

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

**Industrial communication networks – Fieldbus specifications –
WirelessHART™ communication network and communication profile**

Withhold



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

Industrial communication networks – Fieldbus specifications –
WirelessHART™ communication network and communication profile

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE

XH

ICS 25.040.40 ; 35.100.05

ISBN 978-2-88910-811-4

CONTENTS

FOREWORD.....	13
INTRODUCTION.....	13
1 Scope.....	14
1.1 General.....	14
1.2 Specifications.....	14
1.3 Procedures.....	14
1.4 Applicability.....	14
1.5 Conformance.....	14
2 Normative references	15
3 Terms, definitions, abbreviated terms, acronyms, and conventions.....	15
3.1 Terms and definitions	15
3.2 Abbreviated terms and acronyms	20
4 Physical Layer.....	23
5 TDMA Data Link layer.....	24
5.1 Purpose	24
5.2 Overview	25
5.2.1 TDMA Basics.....	25
5.2.2 Mesh Networking.....	27
5.2.3 Network Maintenance.....	28
5.2.4 Time Keeping	28
5.3 Data-Link Layer Services	29
5.3.1 General.....	29
5.3.2 Message SPs	29
5.3.3 Management SPs.....	33
5.4 Logical Link Control.....	35
5.4.1 The DLPDU	35
5.4.2 DLPDU Types.....	39
5.4.3 DLPDU Priority and Flow Control.....	41
5.4.4 Error Detection Coding and Security.....	42
5.5 Medium Access Control.....	43
5.5.1 General	43
5.5.2 Slot Timing	44
5.5.3 Communication Tables and Buffers	46
5.5.4 Link Scheduling	52
5.5.5 MAC Operation.....	56
5.6 Physical Layer-Specific Requirements.....	64
6 Network Management.....	65
6.1 Purpose	65
6.2 WirelessHART™	65
6.2.1 General	65
6.2.2 Mesh Networks.....	66
6.2.3 WirelessHART Network Components.....	67
6.2.4 Message Routing.....	71
6.2.5 Security	73
6.3 Network Layer Services.....	74

6.3.1	General	74
6.3.2	Network Layer Message SPs	74
6.3.3	WirelessHART Network Layer Management Services	78
6.4	WirelessHART Network Layer	81
6.4.1	General	81
6.4.2	Wireless Network Layer PDUs	81
6.4.3	Wireless Transport Layer.....	89
6.4.4	Wireless Network Layer Operation.....	96
6.4.5	WirelessHART Procedures	104
7	Wireless Devices	119
7.1	Purpose	119
7.2	Overview	119
7.2.1	General	119
7.2.2	WirelessHART Network Components.....	119
7.3	WirelessHART Field Devices.....	122
7.3.1	Overview	122
7.3.2	General Requirements.....	122
7.3.3	Maintenance Port	122
7.3.4	WirelessHART Interface	123
7.4	Wireless Adapter	125
7.4.1	Overview	125
7.4.2	General Requirements.....	126
7.4.3	WirelessHART Interface	126
7.5	WirelessHART Gateway	127
7.5.1	Overview to this subclause	127
7.5.2	General Requirements.....	128
7.5.3	Gateway Model.....	130
7.5.4	Gateway Management.....	136
7.5.5	WirelessHART Gateway Superframe	138
7.5.6	Gateway Change Notification Services	138
7.5.7	HART Commands Interface	140
7.6	WirelessHART Network Manager.....	144
7.6.1	General	144
7.6.2	Core Network Functions	146
7.6.3	Network Manager Requirements.....	149
7.6.4	Network Manager Model.....	150
7.6.5	Routing.....	161
7.6.6	Scheduling	162
7.6.7	Network Manager Interface.....	168
7.7	Handheld Devices	173
7.7.1	General	173
7.7.2	General Requirements.....	174
7.7.3	Maintenance Port Connection.....	174
7.7.4	Network Device Connection.....	174
7.7.5	Network Connection as a Maintenance Device	175
7.8	Redundancy	176
8	Wireless Network and Gateway Commands.....	178
8.1	Overview	178
8.2	Subject.....	179

8.3	WirelessHART Command Overview.....	179
8.3.1	Physical Layer Commands	179
8.3.2	Data Link Layer Commands.....	179
8.3.3	Network Layer Commands.....	180
8.3.4	Network Manager Commands.....	181
8.3.5	Gateway Commands.....	181
8.3.6	Wireless Application Commands.....	182
8.4	NETWORK Commands.....	183
8.4.1	General	183
8.4.2	Command 768 Write Join Key.....	183
8.4.3	Command 769 Read Join Status.....	184
8.4.4	Command 770 Request Active Advertising	184
8.4.5	Command 771 Force Join Mode	185
8.4.6	Command 772 Read Join Mode Configuration	186
8.4.7	Command 773 Write Network Id	187
8.4.8	Command 774 Read Network Id	188
8.4.9	Command 775 Write Network Tag	188
8.4.10	Command 776 Read Network Tag	189
8.4.11	Command 777 Read Wireless Device Capabilities.....	189
8.4.12	Command 778 Read Battery Life	190
8.4.13	Command 779 Report Device Health	190
8.4.14	Command 780 Report Neighbor Health List.....	191
8.4.15	Command 781 Read Device Nickname Address	192
8.4.16	Command 782 Read Session List.....	192
8.4.17	Command 783 Read Superframe List	193
8.4.18	Command 784 Read Link List.....	194
8.4.19	Command 785 Read Graph List.....	194
8.4.20	Command 786 Read Neighbor Property Flag.....	195
8.4.21	Command 787 Report Neighbor Signal Levels.....	195
8.4.22	Command 788 Alarm "Path Down".....	196
8.4.23	Command 789 Alarm "Source Route Failed".....	196
8.4.24	Command 790 Alarm "Graph Route Failed"	197
8.4.25	Command 791 Alarm "Transport Layer Failed"	197
8.4.26	Command 793 Write UTC Time Mapping	198
8.4.27	Command 794 Read UTC Time Mapping	198
8.4.28	Command 795 Write Timer Interval.....	199
8.4.29	Command 796 Read Timer Interval	200
8.4.30	Command 797 Write Radio Power Output.....	200
8.4.31	Command 798 Read Radio Output Power.....	201
8.4.32	Command 799 Request Service.....	202
8.4.33	Command 800 Read Service List.....	203
8.4.34	Command 801 Delete Service	204
8.4.35	Command 802 Read Route List	204
8.4.36	Command 803 Read Source-Route.....	205
8.4.37	Command 804 Read CCA Mode	205
8.4.38	Command 805 Write CCA Mode	206
8.4.39	Command 806 Read Handheld Superframe	207
8.4.40	Command 807 Request Handheld Superframe Mode.....	207
8.4.41	Command 808 Read Packet Time-to-Live	

8.4.42	Command 809 Write Packet Time-to-Live	208
8.4.43	Command 810 Read Join Priority	209
8.4.44	Command 811 Write Join Priority	209
8.4.45	Command 812 Read Packet Receive Priority	210
8.4.46	Command 813 Write Packet Receive Priority	210
8.4.47	Command 814 Read Device List Entries	211
8.4.48	Command 815 Add Device List Table Entry	211
8.4.49	Command 816 Delete Device List Table Entry	212
8.4.50	Command 817 Read Channel Blacklist	213
8.4.51	Command 818 Write Channel Blacklist	214
8.4.52	Command 819 Read Back-Off Exponent	214
8.4.53	Command 820 Write Back-Off Exponent	215
8.4.54	Command 821 Write Network Access Mode	216
8.4.55	Command 822 Read Network Access Mode	216
8.4.56	Command 823 Request Session	217
8.5	Gateway and Network Manager Commands	217
8.5.1	Command 832 Read Network Device Identity using Unique ID	217
8.5.2	Command 833 Read Network Device's Neighbor Health	218
8.5.3	Command 834 Read Network Topology Information	219
8.5.4	Command 835 Read Publish Data Message List	220
8.5.5	Command 836 Flush Cached Responses for a Device	220
8.5.6	Command 836 Write Update Notification Bit Mask for a Device	221
8.5.7	Command 838 Read Update Notification Bit Mask for a Device	221
8.5.8	Command 839 Change Notification	222
8.5.9	Command 840 Read Network Device's Statistics	223
8.5.10	Command 841 Read Network Device Identity using Nickname	223
8.5.11	Command 842 Write Network Device's Scheduling Flags	224
8.5.12	Command 843 Read Network Device's Scheduling Flags	225
8.5.13	Command 844 Read Network Constraints	225
8.5.14	Command 845 Write Network Constraints	226
8.6	Network Management Configuration Commands	226
8.6.1	Command 960 Disconnect Device	226
8.6.2	Command 961 Write Network Key	227
8.6.3	Command 962 Write Device Nickname Address	228
8.6.4	Command 963 Write Session	228
8.6.5	Command 964 Delete Session	229
8.6.6	Command 965 Write Superframe	230
8.6.7	Command 966 Delete Superframe	231
8.6.8	Command 967 Write Link	231
8.6.9	Command 968 Delete Link	232
8.6.10	Command 969 Write Graph/Neighbor Pair	233
8.6.11	Command 970 Delete Graph Connection	234
8.6.12	Command 971 Write Neighbor Property Flag	234
8.6.13	Command 972 Write Network Suspend	235
8.6.14	Command 973 Write Service	236
8.6.15	Command 974 Write Route	237
8.6.16	Command 975 Delete Route	237
8.6.17	Command 976 Write Source-Route	238
8.7	Device Specific Wireless-NETWORK Commands	

8.7.1	General	239
8.7.2	Command 64 512 Read Wireless Module Revision	239
9	Application Layer addendum – Device Commands.....	241
9.1	Subject.....	241
9.2	Application of Publish data mode and event commands.....	241
9.2.1	Publish data Mode Commands	241
9.2.2	Event Notification	243
9.3	DEVICE Commands	244
9.3.1	Revisions to IEC 61158-6-20	244
9.3.2	Additional commands	245
10	Security	274
11	Amendment to IEC 61784-1:2007 for Profile 9/2	276
13.3	Profile CP 9/2 (WirelessHART).....	276
13.3.1	Physical layer	276
13.3.2	Data Link Layer	282
13.3.3	Application Layer.....	283
Figure 1	– OSI 7-Layer Communication Model mapped to Type 20.....	13
Figure 2	– Data-Link Layer Scope.....	24
Figure 3	– A TDMA Slot and Superframe.....	25
Figure 4	– Channel Hopping	26
Figure 5	– Mesh Network.....	27
Figure 6	– Message Service Sequences.....	30
Figure 7	– DLPDU Structure	36
Figure 8	– Address Specifier.....	37
Figure 9	– Construction of 8 byte EUI-64 Addresses	37
Figure 10	– DLPDU Specifier.....	38
Figure 11	– Slot Timing.....	44
Figure 12	– Data-Link Table Relationships.....	47
Figure 13	– Relationships Used for Link Scheduling.....	53
Figure 14	– MAC Components	56
Figure 15	– TDMA State Machine	58
Figure 16	– ACK Transmission.....	60
Figure 17	– Transmit State Machine	61
Figure 18	– Receive State Machine	63
Figure 19	– Network Layer.....	65
Figure 20	– WirelessHART Network	66
Figure 21	– Typical WirelessHART Network Components	68
Figure 22	– Single Access Point with Clock	70
Figure 23	– Multiple Access Points with Clocks.....	70
Figure 24	– Access Point Not Providing Clock	70
Figure 25	– Graph Routing.....	72
Figure 26	– Source Routing	73
Figure 27	– Network Layer Message Sequence	75

Figure 28 – WirelessHART Network Layer Context Diagram	81
Figure 29 – WirelessHART NPDU Structure	82
Figure 30 – Network Control Byte	83
Figure 31 – Expanded Routing Information	84
Figure 32 – Security Sub-Layer	84
Figure 33 – Security Control Byte	85
Figure 34 – Transport Layer	90
Figure 35 – Transport Byte	90
Figure 36 – WirelessHART Command Format	91
Figure 37 – Using Transport Layer to Change Network Key	93
Figure 38 – WirelessHART Network Layer Operation	98
Figure 39 – Wireless Network Table Relationships	100
Figure 40 – NPDU Clients	101
Figure 41 – Join Sequence	107
Figure 42 – Network Layer Join Procedure	111
Figure 43 – Data-Link Layer Network Search Procedure	113
Figure 44 – Device leaving the network	115
Figure 45 – Neighbor Discovery	116
Figure 46 – Path Failure	117
Figure 47 – Changing Network Keys	118
Figure 48 – WirelessHART Standalone Gateway	120
Figure 49 – Supporting Publish Data Operation	125
Figure 50 – Wireless Adapter	126
Figure 51 – Gateway Scope	128
Figure 52 – Virtual Gateway and Network Access Points in a WirelessHART Network	129
Figure 53 – Gateway model	130
Figure 54 – Logical Network Device	133
Figure 55 – Physical Network Device	134
Figure 56 – Managing Notification Services	140
Figure 57 – Network Manager Scope	145
Figure 58 – Network Manager in WirelessHART Network	146
Figure 59 – General Model for Network Manager	151
Figure 60 – Kinds of Devices	153
Figure 61 – Network Routing	154
Figure 62 – Network Schedule	156
Figure 63 – Example of a Three-slot Superframe	157
Figure 64 – Multiple Superframes in a Network	158
Figure 65 – Security Manager	159
Figure 66 – Network Management Architecture	160
Figure 67 – Example Four Network Device WirelessHART Network	165
Figure 68 – Example of Command Message Sequences	169
Figure 69 – Initializing a WirelessHART Network	170
Figure 70 – Allocating and using services	171

Figure 71 – Adjusting Network Schedule.....	172
Figure 72 – Health Reports.....	172
Figure 73 – WirelessHART Handheld Connections.....	174
Figure 74 – Network Routing.....	176
Figure 75 – Graph Routing from WirelessHART Device "A" to the Network Manager.....	177
Figure 76 – Redundant Network Managers	178
Figure 77 – Trigger Mode 1: Windowed.....	259
Figure 78 – Windowed Condition on Publish Data with max. Update Time expired	259
Figure 79 – Update Time change on Limit Excess.....	260
Figure 80 – Physical Layer Message SP's.....	280
Table 1 – Local Device Management Commands	33
Table 2 – Network ID Allocation	36
Table 3 – Slot Timing Symbols.....	45
Table 4 – Minimum Table and Buffer Space Requirement	47
Table 5 – Superframe Properties	48
Table 6 – Link Properties	48
Table 7 – Neighbor Table Entry	50
Table 8 – Graph Table Entry	51
Table 9 – Packet Record.....	51
Table 10 – Packet Precedence Order.....	54
Table 11 – Example BOCntr Selection Sets	54
Table 12 – 2 450 MHz IEEE STD 802.15.4-2006 Timing and Specifications	64
Table 13 – Physical Channel Table.....	64
Table 14 – Destination Enumerator.....	76
Table 15 – Transport Type Codes.....	76
Table 16 – Transport Type Codes Pairs.....	77
Table 17 – Local Device Management Commands	78
Table 18 – General Network Layer Attributes	80
Table 19 – Session Table Attributes.....	80
Table 20 – Route Table Attributes.....	80
Table 21 – Security Layer Sizes.....	85
Table 22 – Session Table Entry	86
Table 23 – NPDU Nonce (Byte-String 'N')	87
Table 24 – Transport Table Entries	92
Table 25 – Definitions of Network Layer States.....	96
Table 26 – Minimum Session Table Space Requirement	100
Table 27 – Route Table Entries.....	100
Table 28 – Service Table Entries	101
Table 29 – NPDU Construction	102
Table 30 – Default Route Based on Priority and Transport Type	102
Table 31 – Routing of Forwarded Packets.....	104

Table 32 – Mandatory Commands for WirelessHART Field Devices	122
Table 33 – Wireless Adapter Minimum Capacity Requirements	126
Table 34 – Required Command Responses	139
Table 35 – WirelessHART Gateway Status Flags	142
Table 36 – Gateway Minimum Capacity Requirements	142
Table 37 – Required Gateway Commands	143
Table 38 – Cached Response Messages	144
Table 39 – Network Manager Requirements	149
Table 40 – Routing Requirements	161
Table 41 – Scheduler Requirements	162
Table 42 – FrameId 1: 1 s Update Rate (Superframe Length 100)	166
Table 43 – FrameId 4: 4 s Update (Superframe Length 400)	166
Table 44 – FrameId 0: Management Superframe	166
Table 45 – Join Request (shared w/ management responses)	166
Table 46 – Join Response (shared w/ management requests)	166
Table 47 – Commands	166
Table 48 – Command Responses	167
Table 49 – Node A	167
Table 50 – Node B	167
Table 51 – Node C	168
Table 52 – Node D	168
Table 53 – Void	168
Table 54 – Network Manager Universal Commands	169
Table 55 – Physical layer commands	179
Table 56 – DL commands	179
Table 57 – Network layer commands	180
Table 58 – Network Manager Commands	181
Table 59 – Gateway Commands	182
Table 60 – Wireless Application Commands	182
Table 61 – Command 768 Request Data Bytes	183
Table 62 – Command 768 Response Data Bytes	183
Table 63 – Command 768-specific Response Codes	183
Table 64 – Command 769 Request Data Bytes	184
Table 65 – Command 769 Response Data Bytes	184
Table 66 – Command 769-specific Response Codes	184
Table 67 – Command 770 Request Data Bytes	185
Table 68 – Command 770 Response Data Bytes	185
Table 69 – Command 770-specific Response Codes	185
Table 70 – Command 771 Request Data Bytes	186
Table 71 – Command 771 Response Data Bytes	186
Table 72 – Command 771-specific Response Codes	186
Table 73 – Update periods allowed	242
Table 74 – Minimum Update Rates Allowed by Physical Layer	242

Table 75 – Identify response value field	244
Table 76 – Publish Data Message Priorities	257
Table 77 – Publish Data Message Trigger Source	258
Table 78 – 802.15.4 Physical Layer Requirements adopted by WirelessHART	277
Table 79 – Transceiver Specifications	278
Table 80 – Frequency Assignments	278
Table 81 – Local Device Management Commands	281
Table 82 – CP 9/2: DLL service selection	282
Table 83 – CP 9/2: DLL protocol selection	283

Withdrawn

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
FIELDBUS SPECIFICATIONS –****WirelessHART™ communication network and communication profile**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

A PAS is a technical specification not fulfilling the requirements for a standard, but made available to the public.

IEC/PAS 62591 has been processed by subcommittee 65C: Industrial networks of IEC technical committee 65: Industrial-process measurement, control and automation.

NOTE Use of some of the associated protocol Types in the IEC 61158 series are restricted by their intellectual-property-right holders. In all cases, the commitment to limited release of intellectual property rights made by the holders of those rights permits a particular Data-Link layer protocol Type to be used with physical layer and application layer protocols in Type combinations as specified explicitly in the IEC 61784 series. Use of the various protocol Types in other combinations may require permission from their respective intellectual property right holders.

IEC draws attention to the fact that it is claimed that compliance with this publication may involve the use of patents. IEC takes no position concerning the evidence, validity and scope of these patent rights.

The text of this PAS is based on the following document:

This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document

Draft PAS	Report on voting
65C/506A/PAS	65C/513/RVD

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned may transform it into an International Standard.

This PAS shall remain valid for an initial maximum period of 3 years starting from the publication date. The validity may be extended for a single 3-year period, following which it shall be revised to become another type of normative document, or shall be withdrawn.

Withdrawn

INTRODUCTION

This IEC/PAS 62591 provides the specification, definitions, and profile of a future standard covering additions to IEC 61158 and additions to IEC 61784-1.

IEC 61158-5-20 Ed. 1 and IEC 61158-6-20 Ed.1 contain the application layer. This document adds the following:

- data link layer protocol specification;
- data link layer service definitions;
- fieldbus profile addendum for the data link layer specifying the wireless physical layer.

This document does not provide the required structure of the IEC 61158 series (for example separation of DL-service definitions and DL-protocol specification) and of the IEC 61784-1 series. The required structure will be provided during the process of becoming an International Standard.

The Type 20 protocol supports two-way digital communications for process measurement and control devices. Applications include remote process variable interrogation, cyclical access to process data, parameter setting and diagnostics. This document defines the specification that comprises the Type 20 field communications protocol for wireless devices. Specification of the Type 20 protocol is based largely on the OSI 7-Layer Communication Model (see Figure 1).

OSI Layer	Function	WirelessHART
Application	Provides the User with Network Capable Application	Command Oriented, Predefined Data Types and Application Procedures Auto-Segmented transfer of large data sets
Presentation	Converts Application Data Between Network and Local Machine Formats	
Session	Connection Management Services for Applications	Secured Session between Network Devices
Transport	Provides Network Independent, Transparent Message Transfer	Reliable stream transport, Negotiated Segment Sizes
Network	End to End Routing of Packets. Resolving Network Addresses	Power-Optimized Redundant Path, Mesh to the edge Network
Data Link	Establishes Data Packet Structure, Framing, Error Detection, Bus Arbitration	Secure & Reliable, Time Synced, TDMA/CSMA, Frequency Agile with ARQ
Physical	Mechanical / Electrical Connection. Transmits RawBit Stream	2.4GHz Wireless, 802.15.4 based radios, 10dBm Tx Power

Figure 1 – OSI 7-Layer Communication Model mapped to Type 20

INDUSTRIAL COMMUNICATION NETWORKS – FIELDBUS SPECIFICATIONS – WirelessHART™ communication network and communication profile

1 Scope

1.1 General

The Data-Link layer provides basic messaging communications between devices in an automation environment.

The protocol and services provide a communication for WirelessHART¹ based on a Physical layer according to IEEE 802.15.4.

1.2 Specifications

This PAS specifies

- a) the procedures for the transfer of data and control information from one Data-Link user entity to another user entity or many, and among the Data-Link entities forming the distributed datalink service provider;
- b) the structure of the fieldbus DLPDUs used for the transfer of data and control information by the protocol of this publication, and their representation as physical interface data units.

1.3 Procedures

The procedures are defined in terms of

- a) the interactions between DL-entities (DLEs) through the exchange of fieldbus DLPDUs;
- b) the interactions between a DL-service (DLS) provider and a DLS-user in the same system through the exchange of DLS primitives;
- c) the interactions between a DLS-provider and a Ph-service provider in the same system through the exchange of Ph-service primitives.

1.4 Applicability

These procedures are applicable to instances of communication between systems which support communications services within the Data-Link layer of the OSI or fieldbus reference models, and which require the ability to interconnect in an open systems interconnection environment.

Profiles provide a simple multi-attribute means of summarizing an implementation's capabilities, and thus its applicability to various communications needs.

1.5 Conformance

This PAS also specifies conformance requirements for systems implementing these procedures. This standard does not contain tests to demonstrate compliance with such requirements.

¹ WirelessHART™ is the trademark of HART® Communication Foundation (HCF). HCF is a non-profit trade organization to support the HART Communication. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the trademark holder or any of its products. Compliance to this profile does not require use of the registered trademark. Use of the trademark requires permission of the trade name holder.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61158-5-20:2007, *Industrial communication networks – Fieldbus specifications – Part 5-20: Application layer service definition – Type 20 elements*

IEC 61158-6-20:2007, *Industrial communication networks – Fieldbus specifications – Part 6-20: Application layer protocol specification – Type 20 elements*

IEC 61784-1:2007, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

IEC 61804-3, *Function blocks (FB) for process control – Part 3: Electronic Device Description Language (EDDL)*

IEEE 802.15.4-2006, *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)*

HART *Communication Foundation Common Tables Specification* HCF_SPEC-183, available at <http://www.hartcomm2.org/hcf/services_tools/doc_sales.html>

3 Terms, definitions, abbreviated terms, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1

absolute slot number

count of all slots that have occurred since the network was formed and always contains the number of the current slot

NOTE The Absolute Slot Number is only incremented and is never to be reset.

3.1.2

acknowledge

explicit Data-Link response to the successful reception of a directed, non-broadcast DLPDU from a Data-Link source device and the second DLPDU of a two-DLPDU transaction

3.1.3

antenna gain

apparent power gain resulting from the antenna capability of concentrating power in a given direction

3.1.4

assailant

device generating interference

3.1.5

broadcast

sending of packets to all Network Devices that overhear the transmission

3.1.6

byte

8-bits; sometimes called an Octet

3.1.7

channel

RF band used to transmit a modulated signal carrying packets

3.1.8

channel blacklisting

method of eliminating a RF channel from usage

3.1.9

channel hopping

regular change of transmit / receive frequency to combat interference and fading

3.1.10

channel offset

link-specific value provided by the Network Manager that is used to calculate the channel to use when channel hopping

3.1.11

clear channel assessment

used to avoid initiating a transaction while the RF channel is in use. It is performed by listening to the channel prior to sending the first DLPDU of a transaction. If signal is detected the transaction is deferred to a later TDMA slot

3.1.12

coexistence

ability of one system to perform a task in a given shared environment in which other systems have an ability to perform their tasks and may or may not be using the same set of rules [IEEE 802.15.4-2006]

3.1.13

connection

data structure associated with graph routing that contains an ordered pair of Network Devices

3.1.14

Data-Link Layer

layer 2 in the OSI Basic Reference Model. This layer is responsible for the error-free communication of data. The Data-Link Layer defines the message structure, error detection strategy and bus arbitration rules

3.1.15

Device Id

device nickname that uniquely identifies a device within a WirelessHART Gateway. A Client uses the Device Id to interact with the interfaces provided by the WirelessHART Gateway

3.1.16

device specific document

document provided by the supplier of a device providing details for a given device

3.1.17**discovery**

method to locate or identify WirelessHART Gateways without human interaction

3.1.18**frame**

Data-Link Layer packet which contains the header and trailer information required by the physical medium. That is, Network Layer packets are encapsulated to become frames

3.1.19**frequency channels**

allocation of the frequency spectrum in a given frequency range

3.1.20**gateway**

network device containing at least one host interface (such as serial or Ethernet), acting as ingress or an egress point

3.1.21**graph**

routing structure that forms a directed end-to-end connection between network devices

3.1.22**Graph Id**

identifier used to indicate a specific graph entry

3.1.23**handheld**

host application residing on a portable device

3.1.24**HCF Enumeration**

number of data structures use enumerations which are controlled by the HART Communications Foundation (HCF). HCF maintains current lists of these enumerations

3.1.25**hop**

movement of a packet directly between two adjacent neighbors in one network transaction without the participation of any other nodes in the network. Multiple hops are used to lengthen the transmit distance, bypass interference sources or avoid obstructions

3.1.26**interoperability**

ability for like devices from different manufacturers to work together in a system and be substituted one for another without loss of functionality at the host system level

3.1.27**join**

process by which a Network Device is authenticated and allowed to participate in the network. A device is considered joined when it has the Network Key, a Network Manager Session and a normal (not join) superframe and links

3.1.28**latency**

time it takes for a packet to cross a network connection, from sender to receiver

3.1.29

lease

lease is an agreement between the host and the WirelessHART Gateway to share a resource for a future period of time; after which the resources can be reallocated for other purposes

3.1.30

link

full communication specification between adjacent devices in the network, that means, the communication parameters necessary to move a packet one hop. A link is a function of source/destination address pairing, slot and channel offset assignment, direction, (Tx/Rx or Rx/Tx), dedicated or shared communication, and link type. Links are assigned to Superframes as part of the scheduling process

3.1.31

link margin

difference between the power of a received signal and the sensitivity of the receiver. Typically, this determines the viability of a link. Around 10 dB of margin is desirable for a reliable link

3.1.32

Logical Link Control

higher of the two data link layer sublayers defined in the OSI Model. This sublayer handles error control, flow control, framing, and addressing

3.1.33

Medium Access Control

sub-layer found with the OSI Data-Link Layer (OSI Layer 2) used for arbitrating access to the communication channel

3.1.34

neighbor

adjacent nodes in the network such that the Receive Signal Level (RSL) suggests communication in at least one direction is possible

3.1.35

network device

device with a direct Physical Layer connection to the network. Each network device (e.g., field device or gateway) has a HART Unique Address that is used in communication with the device. Network Devices include Field Devices, Access Points (i.e. Gateways), Adapters, and Handhelds

3.1.36

Network Manager

responsible for configuration of the network, scheduling communication between network devices, management of the routing tables and monitoring and reporting the health of the network

NOTE There must be one and only one network manager per WirelessHART Network. Although the network manager need not have a direct Physical Layer connection it still must have a HART Unique Address.

3.1.37

node

addressable logical or physical device attached to the network

NOTE See also network device 3.1.35.

3.1.38**Nonce**

number constructed so as to be unique to the current packet to ensure that old communications cannot be reused in replay attacks. The nonce is also necessary for maintaining packet secrecy and providing sender authenticity and packet integrity

3.1.39**omni-directional antenna**

antenna with a radiation pattern that, when viewed from above, is equally strong in all directions

NOTE The antenna thus sends or receives signals equally well in all directions.

3.1.40**packet**

generic reference to the set of data communicated across a network

3.1.41**packet error rate**

average number packets (in percent) transmitted but not received correctly. For this specification, the reference PPDU for PER calculations is 20 bytes long (IEEE)

3.1.42**Peer**

correspondent node at the other end of the communication link. The communication link terminates at the same protocol layer in the correspondent node

3.1.43**Physical Layer**

Layer 1 in the OSI model is responsible for transmission of the raw bit stream and defines the mechanical and electrical connections and signaling parameters for devices

3.1.44**receiver sensitivity**

minimum input signal required to produce a PER of less than 1 % with a PPDU 20 bytes long

[IEEE 802.15.4-2006]

3.1.45**Route Id**

identifier used to indicate a specific route

3.1.46**service session**

agreement between a Client and a WirelessHART Gateway that services shall be provided to the Client by the Gateway

3.1.47**Session Id**

An identifier used to indicate a specific session entry

3.1.48**Shed Time**

time between the last good message reception and the assumption of digital communication failure

3.1.49

slot

fixed time interval that may be used for communication between neighbors

3.1.50

superframe

collection of slots repeating at a constant rate. Each slot may have a link associated with it

3.1.51

Superframe Id

An Identifier used to indicate a specific superframe entry

3.1.52

throughput

effective data transfer rate of the network

3.1.53

time sequence diagram

graphical representation used to illustrate the interrelationship between the Protocol services. The protocol layer of interest and the lower, intervening layers are treated as a black box. The internal workings of these layers are not shown on this diagram. The time sequence diagram shows the interactions between the service primitives over time. Sometimes referred to as a Message Sequence Diagram

3.1.54

time to live

field in the network header of each packet that specifies how many more hops a packet can travel before being discarded

3.1.55

transaction

complete atomic cycle of Data-Link activity. A transaction consists of (a) a single DLPDU transmission from a source device, or (b) two DLPDUs: one from the Data-Link source followed by a second, link-level acknowledgement DLPDU from the destination

3.1.56

unicast

sending of a packet to a single node in the network

3.1.57

UTF-8

8-bit UCS/Unicode Transformation Format

variable-length character encoding for Unicode. All XML described in this PAS is encoded using UTF-8 characters

3.2 Abbreviated terms and acronyms

ACK	See Acknowledge [3.1.2] ²
ADC	Analog-to-Digital Converter
ASN	See Absolute Slot Number [3.1.1]

² Figures in square brackets refer to subclause 3.1.

CCA	Clear Channel Assessment
DAC	Digital-to-Analog Converter
DAQ	Data Acquisition. This refers to a device specific ADC or DAC
dB	Relative power decibels (3dB/octave, 10 dB/decade)
dBi	dBi is used to express the gain of an antenna in decibels. The terminal letter 'i' indicates that the gain is relative to an isotropic antenna
dBm	dBm is an abbreviation for the power ratio in decibels (dB) of the measured power, referenced to one milliwatt (1 mW). 0 dBm = 1 mW; 10 dBm = 10 mW; 20 dBm = 100 mW; 30 dBm = 1 W
DLL	Data-Link Layer
DLPDU	Data-Link Protocol Data Unit (i.e., a Data-Link Layer packet)
DR	Delayed Response
DRM	Delayed Response Mechanism
DSSS	Direct Sequence Spread Spectrum
EEPROM	Electrically Erasable Programmable Read Only Memory. Non-volatile memory that is alterable by the Field Device without the use of external programming apparatus
EIRP	Equivalent Isotropic Radiated Power (also Effective Isotropic Radiated Power)
EUI-64	Extended Unique Identifier (64 bits long)
FSK	Frequency Shift Keyed
FTA	Field Termination Assembly (as referenced in Figure 6)
HCF	HART® Communication Foundation
ISM	Industry, Scientific, Medical Frequency bands
LoS	Line of Sight, an unobstructed distance between a transmitter and a receiver
LRV	Lower Range Value. Defines the relationship between a Dynamic Variable value and an analog channel lower endpoint (e.g. 4.00mA)
LSB	Least Significant Byte. The LSB is always the last byte transmitted over a HART data link
LTL	Lower Transducer Limit. The digital value that defines the minimum reliable and accurate value of a dynamic or Device Variable

MAC	See Medium Access Control [3.1.33]
MIC	Message Integrity Code
MSB	Most Significant Byte. The MSB is always the first byte transmitted over a HART data link
NAN	Not-a-Number
NPDU	Network PDU
O-QPSK	Offset - Quadrature Phase Shift Keying
OUI	Organizationally Unique Identifier
OUI	Organizationally unique identifier as defined by IEEE 802
PDU	Protocol Data Unit. The packet of information being communicated
PER	See Packet Error Rate
PhPDU	Physical Layer Protocol Data Unit (i.e., a Physical Layer packet)
PHY	See Physical Layer
PPDU	Physical Protocol Data Unit
RC	Response Codes
RSL	Received Signal Level. The signal level (in dBm) at a receiver input terminal
SP	Service Primitive
STX	Start of a transaction. An STX is used to convey a Network layer packet (an NPDU) from one node to an adjacent node
TDMA	Time Division Multiple Access
TER	Transaction Error Rate
TPDU	Transport PDU
TTL	Time To Live
UART	Universal Asynchronous Receiver Transmitter
URV	Upper Range Value. Defines the relationship between a Dynamic Variable value and an analog channel upper endpoint (e.g. 20,0 mA).
UTL	Upper Transducer Limit. The digital value that defines the maximum reliable and accurate value of a dynamic or Device Variable

WHA WirelessHART Adapter

WHD WirelessHART Device

4 Physical Layer

The Physical Layer is derived from IEEE 802.15.4. The profile is given in Clause 11.

Withdrawn

5 TDMA Data Link layer

5.1 Purpose

Clause 5 defines the HART TDMA Data-Link Layer. This specification is applicable for mesh network communications via an IEEE STD 802.15.4-2006 Physical Layer. The Data-Link Layer is responsible for the secure, reliable, error free communication of data between HART devices. In other words, this publication specifies the rules used by HART devices to wirelessly communicate HART digital information. Figure 2 shows the scope of this specification.

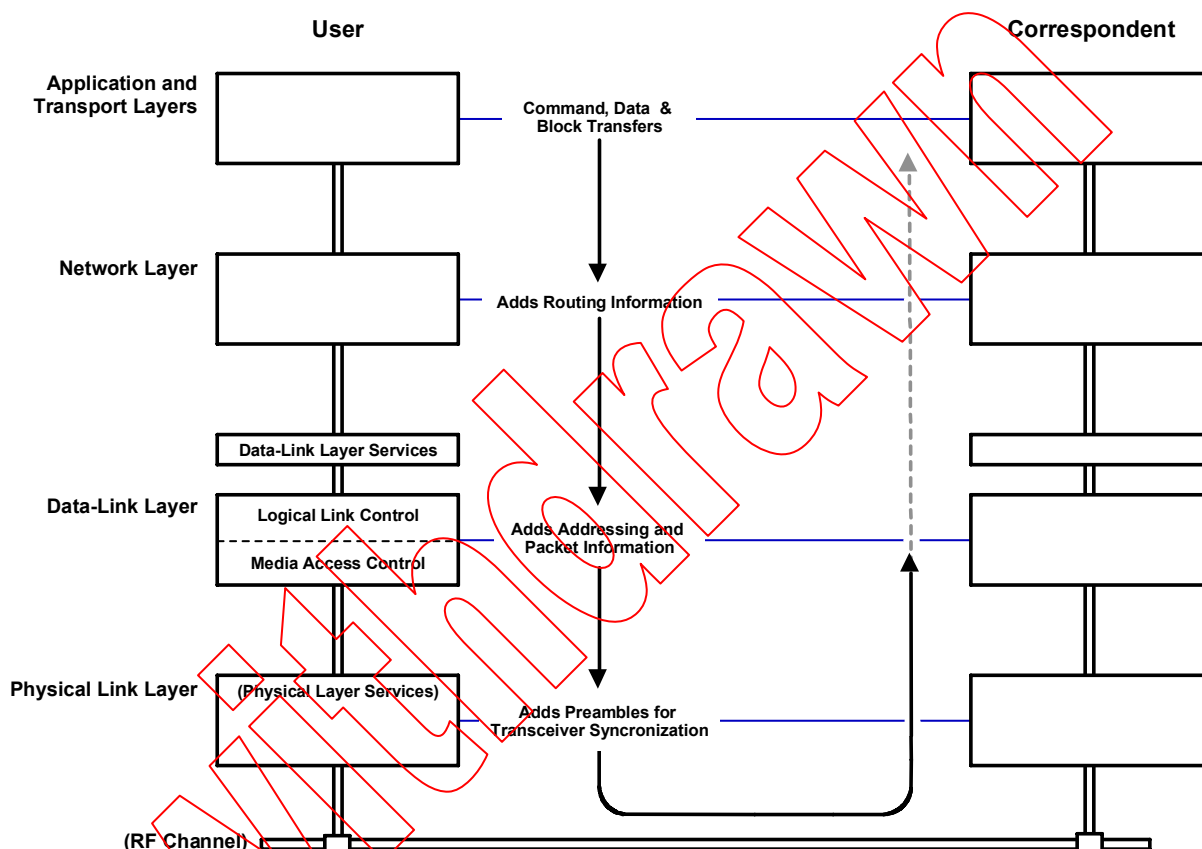


Figure 2 – Data-Link Layer Scope

Clause 5 includes the following:

- The services provided by the Data-Link Layer to the Network Layer. These services constitute a black box model of the Data-Link Layer requirements. These services are specified with the assistance of Time Sequence Diagrams.
- Logical Link Control (LLC) requirements including the format of HART frames, the structure of HART device addresses; the security services used for message integrity and the error detection coding to be used.
- Medium Access Control (MAC) rules ensuring that transmissions by devices occur in an orderly fashion. In other words, the MAC specifies when a device is allowed to transmit a message. MAC specifications themselves are formulated in terms of state transition diagrams, which permit an unambiguous description of the action of the MAC sub-layer.
- The actual timing values required for proper operation of the MAC sub-layer. These timing values directly correspond to Physical Layer performance characteristics (e.g., Clear Channel Assessment time, Tx/Rx turnaround time).

The segregation of requirements into these four categories is intended as a frame of reference rather than as a description of an actual implementation.

Unless specifically noted, HART data is transmitted most significant byte first (i.e., big endian).

Within this context, the Data-Link Layer as a whole has only a one hop scope. Any responsibilities to the network beyond the device's immediate neighbors are allocated to the Network Layer.

5.2 Overview

5.2.1 TDMA Basics

WirelessHART uses Time Division Multiple Access (TDMA) and channel hopping to control access to the network. TDMA is a widely used Medium Access Control (MAC) technique that provides collision free, deterministic communications. TDMA uses time slots where communications between devices occur. A series of time slots form a TDMA superframe. All devices shall support multiple superframes, starting with superframe zero (0). At least one Superframe always enabled while additional superframes can be enabled or disabled (see Clause 6 for more information). Slot sizes and the superframe length (in number of slots) are fixed and form a network cycle with a fixed repetition rate. Superframes are repeated continuously.

Figure 3 illustrates the basics of TDMA: its slots and the superframe.

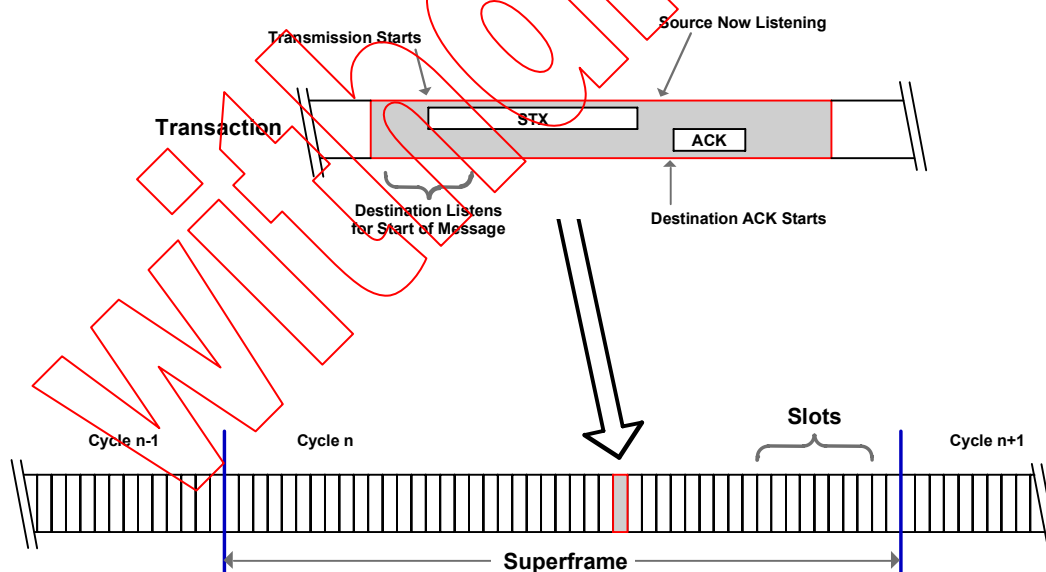


Figure 3 – A TDMA Slot and Superframe

Typically, two devices are assigned to a given slot. One is designated as the source and the other, the destination. A communication transaction within a slot supports the transmission of a Data-Link Protocol Data Unit (DLPDU) from a source followed immediately by the transmission of an acknowledgement (ACK) DLPDU by the addressed device. The addressed device's response DLPDU shall contain either "Success" Response Code indicating the initial DLPDU was successfully received and handled, or an error Response Code. An error Response Code indicates that the initial DLPDU was successfully received, but that further processing failed, e.g., there are no buffers available in the receiving device. See the Command Response Code Tables for more information.

NOTE A broadcast message (i.e., the Data-Link destination address is the broadcast address) is never acknowledged. In this case, multiple receivers are assigned to the same slot.

For successful and efficient TDMA communications, synchronization of clocks between devices in the network is critical. Consequently, tolerances on time keeping and time synchronization mechanisms are specified to ensure network-wide device clock synchronization. It is imperative that devices know when the start of a slot occurs.

Within the slot, transmission of the source message starts at a specified time after the beginning of a slot. This short time delay allows the source and destination to set their frequency channel and allows the receiver to begin listening on the specified channel. Since there is a tolerance on clocks, the receiver shall start to listen before the ideal transmission start time and continue listening after that ideal time. Once the transmission is complete, the communication direction is reversed and the destination device indicates, by transmitting an ACK, whether it received the source device's DLPDU successfully or with a specific class of detected errors. (Non-response implies either non-reception or reception with errors outside of these classes.)

To enhance reliability, channel hopping is combined with TDMA. Channel hopping provides frequency diversity, which can avoid interferers and reduce multi-path fading effects. TDMA enables efficient, low-power and reliable channel hopping communication because the synchronization of the slot and channel used by the communicating devices allows them to rendez-vous in time and frequency, thus promoting successful communications (see Figure 4).

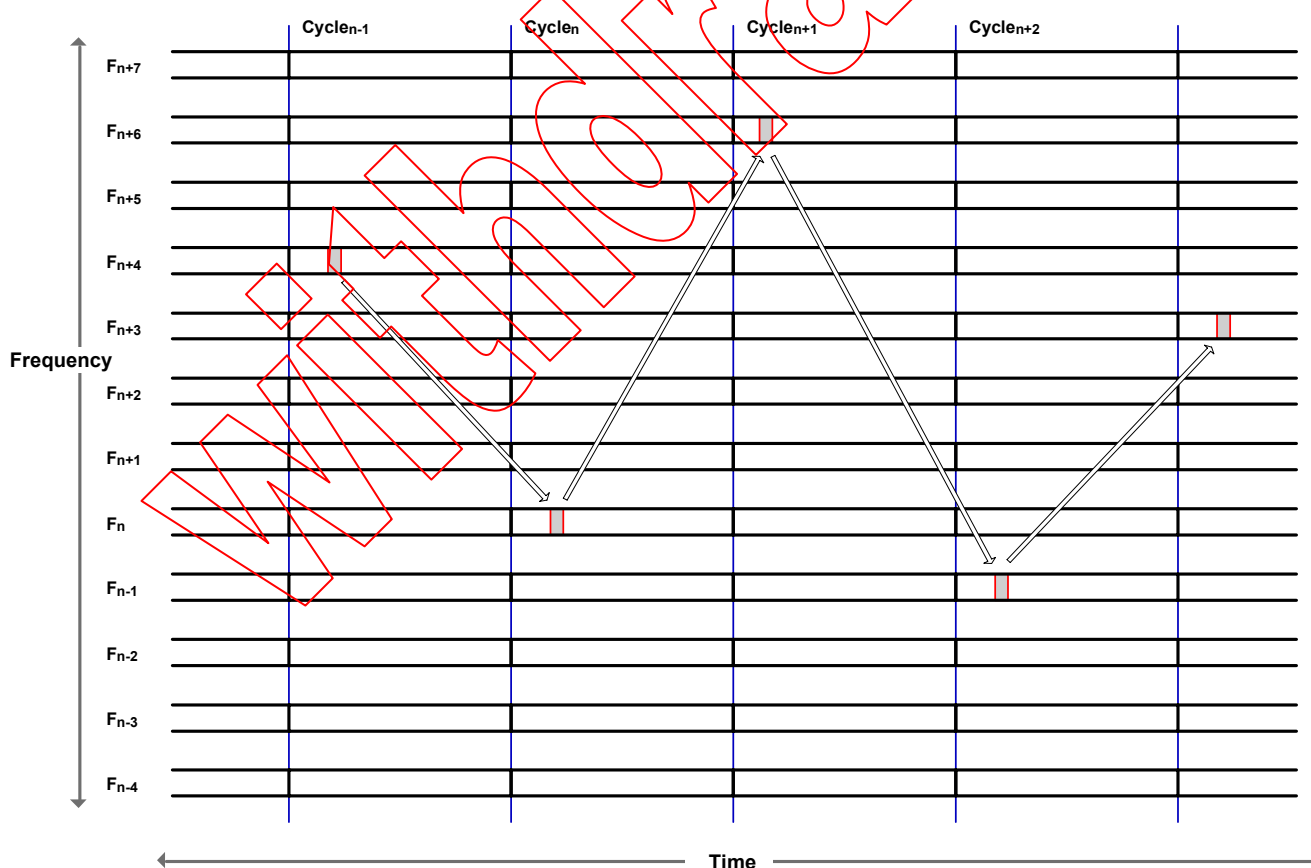


Figure 4 – Channel Hopping

Communicating devices are assigned to a superframe, slot, and channel offset. This forms a communication link between communicating devices. All devices shall support multiple links. The number of possible links is, typically, equal to the number of channels utilized by a network times the number of slots in the superframe. For example, using 15 channels and 9 000 slots per superframe results in 135 000 possible links.

Channel hopping provides channel diversity, so each slot shall be used on multiple channels at the same time by different nodes. This can be achieved by creating links on the same slot, but with different channel offsets. Each device shall maintain a list of channels in use and the specification (e.g., the frequency) for that channel. All devices in a network shall have identical channel lists determined by the Network Manager.

Assignment of links and the devices in a link is the responsibility of the Network Manager (see Clause 6).

Channel blacklisting is the WirelessHART protocol feature that allows the network administrator to restrict the channel hopping of Network Devices network-wide to selected channels in the RF band. For example, network administrators can blacklist channels in order to protect a wireless service that uses a fixed portion of the RF band that would otherwise be shared by the WirelessHART Network. In practice, WirelessHART communication (like WiFi, Bluetooth, and other wireless communication) is very random and uses a tiny amount of the total bandwidth. Consequently, blacklisting seldom provides tangible benefits.

5.2.2 Mesh Networking

WirelessHART is a mesh communication protocol that simplifies installation of wireless field devices, allowing the end user to tailor the installation to the specific application requirement. WirelessHART compatible devices can be deployed in a star topology (i.e., all devices are one hop to the gateway) to support a high performance application, a multi-hop overly-connected mesh topology for a less demanding (e.g., monitoring) application, or any topology in between. In fact, WirelessHART technology is flexible enough, enabling a variety of applications (both high and low performance) to operate in the same network.

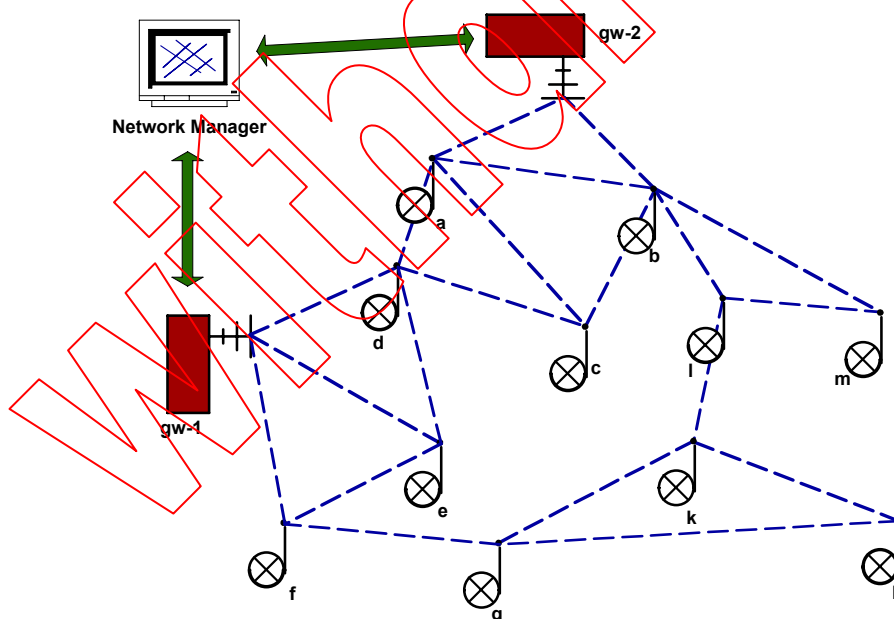


Figure 5 – Mesh Network

All network devices shall be able to source and sink packets and be capable of routing packets on behalf of other devices in the network. Each time a packet moves across a link, it is called a hop. The routing of packets from their initial source to their final destination can take several hops. The actual routing of packets is the responsibility of the Network Layer (see Clause 6).

Each device shall maintain a list of links; the device cycles through links, in slot time order, servicing them as needed. Every link designating the device as the receiver shall be serviced by the device.

NOTE Within that link a transmission may or may not occur.

When a packet is received it is posted to the Network Layer. If the device is the packet's final destination it will be consumed. Otherwise, the Network Layer updates routing information for the next hop (if necessary), makes any required changes in packet addressing, and passes the updated packet back to the Data-Link Layer for transmittal.

The Data-Link Layer maintains a list of DLPDUs awaiting transmittal. Links designating the device as the source are only serviced when there is a DLPDU pending for the link's destination. After successful transmittal (that means an ACK is received) to another device, the DLPDU is discarded.

5.2.3 Network Maintenance

Time and channel are the first two dimensions of a WirelessHART network. The third dimension is space (distance). WirelessHART devices are installed at various locations about a plant and, consequently, a given device has a set of other devices within communications range (i.e., in its neighborhood). Since the RF environment is subject to change, a device shall keep its neighbor list current. Maintenance activities include discovering potential neighbors, gathering statistics about the communication channel to each neighbor, and maintaining time synchronization with neighbors.

Two special DLPDUs, Advertise DLPDUs and Keep-Alive DLPDUs, assist in building and maintaining the device's neighbor list. The network manager can schedule transmissions of Advertise DLPDUs. These DLPDUs contain sufficient information to allow new neighbors to be discovered or to allow a newly installed device to request admission to the network. If accepted, the new device can become a neighbor of the advertising device. Further information about network joining can be found in Clause 6.

Every successful communication with a neighbor confirms the neighbor's presence and allows the quality of the communication link to be assessed. Since communications only occurs when the device has a DLPDU for the neighbor, there can be long intervals during which the link is not exercised. Keep-Alive DLPDUs are used to probe quiescent links and to maintain time synchronization.

5.2.4 Time Keeping

Time synchronization across the network is essential to TDMA communications. No matter the choice of device hardware time source (e.g., crystals, ceramic resonators etc.), some skew between devices (e.g., due to temperature, voltage variations or ageing) is inevitable. Consequently, WirelessHART has several mechanisms to synchronize network-wide time.

When the destination device receives a DLPDU, its time of arrival is noted. Using this information the destination calculates the difference from the ideal time at which it believes the communication should have occurred. This delta-t (Δt) shall be communicated in every ACK reply DLPDU sent to the source device. Thus, every acknowledged transaction measures the alignment of network time between the devices.

Within the neighbor list, selected neighbors, specified by the Network Manager, are used as time synchronization sources. When a DLPDU from a time synch neighbor is received, the network time of the receiving device should be adjusted. Time synchronization is based either on the DLPDU arrival time or on the delta-t in the ACK, depending on which device initiated the transaction.

In addition, device designers shall understand the time drift characteristics of their products. When the device's time source drifts, the device shall transmit Keep-Alive DLPDUs, as needed, to its time-synch neighbors to maintain time synchronization. Devices shall not require a Keep-Alive more often than once per 30 s while temperature is varying 2° C per min or less. Furthermore, device designs shall tolerate one retry in case of packet loss.

safety margin). This corresponds to approximately a compensated clock accuracy of 10 ppm or better.

NOTE Keep-Alive DLPDUs are also used for neighbor discovery and to confirm the viability of quiescent links.

5.3 Data-Link Layer Services

5.3.1 General

Subclause 5.3 specifies the operation of the TDMA Data-Link layer from a "black box" point of view. Subclause 5.3 specifies the Service Primitives (SPs) supplied by the Physical Layer to the Data-Link Layer, which the Data-Link Layer in turn can expose to upper protocol layers (chiefly the Network Layer). In addition to specifying the individual SPs, time sequence diagrams (see [Halsall]) are included to indicate the order in which the SPs should be used and the order of event occurrence at the protocol layer boundaries. See Token-Passing Data-Link Layer Specification for more information on the service methodology.

The Services described in 5.3 are used to obtain:

- A reliable "at least once" transaction service between peer entities. The service is not designed to provide duplicate detection.
- Management services for Data-Link Layer configuration.

All SPs described here shall be supported by the device unless otherwise stated. The mapping of these SPs into an implementation is entirely a local matter and is in no way restricted by this specification.

In the definition of the SPs, parameters are defined. Some parameters are optional and may not be present in all invocations of the SP. Optional parameters are distinguished by enclosing them within square brackets ("[" "]") in the SP definitions.

5.3.2 Message SPs

5.3.2.1 General

Message SPs provide services supporting the basic transfer of data between devices. There is only one required SP (TRANSMIT) and one optional SP (RECEIVE). The TRANSMIT SP initiates the message exchange. The Data-Link Layer supports automatic retransmission (i.e., retries) to ensure error-free data exchange. The time sequence diagram for these SPs is shown in Figure 6.

The transmit sequences illustrate the message traffic across the link between devices. In Figure 6, Sequence 1 shows a simple, error-free transaction. In this sequence the TRANSMIT.request inserts the message into the Data-Link Layer's transmit queue. Sometime later, when a slot, supporting scheduled communication to the destination address, occurs, the message is transmitted. When a non-broadcast message is received and validated, the correspondent Data-Link Layer transmits an ACK and generates a TRANSMIT.indicate. Upon reception of the ACK, or immediately when the message is to the broadcast address, the source Data-Link Layer generates a TRANSMIT.confirm to the requesting Network layer.

The Data-Link Layer shall also allow multiple messages to be queued. In Figure 6, Sequence 2 illustrates this requirement.

NOTE Since messages in the Data-Link Layer's queue may not be posted in the same order as slots occur, the messages may not be delivered in the same order as they are enqueued. In this Sequence, 3 messages are queued for (possibly) 3 different Data-Link destinations.

Both unicast/directed (acknowledged), and multicast/broadcast (un-acknowledged) transactions are supported. In Figure 6, Sequence 3 illustrates a multicast transaction.

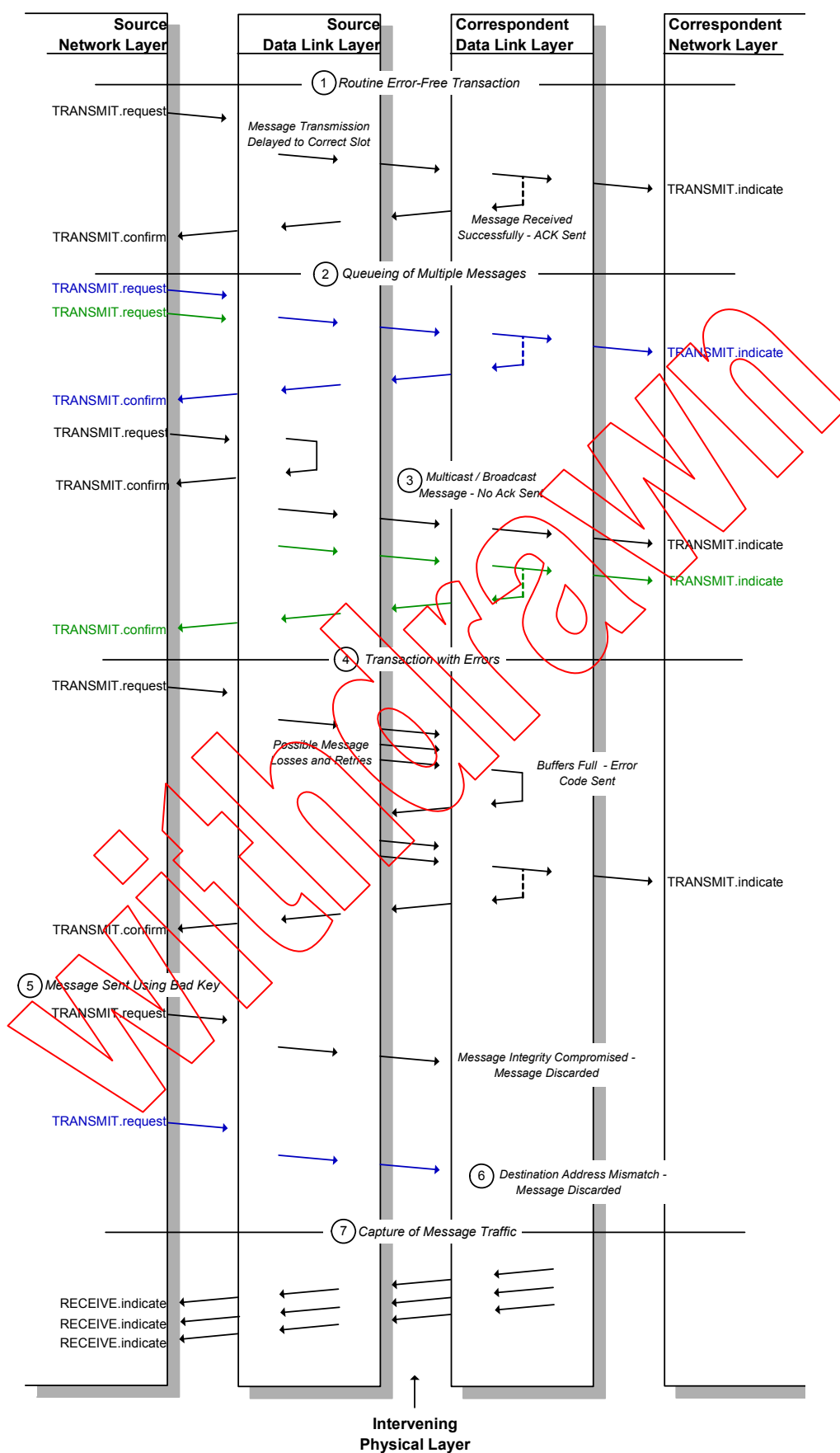


Figure 6 – Message Service Sequences

The Protocol also supports automatic retries to ensure reliable data exchange (see 5.5). A transaction including retries is shown in Figure 6, Sequence 4. As shown, the source Data-Link Layer resends the message until an acknowledge (ACK) with a Response Code of "Success" is received (or until a limit on maximum retries is reached). An individual attempt can result in no received response from the correspondent, or in receipt of an ACK with a Response Code indicating an error. If the packet was not propagated then, the packet will be rescheduled for a later attempt. If the packet resides in the device for an extended interval (i.e., longer than the specified packet timeout) the packet shall be discarded.

A correspondent Data-Link Layer can also receive messages with either an invalid message integrity code (see Figure 6, Sequence 5) or a destination address that does not match the correspondent's (see Figure 6, Sequence 6). These messages can be discarded and, in all cases, shall not be answered.

Figure 6, Sequence 7 shows the optional receive-only SP. This is available in a Data-Link Layer that supports a promiscuous operating mode where communications from other devices are captured.

5.3.2.2 Transmit SPs

5.3.2.2.1 TRANSMIT.request

```
TRANSMIT.request (handle, payload, priority, timeout, graph)           //graph routed
TRANSMIT.request (handle, payload, priority, timeout, sframe, bcast)  //broadcast
TRANSMIT.request (handle, payload, priority, timeout, shortDestAddress) // addressed
TRANSMIT.request (handle, payload, priority, timeout, longDestAddress) // addressed
```

This SP is used by a device's Network Layer to transfer data to another device. The Data-Link will generate the DLPDU and initiate the transmission once a slot to the desired destination is available. All devices shall be capable of queuing multiple requests and transmitting each packet on the appropriate link. The parameter to this SP include the following:

- **handle** - The handle is supported for the convenience of the client layer. The Data-Link returns this value in the corresponding TRANSMIT.confirm.
- NOTE This element is included for clarity and is an API Artifact that is not an essential service element.
- **payload** - The NPDU to be propagated to the destination device.
- **priority** - The packet priority as determined by the contents of the payload, from the set: {**management**, **process-data**, **normal**, **alarm**}. See 5.4.3 for more information.
- **timeout** - The maximum time to attempt packet transmission. The Network Layer shall set this based on the ASN Snippet (see Clause 5).
- **graph** - This parameter is only present if graph routing is to be employed. When employed, the graph indicates the neighbors that can be used as the destination for the next hop.
- **sframe** - This parameter is only present if broadcasting a message. *sframe* indicates the superframe whose broadcast links can be used to be used to forward the packet.
- **bcast** - This flag indicates the NPDU shall be broadcast on the indicated Superframe.
- **shortDestAddress** - This parameter indicates the Nickname of the destination device that shall be used for the next hop.
- **longDestAddress** - This parameter indicates the Unique ID of the destination device that shall be used for the next hop.

This SP is overloaded. When an explicit address is included, the Data-Link shall forward the packet to that destination. Otherwise, the Data-Link chooses the links based on the graph routing or Superframe ID.

5.3.2.2.2 TRANSMIT.confirm (handle, localStatus)

This SP communicates the result of a previously issued TRANSMIT.request. The Status indicates success or failure. The handle can be used to identify the corresponding TRANSMIT.request and shall be identical to those of the TRANSMIT.request.

5.3.2.2.3 TRANSMIT.indicate (localStatus, priority, sourceAddress, payload)

This SP is invoked by the Data-Link Layer to notify the Network layer of a successfully received payload addressed to the device. localStatus indicates the Data-Link key used to authenticate the DLPDU and whether the DLPDU was broadcast.

5.3.2.2.4 FLUSH.request (handle)

Deletes the indicated packet.

5.3.2.2.5 FLUSH.confirm (handle, localStatus)

Indicates whether the packet was deleted.

5.3.2.3 Network Event SPs

5.3.2.3.1 DISCONNECT.indicate (localStatus, sourceAddress)

Notifies that another device is disconnecting from the network. In other words, a DLPDU has been received from a device indicating it is leaving the network.

5.3.2.3.2 PATH_FAILURE.indicate (localStatus, sourceAddress)

Notice that the path to another device with which this device is connected has failed. In other words, (unexpectedly) communications with the indicated device have timed out and the device no longer seems to be available.

5.3.2.3.3 ADVERTISE.indicate (localStatus, AdvertisePayload)

The SP is generated upon reception of an Advertise DLPDU (see 5.4.2.5). Upon receiving an Advertise packet, the device that is trying to join a network shall synchronize to the network using the Absolute Slot Number (ASN) in the packet, and posts this SP to the Network Layer.

5.3.2.3.4 NEIGHBOR.indicate (localStatus, sourceAddress, packetRSL)

The NEIGHBOR.indicate SP shall be generated whenever a device receives a packet from a device not listed in Neighbor Table.

5.3.2.4 Receive SPs

This SP is only used when the device is in promiscuous mode and, thus, forwarding all packets to the client layer.

5.3.2.4.1 RECEIVE.indicate (localStatus, packetRSL, payloadDLPDU)

This optional SP indicates that a frame, not addressed to this device, has been received. The local status byte carries the status of the communication as received by this device. The reception of communications from other devices often provides useful diagnostics. Sometimes this is called a "promiscuous operating mode" and can be used for network troubleshooting.

5.3.3 Management SPs

5.3.3.1 General

Management SPs support both configuration of the Data-Link Layer and access to Data-Link Layer statistics. The fundamental SP is a LOCAL_MANAGEMENT sequence.

NOTE None of the SPs in Clause 5 require any data to be transmitted over the communication link. Remote management of the device's Data-Link Layer configuration is possible using Application Layer messaging of standard HART commands.

These SPs allow the Data-Link Layer to be configured on power up by the device's upper layers. This also allows management of the Field Device's non-volatile and programmable non-volatile memory to be isolated from the Data-Link Layer implementation.

Management SPs can be accessed long after the Field Device has been on-line. For example, the Application Layer can receive a command from a network manager that changes the slots to be used when communicating.

5.3.3.2 LOCAL_MANAGEMENT.request (service, [data])

This SP is used to configure Data-Link Layer properties. The parameters Service and Data are defined in Table 1 hereinafter.

5.3.3.3 LOCAL_MANAGEMENT.confirm (service, status, [data])

This SP is used to return the results of a corresponding LOCAL_MANAGEMENT.request. The status shall return the results of the executed request.

5.3.3.4 LOCAL_MANAGEMENT.indication (service, status, [data])

This SP is used to notify LOCAL_MANAGEMENT of an un-requested MAC-sublayer event report, see Table 1.

Table 1 – Local Device Management Commands

Service	Data	Description
RESET		Initializes the Data-Link Layer
DISCONNECT		Disconnect from the network, cease communications
RE_JOIN		Disconnect from the network, rejoin the network, purging all MAC queues and clearing all MAC tables
WRITE_SUPERFRAME		Creates a new superframe
	Unsigned-8 superframeId	
	Unsigned-16 nSlots	Length of superframe
	Boolean active	Activates (TRUE) or de-activates (FALSE) the superframe
DELETE_SUPERFRAME		Deletes an existing scheduling superframe and any associated links
	superframeId	

Service	Data	Description
ADD_LINK		Adds a new link to another device, possibly updating the neighbor and connection tables in the process
	Unsigned-8 linkHandle	handle of created link record, if any
	Unsigned-8 superframeId	
	Unsigned-16 nodeAddress	Address of neighbor device
	Unsigned-16 slot	Slot in the superframe to use by this link
	Unsigned-8 channelOffset	Offset of logical channel relative to base channel for this slot
	linkOptions	bitmap: {Transmit=b001, Receive=b010, Shared=b100}
	linkType	One of {NORMAL, JOIN, DISCOVERY}
DELETE_LINK		Deletes an existing link, possibly updating the neighbor and connection tables in the process
	linkHandle	
ADD_CONNECTION		Adds a new connection to a device via a specified graph
	Unsigned-8 connectionHandle	Handle for this connection
	Unsigned-16 graphId	graphId for the connection
	Unsigned-16 nodeNickname	address of device being connected via the specified graph
DELETE_CONNECTION		Deletes an existing connection
	Unsigned-8 connectionHandle	Handle of an existing connection
READ_NETWORKID		Reads the ID of the network the device belongs to
	Unsigned-16 NetworkID	
WRITE_NETWORKID		Writes the ID of the network the device belongs to
	Unsigned-16 NetworkID	
WRITE_NETWORK_KEY		This command allows the Network Manager to write the network key on a Network Device. Keys should be protected from pilfering (e.g., by encryption)
	Unsigned-128 networkKey	
	Unsigned-48 SlotNumber	Execution time for command (ASN) (0 means execute immediately)
READ_TIMEOUT_PERIODS		
	Time keepAliveInterval	Interval during which a node shall successfully communicate with each linked neighbor. Any DLPDU received from the neighbor resets the Keep-Alive timer for that neighbor
	Time pathFailInterval	Interval of unsuccessful communication with a given neighbor, indicating a path failure
	Time advertiseInterval	Time period specifying the transmission of Advertise DLPDUs
WRITE_TIMEOUT_PERIOD		Write the indicated time period value.
	Unsigned-8 timerCode	One of { Keep-Alive; Path-Failure; Advertise; or Discovery }
	Time timerPeriodValue	

Service	Data	Description
READ_CAPACITIES		
	Unsigned-16 maxSuperframes	
	Unsigned-16 maxLinks	
	Unsigned-16 maxNeighbors	
	Unsigned-16 maxPktBuffers	
READ_PRIORITY_THRESHOLD		
	Unsigned-4 priorityThreshold	Specifies the lowest priority DLPDU to be accepted from another device
WRITE_PRIORITY_THRESHOLD		
	Unsigned-4 priorityThreshold	
READ_JOIN_PRIORITY		Indicates what join priority the device shall advertise Lower number indicates a better choice for joining
	Unsigned-4 joinPriority	
WRITE_JOIN_PRIORITY		
	Unsigned-4 joinPriority	
READ_PROMISCUOUS_MODE		Indicates whether the sublayer is in "receive all" mode. TRUE indicates the sublayer accepts all PDUs received from the Physical Layer
	Boolean promiscuousMode	
WRITE_PROMISCUOUS_MODE		
	Boolean promiscuousMode	
READ_MAX_BACK_OFF_EXPONENT		The maximum value that can be assumed for the back-off exponent used in shared slots. Valid values are { 4, 5, 6, 7 } MaxBackoffExponent defaults to 4
	Unsigned-4 MaxBackoffExponent	
WRITE_MAX_BACK_OFF_EXPONENT		
	Unsigned-4 MaxBackoffExponent	
ADD_CONNECTION		Adds a new connection to a device with specified graphs
	Unsigned-16 connectionhandle	Handle for this connection
	Unsigned-16 grasphId	graphID for the connection
	Unsigned-16 node Nickname	Address of device being connected via the specified graph
DELETE_CONNECTION		Deletes an existing connections
	Unsigned-16 connectionhandlet	Handle of an existing connection

5.4 Logical Link Control

5.4.1 The DLPDU

5.4.1.1 General

Subclause 5.4 specifies the format of the Data-Link packet (DLPDU). Each DLPDU consists of the following fields:

- A single byte set to 0x41;
- A 1-byte address specifier;
- The 1-byte Sequence Number;
- The 2 byte Network ID
- The Destination and Source Addresses either of which can be 2 or 8-bytes long;
- A 1-byte DLPDU Specifier;
- The DLL payload;
- A 4-byte keyed Message Integrity Code (MIC), and
- A 2-byte ITU-T CRC16.

Figure 7 illustrates the basic PhPDU and DLPDU structure.

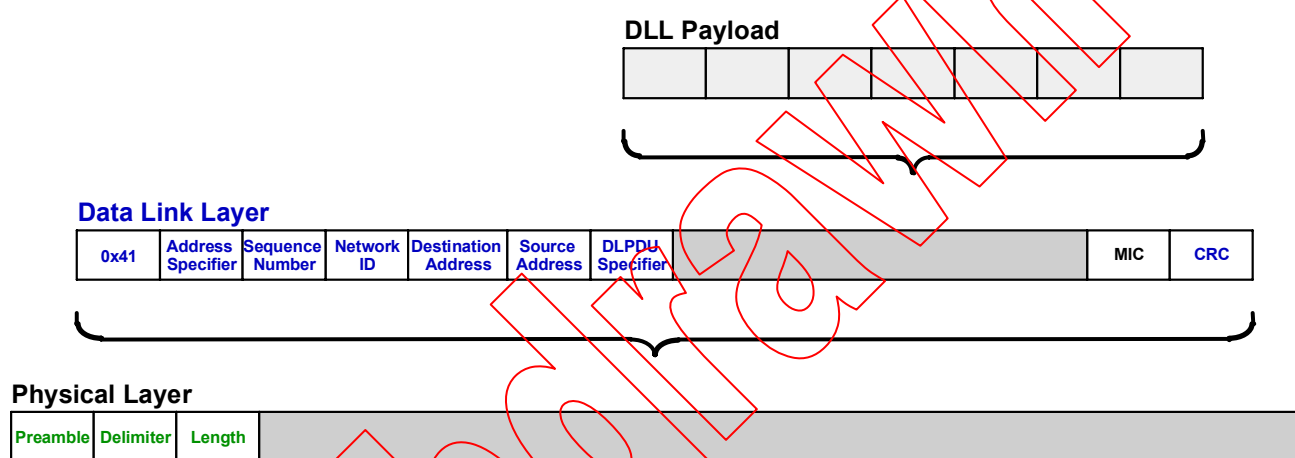


Figure 7 – DLPDU Structure

5.4.1.2 The Sequence Number

The Sequence Number shall be set equal to the least significant byte of the Absolute Slot Number (ASN).

5.4.1.3 The Network ID

All networks are identified using a 2-byte Network ID. This 2 Byte value is transmitted, LSB first, in all DLPDUs. If the Network ID does not match that of the network the device is a member of, then the packet is discarded. The ranges of Network ID values and their application are shown in Table 2.

NOTE Only in the header fields for WirelessHART is this byte ordering followed. Unless specifically noted, data is transmitted most significant byte first in all HART communications (i.e., big endian).

Table 2 – Network ID Allocation

Range	Application
00 000-32 767 (0x0000-0x7FFF)	Permanent User defined networks (Critical networks)
32 768-36 863 (0x8000-0x8FFF)	Temporary User defined networks (Demos, trade shows, field trials, etc.)
36 864-57 343 (0x9000-0xDFFF)	Reserved
57 344-61 439 (0xE000-0xEFFF)	Manufacturing networks (non-public used by device manufacturers)
61 440-65 535 (0xF000-0xFFFF)	Reserved

5.4.1.4 The Destination and Source Addresses

WirelessHART supports two types of addresses: a 2-byte "nickname" and an 8-byte IEEE EUI-64 address. The addresses contained in a DLPDU are indicated in the Address Specifier field (see Figure 8). Setting the bit 6 indicates a long 8-byte source address is contained in the DLPDU. Setting bit 2 indicates a long 8-byte destination address is contained in the DLPDU. Any combination of address lengths can be used in a DLPDU. The other bits shall be set as indicated in Figure 8.

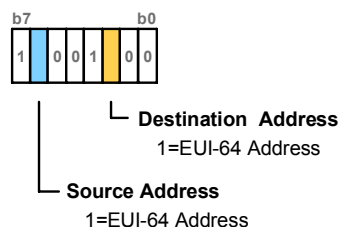


Figure 8 – Address Specifier

The 2-byte nickname is assigned and managed by the Network Manager. Consequently, it is only locally unique (i.e., within the network the device belongs to). Two-byte addresses either indicate a specific network device or they specify the broadcast address (i.e., 0xFFFF).

The EUI-64 address consists of a 3 byte "Organizationally Unique Identifier" (OUI) and the 5-byte Unique ID (controlled by the HART Protocol).

NOTE 1 The value of this central administrative number OUI is given by the IEEE Registration Authority Committee. Available at <http://standards.ieee.org/regauth>.

For WirelessHART, the EUI-64 shall be constructed using HCF's OUI (which is 0x001B1E) concatenated with the 40-bit HART Unique ID as shown in Figure 9. DLPDUs received with EUI-64 addresses that do not specify the HCF OUI shall be discarded.

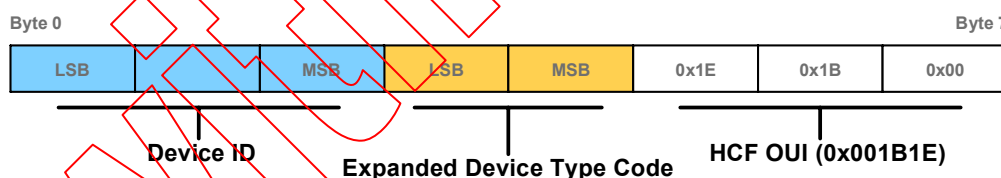


Figure 9 – Construction of 8 byte EUI-64 Addresses

The Unique ID is the concatenation of the 2-byte Expanded Device Type Code and the 3-byte Device Identifier. The Expanded Device Type Code is allocated by the HCF. Each device manufactured with the same Device Type Code shall have a different Device ID

IEEE STD 802.15.4-2006 requires multi-byte fields to be transmitted LSB first (little endian) and the WirelessHART addressing is compliant. Consequently, the long address is transmitted in the DLPDU starting with the LSB of the Device ID and ending with the MSB of the HCF's OUI. The nickname is also transmitted little endian (LSB first).

NOTE 2 Only in the header fields for WirelessHART is this byte ordering followed. Unless specifically noted, data is transmitted most significant byte first in all HART communications (i.e., big endian).

5.4.1.5 The DLPDU Specifier

The DLPDU Specifier is transmitted after the Network ID and addresses (see Figure 10). The most significant two bits are reserved and no device shall make any assumption regarding their possible future use. Implementations shall mask off the most significant two bits. Devices built before any such future use is assigned shall set these bits to zero on transmission.

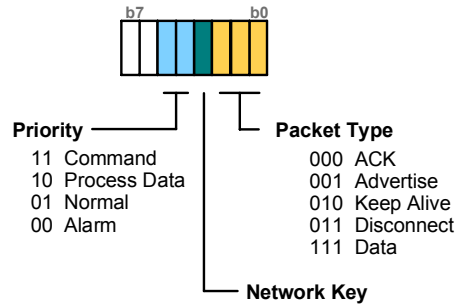


Figure 10 – DLPDU Specifier

The next two bits (i.e., bits 4 and 5) indicate the priority of the message (see 5.4.3). Command level is the highest priority and Alarm level is the lowest priority.

Bit 3 indicates the key being used to authenticate the DLPDU. All communications within the network between authenticated device shall set this bit and use the confidential Network-Key when generating the DLPDU MIC (see 5.4.4 for more information). This bit shall only be reset during the joining process (see Clause 5) while the device is unauthenticated. DLPDUs passed between the unauthenticated device and its neighbor shall use the well known key from this Specification to generate the DLPDU MIC.

The least significant 3 bits of the DLPDU Specifier indicate the DLPDU type. There are five DLPDU types: Data, Keep-Alive, Advertise, Disconnect, and ACK DLPDUs.

5.4.1.6 DLL Payload

The DLL payload depends on the DLPDU type (defined in the DLPDU Specifier field). Data DLPDUs contain a Network Layer header and payload. Data-Link command DLPDUs have contents that depend on the type of command DLPDU. For example, acknowledgement DLPDUs have a payload that consists of a time adjustment as measured by the destination device specified in the prior DLPDU.

5.4.1.7 Keyed Message Integrity Code (MIC)

A keyed Message Integrity Code (MIC) is used for link-layer authentication of DLPDUs (see 5.4.4 for more information). Devices shall reply only to unicast, non-acknowledgement DLPDUs that have been successfully authenticated.

5.4.1.8 Cyclic Redundancy Check (CRC)

The Cyclic Redundancy Check (CRC) Field is based on the 16 bit ITU-T CRC polynomial (also known as a CRC16). The CRC is calculated over the entire frame using the following polynomial:

$$G_{16}(x) = x^{16} + x^{12} + x^5 + 1$$

The CRC is usually calculated in hardware. For more information see RFC 1549 and IEEE STD 802.15.4-2006.

NOTE At receivers, the received byte stream is subjected to a similar calculation. When a receiver may predict the bytes that will contain a CRC, it may omit those bytes from the calculation and check that the received CRC matches those bytes. Alternatively, the receiver may compute a CRC over all the bytes of the message and check that the result matches an expected residual value of zero.

The CRC is used to detect bit errors and devices shall reply only to non-acknowledgement DLPDUs with a CRC matching that calculated by the receiving device, or whose residual value after processing the entire DLPDU, including received CRC bytes, matches the expected residual of zero.

5.4.2 DLPDU Types

5.4.2.1 General

The least significant 3 bits of the DLPDU Specifier indicate the type of DLPDU being communicated and the purpose of the (optional) DLL payload. There are five DLPDU types as follows:

- Data DLPDUs contain network and device data in transit to their final destination device. The source and sink for Data DLPDUs is the Network Layer.
- Keep-Alive DLPDUs facilitate connection maintenance between neighboring devices.
- Advertise DLPDUs provide information to neighboring devices wishing to join the network.
- Disconnect DLPDUs are used to advise neighboring devices that the device is leaving the network.
- ACK DLPDUs are the immediate link level response to receipt of the source device's transmission DLPDU.

Devices receiving a packet with an unknown packet type shall not acknowledge the packet and shall immediately discard it.

ACK, Advertise, Keep-Alive and Disconnect DLPDUs are generated and consumed by peer Data-Link Layers. These packets are not propagated to the Network Layer or onward through the network. In other words, these are DLL command packets originated within the source Data-Link and consumed by a neighboring, destination peer Data-Link.

5.4.2.2 Data DLPDUs

Data DLPDUs contain data in transit to a final destination device. The packet payload in these DLPDUs originates from the Network Layer of this hop's source device and is passed to the destination device's Network Layer. From there, these payloads are forwarded by the peer Network Layer to their final destination.

5.4.2.3 ACK DLPDUs

ACK DLPDUs are transmitted by a device in response to receipt of a non-broadcast, non-ACK DLPDU. All successfully received unicast, non-ACK DLPDUs shall initiate the transmission of an ACK DLPDU. The ACK DLPDU shall always calculate its MIC using the same key used in the received DLPDU. See 5.4.4 for more information about Generating a MIC and keys.

The ACK contains a Response Code that indicates whether the receiving device has accepted the DLPDU. The destination device shall respond with "Success" (RC=0) when the packet is accepted by the device or indicates the reason why the packet was not accepted (e.g., RC=61 if the destination device is out of buffer space). Destination devices shall respond with an ACK DLPDU in response to all Keep-Alive, Advertise, or Disconnect DLPDUs addressed to the device and successfully received.

To manage packet flow through the network, the network manager can raise or lower the priority level of packets that the device may accept. Devices shall accept DLPDUs with a priority greater than or equal to the current priority level set by the Network Manager. In addition, space allowing, the device shall accept DLPDUs whose final destination is the device itself.

In addition to the Response Code, the ACK payload includes the Time Adjustment field. The Time Adjustment is the difference between the expected time of reception of the complete start delimiter that frames a non-ACK DLPDU and the actual reception of that complete start delimiter, measured in μs . The Time Adjustment is a 2-byte, two's-complement integer.

The ACK payload and response codes are as follows:

ACK DLPDU Payload

Byte	Format	Description
0	Unsigned-8	Response Code
1 - 2	Signed-16	Time Adjustment in μ s. The value of the Time Adjustment is positive (negative) if the DLPDU was received earlier (later) than expected

ACK Response Codes

Code	Class	Description
0	Success	Success. DLPDU accepted by destination device
61	Error	No Buffers Available. DLPDU Discarded
62	Error	No Alarm/Event Buffers Available. DLPDU Discarded
63	Error	Priority Too Low. DLPDU Discarded

5.4.2.4 Keep-Alive DLPDUs

The Keep-Alive DLPDU is a Command DLPDU used, as needed, for network maintenance. For Keep-Alive DLPDUs, the payload field is empty. Keep-Alive DLPDUs can be used for the following purposes:

- For network time synchronization. Time synchronization is updated based on the Time Adjustment value returned in the corresponding ACK.
- To assess communication with a neighbor (e.g., to confirm connectivity).
- In Neighbor Discovery. When instructed, the device shall send Keep-Alive DLPDUs periodically to allow the device to be detected by others.

5.4.2.5 Advertise DLPDUs

The Advertise DLPDU is used to invite new devices into the network. When a device wishes to join a network, it listens for these DLPDUs and then uses the information in the DLPDU to synchronize with the network and initiate the join process.

The Advertise packet includes basic network information including: ASN, the join control information, and the security levels supported by the network. In addition, the channel map array is included in the Advertise DLPDU. The absolute slot number and the channel map allows the current channel offset to be identified when issuing a packet to petition the Network Manager for admission to the network. The size of the channel map array depends on the Physical Layer in use. For example, with the IEEE STD 802.15.4-2006 2 450 MHz Physical Layer, it is two bytes long.

Once the basic network information is disclosed, the Advertise DLPDU lists all of its join links by superframe. In addition, each link is identified as either transmit or receive from the perspective of the joining device. The joining device is limited to these links until it is authenticated by the Network Manager and has received its network and session keys. By limiting communication to only the join links, the Network Manager, in effect, can quarantine the device until it is ready for the device to fully participate in the network. The format of this DLPDU is as follows:

Advertise Payload Format

Byte	Format	Description
0-4	Unsigned-40	Absolute slot number. The number of slots since the start of the network to the slot used for transmission of this DLPDU
5	Bits	Join Control
5.7-5.4	Enum-4	Security level supported (see HCF Enumerations)
5.3-5.0	Unsigned-4	Join Control - Join Priority. An unsigned integer indicating the ability of the advertising device to support another child device. The lower the value the better this advertising device is to join

Byte	Format	Description
6	Unsigned-8	Number of bits of channel map array. Maximum size of the channel map array is 64 bits
7- <i>n</i>	Bits []	Channel map array. This is an array of bits starting with the least significant bit (bit 0 of byte 0) and adding bytes as necessary until all bits are accounted for. Each bit corresponds to a channel. If the bit is set, the corresponding channel is in use.
<i>n</i> +1	Unsigned-16	Graph ID
<i>n</i> +3	Unsigned-8	Number of superframes

For each Superframe

Unsigned-8	Superframe ID
Unsigned-16	Superframe size. The number of slots in this superframe
Unsigned-8	Number of Links

For each Link

Unsigned-16	Join slot. The specific slot within the superframe for this Link
Bits	Join slot channel offset
x.7	Reserved. Shall be set to zero. No device shall make any assumption regarding their possible future use of this bit
x.6	When set, the link is for DLPDU transmission by the joining device
x.5-x.0	Channel offset. The frequency channel offset for this slot. This value is used to calculate the link frequency/channel

An Advertise packet can be sent on any transmit link that is not in use. All other Data-Link activities have a higher priority than issuing an Advertise. Advertise DLPDUs shall always calculate their MIC using the well-known key (see 5.4.4 for more information).

5.4.2.6 Disconnect DLPDUs

Disconnect DLPDUs are generated by devices leaving the network. This means the device is no longer available for communication and shall be removed from the neighbor list. In addition, all links connecting the neighbor to this device shall be deleted as well. The Network Layer shall be notified when a Disconnect DLPDU is received.

For Disconnect DLPDUs, the payload is empty. Disconnect DLPDUs always calculate their MIC using the network key (see 5.4.4 for more information).

5.4.3 DLPDU Priority and Flow Control

The priority of a DLPDU is dictated by its contents. There are four priority levels:

- Command (highest priority). Any packet containing a payload with network-related diagnostics, configuration, or control information shall be classified with a priority of "Command".
- Process-Data. Any packet containing process data (e.g., Command 3 or 9) or network statistics (e.g., Command 779, 780) shall be classified as priority level "Process-Data". Only the control of the network (as indicated by the "Command" priority) is more important than delivery of measurements from process transmitters or setpoints to control devices. Process-Data priority packets shall be refused from other devices when three-quarters of the device's packet buffers are occupied.
- Normal. DLPDUs not meeting the criteria for "Command", "Process-Data", or "Alarm" shall be classified as "Normal" priority. Normal priority packets shall be refused from other devices when one-half the device's packet buffers are occupied.
- Alarm (lowest priority). Packets containing only alarm and event payload shall assume a priority of "Alarm". Devices shall buffer no more than one DLPDU having "Alarm" priority.

Since multiple Application Layer commands can be aggregated into a single message, the DLPDU shall assume the priority of the highest priority Application Layer command in the DLPDU.

The priority of the DLPDU is used for flow control to mitigate network congestion and ensure the Network Manager retains control of the network during a process upset or when an adverse RF event occurs. For example, the Network Manager can raise the priority threshold to reduce packet flow through the device.

In addition, the priority setting of a DLPDU has fundamental filtering effects that are applied as packets are received. Upon receiving a DLPDU, the device will use the priority of the DLPDU and the current priority threshold to determine whether the packet is accepted or discarded as follows:

- Keep-Alive, Advertise and Disconnect DLPDUs shall always be received, accepted and generate an ACK with a "Success" response code.
- If any buffers are available, DLPDUs received with "Command" level priority shall always be accepted and either consumed or forwarded. At least one buffer shall be reserved for command packets.
- A DLPDU with "Alarm" priority shall be accepted only if the single buffer reserved for that class of DLPDU is available.
- For all other received DLPDUs, the packet priority is compared to the priority threshold level. Received packets with lower priority shall be discarded. Furthermore, if the device does not have packet buffers available for that DLPDU, it shall be discarded.

In summary, network management packets always propagate through the network allowing the Network Manager to keep the network operational. Alarms' flow through the network is restricted ensuring alarm floods do not disrupt network operation. Since alarms are always time-stamped, no information regarding, for example, failure sequences is lost.

Finally, all other network traffic flows through the network as buffer space and bandwidth allows. Within this network traffic, process data has priority. Operation and control of the process is second only to preventing network communication disruption.

5.4.4 Error Detection Coding and Security

5.4.4.1 General

To perform error detection and to ensure network security, WirelessHART includes an unkeyed CRC and a MIC on every DLPDU. The CRC is used to detect communications errors. The CRC is calculated across the entire DLPDU using the 16-bit ITU-T algorithm (see 5.4.1.8).

5.4.4.2 MIC Calculation

5.4.4.2.1 General

A keyed MIC is used to ensure that the DLPDU is originated from an approved, authenticated device. The DLPDU itself is not enciphered; rather its contents are authenticated using the four-byte MIC. The MIC is generated and confirmed using CCM* mode (Counter with CBC-MAC (corrected)) in conjunction with the AES-128 block cipher to provide authentication. This cipher requires four byte-strings as parameters:

- 'a', the additional data to be authenticated but not enciphered;
- 'm', the message to be enciphered;
- 'N', the 13-byte nonce; and
- 'K', the 128-bit AES Key.

Since the DLPDU is not enciphered, the byte-string 'm' is empty (i.e., its length is zero). The DLPDU, from the 0x41 byte through the end of the payload, is the byte-string 'a'.

5.4.4.2.2 DLL Keys

The key is 128-bits long (16 bytes) and, as per the CCM Mode requirements, is copied into the 'K' byte-string in most significant byte first. In other words, K[0] and K[15] are the most significant and least significant byte of the key, respectively.

There are two DLL keys: the well-known key (used in advertisements and when joining the network), and the network key (used for all other transactions). The well-known key is identical for all WirelessHART devices and has a value of 7777 772E 6861 7274 636F 6D6D 2E6F 7267 hexadecimal. The well-known key is used for messages passed between the joining device and devices already part of the network.

The network key is a write-only value controlled by the network manager and used for all DLL transactions except Advertise and Join DLPDUs. This key is supplied by the Network Manager to joining devices.

NOTE The Network Manager may change the network key from time to time.

5.4.4.2.3 DLL Nonce

The 'N' byte-string shall be exactly 13 bytes long and is the concatenation of the ASN and the source address.

The ASN is the count of all slots that have occurred since forming the network. It is only incremented and shall never be reset. In other words, the ASN always contains the number of the current slot. The ASN is 5-bytes long and is copied (MSB to LSB) into N[0] to N[4].

The final 8-bytes of the nonce contain the source address. If the DLPDU has the EUI-64 address then it is copied (MSB to LSB) into N[5] through N[12]. In other words, 0x00, 0x1b, 0x1E are copied into N[5] through N[7], respectively. The Expanded Device Type Code and Device ID are copied (MSB to LSB) into N[8] through N[9] and N[10] through N[12], respectively.

If the 2-byte Nickname is used in the DLPDU then the nickname is copied (MSB to LSB) into N[11] through N[12]. N[5] through N[10] are set to 0x00.

5.4.4.3 Errors

Two errors may occur and, in both cases, result in the DLPDU being discarded and no response being generated by the destination device. The first potential error is a CRC mismatch. When the DLPDU is first received, the CRC is checked. If the CRC in the message does not match that in the DLPDU, the DLPDU is discarded.

The second potential error is an authentication failure. After confirming the CRC, the MIC is calculated and compared to the MIC in the DLPDU. If they disagree, the DLPDU is not authentic and it is discarded.

5.5 Medium Access Control

5.5.1 General

The primary objectives of the Medium Access Control (MAC) sublayer are to maintain slot synchronization, identify slots that shall be serviced, listen for packets being propagated from neighbors and, in turn, propagate packets received from the Network Layer. Fundamentally, the Medium Access Control (MAC) sub-layer is responsible for propagating DLPDUs across a link. To accomplish this, the device includes the following:

- Tables of neighbors, superframes, links, and graphs that configure the communication between the device and its neighbors (see 5.5.3). These tables are normally populated by the Network Manager. In addition the neighbor table is populated as neighbors are discovered.
- A link scheduler (see 5.5.4) that evaluates the device's tables and chooses the next slot to be serviced by listening for a packet or by sending a packet. In general the link scheduler walks the tables to identify the next slot in which to send a packet and the next slot in which to listen. The slot scheduled is the next of these two slots to occur.
- State machines that control the propagation of packets through the MAC sub-layer. MAC Operation (see 5.5.5) consists of schedule maintenance and service slots. MAC Operation is fundamentally event driven and responds to service primitive invocations and the start of slots needing servicing.

The number one priority of the MAC sublayer is to propagate packets enqueued in the device's buffers. Its next priority is to receive packets from neighboring devices. Both of these operations are performed one slot at a time either by sending a DLPDU or by listening for one. Successful communications depends on slot time synchronization between neighbors and the compliant timing of the transaction within the slot.

5.5.2 Slot Timing

5.5.2.1 General

All transactions occur in slots following specific timing requirements. Figure 11 shows one slot and provides an overview of transaction timing. The top of the timing diagram shows the operation of the source neighbor and the bottom shows the destination neighbor. In the figure, the destination's perception of the slot's start time is slightly retarded when compared to the source's. All of the timing symbols are depicted even though they may not be applicable to every type of transaction. Table 3 defines the timing symbols.

Each slot begins by allowing a time interval to prepare the packet being conveyed for transmission. This includes formatting of the packet and calculation of the MIC and CRC. Of course these calculations are only performed if the source has a packet to propagate to the destination. The source will perform the CCA (when required) and transmit the packet. Depending on the type of transaction, an ACK may be transmitted by the destination device.

When scheduled as the link's destination, the device shall enter receive mode. The device shall be listening for communication, starting $TsRxOffset$ from the start of its slot, before and after the device's estimation of the ideal transmit start time. The receive window (specified by $TsRxWait$) allows device timing to drift while still permitting devices to communicate and resynchronize their slot timers. Sources of drift include temperature, aging, and other effects.

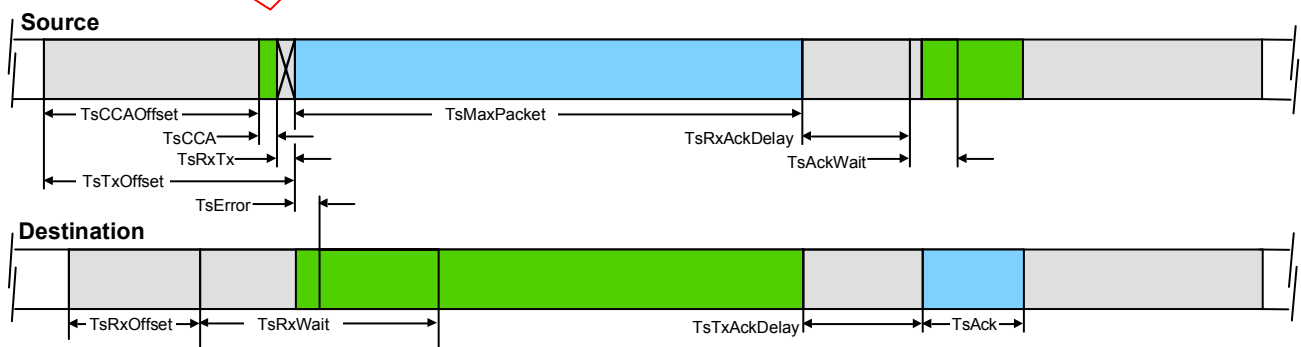


Figure 11 – Slot Timing

If the destination device detects a message, it captures the time when the start of message (i.e., the end of reception of the Physical Layer Delimiter) occurs and calculates $TsError$ as the difference between the device's ideal start time and the actual start time of the message.

If a specific destination address is specified, the source packet will result in the destination device generating and transmitting an ACK packet. If the destination address is the broadcast address no ACK packet is generated. Finally, time is allocated at the end of the slot for processing the propagated packet and preparing for the next slot, (e.g., assessing and prioritizing the packets now queued up in each device). If one of the neighbors was the time source for the other, then the end of the slot time will be aligned after successful communication.

5.5.2.2 Acknowledged Transactions

Most communications consists of the source device propagating a message by transmitting a packet and the destination device acknowledging the reception of that packet. For acknowledged communication, the source and destination address in the DLPDU shall contain a specific device address (i.e. not a broadcast address).

The source device shall begin its transmission such that the Start of Message (SOM) occurs exactly $TsTxOffset$ after its start of slot. SOM occurs upon completing the reception of the Physical Layer Delimiter. When performed, the CCA is performed beginning at $TsCCAOOffset$ after the start of the slot. The CCA is performed ($TsCCA$) and, if the channel is occupied, the transaction attempt is rescheduled for a later slot. Otherwise the transceiver is switched from receive to transmit ($TsRxTx$) and the packet is transmitted.

The destination device shall enter receive mode and be listening for communication by $TsRxOffset$ from its start of the slot. The destination shall listen for the SOM for a duration of $TsRxWait$. If the destination device detects the SOM then it shall receive and validate the message. Any message that cannot be validated shall not be acknowledged.

Table 3 – Slot Timing Symbols

Symbol	Description
$TsTxOffset$	Start of the slot to start of preamble transmission
$TsRxOffset$	Start of the slot to when transceiver shall be listening
$TsRxWait$	The minimum time to wait for start of message. This correlates to the amount of drift between the neighbors that can be tolerated and communications still be maintained
$TsError$	This is the difference between the actual start of message and the ideal start of message time as perceived by the receiving device. In other words, this is how much the receiving device perceives the transmitting device to be out of sync.
$TsMaxPacket$	The amount of time it takes to transmit the longest possible message (includes PhL preamble, delimiter, length and DLPDU)
$TsTxAckDelay$	End of message to start of ACK. The destination device shall validate the STX, and generate an ACK during this interval, see note
$TsRxAckDelay$	End of message to when transceiver shall be listening for ACK
$TsAckWait$	The minimum time to wait for the start of an ACK
$TsAck$	Time to transmit an ACK
$TsCCAOOffset$	Start of slot to beginning of CCA
$TsCCA$	Time to perform CCA
$TsRxTx$	The longer of the time it takes to switch from receive to transmit or vice versa
NOTE Broadcast messages are not acknowledged.	

For validated messages, the destination device shall inspect the destination address in the DLPDU. Under normal conditions, the destination device acknowledges all messages addressed to it. The acknowledgement consists of the device switching from receive mode to transmit mode and beginning its ACK such that the Start of Message (SOM) occurs exactly $TsTxAckDelay$ after the end of the transmitted source device's packet.

Meanwhile the source device is turning around its transceiver by switching from transmit mode to receive mode. The source device shall enter receive mode and be listening for communication by $TsRxAckDelay$ after the end of its transmission. The source shall listen for the ACK's SOM for a duration $TsAckWait$.

For an acknowledged transaction, the packet is successfully forwarded only when both the source packet and the ACK packet have been successfully received by the destination and the source device respectively.

5.5.2.3 Un-Acknowledged (Broadcast) Transmissions

Broadcast transmissions are also supported. In these messages the DLPDU source address is specific and the destination address is the broadcast address. Broadcast messages are not acknowledged at the Data-Link level.

The source device shall begin its transmission such that the end of the Start of Message (SOM) occurs exactly $TsTxOffset$ after the start of the slot (as described in Acknowledged Transactions) whether a CCA is performed or not.

The destination device shall enter receive mode and be listening for communication by $TsRxOffset$ from the start of the slot. The destination shall listen for the SOM for a duration $TsTxWait$. If the destination device detects the SOM then it shall receive and validate the message.

A message containing the broadcast destination address is never acknowledged and, consequently, this completes the transaction and the communications in the slot.

5.5.3 Communication Tables and Buffers

5.5.3.1 General

All devices maintain a series of tables that control the communications performed by the device and collect statistics on those communications. In addition, packets are buffered as messages are received, processed and forwarded.

The tables controlling communication activities include the following:

- Superframe and Link tables. Multiple superframes may be configured by the network manager. Multiple links within a superframe are configured to specify communication with a specific neighbor or broadcast communications to all listening to the link.
- The Neighbor table. The neighbor table is a list of all devices that the device may be able to communicate with.
- The Graph table. Graphs are used to route messages from their source to their destination. The device does not know the entire route rather, the graph indicates the next hop destinations legal for propagating the packet onward toward its destination.

In addition to these tables, there is a packet queue that buffers messages (see 5.5.3.6). Devices shall support the minimum number of table entries shown in Table 4.

The communication tables and the relationships between them are shown in Figure 12. Within the device, the neighbor table is central. This table contains a list of all devices that have been identified by the device.

NOTE Although specific implementation of data and configuration storage is left up to the designers of the WirelessHART devices, general description of the fields contained in the data structures is important to overall understanding. Some fields described in the tables in 5.5.3 may be calculated or derived from other information, and do not necessarily occupy space on the device.

A graph may specify more than one neighbor any of which may be used for the next hop for packets following the route designated by the Graph ID. In other words, when forwarding a packet using graph routing, the device can propagate it to any of the neighbors associated with that packet's Graph ID. For more information see 5.5.4.

The device maintains network time synchronization and tracks the absolute slot number. These slots are organized into superframes. All communications are scheduled to occur within a superframe during specific slots in that superframe. All devices shall support multiple superframes.

Each superframe has one or more links. The links specify the slot and associated information required to forward or accept a packet.

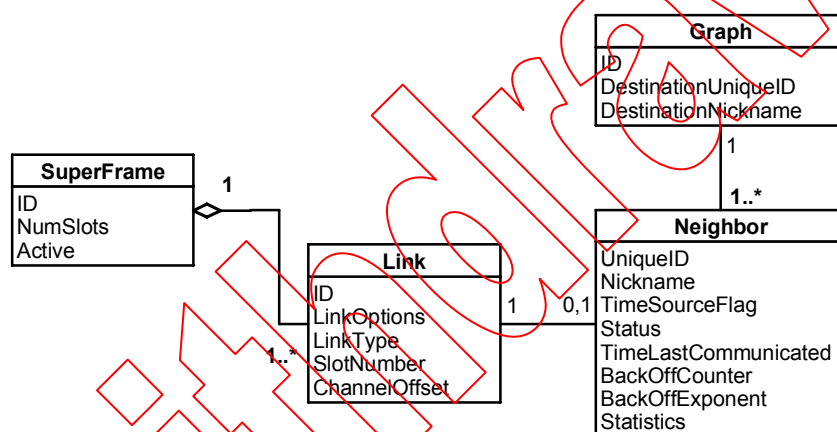


Figure 12 – Data-Link Table Relationships

Each link defines a communications opportunity. A link can belong to one and only one superframe. Links specify a neighbor that is the partner in any communication using the link. A link is either directed to a neighbor or is a broadcast link. For a link, packets are either propagated to or from the neighbor. Broadcast links always propagate packets from the device.

In many cases the information in these tables is shared between the Network and Data-Link Layers (see Clause 5 for more information). Subclause 5.5 describes each of the Data-Link tables and buffers in more detail.

Table 4 – Minimum Table and Buffer Space Requirement

Description	Minimum Number Required
Neighbors	32
Superframes	16
Total Number of Links	64
Graphs	32
Total Number of Graph-Neighbor Connections	128
Packet Buffers	16

5.5.3.2 Superframes

Each device shall support multiple superframes. Superframes are created and maintained by the Network Manager. Superframes consist of a fixed number of slots (see Table 5), initially contain no links and begin as disabled.

Once a superframe is created, the Network Manager adds, deletes and modifies links within the superframe, thus identifying opportunities for device to device communications. Once configured with links, the superframe can be enabled to allow the link scheduler to begin identifying transmit and receive slots.

Table 5 – Superframe Properties

Content	Description
Unsigned-8 SuperframeId	Unique identifier of the superframe. This is supplied by the network manager
Unsigned-16 NumSlots	Number of slots in the superframe (size of superframe)
Bits-1 ActiveFlag	Flag indicating if the superframe is currently activated
Links []	List of links in this superframe

5.5.3.3 Links

5.5.3.3.1 General

Links are allocated to a superframe by the Network Manager. The link includes a reference to a neighbor that is permitted to communicate with the device. This reference can be to a single neighbor or the link can be a broadcast to (an unspecified) group of neighbors. Furthermore, the slot number within the superframe, direction of the communication (transmit/receive), link characteristics (e.g., shared/dedicated), and the initial communication channel are specified.

When the Network Manager designates a link as being shared, contention-based, multiple-sender access is performed within the corresponding link. For these links, messages that are not acknowledged result in a random back-off algorithm being applied (see 5.5.4.4).

Table 6 – Link Properties

Content	Description
LinkId	Unique identifier of the Link
Ref NeighborId	Reference to a Neighbor table entry
Enum-3 LinkType	Indicates the type of link: { normal , broadcast , join , discovery }
Bits-1 TxLink	When set, indicates the link may be used for transmit
Bits-1 RxLink	When set, indicates the link may be used for receive
Bits-1 SharedLink	When set, indicates the link is shared by multiple devices
Unsigned-16 Slot	Slot number in superframe
Unsigned-6 ChannelOffset	Frequency hopping channel offset

NOTE The Network Manager shall not delete or suspend any join links while there are outstanding received join requests.

5.5.3.3.2 Link Channel Calculation

The link also specifies the ChannelOffset and thus implicitly the channel hop order. For a given link and absolute slot, the actual channel used is determined by dividing the sum of the ChannelOffset and absolute slot number by the number of channels currently active. The remainder of this operation indexes the channel table to obtain the actual channel used for communication in the active slot. The channel table contents and length is Physical Layer