

BS EN 61158-4-2:2014



BSI Standards Publication

Industrial communication networks — Fieldbus specifications

Part 4-2: Data-link layer protocol specification — Type 2 elements

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This British Standard is the UK implementation of EN 61158-4-2:2014. It is identical to IEC 61158-4-2:2014. It supersedes BS EN 61158-4-2:2012 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee AMT/7, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014.

Published by BSI Standards Limited 2014

ISBN 978 0 580 79440 7

ICS 25.040.40; 35.100.20; 35.110

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2014.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English Version

**Industrial communication networks - Fieldbus specifications -Part
4-2: Data-link layer protocol specification - Type 2 elements
(IEC 61158-4-2:2014)**

Réseaux de communication industriels - Spécifications des
bus de terrain - Partie 4-2: Spécification du protocole de la
couche liaison de données - Eléments de type 2
(CEI 61158-4-2:2014)

Industrielle Kommunikationsnetze - Feldbusse - Teil 4-2:
Protokollspezifikation des Data Link Layer
(Sicherheitsschicht) - Typ 2-Elemente
(IEC 61158-4-2:2014)

This European Standard was approved by CENELEC on 2014-09-19. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

The text of document 65C/762/FDIS, future edition 3 of IEC 61158-4-2, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61158-4-2:2014.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2015-06-19
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2017-09-19

This document supersedes EN 61158-4-2:2012.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Endorsement notice

The text of the International Standard IEC 61158-4-2:2014 was approved by CENELEC as a European Standard without any modification.

In the official version, for bibliography, the following notes have to be added for the standards indicated:

IEC 61158-1:2014	NOTE	Harmonised as EN 61158-1:2014
IEC 61158-2:2014	NOTE	Harmonised as EN 61158-2:2014
IEC 61784-1:2014	NOTE	Harmonised as EN 61784-1:2014
IEC 61784-2:2014	NOTE	Harmonised as EN 61784-2:2014

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 61131-3	-	Programmable controllers - Part 3: Programming languages	EN 61131-3	-
IEC 61158-3-2	2014	Industrial communication networks - Fieldbus specifications - Part 3-2: Data-link layer service definition - Type 2 elements	EN 61158-3-2	2014
IEC 61158-5-2	2014	Industrial communication networks - Fieldbus specifications -- Part 5-2: Application layer service definition - Type 2 elements	EN 61158-5-2	2014
IEC 61158-6-2	2014	Industrial communication networks - Fieldbus specifications - Part 6-2: Application layer protocol specification - Type 2 elements	EN 61158-6-2	2014
IEC 61588	2009	Precision clock synchronization protocol for - networked measurement and control systems	-	-
IEC 61784-3-2	-	Industrial communication networks - Profiles Part 3-2: Functional safety fieldbuses - Additional specifications for CPF 2	EN 61784-3-2	-
IEC 62026-3	2008	Low-voltage switchgear and controlgear - Controller-device interfaces (CDIs) Part 3: DeviceNet	EN 62026-3	2009
ISO 11898	1993 ¹	Road vehicles - Interchange of digital information - Controller area network (CAN) for high-speed communication	-	-
ISO/IEC 3309	-	Information technology - Telecommunications and information exchange between systems - High-level data link control (HDLC) procedures - Frame structure	-	-
ISO/IEC 7498-1	-	Information technology - Open Systems Interconnection - Basic reference model: The basic model	-	-

¹ Superseded by ISO 11898-1:2003 and ISO 11898-8:2003

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
ISO/IEC 7498-3	-	Information technology - Open Systems Interconnection - Basic reference model: Naming and addressing	-	-
ISO/IEC 8802-3	-	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications	-	-
IEEE 802.1D	2004	IEEE Standard for local and metropolitan area networks - Media Access Control (MAC) Bridges	-	-
IEEE 802.1Q	2005 ²⁾	IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks	-	-
IEEE 802.3	2008	IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications	-	-

²⁾ Superseded by IEEE 802.1Q:2011

CONTENTS

INTRODUCTION.....	13
1 Scope.....	15
1.1 General.....	15
1.2 Specifications.....	15
1.3 Procedures.....	15
1.4 Applicability.....	16
1.5 Conformance.....	16
2 Normative references	16
3 Terms, definitions, symbols, abbreviations and conventions	17
3.1 Reference model terms and definitions.....	17
3.2 Service convention terms and definitions.....	19
3.3 Common terms and definitions	20
3.4 Additional Type 2 definitions.....	22
3.5 Type 2 symbols and abbreviations.....	30
3.6 Conventions for station management objects	31
4 Overview of the data-link protocol.....	31
4.1 General.....	31
4.2 Services provided by the DL.....	34
4.3 Structure and definition of DL-addresses	35
4.4 Services assumed from the PhL	37
4.5 Functional classes.....	39
5 General structure and encoding of PhIDUs and DLPDUs and related elements of procedure	40
5.1 Overview	40
5.2 Media access procedure.....	40
5.3 DLPDU structure and encoding	44
5.4 Lpacket components	48
5.5 DLPDU procedures	50
5.6 Summary of DLL support services and objects	51
6 Specific DLPDU structure, encoding and procedures.....	53
6.1 Modeling language	53
6.2 DLS user services	55
6.3 Generic tag Lpacket	61
6.4 Moderator Lpacket	62
6.5 Time distribution Lpacket	63
6.6 UCMM Lpacket.....	66
6.7 Keeper UCMM Lpacket.....	66
6.8 TUI Lpacket.....	67
6.9 Link parameters Lpacket and tMinus Lpacket	68
6.10 I'm-alive Lpacket	70
6.11 Ping Lpackets.....	71
6.12 WAMI Lpacket.....	73
6.13 Debug Lpacket	73
6.14 IP Lpacket	74
6.15 Ethernet Lpacket	74

7	Objects for station management	74
7.1	General	74
7.2	ControlNet object	76
7.3	Keeper object	86
7.4	Scheduling object	108
7.5	TCP/IP Interface object	119
7.6	Ethernet link object	139
7.7	DeviceNet object	149
7.8	Connection configuration object (CCO)	157
7.9	DLR object	180
7.10	QoS object	195
7.11	Port object	198
8	Other DLE elements of procedure	201
8.1	Network attachment monitor (NAM)	201
8.2	Calculating link parameters	209
9	Detailed specification of DL components	218
9.1	General	218
9.2	Access control machine (ACM)	218
9.3	TxLLC	238
9.4	RxLLC	243
9.5	Transmit machine (TxM)	247
9.6	Receive machine (RxM)	251
9.7	Serializer	257
9.8	Deserializer	260
9.9	DLL management	260
10	Device Level Ring (DLR) protocol	262
10.1	General	262
10.2	Supported topologies	263
10.3	Overview of DLR operation	264
10.4	Classes of DLR implementation	267
10.5	DLR behavior	268
10.6	Implementation requirements	273
10.7	Using non-DLR nodes in the ring network	275
10.8	Redundant gateway devices on DLR network	278
10.9	DLR messages	283
10.10	State diagrams and state-event-action matrices	289
10.11	Performance analysis	316
	Annex A (normative) Indicators and switches	322
A.1	Purpose	322
A.2	Indicators	322
A.2.1	General indicator requirements	322
A.2.2	Common indicator requirements	322
A.2.3	Fieldbus specific indicator requirements (1)	324
A.2.4	Fieldbus specific indicator requirements (2)	328
A.2.5	Fieldbus specific indicator requirements (3)	331
A.3	Switches	335
A.3.1	Common switch requirements	335
A.3.2	Fieldbus specific switch requirements (1)	

A.3.3	Fieldbus specific switch requirements (2)	336
A.3.4	Fieldbus specific switch requirements (3)	337
	Bibliography	338
Figure 1	– Relationships of DLSAPs, DLSAP-addresses and group DL-addresses	21
Figure 2	– Data-link layer internal architecture	33
Figure 3	– Basic structure of a MAC ID address	35
Figure 4	– Basic structure of a generic tag address	35
Figure 5	– Basic structure of a fixed tag address	36
Figure 6	– M_symbols and Manchester encoding at 5 MHz	38
Figure 7	– NUT structure	41
Figure 8	– Media access during scheduled time	42
Figure 9	– Media access during unscheduled time	43
Figure 10	– DLPDU format	44
Figure 11	– Aborting a DLPDU during transmission	48
Figure 12	– Lpacket format	48
Figure 13	– Generic tag Lpacket format	49
Figure 14	– Fixed tag Lpacket format	50
Figure 15	– Goodness parameter of TimeDist_Lpacket	64
Figure 16	– Example I'm alive processing algorithm	71
Figure 17	– Keeper CRC algorithm	92
Figure 18	– Keeper object power-up state diagram	103
Figure 19	– Keeper object operating state diagram	105
Figure 20	– Synchronized network change processing	108
Figure 21	– State transition diagram for TCP/IP Interface object	132
Figure 22	– State transition diagram for TCP/IP Interface object (continued)	133
Figure 23	– ACD Behavior	135
Figure 24	– State transition diagram for Ethernet Link object	149
Figure 25	– Connection configuration object edit flowchart	180
Figure 26	– NAM state machine	202
Figure 27	– DLR rings connected to switches	264
Figure 28	– Normal operation of a DLR network	265
Figure 29	– Beacon and Announce frames	265
Figure 30	– Link failure	266
Figure 31	– Network reconfiguration after link failure	267
Figure 32	– Neighbor Check process	273
Figure 33	– Unsupported topology – example 1	277
Figure 34	– Unsupported topology – example 2	277
Figure 35	– DLR ring connected to switches through redundant gateways	279
Figure 36	– DLR redundant gateway capable device	280
Figure 37	– Advertise frame	282
Figure 38	– State transition diagram for Beacon frame based non-supervisor ring node	290
Figure 39	– State transition diagram for Announce frame based non-supervisor ring node	293

Figure 40 – State transition diagram for ring supervisor	299
Figure 41 – State transition diagram for redundant gateway	312
Figure A.1 – Non redundant network status indicator labeling	328
Figure A.2 – Redundant network status indicator labeling	328
Figure A.3 – Network status indicator state diagram	331
Table 1 – Format of attribute tables	31
Table 2 – Data-link layer components	32
Table 3 – MAC ID addresses allocation	35
Table 4 – Fixed tag service definitions	36
Table 5 – Data encoding rules	37
Table 6 – M Data symbols	39
Table 7 – Truth table for ph_status_indication	39
Table 8 – FCS length, polynomials and constants	45
Table 9 – DLL support services and objects	52
Table 10 – Elementary data types	55
Table 11 – DLL events	59
Table 12 – Time distribution priority	65
Table 13 – Format of the TUI Lpacket	67
Table 14 – ControlNet object class attributes	76
Table 15 – ControlNet object instance attributes	76
Table 16 – TUI status flag bits	80
Table 17 – Mac_ver bits	81
Table 18 – Channel state bits	82
Table 19 – ControlNet object common services	83
Table 20 – ControlNet object class specific services	84
Table 21 – Keeper object revision history	86
Table 22 – Keeper object class attributes	87
Table 23 – Keeper object instance attributes	87
Table 24 – Keeper operating state definitions	90
Table 25 – Port status flag bit definitions	90
Table 26 – TUI status flag bits	91
Table 27 – Keeper attributes	94
Table 28 – Memory requirements (in octets) for the Keeper attributes	94
Table 29 – Keeper object common services	95
Table 30 – Keeper object class specific services	95
Table 31 – Service error codes	96
Table 32 – Wire order format of the TUI Lpacket	100
Table 33 – Service error codes	101
Table 34 – Keeper object operating states	101
Table 35 – Keeper object state event matrix	105
Table 36 – Scheduling object class attributes	109
Table 37 – Scheduling object instance attributes	109

Table 38 – Scheduling object common services	110
Table 39 – Status error descriptions for Create	111
Table 40 – Status error descriptions for Delete and Kick_Timer	112
Table 41 – Scheduling object class specific services	112
Table 42 – Status error descriptions for Read	114
Table 43 – Status error descriptions for Conditional_Write	115
Table 44 – Status error descriptions for Forced_Write	115
Table 45 – Status error descriptions for Change_Start	116
Table 46 – Status error descriptions for Break_Connections	116
Table 47 – Status error descriptions for Change_Complete	117
Table 48 – Status error descriptions for Restart_Connections	118
Table 49 – Revision history	119
Table 50 – TCP/IP Interface object class attributes	120
Table 51 – TCP/IP Interface object instance attributes	120
Table 52 – Status bits	123
Table 53 – Configuration capability bits	124
Table 54 – Configuration control bits	124
Table 55 – Example path	125
Table 56 – Interface configuration components	126
Table 57 – Alloc control values	128
Table 58 – AcdActivity values	129
Table 59 – ArpPdu - ARP Response PDU in binary format	129
Table 60 – TCP/IP Interface object common services	130
Table 61 – Get_Attribute_All reply format	130
Table 62 – Ethernet link object revision history	139
Table 63 – Ethernet link object class attributes	140
Table 64 – Ethernet link object instance attributes	140
Table 65 – Interface flags bits	143
Table 66 – Control bits	145
Table 67 – Interface type	145
Table 68 – Interface state	146
Table 69 – Admin state	146
Table 70 – Ethernet Link object common services	146
Table 71 – Get_Attribute_All reply format	147
Table 72 – Ethernet Link object class specific services	148
Table 73 – DeviceNet object revision history	150
Table 74 – DeviceNet object class attributes	150
Table 75 – DeviceNet object instance attributes	150
Table 76 – Bit rate attribute values	152
Table 77 – BOI attribute values	153
Table 78 – Diagnostic counters bit description	155
Table 79 – DeviceNet object common services	156
Table 80 – Reset service parameter	156

Table 81 – Reset service parameter values	156
Table 82 – DeviceNet object class specific services.....	157
Table 83 – Connection configuration object revision history	158
Table 84 – Connection configuration object class attributes	158
Table 85 – Format number values	159
Table 86 – Connection configuration object instance attributes	160
Table 87 – Originator connection status values	164
Table 88 – Target connection status values	164
Table 89 – Connection flags	165
Table 90 – I/O mapping formats	167
Table 91 – Services valid during a change operation	169
Table 92 – Connection configuration object common services.....	169
Table 93 – Get_Attribute_All Response – class level	170
Table 94 – Get_Attribute_All response – instance level.....	170
Table 95 – Set_Attribute_All error codes.....	172
Table 96 – Set_Attribute_All request.....	172
Table 97 – Create request parameters	174
Table 98 – Create error codes	174
Table 99 – Delete error codes.....	175
Table 100 – Restore error codes.....	175
Table 101 – Connection configuration object class specific services	175
Table 102 – Change_Start error codes	177
Table 103 – Get_Status service parameter	177
Table 104 – Get_Status service response	177
Table 105 – Get_Status service error codes	178
Table 106 – Change_Complete service parameter	178
Table 107 – Change_Complete service error codes	178
Table 108 – Audit_Changes service parameter	179
Table 109 – Audit_Changes service error codes	179
Table 110 – Revision history	181
Table 111 – DLR object class attributes	181
Table 112 – DLR object instance attributes	181
Table 113 – Network Status values	185
Table 114 – Ring Supervisor Status values	185
Table 115 – Capability flags.....	188
Table 116 – Redundant Gateway Status values	190
Table 117 – DLR object common services	191
Table 118 – Get_Attribute_All Response – Object Revision 1, non supervisor device	191
Table 119 – Get_Attribute_All Response – Object Revision 1, supervisor-capable device.....	192
Table 120 – Get_Attribute_All Response – Object Revision 2, non supervisor device	192
Table 121 – Get_Attribute_All Response – All other cases.....	193
Table 122 – DLR object class specific services.....	194

Table 123 – QoS object revision history	195
Table 124 – QoS object class attributes	195
Table 125 – QoS object instance attributes	196
Table 126 – Default DCSP values and usages	197
Table 127 – QoS object common services	197
Table 128 – Port object class attributes	198
Table 129 – Port object instance attributes	199
Table 130 – Port object common services	201
Table 131 – NAM states	201
Table 132 – Default link parameters	202
Table 133 – PhL timing characteristics	210
Table 134 – DLR variables	268
Table 135 – Redundant gateway variables	281
Table 136 – MAC addresses for DLR messages	283
Table 137 – IEEE 802.1Q common frame header format	284
Table 138 – DLR message payload fields	284
Table 139 – DLR frame types	284
Table 140 – Format of the Beacon frame	285
Table 141 – Ring State values	285
Table 142 – Format of the Neighbor_Check request	286
Table 143 – Format of the Neighbor_Check response	286
Table 144 – Format of the Link_Status/Neighbor_Status frame	286
Table 145 – Link/Neighbor status values	287
Table 146 – Format of the Locate_Fault frame	287
Table 147 – Format of the Announce frame	287
Table 148 – Format of the Sign_On frame	288
Table 149 – Format of the Advertise frame	288
Table 150 – Gateway state values	288
Table 151 – Format of the Flush_Tables frame	289
Table 152 – Format of the Learning_Update frame	289
Table 153 – Parameter values for Beacon frame based non-supervisor ring node	290
Table 154 – LastBcnRcvPort bit definitions	291
Table 155 – State-event-action matrix for Beacon frame based non-supervisor ring node	291
Table 156 – Parameter values for Announce frame based non-supervisor ring node	295
Table 157 – State-event-action matrix for Announce frame based non-supervisor ring node	296
Table 158 – Parameter values for ring supervisor node	299
Table 159 – LastBcnRcvPort bit definitions	300
Table 160 – State-event-action matrix for ring supervisor node	301
Table 161 – Parameter values for redundant gateway node	313
Table 162 – State-event-action matrix for redundant gateway node	314
Table 163 – Parameters/assumptions for example performance calculations	316
Table 164 – Example ring configuration parameters and performance	319

Table 165 – Variables for performance analysis	320
Table A.1 – Module status indicator	323
Table A.2 – Time Sync status indication	324
Table A.3 – Network status indicators	326
Table A.4 – Network status indicator	330
Table A.5 – Network status indicator	333
Table A.6 – Combined module/network status indicator	334
Table A.7 – I/O status indicator	335
Table A.8 – Bit rate switch encoding	337

INTRODUCTION

This part of IEC 61158 is one of a series produced to facilitate the interconnection of automation system components. It is related to other standards in the set as defined by the “three-layer” fieldbus reference model described in IEC 61158-1.

The data-link protocol provides the data-link service by making use of the services available from the physical layer. The primary aim of this standard is to provide a set of rules for communication expressed in terms of the procedures to be carried out by peer data-link entities (DLEs) at the time of communication. These rules for communication are intended to provide a sound basis for development in order to serve a variety of purposes:

- a) as a guide for implementers and designers;
- b) for use in the testing and procurement of equipment;
- c) as part of an agreement for the admittance of systems into the open systems environment;
- d) as a refinement to the understanding of time-critical communications within OSI.

This standard is concerned, in particular, with the communication and interworking of sensors, effectors and other automation devices. By using this standard together with other standards positioned within the OSI or fieldbus reference models, otherwise incompatible systems may work together in any combination.

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of patents given in several subclauses as indicated in the table below. These patents are held by their respective inventors under license to ODVA, Inc:

US 5,400,331	[ODVA]	Communication network interface with screeners for incoming messages	Subclause 3.4, Clauses 4 to 9
US 5,471,461	[ODVA]	Digital communication network with a moderator station election process	
US 5,491,531	[ODVA]	Media access controller with a shared class message delivery capability	
US 5,493,571	[ODVA]	Apparatus and method for digital communications with improved delimiter detection	
US 5,537,549	[ODVA]	Communication network with time coordinated station activity by time slot and periodic interval number	
US 5,553,095	[ODVA]	Method and apparatus for exchanging different classes of data during different time intervals	Clause 10
US 8,244,838	[ODVA]	Industrial controller employing the network ring topology	

IEC takes no position concerning the evidence, validity and scope of these patent rights.

ODVA and the holders of these patent rights have assured the IEC that ODVA is willing to negotiate licences either free of charge or under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of ODVA and the holders of these patent rights is registered with IEC. Information may be obtained from:

[ODVA] ODVA, Inc.
2370 East Stadium Boulevard #1000
Ann Arbor, Michigan 48104
USA
Attention: Office of the Executive Director
e-mail: odva@odva.org

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those identified above. IEC shall not be held responsible for identifying any or all such patent rights.

ISO (www.iso.org/patents) and IEC (<http://patents.iec.ch>) maintain on-line databases of patents relevant to their standards. Users are encouraged to consult the databases for the most up to date information concerning patents.

INDUSTRIAL COMMUNICATION NETWORKS – FIELDBUS SPECIFICATIONS –

Part 4-2: Data-link layer protocol specification – Type 2 elements

1 Scope

1.1 General

The data-link layer provides basic time-critical messaging communications between devices in an automation environment.

This protocol provides communication opportunities to all participating data-link entities, sequentially and in a cyclic synchronous manner. Foreground scheduled access is available for time-critical activities together with background unscheduled access for less critical activities.

Deterministic and synchronized transfers can be provided at cyclic intervals up to 1 ms and device separations of 25 km. This performance is adjustable dynamically and on-line by re-configuring the parameters of the local link whilst normal operation continues. By similar means, DL connections and new devices may be added or removed during normal operation.

This protocol provides means to maintain clock synchronization across an extended link with a precision better than 10 μ s.

This protocol optimizes each access opportunity by concatenating multiple DLSDUs and associated DLPCI into a single DLPDU, thereby improving data transfer efficiency for data-link entities that actively source multiple streams of data.

The maximum system size is an unlimited number of links of 99 nodes, each with 255 DLSAP-addresses. Each link has a maximum of 2^{24} related peer and publisher DLCEPs.

1.2 Specifications

This standard specifies

- a) procedures for the timely transfer of data and control information from one data-link user entity to a peer user entity, and among the data-link entities forming the distributed data-link service provider;
- b) the structure of the fieldbus DLPDUs used for the transfer of data and control information by the protocol of this standard, and their representation as physical interface data units.

1.3 Procedures

The procedures are defined in terms of

- a) the interactions between peer 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 time-critical 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 time-critical communications needs.

1.5 Conformance

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

2 Normative references

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

NOTE All parts of the IEC 61158 series, as well as IEC 61784-1 and IEC 61784-2 are maintained simultaneously. Cross-references to these documents within the text therefore refer to the editions as dated in this list of normative references.

IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

IEC 61158-3-2:2014, *Industrial communication networks – Fieldbus specifications – Part 3-2: Data-link layer service definition – Type 2 elements*

IEC 61158-5-2:2014, *Industrial communication networks – Fieldbus specifications – Part 5-2: Application layer service definition – Type 2 elements*

IEC 61158-6-2:2014, *Industrial communication networks – Fieldbus specifications – Part 6-2: Application layer protocol specification – Type 2 elements*

IEC 61588:2009, *Precision clock synchronization protocol for networked measurement and control systems*

IEC 61784-3-2, *Industrial communication networks – Profiles – Part 3-2: Functional safety fieldbuses – Additional specifications for CPF 2*

IEC 62026-3:2008, *Low-voltage switchgear and controlgear – Controller-device interfaces (CDIs) – Part 3: DeviceNet*

ISO/IEC 3309¹, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures – Frame structure*

ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ISO/IEC 7498-3, *Information technology – Open Systems Interconnection – Basic Reference Model: Naming and addressing*

¹ This standard has been withdrawn.

ISO/IEC 8802-3, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

ISO 11898:1993², *Road vehicles – Interchange of digital information – Controller area network (CAN) for high-speed communication*

IEEE 802.1D-2004, *IEEE standard for local and metropolitan area networks – Media Access Control (MAC) bridges*, available at <<http://www.ieee.org>>

IEEE 802.1Q-2005², *IEEE standard for local and metropolitan area networks – Virtual bridged local area networks*, available at <<http://www.ieee.org>>

IEEE 802.3-2008, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*, available at <<http://www.ieee.org>>

IETF RFC 951, *Bootstrap Protocol (BOOTP)*, available at <<http://www.ietf.org>>

IETF RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*, available at <<http://www.ietf.org>>

IETF RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*, available at <<http://www.ietf.org>>

IETF RFC 1643, *Definitions of Managed Objects for the Ethernet-like Interface Types*, available at <<http://www.ietf.org>>

IETF RFC 2131, *Dynamic Host Configuration Protocol*, available at <<http://www.ietf.org>>

IETF RFC 2132, *DHCP Options and BOOTP Vendor Extensions*, available at <<http://www.ietf.org>>

IETF RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*, available at <<http://www.ietf.org>>

IETF RFC 5227:2008, *IPv4 Address Conflict Detection*, available at <<http://www.ietf.org>>

3 Terms, definitions, symbols, abbreviations and conventions

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

3.1 Reference model terms and definitions

This standard is based in part on the concepts developed in ISO/IEC 7498-1 and ISO/IEC 7498-3, and makes use of the following terms defined therein.

3.1.1 called-DL-address [ISO/IEC 7498-3]

3.1.2 calling-DL-address [ISO/IEC 7498-3]

² A newer edition of this standard has been published, but only the cited edition applies.

3.1.3	centralized multi-end-point-connection	[ISO/IEC 7498-1]
3.1.4	correspondent (N)-entities correspondent DL-entities (N=2) correspondent Ph-entities (N=1)	[ISO/IEC 7498-1]
3.1.5	demultiplexing	[ISO/IEC 7498-1]
3.1.6	DL-address	[ISO/IEC 7498-3]
3.1.7	DL-address-mapping	[ISO/IEC 7498-1]
3.1.8	DL-connection	[ISO/IEC 7498-1]
3.1.9	DL-connection-end-point	[ISO/IEC 7498-1]
3.1.10	DL-connection-end-point-identifier	[ISO/IEC 7498-1]
3.1.11	DL-connection-mode transmission	[ISO/IEC 7498-1]
3.1.12	DL-connectionless-mode transmission	[ISO/IEC 7498-1]
3.1.13	DL-data-sink	[ISO/IEC 7498-1]
3.1.14	DL-data-source	[ISO/IEC 7498-1]
3.1.15	DL-duplex-transmission	[ISO/IEC 7498-1]
3.1.16	DL-facility	[ISO/IEC 7498-1]
3.1.17	DL-local-view	[ISO/IEC 7498-3]
3.1.18	DL-name	[ISO/IEC 7498-3]
3.1.19	DL-protocol	[ISO/IEC 7498-1]
3.1.20	DL-protocol-connection-identifier	[ISO/IEC 7498-1]
3.1.21	DL-protocol-control-information	[ISO/IEC 7498-1]
3.1.22	DL-protocol-data-unit	[ISO/IEC 7498-1]
3.1.23	DL-protocol-version-identifier	[ISO/IEC 7498-1]
3.1.24	DL-relay	[ISO/IEC 7498-1]
3.1.25	DL-service-connection-identifier	[ISO/IEC 7498-1]
3.1.26	DL-service-data-unit	[ISO/IEC 7498-1]
3.1.27	DL-simplex-transmission	[ISO/IEC 7498-1]
3.1.28	DL-subsystem	[ISO/IEC 7498-1]
3.1.29	DL-user-data	[ISO/IEC 7498-1]
3.1.30	flow control	[ISO/IEC 7498-1]
3.1.31	layer-management	[ISO/IEC 7498-1]
3.1.32	multiplexing	[ISO/IEC 7498-3]
3.1.33	naming-(addressing)-authority	[ISO/IEC 7498-3]
3.1.34	naming-(addressing)-domain	[ISO/IEC 7498-3]

3.1.35	naming-(addressing)-subdomain	[ISO/IEC 7498-3]
3.1.36	(N)-entity DL-entity Ph-entity	[ISO/IEC 7498-1]
3.1.37	(N)-interface-data-unit DL-service-data-unit (N=2) Ph-interface-data-unit (N=1)	[ISO/IEC 7498-1]
3.1.38	(N)-layer DL-layer (N=2) Ph-layer (N=1)	[ISO/IEC 7498-1]
3.1.39	(N)-service DL-service (N=2) Ph-service (N=1)	[ISO/IEC 7498-1]
3.1.40	(N)-service-access-point DL-service-access-point (N=2) Ph-service-access-point (N=1)	[ISO/IEC 7498-1]
3.1.41	(N)-service-access-point-address DL-service-access-point-address (N=2) Ph-service-access-point-address (N=1)	[ISO/IEC 7498-1]
3.1.42	peer-entities	[ISO/IEC 7498-1]
3.1.43	Ph-interface-control-information	[ISO/IEC 7498-1]
3.1.44	Ph-interface-data	[ISO/IEC 7498-1]
3.1.45	primitive name	[ISO/IEC 7498-3]
3.1.46	reassembling	[ISO/IEC 7498-1]
3.1.47	recombining	[ISO/IEC 7498-1]
3.1.48	reset	[ISO/IEC 7498-1]
3.1.49	responding-DL-address	[ISO/IEC 7498-3]
3.1.50	routing	[ISO/IEC 7498-1]
3.1.51	segmenting	[ISO/IEC 7498-1]
3.1.52	sequencing	[ISO/IEC 7498-1]
3.1.53	splitting	[ISO/IEC 7498-1]
3.1.54	synonymous name	[ISO/IEC 7498-3]
3.1.55	systems-management	[ISO/IEC 7498-1]

3.2 Service convention terms and definitions

This standard also makes use of the following terms defined in ISO/IEC 10731 as they apply to the data-link layer:

- 3.2.1 acceptor**
- 3.2.2 asymmetrical service**
- 3.2.3 confirm (primitive);**

requestor.deliver (primitive)

- 3.2.4 deliver (primitive)**
- 3.2.5 DL-confirmed-facility**
- 3.2.6 DL-facility**
- 3.2.7 DL-local-view**
- 3.2.8 DL-mandatory-facility**
- 3.2.9 DL-non-confirmed-facility**
- 3.2.10 DL-provider-initiated-facility**
- 3.2.11 DL-provider-optional-facility**
- 3.2.12 DL-service-primitive;
primitive**
- 3.2.13 DL-service-provider**
- 3.2.14 DL-service-user**
- 3.2.15 DL-user-optional-facility**
- 3.2.16 indication (primitive)
acceptor.deliver (primitive)**
- 3.2.17 multi-peer**
- 3.2.18 request (primitive);
requestor.submit (primitive)**
- 3.2.19 requestor**
- 3.2.20 response (primitive);
acceptor.submit (primitive)**
- 3.2.21 submit (primitive)**
- 3.2.22 symmetrical service**

3.3 Common terms and definitions

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

NOTE Many definitions are common to more than one protocol Type; they are not necessarily used by all protocol Types.

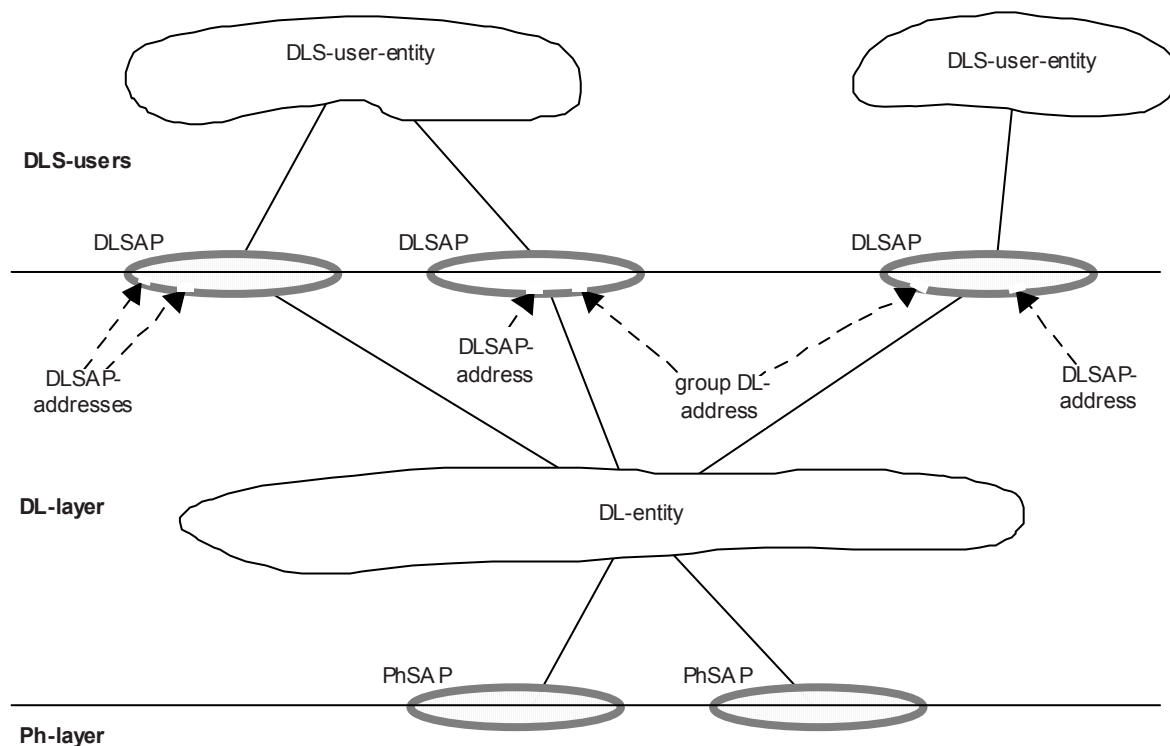
3.3.1

DL-segment

link

local link

single DL-subnetwork in which any of the connected DLEs may communicate directly, without any intervening DL-relaying, whenever all of those DLEs that are participating in an instance of communication are simultaneously attentive to the DL-subnetwork during the period(s) of attempted communication



NOTE 1 DLSAPs and PhSAPs are depicted as ovals spanning the boundary between two adjacent layers.

NOTE 2 DL-addresses are depicted as designating small gaps (points of access) in the DLL portion of a DLSAP.

NOTE 3 A single DL-entity can have multiple DLSAP-addresses and group DL-addresses associated with a single DLSAP.

Figure 1 – Relationships of DLSAPs, DLSAP-addresses and group DL-addresses

3.3.2

DLSAP

distinctive point at which DL-services are provided by a single DL-entity to a single higher-layer entity

Note 1 to entry: This definition, derived from ISO/IEC 7498-1, is repeated here to facilitate understanding of the critical distinction between DLSAPs and their DL-addresses. (See Figure 1.).

3.3.3

DL(SAP)-address

either an individual DLSAP-address, designating a single DLSAP of a single DLS-user, or a group DL-address potentially designating multiple DLSAPs, each of a single DLS-user

Note 1 to entry: This terminology is chosen because ISO/IEC 7498-3 does not permit the use of the term DLSAP-address to designate more than a single DLSAP at a single DLS-user.

3.3.4

(individual) DLSAP-address

DL-address that designates only one DLSAP within the extended link

Note 1 to entry: A single DL-entity may have multiple DLSAP-addresses associated with a single DLSAP.

3.3.5**extended link**

DL-subnetwork, consisting of the maximal set of links interconnected by DL-relays, sharing a single DL-name (DL-address) space, in which any of the connected DL-entities may communicate, one with another, either directly or with the assistance of one or more of those intervening DL-relay entities

Note 1 to entry: An extended link may be composed of just a single link.

3.3.6**frame**

denigrated synonym for DLPDU

3.3.7**group DL-address**

DL-address that potentially designates more than one DLSAP within the extended link. A single DL-entity may have multiple group DL-addresses associated with a single DLSAP. A single DL-entity also may have a single group DL-address associated with more than one DLSAP

3.3.8**node**

single DL-entity as it appears on one local link

3.3.9**receiving DLS-user**

DL-service user that acts as a recipient of DL-user-data

Note 1 to entry: A DL-service user can be concurrently both a sending and receiving DLS-user.

3.3.10**sending DLS-user**

DL-service user that acts as a source of DL-user-data

3.4 Additional Type 2 definitions**3.4.1****actual packet interval****API**

measure of how frequently a specific connection produces its Lpacket data

3.4.2**allocate**

take a resource from a common area and assign that resource for the exclusive use of a specific entity

3.4.3**application**

function or data structure for which data is consumed or produced

3.4.4**application objects**

multiple object classes that manage and provide the run time exchange of messages across the network and within the device

3.4.5**attribute**

description of an externally visible characteristic or feature of an object

Note 1 to entry: The attributes of an object contain information about variable portions of an object. Typically, they provide status information or govern the operation of an object. Attributes may also affect the behavior of an object. Attributes are divided into class attributes and instance attributes.

3.4.6**behavior**

indication of how the object responds to particular events

Note 1 to entry: Its description includes the relationship between attribute values and services.

3.4.7**bit**

unit of information consisting of a 1 or a 0

Note 1 to entry: This is the smallest data unit that can be transmitted.

3.4.8**blanking or blanking time**

length of time required after transmitting before the node is allowed to receive

3.4.9**client**

- 1) An object which uses the services of another (server) object to perform a task
- 2) An initiator of a message to which a server reacts

3.4.10**communication objects**

components that manage and provide run time exchange of messages across the network such as the ControlNet object, the Unconnected Message Manager (UCMM)

3.4.11**connection**

logical binding between two application objects within the same or different devices

3.4.12**connection ID****CID**

identifier assigned to a transmission, associated with a particular connection between producers and consumers, that identifies a specific piece of application information

Note 1 to entry: Within the data link this is a generic tag.

3.4.13**cyclic redundancy check****CRC**

residual value computed from an array of data and used as a representative signature for the array

3.4.14**cyclic**

term used to describe events which repeat in a regular and repetitive manner

3.4.15**deafness**

situation where the node can not hear the moderator DLPDU but can hear other link traffic

3.4.16**device**

physical hardware connection to the link

Note 1 to entry: A device may contain more than one node.

3.4.17**DLPDU**

data-link protocol data unit

Note 1 to entry: A DLPDU consists of a source MAC ID, zero or more Lpackets and an FCS as transmitted or received by an associated PhE.

3.4.18**end delimiter**

unique set of M_symbols that identifies the end of a DLPDU

3.4.19**error**

discrepancy between a computed, observed or measured value or condition and the specified or theoretically correct value or condition

3.4.20**extended link**

links connected by DL-routers (sometimes called a local area network)

3.4.21**FCS error**

error that occurs when the computed frame check sequence value after reception of all the octets in a DLPDU does not match the expected residual

3.4.22**fixed tag**

two octet identifier (tag) which identifies a specific service to be performed by either

- a) that receiving node on the local link which has a specified MAC ID, or
- b) all receiving nodes on the local link

Note 1 to entry: Identification of the target node(s) is included in the two octet tag.

3.4.23**frame**

denigrated synonym for DLPDU

3.4.24**Frame Check Sequence****FCS**

redundant data derived from a block of data within a DLPDU (frame), using a hash function, and stored or transmitted together with the block of data, in order to detect data corruption

3.4.25**generic tag**

three octet identifier (tag) which identifies a specific piece of application information

3.4.26**guardband**

time slot allocated for the transmission of the moderator DLPDU

3.4.27**implicit token**

mechanism that governs the right to transmit

Note 1 to entry: No actual token message is transmitted on the medium. Each node keeps track of the MAC ID of the node that it believes currently holds the right to transmit. The right to transmit is passed from node to node by keeping a record of the node that last transmitted. A slot time is used to allow a missing node to be skipped in the rotation

3.4.28**implicit token register**

register that contains the MAC ID of the node that holds the right to transmit

3.4.29**instance**

actual physical occurrence of an object within a class, identifying one of many objects within the same object class

EXAMPLE California is an instance of the object class state.

Note 1 to entry: The terms object, instance, and object instance are used to refer to a specific instance.

3.4.30**instance attribute**

attribute that is unique to an object instance and not shared by the object class

3.4.31**instantiated**

object that has been created in a device

3.4.32**Keeper**

object responsible for distributing link configuration data to all nodes on the link

3.4.33**link**

collection of nodes with unique MAC IDs, attached to Ph-segments connected by Ph-repeaters

3.4.34**little endian**

model of memory organization which stores the least significant octet at the lowest address, and of transmission organization which transfers the least significant octet first on the medium

3.4.35**Lpacket**

well-defined sub-portion of a DLPDU consisting of

- a) size and control information
- b) a fixed tag or a generic tag, and
- c) DLS-user data or, when the tag has DL-significance, DL-data

3.4.36**M_symbol(s)**

symbols that represent the data bits and related information encoded and transmitted by the PhL

3.4.37**maximum scheduled node**

node with highest MAC ID that can use scheduled time on a link

3.4.38**maximum unscheduled node**

node with highest MAC ID that can use unscheduled time on a link

3.4.39**Message Router**

object within a node that distributes messaging requests to the appropriate application objects

3.4.40**moderator**

node with the lowest MAC ID that is responsible for transmitting the moderator DLPDU

3.4.41**moderator DLPDU**

DLPDU transmitted by the node with the lowest MAC ID for the purpose of synchronizing the nodes and distributing the link configuration parameters

3.4.42**multipoint connection**

connection from one node to many

Note 1 to entry: Multipoint connections allow messages from a single producer (publisher) to be received by many consumer (subscriber) nodes.

3.4.43**network**

series of nodes connected by some type of communication medium

Note 1 to entry: The connection paths between any pair of nodes can include repeaters, routers and gateways.

3.4.44**network access monitor****NAM**

component within a node that manages communication with a temporary node connected to the nodes local NAP

3.4.45**network access port****NAP**

PhL variant that allows a temporary node to be connected to the link by connection to the NAP of a permanent node

3.4.46**network address or node address**

node's address on the link

Note 1 to entry: This is also called MAC ID.

3.4.47**network status indicators**

indicators on a node indicating the status of the Physical and Data Link Layers

3.4.48**network update time****NUT**

repetitive time interval in which data can be sent on the link

3.4.49**node**

logical connection to a local link, requiring a single MAC ID

Note 1 to entry: A single physical device may appear as many nodes on the same local link. For the purposes of this protocol, each node is considered to be a separate DLE.

3.4.50**non-concurrence**

situation where a transmission is received from an unexpected MAC ID, which appears to violate the time based access protocol

Note 1 to entry: This may occur when a connection is made between two working links that are not synchronized with each other but who have the same configuration information.

3.4.51**non-data symbol**

PhL symbol which violates the requirements of Manchester biphase L encoding

3.4.52**object**

abstract representation of a particular component within a device

Note 1 to entry: An object can be

- 1) an abstract representation of a computer's capabilities. Objects can be composed of any or all of the following components:
 - a) data (information which changes with time);
 - b) configuration (parameters for behavior);
 - c) methods (things that can be done using data and configuration);
- 2) a collection of related data (in the form of variables) and methods (procedures) for operating on that data that have clearly defined interface and behavior.

3.4.53**object specific service**

service defined by a particular object class to perform a required function which is not performed by a common service

Note 1 to entry: An object specific service is unique to the object class which defines it.

3.4.54**originator**

client responsible for establishing a connection path to the target

3.4.55**permanent node**

node whose connection to the network does not utilize the network access port (NAP) PhL variant

Note 1 to entry: This node may optionally support a NAP PhL variant to allow temporary nodes to connect to the network.

3.4.56**produce**

act of sending data to be received by a consumer

3.4.57**producer**

node that is responsible for sending data

3.4.58**redundant media**

system using more than one medium to help prevent communication failures

3.4.59**requested packet interval****RPI**

measure of how frequently the originating application requires the transmission of Lpackets or data packets from the target application

3.4.60**rogue**

node that has received a moderator DLPDU that disagrees with the link configuration currently used by this node

3.4.61**scheduled**

data transfers that occur in a deterministic and repeatable manner on predefined NUTs

3.4.62**server**

object which provides services to another (client) object

3.4.63**service**

operation or function than an object and/or object class performs upon request from another object and/or object class

Note 1 to entry: A set of common services is defined and provisions for the definition of object-specific services are provided. Object-specific services are those which are defined by a particular object class to perform a required function which is not performed by a common service.

3.4.64**slot time**

maximum time required for detecting an expected transmission

Note 1 to entry: Each node waits a slot time for each missing node during the implied token pass.

3.4.65**start delimiter**

unique set of M_symbols that identifies the beginning of a DLPDU

3.4.66**supernode**

DLE with a MAC ID of zero

Note 1 to entry: This DLE DL-address is reserved for special DLL functions

3.4.67**table unique identifier****TUI**

unique reference code used by ControlNet and Keeper objects to reference a consistent set of link configuration attribute

3.4.68**tag**

shorthand name for a specific piece of application information, two or three octets in length

3.4.69**target**

end-node to which a connection is established

3.4.70**temporary node**

same as transient node

3.4.71**tMinus**

number of NUTs before a new set of link configuration parameters are to be used

3.4.72**tone**

instant of time which marks the boundary between two NUTs

3.4.73**tool**

executable software program which interacts with the user to perform some function

EXAMPLE Link scheduling software (LSS).

3.4.74**transaction id**

field within a UCMM header that matches a response with the associated request, which a server echoes in the response message

3.4.75**transient node**

node that is only intended to be connected to the network on a temporary basis using the NAP PhL medium connected to the NAP of a permanent node

3.4.76**Unconnected Message Manager****UCMM**

component within a node that transmits and receives unconnected explicit messages and sends them directly to the Message Router object

3.4.77**unconnected service**

messaging service which does not rely on the set up of a connection between devices before allowing information exchanges

3.4.78**unscheduled**

data transfers that use the remaining allocated time in the NUT after the scheduled transfers have been completed

3.4.79**vendor ID**

identification of each product manufacturer/vendor by a unique number

Note 1 to entry: Vendor IDs are assigned by ODVA, Inc.

3.5 Type 2 symbols and abbreviations

ACD	Address Conflict Detection	
ACM	Access control machine	
BOOTP	Bootstrap Protocol	[IETF RFC 951]
CA	Clock accuracy	
CAN	Controller area network	[ISO 11898:1993]
COP	Connection originator password	
DHCP	Dynamic Host Configuration Protocol	[IETF RFC 2131]
DLR	Device level ring	
DSCP	DiffServ code point	
FCS	Frame Check Sequence	
IP	Internet Protocol	[IETF RFC 791]
LED	Light emitting diode.	
LSS	Link scheduling software	
MAC ID	MAC address of a node	
MSTP	Multiple spanning tree protocol	[IEEE 802.1Q]
NAM	Network attachment monitor	
NAP	Network access port	
ND	Non-data symbol	
NUT	Network update time	
PT	Programming terminal (a temporary network connection)	
QoS	Quality of service	
Rcv	Receive	
RPI	Requested Lpacket interval	
RSTP	Rapid spanning tree protocol	[IEEE 802.1D]
Rx	Receive	
RxLLC	Receive logical link control	
RxM	Receive machine	
SEM	State event matrix	
SMAX	MAC ID of the maximum scheduled node	
STD	State transition diagram, used to describe object behavior	
STP	Spanning tree protocol	[IEEE 802.1D]
TCP	Terminal Control Protocol	[IETF RFC 793]
TFTP	Trivial File Transfer Protocol	[IETF RFC 1350]
TUI	Table unique identifier	
Tx	Transmit	
TxLLC	Transmit logical link control	
TxM	Transmit machine	
UCCM	Unconnected Message Manager	
UMAX	MAC ID of maximum unscheduled node	
USR	Unscheduled start register	

3.6 Conventions for station management objects

Objects for station management are specified in Clause 7, using attributes, services and behaviour.

Object attributes are specified in tables formatted according to Table 1.

Table 1 – Format of attribute tables

Attribute ID	Need in implementation	Access rule	NV	Name	Data type	Description of attribute	Semantics of values
See a)	See b)	See c)	See d)	See e)	See 6.1.3.	See f)	See g)

a) “Attribute ID” is the identification value assigned to an attribute.

b) “Need in implementation” specifies whether or not the attribute is necessary in the implementation. An attribute may be optional, required or conditional.

A conditional attribute is required if certain object behaviours and/or attributes are implemented as defined by the class.

If an Attribute is optional, then a default value shall be defined in the semantics. An optional attribute's default value shall provide the same behaviour as if the attribute was not implemented. If the default value of an optional attribute does not match the behaviour of the object when the object does not implement the attribute, the object definition shall declare the behaviour.

In all cases, the term “default” indicates a “factory default” as shipped from the vendor.

c) “Access rule” specifies how a requestor can access an attribute. The definitions for access rules are:

- Settable (Set) – The attribute shall be accessed by at least one of the set services. If the behaviour of the device does not require a set service, then a device implementation of that object is not required to implement the attribute as settable.

Settable attributes, unless otherwise specified by the object definition, shall be also accessed by get services.

- Gettable (Get) – The attribute shall be accessed by at least one of the get services.

d) “NV” indicates whether an attribute value is maintained through power cycles. This column is used in object definitions where non-volatile storage of attribute values is required. An entry of “NV” indicates value shall be saved, “V” means not saved.

e) Name refers to the attribute.

f) Description of Attribute provides general information about the attribute.

g) Semantics of Values specifies the meaning of the value of the attribute.

4 Overview of the data-link protocol

4.1 General

4.1.1 DLL architecture

The Type 2 DLL is modeled as an integrated Access Control Machine (ACM), with scheduling support functions, designed for reliable and efficient support of higher-level connection-mode and connectionless data transfer services. Interoperating with these higher level functions are DLL management functions.

PhL framing and delimiters are managed by DLL functions for serializing and deserializing M_symbol requests and indications.

Within the Data Link Layer, the Access Control Machine (ACM) has the primary responsibility for detecting and recovering from network disruptions. The major objectives of the ACM are

- to make sure that the local node detects and fully utilizes its assigned access slots in the schedule;
- to make sure that the local node does not interfere with the transmissions of other nodes, especially the moderator node;
- to start the next NUT (see 4.1.2) on schedule, whether the moderator DLPDU is heard or not;
- if the local node is the moderator, to transmit each moderator DLPDU strictly on schedule.

The Data Link Layer is comprised of the components listed in Table 2:

Table 2 – Data-link layer components

Components	Description
Access Control Machine (ACM)	receives and transmits control DLPDUs and header information, and determines the timing and duration of transmissions.
Transmit LLC (TxLLC)	buffers DLSUDs received from Station Management and the DLS-user, and determines which should be transmitted next.
Receive LLC (RxLLC)	performs the task of quarantining received link units until they are validated by a good FCS.
Transmit Machine (TxM)	receives requests to send DLPDU headers and trailers, and Lpackets from the ACM, and breaks them down into octet symbol requests that are sent to the Serializer.
Receive Machine (RxM)	assembles received Lpackets from octet symbols received from the Deserializer, and submits them to the RxLLC.
Serializer	receives octet symbols, encodes and serializes them, and sends them as M_symbols to the PhL. It is also responsible for generating the FCS.
Deserializer	receives M_symbols from the PhL, converts M_symbols into octets and sends them to the receive machine. It is also responsible for checking the FCS.
DLL Management Interface	holds the Station Management variables that belong to the DLL, and helps manage synchronized changes of the link parameters.

The internal arrangement of these components, and their interfaces, are shown in Figure 2. The arrowheads illustrate the primary direction of flow of data and control.

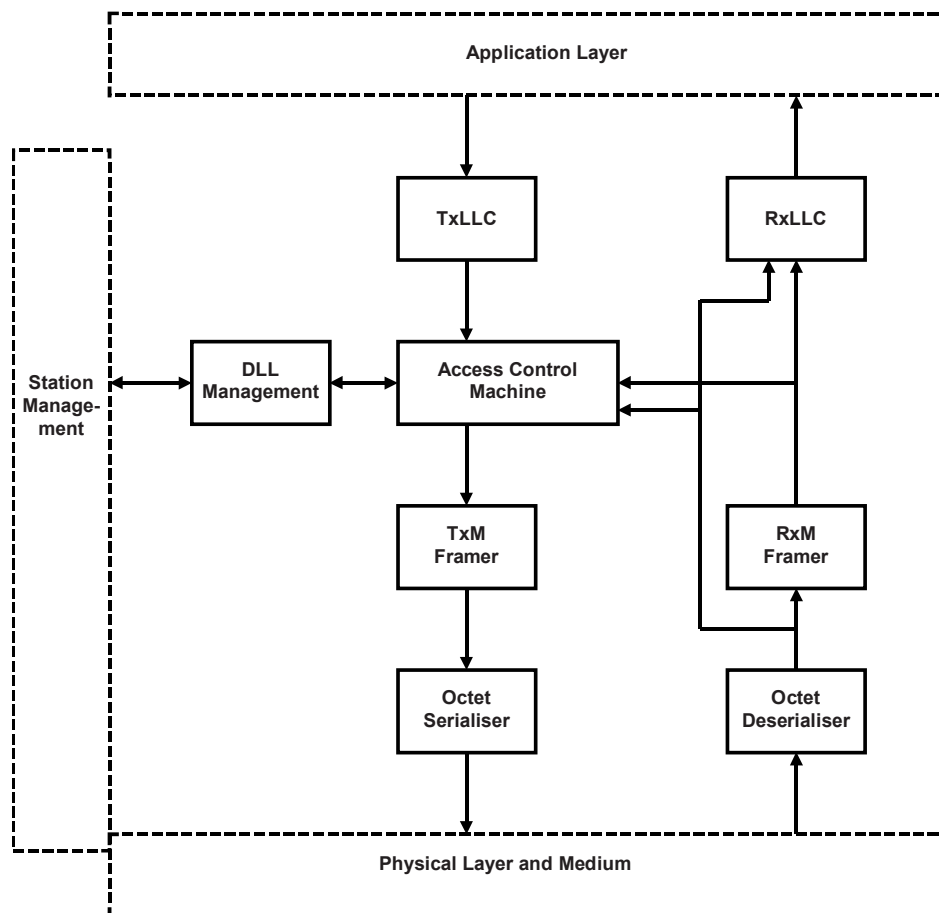


Figure 2 – Data-link layer internal architecture

4.1.2 Access control machine (ACM) and scheduling support functions

The ACM functions schedule all communication from one DLE to another. The timing of this communication are regulated at two levels,

- 1) to provide an accurate time based distribution of scheduled opportunities for designated communications in accord with, and with a pre-established schedule for, the local link and any extended network of links,
- 2) to provide a democratic distribution of unscheduled opportunities for arbitrary communications, generally in a cyclic but asynchronous manner.

Accurate schedule timing as provided by 1) is very important to support many control and data collection tasks in the applications domain of this protocol. The schedule is based on a fixed, repetitive time cycle called network update time (NUT). The NUT is maintained in close synchronism among all nodes participating in the DLL and used to provide two types of access opportunity;

- 1) One opportunity for each active station to transfer one scheduled DLPDU containing multiple scheduled DLSDUs.

Only DLSDUs with scheduled as their QoS parameter may be included in a scheduled DLPDU.

NOTE DLSDUs with scheduled as their QoS parameter are usually connection mode transfers with generic as their tag parameter.

- 2) One opportunity for at least one active station to send one background (unscheduled) DLPDU containing multiple DLSDUs of any QoS type. If time is available within a NUT, one background MAC opportunity is offered to each other active station in order of their MAC ID address. The station MAC ID for the first background opportunity in each NUT is

incremented (+1 modulo the set of background addresses) for each successive NUT to democratically share the available time among active stations.

Support procedures are included for automatic transfer to backup scheduling services and to manage the use of redundant Ph media.

4.1.3 Connection-mode, connectionless-mode data transfer and DL service

The connection mode, connectionless mode and DL services provide the necessary functionality for

- managing DL provider interactions with the DL user by converting request and response primitives into necessary DLE operations and generating indications and confirm primitives where appropriate,
- determination of the DL address and control information to be added to each DLSDU,
- local confirmation of status for each outgoing DLSDU,
- DLPDU formation by concatenation of multiple DL user DLSDUs for efficient transfer as single PhPDUs, subject to DLPDU size limitations, QoS parameters and the type of access opportunity.

4.2 Services provided by the DL

4.2.1 Overview

The DLL provides connectionless data transfer services and connection-mode data transfer services for limited-size DLSDUs, an internally synchronized time service, scheduling services to control the time allocation of the underlying shared PhL service, a DL(SAP)-address and queue management service, and a packing/unpacking service that combines multiple DLSDUs into a single data transfer DLPDU for efficient use of each access opportunity.

4.2.2 QoS

4.2.2.1 Definition

The QoS parameter specifies priority options for DLSDUs and access opportunities. The available values are as follows:

4.2.2.2 DLL scheduled priority

The scheduled priority QoS provides accurate time based cyclic and acyclic sending of DLSDUs. The execution timing for this fieldbus scheduled service can be accurate and repeatable to better than 1 ms. Scheduled priority is normally used with connected mode services.

NOTE The master Keeper is responsible for regular publication of a unique table identifier (TUI) which ensures all nodes have a reference for the current set of link operating parameters. This TUI publication uses a fixed tag and is sent with QoS priority set to scheduled.

4.2.2.3 DLL high priority (unscheduled)

The high priority QoS provides acyclic sending of DLSDUs with a bounded upper time for the sending delay. Data on this priority is sent only when all scheduled data has been sent and a non-scheduled sending opportunity is available.

4.2.2.4 DLL low priority (unscheduled)

The low priority QoS provides for sending of DLSDUs only on an as-available basis. Data on this priority is sent only when all other data priorities have been sent and a non-scheduled sending opportunity is available.

NOTE High and Low priority are used only in a local sense to set the order of servicing among locally submitted, unscheduled DLS-user-data.

4.3 Structure and definition of DL-addresses

4.3.1 General

DL-addresses are used as MAC ID addresses (Link node designators), Fixed tag addresses (DLSAP-addresses and group DL-addresses), and Generic tag addresses (DLCEP-addresses).

Subclause 4.3 defines the form and structure of DL-addresses and includes specific definitions for some standard DL-addresses.

All addresses are formed of octets. Each octet shall be transferred to the Ph layer low-bit first and multiple octets shall be transferred low-order octet first (little endian format).

Three types of DL addresses are used.

4.3.2 MAC ID address

MAC ID addresses identify physical nodes on the local link as shown in Figure 3.

Permitted values are within the range 0 to 99, values from 100 to 254 are reserved.



Figure 3 – Basic structure of a MAC ID address

Table 3 specifies the use of MAC ID addresses.

Table 3 – MAC ID addresses allocation

MAC ID	Meaning and purpose
0x0	temporary address used for maintenance
SMAX	current maximum address value for Scheduled access opportunities. SMAX ≤ UMAX
UMAX	current maximum address value for Unscheduled access opportunities SMAX. ≤ UMAX ≤ 0x63
0x64 to 0xFE	reserved
0xFF	broadcast address to all MAC ID nodes on this link

4.3.3 Generic tag address

Generic tag addresses types identify all data transfers for connected mode services. The available capacity in the DLL is 3 octets, see Figure 4.

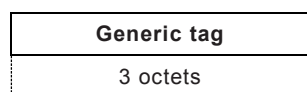


Figure 4 – Basic structure of a generic tag address

Generic tags are used to send connected DLSDUs and may be associated with any of the available QoS priorities (Scheduled, High, Low).

NOTE Negotiation and management of generic tags and connected mode services are the responsibility of the DL user.

4.3.4 Fixed tag address

Fixed tag addresses types identify DLSAPs within a designated station MAC ID. They are used with all data transfers for connectionless mode services.

NOTE Fixed tags are used to send connectionless DLSDUs and are usually associated with unscheduled QoS priorities (High, Low). Typical uses of fixed tags are for station management and to establish connections.

Each fixed tag address shall consist of two octets as shown in Figure 5.

Fixed tag service	Destination MAC ID
1 octet	1 octet

Figure 5 – Basic structure of a fixed tag address

The first octet shall specify the service access point in the destination node as specified in Table 4. The second octet shall be the address of the destination node. The destination address shall be either a MAC ID or 0xFF, which indicates the broadcast address to all MAC IDs on the local link.

Table 4 – Fixed tag service definitions

Fixed tag service	Meaning
0x00	moderator
0x01 - 0x08	vendor specific
0x09	ping request
0x0A - 0x14	vendor specific
0x15	tMinus
0x16 - 0x28	vendor specific
0x29	ping reply
0x2A - 0x3F	vendor specific
0x40 - 0x6F	reserved
0x70 - 0x7F	vendor-specific
0x80	I'm alive
0x81	link parameters
0x82	reserved
0x83	UCMM
0x84	TUI
0x85	IP (reserved for Internet Protocol)
0x86	WAMI
0x87	reserved
0x88	Keeper UCMM
0x89	Ethernet (used for address resolution protocol)
0x8A - 0x8B	reserved
0x8C	Time distribution
0x8D - 0x8F	reserved for time distribution
0x90	debug
0x91 - 0xCF	reserved
0xD0 - 0xEF	group addresses
0xF0 - 0xFF	vendor specific

Fixed tags in the range 0xD0 to 0xEF shall be reserved to permit group screening of connection identifiers.

4.4 Services assumed from the PhL

4.4.1 General requirements

Subclauses 4.4.2 to 4.4.3 include requirements for interface to a Type 2 PhL that are not required for other Types.

- Transmit Machine.
- Receive Machine.
- Serializer.
- Deserializer.

This is necessary because the Ph-Interface Data Units (PhIDUs) that Type 2 passes across the DLL–PhL interface are individual serial data and non-data symbols, designated on the DLE side as M_Symbols (see Table 5), whereas PhIDUs for other Types are not conceptualized in this way. As a consequence, a Type 2 Data Link Layer requires a Type 2 PhL.

4.4.2 Data encoding rules

The M_Symbols transferred at the DLL to PhL interface are of four types designated 0, 1, +, -. They will be encoded inside the PhL into appropriate Ph_Symbols as shown in Table 5. The M_0 and M_1 will be encoded into Ph_Symbols that represent Manchester biphasic L data encoding rules. The M_ND symbols are non-data symbols to allow for the creation of unique data patterns used for start and end delimiters. The example of signal voltage waveform as it might be applied to an electrically-conductive medium is shown in an idealized form in Figure 6 to provide an example of the data encoding rules shown in Table 5.

Table 5 – Data encoding rules

Data bits (common name)	M_Symbol representation	Ph_Symbol encoding	Manchester encoded
data “zero”	M_0 or {0}	{L,H}	0
data “one”	M_1 or {1}	{H,L}	1
“non_data+”	M_ND+ or {+}	{H,H}	no data
“non_data–”	M_ND– or {–}	{L,L}	no data

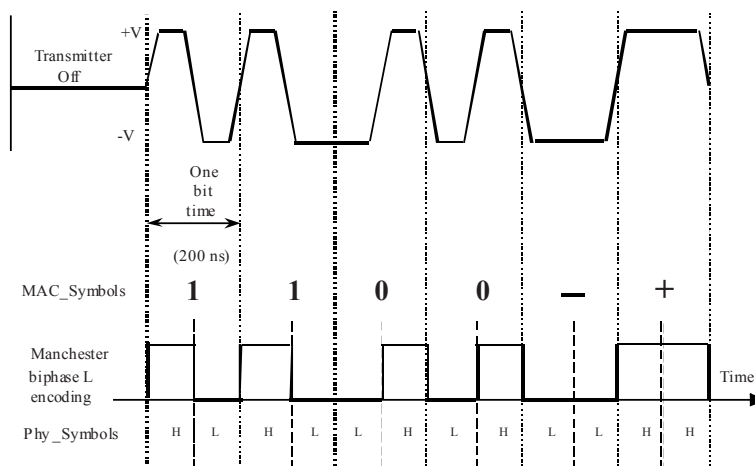


Figure 6 – M_symbols and Manchester encoding at 5 MHz

4.4.3 DLL to PhL interface

4.4.3.1 General

The DLL to PhL interface need not be exposed in the implementation of any PhL variant. This interface may be internal to the node. If conformance to the DLL to PhL interface is claimed, it shall conform to the requirements of 4.4.3.

4.4.3.2 Ph_lock_indication

ph_lock_indication shall provide an indication of either data lock or Ph_Symbol synchronization by the PhL. Valid states for ph_lock_indication shall be true and false. ph_lock_indication shall be true whenever valid Ph_Symbols are present at the PhL interface and the PhL to DLL interface timing of M_Symbols conforms to the PhL requirements. It shall be false between frames (when no Ph_Symbols are present on the medium) or whenever data synchronization is lost or the timing fails to conform to the PhL requirements. ph_lock_indication shall be true prior to the beginning of the start delimiter.

4.4.3.3 Ph_frame_indication

ph_frame_indication shall provide an indication of a valid data frame from the PhL. Valid states for ph_frame_indication shall be true and false. ph_frame_indication shall be true upon ph_lock_indication = true and reception of the first valid start delimiter. ph_frame_indication shall be false at reception of next M_ND symbol (following the start delimiter) or ph_lock_indication = false.

NOTE This signal provides octet synchronization to the DLL.

4.4.3.4 Ph_carrier_indication

ph_carrier_indication shall represent the presence of a signal carrier on the medium. The ph_carrier_indication shall be true if internal PhL identification of signal carrier has been true during any of the last 4 M_symbol times and it shall be false otherwise.

4.4.3.5 Ph_data_indication

ph_data_indication shall represent the M_Symbols that are decoded from the PhL internal representations such as those shown in Table 5. Valid M_symbols shall be M_0 {0}, M_1 {1}, M_ND+ {+}, and M_ND- {-} as shown in Table 6.

Table 6 – M Data symbols

Data bits (common name)	M_Symbol representation
data “zero”	M_0 or {0}
data “one”	M_1 or {1}
“non_data+”	M_ND+ or {+}
“non_data–”	M_ND– or {–}

The ph_data_indication shall represent the M_Symbols as decoded within the PhL whenever ph_lock_indication is true.

4.4.3.6 Ph_status_indication

ph_status_indication shall represent the delimiter status of the frame which was received from the PhL as shown in Table 7. Valid symbols shall be Normal, Abort, and Invalid. ph_status_indication shall indicate Normal after reception of a frame (ph_frame_indication = true) composed of a start delimiter, valid data (no M_ND symbols) and an end delimiter. ph_status_indication shall indicate Abort after reception of a frame (ph_frame_indication = true) composed of a start delimiter, valid data, and a second start delimiter. ph_status_indication shall indicate Invalid after reception of a frame (ph_frame_indication = true) composed of a start delimiter and the detection of any M_ND symbol which was not part of a start or end delimiter.

Table 7 – Truth table for ph_status_indication

Ph_status_indication	Ph_frame_indication	Start delimiters in a single frame	End delimiter detection	Any non-delimiter Manchester violations
Normal	true	1	true	false
Abort	true	2	don't care	false
Invalid	true	1	don't care	true

4.4.3.7 Ph_data_request

ph_data_request shall present the M_Symbols to be transmitted. Valid symbols shall be M_0, M_1, M_ND+ or M_ND– as shown in Table 6. ph_data_request shall indicate M_0 when no data is to be transmitted (and ph_frame_request = false).

4.4.3.8 Ph_frame_request

ph_frame_request shall be true when ph_data_request presents M_Symbols to be encoded into the appropriate Ph_Symbols by the PhL, and shall be false when no valid M_Symbols are to be transferred to the PhL.

4.5 Functional classes

Implementations of this protocol fall into two broad classes:

- connection originators (sometimes called Scanners);
- connection responders or connection targets (sometimes called Adaptors).

Devices with connection origination capability will include functions such as Scheduling object, support for external Configuration Tools and usually a Keeper object.

Connection responders are typically simpler devices which do not need the full set of capabilities.

This specification does not mandate particular groupings of functions for classes of implementation devices.

NOTE Grouping of services and functions into implementation classes can be done by separate specifications for profiles.

5 General structure and encoding of PhIDUs and DLPDUs and related elements of procedure

5.1 Overview

The DLL and its procedures are those necessary to provide the services offered to DLS user by using the services available from the PhL. The main services of this protocol are

- a) provision of timely access opportunities to support scheduled data-transfer DL-services on one link and on an extended multi-link network;
- b) the packing of multiple DLS-user transfers into a single PhL transfer unit (DLPDU) to efficiently use each transfer opportunity;
- c) the efficient distribution of DLS-user data from a publishing DLS-user to a set of subscribing DLS-users;
- d) the provision of a synchronized sense of internal time among the DLEs and available to the DLS-users of the extended link;
- e) the standardized availability of local DL-address, buffer and queue management capabilities.

5.2 Media access procedure

The primary task of the Data Link Layer is to determine, in co-operation with other Data Link Layers on the same link, the granting of permission to transmit on the medium. At its upper interface, the DLL provides services to receive and deliver service data units for the DLS user and Station Management.

The DLL protocol is based on a fixed, repetitive time cycle called a network update time (NUT). The NUT is maintained in close synchronism among all nodes on the link. A node is not permitted access to transmit on the medium if its NUT does not agree with the NUT currently being used on a link wide basis. Different links may have different NUT duration.

Each node contains its own timer synchronized to the NUT for the local link. Media access is determined by local sub-division of the NUT into access slots. Access to the medium is in sequential order based on the MAC ID of the node. Specific behaviors have been incorporated into the access protocol allowing a node which temporarily assumes a MAC ID of zero to perform link maintenance. The MAC ID numbers of all nodes on a link are unique. Any DLL detecting the presence of a duplicate MAC ID shall immediately stop transmitting.

An implicit token passing mechanism is used to grant access to the medium. Each node monitors the source MAC ID of each DLPDU received. At the end of a DLPDU, each DLL sets an "implicit token register" to the received source MAC ID + 1. If the implicit token register is equal to the local MAC ID, then the node shall transmit one DLPDU containing one or more Lpackets with data or a null DLPDU. In all other cases, the node watches for either a new DLPDU from the node identified by the "implicit token register" or a time-out value if the identified node fails to transmit. In each case, the "implicit token" is automatically advanced to the next MAC ID. All nodes have the same value in their "implicit token register" preventing collisions on the medium.

The time-out period (called the "slot time") is based on the amount of time required for

- the current node to hear the end of the transmission from the previous node;
- the current node to begin transmitting;

- the next node to hear the beginning of the transmission from the current node.

The slot time is adjusted to compensate for the total length of the medium since the propagation delay of the medium effects the first and last item on the previous list.

NOTE The calculation of slot time is specified in 8.2.

Each NUT is divided into three major parts: scheduled, unscheduled, and guardband as shown in Figure 7. This sequence is repeated in every NUT. The implicit token passing mechanism is used to grant access to the medium during both the unscheduled and scheduled intervals.

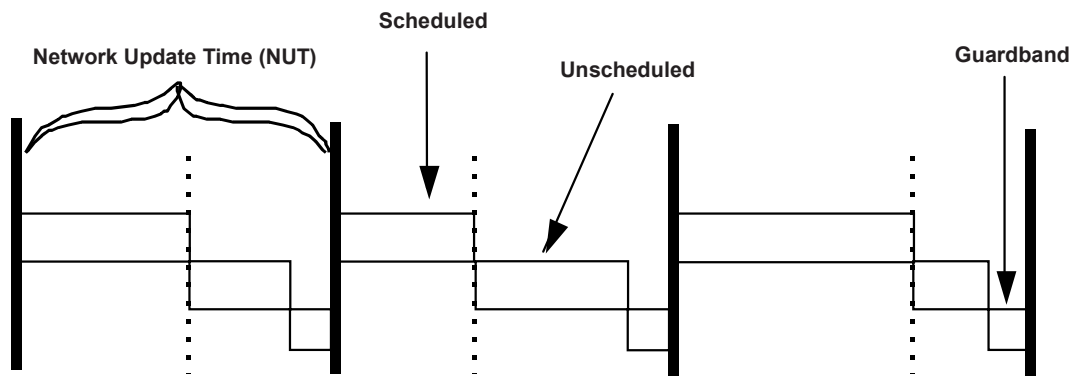


Figure 7 – NUT structure

During the scheduled part of the NUT, each node, starting with node 0 and ending with node SMAX, gets a chance to transmit time-critical (scheduled) data. SMAX is the MAC ID of the highest numbered node that has access to the medium during the scheduled part of the NUT. Every node between 0 and SMAX has only one opportunity to send one DLPDU of scheduled data in each NUT. The opportunity to access the medium during the scheduled time is the same for each node in every NUT. This allows data that is transmitted during the scheduled portion of the NUT to be sent in a predictable and deterministic manner. Figure 8 shows how the permission to transmit is granted during the scheduled time. The DLS-user regulates the amount of data that each node may transmit during this scheduled token pass.

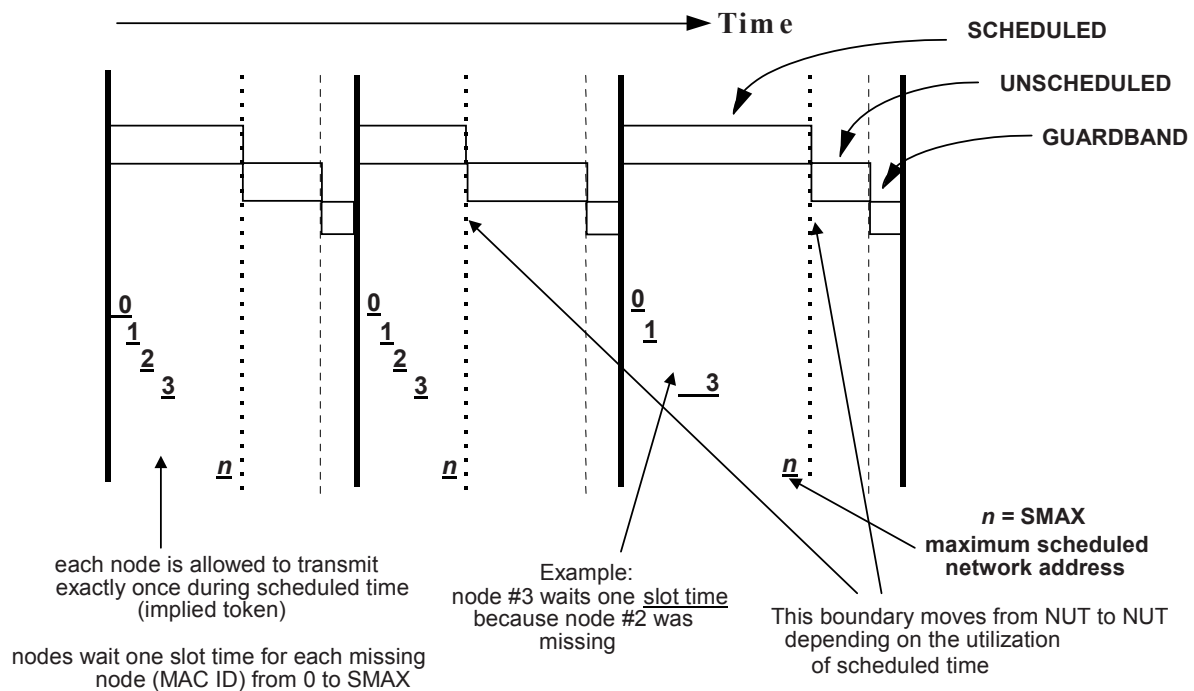


Figure 8 – Media access during scheduled time

During the unscheduled part of the NUT, each node from 0 to UMAX shares the opportunity to transmit one DLPDU of non-time critical data in a round robin fashion, until the allocated NUT duration is exhausted. UMAX is the MAC ID of the highest numbered node that has access to the medium during the unscheduled part of the NUT. The round robin method of access opportunity enables every node between 0 and UMAX to have zero, one or many opportunities to send unscheduled data depending on how much of the NUT remains after the completion of the scheduled time. Variations in scheduled traffic means the opportunity to access the medium during the unscheduled time may be different for each node in every NUT. Figure 9 shows how the permission to transmit is granted during the unscheduled time. The MAC ID of the node that goes first in the unscheduled part of the NUT is incremented by 1 for each NUT. The unscheduled token begins at the MAC ID specified in the unscheduled start register (USR) of the previous moderator DLPDU. The USR increments by one modulo (UMAX+1) each NUT. If the USR reaches UMAX before the guardband, it returns to zero and the token pass continues.

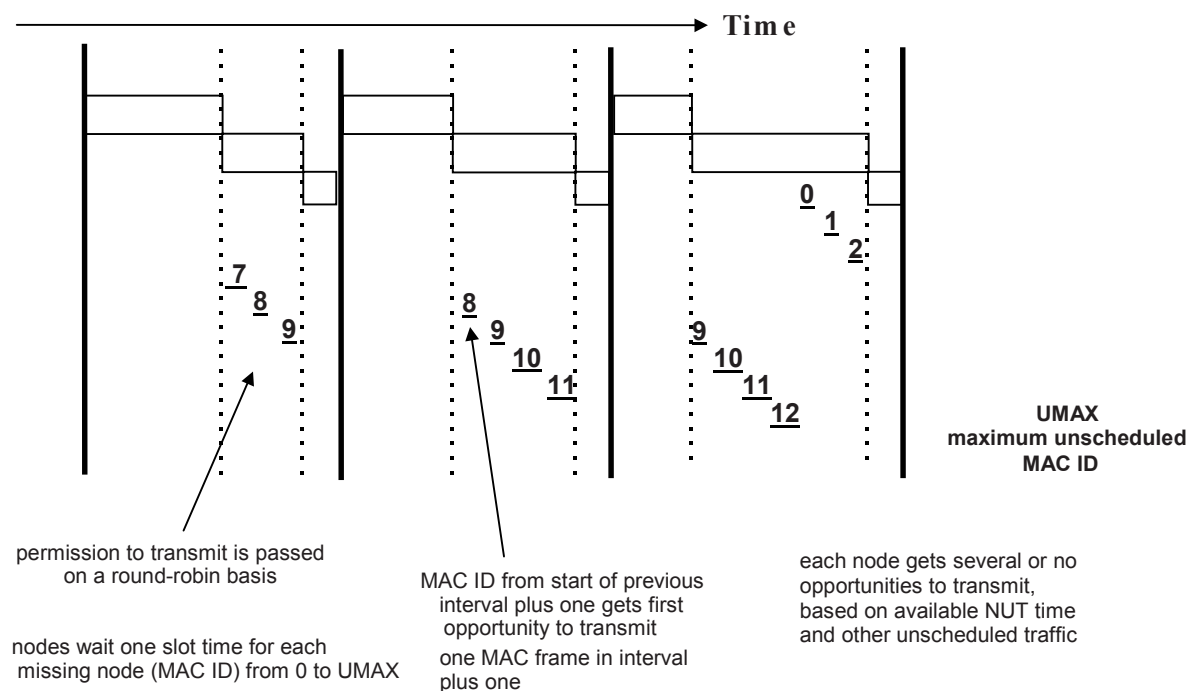


Figure 9 – Media access during unscheduled time

When the guardband is reached, all nodes stop transmitting. A node is not allowed to start a transmission unless it can be completed before the beginning of the guardband. During the guardband, the node with the lowest MAC ID (called the “moderator”) transmits a maintenance message (called the “moderator DLPDU”) that accomplishes two things:

- it keeps the NUT timers of all nodes synchronized;
- it publishes critical link parameters enabling all members of the local DLL group to share a common version of important DLL values such as NUT, slot time, SMAX, UMAX, etc.

The moderator transmits the moderator DLPDU, which re-synchronizes all nodes and restarts the NUT. Following the receipt of a valid moderator DLPDU, each node compares its internal values with those transmitted in the moderator DLPDU. A node using link parameters that disagree with the moderator disables itself. If the moderator DLPDU is not heard for 2 consecutive NUTs, the node with the lowest MAC ID assumes the moderator role, and begins transmitting the moderator DLPDU in the guardband of the third NUT. A moderator node that notices another node on-line and transmitting with a MAC ID lower than its own immediately cancels its moderator role.

Typical situations that may cause disruption of the DLL access protocol include

- induced noise on the link;
- poor cable or termination quality;
- physically connecting two links together while the network is operating.

One common consequence of such disruption is that nodes may be caused to disagree as to which node should be transmitting; this is called a network “non-concurrence”. Another potential problem occurs when the nodes do not agree to the same link configuration parameters. A node that disagrees with the link parameters as transmitted by the moderator is called a “rogue” and immediately stops transmitting. The DLL access protocol is designed to recover a rogue node and bring it back on-line.

5.3 DLPDU structure and encoding

5.3.1 General

DLPDUs are the DLPDUs passed to the Ph layer for sending on the Ph medium. The DLPDUs are formed by the transmit logical link control (TxLLC) protocol in two stages:

- DLSDUs are formed into Link-units (Lpackets);
- Multiple Lpackets are packed into one DLPDU subject to constraints set by the QoS required, the type of access opportunity available and limits on DLPDU overall length.

5.3.2 DLPDU components

The general DLPDU structure is shown in Figure 10 and managed by the DLL support units TxFramer, RxFramer, Octet Serializer and Octet Deserializer as shown in Figure 2.

The components of the DLPDU shall be transmitted in the following order: preamble, start delimiter, source MAC ID, zero or more Lpackets, FCS and end delimiter.

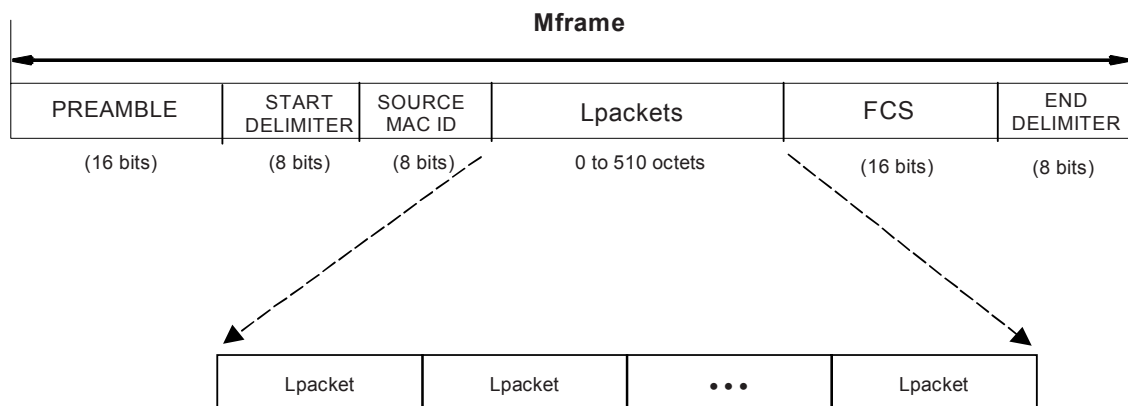


Figure 10 – DLPDU format

5.3.3 Preamble

The preamble shall be composed of 16 consecutive {1} M_Symbols.

5.3.4 Start and end delimiters

The start delimiter shall consist of these M_Symbols, {+, 0, –, +, –, 1, 0, 1}, transmitted from left to right.

The end delimiter shall consist of these M_Symbols, {1, 0, 0, 1, +, –, +, –}, transmitted from left to right.

The use of non-data M_Symbols shall be reserved for the start and end delimiters.

5.3.5 DLPDU octets and ordering

The source MAC ID, Lpackets, and FCS shall be composed of octets. An octet shall be composed of exactly eight M_Symbols each of which shall be either {0} or {1}. An octet shall be transferred to the PhL low bit first. Multiple octet fields shall be transmitted low order octet first (little endian format).

5.3.6 Source MAC ID

The source MAC ID address shall be a single octet as specified in 4.3.2. A node may also temporarily assume a MAC ID of zero to perform link maintenance.

5.3.7 Lpackets field

Zero or more Lpackets shall be concatenated into a single DLPDU subject to the constraint that the maximum number of octets which compose all Lpackets in a DLPDU shall be 510.

An additional constraint is that DLPDUs sent during a scheduled access opportunity shall only contain Lpackets with a QoS parameter of scheduled.

5.3.8 Frame check sequence (FCS)

5.3.8.1 Frame check sequence requirements

The FCS shall be a modified CCITT checksum using the 16 bit polynomial: $G(X) = X^{16} + X^{12} + X^5 + 1$. A two octet FCS shall be included in each DLPDU.

The formal concepts for its generation and checking on reception are described in 5.3.8.2. The generation and checking of the FCS are further specified in 9.7 and 9.8.

5.3.8.2 Frame check sequence formal concepts

5.3.8.2.1 Frame check sequence field

Within 5.3.8.2, any reference to bit K of an octet is a reference to the bit whose weight in a one-octet unsigned integer is 2^K .

NOTE This is sometimes referred to as "little endian" bit numbering.

For this standard, as in other international standards (for example, ISO/IEC 3309, ISO/IEC 8802 and ISO/IEC 9314-2), DLPDU-level error detection is provided by calculating and appending a multi-bit frame check sequence (FCS) to the other DLPDU fields during transmission to form a "systematic code word"³ of length n consisting of k DLPDU message bits followed by $n - k$ (equal to 16) redundant bits, and by calculating during reception that the message and concatenated FCS form a legal (n, k) code word. The mechanism for this checking is as follows, where the generic form of the generator polynomial for this FCS construction is specified in equation (4) and the polynomial for the receiver's expected residue is specified in equation (9). The specific polynomials for this standard are specified in Table 8.

Table 8 – FCS length, polynomials and constants

Item	Value
$n-k$	16
$G(X)$	$X^{16} + X^{12} + X^5 + 1$ (Notes 1, 2)
$R(X)$	$X^{12} + X^{11} + X^{10} + X^8 + X^3 + X^2 + X + 1$ (Notes 2, 3)
NOTE 1 Code words $D(X)$ constructed from this $G(X)$ polynomial have Hamming distance 4 for lengths $\leq 4\ 095$ octets, and all errors of odd weight are detected.	
NOTE 2 These are the same polynomials and method as specified in ISO/IEC 3309 (HDLC).	
NOTE 3 The remainder $R(x)$ should be 0001 1101 0000 1111 (X^{15} to X^0 , respectively) in the absence of errors.	

³ W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes* (2nd edition), MIT Press, Cambridge, 1972.

5.3.8.2.2 At the sending DLE

The original message (that is, the DLPDU without an FCS), the FCS, and the composite message code word (the concatenated DLPDU and FCS) shall be regarded as vectors $M(X)$, $F(X)$, and $D(X)$, of dimension k , $n - k$, and n , respectively, in an extension field over $GF(2)$. If the message bits are $m_1 \dots m_k$ and the FCS bits are $f_{n-k-1} \dots f_0$, where

$m_1 \dots m_8$ form the first octet sent,

$m_{8N-7} \dots m_{8N}$ form the N th octet sent,

$f_7 \dots f_0$ form the last octet sent, and

m_1 is sent by the first PhL symbol(s) of the message and f_0 is sent by the last PhL symbol(s) of the message (not counting PhL framing information),

NOTE 1 This “as transmitted” ordering is critical to the error detection properties of the FCS.

then the message vector $M(X)$ shall be regarded to be

$$M(X) = m_1X^{k-1} + m_2X^{k-2} + \dots + m_{k-1}X^1 + m_k \quad (1)$$

and the FCS vector $F(X)$ shall be regarded to be

$$\begin{aligned} F(X) &= f_{n-k-1}X^{n-k-1} + \dots + f_0 \\ &= f_{15}X^{15} + \dots + f_0 \end{aligned} \quad (2)$$

The composite vector $D(X)$, for the complete DLPDU, shall be constructed as the concatenation of the message and FCS vectors

$$\begin{aligned} D(X) &= M(X)X^{n-k} + F(X) \\ &= m_1X^{n-1} + m_2X^{n-2} + \dots + m_kX^{n-k} + f_{n-k-1}X^{n-k-1} + \dots + f_0 \\ &= m_1X^{n-1} + m_2X^{n-2} + \dots + m_kX^{16} + f_{15}X^{15} + \dots + f_0 \quad (\text{for the case of } k = 15) \end{aligned} \quad (3)$$

The DLPDU presented to the PhL shall consist of an octet sequence in the specified order.

The redundant check bits $f_{n-k-1} \dots f_0$ of the FCS shall be the coefficients of the remainder $F(X)$, after division by $G(X)$, of $L(X)(X^k + 1) + M(X)X^{n-k}$

where $G(X)$ is the degree $n-k$ generator polynomial for the code words

$$G(X) = X^{n-k} + g_{n-k-1}X^{n-k-1} + \dots + 1 \quad (4)$$

and $L(X)$ is the maximal weight (all ones) polynomial of degree $n-k-1$

$$\begin{aligned} L(X) &= (X^{n-k} + 1) / (X + 1) = X^{n-k-1} + X^{n-k-2} + \dots + X + 1 \\ &= X^{15} + X^{14} + X^{13} + X^{12} + \dots + X^2 + X + 1 \quad (\text{for the case of } k = 15) \end{aligned} \quad (5)$$

That is,

$$F(X) = L(X)(X^k + 1) + M(X)X^{n-k} \quad (\text{modulo } G(X)) \quad (6)$$

NOTE 2 The $L(X)$ terms are included in the computation to detect initial or terminal message truncation or extension by adding a length-dependent factor to the FCS.

NOTE 3 As a typical implementation when $n-k = 16$, the initial remainder of the division is preset to all ones. The transmitted message bit stream is multiplied by X^{n-k} and divided (modulo 2) by the generator polynomial $G(X)$, specified in equation (7). The ones complement of the resulting remainder is transmitted as the $(n-k)$ -bit FCS, with the coefficient of X^{n-k-1} transmitted first.

The equation for $D(X)$ does not apply to the Type 8 protocol because that protocol sends the message and check bits in separate DLPDUs. The equation for $F(X)$ as just given does not apply to the Type 8 protocol because that protocol does not complement the check bits before transmission. The equation corresponding to $F(X)$ for the Type 8 protocol is

$$F_{\text{Type 8}}(X) = L(X) X^k + M(X) X^{n-k} \text{ (modulo } G(X)) \quad (7)$$

NOTE 4 As a typical implementation for the Type 8 protocol, the initial remainder of the division is preset to all ones. The transmitted message bit stream is multiplied by X^{n-k} and divided (modulo 2) by the generator polynomial $G(X)$, specified in equation (7). The resulting remainder without ones complementation is transmitted as the (n-k)-bit FCS, with the coefficient of X^0 transmitted first.

5.3.8.2.3 At the receiving DLE

The octet sequence indicated by the PhE shall be concatenated into the received DLPDU and FCS, and regarded as a vector $V(X)$ of dimension u

$$V(X) = v_1 X^{u-1} + v_2 X^{u-2} + \dots + v_{u-1} X + v_u \quad (8)$$

NOTE 1 Because of errors u can be different than n , the dimension of the transmitted code vector.

A remainder $R(X)$ shall be computed for $V(X)$, the received DLPDU and FCS, by a method similar to that used by the sending DLE (see 5.3.8.2.2) in computing $F(X)$

$$\begin{aligned} R(X) &= L(X) X^u + V(X) X^{n-k} \text{ (modulo } G(X)) \\ &= r_{n-k-1} X^{n-k-1} + \dots + r_0 \end{aligned} \quad (9)$$

Define $E(X)$ to be the error code vector of the additive (modulo-2) differences between the transmitted code vector $D(X)$ and the received vector $V(X)$ resulting from errors encountered (in the PhS provider and in bridges) between sending and receiving DLEs.

$$E(X) = D(X) + V(X) \quad (10)$$

If no error has occurred, so that $E(X) = 0$, then $R(X)$ will equal a non-zero constant remainder polynomial

$$R_{ok}(X) = L(X) X^{n-k} \text{ (modulo } G(X)) \quad (11)$$

whose value is independent of $D(X)$. Unfortunately $R(X)$ will also equal $R_{ok}(X)$ in those cases where $E(X)$ is an exact non-zero multiple of $G(X)$, in which case there are “undetectable” errors. In all other cases, $R(X)$ will not equal $R_{ok}(X)$; such DLPDUs are erroneous and shall be discarded without further analysis.

NOTE 2 As a typical implementation, the initial remainder of the division is preset to all ones. The received bit stream is multiplied by X^{n-k} and divided (modulo 2) by the generator polynomial $G(X)$, specified in equation (8).

5.3.9 Null DLPDU

A DLPDU with an empty Lpacket field, called a null DLPDU, shall be sent by a node to indicate that it has no data to send at the QoS allowed by the access opportunity.

5.3.10 Abort DLPDU

To abort a partially transmitted DLPDU, the Data Link Layer shall transmit the following sequence:

- one 0xFF octet;
- start delimiter;
- end delimiter.

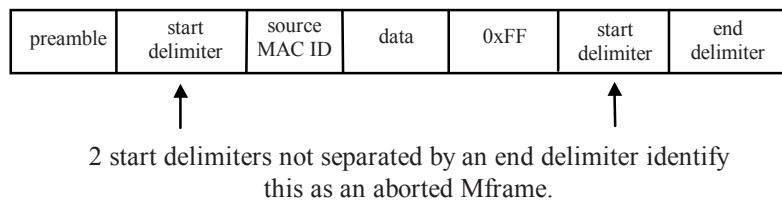


Figure 11 – Aborting a DLPDU during transmission

NOTE 1 Some implementations of this specification can build the DLPDU as it is being transmitted. If a higher layer has provided only a partial DLPDU to the Data Link Layer, and the DLL has begun transmission of the DLPDU assuming that the rest will be provided shortly, a transmit underflow occurs if the rest of the DLPDU is not provided to the DLL soon enough to complete the transmission.

NOTE 2 Although the DLL assembles the entire DLPDU including delimiters, the PhL performs start and end delimiter detection. The PhL identifies a transmit abort as a DLPDU which includes two start delimiters which are not separated by an end delimiter, as shown in Figure 11.

NOTE 3 The 0xFF octet is inserted before the start delimiter / end delimiter pair to avoid violating PhL constraints governing consecutive physical symbol relationships on the media.

5.4 Lpacket components

5.4.1 General Lpacket structure

The Lpacket (or link unit) is the PDU which is used to carry DLSDUs between peer DLS users. The components of the Lpacket shall be transmitted in the following order: size, control, tag, and link data as shown in Figure 12.

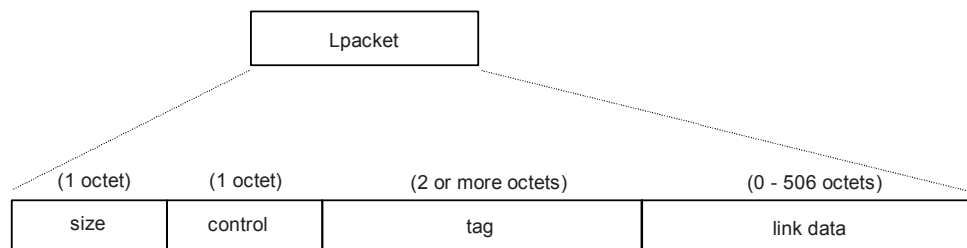


Figure 12 – Lpacket format

5.4.2 Size

The size field shall specify the number of octet pairs (from 3 to 255) contained in an individual Lpacket. The number of octet pairs shall include the size, control, tag, and link data fields counted in accordance with the following rules:

- combined, the size and control shall count as a single octet pair;
- the number of octet pairs from the tag and link data fields shall be counted separately and odd octet counts shall be rounded up;
- although the counting of octet pairs is done independently, the format of an Lpacket as placed into a DLPDU shall not include the extra octets caused by the round up.

NOTE For example, an Lpacket with a 3 octet tag (2 octet pairs) and a 9 octet link data (5 octet pairs) has a size field of $1+2=3$ octet pairs; however the Lpacket occupies $2+3+9=14$ octets in the DLPDU.