.5 interface for a significant period of time.

Parameters:

The “duration” parameter is the amount of time to sleep. A negative duration indicates the IEEE 1451.5 device should sleep until the wakeup method is invoked.

Return result: Error code.

Mapping to the IEEE 1451.5 system:

The implementation of “Sleep” shall be implemented by the IEEE 802.11 **PMD_PWRMGMT** request primitive; refer to 14.5.5.9 of IEEE Std 802.11-2007.

PMD_PWRMGMT.request

Function

This primitive is used by the higher layer entities to manage or control the power consumption of the PMD sublayer when not in use. This allows higher layer entities to put the radio into a sleep or standby mode when receipt or sending of any data is not expected.

Semantics of the service primitive

The primitive shall provide the following parameter:

PMD_PWRMGMT.request (MODE)

The MODE parameter may have one of two values: ON or OFF. When the value of the parameter is ON, the PMD sublayer entity shall enter into a fully functional mode that allows it to send or receive data. When the value of the parameter is OFF, the PMD sublayer entity shall place itself in a standby or power-saving mode. In the low-power mode, the PMD sublayer entity is not expected to be able to perform any request by the PLCP, nor is it expected to indicate any change in PMD sublayer state or status.

When generated

This primitive is delivered by the PLCP but actually is generated by a higher layer management entity.

Effect of receipt

Upon receipt of this primitive, the PMD sublayer entity shall enter a fully functional or low-power consumption state depending on the value of the primitive’s parameter.

6.8.1.4 wakeup

IDL: Args::UInt16 wakeup();

The following method is invoked by the IEEE 1451.0 system to wake up this instance of the IEEE 1451.5 interface from the sleep (i.e., low-power) state. This shall be when the IEEE 1451.0 system has previously put this IEEE 1451.5 interface to sleep and now needs to resume communication.

Parameters:

None.

Return result: Error code.

Mapping to the IEEE 1451.5 system:

The implementation of “WakeUp” shall be implemented by the IEEE 802.11 **MLME_POWERMGT** request primitive, refer to 10.3.1.1 of IEEE Std 802.11-2007:

MLME Power Management

Function

This primitive requests a change in the power management mode.

Semantics of the service primitive

The primitive parameters are as follows:

MLME-POWERMGT.request (
 PowerManagementMode,
 WakeUp,
 ReceiveDTIMs
)

See Table 12 for the definitions of these arguments.

Table 12—Power management modes

Name	Type	Valid range	Description
Power Management Mode	Enumeration	ACTIVE, POWER_SAVE	An enumerated type that describes the desired power management mode of the STA.
WakeUp	Boolean	True, false	When true the MAC is forced immediately into the Awake state. This parameter has no effect if the current power management mode is ACTIVE.
ReceiveDTIMs	Boolean	True, false	When true this parameter causes the STA to awaken to receive all DTIM frames. When false, the STA is not required to awaken for every DTIM frame.

When generated

This primitive is generated by the SME to implement the power-saving strategy of an implementation.

Effect of receipt

This request sets the STA’s power management parameters. The MLME subsequently issues a **MLMEPOWERMGT.confirm** that reflects the results of the power management change request.

6.8.1.5 performOperation

```
IDL: Args::UInt16 performOperation(  
    in Args::UInt16      operationId,  
    in Args::TimeDuration timeout,  
    in Args::ArgumentArray inArgs,  
    out Args::ArgumentArray outArgs);
```

This low-level mechanism sends an arbitrary command to the local IEEE 1451.5 system. This method will perform a blocking operation. The format of input and output arguments are command dependent. The caller shall make sure to use the correct data types for each input argument.

Parameters:

The “operationId” specifies the desired command class code. This standard will define legal operations.

The “timeout” parameter specifies the maximum amount of time the caller is willing to block before a timeout error should be returned. A value of secs==0, nsecs== -1 means “wait forever.”

The “inArgs” are the input arguments in ArgumentArray form.

The [out] “outArgs” are returned output arguments.

Return result: Error code.

Mapping to the IEEE 1451.5 system:

Implementation dependent.

6.8.1.6 describe

```
IDL: UInt16 describe (  
    out UInt8      logicalType,  
    out UInt8      physicalType,  
    out _String name );
```

This is a generic mechanism to describe the type of the underlying IEEE 1451.5 object.

Parameters:

The [out] “logicalType” specifies the type of interface.

The [out] “physicalType” specifies the type of the physical layer.

The [out] “name” is a human readable name that was provided during the registration process.

Return result: Error code.

Table 13—Logical interface type

Enumeration	Logical type
0	Reserved
1	Point to Point (P2P)
2	Network (Net)
3–127	Reserved
128–255	Open to manufacturers

Mapping to the IEEE 1451.5 system:

```
UInt16 describe (
    out UInt8    logicalType => '2',
    out UInt8    physicalType => '802.11',
    out _String name => $name );
```

The [out] \$name is a human readable name that was provided during the registration process.

6.8.2 Ieee1451Dot0::ModuleCommunication::P2PComm

IDL: interface P2PComm { };

The P2PComm interface is appropriate in cases where the node only receives and optionally replies to incoming messages (i.e., it never initiates communications). Also, the P2PComm interface may be used in the case where the node is only initiating communication to a single destination.

The P2PComm interface is provided by the IEEE 1451.5 system and called by the IEEE 1451.0 system to perform communication operations. The point-to-point Comm methods are listed in Table 14.

Table 14—Point-to-point Comm methods

<i>Ieee1451Dot0::ModuleCommunication::P2PComm</i>
Args::UInt16 read(in Args::TimeDuration timeout, inout Args::UInt32 len, out Args::OctetArray payload, out Args::_Boolean last);
Args::UInt16 write(in Args::TimeDuration timeout, in Args::OctetArray payload, in Args::_Boolean last);
Args::UInt16 flush();
Args::UInt16 readSize(out Args::UInt32 cacheSize);
Args::UInt16 setPayloadSize(in Args::UInt32 size);
Args::UInt16 abort();
Args::UInt16 commStatus(out Args::UInt16 statusCode);

6.8.2.1 read

```
IDL: Args::UInt16 read(
    in Args::TimeDuration    timeout,
    in Args::UInt32          maxLen,
    out Args::OctetArray      payload,
    out Args::_Boolean        last);
```

This method is called by the IEEE 1451.0 system to retrieve information on the current communication operation. This method is always called by the IEEE 1451.0 system on the receiving node for both one-way and two-way communication sequences. For two-way sequences, this method is also called on the initiating node to retrieve the response.

In cases where the IEEE 1451.0 system makes multiple read() calls for large payloads, the “len” value returns the length of each transfer, not the total length.

Parameters:

The “timeout” parameter specifies the maximum amount of time the caller is willing to block before a timeout error should be returned. A value of secs==0, nsecs== -1 means “wait forever”.

The “maxLen” parameter indicates the maximum number of octets to be transferred by the IEEE 1451.5 system.

The [out] “payload” parameter is the OctetArray provided by the IEEE 1451.0 system to the IEEE 1451.5 system. The IEEE 1451.5 system will transfer available data into this array.

The [out] “last” parameter indicates if additional calls to read() should be performed by the IEEE 1451.0 system. A false value indicates that the IEEE 1451.5 system has more octets to communicate to the IEEE 1451.0 system, and the IEEE 1451.0 system must make additional read() calls. A true value indicates that the complete payload has been transferred from the IEEE 1451.5 system to the IEEE 1451.0 system.

Return result: Error code.

Mapping to the IEEE 1451.5 system:

Receive

Format: RECEIVE (commId, [payload], maxLen) -> byte count, urgent flag, push flag, last

This command allocates a receiving buffer associated with the specified connection. If no OPEN precedes this command or the calling process is not authorized to use this connection, an error is returned.

In the simplest implementation, control would not return to the calling program until either the buffer was filled or some error occurred, but this scheme is highly subject to deadlocks. A more sophisticated implementation would permit several RECEIVES to be outstanding at once. These would be filled as segments arrive. This strategy permits increased throughput at the cost of a more elaborate scheme (possibly asynchronous) to notify the calling program that a PUSH has been seen or a buffer filled.

If enough data arrive to fill the buffer before a PUSH is seen, the PUSH flag shall not be set in the response to the RECEIVE. The buffer shall be filled with as much data as it may hold. If a PUSH is seen before the buffer is filled, the buffer shall be returned partially filled and PUSH indicated.

If there is urgent data, the user shall have been informed as soon as it arrived via a TCP-to-user signal. The receiving user should thus be in “urgent mode.” If the URGENT flag is on, additional urgent data remains. If the URGENT flag is off, this call to RECEIVE has returned all the urgent data, and the user may now leave “urgent mode.” Note that data following the urgent pointer (non-urgent data) cannot be delivered to the user in the same buffer with preceding urgent data unless the boundary is clearly marked for the user.

To distinguish among several outstanding RECEIVES and to take care of the case that a buffer is not completely filled, the return code is accompanied by both a buffer pointer and a byte count indicating the actual length of the data received.

Alternative implementations of RECEIVE might have the TCPallocate buffer storage, or the TCP might share a ring buffer with the user.

NOTE—“byte count” and “maxLen” shall be used to generate “last” return value.

6.8.2.2 write

```
IDL: Args::UInt16 write(  
    in Args::TimeDuration    timeout,  
    in Args::OctetArray      payload,  
    in Args::_Boolean        last);
```

This method is called by the IEEE 1451.0 system to begin or continue a communication operation. It is always called on the initiating node to begin communication. In two-way communications, it is also called on the receiving node to provide the response.

Parameters:

The “timeout” parameter specifies the maximum amount of time the caller is willing to block before a timeout error should be returned. A value of secs==0, nsecs==−1 means “wait forever.”

The “payload” parameter is the OctetArray to be communicated.

The “last” parameter indicates if additional calls to write() will be made by the IEEE 1451.0 system to provide additional portions of the payload. A false value indicates that the IEEE 1451.0 system has more octets to send and will call write() additional times. A true value indicates that the complete payload has been transferred from the IEEE 1451.0 system to the IEEE 1451.5 system.

Return result: Error code.

Mapping to the IEEE 1451.5 system:

Send

Format: SEND (commId, [payload], byte count, PUSH=last, URGENT flag [,timeout])

This call causes the data contained in the indicated user buffer to be sent on the indicated connection. If the connection has not been opened, the SEND is considered an error. Some implementations may allow users to SEND first; in which case, an automatic OPEN would be done. If the calling process is not authorized to use this connection, an error is returned.

If the PUSH flag is set, the data shall be transmitted promptly to the receiver, and the PUSH bit shall be set in the last TCP segment created from the buffer. If the PUSH flag is not set, the data may be combined with data from subsequent SENDs for transmission efficiency.

If the URGENT flag is set, segments sent to the destination TCP shall have the urgent pointer set. The receiving TCP shall signal the urgent condition to the receiving process if the urgent pointer indicates that data preceding the urgent pointer has not been consumed by the receiving process. The purpose of urgent is to stimulate the receiver to process the urgent data and to indicate to the receiver when all the currently known urgent data has been received. The number of times the sending user’s TCP signals urgent shall not necessarily be equal to the number of times the receiving user shall be notified of the presence of urgent data.

If no foreign socket was specified in the OPEN, but the connection is established (e.g., because a LISTENing connection has become specific due to a foreign segment arriving for the local socket), then the designated buffer is sent to the implied foreign socket. Users who make use of OPEN with an