

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Industrial networks – Wireless communication network and communication profiles – WIA-PA

Réseaux industriels – Réseau de communications sans fil et profils de communication – WIA-PA



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2015 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

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

About IEC publications

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

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

Plus de 60 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.



IEC 62601

Edition 2.0 2015-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Industrial networks – Wireless communication network and communication profiles – WIA-PA

Réseaux industriels – Réseau de communications sans fil et profils de communication – WIA-PA

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40 ; 35.100.05

ISBN 978-2-8322-3040-4

Warning! Make sure that you obtained this publication from an authorized distributor. Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD	13
1 Scope	15
2 Normative references	15
3 Terms, definitions and abbreviations	15
3.1 Terms and definitions	15
3.2 Abbreviations	19
4 Definition of data types	21
5 WIA-PA overview	22
5.1 Device types	22
5.2 Network topology	22
5.3 Protocol architecture	24
5.4 Interconnection	25
6 System management	26
6.1 General	26
6.2 Framework of system management	27
6.3 Joining process	28
6.3.1 Provisioning process	28
6.3.2 Joining process of routing device	29
6.3.3 Joining process of field device	30
6.3.4 Addressing and address assignment	31
6.4 Virtual Communication Relationship (VCR)	32
6.4.1 Definition	32
6.4.2 Protocol support for VCR	33
6.4.3 VCR establishment	33
6.4.4 VCR release	34
6.5 Routing configuration and communication resource allocation	34
6.5.1 Routing configuration	34
6.5.2 Framework of communication resource allocation	34
6.5.3 DLPDU priority and scheduling rules	35
6.5.4 Communication resource allocation to routing device	35
6.5.5 Communication resource allocation to field device	37
6.6 Aggregation and disaggregation	39
6.6.1 Aggregation	39
6.6.2 Disaggregation	41
6.6.3 An example of the two level aggregation process	41
6.6.4 Management of aggregation and disaggregation objects	43
6.7 Performance monitoring	45
6.7.1 Path failure report	45
6.7.2 Device status report	45
6.7.3 Channel condition report	46
6.8 Leaving process	46
6.8.1 General	46
6.8.2 Leaving process of routing device	46
6.8.3 Leaving process of field device	48
6.9 Management information base and services	49
6.9.1 Management information base	49

6.9.2	MIB services	63
7	Physical layer	65
7.1	General.....	65
7.2	General requirements based on IEEE STD 802.15.4-2011	66
7.3	Additional requirements	67
7.3.1	General	67
7.3.2	Frequency allocations	67
7.3.3	Channel numbers and frequency assignments	67
7.3.4	Radio transceivers	67
7.3.5	Unspecified or improved required radio performance	67
7.3.6	Transmit power.....	68
7.3.7	Output power control	68
7.3.8	Receiver sensitivity.....	68
7.3.9	PHY PIB attributes.....	68
8	Data link layer	69
8.1	General.....	69
8.2	Protocol stack	69
8.3	MAC overview and function extension	70
8.3.1	MAC overview	70
8.3.2	General requirements based on IEEE STD 802.15.4-2011	70
8.3.3	MAC function extension	73
8.4	DLSL function description	74
8.4.1	General	74
8.4.2	Coexistence.....	75
8.4.3	Timeslot communication	75
8.4.4	WIA-PA superframe	76
8.4.5	Frequency hopping	76
8.4.6	Transmission of long cycle data.....	78
8.4.7	Retry strategy.....	79
8.4.8	Management service.....	79
8.4.9	Radio link quality and channel condition measurement	79
8.4.10	Security	80
8.4.11	Country code	80
8.4.12	DLSL state machine	80
8.5	Data link sub-layer data services	86
8.5.1	General	86
8.5.2	DLDE-DATA.request.....	86
8.5.3	DLDE-DATA.confirm	87
8.5.4	DLDE-DATA.indication	88
8.5.5	Time sequence of DLSL data service	89
8.6	Data link sub-layer management services	90
8.6.1	General	90
8.6.2	Network discovery services	90
8.6.3	Device joining services	92
8.6.4	Device leaving services	94
8.6.5	DLME-CHANNEL-CONDITION.indication.....	96
8.6.6	DLME-NEIGHBOUR-INFO.indication	96
8.6.7	DLME-COMM-STATUS.indication	97
8.6.8	Keep-alive services	97

8.6.9	Time synchronization services	98
8.7	DLSL frame formats	99
8.7.1	General frame format.....	99
8.7.2	Date frame format.....	100
8.7.3	Command frame format	100
9	Network layer	102
9.1	General.....	102
9.2	Protocol stack	102
9.3	Function description.....	103
9.3.1	General	103
9.3.2	Addressing	103
9.3.3	Routing.....	104
9.3.4	Packet lifecycle management	104
9.3.5	Joining and leaving network of device.....	104
9.3.6	End-to-end network performance monitoring.....	105
9.3.7	Fragmentation and reassembly	105
9.3.8	Network layer state machine	105
9.4	Network layer data services	110
9.4.1	General	110
9.4.2	NLDE-DATA.request.....	110
9.4.3	NLDE-DATA.confirm	111
9.4.4	NLDE-DATA.indication	111
9.4.5	Time sequence of NL data services	112
9.5	Network layer management services	112
9.5.1	General	112
9.5.2	Network communication status report services	112
9.5.3	Network joining services	115
9.5.4	Networkleaving services	120
9.5.5	Cluster member report services	124
9.5.6	Neighbour information report services	126
9.5.7	Route allocation services.....	128
9.5.8	Communication resource allocation services.....	134
9.5.9	Aggregation and disaggregation services.....	150
9.5.10	Device status report services.....	151
9.5.11	Channel condition report services	153
9.5.12	Failure path report services	155
9.5.13	Network attribute getting services	156
9.5.14	Network attribute setting services	160
9.6	Network layer packet formats.....	163
9.6.1	Common packet format.....	163
9.6.2	Data packet format	164
9.6.3	Aggregated packet format.....	165
9.6.4	Command packet format.....	165
10	Application layer	182
10.1	Overview.....	182
10.1.1	General	182
10.1.2	AL structure	182
10.1.3	Functions of UAP.....	182
10.1.4	Functions of ASL	183

10.2	UAP	183
10.2.1	General	183
10.2.2	UAO	183
10.2.3	Method definition	184
10.3	Application sub-layer	188
10.3.1	General	188
10.3.2	Application sub-layer data entity	188
10.4	Application sub-layer packet formats	193
10.4.1	General	193
10.4.2	ASL general packet format	193
10.4.3	Packet formats	195
11	Security	196
11.1	General	196
11.2	Security management framework	197
11.3	Secure communication protocol stack	198
11.3.1	General	198
11.3.2	Data link sub-layer security	199
11.3.3	Application sub-layer security	200
11.4	Key management	201
11.4.1	Key type	201
11.4.2	Key distribution	202
11.4.3	Key update	202
11.4.4	Key status	202
11.5	Secure joining process	203
11.5.1	Secure joining process of a new WIA-PA device	203
11.5.2	Device security material getting services	204
11.6	Secure transportation	211
11.6.1	Process of secure transportation from field device to host configuration computer	211
11.6.2	Process of secure transportation from host configuration computer to field device	212
Annex A (informative)	Security strategy for WIA-PA network	213
A.1	Risk analysis for WIA-PA network	213
A.2	Security principles for WIA-PA network	213
A.3	Security objectives for WIA-PA network	213
A.4	Graded and layered security system	213
Annex B (informative)	Format description	215
B.1	Time sequence diagram	215
B.2	Packet or frame format	215
Annex C (informative)	Example of UAO	217
C.1	General	217
C.2	Analog input object	217
C.2.1	Overview	217
C.2.2	Class attribute of AIO	217
C.2.3	Instance attribute of AIO	217
Annex D (informative)	Country-specific and region-specific provisions	219
Annex E (informative)	Regional modification for compliance with ETSI standards	220
E.1	General	220
E.2	Compliance with EN 300 440-2 V1.4.1	220

E.3 Compliance with EN 300 328 V1.8.1	220
Bibliography.....	222
Figure 1 – Example of WIA-PA physical topology (combination of star and mesh).....	23
Figure 2 – Example of WIA-PA physical topology (star-only)	23
Figure 3 – OSI basic reference model mapped to WIA-PA	24
Figure 4 – The architecture of WIA-PA gateway	25
Figure 5 – DMAP in system management.....	26
Figure 6 – Hybrid centralized and distributed system management scheme	28
Figure 7 – Joining process of routing device through the gateway device.....	29
Figure 8 – Joining process of routing device through an online routing device	30
Figure 9 – Joining process of field device through a gateway device.....	31
Figure 10 – Joining process of field device through a routing device	31
Figure 11 – Long address structure of device.....	31
Figure 12 – Short address structure of routing device	32
Figure 13 – Short address structure of field device	32
Figure 14 – An example of resource allocation.....	35
Figure 15 – Allocation process of routing device's communication resources	36
Figure 16 – Allocation process of field device's communication resources	38
Figure 17 – Example of aggregation and disaggregation	42
Figure 18 – Process of path failure report	45
Figure 19 – Device status report process of field device	45
Figure 20 – Device status report process of routing device	46
Figure 21 – Process of channel condition report	46
Figure 22 – Active leaving process of routing device	47
Figure 23 – Passive leaving process of routing device	47
Figure 24 – Active leaving process of field device (leaving from gateway device).....	48
Figure 25 – Active leaving process of field device (leaving from routing device).....	48
Figure 26 – Passive leaving process of field device (leaving from gateway device)	49
Figure 27 – Passive leaving process of field device (leaving from routing device)	49
Figure 28 – WIA-PA DLL protocol stack	69
Figure 29 – WIA-PA DLSL reference model	75
Figure 30 – WIA-PA superframe	76
Figure 31 – R1, R2 and R3 superframe structures	78
Figure 32 – An example of long cycle data transmission	79
Figure 33 – DLSL state machine for device joining.....	81
Figure 34 – DLSL state machine for in-network running	83
Figure 35 – Time sequence of data service.....	89
Figure 36 – Time sequence of network discovery	92
Figure 37 – General frame format	99
Figure 38 – WIA-PA network layer protocol stack.....	102
Figure 39 – WIA-PA network layer reference model	103
Figure 40 – Network layer state machine	105

Figure 41 – Time sequence of NL data services	112
Figure 42 – Time sequence for field device joining through routing device	118
Figure 43 – One-hop joining process for routing device.....	119
Figure 44 – Multi-hop join process of routing device	119
Figure 45 – Active leaving process of field device (leaving routing device).....	122
Figure 46 – Passive leaving of field device	122
Figure 47 – Active leaving process of routing device	123
Figure 48 – Passive leaving process of routing device	123
Figure 49 – Cluster member reporting process.....	126
Figure 50 – Neighbour information reporting process	128
Figure 51 – Time sequence for route adding	130
Figure 52 – Time sequence for route updating	132
Figure 53 – Time sequence for route deleting	134
Figure 54 – Adding a link originating from gateway device to routing device	137
Figure 55 – Adding a link originating from routing device to field device.....	137
Figure 56 – Updating a link originating by gateway device to routing device.....	139
Figure 57 – Updating a link originating from routing device to field device.....	140
Figure 58 – Releasing a link originating from gateway device to routing device.....	142
Figure 59 – Releasing a link originating from routing device to field device	142
Figure 60 – Adding a superframe originating from gateway device to routing device	144
Figure 61 – Adding a superframe originating from routing device to field device.....	144
Figure 62 – Updating a superframe originating from gateway device to routing device	146
Figure 63 – Updating a superframe originating from routing device to field device	147
Figure 64 – Releasing a superframe originating from gateway device to routing device.....	149
Figure 65 – Releasing a superframe originating from routing device to field device	149
Figure 66 – Device status reporting process from field device to routing device	152
Figure 67 – Device status reporting process from routing device to gateway device.....	153
Figure 68 – Channel condition reporting process from field device to routing device	154
Figure 69 – Channel condition reporting process from routing device to gateway device	155
Figure 70 – Failure path reporting process.....	156
Figure 71 – AL structure	182
Figure 72 – User application process	183
Figure 73 – C/S communication process	191
Figure 74 – P/S communication process (disable aggregation function)	192
Figure 75 – P/S communication process (enable aggregation function).....	192
Figure 76 – R/S communication process	193
Figure 77 – Security management framework of WIA-PA network	197
Figure 78 – Security communication protocol stack.....	199
Figure 79 – Key lifecycle.....	202
Figure 80 – Secure joining process of WIA-PA device.....	203
Figure 81 – Time sequence for field device joining (field device to routing device)	207
Figure 82 – Time sequence for field device joining (routing device to gateway device).....	208
Figure 83 – One-hop joining process for routing device.....	209

Figure 84 – Multi-hop join process of routing device (new routing device to routing device).....	210
Figure 85 – Multi-hop join process of routing device (routing device to gateway device)	211
Figure B.1 – Time sequence diagram.....	215
Table 1 – Definition of data types.....	22
Table 2 – Protocol support for VCR.....	33
Table 3 – Relations between VCR and aggregation function	39
Table 4 – Format of aggregated data followed by field device's DAGO.....	41
Table 5 – Format of aggregated packet followed by routing device's PAGO	41
Table 6 – DAGO class attributes	43
Table 7 – DAGO instance attributes	43
Table 8 – MEM_STRUCT structure	44
Table 9 – PAGO class attributes	44
Table 10 – PAGO instance attributes	44
Table 11 – DGO class attributes	44
Table 12 – DGO instance attributes	45
Table 13 – Unstructured attributes (1 of 5).....	50
Table 14 – Structured attributes.....	55
Table 15 – NLRoute_Struct structure	56
Table 16 – Superframe_Struct structure.....	56
Table 17 – Link_Struct structure	57
Table 18 – Neighbour_Struct structure	58
Table 19 – ChanCon_Struct structure	58
Table 20 – Device_struct structure (1 of 3)	59
Table 21 – VCR_Struct structure.....	61
Table 22 – DevConRep_Struct structure	62
Table 23 – Key_Struct structure.....	62
Table 24 – ObjList_Struct structure	62
Table 25 – DMAP-MIB-GET.request parameters	63
Table 26 – DMAP-MIB-GET.confirm parameters	64
Table 27 – DMAP-MIB-SET.request parameters	64
Table 28 – DMAP-MIB-SET.confirm parameters.....	65
Table 29 – PHY protocol selection	66
Table 30 – Frequency band and data rate	67
Table 31 – Frequency assignments.....	67
Table 32 – PHY PIB attributes (1 of 2)	68
Table 33 – MAC protocol selection (1 of 2)	71
Table 34 – MAC PIB attributes.....	73
Table 35 – MAC extended PIB attributes.....	73
Table 36 – Beacon payload.....	74
Table 37 – Format of Capability Information field	74
Table 38 – Hopping mechanisms	77

Table 39 – DLSL state transitions for device joining	82
Table 40 – DLSL state transitions for in-network running (1 of 3)	83
Table 41 – DLDE-DATA.request parameters	87
Table 42 – DLDE-DATA.confirm parameters	88
Table 43 – Status table	88
Table 44 – DLDE-DATA.indication parameters	89
Table 45 – DLME-DISCOVERY.request parameters	90
Table 46 – DLME- DISCOVERY.confirm parameters	91
Table 47 – Network descriptor list	91
Table 48 – DLME-JOIN.request parameters	93
Table 49 – DLME-JOIN.indication parameters	93
Table 50 – DLME-JOIN.response parameters	94
Table 51 – DLME-JOIN.confirm parameters	94
Table 52 – DLME-LEAVE.request parameters	95
Table 53 – DLME-LEAVE.indication parameters	95
Table 54 – DLME-LEAVE.confirm parameters	95
Table 55 – DLME-CHANNEL-CONDITION.indication parameters	96
Table 56 – DLME-NEIGHBOUR-INFO.indication parameters	96
Table 57 – DLME-COMM-STATUS.indication parameters	97
Table 58 – DLME -KEEP-LIVE.confirm parameters	98
Table 59 – DLME -KEEP-LIVE.indication parameters	98
Table 60 – DLME-TIME-SYN.request parameters	98
Table 61 – DLME -TIME-SYN.confirm parameters	99
Table 62 – DLME-TIME-SYN.indication parameters	99
Table 63 – DLSL frame control field	100
Table 64 – Date frame format	100
Table 65 – General command frame format	100
Table 66 – DLSL command frame	101
Table 67 – Format of keep-alive command frame	101
Table 68 – Format of time synchronization command frame	102
Table 69 – Example of a routing table	104
Table 70 – NL state transitions (1 of 4)	106
Table 71 – NLDE-DATA.request parameters	111
Table 72 – NLDE-DATA.confirm parameters	111
Table 73 – NLDE-DATA.indication parameters	112
Table 74 – NLME-COMM-STATUS.request parameters	113
Table 75 – NLME-COMM-STATUS.indication parameters	114
Table 76 – NLME-COMM-STATUS.confirm parameters	114
Table 77 – NLME-JOIN.request parameters	115
Table 78 – NLME-JOIN.indication parameters	116
Table 79 – NLME-JOIN.response parameters	116
Table 80 – NLME-JOIN.confirm parameters	117
Table 81 – NLME-LEAVE.request parameters	120

Table 82 – NLME-LEAVE.indication parameters	120
Table 83 – NLME-LEAVE.response parameters	121
Table 84 – NLME-LEAVE.confirm parameters	121
Table 85 – NLME-RPT-CLRMEM.request parameters	124
Table 86 – NLME-RPT-CLRMEM.confirm parameter	124
Table 87 – NLME-RPT-CLRMEM.response parameters	125
Table 88 – NLME-NEIGHBOUR-INFO.request parameters	126
Table 89 – NLME-NEIGHBOUR-INFO.confirm parameter	127
Table 90 – NLME-ADD_ROUTE.request parameters	128
Table 91 – NLME-ADD_ROUTE.confirm parameters	129
Table 92 – NLME-UPDATE_ROUTE.request parameters	130
Table 93 – NLME-UPDATE_ROUTE.confirm parameter	131
Table 94 – NLME-UPDATE_ROUTE.request parameters	132
Table 95 – NLME-DELETE_ROUTE.confirm parameters	133
Table 96 – NLME-ADD-LINK.request parameters	135
Table 97 – NLME-ADD-LINK.confirm parameters	136
Table 98 – NLME-UPDATE-LINK.request parameters	138
Table 99 – NLME-UPDATE-LINK.confirm parameters	138
Table 100 – NLME-RELEASE-LINK.request parameters	140
Table 101 – NLME-RELEASE-LINK.confirm parameters	141
Table 102 – NLME-ADD-SFR.request parameters	143
Table 103 – NLME-ADD-SFR.confirm parameters	143
Table 104 – NLME-UPDATA-SFR.request parameters	145
Table 105 – NLME-UPDATE-SFR.confirm parameters	145
Table 106 – NLME-RELEASE-SFR.request parameters	147
Table 107 – NLME-RELEASE-SFR.confirm parameters	148
Table 108 – NLME-AGG.indication parameters	150
Table 109 – NLME-AGO-SEND.request parameters	150
Table 110 – NLME-DAG.indication parameter	151
Table 111 – NLME-DEVICE -STATUS.request parameters	151
Table 112 – NLME-DEVICE -STATUS.indication parameters	152
Table 113 – NLME-DEVICE -STATUS.confirm parameter	152
Table 114 – NLME-CHANNEL-CONDITION.request parameters	153
Table 115 – NLME-CHANNEL-CONDITION.indication parameters	154
Table 116 – NLME-CHANNEL-CONDITION.confirm parameter	154
Table 117 – NLME-PATH_FAILURE.request parameters	155
Table 118 – NLME-PATH_FAILURE.indication parameters	156
Table 119 – NLME-PATH_FAILURE.confirm parameters	156
Table 120 – NLME-INFO_GET.request parameters	157
Table 121 – NLME-INFO_GET.indication parameters	158
Table 122 – NLME-INFO_GET.response parameters	159
Table 123 – NLME-INFO_GET.confirm parameters	160
Table 124 – NLME-INFO_SET.request parameters	161

Table 125 – NLME-INFO_SET.indication parameters	161
Table 126 – NLME-SET.response parameters	162
Table 127 – NLME-SET.confirm parameters	163
Table 128 – Network layer common packet format	163
Table 129 – Control field format	163
Table 130 – Network layer data packet format	164
Table 131 – Aggregated packet format	165
Table 132 – Format of NL command packet	166
Table 133 – Network layer command packet	166
Table 134 – Execution results of commands	167
Table 135 – Format of joining request packet	167
Table 136 – Format of joining response packet	168
Table 137 – Format of communication status report request packet	168
Table 138 – Format of leaving request packet	169
Table 139 – Value of Leaving reason	169
Table 140 – Format of leaving response packet	169
Table 141 – Format of cluster member report request packet	169
Table 142 – Format of cluster member report response packet	170
Table 143 – Format of neighbour information report request packet	170
Table 144 – Format of route adding request packet	171
Table 145 – Format of route adding response packet	171
Table 146 – Format of route update request packet	171
Table 147 – Format of route update response packet	172
Table 148 – Format of route deleting request packet	172
Table 149 – Format of route deleting response packet	172
Table 150 – Format of link adding request packet	173
Table 151 – Format of link adding response packet	173
Table 152 – Format of link update request packet	174
Table 153 – Format of link update response packet	174
Table 154 – Format of link release request packet	175
Table 155 – Format of link release response packet	175
Table 156 – Format of superframe adding request packet	175
Table 157 – Format of superframe adding response packet	176
Table 158 – Format of superframe update request packet	176
Table 159 – Format of superframe update response packet	177
Table 160 – Format of superframe release request packet	177
Table 161 – Format of superframe release response packet	177
Table 162 – Format of device condition report request packet	178
Table 163 – Format of device condition information field	178
Table 164 – Format of channel condition report request packet	179
Table 165 – Format of channel quality information field	179
Table 166 – Format of path failure report request packet	179
Table 167 – Format of attribute getting request packet	180

Table 168 – Format of attribute getting response packet.....	180
Table 169 – Format of attribute setting request packet.....	181
Table 170 – Format of attribute setting response packet	181
Table 171 – UAO method definition.....	185
Table 172 – Request format of READ method	185
Table 173 – Response format of READ method	185
Table 174 – Request format of WRITE method	186
Table 175 – Response format of WRITE method.....	186
Table 176 – Format of PUBLISH method	187
Table 177 – Format of REPORT method	187
Table 178 – Format of REPORT ACK method	187
Table 179 – ASLDE-DATA.request parameters	189
Table 180 – ASLDE-DATA.confirm parameters	189
Table 181 – ASLDE-DATA.indication parameters.....	190
Table 182 – ASLDE-AGG.request parameters	190
Table 183 – ASLDE-DAG.indication parameters	191
Table 184 – Application sub-layer general packet format	193
Table 185 – Packet control field format.....	194
Table 186 – Packet type subfield value.....	194
Table 187 – ASL data packet format	195
Table 188 – ASL acknowledgement packet format	196
Table 189 – Format of security DLPDU	199
Table 190 – Format of DLSSL security header	200
Table 191 – Structure of security control field in DLSSL security header.....	200
Table 192 – Structure of security material control field in DLSSL security header.....	200
Table 193 – Security APDU structure	201
Table 194 – Structure of ASL security header field	201
Table 195 – DLME-SEC.request parameters.....	204
Table 196 – DLME-SEC.indication parameters.....	204
Table 197 – DLME-SEC.response parameters	205
Table 198 – DLME-SEC.confirm parameters	206
Table A.1 – Graded and layered security measures for WIA-PA network.....	214
Table A.2 – Security levels of data packets.....	214
Table B.1 – Packet or frame format in octet(s)	215
Table B.2 – Subfield format in bit(s).....	216
Table C.1 – AIO class attribute	217
Table C.2 – AIO instance attributes	218
Table E.1 – Applicable EN 300 440-2 requirements list	220
Table E.2 – Applicable EN 300 328 requirements list	220
Table E.3 – Timeslot timing definitions and calculations.....	221

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL NETWORKS –
WIRELESS COMMUNICATION NETWORK
AND COMMUNICATION PROFILES –
WIA-PA****FOREWORD**

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

International Standard IEC 62601 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2011. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- changed IEEE STD 802.15.4-2006 to IEEE STD 802.15.4-2011 and added common modification for IEEE STD 802.15.4-2011 MAC profile, PHY profile and IEEE STD 802.15.4-2011 related references;
- added common modifications for regional adoption and added Annex D and Annex E;

- deleted extended MAC management services and added two DLSL management services;
- added specific state machines for DLSL and NL;
- unified representation of frame format and packet format;
- changed format of definition of data types;
- added detailed description of technologies for clearer understanding;
- provided support for CCA modes 1, 2, and 3.

The reader's attention is drawn to the fact that Annex E lists all of the “in-some-country” clauses on differing practices of a less permanent nature relating to the subject of this standard.

The text of this standard is based on the following documents:

FDIS	Report on voting
65C/821/FDIS	65C/833/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INDUSTRIAL NETWORKS – WIRELESS COMMUNICATION NETWORK AND COMMUNICATION PROFILES – WIA-PA

1 Scope

This International Standard specifies the system architecture and the communication protocol of Wireless networks for Industrial Automation – Process Automation (WIA-PA) that is built on IEEE STD 802.15.4-2011.

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.

ISO/IEC 9899, *Information technology – Programming languages – C*

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*

IEEE STD 802.15.4-2011, *IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

3.1.1

absolute timeslot number

number of timeslots from the start of the network, generally denoting the current timeslot

3.1.2

active leaving

process by which an online field device is allowed to leave the network through applying to its routing device or by which an online routing device is allowed to leave the network through applying to the gateway device

3.1.3

adaptive frequency hopping

change of communication channels according to actual condition of channels in every timeslot during the intra-cluster period of WIA-PA superframe

3.1.4

adaptive frequency switch

change of communication channels according to the actual condition of channels during the beacon frame and active period in a superframe cycle, and using different channels in different superframe cycles

3.1.5

aggregation

merging of data from multiple user application objects or merging of several packets from cluster members into one packet

3.1.6

application sub-layer

protocol sub-layer that provides data and management services for the application layer

3.1.7

beacon

special frame broadcast by the routing devices or the gateway device in the WIA-PA network

3.1.8

broadcast

sending one packet to all WIA-PA devices simultaneously

3.1.9

channel

RF medium used to convey a packet from a sender to a receiver

3.1.10

cluster

logical group of devices that is comprised of a routing device and field devices

3.1.11

clusterhead

manager in a cluster, performed by the routing device

3.1.12

clustermember

data source in a cluster, performed by a field device

3.1.13

coexistence

ability of one network to perform its task in a given shared environment without disturbing or being disturbed by other networks

Note 1 to entry: These networks may or may not have the same set of rules.

3.1.14

communication resource

channels and timeslots used to transport a frame

3.1.15

WIA-PA configuration software

software tool for configuring a WIA-PA network and devices

3.1.16

data link sub-layer

upper layer of the IEEE STD 802.15.4-2011 MAC layer, used to handle the aspects of network topology and communication resources in the WIA-PA network

3.1.17

disaggregation

dividing the merged packet into data of user application objects

3.1.18**field device**

device usable in the field, which is connected to or controls the process

3.1.19**frame**

format of aggregated bits from the medium access control (MAC) entity that are transmitted together in time

[SOURCE: IEEE STD 802.15.4-2011]

3.1.20**frequency hopping**

change of transmitting/receiving frequency to combat interference and fading

3.1.21**gateway device**

device connecting the WIA-PA network to other plant networks

3.1.22**handheld device**

portable device used for provisioning, firmware updating, and device status monitoring

3.1.23**hop**

movement of a packet directly between two adjacent neighbour devices in one network transaction without the participation of any other devices in the WIA-PA network

Note 1 to entry: Multiple hops are used to lengthen the transmission distance, bypass interference sources or avoid obstructions.

3.1.24**host configuration computer**

device through which users and maintenance/management personnel perform transactions on the WIA-PA network and the management networks

3.1.25**interconnectable**

using the same communication protocols, communication interface and data access

3.1.26**interoperable**

able to work together to perform a specific role in one or more distributed application programs

Note 1 to entry: In this case parameters and their application-related functionality fit together both syntactically and semantically. Interoperability is achieved when the devices support complementary sets of parameters and functions belonging to the same profile.

3.1.27**interoperability**

ability of two or more network systems to exchange information and to make mutual use of the information that has been exchanged

[SOURCE: ISO/IEC TR 10000-1:1998, 3.2.1 modified by replacing “IT systems” with “network systems”]

3.1.28

joining

process by which a WIA-PA device is authenticated and allowed to participate in the WIA-PA network

3.1.29

link

set of communication parameters necessary to transport a frame between adjacent devices in the network

Note 1 to entry: It includes source/destination address, timeslot, channel, direction, and link type.

3.1.30

mesh

topology formed by routing devices and the gateway device in the WIA-PA network

Note 1 to entry: One routing device may connect to the gateway device and to more than one other routing device.

3.1.31

multicast

sending one packet to a group of WIA-PA devices simultaneously

3.1.32

network address

short address

16-bit unsigned integer uniquely identifying the device in the WIA-PA network

Note 1 to entry: The most significant 8 bits of the network address, assigned by the network manager, identify different clusters.

3.1.33

network manager

logical role for configuring the network, allocating the communication resources, managing the routing tables, and monitoring and reporting the health of the network

3.1.34

packet

formatted, aggregated bits that are transmitted together in time across the physical medium

[SOURCE: IEEE STD 802.15.4-2011, 3.31]

3.1.35

packet lifecycle

maximal packet survival time from being generated to being dropped

3.1.36

passive leaving

process by which an online field device is instructed by its routing device to leave the network or by which an online routing device is instructed by the gateway device to leave the network

3.1.37

physical address

long address

EUI-64 bits uniquely identifying the device in the WIA-PA network

Note 1 to entry: A physical address is assigned by a manufacturer.

3.1.38

routing device

device forwarding packets from one WIA-PA device to another in the WIA-PA network

3.1.39**security manager**

logical role for configuring the security strategies of the whole network, managing keys, and authenticating devices

3.1.40**superframe**

collection of timeslots repeating over time

Note 1 to entry: It specifies the transmitting or receiving time of periodic communication.

3.1.41**timeslot**

basic time unit of data exchange

Note 1 to entry: Its duration is configurable in the WIA-PA network.

3.1.42**timeslot hopping**

regular change of transmitting/receiving frequency per timeslot to avoid interference and fading

3.1.43**unicast**

sending one packet to a single device in the WIA-PA network

3.1.44**virtual communication relation**

communication paths and communication resources between two user application objects

3.1.45**WIA-PA device**

device in the WIA-PA network

EXAMPLE: Host configuration computer, gateway device, routing device, field device or handheld device.

3.2 Abbreviations

ACK	Acknowledge
AFH	Adaptive Frequency Hopping
AFS	Adaptive Frequency Switch
AIO	Analog Input Object
AL	Application Layer
AOO	Analog Output Object
ASDU	Application Service Data Unit
ASL	Application Sub-Layer
ASLDE	Application Sub-Layer Data Entity
ASLDE-SAP	ASLDEService Access Point
ASLME	Application Sub-Layer Management Entity
ASLME-SAP	ASLMEService Access Point
ASLPDU	Application Sub-Layer Protocol Data Unit
ASN	Absolute timeSlot Number
CAP	Contention Access Period
CFP	ContentionFree Period

C/S	Client/Server
CSMA	Carrier Sense Multiple Access
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
DAGO	Data AggreGation Object
DGO	DisaGgregation Object
DIO	Digital Input Object
DLDE	Data Link Sub-Layer Data Entity
DLDE-SAP	DLDE Service Access Point
DLL	Data Link Layer
DLME	Data Link Sub-Layer Management Entity
DLME-SAP	DLME Service Access Point
DLPDU	Data Link Sub-Layer Protocol Data Unit
DLSL	Data Link Sub-Layer
DMAP	Device Management Application Process
DOO	Digital Output Object
EIRP	Equivalent Isotropic Radiated Power
ENC	ENCryption
EUI-64	Extended Unique Identifier-64 bits
FCS	Frame Check Sequence
FDMA	Frequency Division Multiple Access
FFD	Full-Function Device
FH	Frequency Hopping
GTS	Guaranteed Time Slot
GW	GateWay device
ID	IDentifier
IDS	Intrusion Detection System
KED	Data Encryption Key
KEK	Key Encryption Key
KJ	Join Key
KS	Share Key
LME-SAP	Layer Management Entity Service Access Point
LSB	Least Significant Bit
LQI	Link Quality Indication
MAC	Medium Access Control sub-layer
MCPS	MAC Common Part Sub-layer
MHR	Medium Access Control Header
MIB	Management Information Base
MIC	Message Integrity Code
MLDE	MAC sub-Layer Data Entity
MLDE-SAP	MLDE Service Access Point
MLME	MAC sub-Layer Management Entity
MLME-SAP	MLME Service Access Point
MPDU	MAC Protocol Data Unit

MSB	Most Significant Bit
NL	Network Layer
NLDE	Network Layer Data Entity
NLDE-SAP	NLDE Service Access Point
NLME	Network Layer Management Entity
NLME-SAP	NLME Service Access Point
NM	Network Manager
NPDU	Network Protocol Data Unit
NSDU	Network Service Data Unit
PAGO	Packet AGgregation Object
PAN	Personal Area Network
PHY	PHYsical layer
PIB	PAN Information Base
P/S	Publisher/Subscriber
RFD	Reduced-Function Device
R/S	Report source/Sink
SAP	Service Access Point
SM	Security Manager
TDMA	Time Division Multiple Access
TH	Timeslot Hopping
UAO	User Application Object
UAP	User Application Process
UAPME-SAP	UAP Management Entity SAP
UTC	Universal Time Coordinated
VCR	Virtual Communication Relationship
VCR_ID	Virtual Communication Relationship IDentifier
WIA-PA	Wireless network for Industrial Automation – Process Automation

4 Definition of data types

Table 1 gives the WIA-PA definition of data types.

Table 1 – Definition of data types

Definition of data types (see ISO/IEC 9899)			
Data type		Range of values	Length
Boolean	Boolean	Non 0: TRUE; 0: FALSE	1 octet
Unsigned integer	Unsigned8	$0 \leq i \leq 2^8-1$	1 octet
	Unsigned16	$0 \leq i \leq 2^{16}-1$	2 octets
	Unsigned24	$0 \leq i \leq 2^{24}-1$	3 octets
	Unsigned32	$0 \leq i \leq 2^{32}-1$	4 octets
	Unsigned40	$0 \leq i \leq 2^{40}-1$	5 octets
	Unsigned48	$0 \leq i \leq 2^{48}-1$	6 octets
	Unsigned64	$0 \leq i \leq 2^{64}-1$	8 octets
Octet string	Octetstring	8-bit string	1 octet
Float	Float	See IEC 60559	4 octets

5 WIA-PA overview

5.1 Device types

The document specifies five types of WIA-PA devices:

- a) host configuration computer;
- b) gateway device(GW);
- c) routing device;
- d) field device; and
- e) handheld device.

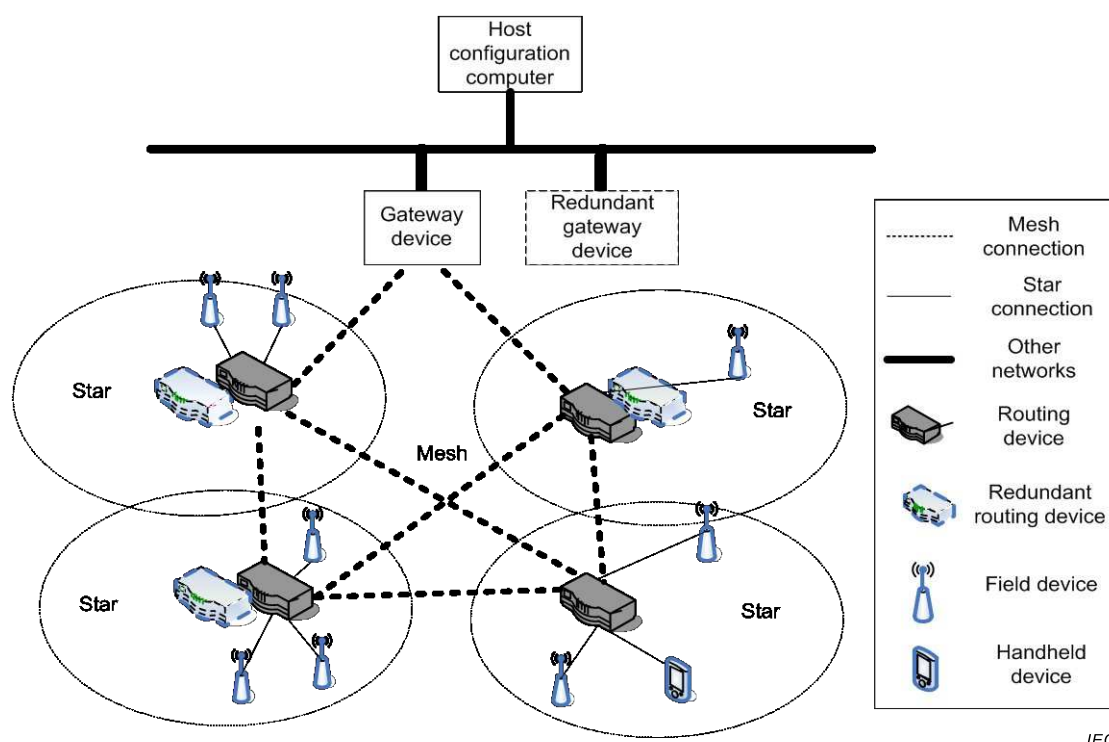
To improve reliability, there may be redundant gateway devices and redundant routing devices in the WIA-PA network. A primary device connects its redundant device in the wired manner. The wired connection is not defined in this document. The short address (see 6.3.4) of a redundant device is the same as that of its primary device. The start-up time of a redundant device is not later than that of the primary device. When primary devices run, redundant devices do not start up their radio modules. When the information of primary devices is changed, the primary devices should backup in timely manner the changed information to their redundant devices in the wired manner. The wired manner is not specified in this document. If SecEnableFlag is enabled, the redundant devices are authenticated (see 11.2).

5.2 Network topology

WIA-PA network supports two different types of network topologies:

- a) a hierarchical network topology that combines star and mesh, and
- b) a star-only network topology.

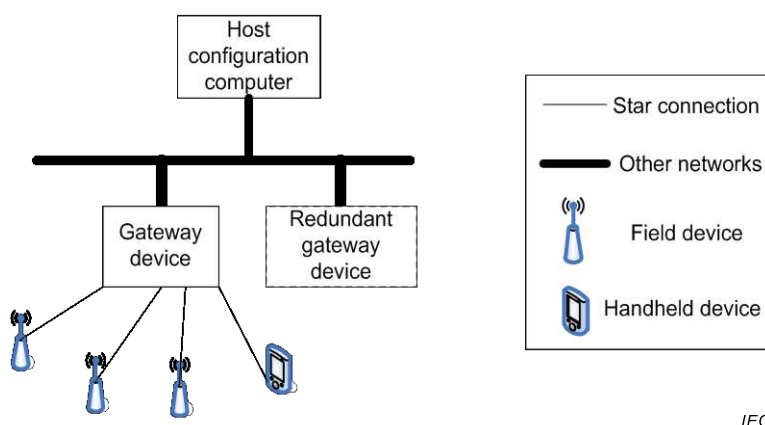
The hierarchical network topology that combines star and mesh is illustrated in Figure 1. The first level of the network is in mesh topology, where routing devices and gateway devices are deployed. The second level of the network is in star topology, where routing devices, field devices, and handheld devices (if they exist) are deployed.



IEC

Figure 1 – Example of WIA-PA physical topology (combination of star and mesh)

The star-only network is comprised of a gateway device, field devices, and handheld devices (if they exist). The star network topology is illustrated in Figure 2.



IEC

Figure 2 – Example of WIA-PA physical topology (star-only)

The star-only network is a special case of the hierarchical network. In this document, the specification of the hierarchical network covers the star-only network. Therefore, there is no explicit specification provided for the star-only network.

In order to facilitate management, this document specifies five kinds of logical roles.

a) Gateway

Gateway handles protocol-translation and data-mapping between the WIA-PA network and other networks.

b) Network manager

Network Manager (NM) manages and monitors the entire network (see 6.2). There should be one and only one network manager per WIA-PA network.

c) Security manager

Security Manager (SM) deals with security key management and security authentication of gateway devices, routing devices, field devices, and handheld devices (if they exist).

d) Cluster head

Cluster head manages and monitors field devices and handheld devices (if they exist). Cluster head also merges and securely forwards packets from local cluster members and other cluster heads.

e) Cluster member

Cluster member collects field data and sends the data to its cluster head.

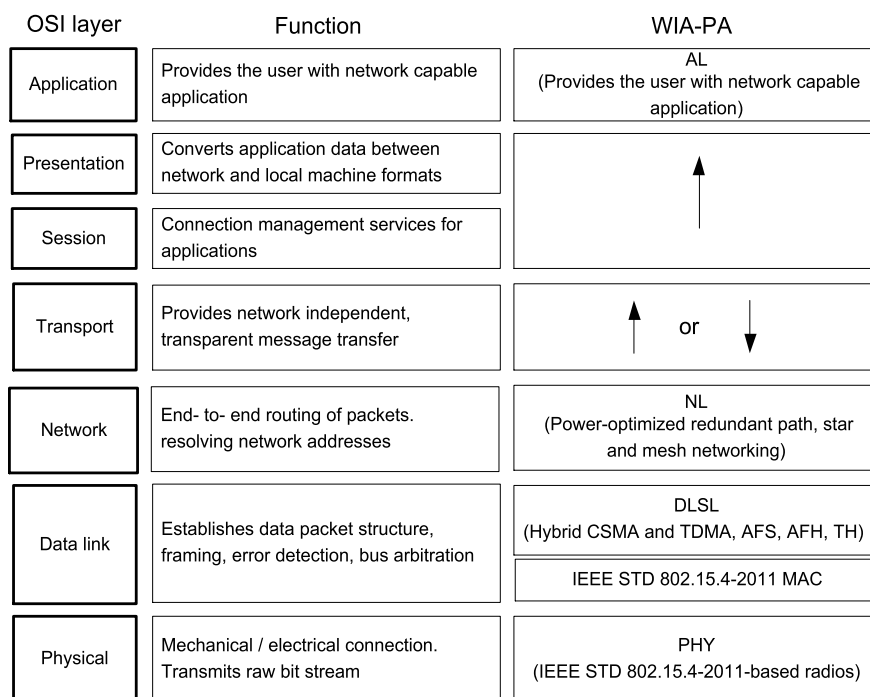
The NM and the SM that are used for system management should reside in a gateway device.

One physical device may perform the functions of several logical roles. In the hierarchical network that combines star and mesh, a gateway device may perform the logical roles of gateway, NM, SM, and cluster head. A routing device should act as a cluster head. A field device/handheld device should only act as a cluster member.

The primary device and the redundant device are marked by the parameter RedundantDevFlag in Table 20.

5.3 Protocol architecture

The WIA-PA protocol architecture, which is illustrated in Figure 3, is based on ISO/IEC 7498-1. The WIA-PA protocol architecture defines the Data Link Sub-Layer (DLSL), Network Layer (NL) and Application Layer (AL), while its PHYSical layer (PHY) and Medium Access Control sub-layer (MAC) are based on IEEE Std 802.15.4-2011.



IEC

Figure 3 – OSI basic reference model mapped to WIA-PA

5.4 Interconnection

The WIA-PA network interconnects with other networks through the WIA-PA gateway. Besides the communication to the WIA-PA NM and SM, the WIA-PA gateway may communicate with other WIA-PA devices in order to exchange information between devices. Meanwhile, the WIA-PA gateway may connect other networks, such as wired fieldbuses. The architecture of the WIA-PA gateway is shown in Figure 4.

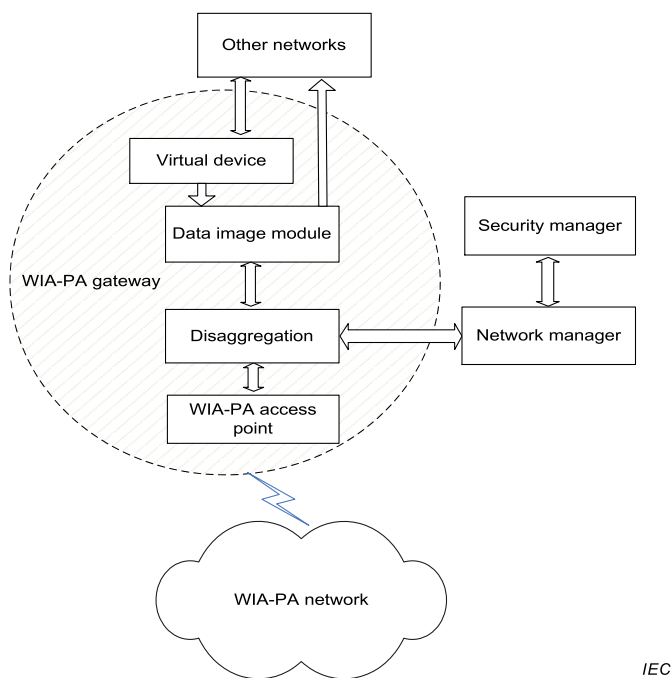


Figure 4 – The architecture of WIA-PA gateway

The WIA-PA gateway includes the following components.

a) WIA-PA access point

The WIA-PA access point realizes the physical connections of the WIA-PA network and transmission of the management information and data.

b) Virtual device

The virtual device defines a communication interface for other networks. The interface is used to map a data source from other networks into a WIA-PA device in order to fulfil communication between the WIA-PA network and other networks.

c) Disaggregation object

This object is used to disaggregate the packets that are aggregated within routing devices and field devices.

d) Data image module

The data image module stores the data of devices in the WIA-PA network and provides an access interface for other networks.

The virtual device and the data image module are optional and implementation-specific, which are not defined in this document.

6 System management

6.1 General

The system management in the WIA-PA network includes both network management and security management. The functions of system management are implemented by the Device Management Application Process (DMAP) in each device. The DMAP, as a system management entity, includes the network management module, the security management module, and the Management Information Base (MIB) module. DMAP is shown as the grey area in Figure 5. The white blocks within the grey area are the function components in the DMAP.

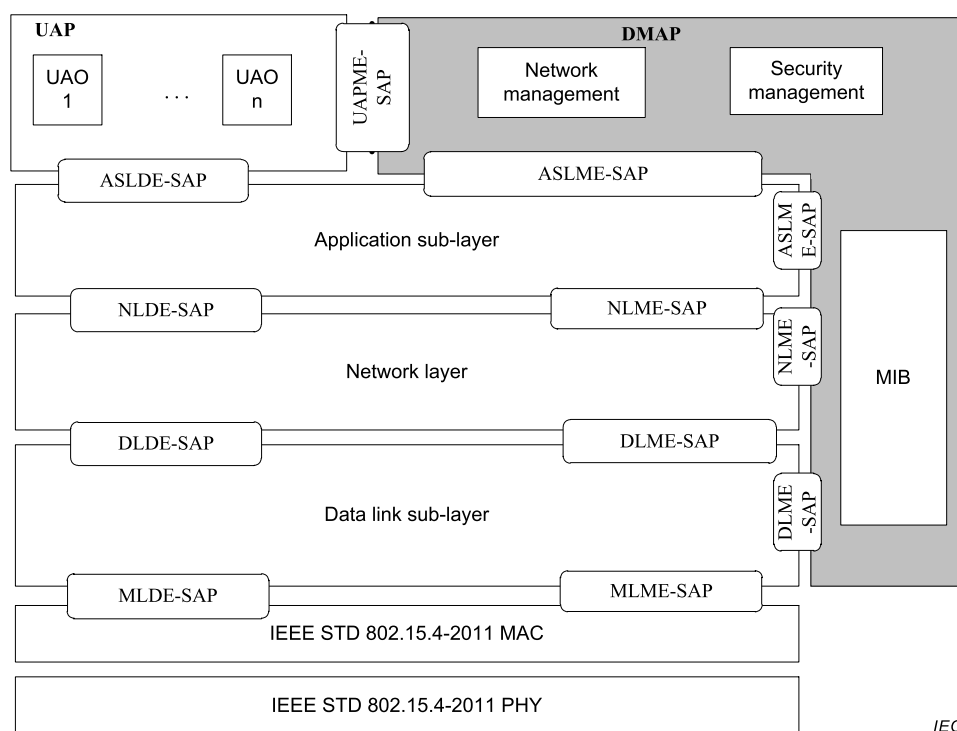


Figure 5 – DMAP in system management

The network management specifies the management of device attributes and attributes that are related to communication and network configuration. The network management functions are accomplished by the DMAPs in the NM, cluster heads, and cluster members. The network management functions include the following actions.

a) Joining and leaving the network

A routing device should join or leave the network through the gateway device or an online routing device. A field device should join or leave the network through an online routing device or the gateway device. The new joining device should be authenticated by the SM.

b) Network address allocation

Each device in the WIA-PA network has a 64-bit Extended Unique Identifier (EUI-64) address and a 16-bit network address. The EUI-64 address is also called long address. The long address of each device is assigned by vendors according to the IEEE EUI-64 address. The 16-bit network address is also called short address. The short address of each network device is assigned by the NM.

c) Routing configuration

Static routing is implemented in the WIA-PA network. The routing table in each routing device is configured by the NM.

d) Communication resource configuration

Communication resources of the WIA-PA network are organized as superframes (see 8.4.4). When a routing device has successfully joined the network, it should be allocated communication resources by the NM. After a field device has successfully joined a cluster, the cluster head should allocate communication resources to it.

e) Time source configuration and services of system time

The WIA-PA network sets only one base time source, which is performed by the gateway device. In order to recognize the order of occurring events, the WIA-PA devices relatively synchronize with the gateway device.

f) Performance monitoring

Performance monitoring is necessary to collect the performance of the WIA-PA network, which includes device status, path failure, and channel condition.

g) MIB maintenance

The MIB module should configure the MIB of the WIA-PA protocol stack.

h) Interfaces for plant operators and maintenance personnel

The NM should provide an interface to allow plant operators and maintenance personnel to monitor and control the performance/activities of the network and devices. The definition of this interface is out of the scope of the current WIA-PA standard.

i) Firmware upgrading

Firmware upgrading should update the protocol stack of WIA-PA devices. Because on-line firmware upgrading is a power-hungry operation, WIA-PA does not recommend this mode and does not specify it in this document. WIA-PA recommends off-line firmware upgrading through handheld devices. Handheld devices connect devices that are to be upgraded by wire or wireless connections. Wired connections may use the serial communication methods. Wireless connections are not specified in this document.

The security management should manage the attributes associated with network security. The security management is performed by the SM and by the security management modules in cluster heads and cluster members. The SM handles the centralized authentication of the whole network, and needs coordination with the NM. See 11.1 for the functions of security management.

The MIB module stores all attributes used in the WIA-PA network, including both structured attributes and unstructured attributes (see 6.9).

6.2 Framework of system management

The WIA-PA network supports the hybrid centralized and distributed management scheme.

The hybrid centralized and distributed management framework is illustrated in Figure 6. The system management is implemented by the NM, the SM, and cluster heads. Cluster heads are directly managed by the NM and the SM. In addition, they are provisioned with the privilege of managing cluster members.

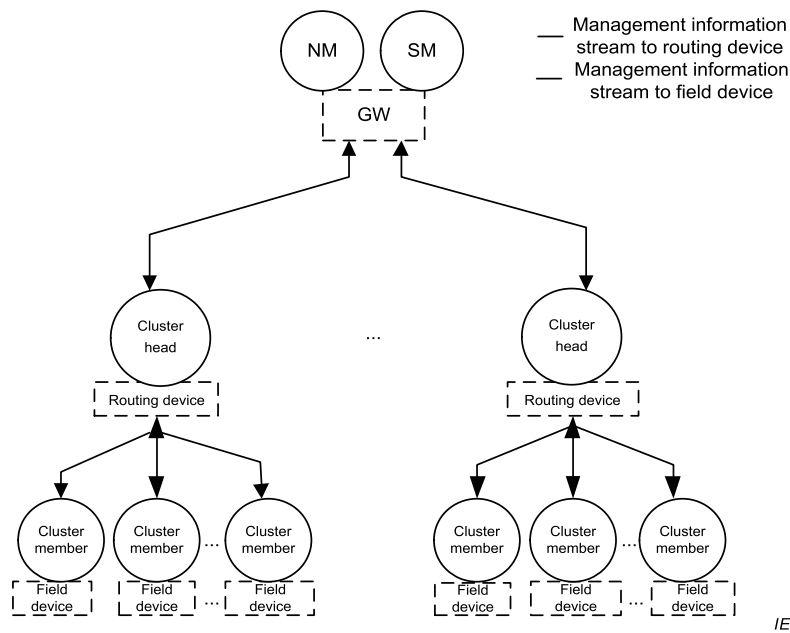


Figure 6 – Hybrid centralized and distributed system management scheme

The NM should perform the following tasks:

- constructing and maintaining the mesh topology comprised of cluster heads, and star topology comprised of cluster heads and cluster members;
- allocating communication resources for cluster heads in mesh topology, and allocating communication resources for cluster members to the cluster heads in star topology;
- monitoring the performance of the WIA-PA network, including device status, path failure, and channel condition.

The SM should perform the following tasks:

- authorizing the cluster heads and cluster members that are attempting to join the WIA-PA network;
- managing keys in the entire network, including key generation, key distribution, key recovery, and key revocation;
- authorizing the relationship of the end-to-end communication.

The cluster head should perform the following tasks:

- constructing and maintaining the star topology; allocating communication resources that are allocated to the star topology by the NM to cluster members in the cluster; providing the monitoring results of the star topology to the NM;
- storing and forwarding keys used in the star topology; authorizing the communication relationship among cluster heads; authorizing the communication relationship between a cluster head and cluster members.

6.3 Joining process

6.3.1 Provisioning process

When a WIA-PA device intends to join the network, it should be provisioned by a handheld device via wired manner.

A new device should have 64-bit long address before joining the WIA-PA network. First, the CountryCode value (see 6.9.1.2.1 and 8.4.11) of a new device shall be set, which reflects the regulatory constraints in the region where it might be deployed. The NetworkTopology value

(see 6.9.1.2.1) shall be set, which indicates the type of the network topology. The SecEnableflag value (see 6.9.1.2.1) shall be set, which indicates whether the authentication is enabled over the network. If authentication is enabled, KJ shall also be set (see 11.2).

To join the WIA-PA network, a new routing device or field device should first listen to beacons.

6.3.2 Joining process of routing device

When a routing device intends to join the network, it should be provisioned a Join Key by a handheld device. See Clause 11 for the detailed provisioning process.

The joining process of a routing device includes the following actions.

- A routing device scans the available channels to get beacons from either the online routing devices or the gateway device.
- The routing device chooses an online routing device or the gateway device as the temporal parent and synchronizes with the network according to the received beacon.
- The routing device sends a joining request to its temporal parent, which will then forward the request to the NM.
- When receiving a joining request, the NM should communicate with the SM to complete the authentication process. Then the NM returns a joining response.
- The routing device receives the joining response relayed by its temporal parent. If the response is negative, the routing device should restart this joining process; otherwise, the joining process should be finished.

The joining process of a routing device through the gateway device is shown in Figure 7.

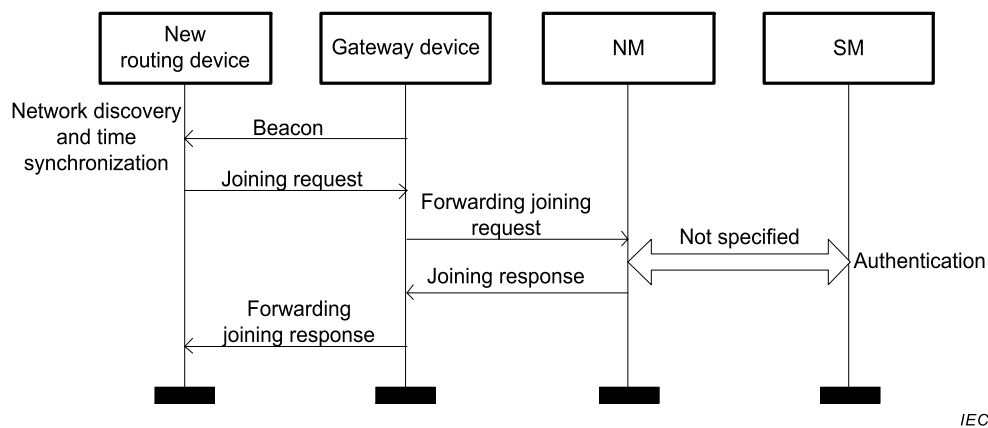


Figure 7 – Joining process of routing device through the gateway device

The joining process of a routing device through an online routing device is shown in Figure 8.

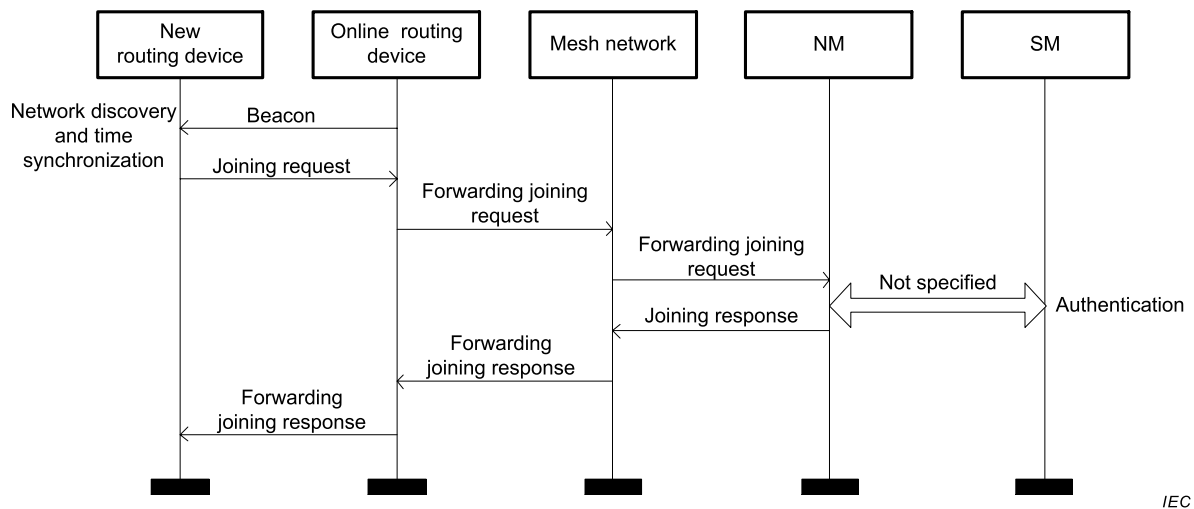


Figure 8 – Joining process of routing device through an online routing device

See 9.5.8 for the allocation of communication resources.

6.3.3 Joining process of field device

The joining process of a field device includes the following actions.

- A field device scans the available channels to get beacons from the online routing devices or the gateway device.
- The field device chooses one online routing device or the gateway device as the cluster head and synchronizes with the network according to the received beacon.
- The field device sends the joining request to the cluster head.
- When receiving the joining request, the cluster head forwards it to the NM.
- After receiving the joining response from the NM, the cluster head returns the joining response to the field device according to the type of network topology and the available communication resources of the cluster head. If the network topology is mismatched, the status in the response is set to FAILURE_TOP_DISMATCH; if there are other types of failures, the status in the response is set to FAILURE_ELSE; if the joining is successful, the status in the response is set to SUCCESS. See 8.6.3.4 for definition of Status.
- The field device receives the joining response from the cluster head. If the status in the response is FAILURE_TOP_DISMATCH, the field device will choose another routing device as its cluster head and restart the joining process as above; if status in the response is FAILURE_ELSE, the field device will restart this joining process; otherwise, if status in the response is SUCCESS, the field device has joined in the network.

The joining processes of a field device through the gateway device and through a routing device are shown in Figure 9 and Figure 10 respectively. See 9.5.8 for the allocation of communication resources.

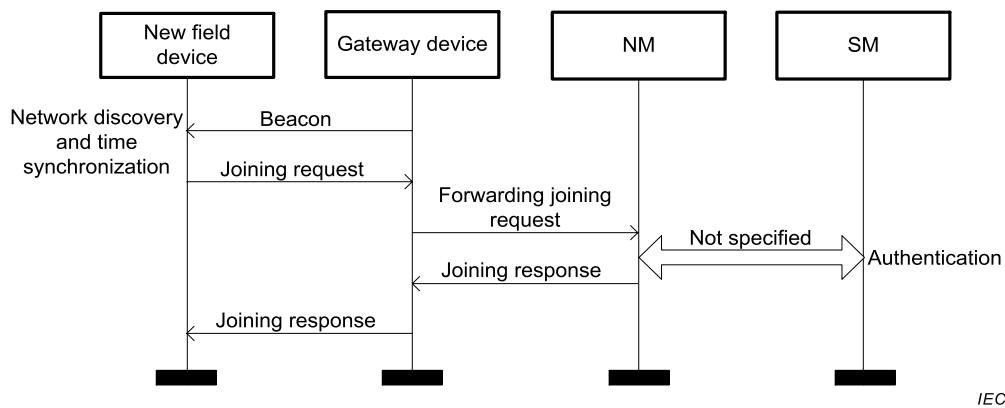


Figure 9 – Joining process of field device through a gateway device

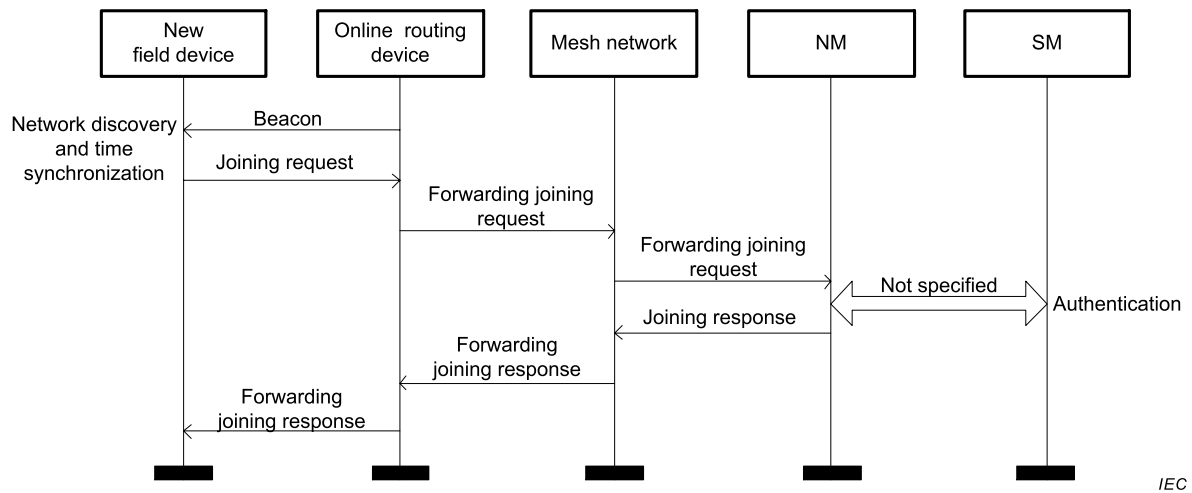


Figure 10 – Joining process of field device through a routing device

A WIA-PA handheld device connects to the WIA-PA network via the gateway device or a routing device. The joining process of the handheld device is the same as other WIA-PA devices. After joining in the network, the WIA-PA handheld device configures the WIA-PA devices and collects the network performance/health information during the Contention Access Period (CAP) period of the WIA-PA superframe.

See Clause 11 for detailed information about security.

6.3.4 Addressing and address assignment

In the WIA-PA network, each WIA-PA device (GW, routing device or field device) has a global unique 64-bit long address and a 16-bit short address. The long address, as shown in Figure 11, is set by manufacturers according to the IEEE EUI-64 address.

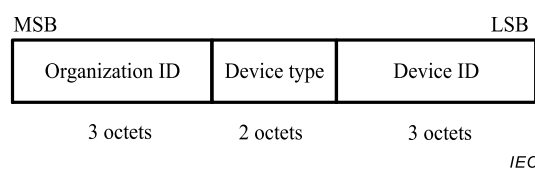


Figure 11 – Long address structure of device

The short address is 16-bit long. The most significant 8 bits of the short address that are assigned by the NM are used to identify different clusters. If the value of the parameter NetworkTopology (see 6.9.1.2.1) is 1, that is the network topology is star-only, the address of the gateway device is also the address of the cluster head.

The short address of GW is allocated by the NM. The NM resides in a gateway device (see 5.2). The address allocation process of the GW is an internal operation, which is not specified in this specification.

The short address of a routing device is shown in Figure 12. For the short address of the routing device, the least significant 8 bits are set to 0.

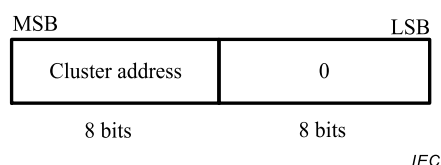


Figure 12 – Short address structure of routing device

The short address of a field device is shown in Figure 13. The least significant 8-bit part of the field device's short address is the intra-cluster address (in the cluster).

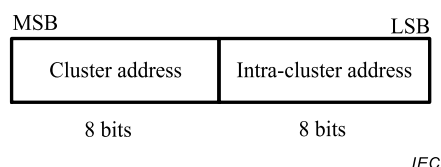


Figure 13 – Short address structure of field device

6.4 Virtual Communication Relationship (VCR)

6.4.1 Definition

Access to the User Application Objects (UAOs) is defined by the VCRs and the endpoints of a VCR are two UAOs. VCRs distinguish the routing and communication resources among different UAOs. Each VCR is identified by a VCR Identifier (VCR_ID). The attributes of a VCR include UAO ID at source side, destination UAO ID, addresses of source device/destination device, VCR type, valid scope, etc (see Table 2).

VCRs are classified into three types according to the application modes:

- a) Publisher/Subscriber(P/S) VCR, which is used to publish periodic data;
- b) Report source /Sink(R/S) VCR, which is used to support aperiodic events and trend reports;
- c) Client/Server(C/S) VCR, which is used to transfer aperiodic and dynamic paired unicast messages.

VCRs are classified into three types according to its aggregation functions:

- a) Non-aggregation VCR

If the aggregation is not supported by a cluster member, the non-aggregation VCR is used by the cluster member to send non-aggregation packets to its cluster head. If the cluster head does not support the aggregation function, it will forward the non-aggregation packets to the gateway through the non-aggregation VCR.

b) Data aggregation VCR

If the aggregation is supported by a cluster member, the data aggregation VCR is used by the cluster member to send the aggregated data from the UAOs to its clusterhead. If the cluster head does not support the aggregation function, it will forward the aggregated data to the gateway through the data aggregation VCR. The effective interval of the data aggregation VCR originates from the Data Aggregation Object (DAGO) of the cluster head to the DisaGgregation Object (DGO) of the gateway.

c) Packet aggregation VCR

If the aggregation is supported by a cluster head, the packet aggregation VCR is used by the cluster head to send aggregated packets to the gateway. The effective interval of the packet aggregation VCR originates from the Packet Aggregation Object (PAGO) of the cluster head to the DisaGgregation Object (DGO) of the gateway.

PAGOs, DGOs, and DAGOs (see 6.6.1) are three special UAOs.

6.4.2 Protocol support for VCR

The protocol supports for VCRs are listed in Table 2.

Table 2 – Protocol support for VCR

Protocol layer support			VCR types		
			P/S VCR	R/SVCR	C/S VCR
AL	User applications		Periodic data transmission of UAO	Aperiodic report e.g. alarm or event	Attribute getting and setting operation in UAO
	Communication modes in Application Sub-Layer (ASL)		P/S	R/S	C/S
	Bidirectional		No	No	Yes
	End-to-end retransmission		No	Optional	Yes
	Packet aggregation supporting		Yes	No	No
NL	Redundant path supporting	Intra-cluster	No	No	No
		Inter-cluster	Yes	Yes	Yes
	Unicast/Broadcast		Broadcast/Unicast	Broadcast/Unicast	Unicast
DLSL	Periodic		Yes	No	No
	Real-time		Yes	Optional	No
	Communication resource	Intra-cluster	Contention Free Period (CFP), exclusive timeslots in intra-cluster communication period	CAP	CAP
		Inter-cluster	Exclusive timeslots in inter-cluster communication period	Shared timeslots	Shared timeslots

6.4.3 VCR establishment

The processes of R/S VCR and C/S VCR establishment are as follows.

- The NM obtains the UAOs of the field devices when they have joined the WIA-PA network. The UAOs are obtained by the NLME-INFO_GET primitives during the CAP (see 9.5.13 and 9.6.4).
- Once the NM obtains the UAOs, it allocates reserved R/S VCRs and C/S VCRs for each UAO to field devices.

The process of P/S VCR establishment (if it is needed) is as follows.

- a) The NM establishes one P/S VCR for each UAO by using the NLME-INFO_SET primitives (see 9.5.14 and 9.6.4). If a field device does not support the data aggregation, each UAO has one non-aggregation P/S VCR, and different VCRs may use the same routing paths. Otherwise, each field device has one data aggregation VCR. If the routing device supports packet aggregation, one packet aggregation VCR is established for the routing device.

See Table 21 for the VCR information.

6.4.4 VCR release

VCRs are released when routing devices and field devices leave the network (see 6.8).

6.5 Routing configuration and communication resource allocation

6.5.1 Routing configuration

Routing devices use static routing that is configured by the NM. The concrete routing algorithms are not specified in this standard. The details of routing paths are shown in Table 15. The redundant paths are supported and use the same RouteID. The routing configuration is realized by route allocation services (see 9.5.7).

6.5.2 Framework of communication resource allocation

Communication resources consist of timeslots and channels. Allocation of communication resources should be considered in two dimensions: time and channel.

The process of communication resource allocation is as follows.

- a) In the mesh network, the communication resources of the cluster heads are allocated by the NM. The communication resources consist of those used by cluster heads in the mesh network and those allocated by cluster heads to cluster members.
- b) In the star network, the communication resources are allocated by cluster heads to cluster members. That is, communication resources are bound to cluster members.

An example of the resource allocation in the hierarchical network topology that combines star and mesh is shown in Figure 14. First, the NM residing in the GW allocates communication resources to the routing devices R1, R2 and R3. These communication resources are used for communication among R1, R2 and R3, for communication between routing devices and the GW, and for communication between intra-cluster field devices and routing devices. Second, after receiving communication resources from the NM, routing devices allocate some of the communication resources to their intra-cluster field devices, which are used for intra-cluster communications among field devices and their corresponding routing devices. As shown in Figure 14, after the NM allocates communication resources for R1, R2 and R3, R1 allocates communication resources for F1 and F2, R2 allocates communication resources for F5, and R3 allocates communication resources for F3 and F4.

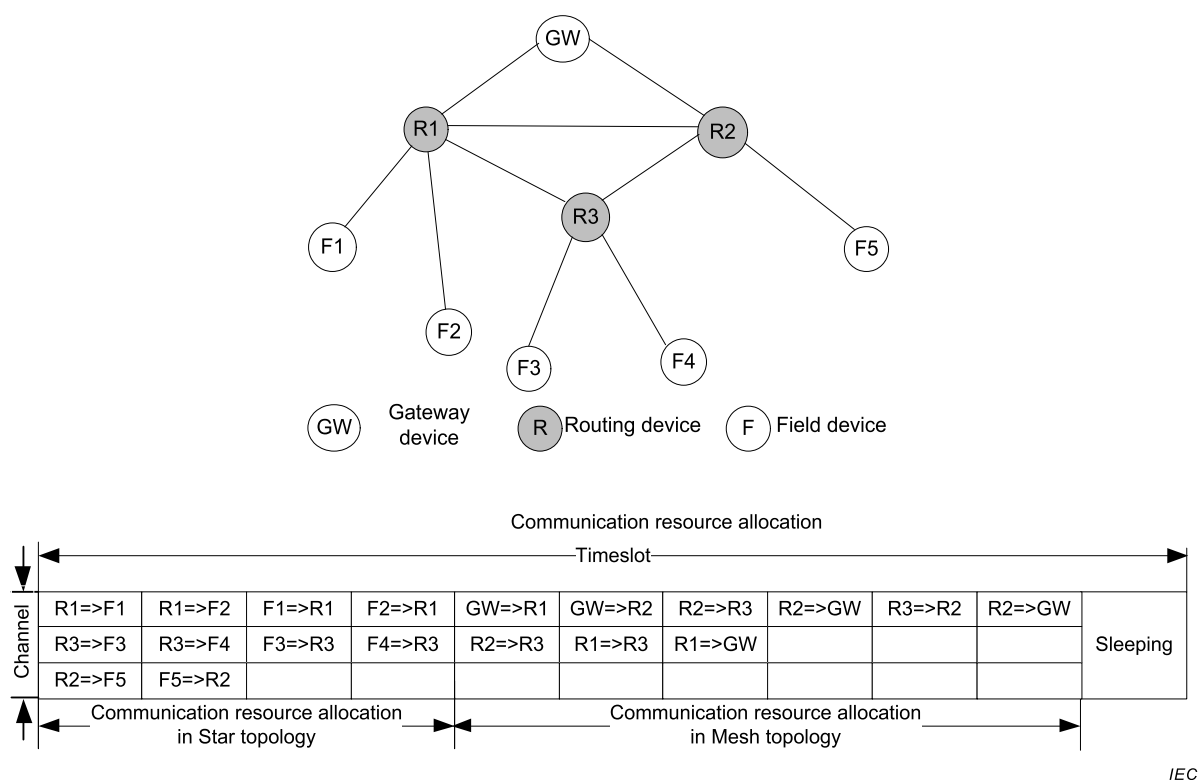


Figure 14 – An example of resource allocation

6.5.3 DLPDU priority and scheduling rules

Four priority levels of DLPDUs are defined.

a) Command (highest priority)

Any packet containing a payload with network-related diagnostics, configuration, control information, or emergent alarms should be classified with a priority of Command.

b) Process data (secondary priority)

Any packet containing process data should be classified as secondary priority level, Process Data.

c) Normal (third priority)

DLPDUs that do not meet the criteria of Command, Process data, or Alarm should be classified as Normal priority.

d) Alarm (lowest priority)

Packets containing only non-emergent alarm and event payload should assume a priority of Alarm. Devices should buffer no more than one DLPDU having Alarm priority.

The following scheduling rules are recommended in this order for allocating communication resources:

- allocating channels to the beacon frame and active period;
- allocating timeslots to the devices with the fastest update rate;
- allocating resources to the packet with the earliest generating time in multi-hop situations;
- allocating resources to the highest priority packet prior to other packets.

6.5.4 Communication resource allocation to routing device

The WIA-PA network applies the integrated management strategy of centralized and distributed schemes. After the routing device joins the network, it should scan its neighbour

devices on each channel and report the neighbour information to the NM. After receiving the neighbour information, the NM should allocate paths, a superframe, and a block of links to the routing device by using the communication resource allocation services (see 9.5.8). The information of every routing device superframe is broadcast to its field devices in the beacon frame. The allocation process of routing device communication resources is illustrated in Figure 15.

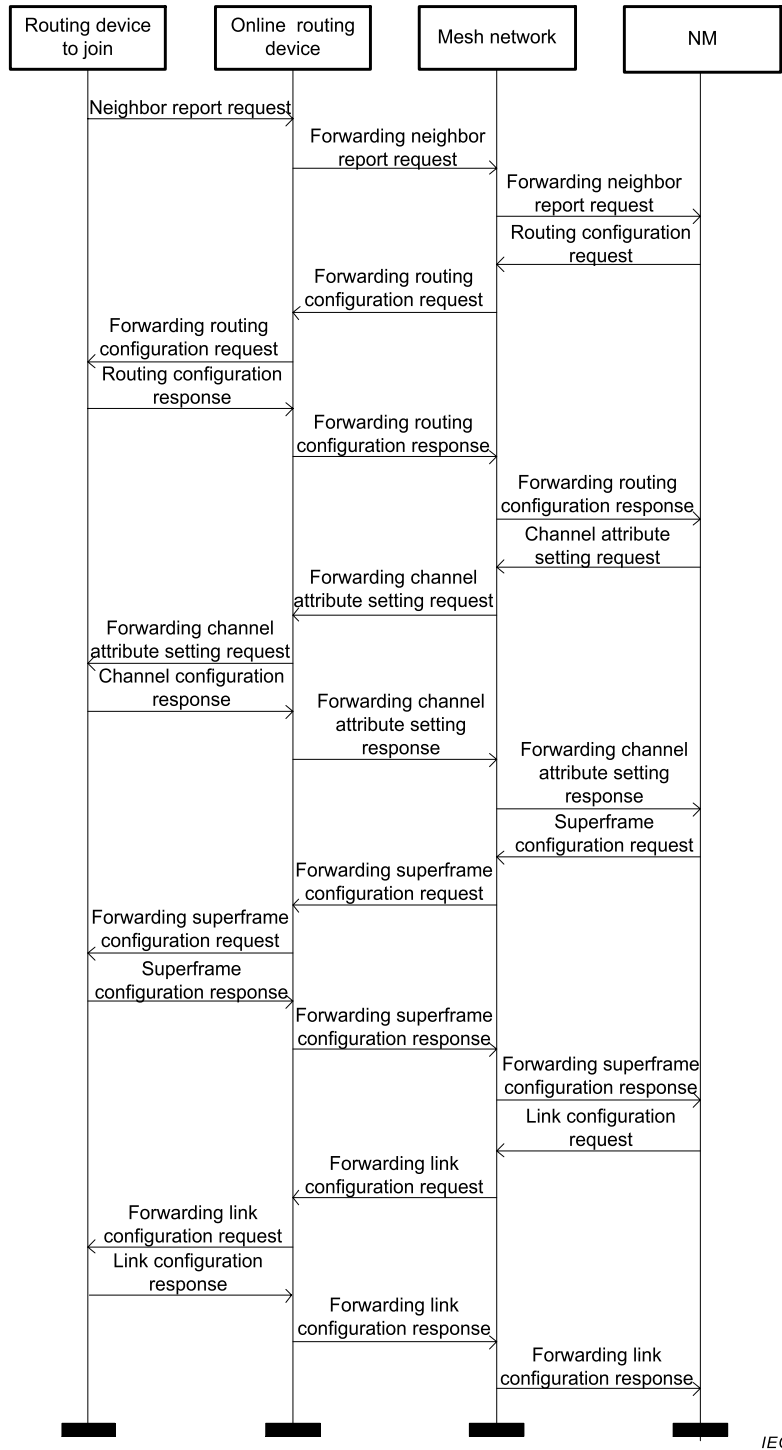


Figure 15 – Allocation process of routing device's communication resources

6.5.5 Communication resource allocation to field device

After VCRs of a field device are established successfully, either the routing device or the gateway device allocates timeslots to its field devices by using the communication resource allocation services (see 9.5.8), which are used in communication between the routing device and the field devices or between the gateway device and the field devices. If the superframes of the routing device and the gateway device are affected by the joining field devices, the routing device and the gateway device should update their RouteTable, Superframe and Link attributes (see 6.9.1.2.2 and 9.5.8).

When a field device joins the network through an online routing device, the communication resource allocation process of the field device is illustrated in Figure 16.



International Electrotechnical Commission

6.6 Aggregation and disaggregation

6.6.1 Aggregation

The aggregation function is optional for field devices and routing devices and is indicated by the aggregation and disaggregation support flag AGGSupportFlag (see Table 20). If the field devices or the routing devices support the aggregation mechanism, the NM sets the aggregation and disaggregation enable flag AGGEnableFlag to 1 (see Table 20).

The WIA-PA network supports a two-level aggregation mechanism in order to reduce the number of packet transmissions.

- a) Data aggregation. If a field device has more than one User Application Object (UAO), it should decide whether or not to invoke the data aggregation mechanism according to the AGGEnableFlag. This mechanism should reduce the data communication frequency and enhance network efficiency.
- b) Packet aggregation. If a routing device receives packets from more than one field device, it should decide whether invoking packet aggregation mechanism or not according to the AGGEnableFlag. This mechanism should reduce the number of packets from the routing device to the gateway device and enhance network efficiency.

The aggregation function is implemented by the DAGOs in field devices and PAGOs in routing devices. The operation parameters of DAGOs and PAGOs are configured by the NM.

The aggregation function supported by the WIA-PA network includes the following four situations.

- 1) A field device supports the aggregation function, while its routing device does not.
- 2) A routing device supports the aggregation function, while its field device does not.
- 3) Both, a field device and its routing device support the aggregation function.
- 4) Neither a field device nor its routing device supports the aggregation function.

Relations between the VCRs and the aggregation functions supported by field device, routing device and gateway device are shown in Table 3.

Table 3 – Relations between VCR and aggregation function

	Field device DAGO (Aggregation function)			Routing device PAGO (Aggregation function)			Gateway device DGO (Disaggregation function)	
	Support	Disable	Enable	Support	Disable	Enable	Disable	Enable
Non-aggregation VCR	NO	X		NO	X		—	—
Data aggregation VCR	YES		X	NO	X ^a			X
	YES		X	NO		X ^b		X
Packet aggregation VCR	NO	— ^c	— ^c	YES		X		X
X Indicates the aggregation/disaggregation function in the corresponding device is enabled or disabled. — Indicates the VCR is independent of the aggregation/disaggregation function. ^a The data aggregation VCR starts with DAGO of a field device and ends at DGO of the gateway device. ^b The data aggregation VCR starts with DAGO of a field device and ends at PAGO of a routing device. ^c Field devices have no packet aggregation function.								

The aggregation configuration process is listed as follows.

- i) NM should read the AGGSupportFlag to verify whether devices support the aggregation function.
- ii) NM should set the value of the AGGEnableFlag attribute to 1 in the MIB if the routing devices support the aggregation function. The NM should allocate packet aggregation VCRs to the routing devices. The aggregation duration of a routing device should be indicated by attribute AggPeriod (see 6.9.1.2.1) and set to the minimum DataUpdateRate attribute (see Table 21) of its field devices in the cluster. When aggregation duration expires, the routing device aggregates all its packets and sends the aggregated packet out.
- iii) NM should set the value of the AGGEnableFlag attribute to 1 in the MIB if the field devices support the aggregation function. The NM should allocate the data aggregation VCRs to the field devices. The aggregation duration of a field device should be indicated by attribute AggPeriod (see 6.9.1.2.1) and set to the minimum DataUpdateRate attribute (see Table 21) of its UAOs. When the aggregation duration expires, the field device aggregates all its packets and sends the aggregated packet to the routing device.

According to whether the aggregation is embedded or not, a field device or a routing device operates as follows.

- a) If the AGGEnableFlag attribute of a field device is set to 0, this field device does not support the aggregation function. Field devices that have no aggregation function send their data to the routing device through the non-aggregation VCR and the related RouteID (see Table 20). If the aggregation flag AGGEnableFlag attribute of the routing device is also set to 0, the routing device should forward this aggregated packet to the DGO of the gateway device through the original RouteID.
- b) If a field device has more than one UAO and its AGGEnableFlag attribute is set to 1, the DAGO of the field device calculates the length of the P/S data from the UAOs and aggregates these data. The format of the aggregated data is shown in Table 4. The aggregated data is sent to the ASL by the DAGO and is encapsulated with the ASL header. The field of the packet type in the ASL header is set to 0b11, which is used to indicate the aggregated packet (see 10.4.2). The aggregation packet in the ASL is sent to the routing device through the data aggregation VCR and the related RouteID; if the AGGEnableFlag attribute of the routing device is 0, the routing device should forward this aggregated packet to the DGO of the gateway device through the original RouteID.
- c) If the aggregation function embedded in a routing device is enabled (AGGEnableFlag = 1) and receives packets from its field devices, it reads the NL packet headers. The routing device should aggregate the packet according to the P/S flags and the Fragment flag in the NL packet headers (see 9.6.3). The aggregation rules are as follows:
 - if the received packet is P/S type and the Fragment flag is 0, the packet should be aggregated;
 - other types should not be aggregated.

If the packet can be aggregated, its source address and NL payload are sent to the PAGO of the DMAP. The PAGO uses the time when the first packet comes (required to be aggregated) as the start time of an aggregation cycle PagoPeriod (see Table 10). Once PagoPeriod expires, the PAGO aggregates the packets according to the format that is shown in Table 5, and searches the packets related to the packet aggregation VCR. The aggregated packet, packet aggregation VCR, and the related packets are then sent to the NL; the NL should send this aggregated packet to the gateway device through the related packets. The format of the aggregated packet in NL is shown in 9.6.3. If the length of the aggregated packet is longer than the maximum length allowed by the NL, the NL should fragment the packet and send the packet to the gateway device by using the packet aggregation VCR and the related packets.

Table 4 – Format of aggregated data followed by field device's DAGO

	Format of aggregated data followed by field device's DAGO					
Length in octet(s)	1	1	Variable length	...	1	Variable length
Field name	Number of aggregated data	Data length	Data	...	Data length	Data

Table 5 – Format of aggregated packet followed by routing device's PAGO

	Format of aggregated data followed by routing device's PAGO							
Length in octet(s)	1	2	1	Variable length	...	2	1	Variable length
Field name	Number of aggregated packet	Source address	Data length	Data	...	Source address	Data length	Data

6.6.2 Disaggregation

The disaggregation function is optional for the gateway device and is indicated by the aggregation and disaggregation support flag AGGSupportFlag (see Table 20). If the gateway device supports the disaggregation mechanism, the NM sets the aggregation and disaggregation enable flag AGGEnableFlag to 1 (see Table 20).

The disaggregation function is implemented by the DGO in the gateway device. The gateway device decides whether to disaggregate the received packet according to the NL header and the ASL header. If the value of packet type in the NL header is 1, the gateway device disaggregates the NL aggregated packet; if the value of the packet type in the ASL header is 0b11, the gateway device continues disaggregating the ASL aggregated packet.

The operation parameters of the DGO are configured by the NM.

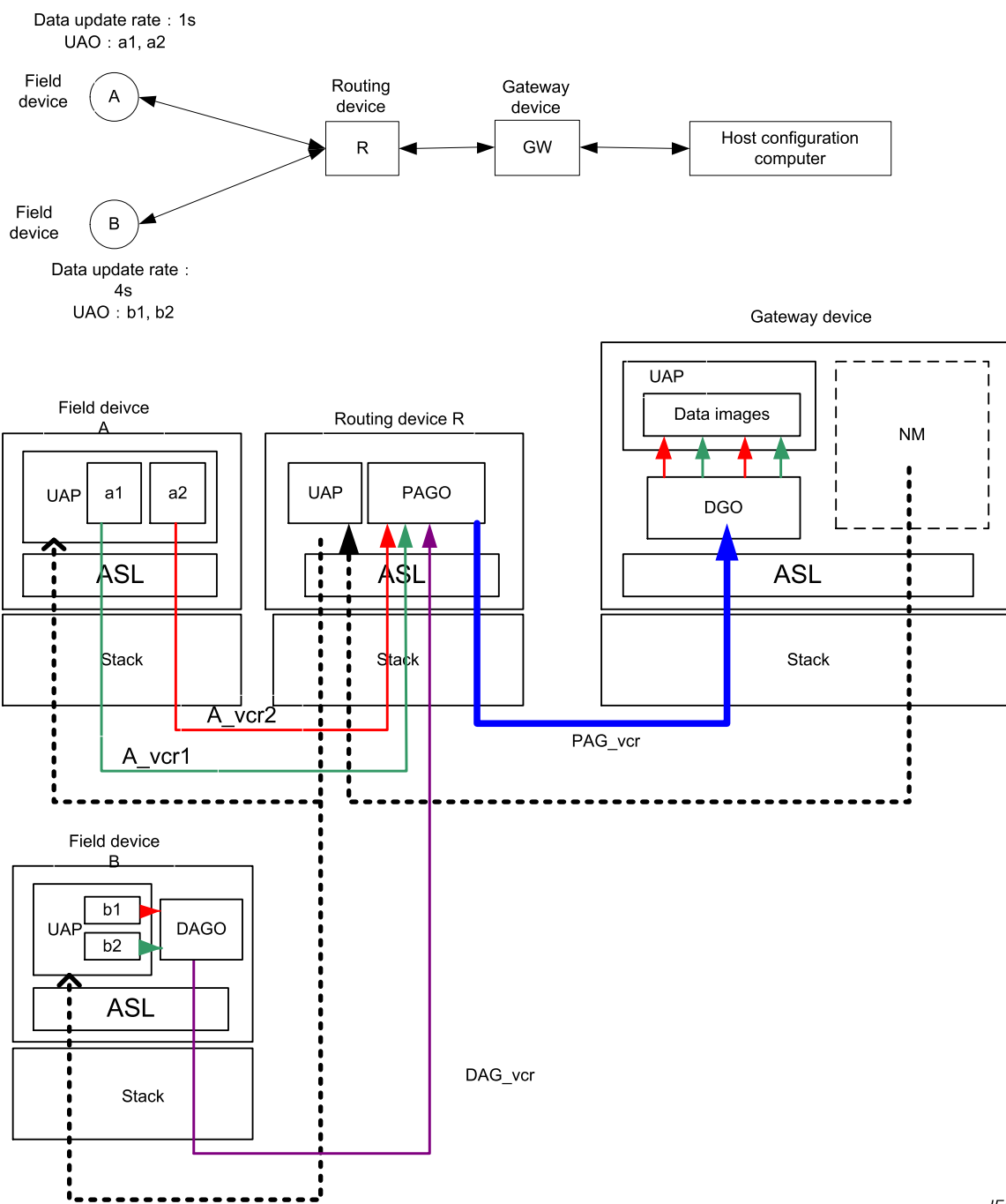
The process of disaggregation is as follows.

- a) After the gateway device receives the aggregated packets from field devices and routing devices, it will notify the DGO in its DMAP to disaggregate the packets.
- b) The DMAP sends the disaggregated packets to UAOs.

6.6.3 An example of the two level aggregation process

The following example illustrates the aggregation and disaggregation processes. The example is based on a network that consists of two field devices, one routing device, the GW, and the host configuration computer. As shown in Figure 17, the routing device R acts as the cluster head of field device A and field device B; there are two UAOs named a1 and a2 residing in field device A and two UAOs named b1 and b2 residing in field device B.

This example supposes that field device A does not support the aggregation function, while field device B and routing device R do. The data update rates of a1 and a2 are configured to 1 s, and the data update rates of b1 and b2 are configured to 4 s. The DAGO of the field device B is responsible for aggregating the packets from b1 and b2, and generates packet p_b. The routing device R has one PAGO and the aggregation duration is the minimum data update rates of a1, a2, b1, and b2, whose value is 1 s. The routing device R has a PAGO, which aggregates the packets from a1, a2 and packet p_b. The gateway device has a DGO, which disaggregates packets from field device A and B.



IEC

Figure 17 – Example of aggregation and disaggregation

The aggregation and disaggregation process is listed below.

- After the network is established, the NM allocates the non-aggregation VCRs to a1, a2, b1, and b2 for the transmissions of non-aggregation packets. The non-aggregation VCRs of a1 and a2 in field device A are indicated by A_vcr1 and A_vcr2. The endpoints of A_vcr1 are a1 and the UAP of the GW, and the endpoints of A_vcr2 are a2 and the UAP of the GW. Because the data transmissions of field device B do not use the non-aggregation VCRs, the non-aggregation VCRs of b1 and b2 in field device B are not indicated in this example.
- After constructing the non-aggregation VCRs, the NM configures the aggregation duration and data aggregation VCR for field device B and configures the aggregation duration and packet aggregation VCR for routing device R. The aggregation durations are the minimum data update rate among all UAOs in a field device or the minimum data update rate among

all field devices for a routing device. Because the data update rates of b1 and b2 are 4 s, the aggregation duration of DAGO in field device B is four seconds; the data aggregation VCR of field device B is indicated by DAG_vcr and its endpoints are DAGO in field device B and the DGO in the GW. The aggregation duration of routing device R is set to the minimum data update rate in a cluster. Because the minimum data update rate among a1, a2, b1, and b2 is one second, the aggregation duration of routing device R is set to 1 s. The packet aggregation VCR of routing device R is indicated by PAG_vcr and its endpoints are PAGO in the routing device R and DGO in the GW.

- c) After A_vcr1, A_vcr2, DAG_vcr, and PAG_vcr are established, the DAGO, PAGO and DGO begin to work. The DAGO in field device B uses the time when the first packet comes (required to be aggregated) as the start time, and aggregates the packets and sends them to routing device R through DAG_vcr at the configured aggregation timeslot. The PAGO in routing device R uses the time when the first packet comes (required to be aggregated) as the start time, and aggregates the packets in DMAP and sends them to the DGO through PAG_vcr in the GW at the configured aggregation timeslot.
- d) After the DGO of the GW receives the aggregated packets, it disaggregates the packets and finds the corresponding UAOs according to the packet source address and UAO identifiers.
- e) The DMAP in GW sends the disaggregated packets to the corresponding UAOs.

6.6.4 Management of aggregation and disaggregation objects

The attributes of the DAGO class are shown in Table 6.

Table 6 – DAGO class attributes

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	DagoID	Unsigned8	0	Mandatory	The identifier of the DAGO	READ
1	DagoRevision	Unsigned8	0	Optional	The version defined by the DAGO	READ

The attributes of the DAGO instance are shown in Table 7.

Table 7 – DAGO instance attributes

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	DagoInsID	Unsigned8	0	Mandatory	The identifier of the DAGO instance	READ
1	DagoPeriod	Unsigned8	1	Mandatory	The aggregation cycle (in seconds)	READ/WRITE
2	DagoMemNum	Unsigned8	1	Mandatory	Count of the aggregated UAOs	READ/WRITE
3	DagoMemLst	MEM_STRUCT structure (see Table 8)		Optional	List of the aggregated UAOs	READ/WRITE
4	DagoMemData Size	Unsigned8	0	Optional	Length of the aggregated data DagoMemData (in octets)	READ/WRITE
5	DagoMemData	Octetstring		Mandatory	Data of the aggregated UAOs	READ/WRITE

The methods supported by the DAGOs are shown in Table 171.

The definition of the MEM_STRUCT structure is shown in Table 8.

Table 8 – MEM_STRUCT structure

Attribute ID	Name	Data type	Description
0	AppObjID	Unsigned8	The identifier of the UAO
1	AppObjInsID	Unsigned8	The identifier of the UAO instance
2	AppObjAttrID	Unsigned8	The attribute identifier of the UAO instance

The attributes of the PAGO class are shown in Table 9.

Table 9 – PAGO class attributes

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	PagoID	Unsigned8	1	Mandatory	The identifier of the PAGO	READ
1	PagoRevision	Unsigned8	0	Optional	The version defined by the PAGO	READ

The attributes of the PAGO instance are shown in Table 10.

Table 10 – PAGO instance attributes

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	PagoInsID	Unsigned8	0	Mandatory	The identifier of the aggregation object instance	READ
1	PagoPeriod	Unsigned8	1	Mandatory	The aggregation cycle (in seconds)	READ/WRITE
2	PagoMemNum	Unsigned8	1	Mandatory	Count of the aggregated cluster members	READ/WRITE
3	PagoMemLst	Octetstring		Optional	List of the aggregated cluster members	READ/WRITE
4	PagoDataSize	Unsigned8	0	Optional	Length of the aggregated packet (in octets)	READ/WRITE
5	PagoMemData	Octetstring		Mandatory	Data of the aggregated cluster members	READ/WRITE

The methods supported by the PAGOs are shown in Table 171.

The attributes of the DGO class are shown in Table 11.

Table 11 – DGO class attributes

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	DgoID	Unsigned8	2	Mandatory	The identifier of the DGO	READ
1	DgoRevision	Unsigned8	0	Optional	The revision defined by the DGO	READ

The attributes of the DGO instance are shown in Table 12.

Table 12 – DGO instance attributes

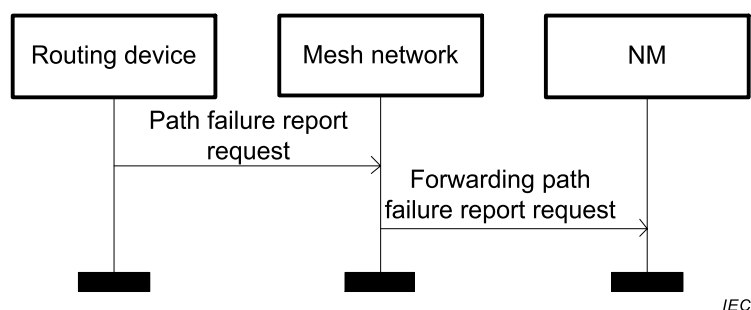
Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	DgoInstID	Unsigned8	0	Mandatory	The identifier of the DGO instance	READ

The methods supported by the DGOs are shown in Table 171.

6.7 Performance monitoring

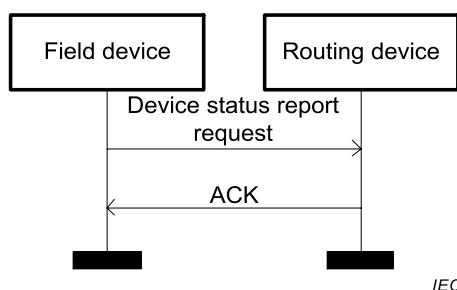
6.7.1 Path failure report

The path failure report is used by routing devices to report path failure events to the NM through the redundant paths. The process of path failure report is shown in Figure 18 (see 9.5.12).

**Figure 18 – Process of path failure report**

6.7.2 Device status report

After receiving device status reports from intra-cluster field devices, a routing device reports its own health and the health of its field devices to the NM periodically. The NM appraises and diagnoses the network performance according to health information, and replies to the change of network environment timely. The NM should detect abnormal conditions in the WIA-PA device, such as low level of battery power and disconnection from neighbouring devices. This is realized by setting alarm levels to the WIA-PA devices. The device status report processes of the field device and the routing device are shown in Figure 19 and Figure 20 (see 9.5.10).

**Figure 19 – Device status report process of field device**

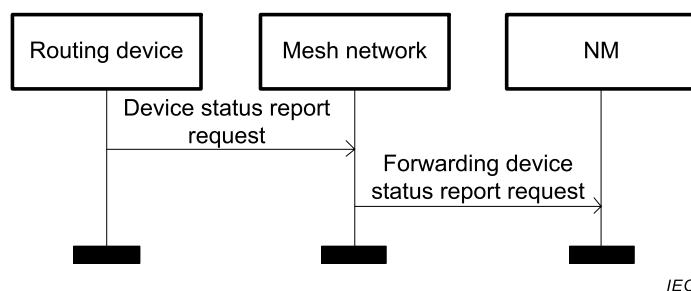


Figure 20 – Device status report process of routing device

6.7.3 Channel condition report

The channel condition report is used for the WIA-PA field devices or routing devices to report the channel condition remotely to the NM. The process of channel condition report is shown in Figure 21 (see 9.5.11).

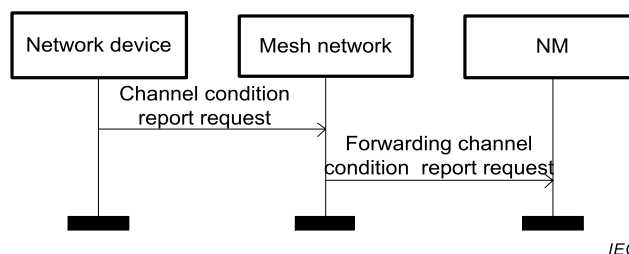


Figure 21 – Process of channel condition report

6.8 Leaving process

6.8.1 General

The leaving process of WIA-PA devices includes the abnormal leaving process, the active leaving process and the passive leaving process. The abnormal leaving process is caused by device failure, device invalidation, and energy depletion, which should be judged by the Keep-alive command frame of DLSL. The active leaving is an optional function and is enabled by setting ActiveLeavingEnable (see 6.9.1.2.1) to 1. The active leaving is requested by field devices from their routing devices or by routing devices from the gateway device. The passive leaving is requested by the gateway device from routing devices or by routing devices from their field devices.

6.8.2 Leaving process of routing device

The WIA-PA network specifies two leaving processes for routing devices: active leaving and passive leaving. The active leaving process of a routing device is as follows (shown in Figure 22).

- A routing device sends the leaving request to the NM.
- The NM gives a leaving response to the routing device.
- After receiving a positive response, the routing device notifies the leaving to its field devices. After passive leaving of field devices, the routing device leaves the network.
- The NM releases the network address, VCR and the communication resources of the departing routing device, and updates the network topology.
- The NM notifies the routing devices that have communication relationships with the departed routing device to release the related communication resources.

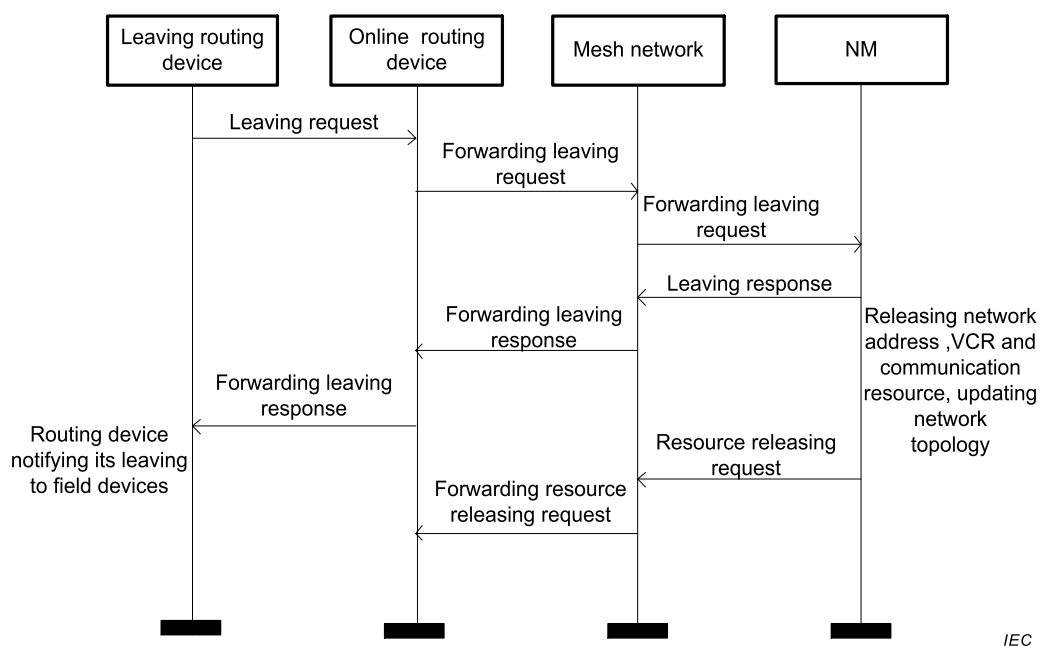


Figure 22 – Active leaving process of routing device

The passive leaving process of a routing device is as follows (shown in Figure 23).

- The NM sends the leaving request to a routing device.
- The routing device notifies its leaving to field devices.
- After passive leaving of field devices, the routing device sends a leaving response to the NM.
- The NM releases the network address, VCR and communication resources, and updates the network topology after receiving the leaving response from the routing device.
- The NM notifies the routing devices that have communication relationships with the departed routing device to release the related communication resources.

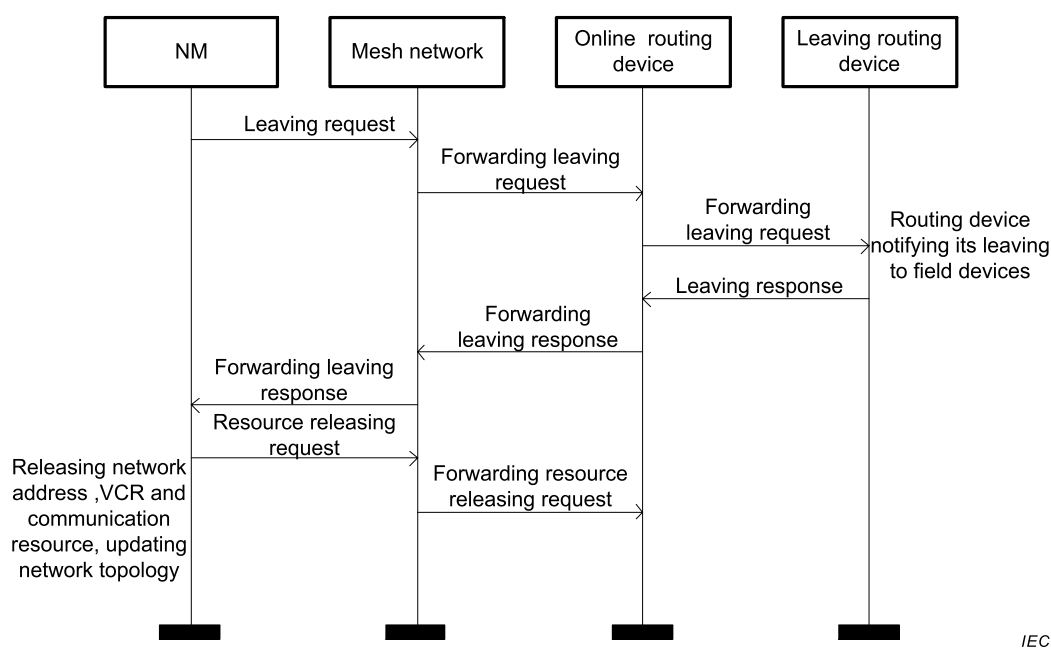


Figure 23 – Passive leaving process of routing device

6.8.3 Leaving process of field device

The WIA-PA network specifies two leaving processes for field devices: active leaving and passive leaving.

The active leaving process of a field device is as follows (shown in Figure 24 and Figure 25).

- A field device sends the leaving request to the routing device or the gateway device in a cluster.
- The routing device or the gateway device returns a leaving response to the leaving field device.
- The routing device or the gateway device releases the intra-cluster network address, VCR, and communication resources and updates the cluster member list and UAO list of the field device that has left the network.
- After receiving the response, the field device leaves the network.
- If the field device leaves the routing device, the routing device reports the updated cluster member list and UAO list to the NM.

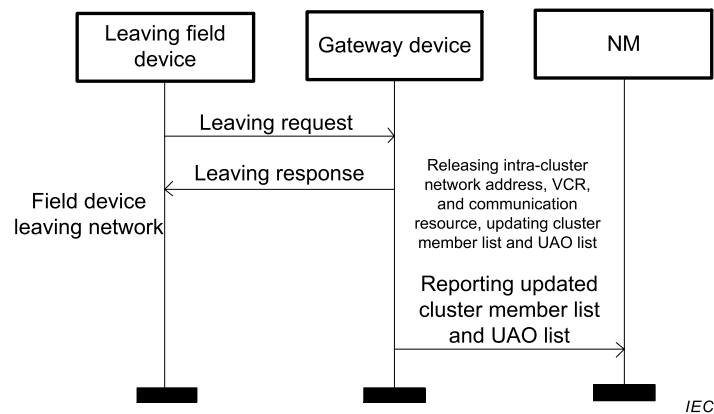


Figure 24 – Active leaving process of field device (leaving from gateway device)

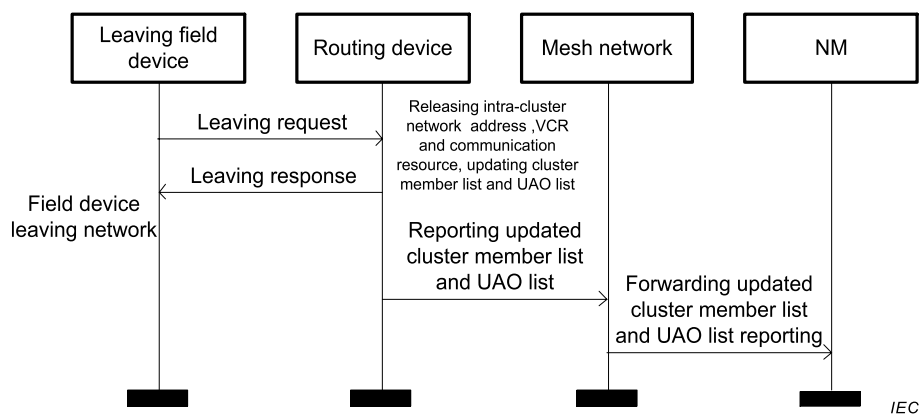


Figure 25 – Active leaving process of field device (leaving from routing device)

The passive leaving process of a field device is as follows (shown in Figure 26 and Figure 27).

- The routing device or the gateway device sends the leaving request to a field device.
- The field device returns the leaving response to the routing device or the gateway device.
- The field device leaves the cluster.

- d) The routing device or the gateway device releases the intra-cluster network address, VCR and communication resources of the departing field device and updates the cluster member list and UAO list.
- e) If the field device leaves the routing device, the routing device reports the cluster member and its UAO list to the NM.

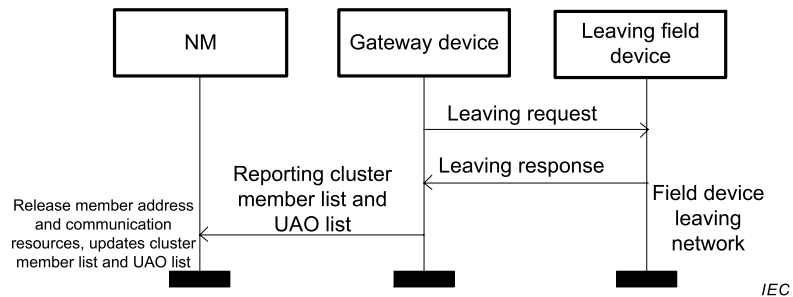


Figure 26 – Passive leaving process of field device (leaving from gateway device)

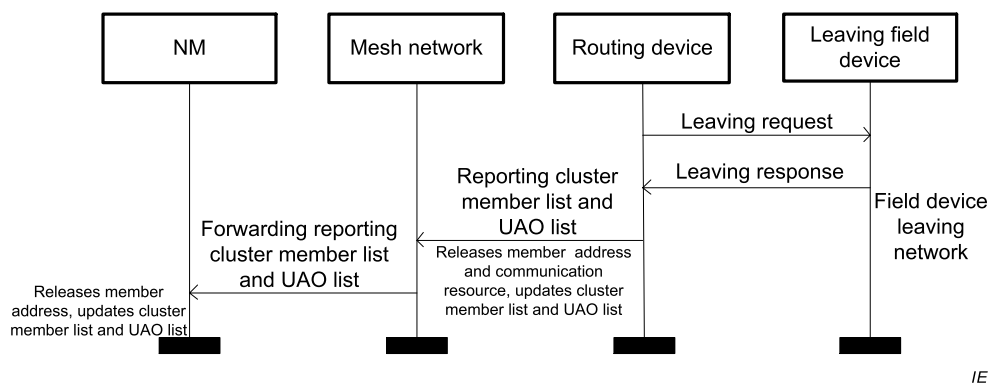


Figure 27 – Passive leaving process of field device (leaving from routing device)

6.9 Management information base and services

6.9.1 Management information base

6.9.1.1 General

Items stored in the MIB are called attributes and are used for monitoring and configuring the WIA-PA network parameters. These attributes can be accessed and updated by the NM.

According to the storage types, the attributes in the MIB are classified into three categories:

- a) constant attribute,
- b) static attribute, and
- c) dynamic attribute.

A constant attribute, such as the serial number of a wireless device, is unchangeable with time. The constant attribute is set when devices leave manufacturers and should not be modified.

A static attribute, such as an alarm limit, changes its value infrequently. The value of the static attribute should be preserved after the warm restart/reset/ power-failure.

A dynamic attribute changes its value frequently without any external command. The value of the dynamic attribute will be lost after the warm restart/reset/power-failure. Warm restart is a sequence of operations that is performed to reset a previously running device after an

unintentional shutdown. When a device is reset, it enters into the idle state. Power-failure indicates that the available power that is used by devices is becoming critically low.

According to the attribute data types, the attributes in the MIB are divided into unstructured attributes and structured attributes.

According to the implementation requirements, the attributes in the MIB are divided into mandatory attributes and optional attributes.

There are two types of the access rights to the attributes in the MIB:

- a) R (Read), which means that the values of the attribute may be read by other devices in WIA-PA network; and
- b) W (Write), which means that the values of the attribute may be set by other devices in WIA-PA network.

6.9.1.2 MIB attributes

6.9.1.2.1 Unstructured attributes

The unstructured attributes are listed in Table 13. The values of attributes numbered 0 to 28 are identical in the entire network; and the values of attributes numbered 29 to 33 are device specific.

Table 13 – Unstructured attributes (1 of 5)

ID	Name	Data type	Valid range	Access type	Storage type	Default value	Description
0	ProtocolVersion ^{de}	Unsigned16	0 to 65 535	R	Static	2013	Protocol version of current WIA-PA protocol stack, which is indicated by years.
1	NetworkID ^{e#}	Unsigned8	0 to 255	R/W	Static	0	Network identifier, used for multiple networks coexisting
2	StatisticsDuration ^{e*}	Unsigned16	0 to 65 535	R/ W	Static	0	Configuring the cycle of the statistic collection (in seconds). After this duration, WIA-PA devices update the statistic data in the neighbour tables. The value of 0 indicates that the device does not collect statistic data.
3	MaxNSDUSize ^{e*}	Unsigned8	0 to 255	R	Static	71	Maximum size of service data unit supported by the NL (in octets). MaxNSDUSize = aMaxPHYPacketSize -maximal length of MAC header – maximal length of DLSL header – maximal length of NL header. See IEEE STD 802.15.4-2011 Table 70 for aMaxPHYPacketSize.

Table 13 (2 of 5)

ID	Name	Data type	Valid range	Access type	Storage type	Default value	Description
4	BitMap ^{ae*}	Unsigned32	32 bits	R/W	Dynamic	0x FFFF	Each bit indicates whether a channel can be used: 0 = Not used; 1 = Used. The value of bit i indicates the usage status of channel i. The value of the bit i indicates whether it is used according to IEEE STD 802.15.4-2011 channel number.
5	KeepAliveDuration ^{ee*}	Unsigned24	0 to $(2^{24}-1)$	R/W	Static	1 000	Duration between two keep-alive frames (in milliseconds) The value of 0 is invalid.
6	TimeSynDuration ^{ee*}	Unsigned24	0 to $(2^{24}-1)$	R/W	Static	25 000	Duration between two time synchronization frames (in milliseconds). The default value is calculated under the assumptions that the drift of crystal oscillator is 20 parts per million and the synchronization error is 1 ms. The value of 0 is invalid.
7	ChannelThreshold ^{ee*}	Unsigned8	0 to $(\text{macMaxFrameRetries} - 2)$	R/W	Static	1	The channel switch threshold in adaptive frequency hopping, indicated as retry count; see IEEE STD 802.15.4-2011, Table 52 for macMaxFrameRetries
8	SecEnableFlag ^{ee*}	Boolean	0, 1	R/W	Static	0	Security enable flag: 0 = the whole network needs authentication; 1 = the whole network does not need authentication.
9	KeyupdateDur ^{be*}	Unsigned32	0 to $(2^{32}-1)$	R/W	Dynamic	0	The updating cycle of key (in milliseconds). The value of 0 indicates that keys are not updated.
10	MaxAttackedCnt ^{be*}	Unsigned16	0 to 65 535	R/W	Static	5	The maximum count of attacks. The value of 0 indicates that this attribute is invalid.
11	MaxKeyAttacked-Cnt ^{be*}	Unsigned16	0 to 65 535	R/W	Static	1	The maximum count of key attacked.
12	MICFailerTimeUnit ^{be*}	Unsigned16	0 to 65 535	R/W	Static	60	The time interval in seconds used to count the MaxAttackedCnt.

Table 13 (3 of 5)

ID	Name	Data type	Valid range	Access type	Storage type	Default value	Description
13	Alert ^{be*}	Unsigned16	0 to 65 535	R/W	Static	0	Bit 0 to 6 represent the security alert, the value 1 represents an alert: Bit0 = AttackedCount reaches the MaxAttackedCnt; Bit1 = KS is attacked; Bit2 = KJ is attacked; Bit3 = DLKEK is attacked; Bit4 = ALKEK is attacked; Bit5 = DLKED is attacked; Bit6 = ALKED is attacked.
14	EtoEACKTimeOut ^{e*}	Unsigned24	0 to $(2^{24}-1)$	R/W	Static	100*macMaxFrameRetries	The upper limit of waiting time for end to end acknowledge (in milliseconds). See IEEE STD 802.15.4-2011, Table 52 for macMaxFrameRetries.
15	TimeSlotDuration ^{e*}	Unsigned16	0 to 65 535	R/W	Static	N/A	Indicating the timeslot duration. The timeslot duration is calculated by: $(aBaseSlotDuration \times 2^{TimeSlotDuration})$. See IEEE STD 802.15.4-2011, Table 51 for aBaseSlotDuration.
16	PLRThreshold ^{e*}	Unsigned8	0 to 100	R/W	Static	50	The threshold of packet loss rate, which is PLRThreshold divided by 100 and is used for adaptive frequency switch. See 8.4.5 for adaptive frequency switch.
17	CmemRptCycle ^{ce*}	Unsigned16	0 to 65 535	R/W	Static	Maximal superframe cycle of the whole WIA-PA network	Configuring the reporting cycle of cluster member information (in seconds) The value of 0 is invalid.
18	ChaStaRptCycle ^{e*}	Unsigned16	0 to 65 535	R/W	Static	Maximal superframe cycle of the whole WIA-PA network	Configuring the reporting cycle of channel condition information (in seconds) The value of 0 is invalid.
19	DevStaRptCycle ^{e*}	Unsigned16	0 to 65 535	R/W	Static	Maximal superframe cycle of the whole WIA-PA network	Configuring the reporting cycle of device status information (in seconds) The value of 0 is invalid.

Table 13 (4 of 5)

ID	Name	Data type	Valid range	Access type	Storage type	Default value	Description
20	PathFailRptCycle ^{ce*}	Unsigned16	0 to 65 535	R/W	Static	Maximal superframe cycle of the whole WIA-PA network	Configuring the reporting cycle of failure path information (in seconds) The value of 0 is invalid.
21	MaxEtoERetry ^{e*}	Unsigned8	0 to 255	R/W	Static	1	The maximum number of end-to-end retry
22	NetworkTopology ^{e*}	Boolean	0, 1	R/W	Static	1	Indicating the network topology: 0 = hierarchical network that is the combination of star and mesh; 1 = star-only network topology.
23	UTCTime ^f	Unsigned32	0 to (2 ³² -1)	R/W	Dynamic	0	Universal Time Coordinated (UTC).
24	ActiveLeaving-Enable ^e	Boolean	0, 1	R/W	Static	0	A flag indicates that if the active leaving function is enabled: 0 = Disabled; 1 = Enabled.
25	SecMode ^{be*}	Unsigned8	0 to 3	R/W	Static	0	Bit 0 represents whether the DLSSL uses security service: 0 = Not used; 1 = Used. Bit 1 represents whether the AL uses security service: 0 = Not used; 1 = Used.
26	SecLevel ^{b*}	Unsigned8	0 to 63	R/W	Static	0	Bit 0, 1 and 2 represent the security levels of the DLSSL frames. 000 = None; 001 = MIC-32; 010 = MIC-64; 011 = MIC-128; 100 = Encryption; 101 = Encryption-MIC-32; 110 = Encryption-MIC-64; 111 = Encryption-MIC-128; Bit 3, 4 and 5 represent the security levels of the AL packets. 000 = None; 001 = Encryption; 010 = MIC-32; 011 = Encryption-MIC-32; Others are reserved.

Table 13 (5 of 5)

ID	Name	Data type	Valid range	Access type	Storage type	Default value	Description
27	CountryCode ^{e*}	Unsigned16	0 to 65 535	R/W	Dynamic	0x3C00	The country code that provides the local and regulatory-constraint guidance. See 8.4.11 for details.
28	EtoEACKEnable ^{e*}	Bool	0, 1	R/W	Dynamic	0	A flag indicates that if the WIA-PA network supports end to end ACK: 0 = Not support; 1 = Support.
29	AuthenState ^{be}	Boolean	0, 1	R/W	Dynamic	0	A flag that marks if a WIA-PA device has been authenticated to be a legal device: 0 = Not authenticated; 1 = Authenticated.
30	AuthenTime ^{be}	Unsigned32	0 to (2 ³² -1)	R/W	Dynamic	0	Time of a device being authenticated (in UTC time)
31	AggPeriod ^{be*}	Unsigned8	0 to 255	R/W	Static	N/A	The aggregation duration (in milliseconds) This value is valid only if aggsupport=1 and enable=1.
32	ObjectNumber ^{e*}	Unsigned8	0 to 255	R/W	Static	N/A	The number of UAOs.
33	AbsoluteSlotNumber ^e	Unsigned48	0 to (2 ⁴⁸ -1)	R/W	Dynamic	0	Number of timeslots from the start of the network, denoting the current timeslot, increasing by one.
^a Attributes are optional for the field device/handheld device. ^b Attributes are optional for all devices in the WIA-PA networks. ^c Attributes are not chosen by the field device/handheld device. ^d ProtocolVersion is configured by manufacturers. ^e Attributes numbered 0 to 33 are stored by all types of WIA-PA devices. If the default value of an attribute is N/A, users may set it; otherwise, if the default value of an attribute is specified, users should set it according to actual application scenarios. # Attributes are configured by the handheld device. * Attributes are configured by the GW.							

6.9.1.2.2 Structured attributes

The structured attributes are listed in Table 14.

Table 14 – Structured attributes

ID	Name	Data type	Access type	Storage type	Default value	Description
100	RouteTable	NLRoute_Struct structure (see Table 15)	R/ W	Dynamic		Including the route ID, destination address, next-hop address, and retry counter. Each list member is identified by storage index.
101	Superframe	Superframe_Struct structure (see Table 16)	R/ W	Dynamic		Describing the superframe information. Each list member is identified by storage index.
102	Link	Link_Struct structure (see Table 17)	R/W	Dynamic		Describing the link information. Each list member is identified by storage index.
103	Neighbour ^a	Neighbour_Struct structure (see Table 18)	R/W	Dynamic		Describing the information of neighbour devices. Each list member is identified by storage index.
104	ChannelCondition	ChanCon_Struct structure (see Table 19)	R/ W	Dynamic		Recording the statistic information of channel condition. Each list member is identified by storage index.
105	DeviceStruct	Device_Struct structure (see Table 20)	R/W	Dynamic/constant/static		Describing the information of WIA-PA devices. Each list member is identified by storage index.
106	VCRList	VCR_Struct structure (see Table 21)	R/ W	Dynamic		Recording the VCR information. Each list member is identified by storage index.
107	DevConRep	DevConRep_Struct structure (see Table 22)	R/W	Dynamic		Recording the information of device condition. Each list member is identified by storage index. This attribute is recorded by routing devices and the gateway device.
108	KeyTable ^b	Key_Struct structure (see Table 23)	R/W	Dynamic		Including the key type, key length, key update time, key using time, key value, and count of key attack. Each list member is identified by storage index.
109	ObjList	ObjList_Struct structure (see Table 24)	R/W	Static		The list of UAO identifiers. Each list member is identified by storage index.
NOTE The sizes of all the lists specified in Table 14 are implementation dependent.						
^a Attributes are not chosen by the field device/handheld device.						
^b Attributes are optional for all devices in the WIA-PA networks.						

The data type of routing attributes RouteTable is shown in Table 15.

Table 15 – NLRoute_Struct structure

Attribute member identifier	Name	Data type	Valid range	Description
0	RouteID	Unsigned16	0 to 65 535	A unique routing identifier
1	SourceAddress	Unsigned16	0 to 65 535	The short address of source device
2	DestinationAddress	Unsigned16	0 to 65 535	The short address of destination device
3	NextHop	Unsigned16	0 to 65 535	The short address of next-hop device
4	RetryCounter	Unsigned8	0 to 255	A counter to record end-to-end retries

The data type of superframe attributes Superframe is shown in Table 16.

Table 16 – Superframe_Struct structure

Attribute member identifier	Name	Data type	Valid range	Description
0	SuperframeID	Unsigned16	0 to 65 535	Unique identifier of the superframe, supplied by the NM
1	SuperframeMultiple	Unsigned8	0 to 255	SuperframeMultiple = maximum data update rates/minimum data update rates. It is used for restricting the WIA-PA superframe length and is also used for processing the long cycle data transmission. See 8.4.6 for details.
2	NumberSlots	Unsigned16	0 to 65 535	Superframe size (counts of timeslots)
3	ActiveFlag	Boolean	0, 1	Superframe active flag: 0 = Inactive; 1 = Active.
4	ActiveSlot	Unsigned48	0 to $(2^{48}-1)$	Absolute timeslot number (ASN) when a superframe begins active

The data type of link attributes Link is shown in Table 17.

Table 17 – Link_Struct structure

Attribute member identifier	Name	Data type	Valid range	Description
0	LinkID	Unsigned16	0 to 65 535	Unique identifier of the link
1	NeighbourAddr	Unsigned16	0 to 65 535	Reference to a neighbour table entry, which is empty when the NM allocates links to a routing device for intra-cluster communication.
2	LinkType	Unsigned8	0 to 31	Bit 0 represents the link type: 0 = Unicast; 1 = Broadcast; Bit 1 and bit 2 represent the character of a link: 00 = Transmitting; 01 = Transmit-shared; 10 = Receiving; Bit 3 represents the type of a timeslot: 0 = Data timeslot; 1 = Management timeslot. Bit 4 represents the aggregation character: 0 = Timeslot for non-aggregated packet; 1 = Timeslot for aggregated packet.
3	RelativeSlotNumber	Unsigned16	0 to 65 535	Relative timeslot number
4	LinkSuperframeNum	Unsigned8	0 to 255	LinkSuperframeNum = data update rate of this device/the minimum data update rate. It is used for processing the long cycle data transmission.
5	ActiveFlag	Boolean	0, 1	Indicating if a link is being used: 0 = Not used; 1 = Being used.
6	ChannelIndex	Unsigned8	0 to 31	The channel sequence numbers for this link, namely, the sequence numbers of the main channels.
7	SuperframeID	Unsigned16	0 to 65 535	Reference to a superframe in the superframe table

The data type of neighbour attributes Neighbour is shown in Table 18.

Table 18 – Neighbour_Struct structure

Attribute member identifier	Name	Data type	Valid range	Description
0	NeighbourAddr	Unsigned16	0 to 65 535	The short address of neighbour device
1	NeighbourStatus	Unsigned8	0 to 3	Bit 0 represents whether this neighbour device is a main time source: 0 = No; 1 = Yes; Bit 1 represents the status of neighbour device: 0 = Normal; 1 = Abnormal.
2	BackoffCounter	Unsigned8	0 to 31	Backoff counter
3	BackoffExponent	Unsigned8	0 to 15	Backoff exponent
4	LastTimeCommunicated	Unsigned48	0 to ($2^{48}-1$)	Time when last communicated with the neighbour device (in ASNs)
5	AveRSL	Unsigned8	0 to 255	The average level of signals received from the neighbour device in StatisticsDuration
6	PacketsTransmitted	Unsigned16	0 to 65 535	The number of un-broadcast frames sent to the neighbour device in StatisticsDuration
7	AckPackets	Unsigned16	0 to 65 535	The number of expected ACK/NACK packets received in StatisticsDuration
8	PacketsReceived	Unsigned16	0 to 65 535	The number of good packets received from the neighbour device in StatisticsDuration
9	BroadcastPackets	Unsigned16	0 to 65 535	The number of good broadcast packets received from the neighbour device in StatisticsDuration

The data type of channel condition attributes ChannelCondition is shown in Table 19.

Table 19 – ChanCon_Struct structure

Attribute member identifier	Name	Data type	Valid range	Description
0	DeviceShortAddress	Unsigned16	0 to 65 535	16-bit address of device
1	ChannelID	Unsigned8	0 to 255	The sequence number of channel
2	NeighbourAddr	Unsigned16	0 to 65 535	16-bit address of neighbour device
3	LinkQuality	Unsigned8	0 to 255	Link Quality Indication (LQI) value of every channel
4	PacketLossRate	Unsigned16	0 to 65 535	Packet loss rate of every channel, which is a percentage and calculated through received ACKs and total sent packets
5	RetryNum	Unsigned8	0 to MaxFrameRetries	The count of retransmission of every channel

The data type of device attributes DeviceStruct is shown in Table 20.

Table 20 – Device_struct structure (1 of 3)

Attribute member identifier	Name	Data type	Valid range	Storage type	Access type	Default value	Description
0	LongAddress	Unsigned64	0 to ($2^{64}-1$)	C	R	N/A	64-bit global unique address Same as for the DeviceType field as defined in 6.3.4: 0 = Gateway device; 1 = Routing device; 2 = Field device; 3 = Handheld device; Others are reserved.
1	Redundant-DevFlag	Boolean	0, 1	S	R/W	0	Flag that indicates whether this device is a redundant device: 0 = Irredundant device; 1 = Redundant device.
2	Redundant-DevLongAddr	Unsigned64	0 to ($2^{64}-1$)	C	R	N/A	64-bit global unique address of a redundant device Same as for the DeviceType field as defined in 6.3.4: 0 = Gateway device; 1 = Routing device; 2 = Field device; 3 = Handheld device; Others are reserved.
3	NetAddress-Assign	Boolean	0, 1	S	R/W	N/A	A flag indicating whether the network address (see 6.3.4) has been assigned: 0 = No; 1 = Yes.
4	DeviceShort-Address	Unsigned16	0 to 65 535	S	R/W	N/A	Short address of WIA-PA device The most significant 8 bits are cluster address and the least significant 8 bits are intra-cluster address
5	ManufacturerID	Unsigned24	0 to ($2^{24}-1$)	C	R	N/A	Manufacturer's identifier
6	DeviceSerial-Num	Unsigned64	0 to ($2^{64}-1$)	C	R	N/A	Device serial number
7	DeviceVersion	Unsigned8	0 to 255	C	R	N/A	Device version number
8	PowerSupply-Status	Unsigned8	0 to 10	S	R/W	N/A	Power condition: 0 = Fixed power supply; 1 = Highest power; 2 = Second highest power; 10 = lowest power.
9	RouterCapable	Boolean	0, 1	S	R/W	0	A flag to indicate if the device has routing function: 0 = No; 1 = Yes.

Table 20 (2 of 3)

Attribute member identifier	Name	Data type	Valid range	Storage type	Access type	Default value	Description
10	Devicestate	Unsigned8	0 to 16	S	R/W		Bits 0 and 1 represent device joining state: 00 = Not joined; 01 = Joining; 10 = Security authentication; 11 = Joined. Bit 2-3 represent device running state: 00 = Inactive; 01 = Active; 10 = Failed. Others are reserved.
11	DeviceMemory-total	Unsigned32	0 to ($2^{32}-1$)	C	R	N/A	Total memory in a device (in octets), including RAM, ROM, Flash...
12	DeviceUsed-Memory	Unsigned32	0 to ($2^{32}-1$)	D	R/W	N/A	Memory used by device (in octets)
13	ClockMaster-Role	Boolean	0, 1	S	R/W	N/A	The device is a time source or not (see 8.3.3.1): 0 = No; 1 = Yes.
14	ClockUpdate	Unsigned32	0 to ($2^{32}-1$)	D	R/W	0	The last adjustment of clock (in seconds)
15	PacketsMACTo-DLSL	Unsigned32	0 to ($2^{32}-1$)	D	R/W	0	Count of the packets from MAC to DLSL
16	PacketsFrom-DLSLRejected	Unsigned32	0 to ($2^{32}-1$)	D	R/W	0	Count of the packets from the DLSL that are rejected by the NL
17	PacketsFrom-DLSLAccepted	Unsigned32	0 to ($2^{32}-1$)	D	R/W	0	Count of the packets from the DLSL that are accepted by the NL
18	PacketsFrom-ASL	Unsigned32	0 to ($2^{32}-1$)	D	R/W	0	Count of the packets from the ASL
19	PacketsFrom-ASLRejected	Unsigned32	0 to ($2^{32}-1$)	D	R/W	0	Count of the packets from the ASL that are dropped by the NL
20	PacketsOutTo-DLSL	Unsigned32	0 to ($2^{32}-1$)	D	R/W	0	Count of the packets from the ASL that are forwarded by the NL to the DLSL
21	AGGSupport-Flag	Boolean	0, 1	S	R/W	N/A	Aggregation and disaggregation support flag (whether a routing device supports aggregation mechanism); 0 = Not support; 1 = Support.
22	AGGEnable-Flag	Boolean	0, 1	S	R/W	0	Aggregation and disaggregation enable flag (whether a routing device enables aggregation mechanism); 0 = Disable; 1 = Enable.
23	IntraChannel-Num	Unsigned8	0 to 31	S	R/W	0	The number of usable channels for intra-cluster communication

Table 20 (3 of 3)

Attribute member identifier	Name	Data type	Valid range	Storage type	Access type	Default value	Description
24	IntraChanel	Unsigned8	0 to 31	S	R/W	0	A list to store all communication channels, which is allocated by the GW to routing devices and field devices. The size of the list is IntraChannelNum. See 8.4.5 for details.
25	SuperframeID	Unsigned16	0 to 65 535	S	R/W	0	Unique identifier of the superframe, supplied by the NM

The Storage types in this table are C = constant, D = Dynamic, and S = static.

The data type of VCR attributes VCR_Struct is shown in Table 21.

Table 21 – VCR_Struct structure

Attribute member identifier	Name	Data type	Valid range	Description
0	VcrID	Unsigned16	0 to 65 535	VCR identifier The VCR is invalid if its identifier is 0xFFFF.
1	VcrType	Unsigned8	0 to 16	Bits 0-1 represent VCR type: 00 = P/S VCR; 01 = R/S VCR; 10 = C/S VCR; Bits 2 and 3 represent aggregation or non aggregation VCR: 00 = Non-aggregation VCR; 01 = Data aggregation VCR; 10 = Packet aggregation VCR; Others are reserved.
2	SrcObjID	Unsigned8	0 to 255	Source object ID
3	SrcObjInstID	Unsigned8	0 to 255	ID of source object instance
4	DesObjID	Unsigned8	0 to 255	Destination object ID
5	DesObjInstID	Unsigned8	0 to 255	ID of destination object instance
6	DataUpdateRate	Unsigned32	0 to (2 ³² -1)	Data update rate (in milliseconds) The data has no cycle if this value is 0xFFFFFFFF.
7	VcrStatus	Boolean	0, 1	VCR status: 0 = Inactive; 1 = Active.
8	VcrActivationTime	Unsigned32	0 to (2 ³² -1)	The activation time of VCR (in milliseconds)
9	ServiceTime	Unsigned32	0 to (2 ³² -1)	The valid service duration of VCR (in milliseconds)
10	SourceChAddress	Unsigned16	0 to 65 535	The cluster head address of the source device
11	SourceAddress	Unsigned16	0 to 65 535	The network address of the source device
12	DestinationAddress	Unsigned16	0 to 65 535	The network address of the destination device
13	SecurityPolicy	Unsigned8	0 to 255	Security level of packets (see Annex A)
14	RouteID	Unsigned16	0 to 65 535	Route identifier

The time unit used in this table is the timeslot used by the superframe.

The data type of device condition attributes DevConRep is shown in Table 22.

Table 22 – DevConRep_Struct structure

Attribute member identifier	Name	Data type	Valid range	Description
0	DevShortAddr	Unsigned16	0 to 65 535	16-bit short address of device
1	NumPktSent	Unsigned16	0 to 65 535	The total number of packets sent after the last report
2	NumPktRcvd	Unsigned16	0 to 65 535	The total number of packets terminated in the device after the last report
3	NumMacMicFailure	Unsigned16	0 to 65 535	The total number of Message Integrity Code (MIC) failures after the last report
4	BatLevel	Unsigned8	1 to 10	Residual power level
5	RestartCount	Unsigned8	0 to 255	Restart count of device
6	Uptime	Unsigned32	0 to $(2^{32}-1)$	Time from the last restart (in seconds)

The data type of key attributes KeyTable is shown in Table 23.

Table 23 – Key_Struct structure

Attribute member identifier	Name	Data type	Valid range	Description
0	KeyID	Unsigned16	0 to 65 535	Key identifier
1	KeyType	Unsigned8	0 to 3	Key type: 0 = Joining key; 1 = Key encryption key; 2 = DLSL encryption key; 3 = AL encryption key.
2	KeyLength	Unsigned8	0 to 255	(KeyLength+1) is the valid length of the key (in bits)
3	KeyActiveTime	Unsigned48	0 to $(2^{48}-1)$	Absolute timeslot number (ASN) when key begins active.
4	KeyData	Octetstring		Key value
5	KeyAttackCnt	Unsigned8	0 to 255	The total number of key attacks
6	KeyState	Unsigned8	0 to 7	The using state of a key: 0 = Backup; 1 = Using; 2 = Invalid; Others are reserved.

The data type of object list attributes ObjList is shown in Table 24.

Table 24 – ObjList_Struct structure

Attribute member identifier	Name	Data type	Valid range	Description
0	ObjectID	Unsigned8	0 to 255	The unique identifier of the UAO
1	InstanceID	Unsigned8	0 to 255	The unique identifier of an object instance
2	ProfileID	Unsigned16	0 to 65 535	The profile ID for the UAO
3	ParameterNumber	Unsigned8	0 to 255	Number of parameters of the UAO
NOTE ObjectID and InstanceID in ObjList_Struct are identical with Object Identifier and Instance ID (see Annex C). DAGO, PAGO, and DGO are three special UAOs. Therefore, the attributes of DAGO, PAGO, or DGO are included in the ObjList if such object is implemented in the device. In addition, DagolD and DagolnsID of DAGO, PagolD and PagolnsID of PAGO as well asDgolD and DgolnsID of DGO are respectively corresponding to the ObjectID and InstanceID in ObjList_Struct.				

6.9.2 MIB services

6.9.2.1 Remote MIB services

The attributes in the MIB can be read and written remotely through the attribute-getting and attribute-setting services provided by the NL.

6.9.2.2 Local MIB services

6.9.2.2.1 General

The attributes in the MIB can be read and written locally through the attribute-getting and attribute-setting services provided by the local DMAP.

6.9.2.2.2 DMAP attribute getting services

DMAP-MIB-GET.request is used by protocol layers to request attributes in the MIB.

The semantics of DMAP-MIB-GET.request are as follows:

```
DMAP-MIB-GET.request (
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```

Table 25 specifies the parameters for DMAP-MIB-GET.request.

Table 25 – DMAP-MIB-GET.request parameters

Name	Data type	Valid range	Description
AttributeID	Unsigned8	0 to 255	Attribute ID in the MIB
AttributeMemID	Unsigned8	0 to 255	The identifier of attribute member, which is used to get the structured MIB attributes The value 255 means that all attributes should be read.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to get the structured MIB attributes
Count	Unsigned8	0 to 255	Number of attribute values or attributes member values, which is used to get the structured MIB attributes; Getting all attribute values from FirstValueStorIndex if Count = 0

DMAP-MIB-GET.confirm is used to return the result of DMAP-MIB-GET.request.

The semantics of DMAP-MIB-GET.confirm are as follows:

```
DMAP-MIB-GET.confirm (
    Status,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count,
    AttributeValue
)
```

Table 26 specifies the parameters for DMAP-MIB-GET.confirm.

Table 26 – DMAP-MIB-GET.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Attribute getting results: 0 = SUCCESS; 1 = UNSUPPORTED_ATTRIBUTE; Others are reserved.
AttributeID	Unsigned8	0 to 255	The requested attribute ID
AttributeMemID	Unsigned8	0 to 255	The identifier of attribute member The value 255 means that all attributes should be read.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple read attribute values
Count	Unsigned8	0 to 255	Number of attribute values or attributes member values
AttributeValue	Octetstring		The value of the attribute

If the operation of getting attributes is successful, the Status should be SUCCESS and the AttributeValue is valid; otherwise, if the MIB does not have the needed attributes, the Status should return UNSUPPORTED_ATTRIBUTE and the AttributeValue is invalid.

6.9.2.2.3 DMAP attribute setting services

DMAP-MIB-SET.request should be used by the protocol layers to write attributes to the MIB.

The semantics of DMAP-MIB-SET.request are as follows:

DMAP-MIB-SET.request (

AttributeID,
AttributeMemID,
FirstValueStorIndex,
Count,
AttributeValue

)

Table 27 specifies the parameters for DMAP-MIB-SET.request.

Table 27 – DMAP-MIB-SET.request parameters

Name	Data type	Valid range	Description
AttributeID	Unsigned8	0 to 255	Attribute ID in the MIB
AttributeMemID	Unsigned8	0 to 255	Identifier of attribute member The value 255 means that all attributes should be read.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to get the structured MIB attributes
Count	Unsigned8	0 to 255	Number of attributes
AttributeValue	Octetstring		Value of the attribute

DMAP-MIB-SET.confirm is used to return the result of DMAP-MIB-SET.request.

The semantics of DMAP-MIB-SET.confirm are as follows:

DMAP-MIB-SET.confirm (

Status,
AttributeID,
AttributeMemID,
FirstValueStorIndex
)

Table 28 specifies the parameters for DMAP-MIB-SET.confirm.

Table 28 – DMAP-MIB-SET.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Attribute setting result: 0 = SUCCESS; 1 = UNSUPPORTED_ATTRIBUTE; 2 = INVALID_PARAMETER; Others are reserved.
AttributeID	Unsigned8	0 to 255	Attribute ID in the MIB
AttributeMemID	Unsigned8	0 to 255	Identifier of attribute member The value 255 means that all attributes should be read.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple written attribute values

If the operation of setting attributes is successful, the Status should be SUCCESS; if the MIB does not have the needed attributes, the Status should be UNSUPPORTED_ATTRIBUTE; otherwise, if the set attributes are not conformable to the specified attributes, the Status should be INVALID_PARAMETER.

7 Physical layer

7.1 General

WIA-PA uses Radio Frequencies (RF) to communicate between devices. The communication distance between two devices depends upon the transmitter power, antenna type, and obstruction between two devices. WIA-PA devices can be powered either by mains power, battery, energy harvesting devices (for example solar, vibration, etc), or a combination there of.

The PHY specification of WIA-PA is based on the IEEE STD 802.15.4-2011 2,4 GHz compliant radio.

WIA-PA PHY defines the signaling method, signal strength, receiver sensitivity, and environment for sending bits across the network media. The PHY is responsible for activation and deactivation of the radio transceiver, energy detection, link quality indicator, channel selection, clear channel assessment, transmitting and receiving packets across the physical medium.

The PHY specification of WIA-PA includes the following:

- the PHY requirements many of which are adopted directly from IEEE STD 802.15.4-2011 including specific requirements on channels, transmit power, and receiver sensitivity, and
- the PHY requirements to ensure inter-connectable among WIA-PA devices.

7.2 General requirements based on IEEE STD 802.15.4-2011

The WIA-PA physical layer shall be based on IEEE STD 802.15.4-2011 2,4 GHz DSSS with additional requirements and exceptions as specified herein.

One of the device provisioning parameters, CountryCode (see 8.4.11), provides the locale and regulatory-constraint guidance needed to drive conformance to the relevant regulations. See Annex D.

The device vendors are responsible that these devices are compliant with this standard and any country- or region-specific regulations.

Table 29 specifies the IEEE STD 802.15.4-2011 PHY selection for a WIA-PA device.

Table 29 – PHY protocol selection

Clause of IEEE STD 802.15.4-2011	Header	Presence	Constraints
6	General PHY requirements		
6.1	General requirements and definitions	Partial	Only 2 450 MHz DSSS PHY, employing O-QPSK modulation
6.1.1	Operating frequency range	Partial	Only 2 450 MHz DSSS band is included (see Table 30)
6.1.2	Channel assignments	Partial	Only Channels 11-25 of channel page 0 are included (see Table 32)
6.1.3	Minimum LIFS and SIFS periods	Partial	Only minimum LIFS and SIFS for 2 450 MHz band is included
6.1.4	RF power measurement	YES	
6.1.5	Transmit power	YES	
6.1.6	Out-of-band spurious emission	YES	
6.1.7	Receiver sensitivity definitions	YES	
6.2	PHY service specifications	YES	
6.3	PPDU format	YES	
6.4	PHY constants and PIB attributes		
6.4.1	PHY constants	YES	
6.4.2	PHY PIB attributes	Partial	See 7.3.9
6.5	2 450 MHz PHY specifications	YES	See 7.3.8 for further explanation
6.6	868/915 MHz band binary phase-shift keying (BPSK) PHY specifications	NO	Only 2 450 MHz band is included
6.7	868/915 MHz band (optional) amplitude shift keying (ASK) PHY specifications	NO	Only 2 450 MHz band is included
6.8	868/915 MHz band (optional) O-QPSK PHY specifications	NO	Only 2 450 MHz band is included
6.9	General radio specifications		
6.9.1	TX-to-RX turnaround time	YES	
6.9.2	RX-to-TX turnaround time	YES	
6.9.3	Error-vector magnitude (EVM) definition	YES	
6.9.4	Transmit center frequency tolerance	YES	
6.9.5	Transmit power	NO	See 7.3.6 for replacement of this subclause
6.9.6	Receiver maximum input level of desired signal	YES	
6.9.7	Receiver ED	YES	
6.9.8	Link quality indicator (LQI)	YES	
6.9.9	Clear channel assessment (CCA)	YES	

7.3 Additional requirements

7.3.1 General

Although the IEEE STD 802.15.4-2011 physical layer supports multiple frequency bands and modulation classes, a device compliant with this standard shall operate in the license-exempt 2 400 MHz to 2 483,5 MHz band using DSSS modulation and coding at 250 kbit/s, which is specified in IEEE STD 802.15.4-2011, Table 51 as 2 450 DSSS PHY. This standard does not support any of the other frequency bands or data rates or modulation and coding techniques specified in IEEE STD 802.15.4-2011.

7.3.2 Frequency allocations

The transceiver shall employ DSSS and operate in the license-free ISM band as shown in Table 30.

Table 30 – Frequency band and data rate

Frequency MHz	Communication rate kchip/s	Modulation	Bit rate kb/s	Symbol rate ksymbol/s	Symbols
2 400 to 2 483,5	2 000	O-QPSK	250	62,5	16-ary Orthogonal

7.3.3 Channel numbers and frequency assignments

The 2 450 MHz band supports channel assignments 11 – 26 as specified by IEEE STD 802.15.4-2011. Since channel 26 is not compliant with the regulation of some world regions, it is not included in this document.

The frequency assignment for the channels 11 – 25 is shown in Table 31.

Table 31 – Frequency assignments

Channel number	Frequency MHz		Channel number	Frequency MHz		Channel number	Frequency MHz
11	2 405		16	2 430		21	2 455
12	2 410		17	2 435		22	2 460
13	2 415		18	2 440		23	2 465
14	2 420		19	2 445		24	2 470
15	2 425		20	2 450		25	2 475

7.3.4 Radio transceivers

The radio transceivers of WIA-PA devices are compliant to IEEE STD 802.15.4-2011 and conform to worldwide regulations in Europe, Canada, Japan, China, the United States and other locations. See Annex D.

7.3.5 Unspecified or improved required radio performance

This document includes the following that is not specified in IEEE STD 802.15.4-2011.

- Recommended time to switch between channels should be 12-symbol periods.
- Recommended cold start radio turn-on time is 4 ms maximum. It includes frequency lock and settling time.

7.3.6 Transmit power

Transmit power shall be the Equivalent Isotropic Radiated Power (EIRP) of the device. WIA-PA devices shall provide a nominal EIRP of +10 dBm (10 mW) ± 3 dB. The maximum radiated power level shall not exceed the regulatory requirements that apply where the device is deployed, as constrained by CountryCode (see 8.4.11).

In both cases the rated transmit power shall be representative of the manufacturer's production device with power source (batteries, solar, or otherwise) at 95 % to 100 % of rated capacity. All devices should be provided with an omni-direction antenna. The rated transmit power data including maximum output power and radiation patterns for all antenna supported by the product shall be available in the product manual or upon request.

7.3.7 Output power control

The device power level shall be programmable at discrete, monotonic levels from –10 dBm to +10 dBm EIRP (within ± 4 dBm of error in actual power level). The output power can be controlled by setting the PHY PIB attribute phyTransmitPower.

7.3.8 Receiver sensitivity

Receiver sensitivity of WIA-PA complies with IEEE STD 802.15.4-2011 and shall be capable of achieving a sensitivity of –85 dBm or better.

7.3.9 PHY PIB attributes

This standard includes the attributes specified in the IEEE STD 802.15.4-2011, 6.4.2 and additional attributes that apply only to this document. Some of these attributes are assigned a constant value as shown in Table 32.

Table 32 – PHY PIB attributes (1 of 2)

Attribute	Comment
phyCurrentChannel	Set by Ph-Enable request
phyChannelsSupported	Only channels 11 – 25 are supported
phyTXPowerTolerance	1dB, 3 dB, 6 dB
phyTXPower	The values from '–10 dBm to +10 dBm' are supported
phyCCAMode	Only value 2 (carrier sense) is included
phyCurrentPage	Only value '0' is included
phyMaxFrameDuration	Only value '266' is included
phySHRDuration	Only value '10' is included
phySymbolsPerOctet	Only value '2' is included
phyPreambleSymbolLength	Only value '0' is included
phyUWBDataRatesSupported	This attribute is invalid in WIA-PA
phyCSSLowDataRateSupported	This attribute is invalid in WIA-PA
phyUWBCoUSupported	This attribute is invalid in WIA-PA
phyUWBBCSSupported	This attribute is invalid in WIA-PA
phyUWBCurrentPulseShape	This attribute is invalid in WIA-PA
phyUWBCoUpulse	This attribute is invalid in WIA-PA
phyUWBBCSpulse	This attribute is invalid in WIA-PA
phyUWBLCWeight1	This attribute is invalid in WIA-PA
phyUWBLCWeight2	This attribute is invalid in WIA-PA
phyUWBLCWeight3	This attribute is invalid in WIA-PA

Table 32 (2 of 2)

Attribute	Comment
phyUWBLCPPWeight4	This attribute is invalid in WIA-PA
phyUWBLCPPDelay2	This attribute is invalid in WIA-PA
phyUWBLCPPDelay3	This attribute is invalid in WIA-PA
phyUWBLCPPDelay4	This attribute is invalid in WIA-PA
phyRanging	This attribute is invalid in WIA-PA
phyRangingCrystalOffset	This attribute is invalid in WIA-PA
phyRangingDPS	This attribute is invalid in WIA-PA
phyCurrentCode	Only value '0' is included
phyNativePRF	This attribute is invalid in WIA-PA
phyUWBScanBinsPerChannel	This attribute is invalid in WIA-PA
phyUWBInsertedPreambleInterval	This attribute is invalid in WIA-PA
phyTXRMARKER Offset	This attribute is invalid in WIA-PA
phyRXRMARKER Offset	This attribute is invalid in WIA-PA
phyRFRAMEProcessingTime	This attribute is invalid in WIA-PA
phyCCADuration	This attribute is invalid in WIA-PA

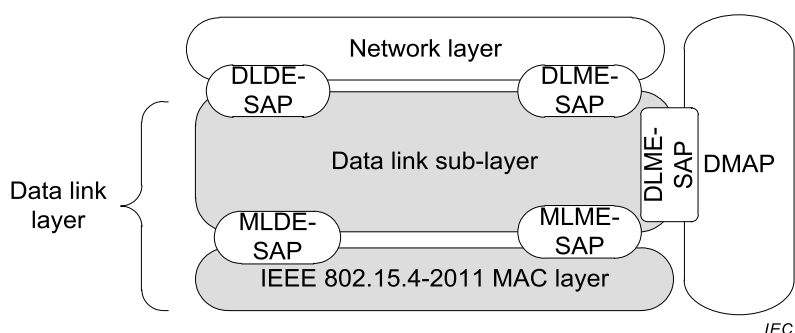
8 Data link layer

8.1 General

The WIA-PA Data Link Layer (DLL) is designed to guarantee communication among WIA-PA devices in a reliable and secure way in real-time. The DLL of WIA-PA extends the IEEE STD 802.15.4-2011 superframe structure. The WIA-PA DLL supports certain key functions, including frequency hopping, retransmission, and Time Division Multiple Access (TDMA) and Carrier Sense Multiple Access (CSMA) hybrid channel access mechanisms. These mechanisms are used to guarantee reliability and real-time transmission in communication. The WIA-PA DLL is designed to use MIC mechanism and encryption technology to guarantee the integrity and confidentiality of the communication process.

8.2 Protocol stack

The WIA-PA DLL is designed to leverage the IEEE STD 802.15.4-2011 to meet the requirements of process automation. The DLL protocol stack is shown in Figure 28.

**Figure 28 – WIA-PA DLL protocol stack**

The WIA-PA DLL includes the following parts:

- a) the IEEE STD 802.15.4-2011 MAC, which handles the mechanisms of sending and receiving individual data frames;
- b) the DLSL, which handles the aspects of communication resource.

8.3 MAC overview and function extension

8.3.1 MAC overview

The following section specifies the MAC of the WIA-PA standard and the content of IEEE STD 802.15.4-2011 MAC is not stated in this document. This document is based on the IEEE STD 802.15.4-2011 beacon-enabled MAC, which handles all access to the physical radio channel and is responsible for the following tasks:

- a) generating network beacons if the device is a gateway device or a routing device,
- b) synchronizing to network beacons,
- c) supporting network point to point association and disassociation,
- d) supporting point to point security,
- e) employing the timeslotted CSMA-CA mechanism for device joining,
- f) handling and maintaining the GTS mechanism, and
- g) providing a reliable link between two peer MAC entities.

Field devices and handheld devices correspond to the Reduced-Function Device (RFD), and routing devices and gateway devices correspond to the Full-Function Device (FFD). None of the optional functions of RFD and FFD in IEEE STD 802.15.4-2011 are required in this standard.

8.3.2 General requirements based on IEEE STD 802.15.4-2011

The WIA-PA MAC shall be based on IEEE STD 802.15.4-2011 MAC with additional requirements and exceptions as specified herein.

The GW acts as the PAN coordinator in IEEE STD 802.15.4-2011 and the routing devices act as coordinators in IEEE STD 802.15.4-2011.

Table 33 specifies the IEEE STD 802.15.4-2011 MAC selection for a WIA-PA device.

Table 33 – MAC protocol selection (1 of 2)

Clause of IEEE STD 802.15.4-2011	Header	Presence	Constraints
5	MAC protocol		
5.1	MAC functional description		
5.1.1	Channel access	YES	
5.1.2	Starting and maintaining PANs	Partial	Only active scan is used in WIA-PA.
5.1.3	Association and disassociation	YES	
5.1.4	Synchronization	YES	
5.1.5	Transaction handling	NO	Transactions can be instigated from the devices themselves.
5.1.6	Transmission, reception, and acknowledgement	YES	
5.1.7	GTS allocation and management	NO	This function is not used in WIA-PA.
5.1.8	Ranging	NO	This function is not used in WIA-PA.
5.2	MAC frame formats		
5.2.1	General MAC frame format	YES	For WIA-PA MAC frame format, the value of the Security Enabled subfield of MHR shall be set to 0 and the length of the Auxiliary Security Header subfield is 0 octets. The PAN ID Compression is set to 1. The length of Source PAN identifier field is 0 and the Destination PAN Identifier is set to NetworkID (see 6.9.1.2.1) of WIA-PA.
5.2.2	Format of individual frame types	YES	
5.2.3	Frame compatibility	YES	
5.3	MAC command frames	Partial	See following 5.3.1 to 5.3.9.
5.3.1	Association request command	YES	
5.3.2	Association response command	YES	
5.3.3	Disassociation notification command	YES	
5.3.4	Data request command	YES	
5.3.5	PAN ID conflict notification command	NO	PAN ID conflict notification command is not used in WIA-PA.
5.3.6	Orphan notification command	NO	Orphan notification command is not used in WIA-PA.
5.3.7	Beacon request command	NO	Beacon request command is not used in WIA-PA.
5.3.8	Coordinator realignment command	NO	Coordinator realignment command is not used in WIA-PA.
5.3.9	GTS request command	NO	GTS request command is not used in WIA-PA.

Table 33 (2 of 2)

Clause of IEEE STD 802.15.4-2011	Header	Presence	Constraints
6	MAC service		
6.1	Overview		
6.2	MAC management service	Partial	See following 6.2.1 to 6.2.17.
6.2.1	Common requirements for MLME primitives	YES	
6.2.2	Association primitives	YES	
6.2.3	Disassociation primitives	YES	
6.2.4	Communications notification primitives	YES	
6.2.5	Primitives for reading PIB attributes	YES	
6.2.6	GTS management primitives	NO	GTS management primitives are not used in WIA-PA.
6.2.7	Primitives for orphan notification	NO	Primitives for orphan notification are not used in WIA-PA.
6.2.8	Primitives for resetting the MAC sublayer	NO	After a node leaving the WIA-PA network, its MAC sublayer resets to the default value.
6.2.9	Primitives for specifying the receiver enable time	YES	
6.2.10	Primitives for channel scanning	YES	
6.2.11	Primitives for writing PIB attributes	YES	
6.2.12	Primitives for updating the superframe configuration	NO	Primitives for updating the superframe configuration are not used in WIA-PA.
6.2.13	Primitives for synchronizing with a coordinator	NO	Primitives for synchronizing with a coordinator are not used in WIA-PA.
6.2.14	Primitives for requesting data from a coordinator	NO	Primitives for requesting data from a coordinator are not used in WIA-PA.
6.2.15	Primitives for specifying dynamic preamble	NO	Primitives for specifying dynamic preamble are not used in WIA-PA.
6.2.16	Primitives for channel sounding	NO	Primitives for channel sounding are not used in WIA-PA.
6.2.17	Primitives for ranging calibration (for UWB PHYs)	NO	Primitives for ranging calibration (for UWB PHYs) are not used in WIA-PA.
6.3	MAC data service	Partial	Following 6.3.1 to 6.3.3 are used in WIA-PA.
6.3.1	MCPS-DATA.request	YES	
6.3.2	MCPS-DATA.confirm	YES	
6.3.3	MCPS-DATA.Indication	YES	
6.3.4	MCPS-PURGE.request	NO	The MCPS-PURGE.request is not used in WIA-PA.
6.3.5	MCPS-PURGE.confirm	NO	The MCPS-PURGE.confirm is not used in WIA-PA.
6.4	MAC constants and PIB attributes		
6.4.1	MAC constants	YES	
6.4.2	MAC PIB attributes	Partial	See Table 34 for details.
6.4.3	Calculating PHY dependent MAC PIB values	YES	

This document includes the attributes specified in the IEEE STD 802.15.4-2011, 6.4.2 and additional attributes that apply only to this document. Some of these attributes are assigned a constant value as shown in Table 34.

Table 34 – MAC PIB attributes

Attribute	Comment
macAckWaitDuration	Only value 54 symbols is included for 2,4 GHz PHY
macAssociatedPANCoord	Only value FALSE is included
macAssociationPermit	Only value TRUE is included
macAutoRequest	Only value FALSE is included
macBattLifeExt	Only value FALSE is included
macBattLifeExtPeriods	This attribute is invalid in WIA-PA
macBeaconPayload	The contents of the beacon payload are extended in WIA-PA
macBeaconPayloadLength	Only value 10 is included
macBeaconTxTime	Only value 0x000000 is included
macCoordExtendedAddress	This attribute is invalid in WIA-PA
macCoordShortAddress	This attribute is invalid in WIA-PA
macGTSPermit	Only value FALSE is included
macMaxFrameTotalWaitTime	Only when phyMaxFrameDuration is 266
macMinLIFSPeriod	Only value 40 is included (for 2,4 GHz PHY)
macMinSIFSPeriod	Only value 12 is included (for 2,4 GHz PHY)
macPromiscuousMode	Only value TRUE is included
macRangingSupported	Only value FALSE is included
macSecurityEnable	Only value FALSE is included
macSyncSymbolOffset	0x000-0x100 for the 2,4 GHz PHY
macTxControlActiveDuration	This attribute is invalid in WIA-PA
macTxControlPauseDuration	This attribute is invalid in WIA-PA

8.3.3 MAC function extension

8.3.3.1 General

This document extends one MAC PIB attribute. The extended PIB attribute is listed in Table 35.

Table 35 – MAC extended PIB attributes

Attribute	Type	Range	Description	Default
macBeaconNum	Integer	1-15	The number of beacon transmissions in one timeslot	1

macBeaconNum is used to indicate the number of beacon transmissions in one timeslot.

8.3.3.2 Beacon payload

The WIA-PA network uses the IEEE STD 802.15.4-2011 MAC beacon payload to distribute superframe information. In IEEE STD 802.15.4-2011, see 5.2.2.1 for the frame format of the MAC beacon.

The beacon payload is shown in Table 36.

Table 36 – Beacon payload

	Beacon payload			
Length in octet(s)	1	6	2	1
Field name	ClusterID	ASN	Timevalue	NextBcnChannel

The subfields in Table 36 are defined as follows:

- ClusterID indicates the identifier of the cluster;
- ASN indicates the absolute timeslot number. Its value shall increase by one (does not decrease). Its current value is always the sequence number of the current timeslot. The maximum value shall be $(2^{48}-1)$. After the maximum value, it shall re-count from zero;
- See Table 60 for Timevalue; and
- NextBcnChannel indicates the channel used to transmit the next beacon.

8.3.3.3 Association request command frame

The WIA-PA network device uses the IEEE STD 802.15.4-2011 MAC association request command frame to join the WIA-PA network. See 5.3.1 in IEEE STD 802.15.4-2011 for the frame format of the MAC association request command frame.

The types of WIA-PA network devices are indicated by Bit 1 in the Capability Information field (See Figure 50 in IEEE STD 802.15.4-2011) of the MAC association request command frame.

The format of the Capability Information field of the MAC association request command frame is shown in Table 37.

Table 37 – Format of Capability Information field

	Format of Capability Information field						
Length in bit(s)	1	1	1	1	2	1	1
Subfield name	Reserved	Device type	Power source	Receiver on when idle	Reserved	Security capability	Allocated address

The subfields in Table 37 are listed as follows:

- the Device type subfield is extended to indicate the WIA-PA device type; 0 indicates the routing device and 1 indicates the field device or handheld device;
- see IEEE STD 802.15.4-2011, 5.3.1.2 for the power source subfield, receiver on when idle subfield, security capability subfield, and allocated address subfield.

8.4 DLSL function description

8.4.1 General

The DLSL provides a service interface between the NL and the MAC. The DLSL conceptually includes a Data Link Sub-Layer Data Entity (DLDE) and a Data Link Sub-Layer Management Entity (DLME). The DLDE provides data service interfaces. The DLME provides layer management services such as the configuration of the parameters of DLSL and the monitoring of the operation status of DLSL.

Figure 29 depicts the components and interfaces of the DLSL.

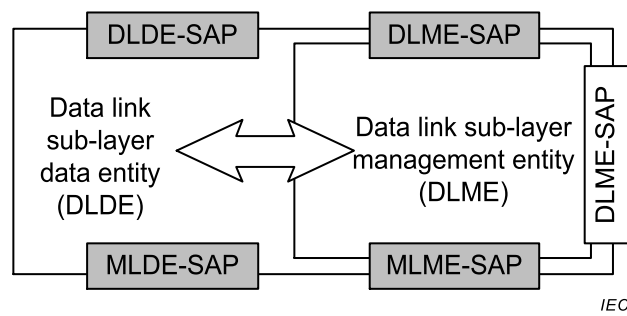


Figure 29 – WIA-PA DLSL reference model

The DLSL provides two services, which are accessed through following two Service Access Points (SAPs):

- a) the DLSL data service, which is accessed through the DLDE Service Access Point (DLDE-SAP);
- b) the DLSL management service, which is accessed through the DLME-SAP.

In this document, the main function of the DLSL is to allocate communication resources among competitive users in order to avoid collisions, improve throughput, and increase bandwidth utilization. The main concepts of the DLSL include timeslot, superframe and link, which are defined as follows.

- a) Timeslot is the basic time unit in packet exchange. The WIA-PA timeslot duration is configurable.
- b) Superframe is a collection of timeslots repeating on a cyclic schedule. The number of timeslots in a given superframe determines the communication cycle for the WIA-PA devices that use the timeslots.
- c) Link includes time and frequency. A link assignment specifies how the device uses a set of superframe timeslots. The link types include transmitting, receiving and transmit-shared. The sharing link allows more than one device to contend this link for packet exchange at the same time. The transmitting and receiving links should only allow designated devices to exchange packets.

8.4.2 Coexistence

The WIA-PA network should consider the following coexistence strategies:

- a) the WIA-PA network extends the IEEE STD 802.15.4-2011 superframe structure;
- b) the WIA-PA DLSL together with the NM achieves coexistence with other wireless networks. The WIA-PA DLSL incorporates several strategies to optimize coexistence:
 - timeslot communication;
 - low duty-cycle;
 - multi-channel;
 - frequency hopping (FH); and
 - collision avoidance.

8.4.3 Timeslot communication

The key requirement of timeslot communication is to guarantee that all transactions occur in a timeslot according to specific timing requirements. That is to say, all packets should be exchanged in a prescriptive timeslot and not be delayed. The timeslot length of WIA-PA DLSL is fully compatible with the timeslot length of IEEE STD 802.15.4-2011.

The timeslot duration is configured by the NM after devices join the network.

8.4.4 WIA-PA superframe

In order to guarantee real-time and reliable communication, this document only takes account of the beacon-enabled IEEE STD 802.15.4-2011 superframe structure.

The WIA-PA superframe structure is shown in Figure 30.

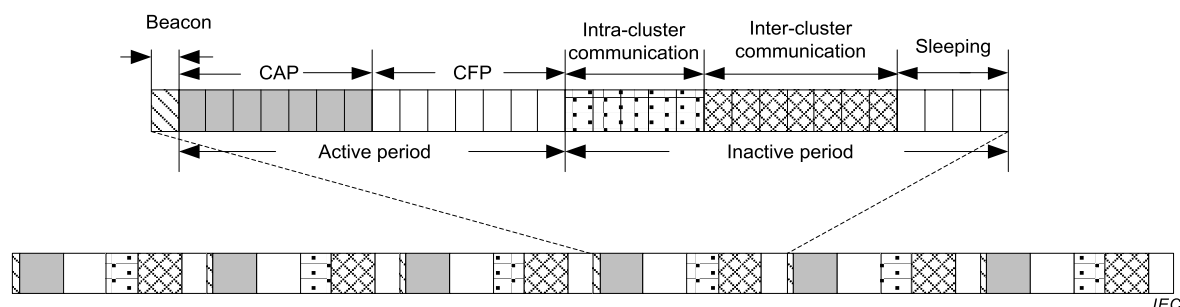


Figure 30 – WIA-PA superframe

The periods of the WIA-PA superframe are defined as follows:

- the CAP period defined in the IEEE STD 802.15.4-2011 superframe is used for device joining, intra-cluster management and retry in the WIA-PA superframe;
- the CFP period defined in the IEEE STD 802.15.4-2011 superframe is used for communication between handheld devices and their cluster head in the WIA-PA superframe; and
- the inactive period defined in the IEEE STD 802.15.4-2011 superframe is used for intra-cluster communication, inter-cluster communication, and sleeping in the WIA-PA superframe.

The NM should generate WIA-PA superframes. The superframe lengths of routing devices are different, and are set as the lowest data update rate of all the members in a cluster. The timeslot types of WIA-PA superframe includes shared timeslots and dedicated timeslots. Shared timeslots are used for transmission of aperiodic data, and dedicated timeslots are used for intra- and inter-cluster transmission of periodic data.

Because the inactive period defined in the IEEE STD 802.15.4-2011 superframe is used for intra-cluster communication, inter-cluster communication, and sleeping in the WIA-PA superframe, the WIA-PA basic superframe duration is defined as thirty-two timeslots. The duration of the WIA-PA superframe is defined as 2^N (N is a natural integer) times the WIA-PA basic superframe duration.

Each routing device has only one superframe and the communication among routing devices happens during the overlapped inter-cluster timeslots. Each field device has only one superframe; the communication among field device and routing device happens during the intra-cluster timeslots.

8.4.5 Frequency hopping

The WIA-PA network supports frequency hopping, and the hopping sequence is designated by the NM. Frequency hopping in the WIA-PA network includes three mechanisms: AFS, AFH, and TH.

Adaptive frequency switch (AFS): in the WIA superframe, the beacon, CAP and CFP use the same channel in the same superframe cycle, and change the channel according to the channel conditions in different superframe cycles. That is to say, bad channel condition, which

means that the packet drop rate is above PLRThreshold, triggers the operation of changing channels. See 6.9.1.2.1 for PLRThreshold.

Adaptive frequency hopping (AFH): irregularly changes communication channels per timeslot of the WIA superframe according to actual channel condition. The channel conditions are measured in retry times. If the channel condition is bad and the retry times of the sender reaches the value of ChannelThreshold, the sender chooses the next channel in sequence from IntraChanel[] and notifies the receiver during the next retry timeslot by using the main channel (see Table 17). If the receiver does not receive the notification, it counts its retry times continuously. When the retry times of the receiver reach the value of ChannelThreshold, the receiver chooses the next channel from IntraChanel[] during the (ChannelThreshold+2)th timeslot. If the receiver receives the notification of a channel switch, it changes the communication channel and returns ACK; otherwise, it does not change the communication channel and retries data by using the main channel. If the retry times of the sender reach macMaxFrameRetries, the sender discards the current packet and transmits the next packet by using the main channel. If the communication between the sender and the receiver is successful before the retry times of the sender reaches macMaxFrameRetries, the sender transmits the next packet by using the standby channel. The Intra-cluster period adopts the AFH mechanism. See 6.9.1.2.1 for ChannelThreshold and IntraChanel[]; see Table 52 in IEEE STD 802.15.4-2011 for the information of macMaxFrameRetries.

The current channel in IntraChanel[] used by sender and receiver is marked as main channel, while other channels in IntraChanel[] are marked as standby channels.

Timeslot Hopping (TH): regularly changes communication channels per timeslot of the WIA superframe to combat interference and fading. The Inter-cluster period adopts the TH mechanism. The hopping structure is: <timeslot 1, channel 1><timeslot 2, channel 2>... <timeslot i, channel i>.

The specific hopping mechanisms of DLSP in the WIA-PA network are shown in Table 38.

Table 38 – Hopping mechanisms

IEEE STD 802.15.4-2011	WIA-PA	Basic MAC mechanism		DLSL Hopping mechanism
Beacon	Beacon	TDMA	Frequency Division Multiple Access (FDMA) and TDMA	AFS
CAP	CAP	CSMA		
CFP	CFP	TDMA		
Inactive	Intra-cluster period	TDMA		AFH
	Inter-cluster period	TDMA		TH
	Sleeping			

Different routing devices use different channels in the active period. If the number of channels is not enough, the WIA-PA network uses the TDMA mechanism to enhance the system capacity. The start time of a superframe is configured by the NM. For example, there are three routing devices R1, R2, and R3 in the WIA-PA network. The superframe lengths of R1, R2 and R3 are respectively one, two and four WIA-PA basic superframe duration(s), as shown in Figure 31. According to the superframe definition, the active period of R1 cannot be multiplexed with the active periods of R2 and R3. However, the active periods of R2 and R3 may be multiplexed with each other. The active periods of R2 and R3 may use the same channel, while the active period of R1 should use a different channel from that of the active periods of R2 and R3.

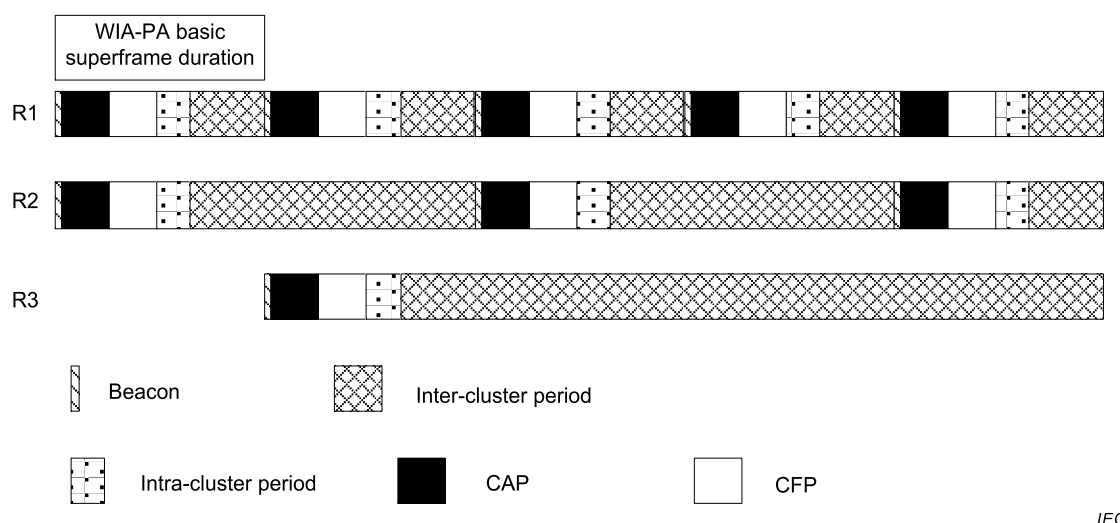


Figure 31 – R1, R2 and R3 superframe structures

8.4.6 Transmission of long cycle data

The long cycle data is defined as the data update rate of a device that is either greater than the maximum superframe length of IEEE STD 802.15.4-2011 or is greater than the data update rate of the routing device in a cluster.

To indicate the transmission of the long cycle data, this document defines a parameter termed TransmitFlag. TransmitFlag is defined as follows:

$$\text{TransmitFlag} = \lceil (\text{AbsoluteSlotNumber} - \text{ActiveSlot} + 1) / \text{NumberSlots} \rceil \% \text{SuperframeMultiple}$$

where

AbsoluteSlotNumber	see 6.9.1.2;
ActiveSlot	see 6.9.1.2;
NumberSlots	see 6.9.1.2;
SuperframeMultiple	see 6.9.1.2.

In every superframe cycle, field devices receive the beacons and decide whether to send data in this superframe cycle. The process of long cycle data transmission is described as follows:

- If $0 < \text{TransmitFlag} < \text{SuperframeMultiple}$ and $\text{TransmitFlag} = \text{LinkSuperframeNum}$, then the field device transmits data in this superframe cycle.
- If $\text{TransmitFlag} = 0$ and $\text{LinkSuperframeNum} = \text{SuperframeMultiple}$, then the field device transmits data in this superframe cycle.

See Table 17 for LinkSuperframeNum.

Figure 32 is an example of long cycle data transmission.

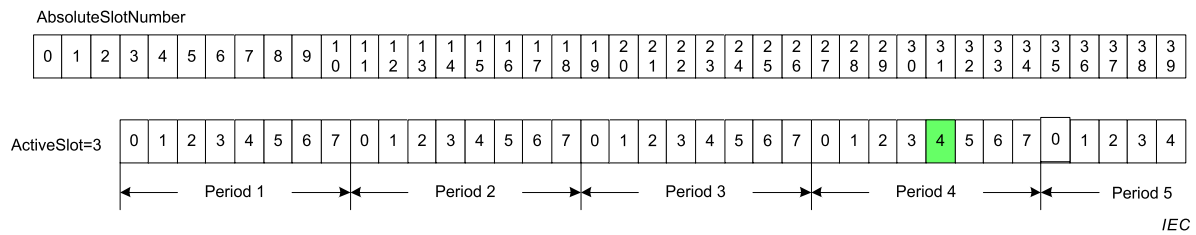


Figure 32 – An example of long cycle data transmission

In Figure 32, ActiveSlot = 3, NumberSlots = 8, SuperframeMultiple = 4, and LinkSuperframeNum = 4.

If the current absolute slot of a beacon is 27 (AbsoluteSlotNumber = 27), *TransmitFlag* is calculated as follows:

$$TransmitFlag = \lceil (27 - 3 + 1) / 8 \rceil \% 4 = 0$$

According to the calculation result, it can be concluded that *TransmitFlag* = 0 and that *SuperframeMultiple* = *LinkSuperframeNum*, which indicates that the packet should be sent during the current superframe cycle.

8.4.7 Retry strategy

The NM in the mesh network and the routing devices in the star network should allocate some timeslots for retries. The retry strategy supports the frequency hopping mechanisms (see 8.4.5).

The number of retry timeslots is bound by the constant *macMaxFrameRetries* in the IEEE STD 802.15.4-2011 MAC PAN Information Base (PIB).

8.4.8 Management service

The WIA-PA DLSL provides management services to the upper layer and the DMAP with DLME-SAP. The services include network discovery, device joining and leaving, resource allocation and operations of management database attributes (see Clause 6).

8.4.9 Radio link quality and channel condition measurement

Radio link quality and channel condition measurements include the link quality measurement of each pair of neighbours and the channel condition measurement of each channel. The collected information may be accumulated at the DLSL and reported through the DMAP. Link quality and channel condition are used to dynamically allocate communication resources.

Generally, the radio link quality measurement is performed according to the following performance indices:

- average signal level received from the neighbour devices in the statistics duration;
- non-broadcast packets sent to the neighbour devices in the statistics duration;
- count of ACK that is not received in the statistics duration; and
- count of the non-broadcast packets received from the neighbour devices in the statistics duration.

The channel condition measurement is performed according to the following performance data:

- a) LQI per link;
- b) packet loss rate per link, which is determined by the count of received ACK and packets that are sent; and
- c) average count of retries per link.

8.4.10 Security

The WIA-PA DLSL applies the MIC mechanism and encryption technology to guarantee the integrity and confidentiality of the communication. See Clause 11 for details.

8.4.11 Country code

The regulatory considerations of DLME are configured through its CountryCode attribute (see 6.9.1.2.1), which is a 16-bit value where:

- a) bits 0-9 provide a 10-bit country code, using ISO 3166-1 numeric three-digit country codes;
- b) bit 10 indicates whether European spectrum regulation apply (0 = no, 1 = yes). A DLME shall operate in compliance with European spectrum regulation when Bit10 = 1;
- c) bit 11 indicates whether FCC rules apply (0 = no, 1 = yes). A DLME should operate in compliance with FCC rules when Bit11 = 1;
- d) bit 12 indicates whether a 10 dBm EIRP limit applies (0 = no, 1 = yes). A DLME should limit its emissions to ≤ 10 dBm EIRP when Bit12 = 1;
- e) bit 13 indicates whether the DLME is considered to be operating under adaptive or non-adaptive rules (0 = non-adaptive, 1 = adaptive);
- f) bit 14 indicates whether the DLME is considered to be operating under frequency-hopping spread-spectrum rules (0 = not-FHSS-rules, 1 = FHSS-rules);
- g) bit 15 indicates whether the value of this attribute is fixed (0 = no, 1 = yes) while the DLME is operational. Once this bit is set, any subsequent attempt to modify this attribute shall be rejected except when it occurs while the DLME is being provisioned.

NOTE 1 This feature supports device operation in regulatory regimes that prohibit the ability to reconfigure a device in such a way that it would violate regulatory restraints, and while still permitting the repair or refurbishment of devices with subsequent resale into markets where other regulations apply.

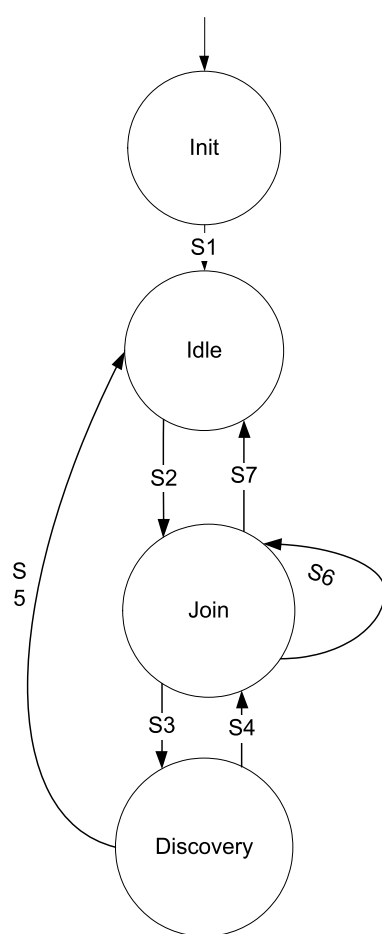
When no specific country of intended use has been identified, the default value for CountryCode shall be 0x3C00, indicating that a device in the default state should comply with ETSI rules, FCC rules, the 10 dBm EIRP limit, and be classified as an adaptive non-FHSS device. See Annex D.

NOTE 2 This default value of CountryCode ensures that the equipment, before it has been provisioned, meets the regulatory requirements of most regions in which it might be deployed. The value of CountryCode could be changed during wired provisioning to reflect the intended regulatory regime that applies to the device's locale of deployment.

8.4.12 DLSL state machine

The WIA-PA DLSL state machine is divided into two state machines: one for device joining and the other for in-network running.

The WIA-PA DLSL state machine for device joining is shown in Figure 33.



IEC

Figure 33 – DLSL state machine for device joining

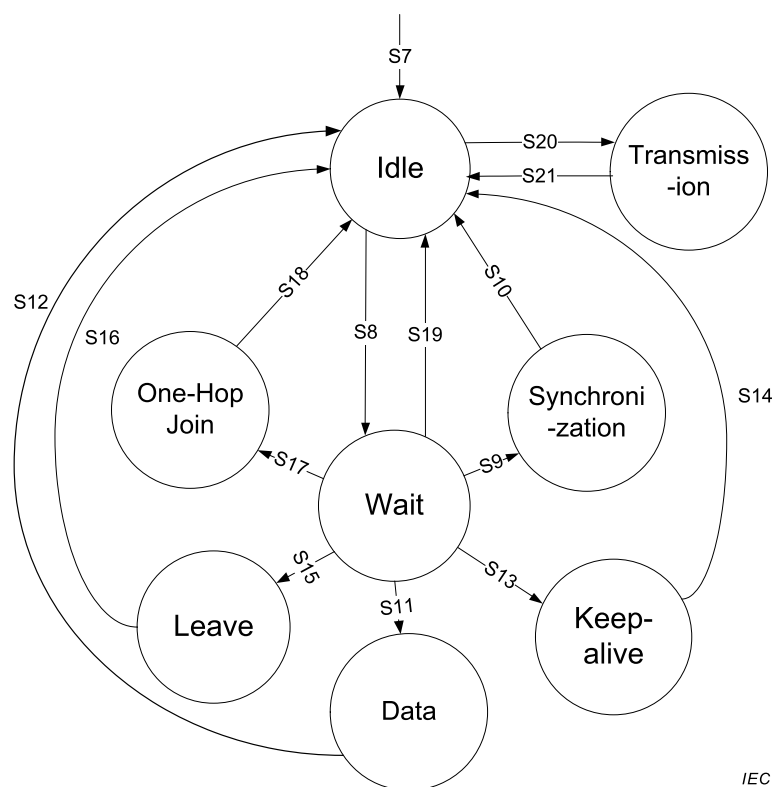
The DLSL state transitions for device joining are shown in Table 39.

Table 39 – DLSL state transitions for device joining

Sequence number #	Current state	Event or condition	Actions	Next state
S1	Init		Initiation	Idle
S2	Idle	Devicestate = Not joined		Join
S3	Join	DLME-DISCOVERY.request()	Parsing the discovery request message and invoke MLME-SCAN.request()	Discovery
S4	Discovery	MLME-SCAN.confirm (status = SUCCESS) and MLME-BEACON-NOTIFY.indication()	Parsing the scan confirm message and beacon notification message; invoke DLME-DISCOVERY.confirm(SUCCESS)	Join
S5	Discovery	MLME-SCAN.confirm (status != SUCCESS) or no confirm received		Idle
S6	Join	DLME-JOIN.request()	Setting Devicestate = Joining; generating association request message and Invoke MLME-ASSOCIATE.request()	Join
S7	Join	MLME-ASSOCIATE.confirm() or no confirm received	If MLME-ASSOCIATE.confirm() received, parsing the associate confirm message: if status = SUCCESS, invoke DLME-JOIN.confirm(Status = SUCCESS) and setting Devicestate = Joined; if status != SUCCESS, invoke DLME-JOIN.confirm(). If no confirm received, no actions.	Idle

After a device joined WIA-PA network, that is Devicestate = Joined, the DLSL runs its state machine for in-network running.

The WIA-PA DLSL state machine for in-network running is shown in Figure 34.



IEC

Figure 34 – DLSL state machine for in-network running

The DLSL state transitions for in-network device are shown in Table 40.

Table 40 – DLSL state transitions for in-network running (1 of 3)

Sequence number #	Current state	Event or condition	Actions	Next state
S8	Idle	Timeslot timeout LinkType = Receiving or LinkType = Transmit-shared	Invoke MLME-RX-ENABLE. request ()	Wait
S9	Wait	From MAC: MLME-COMM-STATUS.indication() or MCPS-DATA.indication(); From DMAP: DLME-TIME-SYN.request()		Synchroniza tion
S10	Synchroniza tion		From MAC: parsing MLME communication status indication message and invoke DLME-TIME-SYN.confirm() or parsing DLPDU from MAC data frame.If Frametype = 1 and Command frame identifier = 11 in DLPDU, invoke DLME-TIME-SYN.indication(); From DMAP: generating DLSL time request command frame and invoke MCPS-DATA.request().	Idle
S11	Wait	From MAC: MCPS-DATA.confirm()or MCPS-DATA.indication(); From NL: DLDE-DATA.request()		Data

Table 40 (2 of 3)

Sequence number #	Current state	Event or condition	Actions	Next state
S12	Data		From MAC: invoke DLSD- DATA.confirm() or parsing DLPDU. If Frame type = 0 in DLPDU, evaluate the LinkQuality and PacketLossRate and invoke DLDE-DATA.indication(); From NL: MCPS-DATA.request()	Idle
S13	Wait	From MAC: MLME-COMM- STATUS.indication() or MCPS-DATA.indication(); From DMAP: DLME-KEEP- LIVE.request()		Keep-alive
S14	Keep-alive		From MAC: parsing MLME communication status indication message and invoke DLME - KEEP-LIVE.confirm() or parsing DLPDU from MAC data frame.If Frame type = 1 and Command frame identifier = 10 in DLPDU, invoke DLME-KEEP- ALIVE.indication(); From DMAP: invoke MLME-KEEP- LIVE.request()	Idle
S15	Wait	From MAC: MLME- DISASSOCIATE.indication() or MLME- DISASSOCIATE.confirm(); From DMAP: DLME-LEAVE.request()		Leave
S16	Leave		From MAC: parsing DLSD leave indication message or confirm message and invoke DLME- LEAVE.indication() or DLME- LEAVE.confirm(); From DMAP: parsing DLSD leave request message and invoke MLME-DISASSOCIATE.request()	Idle
S17	Wait	From MAC:MLME- ASSOCIATE.indication() or MLME-ASSOCIATE.confirm() From DMAP: DLME-JOIN. request () or DLME-JOIN. response ()		One-Hop Join
S18	One-Hop Join		From MAC: parsing MAC association indication message or confirm message and invoke DLME-JOIN.indication() or DLME- JOIN.confirm(); From DMAP: parsing DMAP join request or response message and invoke MLME- ASSOCIATE.request() or MLME- ASSOCIATE.response()	Idle
S19	Wait	From MAC: MLME-COMM- STATUS.indication() and no frame received or received failed From DMAP and NL: no message received	From MAC: invoke DLME-COMM- STATUS.indication(FAILURE_ELS E)	Idle

Table 40 (3 of 3)

Sequence number #	Current state	Event or condition	Actions	Next state
S20	Idle	Timeslot timeout LinkType = Transmitting or LinkType = Transmit-shared	Invoke MCPS-DATA.request()	Transmission
S21	Transmission	MCPS-DATA.confirm()	Reschedule or retry frame if transmit failed; Release frame's buffer if MCPS- DATA.confirm (SUCCESS);	Idle

See 8.5 for DLSP related primitives; see 8.7 for DLSP frame formats; see 9.4 and 9.5 for NL related primitives; see IEEE STD 802.15.4-2011, 6.2 for MAC related primitives; see 6.9.1.2.1 for Devicestate.

The states in DLSP state machine are specified as follows.

a) Join state

This state handles the joining procedure of a device. After a device joins the network, the DLSP runs its state machine as in Figure 34.

b) Leave state

This state handles the leaving procedure of a device.

c) Idle state

After a device joins the network, the DLSP enters the Idle state. The following transitions may occur while the DLSP is in the Idle state:

- When a timeslot arrives, the DLSP enters either the Transmission state or the Receive state according to the link options (transmitting, receiving or transmit-shared).

d) Transmission state

When the timeslot arrives and the link option is a transmit link, the DLSP enters the Transmission state. The following events will happen while the DLSP is in the Transmission state.

- Successful propagation of a frame with a broadcast/multicast destination address happens as soon as the frame is transmitted. The frame's buffer is then released.
- Successful propagation of a frame with a unicast destination address occurs when a validated and successful confirmation is received from the local MAC layer. This indicates that message propagation has been completed successfully; the frame's buffer is then released.
- If a failure confirmation is received from the local MAC layer, the frame should be retried.
- If a response with an error or no response is received, the frame should be re-scheduled or retried.

e) Wait state

The frames that a device can receive include frames whose final destination addresses are this device and frames whose final destination addresses are not this device. The functions of the Wait state are to receive, check and process the frame. The following transitions may occur while the DLSP is in the Wait state.

- If there is no frame received, the DLSP will evaluate the link and return to the Idle state.
- If a beacon frame or a time synchronization command frame is received, then the Synchronization state is entered.
- If a keep-alive command frame is received, then the Keep-alive state is entered.
- If a DMAP leave request is received, then the Leave state is entered.

- If a join command is received from DMAP, then the One-Hop Join state is entered.
- Upon successful frame reception, the DLSL will process the frame according to frame priority (receive or discard), and then the device returns directly to the Idle state.

f) Data state

In this state, the DLSL data is generated or parsed. After received the DLSL data frame, the LinkQuality and PacketLossRate are evaluated. After generating the DLSL data frame, the DLSL enters Wait state.

g) Synchronization state

In this state, time synchronization is executed after a device receives a beacon frame or a time synchronization command frame, and then the DLSL enters Idle state.

h) Keep-alive state

In this state, a neighbour node is marked as keep-alive after a device receives a keep-alive command frame, and then the DLSL enters Idle state.

i) One-Hop Join state

In this state, the one-hop join process is supported by GW device.

8.5 Data link sub-layer data services

8.5.1 General

The DLDE-SAP supports the point-to-point transmission of DLSL Protocol Data Units (DLPDUs) between devices. The primitives supported by DLSL data services include DLDE-DATA.request, DLDE-DATA.confirm, and DLDE-DATA.indication.

8.5.2 DLDE-DATA.request

The DLDE receives the payload from the NL through a DLDE-DATA.request and adds it to the message queue of the DLSL.

The semantics of DLDE-DATA.request are as follows:

```
DLDE-DATA.request (
    NetworkID,
    SrcAddrMode,
    SrcAddr,
    DstAddrMode,
    DstAddr,
    Priority,
    Type,
    PayloadLength,
    Payload,
    PayloadHandle
)
```

Table 41 specifies the parameters for DLDE-DATA.request.

Table 41 – DLDE-DATA.request parameters

Name	Data type	Valid range	Description
NetworkID	Unsigned8	0 to 255	Network identifier
SrcAddrMode	Unsigned8	0 to 3	Mode of source address: 0 = No address; 1 = Reserved; 2 = 16-bit short address; 3 = 64-bit long address.
SrcAddr	Unsigned16/64	0 to 65 535 or $(2^{64}-1)$	Source address 64-bit long address is used only in device joining process, and 16-bit short address is used generally.
DstAddrMode	Unsigned8	0 to 3	Mode of destination address: 0 = No address; 1 = Reserved; 2 = 16-bit short address; 3 = 64-bit long address.
DstAddr	Unsigned16/64	0 to 65 535 or $(2^{64}-1)$	Destination address, 16- or 64-bit
Priority	Unsigned8	0 to 15	Priority of the payload
Data type	Unsigned8	0 to 1	0 = Intra-cluster transmission; 1 = Inter-cluster transmission.
PayloadLength	Unsigned8	$\leq \text{MaxMACFrameSize}$	Length of payload
Payload	Octetstring		Payload
PayloadHandle	Unsigned8	0 to 255	Handle allocated when call DLDE-DATA.request

8.5.3 DLDE-DATA.confirm

The semantics of DLDE-DATA.confirm are as follows:

```
DLDE-DATA.confirm (
    PayloadHandle,
    Status
)
```

Table 42 specifies the parameters for DLDE-DATA.confirm.

Table 42 – DLDE-DATA.confirm parameters

Name	Data type	Valid range	Description
PayloadHandle	Unsigned8	0 to 255	Handle allocated when call DLDE-DATA.confirm
Status	Unsigned8	0 to 255	Result of the data transmission of DSL: 0 = SUCCESS; 1 = TRANSACTION_OVERFLOW; 2 = TRANSACTION_EXPIRED; 3 = NO_ACK; 4 = CHANNEL_ACCESS_FAILURE; 5 = UNAVAILABLE_KEY; 6 = FAILED_SECURITY_CHECK; 7 = INVALID_PARAMETER; Others are reserved. See Table 43 for more detail

Table 43 – Status table

ID	Value	Description
0	SUCCESS	The requested operation is completed successfully. For a transmission request, this value indicates a successful transmission.
1	TRANSACTION_OVERFLOW	Not enough space for storing transactions
2	TRANSACTION_EXPIRED	Transaction has expired and its information is discarded
3	NO_ACK	No acknowledgement message is received after macMaxFrameRetries
4	CHANNEL_ACCESS_FAILURE	Cannot transmit due to channel access failure
5	UNAVAILABLE_KEY	No valid key in access control list
6	SECURITY_ERROR	Cryptographic processing of the received secured frame failed
7	INVALID_PARAMETER	A parameter in the primitives out of value range
8	NO-BEACON	A scan operation failed to find any network beacons
9 to 255	Reserved	

8.5.4 DLDE-DATA.indication

The semantics of DLDE-DATA.indication are as follows:

```
DLDE-DATA.indication (
    NetworkID,
    ScrAddrMode,
    SrcAddr,
    Type,
    Priority,
    PayloadLength,
    Payload,
    PayloadLinkQuality,
)
```

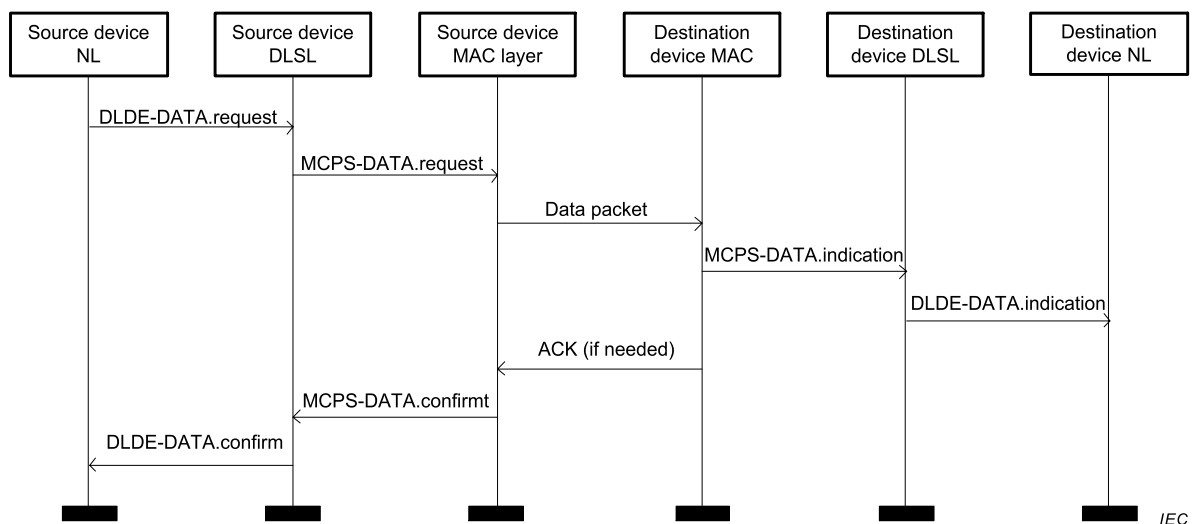
Table 44 specifies the parameters for DLDE-DATA.indication.

Table 44 – DLDE-DATA.indication parameters

Name	Data type	Valid range	Description
NetworkID	Unsigned8	0 to 255	Network identifier
SrcAddrMode	Unsigned8	0 to 3	The source address mode. Four options are available: 0 = No address; 1 = Reserved; 2 = 16-bit short address; 3 = 64-bit long address.
SrcAddr	Unsigned16/64	0 to 65 535 or $(2^{64}-1)$	Source address, using 64-bit long address only in device join process, and using 16-bit short address generally
Type	Unsigned8	0 to 1	0 = Intra-cluster transmission; 1 = Inter-cluster transmission.
Priority	Unsigned8	0 to 15	Priority of payload
PayloadLength	Unsigned8	$\leq \text{MaxMACFrameSize}$	Length of payload
Payload	Octetstring		Payload
PayloadLinkQuality	Unsigned8	0 to 255	LQI value measured during reception of the DLPDU Lower values represent lower link quality.

8.5.5 Time sequence of DLSL data service

Figure 35 shows the data transaction sequence of transporting one data packet from the source device to the destination device.

**Figure 35 – Time sequence of data service**

DLDE-DATA.request is generated by a local Network Layer Data Entity (NLDE) when a Network Protocol Data Unit (NPDU) is to be transferred to a peer NLDE.

On receipt of DLDE-DATA.request, DLDE inserts the message into the sending buffer and begins sending the supplied DLPDU.

DLDE-DATA.confirm is generated by the DLDE of a source device in response to DLDE-DATA.request. DLDE-DATA.confirm returns a status indicating the result of the transmission.

8.6 Data link sub-layer management services

The upper layer uses the DLME-SAP to send management commands to the DLSL. The DLSL management services include subnet discovery, device joining and leaving, channel condition collection and report, neighbour information collection and report, and time synchronization.

8.6.2.1 General

8.6.2.2 DLME-DISCOVERY.request

The semantics of DLME-DISCOVERY.request are as follows:

Table 45 specifies the parameters for DLME-DISCOVERY.request.

Name	Data type	Valid range	Description
ScanChannels	Unsigned32	32-bit Bits-Map	Bit 11 to bit 26 indicate IEEE STD 802.15.4-2011 channels of 2,4 GHz frequency band; others are set. See IEEE STD 802.15.4-2011, 6.2.10 for ScanChannels.
ScanDuration	Unsigned8	0 to 14	A value used to calculate the length of time to spend scanning each channel of ED, active, and passive scans This parameter is ignored for orphan scans. The time spent scanning each channel is: $\text{aBaseSuperframeDuration} \times (2^n + 1)$ symbols, where n is the value of ScanDuration parameter.
See Table 51 in IEEE STD 802.15.4-2011 standard for the definition and value set of aBaseSuperframeDuration.			

8.6.2.3 DLME-DISCOVERY.confirm

DLME-DISCOVERY.confirm is used to respond to DLME-DISCOVERY.request.

The semantics of DLME-DISCOVERY.confirm are as follows:

```
DLME-DISCOVERY.confirm(
    Status,
    NetworkCount,
    NetworkDescriptor
)
```

Table 46 specifies the parameters for DLME- DISCOVERY.confirm. Table 47 specifies the network descriptor list.

Table 46 – DLME- DISCOVERY.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Scan results: 0 = SUCCESS; 7 = INVALID_PARAMETER; 8 = NO_BEACON; Others are reserved. See Table 43 for more detail
NetworkCount	Unsigned8	0 to 255	The count of active network found during scan
NetworkDescriptor	Network descriptor list	0 to NetworkCount	Network Descriptor list of every network found, see Table 47

Table 47 – Network descriptor list

Name	Data type	Valid range	Description
LogicalChannel	Unsigned8	0 to 31	Logic channel used for joining, chosen from valid channels supported by PHY
BeaconOrder	Unsigned8	0 to 15	The frequency sending beacon frame
SuperframeOrder	Unsigned8	0 to 15	Active period length of the superframe
PermitJoining	Boolean	0, 1	Whether routing device permits field device to join: 0 = No permit; 1 = At least one device is permitted to join

If the scan is successful, DLME-DISCOVERY.confirm returns SUCCESS; however if no beacons are found, DLME-DISCOVERY.confirm returns NO_BEACON; if there are some errors or invalid parameters in DLME-DISCOVERY.request, DLME-DISCOVERY.confirm returns INVALID_PARAMETER.

8.6.2.4 Time sequence of subnet discovery

The time sequence for subnet discovery is shown in Figure 36. See IEEE STD 802.15.4-2011 for the primitives of MLME-SCAN.request and MLME-SCAN.confirm.

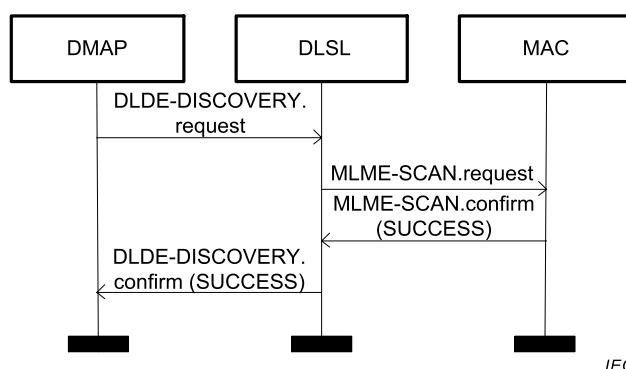


Figure 36 – Time sequence of network discovery

See Figure 12 and Figure 13 in IEEE STD 802.15.4-2011 for the detailed message sequence chart between peer MAC entities.

8.6.3 Device joining services

8.6.3.1 General

There are two instances requiring device joining services:

- a) a new field device joining the star network; or
- b) a new routing device joining the mesh network. The primitives supported by DLSL device joining services include DLME-JOIN.request, DLME-JOIN.indication, DLME-JOIN.response, and DLME-JOIN.confirm.

8.6.3.2 DLME-JOIN.request

DLME-JOIN.request is used for a device to join the network (star or mesh).

The semantics of DLME-JOIN.request are as follows:

```

DLME-JOIN.request (
    LogicalChannel,
    JoinAddr,
    PhyAddr,
    DeviceType
)
    
```

Table 48 specifies the parameters for DLME-JOIN.request.

Table 48 – DLME-JOIN.request parameters

Name	Data type	Valid range	Description
LogicalChannel	Unsigned8	0 to 31	Logic channel used for joining, chosen from valid channels supported by PHY
JoinAddr	Unsigned16	0 to 65 535	The short address of routing device or gateway device that accepts joining request
PhyAddr	Unsigned64	0 to $(2^{64}-1)$	Physical address of the new device waiting to join
DeviceType	Unsigned8	0 to 255	Type of the new device waiting to join: 0 = Gateway device; 1 = Routing device; 2 = Field device; 3 = Handheld device; Others are reserved.

8.6.3.3 DLME-JOIN.indication

DLME-JOIN.indication is used to inform the NLME of a routing device or to inform the gateway device that the joining request from one device has been successfully received.

The semantics of DLME-JOIN.indication are as follows:

DLME-JOIN.indication (

PhyAddr,
DeviceType

)

Table 49 specifies the parameters for DLME-JOIN.indication.

Table 49 – DLME-JOIN.indication parameters

Name	Data type	Valid range	Description
PhyAddr	Unsigned64	0 to $(2^{64}-1)$	Address of new device waiting to join
DeviceType	Unsigned8	0 to 255	Type of device waiting to join: 0 = Gateway device; 1 = Routing device; 2 = Field device; 3 = Handheld device; Others are reserved.

8.6.3.4 DLME-JOIN.response

DLME-JOIN.response is the response of DLME-JOIN.indication.

The semantics of DLME-JOIN.response are as follows:

DLME-JOIN.response (

PhyAddr,
ShortAddr,
TimeSource,
Status

)

Table 50 specifies the parameters for DLME-JOIN.response.

Table 50 – DLME-JOIN.response parameters

Name	Data type	Valid range	Description
PhyAddr	Unsigned64	0 to $(2^{64}-1)$	Address of device waiting to join
ShortAddr	Unsigned16	0 to 65 535	Short address allocated by the NM to device waiting to join
TimeSource	Unsigned8	0 to 1	Whether this device is set as time source: 0 = Not time source; 1 = Time source.
Status	Unsigned8	0 to 255	Result of joining request: 0 = SUCCESS; 1 = FAILURE_TOP_DISMATCH; 2 = FAILURE_ELSE; Others are reserved.

8.6.3.5 DLME-JOIN.confirm

DLME-JOIN.confirm reports the joining result to the DMAP.

The semantics of DLME-JOIN.confirm are as follows:

```
DLME-JOIN.confirm (
    ShortAddr,
    Status
)
```

Table 51 specifies the parameters for DLME-JOIN.confirm.

Table 51 – DLME-JOIN.confirm parameters

Name	Data type	Valid range	Description
ShortAddr	Unsigned16	0 to 65 535	Short address allocated by NM for device waiting to join
Status	Unsigned8	0 to 255	Result of joining request: 0 = SUCCESS; 1 = FAILURE_TOP_DISMATCH; 2 = FAILURE_ELSE; Others are reserved.

8.6.3.6 Time sequence for device joining in the network

See 9.5.3 for the detailed joining process.

8.6.4 Device leaving services**8.6.4.1 General**

There are two instances requiring device leaving services: (1) A field device leaving the star network or (2) a routing device leaving the mesh network. The primitives supported by DLSE network leaving services include DLME-LEAVE.request, DLME-LEAVE.indication, and DLME-LEAVE.confirm.

8.6.4.2 DLME-LEAVE.request

The semantics of DLME-LEAVE.request are as follows:

DLME-LEAVE.request (

ShortAddr

)

Table 52 specifies the parameters for DLME-LEAVE.request.

Table 52 – DLME-LEAVE.request parameters

Name	Data type	Valid range	Description
ShortAddr	Unsigned16	0 to 65 535	The short address of the device asking to leave

8.6.4.3 DLME-LEAVE.indication

DLME-LEAVE.indication is used to indicate to the upper layer that a device leaving request has been received.

The semantics of DLME-LEAVE.indication are as follows:

DLME-LEAVE.indication (

ShortAddr

)

Table 53 specifies the parameters for DLME-LEAVE.indication.

Table 53 – DLME-LEAVE.indication parameters

Name	Data type	Valid range	Description
ShortAddr	Unsigned16	0 to 65 535	The short address of the device asking to leave

8.6.4.4 DLME-LEAVE.confirm

DLME-LEAVE.confirm is used to report the result of DLME-LEAVE.request.

The semantics of DLME-LEAVE.confirm are as follows:

DLME-LEAVE.confirm (

Status

)

Table 54 specifies the parameters for DLME-LEAVE.confirm.

Table 54 – DLME-LEAVE.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Result of leaving request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

8.6.4.5 Time sequence for device leaving

See IEEE STD 802.15.4-2011 for the following primitives: MLME-DISASSOCIATE.request, MLME-DISASSOCIATE.confirm, and MLME-DISASSOCIATE.indication.

The time sequences for devices leaving the network are listed as follows.

- a) The time sequence for routing devices leaving the network

Routing devices connect to both the mesh network and the star network. Therefore, the process of routing devices leaving the network includes routing devices leaving the mesh network and routing devices leaving the star network. According to the leaving originator, the process of routing devices leaving the network includes active leaving and passive leaving.

b) The time sequence for field devices leaving the network

According to the leaving source, the process of field devices leaving the network includes active leaving and passive leaving.

See 9.5.4 for detailed process of device leaving.

8.6.5 DLME-CHANNEL-CONDITION.indication

DLME-CHANNEL-CONDITION.indication is used by DLSL to report channel condition information to DMAP. The reported performance data includes LQI, packet loss rate, and count of retries.

The semantics of DLME-CHANNEL-CONDITION.indication are as follows:

DLME-CHANNEL-CONDITION.indication (

ChannelNum,
ChannelStructure

)

Table 55 specifies the parameters for DLME-CHANNEL-CONDITION.indication.

Table 55 – DLME-CHANNEL-CONDITION.indication parameters

Name	Data type	Valid range	Description
ChannelNum	Unsigned8	0 to 255	Count of channels
ChannelStructure	ChanCon_Struct		Information of channels

8.6.6 DLME-NEIGHBOUR-INFO.indication

DLME-NEIGHBOUR-INFO.indication is used to report the collected neighbour information to the DMAP and is used to update the neighbour attributes.

The semantics of DLME-NEIGHBOUR-INFO.indication are as follows:

DLME-NEIGHBOUR-INFO.indication (

NeighbourCount,
NeighbourStructure

)

Table 56 specifies the parameters for DLME-NEIGHBOUR-INFO.indication.

Table 56 – DLME-NEIGHBOUR-INFO.indication parameters

Name	Data type	Valid range	Description
NeighbourCount	Unsigned8	0 to 255	Count of neighbour devices
NeighbourStructure	Neighbour_Struct structure		Information of neighbours

8.6.7 DLME-COMM-STATUS.indication

DLME-COMM-STATUS.indication is used to report the communication status to the upper layer.

The semantics of DLME-COMM-STATUS.indication are as follows:

DLME-COMM-STATUS.indication (

PhyAddr,
Status

)

Table 57 specifies the parameters for DLME-COMM-STATUS.indication.

Table 57 – DLME-COMM-STATUS.indication parameters

Name	Data type	Valid range	Description
PhyAddr	Unsigned64	0 to $(2^{64}-1)$	Address of new device that has just joined the network
Status	Unsigned8	0 to 255	The joining status of a device: 0 = SUCCESS; 1 = FAILURE_TOP_DISMATCH; 2 = FAILURE_ELSE; Others are reserved.

8.6.8 Keep-alive services

8.6.8.1 DLME-KEEP-LIVE.request

DLME-KEEP-LIVE.request is used to send Keep-alive command frames that are requested by the DMAP.

The semantics of DLME-KEEP-LIVE.request are as follows:

DLME-KEEP-LIVE.request (

)

8.6.8.2 DLME-KEEP-LIVE.confirm

DLME -KEEP-LIVE.confirm is used to respond to DLME -KEEP-LIVE.request.

The semantics of DLME -KEEP-LIVE.confirm are as follows:

DLME -KEEP-LIVE.confirm (

Status

)

Table 58 specifies the parameters for DLME -KEEP-LIVE.confirm.

Table 58 – DLME -KEEP-LIVE.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	The result of the keep alive: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

8.6.8.3 DLME-KEEP-LIVE.indication

DLME-KEEP-LIVE.indication is used to inform the DMAP that the keep-alive command frame has been successfully received.

The semantics of DLME -KEEP-LIVE.indication are as follows:

DLME-KEEP-LIVE.indication (

SrcAddr
)

Table 59 specifies the parameters for DLME -KEEP-LIVE.indication.

Table 59 – DLME -KEEP-LIVE.indication parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	The source address

8.6.9 Time synchronization services

8.6.9.1 DLME-TIME-SYN.request

DLME-TIME-SYN.request is used to send time synchronization command frames that are requested by the DMAP.

The semantics of DLME-TIME-SYN.request are as follows:

DLME-TIME-SYN.request (

TimeValue
)

Table 60 specifies the parameters for DLME-TIME-SYN.request.

Table 60 – DLME-TIME-SYN.request parameters

Name	Data type	Valid range	Description
TimeValue	Unsigned16	0 to $(2^{16}-1)$	Time difference between the transmission beginning and the timeslot beginning (in microsecond)

8.6.9.2 DLME-TIME-SYN.confirm

DLME-TIME-SYN.confirm is used to respond to DLME-TIME-SYN.request.

The semantics of DLME-TIME-SYN.confirm are as follows:

DLME-TIME-SYN.confirm (

Status
)

Table 61 specifies the parameters for DLME-TIME-SYN.confirm.

Table 61 – DLME -TIME-SYN.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	The result of time synchronization: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

8.6.9.3 DLME-TIME-SYN.indication

DLME-TIME-SYN.indication is used to inform the DMAP that the time synchronization command frame has been successfully received.

The semantics of DLME-TIME-SYN.indication are as follows:

DLME-TIME-SYN.indication (

SrcAddr,
TimeValue
)

Table 62 specifies the parameters for DLME-TIME-SYN.indication.

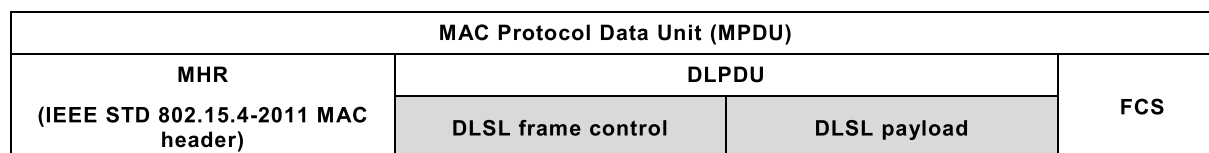
Table 62 – DLME-TIME-SYN.indication parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	The source address
TimeValue	Unsigned16	0 to $(2^{16}-1)$	Time difference between the transmission beginning and the timeslot beginning (in microsecond)

8.7 DLSL frame formats

8.7.1 General frame format

The DLSL general frame format is illustrated in Figure 37.



IEC

Figure 37 – General frame format

The DLSP frame is composed of:

- IEEE STD 802.15.4-2011 MAC Header (MHR) (See IEEE STD 802.15.4-2011, 5.2.1);
- DLSP frame control (see Table 63);
- DLSP payload; and

d) Frame Check Sequence (FCS).

See 11.3.2 for the content of security.

The format of the WIA-PA DLSL frame control is shown in Table 63.

Table 63 – DLSL frame control field

	DLSL frame control field			
Length in bit(s)	1	1	1	5
Subfield name	Frame type	Time source	Security enable	Index of main channel

The subfields in Table 63 are listed as follows.

- The Frame type subfield has 1-bit length and is used to specify the frame type. If a frame is a data frame, this subfield is set to 0; otherwise, this subfield is set to 1.
- The Time source subfield has 1-bit length and is used to indicate whether this device is a time source. If the device is a time source, this subfield is set to 1; otherwise, this subfield is set to 0.
- The Security enable subfield has 1-bit length and is used to instruct DLSL whether or not to use the security mechanism. A value of 0 means that the security mechanism is disabled and a value of 1 means that the security mechanism is enabled.
- The Index of the main channel is used to indicate the current communication channel.

All multiple octet fields should be transmitted or received with the least significant octet first and each octet should be transmitted or received with the Least Significant Bit (LSB) first. The same transmission order should apply to data fields transferred between layers.

8.7.2 Date frame format

The format of the DLSL data frame is shown in Table 64.

Table 64 – Date frame format

	Date frame format	
Length in octet(s)	1	Variable length
Field name	DLSL frame control	Data payload

The subfields in Table 64 are listed as follows:

- the DLSL frame control is defined in Table 63; and
- the Data payload has variable length and is filled with the DLSL data.

8.7.3 Command frame format

8.7.3.1 General command frame format

The general command frame format is shown in Table 65.

Table 65 – General command frame format

	General command frame format		
Length in octet(s)	1	1	Variable length
Field name	DLSL frame control	Command frame identifier	Command payload

The subfields in Table 65 are listed as follows:

- a) the DLSSL frame control is defined in Table 63;
- b) the Command frame identifier is defined in Table 66; and
- c) the Command payload has variable length and is filled with the DLSSL management data.

8.7.3.2 DLSSL command frame

8.7.3.2.1 General

The DLSSL command frames are defined and shown in Table 66.

Table 66 – DLSSL command frame

Command frame identifier	DLSSL command frame		
	Command name	User	Description
1	Keep-alive command frame	Gateway device/Routing device/Field device	Indicating an existing device
2	Time synchronization command frame	Gateway device/Routing device	Realizing synchronization of time the whole network
3 to 255	Reserved	Reserved	To be extended

The Keep-alive command frame facilitates connection maintenance between neighbour devices. After devices join the network, their DMAPs send keep-alive command frame with the keep-alive request primitive. The GW sends the keep-alive command frame during the inter-cluster communication period in order to indicate that it is alive. Routing devices send the keep-alive command frames during the intra-cluster communication period in order to indicate that they are alive to their cluster members; in addition, routing devices send keep-alive command frames during the inter-cluster communication period in order to indicate that they are alive to other routing devices and to the GW. Field devices send the keep-alive command frames during the intra-cluster communication period in order to indicate that they are alive to their cluster heads.

In order to guarantee the reliability of the TDMA communication mode, devices in a network should synchronize with the time source. Time errors among devices are inevitable in spite of any hardware time sources. In order to overcome time clock drifting, the WIA-PA network performs two kinds of time synchronization: IEEE STD 802.15.4-2011 beacon and specifically designed time synchronization command frame. In the star-only network, the GW is the UTC time source. In the combination of star and mesh network, the GW is the UTC time source of the mesh part and all routing devices synchronize with the gateway device; each routing device is the time source for its field devices in the star part, which synchronize with their routing devices.

This document specifies that the maximum synchronization error is less than 10 % of the basic timeslot length of the maximum superframe duration.

8.7.3.2.2 Keep-alive command frame

The format of the keep-alive command frame is shown in Table 67.

Table 67 – Format of keep-alive command frame

Length in octet(s)	Format of keep-alive command frame	
	1	1
Field name	DLSSL frame control	Command frame identifier

The subfields in Table 67 are listed as follows.

- a) See Table 63 for DLSSL frame control.
- b) Command frame identifier is 10.

8.7.3.2.3 Time synchronization command frame

The time synchronization command frame is used to synchronize the entire network. The gateway device and the routing devices send the time synchronization command frames periodically.

If the network topology is star-only, the GW broadcasts the time synchronization command frame periodically. If the network topology is combination of mesh and star, the GW unicasts the time synchronization command frame during the inter-cluster communication period; routing devices broadcast the time synchronization command frames during the intra-cluster communication period to synchronize their star networks and unicast them during the inter-cluster communication period to synchronize the mesh network.

The format of the time synchronization command frame is shown in Table 68.

Table 68 – Format of time synchronization command frame

	Format of time synchronization command frame		
Length in octet(s)	1	1	2
Field name	DLSSL frame control	Command frame identifier	Calibrated value of TimeValue

The subfields in Table 68 are defined as follows:

- a) see Table 63 for DLSSL frame control;
- b) command frame identifier is 11; and
- c) see Table 60 for Calibrated value of TimeValue.

9 Network layer

9.1 General

The WIA-PA network layer (NL) receives and transports packets over networks, provides interfaces to the ASL, and carries out network layer management, configuration and control.

9.2 Protocol stack

The protocol stack of the WIA-PA network layer is shown in Figure 38.

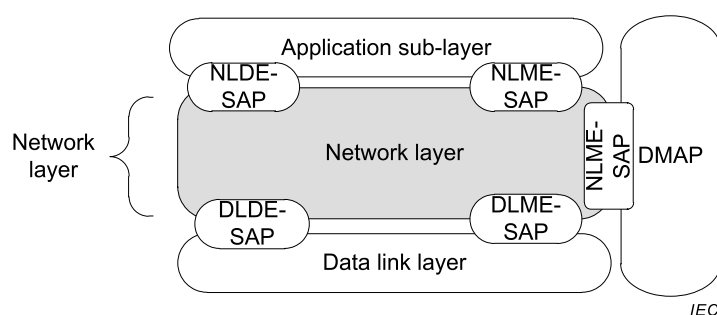


Figure 38 – WIA-PA network layer protocol stack

The layers and entities in Figure 39 are defined as follows:

- the NL defines the NLDE and the Network Layer Management Entity (NLME);
- the NLDE provides the service interface through which the ASL transmits and receives data; and
- the NLME provides the service interfaces through which the layer management functions are invoked by the upper layer and DMAP.

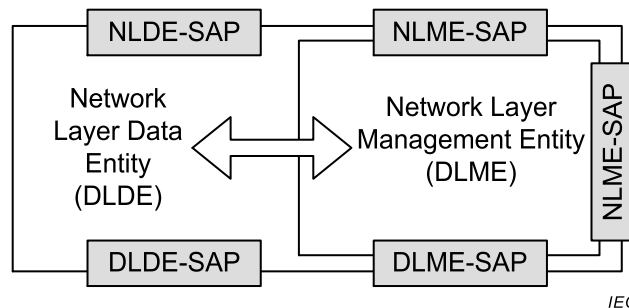


Figure 39 – WIA-PA network layer reference model

The NL provides two kinds of services that are accessed through the following two SAPs:

- the network layer data service, accessed through the NLDE SAP (NLDE-SAP);
- the network layer management service, accessed through the NLME SAP (NLME-SAP).

9.3 Function description

9.3.1 General

The NL is designed to perform the following functions:

- addressing,
- routing,
- communication resource allocation,
- packet lifecycle management,
- management for device joining and leaving network,
- end-to-end network performance monitoring, and
- fragmentation and reassembly.

9.3.2 Addressing

Each device has a global unique 64-bit long address and a 16-bit short address. Each device joins the network by using the long address and communicates with other devices by using the short address after joining the network. The 16-bit short address is indicated as x.y, where x and y are 8-bit integers. The most significant 8-bit in the 16-bit short address is the cluster address, and the least significant 8-bit is the intra-cluster address. The range of the cluster address is 0 to 255, and the range of the intra-cluster address is 0 to 255. The number 255 is used for the broadcast address. A routing device's intra-cluster address is 0.

The classifications of the short address are as follows:

- Unicast addresses: each device's address is the unicast address, which includes the following types:
 - the gateway device's address is 0.0;
 - the routing device's address is x.0, where x is 1 to 254;

- if the network topology is star-only, that is NetworkTopology=1, the field device's address is 0.y, where y is 1 to 254; otherwise, the field device's address is x.y, where x is 1 to 254 and y is 1 to 254; see 6.9.1.2.1 for NetworkTopology.
- b) Broadcast address: according to the different broadcast domains, there are four types of broadcast addresses:
- the intra-cluster broadcast address is x.255, where x is 0 to 254;
 - the global broadcast address is 255.255;
 - the mesh network's broadcast address is 255.0;
 - the gateway device's broadcast address is 0.255.

9.3.3 Routing

9.3.3.1 General

The WIA-PA network supports static routing algorithms configured by the NM. After getting the neighbour information from each routing device, the NM generates the connection relationship of all routing devices. On the basis of the connection relationship, the NM generates and writes the routing information to each routing device in the form of a routing table. Each route in the table is assigned a route ID. Multiple paths correspond to each VCR, including the main path and the redundant path. The main path and the redundant path use the same route ID.

9.3.3.2 Routing table

Each routing device maintains a routing table, which is generated by the NM. The routing table is used for the path selection in the mesh network. The table has five items. RouteID is the identifier of a route. SourceAddress is the address of the start point of a route, DestinationAddress is the endpoint address of a route, NextHop is the address of the next hop device in a route, and RetryCounter records the number of one-hop retries in a route which reflects the status of the route. The RouteIDs of paths with same source address and destination address are same.

An example of a routing table is shown in Table 69.

Table 69 – Example of a routing table

RouteID	SourceAddress	DestinationAddress	NextHop	RetryCounter
5	F1	N1	N3	0
8	F2	Ng	N2	0
...	...	...	...	...
Ng in the table indicates a gateway address; N1, N2 and N3 indicate routing devices' addresses; F1 and F2 indicate field devices' addresses.				

9.3.4 Packet lifecycle management

Each packet has a lifecycle in the WIA-PA network. The lifecycle is expressed as a maximum surviving time. The NL records the generation time of packets by using timestamps. The surviving time is computed according to the generation time. When the surviving time of a packet exceeds its lifecycle, the packet should be discarded.

9.3.5 Joining and leaving network of device

The WIA-PA NL supports the joining and leaving processes of devices. The joining and leaving processes include the joining and leaving of field devices and of routing devices.

9.3.6 End-to-end network performance monitoring

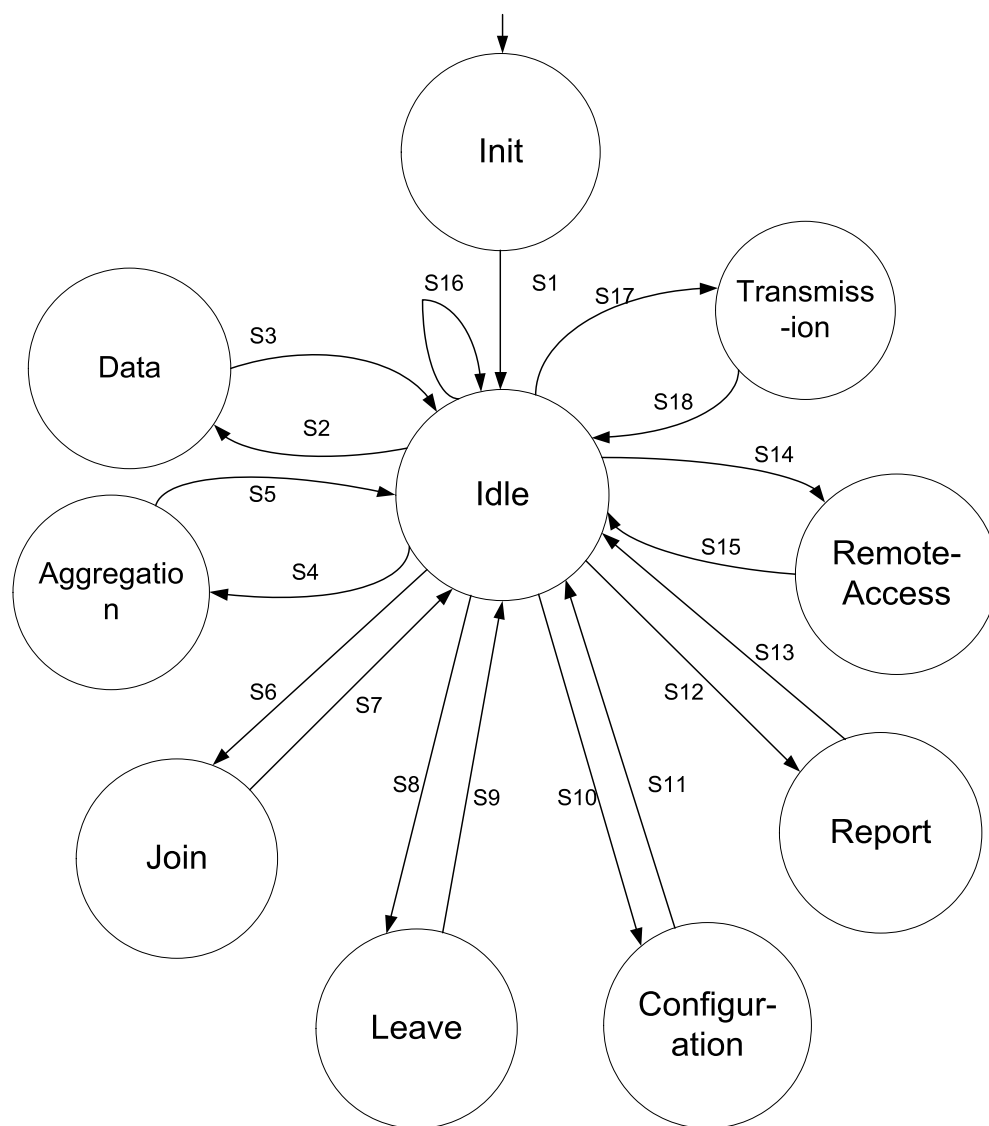
The WIA-PA network layer monitors each path's health status. The NLME records the number of retries of each path to estimate the path failures. If there is a path failure, the NLME sends an indication to the DMAP (see 9.5.12).

9.3.7 Fragmentation and reassembly

Fragmentation and reassembly are handled at the NL. If the length of an NPDU is longer than the maximum DLSL payload, the NPDU should be fragmented at the NL of the sender. When the fragmented NPDUs reach the receiver, they are reassembled at the NL. See 9.6.2 for detailed packet format.

9.3.8 Network layer state machine

The NL state transitions are shown in Figure 40 and Table 70.



IEC

Figure 40 – Network layer state machine

Table 70 – NL state transitions (1 of 4)

Sequence number #	Current state	Event or condition	Actions	Next state
S1	Init		Initiation	Idle
S2	Idle	From DLSL: DLSL-DATA.confirm() or DLSL-DATA.indication() & Packet type = 0 in NSDU; From ASL: NLDE-DATA.request()		Data
S3	Data		From DLSL: invoke NLDE-DATA.confirm() to ASL or parsing NSDU and invoke NLDE-DATA.indication() for NSDU; From ASL: packing NPDU and invoke DLDE-DATA.request(); All messages or packets are sent to transmission queue.	Idle
S4	Idle	From DLSL: DLSL-DATA.indication() & Packet type = 1 in NSDU; From DMAP: NLME-AGOSEND.request()		Aggregation
S5	Aggregation		From DLSL: parsing NSDU according to NL aggregated packet format and invoke NLME-DAG.indication() to DMAP; From DMAP: packing NL aggregated packet; All messages or packets are sent to relate transmission queue.	Idle
S6	Idle	From DLSL: DLSL-DATA.indication() & Packet type = 2 and Command ID = 0, 1 in NSDU; From DMAP: NLME-JOIN.request/response ()		Join
S7	Join		From DLSL: parsing NSDU according to NL joining request packet format if Command ID = 0 or joining response packet format if Command ID = 1 and invoke NLME-JOIN.indication() / NLME-JOIN.confirm() to DMAP; From DMAP: packing NL joining response packet; All messages or packets are sent to related transmission queue.	Idle
S8	Idle	From DLSL: DLSL-DATA.indication() & Packet type = 2 and Command ID = 3, 4 in NSDU; From DMAP: NLME-LEAVE.request/response ()		Leave
S9	Leave		From DLSL: parsing NSDU according to NL leaving request packet format if Command ID = 3 or leaving response packet format if Command ID = 4 and invoke NLME-LEAVE.indication()/NLME-LEAVE.confirm() to DMAP; From DMAP: packing NL leaving response packet; All messages or packets are sent to related transmission queue.	Idle

Table 70 (2 of 4)

Sequence number #	Current state	Event or condition	Actions	Next state
S10	Idle	From DLSL: DLSL-DATA.indication() & Packet type = 2 and Command ID = 8-25 in NSDU; From DMAP: NLME-ADD/UPDATE/DELETE_ROUTE.request/response () or NLME-ADD/UPDATE/RELEASE-LINK/SFR.request/response()		Configuration
S11	Configuration		From DLSL: parsing NSDU according to NL route/link/superframe-add/update/delete/release request/response packet format if Command ID = 8-25 and invoke NLME-ADD/UPDATE/DELETE_ROUTE.indication() or NLME-ADD/UPDATE/RELEASE-LINK/SFR.indication() to DMAP; From DMAP: packing NL route/link/superframe - add/update/delete/release response packet; All messages or packets are sent to related transmission queue.	Idle
S12	Idle	From DLSL: DLSL-COMM-STATUS.confirm() or DLSL-DATA.indication() & Packet type = 2 and Command ID = 2, 5-7, 26-28; From DMAP: NLME-RPT-CLRMEM.response()		Report

Table 70 (3 of 4)

Sequence number #	Current state	Event or condition	Actions	Next state
S13	Report		From DLSL: invoke NLME-COMM-STATUS.cofirm () to DMAP. if Command ID = 2, parsing NSDU according to NL communication status report request packet format and invoke NLME-COMM-STATUS.indication(); if Command ID = 5, 6, parsing NSDU according to NL cluster member report request/response packet format and invoke NLME-RPT-CLRMEM.indication/confirm () to DMAP; if Command ID = 7; parsing NSDU according to NL neighbour information report request packet format and invoke NLME-NEIGHBOUR-INFO.indication() to DMAP; if Command ID = 26; parsing NSDU according to NL device condition report request packet format and invoke NLME-DEVICE-STATUS.indication() to DMAP; if Command ID = 27, parsing NSDU according to NL channel condition report request packet format and invoke NLME-CHANNEL-CONDITION.indication() to DMAP; if Command ID = 28, parsing NSDU according to NL path failure report request packet format and invoke NLME-PATH_FAILURE.indication() to DMAP; From DMAP: packing NL cluster member report response packet; All messages or packets are sent to related transmission queue.	Idle
S14	Idle	From DLSL: DLSL-DATA.indication() & Packet type = 2 and Command ID =29-32; From DMAP: NLME-INFO_GET.response() or NLME-INFO_SET.response()		Remote Access
S15	Remote Access		From DLSL: if Command ID = 29, 30; parsing NSDU according to NL attribute getting request/response packet format and invoke NLME-INFO_GET.indication() / NLME-INFO_GET.confirm to DMAP; if Command ID = 31, 32, parsing NSDU according to NL attribute setting request/response packet format and invoke NLME-INFO_SET.indication() / NLME-INFO_SET.confirm to DMAP; From DMAP: packing NL attribute getting /setting response packet; All messages or packets are sent to relate transmission queue.	Idle

Table 70 (4 of 4)

Sequence number #	Current state	Event or condition	Actions	Next state
S16	Idle	From DLSSL: DLSSL-DATA.indication() & Packet type = 2 and Command ID > 32 or no packet received	Discard related NSDUs	Idle
S17	Idle	Transmission queue is not empty		Transmission
S18	Transmission	Transmission is over		Idle

The states in the NL state machine are specified as follows.

a) Idle state

The following transitions may occur while in the Idle state:

- when the DLSSL invokes DLDE-DATA.indication, the NL enters the Receive state;
- when the ASL invokes NLDE-DATA.request, the NL enters the Transmit state.

b) Transmit state

In the Transmit state, if the NL receives NLDE-DATA.confirm, it enters the Idle state.

c) Receive state

When in the Receive state, the NL enters the Idle state after the NL issues NLDE-DATA.indication to the upper layer.

See 9.4 for NL data services, e.g. NLDE-DATA; see 9.5 for NL management services, e.g. NLME-; See 9.6.1 for Packet type and 9.6.4 for Command ID.

The states in the NL state machine are specified as follows.

a) Idle state

After a device initiates the NL, the NL enters the Idle state. The following transitions may occur while the DLSSL is in the Idle state:

b) When a DLSSL, ASL, or DMAP frame arrives, the NL processes the NSDU.

The packets that a device can receive include packets whose final destination addresses are this device. The functions of the Idle state are to receive and process the packet and process the DMAP, ASL and DLSSL primitives.

The following transitions may occur while the NL is in the Receive state:

- If a data packet is received from DLSSL or NLDE-DATA.request() is received from ASL, the NL enters Data state.
- If an aggregated packer is received from DLSSL or NLME-AGO-SEND.request() is received from DMAP, the NL enters Aggregation state.
- If a join request or response command packet is received from DLSSL or NLME-JOIN.request/response () is received from DMAP, the NL enters Join state.
- If a leave request or response command packet is received from DLSSL or NLME-LEAVE.request/response () is received from DMAP, the NL enters Leave state.
- If a command packet identified from 8 to 25 is received from DLSSL or NLME-ADD/UPDATE/DELETE_ROUTE.request/response () or NLME-ADD/UPDATE/RELEASE-LINK/SFR.request/response() are received from DMAP, the NL enters Configuration state.
- If a command packet identified by 2, 5-7, 26-28 is received from DLSSL or NLME-RPT-CLRMEM.response() is received from DMAP, the NL enters Report state.
- If an attribute getting or setting command packet identified from 29 to 32 is received from DLSSL or NLME-INFO_GET.response() /NLME-INFO_SET.response() is received from DMAP, the NL enters Remote Access state.

- If no packet or primitives is received or command packets identifier bigger than 32 is received from DLSL, the NL enters Idle state.
- c) When the transmission queue is not empty, the NL enters the Transmission state.
- d) Data state
This state handles the data process procedure of a device. If a data from DLSL is received or an ASL data request is received, the NL enters the Data state.
- e) Aggregation state
This state handles the data/packet aggregation and dis-aggregation procedure.
- f) Join state
This state handles the joining procedure of a device.
- g) Leave state
This state handles the leaving procedure of a device.
- h) Configuration state
This state handles the resource allocation procedures, which include the add/update/deleting or release of a route, link, or a superframe.
- i) Report state
This state handles the report procedures, which include the cluster member report, neighbour information report, device condition report, channel condition report, and path failure report.
- j) Remote access state
This state handles the remote attribute access procedures, which include the attribute getting and setting.
- k) Transmission state
This state handles the data or packet transmission procedures. If the transmission queue is not empty, the NL enters the Transmission state.

9.4 Network layer data services

9.4.1 General

The NLDE-SAP is used by the ASL to receive and transmit data. The primitives supported by NL data services include NLDE-DATA.request, NLDE-DATA.confirm, and NLDE-DATA.indication.

9.4.2 NLDE-DATA.request

The NLDE receives the payload from the ASL through NLDE-DATA.request and adds it to the message queue of the NL.

The semantics of NLDE-DATA.request are described as follows:

```
NLDE-DATA.request (
    VcrID,
    SrcAddr,
    Priority,
    PayloadLength,
    Payload,
    PayloadHandle
)
```

Table 71 specifies the parameters for NLDE-DATA.request.

Table 71 – NLDE-DATA.request parameters

Name	Data type	Valid range	Description
VcrID	Unsigned16	0 to 65 535	The VCR identifier
SrcAddr	Unsigned16	0 to 65 535 (Unicast address)	The 16-bit short address of the NSDU's source
Priority	Unsigned8	0 to 15	Priority of this NSDU
PayloadLength	Unsigned16	0 to 65 535	The length of NSDU to be transmitted
Payload	Octetstring		NSDU
PayloadHandle	Unsigned8	0 to 255	The handle associated with the NSDU to be transmitted

9.4.3 NLDE-DATA.confirm

NLDE-DATA.confirm reports the results of NLDE-DATA.request.

The semantics of NLDE-DATA.confirm are described as follows:

```
NLDE-DATA.confirm (
    PayloadHandle,
    Status
)
```

Table 72 specifies the parameters for NLDE-DATA.confirm.

Table 72 – NLDE-DATA.confirm parameters

Name	Data type	Valid range	Description
PayloadHandle	Unsigned8	0 to 255	Handle of the NSDU, which is used to indicate the NL payload.
Status	Unsigned8	0 to 255	Result of NLDE-DATA.request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.4.4 NLDE-DATA.indication

NLDE-DATA.indication informs the ASL when the NL receives a packet.

The semantics of NLDE-DATA.indication are described as follows:

```
NLDE-DATA.indication (
    SrcAddr,
    Priority,
    NSDULength,
    NSDU
)
```

Table 73 specifies the parameters of NLDE-DATA.indication.

Table 73 – NLDE-DATA.indication parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535 (Unicast Address)	The 16-bit short address of the NSDU's source
Priority	Unsigned8	0 to 15	Priority of this NSDU
NSDULength	Unsigned16	0 to 65 535	Length of the NSDU
NSDU	octet		Data of the NSDU

9.4.5 Time sequence of NL data services

Figure 41 shows the basic procedures of packet sending and receiving. NLDE-DATA.request is generated by a local Application Sub-Layer Data Entity (ASLDE) when a data Application Sub-Layer Protocol Data Unit (ASLPDU) is to be transferred to a peer NLDE. On receipt of a NLDE-DATA.request, the NLDE begins transmitting of the NPDU.

NLDE-DATA.confirm is generated by the NLDE of a source device in response to NLDE-DATA.request. NLDE-DATA.confirm returns a status indicating the result of the transmission.

NLDE-DATA.indication is generated by the NLDE of a destination device and is issued to the ASLDE on receipt of a data packet at the local NLDE.

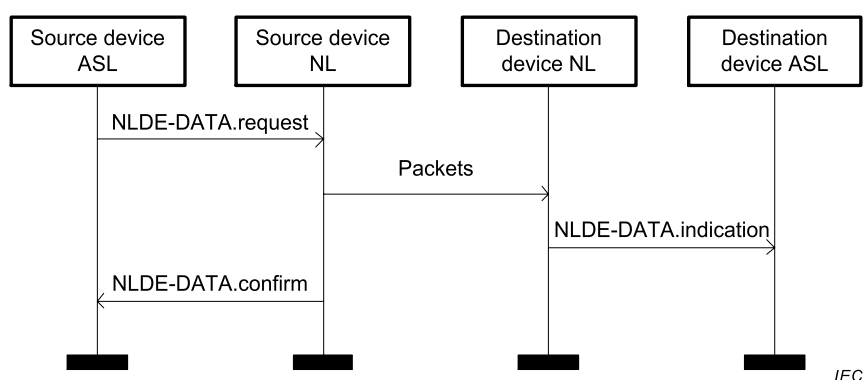


Figure 41 – Time sequence of NL data services

9.5 Network layer management services

9.5.1 General

The DMAP uses the interface supplied by NLME-SAP to configure and control the NL operation.

9.5.2 Network communication status report services

9.5.2.1 NLME-COMM-STATUS.request

The semantics of NLME-COMM-STATUS.request are described as follows:

```

NLME-COMM-STATUS.request (
    ProxyAddr,
    PhyAddr,
    DeviceType,
    Status
)
    
```

Table 74 specifies the parameters for NLME-COMM-STATUS.request.

Table 74 – NLME-COMM-STATUS.request parameters

Name	Data type	Valid range	Description
ProxyAddr	Unsigned16	0 to 65 535	The address of the routing device selected by the new device (unicast address)
PhyAddr	Unsigned64	0 to $(2^{64}-1)$	64-bit physical address of the new device
DeviceType	Unsigned8	0 to 255	The type of the new device: 0 = Gateway device; 1 = Routing device; 2 = Field device; 3 = Handheld device; Others are reserved.
Status	Unsigned8	0 to 255	Results of the joining process of a new device: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.2.2 NLME-COMM-STATUS.indication

The semantics of NLME-COMM-STATUS.indication are described as follows:

NLME-COMM-STATUS.indication (

ProxyAddr,
PhyAddr,
DeviceType,
Status
)

Table 75 specifies the parameters for NLME-COMM-STATUS.indication.

Table 75 – NLME-COMM-STATUS.indication parameters

Name	Data type	Valid range	Description
ProxyAddr	Unsigned16	0 to 65 535	The address of the routing device selected by the new device (unicast address)
PhyAddr	Unsigned64	0 to ($2^{64}-1$)	64-bit physical address of the new device
DeviceType	Unsigned8	0 to 255	The type of the new device: 0 = Gateway device; 1 = Routing device; 2 = Field device; 3 = Handheld device; Others are reserved.
Status	Unsigned8	0 to 255	Results of the joining process of a new device: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

On receipt of NL communication status request packet, the NL of the gateway device will invoke NLME-COMM-STATUS.indication and inform the DMAP.

9.5.2.3 NLME-COMM-STATUS.confirm

The semantics of NLME-COMM-STATUS.confirm are described as follows:

```
NLME-COMM-STATUS.confirm (
    PhyAddr,
    Status
)
```

Table 76 specifies the parameters for NLME-COMM-STATUS.confirm.

Table 76 – NLME-COMM-STATUS.confirm parameters

Name	Data type	Valid range	Description
PhyAddr	Unsigned64	0 to ($2^{64}-1$)	64-bit physical address of the new device
Status	Unsigned8	0 to 255	Execution result of the request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

NLME-COMM-STATUS.confirm is generated by the NL in response to NLME-COMM-STATUS.request. NLME-COMM-STATUS.confirm returns a status of either SUCCESS, indicating that the requested transmission has been successful, or FAILURE, indicating that the transmission has failed.

9.5.3 Network joining services

9.5.3.1 NLME-JOIN.request

The semantics of NLME-JOIN.request are described as follows:

```
NLME-JOIN.request (
    ProxyAddr,
    PhyAddr,
    SecMaterial,
    DeviceType
)
```

Table 77 specifies the parameters for NLME-JOIN.request.

Table 77 – NLME-JOIN.request parameters

Name	Data type	Valid range	Description
ProxyAddr	Unsigned16	0 to 65 535	The address of the routing device selected by the new device (Unicast address)
PhyAddr	Unsigned64	0 to ($2^{64}-1$)	64-bit physical address of the new device
SecMaterial	Unsigned32	0 to ($2^{32}-1$)	The identity information of a device
DeviceType	Unsigned8	0 to 255	The type of the new device: 0 = Gateway device; 1 = Routing device; 2 = Field device; 3 = Handheld device; Others are reserved.

9.5.3.2 NLME-JOIN.indication

The semantics of NLME-JOIN.indication are described as follows:

```
NLME-JOIN.indication (
    ProxyAddr,
    PhyAddr,
    SecMaterial,
    DeviceType
)
```

Table 78 specifies the parameters for NLME-JOIN.indication.

Table 78 – NLME-JOIN.indication parameters

Name	Data type	Valid range	Description
ProxyAddr	Unsigned16	0 to 65 535	Short address of the routing device that generates NL join request
PhyAddr	Unsigned64	0 to $(2^{64}-1)$	Device's physical address
SecMaterial	Unsigned32	0 to $(2^{32}-1)$	The identity information of a device
DeviceType	Unsigned8	0 to 255	The type of the new device: 0 = Gateway device; 1 = Routing device; 2 = Field device; 3 = Handheld device; Others are reserved.

On receipt of NL joining request packet, the NL of the gateway device will invoke NLME-JOIN.indication and inform the DMAP.

9.5.3.3 NLME-JOIN.response

The semantics of NLME-JOIN.response are described as follows:

NLME-JOIN.response (

ProxyAddr,
PhyAddr,
ShortAddr,
Status

)

Table 79 specifies the parameters for NLME-JOIN.response.

Table 79 – NLME-JOIN.response parameters

Name	Data type	Valid range	Description
ProxyAddr	Unsigned16	0 to 65 535	Short address of the routing device that generates NL join request
PhyAddr	Unsigned64	0 to $(2^{64}-1)$	Physical address of new device
ShortAddr	Unsigned16	0 to 65 535	Allocated network address (Unicast address) of new device
Status	Unsigned8	0 to 255	Execution result of the request 0 = SUCCESS; 1 = FAILURE; Others are reserved.

The DMAP invokes NLME-JOIN.response to assign a network address to the new device.

9.5.3.4 NLME-JOIN.confirm

The semantics of NLME-JOIN.confirm are described as follows:

NLME-JOIN.confirm (

ShortAddr,
Status

)

Table 80 specifies the parameters for NLME-JOIN.confirm.

Table 80 – NLME-JOIN.confirm parameters

Name	Data type	Valid range	Description
ShortAddr	Unsigned16	0 to 65 535	Network address (unicast address)
Status	Unsigned8	0 to 255	Execution result of the request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

NLME-JOIN.confirm is generated by the NL in response to NLME-JOIN.request. NLME-JOIN.confirm returns a status of either SUCCESS, indicating that the requested transmission has been successful, or FAILURE, indicating that the transmission has failed.

9.5.3.5 Time sequence for device joining

9.5.3.5.1 Time sequence for field device joining

To join the star network, a field device should initiate a joining request in the MAC layer by DMAP to the routing device or the gateway device. A field device should join the network either through the gateway device or through a routing device.

When the gateway device receives a joining request from a field device, it should indicate the joining to the NM and then return a joining response. If the new field device receives the MAC associate response from the gateway device, it joins the network.

When the routing device receives a joining request from a field device, it should produce a joining request of the NL and send this request to the gateway device. If the new field device receives the joining response, the joining process is finished.

Figure 42 illustrates an example of the joining process of a field device in the hierarchical network that is the combination of star and mesh.



9.5.3.5.2 Time sequence for routing device joining

The gateway device receives the joining request and informs the NM. The NM should return a response. If the new routing device receives the response, its joining process is completed.

Technical Commission

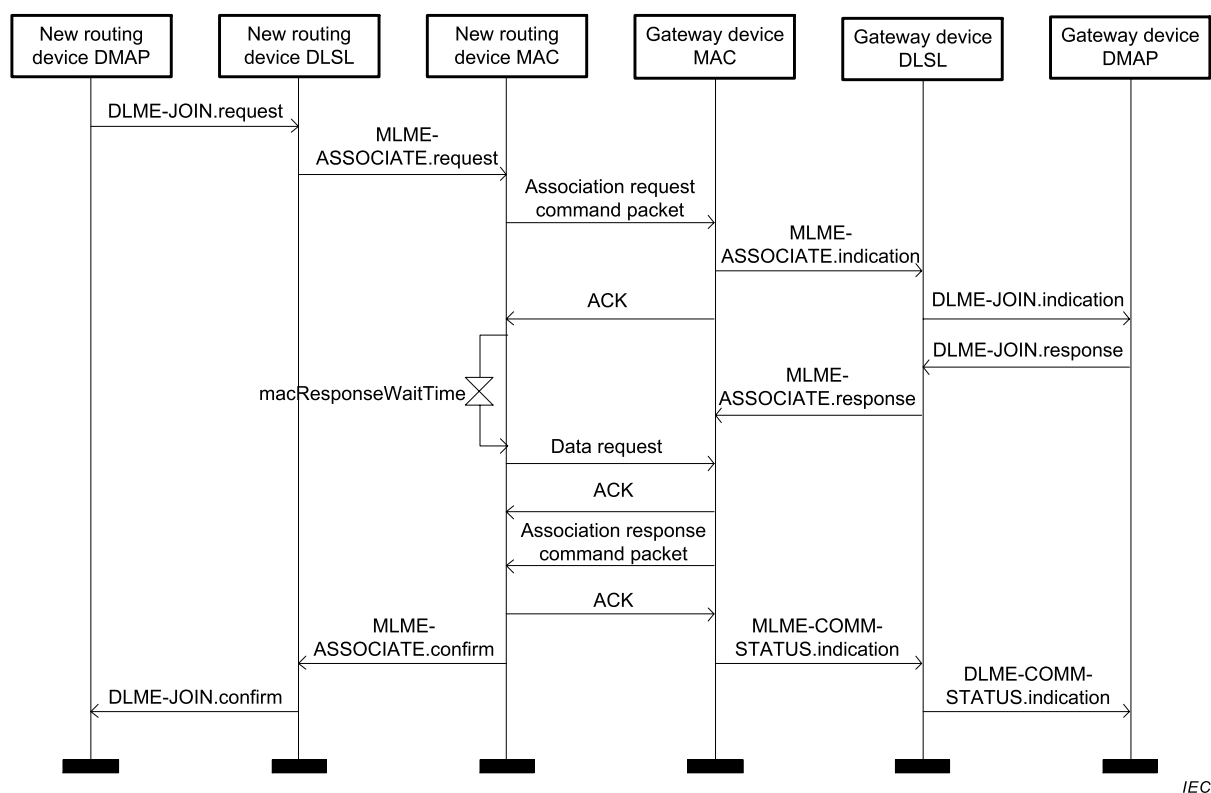


Figure 43 – One-hop joining process for routing device

See IEEE STD 802.15.4-2011, Figure 17 and Figure 18 for the detailed message sequence chart between peer MAC entities.

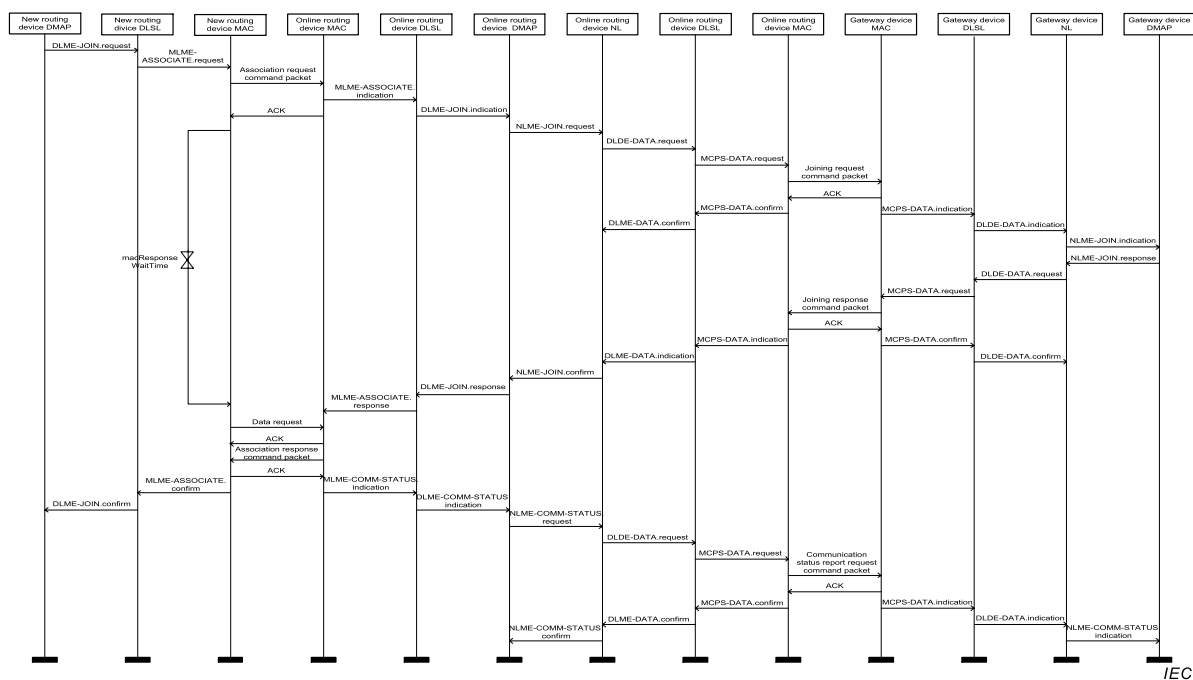


Figure 44 – Multi-hop join process of routing device

Before joining the network, the field devices and the routing devices set the DeviceState (see Table 20) to 0 to indicate that the devices have not joined the network. If the new devices have sent out the joining request and have not received the joining response, they set the

DeviceState to 1 to indicate that the devices are joining the network. If the new devices have sent out the joining request and have received the joining response successfully, they set the DeviceState to 3 to indicate that the devices have joined the network. If the joining process needs security authentication, the devices set the DeviceState to 3 during the authentication process. See Table 20 for DeviceState.

9.5.4 Networkleaving services

9.5.4.1 NLME-LEAVE.request

The semantics of NLME-LEAVE.request are described as follows:

```
NLME-LEAVE.request (
    SrcAddr,
    DstAddr,
    LeavingReason
)
```

Table 81 specifies the parameters for NLME-LEAVE.request.

Table 81 – NLME-LEAVE.request parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	The address of the device to which to send the leaving response
LeavingReason	Unsigned8	0 to 255	1 = Passive leaving of a routing device or a field device 2 = Active leaving of a routing device Others are reserved.

When a routing device wants to leave the network, or the gateway device wants a device to leave the network, the DMAP invokes NLME-LEAVE.request and requests its NL to start the leaving process.

9.5.4.2 NLME-LEAVE.indication

The semantics of NLME-LEAVE.indication are described as follows:

```
NLME-LEAVE.indication (
    DeviceAddr,
    LeavingReason
)
```

Table 82 specifies the parameters for NLME-LEAVE.indication.

Table 82 – NLME-LEAVE.indication parameters

Name	Data type	Valid range	Description
DeviceAddr	Unsigned16	0 to 65 535	The address of the device invoking Leaving request
LeavingReason	Unsigned8	0 to 255	1 = Passive leaving of a routing device or a field device 2 = Active leaving of a routing device Others are reserved.

On receipt of a leaving request command packet, the NL will invoke NLME-LEAVE.indication and inform the DMAP.

9.5.4.3 NLME-LEAVE.response

The semantics of NLME- LEAVE.response are described as follows:

```
NLME-LEAVE.response (
    DevAddr,
    Status
)
```

Table 83 specifies the parameters for NLME-LEAVE.response.

Table 83 – NLME-LEAVE.response parameters

Name	Data type	Valid range	Description
DevAddr	Unsigned16	0 to 65 535	The address of the device that has requested leaving
Status	Unsigned8	0 to 255	Execution result of the request 0 = SUCCESS; 1 = FAILURE; Others are reserved.

NLME-LEAVE.response is used by DMAP or NM to inform the leaving device whether or not the leaving request has been accepted.

9.5.4.4 NLME-LEAVE.confirm

The semantics of NLME-LEAVE.confirm are described as follows:

```
NLME-LEAVE.confirm (
    DevAddr,
    Status
)
```

Table 84 specifies the parameters for NLME-LEAVE.confirm.

Table 84 – NLME-LEAVE.confirm parameters

Name	Data type	Valid range	Description
DevAddr	Unsigned16	0 to 65 535	The address of the device that has either requested leaving or been instructed to leave by Gateway device
Status	Unsigned8	0 to 255	Execution result of the request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

NLME-LEAVE.confirm is generated by the NL in response to NLME-LEAVE.request. NLME-LEAVE.confirm returns a status of either SUCCESS, indicating that the request to transmit is successful, or FAILURE, indicating that the request to transmit is failed.

9.5.4.5 Time sequence for device leaving

9.5.4.5.1 Time sequence for field device leaving

The leaving processes of field devices include the following two types.

- Active leaving. For a field device, the DMAP invokes DLME-LEAVE.request to send a leaving request to the routing device or the gateway device that is its cluster head. After

receiving the leaving request command packet from the field device, the NL of the routing device or the gateway device informs the DMAP with DLME-LEAVE.indication. If the field device leaves the routing device, the routing device sends NLME-RPT-CLRMEM.request to the gateway device. Figure 45 illustrates the time sequence of a field device's active leaving.

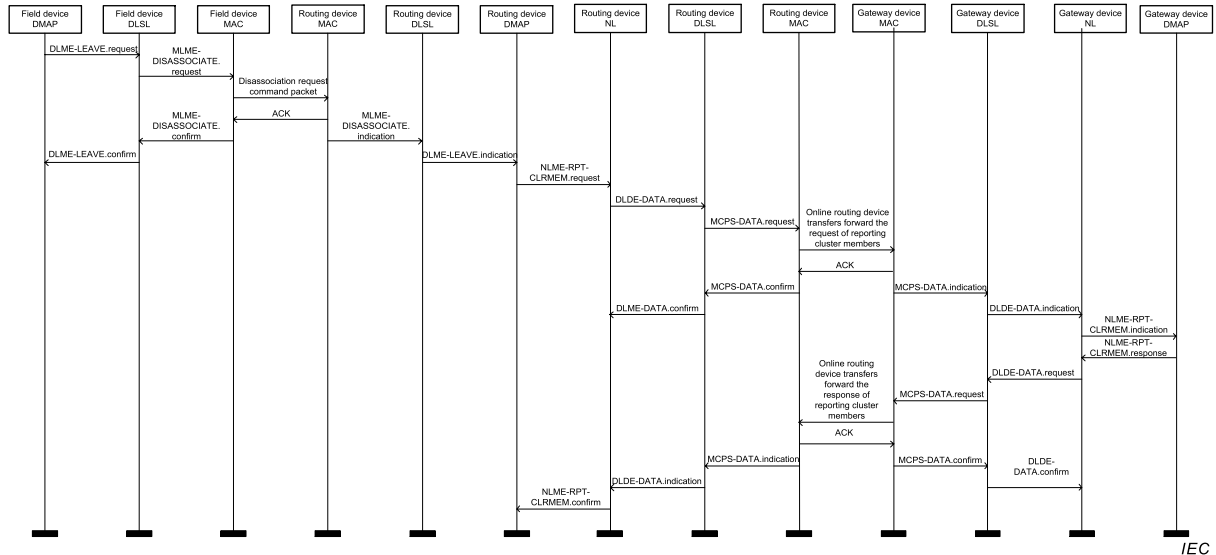


Figure 45 – Active leaving process of field device (leaving routing device)

See IEEE STD 802.15.4-2011, Figure 27 for the detailed message sequence chart between peer MAC entities.

- b) Passive leaving. The DMAP of a routing device requests for its field device to leave the network by DLME-LEAVE.request. After receiving this request, the field device returns Acknowledge (ACK). If the routing device receives DLME-LEAVE.confirm, it sends a cluster member report request to the gateway device. Figure 46 illustrates the time sequence of a field device passive leaving.

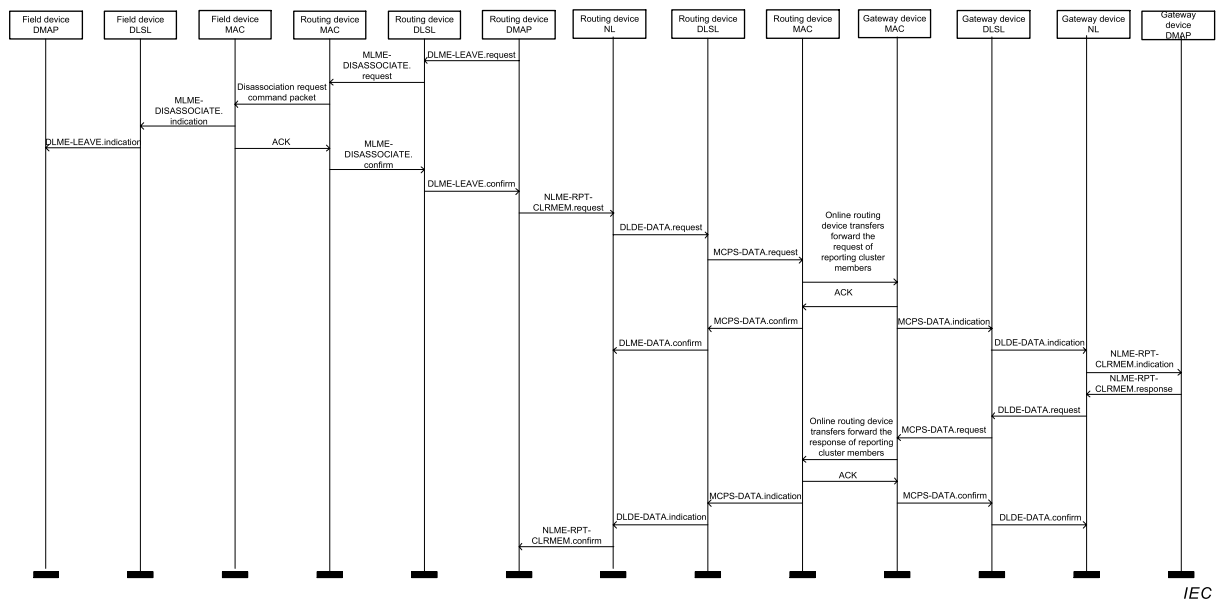


Figure 46 – Passive leaving of field device

Routing devices connect to both the mesh network and the star network. Therefore, the routing device should inform both the gateway device and its field devices of its leaving.

See IEEE STD 802.15.4-2011, Figure 20 for the detailed message sequence chart between peer MAC entities.

9.5.5 Cluster member report services

9.5.5.1 NLME-RPT-CLRMEM.request

NLME-RPT-CLRMEM.request is used by routing devices to report the information of the cluster members to the gateway device.

The semantics of NLME-RPT-CLRMEM.request are described as follows:

```
NLME-RPT-CLRMEM.request (
    SrcAddr,
    DstAddr,
    ClrMemFlag,
    ClrMemAddr
)
```

Table 85 specifies the parameters for NLME-RPT-CLRMEM.request.

Table 85 – NLME-RPT-CLRMEM.request parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	The source address
DstAddr	Unsigned16	0 to 65 535	The destination address
ClrMemFlag	Unsigned8	0 to 255	The flag of the cluster member modification: 0 = Add; 1 = Delete; Others are reserved.
ClrMemAddr	Unsigned16	0 to 65 535	The network address of the modified cluster member

9.5.5.2 NLME-RPT-CLRMEM.confirm

NLME-RPT-CLRMEM.confirm is used by the NL to return the result of NLME-RPT-CLRMEM.request to the DMAP.

The semantics of NLME-RPT-CLRMEM.confirm are described as follows:

```
NLME-RPT-CLRMEM.confirm (
    Status
)
```

Table 86 specifies the parameters for NLME-RPT-CLRMEM.confirm.

Table 86 – NLME-RPT-CLRMEM.confirm parameter

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	The result of the cluster member report: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.5.3 NLME-RPT-CLRMEM.indication

NLME-RPT-CLRMEM.indication is used by the NL to report the successful receipt of cluster member report request packets.

The semantics of NLME-RPT-CLRMEM.indication are described as follows:

```
NLME-RPT-CLRMEM.indication (
    SrcAddr,
    ClrMemFlag,
    ClrMemAddr
)
```

Table 85 specifies the parameters for NLME-RPT-CLRMEM.indication.

9.5.5.4 NLME-RPT-CLRMEM.response

NLME-RPT-CLRMEM.response is used to respond to NLME-RPT-CLRMEM.indication.

The semantics of NLME-RPT-CLRMEM.response are described as follows:

```
NLME-RPT-CLRMEM.response (
    DstAddr,
    Status
)
```

Table 87 specifies the parameters for NLME-RPT-CLRMEM.response.

Table 87 – NLME-RPT-CLRMEM.response parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	The destination address
Status	Unsigned8	0 to 255	The result returned from cluster member report: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.5.5 Time sequence for cluster member reporting

The time sequence diagram for reporting cluster member is shown in Figure 49.

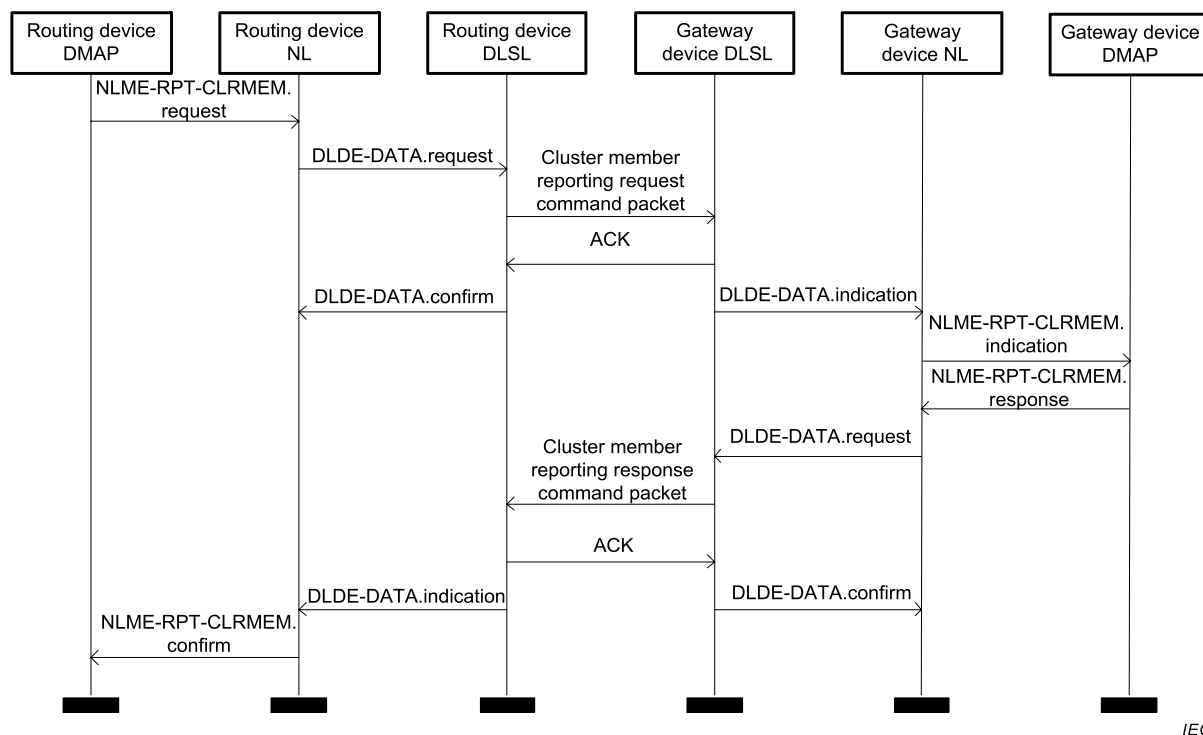


Figure 49 – Cluster member reporting process

9.5.6 Neighbour information report services

9.5.6.1 NLME-NEIGHBOUR-INFO.request

NLME-NEIGHBOUR-INFO.request is used for a routing device to report its one-hop neighbours' information to the gateway device. This usage of NLME-NEIGHBOUR-INFO.request is triggered only when a neighbour joins or leaves the WIA-PA network. The neighbour itself and its next hop neighbour to GW reports neighbour information to GW.

The semantics of NLME-NEIGHBOUR-INFO.request are described as follows:

```

NLME-NEIGHBOUR-INFO.request (
    SrcAddr,
    DstAddr,
    NeighbourCount,
    NeighbourStructure
)
    
```

Table 88 specifies the parameters for NLME-NEIGHBOUR-INFO.request.

Table 88 – NLME-NEIGHBOUR-INFO.request parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	16-bit source address
DstAddr	Unsigned16	0 to 65 535	16-bit destination address
NeighbourCount	Unsigned8	0 to 255	Number of the neighbours
NeighbourStructure	Neighbour_Struct structure (see Table 18)		Information of the neighbours

9.5.6.2 NLME-NEIGHBOUR-INFO.indication

NLME-NEIGHBOUR-INFO.indication is used for the DLSL to report the received NLME-NEIGHBOUR-INFO.request packet to the DMAP.

The semantics of NLME-NEIGHBOUR-INFO.indication are described as follows:

```
NLME-NEIGHBOUR-INFO.indication (
    SrcAddr,
    NeighbourCount,
    NeighbourStructure
)
```

Table 88 specifies the parameters for NLME-NEIGHBOUR-INFO.indication.

9.5.6.3 NLME-NEIGHBOUR-INFO.confirm

NLME-NEIGHBOUR-INFO.confirm is used to report the successful sending of neighbour information report request packets.

The semantics of NLME-NEIGHBOUR-INFO.confirm are described as follows:

```
NLME-NEIGHBOUR-INFO.confirm (
    Status
)
```

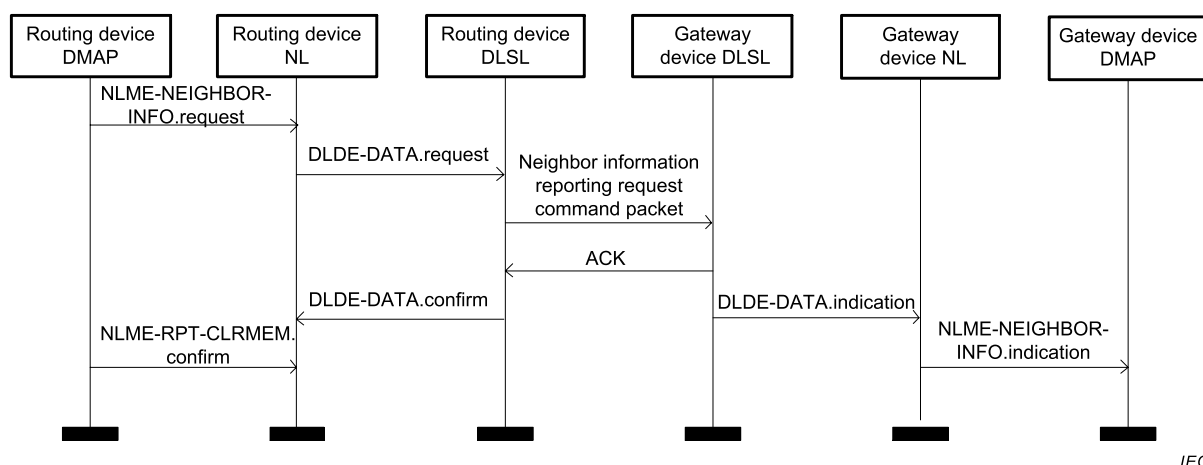
Table 89 specifies the parameters for NLME-NEIGHBOUR-INFO.confirm.

Table 89 – NLME-NEIGHBOUR-INFO.confirm parameter

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Reporting the result of the neighbour information: 0 = SUCCESS; 1 = .FAILURE; Others are reserved.

9.5.6.4 Time sequence for neighbour information reporting

The time sequence diagram for reporting neighbour information is shown in Figure 50.



IEC

Figure 50 – Neighbour information reporting process

9.5.7 Route allocation services

9.5.7.1 Route adding services

9.5.7.1.1 NLME-ADD_ROUTE.request

NLME-ADD_ROUTE.request is used to add a record to the routing table of a routing device.

The semantics of NLME-ADD_ROUTE.request are described as follows:

```

NLME-ADD_ROUTE.request (
    DstAddr,
    RoutingTableRecord
)
    
```

Table 90 specifies the parameters for NLME-ADD_ROUTE.request.

Table 90 – NLME-ADD_ROUTE.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	The 16-bit short address of the routing device
RoutingTableRecord	NLRoute_Struct structure (see Table 15)		A routing table item

9.5.7.1.2 NLME-ADD_ROUTE.confirm

NLME-ADD_ROUTE.confirm reports the result of a NLME-ADD_ROUTE.request.

The semantics of NLME_ADD-ROUTE.confirm are described as follows:

```

NLME-ADD_ROUTE.confirm(
    Status
)
    
```

Table 91 specifies the parameters for NLME-ADD_ROUTE.confirm.

Table 91 – NLME-ADD_ROUTE.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	The result of an NLME-ADD_ROUTE.request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

On receipt of NLME-ADD_ROUTE.request, the NL should transmit an adding-route-request packet to the routing device and should return an NLME-ADD_ROUTE.confirm to report the result.

9.5.7.1.3 NLME-ADD_ROUTE.indication

NLME-ADD_ROUTE.indication is used to report to the DMAP that a device has successfully received a route adding request packet.

The semantics of NLME_ADD-ROUTE.confirm are described as follows:

```
NLME-ADD_ROUTE.indication (
    RoutingTableRecord
)
```

Table 90 specifies the parameters for NLME-ADD_ROUTE.indication.

9.5.7.1.4 NLME-ADD_ROUTE.response

NLME-ADD_ROUTE.response is the response of NLME-ADD_ROUTE.indication.

The semantics of NLME-ADD_ROUTE.response are described as follows:

```
NLME-ADD_ROUTE.response (
    Status
)
```

Table 91 specifies the parameters for NLME-ADD_ROUTE.response.

9.5.7.1.5 Time sequence for route adding

The time sequence diagram for adding a record to the routing table of a routing device is shown in Figure 51.

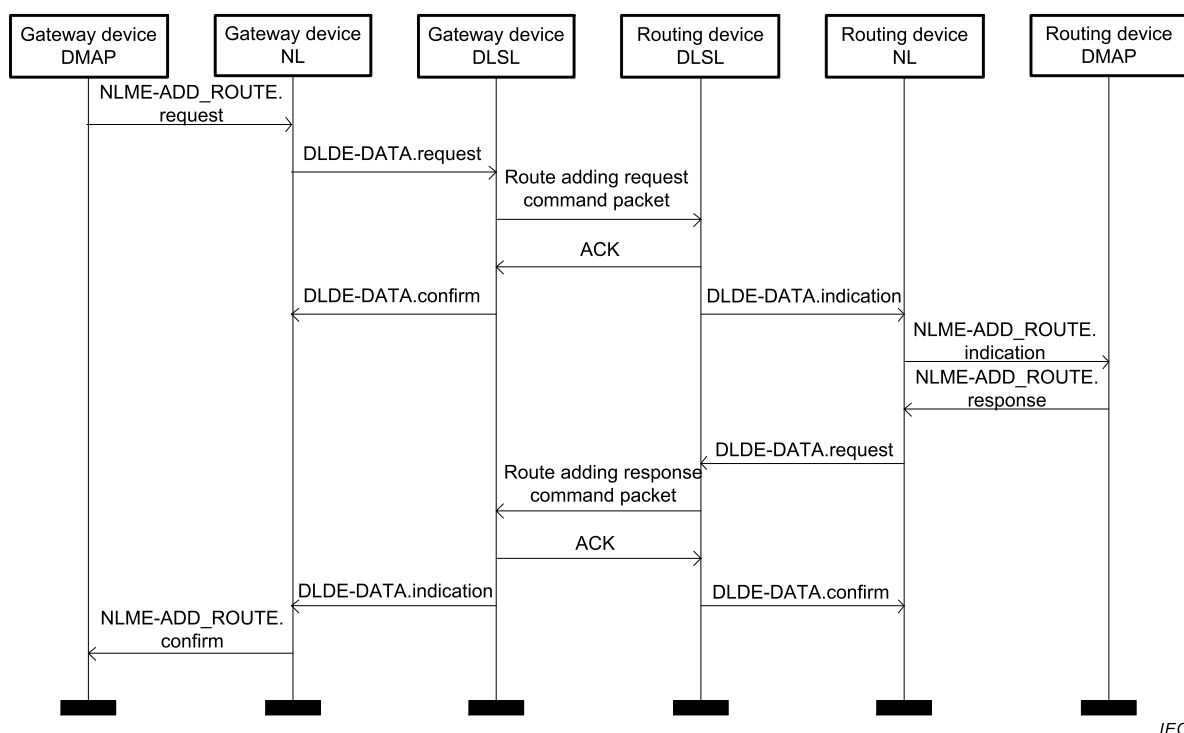


Figure 51 – Time sequence for route adding

9.5.7.2 Route update services

9.5.7.2.1 NLME-UPDATE_ROUTE.request

NLME-UPDATE_ROUTE.request updates a record in the routing table of a routing device.

The semantics of NLME-UPDATE_ROUTE.request are described as follows:

```

NLME-UPDATE_ROUTE.request (
    DstAddr,
    RoutingTableRecord
)
    
```

Table 92 specifies the parameters for NLME-UPDATE_ROUTE.request.

Table 92 – NLME-UPDATE_ROUTE.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit short address of routing device
RoutingTableRecord	NLRoute_Struct structure (see Table 15)		A routing table item

The NM invokes NLME-UPDATE_ROUTE.request to update a record in the routing table of routing devices.

9.5.7.2.2 NLME-UPDATE_ROUTE.confirm

The NLME_UPDATE-ROUTE.confirm reports the execution result of an NLME-UPDATE_ROUTE.request.

The semantics ofNLME_UPDATE-ROUTE.confirm are described as follows:

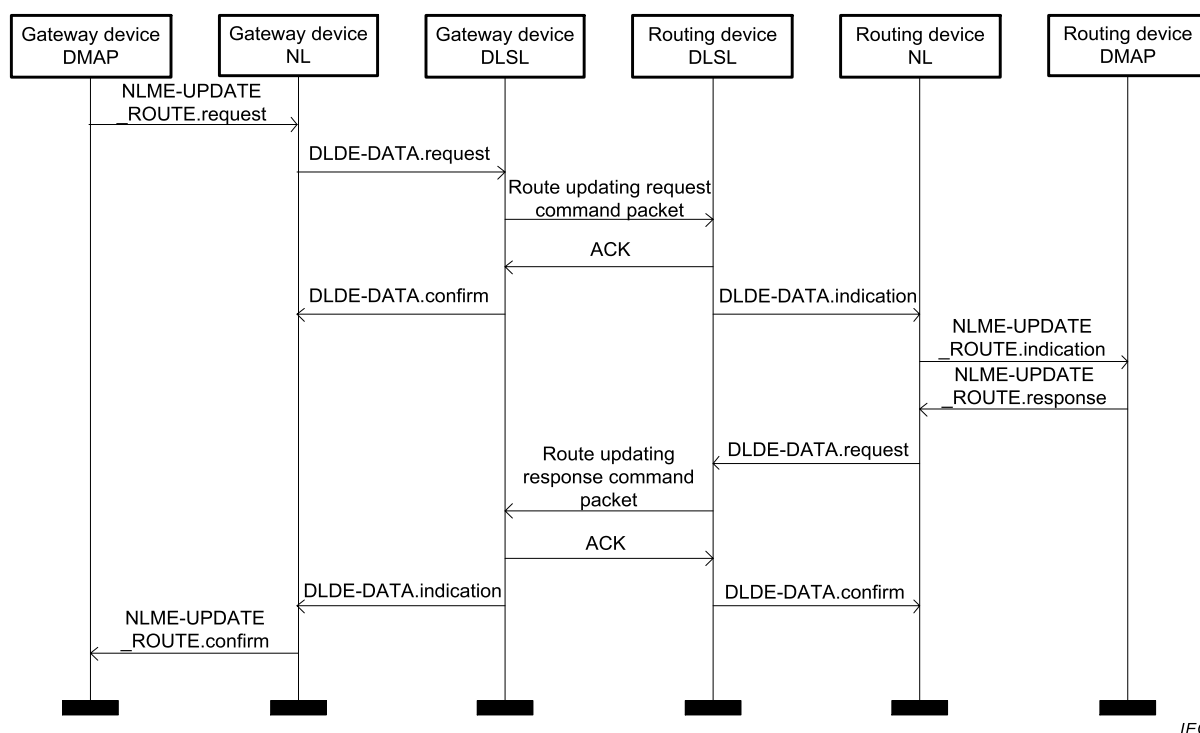


Figure 52 – Time sequence for route updating

9.5.7.3 Route deleting services

9.5.7.3.1 NLME-DELETE_ROUTE.request

The NM invokes NLME-DELETE_ROUTE.request to delete a record in the routing table of a routing device.

The semantics of NLME_DELETE-ROUTE.confirm are described as follows:

```

NLME-DELETE_ROUTE.request(
    DstAddr,
    RouteID
)
    
```

Table 94 specifies the parameters for NLME-DELETE-ROUTE.request.

Table 94 – NLME-UPDATE_ROUTE.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	The 16-bit short address of the destination routing device
RouteID	Unsigned16	0 to 65 535	Route ID

9.5.7.3.2 NLME-DELETE_ROUTE.confirm

The NLME_DELETE-ROUTE.confirm reports the result of executing an NLME-DELETE_ROUTE.request.

The semantics of NLME_DELETE-ROUTE.confirm are described as follows:

```

NLME-DELETE_ROUTE.confirm(
    Status
)

```

Table 95 specifies the parameters for NLME-DELETE_ROUTE.confirm.

Table 95 – NLME-DELETE_ROUTE.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	The result of an NLME-DELETE_ROUTE.request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

On receipt of NLME-DELETE_ROUTE.request, the NL should transmit a route deleting request packet to the routing device and return an NLME-DELETE_ROUTE.confirm to report the result.

9.5.7.3.3 NLME-DELETE_ROUTE.indication

NLME-DELETE_ROUTE.indication is used to report to the DMAP that the device has successfully received a route deleting request packet.

The semantics of NLME-DELETE_ROUTE.confirm are described as follows:

```

NLME-DELETE_ROUTE.indication (
    RouteID
)

```

Table 94 specifies the parameters for NLME-DELETE_ROUTE.indication.

9.5.7.3.4 NLME-DELETE_ROUTE.response

The NLME-NLME-DELETE_ROUTE.response is the response of NLME-DELETE_ROUTE.indication.

The semantics of NLME-DELETE_ROUTE.response are described as follows:

```

NLME-DELETE_ROUTE.response (
    Status
)

```

Table 95 specifies the parameters for NLME-DELETE_ROUTE.response.

9.5.7.3.5 Time sequence for route deleting

The time sequence diagram for deleting records in the routing tables of routing devices is shown in Figure 53.

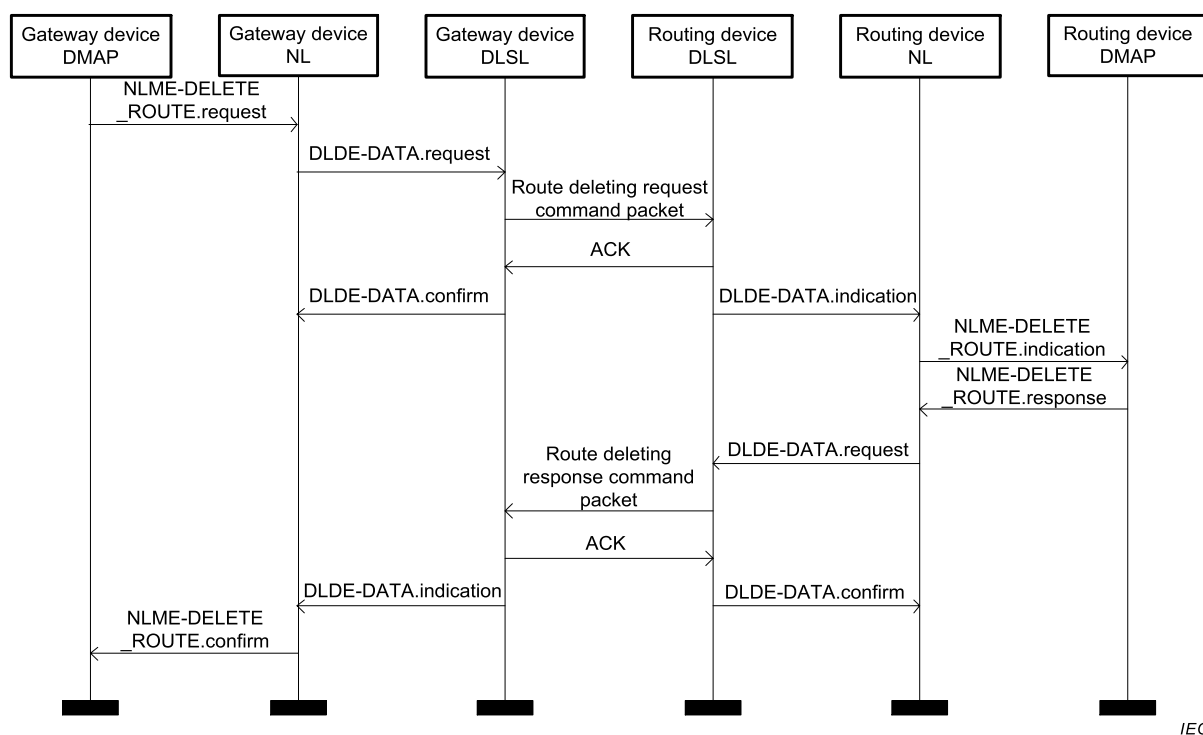


Figure 53 – Time sequence for route deleting

9.5.8 Communication resource allocation services

9.5.8.1 General

Communication resource allocation includes the allocation of link and superframe. These services provide the following primitives:

- Link adding services:
 - NLME-ADD-LINK.request,
 - NLME-ADD-LINK.confirm,
 - NLME-ADD-LINK.response, and
 - NLME-ADD-LINK.indication;
- Link update services:
 - NLME-UPDATE-LINK.request,
 - NLME-UPDATE-LINK.confirm,
 - NLME-UPDATE-LINK.response, and
 - NLME-UPDATE-LINK.indication;
- Link release services:
 - NLME-RELEASE-LINK.request,
 - NLME-RELEASE-LINK.confirm,
 - NLME-RELEASE-LINK.response, and
 - NLME-RELEASE-LINK.indication;
- Superframe adding services:
 - NLME-ADD-SFR.request,
 - NLME-ADD-SFR.confirm,
 - NLME-ADD-SFR.response, and

- NLME-ADD-SFR.indication;
- Superframe update services:
 - NLME-UPDATE-SFR.request,
 - NLME-UPDATE-SFR.confirm,
 - NLME-UPDATE-SFR.response, and
 - NLME-UPDATE-SFR.indication;
- Superframe release services:
 - NLME-RELEASE-SFR.request,
 - NLME-RELEASE-SFR.confirm,
 - NLME-RELEASE-SFR.response, and
 - NLME-RELEASE-SFR.indication.

9.5.8.2 Link adding services

9.5.8.2.1 NLME-ADD-LINK.request

NLME-ADD-LINK.request is used to add one or more record(s) of new link(s), which is originated either from the gateway device to a routing device or from a routing device to a field device.

The semantics of NLME-ADD-LINK.request are described as follows:

```
NLME-ADD-LINK.request (
    DstAddr,
    LinkCount,
    LinkStructure
)
```

Table 96 specifies the parameters for NLME-ADD-LINK.request.

Table 96 – NLME-ADD-LINK.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit destination address
LinkCount	Unsigned16	0 to 65 535	Count of added links to support adding multiple links each time
LinkStructure	Link_Struct structure (See Table 17)		Information of the links

9.5.8.2.2 NLME-ADD-LINK.confirm

NLME-ADD-LINK.confirm reports the results of NLME-ADD-LINK.request.

The semantics of NLME-ADD-LINK.confirm are described as follows:

```
NLME-ADD-LINK.confirm (
    Status
)
```

Table 97 specifies the parameters for NLME-ADD-LINK.confirm.

Table 97 – NLME-ADD-LINK.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Results of link adding request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.8.2.3 NLME-ADD-LINK.indication

NLME-ADD-LINK.indication is used to report to the DMAP that the device has successfully received a link adding request packet.

The semantics of NLME-ADD-LINK.indication are described as follows:

```
NLME-ADD-LINK.indication (
    LinkCount,
    LinkStructure
)
```

Table 96 specifies the parameters for NLME-ADD-LINK.indication.

9.5.8.2.4 NLME-ADD-LINK.response

NLME-ADD-LINK.response is the response of NLME-ADD-LINK.indication.

The semantics of NLME-ADD-LINK.response are described as follows:

```
NLME-ADD-LINK.response (
    Status
)
```

Table 97 specifies the parameters for NLME-ADD-LINK.response.

9.5.8.2.5 Time sequence for link adding

The time sequence for adding a link originating from the gateway device to a routing device is shown in Figure 54.

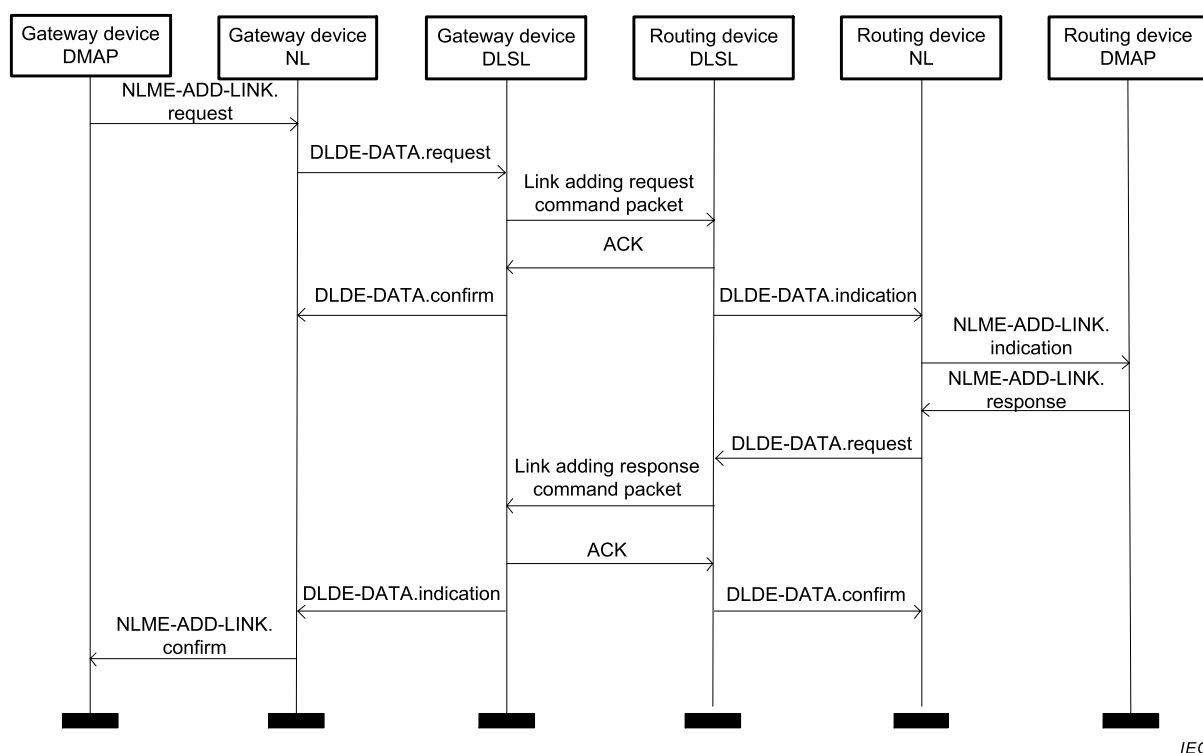


Figure 54 – Adding a link originating from gateway device to routing device

The time sequence for adding a link originating from a routing device to a field device is shown in Figure 55.

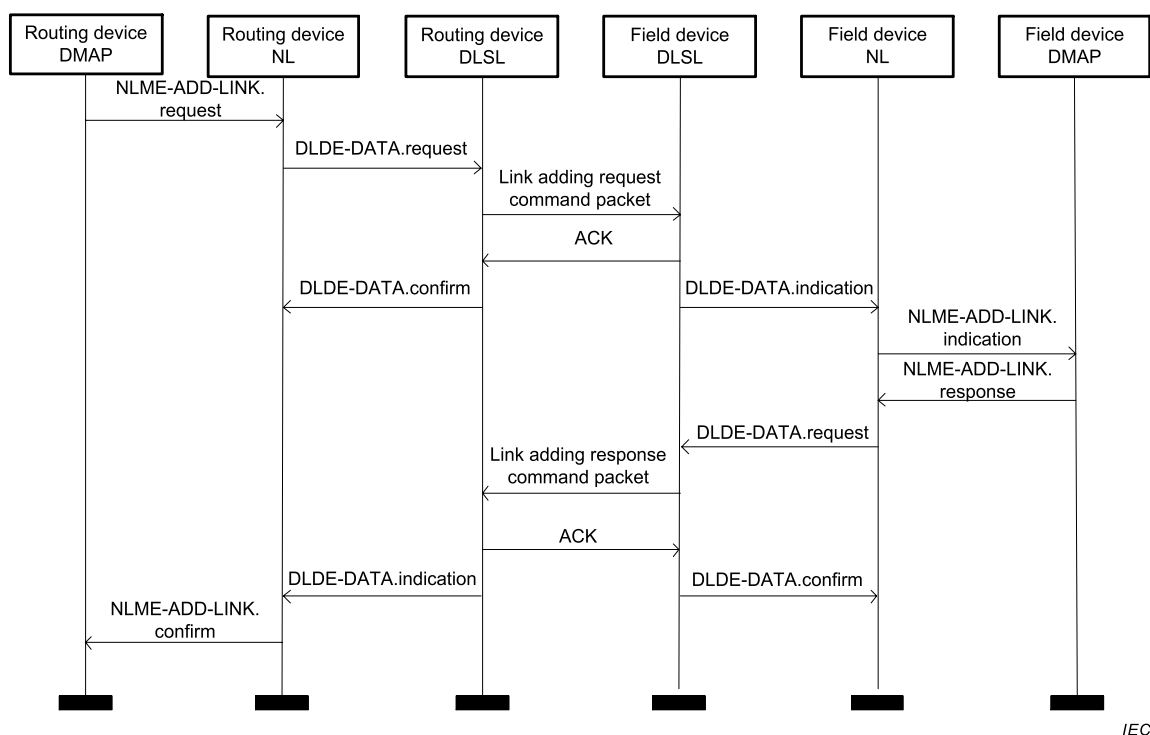


Figure 55 – Adding a link originating from routing device to field device

9.5.8.3 Link update services

9.5.8.3.1 NLME-UPDATE-LINK.request

NLME-UPDATE-LINK.request is used to update one or more record(s) of existing link(s), which is originating either from the gateway device to a routing device or from a routing device to a field device.

The semantics of NLME-UPDATE-LINK.request are described as follows:

```
NLME-UPDATE-LINK.request (
    DstAddr,
    LinkCount,
    LinkStructure
)
```

Table 98 specifies the parameters for NLME-UPDATE-LINK.request.

Table 98 – NLME-UPDATE-LINK.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit destination address
LinkCount	Unsigned16	0 to 65 535	Count of added links to support updating multiple links each time
LinkStructure	Link_Struct structure (See Table 17)		Information of the links

9.5.8.3.2 NLME-UPDATE-LINK.confirm

NLME-UPDATE-LINK.confirm reports the results of NLME-UPDATE-LINK.request.

The semantics of NLME-UPDATE-LINK.confirm are described as follows:

```
NLME-UPDATE-LINK.confirm (
    Status
)
```

Table 99 specifies the parameters for NLME-UPDATE-LINK.confirm.

Table 99 – NLME-UPDATE-LINK.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Results of the link update request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.8.3.3 NLME-UPDATE-LINK.indication

NLME-UPDATE-LINK.indication is used to report to the DMAP that the device has successfully received a link update request packet.

The semantics of NLME-UPDATE-LINK.indication are described as follows:

```
NLME-UPDATE-LINK.indication (
    LinkCount,
    LinkStructure
)
```

Table 98 specifies the parameters for NLME-UPDATE-LINK.indication.

9.5.8.3.4 NLME-UPDATE-LINK.response

NLME-UPDATE-LINK.response is the response to NLME-UPDATE-LINK.indication.

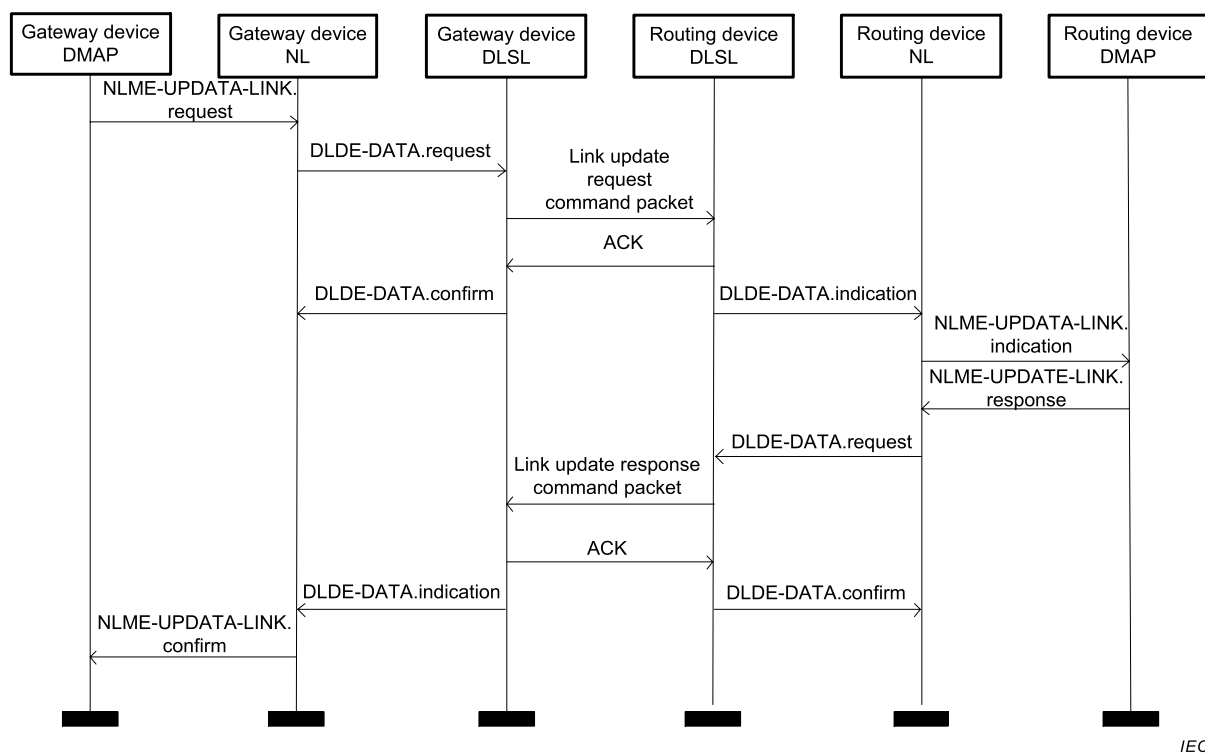
The semantics of NLME-UPDATE-LINK.response are described as follows:

NLME-UPDATE-LINK.response (
 Status
)

Table 99 specifies the parameters for NLME-UPDATE-LINK.response.

9.5.8.3.5 Time sequence for link update

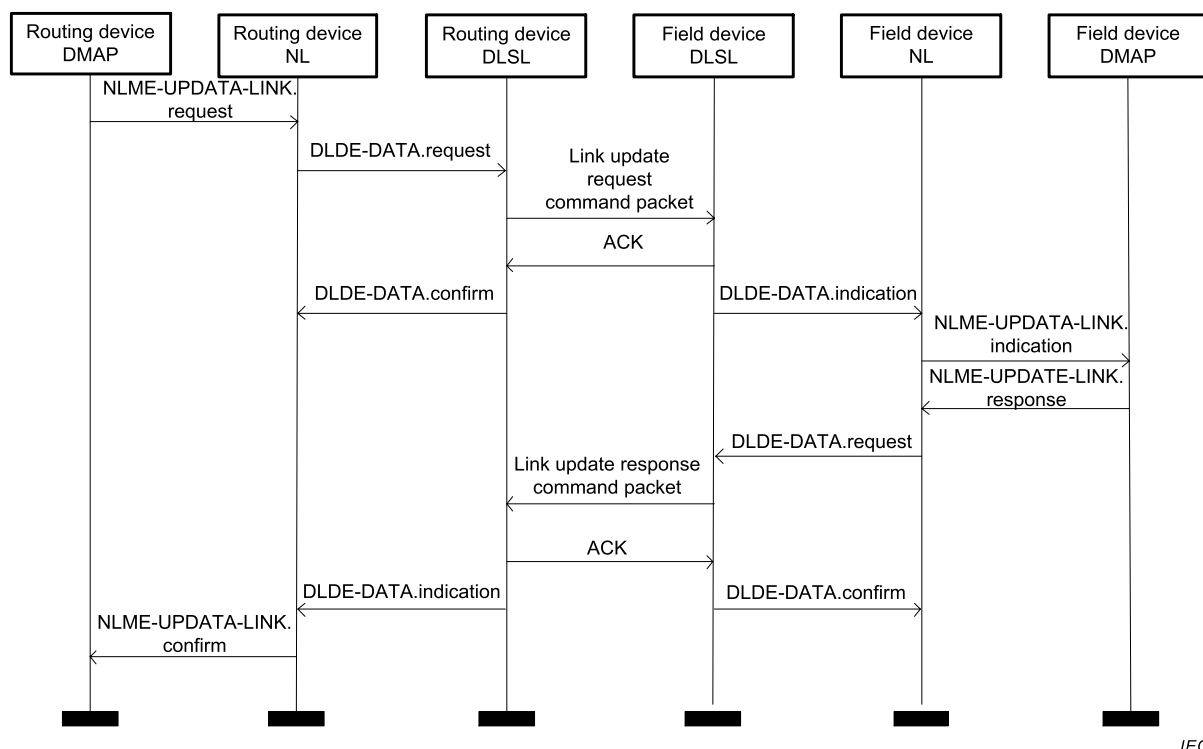
The time sequence for updating a link originating from the gateway device to a routing device is shown in Figure 56.



IEC

Figure 56 – Updating a link originating by gateway device to routing device

The time sequence for updating a link originating from a routing device to a field device is shown in Figure 57.



IEC

Figure 57 – Updating a link originating from routing device to field device

9.5.8.4 Link release services

9.5.8.4.1 NLME-RELEASE-LINK.request

NLME-RELEASE-LINK.request is used to delete one or more existing link(s), which is originated either from the gateway device to a routing device or from a routing device to a field device.

The semantics of NLME-RELEASE-LINK.request are described as follows:

```

NLME-RELEASE-LINK.request (
    DstAddr,
    LinkCount,
    LinkID[LinkCount]
)
    
```

Table 100 specifies the parameters for NLME-RELEASE-LINK.request.

Table 100 – NLME-RELEASE-LINK.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit destination address
LinkCount	Unsigned16	0 to 65 535	Count of added links to support releasing multiple links each time
LinkID[LinkCount]	Unsigned16	0 to 65 535	IDs of the deleted links

9.5.8.4.2 NLME-RELEASE-LINK.confirm

NLME-RELEASE-LINK.confirm reports the results of NLME-RELEASE-LINK.request.

The semantics of NLME-RELEASE-LINK.confirm are described as follows:

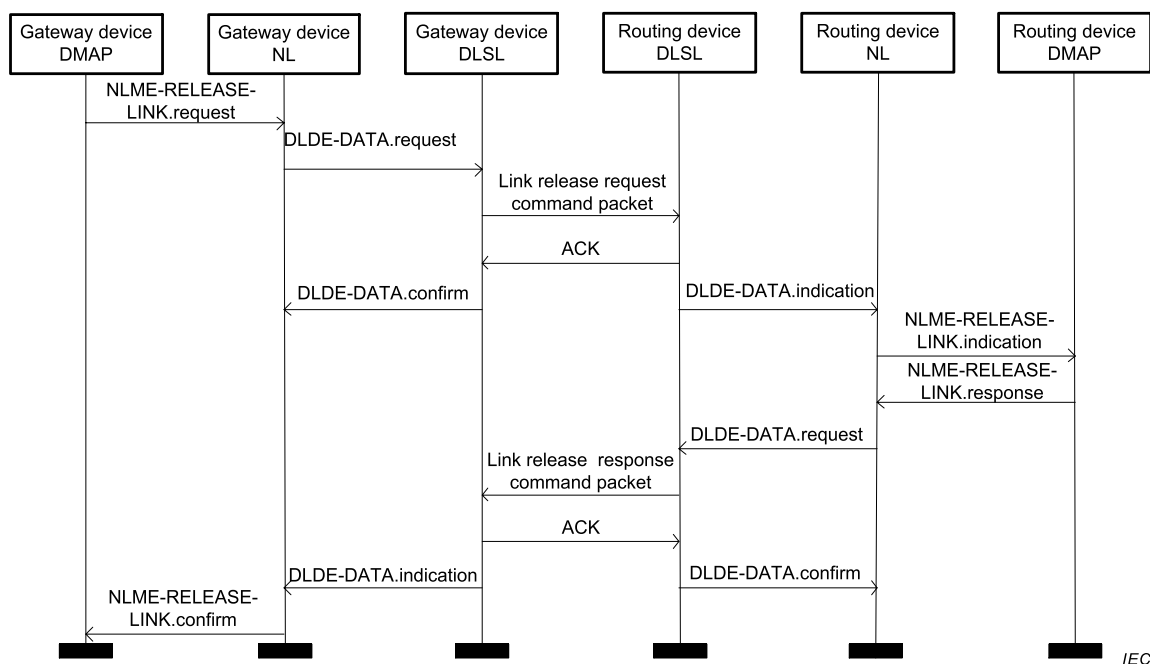


Figure 58 – Releasing a link originating from gateway device to routing device

The time sequence for releasing a link originating from a routing device to a field device is shown in Figure 59.

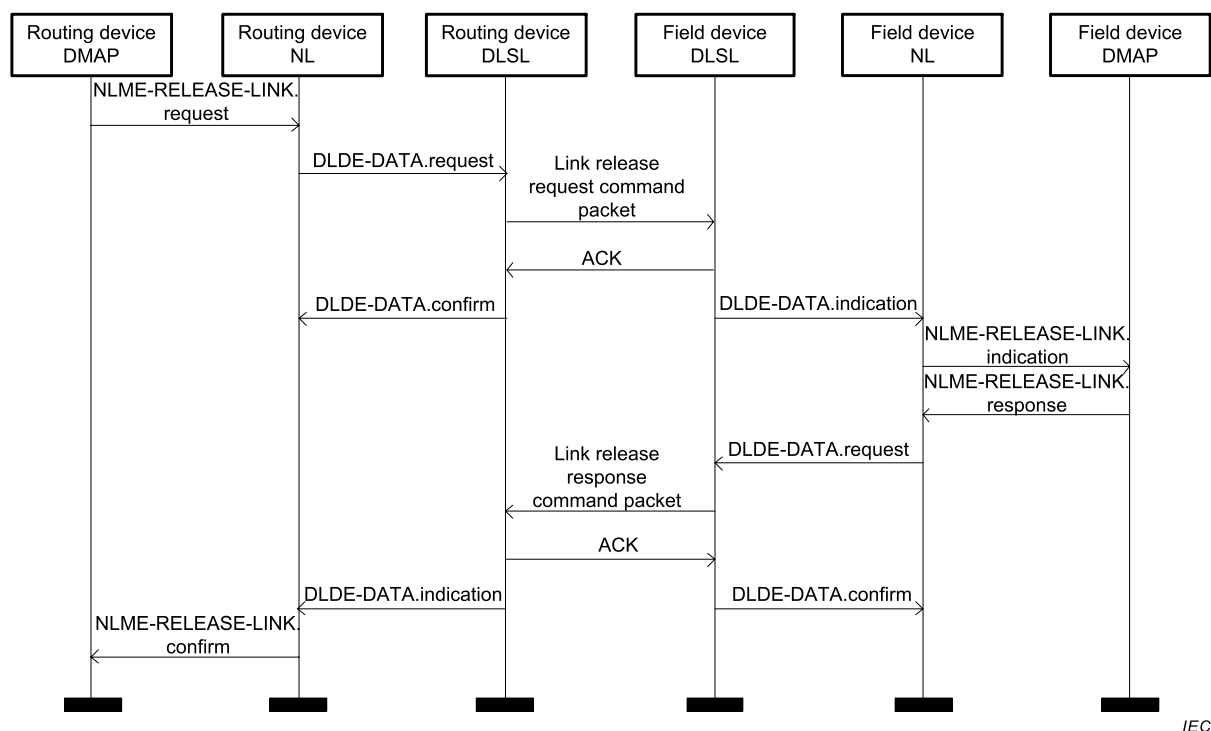


Figure 59 – Releasing a link originating from routing device to field device

9.5.8.5 Superframe adding services

9.5.8.5.1 NLME-ADD-SFR.request

NLME-ADD-SFR.request is used to add a record of a new superframe, which is originated either from the gateway device to a routing device or from a routing device to a field device.

The semantics of NLME-ADD-SFR.request are described as follows:

```
NLME-ADD-SFR.request (
    DstAddr,
    SuperframeStructure
)
```

Table 102 specifies the parameters for NLME-ADD-SFR.request.

Table 102 – NLME-ADD-SFR.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit destination address
SuperframeStructure	Superframe_Structstructure (See Table 16)		Information of superframe attribute

9.5.8.5.2 NLME-ADD-SFR.confirm

NLME-ADD-SFR.confirm reports the result of NLME-ADD-SFR.request.

The semantics of NLME-ADD-SFR.confirm are described as follows:

```
NLME-ADD-SFR.confirm (
    Status
)
```

Table 103 specifies the parameters for NLME-ADD-SFR.confirm.

Table 103 – NLME-ADD-SFR.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Results of superframe release request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.8.5.3 NLME-ADD-SFR.indication

NLME-ADD-SFR.indication is used to report to the DMAP that the device has successfully received a superframe adding request packet.

The semantics of NLME-ADD-SFR.indication are described as follows:

```
NLME-ADD-SFR.indication (
    SuperframeStructure
)
```

Table 102 specifies the parameters for NLME-ADD-SFR.indication.

9.5.8.5.4 NLME-ADD-SFR.response

NLME-ADD-SFR.response is the response to NLME-ADD-SFR.indication.

The semantics of NLME-ADD-SFR.response are described as follows:

```
NLME-ADD-SFR.response (
    Status
)
```

Table 103 specifies the parameters for NLME-ADD-SFR.response.

9.5.8.5.5 Time sequence for superframe adding

The time sequence for adding a superframe originating from the gateway device to a routing device is shown in Figure 60.

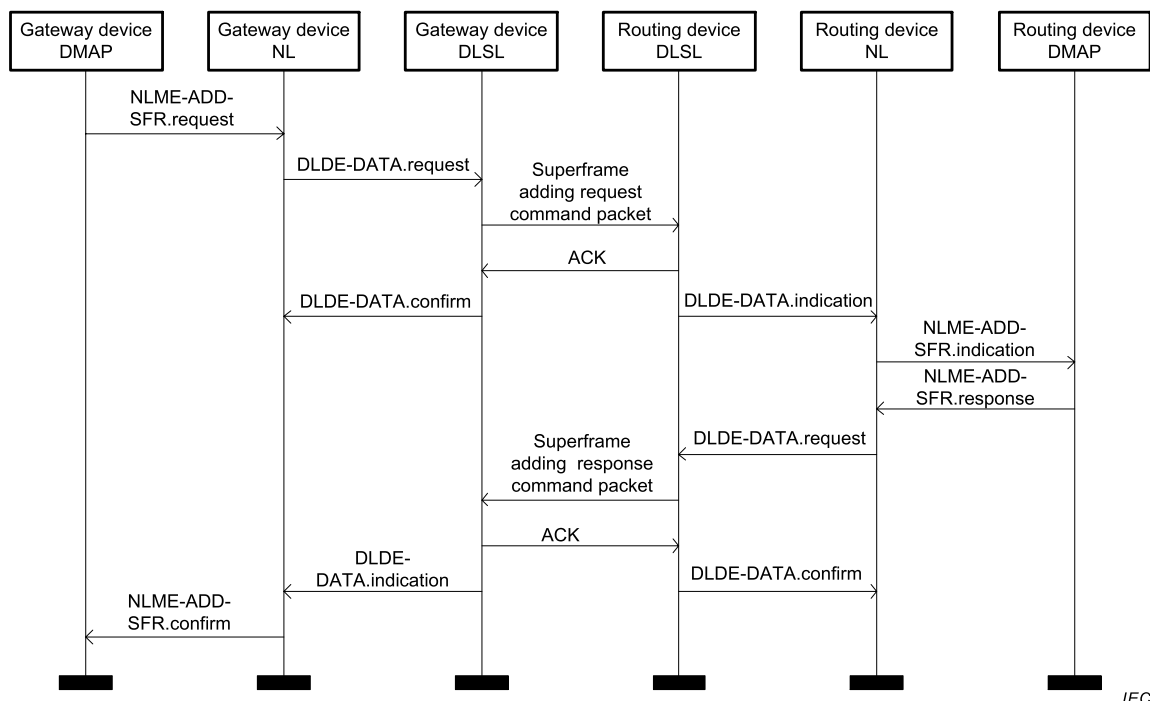


Figure 60 – Adding a superframe originating from gateway device to routing device

The time sequence for adding a superframe originating from a routing device to a field device is shown in Figure 61.

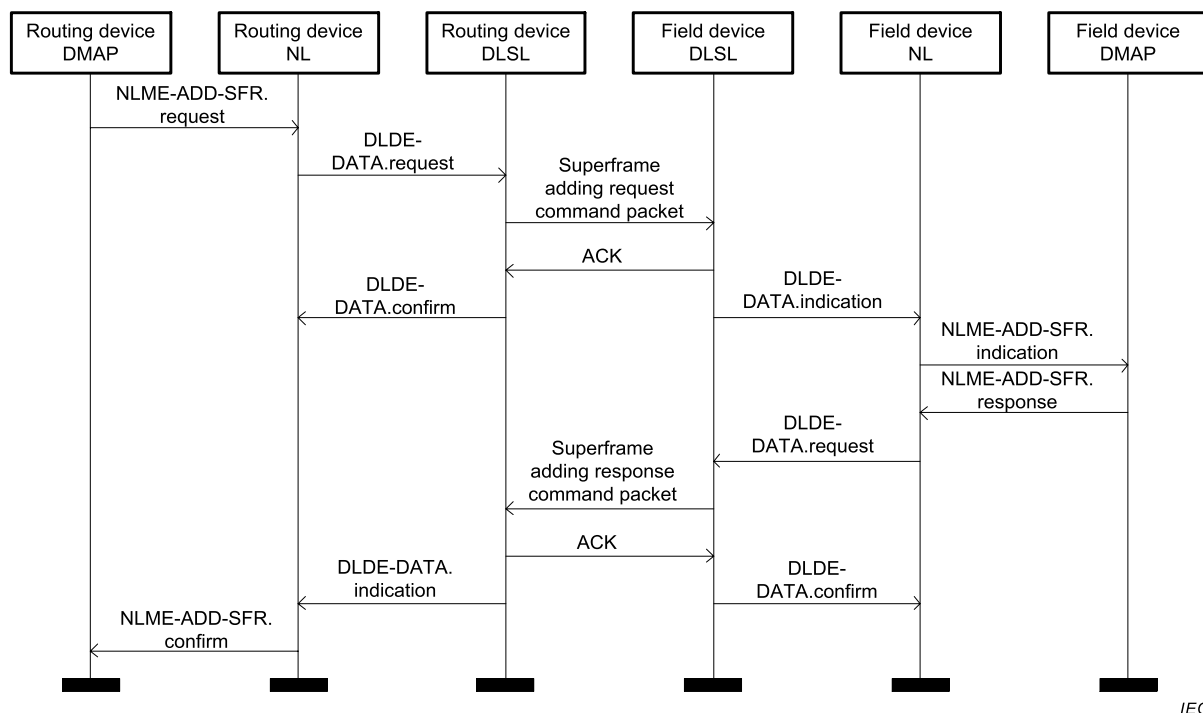


Figure 61 – Adding a superframe originating from routing device to field device

9.5.8.6 Superframe update services

9.5.8.6.1 NLME-UPDATA-SFR.request

NLME-UPDATA-SFR.request is used to modify a record of an existing superframe, which is originated from the gateway device to a routing device or from a routing device to a field device.

The semantics of NLME-UPDATA-SFR.request are described as follows:

```
NLME-UPDATA-SFR.request (
    DstAddr,
    SuperframeStructure
)
```

Table 104 specifies the parameters for NLME-UPDATA-SFR.request.

Table 104 – NLME-UPDATA-SFR.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit address of destination device
SuperframeStructure	Superframe_Struct structure (See Table 16)		Information of superframe attribute

9.5.8.6.2 NLME-UPDATE-SFR.confirm

NLME-UPDATE-SFR.confirm reports the results of NLME-UPDATA-SFR.request.

The semantics of NLME-UPDATE-SFR.confirm are described as follows:

```
NLME-UPDATE-SFR.confirm (
    Status
)
```

Table 105 specifies the parameters for NLME-UPDATE-SFR.confirm.

Table 105 – NLME-UPDATE-SFR.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Results of superframe update request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.8.6.3 NLME-UPDATE-SFR.indication

NLME-UPDATE-SFR.indication is used to report to the DMAP that the device has successfully received a superframe update request packet.

The semantics of NLME-UPDATE-SFR.indication are described as follows:

```
NLME-UPDATE-SFR.indication (
    SuperframeStructure
)
```

Table 104 specifies the parameters for NLME-UPDATE-SFR.indication.

9.5.8.6.4 NLME-UPDATE-SFR.response

NLME-UPDATE-SFR.response is the response to NLME-UPDATE-SFR.indication.

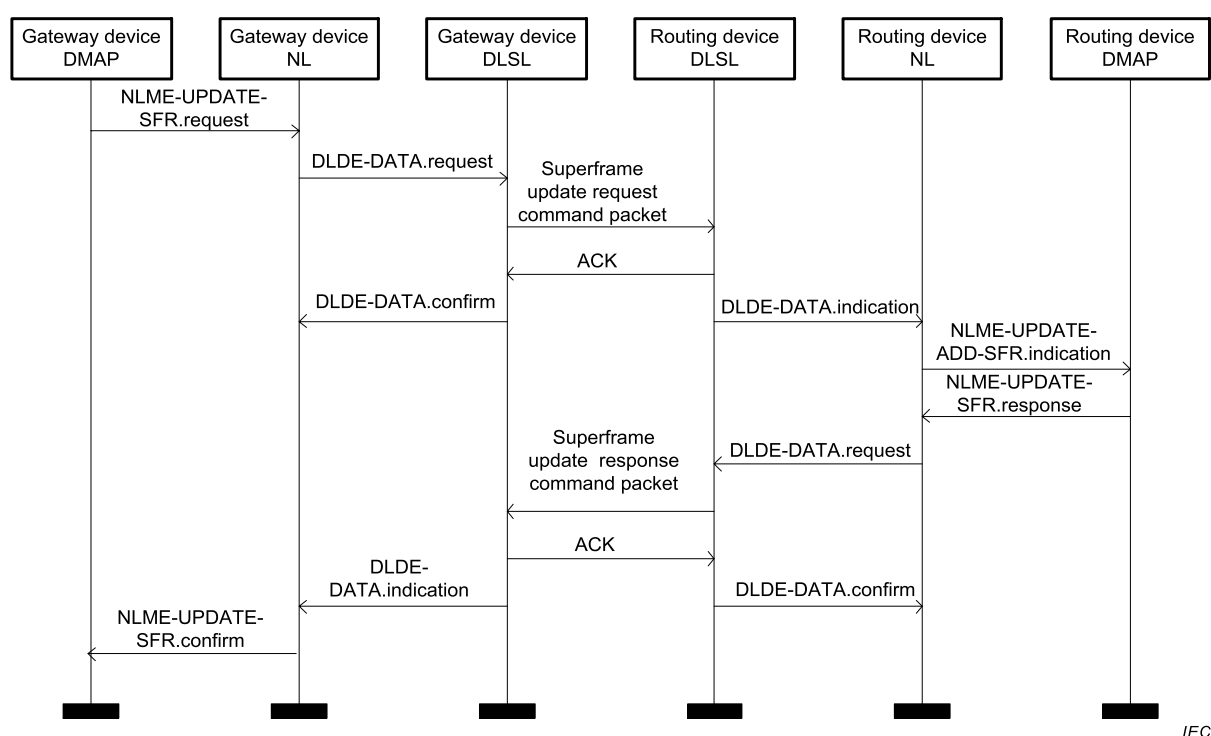
The semantics of NLME-UPDATE-SFR.response are described as follows:

NLME-UPDATE-SFR.response (
 Status
)

Table 105 specifies the parameters for NLME-UPDATE-SFR.response.

9.5.8.6.5 Time sequence for superframe update

The time sequence for updating a superframe originating from the gateway device to a routing device is shown in Figure 62.



IEC

Figure 62 – Updating a superframe originating from gateway device to routing device

The time sequence for updating a superframe originating from a routing device to a field device is shown in Figure 63.

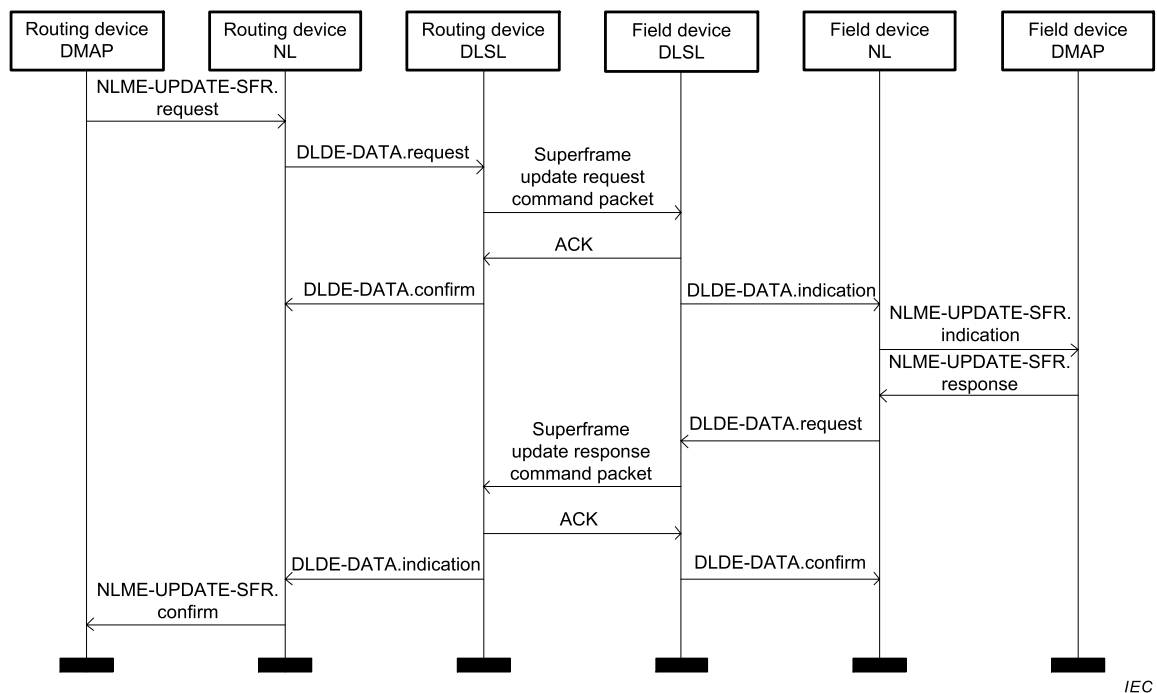


Figure 63 – Updating a superframe originating from routing device to field device

9.5.8.7 Superframe release services

9.5.8.7.1 NLME-RELEASE-SFR.request

NLME-RELEASE-SFR.request is used to delete a record of an existing superframe, which is originated either from the gateway device to a routing device or from a routing device to a field device.

The semantics of NLME-RELEASE-SFR.request are described as follows:

```
NLME-RELEASE-SFR.request (
    DstAddr,
    SuperframeID
)
```

Table 106 specifies the parameters for NLME-RELEASE-SFR.request.

Table 106 – NLME-RELEASE-SFR.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit destination address
SuperframeID	Unsigned16	0 to 65 535	ID of the deleted superframe

9.5.8.7.2 NLME-RELEASE-SFR.confirm

NLME-RELEASE-SFR.confirm reports the result of NLME-RELEASE-SFR.request.

The semantics of NLME-RELEASE-SFR.confirm are described as follows:

```
NLME-RELEASE-SFR.confirm (
    Status
)
```

Table 107 specifies the parameters for NLME-RELEASE-SFR.confirm.

Table 107 – NLME-RELEASE-SFR.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Results of superframe release request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.8.7.3 NLME-RELEASE-SFR.indication

NLME-RELEASE-SFR.indication is used to report to the DMAP that the device has successfully received a superframe release request packet.

The semantics of NLME-RELEASE-SFR.indication are described as follows:

```
NLME-RELEASE-SFR.indication (
    SuperframeID
)
```

Table 106 specifies the parameters for NLME-RELEASE-SFR.indication.

9.5.8.7.4 NLME-RELEASE-SFR.response

NLME-RELEASE-SFR.response is the response of NLME-RELEASE-SFR.indication.

The semantics of NLME-RELEASE-SFR.response are described as follows:

```
NLME-RELEASE-SFR.response (
    Status
)
```

Table 107 specifies the parameters for NLME-RELEASE-SFR.response.

9.5.8.7.5 Time sequence for superframe release

The time sequence for releasing a superframe originating from the gateway device to a routing device is shown in Figure 64.

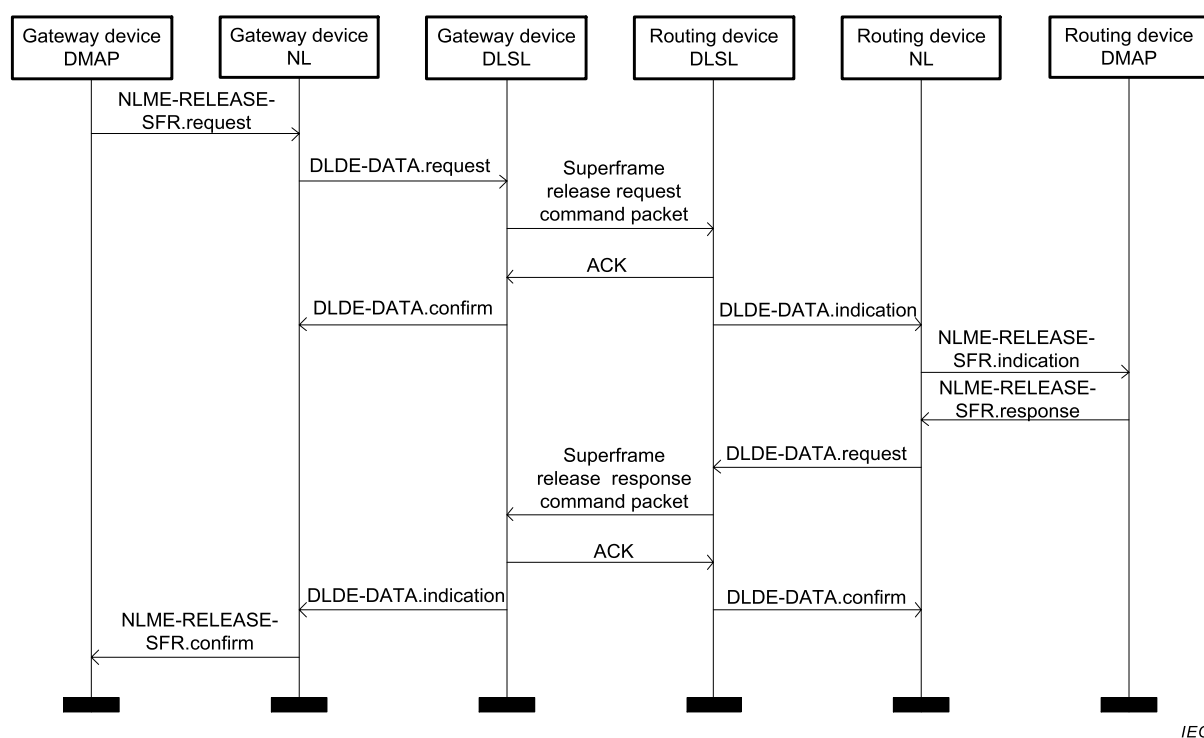


Figure 64 – Releasing a superframe originating from gateway device to routing device

The time sequence for releasing a superframe originating from a routing device to a field device is shown in Figure 65.

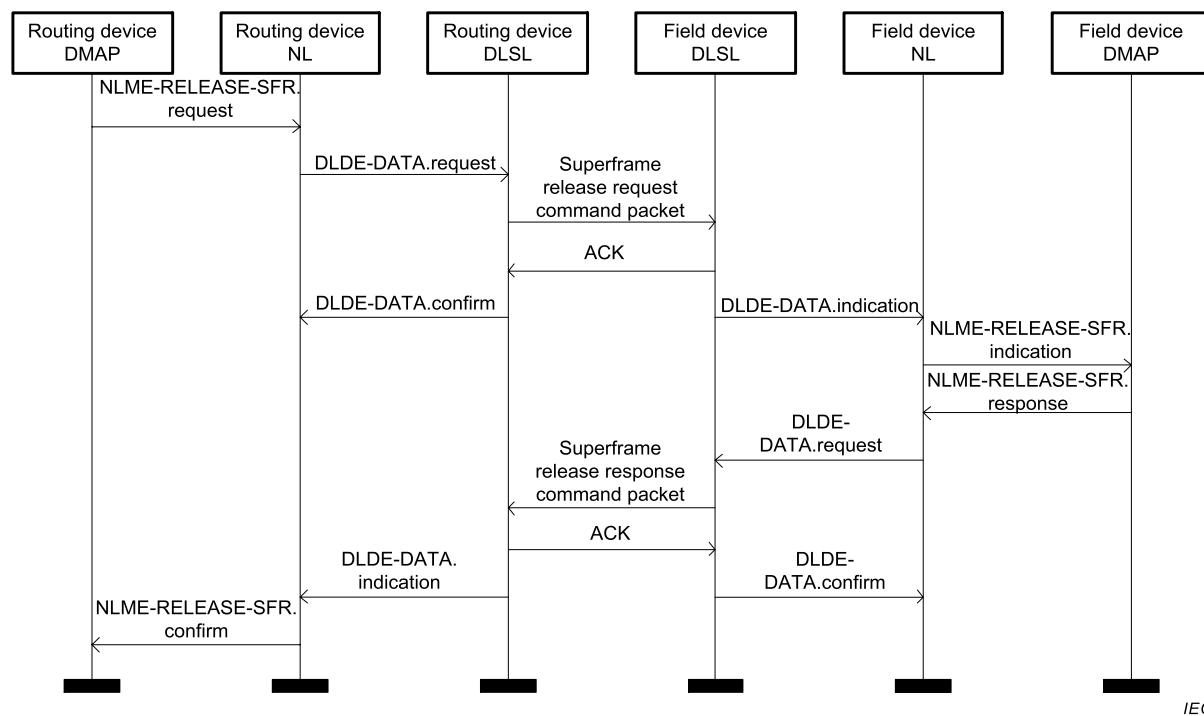


Figure 65 – Releasing a superframe originating from routing device to field device

9.5.9 Aggregation and disaggregation services

9.5.9.1 NLME-AGG.indication

NLME-AGG.indication is used for the NL to report to the DMAP that the received packets need to be aggregated.

The semantics of NLME-AGG.indication are described as follows:

```
NLME-AGG.indication (
    SrcAddr,
    NwkPayload
)
```

Table 108 specifies the parameters for NLME-AGG.indication.

Table 108 – NLME-AGG.indication parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	ID of the aggregation VCR
NwkPayload	Octetstring		Payload of NL

9.5.9.2 NLME-AGO-SEND.request

NLME-AGO-SEND.request is used by the DMAP asking the NL to send the aggregated packet after the aggregation is completed.

The semantics of NLME-AGO-SEND.request are described as follows:

```
NLME-AGO-SEND.request (
    GatewayAddr,
    AggPacketFlag,
    Priority,
    AggNumber,
    AGGRouteID,
    PSFlag,
    AggPayload
)
```

Table 109 specifies the parameters for NLME-AGO-SEND.request.

Table 109 – NLME-AGO-SEND.request parameters

Name	Data type	Valid range	Description
GatewayAddr	Unsigned16	0 to 65 535	Network address of the gateway device
AggPacketFlag	Unsigned8	0, 1	Indicating whether this packet is a data packet or aggregation packet: 0 = Data packet; 1 = Aggregation packet.
Priority	Unsigned8	0 to 15	Priority of process data
AggNumber	Unsigned8	0 to 255	Number of aggregated packets
AGGRouteID	Unsigned16	0 to 65 535	RouteID of the aggregation
PSFlag	Unsigned8	0, 1	Indicating whether this packet is P/S type: 0 = Not P/S type; 1 = P/S type.
AggPayload	Octetstring		DMAP aggregated packet

9.5.9.3 NLME-DAG.indication

NLME-DAG.indication is used to send the aggregated packet to the DMAP for disaggregating when the NL receives an aggregated packet.

The semantics of NLME-DAG.indication are described as follows:

```
NLME-DAG.indication (
    AggNumber,
    NwkPayload
)
```

Table 110 specifies the parameters for NLME-DAG.indication.

Table 110 – NLME-DAG.indication parameter

Name	Data type	Valid range	Description
AggNumber	Unsigned8	0 to 255	Number of aggregated packets
NwkPayload	Octetstring		Payload of NL

9.5.10 Device status report services

9.5.10.1 NLME-DEVICE-STATUS.request

NLME-DEVICE-STATUS.request is used to report the device status either to the routing devices by a field device or to the gateway device by a routing device.

The semantics of NLME-DEVICE -STATUS.request are described as follows:

```
NLME-CHANNEL-DEVICE.request(
    DstAddr,
    DeviceCount,
    DeviceConditionInfo
)
```

Table 111 specifies the parameters for NLME-DEVICE -STATUS.request.

Table 111 – NLME-DEVICE -STATUS.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	Destination address
DeviceCount	Unsigned8	0 to 255	Total number of reported devices
DeviceConditionInfo	DevConRep_Struct structure (see Table 22)		Information of device condition attributes

9.5.10.2 NLME-DEVICE-STATUS.indication

NLME-DEVICE-STATUS.indication is used to report the receipt of a device condition report command packet to the DMAP.

The semantics of NLME-DEVICE -STATUS.indication are described as follows:

```
NLME- DEVICE -STATUS.indication (
    SrcAddr,
    DeviceCount,
    DeviceConditionInfo
)
```

Table 112 specifies the parameters for NLME-DEVICE -STATUS.indication.

Table 112 – NLME-DEVICE -STATUS.indication parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	Source address
DeviceCount	Unsigned8	0 to 255	Total number of reported devices
DeviceConditionInfo	DevConRep_Struct structure (see Table 22)		Information of device condition attributes

9.5.10.3 NLME-DEVICE-STATUS.confirm

NLME-DEVICE-STATUS.confirm is used to return the results of NLME-DEVICE-STATUS.request.

The semantics of NLME-DEVICE-STATUS.confirm are described as follows:

NLME- DEVICE -STATUS.confirm (

Status

)

Table 113 specifies the parameters for NLME-DEVICE -STATUS.confirm.

Table 113 – NLME-DEVICE -STATUS.confirm parameter

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Result of the channel condition report request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.10.4 Time sequence for device status reporting

The time sequence diagram for device status information is shown in Figure 66 and Figure 67.

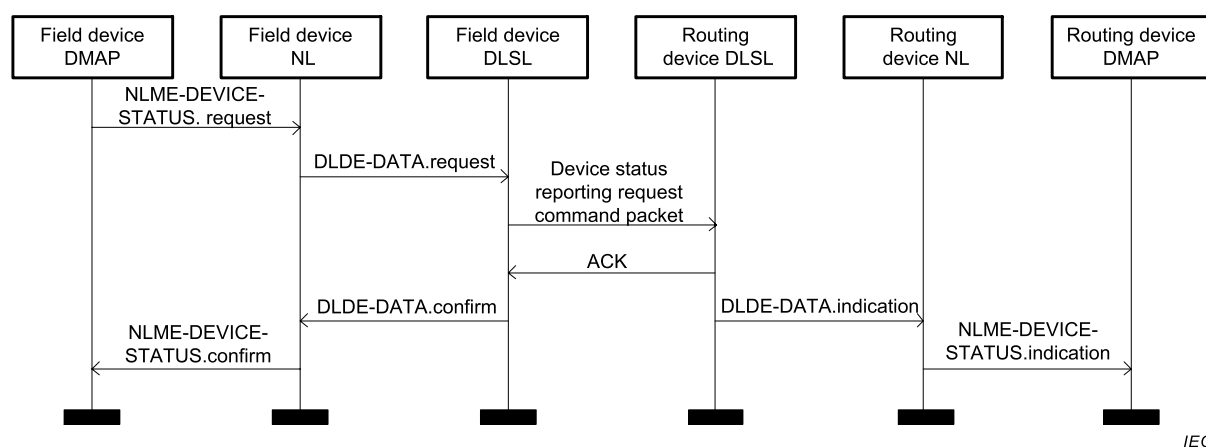
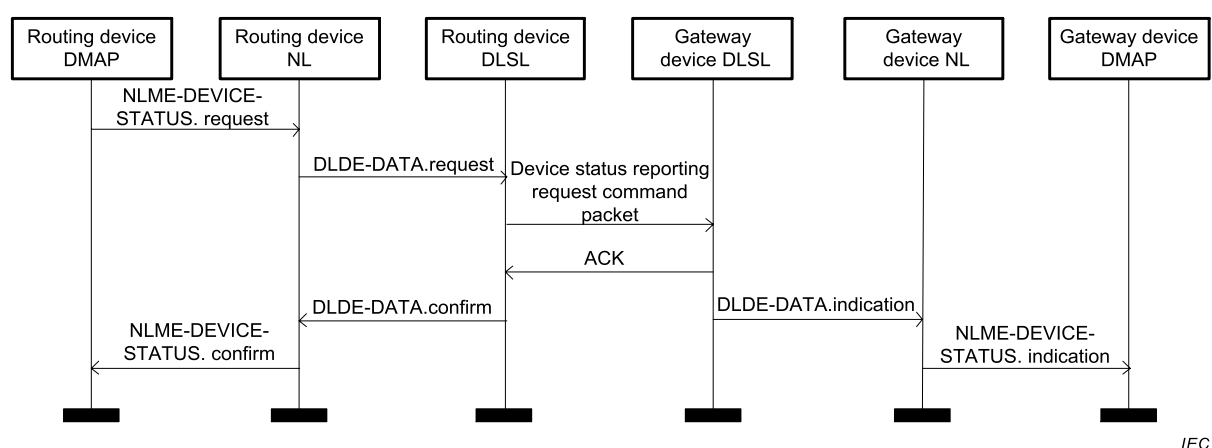


Figure 66 – Device status reporting process from field device to routing device



IEC

Figure 67 – Device status reporting process from routing device to gateway device

9.5.11 Channel condition report services

9.5.11.1 NLME-CHANNEL-CONDITION.request

NLME-CHANNEL-CONDITION.request is used to report the communication channel condition either to the routing device by a field device or to the gateway device by a routing device.

The semantics of NLME-CHANNEL-CONDITION.request are described as follows:

```

NLME-CHANNEL-CONDITION.request(
    DstAddr,
    ChannelCount,
    ChannelConditionInfo
)
  
```

Table 114 specifies the parameters for NLME-CHANNEL-CONDITION.request.

Table 114 – NLME-CHANNEL-CONDITION.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	Destination address
ChannelCount	Unsigned8	0 to 255	Total number of channels
ChannelConditionInfo	ChanCon_Struct structure (See Table 19)		Information of channel condition attributes

9.5.11.2 NLME-CHANNEL-CONDITION.indication

NLME-CHANNEL-CONDITION.indication is used to report the receipt of a channel condition report command packet to the DMAP.

The semantics of NLME-CHANNEL-CONDITION.indication are described as follows:

```

NLME-CHANNEL-CONDITION.indication (
    SrcAddr,
    ChannelCount,
    ChannelConditionInfo
)
  
```

Table 115 specifies the parameters for NLME-CHANNEL-CONDITION.indication.

Table 115 – NLME-CHANNEL-CONDITION.indication parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	Source address
ChannelCount	Unsigned8	0 to 255	Total number of channels
ChannelConditionInfo	ChanCon_Struct structure (see Table 19)		Information of channel condition attributes

9.5.11.3 NLME-CHANNEL-CONDITION.confirm

NLME-CHANNEL-CONDITION.confirm is used to return the results of NLME-CHANNEL-CONDITION.request.

The semantics of NLME-CHANNEL-CONDITION.confirm are described as follows:

NLME-CHANNEL-CONDITION.confirm (

Status

)

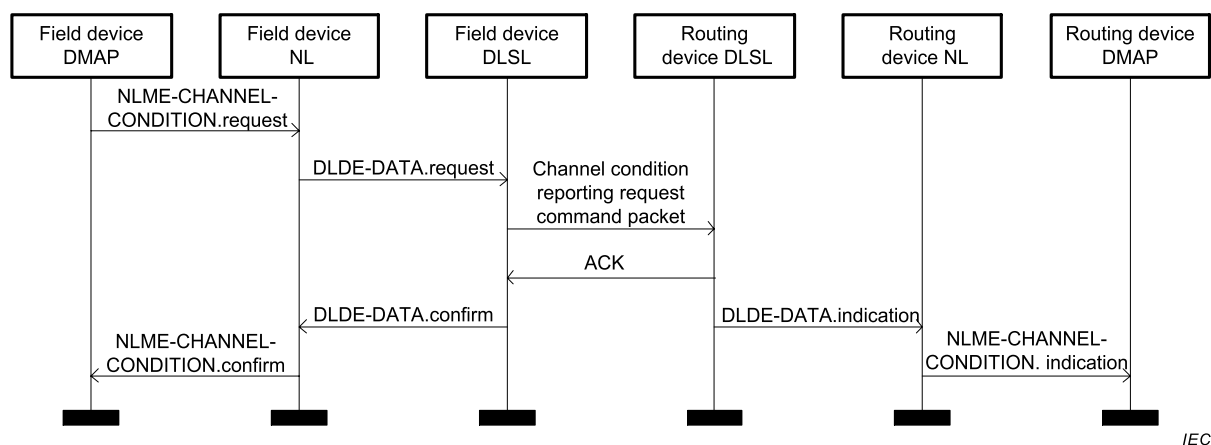
Table 116 specifies the parameters for NLME-CHANNEL-CONDITION.confirm.

Table 116 – NLME-CHANNEL-CONDITION.confirm parameter

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	Result of the channel condition report request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

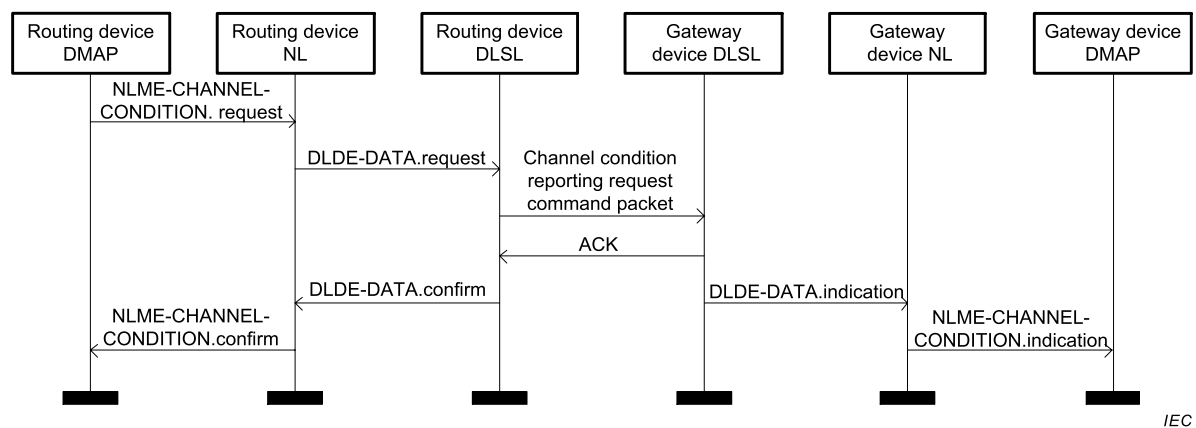
9.5.11.4 Time sequence for channel condition reporting

The time sequence diagram for channel condition information is shown in Figure 68 and Figure 69.



IEC

Figure 68 – Channel condition reporting process from field device to routing device



IEC

Figure 69 – Channel condition reporting process from routing device to gateway device

9.5.12 Failure path report services

9.5.12.1 General

All routing devices on a path record the value of RetryCounter (see Table 69) with next hop routing device. If RetryCounter value of the source routing device or an intermediate routing device exceeds the value of MaxEtoERetry, the source routing device reports the failure of related RouteID to the GW by using the redundant path and the intermediate reports the failure of related RouteID to the GW by using its pre-configured path (see 6.5.1 for redundant path).

9.5.12.2 NLME-PATH_FAILURE.request

NLME-PATH_FAILURE.request is used to report failed paths to the GW by routing devices.

The semantics of NLME-PATH_FAILURE.request are described as follows:

```

NLME-PATH_FAILURE.request (
    SrcAddr,
    DstAddr,
    RouteID
)
  
```

Table 117 specifies the parameters for NLME-PATH_FAILURE.request.

Table 117 – NLME-PATH_FAILURE.request parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	16-bit source address of packets
DstAddr	Unsigned16	0 to 65 535	16-bit destination address of packets
RouteID	Unsigned16	0 to 65 535	Route ID of failing path

9.5.12.3 NLME-PATH_FAILURE.indication

NLME-PATH_FAILURE.indication is used by the NL to report to the DMAP that the device has successfully received a failed-path reporting request packet.

The semantics of NLME-PATH_FAILURE.indication are described as follows:

```

NLME-PATH_FAILURE.indication (
    SrcAddr,
    RouteID
)
  
```

Table 118 specifies the parameters for NLME-LEAVE.response.

Table 118 – NLME-PATH_FAILURE.indication parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	16-bit source address of packets
RouteID	Unsigned16	0 to 65 535	Route ID of failing path

9.5.12.4 NLME-PATH_FAILURE.confirm

NLME-PATH_FAILURE.confirm is used to return the results of NLME-PATH_FAILURE.request.

The semantics of NLME-PATH_FAILURE.confirm are described as follows:

NLME-PATH_FAILURE.confirm (
 Status
)

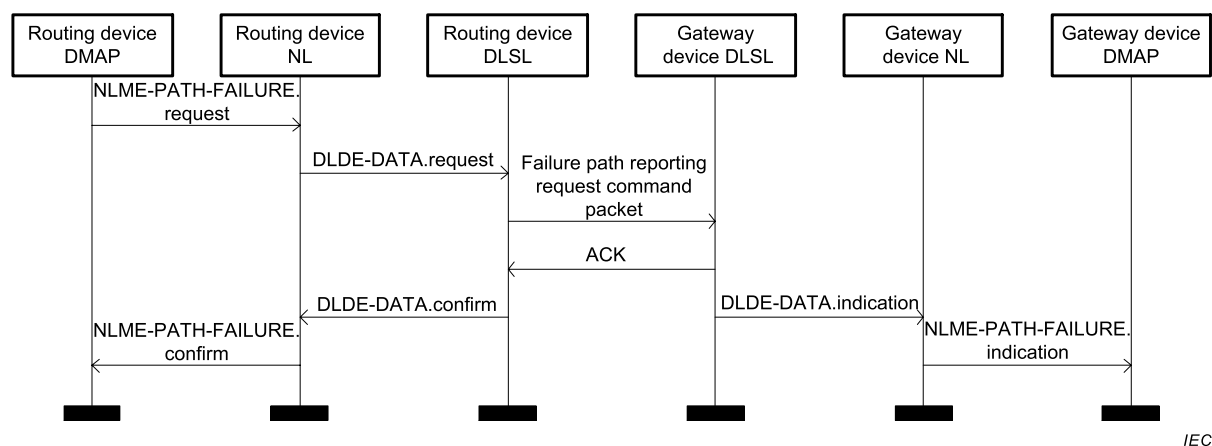
Table 119 specifies the parameters for NLME-PATH_FAILURE.confirm.

Table 119 – NLME-PATH_FAILURE.confirm parameters

Name	Data type	Valid range	Description
Status	Unsigned8	0 to 255	The result of NLME-PATH_FAILURE.request: 0 = SUCCESS; 1 = FAILURE; Others are reserved.

9.5.12.5 Time sequence for failure path reporting

The time sequence diagram for failure path reporting is shown in Figure 70.



IEC

Figure 70 – Failure path reporting process

9.5.13 Network attribute getting services

9.5.13.1 NLME-INFO_GET.request

NLME-INFO_GET.request is used to remotely read the values of the attributes in the MIB.

The semantics of NLME-INFO_GET.request are described as follows:

```
NLME-INFO_GET.request (
    DstAddr,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```

Table 120 specifies the parameters for NLME-INFO_GET.request.

Table 120 – NLME-INFO_GET.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit short address of destination
AttributeID	Unsigned8	0 to 255	ID of attribute in MIB
AttributeMemID	Unsigned8	0 to 255	The ID of attribute member, which is used to read the structured MIB attributes The value 255 means that all attributes should be read.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to read the structured MIB attributes
Count	Unsigned8	0 to 255	Number of attribute values or attributes member values, which is used to read the structured MIB attributes; getting all attribute values from FirstValueStorIndex if Count = 0.

9.5.13.2 NLME-INFO_GET.indication

NLME-INFO_GET.indication is used to inform the DMAP of the successful receipt of an attribute getting request packet.

The semantics of NLME-INFO_GET.indication are described as follows:

```
NLME-INFO_GET.indication (
    SrcAddr,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```

Table 121 specifies the parameters for NLME-INFO_GET.indication.

Table 121 – NLME-INFO_GET.indication parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	16-bit short address of source
AttributeID	Unsigned8	0 to 255	The ID of attribute in MIB
AttributeMemID	Unsigned8	0 to 255	The ID of attribute member, which is used to read the structured MIB attributes The value 255 means that all attributes should be read.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to read the structured MIB attributes
Count	Unsigned8	0 to 255	Number of attribute values or attributes member values, which is used to read the structured MIB attributes; all attribute values from FirstValueStorIndex if Count = 0.

9.5.13.3 NLME-INFO_GET.response

NLME-INFO_GET.response is used to respond to NLME-INFO_GET.request.

The semantics of NLME-INFO_GET.response are described as follows:

NLME-INFO_GET.response (

DstAddr,
Status,
AttributeID,
AttributeMemID,
FirstValueStorIndex,
Count,
AttributeValue

)

Table 122 specifies the parameters for NLME-INFO_GET.response.

Table 122 – NLME-INFO_GET.response parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit short address of the destination
Status	Unsigned8	0 to 255	Result of the attribute read request: 0 = SUCCESS; 1 = UNSUPPORTED_ATTRIBUTE; 2 = UNSUPPORTED_ATTRIBUTE_MEMBER; 3 = UNMATCHED_COUNT; Others are reserved.
AttributeID	Unsigned8	0 to 255	ID of attribute in MIB
AttributeMemID	Unsigned8	0 to 255	ID of attribute member, which is used to read the structured MIB attributes. The value 255 means that all attributes should be read.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to read the structured MIB attributes
Count	Unsigned8	0 to 255	Number of attribute values or attributes member values, which is used to read the structured MIB attributes; all attribute values from FirstValueStorIndex if Count = 0.
AttributeValue	Octetstring		Value of the attribute to be read

If the operation of getting attributes is successful, the Status should be SUCCESS; if the MIB does not have the needed attributes or attribute members, the Status should be UNSUPPORTED_ATTRIBUTE or UNSUPPORTED_ATTRIBUTE_MEMBER; otherwise, if the number of attributes does not equal to the required number, the Status should be UNMATCHED_COUNT.

9.5.13.4 NLME-INFO_GET.confirm

NLME-INFO_GET.confirm is used to return the result of NLME-INFO_GET.request.

The semantics of NLME-INFO_GET.confirm are described as follows:

```

NLME-INFO_GET.confirm (
    SrcAddr,
    Status,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count,
    AttributeValue
)

```

Table 123 specifies the parameters for NLME-INFO_GET.confirm.

Table 123 – NLME-INFO_GET.confirm parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	16-bit short address of the source
Status	Unsigned8	0 to 255	Result of the attribute read request: 0 = SUCCESS; 1 = UNSUPPORTED_ATTRIBUTE; 2 = UNSUPPORTED_ATTRIBUTE_MEMBER; 3 = UNMATCHED_COUNT; Others are reserved.
AttributeID	Unsigned8	0 to 255	ID of attribute in MIB
AttributeMemID	Unsigned8	0 to 255	ID of attribute member, which is used to read the structured MIB attributes The value 255 means that all attributes should be read.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to read the structured MIB attributes
Count	Unsigned8	0 to 255	Number of attribute values or attributes member values, which is used to read the structured MIB attributes; all attribute values from FirstValueStorIndex if Count = 0.
AttributeValue	Octetstring		Value of the attribute to be read

9.5.14 Network attribute setting services

9.5.14.1 NLME-INFO_SET.request

NLME-INFO_SET.request is used by GW to remotely modify the MIB attribute values of routing devices or field devices.

The semantics of NLME-INFO_SET.request are described as follows:

```
NLME-INFO_SET.request (
    DstAddr,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count,
    AttributeValue
)
```

Table 124 specifies the parameters for NLME-INFO_SET.request.

Table 124 – NLME-INFO_SET.request parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit short address of the destination
AttributeID	Unsigned8	0 to 255	ID of attribute in MIB
AttributeMemID	Unsigned8	0 to 255	The ID of attribute member, which is used to write the structured MIB attributes The value 255 means that all attributes should be written
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to write the structured MIB attributes
Count	Unsigned8	0 to 255	Number of attribute values or attributes member values, which is used to read the structured MIB attributes
AttributeValue	Octetstring		Value of the attribute to be written

9.5.14.2 NLME-INFO_SET.indication

NLME-INFO_SET.indication is used to inform the DMAP of the successful receipt of an attribute setting request command packet.

The semantics of NLME-INFO_SET.indication are described as follows:

NLME-INFO_SET.indication (

SrcAddr,
AttributeID,
AttributeMemID,
FirstValueStorIndex,
Count,
AttributeValue

)

Table 125 specifies the parameters for NLME-INFO_SET.indication.

Table 125 – NLME-INFO_SET.indication parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	16-bit short address of the source
AttributeID	Unsigned8	0 to 255	ID of attribute in MIB
AttributeMemID	Unsigned8	0 to 255	ID of attribute member, which is used to write the structured MIB attributes. The value 255 means that all attributes should be written.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to write the structured MIB attributes
Count	Unsigned8	0 to 255	Number of attribute values or attributes member values, which is used to read the structured MIB attributes
AttributeValue	Octetstring		Value of the attribute to be written

9.5.14.3 NLME-INFO_SET.response

NLME-INFO_SET.response is used to respond to NLME-INFO_SET.indication.

The semantics of NLME-INFO_SET.response are described as follows:

```
NLME-INFO_SET.response (
    DstAddr,
    Status,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```

Table 126 specifies the parameters for NLME-INFO_SET.response.

Table 126 – NLME-SET.response parameters

Name	Data type	Valid range	Description
DstAddr	Unsigned16	0 to 65 535	16-bit short address of the destination
Status	Unsigned8	0 to 255	Result of the attribute setting request: 0 = SUCCESS; 1 = UNSUPPORTED_ATTRIBUTE; 2 = UNSUPPORTED_ATTRIBUTE_MEMBER; 3 = UNMATCHED_COUNT; Others are reserved.
AttributeMemID	Unsigned8	0 to 255	ID of attribute member, which is used to write the structured MIB attributes. The value 255 means that all attributes should be written.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to write the structured MIB attributes
AttributeValue	Octetstring		Value of the attribute to be written

If the operation of setting attributes is successful, the Status should be SUCCESS; if the MIB does not have the needed attributes or attribute members, the Status should be UNSUPPORTED_ATTRIBUTE or UNSUPPORTED_ATTRIBUTE_MEMBER; otherwise, if the number of attributes does not equal to the required number, the Status should be UNMATCHED_COUNT.

9.5.14.4 NLME-INFO_SET.confirm

NLME-INFO_SET.confirm is used to return the results of NLME-INFO_SET.request.

The semantics of NLME-INFO_SET.confirm are described as follows:

```
NLME-INFO_SET.confirm (
    SrcAddr,
    Status,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```


Table 127 specifies the parameters for NLME-INFO_SET.confirm.

Table 127 – NLME-SET.confirm parameters

Name	Data type	Valid range	Description
SrcAddr	Unsigned16	0 to 65 535	16-bit short address of the source
Status	Unsigned8	0 to 255	Result of the attribute setting request: 0 = SUCCESS; 1 = UNSUPPORTED_ATTRIBUTE; 2 = UNSUPPORTED_ATTRIBUTE_MEMBER; 3 = UNMATCHED_COUNT; Others are reserved.
AttributeMemID	Unsigned8	0 to 255	ID of attribute member, which is used to write the structured MIB attributes. The value 255 means that all attributes should be written.
FirstValueStorIndex	Unsigned16	0 to 65 535	The first storage index of multiple attribute values, which is used to write the structured MIB attributes
AttributeValue	Octetstring		Value of the attribute to be written

9.6 Network layer packet formats

9.6.1 Common packet format

The NL packet format is shown in Table 128.

Table 128 – Network layer common packet format

	Network layer common packet format										
	Network layer header										Network layer payload
Length in octet(s)	1	2	2	2	4	1	1	0/1	0/1	1	Variable length
Field name	Control	Destination address	Source address	Route-ID	Time-stamp	Priority	Sequence Number	Number of fragments	Fragment sequence number	Payload length	Network layer payload
		Routing									

The control field format is shown in Table 129.

Table 129 – Control field format

Control field format					
Length in bit(s)	2	1	1	1	4
Subfield name	Packet type	Fragment flag	P/S flag	Authentication flag	Reserved

The NL header field has the following subfields:

a) Control subfield, which includes:

- Packet type: this subfield has 2-bit length; the value 0 indicates a data packet, 1 indicates an aggregation packet, 2 indicates a command packet, and others are reserved;
- Fragment flag: this subfield has 1-bit length and is used to indicate whether this packet is a fragment packet; the value 0 indicates no fragment and 1 indicates fragment;

- P/S flag: this subfield has 1-bit length, which is used to indicate whether the data in this packet is P/S type; the value 0 indicates non P/S type and 1 indicates P/S type;
 - Reserved: this subfield has 4-bit length and is used for extension.
- b) Routing field, which includes:
- Destination address: final destination address of a packet (16 bits);
 - Source address: the address from which a packet originates (16 bits);
 - RouteID: unique identifier of the path (16 bits);
- c) Timestamp: this subfield has 4-octet length and is labelled in seconds;
- d) Priority: this subfield has 1-octet length and indicates the priority of a packet;
- e) Sequence number: this subfield has 1-octet length and indicates the sequence number of the NL packet;
- f) Number of fragments: this subfield has 0- or 1-octet length; it is used to indicate the number of fragments; if the packet is a fragment packet, this subfield has 1-octet length and its value is valid; otherwise, this subfield is 0-octet length.
- g) Fragment sequence number: the fragment sequence number subfield is used to indicate the fragment sequence of the fragmentation packet. If the packet is a fragmentation packet, this field has 1-octet length and is valid; otherwise, this field is invalid.
- h) Payload length: this field has 1-octet length and is used to indicate the length of the NL payload;
- i) Network layer payload: this field has variable length and is used to fill in the NL data.

9.6.2 Data packet format

The data packet format is shown in Table 130.

Table 130 – Network layer data packet format

	Network layer common packet format										
	Network layer header										Network layer payload
Length in octet(s)	1	2	2	2	4	1	1	0/1	0/1	1	Variable length
Field name	Control field	Destination address	Source address	RouteID	Time-stamp	Priority	Sequence Number	Number of fragments	Fragment sequence number	Payload length	Network layer payload
		Routing field									

The value of packet type in control field of Network layer header = 0, which indicates a data packet.

The definitions of all the subfields are the same as those in Table 128.

9.6.3 Aggregated packet format

The aggregated packet format is described in Table 131.

Table 131 – Aggregated packet format

	Aggregated packet format								
	Network layer header	Network layer payload							
Length in octet(s)	14/16	1	2	1	Variable length	...	2	1	Variable length
Field name	Network layer header	Aggregated number	Source address 1	Data length1	Data1	...	Source address n	Data length n	Data n
			The first aggregated data			...	The n th aggregated data		

The value of packet type in control field of Network layer header = 1, which indicates an aggregation packet.

The aggregated packet has the following fields or subfields:

- a) Network layer header: the definition of the network layer header is the same as in Table 127;
- b) Aggregated number: this subfield is used to record the number of packets that are aggregated;
- c) First aggregated data: this subfield is used to fill in the first aggregated data, which includes:
 - Source address 1: this field has 2-octet length and indicates the 16-bit address of the first aggregated data;
 - Data length 1: this field has 1-octet length, which is used to fill in the length of the first aggregated data;
 - Data 1: this field has variable length and is used to fill in the first aggregated data.
- d) nth aggregated data: this subfield is used to fill in the nth aggregated data, which is the same as the first aggregated data.

9.6.4 Command packet format

9.6.4.1 Common format of command packet

The NL command packets encapsulate the NL commands to accomplish some management functions. The format of the command packet is shown in Table 132.

Table 132 – Format of NL command packet

	Network layer common packet format										
	Network layer header										Network layer payload
Length in octet(s)	1	2	2	2	4	1	1	0/1	0/1	1	Variable length
Field name	Control field	Destination address	Source address	Router ID	Time-stamp	Priority	Sequence Number	Number of fragment	Fragment sequence number	Payload length	Network layer payload
		Routing field									

The value of packet type in control field of Network layer header = 2, which indicates a command packet.

The data packet has the following fields or subfields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) The network layer payload field includes the following subfields:
 - Command packet identifier: this subfield has 1-octet length and is used to indicate the identifier of the NL command packet (see Table 133);
 - Command packet payload: this subfield has variable length and is used to fill in the payload of the NL command packet.

The NL command packets are listed in Table 133.

Table 133 – Network layer command packet

Command packet identifier	Command	User
0	Joining request	Routing device
1	Joining response	Gateway device
2	Communication status report request	Routing device
3	Leaving request	Routing device/ Gateway device
4	Leaving response	Gateway device/ Routing device
5	Cluster member report request	Routing device
6	Cluster member report response	Gateway device
7	Neighbour information report request	Routing device
8	Routeadding request	Gateway device
9	Routeadding response	Routing device
10	Routeupdate request	Gateway device
11	Route update response	Routing device
12	Route deleting request	Gateway device
13	Route deleting response	Routing device
14	Link adding request	Gateway device/ Routing device
15	Link adding response	Routing device / Field device
16	Link update request	Gateway device/ Routing device
17	Link update response	Routing device / Field device
18	Link release request	Gateway device/ Routing device
19	Link release response	Routing device / Field device
20	Superframe adding request	Gateway device/ Routing device
21	Superframe adding response	Routing device / Field device

Command packet identifier	Command	User
22	Superframe update request	Gateway device/ Routing device
23	Superframe update response	Routing device / Field device
24	Superframe release request	Gateway device/ Routing device
25	Superframe release response	Routing device / Field device
26	Device condition report request	Field device/Routing device
27	Channel status report request	Field device/Routing device
28	Failure path report request	Routing device
29	Attribute getting request	Gateway device/ Routing device
30	Attribute getting response	Routing device / Field device
31	Attribute setting request	Gateway device/ Routing device
32	Attribute setting response	Routing device / Field device
33 to 255	Reserved	Reserved

The execution results of command are shown in Table 134.

Table 134 – Execution results of commands

Command implementing result	Identifier	Description
SUCCESS	0	Command execution succeeds.
FAILURE	1	Command execution fails.

9.6.4.2 Joining request and response

The joining request packet is used by a routing device to forward the joining request. The format of the joining request packet is shown in Table 135.

Table 135 – Format of joining request packet

	Format of joining request packet				
Length in octet(s)	14/16	1	8	0/4	1
Field name	Network layer header	Command ID = 0	Physical address of the new device	Security material	Device type

The joining request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 0;
- Physical address of the new device: this field is used to indicate the 64-bit physical address of the device that is joining the network;
- Security material: this field has 0- or 4-octet length; if the authentication flag in the NL header is 0, the Security material is 0-octet long; otherwise, it is 4-octet long (see Clause 11 for the detailed information);
- Device type: this field has 1-octet length and is used to indicate the type of the joining device. The value 0 indicates the gateway device, 1 indicates a routing device, 2 indicates a field device, and 3 indicates a handheld device; otherwise, this field is reserved.

The joining response packet is used to return the joining request result. The format of the joining response packet is shown in Table 136.

Table 136 – Format of joining response packet

	Format of joining response packet				
Length in octet(s)	14/16	1	1	8	2
Field name	Network layer header	Command ID = 1	Execution result	Physical address of the new device	Short address of the new device

The joining response packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 1;
- Execution result: this field has 1-octet length. The value 0 indicates that the joining process is SUCCESS; otherwise, 1 indicates that the joining process is FAILURE (see Table 134);
- Physical address of the new device: this field is used to indicate the 64-bit physical address of the device that is joining the network;
- Short address of the new device: this field has 2-octet length. If the value of the Execution result field is 0, this field is valid and the value is the newly allocated 16-bit short address for the joining device; otherwise, this field is invalid.

9.6.4.3 Communication status report request

The communication status report request packet is used by a routing device to forward the communication status report request. The format of the communication status report request packet is shown in Table 137.

Table 137 – Format of communication status report request packet

	Format of communication status report request packet				
Length in octet(s)	14/16	1	8	1	1
Field name	Network layer header	Command ID = 2	Physical address of the new device	Device type	Status

The communication status report request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 2;
- Physical address of the new device: this field is used to indicate the 64-bit physical address of the device that has just joined the network;
- Device type: this field has 1-octet length and is used to indicate the type of newly joined device. The value 0 indicates the gateway device, 1 indicates a routing device, 2 indicates a field device, and 3 indicates a handheld device; otherwise, this field is reserved;
- Status: this field has 1-octet length and is used to indicate the result of the joining process; the value 0 indicates that the joining process is successful and 1 indicates that the joining process fails.

9.6.4.4 Leaving request and response

The leaving request packet is used either by a routing device to request departure from the gateway device or by the gateway device to request a routing device to leave the network. The format of the leaving request packet is shown in Table 138.

Table 138 – Format of leaving request packet

	Format of leaving request packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 3	Leaving reason

The leaving request packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 3;
- c) Leaving reason: this field is 1 octet, the valid value of which is shown in Table 139.

Table 139 – Value of Leaving reason

Value	Description
0	Reserved
1	Passive leaving of a routing device or a field device
2	Active leaving of a routing device
3 to 255	Reserved

The leaving response packet is used to return the execution results. The format of the leaving response packet is shown in Table 140.

Table 140 – Format of leaving response packet

	Format of leaving response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 4	Execution result

The leaving response packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 4;
- c) Execution result: this field has 1-octet length and indicates the result of the departure process. If the departure process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.5 Cluster member report request and response

The cluster member report request packet is used by routing devices to report cluster member information to the gateway device. The format of the cluster member report request packet is described in Table 141.

Table 141 – Format of cluster member report request packet

	Format of cluster member report request packet			
Length in octet(s)	14/16	1	1	2
Field name	Network layer header	Command ID = 5	Cluster member modification flag	Cluster member address

The cluster member report request packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 5;
- c) Cluster member modification flag: this field has 1-octet length and indicates the kinds of modification; the value 0 indicates the adding action, and 1 indicates the deleting action; otherwise, this field is reserved;
- d) Cluster member address: this field has 2-octet length and indicates the 16-bit address of the modified cluster member.

The cluster member report response packet is used to return the execution results of the cluster member report request command. The format of the cluster member report response packet is described in Table 142.

Table 142 – Format of cluster member report response packet

	Format of cluster member report response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 6	Execution result

The cluster member report response packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 6;
- c) Execution result: this field has 1-octet length and indicates the result of the cluster member report process. If the report process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.6 Neighbour information report request

The neighbour information report request packet is used by routing devices to report its one-hop neighbour information to the NM. The format of the neighbour information report request packet is described in Table 143.

Table 143 – Format of neighbour information report request packet

	Format of neighbour information report request packet			
Length in octet(s)	14/16	1	1	Variable length
Field name	Network layer header	Command ID = 7	Number of neighbours	Items of neighbour table

The neighbour information report request packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 7;
- c) Number of neighbours: this field has 1-octet length and indicates the number of reported neighbours;
- d) Items of neighbour table: this field has variable length; the structure of neighbour table item is shown in Table 15.

9.6.4.7 Route adding request and response

The route adding request packet is generated by the NM, and is sent to the destination routing device for adding a new routing record into its routing table.

The format of the route adding request packet is illustrated in Table 144.

Table 144 – Format of route adding request packet

	Format of route adding request packet		
Length in octet(s)	14/16	1	9
Field name	Network layer header	Command ID = 8	A record of routing table

The route adding request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 8;
- A record of routing table: this field has 9-octet length; the detailed information is shown in Table 15.

The route adding response packet is used to return the execution results of the route adding request command.

The format of the route adding response packet is illustrated in Table 145.

Table 145 – Format of route adding response packet

	Format of route adding response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 9	Execution result

The route adding response packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 9;
- Execution result: this field has 1-octet length and indicates the results of the route adding response process. If the response process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.8 Route update request and response

The route update request packet is generated by the NM, and is sent to the destination routing device for modifying a routing table record in its routing table.

The format of the route update request packet is illustrated in Table 146.

Table 146 – Format of route update request packet

	Format of route update request packet		
Length in octet(s)	14/16	1	9
Field name	Network layer header	Command ID = 10	A record of routing table

The route update request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 10;

- c) A record of routing table: this field has 9-octet length; the detailed information is shown in Table 15.

The route update response packet is used to return the execution results of the route update request command.

The format of the route update response packet is illustrated in Table 147.

Table 147 – Format of route update response packet

	Format of route update response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 11	Execution result

The route update response packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 11;
- Execution result: this field has 1-octet length and indicates the result of the route update response process. If the response process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.9 Route deleting request and response

The route deleting request packet is generated by the NM, and is sent to the destination routing device for deleting a routing record from its routing table.

The format of the route deleting request packet is illustrated in Table 148.

Table 148 – Format of route deleting request packet

	Format of route update request packet		
Length in octet(s)	14/16	1	2
Field name	Network layer header	Command ID = 12	Route ID

The route update request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 12;
- Route ID: this field has 2-octet length and indicates the identifier of the deleted route.

The route deleting response packet is used to return the execution result of the Route deleting request command.

The format of the route deleting response packet is illustrated as Table 149.

Table 149 – Format of route deleting response packet

	Format of route update response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 13	Execution result

The route deleting response packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 13;
- c) Execution result: this field has 1-octet length and indicates the result of the route deleting response process. If the response process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.10 Link adding request and response

The link adding request packet is used by the NM to add one or more new link(s) to a routing device, and is also used by the routing device to add one or more new link(s) to a field device. After receiving this command packet, the routing device or field device should add a record to its link table.

The format of the link adding request packet is shown in Table 150.

Table 150 – Format of link adding request packet

	Format of link adding request packet					
Length in octet(s)	14/16	1	2	12	...	12
Field name	Network layer header	Command ID = 14	Number of links	Link table item 1	...	Link table item N

The link adding request packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 14;
- c) Number of links: this field has 2-octet length and indicates the number of added links;
- d) Link table item 1 to N (N = Number of links): each of these link table items has 12-octet length, which indicates the detailed information of the added link. The structure of the link table item is shown in Table 17.

The link adding response packet is used to return the execution results of link adding. The format of the link adding response packet is shown in Table 151.

Table 151 – Format of link adding response packet

	Format of link adding response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 15	Execution result

The link adding response packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 15;
- c) Execution result: this field has 1-octet length and indicates the result of the link adding response process. If the response process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.11 Link update request and response

The link update request packet is used by the NM to update one or more existing link(s) of a routing device, and is also used by the routing device to update one or more existing link(s) to a field device. After receiving this command packet, the routing device or field device should update a record in its link table.

The format of the link update request packet is shown in Table 152.

Table 152 – Format of link update request packet

	Format of link update request packet					
Length in octet(s)	14/16	1	2	12	...	12
Field name	Network layer header	Command ID = 16	Number of links	Link table item 1	...	Link table item N

The link update request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 16;
- Number of links: this field has 2-octet length and indicates the number of updated links;
- Link table item 1 to N (N = Number of links): each of these link table items has 12-octet length, which indicates the detailed information of the updated links. The structure of the link table item is shown in Table 17.

The link update response packet is used to return the execution results of link update. The format of the link update response packet is shown in Table 153.

Table 153 – Format of link update response packet

	Format of route update response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 17	Execution result

The link update response packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 17;
- Execution result: this field has 1-octet length and indicates the result of the link update response process. If the response process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.12 Link release request and response

The link release request packet is used by the NM to release one or more existing link(s) to a routing device, and is also used by the routing device to release one or more existing link(s) to a field device. After receiving this command packet, the routing device or field device should release a record in its link table.

The format of the link release request packet is shown in Table 154.

Table 154 – Format of link release request packet

	Format of link release request packet					
Length in octet(s)	14/16	1	1	2	...	2
Field name	Network layer header	Command ID = 18	Number of links	Link ID 1	...	Link ID N

The link release request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 18;
- Number of links: this field has 2-octet length and indicates the number of released links;
- Link ID 1 to N of link table (N = Number of links): each Link ID has 2-octet length, which indicates the identifiers of the released links.

The link release response packet is used to return the execution results of link release. The format of the link release response packet is shown in Table 155.

Table 155 – Format of link release response packet

	Format of link release response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 19	Execution result

The link release response packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 19;
- Execution result: this field has 1-octet length and indicates the result of the link release response process. If the response process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.13 Superframe adding request and response

The superframe adding request packet is used by the NM to add a new superframe to a routing device, and is also used by the routing device to add a new superframe to a field device. After receiving this command packet, the routing device or field device should add a record in its superframe table.

The format of the superframe adding request packet is shown in Table 156.

Table 156 – Format of superframe adding request packet

	Format of superframe adding request packet		
Length in octet(s)	14/16	1	12
Field name	Network layer header	Command ID = 20	Superframe table item

The superframe adding request packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 20;
- c) Superframe table item: this field has 12-octet length and indicates the detailed information of the added superframe (see Table 16).

The superframe adding response packet is used to return the execution results of superframe adding. The format of the superframe adding response packet is shown in Table 157.

Table 157 – Format of superframe adding response packet

	Format of superframe adding response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 21	Execution result

The superframe adding response packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 21;
- c) Execution result: this field has 1-octet length and indicates the result of the superframe adding response process. If the response process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.14 Superframe update request and response

The superframe update request packet is used by the NM to update an existing superframe to a routing device, and is also used by the routing device to update an existing superframe to a field device. After receiving this command packet, the routing device or field device should update a record in its superframe table.

The format of the superframe update request packet is shown in Table 158.

Table 158 – Format of superframe update request packet

	Format of superframe update request packet		
Length in octet(s)	14/16	1	12
Field name	Network layer header	Command ID = 22	Superframe table item

The superframe update request packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 22;
- c) Superframe table item: this field has 12-octet length and indicates the detailed information of the updated superframe (see Table 16).

The superframe update response packet is used to return the execution results of superframe update. The format of the superframe update response packet is shown in Table 159.

Table 159 – Format of superframe update response packet

	Format of superframe update response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 23	Execution result

The superframe update response packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 23;
- Execution result: this field has 1-octet length and indicates the result of the superframe update response process. If the response process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.15 Superframe release request and response

The superframe release request command frame is used by the NM to release an existing superframe to a routing device, and is also used by the routing device to release an existing superframe to a field device. After receiving this command packet, the routing device or field device should release a record in its superframe table.

The format of the superframe release request packet is shown in Table 160.

Table 160 – Format of superframe release request packet

	Format of superframe release request packet		
Length in octet(s)	14/16	1	2
Field name	Network layer header	Command ID = 24	Superframe ID

The superframe release request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 24;
- Superframe ID: this field has 2-octet length and indicates the identifier of the superframe to be the released (see Table 16).

The superframe release response packet is used to return the execution results of superframe release. The format of the superframe release response packet is shown in Table 161.

Table 161 – Format of superframe release response packet

	Format of superframe release response packet		
Length in octet(s)	14/16	1	1
Field name	Network layer header	Command ID = 25	Execution result

The superframe release response packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 25;
- Execution result: this field has 1-octet length and indicates the result of the superframe release response process. If the response process is successful, the value of this field is 0; otherwise, the value of this field is 1 (see Table 134).

9.6.4.16 Device condition report request

The device condition report request packet is used to report the conditions of the devices remotely. The format of the device condition report request packet is described in Table 162.

Table 162 – Format of device condition report request packet

	Format of device condition report request packet			
Length in octet(s)	14/16	1	1	Variable length
Field name	Network layer header	Command ID = 26	Number of devices	Items of device condition information

The device condition report request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 26;
- Number of devices: this field has 1-octet length and indicates the number of reported devices.
- Items of device condition information: the detailed format of the device condition information field is described in Table 163. This field has $N \times 11$ octet length, where N = Number of devices.

Table 163 – Format of device condition information field

	Format of device condition information field						
Length in octet(s)	2	2	2	2	1	2	4
Field name	Device short address	Number of packets transmitted after last report	Number of packets terminated in this device after last report	Number of packets with MAC MIC failure after last report	Battery level	Restart count of device after last report	Uptime

The device condition information field includes the following subfields (see Table 22):

- Device short address: this subfield has 2-octet length and indicates the short address of the reported device;
- Number of packets transmitted after last report: this subfield has 2-octet length and indicates the number of transmitted packets since the last report of the reported device;
- Number of packets terminated in this device after last report: this subfield has 2-octet length and indicates the number of received packets since the last report of the reported device;
- Number of packets with MAC MIC failure after last report: this subfield has 2-octet length and indicates the number of packets with MAC MIC failure since the last report;
- Battery level: this subfield has 1-octet length and indicates the residual power level;
- Restart count of device after last report: this subfield has 2-octet length and indicates the number of restarts since the last report.
- Uptime: this subfield has 4-octet length and indicates the uptime of a device.

9.6.4.17 Channel condition report request

The channel condition report request packet is used to report the quality status of the communication channels remotely. The format of the channel condition report request packet is described in Table 164.

Table 164 – Format of channel condition report request packet

	Format of channel condition report request packet			
Length in octet(s)	14/16	1	1	Variable length
Field name	Network layer header	Command ID = 27	Number of channels	Items of channel quality information

The channel condition report request packet has the following fields:

- Network layer header: the definition of the network layer header is the same as in Table 128;
- Command ID: this field has 1-octet length and the value of it is 27;
- Number of channels: this field has 1-octet length and indicates the number of reported channels;
- Channel quality information: this field has variable length;
- Items of channel quality information: the detailed format of the channel quality information is shown in Table 165. This field has $N \times 5$ octet length, where N = Number of channels.

Table 165 – Format of channel quality information field

	Format of channel quality information field			
Length in octet(s)	1	1	2	1
Field name	Channel index	Link quality	Packet loss rate	Number of retries

The channel quality information field includes the following subfields:

- Channel index: this field has 1-octet length and indicates the sequence number of channels;
- Link quality: this field has 1-octet length and indicates the LQI value of each channels;
- Packet loss rate: this field has 2-octet length and indicates the packet loss rate of each channel;
- Number of retries: this field has 1-octet length and indicates the number of retransmissions of each channel.

9.6.4.18 Path failure report request

The path failure report request packet is used by routing devices to report the failure of a path. The format of the path failure report request packet is described in Table 166.

Table 166 – Format of path failure report request packet

	Format of path failure report request packet		
Length in octet(s)	14/16	1	2
Field name	Network layer header	Command ID = 28	Route ID

The path failure report request packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 28;
- c) Route ID: this field has 1-octet length and indicates the identifier of the reported route.

9.6.4.19 Attribute getting request

The attribute getting request packet is used to ask a specified device to report the attributes of its MIB. The format of the attribute getting request packet is described in Table 167.

Table 167 – Format of attribute getting request packet

	Format of attribute getting request packet					
Length in octet(s)	14/16	1	1	1	2	1
Field name	Network layer header	Command ID = 29	Attribute ID	Attribute member ID	First storage index of multiple attribute values	Number of attributes

The attribute getting request packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 29;
- c) Attribute ID: this field has 1-octet length and indicates the index of the requested attribute;
- d) Attributed member ID: this field has 1-octet length and indicates the index of the requested attribute member;
- e) First storage index of multiple attribute values: this field has 2-octet length and indicates the first storage index of multiple attribute values;
- f) Number of attributes: this field has 1-octet length and indicates either the number of attribute values or the number of attribute member values.

9.6.4.20 Attribute getting response

The attribute getting response packet is used to respond to the attribute getting request, which should return the values of the attributes. The format of the attribute getting response packet is described in Table 168.

Table 168 – Format of attribute getting response packet

	Format of attribute getting response packet							
Length in octet(s)	14/16	1	1	1	1	2	1	Variable length
Field name	Network layer header	Command ID = 30	Status	Attribute ID	Attribute member ID	First storage index of multiple attribute values	Number of attributes	Attribute value

The attribute getting response packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 30;
- c) Status: this field has 1-octet length and indicates the result of the attribute getting; the value 0 indicates the getting process is successful, and 1 indicates that the requested attribute is unsupported; otherwise, this field is reserved (see Table 122);

- d) Attribute ID: this field has 1-octet length and indicates the index of the requested attribute;
- e) Attributed member ID: this field has 1-octet length and indicates the index of the requested attribute member;
- f) First storage index of multiple attribute values: this field has 2-octet length and indicates the first storage index of multiple attribute values;
- g) Number of attributes: this field has 1-octet length and indicates either the number of attribute values or the number of attribute member values.
- h) Attribute values: this field has variable length and indicates the requested attribute values.

9.6.4.21 Attribute setting request

The attribute setting request packet is used to ask a device to add or modify the attribute value in its MIB. The format of the attribute setting request packet is described in Table 169.

Table 169 – Format of attribute setting request packet

	Format of attribute setting request packet						
Length in octet(s)	14/16	1	1	1	2	1	Variable length
Field name	Network layer header	Command ID = 31	Attribute ID	Attribute member ID	First storage index of multiple attribute values	Number of attributes	Attribute value

The attribute setting request packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;
- b) Command ID: this field has 1-octet length and the value of it is 31;
- c) Attribute ID: this field has 1-octet length and indicates the index of the requested attribute;
- d) Attributed member ID: this field has 1-octet length and indicates the index of the requested attribute member;
- e) First storage index of multiple attribute values: this field has 2-octet length and indicates the first storage index of multiple attribute values;
- f) Number of attributes: this field has 1-octet length and indicates either the number of attribute values or the number of attribute member values.
- g) Attribute values: this field has variable length and indicates the attribute values to be set.

9.6.4.22 Attribute setting response

The attribute setting response packet is used to respond to the attribute setting request. The format of the attribute setting response packet is described in Table 170.

Table 170 – Format of attribute setting response packet

	Format of attribute setting response packet						
Length in octet(s)	14/16	1	1	1	1	2	1
Field name	Network layer header	Command ID = 32	Status	Attribute ID	Attribute member ID	First storage index of multiple attribute values	Number of attributes

The attribute setting response packet has the following fields:

- a) Network layer header: the definition of the network layer header is the same as in Table 128;

- b) Command ID: this field has 1-octet length and the value of it is 32;
- c) Status: this field has 1-octet length and indicates the result of the attribute setting; the value 0 indicates the setting process is successful, and 1 indicates that the requested attribute is unsupported; otherwise, this field is reserved (see Table 126);
- d) Attribute ID: this field has 1-octet length and indicates the index of the requested attribute;
- e) Attributed member ID: this field has 1-octet length and indicates the index of the requested attribute member;
- f) First storage index of multiple attribute values: this field has 2-octet length and indicates the first storage index of multiple attribute values;
- g) Number of attributes: this field has 1-octet length and indicates either the number of attribute values or the number of attribute member values.

10 Application layer

10.1 Overview

10.1.1 General

The WIA-PA AL is comprised of UAP and ASL. AL defines application objects that interact with the industrial processes. It also defines communication services that support communications among multiple objects for the distributed industry applications.

The local operations among UAOs are not specified in this document.

10.1.2 AL structure

The AL structure is shown in Figure 71.

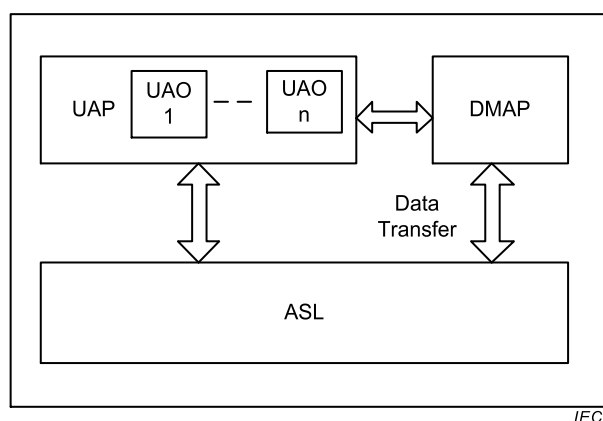


Figure 71 – AL structure

The distributed applications of industrial processes may be implemented by UAPs. A UAP is comprised of one or more UAOs. All UAOs in a device can interact with each other. The UAOs in different devices may interact with each other through the communication services that are provided by AL.

ASL provides transparent services of data transmission: between ASL and UAP.

10.1.3 Functions of UAP

UAP has the following functions:

- a) collecting process data, such as the process data of temperature, pressure, and flow;

- b) processing collected process data, such as conversion, linearization, compensation, and filtration;
- c) computing and generating output data based on the processed data of the device and that of other devices;
- d) controlling the process;
- e) generating and reporting alarm: UAP should report an alarm event, e.g. the process data is beyond the limits, the unexpected state of UAO changes, etc.; and
- f) inter-operating among devices in WIA-PA network.

10.1.4 Functions of ASL

ASL provides data services and management services as follows:

- a) Data transmission services: ASL provides end-to-end transparent data transmission services for UAP, and it supports C/S, P/S, and R/S data transmissions; and
- b) ASL management services are not specified in this document.

10.2 UAP

10.2.1 General

UAP is a unit for processing information for specific applications and is used to implement the distributed applications within WIA-PA network.

A UAP may be constructed as an application process either according to IEC 61499-1 and IEC 61499-2 or IEC 61804-2. A UAP may also be an application process that is defined by users. The implementation of a UAP may be achieved either with function blocks or by other approaches, which is shown in Figure 72.

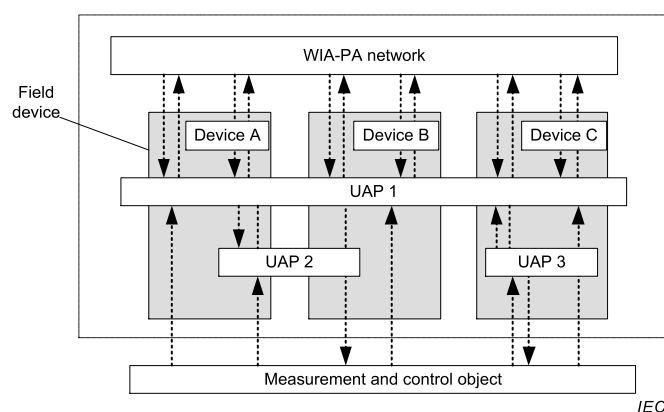


Figure 72 – User application process

A UAP may be composed of several UAOs within one device, which is shown as UAP 3 in Figure 72. A UAP may also be composed of several UAOs locating in different devices, which is shown as UAP 1 and UAP 2 in Figure 72.

10.2.2 UAO

10.2.2.1 General

UAO is defined according to different functions, which may be defined as function blocks by other approaches.

In order to support the interoperability among different devices, each UAO has its own attributes. The attributes of UAO are used to describe application profiles, which the application objects shall follow.

Each UAO shall be identified by object ID and instance ID. If some attributes of the UAO may be operated remotely, they shall be accessed further by the attribute identifier.

10.2.2.2 Functions of UAO

In WIA-PA, UAOs collect and process the data from industrial processes (such as temperature, pressure, and flow) by using different kinds of sensors, and control the process with actuators. The functions of a UAO are described in the following.

a) Range scaling

Range scaling is a linear transformation, which converts the process data from one unit to another unit in order to simplify further measurement and computation. For example, 4 mA ~ 20 mA signals may be converted into 0 Kpa to 10 Kpa signals. Range scaling may also convert the data with units into data without units, such as percentage.

b) Linearization

Sensor characteristics mostly are nonlinear and irregular. Therefore, linearization is necessary for dealing with the sensed data.

c) Compensation

Measured values of sensors may have linear drift due to the environment influence. Therefore, compensation is necessary.

d) Filtering

In industrial process, sensors may be interfered and result in a relatively abrupt jump in the measured values. In order to avoid this situation, filtering is used to eliminate the influence of the jump signals.

e) Storage

Storage involves copying the data to a temporary storage area so that it can be resent if the original data is lost.

f) Engineering unit conversion

Engineering unit conversion involves converting the units of input signals to other units that may be identified by I/O subsystems.

g) Measuring timestamp

The current time is added to the measured data as a timestamp.

UAO is not specified in this document. See Annex C for an example of UAO.

10.2.3 Method definition

10.2.3.1 General

Table 171 specifies the methods that are used to handle parameters of UAOs.

Table 171 – UAO method definition

Method	Method identifier	Scope		Description
		Object	Instance	
READ	request: 0x00	Mandatory	Mandatory	Reading the attributes of UAOs
	response: 0x80	Mandatory	Mandatory	Response of reading the attributes of UAOs
WRITE	request: 0x01	Unsupport	Optional	Writing the attributes of UAOs
	response: 0x81	Unsupport	Optional	Response of writing the attributes of UAOs
PUBLISH	request: 0x02	Unsupport	Optional	Publishing attributes of UAOs
REPORT	request: 0x03	Unsupport	Optional	Reporting alarm and event data
REPORT ACK	request: 0x04	Unsupport	Optional	Alarm acknowledgement

10.2.3.2 READ format

The request format of the READ method is shown in Table 172.

Table 172 – Request format of READ method

	Request format of the READ method		
Length in octet(s)	1	1	1
Field name	Object identifier	Object instance identifier	Object attribute identifier

The request format of the READ method includes the following fields:

- Object identifier: this field has 1-octet length and indicates the identifier of a UAO;
- Object instance identifier: this field has 1-octet length and indicates the identifier of an object instance;
- Object attribute identifier: this field has 1-octet length and indicates the identifier of an object attribute; when the object attribute identifier is 0, all attributes of the instance should be read.

The response format of the READ method is shown in Table 173.

Table 173 – Response format of READ method

	Response format of the READ method				
Length in octet(s)	1	1	1	1	Variable length
Field name	Object identifier	Object instance identifier	Object attribute identifier	Data length	Data

The response format of the READ method includes the following fields:

- Object identifier: this field has 1-octet length and indicates the identifier of a UAO;
- Object instance identifier: this field has 1-octet length and indicates the identifier of an object instance;
- Object attribute identifier: this field has 1-octet length and indicates the identifier of an object attribute; if value the object attribute identifier is 0, all attributes of the instance should be read;
- Data length: this field has 1-octet length and indicates the data length of the object attribute; the value 0 of Data length indicates the read operation fails.

- e) Data: this field has variable length, which indicates the data of the object attribute. If the value of Data length is 0, this field shall be ignored.

10.2.3.3 WRITE format

The request format of the WRITE method is shown in Table 174.

Table 174 – Request format of WRITE method

	Request format of the WRITE method				
Length in octet(s)	1	1	1	1	Variable length
Field name	Object identifier	Object instance identifier	Object attribute identifier	Data length	Data

The request format of the WRITE method includes the following fields:

- Object identifier: this field has 1-octet length and indicates the identifier of a UAO;
- Object instance identifier: this field has 1-octet length and indicates the identifier of an object instance;
- Object attribute identifier: this field has 1-octet length and indicates the identifier of an object attribute; when the value object attribute identifier is 0, all attributes of the instance should be written.
- Data length: this field has 1-octet length and indicates the data length of the object attribute;
- Data: this field has variable length, which indicates the data of the object attribute.

The response format of the WRITE method is shown in Table 175.

Table 175 – Response format of WRITE method

	Response format of the WRITE method			
Length in octet(s)	1	1	1	1
Field name	Object identifier	Object instance identifier	Object attribute identifier	Status

The response format of the WRITE method includes the following fields:

- Object identifier: this field has 1-octet length and indicates the identifier of a UAO;
- Object instance identifier: this field has 1-octet length and indicates the identifier of an object instance;
- Object attribute identifier: this field has 1-octet length and indicates the identifier of an object attribute;
- Status: this field has 1-octet length and indicates the result of the WRITE operation; the value 0 indicates the process is successful and 1 indicates that the process fails.

10.2.3.4 PUBLISH format

The format of the PUBLISH method is shown in Table 176.

Table 176 – Format of PUBLISH method

	Format of the PUBLISH method				
Length in octet(s)	1	1	1	1	Variable length
Field name	Object identifier	Object instance identifier	Object attribute identifier	Data length	Data

The format of the PUBLISH method includes the following fields:

- Object identifier: this field has 1-octet length and indicates the identifier of a UAO;
- Object instance identifier: this field has 1-octet length and indicates the identifier of an object instance;
- Object attribute identifier: this field has 1-octet length and indicates the identifier of an object attribute; when the object attribute identifier is 0, all attributes of the instance should be published.
- Data length: this field has 1-octet length and indicates the data length of the published object attribute;
- Data: this field has variable length and indicates the data of the published object attribute.

10.2.3.5 REPORT format

The format of the REPORT method is shown in Table 177.

Table 177 – Format of REPORT method

	Format of the REPORT method				
Length in octet(s)	1	1	1	1	Variable length
Field name	Object identifier	Object instance identifier	Object attribute identifier	Data length	Data

The format of the REPORT method includes the following fields:

- Object identifier: this field has 1-octet length and indicates the identifier of a UAO;
- Object instance identifier: this field has 1-octet length and indicates the identifier of an object instance;
- Object attribute identifier: this field has 1-octet length and indicates the identifier of an object attribute; when the object attribute identifier is 0, all attributes of the instance should be reported.
- Data length: this field has 1-octet length and indicates the data length of the reported object attribute;
- Data: this field has variable length and indicates the data of the reported object attribute.

10.2.3.6 REPORT ACK format

The format of the REPORT ACK method is shown in Table 178.

Table 178 – Format of REPORT ACK method

	Format of REPORT ACK method			
Length in octet(s)	1	1	1	1
Field name	Object identifier	Object instance identifier	Object attribute identifier	Status

The format of the REPORT ACK method includes the following fields:

- a) Object identifier: this field has 1-octet length and indicates the identifier of a UAO;
- b) Object instance identifier: this field has 1-octet length and indicates the identifier of an object instance;
- c) Object attribute identifier: this field has 1-octet length and indicates the identifier of the reported object attribute;
- d) Status: this field has 1-octet length and indicates the result of the REPORT process; the value 0 indicates to clear the alarm event and 1 indicates to keep the alarm event.

10.3 Application sub-layer

10.3.1 General

ASL provides data communication services among UAOs in the WIA-PA network.

10.3.2 Application sub-layer data entity

10.3.2.1 General

ASL defines the ASLDE, which provides transparent interfaces for sending and receiving data between ASL and NL. ASLDE supports the transport of APDU between UAOs.

The ASL supports three communication modes: C/S mode, P/S mode, and R/S mode:

- a) C/S mode supports unicast transmission of dynamic and aperiodic data;
- b) P/S mode supports unicast and multicast transmission of the periodic data;
- c) R/S mode supports unicast and multicast transmission of aperiodic data, such as alarms, alerts or events.

These communication modes are supported by corresponding types of VCRs.

The AL data services should be supported by three primitives: ASLDE-DATA.request, ASLDE-DATA.confirm, and ASLDE-DATA.indication.

10.3.2.2 ASLDE-DATA.request

The upper layer sends data to the ASL by using the ASLDE-DATA.request primitive.

The semantics of this primitive are as follows:

```
ASLDE-DATA.request (
    VcrID,
    Priority,
    MethodIdentifier
    AsduLength,
    Asdu
)
```

Table 179 specifies the parameters of the ASLDE-DATA.request primitive.

Table 179 – ASLDE-DATA.request parameters

Name	Data type	Valid range	Description
VcrID	Unsigned16	0 to 65 535	VCR used for the transmission
Priority	Unsigned8	0 to 255	Priority of UAO data
MethodIdentifier	Unsigned8	0 to 255	The identifier of method (see Table 171)
AsduLength	Unsigned16	0 to 65 535	Number of octets consisting the ASDU to be transferred
Asdu	Octetstring		Set of octets comprising the ASDU to be transferred

When ASL receives a data request from the upper layer, it should encapsulate the ASDU according to the ASL packet format and send it to NL. After transporting the data, the ASL should issue ASLDE-DATA.confirm to the upper layer with the Status parameter set to the status value returned by the NL.

10.3.2.3 ASLDE-DATA.confirm

The ASLDE-DATA.confirm primitive is invoked to indicate the transmission result. When the data is transferred successfully, the Status parameter in this primitive should be set to SUCCESS. Otherwise, the Status parameter should be set to corresponding error code to indicate the reason for the failure.

The semantics of this primitive are as follows:

```
ASLDE-DATA.confirm (
    VcrID,
    Status
)
```

Table 180 specifies the parameters for the ASLDE-DATA.confirm primitive.

Table 180 – ASLDE-DATA.confirm parameters

Name	Data type	Valid range	Description
VcrID	Unsigned16	0 to 65 535	VCR unique identifier used for this transmission
Status	Unsigned8	0 to 255	The status of the corresponding request: 0 = SUCCESS; 1 = INVALID_ADDRESS; 2 = FAIL; Others are reserved.

10.3.2.4 ASLDE-DATA.indication

After receiving packets from the NL, the ASL transfers the user data to the upper layer by using the ASLDE-DATA.indication primitive; the upper layer then performs the corresponding operation and processes the user data according to different service types.

The semantics of this primitive are as follows:

```
ASLDE-DATA.indication(
    MethodIdentifier,
    Priority,
    AsduLength,
    Asdu
)
```

Table 181 specifies the parameters for the ASLDE-DATA.indication primitive.

Table 181 – ASLDE-DATA.indication parameters

Name	Data type	Valid range	Description
MethodIdentifier	Unsigned8	0 to 255	The identifier of method (see Table 171)
Priority	Unsigned8	0 to 255	Priority of packet
AsduLength	Unsigned16	0 to 65 535	Number of octets comprising the ASDU received
Asdu	Octetstring		Set of octets comprising the ASDU received

10.3.2.5 ASLDE-AGG.request

The ASLDE-AGG.request primitive is invoked by the DMAP to request the ASL to send the aggregated packet.

The semantics of this primitive are as follows:

```
ASLDE-AGG.request(
    VcrID,
    SrcAddr,
    GatewayAddr,
    Priority,
    AggPacketFlag,
    AggRouteID,
    AggPayload
)
```

Table 182 specifies the parameters for the ASLDE-AGG.request primitive.

Table 182 – ASLDE-AGG.request parameters

Name	Data type	Valid range	Description
VcrID	Unsigned16	0 to 65 535	VCR unique identifier used for this transmission
SrcAddr	Unsigned16	0 to 65 535	Network address of source
GatewayAddr	Unsigned16	0 to 65 535	Network address of gateway device
Priority	Unsigned8	0 to 255	Priority of process data
AggPacketFlag	Unsigned8	0 to 255	Indicating whether this packet is a data packet or aggregation packet: 0 = Data packet; 1 = Aggregation packet.
AggRouteID	Unsigned16	0 to 65 535	Route identifier for aggregation data
AggPayload	Octetstring		DMAP aggregated packet

10.3.2.6 ASLDE-DAG.indication

The ASLDE-DAG.indication primitive is invoked by the ASL to instruct the DMAP to disaggregate the packet.

The semantics of this primitive are as follows:

```
ASLDE-DAG.indication (
    AggPayload
)
```


resources to the device according to this attribute. In Subscriber, the corresponding VCRs have attributes including the address information of the Publisher data and the Subscriber UAOs, respectively. The published data should be transferred to the corresponding UAOs.

The P/S communication process is shown in Figure 74 and Figure 75. Figure 74 shows the P/S communication process when the devices disable the aggregation function. Figure 75 shows the P/S communication process when the devices enable the aggregation function.

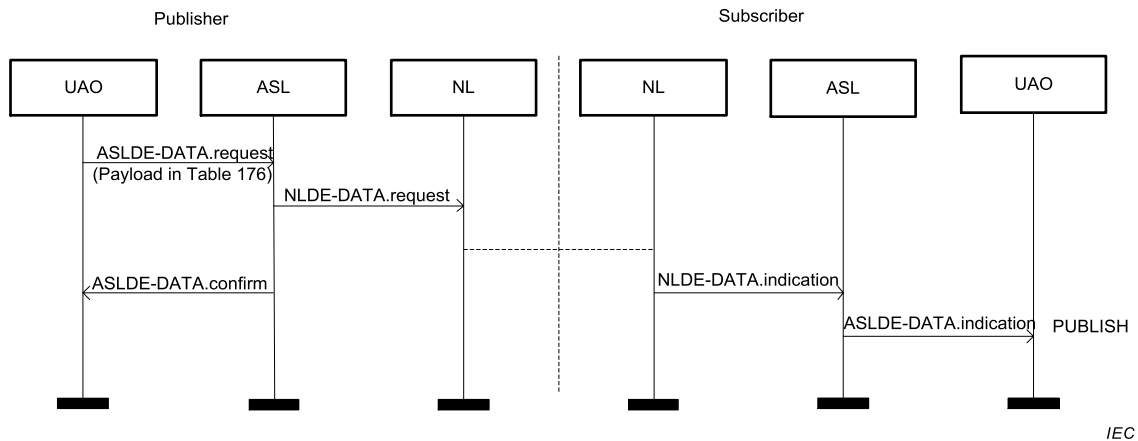


Figure 74 – P/S communication process (disable aggregation function)

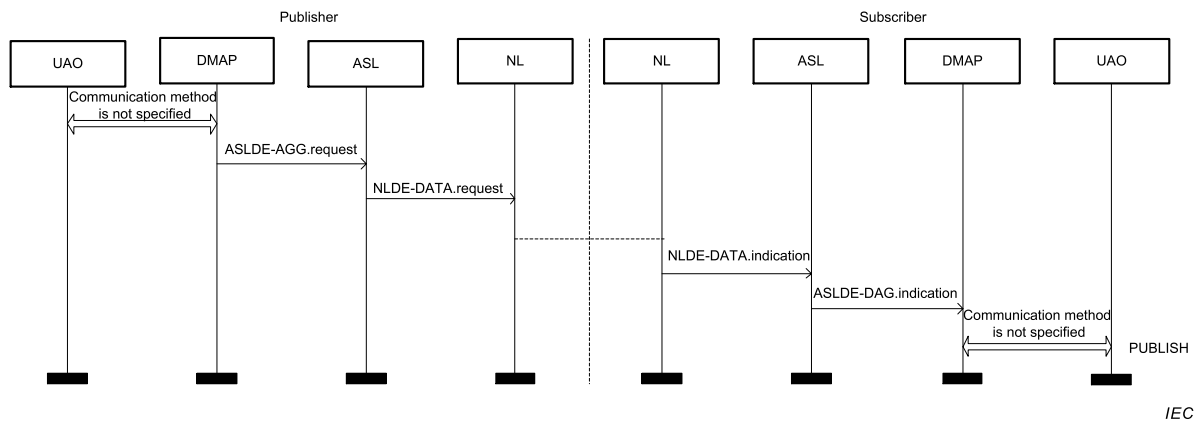


Figure 75 – P/S communication process (enable aggregation function)

10.3.2.7.4 Report source/Sink communication mode

The ASL provides the R/S mode to support the aperiodic alarm or event reports and to report the acknowledgement of the UAOs. The R/S mode is supported by the R/S VCRs.

In the R/S mode, the UAO should send the alarm or event produced by it through an allocated R/S VCR. In Report/Sink, the alarm or event received should be transferred to the corresponding UAOs.

The R/S communication process is shown in Figure 76.

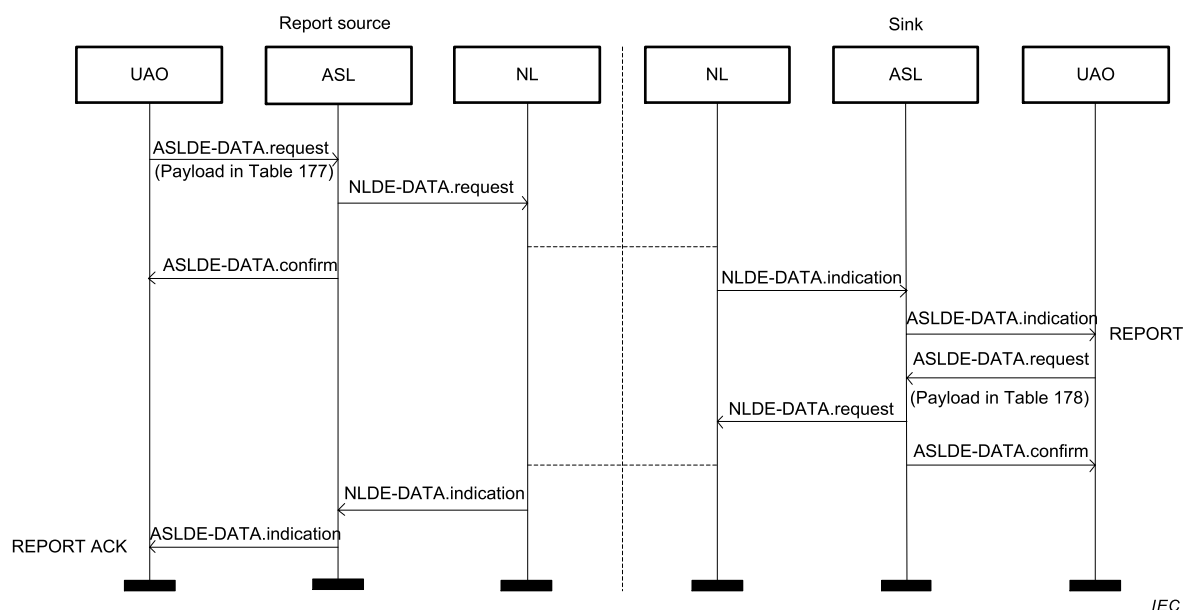


Figure 76 – R/S communication process

10.4 Application sub-layer packet formats

10.4.1 General

This part specifies the application sub-layer packet formats. Each application sub-layer packet includes the following two parts:

- Application sub-layer packet header (ASL Header), which includes the packet control field, sequence number, method identifier, and payload length;
- Application sub-layer packet payload (ASL Payload), whose length is variable.

10.4.2 ASL general packet format

10.4.2.1 General

The format of the ASL general packet is shown in Table 184.

Table 184 – Application sub-layer general packet format

	Format of ASL general packet				
	ASL header				ASL payload
Length in octet(s)	1	1	1	2	Variable length
Field name	Packet control	Sequence Number	Method identifier	Payload length	Payload

The ASL general packet includes the following fields or subfields:

- ASL packet head, which includes the following subfields:
 - Packet control: this subfield has 1-octet length and is described in Table 185;
 - Sequence number: this subfield has 1-octet length and indicates the sequence number of the ASL packet;
 - Method identifier: this subfield has 1-octet length and indicates the identifier of the method (see 10.2.3);

- Payload length: this subfield has 2-octet length and indicates the length of the ASL payload;

b) ASL payload: this subfield has variable length and is used to fill in the ASL data.

10.4.2.2 ASL packet control field

10.4.2.2.1 General

The length of the packet control field is 8-bit. The format of the packet control field is shown in Table 185.

Table 185 – Packet control field format

	Packet control field format			
Length in bit(s)	2	1	1	4
Subfield name	Packet type	Security	ACK	Reserved

The packet control field includes the packet type, security, ACK, and reserved subfields, which should be described in the following sections.

10.4.2.2.2 Packet type subfield

The length of the packet type subfield is 2-bit. Its value is shown in Table 186.

Table 186 – Packet type subfield value

Packet type value b0b1	Packet type name
00	Data
01	Reserved
10	Acknowledgement
11	Aggregated packet

10.4.2.2.3 Security subfield

The length of the security subfield is 1 bit. The security subfield is used to control whether the AL uses the security function when transmitting the data. If the security subfield (namely b2) is set to 0, it indicates that the AL does not use security operation; if b2 is 1, it indicates that the AL uses the security operation to encrypt the data payload part of the application packet.

10.4.2.2.4 Acknowledgement subfield

The length of the acknowledgement subfield is 1 bit. It is used to specify whether application packet acknowledgement is needed. If the acknowledgement subfield (namely b3) is set to 0, it indicates that the acknowledgement is not needed; if the value of this bit is set to 1, it indicates that the acknowledgement is needed.

10.4.2.3 Sequence number field

The length of the sequence number field is 1 octet. The ASL should maintain the packet sequence number. If it transmits an AL packet, the sequence number should be increased by one. For the response data packet transmitted in the C/S communication mode, its sequence number is consistent with the corresponding request packet. The sequence number is used to match the request/response and acknowledgement packet. When the sequence number reaches its maximum value, it should be reset to 0.

10.4.2.4 Method identifier field

The length of the method identifier field is 1 octet (see Table 171).

10.4.2.5 Payload length field

The length of the payload length field is 1 octet. This field is used to indicate the length of the ASL payload in octets.

10.4.2.6 ASL payload

The length of the ASL payload is variable.

10.4.3 Packet formats

10.4.3.1 General

Two types of packet formats are defined in the ASL: ASL data packet and ASL acknowledgement packet.

10.4.3.2 ASL data packet

10.4.3.2.1 General

The format of the ASL data packet is shown in Table 187.

Table 187 – ASL data packet format

	ASL data packet format				
	ASL header				ASL payload
Length in octet(s)	1	1	1	2	Variable length
Field name	Packet control (Packet type = 0b00)	Sequence Number	Method identifier	Payload length	Data payload

The ASL header of the data packet includes the packet control, sequence number, method identifier, and payload length subfields. Detailed descriptions of these subfields are listed in 10.4.3.2.2 to 10.4.3.2.3.

10.4.3.2.2 ASL header field of data packet

The ASL header of the data packet includes the packet control field, sequence number field, method identifier, and payload length. The packet type subfield of the packet control field should be set to 0b00 in order to indicate that it is an ASL data packet. Other fields should be set according to the ASLDE-DATA.request of the ASL.

Once the AL transmits an application layer packet, its sequence number should increase by one. The sequence number of the response data packet that transmitted in the C/S communication mode is consistent with the corresponding request data packet.

10.4.3.2.3 ASL payload field

The ASL payload field includes the request data of the upper layer (see 10.3.2).

10.4.3.3 ASL acknowledgement packet

The acknowledgement is used to confirm whether or not the destination device has received the packet. If the acknowledgement is not returned after a certain period (configurable by EtoEACKTimeOut, see 6.9.1.2.1), the source device should retry the previous packet.

For the data packet sent by P/S mode, broadcast packet and acknowledgement packet, the ASL does not need to be acknowledged, and the acknowledgement subfield of the packet control field is set to 0.

The ASL indicates that the current packet needs to be acknowledged by setting the acknowledgement subfield of the packet control field to 1.

After receiving the AL packet that needs to be acknowledged, the local ASL should confirm it by returning an acknowledgement packet. The sequence number of the acknowledgement packet should be the same as that in the corresponding request packet.

The format of the acknowledgement packet is shown in Table 188.

Table 188 – ASL acknowledgement packet format

	ASL acknowledgement packet format			
	ASL header			
Length in octet(s)	1	1	1	2
Field name	Packet control (Packet type = 0b10)	Sequence Number	Method identifier	Payload length

The acknowledgement packet has only the ASL header, which includes the following subfields.

- Packet control: this subfield has 1-octet length and is described in Table 185. The packet type subfield of the packet control field should be set to 0b10 in order to indicate that this packet is an acknowledgement packet. If using security, the security subfield should be set to 1; otherwise, the security subfield should be set to 0.
- Sequence number: this subfield has 1-octet length and indicates the sequence number of the ASL acknowledgement packet; the sequence number subfield should be set to the same sequence number as that of in the corresponding received request packet.
- Method identifier: this subfield has 1-octet length and indicates the identifier of the method (see 10.2.3); the method identifier of the acknowledgement packet is 0b04.
- Payload length: this subfield has 2-octet length and indicates the length of the ASL payload; the payload length of the acknowledgement packet is 0.

11 Security

11.1 General

The security requirements, security principles and security objectives of the WIA-PA network should be analyzed before establishing the security strategies and security measures for the WIA-PA network. See Clauses A.1 to A.3 for the recommendation of the WIA-PA security risk analysis, security principles, and security objectives.

The WIA-PA MAC layer applies the security services defined in the IEEE STD 802.15.4-2011 MAC layer. The WIA-PA upper layers provide the following security services:

- Data integrity. The data integrity check service is provided in the AL and the DLSSL. A source device generates a check code with a check algorithm; the destination device verifies the check code and determines whether the received packet has been compromised.
- Data confidentiality. The data confidentiality service is provided in the AL and the DLSSL. A source device encrypts packets by using a symmetric key algorithm and sends the encrypted packets out. The destination device decrypts the encrypted packets using the same symmetric key algorithm.

- c) Device authentication. The SM uses the security material to authenticate a device. The security material is generated by the Join Key and the long address. It should be irreversible.

The definition of the check algorithm and the symmetric key algorithm are not included in this document.

11.2 Security management framework

Considering the real-time requirement and the limited resources of devices, the WIA-PA network needs different security strategies and measures to be achieved in different layers. The recommendation of the graded and layered measures of the system and the graded measures of the secure packets are defined in Clause A.4. The security management framework of the WIA-PA network is shown in Figure 77.

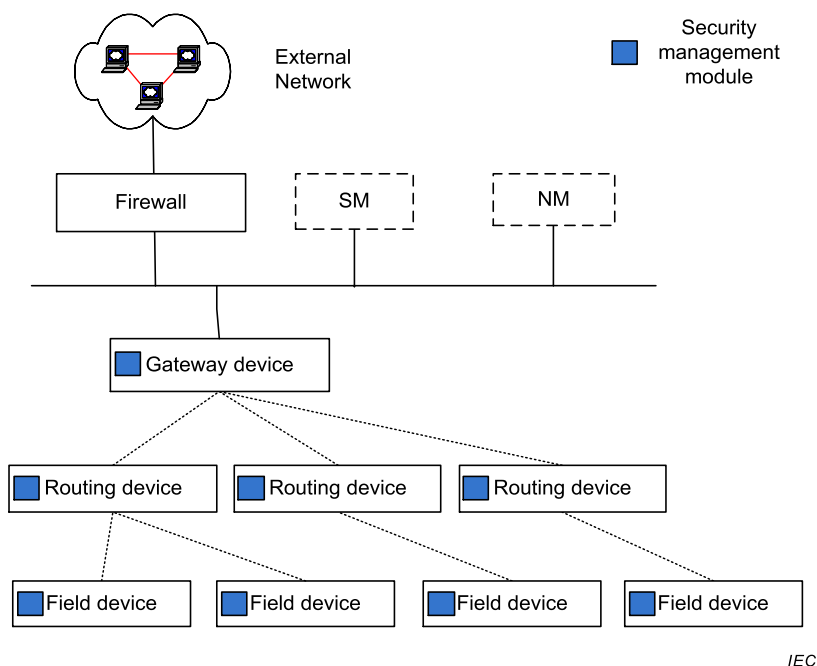


Figure 77 – Security management framework of WIA-PA network

As shown in Figure 77, the security management framework is comprised of an SM and security management modules in the gateway device, routing devices and field devices.

The security management framework interacts with external networks through the firewall. It protects the border of the whole WIA-PA network, and guarantees the normal operations of the WIA-PA network. The firewall is not specified in this document.

The SM should configure the security measures of the WIA-PA network, manage keys, and authenticate devices. It performs the following functions:

- configuring the system security strategies and the security measures of the WIA-PA network according to specific applications;
- configuring and monitoring the gateway device and routing devices according to specific applications and system security strategies;
- authorizing the routing devices and field devices that are attempting to join in the WIA-PA network;
- key management, including key generation, key distribution, key recovery, and key update.

The security management module of gateway device provides the following functions:

- a) managing self security measures;
- b) providing the functions of security management module in the routing devices.

The security management module in the routing device provides the following functions:

- a) managing the keys used by the cluster and forwarding the keys allocated by the SM;
- b) implementing the security measures of data encryption, decryption and data integrity check;
- c) sending authentication request.

The security management module in the field device performs the following functions:

- a) managing security measures of DLSL and ASL;
- b) implementing the security measures of data encryption, decryption and data integrity check;
- c) managing the keys.

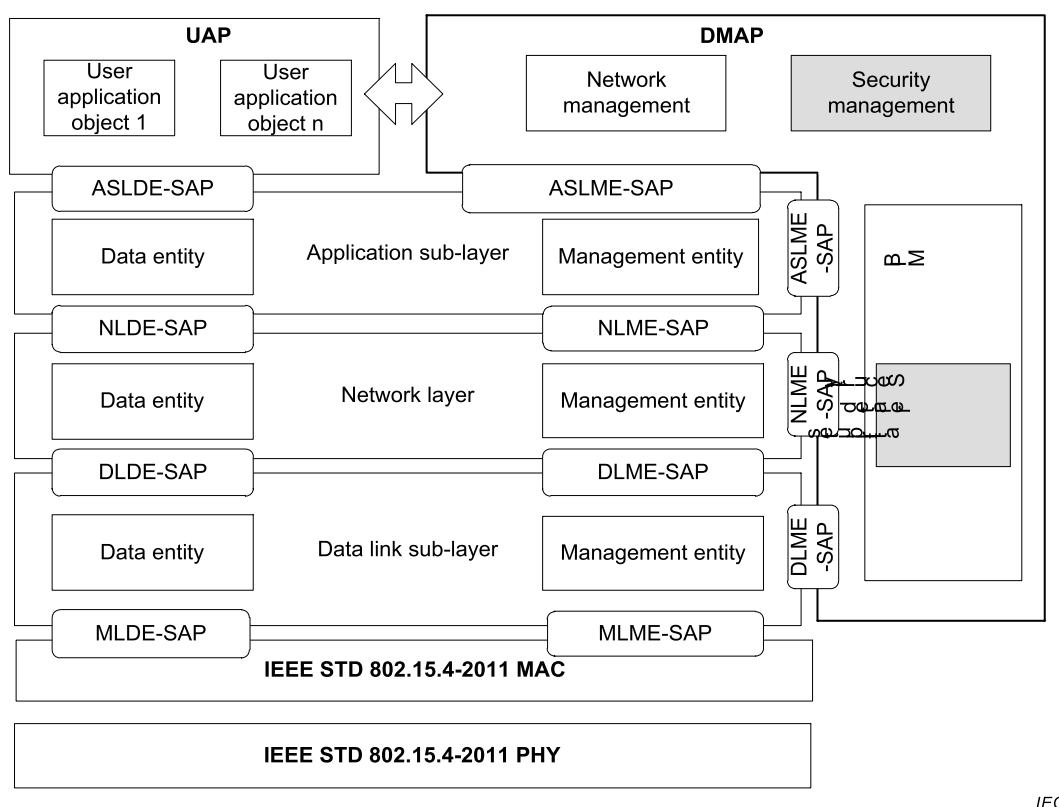
The routing devices and field devices also provide alert reporting function. When the Attacked count reach to MaxAttackedCnt or the KeyAttackCnt reach MaxKeyAttackedCnt, the routing devices/field devices should report Alert to gateway device by using NLME_INFO_SET.

Redundant devices connect with primary devices by wires. The redundant device has the same KJ as the primary device. When security authentication is needed, the primary device uses the long address of the redundant device and the KJ to authenticate the latter.

11.3 Secure communication protocol stack

11.3.1 General

The secure communication protocol stack includes the security measures for each layer. Keys are stored in the MIB (see Table 23). Coordinating with SM, the security management module of the DMAP also provides management and maintenance of keys (see 11.4). DLSL and ASL deal with the secure transportation independently. The secure communication protocol stack is shown in Figure 78, where the grey modules are related to the security. The attributes related to security in MIB are defined as security management information base. The security management module uses the network attribute setting services to set security management information base.



IEC

Figure 78 – Security communication protocol stack

11.3.2 Data link sub-layer security

11.3.2.1 General

The security measures are provided by DLSSL in the WIA-PA network. The security of MAC layer is disabled. DLSSL uses CCM MIC and the data encryption to guarantee point-to-point transportation security, in which the frame counter is replaced by ASN. The MIC is generated with the DLSSL keys and the DLSSL header and DLSSL payload. It is used for message integrity check. The data encryption is used for data confidentiality. Encryption key getting is implemented by network attribute getting services (see 9.5.13).

The security manager can configure or read the key of devices by using NLME_INFO_SET or NLME_INFO_GET services.

11.3.2.2 Data link sub-layer frame security

The format of a security DLPDU is shown in Table 189.

Table 189 – Format of security DLPDU

	Format of security DLPDU			
Length in octet(s)	1	1	Variable length	0/4/8/16
Subfield name	DLSSL frame control	DLSSL security header	DLSSL payload	MIC

If the security enabled subfield in the DLSSL frame control field is set to 1, it should use the DLSSL security header, as shown in Table 190.

Table 190 – Format of DLSL security header

	Format of DLSL security header		
Length in bit(s)	3	2	3
Subfield name	Security control field	Security material control field	Reserved

The size of the security control field is 3 bits, as described in Table 191. The security control field defines the security attributes.

Table 191 – Structure of security control field in DLSL security header

Security control field b2b1b0	Security attributes
000	None
001	MIC-32
010	MIC-64
011	MIC-128
100	ENC
101	ENC-MIC-32
110	ENC-MIC-64
111	ENC-MIC-128

If encryption and MIC check are both provided, the sender calculates MIC firstly and then encrypts the frames. Furthermore, the receiver should decrypt the frames and then check the MIC.

The security material control field defines packet type of the device security material service in Table 192.

Table 192 – Structure of security material control field in DLSL security header

Security material control field b1b0	Security attributes
00	Data packet
01	The device security material getting request packet
10	The device security material getting response packet
11	Reserve

11.3.3 Application sub-layer security

11.3.3.1 General

The ASL security implements end-to-end data transportation security. ASL uses CCM data encryption and MIC to guarantee end-to-end transportation security, in which the frame counter is replaced by ASN. The ASL establishes and maintains the keys in the security management information base. The MIC is generated with the ASL keys and ASL payload. It is used for message integrity check.

11.3.3.2 Application sub-layer packet security

The structure of a security APDU is shown in Table 193.

Table 193 – Security APDU structure

	Security APDU structure			
Length in octet(s)	5	1	Variable length	0/4
Field name	ASL header	ASL security header	ASL payload	MIC

If the security enabled subfield in the packet control of the ASL header is set to 1, it should use the ASL security header, as shown in Table 194.

Table 194 – Structure of ASL security header field

Bits: 0 to 1	2 to 7
00 = NONE 01 = ENC 10 = MIC-32 11 = ENC-MIC-32	Reserved

If encryption and MIC check are both provided, the sender calculates MIC firstly and then encrypts the frames. Furthermore, the receiver should decrypt the frames and then check the MIC.

11.4 Key management

11.4.1 Key type

The SM and the security management modules manage the keys used in the WIA-PA network. The following cryptographic keys are defined.

a) Join Key (KJ)

It is a temporary key used during the device joining. The KJ is established in the provisioning process. It is distributed by the security manager through the handheld devices. It is used to encrypt the 64-bit long address of the new device to produce the security material. After the device successfully joins the network, KJ is also used to protect the KEK when the KEK is distributed for the first time.

b) Share Key (KS)

It is a share key with unified value. The KS is established in the provisioning process. It is distributed by the security manager through the handheld devices. It is used to encrypt beacon and broadcast frame. During the joining process, the NM will return joining result, in the last hop, the KS is used to encrypt the joining response by the online routing device or gateway device,

c) Key Encryption Key (KEK)

KEK is distributed by the SM after a device has joined the WIA-PA network. It is used to encrypt other keys. When the SM distributes the KEK for the first time, the KEK is protected by KJ. After that, the new KEK is protected by the KEK which is used currently in its update period.

d) Data Encryption Key (KED)

KED is distributed by the SM after a device has joined the WIA-PA network, including the DLSL encryption key and the AL encryption key. It is used to protect data and check integrity during data transmission. The KED is protected by the KEK in its distribution and update period.

The key lifecycle is shown in Figure 79.

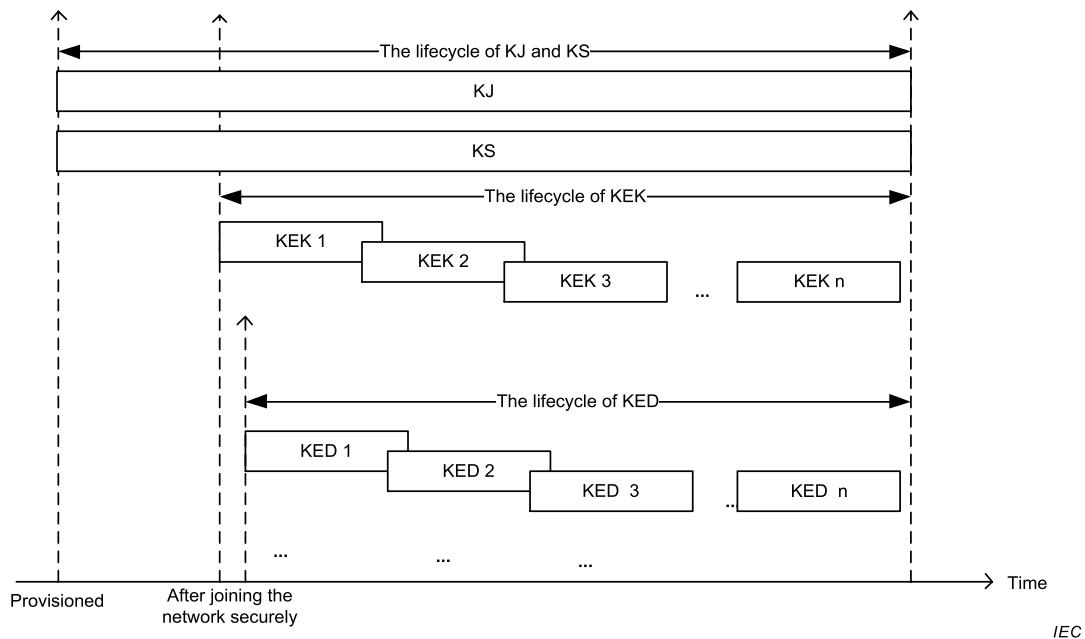


Figure 79 – Key lifecycle

The KEK and the KED need to be updated periodically by SM setting the key-related parameters in the MIB (see Table 23).

11.4.2 Key distribution

Before a device joins the network, the KJ should be distributed to the device. The KJ should be directly distributed by the handheld devices.

After the device has joined the WIA-PA network, KEK and KED should be distributed to the joined devices by SM. The key distribution is implemented by the network attribute setting services (see 9.5.14).

11.4.3 Key update

When the SM needs to update a device key, it should generate a new key. Then the new key is encrypted by the KEK and the encrypted new key is distributed to the WIA-PA device by using network attribute setting services (see 9.5.14).

Upon successful distribution of the new key, the device should decrypt the encrypted new key with its KEK and update its key.

The key update cycle is determined by users according to their requirements, and is recommended to be no more than 24 h in length.

The new key requires the following properties.

- The new key should be different from keys used by other devices in the WIA-PA network.
- The new key should be guaranteed to be the latest.
- The new key should be sent to the related devices in time.

11.4.4 Key status

From its establishment to its abolition, a key should experience the following statuses:

- a) **BACKUP**: this status is defined as when a key has been established but has not been used for normal operation;
- b) **USING**: this status is defined as when a key is being used;
- c) **INVAILD**: this status is defined as when a key is not available.

When the KeyActiveTime (see Table 23) of a key with BACKUP is reached, the key changes its status from BACKUP to USING. At the same time the key in USING status (if it exists) changes to INVAILD status.

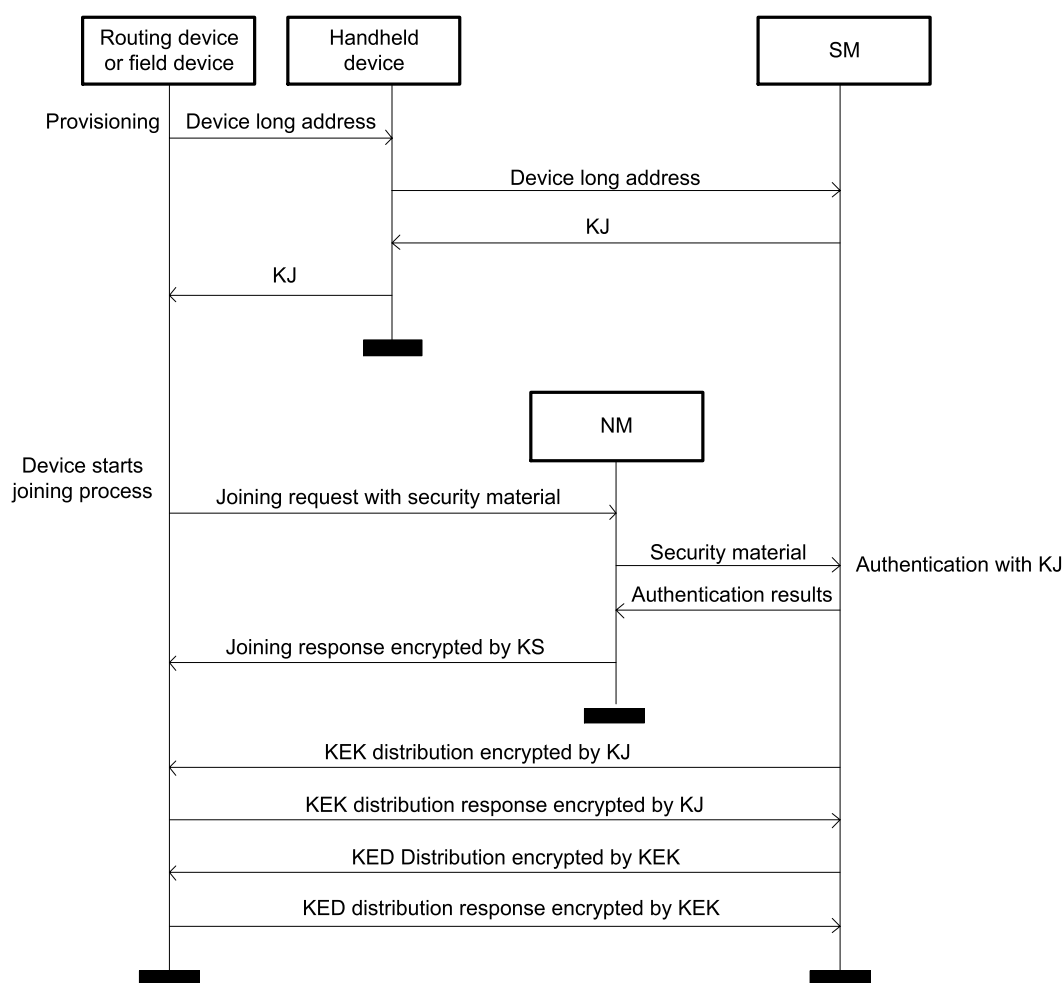
11.5 Secure joining process

11.5.1 Secure joining process of a new WIA-PA device

When a new field device or a new routing device joins the WIA-PA network, SM should authenticate the new field device or the new routing device.

A new device should have the KJ and 64-bit long address before joining the WIA-PA network. KJ should be written by handheld devices

The secure joining process of a new WIA-PA device is shown in Figure 80.



IEC

Figure 80 – Secure joining process of WIA-PA device

A new device that wants to join the WIA-PA network should proceed with the following steps.

- a) Before the new device joins the WIA-PA network, the handheld device reads the 64-bit long address of the new device and transfers it to the SM. The SM generates the KJ for the new device and the handheld device transfers the KJ to the new device.
- b) The new device with the KJ keeps scanning the available channels to get beacons from the online routing devices or the gateway device.
- c) The new device chooses an online routing device or the gateway device as the cluster head, and synchronizes with the network according to the received beacon.
- d) The new device generates the security material with the device long address and KJ, and sends it to the cluster head. The cluster head sends a joining request with security material to the NM for the new device.
- e) After the NM receives the joining request, it should forward the security material to the SM. The SM verifies the security material. If the authentication fails, the NM will return failure response. If authentication succeeds, the NM will return the success response.
- f) After the device completes the join process, the SM should generate the KEK for the new device and distribute the KEK encrypted by the KJ. Then the SM should generate the KED for the new device and distribute the KED encrypted by the KEK.

11.5.2 Device security material getting services

11.5.2.1 DLME-SEC.request

The routing devices use DLME-SEC.request to request the security material.

The semantics of DLME-SEC.request are described as follows:

DLME-SEC.request (

DstPhyAddr

)

Table 195 specifies the parameters for DLME-SEC.request.

Table 195 – DLME-SEC.request parameters

Name	Data type	Valid range	Description
DstPhyAddr	Unsigned64	0 to $(2^{64}-1)$	64-bit physical address of the new device

11.5.2.2 DLME-SEC.indication

On receipt of device security material getting request packet, the DLSE of the new device will invoke DLME-SEC.indication and inform the DMAP.

The semantics of DLME-SEC. indication are described as follows:

DLME-SEC.indication (

DstPhyAddr

)

Table 196 specifies the parameters for DLME-SEC.request.

Table 196 – DLME-SEC.indication parameters

Name	Data type	Valid range	Description
DstPhyAddr	Unsigned64	0 to $(2^{64}-1)$	64-bit physical address of the new device

11.5.2.3 DLME-SEC.response

The DMAP of the new device invokes DLME-SEC.response to provide its security material.

The semantics of DLME-SEC.response are described as follows:

```
DLME-SEC.response (
    ProxyAddr,
    PhyAddr,
    SecMaterial,
    Status
)
```

Table 197 specifies the parameters for DLME-SEC.response.

Table 197 – DLME-SEC.response parameters

Name	Data type	Valid range	Description
ProxyAddr	Unsigned16	0 to 65 535	The address of the routing device selected by the new device (Unicast address)
PhyAddr	Unsigned64	0 to $(2^{64}-1)$	64-bit physical address of the new device
SecMaterial	Unsigned32	0 to $(2^{32}-1)$	Device security material. It is generated with 64-bit address encrypted by KJ. Using bit 0-bit 31
Status	Unsigned8	0 to 255	Execution result of the request 0 = SUCCESS; 1 = FAILURE; Others are reserved

11.5.2.4 DLME-SEC.confirm

On receipt of the device security material getting response packet, the DLSL of the new device will invoke DLME-SEC.confirm and inform the DMAP.

The semantics of DLME-SEC.confirm are described as follows:

```
DLME-SEC.confirm (
    PhyAddr,
    SecMaterial,
    Status
)
```

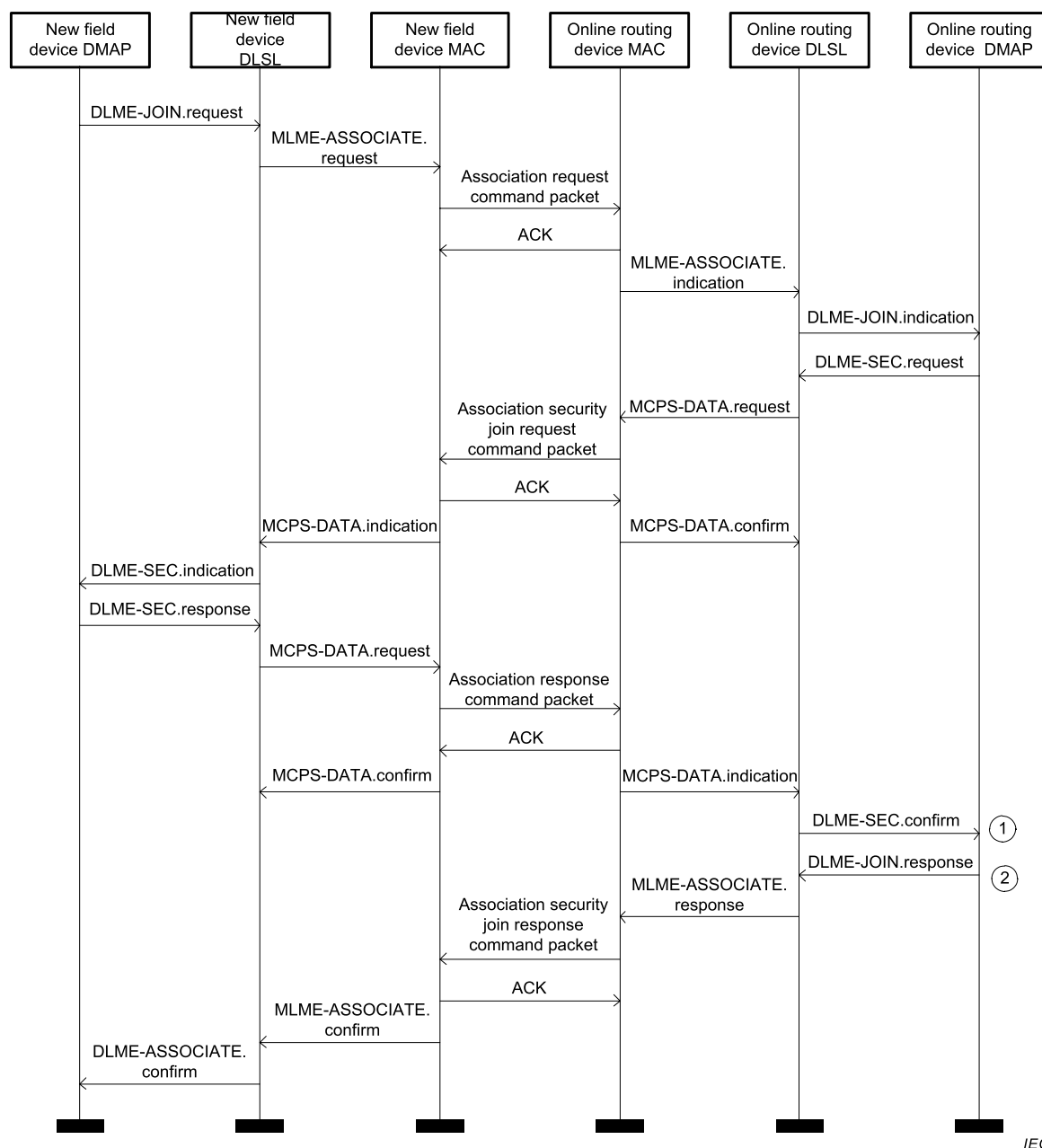
Table 198 specifies the parameters for DLME-SEC. confirm.

Table 198 – DLME-SEC.confirm parameters

Name	Data type	Valid range	Description
PhyAddr	Unsigned64	0 to $(2^{64}-1)$	The address of the routing device selected by the new device (unicast address)
SecMaterial	Unsigned32	0 to $(2^{32}-1)$	Device security material. It is generated by 64-bit address encrypted by the KJ. Using 0-31 bits.
Status	Unsigned8	0 to 255	Execution result of the request 0 = SUCCESS; 1 = FAILURE; Others are reserved.

11.5.2.5 Time sequence for device security joining

In the star and mesh architecture, if the SecEnableFlag = 1 (see 6.9.1.2.1), Figure 81 and Figure 82 illustrate examples of the security joining process of field devices.



IEC

Figure 81 – Time sequence for field device joining (field device to routing device)

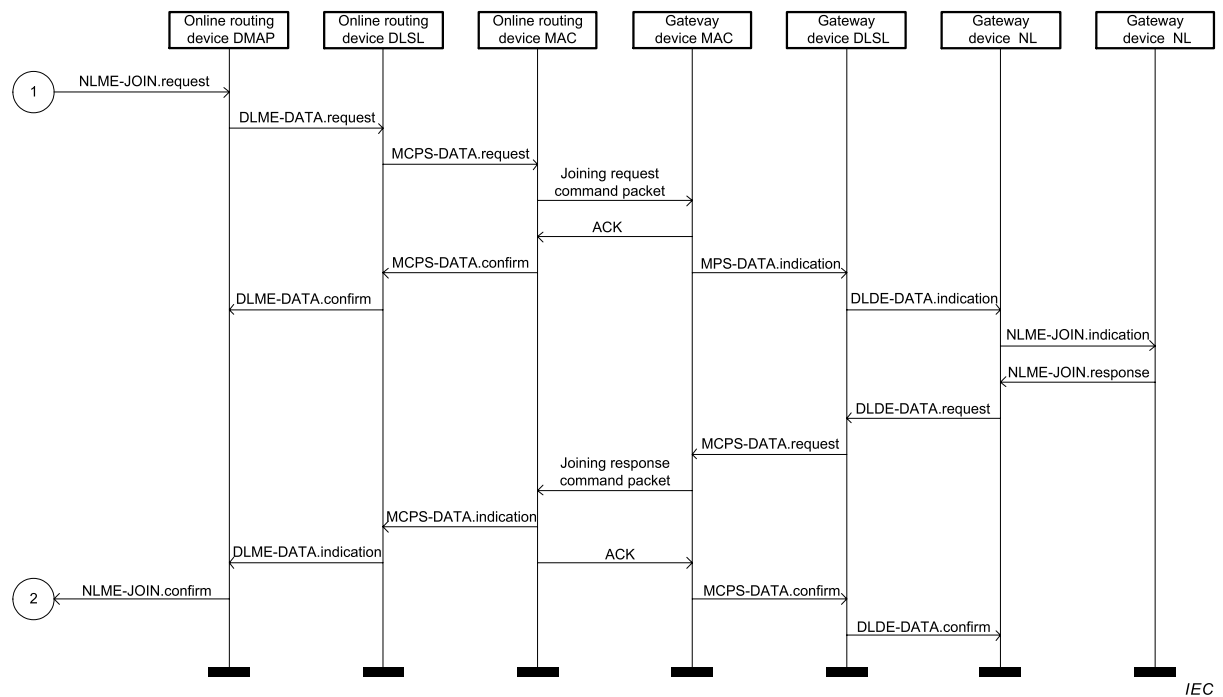
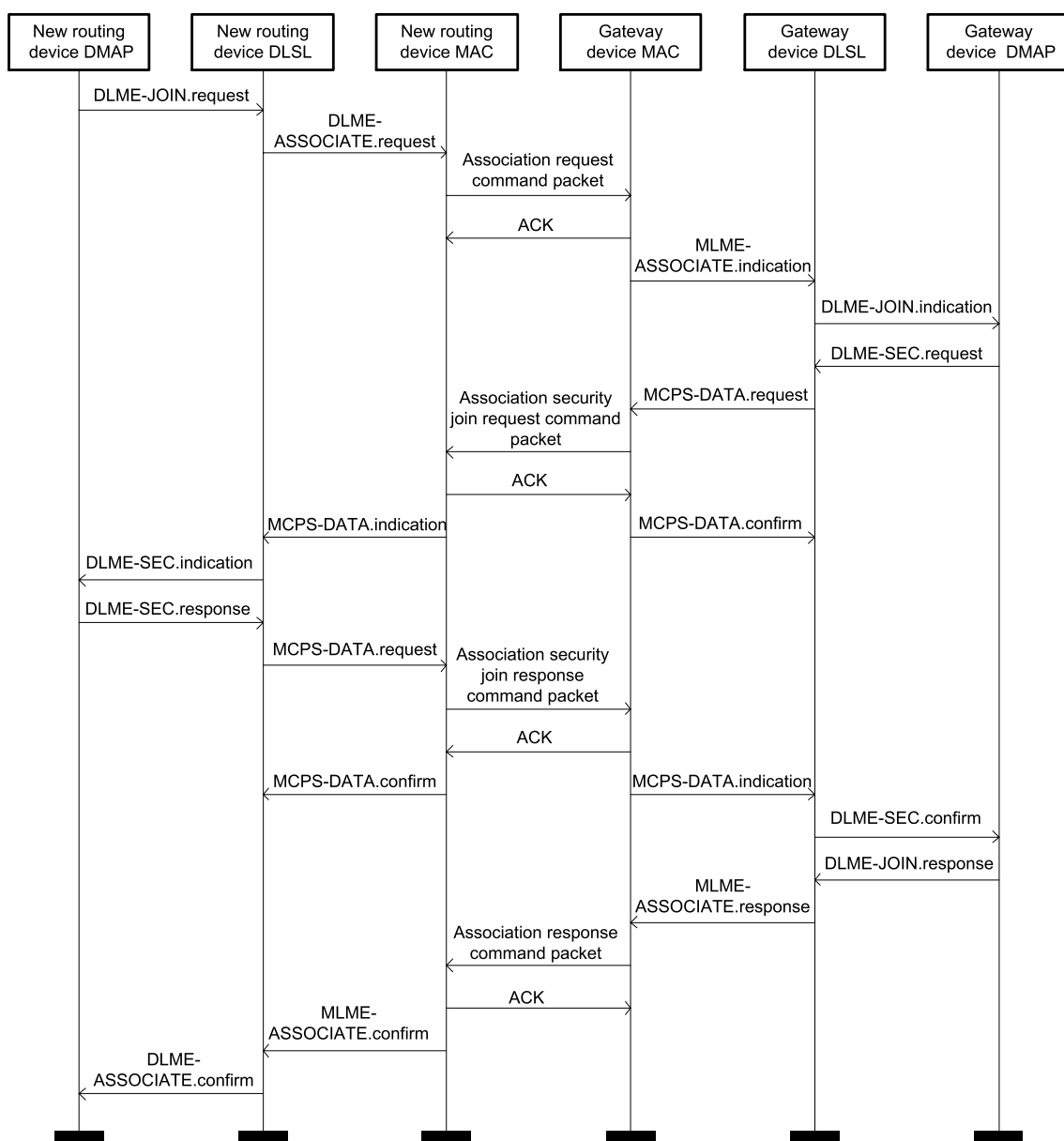


Figure 82 – Time sequence for field device joining (routing device to gateway device)

Figure 83, Figure 84, and Figure 85 illustrate examples of the join process of a routing device.



IEC

Figure 83 – One-hop joining process for routing device

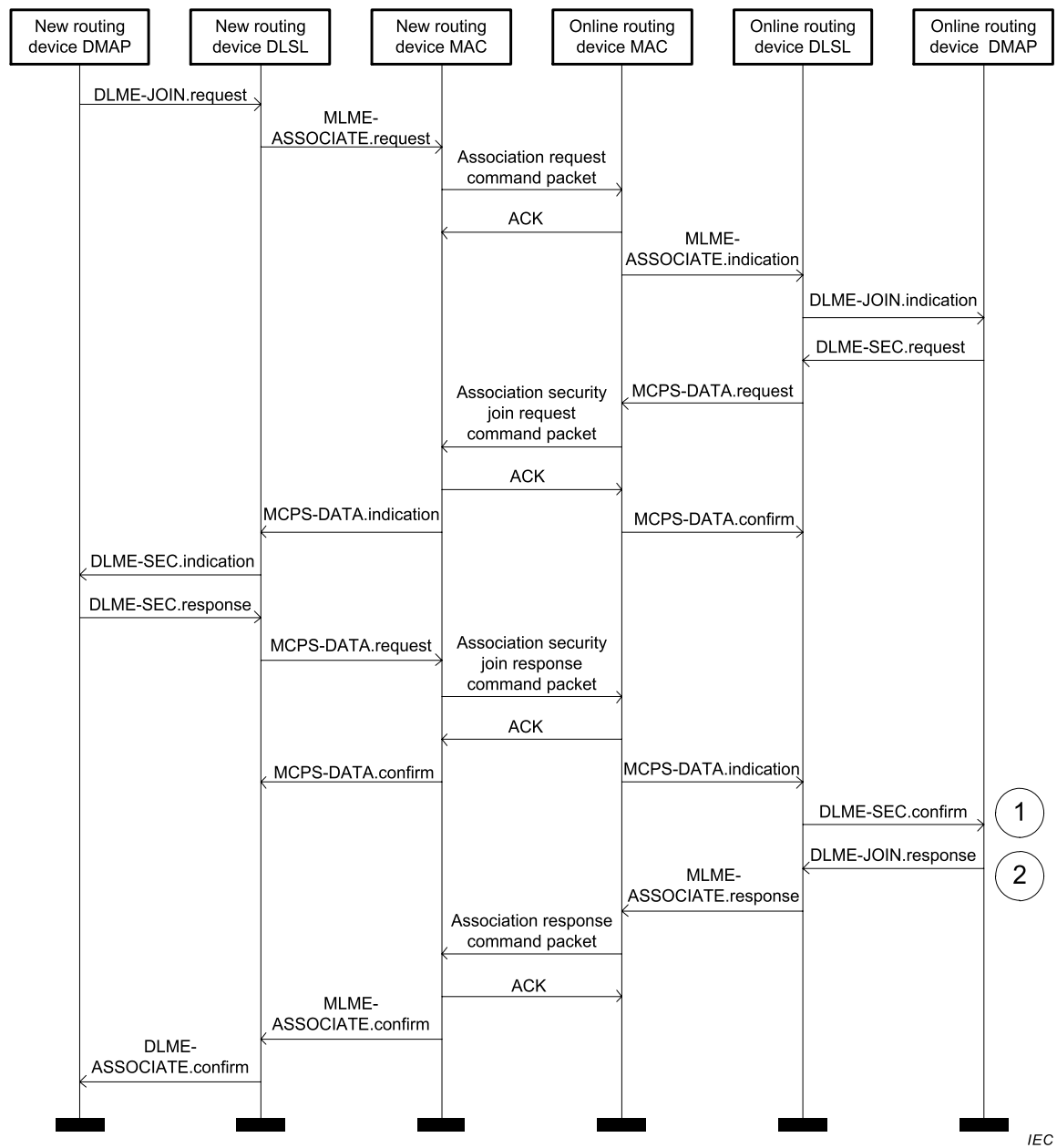


**Figure 84 – Multi-hop join process of routing device
(new routing device to routing device)**

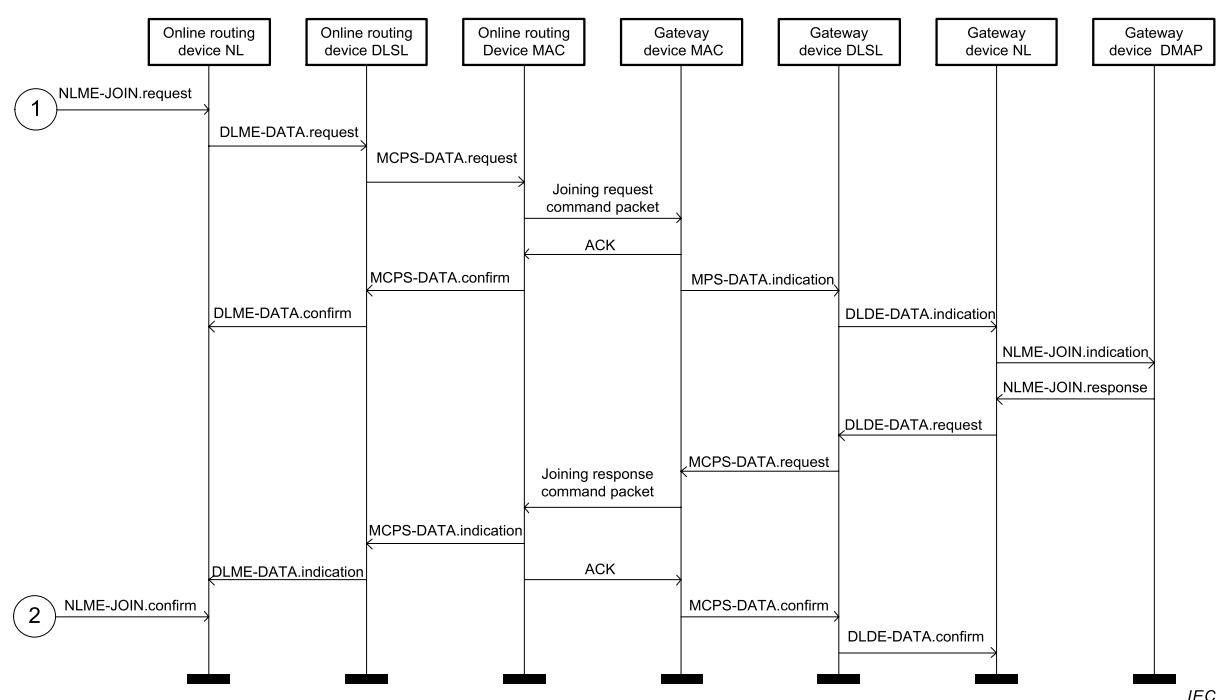


Figure 85 – Multi-hop join process of routing device (routing device to gateway device)

11.6 Secure transportation

11.6.1 Process of secure transportation from field device to host configuration computer

If the aggregation functions of routing devices and field device are not supported, the process of secure transportation from a field device to the host configuration computer includes the following steps.

- a) According to the SecMode and SecLevel in the MIB, the security management module of the DMAP in the field device encrypts the ASL payload, gets the integrity MIC in AL and sends it to the NL. According to the SecMode and SecLevel in the MIB, the security management module of the DMAP in the field device encrypts the DLSL payload and acquires the integrity MIC. Then it is sent to the routing device.
- b) When the routing device receives the packet, it decrypts the data frame and checks the integrity with the MIC in the DLSL, and then uses the next hop DLSL key to get the integrity MIC and encrypt the DLSL payload. Then the packet will be forwarded to the gateway device.
- c) When the gateway device receives the packet, the security management module will decrypt the packet and check the MIC on the DLSL and the ASL. Then the gateway device sends these data to the host configuration computer.

If the aggregation function of a field device is supported, the process of secure transportation from a field device to the host configuration computer includes the following steps.

- a) If the field device supports the data aggregation, it encrypts the payloads of multiple process data from multiple UAOs. According to the SecMode and SecLevel in the MIB, the security management module of the DMAP in the field device encrypts the ASL payload, acquires the integrity MIC in AL and sends it to the NL. According to the SecMode and SecLevel in the MIB, the security management module of the DMAP in the field device encrypts the DLSL payload and acquires the integrity MIC. Then the encrypted packet is sent to the routing device.
- b) If the aggregation function of a routing device is not supported, the routing device receives the packet. The routing device checks the MIC and decrypts the data packet on the DLSL. According to the SecMode and SecLevel in the MIB, the security management

module of the DMAP in the routing device encrypts the DLSL payload and gets the integrity MIC. Then the packet will be forwarded to the gateway device.

- c) If the aggregation function of a routing device is supported, the NL informs the DMAP to aggregate these payloads and obtains a new packet. According to the SecMode and SecLevel in the MIB, the security management module of the DMAP in the routing device firstly encrypts the ASL payload and acquires the integrity MIC; then the security management module of the DMAP in the routing device encrypts the DLSL payload and acquires the integrity MIC in the DLSL. The encrypted packet will be forwarded to the gateway device.
- d) When the gateway device receives the packet, the security management module checks the MIC and decrypts the packet in the DLSL and ASL. The packet is disaggregated and is sent to the host configuration computer.

11.6.2 Process of secure transportation from host configuration computer to field device

This process is the reverse transportation process from a field device to the host configuration computer.

Annex A **(informative)**

Security strategy for WIA-PA network

A.1 Risk analysis for WIA-PA network

As an open system, the WIA-PA network has potential security risks. According to the sources, these risks may either be from inter-networks or other intra-networks of a company or be from the internal WIA-PA networks. The WIA-PA network may suffer some threats, such as invasion, data destruction, and replay attacks.

Therefore, some security measures should be taken to ensure the security operations by the WIA-PA users, to protect the internal resources, and to maintain the normal system operations. The main objectives of the WIA-PA network security are to protect the normal system operations, to find the attacks and adopt corresponding methods as soon as possible, to limit the damage to the lowest level, and to return the network to its normal state as soon as possible after being attacked.

A.2 Security principles for WIA-PA network

According to the characteristics of the WIA-PA network, the following security measures and security principles are recommended:

- a) easy deployment and use;
- b) be optional for the security services and security measures;
- c) reduce the manual operation as much as possible;
- d) reduce the transmission of security information as much as possible;
- e) use encryption technologies based on hardware; and
- f) use the existing encryption and authentication technologies in addition to the published standard.

A.3 Security objectives for WIA-PA network

The objectives of security in the WIA-PA network include:

- a) border protection, which provides the border protection for the physical network;
- b) system availability, which is used to access system resources when needed by legal users;
- c) data integrity, which is used to ensure the consistency of the information and to prevent the illegal users in the system from modifying the data;
- d) device authenticity, which is used to authenticate the device identity in the WIA-PA network;
- e) confidentiality, which is used to ensure that the system hardware, software, and data can only be used by legal users;
- f) key management, which is used to perform the functions of security key updating and management.

A.4 Graded and layered security system

Based on their business, service types, and service objects, users employ different security methods and measures to confront security risks, risk grades, and required security levels. As for the limitations of the computing resources and the computing abilities of field devices, more attention should be paid to the border security of the WIA-PA network.

The graded and layered security system is shown in Table A.1.

Table A.1 – Graded and layered security measures for WIA-PA network

WIA-PA network security level	Level 0	Level 1	Level 2
Border protection	Gateway of message filtering	Gateway of protocol translation and message filtering	Gateway of IPSec translation and message filtering
Security measure	Authentication Integrity check	Authentication Access control Integrity check XOR encryption	Authentication Access control Integrity check Encryption

Both the DLSL and the AL in the WIA-PA network have the ability to establish secure connections. When a routing device forwards data packets, the security levels of the original data packets cannot be lowered. The security levels of the data packets are set according to Table A.2.

Table A.2 – Security levels of data packets

Incoming security level	Outgoing security level			
	Uncheck and unencryption	Encryption and Uncheck	Check and unencryption	Encryption and check
Uncheck and unencryption	allowed	allowed	allowed	allowed
Encryption and uncheck	not allowed	allowed	not allowed	allowed
Check and unencryption	not allowed	not allowed	allowed	allowed
Encryption and check	not allowed	not allowed	not allowed	allowed

Annex B (informative)

Format description

B.1 Time sequence diagram

Figure B.1 depicts the time sequence diagram. It is an interaction that focuses on the sequence of messages between stack layers of the WIA-PA network devices on the lifelines.

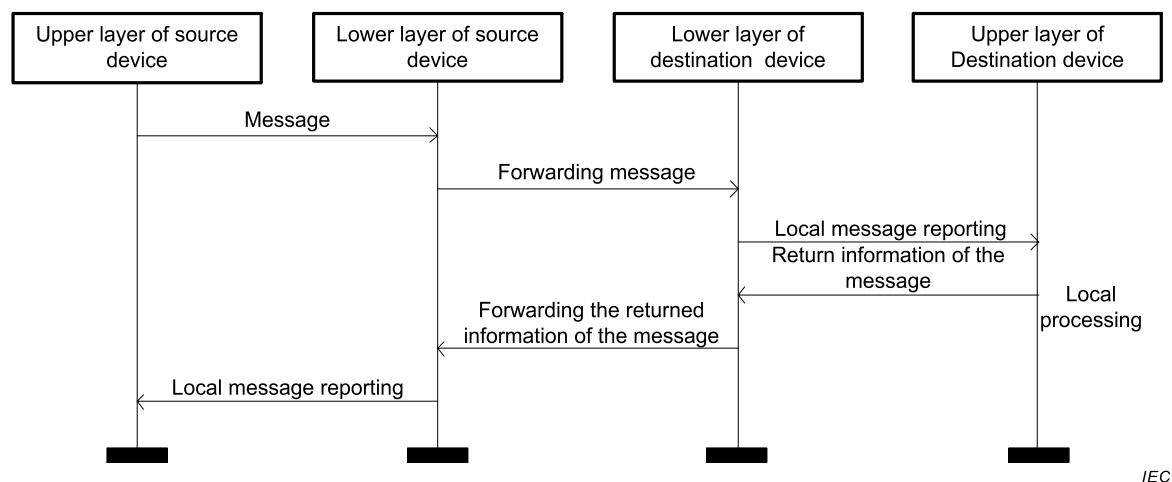


Figure B.1 – Time sequence diagram

The stack layers of the WIA-PA network devices are represented by rectangular blocks. Time is represented by vertical lines. A message is represented by an arrow. In this document, a full arrow is used to depict the general occurrence of a message independently of synchronous or asynchronous handling of the message. The sequence of messages is defined as the order of messages starting from the top of the diagram.

B.2 Packet or frame format

The definitions of a packet and a frame format have same structure. The main difference is their functional range. The packet format is used for NL and ASL, while the frame format is used for MAC and DLSL.

The field format in octet(s) of a packet or a frame is shown in Table B.1.

Table B.1 – Packet or frame format in octet(s)

	Packet or frame format in octet(s)			
Length in octet(s)	X_1	X_2	...	X_N
Field name	Field 1	Field 2	...	Field N

As shown in Table B.1, the value of X_i ($i=1,2,\dots, N$) describes the length in the octet(s) of the corresponding packet/frame field. The transmission of a packet/frame should be from the least significant octet to the most significant octet, i.e. the least significant octet of Field 1 should be transmitted first.

One field may have several lengths, depending on different contexts. In those cases, $X_{i1}/\dots/X_{iM}$ should be used instead of X_i to specify the length of Field i .

One field may contain subfields. Table B.2 specifies the definition of the subfield format if a field with 1-octet length is further divided into several subfields in bit(s).

Table B.2 – Subfield format in bit(s)

	Subfield format in bit(s)			
Length in bit(s)	X_1	X_2	...	X_N
Subfield name	Subfield 1	Subfield 2	...	Subfield m

As shown in Table B.2, the value of X_i ($i=1,2,\dots, N$) describes how many bits are occupied by the corresponding subfield, which is set from 1 to 8. The sum of $X_1, X_2, \dots$ and X_N is fixed at 8. The subfields from left to right are allocated from bit 0 to bit 7. The transmission of the subfield format should be from the least significant bit to the most significant bit, i.e. the least significant bit of Subfield 1 should be transmitted first.

Annex C (informative)

Example of UAO

C.1 General

This document specifies UAOs by using an object-oriented approach. An UAO has its own attributes and methods. The attributes include the object name, attribute name, attribute identifier, and data type of the attribute. The methods provided by the UAOs are used to realize the operations of these attributes.

The UAOs may include Analog Input Object (AIO), Analog Output Object (AOO), Digital Input Object (DIO), and Digital Output Object (DOO). These objects should be defined in the application profiles. This document utilizes AIO as an example to specify the use of UAOs. Furthermore, DAGO, PAGO, and DGO are regarded as special UAOs.

C.2 Analog input object

C.2.1 Overview

An AIO is used to sample the industrial process and convert the measured value to the data value with physical dimensions. The methods supported by the AIO are shown in Table 171.

C.2.2 Class attribute of AIO

Table C.1 specifies the class attribute of AIO.

Table C.1 – AIO class attribute

Attribute name	Attribute identifier	Data type	Supporting method	Description
Object identifier	0	Unsigned8	Read	The unique identifier of an object that is used for object addressing.

C.2.3 Instance attribute of AIO

Table C.2 specifies the instance attributes of AIO.

Table C.2 – AIO instance attributes

Attribute identifier	Attribute name	Data type	Supporting method	Description
1	Instance ID	Unsigned8	READ	The unique identifier of an object instance
2	ProcessValue	Float	READ	Industrial process variable
3	OutValue	Float	READ PUBLISH REPORT	Output value based on ProcessValue
4	SimulateValue	Float	READ/WRITE	Value written by operator to simulate the OutValue
5	DefaultValue	Float	READ/WRITE	Default value for the OutValue if a sensor or sensor electronic fault is detected
6	HighWarning	Float	READ/WRITE	High limit value of warning
7	HighHighAlm	Float	READ/WRITE	High limit value of alarm
8	LowWarning	Float	READ/WRITE	Low limit value of warning
9	LowLowAlm	Float	READ/WRITE	Low limit value of alarm
10	EngineeringUnit	Unsigned16	READ/WRITE	Engineering unit for all the values
10	Action	Unsigned8	READ/WRITE	Start-up/stop measurement process
11	SamplePeriod	Unsigned32	READ/WRITE	Used for setting sampling cycle
12	Alarm	Unsigned8	READ	0 = Normal; 1 = HighWarning; 2 = LowWarning; 3 = HighAlarm; 4 = LowAlarm 5 to 255 = Reserved.
13 to 99	Reserved			Reserved for future usage
100 to 255	Manufacturer specific			Manufacturer specific attributes

Annex D (informative)

Country-specific and region-specific provisions

The WIA-PA field medium employs a widely used and accepted physical interface and is therefore appropriate for use in many geographic regions of the world. However, some regions have special considerations that may impose different regulatory requirements. Even if a product is designed to meet those regulatory requirements, its use is often not legally permitted until it has undergone compliance testing and any required local permits or certificates have been issued by country-specific regulatory agencies.

This document is designed to support operation within a fixed geographic area that operates under uniform regulations. As such it is intended to support operation anywhere in the world, as discussed in 8.4.11.

This document does not specify what regulatory certifications or permit a product compliant to this document needs; this is the responsibility of the product manufacturer and the end user to determine. A product may have certifications for operation in multiple countries or regions.

Annex E addresses specific provisions that have been made in this document to support regulatory approval of fixed-locale equipment and systems.

Radio regulations often require devices to operate at constrained power levels at all times, including during over-the-air provisioning. Some identified EIRP thresholds are: 10 mW/MHz (Japan); 10 dBm (China); 10 dBm, 10 dBm/MHz, or 20 dBm (EC in the 2,4 GHz ISM-band); 36 dBm with at most 6 dBi antenna gain (US FCC).

In some countries, such as France, emission levels on certain channels may need to be attenuated. In other countries, such as Korea, the number and range of channels needs to be constrained.

Annex E (informative)

Regional modification for compliance with ETSI standards

E.1 General

WIA-PA restricts the usage of the spectrum to the 2,4 GHz ISM band, see Clause 7.

Additional requirements apply in Europe to wide band radio frequency transmitting equipment operating in this 2,4 GHz ISM band. Some of these European requirements can be met by complying with two Harmonized Standards from ETSI, EN 300 328 and EN 300 440-2.

Annex E provides additional requirements for compliance of WIA-PA (IEC 62601) devices operating in the 2,4 GHz ISM band with these two ETSI standards:

- EN 300 440-2 is applicable for equipment (devices) with a maximum transmit power between 0 dBm and 10 dBm EIRP. (see Clause E.2);
- EN 300 328 is applicable for equipment (devices) with a maximum transmit power between 10 dBm and 100 dBm EIRP. (see Clause E.3).

NOTE In Annex E, the term “devices” refers to electronics with radios operating according to the appropriate standard; these include but are not limited to gateway devices, routing devices and field devices.

E.2 Compliance with EN 300 440-2

Table E.1 specifies the additional requirements which allow WIA-PA devices operating in the 2,4 GHz ISM band to satisfy the transmit power limitation requirements of EN 300 440-2.

NOTE EN 300 440-2 is listed as a Harmonized Standard under the R&TTE Directive 1999/5/EC which will be superseded by the Radio Equipment Directive 2014/53/EU.

Table E.1 – Applicable EN 300 440-2 requirements list

Parameter	EN 300 440-2 requirements	Additional requirements
Maximum Transmit Power	10 dBm (10 mW) EIRP	Devices shall be configured to emit less than 10 dBm EIRP, that means less than 10 dBm electrical power with an antenna gain of 0 dBi. If the antenna gain is different from 0 dBi, then the resulting EIRP shall be less than 10 dBm by an adequate electrical power adjustment. This requirement overwrites the requirement about electrical power given in 7.3.6.

E.3 Compliance with EN 300 328

Table E.2 specify the additional requirements which allow WIA-PA devices operating in the 2,4 GHz ISM band to satisfy various requirements of EN 300 328.

NOTE EN 300 328 V1.9.1 is listed as a Harmonized Standard under the R&TTE Directive 1999/5/EC which will be superseded by the Radio Equipment Directive 2014/53/EU.

Table E.2 – Applicable EN 300 328 requirements list

Parameter	EN 300 328 V1.9.1 requirements	Additional requirements
Maximum Transmit Power	20 dBm (100 mW) EIRP	Devices shall be configured to emit less than 10 dBm $\pm$ 3 dBm EIRP according to 7.3.6.

Parameter	EN 300 328 V1.9.1 requirements	Additional requirements
Maximum Power Spectral Density	10 mW/MHz EIRP	Due to the nature of DSSS (see IEEE 802.15.4-2011, Clause 10), a maximum EIRP of 13 dBm results in a spectral density below 10mW/MHz as required.
Duty Cycle, Tx-sequence, Tx-gap	For non-adaptive equipment with maximum EIRP above 10 dBm: The Duty Cycle shall be equal to or less than the maximum value declared by the supplier. Tx-sequence time $\leq$ 10ms. The minimum Tx-gap time following a Tx-sequence shall be equal to the duration of that proceeding Tx-sequence with a minimum of 3.5 ms	No additional requirement needed. The requirements are fulfilled by the following characteristics. The maximum Tx-sequence time for a WIA-PA packet is 4,256 ms in a 10 ms time slot according to Table E.3, T_{maxPHY} and the transmission time for a WIA-PA ACK is 352 μs according to Table E.3 TACK. The Maximum Tx-sequence Time for WIA-PA is identical to maximum transmission time; the Minimum Tx-gap Time for WIA-PA is identical to maximum transmission time.
Medium Utilization Limit	For non-adaptive equipment with maximum EIRP above 10 dBm: Maximum Medium Utilization factor = 10 %.	The Duty Cycle of a WIA-PA device cannot exceed 43 % based on a 10 ms timeslot and a maximum transmission time for a WIA-PA packet of 4,256 ms in a 10 ms time slot according to Table E.3. This results in a MU factor value of less than 10 % as required. $MU = 13 \text{ dBm EIRP} \times 43 \% < 9 \%$

Table E.3 – Timeslot timing definitions and calculations

Symbol	Time value	Calculation basis
T _{maxPHY}	4 256 μ s	For 2 400 to 2 483, 5 MHz frequency band and 250 Kbps bit rate, the maximum time to transmit a PHY packet is 4 256 μ s, which includes 128 μ s Preamble (see Table 71 of IEEE STD 802.15.4-2011), 32 μ s SFD (see Table 71 of IEEE STD 802.15.4-2011), and 4 096 μ s PHR/PHY Payload (see Table 70 of IEEE STD 802.15.4-2011)
T _{ACK}	352 μ s	WIA-PA devices shall use the IEEE STD 802.15.4-2011 ACK. The total length of ACK is 11 octets (see Figure 47 and Figure 67 in IEEE STD 802.15.4-2011,) and the time to transmit an ACK is 352 μ s for 2 400 – 2 483,5 MHz frequency band and 250 Kbps bit rate
T _{Offset}	2 120 μ s	Beginning of the timeslot to when the receiver shall be listening
T _{Delay}	1 000 μ s	End of frame to start of Acknowledgment

Bibliography

ISO/IEC/IEEE 60559:2011, *Information technology – Microprocessor Systems – Floating-Point arithmetic*

IEC 61804-2, *Function blocks (FB) for process control – Part 2: Specification of FB concept*

IEC 61499-1, *Function blocks – Part 1: Architecture*

IEC 61499-2, *Function blocks – Part 2: Software tools requirements*

IEC TR 62390:2005, *Common automation device – Profile guideline*

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

ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*

ISO/IEC 9797-2:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*

ISO 3166-1, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*

ISO 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*

ISO 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*

ISO 10181-5:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework*

ISO 10181-6:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework*

ISO/IEC 15408-1, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components*

ISO/IEC TR 10000-1:1998, *Information technology – Framework and taxonomy of International Standardized Profiles – Part 1: General principles and documentation framework*

ISO/IEC 17799:2005¹, *Information technology – Security techniques – Code of practice for information security management*

ETSI EN 300 328 V1.8.1 (2012-06), *Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in*

¹ Withdrawn.

the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

ETSI EN 300 440-2, V1.4.1 (2010-08), *Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Part 2: Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive*

Directive 1999/5/EC of the European Commission, Radio equipment and telecommunication terminal equipment (R&TTE),
available at: <http://ec.europa.eu/enterprise/sectors/rtte/index_en.htm>

Directive 2014/53/EU of the European Parliament and of the Council, Radio Equipment (repealing Directive 1999/5/EC),
available at: <http://ec.europa.eu/enterprise/sectors/rtte/index_en.htm>

IEEE 64, *Guidelines for 64-bit Global Identifier (EUI-64™)*

IEEE 754:2008, *Standard for floating-point arithmetic*

SOMMAIRE

AVANT-PROPOS	236
1 Domaine d'application	238
2 Références normatives	238
3 Termes, définitions et abréviations	238
3.1 Termes et définitions	238
3.2 Abréviations	243
4 Définition des types de données	245
5 Aperçu de WIA-PA	245
5.1 Types d'appareils	245
5.2 Topologie de réseau	246
5.3 Architecture de protocole	249
5.4 Interconnexions	251
6 Gestion de système	252
6.1 Généralités	252
6.2 Cadre de travail de la gestion système	254
6.3 Processus de rattachement	256
6.3.1 Processus de mise en service	256
6.3.2 Processus de rattachement d'un appareil de routage	256
6.3.3 Processus de rattachement d'un appareil de terrain	258
6.3.4 Adressage et attribution d'adresses	260
6.4 Relation de communication virtuelle (VCR, Virtual Communication Relationship)	262
6.4.1 Définition	262
6.4.2 Prise en charge du protocole pour la VCR	263
6.4.3 Etablissement de VCR	263
6.4.4 Libération de VCR	264
6.5 Configuration du routage et allocation de ressources de communication	264
6.5.1 Configuration de routage	264
6.5.2 Cadre de travail de l'allocation de ressources de communication	264
6.5.3 Règles de priorité des unités DLPDU et de programmation	265
6.5.4 Affectation de ressources de communication à l'appareil de routage	266
6.5.5 Affectation de ressources de communication à l'appareil de terrain	268
6.6 Agrégation et désagrégation	271
6.6.1 Agrégation	271
6.6.2 Désagrégation	273
6.6.3 Exemple du processus d'agrégation à deux niveaux	274
6.6.4 Gestion des objets d'agrégation et de désagrégation	276
6.7 Surveillance de performance	278
6.7.1 Rapport sur la défaillance des chemins	278
6.7.2 Rapport sur l'état des appareils	279
6.7.3 Rapport sur la condition des canaux	280
6.8 Processus de départ	280
6.8.1 Généralités	280
6.8.2 Processus de départ d'un appareil de routage	281
6.8.3 Processus de départ d'un appareil de terrain	283
6.9 Services et base d'informations de gestion	286

6.9.1	Base d'informations de gestion	286
6.9.2	Services MIB	301
7	Couche physique	304
7.1	Généralités	304
7.2	Exigences générales basées sur l'IEEE 802.15.4-2011	305
7.3	Exigences supplémentaires	306
7.3.1	Généralités	306
7.3.2	Affectations de fréquence	306
7.3.3	Numéros de canal et affectations de fréquence	306
7.3.4	Emetteurs-récepteurs radio	307
7.3.5	Performance radio exigée améliorée ou non spécifiée	307
7.3.6	Puissance d'émission	307
7.3.7	Contrôle de la puissance de sortie	307
7.3.8	Sensibilité du récepteur	307
7.3.9	Attributs PIB de la PHY	308
8	Couche liaison de données	309
8.1	Généralités	309
8.2	Pile de protocole	309
8.3	Vue d'ensemble de la couche MAC et extension de fonction	309
8.3.1	Vue d'ensemble de la couche MAC	309
8.3.2	Exigences générales basées sur l'IEEE 802.15.4-2011	310
8.3.3	Extension de fonction MAC	314
8.4	Description de la fonction de la sous-couche liaison de données (DLSL)	315
8.4.1	Généralités	315
8.4.2	Coexistence	316
8.4.3	Communication en intervalles de temps	316
8.4.4	Superframe WIA-PA	316
8.4.5	Saut de fréquence	318
8.4.6	Transmission des données de cycle long	319
8.4.7	Stratégie de nouvelle tentative	320
8.4.8	Service de gestion	321
8.4.9	Mesure de la qualité de liaison radio et de la condition des canaux	321
8.4.10	Sécurité	321
8.4.11	Code de pays	321
8.4.12	Diagramme d'états de DLSL	322
8.5	Services de données de la sous-couche liaison de données	329
8.5.1	Généralités	329
8.5.2	DLDE-DATA.request	329
8.5.3	DLDE-DATA.confirm	330
8.5.4	DLDE-DATA.indication	331
8.5.5	Séquence temporelle de service de données DLSL	332
8.6	Services de gestion de la sous-couche liaison de données	333
8.6.1	Généralités	333
8.6.2	Services de découverte de réseau	334
8.6.3	Services de rattachement d'appareil	336
8.6.4	Services de départ d'appareil	339
8.6.5	DLME-CHANNEL-CONDITION.indication	340
8.6.6	DLME-NEIGHBOUR-INFO.indication	340
8.6.7	DLME-COMM-STATUS.indication	341

8.6.8	Services d'entretien	341
8.6.9	Services de synchronisation du temps	342
8.7	Formats de trame DLSL	343
8.7.1	Format général de trame	344
8.7.2	Format de trame de données	345
8.7.3	Format de trame de commande	345
9	Couche Réseau	347
9.1	Généralités	347
9.2	Pile de protocole	347
9.3	Description de fonction	348
9.3.1	Généralités	348
9.3.2	Adressage	349
9.3.3	Routage.....	349
9.3.4	Gestion du cycle de vie des paquets.....	350
9.3.5	Rattachement à un réseau et départ d'un réseau pour un appareil.....	350
9.3.6	Surveillance bout en bout des performances du réseau	350
9.3.7	Fragmentation et réassemblage.....	350
9.3.8	Diagramme d'états de la couche réseau	350
9.4	Services de données de la couche réseau	357
9.4.1	Généralités	357
9.4.2	NLDE-DATA.request.....	357
9.4.3	NLDE-DATA.confirm	357
9.4.4	NLDE-DATA.indication	358
9.4.5	Séquence temporelle des services de données de la NL	358
9.5	Services de gestion de la NL	359
9.5.1	Généralités	359
9.5.2	Services de rapport sur l'état de communication du réseau.....	359
9.5.3	Services de rattachement au réseau.....	362
9.5.4	Services de départ de réseau	368
9.5.5	Services de rapport sur l'élément de groupe	373
9.5.6	Services de rapport sur les informations de voisins	376
9.5.7	Services d'allocation d'itinéraire.....	378
9.5.8	Services d'allocation de ressources de communication	384
9.5.9	Services d'agrégation et désagrégation	403
9.5.10	Services de rapport sur l'état des appareils	405
9.5.11	Rapport sur la condition des canaux	407
9.5.12	Services de rapport sur les chemins défaillants	410
9.5.13	Services d'obtention des attributs de réseau.....	412
9.5.14	Services d'établissement des attributs de réseau.....	415
9.6	Formats de paquets de couche réseau.....	418
9.6.1	Format commun des paquets.....	418
9.6.2	Format des paquets de données.....	420
9.6.3	Format de paquet agrégé.....	420
9.6.4	Format de paquet de commande.....	421
10	Application layer, couche d'application	441
10.1	Vue d'ensemble	441
10.1.1	Généralités	441
10.1.2	Structure de la couche AL.....	441
10.1.3	Fonctions de l'UAP	442

10.1.4	Fonctions de la sous-couche application (ASL)	442
10.2	UAP	443
10.2.1	Généralités	443
10.2.2	UAO	443
10.2.3	Définition des méthodes	444
10.3	Sous-couche application	448
10.3.1	Généralités	448
10.3.2	Entité de données de la sous-couche application (ASLDE)	448
10.4	Formats des paquets de la sous-couche application (ASL)	454
10.4.1	Généralités	454
10.4.2	Format de paquet général ASL	454
10.4.3	Formats de paquet	456
11	Sécurité	458
11.1	Généralités	458
11.2	Cadre de travail de gestion de la sécurité	459
11.3	Pile de protocole de communications sécurisées	460
11.3.1	Généralités	460
11.3.2	Sécurité de la sous-couche liaison de données	461
11.3.3	Sécurité de la sous-couche application (ASL)	463
11.4	Gestion de clés	464
11.4.1	Type de clé	464
11.4.2	Distribution de clés	465
11.4.3	Mise à jour de clé	465
11.4.4	Etat de clé	466
11.5	Processus de rattachement sécurisé	466
11.5.1	Processus de rattachement sécurisé d'un nouvel appareil WIA-PA	466
11.5.2	Services d'obtention des renseignements de sécurité de l'appareil	468
11.6	Transport sécurisé	475
11.6.1	Processus de transport sécurisé entre un appareil de terrain et l'ordinateur de configuration d'hôte	475
11.6.2	Processus de transport sécurisé entre l'ordinateur de configuration d'hôte et un appareil de terrain	476
Annexe A (informative)	Stratégie de sécurité pour le réseau WIA-PA	477
A.1	Analyse du risque pour le réseau WIA-PA	477
A.2	Principes de sécurité pour le réseau WIA-PA	477
A.3	Objectifs de sécurité pour le réseau WIA-PA	477
A.4	Système de sécurité gradué et stratifié	477
Annexe B (informative)	Description de format	479
B.1	Diagramme de séquence temporelle	479
B.2	Format de paquet ou de trame	479
Annexe C (informative)	Exemple d'objet d'application utilisateur (UAO)	481
C.1	Généralités	481
C.2	Objet d'entrée analogique	481
C.2.1	Vue d'ensemble	481
C.2.2	Attribut de classe de l'AIO	481
C.2.3	Attribut d'instance de l'AIO	481
Annexe D (informative)	Configurations spécifiques à un pays et spécifiques à une région	483
Annexe E (informative)	Modifications régionales pour conformité aux normes ETSI	484

E.1	Généralités	484
E.2	Conformité à l'EN 300 440-2 V1.4.1	484
E.3	Conformité à l'EN 300 328 V1.8.1	484
	Bibliographie.....	486

Figure 1	Exemple de topologie physique WIA-PA (combinaison de la configuration en étoile et de la configuration maillée).....	247
Figure 2	Exemple de topologie physique WIA-PA (en étoile uniquement)	248
Figure 3	Modèle de référence OSI de base mappé au réseau WIA-PA	251
Figure 4	Architecture de passerelle WIA-PA.....	251
Figure 5	Processus DMAP dans la gestion du système	253
Figure 6	Plan de gestion de système hybride centralisée et répartie	255
Figure 7	Processus de rattachement d'un appareil de routage par l'intermédiaire de l'appareil de passerelle	257
Figure 8	Processus de rattachement d'un appareil de routage par l'intermédiaire d'un appareil de routage en ligne	258
Figure 9	Processus de rattachement d'un appareil de terrain par l'intermédiaire d'un appareil de passerelle.....	259
Figure 10	Processus de rattachement d'un appareil de terrain par l'intermédiaire d'un appareil de routage	260
Figure 11	Structure d'adresse longue d'un appareil.....	261
Figure 12	Structure d'adresse courte d'un appareil de routage	261
Figure 13	Structure d'adresse courte d'un appareil de terrain.....	262
Figure 14	Exemple d'affectation de ressources	265
Figure 15	Processus d'affectation de ressources de communication d'un appareil de routage	268
Figure 16	Processus d'affectation de ressources de communication d'un appareil de terrain	271
Figure 17	Exemple d'agrégation et de désagrégation	276
Figure 18	Processus de rapport sur la défaillance des chemins	279
Figure 19	Processus de rapport sur l'état des appareils pour l'appareil de terrain	279
Figure 20	Processus de rapport sur l'état des appareils pour l'appareil de routage	280
Figure 21	Processus de rapport sur la condition des canaux	280
Figure 22	Processus de départ actif d'un appareil de routage	281
Figure 23	Processus de départ passif d'un appareil de routage.....	282
Figure 24	Processus de départ actif d'un appareil de terrain (quittant l'appareil de passerelle).....	283
Figure 25	Processus de départ actif d'un appareil de terrain (quittant l'appareil de routage).....	284
Figure 26	Processus de départ passif d'un appareil de terrain (quittant l'appareil de passerelle).....	285
Figure 27	Processus de départ passif d'un appareil de terrain (quittant l'appareil de routage).....	285
Figure 28	Pile de protocole de la couche DLL du réseau WIA-PA	309
Figure 29	Modèle de référence de la DLSL du réseau WIA-PA.....	315
Figure 30	Supertrame WIA-PA	317
Figure 31	Structures des supertrames R1, R2 et R3	319

Figure 32 – Exemple de transmission de données de cycle long	320
Figure 33 – Diagramme d'états de la sous-couche DLSL pour le rattachement d'appareil	323
Figure 34 – Diagramme d'états de la sous-couche DLSL pour l'exécution dans le réseau	325
Figure 35 – Séquence temporelle de service de données.....	333
Figure 36 – Séquence temporelle de découverte de réseau	336
Figure 37 – Format général de trame	344
Figure 38 – Pile de protocole de la couche réseau WIA-PA.....	348
Figure 39 – Modèle de référence de couche réseau WIA-PA.....	348
Figure 40 – Diagramme d'états de la couche réseau	351
Figure 41 – Séquence temporelle des services de données de la NL	359
Figure 42 – Séquence temporelle pour le rattachement d'appareil de terrain via un appareil de routage	365
Figure 43 – Processus de rattachement en un saut d'un appareil de routage	366
Figure 44 – Processus de rattachement multisaut de l'appareil de routage	367
Figure 45 – Processus de départ actif d'un appareil de terrain (appareil de routage partant).....	370
Figure 46 – Départ passif d'un appareil de terrain	371
Figure 47 – Processus de départ actif d'un appareil de routage	372
Figure 48 – Processus de départ passif d'un appareil de routage.....	373
Figure 49 – Processus de production de rapport sur l'élément de groupe.....	376
Figure 50 – Processus de production de rapport sur les informations de voisins	378
Figure 51 – Séquence temporelle pour l'ajout d'itinéraire	380
Figure 52 – Séquence temporelle pour la mise à jour d'itinéraire	382
Figure 53 – Séquence temporelle pour la suppression d'itinéraire	384
Figure 54 – Ajout d'une liaison allant d'un appareil de passerelle à un appareil de routage	387
Figure 55 – Ajout d'une liaison allant d'un appareil de routage à un appareil de terrain	388
Figure 56 – Mise à jour d'une liaison allant d'un appareil de passerelle à un appareil de routage	390
Figure 57 – Mise à jour d'une liaison allant d'un appareil de routage à un appareil de terrain	391
Figure 58 – Libération d'une liaison allant d'un appareil de passerelle à un appareil de routage	393
Figure 59 – Libération d'une liaison allant d'un appareil de routage à un appareil de terrain	394
Figure 60 – Ajout d'une supertrame allant d'un appareil de passerelle à un appareil de routage	396
Figure 61 – Ajout d'une supertrame allant d'un appareil de routage à un appareil de terrain	397
Figure 62 – Mise à jour d'une supertrame allant d'un appareil de passerelle à un appareil de routage.....	399
Figure 63 – Mise à jour d'une supertrame allant d'un appareil de routage à un appareil de terrain	400
Figure 64 – Libération d'une supertrame allant d'un appareil de passerelle à un appareil de routage.....	402

Figure 65 – Libération d'une supertrame allant d'un appareil de routage à un appareil de terrain	403
Figure 66 – Processus de production de rapport sur l'état des appareils d'un appareil de terrain à un appareil de routage	406
Figure 67 – Processus de production de rapport sur l'état des appareils d'un appareil de routage à un appareil de passerelle	407
Figure 68 – Processus de production de rapport sur la condition des canaux d'un appareil de terrain à un appareil de routage	409
Figure 69 – Processus de production de rapport sur la condition des canaux d'un appareil de routage à un appareil de passerelle	409
Figure 70 – Processus de production de rapport sur les chemins défaillants	411
Figure 71 – Structure de la couche application (AL)	442
Figure 72 – Processus d'application utilisateur (UAP)	443
Figure 73 – Processus de communication C/S	452
Figure 74 – Processus de communication P/S (fonction d'agrégation désactivée)	453
Figure 75 – Processus de communication P/S (fonction d'agrégation activée)	453
Figure 76 – Processus de communication R/S	454
Figure 77 – Cadre de travail de la gestion de la sécurité pour le réseau WIA-PA	459
Figure 78 – Pile de protocole de communication en sécurité	461
Figure 79 – Cycle de vie des clés	465
Figure 80 – Processus de rattachement sécurisé d'un nouvel appareil WIA-PA	467
Figure 81 – Séquence temporelle pour le rattachement d'un appareil de terrain (appareil de terrain vers appareil de routage)	471
Figure 82 – Séquence temporelle pour le rattachement d'un appareil de terrain (appareil de routage vers appareil de passerelle)	472
Figure 83 – Processus de rattachement en un saut d'un appareil de routage	473
Figure 84 – Processus de rattachement multisaut d'un appareil de routage (nouvel appareil de routage vers appareil de routage)	474
Figure 85 – Processus de rattachement multisaut d'un appareil de routage (appareil de routage vers appareil de passerelle)	475
Figure B.1 – Diagramme de séquence temporelle	479
Tableau 1 – Définition des types de données	245
Tableau 2 – Prise en charge du protocole pour la VCR	263
Tableau 3 – Relations entre la VCR et la fonction d'agrégation	272
Tableau 4 – Format des données agrégées suivies par l'objet DAGO de l'appareil de terrain	273
Tableau 5 – Format du paquet agrégé suivi par l'objet PAGO de l'appareil de routage	273
Tableau 6 – Attributs de la classe DAGO	277
Tableau 7 – Attributs de l'instance DAGO	277
Tableau 8 – Structure MEM_STRUCT	277
Tableau 9 – Attributs de la classe PAGO	277
Tableau 10 – Attributs de l'instance PAGO	278
Tableau 11 – Attributs de la classe DGO	278
Tableau 12 – Attributs de l'instance DGO	278
Tableau 13 – Attributs non structurés (1 de 5)	287

Tableau 14 – Attributs structurés	292
Tableau 15 – Structure NLRoute_Struct.....	293
Tableau 16 – Structure Superframe_Struct	293
Tableau 17 – Structure Link_Struct.....	294
Tableau 18 – Structure Neighbour_Struct	295
Tableau 19 – Structure ChanCon_Struct.....	295
Tableau 20 – Structure Device_struct (1 de 3)	296
Tableau 21 – Structure VCR_Struct	299
Tableau 22 – Structure DevConRep_Struct.....	300
Tableau 23 – Structure Key_Struct	300
Tableau 24 – Structure ObjList_Struct	301
Tableau 25 – Paramètres de DMAP-MIB-GET.request	302
Tableau 26 – Paramètres de DMAP-MIB-GET.confirm	302
Tableau 27 – Paramètres de DMAP-MIB-SET.request	303
Tableau 28 – Paramètres de DMAP-MIB-SET.confirm.....	304
Tableau 29 – Sélection de protocoles PHY (1 de 2)	305
Tableau 30 – Bande de fréquence et débit de données.....	306
Tableau 31 – Affectations de fréquence	307
Tableau 32 – Attributs de PHY PIB	308
Tableau 33 – Sélection de protocoles MAC (1 of 3).....	311
Tableau 34 – Attributs PIB de la couche MAC.....	313
Tableau 35 – Attributs PIB étendus de la couche MAC	314
Tableau 36 – Charge utile de balise.....	314
Tableau 37 – Format du champ Capability Information (informations de capacité)	315
Tableau 38 – Mécanismes de saut.....	318
Tableau 39 – Transitions d'états de la sous-couche DLSE pour le rattachement d'appareil.....	324
Tableau 40 – Transitions d'états de la sous-couche DLSE pour l'exécution dans le réseau (1 de 3)	326
Tableau 41 – Paramètres de DLDE-DATA.request.....	330
Tableau 42 – Paramètres de DLDE-DATA.confirm	331
Tableau 43 – Tableau pour Status (état)	331
Tableau 44 – Paramètres de DLDE-DATA.indication.....	332
Tableau 45 – Paramètres de DLME-DISCOVERY.request.....	334
Tableau 46 – Paramètres de DLME- DISCOVERY.confirm.....	335
Tableau 47 – Network descriptor list (liste de descripteurs de réseau)	335
Tableau 48 – Paramètres de DLME-JOIN.request.....	337
Tableau 49 – Paramètres de DLME-JOIN.indication.....	337
Tableau 50 – Paramètres de DLME-JOIN.response	338
Tableau 51 – Paramètres de DLME-JOIN.confirm	338
Tableau 52 – Paramètres de DLME-LEAVE.request.....	339
Tableau 53 – Paramètres de DLME-LEAVE.indication	339
Tableau 54 – Paramètres de DLME-LEAVE.confirm.....	340
Tableau 55 – Paramètres de DLME-CHANNEL-CONDITION.indication	340

Tableau 56 – Paramètres de DLME-NEIGHBOUR-INFO.indication	341
Tableau 57 – Paramètres de DLME-COMM-STATUS.indication	341
Tableau 58 – Paramètres de DLME -KEEP-LIVE.confirm	342
Tableau 59 – Paramètres de DLME -KEEP-LIVE.indication.....	342
Tableau 60 – Paramètres de DLME-TIME-SYN.request	343
Tableau 61 – Paramètres de DLME -TIME-SYN.confirm	343
Tableau 62 – Paramètres de DLME-TIME-SYN.indication	343
Tableau 63 – Champ DLSL frame control (contrôle de trame DLSL).....	344
Tableau 64 – Format de trame de données	345
Tableau 65 – Format général d'une trame de commande	345
Tableau 66 – Trame de commande DLSL	346
Tableau 67 – Format de la trame de commande d'entretien	346
Tableau 68 – Format de la trame de commande de synchronisation du temps	347
Tableau 69 – Exemple de table de routage	350
Tableau 70 – Transitions d'états de la NL (1 de 4)	352
Tableau 71 – Paramètres de NLDE-DATA.request	357
Tableau 72 – Paramètres de NLDE-DATA.confirm	358
Tableau 73 – Paramètres de NLDE-DATA.indication	358
Tableau 74 – Paramètres de NLLME-COMM-STATUS.indication	360
Tableau 75 – Paramètres de NLME-COMM-STATUS.indication	361
Tableau 76 – Paramètres de NLME-COMM-STATUS.confirm.....	361
Tableau 77 – Paramètres de NLME-JOIN.request	362
Tableau 78 – Paramètres de NLME-JOIN.indication.....	363
Tableau 79 – Paramètres de NLME-JOIN.response	363
Tableau 80 – Paramètres de NLME-JOIN.confirm	364
Tableau 81 – Paramètres de NLME-LEAVE.request.....	368
Tableau 82 – Paramètres de NLME-LEAVE.indication	368
Tableau 83 – Paramètres de NLME-LEAVE.response	369
Tableau 84 – Paramètres de NLME-LEAVE.confirm	369
Tableau 85 – Paramètres de NLME-RPT-CLRMEM.request	374
Tableau 86 – Paramètres de NLME-RPT-CLRMEM.confirm	374
Tableau 87 – Paramètres de NLME-RPT-CLRMEM.response	375
Tableau 88 – Paramètres de NLME-NEIGHBOUR-INFO.request.....	377
Tableau 89 – Paramètres de NLME-NEIGHBOUR-INFO.confirm	377
Tableau 90 – Paramètres de NLME-ADD_ROUTE.request.....	378
Tableau 91 – Paramètres de NLME-ADD_ROUTE.confirm	379
Tableau 92 – Paramètres de NLME-UPDATE_ROUTE.request	380
Tableau 93 – Paramètres de NLME-UPDATE-ROUTE.confirm	381
Tableau 94 – Paramètres de NLME-UPDATE_ROUTE.request	382
Tableau 95 – Paramètres de NLME-DELETE-ROUTE.confirm.....	383
Tableau 96 – Paramètres de NLME-ADD-LINK.request.....	385
Tableau 97 – Paramètres de NLME-ADD-LINK.confirm	386
Tableau 98 – Paramètres de NLME-UPDATE-LINK.request	389

Tableau 99 – Paramètres de NLME-UPDATE-LINK.confirm	389
Tableau 100 – Paramètres de NLME-RELEASE-LINK.request	392
Tableau 101 – Paramètres de NLME-RELEASE-LINK.confirm	392
Tableau 102 – Paramètres de NLME-ADD-SFR.request.....	395
Tableau 103 – Paramètres de NLME-ADD-SFR.confirm.....	395
Tableau 104 – Paramètres de NLME-UPDATA-SFR.request	398
Tableau 105 – Paramètres de NLME-UPDATE-SFR.confirm	398
Tableau 106 – Paramètres de NLME-RELEASE-SFR.request	401
Tableau 107 – Paramètres de NLME-RELEASE-SFR.confirm	401
Tableau 108 – Paramètres de NLME-AGG.indication	404
Tableau 109 – Paramètres de NLME-AGO-SEND.request.....	404
Tableau 110 – Paramètres de NLME-DAG.indication	405
Tableau 111 – Paramètres de NLME-DEVICE-STATUS.request	405
Tableau 112 – Paramètres de NLME-DEVICE-STATUS.indication	405
Tableau 113 – Paramètres de NLME-DEVICE-STATUS.confirm.....	406
Tableau 114 – Paramètres de NLME-CHANNEL-CONDITION.request	407
Tableau 115 – Paramètres de NLME-CHANNEL-CONDITION.indication	408
Tableau 116 – Paramètres de NLME-CHANNEL-CONDITION.confirm	408
Tableau 117 – Paramètres de NLME-PATH_FAILURE.request	410
Tableau 118 – Paramètres de NLME-PATH_FAILURE.indication	410
Tableau 119 – Paramètres de NLME-PATH_FAILURE.confirm.....	411
Tableau 120 – Paramètres de NLME-INFO_GET.request.....	412
Tableau 121 – Paramètres de NLME-INFO_GET.indication	413
Tableau 122 – Paramètres de NLME-INFO_GET.response	414
Tableau 123 – Paramètres de NLME-INFO_GET.confirm.....	415
Tableau 124 – Paramètres de NLME-INFO_SET.request.....	416
Tableau 125 – Paramètres de NLME-INFO_SET.indication.....	416
Tableau 126 – Paramètres de NLME-SET.response	417
Tableau 127 – Paramètres de NLME-SET.confirm	418
Tableau 128 – Format commun des paquets de couche réseau	418
Tableau 129 – Format du champ Control (contrôle).....	419
Tableau 130 – Format commun des paquets de données de couche réseau	420
Tableau 131 – Format de paquet agrégé.....	421
Tableau 132 – Format commun de paquet de commande NL	422
Tableau 133 – Paquet de commande de couche réseau	422
Tableau 134 – Résultats d'exécution des commandes	423
Tableau 135 – Format du paquet de demande de rattachement	424
Tableau 136 – Format du paquet de réponse de rattachement.....	424
Tableau 137 – Format du paquet de demande de rapport sur l'état des communications	425
Tableau 138 – Format du paquet de demande de départ	425
Tableau 139 – Valeur du champ Leaving reason (raison du départ)	426
Tableau 140 – Format du paquet de réponse de départ	426
Tableau 141 – Format du paquet de demande de rapport sur l'élément de groupe	426

Tableau 142 – Format du paquet de réponse de rapport sur l'élément de groupe.....	427
Tableau 143 – Format du paquet de demande de rapport sur les informations de voisins	427
Tableau 144 – Format du paquet de demande d'ajout d'itinéraire.....	428
Tableau 145 – Format du paquet de réponse d'ajout d'itinéraire	428
Tableau 146 – Format du paquet de demande de mise à jour d'itinéraire	429
Tableau 147 – Format du paquet de réponse de mise à jour d'itinéraire	429
Tableau 148 – Format du paquet de demande de suppression d'itinéraire	429
Tableau 149 – Format du paquet de réponse de suppression d'itinéraire	430
Tableau 150 – Format du paquet de demande d'ajout de liaison	430
Tableau 151 – Format du paquet de réponse d'ajout de liaison	431
Tableau 152 – Format du paquet de demande de mise à jour de liaison	431
Tableau 153 – Format du paquet de réponse de mise à jour de liaison	432
Tableau 154 – Format du paquet de demande de libération de liaison	432
Tableau 155 – Format du paquet de réponse de libération de liaison	433
Tableau 156 – Format du paquet de demande d'ajout de supertrame.....	433
Tableau 157 – Format du paquet de réponse d'ajout de supertrame	434
Tableau 158 – Format du paquet de demande de mise à jour de supertrame	434
Tableau 159 – Format du paquet de réponse de mise à jour de supertrame.....	434
Tableau 160 – Format du paquet de demande de libération de supertrame.....	435
Tableau 161 – Format du paquet de réponse de libération de supertrame	435
Tableau 162 – Format du paquet de demande de rapport sur la condition des appareils	436
Tableau 163 – Format du champ d'informations sur la condition des appareils.....	436
Tableau 164 – Format du paquet de demande de rapport sur la condition des canaux	437
Tableau 165 – Format du champ d'informations sur la qualité des canaux	438
Tableau 166 – Format du paquet de demande de rapport sur la défaillance des chemins	438
Tableau 167 – Format du paquet de demande d'obtention d'attribut.....	439
Tableau 168 – Format du paquet de réponse d'obtention d'attribut	439
Tableau 169 – Format du paquet de demande d'établissement d'attribut.....	440
Tableau 170 – Format du paquet de réponse d'établissement d'attribut	441
Tableau 171 – Définition des méthodes pour les objets d'application utilisateur (UAO)	445
Tableau 172 – Format de demande de la méthode READ	445
Tableau 173 – Format de réponse de la méthode READ	445
Tableau 174 – Format de demande de la méthode WRITE.....	446
Tableau 175 – Format de réponse de la méthode WRITE	446
Tableau 176 – Format de la méthode PUBLISH	447
Tableau 177 – Format de la méthode REPORT.....	447
Tableau 178 – Format de la méthode REPORT ACK.....	448
Tableau 179 – Paramètres de ASLDE-DATA.request.....	449
Tableau 180 – Paramètres de ASLDE-DATA.confirm	450
Tableau 181 – Paramètres de ASLDE-DATA.indication.....	450
Tableau 182 – Paramètres de ASLDE-AGG.request	451
Tableau 183 – Paramètres de ASLDE-DAG.indication	451

Tableau 184 – Format de paquet général de la sous-couche application (ASL)	455
Tableau 185 – Format du champ contrôle de paquet	455
Tableau 186 – Valeur du sous-champ Packet type (type de paquet)	456
Tableau 187 – Format du paquet de données ASL	457
Tableau 188 – Format du paquet d'acquiescement ASL	458
Tableau 189 – Format d'une DLPDU de sécurité	462
Tableau 190 – Format de l'en-tête de sécurité DLSL	462
Tableau 191 – Structure du champ Security control (contrôle de sécurité) dans l'en-tête de sécurité DLSL	462
Tableau 192 – Structure du champ Security material control (contrôle des renseignements de sécurité) dans l'en-tête de sécurité DLSL	463
Tableau 193 – Structure d'une APDU de sécurité	463
Tableau 194 – Structure du champ ASL security header (en-tête de sécurité ASL)	463
Tableau 195 – Paramètres de DLME-SEC.request	468
Tableau 196 – Paramètres de DLME-SEC.indication	469
Tableau 197 – Paramètres de DLME-SEC.response	469
Tableau 198 – Paramètres de DLME-SEC.confirm	470
Tableau A.1 – Mesures de sécurité graduées et stratifiées pour réseau WIA-PA	478
Tableau A.2 – Niveaux de sécurité des paquets de données	478
Tableau B.1 – Format de paquet ou de trame en octet(s)	480
Tableau B.2 – Format des sous-champs en bit(s)	480
Tableau C.1 – Attribut de classe de l'AIO	481
Tableau C.2 – Attributs d'instance de l'AIO	482
Tableau E.1 – Liste des exigences applicables de l'EN 300 440-2	484
Tableau E.2 – Liste des exigences applicables de l'EN 300 328	485
Tableau E.3 – Définitions et calculs de la temporisation des intervalles de temps	485

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

RÉSEAUX INDUSTRIELS – RÉSEAU DE COMMUNICATIONS SANS FIL ET PROFILS DE COMMUNICATION – WIA-PA

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62601 a été établie par le sous-comité 65C: Réseaux industriels, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition parue en 2011. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- remplacement de l'IEEE 802.15.4-2006 par l'IEEE 802.15.4-2011 et ajout de modification commune pour les profils MAC et PHY de l'IEEE 802.15.4-2011 et les références relatives à l'IEEE 802.15.4-2011;
- ajout de modifications communes pour l'adoption régionale et ajout de l'Annexe D et de l'Annexe E;
- suppression des services de gestion MAC étendus et ajout de deux services de gestion DLSL;
- ajout de diagramme d'états spécifiques aux couches DLSL et NL;
- unification de la représentation du format de trame et du format de paquet;
- modification du format de définition des types de données;
- ajout d'une description détaillée des technologies pour une meilleure compréhension;
- fourniture d'un support pour les modes CCA 1, 2 et 3.

L'attention du lecteur est attirée sur le fait que l'Annexe E énumère tous les articles traitant des différences à caractère moins permanent inhérentes à certains pays, concernant le sujet de la présente norme.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
65C/821/FDIS	65C/833/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

RÉSEAUX INDUSTRIELS – RÉSEAU DE COMMUNICATIONS SANS FIL ET PROFILS DE COMMUNICATION – WIA-PA

1 Domaine d'application

La présente Norme internationale spécifie l'architecture système et le protocole de communication de réseaux sans fil pour automation industrielle – automation dans les processus (WIA-PA, *Wireless network for Industrial Automation – Process Automation*) exploitant la norme IEEE STD 802.15.4-2011.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 9899, *Information technology – Programming languages – C* (disponible en anglais seulement)

ISO 3166-1, *Codes pour la représentation des noms de pays et de leurs subdivisions – Partie 1: Codes de pays*

IEEE 802.15.4-2011, *IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)* (disponible en anglais seulement)

3 Termes, définitions et abréviations

3.1 Termes et définitions

3.1.1

nombre absolu d'intervalles de temps

nombre d'intervalles de temps depuis le démarrage du réseau, c'est-à-dire l'intervalle de temps courant en général

3.1.2

départ actif

processus par lequel un appareil de terrain en ligne peut quitter le réseau en souscrivant à son appareil de routage ou par lequel un appareil de routage en ligne peut quitter le réseau en souscrivant à un appareil de passerelle

3.1.3

saut de fréquence adaptatif

changement de canaux de communication en fonction de la condition réelle des canaux dans chaque intervalle de temps au cours de la période intragroupe de supertrame WIA-PA

3.1.4

commutation de fréquence adaptative

changement de canaux de communication en fonction de la condition réelle des canaux au cours de la trame balise et de la période active dans un cycle de supertrame et en utilisant des canaux différents dans des cycles de supertrames différents

3.1.5**agrégation**

fusion de données de multiples objets d'application utilisateur ou de plusieurs paquets d'éléments de groupe en un seul paquet

3.1.6**sous-couche application**

sous-couche de protocole qui fournit des données et des services de gestion pour la couche application

3.1.7**balise**

trame spéciale diffusée par les appareils de routage ou l'appareil de passerelle dans le réseau WIA-PA

3.1.8**diffusion**

envoi simultané d'un paquet à tous les appareils WIA-PA

3.1.9**canal**

support à fréquences radioélectriques utilisé pour acheminer un paquet d'un expéditeur vers un destinataire

3.1.10**groupe**

groupe logique d'appareils qui est constitué d'un appareil de routage et d'appareils de terrain

3.1.11**tête de groupe**

gestionnaire dans un groupe, joué par l'appareil de routage

3.1.12**élément de groupe**

source de données dans un groupe, jouée par un appareil de terrain

3.1.13**coexistence**

aptitude d'un réseau à accomplir sa tâche dans un environnement partagé donné sans perturber les autres réseaux ni être perturbé par d'autres réseaux

Note 1 à l'article: Ces réseaux peuvent ou peuvent ne pas avoir le même ensemble de règles.

3.1.14**ressource de communication**

ensemble des canaux et des intervalles de temps utilisés pour transporter une trame

3.1.15**logiciel de configuration WIA-PA**

outil logiciel pour configurer le réseau et les appareils WIA-PA

3.1.16**sous-couche liaison de données**

couche supérieure de la couche MAC de l'IEEE 802.15.4-2011, utilisée pour gérer les aspects relatifs à la topologie de réseau et aux ressources de communication dans le réseau WIA-PA

3.1.17

désagrégation

division du paquet fusionné en données d'objets d'application utilisateur

3.1.18

appareil de terrain

appareil utilisable sur le terrain, qui est relié au processus ou commande celui-ci

3.1.19

trame

format de bits agrégés à partir de l'entité de contrôle d'accès au support (MAC) qui sont émis ensemble simultanément

[SOURCE: IEEE 802.15.4-2011]

3.1.20

saut de fréquence

changement de fréquence d'émission/réception pour combattre les interférences et l'évanouissement

3.1.21

appareil de passerelle

appareil reliant le réseau WIA-PA à des réseaux d'autres installations

3.1.22

appareil tenu à la main

appareil portatif utilisé pour le dimensionnement, la mise à jour de firmware et la surveillance des états des appareils

3.1.23

saut

mouvement d'un paquet directement entre deux appareils voisins dans une transaction de réseau sans la participation d'aucun autre appareil du réseau WIA-PA

Note 1 à l'article: Plusieurs sauts sont utilisés pour allonger la distance d'émission, contourner les sources d'interférences ou éviter les obstacles.

3.1.24

ordinateur de configuration d'hôte

appareil par lequel les utilisateurs et le personnel d'entretien/de gestion accomplissent des transactions sur le réseau WIA-PA et les réseaux de gestion

3.1.25

interconnectable

utilisant les mêmes protocoles de communication, interface de communication et accès aux données

3.1.26

interopérables

capables de fonctionner ensemble pour accomplir un rôle spécifique dans un ou plusieurs programmes d'application distribués

Note 1 à l'article: Dans ce cas, les paramètres et leurs fonctionnalités applicatives s'ajustent à la fois de manière syntaxique et sémantique. L'interopérabilité est accomplie lorsque les appareils prennent en charge des ensembles complémentaires de paramètres et fonctions appartenant au même profil.

3.1.27**interopérabilité**

aptitude de deux ou plusieurs systèmes de réseau pour échanger des informations et faire une utilisation mutuelle des informations qui ont été échangées

[Cette source n'existe que dans la langue anglaise]

3.1.28**rattachement**

processus par lequel un appareil WIA-PA est authentifié et autorisé à participer au réseau WIA-PA

3.1.29**liaison**

ensemble de paramètres de communication nécessaires pour transporter une trame entre des appareils voisins dans le réseau

Note 1 à l'article: Elle inclut l'adresse de la source/destination, l'intervalle de temps, le canal, la direction et le type de liaison.

3.1.30**maille**

topologie formée par des appareils de routage et l'appareil de passerelle dans le réseau WIA-PA

Note 1 à l'article: Un même appareil de routage peut se relier à l'appareil de passerelle et à plus d'un appareil de routage.

3.1.31**multidiffusion**

envoi simultané d'un paquet à un groupe d'appareils WIA-PA

3.1.32**adresse réseau****adresse courte**

nombre entier non signé de 16 bits identifiant de façon univoque l'appareil dans le réseau WIA-PA

Note 1 à l'article: Les 8 bits de poids fort de l'adresse réseau, assignée par le gestionnaire de réseau, identifient les différents groupes

3.1.33**gestionnaire de réseau**

rôle logique pour configurer le réseau, attribuer les ressources de communication, gérer les tables de routage, et surveiller et rapporter la santé du réseau

3.1.34**paquet**

bits agrégés et formatés qui sont émis ensemble simultanément à travers le support physique

[SOURCE: IEEE 802.15.4-2011, 3.31]

3.1.35**cycle de vie de paquet**

durée maximale de survie d'un paquet depuis sa création jusqu'à son abandon

3.1.36

départ passif

processus par lequel un appareil de terrain en ligne est enjoint de quitter le réseau par son appareil de routage ou par lequel un appareil de routage en ligne est enjoint de quitter le réseau par l'appareil de passerelle

3.1.37

adresse physique

adresse longue

bits de format EUI-64 identifiant de façon univoque l'appareil dans le réseau WIA-PA

Note 1 à l'article: Une adresse physique est assignée par un fabricant.

3.1.38

appareil de routage

appareil transmettant des paquets d'un appareil WIA-PA à un autre dans le réseau WIA-PA

3.1.39

gestionnaire de sécurité

rôle logique pour configurer les stratégies de sécurité du réseau tout entier, gérer les clés et authentifier les appareils

3.1.40

supertrame

collection d'intervalles de temps se répétant au fil du temps

Note 1 à l'article: Elle spécifie le temps d'émission ou de réception de la communication périodique.

3.1.41

intervalle de temps

unité temporelle de base pour l'échange de données

Note 1 à l'article: Sa durée est configurable dans le réseau WIA-PA.

3.1.42

saut d'intervalle de temps

changement régulier de la fréquence d'émission/réception par intervalle de temps pour éviter les interférences et l'évanouissement

3.1.43

monodiffusion

envoi d'un paquet vers un seul appareil dans le réseau WIA-PA

3.1.44

relation de communication virtuelle

chemins de communication et ressources de communication entre deux objets d'application utilisateur

3.1.45

appareil WIA-PA

appareil dans le réseau WIA-PA

EXEMPLE: Ordinateur de configuration d'hôte, appareil de passerelle, appareil de routage, appareil de terrain ou appareil tenu à la main.

3.2 Abréviations

ACK	Acknowledge (acquitter)
AFH	Adaptive Frequency Hopping (saut de fréquence adaptatif)
AFS	Adaptive Frequency Switch (commutation de fréquence adaptative)
AIO	Analog Input Object (objet d'entrée analogique)
AL	Application Layer (couche application)
AOO	Analog Output Object (objet de sortie analogique)
ASDU	Application Service Data Unit (unité de données de service application)
ASL	Application Sub-Layer (sous-couche application)
ASLDE	Application Sub-Layer Data Entity (entité de données de sous-couche application)
ASLDE-SAP	ASLDE Service Access Point (point d'accès au service ASLDE)
ASLME	Application Sub-Layer Management Entity (entité de gestion de sous-couche application)
ASLME-SAP	ASLME Service Access Point (point d'accès au service ASLME)
ASLPDU	Application Sub-Layer Protocol Data Unit (unité de données de protocole de sous-couche application)
ASN	Absolute timeSlot Number (nombre absolu d'intervalles de temps)
CAP	Contention Access Period (période d'accès avec conflit)
CFP	Contention Free Period (période sans conflit)
C/S	Client/Server (client/serveur)
CSMA	Carrier Sense Multiple Access (accès multiple par détection de porteuse)
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance (accès multiple par détection de porteuse et évitement de collision)
DAGO	Data AggreGation Object (objet d'agrégation de données)
DGO	DisaGgregation Object (objet de désagrégation)
DIO	Digital Input Object (objet d'entrée numérique)
DLDE	Data Link Sub-Layer Data Entity (entité de données de sous-couche liaison de données)
DLDE-SAP	DLDE Service Access Point (point d'accès au service DLDE)
DLL	Data Link Layer (couche liaison de données)
DLME	Data Link Sub-Layer Management Entity (entité de gestion de sous-couche liaison de données)
DLME-SAP	DLME Service Access Point (point d'accès au service DLME)
DLPDU	Data Link Sub-Layer Protocol Data Unit (unité de données de protocole de sous-couche liaison de données)
DLSL	Data Link Sub-Layer (sous-couche liaison de données)
DMAP	Device Management Application Process (processus d'application de gestion de l'appareil)
DOO	Digital Output Object (objet de sortie numérique)
EIRP	Equivalent Isotropic Radiated Power (puissance isotrope rayonnée équivalente)
ENC	ENCryption (chiffrement)
EUI-64	Extended Unique Identifier-64 bits (identificateur unique étendu de 64 bits)
FCS	Frame Check Sequence (séquence de contrôle de trame)

AMRF	FDMA, Frequency Division Multiple Access (accès multiple par répartition en fréquence)
FFD	Full-Function Device (appareil pleinement fonctionnel)
SF	FH, Frequency Hopping (saut de fréquence)
GTS	Guaranteed Time Slot (intervalle de temps garanti)
GW	GateWay device (appareil de passerelle)
ID	IDentifier (IDentificateur)
IDS	Intrusion Detection System (système de détection des intrusions)
KED	Data Encryption Key (clé de chiffrement de données)
KEK	Key Encryption Key (clé de chiffrement de clé)
KJ	Join Key (clé de rattachement)
KS	Share Key (clé de partage)
LME-SAP	Layer Management Entity Service Access Point (point d'accès au service d'entité de gestion de couche)
LSB	Least Significant Bit (bit de poids faible)
LQI	Link Quality Indication (indication de qualité de liaison)
MAC	Medium Access Control sub-layer (sous-couche contrôle d'accès au support)
MCPS	MAC Common Part Sub-layer (sous-couche partie commune de la couche MAC)
MHR	Medium Access Control Header (en-tête de contrôle d'accès au support)
MIB	Management Information Base (base d'informations de gestion)
MIC	Message Integrity Code (code d'intégrité de message)
MLDE	MAC sub-Layer Data Entity (entité de données de sous-couche MAC)
MLDE-SAP	MLDE Service Access Point (point d'accès au service MLDE)
MLME	MAC sub-Layer Management Entity (entité de gestion de sous-couche MAC)
MLME-SAP	MLME Service Access Point (point d'accès au service MLME)
MPDU	MAC Protocol Data Unit (unité de données de protocole MAC)
MSB	Most Significant Bit (bit de poids fort)
NL	Network Layer (couche réseau)
NLDE	Network Layer Data Entity (entité de données de couche réseau)
NLDE-SAP	NLDE Service Access Point (point d'accès au service NLDE)
NLME	Network Layer Management Entity (entité de gestion de couche réseau)
NLME-SAP	NLME Service Access Point (point d'accès au service NLME)
NM	Network Manager (gestionnaire de réseau)
NPDU	Network Protocol Data Unit (unité de données de protocole réseau)
NSDU	Network Service Data Unit (unité de données de services réseau)
PAGO	Packet AGgregation Object (objet d'agrégation de paquets)
PAN	Personal Area Network (réseau local personnel)
PHY	PHYsical layer (couche physique)
PIB	PAN Information Base (base d'informations de PAN)
P/S	Publisher/Subscriber (éditeur/abonné)
RFD	Reduced-Function Device (appareil à fonctions limitées)
R/S	Report source/Sink (source/puits de rapports)
SAP	Service Access Point (point d'accès au service)
SM	Security Manager (gestionnaire de sécurité)

AMRT	TDMA, Time Division Multiple Access (accès multiple par répartition dans le temps)
TH	Timeslot Hopping (saut d'intervalle de temps)
UAO	User Application Object (objet d'application utilisateur)
UAP	User Application Process (processus d'application utilisateur)
UAPME-SAP	UAP Management Entity SAP (point d'accès au service d'entité de gestion UAP)
TUC	UTC, Universal Time Coordinated (temps universel coordonné)
VCR	Virtual Communication Relationship (relation de communication virtuelle)
VCR_ID	Virtual Communication Relationship IDentifier (IDentificateur de relation de communication virtuelle)
WIA-PA	Wireless network for Industrial Automation – Process Automation (réseau sans fil pour automation industrielle – automation dans les processus)

4 Définition des types de données

Le Tableau 1 présente la définition WIA-PA des types de données.

Tableau 1 – Définition des types de données

Définition des types de données (voir ISO/IEC 9899)			
Type de données		Plage de valeurs	Length
Booléen	Boolean	Non 0: TRUE; 0: FALSE	1 octet
Entier non signé	Unsigned8	$0 \leq i \leq 2^8-1$	1 octet
	Unsigned16	$0 \leq i \leq 2^{16}-1$	2 octets
	Unsigned24	$0 \leq i \leq 2^{24}-1$	3 octets
	Unsigned32	$0 \leq i \leq 2^{32}-1$	4 octets
	Unsigned40	$0 \leq i \leq 2^{40}-1$	5 octets
	Unsigned48	$0 \leq i \leq 2^{48}-1$	6 octets
	Unsigned64	$0 \leq i \leq 2^{64}-1$	8 octets
Chaîne d'octets	Octetstring	Chaîne de 8 bits	1 octet
Nombre réel simple	Float	Voir l'IEC 60559	4 octets

5 Aperçu de WIA-PA

5.1 Types d'appareils

Le document spécifie cinq types d'appareils WIA-PA:

- ordinateur de configuration d'hôte;
- appareil de passerelle (GW);
- appareil de routage;
- appareil de terrain;
- appareil tenu à la main.

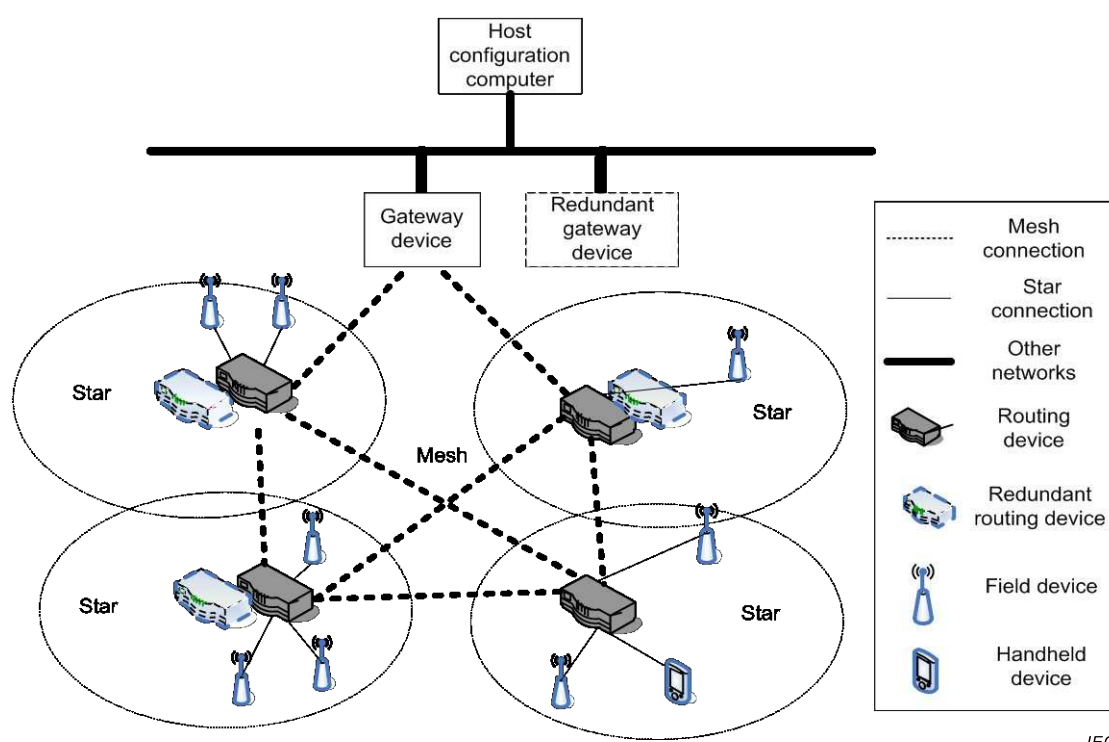
Pour améliorer la fiabilité, le réseau WIA-PA peut comporter des appareils de passerelle et des appareils de routage redondants. Un appareil principal connecte son appareil redondant à l'aide d'un câble. La connexion câblée n'est pas définie dans le présent document. L'adresse courte (voir 6.3.4) d'un appareil redondant est la même que celle de l'appareil principal. Le temps de démarrage d'un appareil redondant n'est pas plus long que celui de l'appareil principal. Lorsque l'appareil principal fonctionne, les appareils redondants ne démarrent pas leurs modules radio. Lorsque les informations relatives aux appareils principaux sont modifiées, il convient que ces derniers sauvegardent rapidement les informations modifiées sur leurs appareils redondants via une connexion câblée. La connexion câblée n'est pas spécifiée dans le présent document. Si SecEnableFlag est activée, les appareils redondants sont authentifiés (voir 11.2).

5.2 Topologie de réseau

Le réseau WIA-PA prend en charge deux types différents de topologies de réseau:

- a) une topologie de réseau hiérarchique qui est la combinaison de la configuration en étoile et de la configuration maillée;
- b) une topologie de réseau en étoile uniquement.

La topologie de réseau hiérarchique qui est la combinaison de la configuration en étoile et de la configuration maillée est représentée à la Figure 1. Le premier niveau du réseau est en topologie maillée, dans laquelle des appareils de routage et des appareils de passerelle sont déployés. Le second niveau du réseau est en topologie en étoile, dans laquelle des appareils de routage, des appareils de terrain et des appareils tenus à la main (le cas échéant) sont déployés.

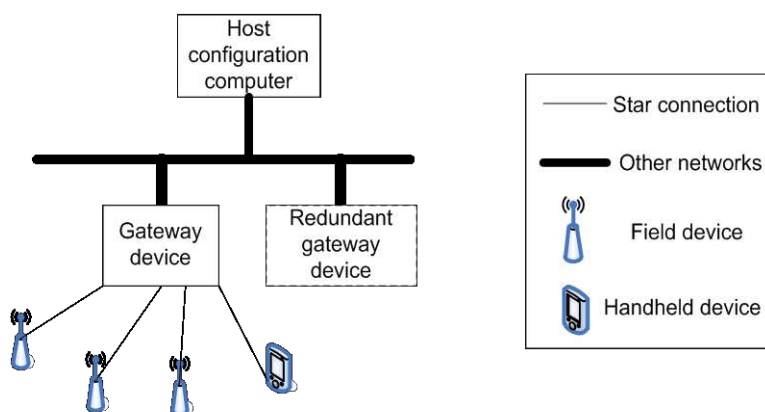


IEC

Anglais	Français
Host configuration computer	Ordinateur de configuration d'hôte
Gateway device	Appareil passerelle
Redundant gateway device	Appareil passerelle redondant
Star	Etoile
Mesh	Maille
Mesh connection	Connexion maillée (polygonale)
Star connection	Connexion en étoile
Other networks	Autres réseaux
Routing device	Appareil de routage
Redundant routing device	Appareil de routage redondant
Field device	Appareil de terrain
Handheld device	Appareil tenu à la main

Figure 1 – Exemple de topologie physique WIA-PA (combinaison de la configuration en étoile et de la configuration maillée)

Le réseau en étoile uniquement est composé d'un appareil de passerelle, d'appareils de terrain et d'appareils tenus à la main (le cas échéant). La topologie de réseau en étoile est représentée à la Figure 2.



IEC

Anglais	Français
Host configuration computer	Ordinateur de configuration d'hôte
Gateway device	Appareil passerelle
Redundant gateway device	Appareil passerelle redondant
Star connection	Connexion en étoile
Other networks	Autres réseaux
Field device	Appareil de terrain
Handheld device	Appareil tenu à la main

Figure 2 – Exemple de topologie physique WIA-PA (en étoile uniquement)

Le réseau en étoile uniquement représente un cas particulier du réseau hiérarchique. Dans le présent document, la spécification du réseau hiérarchique couvre le réseau en étoile uniquement. Par conséquent, aucune spécification explicite fournie pour le réseau en étoile uniquement n'est disponible.

Afin de faciliter la gestion, le présent document spécifie cinq rôles logiques.

a) Passerelle

La passerelle gère la conversion de protocole et le mapping des données entre le réseau WIA-PA et les autres réseaux.

b) Gestionnaire de réseau

Le gestionnaire de réseau (NM) gère et surveille la totalité du réseau (voir 6.2). Dans un réseau WIA-PA, il convient qu'il n'y ait qu'un seul gestionnaire de réseau.

c) Gestionnaire de sécurité

Le gestionnaire de sécurité (SM) traite de la gestion des clés de sécurité et de l'authentification de la sécurité des appareils de passerelle, de routage, de terrain et tenus à la main (le cas échéant).

d) Tête de groupe

La tête de groupe gère et surveille les appareils de terrain et tenus à la main (le cas échéant). De plus, elle fusionne et transmet en toute sécurité des paquets provenant d'éléments de groupe locaux et d'autres têtes de groupe.

e) Élément de groupe

L'élément de groupe recueille des données de terrain et les envoie à sa tête de groupe.

Il convient que le gestionnaire de réseau (NM) et le gestionnaire de sécurité (SM) qui sont utilisés pour la gestion du système résident dans un appareil de passerelle.

Un même appareil physique peut accomplir les fonctions de plusieurs rôles logiques. Dans le réseau hiérarchique qui est la combinaison de la configuration en étoile et de la configuration maillée, un appareil de passerelle peut endosser les rôles logiques de passerelle, NM, SM et tête de groupe. Il convient qu'un appareil de routage doit agir comme tête de groupe. Il convient qu'un appareil de terrain/tenu à la main agisse uniquement comme élément de groupe.

L'appareil principal et l'appareil redondant sont marqués par le paramètre RedundantDevFlag dans le Tableau 20.

5.3 Architecture de protocole

L'architecture de protocole WIA-PA, représentée à la Figure 3, est issue de la norme ISO/IEC 7498-1. Elle définit la sous-couche Liaison de données (DLSL), la couche Réseau (NL) et la couche Application (AL), alors que sa couche PHYsique (PHY) et sa sous-couche Contrôle d'accès au support (MAC) sont basées sur la norme IEEE STD 802.15.4-2011.

OSI layer	Function	WIA-PA
Application	Provides the user with network capable application	AL (Provides the user with network capable application)
Presentation	Converts application data between network and local machine formats	↑
Session	Connection management services for applications	
Transport	Provides network independent, transparent message transfer	↑ or ↓
Network	End- to- end routing of packets. resolving network addresses	NL (Power-optimized redundant path, star and mesh networking)
Data link	Establishes data packet structure, framing, error detection, bus arbitration	DLSL (Hybrid CSMA and TDMA, AFS, AFH, TH)
		IEEE STD 802.15.4-2011 MAC
Physical	Mechanical / electrical connection. Transmits raw bit stream	PHY (IEEE STD 802.15.4-2011-based radios)

IEC

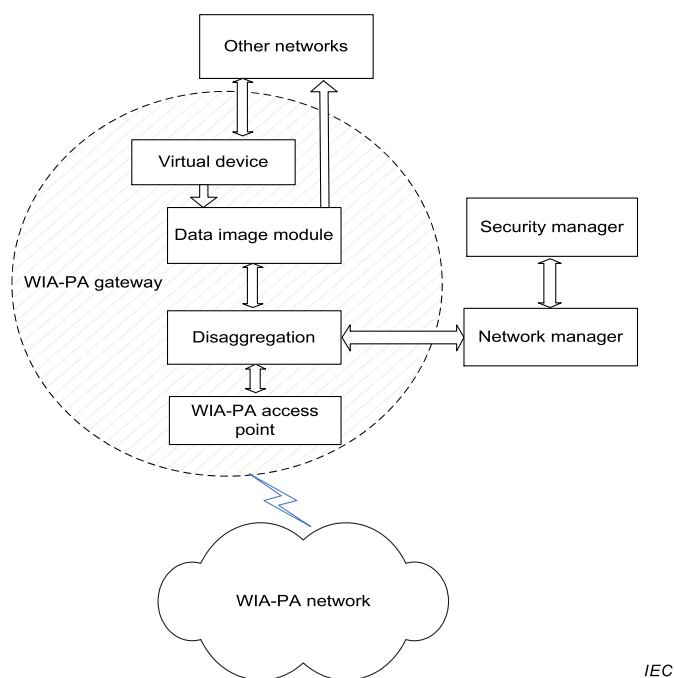
Anglais	Français
OSI layer	Couche OSI
Function	Fonction
WIA-PA	WIA-PA
Application	Application
Provides the user with network capable application	Fournit à l'utilisateur une application avec capacité réseau
or	ou
AL (Provides the user with network capable application)	AL (Fournit à l'utilisateur une application avec capacité réseau)
Presentation	Présentation
Converts application data between network and local machine formats	Convertit les données d'application entre les formats réseau et machine locale
Session	Session
Connection management services for applications	Services de gestion de connexion pour applications
Transport	Transport
Provides network independent, transparent message transfer	Fournit un transfert de messages transparent, indépendant du réseau
Network	Réseau
End-to-end routing of packets, resolving network addresses	Routage de bout en bout de paquets, résolution des adresses réseau
NL (Power-optimized redundant path, star and mesh networking)	NL (chemin redondant optimisé en puissance, connexion réseau en étoile et maillée)
Data link	Liaison de données
Establishes data packet structure, framing, error detection, bus arbitration	Etablit une structure de données en paquet, le verrouillage de trame, la détection d'erreur et le contrôle d'accès au bus
DLSL (Hybrid CSMA and TDMA, AFS, AFH, TH)	DLSL (hybride CSMA et AMRT, AFS, AFH, TH)
IEEE STD 802.15.4-2011 MAC	MAC selon l'IEEE 802.15.4-2011
Physical	Physique
Mechanical/electrical connection. Transmits raw bit stream	Connexion mécanique/électrique. Emission d'un flux binaire brut

Anglais	Français
PHY (IEEE STD 802.15.4-2011-based radios)	PHY (équipements radioélectriques basés sur l'IEEE 802.15.4-2011)

Figure 3 – Modèle de référence OSI de base mappé au réseau WIA-PA

5.4 Interconnexions

Le réseau WIA-PA interconnecte avec les autres réseaux par l'intermédiaire de la passerelle WIA-PA. Outre la communication avec le NM et le SM du réseau WIA-PA, la passerelle WIA-PA peut communiquer avec d'autres appareils du réseau WIA-PA afin d'échanger des informations entre les appareils. Par ailleurs, la passerelle WIA-PA peut connecter d'autres réseaux, tels que les bus de terrain câblés. L'architecture de la passerelle WIA-PA est indiquée à la Figure 4.



IEC

Anglais	Français
Other networks	Autres réseaux
Virtual device	Appareil virtuel
Data image module	Module d'image de données
WIA-PA gateway	Passerelle WIA-PA
Security manager	Gestionnaire de sécurité (SM)
Disaggregation	Désagrégation
Network manager	Gestionnaire de réseau (NM)
WIA-PA access point	Point d'accès WIA-PA
WIA-PA network	Réseau WIA-PA

Figure 4 – Architecture de passerelle WIA-PA

La passerelle WIA-PA comporte les composants suivants.

a) Point d'accès WIA-PA

Le point d'accès WIA-PA réalise les connexions physiques du réseau WIA-PA et la transmission des informations et données de gestion.

b) Appareil virtuel

L'appareil virtuel définit une interface de communication avec d'autres réseaux. L'interface est utilisée pour mapper une source de données d'autres réseaux à un appareil WIA-PA afin d'établir la communication entre le réseau WIA-PA et d'autres réseaux.

c) **Objet désagrégation**

Cet objet est utilisé pour désagréger les paquets, qui sont agrégés dans des appareils de routage et des appareils de terrain.

d) **Module d'image de données**

Le module d'image de données sauvegarde les données des appareils dans le réseau WIA-PA et fournit une interface d'accès pour d'autres réseaux.

L'appareil virtuel et le module d'image de données sont facultatifs et spécifiques à la mise en œuvre et ne sont pas définis dans le présent document.

6 Gestion de système

6.1 Généralités

La gestion de système dans le réseau WIA-PA comprend à la fois la gestion de réseau et la gestion de la sécurité. Les fonctions de la gestion du système sont mises en œuvre par le processus d'application de gestion d'appareil (DMAP) dans chaque appareil. Le processus DMAP, en tant qu'entité de gestion de système, comprend le module de gestion de réseau, le module de gestion de la sécurité et le module de base d'informations de gestion (MIB). Le processus DMAP est représenté par la zone grise dans la Figure 5. Les blocs blancs dans la zone grise sont les composants fonctions dans le processus DMAP.

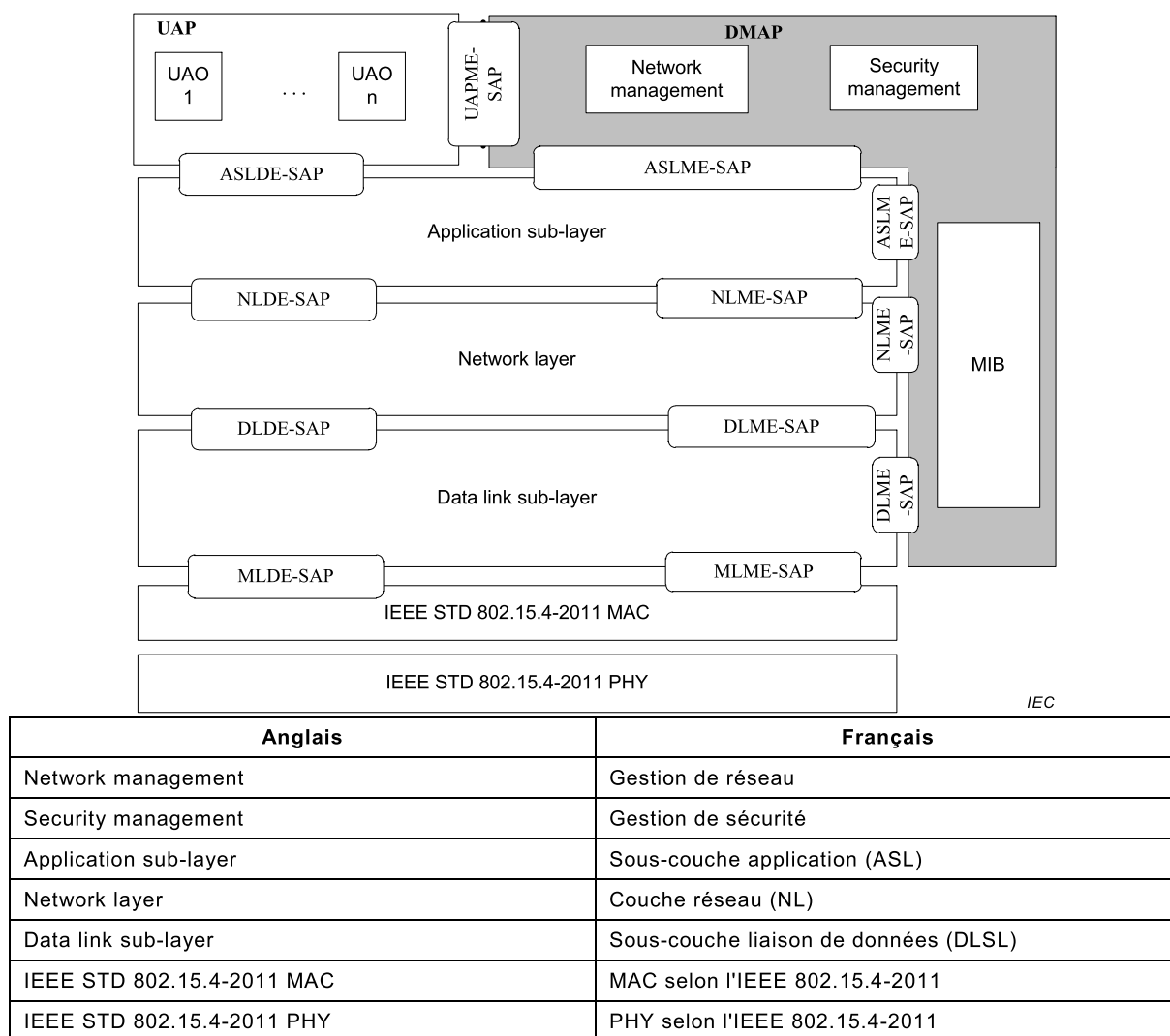


Figure 5 – Processus DMAP dans la gestion du système

La gestion de réseau spécifie la gestion d'attributs d'appareils et d'attributs qui sont relatifs à la communication et à la configuration du réseau. Les fonctions de gestion de réseau sont accomplies par les processus DMAP du NM, des têtes de groupe et des éléments de groupe. Les fonctions de gestion de réseau comprennent les actions suivantes.

a) Rattachement au réseau et départ du réseau

Il convient qu'un appareil de routage soit rattaché au réseau ou le quitte par le biais de l'appareil de passerelle ou d'un appareil de routage en ligne. Il convient qu'un appareil de terrain soit rattaché au réseau ou le quitte par l'intermédiaire d'un appareil de routage en ligne ou de l'appareil de passerelle. Il convient que le nouvel appareil de rattachement soit authentifié par le SM.

b) Attribution d'adresse réseau

Chaque appareil dans le réseau WIA-PA possède une adresse avec identificateur unique étendu de 64 bits (EUI-64) et une adresse réseau de 16 bits. L'adresse EUI-64 est également appelée adresse longue. L'adresse longue de chaque appareil est assignée par les fournisseurs conformément à l'adresse EUI-64 de l'IEEE. L'adresse réseau de 16 bits est également appelée adresse courte. L'adresse courte de chaque appareil de réseau est assignée par le NM.

c) Configuration de routage

Le routage statique est mis en œuvre dans le réseau WIA-PA. La table de routage dans chaque appareil de routage est configurée par le NM.

d) Configuration des ressources de communication

Les ressources de communication du réseau WIA-PA sont organisées comme supertrames (voir 8.4.4). Lorsqu'un appareil de routage a réussi à se rattacher au réseau, il convient que des ressources de communication lui soient affectées par le NM. Une fois qu'un appareil de terrain a réussi à se rattacher à un groupe, il convient que la tête de groupe lui affecte des ressources de communication.

e) Configuration de la source temporelle et services de temps système

Le réseau WIA-PA établit une seule source de temps de base, qui est accomplie par l'appareil de passerelle. Afin de reconnaître l'ordre des événements qui surviennent, les appareils WIA-PA se synchronisent relativement à l'appareil de passerelle.

f) Surveillance de performance

La surveillance de performance permet de recueillir la performance du réseau WIA-PA, qui inclut l'état des appareils, la défaillance de chemin et la condition des canaux.

g) Maintenance de la MIB

Il convient que le module MIB configure la MIB (base d'informations de gestion) de la pile de protocole du réseau WIA-PA.

h) Interfaces pour le personnel d'exploitation et de maintenance

Il convient que le NM fournisse une interface pour permettre au personnel d'exploitation et de maintenance de surveiller et contrôler la performance et les activités du réseau et des appareils. La définition de cette interface ne relève pas du domaine d'application de la présente norme WIA-PA.

i) Mise à niveau du firmware

Il convient que la mise à niveau du firmware mette à jour la pile de protocole des appareils WIA-PA. Sachant que la mise à niveau en ligne du firmware est une opération énergivore, le réseau WIA-PA ne recommande pas ce mode et ne le spécifie pas dans le présent document. Le réseau WIA-PA recommande la mise à niveau hors ligne du firmware par l'intermédiaire d'appareils tenus à la main. Les appareils tenus à la main connectent les appareils devant être mis à niveau par connexion câblée ou sans fil. Les connexions câblées peuvent utiliser les méthodes de communication série. Les connexions sans fil ne sont pas spécifiées dans le présent document.

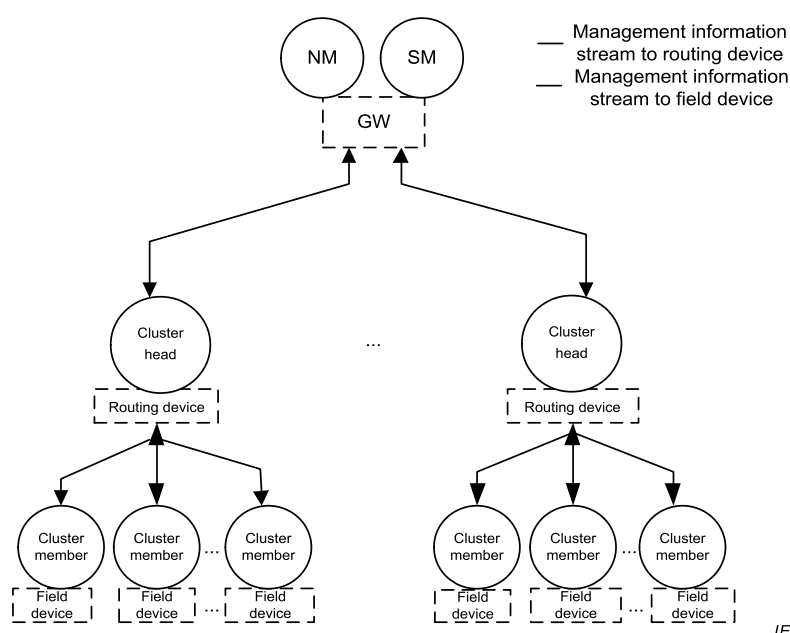
Il convient que la gestion de la sécurité gère les attributs associés à la sécurité réseau. La gestion de la sécurité est accomplie par le SM et les modules de gestion de la sécurité dans les têtes de groupe et éléments de groupe. Le SM gère l'authentification centralisée du réseau tout entier et nécessite une coordination avec le NM. Voir 11.1 pour les fonctions relatives à la gestion de la sécurité.

Le module MIB stocke tous les attributs utilisés dans le réseau WIA-PA, y compris les attributs structurés comme les attributs non structurés (voir 6.9).

6.2 Cadre de travail de la gestion système

Le réseau WIA-PA prend en charge le plan de gestion hybride centralisée et répartie.

Le cadre de travail pour la gestion hybride centralisée et répartie est représenté à la Figure 6. La gestion de système est mise en œuvre par le NM, le SM et les têtes de groupe. Les têtes de groupe sont directement gérées par le NM et le SM. En outre, le privilège de gérer les éléments de groupe leur est octroyé.



Anglais	Français
Management information stream to routing device	Flux d'informations de gestion à destination de l'appareil de routage
Management information stream to field device	Flux d'informations de gestion à destination de l'appareil de terrain
NM	Gestionnaire de réseau (NM)
SM	Gestionnaire de sécurité (SM)
GW	Passerelle (GW)
Cluster head	Tête de groupe
Routing device	Appareil de routage
Cluster member	Élément de groupe
Field device	Appareil de terrain

Figure 6 – Plan de gestion de système hybride centralisée et répartie

Il convient que le NM accomplisse les tâches suivantes:

- construire et maintenir la topologie maillée constituée de têtes de groupe et la topologie en étoile constituée de têtes de groupe et d'éléments de groupe;
- affecter des ressources de communication aux têtes de groupe dans la topologie maillée et affecter des ressources de communication pour les éléments de groupe aux têtes de groupe dans la topologie en étoile;
- surveiller la performance du réseau WIA-PA, notamment l'état des appareils, la défaillance de chemin et la condition des canaux.

Il convient que le SM accomplisse les tâches suivantes:

- admettre les têtes de groupe et éléments de groupe qui tentent de se rattacher au réseau WIA-PA;
- gérer les clés dans la totalité du réseau, y compris la création de clés, la distribution de clés, la récupération de clés et la révocation de clés;
- permettre la relation de communication de bout en bout.

Il convient que la tête de groupe accomplisse les tâches suivantes:

- a) construire et maintenir la topologie en étoile; affecter des ressources de communication qui sont affectées à la topologie en étoile par le NM aux éléments de groupe dans le groupe; fournir au NM les résultats de la surveillance de la topologie en étoile;
- b) sauvegarder et transmettre les clés utilisées dans la topologie en étoile; permettre la relation de communication entre têtes de groupe; permettre la relation de communication entre une tête de groupe et des éléments de groupe.

6.3 Processus de rattachement

6.3.1 Processus de mise en service

Lorsqu'un appareil WIA-PA tente de se rattacher au réseau, il convient qu'il soit mis en service par un appareil tenu à la main via une connexion câblée.

Il convient qu'un nouvel appareil soit doté d'une adresse longue de 64 bits avant de se rattacher au réseau WIA-PA. D'abord, la valeur CountryCode (voir 6.9.1.2.1 et 8.4.11) d'un nouvel appareil doit être configurée, car elle reflète les contraintes de réglementation propres à la zone géographique dans laquelle il pourrait être déployé. Ensuite, la valeur NetworkTopology (voir 6.9.1.2.1) doit être définie, puisqu'elle indique le type de topologie de réseau. Puis la valeur SecEnableflag (voir 6.9.1.2.1) doit être déterminée, parce qu'elle indique si l'authentification est activée sur le réseau. Si l'authentification est activée, la valeur KJ doit également être définie (voir 11.2).

Pour se rattacher au réseau WIA-PA, il convient qu'un nouvel appareil de routage ou appareil de terrain écoute d'abord les balises.

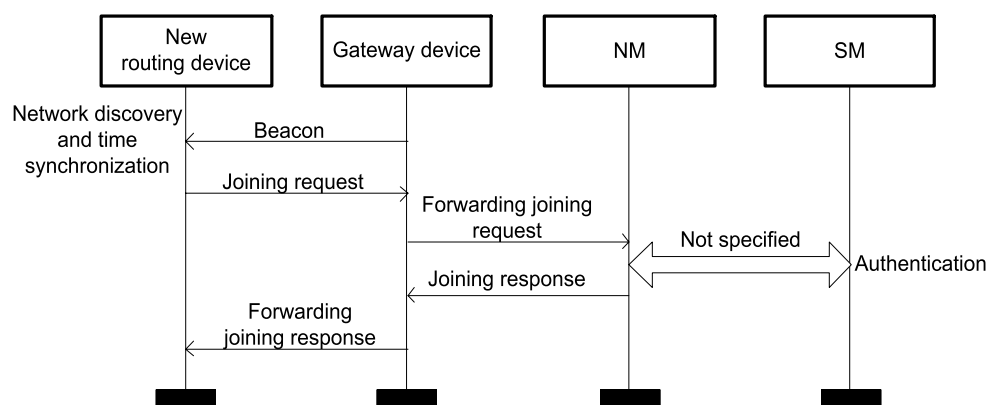
6.3.2 Processus de rattachement d'un appareil de routage

Lorsqu'un appareil de routage tente de se rattacher au réseau, il convient qu'une clé de rattachement soit mise en service par un appareil tenu à la main. Voir l'Article 11 pour le processus détaillé de mise en service.

Le processus de rattachement d'un appareil de routage inclut les opérations suivantes.

- a) Un appareil de routage balaye les canaux disponibles pour obtenir des balises de la part des appareils de routage en ligne ou de l'appareil de passerelle.
- b) L'appareil de routage choisit un appareil de routage en ligne ou l'appareil de passerelle comme parent temporel et se synchronise au réseau conformément à la balise reçue.
- c) L'appareil de routage envoie une demande de rattachement à son parent temporel qui transmettra ensuite la demande au NM.
- d) Lorsqu'il reçoit une demande de rattachement, il convient que le NM communique avec le SM pour parachever le processus d'authentification. Puis, le NM retourne une réponse de rattachement.
- e) L'appareil de routage reçoit la réponse de rattachement relayée par son parent temporel. Si la réponse est négative, il convient que l'appareil de routage recommence ce processus de rattachement; sinon, il convient que le processus de rattachement soit terminé.

Le processus de rattachement d'un appareil de routage par l'intermédiaire de l'appareil de passerelle est indiqué à la Figure 7.

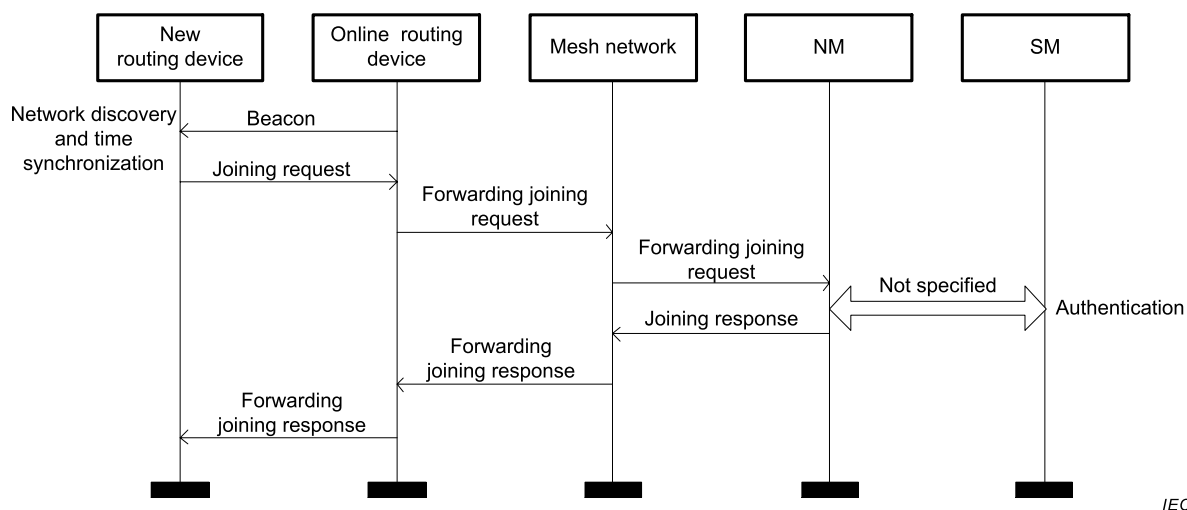


IEC

Anglais	Français
New routing device	Nouvel appareil de routage
Gateway device	Appareil passerelle
NM	Gestionnaire de réseau (NM)
SM	Gestionnaire de sécurité (SM)
Network discovery and time synchronization	Découverte de réseau et synchronisation de l'heure
Beacon	Balise
Joining request	Demande de rattachement
Forwarding joining response	Transmission de la réponse de rattachement
Forwarding joining request	Transmission de la demande de rattachement
Joining response	Réponse de rattachement
Not specified	Non spécifié
Authentication	Authentification

Figure 7 – Processus de rattachement d'un appareil de routage par l'intermédiaire de l'appareil de passerelle

Le processus de rattachement d'un appareil de routage par l'intermédiaire d'un appareil de routage en ligne est indiqué à la Figure 8.



Anglais	Français
New routing device	Nouvel appareil de routage
Online routing device	Appareil de routage en ligne
Mesh network	Réseau maillé
NM	Gestionnaire de réseau (NM)
SM	Gestionnaire de sécurité (SM)
Network discovery and time synchronization	Découverte de réseau et synchronisation de l'heure
Beacon	Balise
Joining request	Demande de rattachement
Forwarding joining response	Transmission de la réponse de rattachement
Forwarding joining request	Transmission de la demande de rattachement
Joining response	Réponse de rattachement
Not specified	Non spécifié
Authentication	Authentification

Figure 8 – Processus de rattachement d'un appareil de routage par l'intermédiaire d'un appareil de routage en ligne

Voir 9.5.8 pour l'affectation de ressources de communication.

6.3.3 Processus de rattachement d'un appareil de terrain

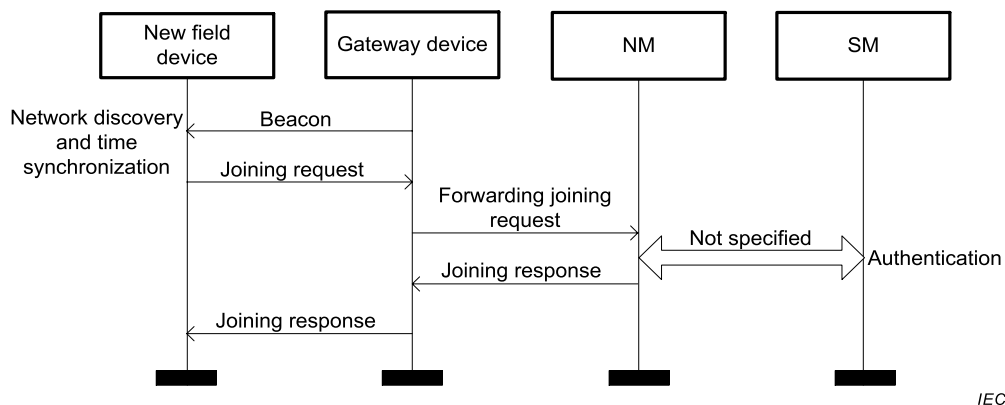
Le processus de rattachement d'un appareil de terrain inclut les opérations suivantes.

- Un appareil de terrain balaye les canaux disponibles pour obtenir des balises de la part des appareils de routage en ligne ou de l'appareil de passerelle.
- L'appareil de terrain choisit un appareil de routage en ligne ou l'appareil de passerelle comme tête de groupe et se synchronise au réseau conformément à la balise reçue.
- L'appareil de terrain envoie à la tête de groupe la demande de rattachement.
- Lorsqu'elle reçoit la demande de rattachement, la tête de groupe la transmet au NM.
- Après avoir reçu la réponse de rattachement du NM, la tête de groupe retourne la réponse de rattachement à l'appareil de terrain en fonction du type de topologie de réseau et des ressources de communication disponibles de la tête de groupe. Si la topologie de réseau ne correspond pas, l'état de la réponse est défini sur FAILURE_TOP_DISMATCH; s'il

existe d'autres types de défaillances, l'état de la réponse est défini sur FAILURE_ELSE; si le rattachement a fonctionné, l'état de la réponse est défini sur SUCCESS. Voir 8.6.3.4 pour la définition de l'état.

- f) L'appareil de terrain reçoit la réponse de rattachement de la tête de groupe. Si l'état de la réponse est FAILURE_TOP_DISMATCH, l'appareil de terrain sélectionnera un autre appareil de routage comme tête de groupe et redémarrera le processus de rattachement décrit ci-dessus; si l'état de la réponse est FAILURE_ELSE, l'appareil de terrain redémarrera ce processus de rattachement; si l'état de la réponse est SUCCESS, l'appareil de terrain est rattaché au réseau.

Les processus de rattachement d'un appareil de terrain par l'intermédiaire de l'appareil de passerelle et d'un appareil de routage sont respectivement indiqués à la Figure 9 et à la Figure 10. Voir 9.5.8 pour l'affectation de ressources de communication.



Anglais	Français
New field device	Nouvel appareil de terrain
Gateway device	Appareil passerelle
NM	Gestionnaire de réseau (NM)
SM	Gestionnaire de sécurité (SM)
Network discovery and time synchronization	Découverte de réseau et synchronisation de l'heure
Beacon	Balise
Joining request	Demande de rattachement
Joining response	Réponse de rattachement
Forwarding joining request	Transmission de la demande de rattachement
Not specified	Non spécifié
Authentication	Authentification

Figure 9 – Processus de rattachement d'un appareil de terrain par l'intermédiaire d'un appareil de passerelle

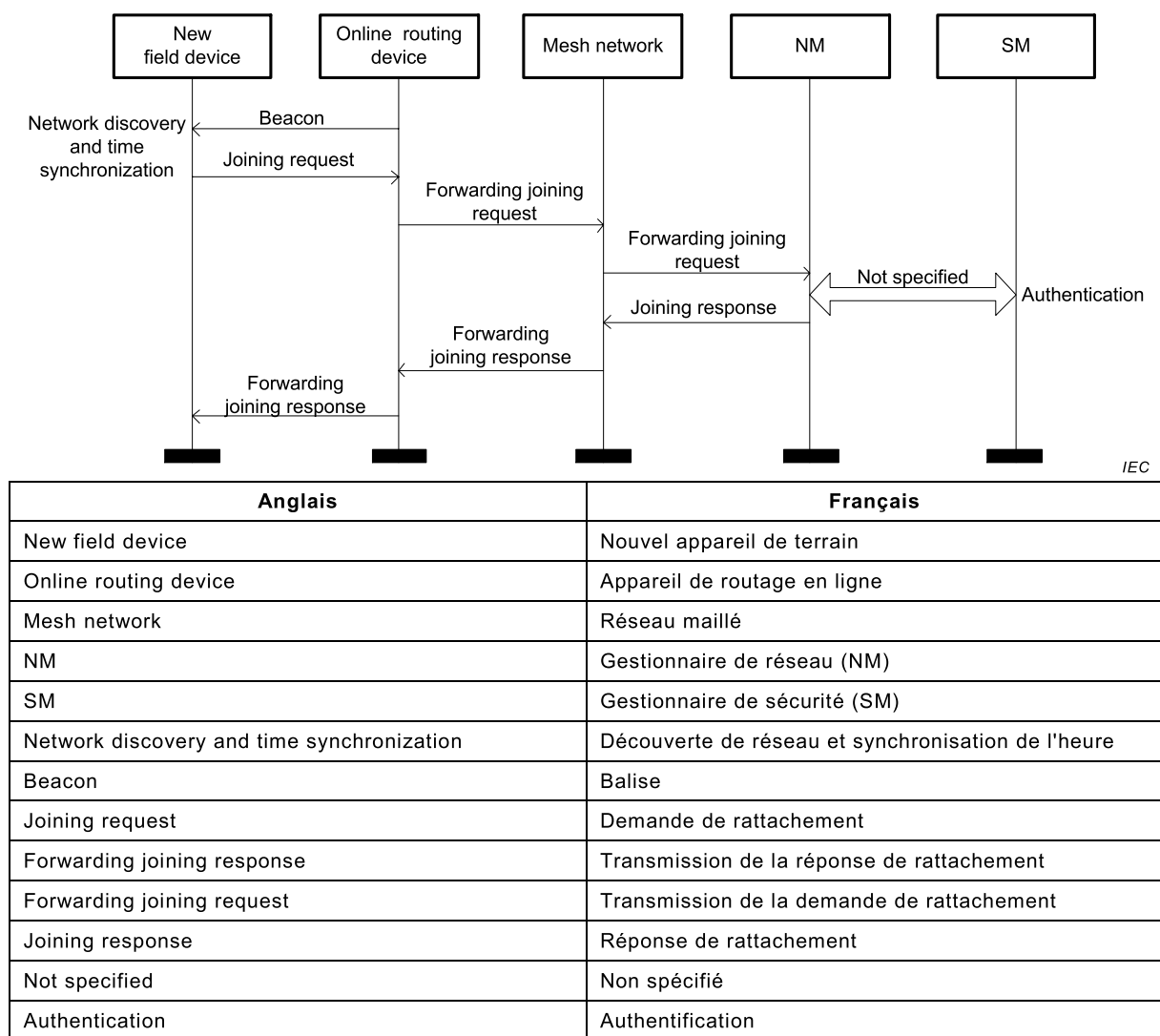


Figure 10 – Processus de rattachement d'un appareil de terrain par l'intermédiaire d'un appareil de routage

Un appareil tenu à la main WIA-PA se connecte au réseau WIA-PA via l'appareil de passerelle ou un appareil de routage. Le processus de rattachement de l'appareil tenu à la main est le même que celui des autres appareils WIA-PA. Après s'être rattaché au réseau, l'appareil tenu à la main WIA-PA configure les appareils WIA-PA et rassemble les informations relatives à la santé/à la performance du réseau au cours de la période d'accès avec conflit (CAP) de la supertrame WIA-PA.

Voir l'Article 11 pour plus d'informations au sujet de la sécurité.

6.3.4 Adressage et attribution d'adresses

Dans le réseau WIA-PA, chaque appareil WIA-PA (appareil de passerelle, appareil de routage ou appareil de terrain) possède une adresse longue globale unique de 64 bits et une adresse courte de 16 bits. L'adresse longue, telle qu'indiquée à la Figure 11, est fixée par les fabricants conformément à l'adresse EUI-64 de l'IEEE.

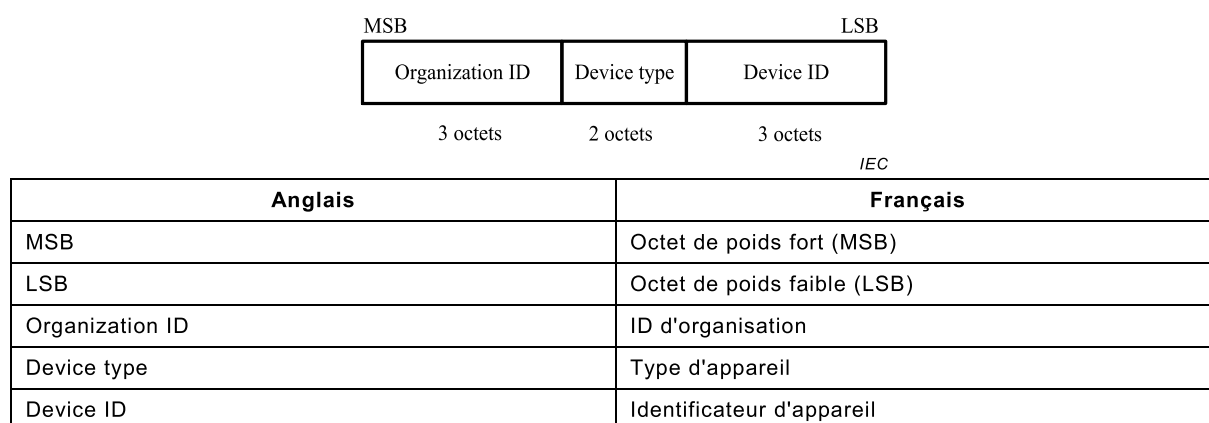


Figure 11 – Structure d'adresse longue d'un appareil

L'adresse courte a une longueur de 16 bits. Les huit bits de poids fort de l'adresse courte qui sont assignés par le NM sont utilisés pour identifier les différents groupes. Si la valeur du paramètre NetworkTopology (voir 6.9.1.2.1) est définie sur 1, correspondant à la topologie de réseau en étoile uniquement, l'adresse de l'appareil de passerelle est également l'adresse de la tête de groupe.

L'adresse courte de l'appareil de passerelle est affectée par le NM. Le NM réside dans un appareil de passerelle (voir 5.2). Le processus d'affectation d'adresse de l'appareil de passerelle est une opération interne qui n'est pas spécifiée dans la présente spécification.

L'adresse courte d'un appareil de routage est indiquée à la Figure 12. Pour l'adresse courte d'un appareil de routage, les 8 bits de poids faible sont définis sur 0.

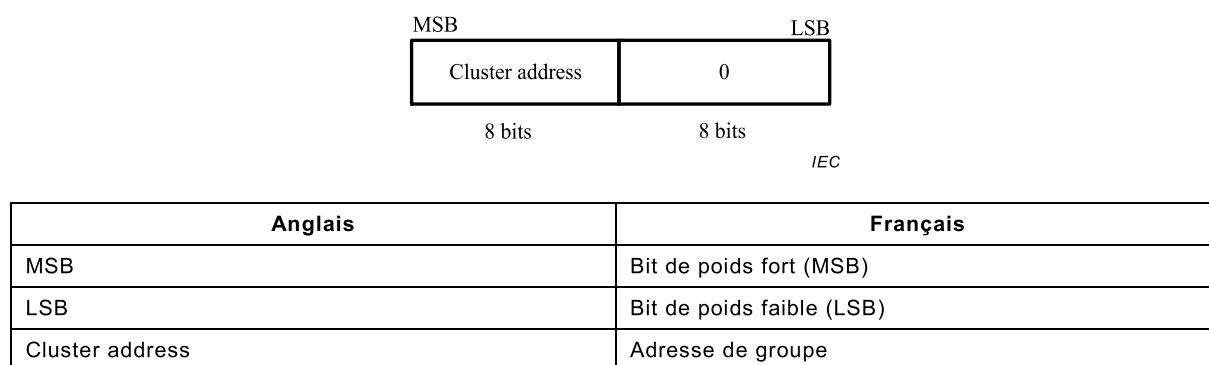
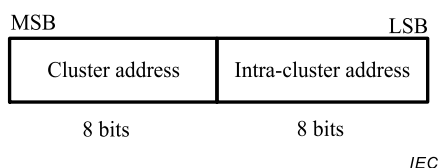


Figure 12 – Structure d'adresse courte d'un appareil de routage

L'adresse courte d'un appareil de terrain est indiquée à la Figure 13. La partie des 8 bits de poids faible dans l'adresse courte de l'appareil de terrain est l'adresse intragroupe (dans le groupe).



Anglais	Français
MSB	Bit de poids fort (MSB)
LSB	Bit de poids faible (LSB)
Cluster address	Adresse de groupe
Intra-cluster address	Adresse intragroupe (dans le groupe)

Figure 13 – Structure d'adresse courte d'un appareil de terrain

6.4 Relation de communication virtuelle (VCR, Virtual Communication Relationship)

6.4.1 Définition

L'accès aux objets d'application utilisateur (UAO) est défini par les VCR et les points d'extrémité d'un VCR sont deux objets UAO. Les VCR distinguent les ressources de routage et de communication parmi différents objets UAO. Chaque relation VCR est identifiée par un identificateur de VCR (VCR_ID). Les attributs d'une VCR comprennent l'identificateur d'objet UAO du côté source, l'identificateur d'objet UAO du côté destination, les adresses de l'appareil source/de destination, le type de VCR, le domaine d'application valide, etc. (voir Tableau 2).

Les VCR sont classées en trois types selon les modes d'application:

- a) VCR Editeur/Abonné (P/S), utilisée pour publier des données périodiques;
- b) VCR Source/Puits de rapports (R/S), utilisée pour prendre en charge les rapports non périodiques sur les événements et les tendances;
- c) VCR Client/Serveur (C/S), utilisée pour transférer les messages de monodiffusion par paires dynamiques et non périodiques.

Les VCR sont classées en trois types selon leurs fonctions d'agrégation:

- a) VCR de non-agrégation

Si l'agrégation n'est pas prise en charge par un élément de groupe, la VCR de non-agrégation est utilisée par l'élément de groupe pour envoyer des paquets de non-agrégation vers sa tête de groupe. Si la tête de groupe ne prend pas en charge la fonction d'agrégation, elle transmettra les paquets de non-agrégation à la passerelle par le truchement de la VCR de non-agrégation.

- b) VCR d'agrégation de données

Si l'agrégation est prise en charge par un élément de groupe, la VCR d'agrégation de données est utilisée par l'élément de groupe pour envoyer les données agrégées à partir des objets UAO vers sa tête de groupe. Si la tête de groupe ne prend pas en charge la fonction d'agrégation, elle transmettra les données agrégées à la passerelle par l'intermédiaire de la VCR d'agrégation de données. L'intervalle effectif de la VCR d'agrégation de données va de l'objet d'agrégation de données (DAGO) de la tête de groupe à l'objet de désagrégation (DGO) de la passerelle.

- c) VCR d'agrégation de paquets

Si l'agrégation est prise en charge par une tête de groupe, la VCR d'agrégation de paquets est utilisée par la tête de groupe pour envoyer des paquets agrégés vers la passerelle. L'intervalle effectif de la VCR d'agrégation de paquets va de l'objet

d'agrégation de paquet (PAGO) de la tête de groupe à l'objet de désagrégation (DGO) de la passerelle.

Les PAGO, DGO et DAGO (voir 6.6.1) sont trois types spéciaux d'objets UAO.

6.4.2 Prise en charge du protocole pour la VCR

Les prises en charge du protocole pour les VCR sont énumérées au Tableau 2.

Tableau 2 – Prise en charge du protocole pour la VCR

Prise en charge de la couche de protocole			Types de VCR		
			VCR P/S	VCR R/S	VCR C/S
AL	Applications utilisateur		Emission de données périodique d'objet UAO	Rapport apériodique, par exemple alarme ou événement	Opération d'obtention et d'établissement d'attribut dans l'objet UAO
	Modes de communications dans la sous-couche application (ASL)		P/S	R/S	C/S
	Bidirectionnelle		Non	Non	Oui
	Retransmission de bout en bout		Non	Facultatif	Oui
	Prise en charge de l'agrégation de paquets		Oui	Non	Non
NL	Prise en charge de chemins redondants	Intragroupe	Non	Non	Non
		Intergroupe	Oui	Oui	Oui
	Monodiffusion/Diffusion		Diffusion/Monodiffusion	Diffusion/Monodiffusion	Monodiffusion
DLSL	Périodique		Oui	Non	Non
	Temps réel		Oui	Facultatif	Non
	Ressource de communication	Intragroupe	Période sans conflit (CFP), intervalles de temps exclusifs dans la période de communication intragroupe	CAP	CAP
		Intergroupe	Intervalles de temps exclusifs dans la période de communication intergroupe	Intervalles de temps partagés	Intervalles de temps partagés

6.4.3 Etablissement de VCR

Les processus d'établissement de VCR R/S et C/S sont les suivants.

- Le NM obtient les objets UAO des appareils de terrain lorsqu'ils sont rattachés au réseau WIA-PA. Les objets UAO sont obtenus par les primitives NLME-INFO_GET au cours de la période d'accès avec conflit (CAP) (voir 9.5.13 et 9.6.4);
- Une fois que le NM obtient les objets UAO, il affecte les VCR R/S et C/S réservées à chaque objet UAO aux appareils de terrain.

S'il est nécessaire, le processus d'établissement de VCR P/S se déroule comme suit.

- Le NM établit une VCR P/S pour chaque objet UAO en utilisant les primitives NLME-INFO_SET (voir 9.5.14 et 9.6.4). Si un appareil de terrain ne prend pas en charge l'agrégation de données, chaque objet UAO a une VCR P/S de non-agrégation et

des VCR différentes peuvent utiliser les mêmes chemins de routage. Autrement, chaque appareil de terrain a une VCR d'agrégation de données. Si l'appareil de routage prend en charge l'agrégation de paquets, une VCR d'agrégation de paquets est établie pour l'appareil de routage.

Voir Tableau 21 pour plus d'informations au sujet des VCR.

6.4.4 Libération de VCR

Les VCR sont libérées lorsque les appareils de routage et les appareils de terrain quittent le réseau (voir 6.8).

6.5 Configuration du routage et allocation de ressources de communication

6.5.1 Configuration de routage

Les appareils de routage utilisent un routage statique qui est configuré par le NM. Les algorithmes de routage concrets ne sont pas spécifiés dans la présente norme. Les détails sur les chemins de routage sont indiqués au Tableau 15. Les chemins redondants sont pris en charge et utilisent le même RoutelD. La configuration du routage est réalisée par les services d'affectation d'itinéraire (voir 9.5.7).

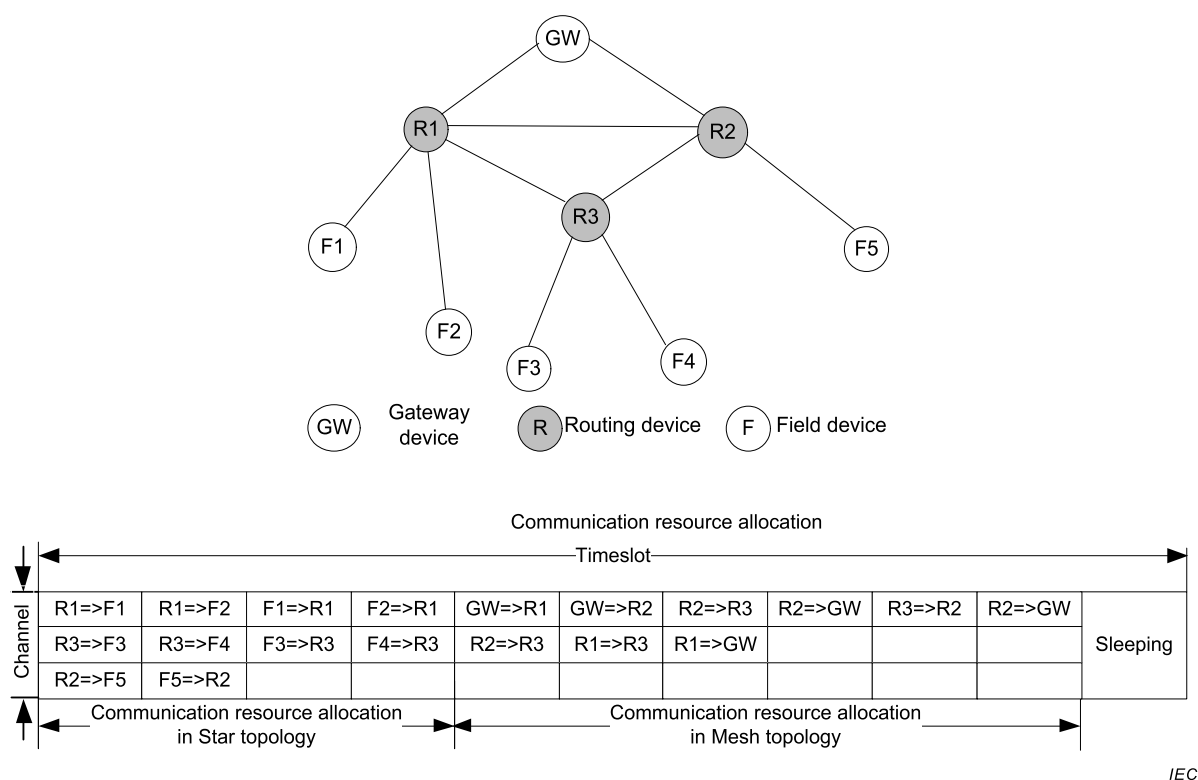
6.5.2 Cadre de travail de l'allocation de ressources de communication

Les ressources de communication sont constituées d'intervalles de temps et de canaux. Il convient que l'affectation de ressources de communication soit considérée selon deux dimensions, à savoir le temps et le canal.

Le processus d'allocation de ressource de communication se déroule comme suit.

- a) dans le réseau maillé, les ressources de communication des têtes de groupe sont affectées par le gestionnaire de réseau (NM). Les ressources de communication sont constituées de celles utilisées par les têtes de groupe dans le réseau maillé et de celles affectées par les têtes de groupe aux éléments de groupe;
- b) dans le réseau en étoile, les ressources de communication sont affectées par les têtes de groupe aux éléments de groupe. Cela signifie que les ressources de communication sont liées aux éléments de groupe.

Un exemple de l'affectation de ressources dans la topologie de réseau hiérarchique qui est la combinaison de la configuration en étoile et de la configuration maillée est présentée à la Figure 14. En premier lieu, le NM résidant dans l'appareil de passerelle (GW) affecte des ressources de communication aux appareils de routage R1, R2 et R3. Ces ressources de communication sont utilisées pour la communication parmi R1, R2 et R3, pour la communication entre les appareils de routage et l'appareil de passerelle et pour la communication entre les appareils de terrain et appareils de routage intragroupe. Ensuite, après avoir reçu les ressources de communication du NM, les appareils de routage affectent certaines ressources de communication à leurs appareils de terrain intragroupe, qui sont utilisés pour les communications intragroupes parmi les appareils de terrain et leurs appareils de routage correspondants. Comme indiqué à la Figure 14, après que le NM a affecté des ressources de communication à R1, R2 et R3, R1 affecte des ressources de communication à F1 et F2, R2 affecte des ressources de communication à F5, et R3 affecte des ressources de communication à F3 et F4.



IEC

Anglais	Français
Gateway device	Appareil de passerelle
Routing device	Appareil de routage
Field device	Appareil de terrain
Communication resource allocation	Allocation de ressources de communication
Timeslot	Intervalle de temps
Channel	Canal
Sleeping	Sommeil
Communication resource allocation in Star topology	Allocation de ressources de communication dans la topologie en étoile
Communication resource allocation in Mesh topology	Allocation de ressources de communication dans la topologie maillée

Figure 14 – Exemple d'affectation de ressources

6.5.3 Règles de priorité des unités DLPDU et de programmation

Quatre niveaux de priorité sont définis pour les unités DLPDU.

a) Command (priorité la plus haute)

Il convient de classer tout paquet contenant une charge utile avec des informations relatives au diagnostic, à la configuration, à la commande, liées au réseau ou des alarmes urgentes avec une priorité Command.

b) Process data (priorité secondaire)

Il convient de classer tout paquet contenant des données de processus avec le niveau de priorité secondaire Process Data.

c) Normal (troisième priorité)

Il convient de classer les unités DLPDU qui ne satisfont pas aux critères de Command, Process data ou Alarm avec la priorité Normal.

d) Alarm (priorité la plus basse)

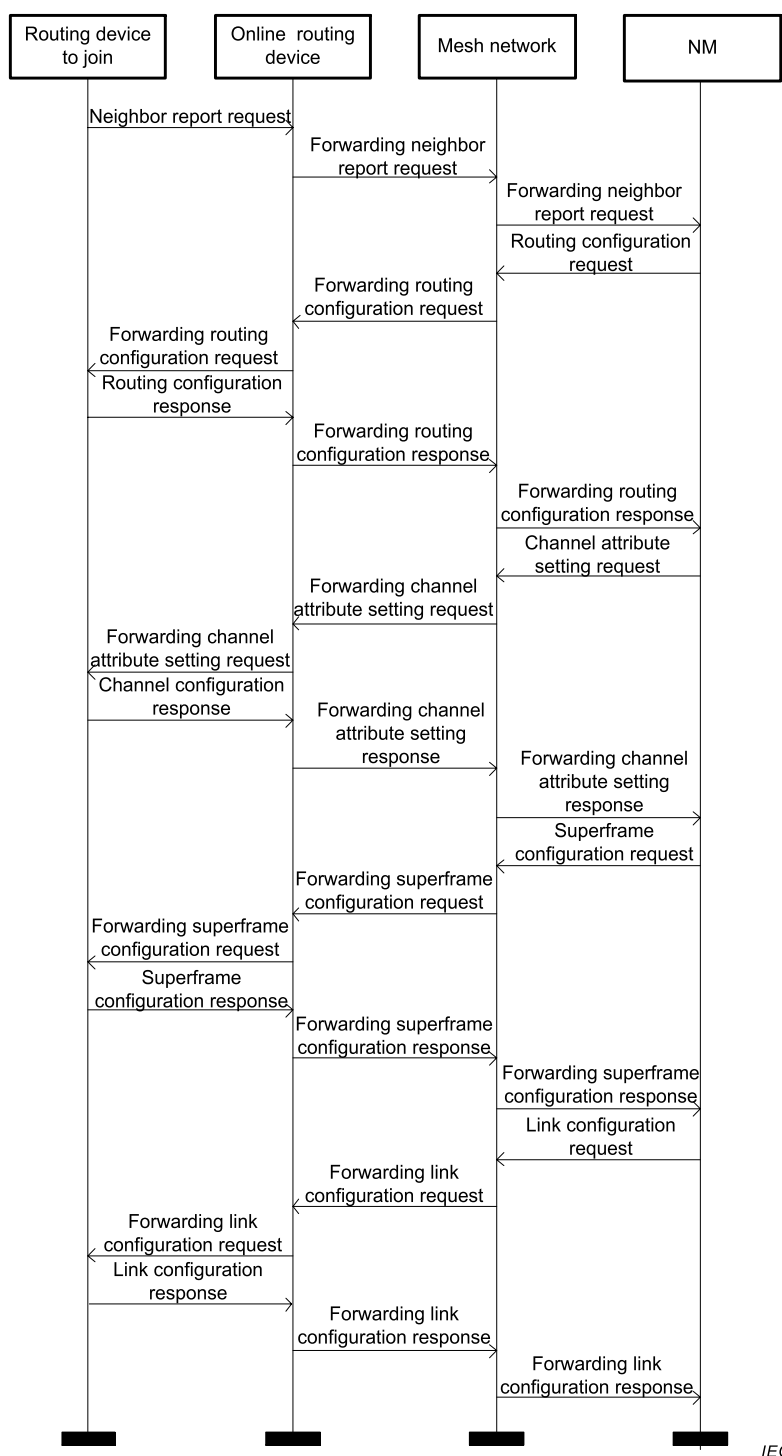
Il convient que les paquets contenant uniquement une alarme non urgente et une charge utile d'événement prennent une priorité Alarm. Il convient que les appareils ne mettent pas en tampon plus d'une unité DLPDU ayant la priorité Alarm.

Les règles de programmation suivantes sont recommandées dans cet ordre pour l'affectation des ressources de communication:

- a) affecter des canaux à la trame balise et à la période active;
- b) affecter des intervalles de temps aux appareils ayant la vitesse de mise à jour la plus rapide;
- c) affecter des ressources au paquet ayant le temps de création le plus précoce dans des situations de sauts multiples;
- d) affecter des ressources au paquet ayant la priorité la plus haute avant les autres paquets.

6.5.4 Affectation de ressources de communication à l'appareil de routage

Le réseau WIA-PA applique la stratégie de gestion intégrée de plans centralisée et répartie. Après que l'appareil de routage a été rattaché au réseau, il convient qu'il balaie ses appareils voisins sur chaque canal et transmette au NM les informations relatives à ces derniers. Après avoir reçu les informations relatives aux voisins, il convient que le NM affecte les chemins, une supertrame et un bloc de liaisons à l'appareil de routage à l'aide des services d'affectation de ressources de communication (voir 9.5.8). Les informations de chaque supertrame d'appareil de routage sont diffusées à ses appareils de terrain dans la trame balise. Le processus d'affectation de ressources de communication de l'appareil de routage est représenté à la Figure 15.



IEC

Anglais	Français
Routing device to join	Appareil de routage à rattacher
Online routing device	Appareil de routage en ligne
Mesh network	Réseau maillé
NM	Gestionnaire de réseau (NM)
Neighbour report request	Demande de rapport de voisin
Forwarding neighbor report request	Transmission de la demande de rapport de voisin
Routing configuration request	Demande de configuration de routage
Forwarding routing configuration request	Transmission de la demande de configuration de routage

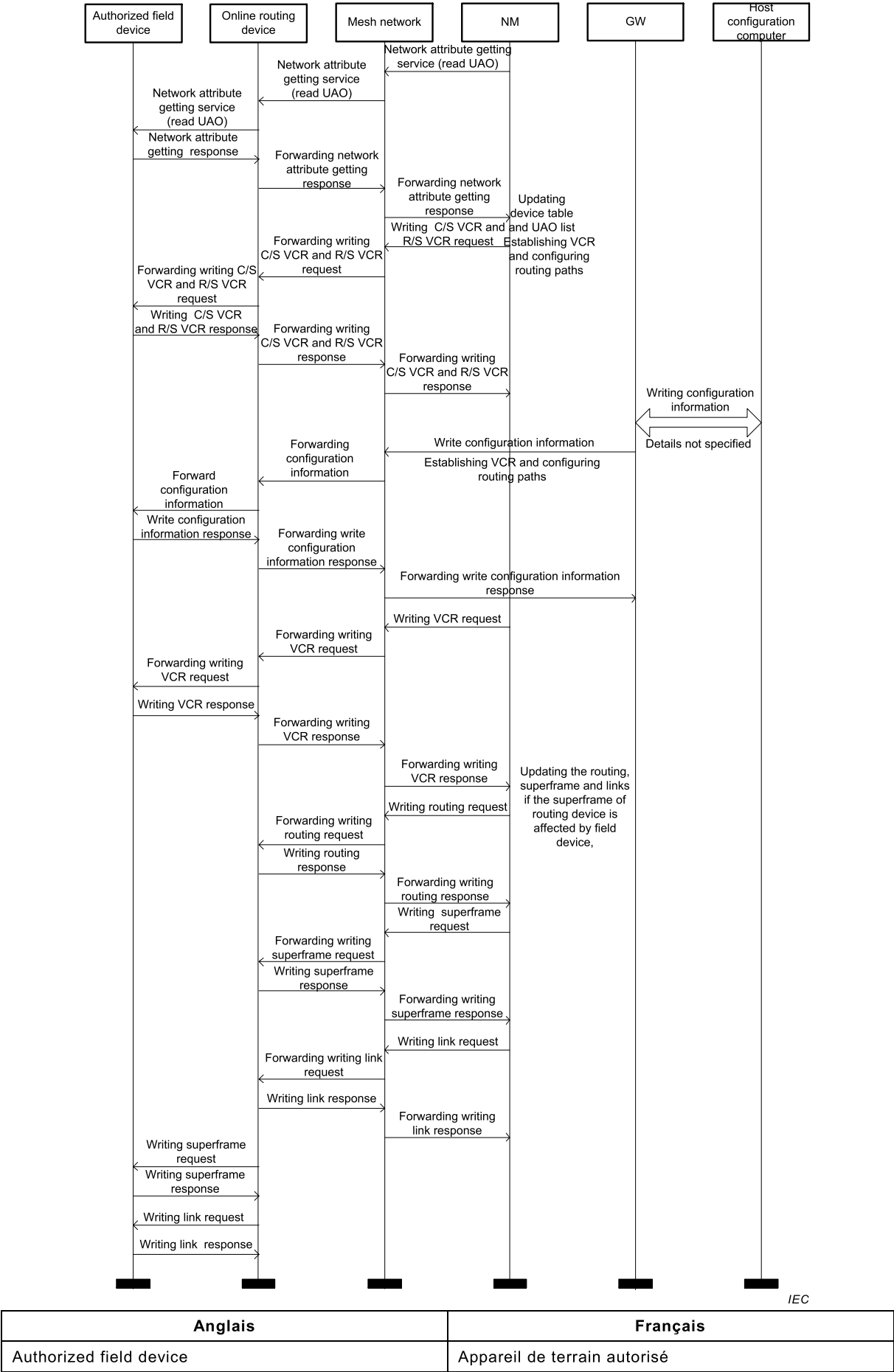
Anglais	Français
Routing configuration response	Réponse de configuration de routage
Forwarding routing configuration response	Transmission de la réponse de configuration de routage
Channel attribute setting request	Demande d'établissement d'attributs de canal
Forwarding channel attribute setting request	Transmission de la demande d'établissement d'attributs de canal
Channel configuration response	Réponse de configuration de canal
Forwarding channel attribute setting response	Transmission de la réponse d'établissement d'attributs de canal
Superframe configuration request	Demande de configuration de supertrame
Forwarding superframe configuration request	Transmission de la demande de configuration de supertrame
Superframe configuration response	Réponse de configuration de supertrame
Forwarding superframe configuration response	Transmission de la réponse de configuration de supertrame
Link configuration request	Réponse de configuration de liaison
Forwarding link configuration request	Transmission de la demande de configuration de liaison
Link configuration response	Réponse de configuration de liaison
Forward link configuration response	Transmission de la réponse de configuration de liaison

Figure 15 – Processus d'affectation de ressources de communication d'un appareil de routage

6.5.5 Affectation de ressources de communication à l'appareil de terrain

Après que des relations VCR d'un appareil de terrain ont été établies avec succès, l'appareil de routage ou l'appareil de passerelle affecte des intervalles de temps à ses appareils de terrain en utilisant les services d'allocation de ressources de communication (voir 9.5.8), qui sont utilisés pour la communication entre l'appareil de routage et les appareils de terrain ou entre l'appareil de passerelle et les appareils de terrain. Si les supertrames de l'appareil de routage et de l'appareil de passerelle sont affectées par les appareils de terrain rattachés, il convient que l'appareil de routage et l'appareil de passerelle mettent à jour leurs attributs RouteTable, Superframe et Link (voir 6.9.1.2.2 et 9.5.8).

Lorsqu'un appareil de terrain se rattache au réseau par l'intermédiaire d'un appareil de routage en ligne, le processus d'affectation de ressources de communication de l'appareil de terrain est représenté à la Figure 16.



Anglais	Français
Online routing device	Appareil de routage en ligne
Mesh network	Réseau maillé
NM	Gestionnaire de réseau (NM)
GW	Passerelle (GW)
Host configuration computer	Ordinateur de configuration d'hôte
Network attribute getting service (read UAO)	Service d'obtention d'attributs réseau (lire l'objet UAO)
Network attribute getting response	Réponse d'obtention d'attributs réseau
Forwarding network attribute getting response	Transmission de la réponse d'obtention d'attributs réseau
Updating device table and UAO list	Mise à jour de la table des appareils et de la liste des objets UAO
Establishing VCR and configuring routing paths	Etablissement de la VCR et configuration des chemins de routage
Writing C/S VCR and R/S VCR request	Demande d'écriture de la VCR C/S et de la VCR R/S
Forwarding writing C/S VCR and R/S VCR request	Transmission de la demande d'écriture de la VCR C/S et de la VCR R/S
Writing C/S VCR and R/S VCR response	Réponse d'écriture de la VCR C/S et de la VCR R/S
Write configuration information response	Ecriture de la réponse d'informations de configuration
Forwarding write configuration information response	Transmission de la réponse d'écriture des informations de configuration
Writing VCR request	Demande d'écriture de la VCR
Forwarding writing VCR request	Transmission de la demande d'écriture de la VCR
Writing VCR response	Réponse d'écriture de la VCR
Forwarding writing VCR response	Transmission de la réponse d'écriture de la VCR
Network attribute getting service to read UAO	Service d'obtention d'attributs réseau pour lire l'objet UAO
Forwarding writing C/S VCR and R/S VCR request	Transmission de la demande d'écriture de la VCR C/S et de la VCR R/S
Network attribute getting service to read UAO	Service d'obtention d'attributs réseau pour lire l'objet UAO
Forwarding writing C/S VCR and R/S VCR response	Transmission de la réponse d'écriture de la VCR C/S et de la VCR R/S
Write configuration information	Ecriture des informations de configuration
Details not specified	Détails non spécifiés
Establishing VCR and configuring routing paths	Etablissement de la VCR et configuration de chemins de routage
Forwarding configuration information	Transmission des informations de configuration
Updating the routing, superframe and links if the superframe of routing device is affected by field device	Mise à jour du routage, de la supertrame et des liaisons si la supertrame de l'appareil de routage est affectée par l'appareil de terrain
Writing routing request	Demande d'écriture de routage
Forwarding writing routing response	Transmission de la réponse d'écriture de routage
Writing routing response	Réponse d'écriture de routage
Forwarding writing routing response	Transmission de la réponse d'écriture de routage
Forwarding writing superframe request	Transmission de la demande d'écriture de liaison
Forwarding writing superframe response	Transmission de la réponse d'écriture de supertrame
Writing link response	Réponse d'écriture de liaison
Forwarding writing link response	Transmission de la réponse d'écriture de liaison
Writing superframe request	Demande d'écriture de supertrame

Anglais	Français
Writing superframe response	Réponse d'écriture de supertrame
Writing link request	Demande d'écriture de liaison

Figure 16 – Processus d'affectation de ressources de communication d'un appareil de terrain

6.6 Agrégation et désagrégation

6.6.1 Agrégation

La fonction d'agrégation est facultative pour les appareils de terrain et les appareils de routage. Elle est signalée par le fanion de prise en charge d'agrégation et de désagrégation AGGSupportFlag (voir Tableau 20). Si les appareils de terrain ou les appareils de routage prennent en charge le mécanisme d'agrégation, le NM configure le fanion d'activation d'agrégation et de désagrégation AGGEnableFlag sur la valeur 1 (voir Tableau 20).

Le réseau WIA-PA prend en charge un mécanisme d'agrégation à deux niveaux afin de réduire le nombre de transmissions de paquets.

- a) Agrégation de données. Si un appareil de terrain a plus d'un objet d'application utilisateur (UAO), il convient qu'il décide d'invoquer ou non le mécanisme d'agrégation de données en fonction du fanion AGGEnableFlag. Il convient que ce mécanisme réduise la fréquence de communication de données et renforce le rendement du réseau.
- b) Agrégation de paquets. Si un appareil de routage reçoit des paquets provenant de plus d'un appareil de terrain, il convient qu'il décide d'invoquer ou non le mécanisme d'agrégation de paquets en fonction du fanion AGGEnableFlag. Il convient que ce mécanisme réduise le nombre de paquets délivrés par l'appareil de routage à l'appareil de passerelle et renforce le rendement du réseau.

La fonction d'agrégation est mise en œuvre par les objets DAGO dans les appareils de terrain et par les objets PAGO dans les appareils de routage. Les paramètres de fonctionnement des DAGO et des PAGO sont configurés par le NM.

La fonction d'agrégation prise en charge par le réseau WIA-PA inclut les quatre situations suivantes:

- 1) Un appareil de terrain prend en charge la fonction d'agrégation alors que son appareil de routage ne le fait pas.
- 2) Un appareil de routage prend en charge la fonction d'agrégation alors que son appareil de terrain ne le fait pas.
- 3) Un appareil de terrain et son appareil de routage prennent tous deux en charge la fonction d'agrégation.
- 4) Ni l'appareil de terrain ni son appareil de routage ne prennent en charge la fonction d'agrégation.

Les relations entre les VCR et les fonctions d'agrégation prises en charge par l'appareil de terrain, l'appareil de routage et l'appareil de passerelle sont indiquées dans le Tableau 3.

Tableau 3 – Relations entre la VCR et la fonction d'agrégation

	Appareil de terrain DAGO (Fonction d'agrégation)			Appareil de routage PAGO (Fonction d'agrégation)			Appareil de passerelle DGO (Fonction de désagrégation)	
	Prise en charge	Désactivé	Activé	Prise en charge	Désactivé	Activé	Désactivé	Activé
VCR de non-agrégation	NON	X		NON	X		—	—
VCR d'agrégation de données	OUI		X	NON	X ^a			X
	OUI		X	NON		X ^b		X
VCR d'agrégation de paquets	NON	— ^c	— ^c	OUI		X		X
X Indique si la fonction d'agrégation/de désagrégation est activée ou désactivée dans l'appareil correspondant. — Indique que la VCR est indépendante de la fonction d'agrégation/de désagrégation. ^a La VCR d'agrégation de données commence avec l'objet DAGO d'un appareil de terrain et se termine avec l'objet DGO de l'appareil de passerelle. ^b La VCR d'agrégation de données commence avec l'objet DAGO d'un appareil de terrain et se termine avec l'objet PAGO d'un appareil de routage. ^c Les appareils de terrain ne sont pas dotés de fonction d'agrégation de paquet.								

Le processus de configuration d'agrégation se déroule comme suit.

- i) Il convient que le NM lise le fanion AGGSupportFlag pour vérifier si les appareils prennent en charge la fonction d'agrégation.
- ii) Si les appareils de routage prennent en charge la fonction d'agrégation, il convient que le NM définisse la valeur de l'attribut AGGEnableFlag à 1 dans la MIB. Il convient que le NM affecte les VCR d'agrégation de paquets aux appareils de routage. Il convient d'indiquer la durée d'agrégation d'un appareil de routage par l'attribut AggPeriod (voir 6.9.1.2.1) et de régler l'attribut DataUpdateRate à la valeur minimale (voir Tableau 21) de ses appareils de terrain dans le groupe. Lorsque la durée d'agrégation expire, l'appareil de routage agrège tous ses paquets et les envoie.
- iii) Si les appareils de terrain prennent en charge la fonction d'agrégation, il convient que le NM définisse la valeur de l'attribut AGGEnableFlag à 1 dans la MIB. Il convient que le NM affecte les VCR d'agrégation de données aux appareils de terrain. Il convient d'indiquer la durée d'agrégation d'un appareil de terrain par l'attribut AggPeriod (voir 6.9.1.2.1) et de régler l'attribut DataUpdateRate à la valeur minimale (voir Tableau 21) de ses objets UAO. Lorsque la durée d'agrégation expire, l'appareil de terrain agrège tous ses paquets et les envoie à l'appareil de routage.

Selon que l'agrégation est imbriquée ou non, un appareil de terrain ou un appareil de routage fonctionne de la manière suivante.

- a) si l'attribut du fanion d'agrégation AGGEnableFlag d'un appareil de terrain est défini sur 0, cet appareil de terrain ne prend pas en charge la fonction d'agrégation. Les appareils de terrain qui ne sont pas dotés de la fonction d'agrégation envoient leurs données à l'appareil de routage par l'intermédiaire de la VCR de non-agrégation et du RouteID relatif (voir Tableau 20) Si l'attribut du fanion d'agrégation AGGEnableFlag de l'appareil de routage est également défini sur 0, il convient que l'appareil de routage transmette ce paquet agrégé au DGO de l'appareil de passerelle par l'intermédiaire du RouteID d'origine.
- b) Si un appareil de terrain dispose de plus d'un UAO et que son attribut AGGEnableFlag est égal à 1, le DAGO de l'appareil de terrain calcule la longueur des données P/S à partir des UAO puis agrège ces données. Le format des données agrégées est décrit au

Tableau 4. Les données agrégées sont envoyées à la sous-couche application (ASL) par le DAGO et sont encapsulées avec l'en-tête ASL. Le champ de type de paquet dans l'en-tête ASL est défini sur 0b11, qui est utilisé pour indiquer le paquet agrégé (voir 10.4.2). Le paquet d'agrégation dans la sous-couche application (ASL) est envoyé à l'appareil de routage par l'intermédiaire de la VCR d'agrégation de données et du RouteID relatif; si la valeur de l'attribut AGGEnableFlag de l'appareil de routage est 0, il convient que l'appareil de routage transmette ce paquet agrégé au DGO de l'appareil de passerelle par l'intermédiaire du RouteID d'origine.

- c) Si la fonction d'agrégation imbriquée dans un appareil de routage est activée (AGGEnableFlag = 1) et reçoit les paquets des appareils de terrain, l'appareil lit les en-têtes de paquet de couche réseau (NL). Il convient que l'appareil de routage agrège le paquet conformément aux fanions P/S et au fanion Fragment dans les en-têtes de paquet de NL (voir 9.6.3). Les règles d'agrégation sont les suivantes:
- si le paquet reçu est de type P/S et que le fanion Fragment est égal à 0, il convient d'agrèger le paquet;
 - il convient de ne pas agrèger les autres types.

Si le paquet peut être agrégé, son adresse source et la charge utile de la couche réseau (NL) sont envoyées au PAGO du processus DMAP. Le PAGO utilise l'heure d'arrivée du premier paquet (devant être agrégé) comme instant de départ d'un cycle d'agrégation PagoPeriod (voir Tableau 10). Une fois que PagoPeriod expire, le PAGO agrège les paquets conformément au format indiqué au Tableau 5 et cherche les paquets relatifs à la VCR d'agrégation de paquets. Le paquet agrégé, la VCR d'agrégation de paquets et les paquets relatifs sont ensuite envoyés à la NL; il convient que la NL envoie ce paquet agrégé à l'appareil de passerelle par l'intermédiaire des paquets relatifs. Le format du paquet agrégé dans la NL est présenté en 9.6.3. Si la longueur du paquet agrégé est plus grande que la longueur maximale permise par la couche réseau (NL), il convient que celle-ci fragmente le paquet et l'envoie à l'appareil de passerelle en utilisant la VCR d'agrégation de paquets ainsi que les paquets relatifs.

Tableau 4 – Format des données agrégées suivies par l'objet DAGO de l'appareil de terrain

	Format des données agrégées suivies par l'objet DAGO de l'appareil de terrain					
Longueur en octet(s)	1	1	Longueur variable	...	1	Longueur variable
Nom de champ	Number of aggregated data (nombre de données agrégées)	Data length (longueur des données)	Data (données)	...	Data length (longueur des données)	Data (données)

Tableau 5 – Format du paquet agrégé suivi par l'objet PAGO de l'appareil de routage

	Format du paquet agrégé suivi par l'objet PAGO de l'appareil de routage							
Longueur en octet(s)	1	2	1	Longueur variable	...	2	1	Longueur variable
Nom de champ	Number of aggregated packet (nombre de paquets agrégés)	Source address (adresse source)	Data length (longueur des données)	Data (données)	...	Source address (adresse source)	Data length (longueur des données)	Data (données)

6.6.2 Désagrégation

La fonction de désagrégation est facultative pour l'appareil de passerelle. Elle est signalée par le fanion de prise en charge d'agrégation et de désagrégation AGGSupportFlag (voir Tableau 20). Si l'appareil de passerelle prend en charge le mécanisme de désagrégation,

le NM configure le fanion d'activation d'agrégation et de désagrégation AGGEnableFlag sur la valeur 1 (voir Tableau 20).

La fonction de désagrégation est mise en œuvre par le DGO dans l'appareil de passerelle. L'appareil de passerelle décide de désagréger ou non le paquet reçu en fonction de l'en-tête de NL et de l'en-tête ASL. Si la valeur du type de paquet dans l'en-tête de NL est égale à 1, l'appareil de passerelle désagrège le paquet agrégé de NL; si la valeur du type de paquet dans l'en-tête ASL est égale à 0b11, l'appareil de passerelle continue de désagréger le paquet agrégé ASL.

Les paramètres de fonctionnement du DGO sont configurés par le NM.

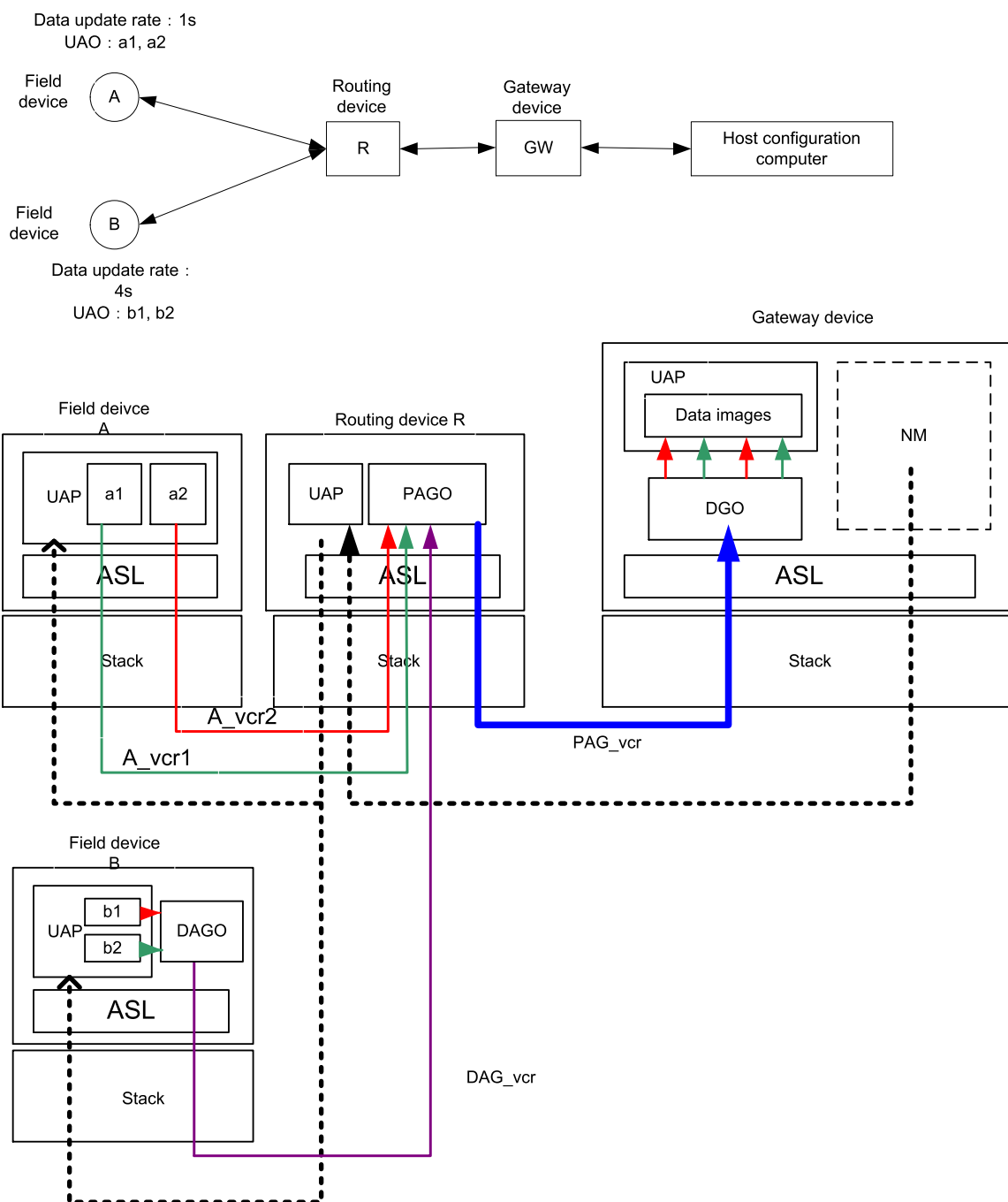
Le processus de désagrégation se déroule comme suit.

- a) Après que l'appareil de passerelle a reçu les paquets agrégés issus des appareils de terrain et des appareils de routage, il notifie le DGO dans son DMAP (processus d'application de gestion d'appareil) de désagréger les paquets.
- b) Le DMAP envoie les paquets désagrégés aux objets UAO.

6.6.3 Exemple du processus d'agrégation à deux niveaux

L'exemple ci-après illustre les processus d'agrégation et de désagrégation. L'exemple est basé sur un réseau constitué de deux appareils de terrain, d'un appareil de routage, de l'appareil de passerelle (GW) et de l'ordinateur de configuration d'hôte. Comme l'illustre la Figure 17, l'appareil de routage R agit comme tête de groupe de l'appareil de terrain A et de l'appareil de terrain B; on remarque la présence de deux UAO appelés a1 et a2 résidant dans l'appareil de terrain A et de deux UAO appelés b1 et b2 résidant dans l'appareil de terrain B.

Cet exemple suppose que l'appareil de terrain A ne prend pas en charge la fonction d'agrégation, contrairement à l'appareil de terrain B et à l'appareil de routage R. La vitesse de mise à jour des données de a1 et a2 est configurée à 1 s, et celle de b1 et b2 à 4 s. Le DAGO de l'appareil de terrain B est responsable de l'agrégation des paquets de b1 et b2 et génère le paquet p_b. L'appareil de routage R dispose d'un PAGO et la durée d'agrégation est la vitesse minimale de mise à jour des données de a1, a2, b1 et b2, dont la valeur est égale à 1 s. L'appareil de routage R dispose d'un PAGO qui agrège les paquets de a1, a2 et le paquet p_b. L'appareil de passerelle est doté d'un DGO qui désagrège les paquets des appareils de terrain A et B.



IEC

Anglais	Français
Data update rate	Vitesse de mise à jour des données
Field device	Appareil de terrain
Routing device	Appareil de routage
Gateway device	Appareil passerelle
Host configuration computer	Ordinateur de configuration d'hôte
Data images	Images de données
NM	NM
UAP	UAP
DGO	DGO
NMA	NMA

Anglais	Français
PAGO	PAGO
ASL	ASL
Stack	Pile
DABO	DABO

Figure 17 – Exemple d'agrégation et de désagrégation

Le processus d'agrégation et de désagrégation est énuméré ci-dessous.

- a) Après l'établissement du réseau, le NM affecte les VCR de non-agrégation à a1, a2, b1 et b2 pour la transmission des paquets de non-agrégation. Les VCR de non-agrégation de a1 et a2 dans l'appareil de terrain A sont indiqués par A_vcr1 et A_vcr2. Les points d'extrémité de A_vcr1 sont a1 et le processus d'application utilisateur (UAP) dans l'appareil de passerelle; et les points d'extrémité de A_vcr2 sont a2 et l'UAP dans l'appareil de passerelle. Dans la mesure où la transmission des données de l'appareil de terrain B n'utilise pas de VCR de non-agrégation, les VCR de non-agrégation de b1 et b2 dans l'appareil de terrain B ne sont pas indiqués dans cet exemple.
- b) Suite à la création des VCR de non-agrégation, le NM configure la durée d'agrégation et la VCR d'agrégation de données pour l'appareil de terrain B ainsi que la durée d'agrégation et la VCR d'agrégation de paquets pour l'appareil de routage R. Les durées d'agrégation correspondent à la vitesse minimale de mise à jour des données parmi tous les UAO dans un appareil de terrain ou à la vitesse minimale de mise à jour des données parmi tous les appareils de terrain pour un appareil de routage. Dans la mesure où la vitesse de mise à jour des données de b1 et b2 est de 4 s, la durée d'agrégation du DAGO dans l'appareil de terrain B est de quatre secondes; la VCR d'agrégation de données de l'appareil de terrain B est indiquée par DAG_vcr et ses points d'extrémité sont le DAGO dans l'appareil de terrain B et le DGO dans l'appareil de passerelle. La durée d'agrégation de l'appareil de routage R est réglée à la vitesse minimale de mise à jour des données dans un groupe. Du fait que la vitesse minimale de mise à jour des données parmi a1, a2, b1 et b2 correspond à une seconde, la durée d'agrégation de l'appareil de routage R est définie sur 1 s. La VCR d'agrégation de paquets de l'appareil de routage R est indiquée par PAG_vcr et ses points d'extrémité sont le PAGO dans l'appareil de routage R et le DGO dans l'appareil de passerelle.
- c) Après l'établissement de A_vcr1, A_vcr2, DAG_vcr et PAG_vcr, le DAGO, le PAGO et le DGO commencent à fonctionner. Le DAGO dans l'appareil de terrain B utilise l'heure d'arrivée du premier paquet (devant être agrégé) comme instant de départ et agrège les paquets puis les envoie à l'appareil de routage R via DAG_vcr à l'intervalle de temps d'agrégation configuré. Le PAGO dans l'appareil de routage R utilise l'heure d'arrivée du premier paquet (devant être agrégé) comme instant de départ et agrège les paquets dans le processus DMAP puis les envoie au DGO via PAG_vcr dans l'appareil de passerelle à l'intervalle de temps d'agrégation configuré.
- d) Après que le DGO de l'appareil de passerelle a reçu les paquets agrégés, il désagrège les paquets et trouve les UAO correspondants conformément à l'adresse source du paquet et aux identificateurs des objets UAO.
- e) Le processus DMAP dans l'appareil de passerelle envoie les paquets désagrégés aux objets UAO correspondants.

6.6.4 Gestion des objets d'agrégation et de désagrégation

Les attributs de la classe DAGO sont indiqués au Tableau 6.

Tableau 6 – Attributs de la classe DAGO

ID d'attribut	Nom	Type de données	Valeur par défaut	Utilisation	Description	Méthode de prise en charge
0	DagoID	Unsigned8	0	Obligatoire	Identificateur du DAGO	READ
1	DagoRevision	Unsigned8	0	Facultatif	Version définie par le DAGO	READ

Les attributs de l'instance DAGO sont indiqués au Tableau 7.

Tableau 7 – Attributs de l'instance DAGO

ID d'attribut	Nom	Type de données	Valeur par défaut	Utilisation	Description	Méthode de prise en charge
0	DagoInsID	Unsigned8	0	Obligatoire	Identificateur de l'instance DAGO	READ
1	DagoPeriod	Unsigned8	1	Obligatoire	Cycle d'agrégation (en secondes)	READ/WRITE
2	DagoMemNum	Unsigned8	1	Obligatoire	Nombre des objets UAO agrégés	READ/WRITE
3	DagoMemLst	Structure MEM_STRUCT (voir Tableau 8)		Facultatif	Liste des objets UAO agrégés	READ/WRITE
4	DagoMemData Size	Unsigned8	0	Facultatif	Longueur des données agrégées DagoMemData (en octets)	READ/WRITE
5	DagoMemData	Octetstring		Obligatoire	Données des objets UAO agrégés	READ/WRITE

Les méthodes prises en charge par les objets DAGO sont indiquées au Tableau 171.

La définition de la structure MEM_STRUCT est indiquée au Tableau 8.

Tableau 8 – Structure MEM_STRUCT

ID d'attribut	Nom	Type de données	Description
0	AppObjID	Unsigned8	Identificateur de l'objet UAO
1	AppObjInsID	Unsigned8	Identificateur de l'instance UAO
2	AppObjAttrID	Unsigned8	Identificateur d'attribut de l'instance UAO

Les attributs de la classe PAGO sont indiqués au Tableau 9.

Tableau 9 – Attributs de la classe PAGO

ID d'attribut	Nom	Type de données	Valeur par défaut	Utilisation	Description	Méthode de prise en charge
0	PagoID	Unsigned8	1	Obligatoire	Identificateur de l'objet PAGO	READ
1	PagoRevision	Unsigned8	0	Facultatif	Version définie par le PAGO	READ

Les attributs de l'instance PAGO sont indiqués au Tableau 10.

Tableau 10 – Attributs de l'instance PAGO

ID d'attribut	Nom	Type de données	Valeur par défaut	Utilisation	Description	Méthode de prise en charge
0	PagoInsID	Unsigned8	0	Obligatoire	Identificateur de l'instance d'agrégation d'objet	READ
1	PagoPeriod	Unsigned8	1	Obligatoire	Cycle d'agrégation (en secondes)	READ/WRITE
2	PagoMemNum	Unsigned8	1	Obligatoire	Nombre des éléments de groupe agrégés	READ/WRITE
3	PagoMemLst	Octetstring		Facultatif	Liste des éléments de groupe agrégés	READ/WRITE
4	PagoDataSize	Unsigned8	0	Facultatif	Longueur du paquet agrégé (en octets)	READ/WRITE
5	PagoMemData	Octetstring		Obligatoire	Données des éléments de groupe agrégés	READ/WRITE

Les méthodes prises en charge par les objets PAGO sont indiquées au Tableau 171.

Les attributs de la classe DGO sont indiqués au Tableau 11.

Tableau 11 – Attributs de la classe DGO

ID d'attribut	Nom	Type de données	Valeur par défaut	Utilisation	Description	Méthode de prise en charge
0	DgoID	Unsigned8	2	Obligatoire	Identificateur de l'objet DGO	READ
1	DgoRevision	Unsigned8	0	Facultatif	Révision définie par le DGO	READ

Les attributs de l'instance DGO sont indiqués au Tableau 12.

Tableau 12 – Attributs de l'instance DGO

ID d'attribut	Nom	Type de données	Valeur par défaut	Utilisation	Description	Méthode de prise en charge
0	DgoInsID	Unsigned8	0	Obligatoire	Identificateur de l'instance DGO	READ

Les méthodes prises en charge par les objets DGO sont indiquées au Tableau 171.

6.7 Surveillance de performance

6.7.1 Rapport sur la défaillance des chemins

Le rapport sur la défaillance des chemins est utilisé par les appareils de routage pour signaler des événements défaillance de chemin au NM par le biais des chemins redondants. Le processus de rapport sur la défaillance des chemins est indiqué à la Figure 18 (voir 9.5.12).

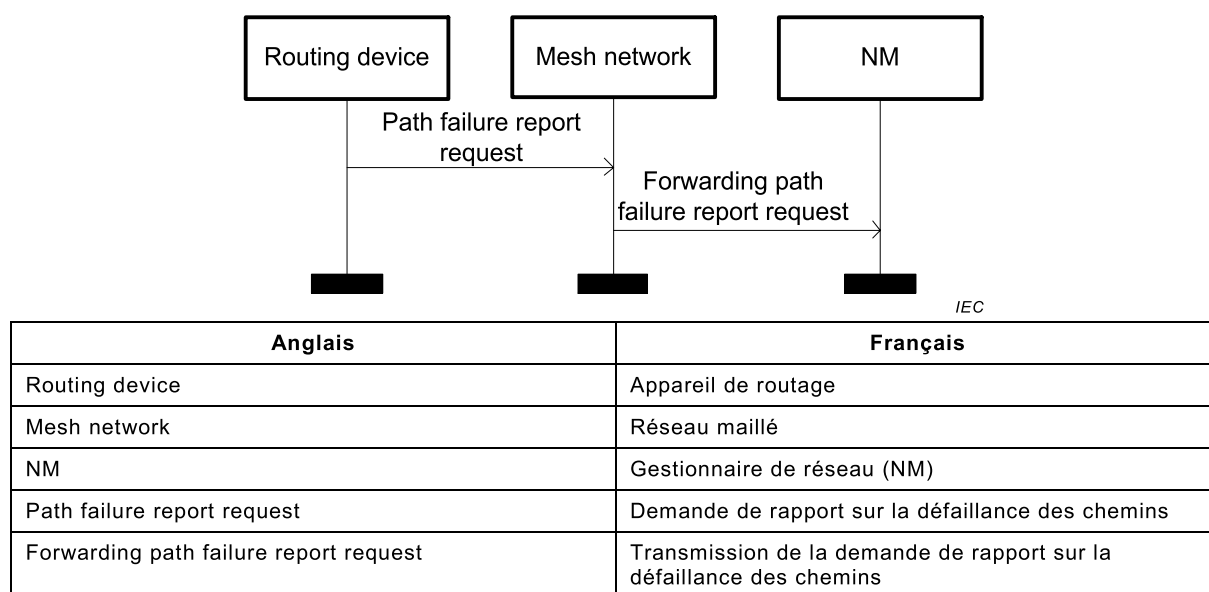


Figure 18 – Processus de rapport sur la défaillance des chemins

6.7.2 Rapport sur l'état des appareils

Après avoir reçu des appareils de terrain intragroupe les rapports sur l'état des appareils, un appareil de routage adresse périodiquement au NM un rapport sur sa propre santé et celle de ses appareils de terrain. Le NM évalue et diagnostique la performance du réseau en fonction des informations de santé puis répond dans les délais au changement d'environnement du réseau. Il convient que le NM détecte des conditions anormales dans l'appareil WIA-PA, tel qu'un faible niveau de puissance de la batterie ou la déconnexion d'appareils voisins. Cela est réalisé en fixant des niveaux d'alarme aux appareils WIA-PA. Les processus de rapport sur l'état des appareils pour l'appareil de terrain et l'appareil de routage sont indiqués à la Figure 19 et à la Figure 20 (voir 9.5.10).

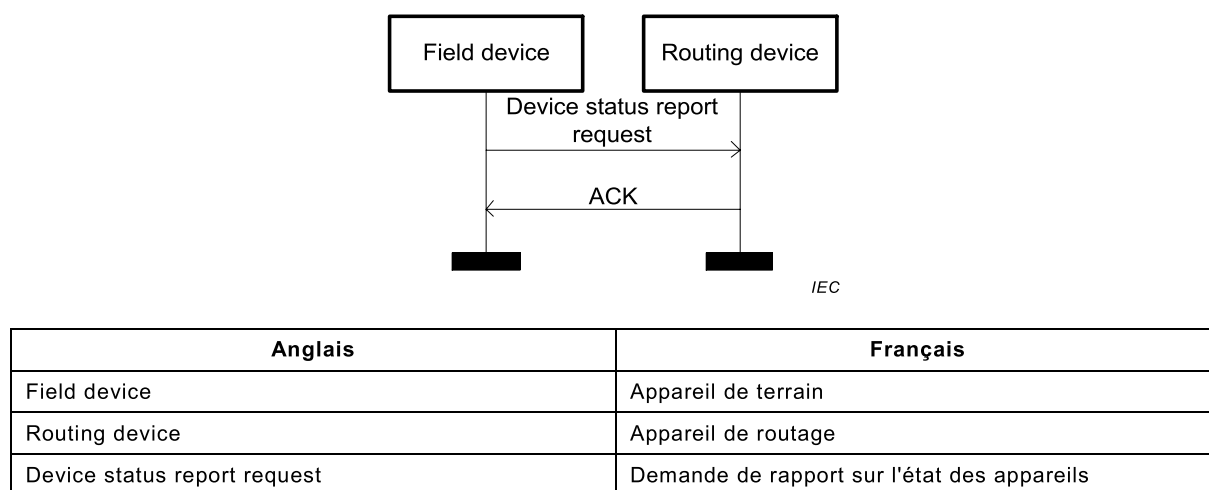


Figure 19 – Processus de rapport sur l'état des appareils pour l'appareil de terrain

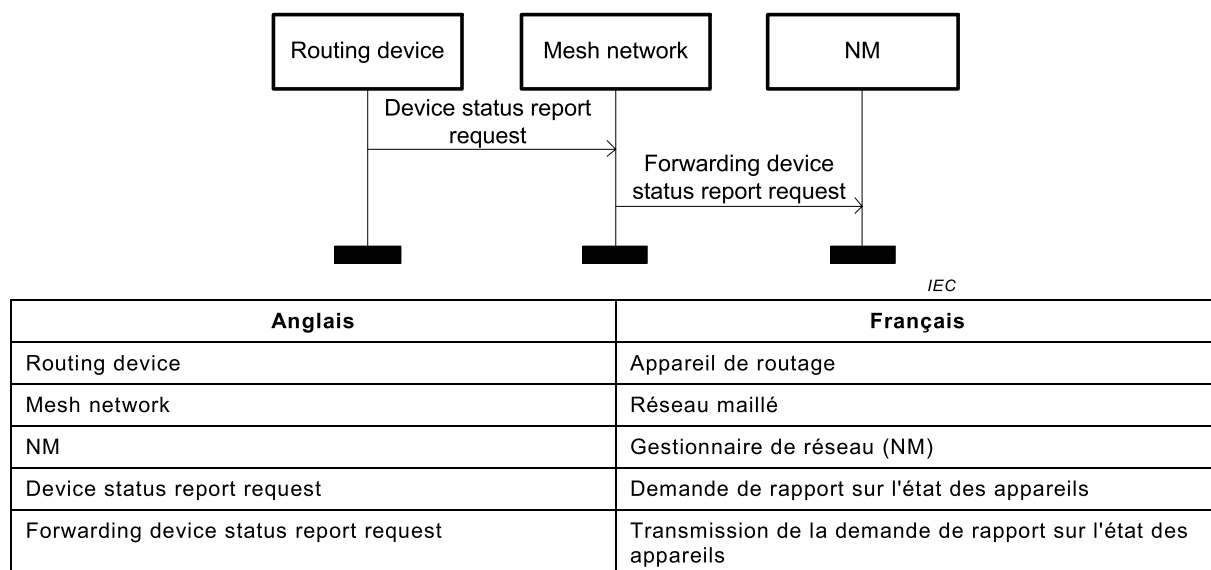


Figure 20 – Processus de rapport sur l'état des appareils pour l'appareil de routage

6.7.3 Rapport sur la condition des canaux

Le rapport sur la condition des canaux est utilisé pour que les appareils de terrain WIA-PA ou les appareils de routage rapportent à distance au NM la condition des canaux. Le processus de rapport sur la condition des canaux est indiqué à la Figure 21 (voir 9.5.11).

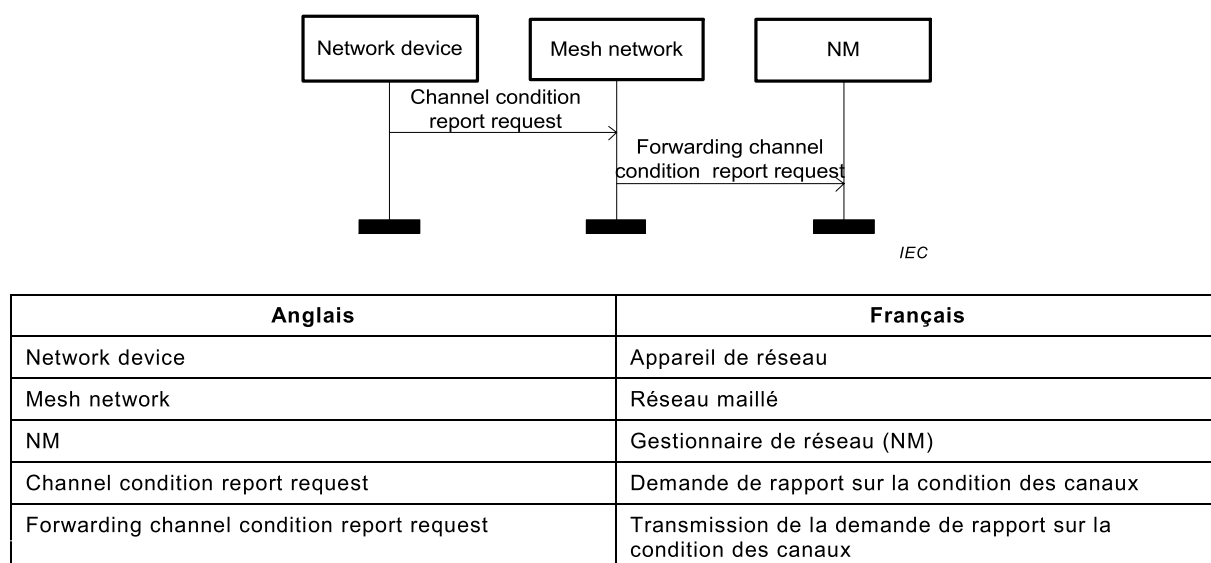


Figure 21 – Processus de rapport sur la condition des canaux

6.8 Processus de départ

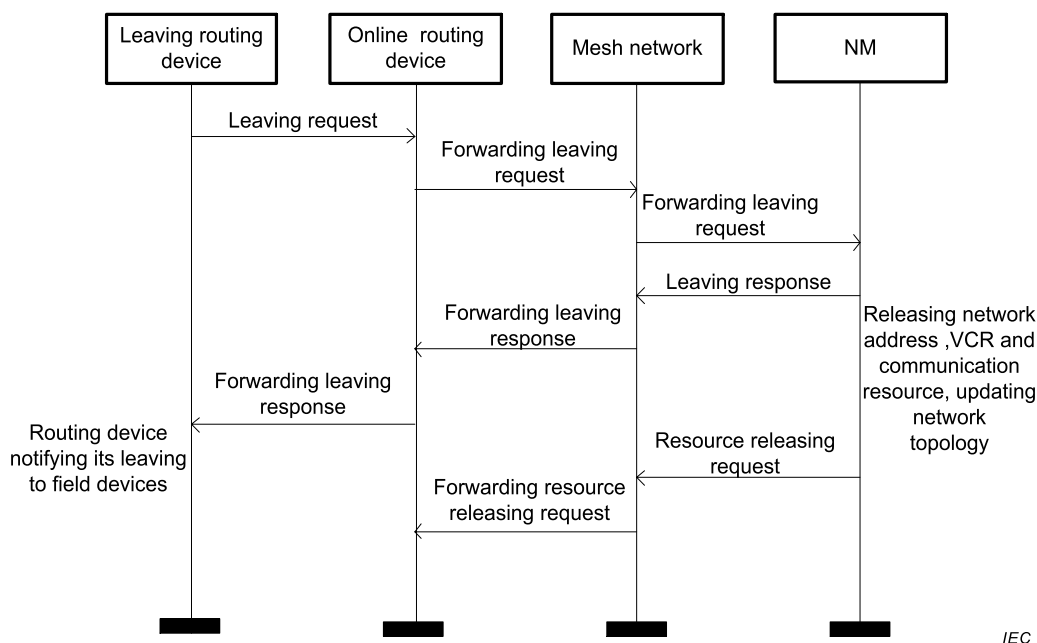
6.8.1 Généralités

Le processus de départ des appareils WIA-PA inclut le processus de départ anormal, le processus de départ actif et le processus de départ passif. Le processus de départ anormal est causé par la défaillance d'un appareil, l'invalidation d'un appareil et l'épuisement de l'énergie, qu'il convient de juger par la trame de commande d'entretien de la DLSL. Le départ actif est une fonction facultative qui est activée par la configuration de ActiveLeavingEnable sur la valeur 1 (voir 6.9.1.2.1). Le départ actif est demandé par les appareils de terrain à partir de leurs appareils de routage ou par les appareils de routage à partir de l'appareil de passerelle. Le départ passif est demandé par l'appareil de passerelle à partir des appareils de routage ou par les appareils de routage à partir de leurs appareils de terrain.

6.8.2 Processus de départ d'un appareil de routage

Le réseau WIA-PA spécifie deux processus de départ pour les appareils de routage: le départ actif et le départ passif. Le processus de départ actif d'un appareil de routage se déroule comme suit (voir Figure 22).

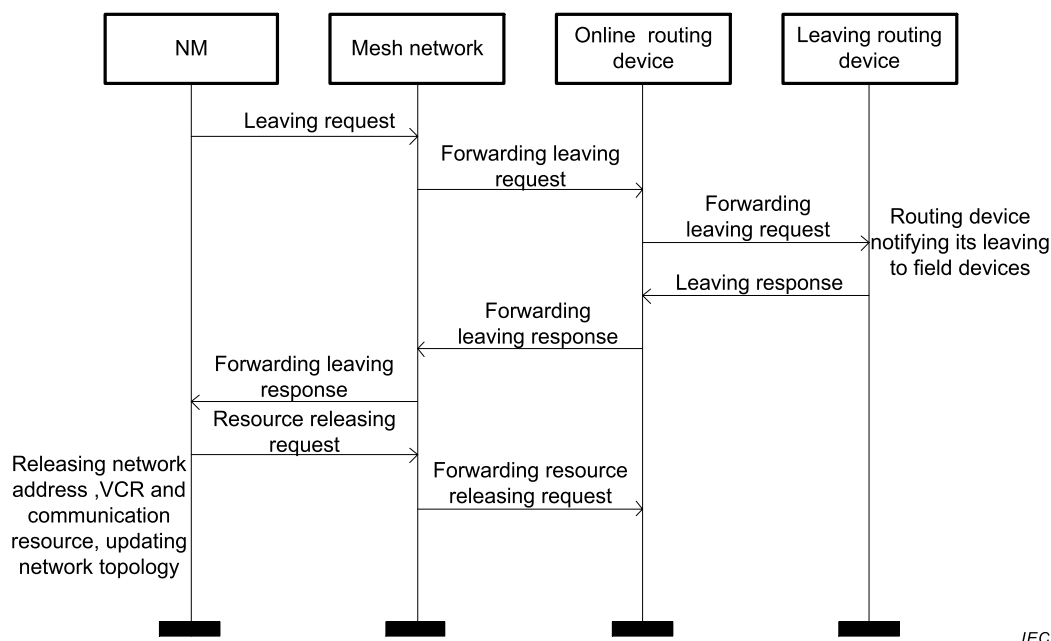
- Un appareil de routage envoie la demande de départ au NM.
- Le NM fournit une réponse relative au départ à l'appareil de routage.
- Après avoir reçu une réponse positive, l'appareil de routage notifie ses appareils de terrain du départ. Après le départ passif des appareils de terrain, l'appareil de routage quitte le réseau.
- Le NM libère l'adresse réseau, la VCR et les ressources de communication de l'appareil de routage parti et met à jour la topologie de réseau.
- Le NM notifie aux appareils de routage qui ont une relation de communication avec l'appareil de routage parti de libérer les ressources de communication associées.



Anglais	Français
Leaving routing device	Appareil de routage partant
Online routing device	Appareil de routage en ligne
Mesh network	Réseau maillé
NM	Gestionnaire de réseau (NM)
Leaving request	Demande de départ
Forwarding leaving request	Transmission de la demande de départ
Releasing network address, VCR and communication resource, updating network topology	Libération de l'adresse réseau, de la VCR et de la ressource de communication, mise à jour de la topologie réseau
Leaving response	Réponse de départ
Forwarding leaving response	Transmission de la réponse de départ
Routing device notifying its leaving to field devices	Appareil de routage notifiant son départ aux appareils de terrain
Resource releasing request	Demande de libération de ressource
Forwarding resource releasing request	Transmission de la demande de libération de ressource

Figure 22 – Processus de départ actif d'un appareil de routage

- a) Le NM envoie la demande de départ à un appareil de routage.
- b) L'appareil de routage notifie son départ aux appareils de terrain.
- c) Après le départ passif des appareils de terrain, l'appareil de routage envoie au NM une réponse de départ.
- d) Le NM libère l'adresse réseau, la VCR et les ressources de communication et met à jour la topologie de réseau après avoir reçu la réponse de départ issue de l'appareil de routage.
- e) Le NM notifie aux appareils de routage qui ont une relation de communication avec l'appareil de routage parti de libérer les ressources de communication associées.



Anglais	Français
NM	Gestionnaire de réseau (NM)
Mesh network	Réseau maillé
Online routing device	Appareil de routage en ligne
Leaving routing device	Appareil de routage partant
Leaving request	Demande de départ
Forwarding leaving request	Transmission de la demande de départ
Routing device notifying its leaving to field devices	Appareil de routage notifiant son départ aux appareils de terrain
Leaving response	Réponse de départ
Forwarding leaving response	Transmission de la réponse de départ
Releasing network address, VCR and communication resource, updating network topology	Libération d'adresse réseau, de la VCR et de ressource de communication, mise à jour de topologie réseau
Resource releasing request	Demande de libération de ressource
Forwarding resource releasing request	Transmission de la demande de libération de ressource

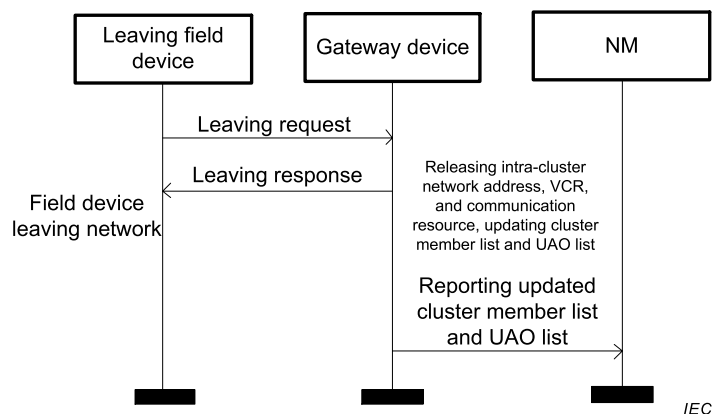
Figure 23 – Processus de départ passif d'un appareil de routage

6.8.3 Processus de départ d'un appareil de terrain

Le réseau WIA-PA spécifie deux processus de départ pour les appareils de terrain: le départ actif et le départ passif.

Le processus de départ actif d'un appareil de terrain se déroule comme suit (voir Figure 24 et Figure 25).

- Un appareil de terrain envoie la demande de départ à l'appareil de routage ou à l'appareil de passerelle dans un groupe.
- L'appareil de routage ou l'appareil de passerelle renvoie une réponse de départ à l'appareil de terrain sur le départ.
- L'appareil de routage ou l'appareil de passerelle libère l'adresse réseau intragroupe, la VCR et les ressources de communication puis met à jour la liste des éléments de groupe et la liste des objets UAO de l'appareil de terrain qui a quitté le réseau.
- Après avoir reçu la réponse, l'appareil de terrain quitte le réseau.
- Si l'appareil de terrain quitte l'appareil de routage, l'appareil de routage envoie au NM la liste des éléments de groupe et la liste des UAO mises à jour.



Anglais	Français
Leaving field device	Appareil de terrain partant
Gateway device	Appareil de passerelle
NM	Gestionnaire de réseau (NM)
Leaving request	Demande de départ
Releasing intra-cluster network address, VCR, and communication resource, updating cluster member list and UAO list	Libération d'adresse réseau intragroupe, de la VCR et de la ressource de communication, mise à jour de la liste des éléments du groupe et de la liste des objets UAO
Leaving response	Réponse de départ
Field device leaving network	Appareil de terrain quittant le réseau
Reporting updated cluster member list and UAO list	Production d'un rapport sur la liste mise à jour des éléments de groupe et la liste mise à jour des objets UAO

Figure 24 – Processus de départ actif d'un appareil de terrain (quittant l'appareil de passerelle)

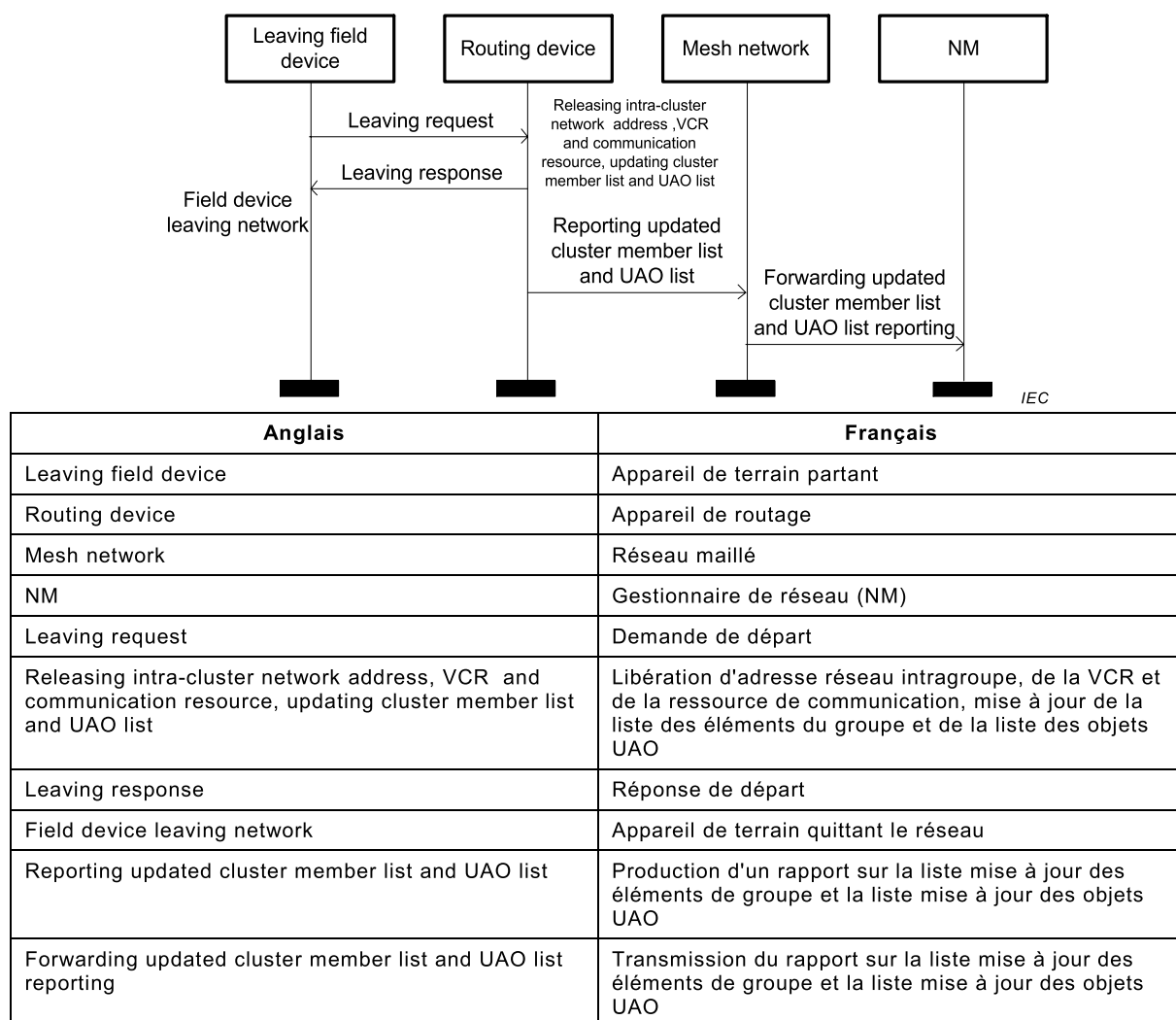


Figure 25 – Processus de départ actif d'un appareil de terrain (quittant l'appareil de routage)

Le processus de départ passif d'un appareil de terrain se déroule comme suit (voir Figure 26 et Figure 27).

- L'appareil de routage ou l'appareil de passerelle envoie la demande de départ à l'appareil de terrain.
- L'appareil de terrain renvoie la réponse de départ à l'appareil de routage ou à l'appareil de passerelle.
- L'appareil de terrain quitte le groupe.
- L'appareil de routage ou l'appareil de passerelle libère l'adresse réseau intragroupe, la VCR et les ressources de communication de l'appareil de terrain sur le départ puis met à jour la liste des éléments de groupe et la liste des objets UAO.
- Si l'appareil de terrain quitte l'appareil de routage, l'appareil de routage notifie au NM l'élément de groupe et sa liste des UAO.

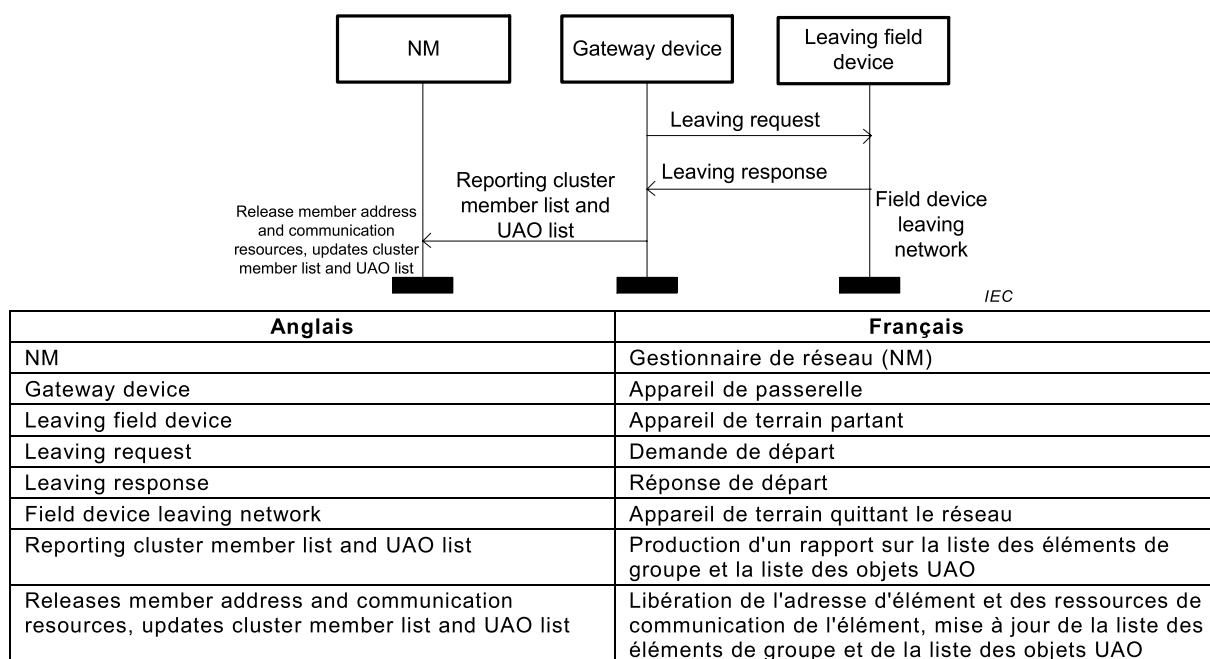


Figure 26 – Processus de départ passif d'un appareil de terrain (quittant l'appareil de passerelle)

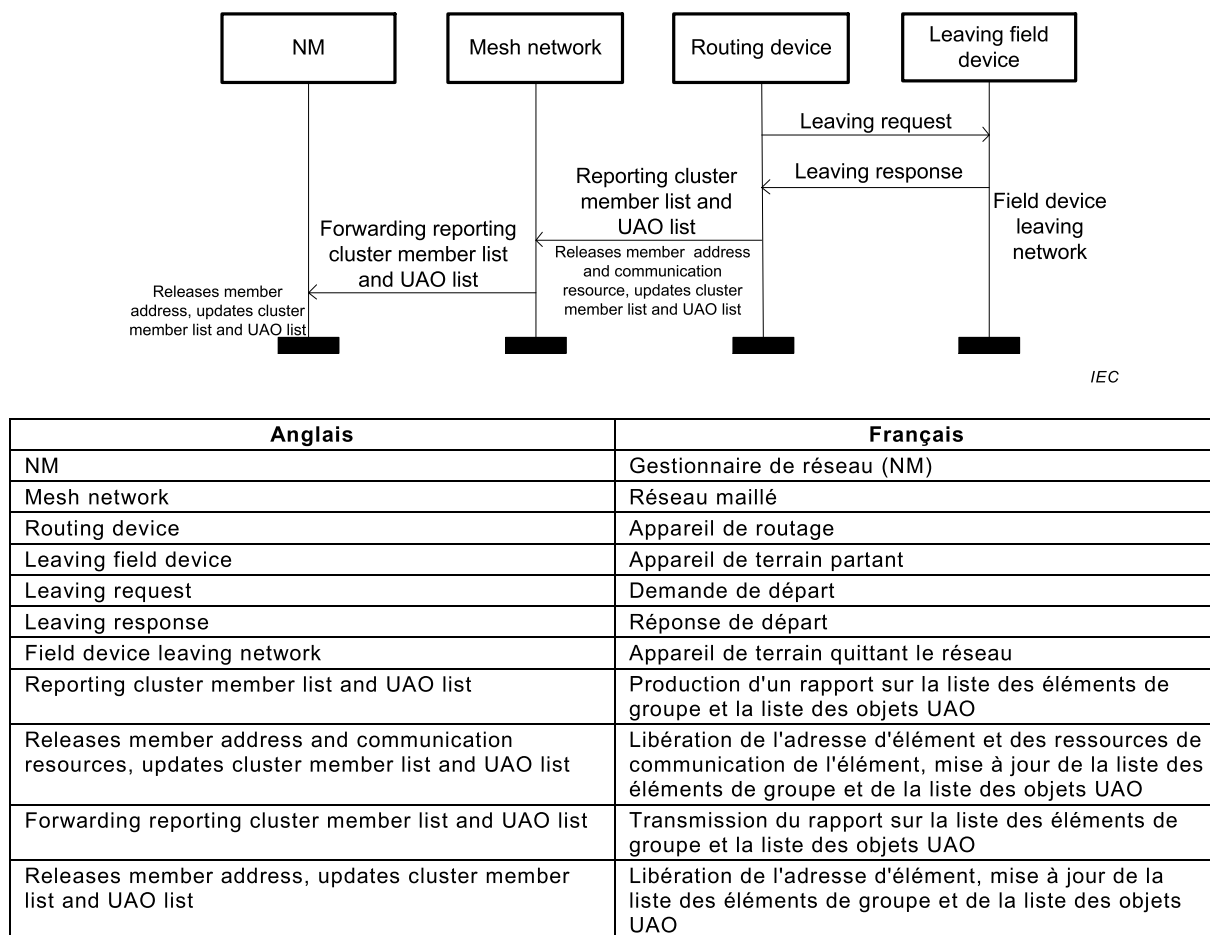


Figure 27 – Processus de départ passif d'un appareil de terrain (quittant l'appareil de routage)

6.9 Services et base d'informations de gestion

6.9.1 Base d'informations de gestion

6.9.1.1 Généralités

Les éléments stockés dans la base d'informations de gestion (MIB) sont appelés attributs et sont utilisés pour la surveillance et la configuration des paramètres du réseau WIA-PA. Le NM peut accéder à ces attributs et les mettre à jour.

En fonction des types de stockage, les attributs de la MIB sont classés en trois catégories:

- a) attribut constant,
- b) attribut statique, et
- c) attribut dynamique.

Un attribut constant, tel que le numéro de série d'un appareil sans fil, est interchangeable au fil du temps. L'attribut constant est réglé lorsque les fabricants transmettent les appareils. Il convient de ne pas le modifier.

Un attribut statique, tel qu'une limite d'alarme, change de valeur peu fréquemment. Il convient de préserver la valeur de l'attribut statique après un redémarrage à chaud, une réinitialisation ou une panne d'alimentation électrique.

Un attribut dynamique change fréquemment de valeur sans la moindre commande extérieure. La valeur de l'attribut dynamique sera perdue après un redémarrage à chaud, une réinitialisation ou une panne d'alimentation électrique. Le redémarrage à chaud est une séquence d'opérations réalisée pour réinitialiser un appareil préalablement exploité qui a subi un arrêt inopiné. Lorsqu'un appareil est réinitialisé, il entre dans l'état Idle (repos). Une panne d'alimentation électrique indique que l'alimentation électrique disponible utilisée par les appareils est devenue dangereusement faible.

En fonction des types de données d'attribut, les attributs de la MIB sont divisés en attributs non structurés et structurés.

En fonction des exigences de mise en œuvre, les attributs de la MIB sont divisés en attributs obligatoires et facultatifs.

Il existe deux types de droits d'accès aux attributs de la MIB.

- a) R (Read), qui signifie que les valeurs de l'attribut peuvent être lues par d'autres appareils dans le réseau WIA-PA; et
- b) W (Write), qui signifie que les valeurs de l'attribut peuvent être configurées par d'autres appareils dans le réseau WIA-PA.

6.9.1.2 Attributs MIB

6.9.1.2.1 Attributs non structurés

Les attributs non structurés sont énumérés dans le Tableau 13. Les valeurs des attributs comprises entre 0 et 28 sont identiques dans tout le réseau et les valeurs des attributs comprises entre 29 et 33 sont spécifiques à l'appareil.

Tableau 13 – Attributs non structurés (1 de 5)

ID	Nom	Type de données	Plage valide	Type d'accès	Type de stockage	Valeur par défaut	Description
0	ProtocolVersion ^{de}	Unsigned16	0 à 65 535	R	Statique	2013	Version de protocole de la pile de protocole du réseau WIA-PA actuelle, indiquée en années.
1	NetworkID ^{e#}	Unsigned8	0 à 255	R/W	Statique	0	Identificateur de réseau, utilisé lorsque plusieurs réseaux coexistent
2	StatisticsDuration ^{e*}	Unsigned16	0 à 65 535	R/W	Statique	0	Configuration du cycle de recueil statistique (en secondes). Au bout de cette durée, les appareils WIA-PA mettent à jour les données statistiques dans les tables des voisins. La valeur 0 indique que l'appareil ne recueille aucune donnée statistique.
3	MaxNSDUSize ^{e*}	Unsigned8	0 à 255	R	Statique	71	Taille maximale de l'unité de données de service prise en charge par la couche réseau (NL), en octets. MaxNSDUSize = aMaxPHYPacketSize – longueur maximale de l'en-tête MAC – longueur maximale de l'en-tête DLSL – longueur maximale de l'en-tête de NL. Voir Tableau 70 de l'IEEE 802.15.4-2011 pour aMaxPHYPacketSize.
4	BitMapa ^{e*}	Unsigned32	32 bits	R/W	Dynamique	0x FFFF	Chaque bit indique si un canal peut être utilisé: 0 = Non utilisé 1 = Utilisé La valeur du bit i indique l'état d'utilisation du canal i. La valeur du bit i indique s'il est utilisé ou non, conformément au numéro de canal de l'IEEE 802.15.4-2011.
5	KeepAliveDuration ^{e*}	Unsigned24	0 à (2 ²⁴ -1)	R/W	Statique	1 000	Durée entre deux trames d'entretien (en millisecondes). La valeur 0 n'est pas valide.
6	TimeSynDuration ^{e*}	Unsigned24	0 à (2 ²⁴ -1)	R/W	Statique	25 000	Durée entre deux trames de synchronisation du temps (en millisecondes). La valeur par défaut est calculée d'après l'hypothèse supposant que la dérive de l'oscillateur à quartz est de 20 parties par million et que l'erreur de synchronisation correspond à 1 ms. La valeur 0 n'est pas valide.

Tableau 13 (2 de 5)

ID	Nom	Type de données	Plage valide	Type d'accès	Type de stockage	Valeur par défaut	Description
7	ChannelThreshold ^{e*}	Unsigned8	0 à (macMaxFrameRetries – 2)	R/W	Statique	1	Seuil de commutation de canal dans le saut de fréquence adaptatif, indiqué comme comptage des nouvelles tentatives; voir Tableau 52 de l'IEEE 802.15.4-2011 pour macMaxFrameRetries.
8	SecEnableFlag ^{e*}	Booléen	0, 1	R/W	Statique	0	Fanion Security enable (activation de la sécurité): 0 = l'ensemble du réseau a besoin d'une authentification 1 = l'ensemble du réseau n'a pas besoin d'une authentification
9	KeyupdateDur ^{be*}	Unsigned32	0 à (2 ³² -1)	R/W	Dynamique	0	Cycle de mise à jour de clé (en millisecondes). La valeur 0 indique que les clés ne sont pas mises à jour.
10	MaxAttackedCnt ^{be*}	Unsigned16	0 à 65 535	R/W	Statique	5	Nombre maximal d'attaques. La valeur 0 indique que cet attribut n'est pas valide.
11	MaxKeyAttacked-Cnt ^{be*}	Unsigned16	0 à 65 535	R/W	Statique	1	Nombre maximal de clés attaquées.
12	MICFailerTimeUnit ^{be*}	Unsigned16	0 à 65 535	R/W	Statique	60	Intervalle de temps en secondes utilisé pour compter MaxAttackedCnt.
13	Alert ^{be*}	Unsigned16	0 à 65 535	R/W	Statique	0	Les bits de 0 à 6 représentent l'alerte de sécurité, la valeur 1 représente une alerte: Bit0 = AttackedCount atteint MaxAttackedCnt Bit1 = KS est attaquée Bit2 = KJ est attaquée Bit3 = DLKEK est attaquée Bit4 = ALKEK est attaquée Bit5 = DLKED est attaquée Bit6 = ALKED est attaquée
14	EtoEACKTimeOut ^{e*}	Unsigned24	0 à (2 ²⁴ -1)	R/W	Statique	100*macMaxFrameRetries	Limite supérieure du temps d'attente pour l'acquittement de bout en bout (en millisecondes). Voir Tableau 52 de l'IEEE 802.15.4-2011 pour macMaxFrameRetries.
15	TimeSlotDuration ^{e*}	Unsigned16	0 à 65 535	R/W	Statique	N/A	Indiquant la durée de l'intervalle de temps. La durée d'intervalle de temps est calculée par: (aBaseSlotDuration×2TimeSlotDuration). Voir Tableau 51 de l'IEEE 802.15.4-2011 pour aBaseSlotDuration.

Tableau 13 (3 de 5)

ID	Nom	Type de données	Plage valide	Type d'accès	Type de stockage	Valeur par défaut	Description
16	PLRThreshold ^{e*}	Unsigned8	0 à 100	R/W	Statique	50	Seuil de taux de perte de paquets, qui correspond à PLRThreshold divisé par 100 et qui est utilisé pour la commutation de fréquence adaptative. Voir 8.4.5 pour la commutation de fréquence adaptative.
17	CmemRptCycle ^{ce*}	Unsigned16	0 à 65 535	R/W	Statique	Cycle maximal de super-trame de l'ensemble du réseau WI A-PA	Configuration du cycle de production de rapports sur les informations d'élément de groupe (en secondes) La valeur 0 n'est pas valide.
18	ChaStaRptCycle ^{e*}	Unsigned16	0 à 65 535	R/W	Statique	Cycle maximal de super-trame de l'ensemble du réseau WI A-PA	Configuration du cycle de production de rapports sur les informations concernant la condition des canaux (en secondes) La valeur 0 n'est pas valide.
19	DevStaRptCycle ^{e*}	Unsigned16	0 à 65 535	R/W	Statique	Cycle maximal de super-trame de l'ensemble du réseau WI A-PA	Configuration du cycle de production de rapports sur les informations concernant l'état des appareils (en secondes) La valeur 0 n'est pas valide.
20	PathFailRptCycle ^{ce*}	Unsigned16	0 à 65 535	R/W	Statique	Cycle maximal de super-trame de l'ensemble du réseau WI A-PA	Configuration du cycle de production de rapports sur les informations sur les chemins défectueux (en secondes) La valeur 0 n'est pas valide.
21	MaxEtoERetry ^{e*}	Unsigned8	0 à 255	R/W	Statique	1	Le nombre maximal des tentatives de bout en bout
22	NetworkTopology ^{e*}	Booléen	0, 1	R/W	Statique	1	Indique la topologie de réseau: 0 = réseau hiérarchique qui est la combinaison de la configuration en étoile et de la configuration maillée 1 = topologie de réseau en étoile uniquement
23	UTCTime ^e	Unsigned32	0 à (2 ³² -1)	R/W	Dynamique	0	Temps universel coordonné (TUC)

Tableau 13 (4 de 5)

ID	Nom	Type de données	Plage valide	Type d'accès	Type de stockage	Valeur par défaut	Description
24	ActiveLeaving-Enable ^e	Booléen	0, 1	R/W	Statique	0	Fanion qui indique si la fonction de départ actif est activée: 0 = Désactivée 1 = Activée
25	SecMode ^{be*}	Unsigned8	0 à 3	R/W	Statique	0	Le bit 0 indique si la DLSP utilise ou non un service de sécurité: 0 = Non utilisé 1 = Utilisé Le bit 1 indique si la couche Application (AL) utilise ou non un service de sécurité: 0 = Non utilisé 1 = Utilisé
26	SecLevel ^{b*}	Unsigned8	0 à 63	R/W	Statique	0	Les bits 0, 1 et 2 représentent les niveaux de sécurité des trames DLSP. 000 = Aucun 001 = MIC-32 010 = MIC-64 011 = MIC-128 100 = Chiffrement 101 = Chiffrement-MIC-32 110 = Chiffrement-MIC-64 111 = Chiffrement-MIC-128 Les bits 3, 4 et 5 représentent les niveaux de sécurité des paquets AL. 000 = Aucun 001 = Chiffrement 010 = MIC-32 011 = Chiffrement-MIC-32 Les autres valeurs sont réservées.
27	CountryCode ^{e*}	Unsigned16	0 à 65 535	R/W	Dynamique	0x3C00	Code de pays qui fournit les lignes directrices relatives au lieu et aux contraintes de réglementation. Voir 8.4.11 pour plus de détails
28	EtoEACKEnable ^{e*}	Bool	0, 1	R/W	Dynamique	0	Fanion indiquant si le réseau WIA-PA prend en charge l'acquittement (ACK) de bout en bout: 0 = Non-prise en charge 1 = Prise en charge

Tableau 13 (5 de 5)

ID	Nom	Type de données	Plage valide	Type d'accès	Type de stockage	Valeur par défaut	Description
29	AuthenState ^{be}	Booléen	0, 1	R/W	Dynamique	0	Fanion qui indique si un appareil WIA-PA a été authentifié comme étant un appareil légitime: 0 = Non authentifié 1 = Authentifié
30	AuthenTime ^{be}	Unsigned32	0 à (2 ³² -1)	R/W	Dynamique	0	Heure à laquelle un appareil est authentifié (en TUC)
31	AggPeriod ^{be*}	Unsigned8	0 à 255	R/W	Statique	N/A	Durée d'agrégation (en millisecondes). Cette valeur n'est valide que si aggsupport=1 et enable=1.
32	ObjectNumber ^{e*}	Unsigned8	0 à 255	R/W	Statique	N/A	Nombre d'objets UAO.
33	AbsoluteSlotNumber ^e	Unsigned48	0 à (2 ⁴⁸ -1)	R/W	Dynamique	0	Nombre d'intervalles de temps depuis le démarrage du réseau, c'est-à-dire l'intervalle de temps courant, augmentant de la valeur 1.
^a Attributs facultatifs pour l'appareil de terrain/l'appareil tenu à la main. ^b Attributs facultatifs pour l'ensemble des appareils dans les réseaux WIA-PA. ^c Attributs non sélectionnés par l'appareil de terrain/l'appareil tenu à la main. ^d ProtocolVersion est configuré par les fabricants. ^e Les attributs numérotés de 0 à 33 sont stockés par tous les types d'appareils WIA-PA. Si la valeur par défaut d'un attribut est N/A, les utilisateurs peuvent la configurer; en revanche, si la valeur par défaut d'un attribut est spécifiée, il convient que les utilisateurs la configurent conformément aux scénarios d'application actuels. # Attributs configurés par l'appareil tenu à la main. * Attributs configurés par l'appareil de passerelle (GW).							

6.9.1.2.2 Attributs structurés

Les attributs structurés sont énumérés dans le Tableau 14.

Tableau 14 – Attributs structurés

ID	Nom	Type de données	Type d'accès	Type de stockage	Valeur par défaut	Description
100	RouteTable	Structure NLRoute_Struct (voir Tableau 15)	R/W	Dynamique		Inclut l'ID d'itinéraire, l'adresse de destination, l'adresse du prochain saut et le compteur de nouvelles tentatives. Chaque élément de la liste est identifié par l'indice de stockage.
101	Superframe	Structure Superframe_Struct (voir Tableau 16)	R/W	Dynamique		Décrivant les informations relatives à la superframe. Chaque élément de la liste est identifié par l'indice de stockage.
102	Link	Structure Link_Struct (voir Tableau 17)	R/W	Dynamique		Décrivant les informations relatives à la liaison. Chaque élément de la liste est identifié par l'indice de stockage.
103	Neighbour ^a	Structure Neighbour_Struct (voir Tableau 18)	R/W	Dynamique		Décrivant les informations relatives aux appareils des voisins. Chaque élément de la liste est identifié par l'indice de stockage.
104	ChannelCondition	Structure ChanCon_Struct (voir Tableau 19)	R/W	Dynamique		Enregistrant les informations statistiques relatives à la condition des canaux. Chaque élément de la liste est identifié par l'indice de stockage.
105	DeviceStruct	Structure Device_struct (voir Tableau 20)	R/W	Dynamique/constant/statique		Décrivant les informations relatives aux appareils WIA-PA. Chaque élément de la liste est identifié par l'indice de stockage.
106	VCRList	Structure VCR_Struct (voir Tableau 21)	R/W	Dynamique		Enregistrant les informations relatives aux VCR. Chaque élément de la liste est identifié par l'indice de stockage.
107	DevConRep	Structure DevConRep_Struct (voir Tableau 22)	R/W	Dynamique		Enregistrant les informations relatives à la condition des appareils. Chaque élément de la liste est identifié par l'indice de stockage. Cet attribut est enregistré par les appareils de routage et l'appareil de passerelle.
108	KeyTable ^b	Structure Key_Struct (voir Tableau 23)	R/W	Dynamique		Incluant le type de la clé, la longueur de la clé, l'heure de mise à jour de la clé, l'heure d'utilisation de la clé, la valeur de la clé et le nombre d'attaques contre la clé. Chaque élément de la liste est identifié par l'indice de stockage.
109	ObjList	Structure ObjList_Struct (voir Tableau 24)	R/W	Statique		Liste des identificateurs des objets UAO. Chaque élément de la liste est identifié par l'indice de stockage.

NOTE Les tailles de toutes les listes spécifiées dans le Tableau 14 dépendent de la mise en œuvre.

^a Attributs non sélectionnés par l'appareil de terrain/l'appareil tenu à la main.

^b Attributs facultatifs pour l'ensemble des appareils dans les réseaux WIA-PA.

Le type de données des attributs de routage RouteTable est indiqué au Tableau 15.

Tableau 15 – Structure NLRoute_Struct

Identificateur d'élément d'attribut	Nom	Type de données	Plage valide	Description
0	RouteID	Unsigned16	0 à 65 535	Identificateur de routage unique
1	SourceAddress	Unsigned16	0 à 65 535	Adresse courte de l'appareil source
2	DestinationAddress	Unsigned16	0 à 65 535	Adresse courte de l'appareil de destination
3	NextHop	Unsigned16	0 à 65 535	Adresse courte de l'appareil de prochain saut
4	RetryCounter	Unsigned8	0 à 255	Compteur pour enregistrer les tentatives de bout en bout

Le type de données des attributs de supertrame Superframe est indiqué au Tableau 16.

Tableau 16 – Structure Superframe_Struct

Identificateur d'élément d'attribut	Nom	Type de données	Plage valide	Description
0	SuperframeID	Unsigned16	0 à 65 535	Identificateur unique de la supertrame, fourni par le NM
1	SuperframeMultiple	Unsigned8	0 à 255	SuperframeMultiple = vitesse maximale de mise à jour des données/vitesse minimale de mise à jour des données. Il est utilisé pour limiter la longueur de la supertrame WIA-PA ainsi que pour le traitement de la transmission des données de cycle long. Voir 8.4.6 pour plus de détails
2	NumberSlots	Unsigned16	0 à 65 535	Taille de supertrame (nombres d'intervalles de temps)
3	ActiveFlag	Booléen	0, 1	Fanion de supertrame active: 0 = Inactive 1 = Active
4	ActiveSlot	Unsigned48	0 à ($2^{48}-1$)	Nombre absolu d'intervalles de temps(ASN) lorsqu'une supertrame commence active.

Le type de données des attributs de liaison Link est indiqué au Tableau 17.

Tableau 17 – Structure Link_Struct

Identificateur d'élément d'attribut	Nom	Type de données	Plage valide	Description
0	LinkID	Unsigned16	0 à 65 535	Identificateur unique de la liaison
1	NeighbourAddr	Unsigned16	0 à 65 535	Référence à une entrée de la table de voisins, qui est vide lorsque le NM alloue des liaisons à un appareil de routage pour une communication intragroupe.
2	LinkType	Unsigned8	0 à 31	Le bit 0 indique le type de liaison: 0 = Monodiffusion 1 = Diffusion Le bit 1 et le bit 2 indiquent le caractère d'une liaison: 00 = Transmission 01 = Transmission-partagée 10 = Réception Le bit 3 indique le type d'un intervalle de temps: 0 = Intervalle de temps de données 1 = Intervalle de temps de gestion Le bit 4 indique le caractère d'agrégation: 0 = Intervalle de temps pour paquet non agrégé 1 = Intervalle de temps pour paquet agrégé
3	RelativeSlotNumber	Unsigned16	0 à 65 535	Nombre d'intervalles de temps relatifs
4	LinkSuperframeNum	Unsigned8	0 à 255	LinkSuperframeNum = vitesse de mise à jour des données pour cet appareil et vitesse minimale de mise à jour des données. Il sert à traiter l'émission des données de cycle long.
5	ActiveFlag	Booléen	0, 1	Indique si une liaison est en cours d'utilisation: 0 = Non utilisé 1 = En cours d'utilisation
6	ChannelIndex	Unsigned8	0 à 31	Numéros séquentiels des canaux pour cette liaison, à savoir, les numéros séquentiels des canaux principaux.
7	SuperframeID	Unsigned16	0 à 65 535	Référence à une supertrame dans la table des supertrames

Le type de donnée des attributs des voisins Neighbour est indiqué au Tableau 18.

Tableau 18 – Structure Neighbour_Struct

Identificateur d'élément d'attribut	Nom	Type de données	Plage valide	Description
0	NeighbourAddr	Unsigned16	0 à 65 535	Adresse courte de l'appareil voisin
1	NeighbourStatus	Unsigned8	0 à 3	Le bit 0 indique si l'appareil voisin est une source temporelle principale ou non: 0 = Non 1 = Oui Le bit 1 indique l'état de l'appareil voisin: 0 = Normal 1 = Anormal
2	BackoffCounter	Unsigned8	0 à 31	Compteur de backoff (Compteur de réductions de puissance)
3	BackoffExponent	Unsigned8	0 à 15	Exposant de backoff
4	LastTimeCommunicated	Unsigned48	0 à ($2^{48}-1$)	Heure de la dernière communication avec l'appareil voisin (en ASN)
5	AveRSL	Unsigned8	0 à 255	Niveau moyen des signaux reçus en provenance de l'appareil voisin dans la durée StatisticsDuration
6	PacketsTransmitted	Unsigned16	0 à 65 535	Nombre de trames non diffusées envoyées à l'appareil voisin dans la durée StatisticsDuration
7	AckPackets	Unsigned16	0 à 65 535	Nombre de paquets ACK/NACK attendus reçus dans la durée StatisticsDuration
8	PacketsReceived	Unsigned16	0 à 65 535	Nombre de bons paquets reçus en provenance de l'appareil voisin dans la durée StatisticsDuration
9	BroadcastPackets	Unsigned16	0 à 65 535	Nombre de bons paquets de diffusion reçus en provenance de l'appareil voisin dans la durée StatisticsDuration

Le type de données des attributs de condition des canaux ChannelCondition est indiqué au Tableau 19.

Tableau 19 – Structure ChanCon_Struct

Identificateur d'élément d'attribut	Nom	Type de données	Plage valide	Description
0	DeviceShortAddress	Unsigned16	0 à 65 535	Adresse 16 bits de l'appareil
1	ChannelID	Unsigned8	0 à 255	Le numéro séquentiel du canal
2	NeighbourAddr	Unsigned16	0 à 65 535	Adresse 16 bits de l'appareil voisin
3	LinkQuality	Unsigned8	0 à 255	Valeur d'indication de qualité de liaison (LQI, Link Quality Indication) de chaque canal
4	PacketLossRate	Unsigned16	0 à 65 535	Taux de perte de paquet dans chaque canal, qui est un pourcentage calculé entre les acquittements (ACK) reçus et le nombre total de paquets envoyés
5	RetryNum	Unsigned8	0 à MaxFrameRetries	Le nombre de retransmissions de chaque canal

Le type de données des attributs d'appareil DeviceStruct est indiqué au Tableau 20.

Tableau 20 – Structure Device_struct (1 de 3)

Identifica- teur d'élément d'attribut	Nom	Type de données	Plage valide	Type de stockage	Type d'accès	Valeur par défaut	Description
0	LongAddress	Unsigned64	0 à ($2^{64}-1$)	C	R	N/A	Adresse unique globale de 64 bits Idem que pour le champ DeviceType tel que défini en 6.3.4: 0 = Appareil de passerelle 1 = Appareil de routage 2 = Appareil de terrain 3 = Appareil tenu à la main Les autres valeurs sont réservées.
1	Redundant- DevFlag	Booléen	0, 1	S	R/W	0	Fanion indiquant si un appareil est redondant ou non: 0 = Appareil non redondant 1 = Appareil redondant
2	Redundant- DevLongAddr	Unsigned64	0 à ($2^{64}-1$)	C	R	N/A	Adresse unique globale de 64 bits d'un appareil redondant Idem que pour le champ DeviceType tel que défini en 6.3.4: 0 = Appareil de passerelle 1 = Appareil de routage 2 = Appareil de terrain 3 = Appareil tenu à la main Les autres valeurs sont réservées.
3	NetAddress- Assign	Booléen	0, 1	S	R/W	N/A	Fanion indiquant si l'adresse réseau (voir 6.3.4) a été assignée ou non: 0 = Non 1 = Oui
4	DeviceShort- Address	Unsigned16	0 à 65 535	S	R/W	N/A	Adresse courte de l'appareil WIA- PA Les 8 bits de poids fort sont l'adresse de groupe et les 8 bits de poids faible sont l'adresse intragroupe.
5	ManufacturerID	Unsigned24	0 à ($2^{24}-1$)	C	R	N/A	Identificateur du fabricant
6	DeviceSerial- Num	Unsigned64	0 à ($2^{64}-1$)	C	R	N/A	Numéro de série de l'appareil
7	DeviceVersion	Unsigned8	0 à 255	C	R	N/A	Numéro de version de l'appareil
8	PowerSupply- Status	Unsigned8	0 à 10	S	R/W	N/A	Condition de l'alimentation électrique: 0 = Alimentation électrique fixe 1 = Alimentation la plus puissante 2 = Deuxième alimentation la plus puissante 10 = Alimentation la plus faible
9	RouterCapable	Booléen	0, 1	S	R/W	0	Fanion pour indiquer si l'appareil dispose d'une fonction de routage: 0 = Non 1 = Oui

Tableau 20 (2 de 3)

Identifica- teur d'élément d'attribut	Nom	Type de données	Plage valide	Type de stockage	Type d'accès	Valeur par défaut	Description
10	Devicestate	Unsigned8	0 à 16	S	R/W		Les bits 0 et 1 représentent l'état de rattachement de l'appareil: 00 = Pas rattaché 01 = Rattachement 10 = Authentification de sécurité 11 = Rattaché Les bits 2 et 3 représentent l'état de marche de l'appareil: 00 = Inactive 01 = Actif 10 = Défaillant Les autres valeurs sont réservées.
11	DeviceMemory-total	Unsigned32	0 à (2 ³² -1)	C	R	N/A	Mémoire totale d'un appareil (en octets), notamment RAM, ROM, Flash...
12	DeviceUsed-Memory	Unsigned32	0 à (2 ³² -1)	D	R/W	N/A	Mémoire utilisée par l'appareil (en octets)
13	ClockMaster-Role	Booléen	0, 1	S	R/W	N/A	L'appareil est une source temporelle ou non (voir 8.3.3.1): 0 = Non 1 = Oui
14	ClockUpdate	Unsigned32	0 à (2 ³² -1)	D	R/W	0	Dernier réajustement d'horloge (en secondes)
15	PacketsMACTo-DLSL	Unsigned32	0 à (2 ³² -1)	D	R/W	0	Nombre de paquets issus de la sous-couche MAC vers la DLSL
16	PacketsFrom-DLSLRejected	Unsigned32	0 à (2 ³² -1)	D	R/W	0	Nombre de paquets provenant de la DLSL qui sont rejetés par la NL
17	PacketsFrom-DLSLAccepted	Unsigned32	0 à (2 ³² -1)	D	R/W	0	Nombre de paquets provenant de la DLSL qui sont acceptés par la NL
18	PacketsFrom-ASL	Unsigned32	0 à (2 ³² -1)	D	R/W	0	Nombre de paquets issus de la sous-couche application (ASL)
19	PacketsFrom-ASLRejected	Unsigned32	0 à (2 ³² -1)	D	R/W	0	Nombre de paquets provenant de la sous-couche application (ASL) qui sont abandonnés par la NL
20	PacketsOutTo-DLSL	Unsigned32	0 à (2 ³² -1)	D	R/W	0	Nombre de paquets provenant de la sous-couche application (ASL) qui sont transmis à la DLSL par la NL.
21	AGGSupport-Flag	Booléen	0, 1	S	R/W	N/A	Fanion de prise en charge d'agrégation et de désagrégation (indique si un appareil de routage prend en charge le mécanisme d'agrégation ou non): 0 = Non-prise en charge 1 = Prise en charge

Tableau 20 (3 de 3)

Identifica- teur d'élément d'attribut	Nom	Type de données	Plage valide	Type de stockage	Type d'accès	Valeur par défaut	Description
22	AGGEnable- Flag	Booléen	0, 1	S	R/W	0	Fanion d'activation d'agrégation et de désagrégation (indique si un appareil de routage active le mécanisme d'agrégation ou non): 0 = Désactivation 1 = Activation
23	IntraChannel- Num	Unsigned8	0 à 31	S	R/W	0	Nombre de canaux utilisables pour la communication intragroupe
24	IntraChanel	Unsigned8	0 à 31	S	R/W	0	Liste pour stocker tous les canaux de communication, pré-affectée par l'appareil de passerelle (GW) aux appareils de routage et aux appareils de terrain. La taille de la liste est IntraChannelNum. Voir 8.4.5 pour plus de détails
25	SuperframeID	Unsigned16	0 à 65 535	S	R/W	0	Identificateur unique de la supertrame, fourni par le NM
Dans ce tableau, les types de stockage sont C = constant, D = dynamique et S = statique.							

Le type de données des attributs de la VCR VCR_Struct est indiqué au Tableau 21.

Tableau 21 – Structure VCR_Struct

Identifica- teur d'élément d'attribut	Nom	Type de données	Plage valide	Description
0	VcrID	Unsigned16	0 à 65 535	Identificateur de VCR La relation VCR n'est pas valide si son identificateur est 0xFFFF.
1	VcrType	Unsigned8	0 à 16	Les bits 0-1 indiquent le type de VCR: 00 = VCR P/S 01 = VCR R/S 10 = VCR C/S Les bits 2 et 3 indiquent une VCR d'agrégation ou non: 00 = VCR de non-agrégation 01 = VCR d'agrégation de données 10 = VCR d'agrégation de paquets Les autres valeurs sont réservées.
2	SrcObjID	Unsigned8	0 à 255	ID de l'objet source
3	SrcObjInsID	Unsigned8	0 à 255	ID de l'instance d'objet source
4	DesObjID	Unsigned8	0 à 255	ID de l'objet de destination
5	DesObjInsID	Unsigned8	0 à 255	ID de l'instance d'objet de destination
6	DataUpdateRate	Unsigned32	0 à $(2^{32}-1)$	Vitesse de mise à jour des données (en millisecondes) Les données n'ont pas de cycle si cette valeur est 0xFFFFFFFF.
7	VcrStatus	Booléen	0, 1	Etat de la VCR: 0 = Inactive 1 = Active
8	VcrActivationTime	Unsigned32	0 à $(2^{32}-1)$	Temps d'activation de la VCR (en millisecondes)
9	ServiceTime	Unsigned32	0 à $(2^{32}-1)$	Durée de service valide de la VCR (en millisecondes)
10	SourceChAddress	Unsigned16	0 à 65 535	Adresse de la tête de groupe pour l'appareil source
11	SourceAddress	Unsigned16	0 à 65 535	Adresse réseau pour l'appareil source
12	DestinationAddresses	Unsigned16	0 à 65 535	Adresse réseau pour l'appareil de destination
13	SecurityPolicy	Unsigned8	0 à 255	Niveau de sécurité des paquets (voir Annexe A)
14	RouteID	Unsigned16	0 à 65 535	Identificateur d'itinéraire
L'unité de temps utilisée dans ce tableau est l'intervalle de temps utilisé par la supertrame.				

Le type de données des attributs de condition des appareils DevConRep est indiqué au Tableau 22.

Tableau 22 – Structure DevConRep_Struct

Identificateur d'élément d'attribut	Nom	Type de données	Plage valide	Description
0	DevShortAddr	Unsigned16	0 à 65 535	Adresse courte 16 bits de l'appareil
1	NumPktSent	Unsigned16	0 à 65 535	Nombre total de paquets envoyés après le dernier rapport
2	NumPktRcvd	Unsigned16	0 à 65 535	Nombre total de paquets terminés dans l'appareil après le dernier rapport
3	NumMacMicFailure	Unsigned16	0 à 65 535	Nombre total de défaillances de code d'intégrité de message (MIC) après le dernier rapport
4	BatLevel	Unsigned8	1 à 10	Niveau de puissance résiduel
5	RestartCount	Unsigned8	0 à 255	Nombre de démarrages de l'appareil
6	Uptime (durée de fonctionnement)	Unsigned32	0 à (2 ³² -1)	Temps depuis le dernier redémarrage (en secondes)

Le type de données des attributs clé KeyTable est indiqué au Tableau 23.

Tableau 23 – Structure Key_Struct

Identificateur d'élément d'attribut	Nom	Type de données	Plage valide	Description
0	KeyID	Unsigned16	0 à 65 535	Identificateur de clé
1	KeyType	Unsigned8	0 à 3	Type de clé: 0 = Clé de rattachement 1 = Clé de chiffrement de clé 2 = Clé de chiffrement de DLSSL 3 = Clé de chiffrement d'AL
2	KeyLength	Unsigned8	0 à 255	(KeyLength+1) est la longueur valide de la clé (en bits)
3	KeyActiveTime	Unsigned48	0 à (2 ⁴⁸ -1)	Nombre absolu d'intervalles de temps (ASN) lorsqu'une clé commence à être active
4	KeyData	Octetstring		Valeur de la clé
5	KeyAttackCnt	Unsigned8	0 à 255	Nombre total d'attaques contre la clé
6	KeyState	Unsigned8	0 à 7	Etat d'utilisation d'une clé: 0 = Sauvegarde 1 = En cours d'utilisation 2 = Invalide Les autres valeurs sont réservées.

Le type de données des attributs de liste d'objets ObjList est indiqué au Tableau 24.

Tableau 24 – Structure ObjList_Struct

Identificateur d'élément d'attribut	Nom	Type de données	Plage valide	Description
0	ObjectID	Unsigned8	0 à 255	Identificateur unique de l'objet UAO
1	InstanceID	Unsigned8	0 à 255	Identificateur unique d'une instance d'objet
2	ProfileID	Unsigned16	0 à 65 535	ID de profil de l'objet UAO
3	ParameterNumber	Unsigned8	0 à 255	Nombre de paramètres de l'UAO
NOTE ObjectID et InstanceID dans ObjList_Struct sont identiques à l'identificateur d'objet et l'ID d'instance (voir Annexe C). Les DAGO, PAGO et DGO sont trois types spéciaux d'objets UAO. Par conséquent, les attributs de DAGO, PAGO, ou DGO sont inclus dans ObjList_Struct si un tel objet est mis en œuvre dans l'appareil. En outre, DagolD et DagolnsID de DAGO, PagolD et PagolnsID de PAGO ainsi que DgolD et DgolnsID de DGO correspondent respectivement à ObjectID et InstanceID dans ObjList_Struct.				

6.9.2 Services MIB

6.9.2.1 Services MIB à distance

Les attributs dans la base d'informations de gestion (MIB) peuvent être lus et écrits à distance par l'intermédiaire des services d'obtention d'attribut et d'établissement d'attribut fournis par la couche réseau (NL).

6.9.2.2 Services de MIB locaux

6.9.2.2.1 Généralités

Les attributs dans la MIB peuvent être lus et écrits localement par l'intermédiaire des services d'obtention d'attribut et d'établissement d'attribut fournis par le processus DMAP local.

6.9.2.2.2 Services DMAP d'obtention d'attribut

DMAP-MIB-GET.request est utilisée par les couches de protocoles pour demander des attributs dans la base MIB.

La sémantique de DMAP-MIB-GET.request est décrite comme suit:

```
DMAP-MIB-GET.request (
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```

Le Tableau 25 spécifie les paramètres pour DMAP-MIB-GET.request.

Tableau 25 – Paramètres de DMAP-MIB-GET.request

Nom	Type de données	Plage valide	Description
AttributeID	Unsigned8	0 à 255	ID d'attribut dans la MIB
AttributeMemID	Unsigned8	0 à 255	Identificateur d'élément d'attribut, qui est utilisé pour obtenir les attributs MIB structurés La valeur 255 signifie qu'il convient de lire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour obtenir les attributs MIB structurés
Count	Unsigned8	0 à 255	Nombre de valeurs d'attribut ou de valeurs d'élément d'attribut, qui est utilisé pour obtenir les attributs MIB structurés; obtention de toutes les valeurs d'attributs à partir de FirstValueStorIndex si Count= 0.

DMAP-MIB-GET.confirm est utilisé pour retourner le résultat de DMAP-MIB-GET.request.

La sémantique de DMAP-MIB-GET.confirm est décrite comme suit:

DMAP-MIB-GET.confirm (

Status,
AttributeID,
AttributeMemID,
FirstValueStorIndex,
Count,
AttributeValue

)

Le Tableau 26 spécifie les paramètres pour DMAP-MIB-GET.confirm.

Tableau 26 – Paramètres de DMAP-MIB-GET.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultats de l'obtention d'attribut 0 = SUCCESS (succès) 1 = UNSUPPORTED_ATTRIBUTE (attribut non pris en charge) Les autres valeurs sont réservées.
AttributeID	Unsigned8	0 à 255	ID d'attribut demandé
AttributeMemID	Unsigned8	0 à 255	Identificateur de l'élément d'attribut La valeur 255 signifie qu'il convient de lire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut lues
Count	Unsigned8	0 à 255	Nombre de valeurs d'attribut ou de valeurs d'élément d'attribut
AttributeValue	Octetstring		Valeur de l'attribut

Si l'opération d'obtention d'attribut a réussi, il convient que le paramètre Status soit SUCCESS et, dans ce cas, AttributeValue est valide; sinon, si la base MIB n'a pas les attributs demandés, il convient que Status renvoie UNSUPPORTED_ATTRIBUTE et, dans ce cas, le paramètre AttributeValue n'est pas valide.

6.9.2.2.3 Services DMAP d'établissement d'attribut

Il convient que DMAP-MIB-SET.request soit utilisée par les couches de protocoles pour écrire des attributs dans la base MIB.

La sémantique de DMAP-MIB-SET.request est décrite comme suit:

```
DMAP-MIB-SET.request (
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count,
    AttributeValue
)
```

Le Tableau 27 spécifie les paramètres pour DMAP-MIB-SET.request.

Tableau 27 – Paramètres de DMAP-MIB-SET.request

Nom	Type de données	Plage valide	Description
AttributeID	Unsigned8	0 à 255	ID d'attribut dans la MIB
AttributeMemID	Unsigned8	0 à 255	Identificateur de l'élément d'attribut La valeur 255 signifie qu'il convient de lire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour obtenir les attributs MIB structurés
Count	Unsigned8	0 à 255	Number of attributes (nombre d'attributs)
AttributeValue	Octetstring		Valeur de l'attribut

DMAP-MIB-SET.confirm est utilisée pour retourner le résultat de DMAP-MIB-SET.request.

La sémantique de DMAP-MIB-SET.confirm est décrite comme suit:

```
DMAP-MIB-SET.confirm (
    Status,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex
)
```

Le Tableau 28 spécifie les paramètres pour DMAP-MIB-SET.confirm.

Tableau 28 – Paramètres de DMAP-MIB-SET.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultat de l'établissement d'attribut: 0 = SUCCESS (succès) 1 = UNSUPPORTED_ATTRIBUTE (attribut non pris en charge) 2 = INVALID_PARAMETER Les autres valeurs sont réservées.
AttributeID	Unsigned8	0 à 255	ID d'attribut dans la MIB
AttributeMemID	Unsigned8	0 à 255	Identificateur de l'élément d'attribut La valeur 255 signifie qu'il convient de lire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut écrites

Si l'opération d'établissement d'attribut a réussi, il convient que le paramètre Status soit SUCCESS; si la base MIB n'a pas les attributs demandés, il convient que Status soit UNSUPPORTED_ATTRIBUTE; sinon, si les attributs définis ne sont pas conformes aux attributs spécifiés, il convient que Status soit INVALID_PARAMETER.

7 Couche physique

7.1 Généralités

Le réseau WIA-PA utilise les radiofréquences (RF) comme moyen de communication entre ses appareils. La distance de communication entre deux appareils dépend de la puissance d'émetteur, du type d'antenne et de l'obstruction entre deux appareils. Les appareils WIA-PA peuvent être alimentés soit principalement par un réseau d'alimentation, batterie, appareils de récupération d'énergie (par exemple appareils solaires, à vibrations, etc.) ou par une combinaison de ces méthodes d'alimentation.

La spécification relative à la couche physique (PHY) du réseau WIA-PA s'appuie sur les ondes radio de 2,4 GHz conformes à l'IEEE 802.15.4-2011.

La PHY du réseau WIA-PA définit la méthode de signalisation, la puissance du signal, la sensibilité du récepteur et l'environnement d'envoi des bits sur le support réseau. La couche PHY est chargée de l'activation et de la désactivation de l'émetteur-récepteur radio, de la détection d'énergie, de l'indicateur de qualité de liaison, de la sélection de canaux, de l'évaluation de canal libre, des paquets d'émission et de réception à travers le support physique.

La spécification relative à la PHY du réseau WIA-PA inclut les éléments suivants:

- exigences relatives à la PHY, dont la plupart sont adoptées directement à partir de l'IEEE 802.15.4-2011, notamment les exigences spécifiques sur les canaux, la puissance d'émission et la sensibilité du récepteur;
- exigences relatives à la PHY garantissant l'interconnexion entre les appareils WIA-PA.

7.2 Exigences générales basées sur l'IEEE 802.15.4-2011

La couche physique WIA-PA doit être basée sur DSSS dans la bande de 2,4 GHz conformément à l'IEEE 802.15.4-2011 avec des exigences et des exceptions supplémentaires telles que spécifiées dans le présent document.

L'un des paramètres de mise en service de l'appareil, CountryCode (voir 8.4.11), fournit les lignes directrices relatives au lieu et aux contraintes de réglementation nécessaires pour obtenir la conformité aux réglementations applicables. Voir Annexe D.

Les fournisseurs d'appareils sont responsables de la conformité de ces appareils à la présente norme et à toutes les éventuelles réglementations spécifiques à un pays ou à une région.

Le Tableau 29 spécifie la sélection de la couche PHY pour un appareil WIA-PA conformément à l'IEEE 802.15.4-2011.

Tableau 29 – Sélection de protocoles PHY (1 de 2)

Article de l'IEEE 802.15.4-2011	Header	Présence	Contraintes
6	Exigences générales relatives à la PHY		
6.1	Exigences générales et définitions	Partielle	Seulement PHY de DSSS de 2 450 MHz utilisant la modulation O-QPSK
6.1.1	Plage de fréquence d'exploitation	Partielle	Seule la bande de DSSS de 2 450 MHz est incluse (voir Tableau 30)
6.1.2	Affectations de canaux	Partielle	Seuls les canaux 11-25 de la page de canaux 0 sont inclus (voir Tableau 32)
6.1.3	Périodes LIFS et SIFS minimales	Partielle	Uniquement les LIFS et SIFS minimales pour la bande de 2 450 MHz sont incluses
6.1.4	Mesure de puissance RF	OUI	
6.1.5	Puissance d'émission	OUI	
6.1.6	Emission parasite hors bande	OUI	
6.1.7	Définitions de la sensibilité du récepteur	OUI	
6.2	Spécifications relatives au service PHY	OUI	
6.3	Format PPDU	OUI	
6.4	Constantes PHY et attributs PIB		
6.4.1	Constantes PHY	OUI	
6.4.2	Attributs PIB de la PHY	Partielle	Voir 7.3.9
6.5	Spécifications relatives à la PHY de 2 450 MHz	OUI	Voir 7.3.8 pour des explications supplémentaires
6.6	Spécifications relatives à la PHY de modulation par déphasage binaire (BPSK, Binary phase-shift keying) sur la bande 868/915 MHz	NON	Seule la bande de 2 450 MHz est incluse
6.7	Spécifications relatives à la PHY de modulation par déplacement d'amplitude (ASK, Amplitude shift keying) (facultatives) sur la bande 868/915 MHz	NON	Seule la bande de 2 450 MHz est incluse

Tableau 29 (2 de 2)

Article de l'IEEE 802.15.4-2011	Header	Présence	Contraintes
6.8	Spécifications relatives à la PHY d'O-QPSK (facultatives) sur la bande 868/915 MHz	NON	Seule la bande de 2 450 MHz est incluse
6.9	Spécifications générales relatives aux ondes radio		
6.9.1	Temps de retournement TX-à-RX	OUI	
6.9.2	Temps de retournement RX-à-TX	OUI	
6.9.3	Définition de la magnitude de vecteur d'erreur (EVM, Error-vector magnitude)	OUI	
6.9.4	Tolérance de fréquence du centre d'émission	OUI	
6.9.5	Puissance d'émission	NON	Voir 7.3.6 pour le remplacement de ce paragraphe
6.9.6	Niveau d'entrée maximal du signal souhaité au niveau du récepteur	OUI	
6.9.7	Détection d'énergie (ED, Energy Detection) du récepteur	OUI	
6.9.8	Indicateur de qualité de liaison (LQI, Link Quality Indicator)	OUI	
6.9.9	Evaluation de canal libre (CLA, Clear Channel Assessment)	OUI	

7.3 Exigences supplémentaires

7.3.1 Généralités

Bien que la couche physique de l'IEEE 802.15.4-2011 prenne en charge plusieurs bandes de fréquence et classes de modulation, un appareil conforme à la présente norme doit fonctionner dans la bande de 2 400 MHz à 2 483,5 MHz sans licence utilisant la modulation DSSS et le codage à 250 kbit/s, qui est spécifiée dans l'IEEE 802.15.4-2011, Tableau 51, comme étant la PHY de DSSS de 2 450. La présente norme ne prend en charge aucune des autres bandes de fréquences, aucun des autres débits de données et aucune des autres techniques de modulation et de codage spécifiés dans l'IEEE 802.15.4-2011.

7.3.2 Affectations de fréquence

L'émetteur-récepteur doit utiliser le DSSS et fonctionner dans la bande ISM sans licence, tel que représenté au Tableau 30.

Tableau 30 – Bande de fréquence et débit de données

Fréquence MHz	Débit de communication kchip/s	Modulation	Débit binaire kbit/s	Débit de symboles ksymbol/s	Symboles
2 400 à 2 483,5	2 000	O-QPSK	250	62,5	16-aire orthogonal

7.3.3 Numéros de canal et affectations de fréquence

La bande de 2 450 MHz prend en charge les affectations de canal de 11-26, tel que spécifié dans l'IEEE 802.15.4-2011. Le canal 26 n'étant pas conforme à la réglementation de certaines régions du monde, il n'est pas inclus dans le présent document.

L'affectation de fréquence pour les canaux 11-25 est indiquée au Tableau 31.

Tableau 31 – Affectations de fréquence

Numéro de canal	Fréquence MHz		Numéro canal	Fréquence MHz		Numéro de canal	Fréquence MHz
11	2 405		16	2 430		21	2 455
12	2 410		17	2 435		22	2 460
13	2 415		18	2 440		23	2 465
14	2 420		19	2 445		24	2 470
15	2 425		20	2 450		25	2 475

7.3.4 Émetteurs-récepteurs radio

Les émetteurs-récepteurs radio des appareils WIA-PA sont conformes à l'IEEE 802.15.4-2011 ainsi qu'aux réglementations d'Europe, du Canada, du Japon, de Chine et des États-Unis, entre autres. Voir Annexe D.

7.3.5 Performance radio exigée améliorée ou non spécifiée

Le présent document inclut les éléments suivants, qui ne sont pas spécifiés dans l'IEEE 802.15.4-2011.

- a) Il convient que le temps recommandé pour commuter entre les canaux corresponde à 12 périodes symboles.
- b) Le temps maximal recommandé d'allumage de la radio pour un démarrage à froid est de 4 ms. Il comprend le verrouillage de fréquence et le temps d'établissement.

7.3.6 Puissance d'émission

La puissance d'émission doit être la puissance isotrope rayonnée équivalente, à savoir la PIRE (EIRP, Equivalent Isotropic Radiated Power) de l'appareil. Les appareils WIA-PA doivent fournir une p.i.r.e. nominale de +10 dBm (10 mW) ± 3 dB. Le niveau de puissance rayonnée maximal ne doit pas dépasser les exigences réglementaires applicables dans le lieu de déploiement de l'appareil, tel que contraint par CountryCode (voir 8.4.11).

Dans les deux cas, la puissance d'émission assignée doit être représentative de l'appareil de production du fabricant avec une source d'alimentation (batteries, solaire, ou autre) comprise entre 95 % et 100 % de sa capacité assignée. Il convient de fournir tous les appareils avec une antenne omnidirectionnelle. Les données relatives à la puissance d'émission assignée comprenant la puissance de sortie maximale et les diagrammes de rayonnement pour toutes les antennes prises en charge par le produit doivent être disponibles dans le manuel d'instructions du produit ou sur demande.

7.3.7 Contrôle de la puissance de sortie

Le niveau de puissance de l'appareil doit être programmable à des niveaux discrets et monotones de PIRE allant de -10 dBm à $+10$ dBm (avec ± 4 dBm d'erreur par rapport au niveau de puissance réel). La puissance de sortie peut être contrôlée en configurant l'attribut PIB phyTransmitPower de la couche physique PHY.

7.3.8 Sensibilité du récepteur

La sensibilité du récepteur du réseau WIA-PA est conforme à l'IEEE 802.15.4-2011 et doit pouvoir atteindre une sensibilité minimale de -85 dBm.

7.3.9 Attributs PIB de la PHY

La présente norme inclut les attributs spécifiés en 6.4.2 de l'IEEE 802.15.4-2011 et des attributs supplémentaires qui s'appliquent uniquement au présent document. Une valeur constante est affectée à certains de ces attributs, tel que représenté au Tableau 32.

Tableau 32 – Attributs de PHY PIB

Attribut	Commentaire
phyCurrentChannel	Configuré sur demande Ph-Enable
phyChannelsSupported	Seuls les canaux 11 – 25 sont pris en charge
phyTXPowerTolerance	1 dB, 3 dB, 6 dB
phyTXPower	Les valeurs comprises entre –10 dBm et +10 dBm sont prises en charge
phyCCAMode	Seule la valeur 2 (détection de porteuse) est incluse
phyCurrentPage	Seule la valeur "0" est incluse
phyMaxFrameDuration	Seule la valeur 266 est incluse
phySHRDuration	Seule la valeur 10 est incluse
phySymbolsPerOctet	Seule la valeur 2 est incluse
phyPreambleSymbolLength	Seule la valeur 0 est incluse
phyUWBDataRatesSupported	Cet attribut n'est pas valide dans le réseau WIA-PA
phyCSSLowDataRateSupported	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWBCoUSupported	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB CSSSupported	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWBCurrentPulseShape	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB CoUpulse	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB CSpulse	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB LCPWeight1	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB LCPWeight2	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB LCPWeight3	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB LCPWeight4	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB LCPDelay2	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB LCPDelay3	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWB LCPDelay4	Cet attribut n'est pas valide dans le réseau WIA-PA
phyRanging	Cet attribut n'est pas valide dans le réseau WIA-PA
phyRangingCrystalOffset	Cet attribut n'est pas valide dans le réseau WIA-PA
phyRangingDPS	Cet attribut n'est pas valide dans le réseau WIA-PA
phyCurrentCode	Seule la valeur 0 est incluse
phyNativePRF	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWBScanBinsPerChannel	Cet attribut n'est pas valide dans le réseau WIA-PA
phyUWBInsertedPreambleInterval	Cet attribut n'est pas valide dans le réseau WIA-PA
phyTXRMARKER Offset	Cet attribut n'est pas valide dans le réseau WIA-PA
phyRXRMARKER Offset	Cet attribut n'est pas valide dans le réseau WIA-PA
phyRFRAMEProcessingTime	Cet attribut n'est pas valide dans le réseau WIA-PA
phyCCADuration	Cet attribut n'est pas valide dans le réseau WIA-PA

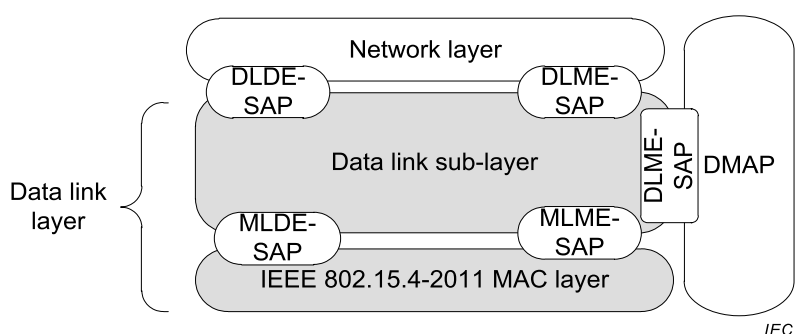
8 Couche liaison de données

8.1 Généralités

La couche liaison de données (DLL) du réseau WIA-PA est conçue pour garantir la communication en temps réel parmi des appareils WIA-PA en toute fiabilité et sécurité. La couche DLL du réseau WIA-PA étend la structure de supertrame de l'IEEE 802.15.4-2011. La couche WIA-PA DLL prend en charge certaines fonctions clés, y compris le saut de fréquence, la retransmission, et les mécanismes d'accès hybride aux canaux d'Accès multiple par répartition dans le temps (AMRT) et d'Accès multiple à détection de porteuse (CSMA). Ces mécanismes sont utilisés pour garantir la fiabilité et la transmission en temps réel pendant la communication. La couche DLL du réseau WIA-PA est conçue pour utiliser le mécanisme MIC et la technologie de chiffrement afin de garantir l'intégrité et la confidentialité du processus de communication.

8.2 Pile de protocole

La couche DLL du réseau WIA-PA est conçue pour optimiser l'IEEE 802.15.4-2011 afin de satisfaire aux exigences relatives à l'automation dans les processus. La pile de protocole de la couche DLL est indiquée à la Figure 28.



Anglais	Français
Network layer	Couche réseau (NL)
Data link layer	Couche liaison de données (DLL)
Data link sub-layer	Sous-couche liaison de données

Figure 28 – Pile de protocole de la couche DLL du réseau WIA-PA

La couche DLL du réseau WIA-PA comprend les parties suivantes:

- la couche MAC de l'IEEE 802.15.4-2011, qui gère les mécanismes d'envoi et de réception de trames de données individuelles;
- la sous-couche liaison de données (DLSL), qui gère les aspects de ressource de communication.

8.3 Vue d'ensemble de la couche MAC et extension de fonction

8.3.1 Vue d'ensemble de la couche MAC

La section suivante spécifie la couche MAC selon la norme WIA-PA et le contenu de la couche MAC selon l'IEEE 802.15.4-2011 n'est pas énoncé dans le présent document. Le présent document est basé sur la couche de contrôle d'accès au support (MAC) à balise de l'IEEE 802.15.4-2011. Cette couche MAC gère tous les accès au canal radio physique et elle est chargée des tâches suivantes:

- générer des balises réseau si l'appareil est un appareil de passerelle ou un appareil de routage;

- b) se synchroniser à des balises réseau;
- c) prendre en charge l'association et la dissociation point par point du réseau;
- d) prendre en charge la sécurité point par point;
- e) utiliser le mécanisme d'accès multiple par détection de porteuse et évitement de collision (CSMA-CA) en intervalles de temps pour le rattachement d'appareil;
- f) gérer et maintenir le mécanisme d'intervalle de temps garanti (GTS);
- g) fournir une liaison fiable entre deux entités MAC homologues.

Les appareils de terrain et les appareils tenus à la main correspondent à des appareils à fonctions limitées (RFD) tandis que les appareils de routage et les appareils de passerelle correspondent à des appareils pleinement fonctionnels (FFD). Aucune fonction facultative des appareils RFD et FFD dans l'IEEE 802.15.4-2011 n'est exigée dans la présente norme.

8.3.2 Exigences générales basées sur l'IEEE 802.15.4-2011

La couche MAC du réseau WIA-PA doit être basée sur la couche MAC de l'IEEE 802.15.4-2011 avec des exigences et des exceptions supplémentaires telles que spécifiées dans le présent document.

L'appareil de passerelle joue le rôle de coordinateur PAN dans l'IEEE 802.15.4-2011 et les appareils de routage agissent en tant que coordinateurs dans l'IEEE 802.15.4-2011.

Le Tableau 33 spécifie la sélection de la couche MAC pour un appareil WIA-PA conformément à l'IEEE 802.15.4-2011.

Tableau 33 – Sélection de protocoles MAC (1 of 3)

Article de l'IEEE 802.15.4-2011	Header	Présence	Contraintes
5	Protocole MAC		
5.1	Description fonctionnelle de la couche MAC		
5.1.1	Accès au canal	OUI	
5.1.2	Démarrage et maintien des PAN	Partielle	Seul le balayage actif est utilisé dans le réseau WIA-PA.
5.1.3	Association et dissociation	OUI	
5.1.4	Synchronisation	OUI	
5.1.5	Gestion des transactions	NON	Les transactions peuvent être réalisées à partir des appareils eux-mêmes.
5.1.6	Transmission, réception et acquittement	OUI	
5.1.7	Affectation et gestion du mécanisme GTS	NON	Cette fonction n'est pas utilisée dans le réseau WIA-PA.
5.1.8	Plage de valeurs	NON	Cette fonction n'est pas utilisée dans le réseau WIA-PA.
5.2	Formats de trame MAC		
5.2.1	Format général d'une trame MAC	OUI	Pour le format de trame MAC du réseau WIA-PA, la valeur du sous-champ Security enabled (sécurité activée) de l'en-tête de contrôle d'accès au support (MHR) doit être configurée à 0 et la longueur du sous-champ Auxiliary Security Header (en-tête auxiliaire de sécurité) est de 0 octet. La compression de l'ID PAN est configurée à 1. La longueur du champ Source PAN identifier (identificateur PAN source) est de 0 et le champ Destination PAN Identifier (identificateur PAN de destination) est configuré sur NetworkID (voir 6.9.1.2.1) du réseau WIA-PA.
5.2.2	Format de types de trame individuelle	OUI	
5.2.3	Compatibilité de trames	OUI	
5.3	Trames de commande MAC	Partielle	Voir les points 5.3.1 à 5.3.9. suivants
5.3.1	Commande de demande d'association	OUI	
5.3.2	Commande de réponse d'association	OUI	
5.3.3	Commande de notification de dissociation	OUI	
5.3.4	Commande de demande de données	OUI	
5.3.5	Commande de notification de conflit d'ID PAN	NON	La commande de notification de conflit d'ID PAN n'est pas utilisée dans le réseau WIA-PA.
5.3.6	Commande de notification orpheline	NON	La commande de notification orpheline n'est pas utilisée dans le réseau WIA-PA.
5.3.7	Commande de demande de balise	NON	La commande de demande de balise n'est pas utilisée dans le réseau WIA-PA.

Tableau 33 (2 de 3)

Article de l'IEEE 802.15.4-2011	Header	Présence	Contraintes
5.3.8	Commande de réalignement du coordinateur	NON	La commande de réalignement du coordinateur n'est pas utilisée dans le réseau WIA-PA.
5.3.9	Commande de demande de GTS	NON	La commande de demande de GTS n'est pas utilisée dans le réseau WIA-PA.
6	Service MAC		
6.1	Vue d'ensemble		
6.2	Service de gestion de la couche MAC	Partielle	Voir les points 6.2.1 à 6.2.17 suivants
6.2.1	Exigences communes pour les primitives MLME	OUI	
6.2.2	Primitives d'association	OUI	
6.2.3	Primitives de dissociation	OUI	
6.2.4	Primitives de notification de communications	OUI	
6.2.5	Primitives de lecture des attributs PIB	OUI	
6.2.6	Primitives de gestion du GTS	NON	Les primitives de gestion du GTS ne sont pas utilisées dans le réseau WIA-PA.
6.2.7	Primitives de notification orpheline	NON	Les primitives de notification orpheline ne sont pas utilisées dans le réseau WIA-PA.
6.2.8	Primitives de reconfiguration de la sous-couche MAC	NON	Après le départ d'un nœud du réseau WIA-PA, sa sous-couche MAC est reconfigurée à la valeur par défaut.
6.2.9	Primitives de spécification du temps d'activation du récepteur	OUI	
6.2.10	Primitives de balayage des canaux	OUI	
6.2.11	Primitives d'écriture des attributs PIB	OUI	
6.2.12	Primitives de mise à jour de la configuration de la supertrame	NON	Les primitives de mise à jour de la configuration de la supertrame ne sont pas utilisées dans le réseau WIA-PA.
6.2.13	Primitives de synchronisation avec un coordinateur	NON	Les primitives de synchronisation avec un coordinateur ne sont pas utilisées dans le réseau WIA-PA.
6.2.14	Primitives de demande de données d'un coordinateur	NON	Les primitives de demande de données d'un coordinateur ne sont pas utilisées dans le réseau WIA-PA.
6.2.15	Primitives de spécification de préambule dynamique	NON	Les primitives de spécification de préambule dynamique ne sont pas utilisées dans le réseau WIA-PA.
6.2.16	Primitives de sondage des canaux	NON	Les primitives de sondage des canaux ne sont pas utilisées dans le réseau WIA-PA.
6.2.17	Primitives de classement de l'étalonnage (pour les couches PHY d'UWB)	NON	Les primitives de classement de l'étalonnage (pour les couches PHY d'UWB) ne sont pas utilisées dans le réseau WIA-PA.

Tableau 33 (3 de 3)

Article de l'IEEE 802.15.4-2011	Header	Présence	Contraintes
6.3	Service de données MAC	Partielle	Les points 6.3.1 à 6.3.3 suivants sont utilisés dans le réseau WIA-PA.
6.3.1	MCPS-DATA.request	OUI	
6.3.2	MCPS-DATA.confirm	OUI	
6.3.3	MCPS-DATA. Indication	OUI	
6.3.4	MCPS-PURGE.request	NON	La primitive MCPS-PURGE.request n'est pas utilisée dans le réseau WIA-PA.
6.3.5	MCPS-PURGE. confirm	NON	La primitive MCPS-PURGE.confirm n'est pas utilisée dans le réseau WIA-PA.
6.4	Constantes MAC et attributs PIB		
6.4.1	Constantes MAC	OUI	
6.4.2	Attributs PIB de la couche MAC	Partielle	Voir Tableau 34 pour plus de détails.
6.4.3	Calcul des valeurs PIB de la couche MAC dépendantes de la couche PHY	OUI	

Le présent document inclut les attributs spécifiés en 6.4.2 de l'IEEE 802.15.4-2011 et des attributs supplémentaires qui s'appliquent uniquement au présent document. Une valeur constante est affectée à certains de ces attributs, tel que représenté au Tableau 34.

Tableau 34 – Attributs PIB de la couche MAC

Attribut (Attribut)	Commentaire
macAckWaitDuration	Seule la valeur 54 symboles est incluse dans la PHY de 2,4 GHz
macAssociatedPANCoord	Seule la valeur FALSE (faux) est incluse
macAssociationPermit	Seule la valeur TRUE (vrai) est incluse
macAutoRequest	Seule la valeur FALSE (faux) est incluse
macBattLifeExt	Seule la valeur FALSE (faux) est incluse
macBattLifeExtPeriods	Cet attribut n'est pas valide dans le réseau WIA-PA
macBeaconPayload	Le contenu de la charge utile de balise est étendu dans le réseau WIA-PA
macBeaconPayloadLength	Seule la valeur 10 est incluse
macBeaconTxTime	Seule la valeur 0x000000 est incluse
macCoordExtendedAddress	Cet attribut n'est pas valide dans le réseau WIA-PA
macCoordShortAddress	Cet attribut n'est pas valide dans le réseau WIA-PA
macGTSPermit	Seule la valeur FALSE (faux) est incluse
macMaxFrameTotalWaitTime	Uniquement lorsque phyMaxFrameDuration est égale à 266
macMinLIFSPeriod	Seule la valeur 40 est incluse (PHY de 2,4 GHz)
macMinSIFSPeriod	Seule la valeur 12 est incluse (PHY de 2,4 GHz)
macPromiscuousMode	Seule la valeur TRUE (vrai) est incluse
macRangingSupported	Seule la valeur FALSE (faux) est incluse
macSecurityEnable	Seule la valeur FALSE (faux) est incluse
macSyncSymbolOffset	0x000-0x100 pour la PHY de 2,4 GHz
macTxControlActiveDuration	Cet attribut n'est pas valide dans le réseau WIA-PA
macTxControlPauseDuration	Cet attribut n'est pas valide dans le réseau WIA-PA

8.3.3 Extension de fonction MAC

8.3.3.1 Généralités

Le présent document étend un attribut PIB de la couche MAC. L'attribut PIB étendu est présenté au Tableau 35.

Tableau 35 – Attributs PIB étendus de la couche MAC

Attribut	Type	Plage	Description	Défaut
macBeaconNum	Integer	1-15	Nombre de transmissions de balise en un intervalle de temps	1

L'attribut macBeaconNum est utilisé pour indiquer le nombre de transmissions de balise en un intervalle de temps.

8.3.3.2 Charge utile de balise

Le réseau WIA-PA utilise la charge utile de balise MAC de l'IEEE 802.15.4-2011 pour distribuer les informations de superframes. L'Article 5.2.2.1 de l'IEEE 802.15.4-2011 traite du format de trame de la balise MAC.

La charge utile de balise est indiquée au Tableau 36.

Tableau 36 – Charge utile de balise

	Charge utile de balise			
Longueur en octet(s)	1	6	2	1
Nom de champ	ClusterID	ASN	TimeValue	NextBcnChannel

Les sous-champs du Tableau 36 sont définis comme suit:

- a) ClusterID indique l'identificateur du groupe;
- b) ASN indique le nombre absolu d'intervalles de temps. Sa valeur doit augmenter de la valeur 1 (elle ne diminue pas). Sa valeur courante est toujours le numéro séquentiel de l'intervalle de temps courant. La valeur maximale doit être de $(2^{48}-1)$. Après avoir atteint la valeur maximale, le compte doit repartir de zéro;
- c) voir Tableau 60 pour Timevalue;
- d) NextBcnChannel indique le canal utilisé pour émettre la prochaine balise.

8.3.3.3 Trame de commande de demande d'association

L'appareil de réseau WIA-PA utilise la trame de commande de demande d'association MAC de l'IEEE 802.15.4-2011 pour se rattacher au réseau WIA-PA. Voir 5.3.1 de l'IEEE 802.15.4-2011 pour le format de trame de la trame de commande de demande d'association MAC.

Les types d'appareils de réseau WIA-PA sont indiqués par le bit 1 dans le champ Capability Information (informations de capacité) de la trame de commande de demande d'association MAC (voir Figure 50 de l'IEEE 802.15.4-2011).

Le format du champ Capability Information (informations de capacité) de la trame de commande de demande d'association MAC est indiqué au Tableau 37.

Tableau 37 – Format du champ Capability Information (informations de capacité)

Format du champ Capability Information (informations de capacité)							
Longueur en bit(s)	1	1	1	1	2	1	1
Nom de sous-champ	Réservé	Device type (type d'appareil)	Power source (source d'alimentation)	Receiver on when idle (récepteur allumé lorsqu'il est à l'état repos)	Réservé	Security capability (capacité de sécurité)	Allocated address (adresse affectée)

Les sous-champs du Tableau 37 sont définis comme suit:

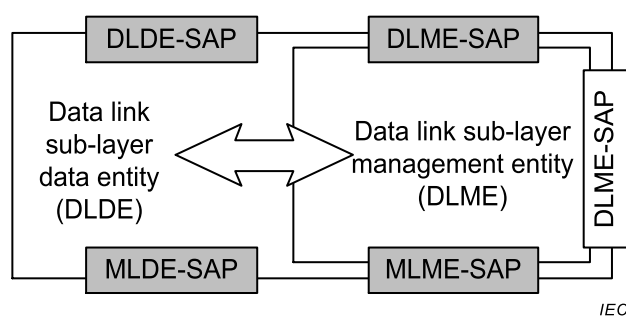
- le sous-champ Device type (type d'appareil) est étendu pour indiquer le type d'appareil du réseau WIA-PA; 0 indique l'appareil de routage et 1 correspond à l'appareil de terrain ou à l'appareil tenu à la main;
- voir 5.3.1.2 de l'IEEE 802.15.4-2011 pour les sous-champs Power source (source d'alimentation), Receiver on when idle (récepteur allumé lorsqu'il est à l'état repos), Security capability (capacité de sécurité) et Allocated address (adresse affectée).

8.4 Description de la fonction de la sous-couche liaison de données (DLSL)

8.4.1 Généralités

La DLSL fournit une interface de service entre la couche réseau (NL) et la couche MAC. La DLSL contient conceptuellement une entité de donnée de sous-couche liaison de données (DLDE) et une entité de gestion de sous-couche liaison de données (DLME). L'entité DLDE fournit les interfaces de services de données. L'entité DLME fournit les services de gestion de couche tels que la configuration des paramètres de la DLSL et la surveillance de l'état de fonctionnement de la DLSL.

La Figure 29 représente les composants et les interfaces de la sous-couche DLSL.



Anglais	Français
Data link sub-layer data entity (DLDE)	Entité de données de la couche réseau (DLDE)
Data link sub-layer management entity (DLME)	Entité de gestion de la couche réseau (DLME)

Figure 29 – Modèle de référence de la DLSL du réseau WIA-PA

La DLSL fournit deux services, auxquels on accède par l'intermédiaire des deux points d'accès au service (SAP) suivants:

- a) le service de données DLSL, auquel on accède par le point d'accès au service DLDE (DLDE-SAP);
- b) le service de gestion de DLSL, auquel on accède par le point d'accès au service DLME (DLME-SAP).

Dans le présent document, la fonction principale de la sous-couche DLSL est d'affecter des ressources de communication parmi des utilisateurs concurrents afin d'éviter les collisions, d'améliorer le rendement et d'accroître l'utilisation de la largeur de bande. Les principaux concepts de la DLSL comprennent l'intervalle de temps, la supertrame et la liaison, qui sont définis de la manière suivante.

- a) L'intervalle de temps est l'unité de temps de base dans l'échange de paquets. La durée de l'intervalle de temps WIA-PA est configurable.
- b) La supertrame est une collection d'intervalles de temps se répétant sur un programme cyclique. Le nombre d'intervalles de temps dans une supertrame donnée détermine le cycle de communication pour les appareils WIA-PA qui utilisent les intervalles de temps.
- c) La liaison comprend le temps et la fréquence. Une attribution de liaison spécifie comment l'appareil utilise un jeu d'intervalles de temps d'une supertrame. Les types de liaison comprennent l'émission, la réception et l'émission en partage. La liaison de partage permet à plus d'un seul appareil de rivaliser pour cette liaison en vue de l'échange de paquet au même moment. Il convient que la liaison d'émission et la liaison de réception ne permettent qu'aux appareils désignés d'échanger des paquets.

8.4.2 Coexistence

Il convient que le réseau WIA-PA considère les stratégies de coexistence suivantes:

- a) le réseau WIA-PA étend la structure de supertrame de l'IEEE 802.15.4-2011;
- b) la sous-couche DLSL du réseau WIA-PA associée avec le NM réalise la coexistence avec d'autres réseaux sans fil. La sous-couche WIA-PA DLSL incorpore plusieurs stratégies pour optimiser la coexistence:
 - communication en intervalles de temps;
 - faible facteur d'utilisation;
 - multicanal;
 - saut de fréquence (SF);
 - évitement de collision.

8.4.3 Communication en intervalles de temps

L'exigence clé de la communication en intervalles de temps est de garantir que toutes les transactions se produisent dans un intervalle de temps conformément aux exigences de synchronisation spécifiques. Cela veut dire qu'il convient d'échanger tous les paquets dans un intervalle de temps prescriptif et qu'ils ne soient pas différés. La longueur d'intervalle de temps de la sous-couche WIA-PA DLSL est totalement compatible avec la longueur d'intervalle de temps de la norme IEEE STD 802.15.4-2011.

La durée de l'intervalle de temps est configurée par le NM après que les appareils se sont rattachés au réseau.

8.4.4 Supertrame WIA-PA

Afin de garantir une communication fiable et en temps réel, le présent document prend uniquement en compte la structure de supertrame à balise de l'IEEE 802.15.4-2011.

La structure de supertrame WIA-PA est indiquée à la Figure 30.

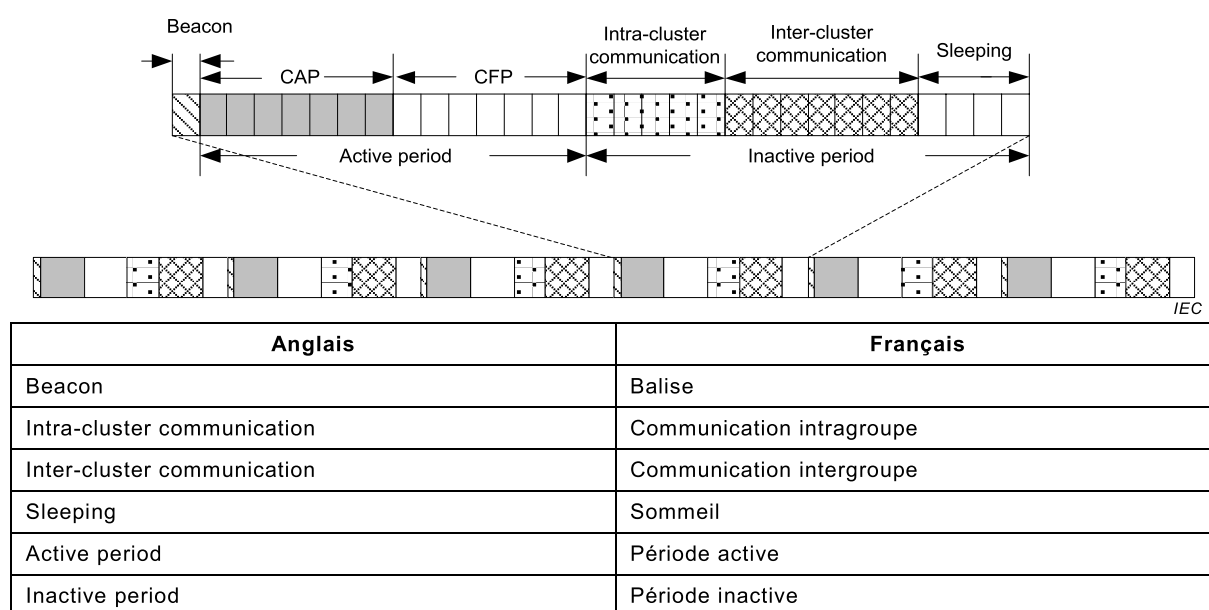


Figure 30 – Superframe WIA-PA

Les périodes de la superframe WIA-PA sont définies de la manière suivante:

- la période d'accès avec conflit (CAP) définie dans la superframe de l'IEEE 802.15.4-2011 est utilisée pour le rattachement d'appareil, la gestion intragroupe et les nouvelles tentatives dans la superframe WIA-PA;
- la période sans conflit (CFP) définie dans la superframe de l'IEEE 802.15.4-2011 est utilisée pour la communication entre des appareils tenus à la main et leur tête de groupe dans la superframe WIA-PA;
- la période inactive définie dans la superframe de l'IEEE 802.15.4-2011 est utilisée pour la communication intragroupe, la communication intergroupe et le sommeil dans la superframe WIA-PA.

Il convient que le NM génère les superframes WIA-PA. Les longueurs de superframe des appareils de routage sont différentes et sont fixées comme étant la vitesse minimale de mise à jour des données de tous les éléments dans un groupe. Les types d'intervalles de temps de superframe WIA-PA incluent les intervalles de temps partagés et les intervalles de temps dédiés. Les intervalles de temps partagés sont utilisés pour la transmission de données non périodiques et les intervalles de temps dédiés sont utilisés pour la transmission intragroupe et intergroupe de données périodiques.

La période inactive définie dans la superframe de l'IEEE 802.15.4-2011 étant utilisée pour la communication intragroupe, la communication intergroupe et le sommeil dans la superframe WIA-PA, la durée de superframe de base WIA-PA est définie à la valeur de trente-deux intervalles de temps. La durée de superframe WIA-PA est définie comme étant égale à 2^N (N est un nombre entier naturel) fois la durée de superframe de base WIA-PA.

Chaque appareil de routage dispose d'une seule superframe et la communication parmi les appareils de routage se produit au cours des intervalles de temps intergroupe qui se chevauchent. Chaque appareil de terrain dispose d'une seule superframe; la communication entre les appareils de terrain et les appareils de routage a lieu au cours des intervalles de temps intragroupe.

8.4.5 Saut de fréquence

Le réseau WIA-PA prend en charge le saut de fréquence, et la séquence de saut est désignée par le NM. Le saut de fréquence dans le réseau WIA-PA inclut trois mécanismes: AFS, AFH, et TH.

Commutation de fréquence adaptative (AFS): dans la supertrame WIA, la balise, la période CAP et la période CFP utilisent le même canal dans le même cycle de supertrame et changent de canal en fonction des conditions des canaux dans les cycles de supertrame différents. Autrement dit, un mauvais état de canaux, qui signifie que le taux d'abandons de paquets est supérieur à PLRThreshold, déclenche l'opération de changement de canaux. Voir 6.9.1.2.1 pour PLRThreshold.

Saut de fréquence adaptatif (AFH): changements irréguliers de canaux de communication par intervalle de temps de la supertrame WIA en fonction de la condition réelle des canaux. Les conditions de canaux sont mesurées avec le nombre de nouvelles tentatives. Si le canal est en mauvaise condition et le nombre de nouvelles tentatives de l'expéditeur atteint la valeur de ChannelThreshold, l'expéditeur choisit séquentiellement le canal suivant dans IntraChanel[] et notifie le destinataire au cours du prochain intervalle de nouvelle tentative en utilisant le canal principal (voir Tableau 17). Si le destinataire ne reçoit pas la notification, il compte en continu ses nombres de tentatives. Lorsque le nombre de nouvelles tentatives du destinataire atteint la valeur de ChannelThreshold, le destinataire choisit le prochain canal dans IntraChanel[] au cours du (ChannelThreshold+2)ème intervalle de temps. Si le destinataire reçoit la notification de commutation d'un canal, il change de canal de communication et renvoie un acquittement ACK; sinon, il ne change pas de canal de communication et effectue une nouvelle tentative avec les données en utilisant le canal principal. Si le nombre de nouvelles tentatives de l'expéditeur atteint macMaxFrameRetries, l'expéditeur rejette le paquet courant et émet le paquet suivant en utilisant le canal principal. Si la communication entre l'expéditeur et le destinataire a réussi avant que le nombre de nouvelles tentatives de l'expéditeur n'atteigne macMaxFrameRetries, l'expéditeur émet le paquet suivant en utilisant le canal de réserve. La période intragroupe adopte le mécanisme AFH. Voir 6.9.1.2.1 pour plus de détails sur ChannelThreshold et IntraChanel[]; voir Tableau 52 de l'IEEE 802.15.4-2011 pour plus d'informations sur macMaxFrameRetries.

Le canal en cours dans IntraChanel[] utilisé par l'expéditeur et le destinataire est marqué comme canal principal alors que les autres canaux dans IntraChanel[] sont marqués comme canaux de réserve.

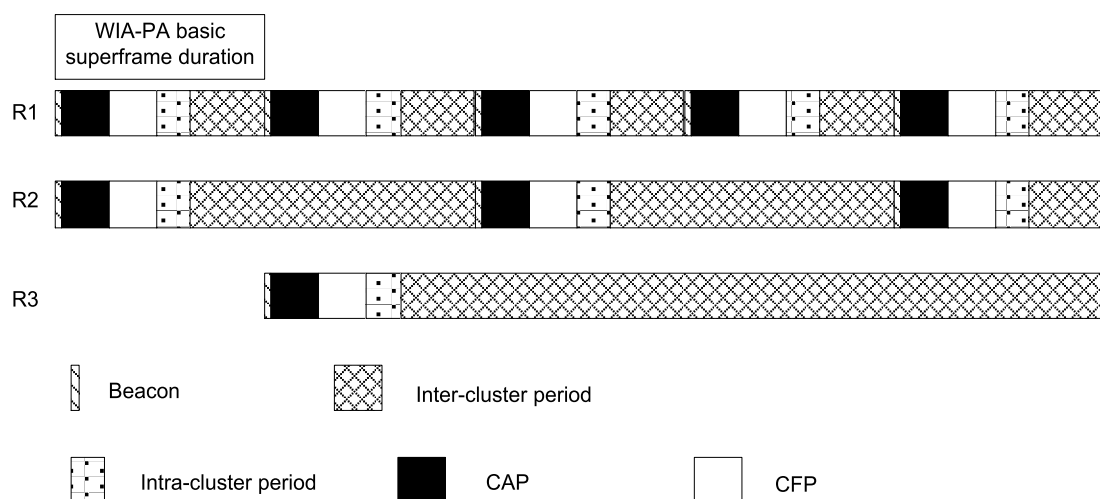
Saut d'intervalle de temps (TH): changement régulier de canaux de communication par intervalle de temps de la supertrame WIA pour combattre les interférences et l'évanouissement. La période intergroupe adopte le mécanisme TH. La structure de saut est: <intervalle de temps 1, canal 1><intervalle de temps 2, canal 2>... <intervalle de temps i, canal i>.

Les mécanismes spécifiques de saut de DLSL dans le réseau WIA-PA sont indiqués au Tableau 38.

Tableau 38 – Mécanismes de saut

IEEE 802.15.4-2011	WIA-PA	Mécanisme MAC de base		Mécanisme de saut DLSL
Balise	Balise	AMRT	Accès multiple par répartition en fréquence (AMRF) et AMRT	AFS
CAP	CAP	CSMA		
CFP	CFP	AMRT		
Inactive	Période intragroupe	AMRT		AFH
	Période intergroupe	AMRT		TH
	Sommeil			

Des appareils de routage différents utilisent des canaux différents dans la période active. Si le nombre de canaux n'est pas suffisant, le réseau WIA-PA utilise le mécanisme AMRT pour renforcer la capacité système. L'instant de début d'une supertrame est configuré par le NM. Par exemple, il y a trois appareils de routage R1, R2, et R3 dans le réseau WIA-PA. Les longueurs de supertrame de R1, R2 et R3 sont respectivement une, deux et quatre durée(s) de supertrame de base WIA-PA, telles qu'indiquées à la Figure 31. Conformément à la définition de la supertrame, la période active de R1 ne peut pas être multiplexée avec les périodes actives de R2 et R3. Toutefois, les périodes actives de R2 et R3 peuvent être multiplexées entre elles. Les périodes actives de R2 et R3 peuvent utiliser le même canal alors qu'il convient que la période active de R1 utilise un autre canal.



IEC

Anglais	Français
WIA-PA basic superframe duration	Durée de supertrame de base WIA-PA
Beacon	Balise
Intra-cluster period	Période intragroupe
Inter-cluster period	Période intergroupe
CAP	CAP
CFP	CFP

Figure 31 – Structures des supertrames R1, R2 et R3

8.4.6 Transmission des données de cycle long

Les données de cycle long sont caractérisées par leur vitesse de mise jour dans un appareil supérieure à la longueur maximale de supertrame de l'IEEE 802.15.4-2011 ou à la vitesse de mise à jour des données de l'appareil de routage dans un groupe.

Pour indiquer la transmission de données de cycle long, le présent document définit un paramètre appelé TransmitFlag. TransmitFlag est défini comme suit:

$$\text{TransmitFlag} = \lceil (\text{AbsoluteSlotNumber} - \text{ActiveSlot} + 1) / \text{NumberSlots} \rceil \% \text{SuperframeMultiple}$$

où

AbsoluteSlotNumber	voir 6.9.1.2;
ActiveSlot	voir 6.9.1.2;
NumberSlots	voir 6.9.1.2;

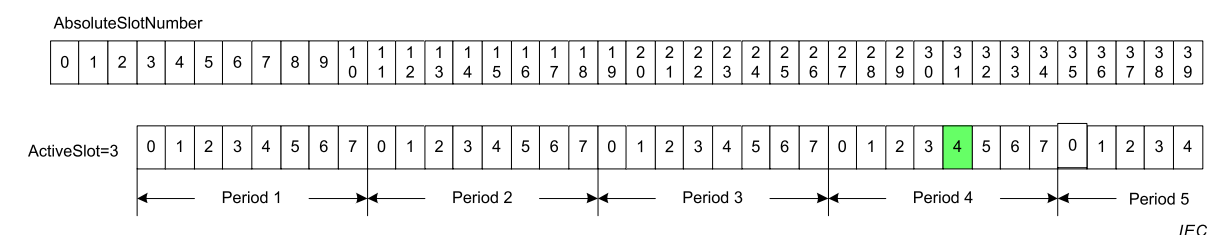
SuperframeMultiple voir 6.9.1.2.

Dans chaque cycle de supertrame, les appareils de terrain reçoivent les balises et décident d'envoyer ou non des données dans ce cycle de supertrame. Le processus de transmission de données de cycle long est décrit comme suit:

- si $0 < \text{TransmitFlag} < \text{SuperframeMultiple}$ et $\text{TransmitFlag} = \text{LinkSuperframeNum}$, alors l'appareil de terrain transmet les données dans ce cycle de supertrame;
- si $\text{TransmitFlag} = 0$ et $\text{LinkSuperframeNum} = \text{SuperframeMultiple}$, alors l'appareil de terrain transmet les données dans ce cycle de supertrame.

Voir Tableau 17 pour LinkSuperframeNum.

La Figure 32 est un exemple de transmission de données de cycle long.



Anglais	Français
AbsoluteSlotNumber	AbsoluteSlotNumber
ActiveSlot=3	ActiveSlot=3
Period 1	Période 1
Period 2	Période 2
Period 3	Période 3
Period 4	Période 4
Period 5	Période 5

Figure 32 – Exemple de transmission de données de cycle long

A la Figure 32, ActiveSlot = 3, NumberSlots = 8, SuperframeMultiple = 4 et LinkSuperframeNum = 4.

Si l'intervalle de temps absolu courant d'une balise est 27 (AbsoluteSlotNumber = 27), TransmitFlag se calcule par:

$$\text{TransmitFlag} = \lceil (27 - 3 + 1) / 8 \rceil \% 4 = 0$$

D'après les résultats du calcul, on peut conclure que TransmitFlag = 0 et que SuperframeMultiple = LinkSuperframeNum, ce qui indique qu'il convient d'envoyer le paquet pendant le cycle de supertrame en cours.

8.4.7 Stratégie de nouvelle tentative

Il convient que le NM dans le réseau maillé et les appareils de routage dans le réseau en étoile affectent un certain nombre d'intervalles de temps pour les nouvelles tentatives. La stratégie de nouvelle tentative prend en charge les mécanismes de saut de fréquence (voir 8.4.5).

Le nombre d'intervalles de temps de nouvelles tentatives dépend de la constante `macMaxFrameRetries` dans la base d'informations de réseau local personnel (PIB, PAN Information Base) de la couche MAC de l'IEEE 802.15.4-2011.

8.4.8 Service de gestion

La sous-couche DLSL du réseau WIA-PA fournit des services de gestion à la couche supérieure et au processus DMAP avec le DLME-SAP (point d'accès au service d'entité de gestion de sous-couche liaison de données). Les services comprennent la découverte de réseau, le rattachement et le départ d'appareils, l'allocation de ressources et les opérations de gestion des attributs de base de données (voir Article 6).

8.4.9 Mesure de la qualité de liaison radio et de la condition des canaux

La mesure de la qualité de liaison radio et de la condition des canaux comprend la mesure de la qualité de liaison par paire de voisins et la mesure de la condition par canal. Les informations recueillies peuvent être cumulées à la sous-couche DLSL et rapportées par le biais du processus DMAP. La qualité de liaison et la condition des canaux sont utilisées pour allouer dynamiquement des ressources de communication.

En général, la mesure de la qualité d'une liaison radio est accomplie en fonction des indices de performance suivants:

- a) niveau de signal moyen reçu en provenance d'appareils voisins dans la durée statistique;
- b) paquets de non-diffusion envoyés aux appareils voisins dans la durée statistique;
- c) nombre d'acquittements (ACK) qui n'ont pas été reçus dans la durée statistique;
- d) nombre de paquets de non-diffusion reçus en provenance des appareils voisins dans la durée statistique.

La mesure de la condition des canaux est accomplie en fonction des données de performance suivantes:

- a) LQI par liaison;
- b) taux de perte de paquets par liaison, déterminé par le nombre d'acquittements (ACK) reçus et de paquets envoyés;
- c) nombre moyen de nouvelles tentatives par liaison.

8.4.10 Sécurité

La sous-couche DLSL du réseau WIA-PA applique le mécanisme MIC et la technologie de chiffrement afin de garantir l'intégrité et la confidentialité de la communication. Voir l'Article 11 pour plus de détails.

8.4.11 Code de pays

Les considérations de réglementations de la DMLE sont configurées via son attribut `CountryCode` (voir 6.9.1.2.1), qui est une valeur à 16 bits pour laquelle:

- a) les bits 0-9 fournissent un code de pays de 10 bits utilisant les codes de pays numériques à trois chiffres conformes à l'ISO 3166-1;
- b) le bit 10 indique si la réglementation européenne s'applique ou non (0 = non, 1 = oui). Une DLME doit fonctionner conformément à la réglementation européenne lorsque `Bit10 = 1`;
- c) le bit 11 indique si, oui ou non, les règles de la FCC s'appliquent (0 = non, 1 = oui). Il convient qu'une DLME opère en conformité avec les règles FCC lorsque `Bit11 = 1`;
- d) le bit 12 indique si, oui ou non, une limite de PIRE de 10 dBm s'applique (0 = non, 1 = oui). Il convient qu'une DLME limite ses émissions à une valeur de PIRE ≤ 10 dBm lorsque `Bit12 = 1`;

- e) le bit 13 indique si la DLME est considérée comme fonctionnant selon des règles adaptatives ou non adaptatives (0 = non adaptatives, 1 = adaptatives);
- f) le bit 14 indique si la DLME est considérée comme fonctionnant ou non selon des règles d'étalement de spectre à saut de fréquence (FHSS, Frequency-hopping spread-spectrum) (0 = règles non FHSS, 1 = règles FHSS);
- g) le bit 15 indique si, oui ou non, la valeur de cet attribut est fixe (0 = non, 1 = oui) pendant que la DLME est opérationnelle. Une fois que ce bit est défini, toute tentative ultérieure de modifier cet attribut doit être rejetée, sauf lorsqu'elle se produit pendant que la DLME est en cours de mise en service.

NOTE 1 Cette caractéristique prend en charge le fonctionnement d'appareils dans des régimes de réglementation qui interdisent l'aptitude à reconfigurer un appareil de telle manière qu'il violerait les contraintes de réglementation, tout en permettant toujours la réparation ou la remise à neuf d'appareils avec une revente ultérieure sur des marchés où d'autres réglementations s'appliquent.

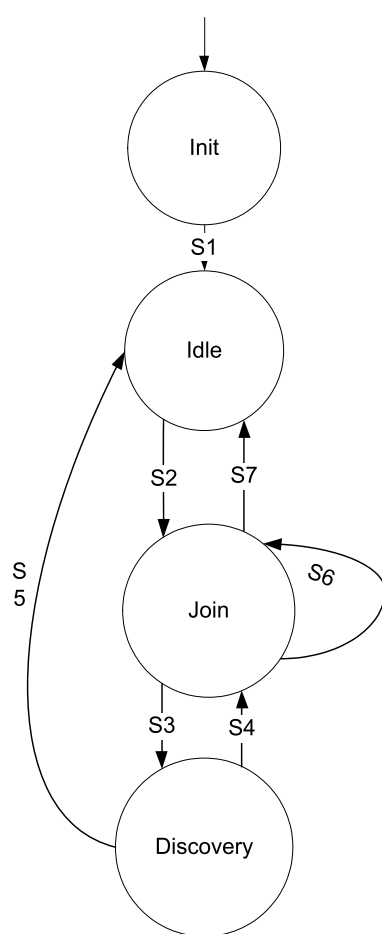
Lorsqu'aucun pays spécifique d'utilisation prévue n'a été identifié, la valeur par défaut de CountryCode doit être 0x3C00, indiquant qu'il convient qu'un appareil dans l'état par défaut se conforme aux règles de l'ETSI, aux règles FCC, à la limite de PIRE de 10 dBm et soit classé comme appareil adaptatif non FHSS. Voir Annexe D.

NOTE 2 Cette valeur par défaut de CountryCode garantit que l'équipement, avant sa mise en service, satisfait aux exigences de réglementation de la plupart des régions dans lesquelles il pourrait être déployé. La valeur de CountryCode pourrait être modifiée au cours de la mise en service câblée afin de refléter le régime de réglementation visé applicable au site de déploiement de l'appareil.

8.4.12 Diagramme d'états de DLSS

Le diagramme d'états de la sous-couche DLSS du réseau WIA-PA est divisé en deux diagrammes d'états: un premier pour le rattachement d'appareil et l'autre pour l'exécution dans le réseau.

Le diagramme d'états de la sous-couche DLSS du réseau WIA-PA pour le rattachement d'appareil est indiqué à la Figure 33.



IEC

Anglais	Français
Init	Initialisation
Idle	Repos
Join	Rattachement
Discovery	Découverte

Figure 33 – Diagramme d'états de la sous-couche DLSL pour le rattachement d'appareil

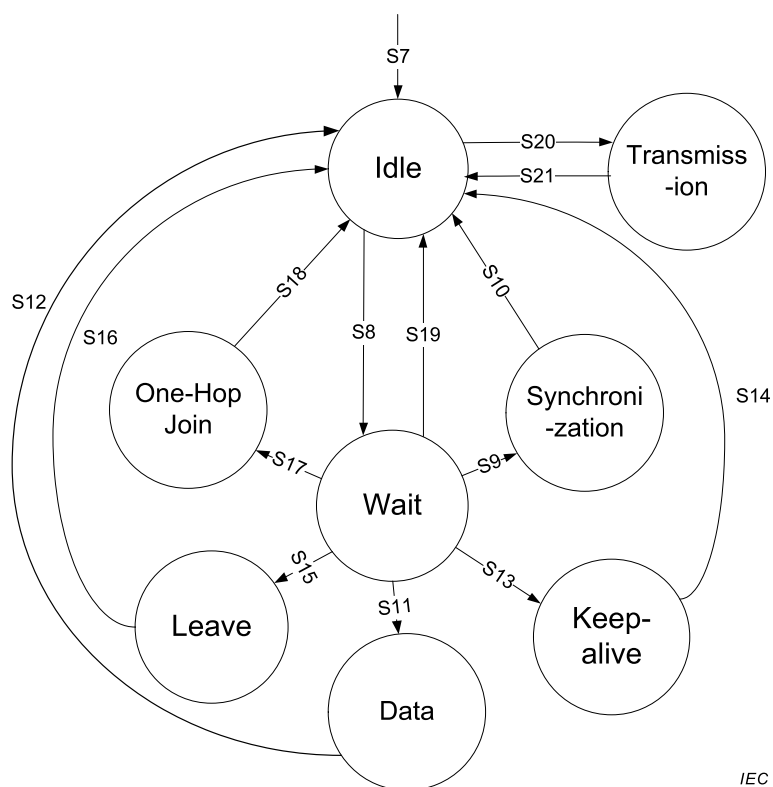
Les transitions d'états de la sous-couche DLSSL pour le rattachement d'appareil sont indiquées au Tableau 39.

Tableau 39 – Transitions d'états de la sous-couche DLSSL pour le rattachement d'appareil

Numéro séquentiel #	Etat courant	Événement ou condition	Actions	Prochain état
S1	Init		Début	Idle
S2	Idle	Devicestate = Pas rattaché		Join
S3	Join	DLME-DISCOVERY.request()	Analyse du message de demande de découverte et invocation de MLME-SCAN.request()	Discovery
S4	Discovery	MLME-SCAN.confirm (status = SUCCESS) et MLME-BEACON-NOTIFY.indication()	Analyse du message de confirmation de balayage et du message de notification de balise, invocation de DLME-DISCOVERY.confirm(SUCCESS)	Join
S5	Discovery	MLME-SCAN.confirm (status != SUCCESS) ou pas de confirmation reçue		Idle
S6	Join	DLME-JOIN.request()	Configuration de Devicestate = Rattachement; génération de message de demande d'association et invocation de MLME-ASSOCIATE.request()	Join
S7	Join	MLME-ASSOCIATE.confirm() ou pas de confirmation reçue	Si MLME-ASSOCIATE.confirm() reçue, analyse du message de confirmation d'association: si status = SUCCESS, invocation de DLME-JOIN.confirm(Status = SUCCESS) et configuration de Devicestate = Rattaché; si status != SUCCESS, invocation de DLME-JOIN.confirm(). Si aucune confirmation reçue, pas d'action entreprise.	Idle

Après le rattachement au réseau WIA-PA d'un appareil, qui correspond à Devicestate = Rattaché, le DLSSL exécute son diagramme d'états pour l'exécution dans le réseau.

Le diagramme d'états de la sous-couche DLSSL du réseau WIA-PA pour l'exécution dans le réseau est indiqué à la Figure 34.



IEC

Anglais	Français
Idle	Repos
Transmission	Emission
One-hop join	Rattachement en un saut
Synchronization	Synchronisation
Wait	Attente
Leave	Départ
Data	Données
Keep-alive	Entretien

Figure 34 – Diagramme d'états de la sous-couche DLSL pour l'exécution dans le réseau

Les transitions d'états de la sous-couche DLSL pour un appareil dans le réseau sont indiquées au Tableau 40.

Tableau 40 – Transitions d'états de la sous-couche DLSL pour l'exécution dans le réseau (1 de 3)

Numéro séquentiel #	Etat courant	Événement ou condition	Actions	Prochain état
S8	Idle	Temporisation d'intervalle de temps LinkType = Réception ou LinkType = Transmission partagée	Invocation de MLME-RX-ENABLE.request ()	Wait
S9	Wait	A partir de la couche MAC: MLME-COMM-STATUS.indication() ou MCPS-DATA.indication(); A partir du processus DMAP: DLME-TIME-SYN.request()		Synchronisation
S10	Synchronisation		A partir de la couche MAC: analyse du message d'indication d'état de communication de la MLME et invocation de DLME-TIME-SYN.confirm() ou analyse de la DLPDU à partir de la trame de données MAC. Si Frametype = 1 et l'identificateur de trame de commande = 11 dans la DLPDU, invocation de DLME-TIME-SYN.indication(); A partir du processus DMAP: génération de trame de commande de demande de temps de la DLSL et invocation de MCPS-DATA.request().	Idle
S11	Wait	A partir de la couche MAC: MCPS-DATA.confirm() ou MCPS-DATA.indication(); A partir de la NL: DLDE-DATA.request()		Data
S12	Data		A partir de la couche MAC: invocation de DLSL-DATA.confirm() ou analyse de la DLPDU. Si Frame type (type de trame) = 0 dans la DLPDU, évaluation de LinkQuality et PacketLossRate et invocation de DLDE-DATA.indication(); A partir de la NL: MCPS-DATA.request()	Idle
S13	Wait	A partir de la couche MAC: MLME-COMM-STATUS.indication() ou MCPS-DATA.indication(); A partir du processus DMAP: DLME-KEEP-LIVE.request()		Keep-alive

Tableau 40 (2 de 3)

Numéro séquentiel #	Etat courant	Evénement ou condition	Actions	Prochain état
S14	Keep-alive		A partir de la couche MAC: analyse du message d'indication d'état de communication de la MLME et invocation de DLME - KEEP-LIVE.confirm() ou analyse de la DLPDU à partir de la trame de données MAC. Si Frametype = 1 et l'identificateur de trame de commande = 10 dans la DLPDU, invocation de DLME-KEEP-ALIVE.indication(); A partir du processus DMAP: invocation de MLME-KEEP-LIVE.request()	Idle
S15	Wait	A partir de la couche MAC: MLME-DISASSOCIATE.indication() ou MLME-DISASSOCIATE.confirm(); A partir du processus DMAP: DLME-LEAVE.request()		Leave
S16	Leave		A partir de la couche MAC: analyse du message d'indication de départ de la DLSL ou message de confirmation et invocation de DLME-LEAVE.indication() ou DLME-LEAVE.confirm(); A partir du processus DMAP: analyse du message de demande de départ de la DLSL et invocation de MLME-DISASSOCIATE.request()	Idle
S17	Wait	A partir de la couche MAC: MLME-ASSOCIATE.indication() ou MLME-ASSOCIATE.confirm() A partir du processus DMAP: DLME-JOIN.request () ou DLME-JOIN.response ()		One-Hop Join
S18	One-Hop Join		A partir de la couche MAC: analyse du message d'indication d'association de MAC ou message de confirmation et invocation de DLME-JOIN.indication() ou DLME-JOIN.confirm(); A partir du processus DMAP: analyse de la demande de rattachement du DMPA ou message de réponse et invocation de MLME-ASSOCIATE.request() ou MLME-ASSOCIATE.response()	Idle
S19	Wait	A partir de la couche MAC: MLME-COMM-STATUS.indication() et pas de trame reçue ou échec de réception A partir du processus DMAP et de la NL: pas de message reçu	A partir de la couche MAC: invocation de DLME-COMM-STATUS.indication(FAILURE_ELSE)	Idle

Tableau 40 (3 de 3)

Numéro séquentiel #	Etat courant	Evénement ou condition	Actions	Prochain état
S20	Idle	Temporisation d'intervalle de temps LinkType = Transmission ou LinkType = Transmission partagée	Invocation de MCPS-DATA.request()	Transmission
S21	Transmission	MCPS-DATA.confirm()	Reprogrammation ou nouvelle tentative de trame si la transmission a échoué; Libération du tampon de trame si MCPS-DATA.confirm (SUCCESS);	Idle

Voir 8.5 pour les primitives relatives à la DLSL; voir 0 pour les formats de trames relatifs à la DLSL; voir 9.4 et 9.5 pour les primitives relatives à la NL; voir 6.2 de l'IEEE 802.15.4-2011 pour les primitives relatives à la couche MAC; voir 6.9.1.2.1 pour Devicestate.

Les états dans le diagramme d'états de la DLSL sont spécifiés ci-après.

a) Etat Join (rattachement)

Cet état gère la procédure de rattachement d'un appareil. Après qu'un appareil s'est rattaché au réseau, le diagramme d'états de la sous-couche DLSL se met en marche, comme représenté à la Figure 34.

b) Etat Leave (départ)

Cet état gère la procédure de départ d'un appareil.

c) Etat Idle (repos)

Après qu'un appareil s'est rattaché au réseau, la sous-couche DLSL se met dans l'état Idle (repos). Les transitions suivantes peuvent survenir pendant que la sous-couche DLSL est dans l'état Idle (repos):

- Lorsqu'un intervalle de temps arrive, la DLSL se met dans l'état Transmission (émission) ou Receive (réception) en fonction des options de la liaison (émission, réception ou transmission partagée).

d) Etat Transmission (émission)

Lorsque l'intervalle de temps arrive et que l'option de liaison est la liaison d'émission, la sous-couche DLSL se met dans l'état Transmission (émission). Les événements suivants se produiront pendant que la DLSL est dans l'état Transmission (émission):

- La propagation réussie d'une trame avec une adresse de destination de diffusion/multidiffusion survient dès que la trame est émise. Après quoi, le tampon de trame est libéré.
- La propagation réussie d'une trame avec une adresse de destination de monodiffusion survient lorsqu'une confirmation validée et réussie est reçue de la couche MAC locale. Cela indique que la propagation du message s'est achevée avec succès et le tampon de trame est ensuite libéré.
- Si une confirmation de défaillance est reçue de la couche MAC locale, il convient que la trame fasse l'objet d'une nouvelle tentative.
- En cas de réception d'une réponse avec une erreur ou en cas d'absence de réponse, il convient de reprogrammer la trame ou que cette dernière fasse l'objet d'une nouvelle tentative.

e) Etat Wait (attente)

Les trames qu'un appareil peut recevoir comprennent les trames dont les adresses de destination finale sont les appareils et les trames dont les adresses de destination finale ne sont pas celles de l'appareil en question. Les fonctions de l'état Wait (attente) sont de recevoir, vérifier et traiter la trame. Les transitions suivantes peuvent survenir pendant que la sous-couche DLSL est dans l'état Wait (attente).

- Si aucune trame n'est reçue, la sous-couche DLSL évaluera la liaison et retournera à l'état Idle (repos).
- Si une trame balise ou une trame de commande de synchronisation du temps est reçue, c'est l'état Synchronization (synchronisation) qui est en vigueur.
- Si une trame de commande d'entretien est reçue, alors l'état Keep-alive (entretien) est en vigueur;
- Si une demande de départ du DMAP est reçue, alors l'état Leave (départ) est en vigueur.
- Si une commande de rattachement en provenance du DMAP est reçue, alors l'état One-Hop Join (rattachement en un saut) est en vigueur.
- A la réception d'une trame réussie, la sous-couche DLSL traitera la priorité de la trame (réception ou rejet), puis l'appareil retourne directement à l'état Idle (repos).

f) Etat Data (données)

Dans cet état, les données de la DLSL sont générées ou analysées. Après avoir reçu la trame de données de la DLSL, LinkQuality et PacketLossRate sont évaluées. Après avoir généré la trame de données de la DLSL, la DLSL se met dans l'état Wait (attente).

g) Etat Synchronization (synchronisation)

Dans cet état, la synchronisation du temps est exécutée après réception d'une trame balise ou d'une trame de commande de synchronisation du temps par un appareil, puis la sous-couche DLSL se met dans l'état Idle (repos).

h) Etat Keep-alive (entretien)

Dans cet état, un nœud voisin est marqué comme nœud d'entretien après réception d'une trame de commande d'entretien par un appareil, puis la sous-couche DLSL se met dans l'état Idle (repos).

i) Etat One-Hop Join (rattachement en un saut)

Dans cet état, le processus de rattachement en un saut est pris en charge par l'appareil de passerelle.

8.5 Services de données de la sous-couche liaison de données

8.5.1 Généralités

Le DLDE-SAP prend en charge la transmission point à point d'unités de données de protocole DLSL (DLDPDU) entre les appareils. Les primitives prises en charge par les services de données de la sous-couche comprennent DLDE-DATA.request, DLDE-DATA.confirm et DLDE-DATA.indication.

8.5.2 DLDE-DATA.request

L'entité de données de sous-couche liaison de données (DLDE) reçoit la charge utile de la couche réseau (NL) par le biais de DLDE-DATA.request et l'ajoute à la file d'attente de messages de la sous-couche DLSL.

La sémantique de DLDE-DATA.request est décrite comme suit:

```
DLDE-DATA.request (
    NetworkID,
    SrcAddrMode,
    SrcAddr,
    DstAddrMode,
    DstAddr,
    Priority,
    Type,
    PayloadLength,
    Payload,
    PayloadHandle
)
```

Le Tableau 41 spécifie les paramètres pour DLDE-DATA.request.

Tableau 41 – Paramètres de DLDE-DATA.request

Nom	Type de données	Plage valide	Description
NetworkID	Unsigned8	0 à 255	Identificateur réseau
SrcAddrMode	Unsigned8	0 à 3	Mode d'adresse source: 0 = Aucune adresse 1 = Réservé 2 = Adresse courte 16 bits 3 = Adresse longue 64 bits
SrcAddr	Unsigned16/64	0 à 65 535 ou $(2^{64}-1)$	Source address (adresse source) L'adresse longue 64 bits est utilisée uniquement dans le processus de rattachement d'appareil alors que l'adresse courte 16 bits est d'usage général.
DstAddrMode	Unsigned8	0 à 3	Mode d'adresse de destination: 0 = Aucune adresse 1 = Réservé 2 = Adresse courte 16 bits 3 = Adresse longue 64 bits
DstAddr	Unsigned16/64	0 à 65 535 ou $(2^{64}-1)$	Adresse de destination, 16 bits ou 64 bits
Priorité	Unsigned8	0 à 15	Priorité de la charge utile
Type de données	Unsigned8	0 à 1	0 = Emission intragroupe 1 = Emission intergroupe
PayloadLength	Unsigned8	$\leq \text{MaxMACFrameSize}$	Longueur de la charge utile
Payload (charge utile)	Octetstring		Payload (charge utile)
PayloadHandle	Unsigned8	0 à 255	Descripteur alloué lors de l'appel de DLDE-DATA.request

8.5.3 DLDE-DATA.confirm

La sémantique de DLDE-DATA.confirm est décrite comme suit:

```
DLDE-DATA.confirm (
    PayloadHandle,
    Status
)
```


Le Tableau 42 spécifie les paramètres pour DLDE-DATA.confirm.

Tableau 42 – Paramètres de DLDE-DATA.confirm

Nom	Type de données	Plage valide	Description
PayloadHandle	Unsigned8	0 à 255	Descripteur alloué lors de l'appel de DLDE-DATA.confirm
Statut	Unsigned8	0 à 255	Résultat de la transmission de données de la DSL: 0 = SUCCESS (succès) 1 = TRANSACTION_OVERFLOW 2 = TRANSACTION_EXPIRED 3 = NO_ACK 4 = CHANNEL_ACCESS_FAILURE 5 = UNAVAILABLE_KEY 6 = FAILED_SECURITY_CHECK 7 = INVALID_PARAMETER Les autres valeurs sont réservées. Voir Tableau 43 pour plus de détails.

Tableau 43 – Tableau pour Status (état)

ID	Valeur	Description
0	SUCCESS	L'opération demandée est parachevée avec succès. Pour une demande d'émission, cette valeur indique une émission réussie.
1	TRANSACTION_OVERFLOW	Insuffisance d'espace pour stocker les transactions
2	TRANSACTION_EXPIRED	La transaction a expiré et ses informations ont été supprimées
3	NO_ACK	Aucun message d'acquittement n'a été reçu après macMaxFrameRetries
4	CHANNEL_ACCESS_FAILURE	Ne peut pas émettre en raison de la défaillance d'accès au canal.
5	UNAVAILABLE_KEY	Aucune clé valide dans la liste de contrôle d'accès
6	SECURITY_ERROR	Echec du traitement cryptographique de la trame sécurisée reçue
7	INVALID_PARAMETER	Un paramètre des primitives se situe en dehors de la plage de valeurs
8	NO-BEACON	Une opération de balayage n'a pas pu trouver de balise réseau.
9 à 255	Réservé	

8.5.4 DLDE-DATA.indication

La sémantique de DLDE-DATA.indication est décrite comme suit:

DLDE-DATA.indication (

NetworkID,
ScrAddrMode,
SrcAddr,
Type,
Priority,
PayloadLength,
Payload,
PayloadLinkQuality,

)

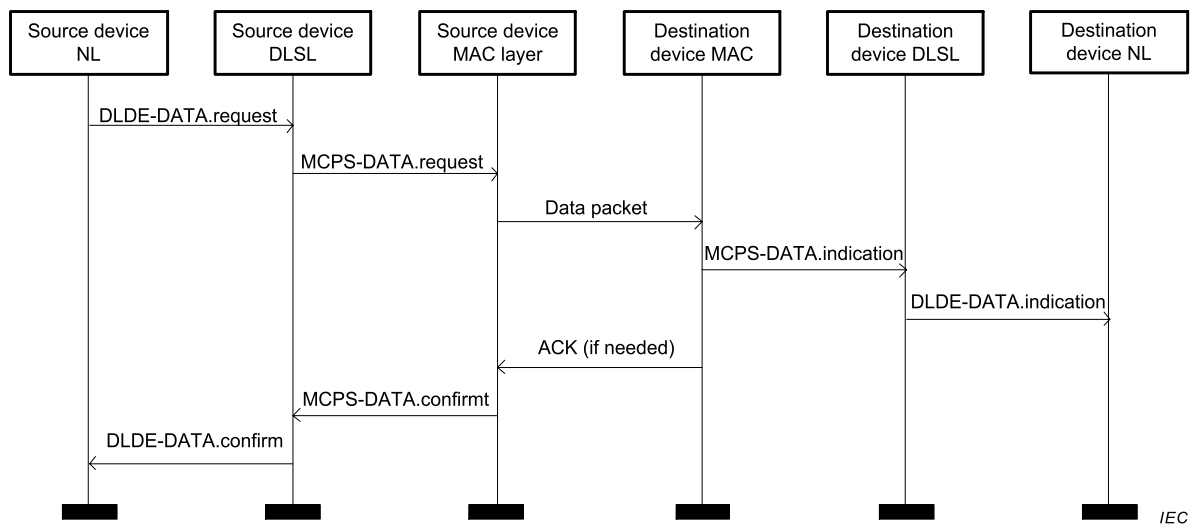
Le Tableau 44 spécifie les paramètres pour DLDE-DATA.indication.

Tableau 44 – Paramètres de DLDE-DATA.indication

Nom	Type de données	Plage valide	Description
NetworkID	Unsigned8	0 à 255	Identificateur réseau
SrcAddrMode	Unsigned8	0 à 3	Mode d'adresse source. Quatre options sont disponibles: 0 = Aucune adresse 1 = Réservé 2 = Adresse courte 16 bits 3 = Adresse longue 64 bits
SrcAddr	Unsigned16/64	0 à 65 535 ou $(2^{64}-1)$	Adresse source, utilisant l'adresse longue 64 bits uniquement dans le processus de rattachement d'appareil et utilisant l'adresse courte 16 bits d'une manière générale
Type	Unsigned8	0 à 1	0 = Emission intragroupe 1 = Emission intergroupe
Priorité	Unsigned8	0 à 15	Priorité de la charge utile
PayloadLength	Unsigned8	$\leq \text{MaxMACFrameSize}$	Longueur de la charge utile
Payload (charge utile)	Octetstring		Payload (charge utile)
PayloadLinkQuality	Unsigned8	0 à 255	Valeur de LQI mesurée pendant la réception de l'unité DLPDU Les valeurs plus basses représentent une qualité de liaison inférieure.

8.5.5 Séquence temporelle de service de données DLSL

La Figure 35 montre la séquence des transactions de données pour transporter un paquet de données depuis un appareil source jusqu'à un appareil de destination.



Anglais	Français
Source device NL	Appareil source NL
Source device DLSL	Appareil source DLSL
Source device MAC layer	Appareil source couche MAC
Destination device MAC	Appareil de destination MAC
Destination device DLSL	Appareil de destination DLSL
Destination device DL	Appareil de destination DL
Data packet	Paquet de données
ACK (if needed)	ACK (si nécessaire)

Figure 35 – Séquence temporelle de service de données

La primitive DLDE-DATA.request est générée par une entité de données de couche réseau (NLDE) locale lorsqu'une unité de données de protocole réseau (NPDU) doit être transférée à une entité NLDE homologue.

A la réception de DLDE-DATA.request, l'entité DLDE insère le message dans le tampon d'envoi et commence l'envoi de l'unité DLPDU fournie.

La primitive DLDE-DATA.indication est générée par l'entité DLDE d'un appareil de destination et envoyée à l'entité NLDE à la réception d'une trame de données au niveau de l'entité DLDE locale qui passe les opérations appropriées de filtrage de messages.

La primitive DLDE-DATA.confirm est générée par l'entité DLDE d'un appareil source en réponse à la primitive DLDE-DATA.request. La primitive DLDE-DATA.confirm renvoie un état indiquant le résultat de l'émission.

Voir la Figure 27 de l'IEEE 802.15.4-2011 pour le diagramme de séquence de message détaillé entre les entités MAC homologues.

8.6 Services de gestion de la sous-couche liaison de données

8.6.1 Généralités

La couche supérieure utilise le point d'accès DLME-SAP pour envoyer des commandes de gestion à la sous-couche DLSL. Les services de gestion DLSL comprennent la découverte de sous-réseau, le rattachement et le départ d'appareils, la collecte et le rapport sur les

conditions de canal et sur les informations relatives aux voisins ainsi que la synchronisation du temps.

8.6.2 Services de découverte de réseau

8.6.2.1 Généralités

Les services de découverte de réseau de la sous-couche DLSL sont utilisés pour balayer une liste donnée de canaux de communication. Un appareil peut utiliser les services de découverte de réseau pour rechercher des têtes de groupe envoyant des trames balise dans les limites de sa portée de communication. Les primitives prises en charge par les services de découverte de réseau DLSL comprennent DLME-DISCOVERY.request et DLME-DISCOVERY.confirm.

8.6.2.2 DLME-DISCOVERY.request

DLME-DISCOVERY.request est utilisée pour demander à un appareil de balayer les canaux.

La sémantique de DLME-DISCOVERY.request est décrite comme suit:

DLME-DISCOVERY.request (

ScanChannels,

ScanDuration

)

Le Tableau 45 spécifie les paramètres pour DLME-DISCOVERY.request.

Tableau 45 – Paramètres de DLME-DISCOVERY.request

Nom	Type de données	Plage valide	Description
ScanChannels	Unsigned32	Carte de bits de 32 bits	Les bits 11 à 26 indiquent les canaux de l'IEEE 802.15.4-2011 de la bande de fréquences de 2,4 GHz; les autres sont définis. Voir 6.2.10 de l'IEEE 802.15.4-2011 pour ScanChannels.
ScanDuration	Unsigned8	0 à 14	Valeur utilisée pour calculer la durée à passer à balayer chaque canal pour les balayages de détection d'énergie (ED, energy detection), actifs et passifs Ce paramètre est ignoré pour les balayages d'orphelin. La durée de balayage de chaque canal est: $aBaseSuperframeDuration \times (2^n + 1)$ où n est la valeur du paramètre ScanDuration..
Voir le Tableau 51 de l'IEEE 802.15.4-2011 pour la définition et l'établissement de la valeur de aBaseSuperframeDuration.			

8.6.2.3 DLME-DISCOVERY.confirm

La primitive DLME-DISCOVERY.confirm est utilisée pour répondre à la primitive DLME-DISCOVERY.request.

La sémantique de DLME-DISCOVERY.confirm est décrite comme suit:

```
DLME-DISCOVERY.confirm(
    Status,
    NetworkCount,
    NetworkDescriptor
)
```

Le Tableau 46 spécifie les paramètres pour DLME-DISCOVERY.confirm. Le Tableau 47 spécifie la liste des descripteurs de réseau.

Tableau 46 – Paramètres de DLME- DISCOVERY.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultats du balayage 0 = SUCCESS (succès) 7 = INVALID_PARAMETER 8 = NO_BEACON Les autres valeurs sont réservées. Voir Tableau 43 pour plus de détails.
NetworkCount	Unsigned8	0 à 255	Nombre de réseaux actifs trouvés au cours du balayage
NetworkDescriptor	Network descriptor list (liste de descripteurs de réseau)	0 à NetworkCount	Liste de descripteurs de réseau pour chaque réseau trouvé, voir Tableau 47

Tableau 47 – Network descriptor list (liste de descripteurs de réseau)

Nom	Type de données	Plage valide	Description
LogicalChannel	Unsigned8	0 à 31	Canal logique pour le rattachement, choisi parmi les canaux valides pris en charge par la couche PHY
BeaconOrder	Unsigned8	0 à 15	Fréquence envoyant la trame balise
SuperframeOrder	Unsigned8	0 à 15	Longueur de période active de la supertrame
PermitJoining	Booléen	0, 1	Savoir si l'appareil de routage autorise l'appareil de terrain à se rattacher: 0 = Aucune permission 1 = Il est permis à au moins un appareil de se rattacher

Si le balayage a réussi, DLME-DISCOVERY.confirm retourne SUCCESS; cependant, si aucune balise n'est trouvée, DLME-DISCOVERY.confirm retourne NO_BEACON; S'il y a des erreurs ou des paramètres non valides dans la primitive DLME-DISCOVERY.request, DLME-DISCOVERY.confirm retourne INVALID_PARAMETER.

8.6.2.4 Séquence temporelle de découverte de sous-réseau

La séquence temporelle pour la découverte de sous-réseau est indiquée à la Figure 36. Voir l'IEEE 802.15.4-2011 pour les primitives MLME-SCAN.request et MLME-SCAN.confirm.

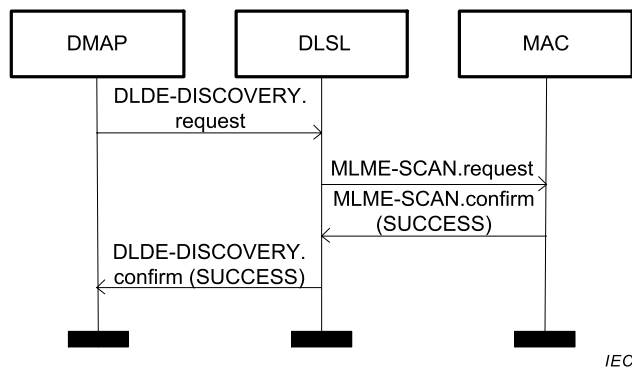


Figure 36 – Séquence temporelle de découverte de réseau

Voir la Figure 12 et la Figure 13 de l'IEEE STD 802.15.4-2011 pour le diagramme de séquence de message détaillé entre les entités MAC homologues.

8.6.3 Services de rattachement d'appareil

8.6.3.1 Généralités

Il existe deux instances exigeant les services de rattachement d'appareil:

- a) un nouvel appareil de terrain se rattache au réseau en étoile;
- b) un nouvel appareil de routage se rattache au réseau maillé. Les primitives prises en charge par les services de rattachement d'appareils de la DLSL comprennent DLME-JOIN.request, DLME-JOIN.indication, DLME-JOIN.response, et DLME-JOIN.confirm.

8.6.3.2 DLME-JOIN.request

La primitive DLME-JOIN.request est utilisée pour un appareil se rattachant au réseau (en étoile ou maillé).

La sémantique de DLME-JOIN.request est décrite comme suit:

```

DLME-JOIN.request (
    LogicalChannel,
    JoinAddr,
    PhyAddr,
    DeviceType
)
    
```

Le Tableau 48 spécifie les paramètres pour DLME-JOIN.request.

Tableau 48 – Paramètres de DLME-JOIN.request

Nom	Type de données	Plage valide	Description
LogicalChannel	Unsigned8	0 à 31	Canal logique pour le rattachement, choisi parmi les canaux valides pris en charge par la couche PHY
JoinAddr	Unsigned16	0 à 65 535	Adresse courte de l'appareil de routage ou de l'appareil de passerelle qui accepte la demande de rattachement
PhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse physique du nouvel appareil attendant de se rattacher.
DeviceType	Unsigned8	0 à 255	Type du nouvel appareil attendant de se rattacher: 0 = Appareil de passerelle 1 = Appareil de routage 2 = Appareil de terrain 3 = Appareil tenu à la main Les autres valeurs sont réservées.

8.6.3.3 DLME-JOIN.indication

La primitive DLME-JOIN.indication est utilisée pour informer l'entité NLME d'un appareil de routage ou pour informer l'appareil de passerelle que la demande de rattachement d'un appareil a été reçue avec succès.

La sémantique de DLME- JOIN.indication est décrite comme suit:

DLME-JOIN.indication (

PhyAddr,
DeviceType

)

Le Tableau 49 spécifie les paramètres pour DLME-JOIN.indication.

Tableau 49 – Paramètres de DLME-JOIN.indication

Nom	Type de données	Plage valide	Description
PhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse du nouvel appareil attendant de se rattacher
DeviceType	Unsigned8	0 à 255	Type du nouvel appareil attendant de se rattacher: 0 = Appareil de passerelle 1 = Appareil de routage 2 = Appareil de terrain 3 = Appareil tenu à la main Les autres valeurs sont réservées.

8.6.3.4 DLME-JOIN.response

La primitive DLME-JOIN.response est la réponse de la primitive DLME-JOIN.indication.

La sémantique de DLME-JOIN.response est décrite comme suit:

```
DLME-JOIN.response (
    PhyAddr,
    ShortAddr,
    TimeSource,
    Status
)
```

Le Tableau 50 spécifie les paramètres pour DLME-JOIN.response.

Tableau 50 – Paramètres de DLME-JOIN.response

Nom	Type de données	Plage valide	Description
PhyAddr	Unsigned64	0 à $(2^{64}-1)$	Adresse de l'appareil attendant de se rattacher
ShortAddr	Unsigned16	0 à 65 535	Adresse courte allouée par le NM à l'appareil attendant de se rattacher
TimeSource	Unsigned8	0 à 1	Savoir si cet appareil est réglé comme source temporelle: 0 = Pas une source temporelle 1 = Source temporelle
Statut	Unsigned8	0 à 255	Résultat de la demande de rattachement: 0 = SUCCESS (succès) 1 = FAILURE_TOP_DISMATCH 2 = FAILURE_ELSE Les autres valeurs sont réservées.

8.6.3.5 DLME-JOIN.confirm

La primitive DLME-JOIN.confirm rapporte le résultat du rattachement au DMAP.

La sémantique de DLME-JOIN.confirm est décrite comme suit:

```
DLME-JOIN.confirm (
    ShortAddr,
    Status
)
```

Le Tableau 51 spécifie les paramètres pour DLME-JOIN.confirm.

Tableau 51 – Paramètres de DLME-JOIN.confirm

Nom	Type de données	Plage valide	Description
ShortAddr	Unsigned16	0 à 65 535	Adresse courte allouée par NM pour l'appareil attendant de se rattacher
Statut	Unsigned8	0 à 255	Résultat de la demande de rattachement: 0 = SUCCESS (succès) 1 = FAILURE_TOP_DISMATCH 2 = FAILURE_ELSE Les autres valeurs sont réservées.

8.6.3.6 Séquence temporelle pour l'appareil se rattachant au réseau

Voir 9.5.3 pour le processus détaillé de rattachement.

8.6.4 Services de départ d'appareil

8.6.4.1 Généralités

Il existe deux instances exigeant les services de départ d'appareil: (1) un appareil de terrain quitte le réseau en étoile ou (2) un appareil de routage quitte le réseau maillé. Les primitives prises en charge par les services de départ d'appareil DSLR comprennent DLME-LEAVE.request, DLME-LEAVE.indication et DLME-LEAVE.confirm.

8.6.4.2 DLME-LEAVE.request

La sémantique de DLME-LEAVE.request est décrite comme suit:

```
DLME-LEAVE.request (
    ShortAddr
)
```

Le Tableau 52 spécifie les paramètres pour DLME-LEAVE.request.

Tableau 52 – Paramètres de DLME-LEAVE.request

Nom	Type de données	Plage valide	Description
ShortAddr	Unsigned16	0 à 65 535	Adresse courte de l'appareil demandant de partir

8.6.4.3 DLME-LEAVE.indication

La primitive DLME-LEAVE.indication est utilisée pour indiquer à la couche supérieure qu'une demande de départ d'appareil a été reçue.

La sémantique de DLME-LEAVE.indication est décrite comme suit:

```
DLME-LEAVE.indication (
    ShortAddr
)
```

Le Tableau 53 spécifie les paramètres pour DLME-LEAVE.indication.

Tableau 53 – Paramètres de DLME-LEAVE.indication

Nom	Type de données	Plage valide	Description
ShortAddr	Unsigned16	0 à 65 535	Adresse courte de l'appareil demandant de partir

8.6.4.4 DLME-LEAVE.confirm

La primitive DLME-LEAVE.confirm est utilisée pour rapporter le résultat de DLME-LEAVE.request.

La sémantique de DLME-LEAVE.confirm est décrite comme suit:

```
DLME-LEAVE.confirm (
    Statut
)
```

Le Tableau 54 spécifie les paramètres pour DLME-LEAVE.confirm.

Tableau 54 – Paramètres de DLME-LEAVE.confirm

Nom	Type de données	Plage valide	Description
Status	Unsigned8	0 à 255	Résultat de la demande de départ: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

8.6.4.5 Séquence temporelle pour le départ d'appareil

Voir l'IEEE 802.15.4-2011 pour les primitives suivantes: MLME-DISASSOCIATE.request, MLME-DISASSOCIATE.confirm et MLME-DISASSOCIATE.indication.

Les séquences temporelles pour les appareils quittant le réseau sont définies comme suit.

a) Séquence temporelle pour les appareils de routage quittant le réseau

Les appareils de routage se connectent tant au réseau maillé qu'au réseau en étoile. Par conséquent, le processus des appareils de routage quittant le réseau comprend les appareils de routage quittant le réseau maillé et ceux quittant le réseau en étoile. En fonction du demandeur du départ, le processus des appareils de routage quittant le réseau inclut le départ actif et le départ passif.

b) Séquence temporelle pour les appareils de terrain quittant le réseau

En fonction de la source du départ, le processus des appareils de terrain quittant le réseau inclut le départ actif et le départ passif.

Voir 9.5.4 pour le processus détaillé du départ d'appareil.

8.6.5 DLME-CHANNEL-CONDITION.indication

La primitive DLME-CHANNEL-CONDITION.indication est utilisée pour que la DLSL rapporte les informations concernant les conditions de canaux au DMAP. Les données de performance rapportées comprennent l'indication de qualité de liaison (LQI), le taux de perte de paquets et le nombre de nouvelles tentatives.

La sémantique de DLME-CHANNEL-CONDITION.indication est décrite comme suit:

DLME-CHANNEL-CONDITION.indication (

ChannelNum,
ChannelStructure
)

Le Tableau 55 spécifie les paramètres pour DLME-CHANNEL-CONDITION.indication.

Tableau 55 – Paramètres de DLME-CHANNEL-CONDITION.indication

Nom	Type de données	Plage valide	Description
ChannelNum	Unsigned8	0 à 255	Nombre de canaux
ChannelStructure	ChanCon_Struct		Informations de canaux

8.6.6 DLME-NEIGHBOUR-INFO.indication

La primitive DLME-NEIGHBOUR-INFO.indication est utilisée pour rapporter les informations recueillies concernant les voisins au DMAP et mettre à jour les attributs voisins.

La sémantique de DLME-NEIGHBOUR-INFO.indication est décrite comme suit:

DLME-NEIGHBOUR-INFO.indication (

NeighbourCount,
NeighbourStructure
)

Le Tableau 56 spécifie les paramètres pour DLME-NEIGHBOUR-INFO.indication.

Tableau 56 – Paramètres de DLME-NEIGHBOUR-INFO.indication

Nom	Type de données	Plage valide	Description
NeighbourCount	Unsigned8	0 à 255	Nombre d'appareils voisins
NeighbourStructure	Structure Neighbour_Struct		Informations de voisins

8.6.7 DLME-COMM-STATUS.indication

La primitive DLME-COMM-STATUS.indication est utilisée pour rapporter l'état de communication à la couche supérieure.

La sémantique de DLME-COMM-STATUS.indication est décrite comme suit:

DLME-COMM-STATUS.indication (

PhyAddr,
Statut
)

Le Tableau 57 spécifie les paramètres pour DLME-COMM-STATUS.indication.

Tableau 57 – Paramètres de DLME-COMM-STATUS.indication

Nom	Type de données	Plage valide	Description
PhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse d'un nouvel appareil qui vient juste de se rattacher au réseau
Status	Unsigned8	0 à 255	L'état de rattachement d'un appareil: 0 = SUCCESS (succès) 1 = FAILURE_TOP_DISMATCH 2 = FAILURE_ELSE Les autres valeurs sont réservées.

8.6.8 Services d'entretien

8.6.8.1 DLME-KEEP-LIVE.request

La primitive DLME-KEEP-LIVE.request est utilisée pour envoyer les trames de commande d'entretien qui sont demandées par le DMAP.

La sémantique de DLME-KEEP-LIVE.request est décrite comme suit:

DLME-KEEP-LIVE.request (
)

8.6.8.2 DLME-KEEP-LIVE.confirm

La primitive DLME-KEEP-LIVE.confirm est utilisée pour répondre à la primitive DLME -KEEP-LIVE.request.

La sémantique de DLME -KEEP-LIVE.confirm est décrite comme suit:

```
DLME -KEEP-LIVE.confirm (
                                Statut
)
```

Le Tableau 58 spécifie les paramètres pour DLME-KEEP-LIVE.confirm.

Tableau 58 – Paramètres de DLME -KEEP-LIVE.confirm

Nom	Type de données	Plage valide	Description
Status	Unsigned8	0 à 255	Résultat de l'entretien: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

8.6.8.3 DLME-KEEP-LIVE.indication

La primitive DLME-KEEP-LIVE.indication est utilisée pour informer le DMAP que la trame de commande d'entretien a été reçue avec succès.

La sémantique de DLME-KEEP-LIVE.indication est décrite comme suit:

```
DLME-KEEP-LIVE.indication (
                                SrcAddr
)
```

Le Tableau 59 spécifie les paramètres pour DLME-KEEP-LIVE.indication.

Tableau 59 – Paramètres de DLME -KEEP-LIVE.indication

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse source

8.6.9 Services de synchronisation du temps

8.6.9.1 DLME-TIME-SYN.request

La primitive DLME-TIME-SYN.request est utilisée pour envoyer des trames de commande de synchronisation du temps qui sont demandées par le DMAP.

La sémantique de DLME-TIME-SYN.request est décrite comme suit:

```
DLME-TIME-SYN.request (
                                TimeValue
)
```

Le Tableau 60 spécifie les paramètres pour DLME-TIME-SYN.request.

Tableau 60 – Paramètres de DLME-TIME-SYN.request

Nom	Type de données	Plage valide	Description
TimeValue	Unsigned16	0 à $(2^{16}-1)$	Différence de temps entre le début de l'émission et le début de l'intervalle de temps (en microsecondes)

8.6.9.2 DLME-TIME-SYN.confirm

La primitive DLME-TIME-SYN.confirm est utilisée pour répondre à la primitive DLME-TIME-SYN.request.

La sémantique de DLME-TIME-SYN.confirm est décrite comme suit:

DLME-TIME-SYN.confirm (

Statut
)

Le Tableau 61 spécifie les paramètres pour DLME-TIME-SYN.confirm.

Tableau 61 – Paramètres de DLME -TIME-SYN.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultat de la synchronisation du temps: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

8.6.9.3 DLME-TIME-SYN.indication

La primitive DLME-TIME-SYN.indication est utilisée pour informer le DMAP que la trame de commande de synchronisation de temps a été reçue avec succès.

La sémantique de DLME-TIME-SYN.indication est décrite comme suit:

DLME-TIME-SYN.indication (

SrcAddr,
TimeValue
)

Le Tableau 62 spécifie les paramètres pour DLME-TIME-SYN.indication.

Tableau 62 – Paramètres de DLME-TIME-SYN.indication

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse source
TimeValue	Unsigned16	0 à $(2^{16}-1)$	Différence de temps entre le début de l'émission et le début de l'intervalle de temps (en microsecondes)

8.7 Formats de trame DLSL

8.7.1 Format général de trame

Le format général de trame DLSL est représenté à la Figure 37.

MAC Protocol Data Unit (MPDU); Unité de données de protocole MAC (MPDU)			
MHR	DLPDU		FCS
IEEE 802.15.4-2011 MAC header (MHR) (En-tête MAC [MHR] de l'IEEE 802.15.4-2011)	DLSL frame control (contrôle de trame DLSL)	DLSL payload (charge utile DLSL)	

IEC

Figure 37 – Format général de trame

La trame DLSL se compose de:

- l'en-tête MAC (MHR) IEEE 802.15.4-2011 (voir 5.2.1 de l'IEEE 802.15.4-2011);
- la commande de trame DLSL (voir Tableau 63);
- la charge utile DLSL;
- Séquence de contrôle de trame (FCS, Frame Check Sequence).

Voir 11.3.2 pour le contenu relatif à la sécurité.

Le format du contrôle de trame de sous-couche DLSL du réseau WIA-PA est indiqué au Tableau 63.

Tableau 63 – Champ DLSL frame control (contrôle de trame DLSL)

Champ DLSL frame control (contrôle de trame DLSL)				
Longueur en bit(s)	1	1	1	5
Nom de sous-champ	Frame type (type de trame)	Time source (source temporelle)	Security enable (activation de la sécurité)	Index of main channel (indice de canal principal)

Les sous-champs du Tableau 63 sont définis comme suit.

- Le sous-champ Frame type (type de trame) est de 1 bit, il est utilisé pour spécifier le type d'une trame. Si une trame est une trame de données, ce sous-champ est défini sur 0; autrement, il est défini sur 1.
- Le sous-champ Time source (source temporelle) est de 1 bit, il est utilisé pour indiquer si cet appareil est une source temporelle ou non. Si l'appareil est une source temporelle, ce sous-champ est défini sur 1; autrement, il est défini sur 0.
- Le sous-champ Security enable (activation de la sécurité) est de 1 bit, il est utilisé pour spécifier à la DLSL d'utiliser le mécanisme de sécurité ou non. La valeur 0 signifie que le mécanisme de sécurité est désactivé et la valeur 1 signifie que le mécanisme de sécurité est activé.
- Le sous-champ Index of main channel (indice de canal principal) est utilisé pour indiquer le canal de communication courant.

Il convient de transmettre ou recevoir tous les champs d'octets multiples avec l'octet de poids faible en premier lieu et il convient de transmettre ou recevoir d'abord chaque octet avec le bit de poids faible (LSB). Il convient d'appliquer le même ordre de transmission aux champs de données transférés entre les couches.

8.7.2 Format de trame de données

Le format de la trame de données DLSL est indiqué au Tableau 64.

Tableau 64 – Format de trame de données

	Format de trame de données	
Longueur en octet(s)	1	Longueur variable
Nom de champ	DLSL frame control (contrôle de trame DLSL)	Data payload (charge utile de données)

Les sous-champs du Tableau 64 sont définis comme suit:

- a) le sous-champ DLSL frame control (contrôle de trame DLSL) est défini au Tableau 63;
- b) le sous-champ Data payload (charge utile de données) est doté d'une longueur variable et il est rempli avec les données DLSL.

8.7.3 Format de trame de commande

8.7.3.1 Format général d'une trame de commande

Le format général de trame de commande est indiqué au Tableau 65.

Tableau 65 – Format général d'une trame de commande

	Format général d'une trame de commande		
Longueur en octet(s)	1	1	Longueur variable
Nom de champ	DLSL frame control (contrôle de trame DLSL)	Command frame identifier (identificateur de trame de commande)	Command payload (charge utile de commande)

Les sous-champs du Tableau 65 sont définis comme suit:

- a) le sous-champ DLSL frame control (contrôle de trame DLSL) est défini au Tableau 63;
- b) le sous-champ Command frame identifier (identificateur de trame de commande) est défini au Tableau 66;
- c) le sous-champ Command payload (charge utile de commande) est doté d'une longueur variable et il est rempli avec les données de gestion DLSL.

8.7.3.2 Trame de commande DLSL

8.7.3.2.1 Généralités

Les trames de commande DLSL sont définies et indiquées au Tableau 66.

Tableau 66 – Trame de commande DLSL

Command frame identifier (identificateur de trame de commande)	Trame de commande DLSL		
	Nom de commande	Utilisateur	Description
1	Trame de commande d'entretien	Appareil de passerelle/Appareil de routage/Appareil de terrain	Indiquant un appareil existant
2	Trame de commande de synchronisation de l'heure	Appareil de passerelle/Appareil de routage	Réalisation la synchronisation de l'heure pour le réseau tout entier
3 à 255	Réservé	Réservé	A étendre

La trame de commande d'entretien facilite la maintenance des connexions entre appareils voisins. Après le rattachement des appareils au réseau, leurs DMAP envoient une trame de commande d'entretien avec la primitive de demande d'entretien. L'appareil de passerelle envoie la trame de commande d'entretien pendant la période de communication intergroupe, afin d'indiquer l'état vivant. Les appareils de routage envoient les trames de commande d'entretien pendant la période de communication intragroupe, afin d'indiquer qu'ils sont vivants à leurs éléments de groupe; en outre, les appareils de routage envoient des trames de commande d'entretien pendant la période de communication intergroupe, afin d'indiquer qu'ils sont vivants aux autres appareils de routage et à l'appareil de passerelle. Les appareils de terrain envoient les trames de commande d'entretien pendant la période de communication intragroupe, afin d'indiquer qu'ils sont vivants à leurs têtes de groupe.

Afin de garantir la fiabilité du code de communication AMRT, il convient que les appareils dans un réseau se synchronisent avec la source temporelle. Les erreurs de temps parmi les appareils sont inévitables en dépit de toute source temporelle matérielle. Afin de surmonter la dérive d'horloge temporelle, le réseau WIA-PA accomplit deux sortes de synchronisation du temps: balise de l'IEEE 802.15.4-2011 et la trame de commande de synchronisation du temps spécialement conçue. Dans le réseau en étoile uniquement, l'appareil de passerelle est la source de temps TUC. Dans la combinaison de réseau en étoile et de réseau maillé, l'appareil de passerelle est la source de temps TUC de la partie maillée et tous les appareils de routage se synchronisent avec l'appareil de passerelle; chaque appareil de routage est la source temporelle pour ses appareils de terrain dans la partie en étoile, qui se synchronise avec leurs appareils de routage.

Le présent document spécifie que l'erreur maximale de synchronisation est inférieure à 10 % de la longueur d'intervalle de temps de base de la durée maximale de supertrame.

8.7.3.2.2 Trame de commande d'entretien

Le format de la trame de commande d'entretien est indiqué au Tableau 67.

Tableau 67 – Format de la trame de commande d'entretien

Longueur en octet(s)	Format de la trame de commande d'entretien	
	1	1
Nom de champ	DLSL frame control (contrôle de trame DLSL)	Command frame identifier (identificateur de trame de commande)

Les sous-champs du Tableau 67 sont définis comme suit.

- Voir Tableau 63 pour DLSL frame control (contrôle de trame DLSL).
- Le sous-champ Command frame identifier (identificateur de trame de commande) est 10.

8.7.3.2.3 Trame de commande de synchronisation de l'heure

La trame de commande de synchronisation du temps est utilisée pour la synchronisation du réseau tout entier. L'appareil de passerelle et les appareils de routage envoient périodiquement les trames de commande de synchronisation du temps.

Si la topologie de réseau est en étoile uniquement, l'appareil de passerelle diffuse périodiquement la trame de commande de synchronisation du temps. Si la topologie de réseau est une combinaison de la configuration en étoile et de la configuration maillée, l'appareil de passerelle envoie en monodiffusion la trame de commande de synchronisation du temps au cours de la période de communication intergroupe; les appareils de routage diffusent les trames de commande de synchronisation du temps au cours de la période de communication intragroupe pour synchroniser leurs réseaux en étoile et les envoient en monodiffusion pendant la période de communication intergroupe pour se synchroniser avec le réseau maillé.

Le format de la trame de commande de synchronisation du temps est indiqué au Tableau 68.

Tableau 68 – Format de la trame de commande de synchronisation du temps

	Format de la trame de commande de synchronisation de l'heure		
Longueur en octet(s)	1	1	2
Nom de champ	DLSL frame control (contrôle de trame DLSL)	Command frame identifier (identificateur de trame de commande)	Valeur étalonée de TimeValue

Les sous-champs du Tableau 68 sont définis comme suit:

- a) voir Tableau 63 pour DLSL frame control (contrôle de trame DLSL);
- b) le sous-champ Command frame identifier (identificateur de trame de commande) est 11;
- c) voir Tableau 60 pour le sous-champ Calibrated value of TimeValue (valeur étalonée de TimeValue).

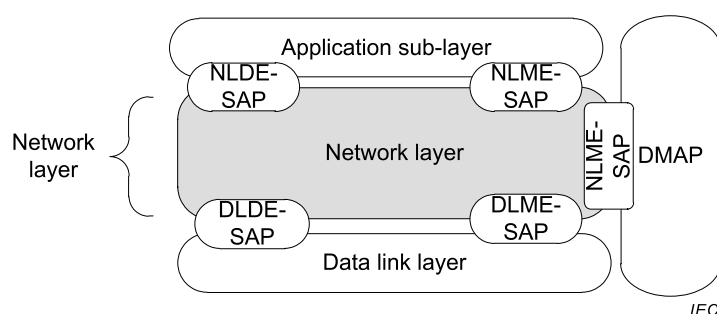
9 Couche Réseau

9.1 Généralités

La couche réseau (NL) du réseau WIA-PA reçoit et transporte des paquets sur les réseaux, fournit des interfaces à la sous-couche application (ASL) et exécute la gestion, la configuration et la commande de couche réseau.

9.2 Pile de protocole

La pile de protocole de la couche réseau WIA-PA est indiquée à la Figure 38.

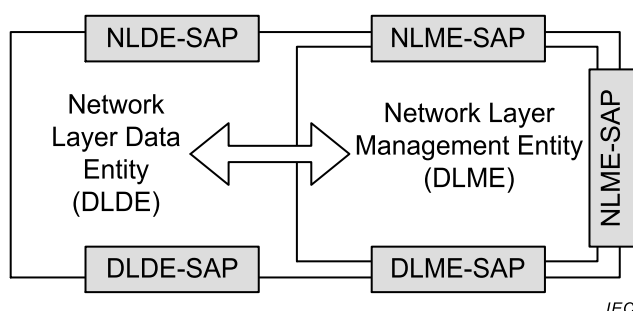


Anglais	Français
Application sub-layer	Sous-couche application (ASL)
Network layer	Couche réseau (NL)
Data link layer	Couche liaison de données (DLL)

Figure 38 – Pile de protocole de la couche réseau WIA-PA

Les couches et entités à la Figure 39 sont définies comme suit:

- la couche NL définit l'entité NLDE et l'entité de gestion de couche réseau (NLME);
- l'entité NLDE fournit l'interface de service par laquelle la sous-couche ASL émet et reçoit des données;
- l'entité NLME fournit les interfaces de service par lesquelles les fonctions de gestion de couche sont invoquées par la couche supérieure et le processus DMAP.



Anglais	Français
Network Layer Data Entity (NLDE)	Entité de données de la couche réseau (NLDE)
Network Layer Management Entity (NLME)	Entité de gestion de la couche réseau (NLME)

Figure 39 – Modèle de référence de couche réseau WIA-PA

La NL fournit deux types de services auxquels on accède grâce aux deux SAP suivants:

- le service de données de couche réseau, accédé via le point d'accès au service entité de données de couche réseau (NLDE-SAP);
- le service de gestion de couche réseau, accédé via le point d'accès au service entité de gestion de couche réseau (NLME-SAP).

9.3 Description de fonction

9.3.1 Généralités

La couche réseau (NL) est conçue pour accomplir les fonctions suivantes:

- adressage;
- routing;

- c) affectation de ressources de communication;
- d) gestion de cycle de vie des paquets;
- e) gestion des appareils se rattachant et quittant le réseau;
- f) surveillance bout en bout des performances du réseau;
- g) fragmentation et réassemblage.

9.3.2 Adressage

Chaque appareil a une adresse longue unique globale de 64 bits et une adresse courte de 16 bits. Chaque appareil se rattache au réseau en utilisant l'adresse longue et communique avec d'autres appareils en utilisant l'adresse courte après s'être rattaché au réseau. L'adresse courte de 16 bits est désignée comme x.y, où x et y sont des nombres entiers de 8 bits. Les 8 bits de poids fort dans l'adresse courte de 16 bits correspondent à l'adresse de groupe tandis que les 8 bits de poids faible correspondent à l'adresse intragroupe. La plage d'adresses de groupe s'étend de 0 à 255 tandis que la plage d'adresses intragroupe s'étend de 0 à 255. Le nombre 255 est utilisé pour l'adresse de diffusion. L'adresse intragroupe d'un appareil de routage est 0.

Les classifications des adresses courtes sont définies de la manière suivante:

- a) Adresses de monodiffusion: chaque adresse d'appareil est l'adresse de monodiffusion, y compris les types suivants:
 - l'adresse de l'appareil de passerelle est 0.0;
 - l'adresse de l'appareil de routage est x.0, où x est compris entre 1 et 254;
 - si la topologie de réseau est en étoile uniquement, à savoir NetworkTopology=1, l'adresse de l'appareil de terrain est 0.y, où y est compris entre 1 et 254; sinon, l'adresse de l'appareil de terrain est x.y, où x et y sont compris entre 1 et 254; voir 6.9.1.2.1 pour NetworkTopology.
- b) Adresse de diffusion: conformément aux différents domaines de diffusion, il y a quatre types d'adresses de diffusion:
 - l'adresse de diffusion intragroupe est x.255, où x est compris entre 0 et 254;
 - l'adresse de diffusion globale est 255.255;
 - l'adresse de diffusion du réseau maillé est 255.0;
 - l'adresse de diffusion de l'appareil de passerelle est 0.255.

9.3.3 Routage

9.3.3.1 Généralités

Le réseau WIA-PA prend en charge les algorithmes de routage statique configurés par le gestionnaire de réseau (NM). Après avoir obtenu de chaque appareil de routage les informations relatives aux voisins, le NM génère la relation de connexion de tous les appareils de routage. Sur la base de la relation de connexion, le NM génère et écrit les informations de routage dans chaque appareil de routage sous la forme d'une table de routage. Un identificateur d'itinéraire est assigné à chaque itinéraire de la table. Plusieurs chemins correspondent à chaque VCR, notamment le chemin principal et le chemin redondant. Le chemin principal et le chemin redondant utilisent le même identificateur d'itinéraire.

9.3.3.2 Table de routage

Chaque appareil de routage maintient une table de routage, qui est générée par le NM. La table de routage est utilisée pour choisir un chemin dans le réseau maillé. La table comporte cinq éléments. RouteID est l'identificateur d'un itinéraire. SourceAddress est l'adresse du point de départ d'un itinéraire, DestinationAddress est l'adresse du point d'extrémité d'un itinéraire, NextHop est l'adresse de l'appareil de prochain saut dans un itinéraire et RetryCounter enregistre le nombre de nouvelles tentatives en un saut dans un itinéraire qui

reflète l'état de l'itinéraire. Les RouteID des chemins avec la même adresse source et adresse de destination sont identiques.

Un exemple d'une table de routage est fourni au Tableau 69.

Tableau 69 – Exemple de table de routage

RouteID	SourceAddress	DestinationAddress	NextHop	RetryCounter
5	F1	N1	N3	0
8	F2	Ng	N2	0
...	...	...	...	...
Ng dans la table désigne une adresse passerelle; N1, N2 et N3 désignent des adresses d'appareils de routage; F1 et F2 désignent des adresses d'appareils de terrain.				

9.3.4 Gestion du cycle de vie des paquets

Chaque paquet a un cycle de vie dans le réseau WIA-PA. Le cycle de vie est exprimé comme un temps maximal de survie. La couche NL enregistre l'heure de création des paquets à l'aide de marqueurs temporels. Le temps de survie est calculé en fonction de l'heure de création. Lorsque le temps de survie d'un paquet dépasse son cycle de vie, il convient de rejeter le paquet.

9.3.5 Rattachement à un réseau et départ d'un réseau pour un appareil

La couche NL du réseau WIA-PA prend en charge les processus de rattachement et de départ des appareils. Les processus de rattachement et de départ comprennent le rattachement et le départ d'appareils de terrain et d'appareils de routage.

9.3.6 Surveillance bout en bout des performances du réseau

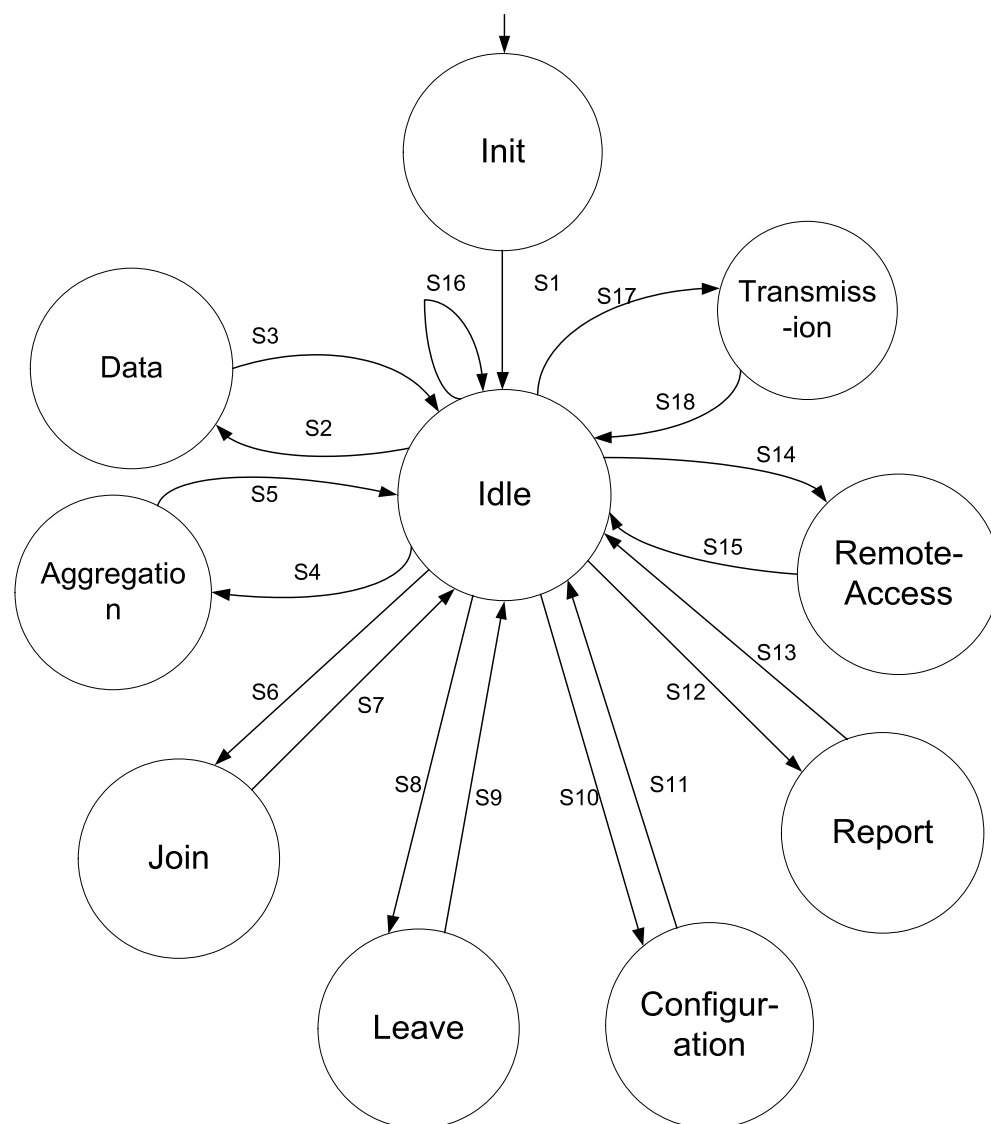
La couche réseau WIA-PA surveille chaque état de santé de chemin. L'entité NLME enregistre le nombre de nouvelles tentatives de chaque chemin pour estimer les défaillances de chemin. En cas de défaillance de chemin, l'entité NLME envoie une indication DMAP (voir 9.5.12).

9.3.7 Fragmentation et réassemblage

La fragmentation et le réassemblage sont gérés par la couche NL. Si la longueur d'une unité NPDU est plus grande que celle de la charge utile DLSL maximale, il convient de fragmenter l'unité NPDU au niveau de la NL de l'expéditeur. Lorsque les unités NPDU défragmentées atteignent le destinataire, elles sont réassemblées au niveau de la NL. Voir 9.6.2 pour les détails du format de paquet.

9.3.8 Diagramme d'états de la couche réseau

Les transitions d'états de la NL sont indiquées à la Figure 40 et au Tableau 70.



IEC

Anglais	Français
Init	Init
Idle	Repos
Transmission	Emission
Remote-access	Accès à distance
Report	Rapport
Configuration	Configuration
Leave	Départ
Join	Rattachement
Aggregation	Agrégation
Data	Données

Figure 40 – Diagramme d'états de la couche réseau

Tableau 70 – Transitions d'états de la NL (1 de 4)

Numéro séquentiel #	Etat courant	Evénement ou condition	Actions	Prochain état
S1	Init		Initiation	Idle
S2	Idle	A partir de la DLSL: DLSL-DATA.confirm() ou DLSL-DATA.indication() & Packet type = 0 dans la NSDU; A partir de la sous-couche application (ASL): NLDE-DATA.request()		Data
S3	Data		A partir de la DLSL: invocation de NLDE-DATA.confirm() pour la sous-couche application (ASL) ou analyse de la NSDU et invocation de NLDE-DATA.indication() pour la NSDU; A partir de la sous-couche application (ASL): compression de la NPDU et invocation de DLDE-DATA.request(); Tous les messages ou paquets sont envoyés dans la file d'attente d'émission.	Idle
S4	Idle	A partir de la DLSL: DLSL-DATA.indication() & Packet type = 1 dans la NSDU; A partir du processus DMAP: NLME-AGO-SEND.request()		Aggregation
S5	Aggregation		A partir de la DLSL: analyse de la NSDU en fonction du format de paquets agrégés de la NL et invocation de NLME-DAG.indication() pour le DMAP; A partir du processus DMAP: compression de paquets agrégés de la NL; Tous les messages ou paquets sont envoyés dans la file d'attente d'émission relative.	Idle
S6	Idle	A partir de la DLSL: DLSL-DATA.indication() & Packet type = 2 et Command ID = 0, 1 dans la NSDU; A partir du processus DMAP: NLME-JOIN.request/response()		Join
S7	Join		A partir de la DLSL: analyse de la NSDU en fonction du format de paquet de demande de rattachement de la NL si Command ID = 0 ou format de paquet de réponse de rattachement si Command ID = 1 et invocation de NLME-JOIN.indication() / NLME-JOIN.confirm() pour le DMAP; A partir du processus DMAP: compression de paquets de réponse de rattachement de la NL; Tous les messages ou paquets sont envoyés dans la file d'attente d'émission relative.	Idle

Tableau 70 (2 de 4)

Numéro séquen- tiel #	Etat courant	Événement ou condition	Actions	Prochain état
S8	Idle	A partir de la DLSL: DLSL-DATA.indication() & Packet type = 2 et Command ID = 3, 4 dans la NSDU; A partir du processus DMAP: NLME- LEAVE. request/response ()		Leave
S9	Leave		A partir de la DLSL: analyse de la NSDU en fonction du format de paquet de demande de départ de la NL si Command ID = 3 ou format de paquet de réponse de départ si Command ID = 4 et invocation de NLME-LEAVE.indication()/NLME-LEAVE.confirm() pour le DMAP; A partir du processus DMAP: compression de paquets de réponse de départ de la NL; Tous les messages ou paquets sont envoyés dans la file d'attente d'émission relative.	Idle
S10	Idle	A partir de la DLSL: DLSL-DATA.indication() & Packet type = 2 et Command ID = 8-25 dans la NSDU; A partir du processus DMAP: NLME-ADD/UPDATE/DELETE_ROUTE.request/response () ou NLME-ADD/UPDATE/RELEASE-LINK/SFR. request/response()		Configuration
S11	Configuration		A partir de la DLSL: analyse de la NSDU en fonction du format de paquet de demande d'itinéraire/de liaison/d'ajout de supertrame/de mise à jour/de suppression/de demande de libération/de réponse de la NL si Command ID = 8-25 et invocation de NLME-ADD/UPDATE/DELETE_ROUTE.indication() ou NLME-ADD/UPDATE/RELEASE-LINK/SFR.indication() pour le DMAP; A partir du processus DMAP: compression des paquets d'itinéraire/de liaison/d'ajout de supertrame/de mise à jour/de suppression/de réponse de libération de la NL; Tous les messages ou paquets sont envoyés dans la file d'attente d'émission relative.	Idle
S12	Idle	A partir de la DLSL: DLSL-COMM-STATUS.confirm() ou DLSL-DATA.indication() & Packet type = 2 et Command ID = 2, 5-7, 26-28; A partir du processus DMAP: NLME-RPT-CLRMEM.response()		Report

Tableau 70 (3 de 4)

Numéro séquentiel #	Etat courant	Evénement ou condition	Actions	Prochain état
S13	Report		A partir de la DLSL: invocation de NLME-COMM-STATUS.confirm () pour le DMAP. si Command ID = 2, analyse de la NSDU en fonction du format de paquet de demande de rapport sur l'état de communication de la NL et invocation de NLME-COMM-STATUS.indication(); si Command ID = 5, 6, analyse de la NSDU en fonction du format de paquet de demande/réponse du rapport sur l'élément de groupe de la NL et invocation de NLME-RPT-CLRMEM.indication/confirm () pour le DMAP; si Command ID = 7; analyse de la NSDU en fonction du format de paquets de demande de rapport sur les informations de voisins de la NL et invocation de NLME-NEIGHBOUR-INFO.indication() pour le DMAP; si Command ID = 26; analyse de la NSDU en fonction du format de paquets de demande de rapport sur la condition d'appareil de la NL et invocation de NLME-DEVICE-STATUS.indication() pour le DMAP; si Command ID = 27, analyse de la NSDU en fonction du format de paquets de demande de rapport sur la condition de canal de la NL et invocation de NLME-CHANNEL-CONDITION.indication() pour le DMAP; si Command ID = 28, analyse de la NSDU en fonction du format de paquets de demande de rapport sur la défaillance des chemins de la NL et invocation de NLME-PATH_FAILURE.indication() pour le DMAP; A partir du processus DMAP: compression de paquets de réponse de rapport sur l'élément de groupe de la NL; Tous les messages ou paquets sont envoyés dans la file d'attente d'émission relative.	Idle
S14	Idle	A partir de la DLSL: DLSL-DATA.indication() & Packet type = 2 et Command ID =29-32; A partir du processus DMAP: NLME-INFO_GET.response() ou NLME-INFO_SET.response()		Remote Access

Tableau 70 (4 de 4)

Numéro séquentiel #	Etat courant	Evénement ou condition	Actions	Prochain état
S15	Remote Access		A partir de la DLSL: si Command ID = 29, 30, analyse de la NSDU en fonction du format de paquets de demande/réponse d'obtention d'attribut de la NL et invocation de NLME-INFO_GET.indication() / NLME-INFO_GET.confirm pour le DMAP; si Command ID = 31, 32, analyse de la NSDU en fonction du format de paquets de demande/réponse d'établissement d'attribut de la NL et invocation de NLME-INFO_SET.indication() / NLME-INFO_SET.confirm pour le DMAP; A partir du processus DMAP: compression de paquets de réponse d'obtention/établissement d'attribut de la NL; Tous les messages ou paquets sont envoyés dans la file d'attente d'émission relative.	Repos
S16	Idle	A partir de la DLSL: DLSL-DATA.indication() & Packet type = 2 et Command ID > 32 ou aucun paquet reçu	Rejet des NSDU relatives	Idle
S17	Idle	La file d'attente n'est pas vide.		Transmission
S18	Transmission	La transmission est terminée		Idle

Les états dans le diagramme d'états de la NL sont spécifiés ci-après.

a) Etat Idle (repos)

Les transitions suivantes peuvent survenir pendant l'état Idle (repos):

- lorsque la DLSL invoque la primitive DLDE-DATA.indication, la couche réseau (NL) entre dans l'état Receive (réception);
- lorsque la sous-couche application (ASL) invoque la primitive NLDE-DATA.request, la couche réseau (NL) entre dans l'état Transmit (émission).

b) Etat Transmit (émission)

Dans l'état Transmit (émission), si la couche NL reçoit la primitive NLDE-DATA.confirm, elle entre dans l'état Idle (repos).

c) Etat Receive (réception)

Dans l'état Receive (réception), la NL entre dans l'état Idle (repos) après que la NL a émis la primitive NLDE-DATA.indication à la couche supérieure.

Voir 9.4 pour les services NLdata, par exemple NLDE-DATA; voir 9.5 pour les services de gestion NL, par exemple NLME-; voir 9.6.1 pour le type de paquet et 9.6.4 pour l'ID de commande.

Les états dans le diagramme d'états de la NL sont spécifiés ci-après.

a) Etat Idle (repos)

Après qu'un appareil déclenche la NL, la NL se met dans l'état Idle (repos). Les transitions suivantes peuvent survenir pendant que la sous-couche DLSL est dans l'état Idle (repos):

b) Lorsqu'une trame DLSL, ASL, ou DMAP arrive, la NL traite la NSDU.

Les paquets qu'un appareil peut recevoir englobent les paquets dont les adresses de destination finale sont celles de cet appareil. Les fonctions de l'état Idle (repos) sont de recevoir et traiter le paquet et traiter les primitives DMAP, ASL et DLSL.

Les transitions suivantes peuvent survenir pendant que la NL est dans l'état Receive (réception):

- Si un paquet de données est reçu de la DLSL ou si la primitive NLDE-DATA.request() est reçue de la sous-couche application (ASL), la NL se met à l'état Data (données).
 - Si un paquet agrégé est reçu de la DLSL ou si la primitive NLME-AGO-SEND.request() est reçue du DMAP, la NL se met à l'état Aggregation (agrégation).
 - Si un paquet de demande de rattachement ou de commande de réponse est reçu de la DLSL ou si la primitive NLME-JOIN.request/response () est reçue du DMAP, la NL se met à l'état Join (rattachement).
 - Si un paquet de demande de départ ou de commande de réponse est reçu de la DLSL ou si la primitive NLME- LEAVE. request/response () est reçue du DMAP, la NL se met à l'état Leave (départ).
 - Si un paquet de commande identifié de 8 à 25 est reçu de la DLSL ou si les primitives NLME-ADD/UPDATE/DELETE_ROUTE.request/response() ou NLME-ADD/UPDATE/RELEASE-LINK/SFR. request/response() sont reçues du DMAP, la NL se met à l'état Configuration (configuration).
 - Si un paquet de commande identifié par 2, 5-7, 26-28 est reçu de la DLSL ou si la primitive NLME-RPT-CLRMEM.response() est reçue du DMAP, la NL se met à l'état Report (rapport).
 - Si un paquet de commande d'obtention ou d'établissement d'attribut identifié de 29 à 32 est reçu de la DLSL ou si la primitive NLME-INFO_GET.response() /NLME-INFO_SET.response() est reçue du DMAP, la NL se met à l'état Remote Access (accès à distance).
 - Si aucun paquet ou aucune primitive n'est reçu(e) ou si un identificateur de paquets de commande supérieur à 32 est reçu de la DLSL, la NL entre dans l'état Idle (repos).
- c) Lorsque la file d'attente de transmission n'est pas vide, la NL se met à l'état Transmission (émission).
- d) Etat Data (données)
- Cet état gère la procédure de traitement des données d'un appareil. Si des données sont reçues d'une DLSL ou si une demande de données ASL est reçue, la NL passe à l'état Data (données).
- e) Etat Aggregation (agrégation)
- Cet état gère les procédures d'agrégation et de désagrégation de données/paquets.
- f) Etat Join (rattachement)
- Cet état gère la procédure de rattachement d'un appareil.
- g) Etat Leave (départ)
- Cet état gère la procédure de départ d'un appareil.
- h) Etat Configuration (configuration)
- Cet état gère les procédures d'affectation de ressources, qui comprennent l'ajout/la mise à jour/la suppression ou la libération d'un itinéraire, d'une liaison ou d'une supertrame.
- i) Etat Report (rapport)
- Cet état gère les procédures de rapport, qui incluent les rapports sur l'élément de groupe, d'informations de voisins, de conditions d'appareil, de conditions de canaux et de défaillance des chemins.
- j) Etat Remote access (accès à distance)
- Cet état gère les procédures d'accès d'attribut à distance, notamment l'obtention et l'établissement d'attribut.
- k) Etat Transmission (émission)

Cet état gère les procédures de transmission de données ou de paquets. Si la file d'attente de transmission n'est pas vide, la NL se met à l'état Transmission (émission).

9.4 Services de données de la couche réseau

9.4.1 Généralités

Le point d'accès NLDE-SAP est utilisé par la sous-couche ASL pour recevoir et émettre des données. Les primitives prises en charge par les services de données de la NL comprennent NLDE-DATA.request, NLDE-DATA.confirm et NLDE-DATA.indication.

9.4.2 NLDE-DATA.request

L'entité NLDE reçoit la charge utile de la sous-couche application (ASL) par le biais de NLDE-DATA.request et l'ajoute à la file d'attente de messages de la couche NL.

La sémantique de NLDE-DATA.request est décrite comme suit:

```
NLDE-DATA.request (
    VcrID,
    SrcAddr,
    Priority,
    PayloadLength,
    Payload,
    PayloadHandle
)
```

Le Tableau 71 spécifie les paramètres pour NLDE-DATA.request.

Tableau 71 – Paramètres de NLDE-DATA.request

Nom	Type de données	Plage valide	Description
VcrID	Unsigned16	0 à 65 535	Identificateur de la VCR
SrcAddr	Unsigned16	0 à 65 535 (adresse monodiffusion)	Adresse courte 16 bits de la source d'unités NSDU
Priorité	Unsigned8	0 à 15	Priorité de cette NSDU
PayloadLength	Unsigned16	0 à 65 535	Longueur de la NSDU à émettre
Payload (charge utile)	Octetstring		NSDU
PayloadHandle	Unsigned8	0 à 255	Descripteur associé à la NSDU à émettre

9.4.3 NLDE-DATA.confirm

La primitive NLDE-DATA.confirm retourne les résultats de NLDE-DATA.request.

La sémantique de NLDE-DATA.confirm est décrite comme suit:

```
NLDE-DATA.confirm (
    PayloadHandle,
    Statut
)
```

Le Tableau 72 spécifie les paramètres pour NLDE-DATA.confirm.

Tableau 72 – Paramètres de NLDE-DATA.confirm

Nom	Type de données	Plage valide	Description
PayloadHandle	Unsigned8	0 à 255	Gestion de la NSDU, qui est utilisée pour indiquer la charge utile de la NL
Statut	Unsigned8	0 à 255	Résultat de NLDE-DATA.request: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.4.4 NLDE-DATA.indication

La primitive NLDE-DATA.indication informe la sous-couche ASL lorsque la NL reçoit un paquet.

La sémantique de NLDE-DATA.indication est décrite comme suit:

```
NLDE-DATA.indication (
    SrcAddr,
    Priority,
    NSDULength,
    NSDU
)
```

Le Tableau 73 spécifie les paramètres pour NLDE-DATA.indication.

Tableau 73 – Paramètres de NLDE-DATA.indication

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535 (adresse de monodiffusion)	Adresse courte 16 bits de la source d'unités NSDU
Priorité	Unsigned8	0 à 15	Priorité de cette NSDU
NSDULength	Unsigned16	0 à 65 535	Longueur de la NSDU
NSDU	octet		Données de la NSDU

9.4.5 Séquence temporelle des services de données de la NL

La Figure 41 montre les procédures de base de l'envoi et de la réception de paquets. La primitive NLDE-DATA.request est générée par une entité de données de sous-couche application (ASLDE) locale lorsqu'une unité de données de protocole de sous-couche application (ASLPDU) doit être transférée à une entité NLDE homologue. A la réception d'une primitive NLDE-DATA.request, l'entité NLDE commence à émettre la NPDU.

La primitive NLDE-DATA.confirm est générée par l'entité NLDE d'un appareil source en réponse à la primitive NLDE-DATA.request. La primitive NLDE-DATA.confirm renvoie un état indiquant le résultat de l'émission.

La primitive NLDE-DATA.indication est générée par l'entité NLDE d'un appareil de destination et envoyée à l'entité ASLDE à la réception d'un paquet de données au niveau de l'entité NLDE locale.

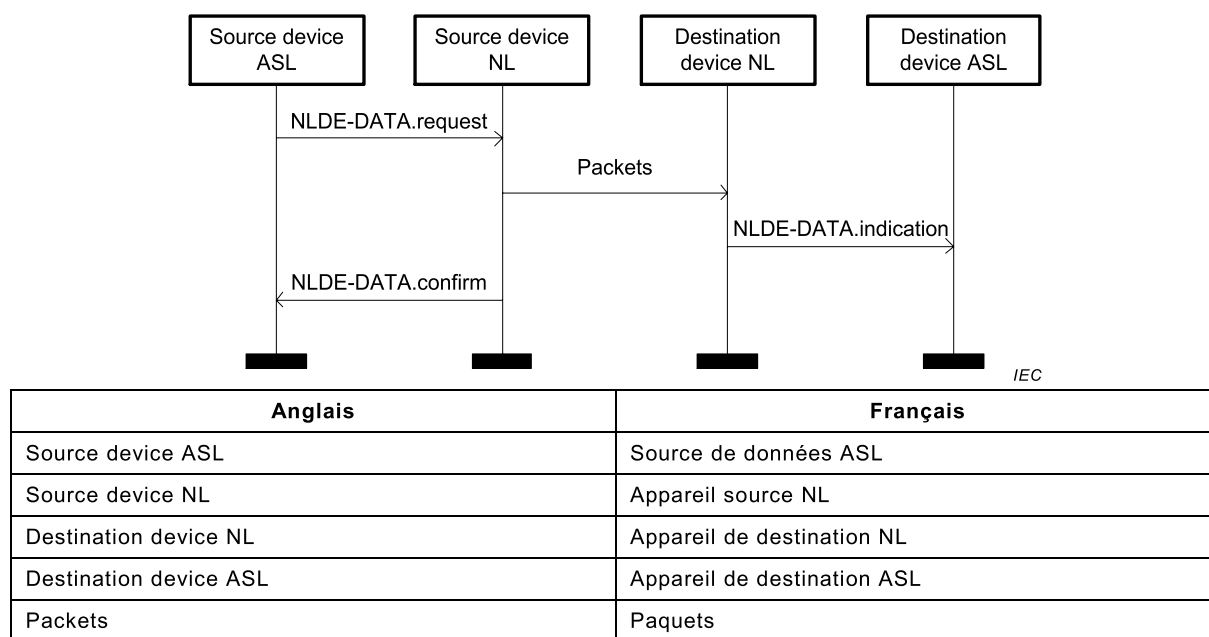


Figure 41 – Séquence temporelle des services de données de la NL

9.5 Services de gestion de la NL

9.5.1 Généralités

Le processus DMAP utilise l'interface fournie par le point d'accès NLME-SAP pour configurer et commander le fonctionnement de la couche réseau (NL).

9.5.2 Services de rapport sur l'état de communication du réseau

9.5.2.1 NLME-COMM-STATUS.request

La sémantique de NLME-COMM-STATUS.request est décrite comme suit:

```
NLME-COMM-STATUS.request (
    ProxyAddr,
    PhyAddr,
    DeviceType,
    Statut
)
```

Le Tableau 74 spécifie les paramètres pour NLME-COMM-STATUS.request.

Tableau 74 – Paramètres de NLLME-COMM-STATUS.indication

Nom	Type de données	Plage valide	Description
ProxyAddr	Unsigned16	0 à 65 535	Adresse de l'appareil de routage choisie par le nouvel appareil (adresse de monodiffusion)
PhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse physique 64 bits du nouvel appareil
DeviceType (Type d'appareil)	Unsigned8	0 à 255	Type du nouvel appareil: 0 = Appareil de passerelle 1 = Appareil de routage 2 = Appareil de terrain 3 = Appareil tenu à la main Les autres valeurs sont réservées.
Statut	Unsigned8	0 à 255	Résultats du processus de rattachement d'un nouvel appareil: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.2.2 NLME-COMM-STATUS.indication

La sémantique de NLME-COMM-STATUS.indication est décrite comme suit:

NLME-COMM-STATUS.indication (

ProxyAddr,
PhyAddr,
DeviceType,
Statut
)

Le Tableau 75 spécifie les paramètres pour NLME-COMM-STATUS.indication.

Tableau 75 – Paramètres de NLME-COMM-STATUS.indication

Nom	Type de données	Plage valide	Description
ProxyAddr	Unsigned16	0 à 65 535	Adresse de l'appareil de routage choisie par le nouvel appareil (adresse de monodiffusion)
PhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse physique 64 bits du nouvel appareil
DeviceType (Type d'appareil)	Unsigned8	0 à 255	Type du nouvel appareil: 0 = Appareil de passerelle 1 = Appareil de routage 2 = Appareil de terrain 3 = Appareil tenu à la main Les autres valeurs sont réservées.
Statut	Unsigned8	0 à 255	Résultats du processus de rattachement d'un nouvel appareil: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

A la réception d'un paquet de demande d'état de communication de la NL, la NL de l'appareil de passerelle invoquera la primitive NLME-COMM-STATUS.indication et informera le DMAP.

9.5.2.3 NLME-COMM-STATUS.confirm

La sémantique de NLME-COMM-STATUS.confirm est décrite comme suit:

```
NLME-COMM-STATUS.confirm (
    PhyAddr,
    Statut
)
```

Le Tableau 76 spécifie les paramètres pour NLME-COMM-STATUS.confirm.

Tableau 76 – Paramètres de NLME-COMM-STATUS.confirm

Nom	Type de données	Plage valide	Description
PhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse physique 64 bits du nouvel appareil
Statut	Unsigned8	0 à 255	Résultat d'exécution de la demande: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

NLME-COMM-STATUS.confirm est générée par la NL en réponse à NLME-COMM-STATUS.request. NLME-COMM-STATUS.confirm retourne à un état soit SUCCESS (succès) indiquant que l'émission demandée a réussi, soit FAILURE (échec) indiquant que l'émission demandée a échoué.

9.5.3 Services de rattachement au réseau

9.5.3.1 NLME-JOIN.request

La sémantique de NLME-JOIN.request est décrite comme suit:

```
NLME-JOIN.request (
    ProxyAddr,
    PhyAddr,
    SecMaterial,
    DeviceType (Type d'appareil)
)
```

Le Tableau 77 spécifie les paramètres pour NLME-JOIN.request.

Tableau 77 – Paramètres de NLME-JOIN.request

Nom	Type de données	Plage valide	Description
ProxyAddr	Unsigned16	0 à 65 535	Adresse de l'appareil de routage choisie par le nouvel appareil (adresse de monodiffusion)
PhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse physique 64 bits du nouvel appareil
SecMaterial	Unsigned32	0 à ($2^{32}-1$)	Informations sur l'identité d'un appareil
DeviceType (Type d'appareil)	Unsigned8	0 à 255	Type du nouvel appareil: 0 = Appareil de passerelle 1 = Appareil de routage 2 = Appareil de terrain 3 = Appareil tenu à la main Les autres valeurs sont réservées.

9.5.3.2 NLME-JOIN.indication

La sémantique de NLME-JOIN.indication est décrite comme suit:

```
NLME-JOIN.indication (
    ProxyAddr,
    PhyAddr,
    SecMaterial,
    DeviceType (Type d'appareil)
)
```


Le Tableau 78 spécifie les paramètres pour NLME-JOIN.indication.

Tableau 78 – Paramètres de NLME-JOIN.indication

Nom	Type de données	Plage valide	Description
ProxyAddr	Unsigned16	0 à 65 535	Adresse courte de l'appareil de routage qui génère la demande de rattachement de NL
PhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse physique de l'appareil
SecMaterial	Unsigned32	0 à ($2^{32}-1$)	Informations sur l'identité d'un appareil
DeviceType (Type d'appareil)	Unsigned8	0 à 255	Type du nouvel appareil: 0 = Appareil de passerelle 1 = Appareil de routage 2 = Appareil de terrain 3 = Appareil tenu à la main Les autres valeurs sont réservées.

A la réception d'un paquet de demande de rattachement de la NL, la NL de l'appareil de passerelle invoquera la primitive NLME-JOIN.indication et informera le DMAP.

9.5.3.3 NLME-JOIN.response

La sémantique de NLME-JOIN.response est décrite comme suit:

NLME-JOIN.response (

ProxyAddr,
PhyAddr,
ShortAddr,
Statut
)

Le Tableau 79 spécifie les paramètres pour NLME-JOIN.response.

Tableau 79 – Paramètres de NLME-JOIN.response

Nom	Type de données	Plage valide	Description
ProxyAddr	Unsigned16	0 à 65 535	Adresse courte de l'appareil de routage qui génère la demande de rattachement de NL
PhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse physique du nouvel appareil
ShortAddr	Unsigned16	0 à 65 535	Adresse réseau allouée (Adresse de monodiffusion) au nouvel appareil
Statut	Unsigned8	0 à 255	Résultat d'exécution de la demande: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

Le DMAP invoque NLME-JOIN.response pour assigner une adresse réseau au nouvel appareil.

9.5.3.4 NLME-JOIN.confirm

La sémantique de NLME-JOIN.confirm est décrite comme suit:

NLME-JOIN.confirm (ShortAddr,
 Statut
)

Le Tableau 80 spécifie les paramètres pour NLME-JOIN.confirm.

Tableau 80 – Paramètres de NLME-JOIN.confirm

Nom	Type de données	Plage valide	Description
ShortAddr	Unsigned16	0 à 65 535	Adresse réseau (adresse de monodiffusion)
Statut	Unsigned8	0 à 255	Résultat d'exécution de la demande: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

NLME-JOIN.confirm est générée par la NL en réponse à NLME-JOIN.request. NLME-JOIN.confirm retourne à un état soit SUCCESS (succès) indiquant que l'émission demandée a réussi, soit FAILURE (échec) indiquant que l'émission demandée a échoué.

9.5.3.5 Séquence temporelle pour le rattachement d'appareil

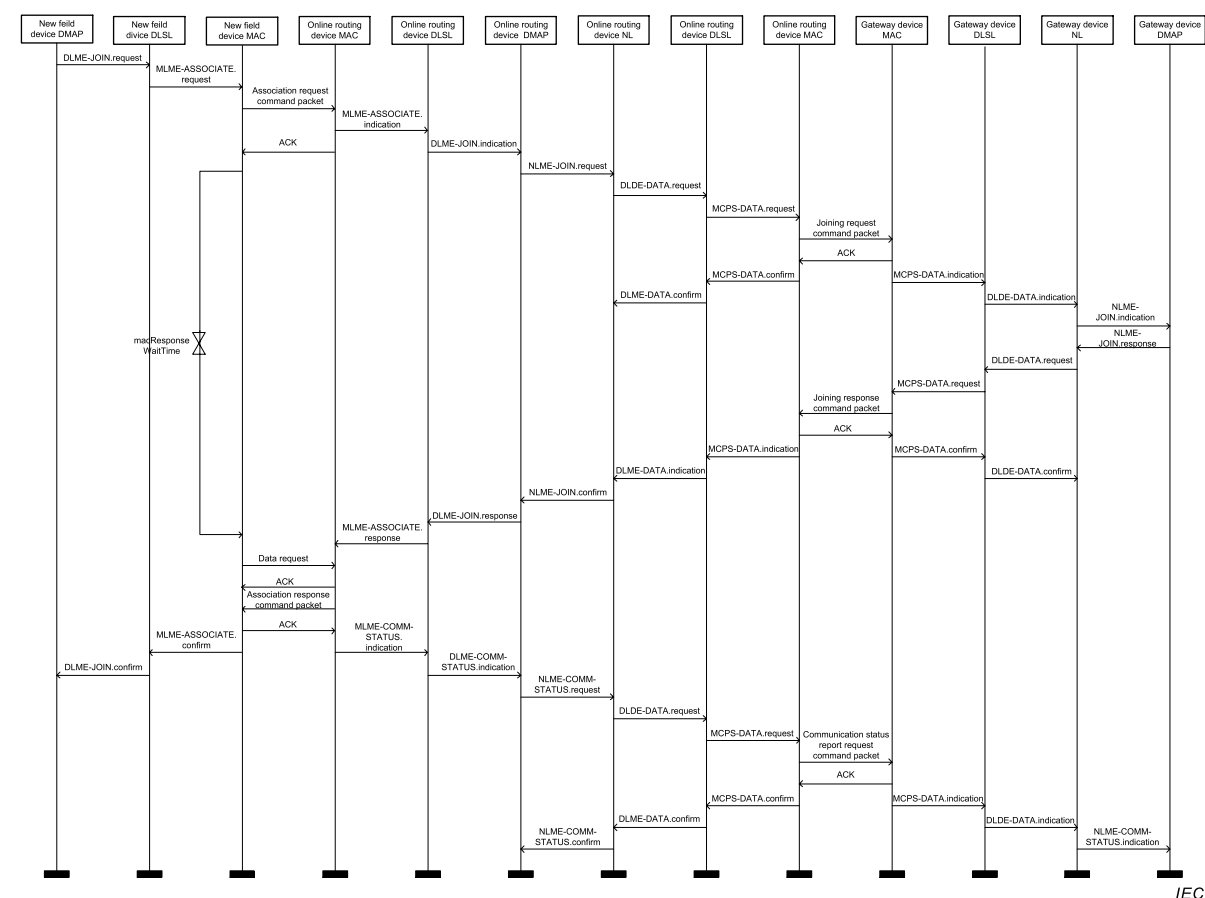
9.5.3.5.1 Séquence temporelle pour le rattachement d'appareil de terrain

Pour se rattacher au réseau en étoile, il convient qu'un appareil de terrain lance une demande de rattachement dans la couche MAC par le DMAP à l'appareil de routage ou à l'appareil de passerelle. Il convient qu'un appareil de terrain soit rattaché au réseau par le biais de l'appareil de passerelle ou d'un appareil de routage.

Lorsque l'appareil de passerelle reçoit une demande de rattachement d'un appareil de terrain, il convient qu'il indique le rattachement au NM puis renvoie une réponse de rattachement. Si le nouvel appareil de terrain reçoit la réponse d'association à la couche MAC de l'appareil de passerelle, il rejoint le réseau.

Lorsque l'appareil de routage reçoit une demande de rattachement issue d'un appareil de terrain, il convient qu'il produise une demande de rattachement de la NL et envoie cette demande à l'appareil de passerelle. Si le nouvel appareil de terrain reçoit la réponse de rattachement, le processus de rattachement est terminé.

La Figure 42 représente un exemple de processus de rattachement d'un appareil de terrain dans le réseau hiérarchique qui est la combinaison de la configuration en étoile et de la configuration maillée.



Anglais	Français
New field device DMAP	DMAP du nouvel appareil de terrain
New field device DLSL	DLSL du nouvel appareil de terrain
New field device MAC	MAC du nouvel appareil de terrain
Online routing device MAC	MAC de l'appareil de routage en ligne
Online routing device DLSL	DLSL de l'appareil de routage en ligne
Online routing device DMAP	DMAP de l'appareil de routage en ligne
Online routing device NL	NL de l'appareil de routage en ligne
Gateway device	Appareil de passerelle
Association request command packet	Paquet de commande de demande d'association
Joining request command packet	Paquet de commande de demande de rattachement
Joining response command packet	Paquet de commande de réponse de rattachement
Data request	Demande de données
ACK	ACK
Association response command packet	Paquet de commande de réponse d'association
Communication status report request command packet	Paquet de commande de demande de rapport sur l'état des communications

Figure 42 – Séquence temporelle pour le rattachement d'appareil de terrain via un appareil de routage

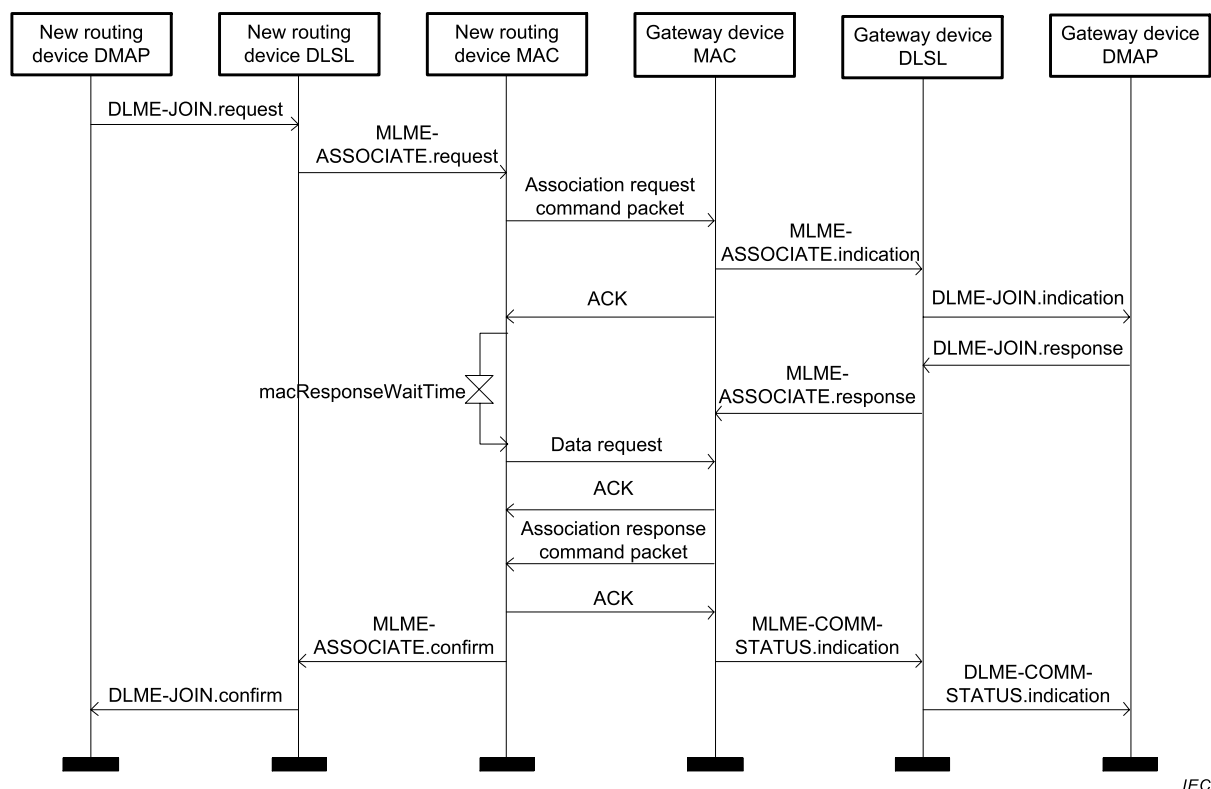
9.5.3.5.2 Séquence temporelle pour le rattachement d'appareil de routage

Si un appareil de routage souhaite se rattacher au réseau maillé, il convient qu'il envoie une demande de rattachement à l'appareil de passerelle, et la demande inclut l'adresse longue de cet appareil de routage. Les processus de rattachement pour les appareils de routage sont de

deux sortes: rattachement en un saut et rattachement multisaut. Si le nouvel appareil de routage envoie une demande de rattachement à l'appareil de passerelle, le processus de rattachement en un saut est utilisé; si le nouvel appareil de routage se rattache au réseau maillé via un autre appareil de routage existant, le processus de rattachement multisaut est utilisé.

L'appareil de passerelle reçoit la demande de rattachement et informe le NM. Il convient que le NM retourne une réponse. Si le nouvel appareil de routage reçoit la réponse, son processus de rattachement est terminé.

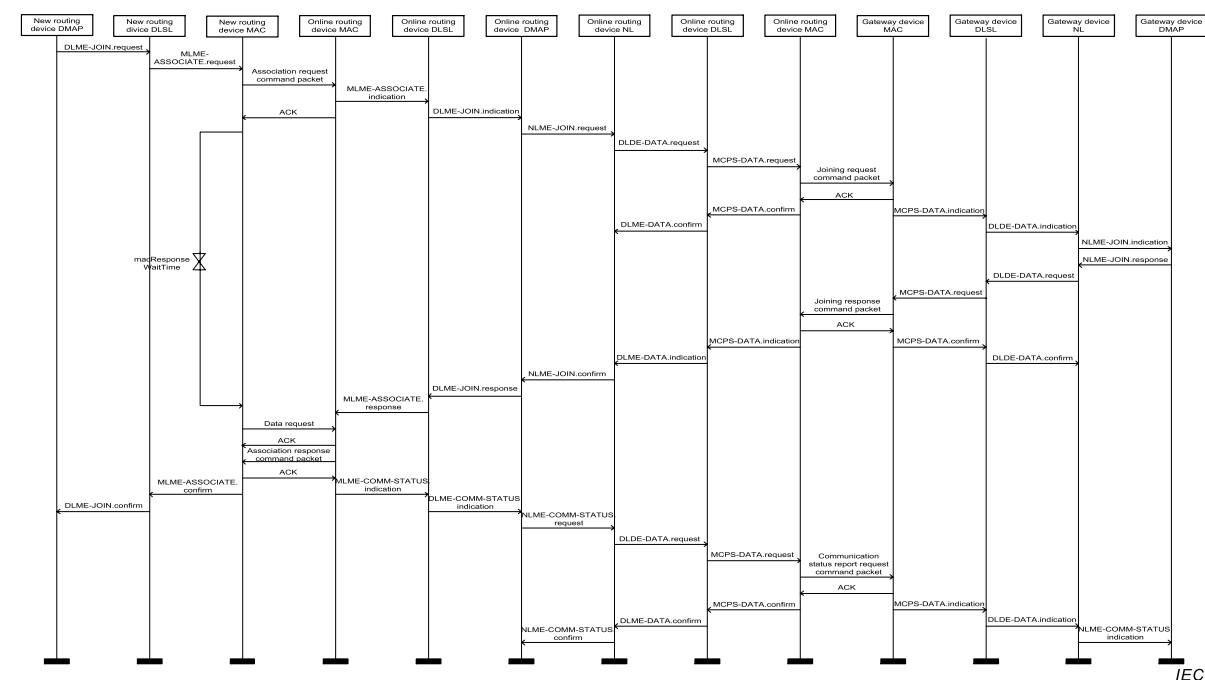
La Figure 43 et la Figure 44 représentent des exemples du processus de rattachement des appareils de routage.



Anglais	Français
New routing device DMAP	DMAP du nouvel appareil de routage
New routing device DLSL	DLSL du nouvel appareil de routage
New routing device MAC	MAC du nouvel appareil de routage
Gateway device MAC	MAC de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device DMAP	DMAP de l'appareil passerelle
Association request command packet	Paquet de commande de demande d'association
Data request	Demande de données
ACK	ACK
Association response command packet	Paquet de commande de réponse d'association

Figure 43 – Processus de rattachement en un saut d'un appareil de routage

Se référer à l'IEEE 802.15.4-2011 (Figure 17 et Figure 18) pour le diagramme de séquence de message détaillé entre les entités MAC homologues.



Anglais	Français
New routing device DMAP	DMAP du nouvel appareil de routage
New routing device DLSL	DLSL du nouvel appareil de routage
New routing device MAC	MAC du nouvel appareil de routage
Online routing device MAC	MAC de l'appareil de routage en ligne
Online routing device DLSL	DLSL de l'appareil de routage en ligne
Online routing device DMAP	DMAP de l'appareil de routage en ligne
Online routing device NL	NL de l'appareil de routage en ligne
Gateway device MAC	MAC de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DMAP	DMAP de l'appareil passerelle
Association request command packet	Paquet de commande de demande d'association
Joining request command packet	Paquet de commande de demande de rattachement
Joining response command packet	Paquet de commande de réponse de rattachement
Data request	Demande de données
ACK	ACK
Association response command packet	Paquet de commande de réponse d'association
Communication status report request command packet	Paquet de commande de demande de rapport sur l'état des communications

Figure 44 – Processus de rattachement multisaut de l'appareil de routage

Avant de se rattacher au réseau, les appareils de terrain et les appareils de routage règlent DeviceState (voir Tableau 20) sur 0 pour indiquer que les appareils ne se sont pas rattachés au réseau. Si les nouveaux appareils ont envoyé la demande de rattachement mais qu'ils n'ont pas reçu la réponse de rattachement, ils règlent DeviceState sur 1 pour indiquer que les appareils rejoignent le réseau. Si les nouveaux appareils ont envoyé la demande de rattachement et qu'ils ont reçu la réponse de rattachement, ils règlent DeviceState sur 3 pour indiquer que les appareils ont rejoint le réseau. Si le processus de rattachement nécessite une authentification de sécurité, les appareils règlent DeviceState sur 3 durant le processus d'authentification. Pour plus d'informations sur l'attribut DeviceState, voir le Tableau 20.

9.5.4 Services de départ de réseau

9.5.4.1 NLME-LEAVE.request

La sémantique de NLME-LEAVE.request est décrite comme suit:

```
NLME-LEAVE.request (
    SrcAddr,
    DstAddr,
    LeavingReason
)
```

Le Tableau 81 spécifie les paramètres pour NLME-LEAVE.request.

Tableau 81 – Paramètres de NLME-LEAVE.request

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse de l'appareil auquel la réponse de départ doit être envoyée
LeavingReason	Unsigned8	0 à 255	1 = départ passif d'un appareil de routage ou d'un appareil de terrain 2 = départ actif d'un appareil de routage Les autres valeurs sont réservées.

Lorsqu'un appareil de routage souhaite quitter le réseau ou que l'appareil de passerelle souhaite qu'un appareil quitte le réseau, le DMAP invoque la primitive NLME-LEAVE.request et demande à sa couche réseau (NL) de démarrer le processus de départ.

9.5.4.2 NLME-LEAVE.indication

La sémantique de NLME-LEAVE.indication est décrite comme suit:

```
NLME-LEAVE.indication (
    DeviceAddr,
    LeavingReason
)
```

Le Tableau 82 spécifie les paramètres pour NLME-LEAVE.indication.

Tableau 82 – Paramètres de NLME-LEAVE.indication

Nom	Type de données	Plage valide	Description
DeviceAddr	Unsigned16	0 à 65 535	Adresse de l'appareil invoquant la demande de départ
LeavingReason	Unsigned8	0 à 255	1 = départ passif d'un appareil de routage ou d'un appareil de terrain 2 = départ actif d'un appareil de routage Les autres valeurs sont réservées.

A la réception d'un paquet de commande de demande de départ, la NL invoquera la primitive NLME-LEAVE.indication et informera le DMAP.

9.5.4.3 NLME-LEAVE.response

La sémantique de NLME-LEAVE.response est décrite comme suit:

```
NLME-LEAVE.response (
    DevAddr,
    Statut
)
```

Le Tableau 83 spécifie les paramètres pour NLME-LEAVE.response.

Tableau 83 – Paramètres de NLME-LEAVE.response

Nom	Type de données	Plage valide	Description
DevAddr	Unsigned16	0 à 65 535	Adresse de l'appareil qui a demandé le départ
Statut	Unsigned8	0 à 255	Résultat d'exécution de la demande: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

La primitive NLME-LEAVE.response est utilisée par le DMAP ou la NM pour signaler à l'appareil partant si la demande de départ a été acceptée ou non.

9.5.4.4 NLME-LEAVE.confirm

La sémantique de NLME-LEAVE.confirm est décrite comme suit:

```
NLME-LEAVE.confirm (
    DevAddr,
    Statut
)
```

Le Tableau 84 spécifie les paramètres pour NLME-LEAVE.confirm.

Tableau 84 – Paramètres de NLME-LEAVE.confirm

Nom	Type de données	Plage valide	Description
DevAddr	Unsigned16	0 à 65 535	Adresse de l'appareil qui a demandé le départ ou à qui l'appareil de passerelle a demandé de quitter le réseau
Statut	Unsigned8	0 à 255	Résultat d'exécution de la demande: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

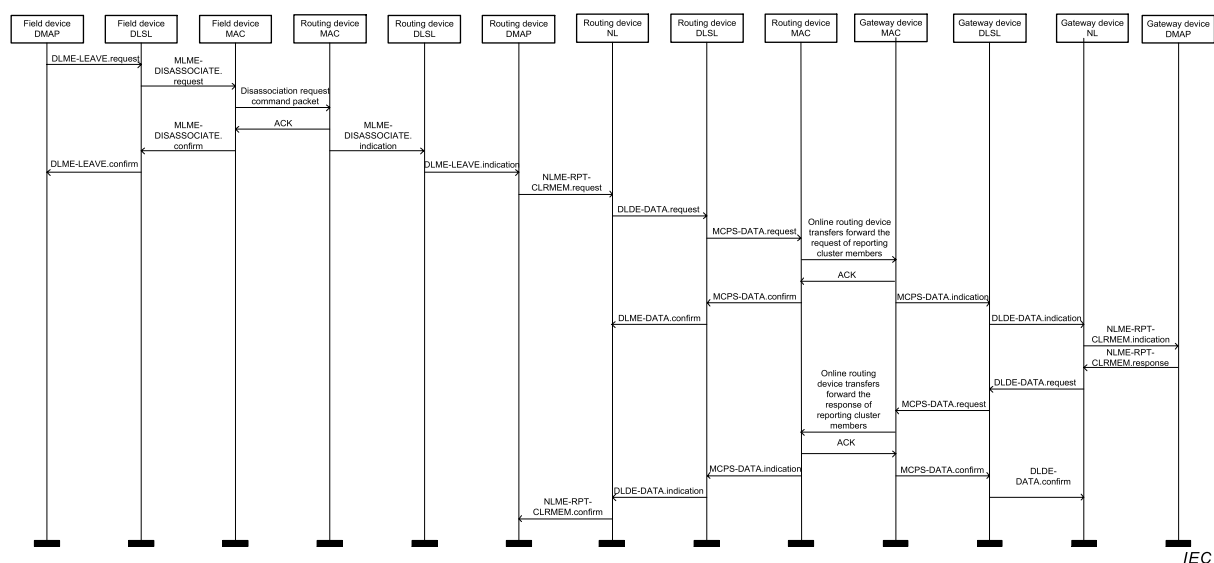
NLME-LEAVE.confirment générée par la NL en réponse à NLME-LEAVE.request. NLME-LEAVE.confirm retourne un état soit SUCCESS (succès) indiquant que la demande d'émettre a réussi, soit FAILURE (échec) indiquant que la demande d'émettre a échoué.

9.5.4.5 Séquence temporelle pour le départ d'appareil

9.5.4.5.1 Séquence temporelle pour le départ d'appareil de terrain

Les processus de départ des appareils de terrain comprennent les deux types suivants.

- a) Départ actif. Pour un appareil de terrain, le DMAP invoque DLME-LEAVE.request pour envoyer une demande de départ à l'appareil de routage ou à l'appareil de passerelle qui est sa tête de groupe. Après avoir reçu de l'appareil de terrain le paquet de commande de demande de départ, la NL de l'appareil de routage ou de l'appareil de passerelle informe le DMAP en émettant une DLME-LEAVE.indication. Si l'appareil de terrain quitte l'appareil de routage, l'appareil de routage envoie NLME-RPT-CLRMEM.request à l'appareil de passerelle. La Figure 45 représente la séquence temporelle pour le départ actif d'un appareil de terrain.

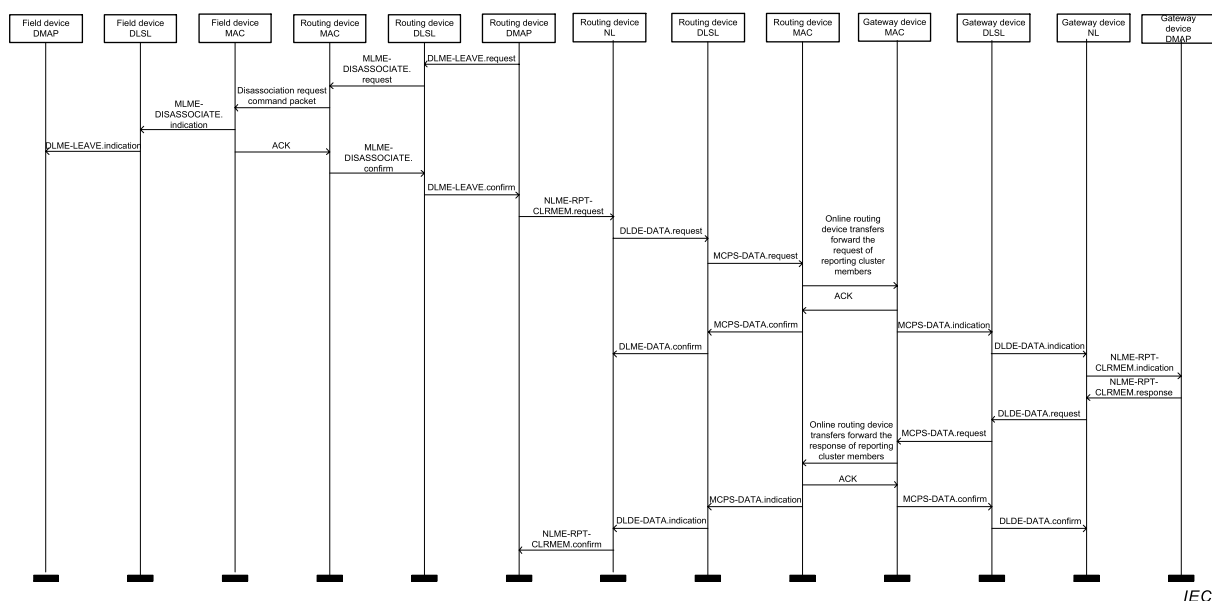


Anglais	Français
Field device DMAP	DMAP de l'appareil de terrain
Field device DLSL	DLSL de l'appareil de terrain
Field device MAC	MAC de l'appareil de terrain
Routing device MAC	MAC de l'appareil de routage
Routing device DLSL	DLSL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Gateway device MAC	MAC de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DMAP	DMAP de l'appareil passerelle
Disassociation request command packet	Paquet de commande de demande de dissociation
Online routing device transfers forward the request of reporting cluster members	L'appareil de routage en ligne retransmet la demande de rapport d'éléments de groupe

Figure 45 – Processus de départ actif d'un appareil de terrain (appareil de routage partant)

Se référer à l'IEEE 802.15.4-2011 (Figure 27) pour le diagramme de séquence de message détaillé entre les entités MAC homologues.

- b) **Départ passif.** Le DMAP d'un appareil de routage demande pour son appareil de terrain de quitter le réseau par la primitive DLME-LEAVE.request. Après avoir reçu cette demande, l'appareil de terrain retourne un acquittement (ACK). Si l'appareil de routage reçoit la primitive DLME-LEAVE.confirm, il envoie la demande de rapport sur l'élément de groupe à l'appareil de passerelle. La Figure 46 représente la séquence temporelle pour le départ passif d'un appareil de terrain.

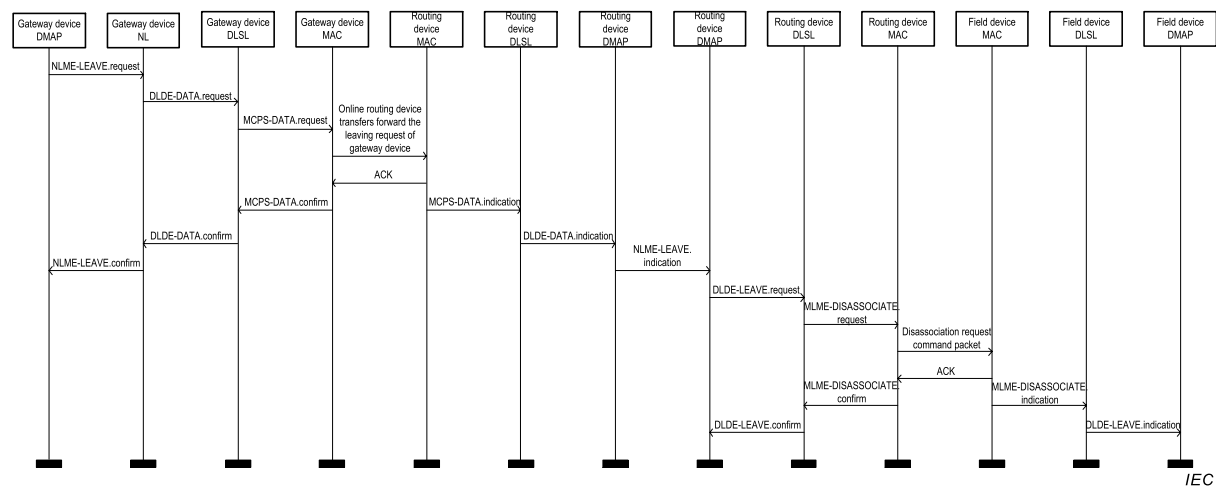


Anglais	Français
Field device DMAP	DMAP de l'appareil de terrain
Field device DLSL	DLSL de l'appareil de terrain
Field device MAC	MAC de l'appareil de terrain
Routing device MAC	MAC de l'appareil de routage
Routing device DLSL	DLSL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Gateway device MAC	MAC de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DMAP	DMAP de l'appareil passerelle
Disassociation request command packet	Paquet de commande de demande de dissociation
Online routing device transfers forward the request of reporting cluster members	L'appareil de routage en ligne retransmets la demande de rapport d'éléments de groupe

Figure 46 – Départ passif d'un appareil de terrain

Les appareils de routage se connectent tant au réseau maillé qu'au réseau en étoile. Par conséquent, il convient que l'appareil de routage informe de son départ tant l'appareil de passerelle que ses appareils de terrain.

Se référer à l'IEEE 802.15.4-2011, Figure 27 pour le diagramme de séquence de message détaillé entre les entités MAC homologues.



Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLDSL	DLDSL de l'appareil passerelle
Gateway device MAC	MAC de l'appareil passerelle
Routing device MAC	MAC de l'appareil de routage
Routing device DLDSL	DLDSL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Field device MAC	MAC de l'appareil de terrain
Field device DLDSL	DLDSL de l'appareil de terrain
Field device DMAP	DMAP de l'appareil de terrain
Online routing device transfers forward the leaving request of the gateway device	L'appareil de routage en ligne retransmet la demande de départ de l'appareil passerelle
Disassociation request command packet	Paquet de commande de demande de dissociation

Figure 48 – Processus de départ passif d'un appareil de routage

Se référer à l'IEEE 802.15.4-2011, Figure 20 pour le diagramme de séquence de message détaillé entre les entités MAC homologues.

9.5.5 Services de rapport sur l'élément de groupe

9.5.5.1 NLME-RPT-CLRMEM.request

La primitive NLME-RPT-CLRMEM.request est utilisée par les appareils de routage pour rapporter les informations des éléments de groupe à l'appareil de passerelle.

La sémantique de NLME-RPT-CLRMEM.request est décrite comme suit:

NLME-RPT-CLRMEM.request (

SrcAddr,
DstAddr,
ClrMemFlag,
ClrMemAddr

)

Le Tableau 85 spécifie les paramètres pour NLME-RPT-CLRMEM.request.

Tableau 85 – Paramètres de NLME-RPT-CLRMEM.request

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse source
DstAddr	Unsigned16	0 à 65 535	Adresse de destination
ClrMemFlag	Unsigned8	0 à 255	Fanion de la modification d'élément de groupe: 0 = Ajouter 1 = Supprimer Les autres valeurs sont réservées.
ClrMemAddr	Unsigned16	0 à 65 535	Adresse réseau de l'élément de groupe modifié

9.5.5.2 NLME-RPT-CLRMEM.confirm

La primitive NLME-RPT-CLRMEM.confirm est utilisée par la NL pour envoyer le résultat de NLME-RPT-CLRMEM.request au DMAP.

La sémantique de NLME-RPT-CLRMEM.confirm est décrite comme suit:

```
NLME-RPT-CLRMEM.confirm (
    Statut
)
```

Le Tableau 86 spécifie les paramètres pour NLME-RPT-CLRMEM.confirm.

Tableau 86 – Paramètres de NLME-RPT-CLRMEM.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultat du rapport sur l'élément de groupe: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.5.3 NLME-RPT-CLRMEM.indication

La primitive NLME-RPT-CLRMEM.indication est utilisée par la NL pour rapporter la réception réussie du paquet de demande de rapport sur l'élément de groupe.

La sémantique de NLME-RPT-CLRMEM.indication est décrite comme suit:

```
NLME-RPT-CLRMEM.indication (
    SrcAddr,
    ClrMemFlag,
    ClrMemAddr
)
```

Le Tableau 85 spécifie les paramètres pour NLME-RPT-CLRMEM.indication.

9.5.5.4 NLME-RPT-CLRMEM.response

La primitive NLME-RPT-CLRMEM.response est utilisée pour répondre à NLME-RPT-CLRMEM.indication.

La sémantique de NLME-RPT-CLRMEM.response est décrite comme suit:

NLME-RPT-CLRMEM.response (

DstAddr,

Statut

)

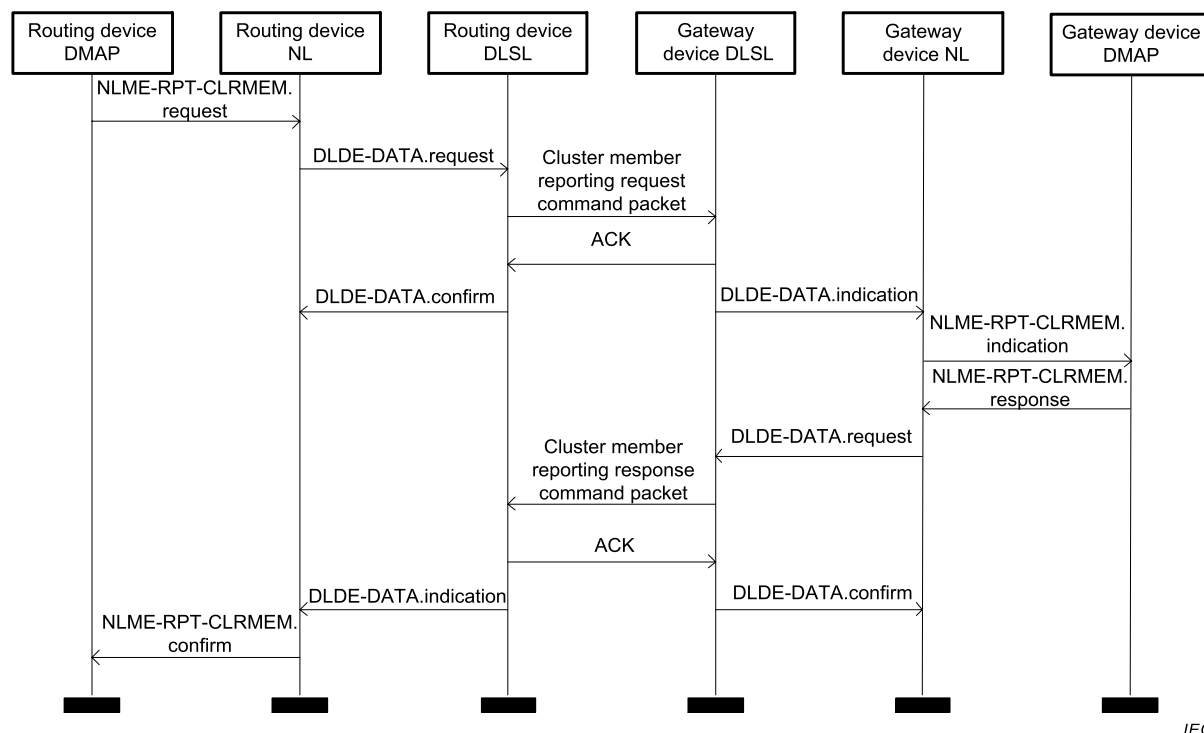
Le Tableau 87 spécifie les paramètres pour NLME-RPT-CLRMEM.response.

Tableau 87 – Paramètres de NLME-RPT-CLRMEM.response

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination
Statut	Unsigned8	0 à 255	Résultat retourné du rapport sur l'élément de groupe: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.5.5 Séquence temporelle pour la production de rapport sur l'élément de groupe

Le diagramme de séquence temporelle pour la production de rapport sur l'élément de groupe est représenté à la Figure 49.



IEC

Anglais	Français
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DLSL	DLSL de l'appareil de routage
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DMAP	DMAP de l'appareil passerelle
Cluster member reporting request command packet	Paquet de commande de demande pour la production de rapport d'élément de groupe
Cluster member reporting response command packet	Paquet de commande de réponse pour la production de rapport d'élément de groupe

Figure 49 – Processus de production de rapport sur l'élément de groupe

9.5.6 Services de rapport sur les informations de voisins

9.5.6.1 NLME-NEIGHBOUR-INFO.request

La primitive NLME-NEIGHBOUR-INFO.request est utilisée par un appareil de routage pour rapporter ses informations de voisins à un saut à l'appareil de passerelle. Cette utilisation de NLME-NEIGHBOUR-INFO.request est déclenchée uniquement lorsqu'un voisin se rattache au réseau WIA-PA ou le quitte. Le voisin proprement dit et son voisin de prochain saut vers l'appareil de passerelle (GW) rapporte les informations de voisins à l'appareil de passerelle (GW).

La sémantique de NLME-NEIGHBOUR-INFO.request est décrite comme suit:

```

NLME-NEIGHBOUR-INFO.request (
    SrcAddr,
    DstAddr,
    NeighbourCount,
    NeighbourStructure
)
    
```

Le Tableau 88 spécifie les paramètres pour NLME-NEIGHBOUR-INFO.request.

Tableau 88 – Paramètres de NLME-NEIGHBOUR-INFO.request

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse source de 16 bits
DstAddr	Unsigned16	0 à 65 535	Adresse de destination 16 bits
NeighbourCount	Unsigned8	0 à 255	Nombre de voisins
NeighbourStructure	Structure Neighbour_Struct (voir Tableau 18)		Informations des voisins

9.5.6.2 NLME-NEIGHBOUR-INFO.indication

NLME-NEIGHBOUR-INFO.indication est utilisée pour que la DLSL rapporte au DMAP le paquet de NLME-NEIGHBOUR-INFO.request.

La sémantique de NLME-NEIGHBOUR-INFO.indication est décrite comme suit:

NLME-NEIGHBOUR-INFO.indication (

SrcAddr,
NeighbourCount,
NeighbourStructure
)

Le Tableau 88 spécifie les paramètres pour NLME-NEIGHBOUR-INFO.indication.

9.5.6.3 NLME-NEIGHBOUR-INFO.confirm

NLME-NEIGHBOUR-INFO.confirm est utilisée pour rapporter l'envoi réussi des paquets de demande de rapport sur les informations des voisins.

La sémantique de NLME-NEIGHBOUR-INFO.confirm est décrite comme suit:

NLME-NEIGHBOUR-INFO.confirm (

Statut
)

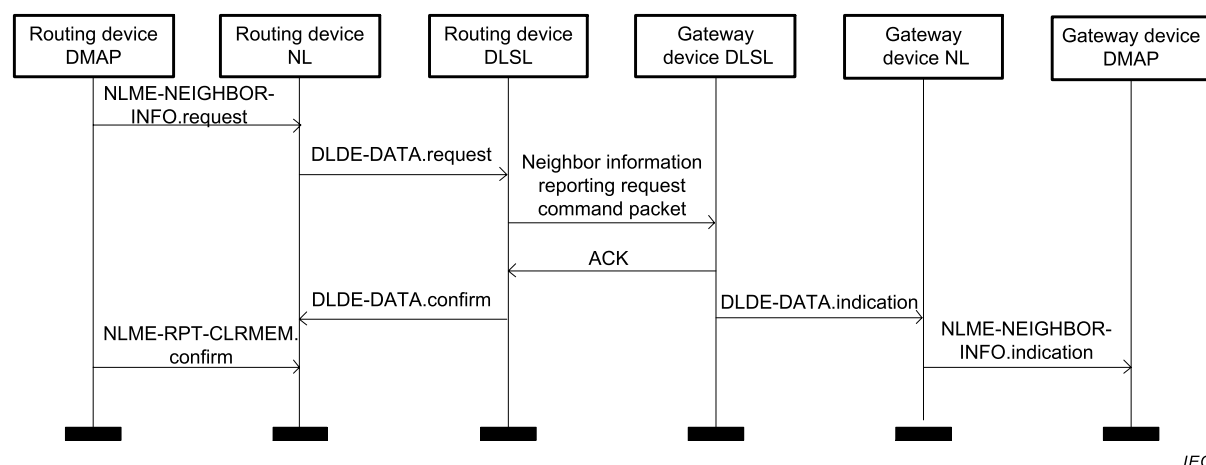
Le Tableau 89 spécifie les paramètres pour NLME-NEIGHBOUR-INFO.confirm.

Tableau 89 – Paramètres de NLME-NEIGHBOUR-INFO.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Production de rapport sur le résultat des informations de voisins: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.6.4 Séquence temporelle de production de rapport sur les informations de voisins

Le diagramme de séquence temporelle pour la production de rapport sur les informations de voisins est représenté à la Figure 50.



IEC

Anglais	Français
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DLSL	DLSL de l'appareil de routage
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DMAP	DMAP de l'appareil passerelle
Neighbour reporting request command packet	Paquet de commande de demande de rapport sur les voisins

Figure 50 – Processus de production de rapport sur les informations de voisins

9.5.7 Services d'allocation d'itinéraire

9.5.7.1 Services d'ajout d'itinéraire

9.5.7.1.1 NLME-ADD_ROUTE.request

La primitive NLME-ADD_ROUTE.request est utilisée pour ajouter un enregistrement à la table de routage d'un appareil de routage.

La sémantique de NLME-ADD_ROUTE.request est décrite comme suit:

```

NLME-ADD_ROUTE.request (
    DstAddr,
    RoutingTableRecord
)
    
```

Le Tableau 90 spécifie les paramètres pour NLME-ADD_ROUTE.request.

Tableau 90 – Paramètres de NLME-ADD_ROUTE.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse courte 16 bits de l'appareil de routage
RoutingTableRecord	Structure NLRoute_Struct (voir Tableau 15)		Élément de la table de routage

9.5.7.1.2 NLME-ADD_ROUTE.confirm

La primitive NLME-ADD_ROUTE.confirm retourne le résultat d'une NLME-ADD_ROUTE.request.

La sémantique de NLME_ADD-ROUTE.confirm est décrite comme suit:

```
NLME-ADD_ROUTE.confirm(
    Statut
)
```

Le Tableau 91 spécifie les paramètres pour NLME-ADD_ROUTE.confirm.

Tableau 91 – Paramètres de NLME-ADD_ROUTE.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultat d'une NLME-ADD_ROUTE.request: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

A la réception de NLME-ADD_ROUTE.request, il convient que la NL émette un paquet de demande d'ajout d'itinéraire (adding-route-request packet) vers l'appareil de routage et il convient qu'il retourne une NLME-ADD_ROUTE.confirm pour rapporter le résultat.

9.5.7.1.3 NLME-ADD_ROUTE.indication

La primitive NLME-ADD_ROUTE.indication est utilisée pour rapporter au DMAP qu'un appareil a reçu avec succès un paquet de demande d'ajout d'itinéraire.

La sémantique de NLME_ADD-ROUTE.confirm est décrite comme suit:

```
NLME-ADD_ROUTE.indication (
    RoutingTableRecord
)
```

Le Tableau 90 spécifie les paramètres pour NLME-ADD_ROUTE.indication.

9.5.7.1.4 NLME-ADD_ROUTE.response

La primitive NLME-ADD_ROUTE.response est la réponse de NLME-ADD_ROUTE.indication.

La sémantique de NLME-ADD_ROUTE.response est décrite comme suit:

```
NLME-ADD_ROUTE.response (
    Statut
)
```

Le Tableau 91 spécifie les paramètres pour NLME-ADD_ROUTE.response.

9.5.7.1.5 Séquence temporelle pour l'ajout d'itinéraire

Le diagramme de séquence temporelle pour ajouter un enregistrement à la table de routage d'un appareil de routage est représenté à la Figure 51.



Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Routing device DLSL	DLSL de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Route adding request command packet	Paquet de commande de demande d'ajout d'itinéraire
Route adding response command packet	Paquet de commande de réponse à l'ajout d'itinéraire

Figure 51 – Séquence temporelle pour l'ajout d'itinéraire

9.5.7.2 Services de mise à jour d'itinéraire

9.5.7.2.1 NLME-UPDATE_ROUTE.request

NLME-UPDATE_ROUTE.request met à jour un enregistrement dans la table de routage d'un appareil de routage.

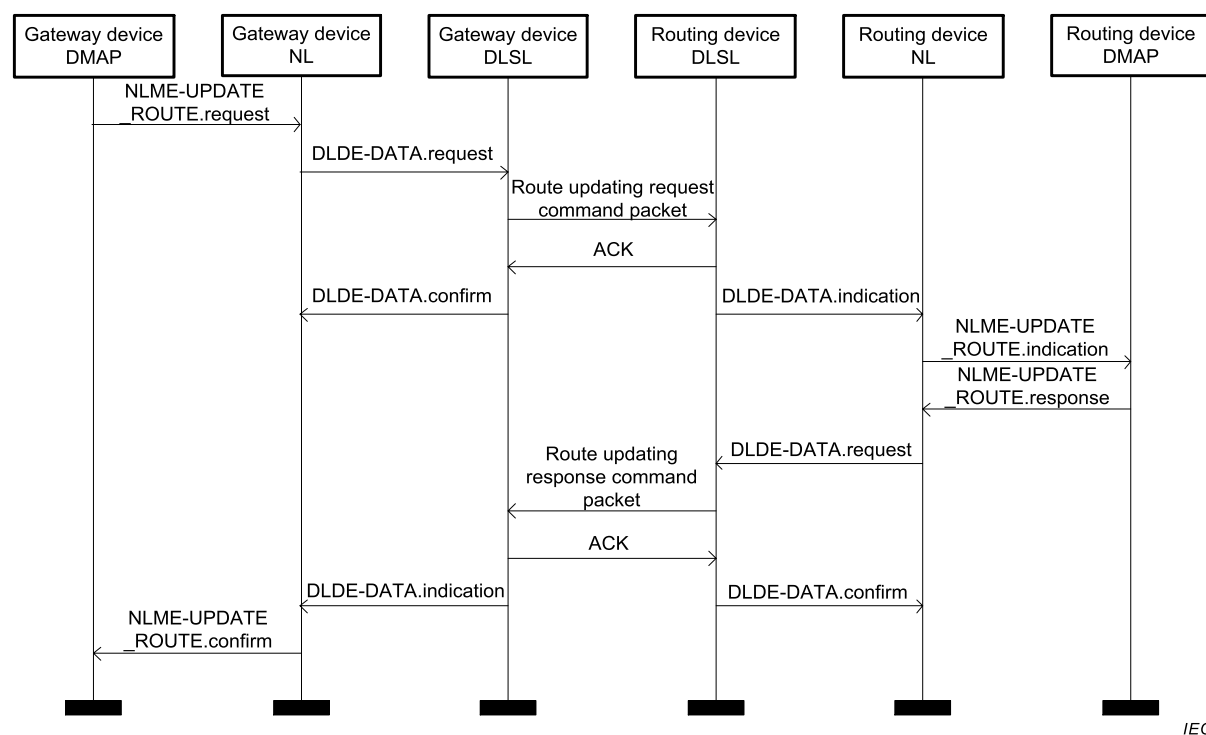
La sémantique de NLME-UPDATE_ROUTE.request est décrite comme suit:

```
NLME-UPDATE_ROUTE.request (
    DstAddr,
    RoutingTableRecord
)
```

Le Tableau 92 spécifie les paramètres pour NLME-UPDATE_ROUTE.request.

Tableau 92 – Paramètres de NLME-UPDATE_ROUTE.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse courte 16 bits de l'appareil de routage
RoutingTableRecord	Structure NLRoute_Struct (voir Tableau 15)		Élément de la table de routage



Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Routing device DLSL	DLSL de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Route updating request command packet	Paquet de commande de demande de mise à jour d'itinéraire
Route updating response command packet	Paquet de commande de réponse de mise à jour d'itinéraire

Figure 52 – Séquence temporelle pour la mise à jour d'itinéraire

9.5.7.3 Services de suppression d'itinéraire

9.5.7.3.1 NLME-DELETE_ROUTE.request

Le gestionnaire de réseau (NM) invoque NLME-DELETE_ROUTE.request pour supprimer un enregistrement dans la table de routage d'un appareil de routage.

La sémantique de NLME_DELETE-ROUTE.confirm est décrite comme suit:

```
NLME-DELETE_ROUTE.request(
    DstAddr,
    RouteID
)
```

Le Tableau 94 spécifie les paramètres pour NLME-DELETE-ROUTE.request.

Tableau 94 – Paramètres de NLME-UPDATE_ROUTE.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse courte 16 bits de l'appareil de routage de destination
RouteID	Unsigned16	0 à 65 535	ID d'itinéraire

9.5.7.3.2 NLME-DELETE_ROUTE.confirm

La primitive NLME_DELETE_ROUTE.confirm retourne le résultat d'exécution d'une NLME_DELETE_ROUTE.request.

La sémantique de NLME_DELETE_ROUTE.confirm est décrite comme suit:

```
NLME-DELETE_ROUTE.confirm(
    Statut
)
```

Le Tableau 95 spécifie les paramètres pour NLME_DELETE_ROUTE.confirm.

Tableau 95 – Paramètres de NLME-DELETE_ROUTE.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultat d'une NLME_DELETE_ROUTE.request: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

A la réception de NLME_DELETE_ROUTE.request, il convient que la NL émette un paquet de demande de suppression d'itinéraire vers l'appareil de routage et retourne une NLME_DELETE_ROUTE.confirm pour rapporter le résultat.

9.5.7.3.3 NLME-DELETE_ROUTE.indication

La primitive NLME_DELETE_ROUTE.indication est utilisée pour rapporter au DMAP que l'appareil a reçu avec succès un paquet de demande de suppression d'itinéraire.

La sémantique de NLME_DELETE_ROUTE.confirm est décrite comme suit:

```
NLME-DELETE_ROUTE.indication (
    RouteID
)
```

Le Tableau 94 spécifie les paramètres pour NLME_DELETE_ROUTE.indication.

9.5.7.3.4 NLME-DELETE_ROUTE.response

La primitive NLME_DELETE_ROUTE.response est la réponse de NLME_DELETE_ROUTE.indication.

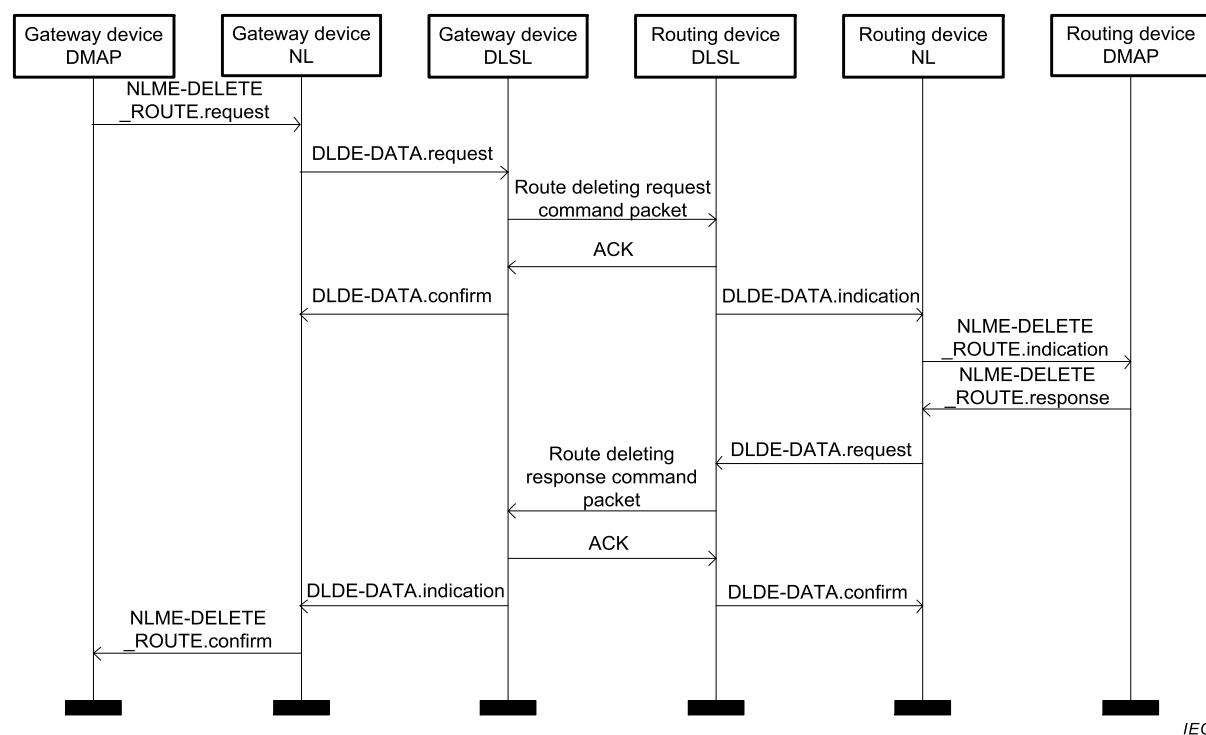
La sémantique de NLME_DELETE_ROUTE.response est décrite comme suit:

```
NLME-DELETE_ROUTE.response (
    Statut
)
```

Le Tableau 95 spécifie les paramètres pour NLME_DELETE_ROUTE.response.

9.5.7.3.5 Séquence temporelle pour la suppression d'itinéraire

Le diagramme de séquence temporelle pour supprimer des enregistrements des tables de routage des appareils de routage est représenté à la Figure 53.



IEC

Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Routing device DLSL	DLSL de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Route deleting request command packet	Paquet de commande de demande de suppression d'itinéraire
Route deleting response command packet	Paquet de commande de réponse de suppression d'itinéraire

Figure 53 – Séquence temporelle pour la suppression d'itinéraire

9.5.8 Services d'allocation de ressources de communication

9.5.8.1 Généralités

L'allocation de ressources de communication comprend l'allocation de liaison et de supertrame. Ces services fournissent les primitives suivantes:

- Services d'ajout de liaison:
 - NLME-ADD-LINK.request,
 - NLME-ADD-LINK.confirm,
 - NLME-ADD-LINK.response, et
 - NLME-ADD-LINK.indication;
- Services de mise à jour de liaison:
 - NLME-UPDATE-LINK.request,
 - NLME-UPDATE-LINK.confirm,
 - NLME-UPDATE-LINK.response, et
 - NLME-UPDATE-LINK.indication;
- Services de libération de liaison:
 - NLME-RELEASE-LINK.request,

- NLME-RELEASE-LINK.confirm,
- NLME-RELEASE-LINK.response, et
- NLME-RELEASE-LINK.indication;
- Services d'ajout de supertrame:
 - NLME-ADD-SFR.request,
 - NLME-ADD-SFR.confirm,
 - NLME-ADD-SFR.response, et
 - NLME-ADD-SFR.indication;
- Services de mise à jour de supertrame:
 - NLME-UPDATE-SFR.request,
 - NLME-UPDATE-SFR.confirm,
 - NLME-UPDATE-SFR.response, et
 - NLME-UPDATE-SFR.indication;
- Services de libération de supertrame:
 - NLME-RELEASE-SFR.request,
 - NLME-RELEASE-SFR.confirm,
 - NLME-RELEASE-SFR.response, et
 - NLME-RELEASE-SFR.indication.

9.5.8.2 Services d'ajout de liaison

9.5.8.2.1 NLME-ADD-LINK.request

La primitive NLME-ADD-LINK.request est utilisée pour ajouter un ou plusieurs enregistrements de nouvelle(s) liaison(s) allant de l'appareil de passerelle à un appareil de routage ou d'un appareil de routage à un appareil de terrain.

La sémantique de NLME-ADD-LINK.request est décrite comme suit:

```
NLME-ADD-LINK.request (
    DstAddr,
    LinkCount,
    LinkStructure
)
```

Le Tableau 96 spécifie les paramètres pour NLME-ADD-LINK.request.

Tableau 96 – Paramètres de NLME-ADD-LINK.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination 16 bits
LinkCount	Unsigned16	0 à 65 535	Nombre de liaisons ajoutées pour prendre en charge l'ajout de plusieurs liaisons chaque fois
LinkStructure	Structure Link_Struct (voir Tableau 17)		Informations des liaisons

9.5.8.2.2 NLME-ADD-LINK.confirm

La primitive NLME-ADD-LINK.confirm retourne les résultats de NLME-ADD-LINK.request.

La sémantique de NLME-ADD-LINK.confirm est décrite comme suit:

NLME-ADD-LINK.confirm (

Statut
)

Le Tableau 97 spécifie les paramètres pour NLME-ADD-LINK.confirm.

Tableau 97 – Paramètres de NLME-ADD-LINK.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultats de la demande d'ajout de liaison: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.8.2.3 NLME-ADD-LINK.indication

La primitive NLME-ADD_LINK.indication est utilisée pour rapporter au DMAP que l'appareil a reçu avec succès un paquet de demande d'ajout de liaison.

La sémantique de NLME-ADD-LINK.indication est décrite comme suit:

NLME-ADD-LINK.indication (

LinkCount,
LinkStructure

)

Le Tableau 96 spécifie les paramètres pour NLME-ADD-LINK.indication.

9.5.8.2.4 NLME-ADD-LINK.response

La primitive NLME-ADD_LINK.response est la réponse de NLME-ADD_LINK.indication.

La sémantique de NLME-ADD-LINK.response est décrite comme suit:

NLME-ADD-LINK.response (

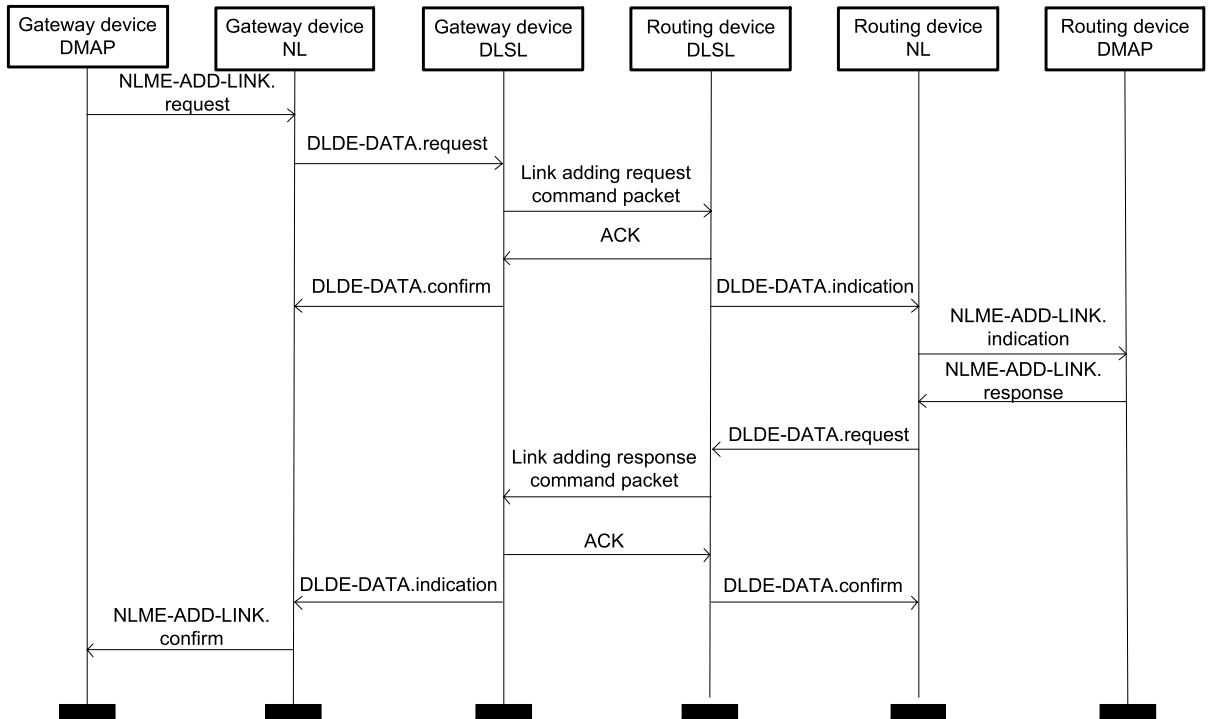
Statut

)

Le Tableau 97 spécifie les paramètres pour NLME-ADD-LINK.response.

9.5.8.2.5 Séquence temporelle pour l'ajout de liaison

Le diagramme de séquence temporelle pour l'ajout d'une liaison allant d'un appareil de passerelle à un appareil de routage est représenté à la Figure 54.

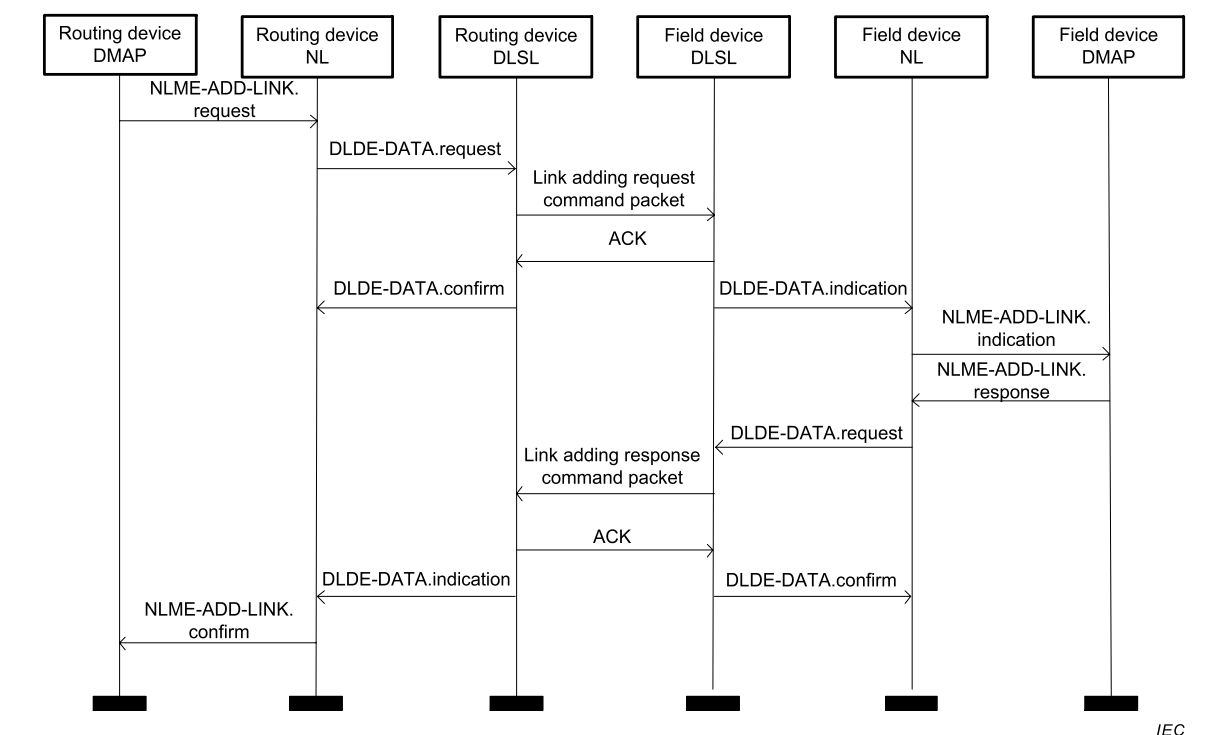


IEC

Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Routing device DLSL	DLSL de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Link adding request command packet	Paquet de commande de demande d'ajout de liaison
Link adding response command packet	Paquet de commande de réponse à l'ajout de liaison

**Figure 54 – Ajout d'une liaison allant d'un
appareil de passerelle à un appareil de routage**

Le diagramme de séquence temporelle pour ajouter une liaison allant d'un appareil de routage à un appareil de terrain est représenté à la Figure 55.



Anglais	Français
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DLSL	DLSL de l'appareil de routage
Field device DLSL	DLSL de l'appareil de terrain
Field device NL	NL de l'appareil de terrain
Field device DMAP	DMAP de l'appareil de terrain
Link adding request command packet	Paquet de commande de demande d'ajout de liaison
Link adding response command packet	Paquet de commande de réponse à l'ajout de liaison

Figure 55 – Ajout d'une liaison allant d'un appareil de routage à un appareil de terrain

9.5.8.3 Services de mise à jour de liaison

9.5.8.3.1 NLME-UPDATE-LINK.request

La primitive NLME-UPDATE-LINK.request est utilisée pour mettre à jour un ou plusieurs enregistrements de liaison(s) existante(s) allant de l'appareil de passerelle à un appareil de routage ou d'un appareil de routage à un appareil de terrain.

La sémantique de NLME-UPDATE-LINK.request est décrite comme suit:

```

NLME-UPDATE-LINK.request (
    DstAddr,
    LinkCount,
    LinkStructure
)
    
```

Le Tableau 98 spécifie les paramètres pour NLME-UPDATE-LINK.request.

Tableau 98 – Paramètres de NLME-UPDATE-LINK.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination 16 bits
LinkCount	Unsigned16	0 à 65 535	Nombre de liaisons ajoutées pour prendre en charge la mise à jour de plusieurs liaisons chaque fois
LinkStructure	Structure Link_Struct (voir Tableau 17)		Informations des liaisons

9.5.8.3.2 NLME-UPDATE-LINK.confirm

La primitive NLME-UPDATE-LINK.confirm retourne les résultats de NLME-UPDATE-LINK.request.

La sémantique de NLME-UPDATE-LINK.confirm est décrite comme suit:

```
NLME-UPDATE-LINK.confirm (
    Statut
)
```

Le Tableau 99 spécifie les paramètres pour NLME-UPDATE-LINK.confirm.

Tableau 99 – Paramètres de NLME-UPDATE-LINK.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultats de la demande de mise à jour de liaison: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.8.3.3 NLME-UPDATE-LINK.indication

La primitive NLME-UPDATE_LINK.indication est utilisée pour rapporter au DMAP que l'appareil a reçu avec succès un paquet de demande de mise à jour de liaison.

La sémantique de NLME-UPDATE-LINK.indication est décrite comme suit:

```
NLME-UPDATE-LINK.indication (
    LinkCount,
    LinkStructure
)
```

Le Tableau 98 spécifie les paramètres pour NLME-UPDATE-LINK.indication.

9.5.8.3.4 NLME-UPDATE-LINK.response

La primitive NLME-UPDATE-LINK.response est la réponse de NLME-UPDATE-LINK.indication.

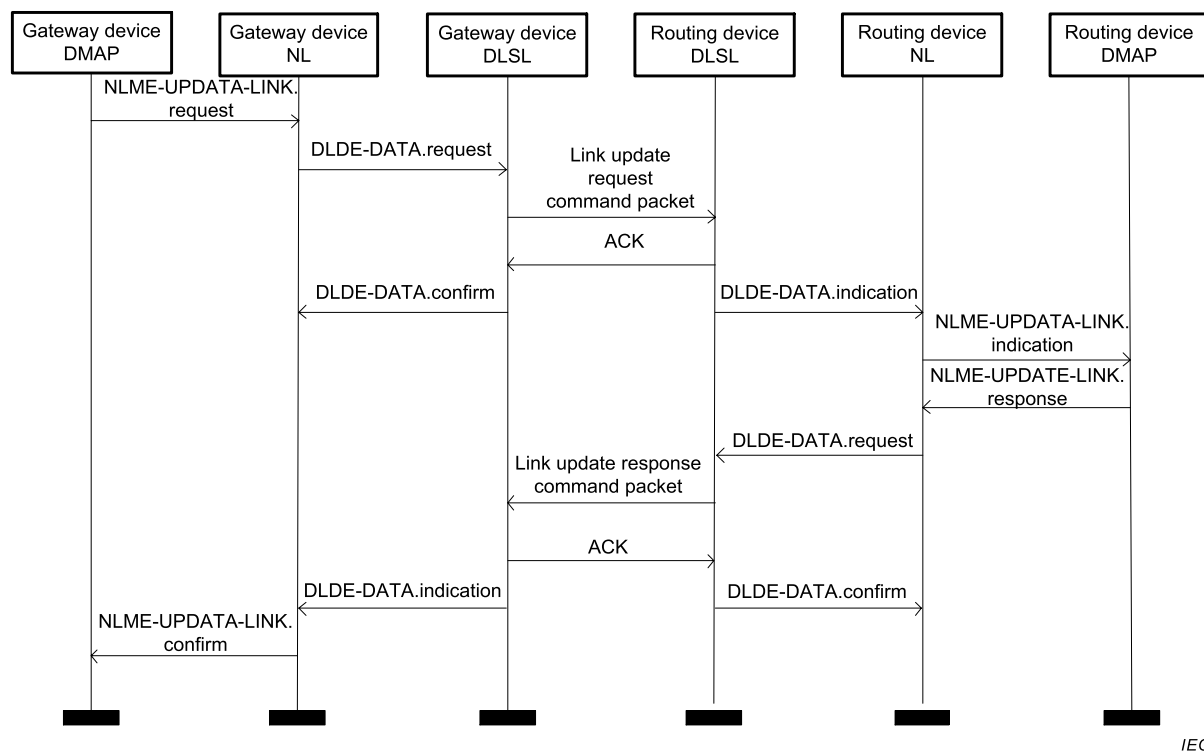
La sémantique de NLME-UPDATE-LINK.response est décrite comme suit:

```
NLME-UPDATE-LINK.response (
    Statut
)
```

Le Tableau 99 spécifie les paramètres pour NLME-UPDATE-LINK.response.

9.5.8.3.5 Séquence temporelle pour la mise à jour de liaison

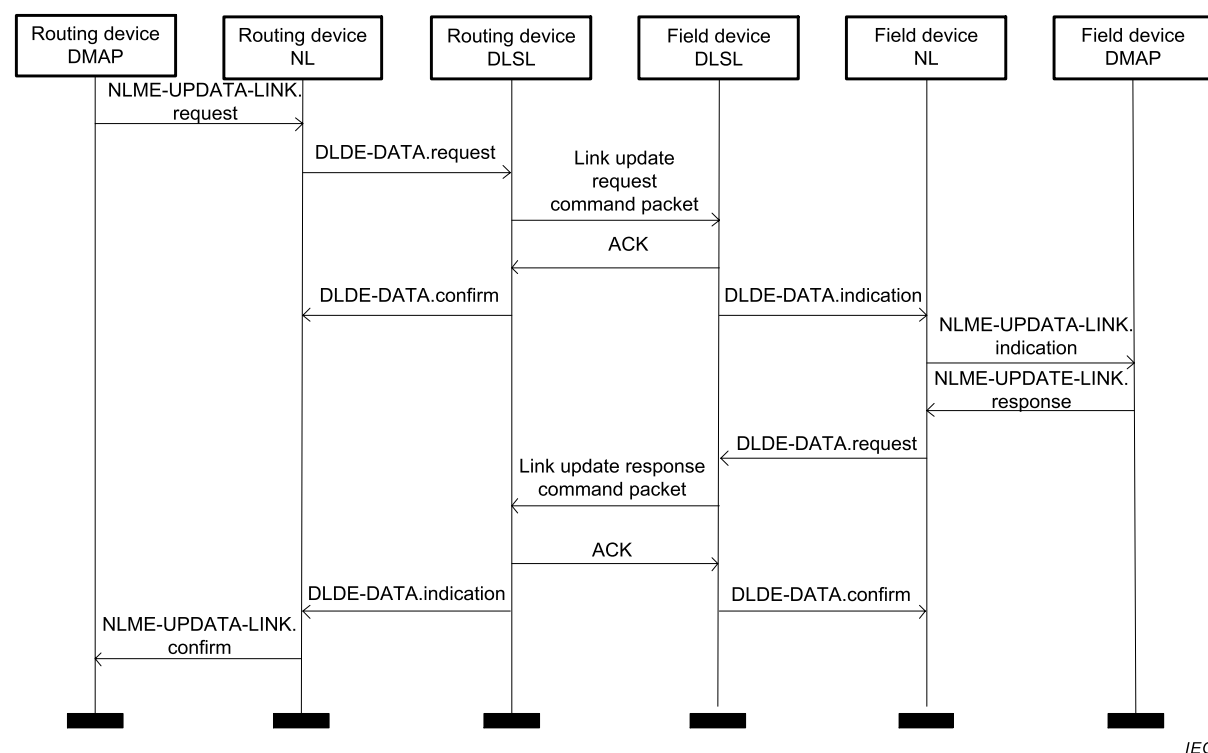
Le diagramme de séquence temporelle pour mettre à jour une liaison allant d'un appareil de passerelle à un appareil de routage est représenté à la Figure 56.



Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Routing device DLSL	DLSL de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Link update request command packet	Paquet de commande de demande de mise à jour de liaison
Link update response command packet	Paquet de commande de réponse de mise à jour de liaison

Figure 56 – Mise à jour d'une liaison allant d'un appareil de passerelle à un appareil de routage

Le diagramme de séquence temporelle pour mettre à jour une liaison allant d'un appareil de routage à un appareil de terrain est représenté à la Figure 57.



Anglais	Français
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DLSL	DLSL de l'appareil de routage
Field device DLSL	DLSL de l'appareil de terrain
Field device NL	NL de l'appareil de terrain
Field device DMAP	DMAP de l'appareil de terrain
Link update request command packet	Paquet de commande de demande de mise à jour de liaison
Link update response command packet	Paquet de commande de réponse de mise à jour de liaison

Figure 57 – Mise à jour d'une liaison allant d'un appareil de routage à un appareil de terrain

9.5.8.4 Services de libération de liaison

9.5.8.4.1 NLME-RELEASE-LINK.request

La primitive NLME-RELEASE-LINK.request est utilisée pour supprimer une ou plusieurs liaison(s) existante(s) allant de l'appareil de passerelle à un appareil de routage ou d'un appareil de routage à un appareil de terrain.

La sémantique de NLME-RELEASE-LINK.request est décrite comme suit:

```

NLME-RELEASE-LINK.request (
    DstAddr,
    LinkCount,
    LinkID[LinkCount]
)
  
```

Le Tableau 100 spécifie les paramètres pour NLME-RELEASE-LINK.request.

Tableau 100 – Paramètres de NLME-RELEASE-LINK.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination 16 bits
LinkCount	Unsigned16	0 à 65 535	Nombre de liaisons ajoutées pour prendre en charge la libération de plusieurs liaisons chaque fois
LinkID[LinkCount]	Unsigned16	0 à 65 535	Identificateurs des liaisons supprimées

9.5.8.4.2 NLME-RELEASE-LINK.confirm

La primitive NLME-RELEASE-LINK.confirm retourne les résultats de NLME-RELEASE-LINK.request.

La sémantique de NLME-RELEASE-LINK.confirm est décrite comme suit:

```
NLME-RELEASE-LINK.confirm (      Statut
                                )
```

Le Tableau 101 spécifie les paramètres pour NLME-RELEASE-LINK.confirm.

Tableau 101 – Paramètres de NLME-RELEASE-LINK.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultats de la demande de libération de liaison: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.8.4.3 NLME-RELEASE-LINK.indication

La primitive NLME-RELEASE_LINK.indication est utilisée pour rapporter au DMAP que l'appareil a reçu avec succès un paquet de demande de libération de liaison.

La sémantique de NLME-RELEASE-LINK.indication est décrite comme suit:

```
NLME-RELEASE-LINK.indication (
    LinkCount,
    LinkID[LinkCount]
)
```

Le Tableau 100 spécifie les paramètres pour NLME-RELEASE-LINK.indication.

9.5.8.4.4 NLME-RELEASE-LINK.response

La primitive NLME-RELEASE-LINK.response est la réponse de NLME-RELEASE-LINK.indication.

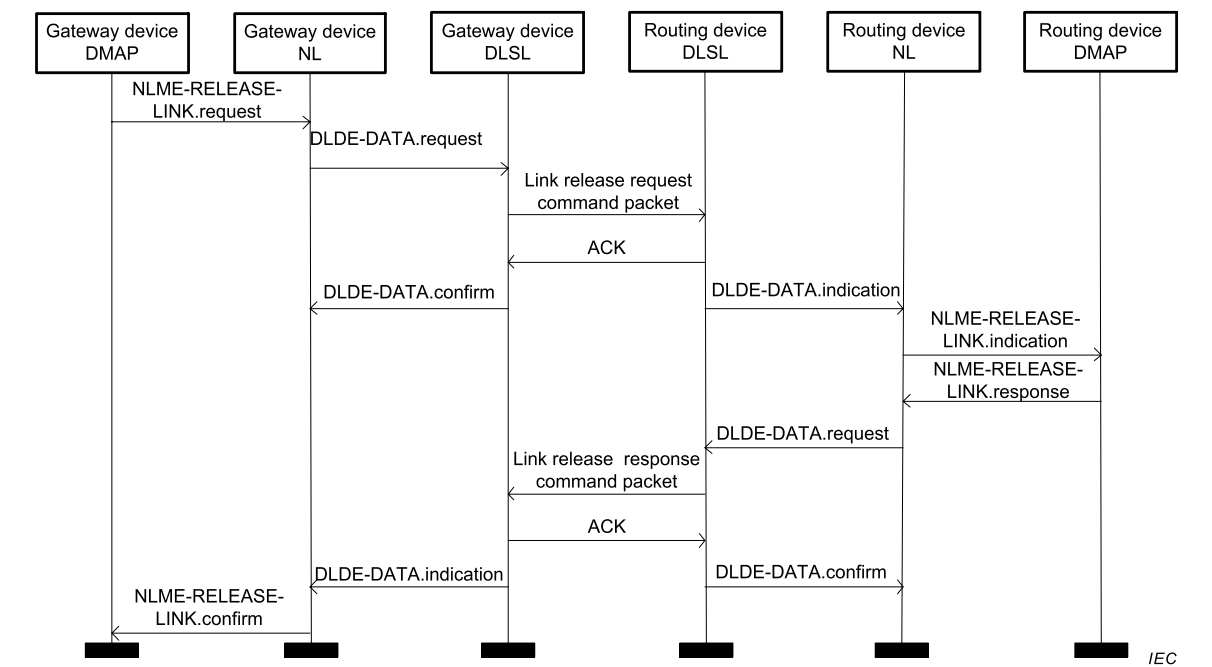
La sémantique de NLME-RELEASE-LINK.response est décrite comme suit:

```
NLME-RELEASE-LINK.response (          Statut
                                )
```

Le Tableau 101 spécifie les paramètres pour NLME-RELEASE-LINK.response.

9.5.8.4.5 Séquence temporelle pour la libération de liaison

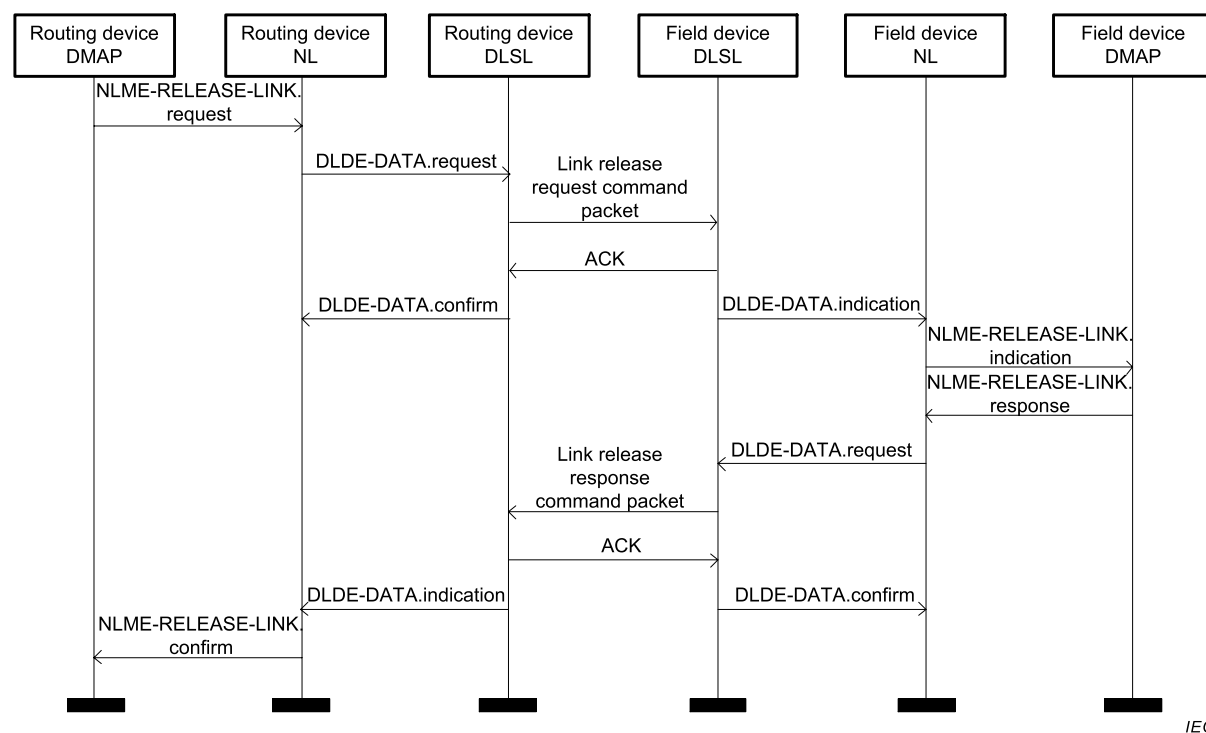
Le diagramme de séquence temporelle pour libérer une liaison allant de l'appareil de passerelle à un appareil de routage est représenté à la Figure 58.



Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Routing device DLSL	DLSL de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Link release request command packet	Paquet de commande de demande de libération de liaison
Link release response command packet	Paquet de commande de réponse à la libération de liaison

Figure 58 – Libération d'une liaison allant d'un appareil de passerelle à un appareil de routage

Le diagramme de séquence temporelle pour libérer une liaison allant d'un appareil de routage à un appareil de terrain est représenté à la Figure 59.



IEC

Anglais	Français
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DLDSL	DLDSL de l'appareil de routage
Field device DLDSL	DLDSL de l'appareil de terrain
Field device NL	NL de l'appareil de terrain
Field device DMAP	DMAP de l'appareil de terrain
Link release request command packet	Paquet de commande de demande de libération de liaison
Link release response command packet	Paquet de commande de réponse à la libération de liaison

Figure 59 – Libération d'une liaison allant d'un appareil de routage à un appareil de terrain

9.5.8.5 Services d'ajout de supertrame

9.5.8.5.1 NLME-ADD-SFR.request

La primitive NLME-ADD-SFR.request est utilisée pour ajouter un enregistrement d'une nouvelle supertrame allant de l'appareil de passerelle à un appareil de routage ou d'un appareil de routage à un appareil de terrain.

La sémantique de NLME-ADD-SFR.request est décrite comme suit:

NLME-ADD-SFR.request (

DstAddr,

SuperframeStructure

)

Le Tableau 102 spécifie les paramètres pour NLME-ADD-SFR.request.

Tableau 102 – Paramètres de NLME-ADD-SFR.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination 16 bits
SuperframeStructure	Structure Superframe_Struct (voir Tableau 16)		Attribut information de supertrame

9.5.8.5.2 NLME-ADD-SFR.confirm

La primitive NLME-ADD-SFR.confirm retourne le résultat de NLME-ADD-SFR.request.

La sémantique de NLME-ADD-SFR.confirm est décrite comme suit:

NLME-ADD-SFR.confirm (
 Statut
)

Le Tableau 103 spécifie les paramètres pour NLME-ADD-SFR.confirm.

Tableau 103 – Paramètres de NLME-ADD-SFR.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultats de la demande de libération de supertrame: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.8.5.3 NLME-ADD-SFR.indication

La primitive NLME-ADD_SFR.indication est utilisée pour rapporter au DMAP que l'appareil a reçu avec succès un paquet de demande d'ajout de supertrame.

La sémantique de NLME-ADD-SFR.indication est décrite comme suit:

NLME-ADD-SFR.indication (
 SuperframeStructure
)

Le Tableau 102 spécifie les paramètres pour NLME-ADD-SFR.indication.

9.5.8.5.4 NLME-ADD-SFR.response

La primitive NLME-ADD-SFR.response est la réponse de NLME-ADD-SFR.indication.

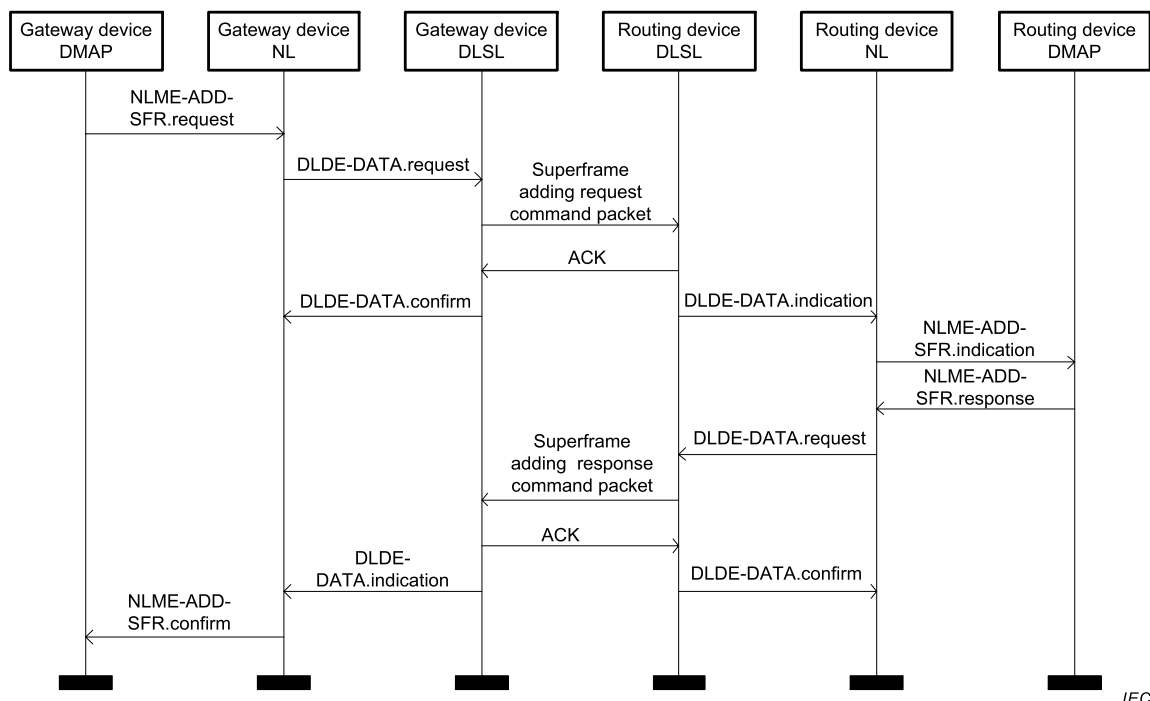
La sémantique de NLME-ADD-SFR.response est décrite comme suit:

NLME-ADD-SFR.response (
 Statut
)

Le Tableau 103 spécifie les paramètres pour NLME-ADD-SFR.response.

9.5.8.5.5 Séquence temporelle pour l'ajout de supertrame

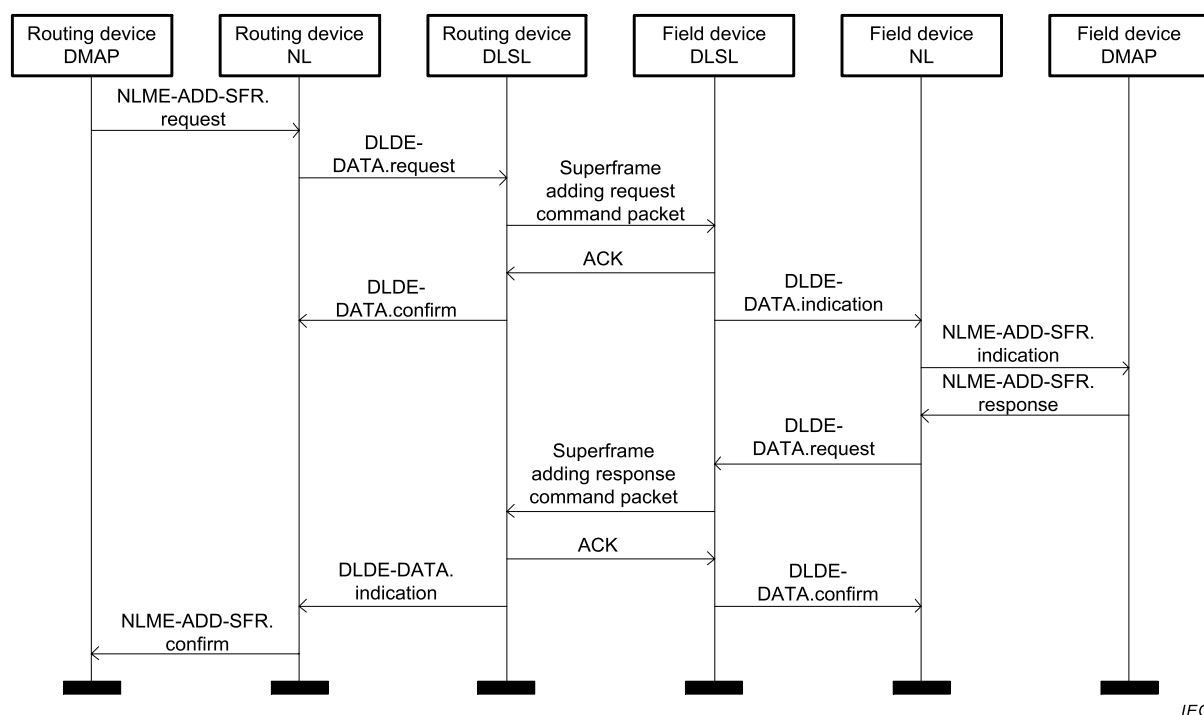
Le diagramme de séquence temporelle pour ajouter une supertrame allant de l'appareil de passerelle à un appareil de routage est représenté à la Figure 60.



Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Routing device DLSL	DLSL de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Superframe adding request command packet	Paquet de commande de demande d'ajout de supertrame
Superframe adding response command packet	Paquet de commande de réponse à l'ajout de supertrame

Figure 60 – Ajout d'une supertrame allant d'un appareil de passerelle à un appareil de routage

Le diagramme de séquence temporelle pour ajouter une supertrame allant d'un appareil de routage à un appareil de terrain est représenté à la Figure 61.



IEC

Anglais	Français
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DLSL	DLSL de l'appareil de routage
Field device DLSL	DLSL de l'appareil de terrain
Field device NL	NL de l'appareil de terrain
Field device DMAP	DMAP de l'appareil de terrain
Superframe adding request command packet	Paquet de commande de demande d'ajout de supertrame
Superframe adding response command packet	Paquet de commande de réponse à l'ajout de supertrame

Figure 61 – Ajout d'une supertrame allant d'un appareil de routage à un appareil de terrain

9.5.8.6 Services de mise à jour de supertrame

9.5.8.6.1 NLME-UPDATA-SFR.request

La primitive NLME-UPDATA-SFR.request est utilisée pour modifier un enregistrement d'une supertrame existante allant de l'appareil de passerelle à un appareil de routage ou d'un appareil de routage à un appareil de terrain.

La sémantique de NLME-UPDATA-SFR.request est décrite comme suit:

```
NLME-UPDATA-SFR.request (
    DstAddr,
    SuperframeStructure
)
```

Le Tableau 104 spécifie les paramètres pour NLME-UPDATA-SFR.request.

Tableau 104 – Paramètres de NLME-UPDATA-SFR.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse 16 bits de l'appareil de destination
SuperframeStructure	Structure Superframe_Struct (voir Tableau 16)		Attribut information de supertrame

9.5.8.6.2 NLME-UPDATE-SFR.confirm

La primitive NLME-UPDATE-SFR.confirm retourne les résultats de NLME-UPDATA-SFR.request.

La sémantique de NLME-UPDATE-SFR.confirm est décrite comme suit:

NLME-UPDATE-SFR.confirm (
 Statut
)

Le Tableau 105 spécifie les paramètres pour NLME-UPDATE-SFR.confirm.

Tableau 105 – Paramètres de NLME-UPDATE-SFR.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultats de la demande de mise à jour de supertrame: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.8.6.3 NLME-UPDATE-SFR.indication

La primitive NLME-UPDATE_SFR.indication est utilisée pour rapporter au DMAP que l'appareil a reçu avec succès un paquet de demande de mise à jour de supertrame.

La sémantique de NLME-UPDATA-SFR.indication est décrite comme suit:

NLME-UPDATE-SFR.indication (
 SuperframeStructure
)

Le Tableau 104 spécifie les paramètres pour NLME-UPDATE-SFR.indication.

9.5.8.6.4 NLME-UPDATE-SFR.response

La primitive NLME-UPDATE-SFR.response est la réponse de NLME-UPDATE-SFR.indication.

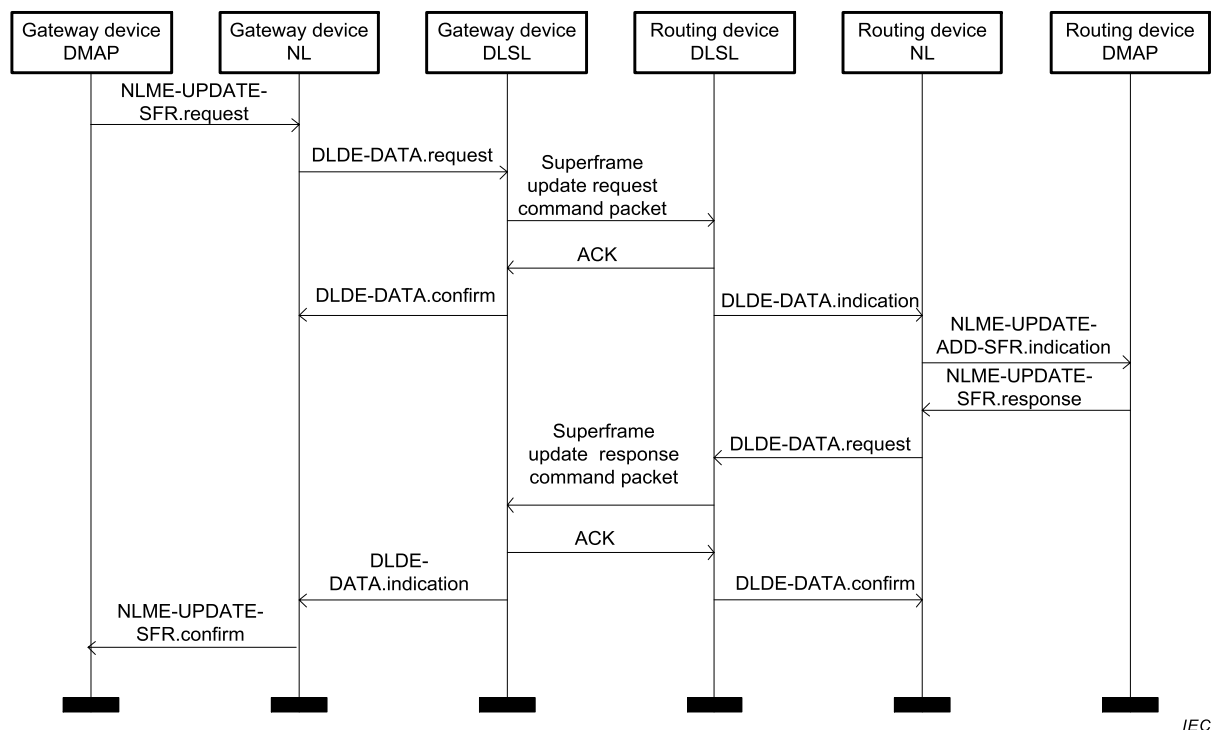
La sémantique de NLME-UPDATA-SFR.response est décrite comme suit:

NLME-UPDATE-SFR.response (
 Statut
)

Le Tableau 105 spécifie les paramètres pour NLME-UPDATE-SFR.response.

9.5.8.6.5 Séquence temporelle pour la mise à jour de supertrame

Le diagramme de séquence temporelle pour mettre à jour une supertrame allant de l'appareil de passerelle à un appareil de routage est représenté à la Figure 62.



Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Routing device DLSL	DLSL de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Superframe update request command packet	Paquet de commande de demande de mise à jour de supertrame
Superframe update response command packet	Paquet de commande de réponse de mise à jour de supertrame

Figure 62 – Mise à jour d'une supertrame allant d'un appareil de passerelle à un appareil de routage

Le diagramme de séquence temporelle pour mettre à jour une supertrame allant d'un appareil de routage à un appareil de terrain est représenté à la Figure 63.

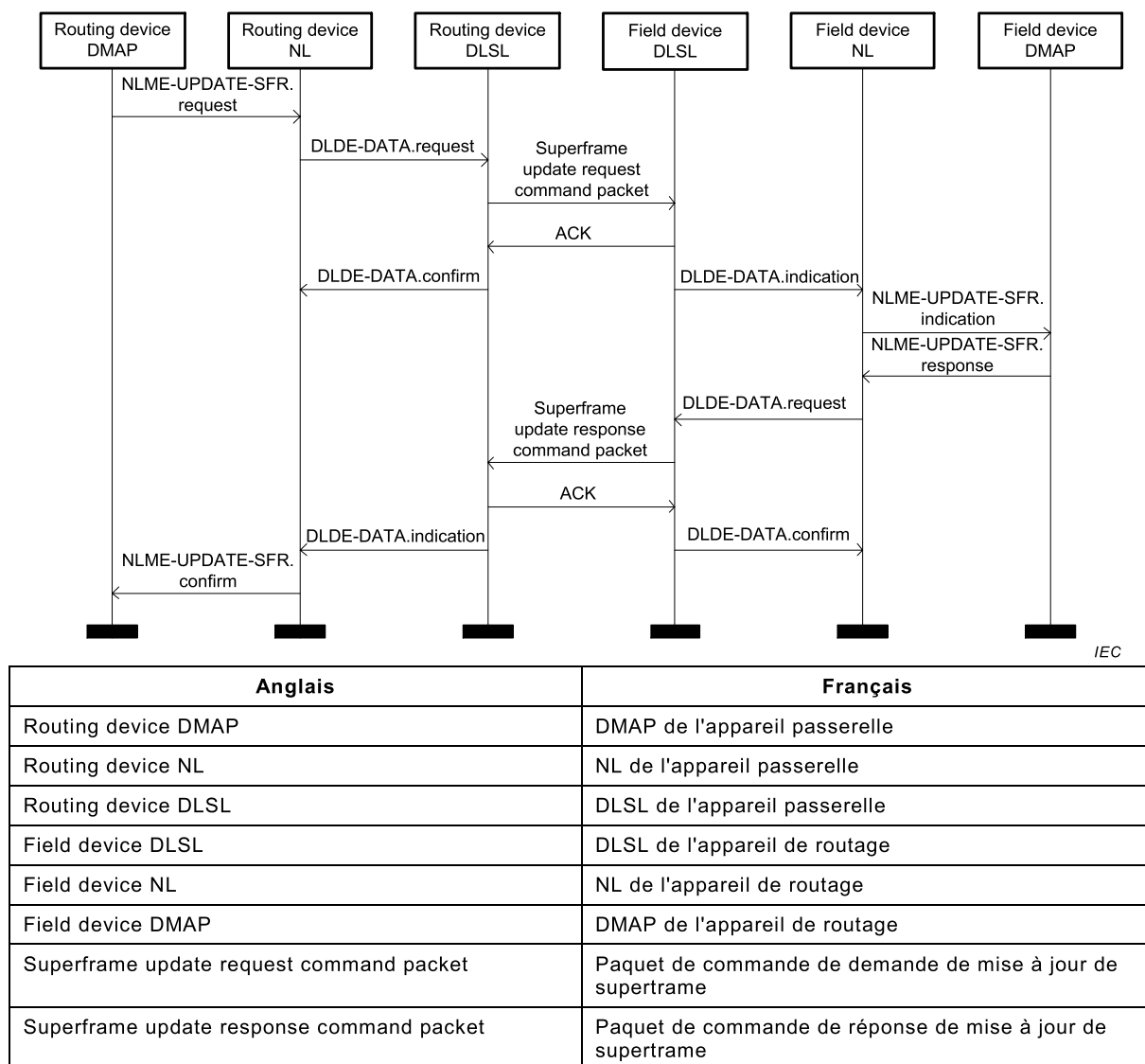


Figure 63 – Mise à jour d'une supertrame allant d'un appareil de routage à un appareil de terrain

9.5.8.7 Services de libération de supertrame

9.5.8.7.1 NLME-RELEASE-SFR.request

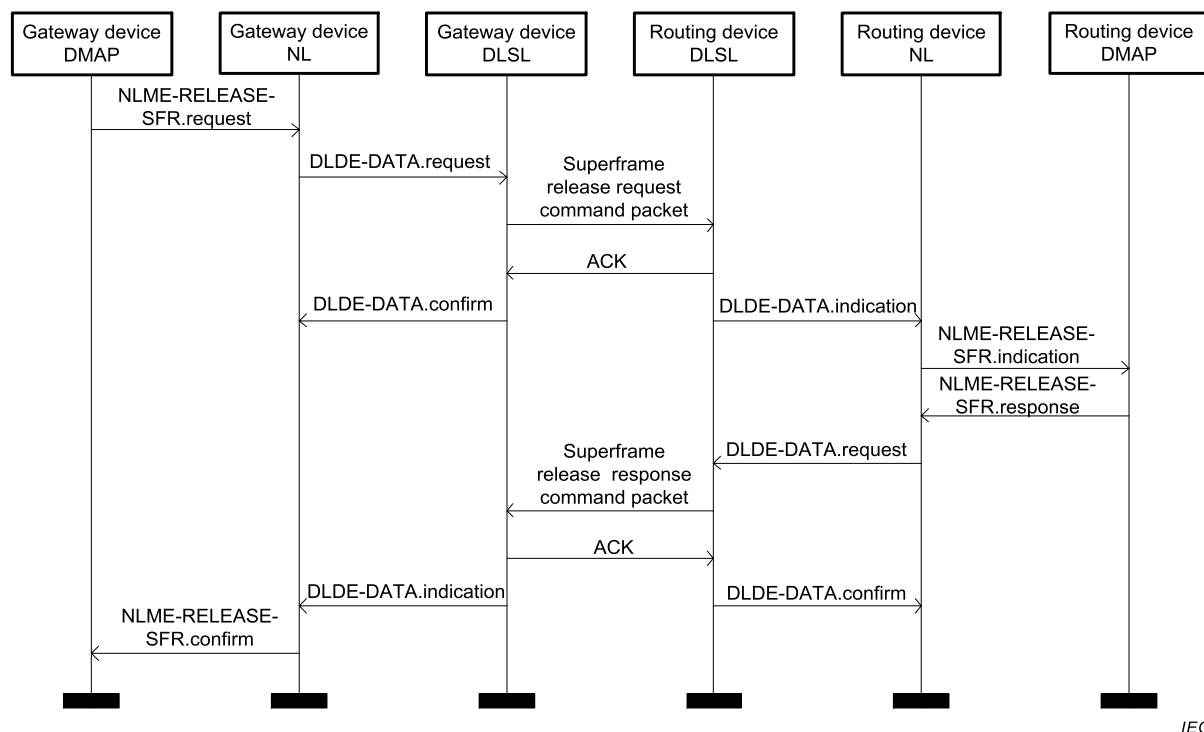
La primitive NLME-RELEASE-SFR.request est utilisée pour supprimer un enregistrement d'une supertrame existante allant de l'appareil de passerelle à un appareil de routage ou d'un appareil de routage à un appareil de terrain.

La sémantique de NLME-RELEASE-SFR.request est décrite comme suit:

```
NLME-RELEASE-SFR.request (
    DstAddr,
    SuperframeID
)
```


9.5.8.7.5 Séquence temporelle pour la libération de supertrame

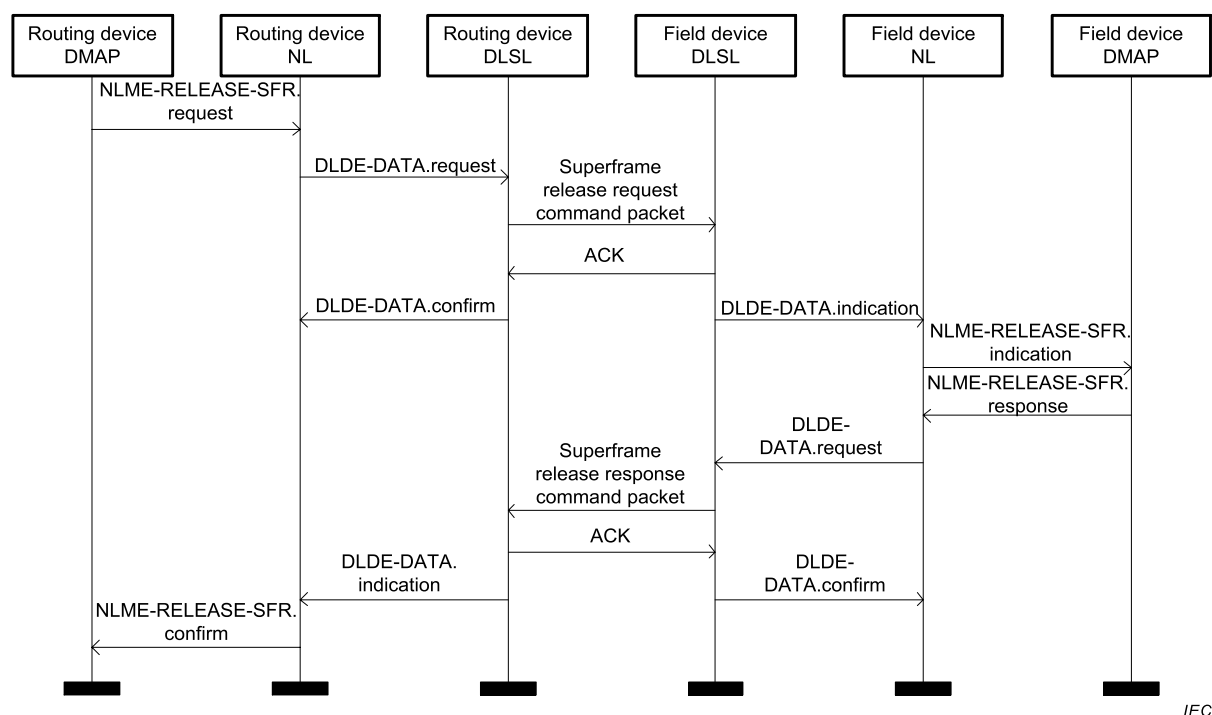
Le diagramme de séquence temporelle pour libérer une supertrame allant de l'appareil de passerelle à l'appareil de routage est représenté à la Figure 64.



Anglais	Français
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DLSSL	DLSSL de l'appareil passerelle
Routing device DLSSL	DLSSL de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Superframe release request command packet	Paquet de commande de demande de libération de supertrame
Superframe release response command packet	Paquet de commande de réponse de libération de supertrame

Figure 64 – Libération d'une supertrame allant d'un appareil de passerelle à un appareil de routage

Le diagramme de séquence temporelle pour libérer une supertrame allant d'un appareil de routage à un appareil de terrain est représenté à la Figure 65.



IEC

Anglais	Français
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DLSL	DLSL de l'appareil de routage
Field device DLSL	DLSL de l'appareil de terrain
Field device NL	NL de l'appareil de terrain
Field device DMAP	DMAP de l'appareil de terrain
Superframe release request command packet	Paquet de commande de demande de libération de supertrame
Superframe release response command packet	Paquet de commande de réponse de libération de supertrame

Figure 65 – Libération d'une supertrame allant d'un appareil de routage à un appareil de terrain

9.5.9 Services d'agrégation et désagrégation

9.5.9.1 NLME-AGG.indication

La primitive NLME-AGG.indication est utilisée pour que la NL rapporte au DMAP que les paquets reçus ont besoin d'être agrégés.

La sémantique de NLME-AGG.indication est décrite comme suit:

```

NLME-AGG.indication (
    SrcAddr,
    NwkPayload
)
  
```

Le Tableau 108 spécifie les paramètres pour NLME-AGG.indication.

Tableau 108 – Paramètres de NLME-AGG.indication

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	ID de la VCR d'agrégation
NwkPayload	Octetstring		Charge utile de couche réseau (NL)

9.5.9.2 NLME-AGO-SEND.request

NLME-AGO-SEND.request est utilisée pour que le DMAP demande à la NL d'envoyer le paquet agrégé après que l'agrégation a été faite.

La sémantique de NLME-AGO-SEND.request est décrite comme suit:

```
NLME-AGO-SEND.request (
    GatewayAddr,
    AggPacketFlag,
    Priority,
    AggNumber,
    AGGRouteID,
    PSFlag,
    AggPayload
)
```

Le Tableau 109 spécifie les paramètres pour NLME-AGO-SEND.request.

Tableau 109 – Paramètres de NLME-AGO-SEND.request

Nom	Type de données	Plage valide	Description
GatewayAddr	Unsigned16	0 à 65 535	Adresse réseau de l'appareil de passerelle
AggPacketFlag	Unsigned8	0, 1	Indique si ce paquet est un paquet de données ou un paquet d'agrégation: 0 = paquet de données; 1 = paquet d'agrégation.
Priorité	Unsigned8	0 à 15	Priorité des données de processus
AggNumber	Unsigned8	0 à 255	Nombre de paquets agrégés
AGGRouteID	Unsigned16	0 à 65 535	RouteID de l'agrégation
PSFlag	Unsigned8	0, 1	Indique si ce paquet est de type P/S: 0 = pas de type P/S; 1 = type P/S.
AggPayload	Octetstring		Paquet agrégé de DMAP

9.5.9.3 NLME-DAG.indication

La primitive NLME-DAG.indication est utilisée pour envoyer le paquet agrégé au DMAP pour sa désagrégation lorsque la NL reçoit un paquet agrégé.

La sémantique de NLME-DAG.indication est décrite comme suit:

```
NLME-DAG.indication (
    AggNumber,
    NwkPalyload
)
```

Le Tableau 110 spécifie les paramètres pour NLME-DAG.indication.

Tableau 110 – Paramètres de NLME-DAG.indication

Nom	Type de données	Plage valide	Description
AggNumber	Unsigned8	0 à 255	Nombre de paquets agrégés
NwkPayload	Octetstring		Charge utile de couche réseau (NL)

9.5.10 Services de rapport sur l'état des appareils

9.5.10.1 NLME-DEVICE-STATUS.request

La primitive NLME-DEVICE-STATUS.request est utilisée pour rapporter l'état des appareils aux appareils de routage par un appareil de terrain ou à l'appareil de passerelle par un appareil de routage.

La sémantique de NLME-DEVICE-STATUS.request est décrite comme suit:

```
NLME-CHANNEL-DEVICE.request(
                                DstAddr,
                                DeviceCount,
                                DeviceConditionInfo
                                )
```

Le Tableau 111 spécifie les paramètres pour NLME-DEVICE-STATUS.request.

Tableau 111 – Paramètres de NLME-DEVICE-STATUS.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination
DeviceCount	Unsigned8	0 à 255	Nombre total des appareils ayant fait l'objet d'un rapport
DeviceConditionInfo	Structure DevConRep_Struct (voir Tableau 22)		Informations sur les attributs de condition d'un appareil

9.5.10.2 NLME-DEVICE-STATUS.indication

La primitive NLME-DEVICE-STATUS.indication est utilisée pour rapporter au DMAP la réception d'un paquet de commande de rapport sur la condition des appareils.

La sémantique de NLME-DEVICE-STATUS.indication est décrite comme suit:

```
NLME-DEVICE-STATUS.indication (
                                SrcAddr,
                                DeviceCount,
                                DeviceConditionInfo
                                )
```

Le Tableau 112 spécifie les paramètres pour NLME-DEVICE-STATUS.indication.

Tableau 112 – Paramètres de NLME-DEVICE-STATUS.indication

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Source address (adresse source)
DeviceCount	Unsigned8	0 à 255	Nombre total des appareils ayant fait l'objet d'un rapport
DeviceConditionInfo	Structure DevConRep_Struct (voir Tableau 22)		Informations sur les attributs de condition d'un appareil

9.5.10.3 NLME-DEVICE-STATUS.confirm

La primitive NLME-DEVICE-STATUS.confirm est utilisée pour retourner les résultats de NLME-DEVICE-STATUS.request.

La sémantique de NLME-DEVICE-STATUS.confirm est décrite comme suit:

NLME-DEVICE-STATUS.confirm (

Statut

)

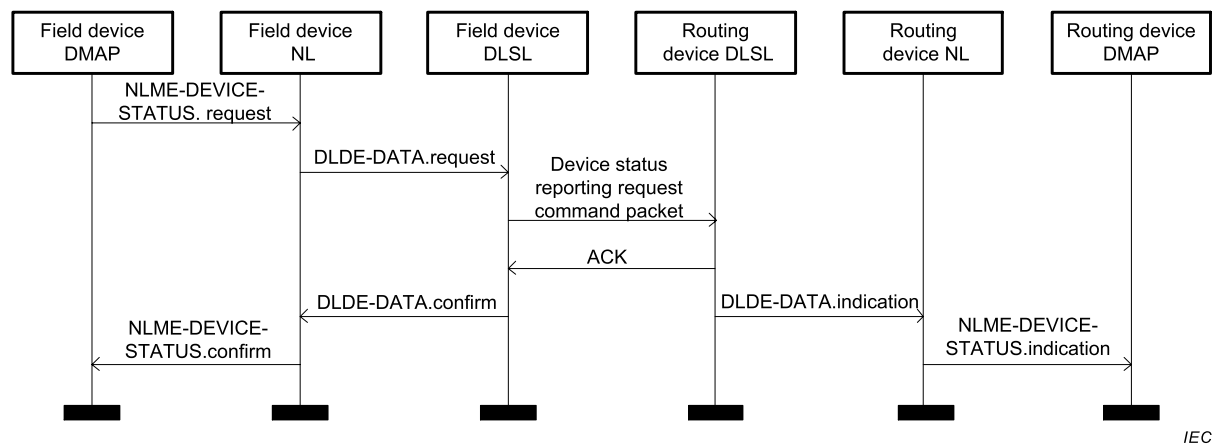
Le Tableau 113 spécifie les paramètres pour NLME-DEVICE-STATUS.confirm.

Tableau 113 – Paramètres de NLME-DEVICE-STATUS.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultat de la demande de rapport sur la condition des canaux: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

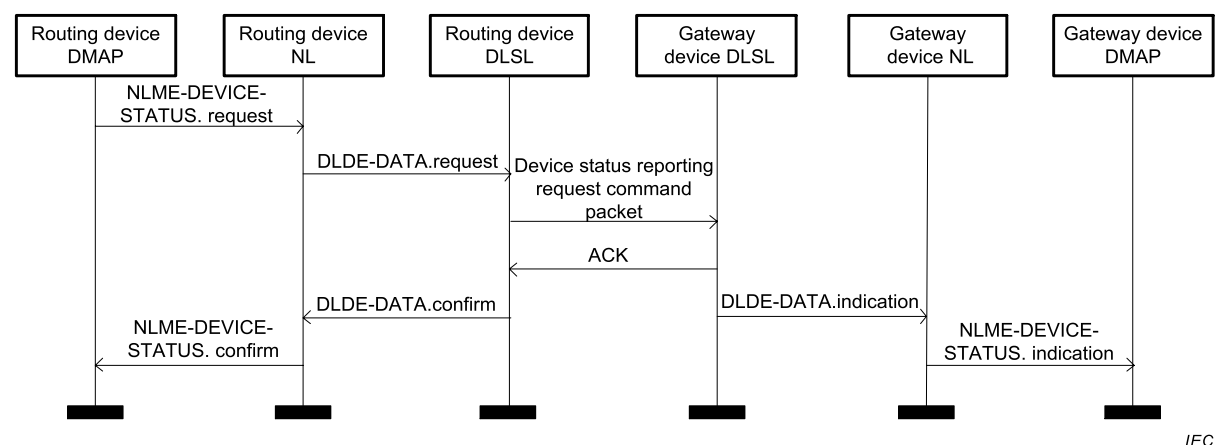
9.5.10.4 Séquence temporelle pour la production de rapport sur l'état des appareils

Le diagramme de séquence temporelle pour les informations sur l'état des appareils est représenté à la Figure 66 et à la Figure 67.



Anglais	Français
Field device DMAP	DMAP de l'appareil de terrain
Field device DLSL	DLSL de l'appareil de terrain
Field device NL	NL de l'appareil de terrain
Routing device DLSL	DLSL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Device status reporting request command packet	Paquet de commande de demande de rapport sur l'état de l'appareil

Figure 66 – Processus de production de rapport sur l'état des appareils d'un appareil de terrain à un appareil de routage



IEC

Anglais	Français
Routing device DLSL	DLSL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Device status reporting request command packet	Paquet de commande de demande de rapport sur l'état de l'appareil

Figure 67 – Processus de production de rapport sur l'état des appareils d'un appareil de routage à un appareil de passerelle

9.5.11 Rapport sur la condition des canaux

9.5.11.1 NLME-CHANNEL-CONDITION.request

La primitive NLME-CHANNEL-CONDITION.request est utilisée pour rapporter la condition des canaux de communication à l'appareil de routage par un appareil de terrain ou à l'appareil de passerelle par un appareil de routage.

La sémantique de NLME-CHANNEL-CONDITION.request est décrite comme suit:

```

NLME-CHANNEL-CONDITION.request(
    DstAddr,
    ChannelCount,
    ChannelConditionInfo
)
  
```

Le Tableau 114 spécifie les paramètres pour NLME-CHANNEL-CONDITION.request.

Tableau 114 – Paramètres de NLME-CHANNEL-CONDITION.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination
ChannelCount	Unsigned8	0 à 255	Nombre total de canaux
ChannelConditionInfo	Structure ChanCon_Struct (voir Tableau 19)		Informations sur les attributs de condition des canaux

9.5.11.2 NLME-CHANNEL-CONDITION.indication

La primitive NLME-CHANNEL-CONDITION.indication est utilisée pour rapporter au DMAP la réception d'un paquet de commande de rapport sur la condition des canaux.

La sémantique de NLME-CHANNEL-CONDITION.indication est décrite comme suit:

NLME-CHANNEL-CONDITION.indication (

SrcAddr,
ChannelCount,
ChannelConditionInfo
)

Le Tableau 115 spécifie les paramètres pour NLME-CHANNEL-CONDITION.indication.

Tableau 115 – Paramètres de NLME-CHANNEL-CONDITION.indication

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Source address (adresse source)
ChannelCount	Unsigned8	0 à 255	Nombre total de canaux
ChannelConditionInfo	Structure ChanCon_Struct (voir Tableau 19)		Informations sur les attributs de condition des canaux

9.5.11.3 NLME-CHANNEL-CONDITION.confirm

La primitive NLME-CHANNEL-CONDITION.confirm est utilisée pour retourner les résultats de NLME-CHANNEL-CONDITION.request.

La sémantique de NLME-CHANNEL-CONDITION.confirm est décrite comme suit:

NLME-CHANNEL-CONDITION.confirm (

Statut
)

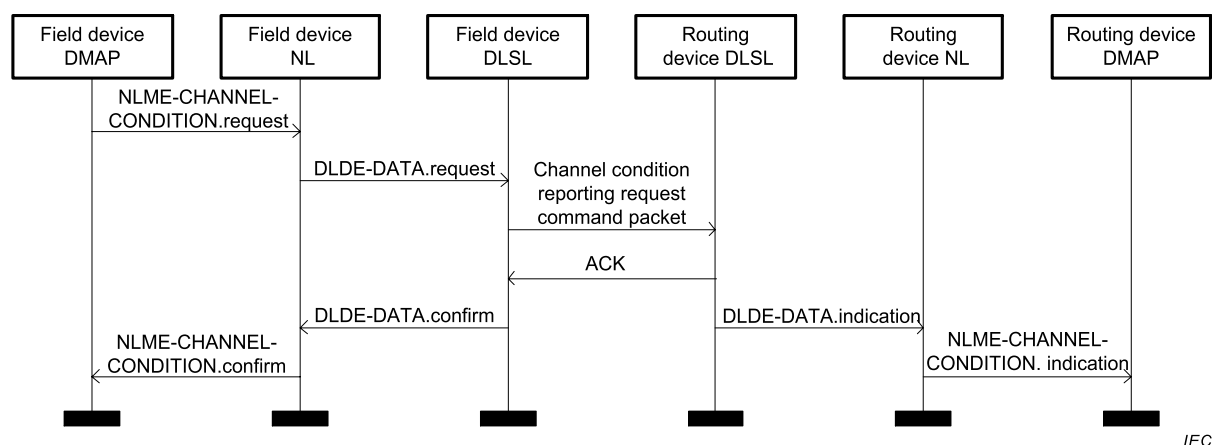
Le Tableau 116 spécifie les paramètres pour NLME-CHANNEL-CONDITION.confirm.

Tableau 116 – Paramètres de NLME-CHANNEL-CONDITION.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultat de la demande de rapport sur la condition des canaux: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.11.4 Séquence temporelle pour la production de rapport sur la condition des canaux

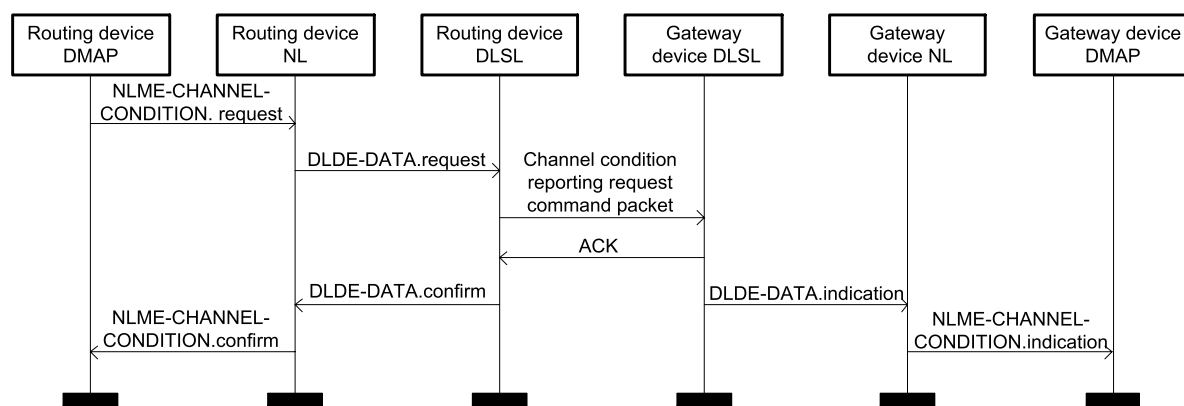
Le diagramme de séquence temporelle pour les informations sur la condition des canaux est représenté à la Figure 68 et à la Figure 69.



IEC

Anglais	Français
Field device DMAP	DMAP de l'appareil de terrain
Field device DLSL	DLSL de l'appareil de terrain
Field device NL	NL de l'appareil de terrain
Routing device DLSL	DLSL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Channel condition reporting request command packet	Paquet de commande de demande de rapport sur la condition des canaux

Figure 68 – Processus de production de rapport sur la condition des canaux d'un appareil de terrain à un appareil de routage



IEC

Anglais	Français
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Routing device DLSL	DLSL de l'appareil de routage
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Channel condition reporting request command packet	Paquet de commande de demande de rapport sur la condition des canaux

Figure 69 – Processus de production de rapport sur la condition des canaux d'un appareil de routage à un appareil de passerelle

9.5.12 Services de rapport sur les chemins défaillants

9.5.12.1 Généralités

Tous les appareils de routage résidant sur un chemin enregistrent la valeur de RetryCounter (voir Tableau 69) avec l'appareil de routage de prochain saut. Si la valeur RetryCounter de l'appareil de routage source ou d'un appareil de routage intermédiaire dépasse la valeur de MaxEtoERetry, l'appareil de routage source rapporte la défaillance du RouteID associé à la passerelle en utilisant le chemin redondant et l'appareil de routage intermédiaire rapporte la défaillance du RouteID associé à la passerelle en utilisant son chemin préconfiguré (voir 6.5.1 pour plus d'informations sur le chemin redondant).

9.5.12.2 NLME-PATH_FAILURE.request

La primitive NLME-PATH_FAILURE.request est utilisée pour rapporter les chemins défaillants à l'appareil de passerelle par les appareils de routage.

La sémantique de NLME-PATH_FAILURE.request est décrite comme suit:

```
NLME-PATH_FAILURE.request (
    SrcAddr,
    DstAddr,
    RouteID
)
```

Le Tableau 117 spécifie les paramètres pour NLME-PATH_FAILURE.request.

Tableau 117 – Paramètres de NLME-PATH_FAILURE.request

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse source 16 bits des paquets
DstAddr	Unsigned16	0 à 65 535	Adresse de destination 16 bits des paquets
RouteID	Unsigned16	0 à 65 535	Identificateur d'itinéraire du chemin défaillant

9.5.12.3 NLME-PATH_FAILURE.indication

La primitive NLME-PATH_FAILURE.indication est utilisée par la NL pour rapporter au DMAP que l'appareil a reçu avec succès un paquet de demande de rapport sur les chemins défaillants.

La sémantique de NLME-PATH_FAILURE.indication est décrite comme suit:

```
NLME-PATH_FAILURE.indication (
    SrcAddr,
    RouteID
)
```

Le Tableau 118 spécifie les paramètres pour NLME-LEAVE.response.

Tableau 118 – Paramètres de NLME-PATH_FAILURE.indication

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse source 16 bits des paquets
RouteID	Unsigned16	0 à 65 535	Identificateur d'itinéraire du chemin défaillant

9.5.12.4 NLME-PATH_FAILURE.confirm

La primitive NLME-PATH_FAILURE.confirm est utilisée pour retourner les résultats de NLME-PATH_FAILURE.request.

La sémantique de NLME-PATH_FAILURE.confirm est décrite comme suit:

NLME-PATH_FAILURE.confirm (
 Statut
)

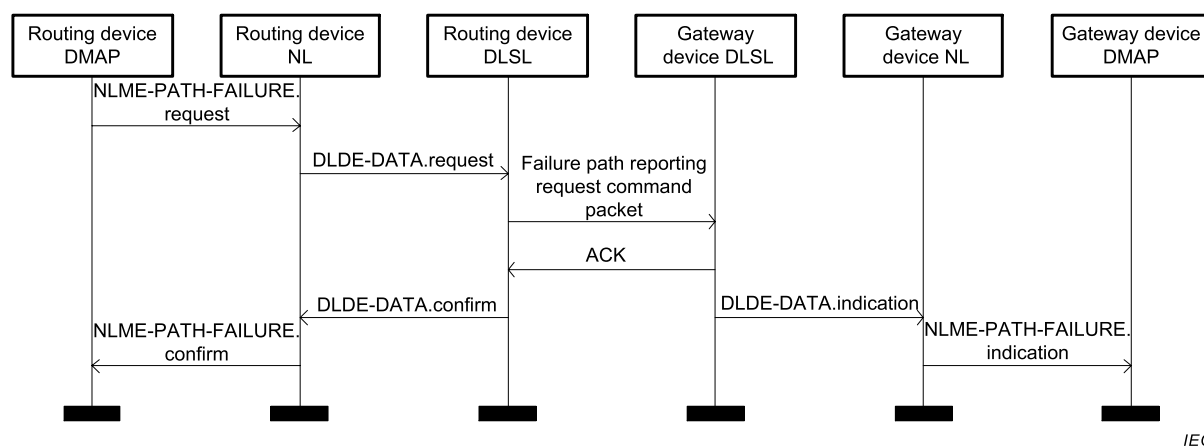
Le Tableau 119 spécifie les paramètres pour NLME-PATH_FAILURE.confirm.

Tableau 119 – Paramètres de NLME-PATH_FAILURE.confirm

Nom	Type de données	Plage valide	Description
Statut	Unsigned8	0 à 255	Résultat d'une NLME-PATH_FAILURE.request: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

9.5.12.5 Séquence temporelle de production de rapport sur les chemins défaillants

Le diagramme de séquence temporelle pour la production de rapport sur les chemins défaillants est représenté à la Figure 70.



IEC

Anglais	Français
Routing device DLSL	DLSL de l'appareil de routage
Routing device DMAP	DMAP de l'appareil de routage
Routing device NL	NL de l'appareil de routage
Gateway device DMAP	DMAP de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Failure path reporting request command packet	Paquet de commande de demande de rapport sur les chemins défaillants

Figure 70 – Processus de production de rapport sur les chemins défaillants

9.5.13 Services d'obtention des attributs de réseau

9.5.13.1 NLME-INFO_GET.request

La primitive NLME-INFO_GET.request est utilisée pour lire à distance les valeurs des attributs dans la base MIB.

La sémantique de NLME-INFO_GET.request est décrite comme suit:

```
NLME-INFO_GET.request (
    DstAddr,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```

Le Tableau 120 spécifie les paramètres pour NLME-INFO_GET.request.

Tableau 120 – Paramètres de NLME-INFO_GET.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination courte de 16 bits
AttributeID	Unsigned8	0 à 255	ID d'attribut dans la MIB
AttributeMemID	Unsigned8	0 à 255	Identificateur d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés La valeur 255 signifie qu'il convient de lire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour lire les attributs MIB structurés
Count	Unsigned8	0 à 255	Nombre de valeurs d'attribut ou de valeurs d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés; obtention de toutes les valeurs d'attributs à partir de FirstValueStorIndex si Count = 0.

9.5.13.2 NLME-INFO_GET.indication

La primitive NLME-INFO_GET.indication est utilisée pour informer le DMAP de la réception réussie d'un paquet de demande d'obtention d'attribut.

La sémantique de NLME-INFO_GET.indication est décrite comme suit:

```
NLME-INFO_GET.indication (
    SrcAddr,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```

Le Tableau 121 spécifie les paramètres pour NLME-INFO_GET.indication.

Tableau 121 – Paramètres de NLME-INFO_GET.indication

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse courte 16 bits de source
AttributeID	Unsigned8	0 à 255	Identificateur d'attribut dans la MIB
AttributeMemID	Unsigned8	0 à 255	Identificateur d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés La valeur 255 signifie qu'il convient de lire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour lire les attributs MIB structurés
Count	Unsigned8	0 à 255	Nombre de valeurs d'attribut ou de valeurs d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés; toutes les valeurs d'attribut à partir de FirstValueStorIndex si Count = 0.

9.5.13.3 NLME-INFO_GET.response

La primitive NLME-INFO_GET.response est utilisée pour répondre à NLME-INFO_GET.request.

La sémantique de NLME-INFO_GET.response est décrite comme suit:

NLME-INFO_GET.response (

DstAddr,
Status,
AttributeID,
AttributeMemID,
FirstValueStorIndex,
Count,
AttributeValue

)

Le Tableau 122 spécifie les paramètres pour NLME-INFO_GET.response.

Tableau 122 – Paramètres de NLME-INFO_GET.response

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination courte de 16 bits
Statut	Unsigned8	0 à 255	Résultat de la demande de lecture d'attribut: 0 = SUCCESS (succès) 1 = UNSUPPORTED_ATTRIBUTE (attribut non pris en charge) 2 = UNSUPPORTED_ATTRIBUTE_MEMBER (élément d'attribut non pris en charge) 3 = UNMATCHED_COUNT (nombre non conforme) Les autres valeurs sont réservées.
AttributeID	Unsigned8	0 à 255	ID d'attribut dans la MIB
AttributeMemID	Unsigned8	0 à 255	Identificateur d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés. La valeur 255 signifie qu'il convient de lire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour lire les attributs MIB structurés
Count	Unsigned8	0 à 255	Nombre de valeurs d'attribut ou de valeurs d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés; toutes les valeurs d'attribut à partir de FirstValueStorIndex si Count = 0.
AttributeValue	Octetstring		Valeur de l'attribut devant être lu

Si l'opération d'obtention des attributs a réussi, il convient que le paramètre Status soit égal à SUCCESS; si la base MIB n'a pas les attributs ou éléments d'attribut demandés, il convient que le paramètre Status soit égal à UNSUPPORTED_ATTRIBUTE ou UNSUPPORTED_ATTRIBUTE_MEMBER; sinon, si le nombre d'attributs n'est pas égal au nombre exigé, il convient que le paramètre Status soit égal à UNMATCHED_COUNT.

9.5.13.4 NLME-INFO_GET.confirm

La primitive NLME-INFO_GET.confirm est utilisée pour retourner le résultat de NLME-INFO_GET.request.

La sémantique de NLME-INFO_GET.confirm est décrite comme suit:

```
NLME-INFO_GET.confirm (
    SrcAddr,
    Status,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count,
    AttributeValue
)
```

Le Tableau 123 spécifie les paramètres pour NLME-INFO_GET.confirm.

Tableau 123 – Paramètres de NLME-INFO_GET.confirm

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse courte 16 bits de la source
Statut	Unsigned8	0 à 255	Résultat de la demande de lecture d'attribut: 0 = SUCCESS (succès) 1 = UNSUPPORTED_ATTRIBUTE (attribut non pris en charge) 2 = UNSUPPORTED_ATTRIBUTE_MEMBER (élément d'attribut non pris en charge) 3 = UNMATCHED_COUNT (nombre non conforme) Les autres valeurs sont réservées.
AttributeID	Unsigned8	0 à 255	ID d'attribut dans la MIB
AttributeMemID	Unsigned8	0 à 255	Identificateur d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés La valeur 255 signifie qu'il convient de lire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour lire les attributs MIB structurés
Count	Unsigned8	0 à 255	Nombre de valeurs d'attribut ou de valeurs d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés; toutes les valeurs d'attribut à partir de FirstValueStorIndex si Count = 0.
AttributeValue	Octetstring		Valeur de l'attribut devant être lu

9.5.14 Services d'établissement des attributs de réseau

9.5.14.1 NLME-INFO_SET.request

La primitive NLME-INFO_SET.request est utilisée par la passerelle pour modifier à distance les valeurs d'attribut MIB des appareils de routage ou des appareils de terrain.

La sémantique de NLME-INFO_SET.request est décrite comme suit:

```
NLME-INFO_SET.request (
    DstAddr,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count,
    AttributeValue
)
```

Le Tableau 124 spécifie les paramètres pour NLME-INFO_SET.request.

Tableau 124 – Paramètres de NLME-INFO_SET.request

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination courte de 16 bits
AttributeID	Unsigned8	0 à 255	ID d'attribut dans la MIB
AttributeMemID	Unsigned8	0 à 255	Identificateur d'élément d'attribut, qui est utilisé pour écrire les attributs MIB structurés La valeur 255 signifie qu'il convient d'écrire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour écrire les attributs MIB structurés
Count	Unsigned8	0 à 255	Nombre de valeurs d'attribut ou de valeurs d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés
AttributeValue	Octetstring		Valeur de l'attribut devant être écrit

9.5.14.2 NLME-INFO_SET.indication

La primitive NLME-INFO_SET.indication est utilisée pour informer le DMAP de la réception réussie d'un paquet de commande de demande d'établissement d'attribut.

La sémantique de NLME-INFO_SET.indication est décrite comme suit:

```
NLME-INFO_SET.indication (
    SrcAddr,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count,
    AttributeValue
)
```

Le Tableau 125 spécifie les paramètres pour NLME-INFO_SET.indication.

Tableau 125 – Paramètres de NLME-INFO_SET.indication

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse courte 16 bits de la source
AttributeID	Unsigned8	0 à 255	ID d'attribut dans la MIB
AttributeMemID	Unsigned8	0 à 255	Identificateur d'élément d'attribut, qui est utilisé pour écrire les attributs MIB structurés. La valeur 255 signifie qu'il convient d'écrire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour écrire les attributs MIB structurés
Count	Unsigned8	0 à 255	Nombre de valeurs d'attribut ou de valeurs d'élément d'attribut, qui est utilisé pour lire les attributs MIB structurés
AttributeValue	Octetstring		Valeur de l'attribut devant être écrit

9.5.14.3 NLME-INFO_SET.response

La primitive NLME-INFO_SET.response est utilisée pour répondre à NLME-INFO_SET.indication.

La sémantique de NLME-INFO_SET.response est décrite comme suit:

```
NLME-INFO_SET.response (
    DstAddr,
    Status,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```

Le Tableau 126 spécifie les paramètres pour NLME-INFO_SET.response.

Tableau 126 – Paramètres de NLME-SET.response

Nom	Type de données	Plage valide	Description
DstAddr	Unsigned16	0 à 65 535	Adresse de destination courte de 16 bits
Statut	Unsigned8	0 à 255	Résultat de la demande d'établissement d'attribut: 0 = SUCCESS (succès) 1 = UNSUPPORTED_ATTRIBUTE (attribut non pris en charge) 2 = UNSUPPORTED_ATTRIBUTE_MEMBER (élément d'attribut non pris en charge) 3 = UNMATCHED_COUNT (nombre non conforme) Les autres valeurs sont réservées.
AttributeMemID	Unsigned8	0 à 255	Identificateur d'élément d'attribut, qui est utilisé pour écrire les attributs MIB structurés. La valeur 255 signifie qu'il convient d'écrire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour écrire les attributs MIB structurés
AttributeValue	Octetstring		Valeur de l'attribut devant être écrit

Si l'opération d'établissement des attributs a réussi, il convient que le paramètre Status soit égal à SUCCESS; si la base MIB n'a pas les attributs ou éléments d'attribut demandés, il convient que le paramètre Status soit égal à UNSUPPORTED_ATTRIBUTE ou UNSUPPORTED_ATTRIBUTE_MEMBER; sinon, si le nombre d'attributs n'est pas égal au nombre exigé, il convient que le paramètre Status soit égal à UNMATCHED_COUNT.

9.5.14.4 NLME-INFO_SET.confirm

La primitive NLME-INFO_SET.confirm est utilisée pour retourner les résultats de NLME-INFO_SET.request.

La sémantique de NLME-INFO_SET.confirm est décrite comme suit:

```
NLME-INFO_SET.confirm (
    SrcAddr,
    Status,
    AttributeID,
    AttributeMemID,
    FirstValueStorIndex,
    Count
)
```

Le Tableau 127 spécifie les paramètres pour NLME-INFO_SET.confirm.

Tableau 127 – Paramètres de NLME-SET.confirm

Nom	Type de données	Plage valide	Description
SrcAddr	Unsigned16	0 à 65 535	Adresse courte 16 bits de la source
Statut	Unsigned8	0 à 255	Résultat de la demande d'établissement d'attribut: 0 = SUCCESS (succès) 1 = UNSUPPORTED_ATTRIBUTE (attribut non pris en charge) 2 = UNSUPPORTED_ATTRIBUTE_MEMBER (élément d'attribut non pris en charge) 3 = UNMATCHED_COUNT (nombre non conforme) Les autres valeurs sont réservées.
AttributeMemID	Unsigned8	0 à 255	Identificateur d'élément d'attribut, qui est utilisé pour écrire les attributs MIB structurés. La valeur 255 signifie qu'il convient d'écrire tous les attributs.
FirstValueStorIndex	Unsigned16	0 à 65 535	Premier indice de stockage des multiples valeurs d'attribut, qui est utilisé pour écrire les attributs MIB structurés
AttributeValue	Octetstring		Valeur de l'attribut devant être écrit

9.6 Formats de paquets de couche réseau

9.6.1 Format commun des paquets

Le format de paquet de la NL est indiqué au Tableau 128.

Tableau 128 – Format commun des paquets de couche réseau

	Format commun des paquets de couche réseau										
	Network layer header (en-tête de couche réseau)										Network layer payload (charge utile de couche réseau)
Longueur en octet(s)	1	2	2	2	4	1	1	0/1	0/1	1	Longueur variable

Champ name	Contrôle	Destination address (adresse de destination)	Source address (adresse source)	Route-ID (ID d'itinéraire)	Time-stamp (référence temporelle)	Priorité	Sequence Number (numéro séquentiel)	Number of fragments (nombre de fragments)	Fragment sequence number (numéro séquentiel de fragment)	Payload length (longueur de charge utile)	Network layer payload (charge utile de couche réseau)
		Routage									

Le format du champ Control (contrôle) est indiqué au Tableau 129.

Tableau 129 – Format du champ Control (contrôle)

	Format du champ Control (contrôle)				
Longueur en bit(s)	2	1	1	1	4
Nom de sous-champ	Packet type (type de paquet)	Fragment flag (fanion fragment)	P/S flag (fanion P/S)	Authentication flag (fanion d'authentification)	Réservé

Le champ NL header (en-tête de couche réseau) comporte les sous-champs suivants:

- a) le sous-champ Control (contrôle), qui inclut:
 - Packet type (type de paquet): ce sous-champ a une longueur de 2 bits; la valeur 0 indique un paquet de données, la valeur 1 indique un paquet d'agrégation, la valeur 2 indique un paquet de commande et les autres valeurs sont réservées;
 - Fragment flag (fanion fragment): ce sous-champ a une longueur de 1 bit et est utilisé pour indiquer si ce paquet est un paquet de fragment; la valeur 0 indique "pas un fragment" tandis que la valeur 1 indique "fragment";
 - P/S flag (fanion P/S): ce sous-champ a une longueur de 1 bit et est utilisé pour indiquer si les données de ce paquet sont de type P/S; la valeur 0 indique "pas de type P/S" tandis que la valeur 1 indique "type P/S";
 - Reserved (réservé): ce sous-champ a une longueur de 4 bits et est utilisé à des fins d'extension.
- b) le sous-champ Routing (routage), qui inclut:
 - Destination address (adresse de destination): adresse de destination finale d'un paquet (16 bits);
 - Source address (adresse source): adresse de provenance d'un paquet (16 bits);
 - RouteID: identificateur unique du chemin (16 bits);
- c) Timestamp (référence temporelle): ce sous-champ a une longueur de 4 octets et est libellé en secondes;
- d) Priority (priorité): ce sous-champ a une longueur de 1 octet et indique la priorité d'un paquet;
- e) Sequence number (numéro séquentiel): ce sous-champ a une longueur de 1 octet et indique le numéro séquentiel du paquet NL;
- f) Number of fragments (nombre de fragments): ce sous-champ a une longueur de 0 ou 1 octet; il est utilisé pour indiquer le nombre de fragments; si le paquet est un paquet de fragment, ce sous-champ a une longueur de 1 octet et sa valeur est valide; sinon, ce sous-champ a une longueur de 0 octet.
- g) Fragment sequence number (numéro séquentiel de fragment): ce sous-champ est utilisé pour indiquer le numéro séquentiel de fragment du paquet de fragmentation. Si le paquet est un paquet de fragmentation, ce champ a une longueur de 1 octet et est valide; sinon, il n'est pas valide.
- h) Payload length (longueur de charge utile): ce champ a une longueur de 1 octet et est utilisé pour indiquer la longueur de charge utile de la NL;

- i) Network layer payload (charge utile de couche réseau): ce champ a une longueur variable et est utilisé pour remplir les données de la NL.

9.6.2 Format des paquets de données

Le format des paquets de données est indiqué au Tableau 130.

Tableau 130 – Format commun des paquets de données de couche réseau

	Format commun des paquets de couche réseau										
	Network layer header (en-tête de couche réseau)										Network layer payload (charge utile de couche réseau)
Longueur en octet(s)	1	2	2	2	4	1	1	0/1	0/1	1	Longueur variable
Nom de champ	Control (contrôle)	Destination address (adresse de destination)	Source address (adresse source)	RouteID	Time-stamp (référence temporelle)	Priorité	Sequence Number (numéro séquentiel)	Number of fragments (nombre de fragments)	Fragment sequence number (numéro séquentiel de fragment)	Payload length (longueur de charge utile)	Network layer payload (charge utile de couche réseau)
		Routing (routage)									

La valeur du type de paquet dans le champ Control (contrôle) de l'en-tête de couche réseau = 0, ce qui indique un paquet de données.

Les définitions de l'ensemble des sous-champs sont identiques à celles données dans le Tableau 128.

9.6.3 Format de paquet agrégé

Le format de paquet agrégé est décrit dans le Tableau 131.

Tableau 131 – Format de paquet agrégé

	Format de paquet agrégé								
	Network layer header (en-tête de couche réseau)	Network layer payload (charge utile de couche réseau)							
Longueur en octet(s)	14/16	1	2	1	Longueur variable	...	2	1	Longueur variable
Nom de champ	En-tête de couche réseau	Aggregated number (nombre de paquets agrégés)	Source address 1 (adresse source 1)	Data length 1 (longueur des données 1)	Data 1 (données 1)	...	Source address n (adresse source n)	Data length n (longueur des données n)	Data n (données n)
			La première donnée agrégée			...	La n ^{ème} donnée agrégée		

La valeur du type de paquet dans le champ Control (contrôle) de l'en-tête de couche réseau = 1, ce qui indique un paquet d'agrégation.

Le paquet agrégé comporte les champs ou sous-champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 127;
- Aggregated number (nombre de paquets agrégés): ce sous-champ est utilisé pour enregistrer le nombre de paquets qui sont agrégés;
- First aggregated data (première donnée agrégée): ce sous-champ est utilisé pour remplir la première donnée agrégée, ce qui inclut:
 - Source address 1 (adresse source 1): ce sous-champ a une longueur de 2 octets et indique l'adresse 16 bits de la première donnée agrégée;
 - Data length 1 (longueur de données 1): ce champ a une longueur de 1 octet et est utilisé pour indiquer la première donnée agrégée;
 - Data 1 (donnée 1): ce champ a une longueur variable et est utilisé pour remplir la première donnée agrégée;
- nth aggregated data (n^{ème} donnée agrégée): ce sous-champ est utilisé pour remplir la n^{ème} donnée agrégée, qui est identique à la première donnée agrégée.

9.6.4 Format de paquet de commande

9.6.4.1 Format commun de paquet de commande

Les paquets de commande NL encapsulent des commandes NL pour accomplir un certain nombre de fonctions de gestion. Le format du paquet de commande est décrit au Tableau 132.

Tableau 132 – Format commun de paquet de commande NL

	Format commun des paquets de couche réseau										
	Network layer header (en-tête de couche réseau)										Network layer payload (charge utile de couche réseau)
Longueur en octet(s)	1	2	2	2	4	1	1	0/1	0/1	1	Longueur variable
Nom de champ	Control (contrôle)	Destination address (adresse de destination)	Source address (adresse source)	Routing (routage)	Timestamp (référence temporelle)	Priorité	Sequence Number (numéro séquentiel)	Number of fragment (nombre de fragments)	Fragment sequence number (numéro séquentiel de fragment)	Payload length (longueur de charge utile)	Network layer payload (charge utile de couche réseau)

La valeur du type de paquet dans le champ Control (contrôle) de l'en-tête de couche réseau = 2, ce qui indique un paquet de commande.

Le paquet de données comporte les champs ou sous-champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Network layer payload (charge utile de couche réseau) comporte les sous-champs suivants:
 - Command packet identifier (identificateur de paquet de commande): ce sous-champ a une longueur de 1 octet et est utilisé pour indiquer l'identificateur du paquet de commande NL (voir Tableau 133);
 - Command packet payload (charge utile de paquet de commande): ce champ a une longueur variable et est utilisé pour remplir la charge utile du paquet de commande NL.

Les paquets de commandes NL sont répertoriés au Tableau 133.

Tableau 133 – Paquet de commande de couche réseau

Identificateur de paquet de commande	Command	Utilisateur
0	Demande de rattachement	Appareil de routage
1	Réponse de rattachement	Appareil de passerelle
2	Demande de rapport sur l'état des communications	Appareil de routage
3	Demande de départ	Appareil de routage/Appareil de passerelle
4	Réponse de départ	Appareil de passerelle/Appareil de routage
5	Demande de rapport sur l'élément de groupe	Appareil de routage
6	Réponse de rapport sur l'élément de groupe	Appareil de passerelle
7	Demande de rapport sur les informations de voisins	Appareil de routage
8	Demande d'ajout d'itinéraire	Appareil de passerelle
9	Réponse d'ajout d'itinéraire	Appareil de routage
10	Demande de mise à jour d'itinéraire	Appareil de passerelle

Identificateur de paquet de commande	Command	Utilisateur
11	Réponse de mise à jour d'itinéraire	Appareil de routage
12	Demande de suppression d'itinéraire	Appareil de passerelle
13	Réponse de suppression d'itinéraire	Appareil de routage
14	Demande d'ajout de liaison	Appareil de passerelle/Appareil de routage
15	Réponse d'ajout de liaison	Appareil de routage/Appareil de terrain
16	Demande de mise à jour de liaison	Appareil de passerelle/Appareil de routage
17	Réponse de mise à jour de liaison	Appareil de routage/Appareil de terrain
18	Demande de libération de liaison	Appareil de passerelle/Appareil de routage
19	Réponse de libération de liaison	Appareil de routage/Appareil de terrain
20	Demande d'ajout de supertrame	Appareil de passerelle/Appareil de routage
21	Réponse d'ajout de supertrame	Appareil de routage/Appareil de terrain
22	Demande de mise à jour de supertrame	Appareil de passerelle/Appareil de routage
23	Réponse de mise à jour de supertrame	Appareil de routage/Appareil de terrain
24	Demande de libération de supertrame	Appareil de passerelle/Appareil de routage
25	Réponse de libération de supertrame	Appareil de routage/Appareil de terrain
26	Demande de rapport sur la condition des appareils	Appareil de terrain/Appareil de routage
27	Demande de rapport sur l'état des canaux	Appareil de terrain/Appareil de routage
28	Demande de rapport sur les chemins défaillants	Appareil de routage
29	Demande d'obtention d'attribut	Appareil de passerelle/Appareil de routage
30	Réponse d'obtention d'attribut	Appareil de routage/Appareil de terrain
31	Demande d'établissement d'attribut	Appareil de passerelle/Appareil de routage
32	Réponse d'établissement d'attribut	Appareil de routage/Appareil de terrain
33 à 255	Réservé	Réservé

Les résultats d'exécution des commandes sont indiqués au Tableau 134.

Tableau 134 – Résultats d'exécution des commandes

Résultat de la mise en œuvre de la commande	Identificateur	Description
SUCCESS (succès)	0	L'exécution de la commande réussit.
FAILURE (échec)	1	L'exécution de la commande échoue.

9.6.4.2 Demande de rattachement et réponse

Le paquet de demande de rattachement est utilisé par un appareil de routage pour transmettre la demande de rattachement. Le format du paquet de demande de rattachement est décrit au Tableau 135.

Tableau 135 – Format du paquet de demande de rattachement

	Format du paquet de demande de rattachement				
Longueur en octet(s)	14/16	1	8	0/4	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 0 (ID de commande = 0)	Physical address of the new device (adresse physique du nouvel appareil)	Security material (renseignements de sécurité)	Device type (type d'appareil)

Le paquet de demande de rattachement comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 0;
- Physical address of the new device (adresse physique du nouvel appareil): ce champ est utilisé pour indiquer l'adresse physique 64 bits de l'appareil qui se rattache au réseau;
- Security material (renseignements de sécurité): ce champ a une longueur de 0 ou 4 octets; si le fanion d'authentification dans l'en-tête NL est égal à 0, les renseignements de sécurité font 0 octet de long; sinon, ils font 4 octets de long (voir Article 11 pour les informations détaillées);
- Device type (type d'appareil): ce champ a une longueur de 1 octet et est utilisé pour indiquer le type de l'appareil se rattachant. La valeur 0 indique l'appareil de passerelle, la valeur 1 indique un appareil de routage, la valeur 2 indique un appareil de terrain et la valeur 3 indique un appareil tenu à la main; sinon, ce champ est réservé.

Le paquet de réponse de rattachement est utilisé pour retourner le résultat de la demande de rattachement. Le format du paquet de réponse de rattachement est décrit au Tableau 136.

Tableau 136 – Format du paquet de réponse de rattachement

	Format du paquet de réponse de rattachement				
Longueur en octet(s)	14/16	1	1	8	2
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 1 (ID de commande = 1)	Execution result (résultat d'exécution)	Physical address of the new device (adresse physique du nouvel appareil)	Short address of the new device (adresse courte du nouvel appareil)

Le paquet de réponse de rattachement comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 1;
- Execution result (résultat d'exécution): ce champ a une longueur de 1 octet. La valeur 0 indique que le processus de rattachement est SUCCESS; sinon, la valeur 1 indique que le processus de rattachement est FAILURE (voir Tableau 134);
- Physical address of the new device (adresse physique du nouvel appareil): ce champ est utilisé pour indiquer l'adresse physique 64 bits de l'appareil qui se rattache au réseau;

- e) Short address of the new device (adresse courte du nouvel appareil): ce champ a une longueur de 2 octets. Si la valeur du champ Execution (exécution) est 0, ce champ est valide et la valeur correspond à l'adresse courte 16 bits nouvellement allouée de l'appareil se rattachant; sinon, ce champ n'est pas valide.

9.6.4.3 Demande de rapport sur l'état des communications

Le paquet de demande de rapport sur l'état des communications est utilisé par un appareil de routage pour transmettre la demande de rapport sur l'état des communications. Le format du paquet de demande de rapport sur l'état des communications est décrit au Tableau 137.

Tableau 137 – Format du paquet de demande de rapport sur l'état des communications

	Format du paquet de demande de rapport sur l'état des communications				
Longueur en octet(s)	14/16	1	8	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 2 (ID de commande = 32)	Physical address of the new device (adresse physique du nouvel appareil)	Device type (type d'appareil)	Statut

Le paquet de demande de rapport sur l'état des communications comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 2;
- Physical address of the new device (adresse physique du nouvel appareil): ce champ est utilisé pour indiquer l'adresse physique 64 bits de l'appareil qui vient de se rattacher au réseau;
- Device type (type d'appareil): ce champ a une longueur de 1 octet et est utilisé pour indiquer le type de l'appareil nouvellement rattaché. La valeur 0 indique l'appareil de passerelle, la valeur 1 indique un appareil de routage, la valeur 2 indique un appareil de terrain et la valeur 3 indique un appareil tenu à la main; sinon, ce champ est réservé;
- Status (état): ce champ a une longueur de 1 octet et est utilisé pour indiquer le résultat du processus de rattachement; la valeur 0 indique que le processus de rattachement a réussi et la valeur 1 indique que le processus de rattachement a échoué.

9.6.4.4 Demande de départ et réponse

Le paquet de demande de départ est utilisé par un appareil de routage pour demander le départ de l'appareil de passerelle ou par l'appareil de passerelle pour demander à un appareil de routage de quitter le réseau. Le format du paquet de demande de départ est décrit au Tableau 138.

Tableau 138 – Format du paquet de demande de départ

	Format du paquet de demande de départ		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 3 (ID de commande = 3)	Leaving reason (raison du départ)

Le paquet de demande de départ comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 3;
- c) Leaving reason (raison du départ): ce champ a une longueur de 1 octet, ce qui correspond à la valeur valide (voir Tableau 139).

Tableau 139 – Valeur du champ Leaving reason (raison du départ)

Valeur	Description
0	Réservé
1	Départ passif d'un appareil de routage ou d'un appareil de terrain
2	Départ actif d'un appareil de routage
3 à 255	Réservé

Le paquet de réponse de départ est utilisé pour retourner les résultats d'exécution. Le format du paquet de réponse de départ est décrit au Tableau 140.

Tableau 140 – Format du paquet de réponse de départ

	Format du paquet de réponse de départ		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 4 (ID de commande = 4)	Execution result (résultat d'exécution)

Le paquet de réponse de départ comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 4;
- c) Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de départ. Si le processus de départ réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.5 Demande de rapport sur l'élément de groupe et réponse

Le paquet de demande de rapport sur l'élément de groupe est utilisé par les appareils de routage pour rapporter les informations d'élément de groupe à l'appareil de passerelle. Le format du paquet de demande de rapport sur l'élément de groupe est décrit au Tableau 141.

Tableau 141 – Format du paquet de demande de rapport sur l'élément de groupe

	Format de paquet de demande de rapport sur l'élément de groupe			
Longueur en octet(s)	14/16	1	1	2
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 5 (ID de commande = 32)	Cluster member modification flag (fanion de modification d'élément de groupe)	Cluster member address (adresse d'élément de groupe)

Le paquet de demande de rapport sur l'élément de groupe comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 5;
- c) Cluster member modification flag (fanion de modification d'élément de groupe): ce champ a une longueur de 1 octet et indique les types de modification; la valeur 0 indique l'action d'ajout, la valeur 1 indique l'action de suppression; sinon, ce champ est réservé;
- d) Cluster member address (adresse d'élément de groupe): ce champ a une longueur de 2 octets et indique l'adresse 16 bits de l'élément de groupe modifié.

Le paquet de réponse de rapport sur l'élément de groupe est utilisé pour retourner les résultats d'exécution de la commande de demande de rapport sur l'élément de groupe. Le format du paquet de réponse de rapport sur l'élément de groupe est décrit au Tableau 142.

Tableau 142 – Format du paquet de réponse de rapport sur l'élément de groupe

	Format de paquet de réponse de rapport sur l'élément de groupe		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 6 (ID de commande = 32)	Execution result (résultat d'exécution)

Le paquet de réponse de rapport sur l'élément de groupe comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 6;
- c) Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de rapport sur l'élément de groupe. Si le processus de rapport réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.6 Demande de rapport sur les informations de voisins

Le paquet de demande de rapport sur les informations de voisins est utilisé par les appareils de routage pour rapporter ses informations de voisins à un saut au gestionnaire de réseau NM. Le format du paquet de demande de rapport sur les informations de voisins est décrit au Tableau 143.

Tableau 143 – Format du paquet de demande de rapport sur les informations de voisins

	Format de paquet de demande de rapport sur les informations de voisins			
Longueur en octet(s)	14/16	1	1	Longueur variable
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 7 (ID de commande = 32)	Number of neighbours (nombre de voisins)	Items of neighbour table (éléments de la table des voisins)

Le paquet de demande de rapport sur les informations de voisins comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 7;
- c) Number of neighbours (nombre de voisins): ce champ a une longueur de 1 octet et indique le nombre de voisins rapportés;

- d) Items of neighbour table (éléments de la table des voisins): ce champ a une longueur variable; la structure des éléments de la table des voisins est décrite au Tableau 15.

9.6.4.7 Demande d'ajout d'itinéraire et réponse

Le paquet de demande d'ajout d'itinéraire est généré par le NM et est envoyé à l'appareil de routage de destination pour ajouter un nouvel enregistrement de routage dans sa table de routage.

Le format du paquet de demande d'ajout d'itinéraire est décrit au Tableau 144.

Tableau 144 – Format du paquet de demande d'ajout d'itinéraire

	Format de paquet de demande d'ajout d'itinéraire		
Longueur en octet(s)	14/16	1	9
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 8 (ID de commande = 8)	A record of routing table (un enregistrement de la table de routage)

Le paquet de demande d'ajout d'itinéraire comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 8;
- A record of routing table (un enregistrement de la table de routage): ce champ a une longueur de 9 octets; les informations détaillées sont données au Tableau 15.

Le paquet de réponse d'ajout d'itinéraire est utilisé pour retourner les résultats d'exécution de la commande de demande d'ajout d'itinéraire.

Le format du paquet de réponse d'ajout d'itinéraire est décrit au Tableau 145.

Tableau 145 – Format du paquet de réponse d'ajout d'itinéraire

	Format de paquet de réponse d'ajout d'itinéraire		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 9 (ID de commande = 9)	Execution result (résultat d'exécution)

Le paquet de réponse d'ajout d'itinéraire comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 9;
- Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de réponse d'ajout d'itinéraire. Si le processus de réponse réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.8 Demande de mise à jour d'itinéraire et réponse

Le paquet de demande de mise à jour d'itinéraire est généré par le NM et est envoyé à l'appareil de routage de destination pour modifier un enregistrement de table de routage dans sa table de routage.

Le format du paquet de demande de mise à jour d'itinéraire est décrit au Tableau 146.

Tableau 146 – Format du paquet de demande de mise à jour d'itinéraire

	Format de paquet de demande de mise à jour d'itinéraire		
Longueur en octet(s)	14/16	1	9
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 10 (ID de commande = 10)	A record of routing table (un enregistrement de la table de routage)

Le paquet de demande de mise à jour d'itinéraire comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 10;
- A record of routing table (un enregistrement de la table de routage): ce champ a une longueur de 9 octets; les informations détaillées sont données au Tableau 15.

Le paquet de réponse de mise à jour d'itinéraire est utilisé pour retourner les résultats d'exécution de la commande de demande de mise à jour d'itinéraire.

Le format du paquet de réponse de mise à jour d'itinéraire est décrit au Tableau 147.

Tableau 147 – Format du paquet de réponse de mise à jour d'itinéraire

	Format de paquet de réponse de mise à jour d'itinéraire		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 11 (ID de commande = 11)	Execution result (résultat d'exécution)

Le paquet de réponse de mise à jour d'itinéraire comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 11;
- Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de réponse de mise à jour d'itinéraire. Si le processus de réponse réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.9 Demande de suppression d'itinéraire et réponse

Le paquet de demande de suppression d'itinéraire est généré par le NM et est envoyé à l'appareil de routage de destination pour supprimer un enregistrement de routage de sa table de routage.

Le format du paquet de demande de suppression d'itinéraire est décrit au Tableau 148.

Tableau 148 – Format du paquet de demande de suppression d'itinéraire

	Format de paquet de demande de suppression d'itinéraire		
Longueur en octet(s)	14/16	1	2
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 12 (ID de commande = 12)	ID d'itinéraire

Le paquet de demande de mise à jour d'itinéraire comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 12;
- c) Route ID (ID d'itinéraire): ce champ a une longueur de 2 octets et indique l'identificateur de l'itinéraire supprimé.

Le paquet de réponse de suppression d'itinéraire est utilisé pour retourner les résultats d'exécution de la commande de demande de suppression d'itinéraire.

Le format du paquet de réponse de suppression d'itinéraire est décrit au Tableau 149.

Tableau 149 – Format du paquet de réponse de suppression d'itinéraire

	Format de paquet de réponse de mise à jour d'itinéraire		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 13 (ID de commande = 13)	Execution result (résultat d'exécution)

Le paquet de réponse de suppression d'itinéraire comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 13;
- c) Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de réponse de suppression d'itinéraire. Si le processus de réponse réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.10 Demande d'ajout de liaison et réponse

Le paquet de demande d'ajout de liaison est utilisé par le NM pour ajouter une ou plusieurs nouvelles liaisons à l'appareil de routage et est également utilisé par l'appareil de routage pour ajouter une ou plusieurs nouvelles liaisons à un appareil de terrain. Après avoir reçu ce paquet de commande, il convient que l'appareil de routage ou l'appareil de terrain ajoute un enregistrement à sa table de liaisons.

Le format du paquet de demande d'ajout de liaison est décrit au Tableau 150.

Tableau 150 – Format du paquet de demande d'ajout de liaison

	Format de paquet de demande d'ajout de liaison					
Longueur en octet(s)	14/16	1	2	12	...	12
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 14 (ID de commande = 14)	Number of links (nombre de liaisons)	Link table item 1 (élément 1 de la table de liaisons)	...	Link table item N (élément N de la table de liaisons)

Le paquet de demande d'ajout de liaison comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;

- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 14;
- c) Number of links (nombre de liaisons): ce champ a une longueur de 2 octets et indique le nombre de liaisons ajoutées;
- d) Link table item 1 to N (élément 1 à N, où N = nombre de liaisons) de la table de liaisons: chacun de ces éléments de la table de liaisons a une longueur de 12 octets; ce champ indique les informations détaillées de la liaison ajoutée. La structure de l'élément de table de liaisons est décrite au Tableau 17.

Le paquet de réponse d'ajout de liaison est utilisé pour retourner les résultats d'exécution de l'ajout de liaison. Le format du paquet de réponse d'ajout de liaison est décrit au Tableau 151.

Tableau 151 – Format du paquet de réponse d'ajout de liaison

	Format de paquet de réponse d'ajout de liaison		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 15 (ID de commande = 15)	Execution result (résultat d'exécution)

Le paquet de réponse d'ajout de liaison comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 15;
- c) Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de réponse d'ajout de liaison. Si le processus de réponse réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.11 Demande de mise à jour de liaison et réponse

Le paquet de demande de mise à jour de liaison est utilisé par le NM pour mettre à jour une ou plusieurs liaisons existantes d'un appareil de routage et il est également utilisé par l'appareil de routage pour mettre à jour une ou plusieurs liaisons existantes à un appareil de terrain. Après avoir reçu ce paquet de commande, il convient que l'appareil de routage ou l'appareil de terrain mette à jour un enregistrement dans sa table de liaisons.

Le format du paquet de demande de mise à jour de liaison est décrit au Tableau 152.

Tableau 152 – Format du paquet de demande de mise à jour de liaison

	Format de paquet de demande de mise à jour de liaison					
Longueur en octet(s)	14/16	1	2	12	...	12
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 16 (ID de commande = 16)	Number of links (nombre de liaisons)	Link table item 1 (élément 1 de la table de liaisons)	...	Link table item N (élément N de la table de liaisons)

Le paquet de demande de mise à jour de liaison comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 16;

- c) Number of links (nombre de liaisons): ce champ a une longueur de 2 octets et indique le nombre de liaisons mises à jour;
- d) Link table item 1 to N (élément 1 à N, où N = nombre de liaisons) de la table de liaisons: chacun de ces éléments de la table de liaisons a une longueur de 12 octets; ce champ indique les informations détaillées des liaisons ajoutées. La structure de l'élément de table de liaisons est décrite au Tableau 17.

Le paquet de réponse de mise à jour de liaison est utilisé pour retourner les résultats d'exécution de la mise à jour de liaison. Le format du paquet de réponse de mise à jour de liaison est décrit au Tableau 153.

Tableau 153 – Format du paquet de réponse de mise à jour de liaison

	Format de paquet de réponse de mise à jour d'itinéraire		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 17 (ID de commande = 17)	Execution result (résultat d'exécution)

Le paquet de réponse de mise à jour de liaison comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 17;
- c) Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de réponse de mise à jour de liaison. Si le processus de réponse réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.12 Demande de libération de liaison et réponse

Le paquet de demande de libération de liaison est utilisé par le NM pour libérer une ou plusieurs liaisons existantes d'un appareil de routage et est également utilisé par l'appareil de routage pour libérer une ou plusieurs liaisons existantes à un appareil de terrain. Après avoir reçu ce paquet de commande, il convient que l'appareil de routage ou l'appareil de terrain libère un enregistrement dans sa table de liaisons.

Le format du paquet de demande de libération de liaison est décrit au Tableau 154.

Tableau 154 – Format du paquet de demande de libération de liaison

	Format de paquet de demande de libération de liaison					
Longueur en octet(s)	14/16	1	1	2	...	2
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 18 (ID de commande = 18)	Number of links (nombre de liaisons)	Link ID 1 (ID de liaison 1)	...	Link ID N (ID de liaison N)

Le paquet de demande de libération de liaison comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 18;
- c) Number of links (nombre de liaisons): ce champ a une longueur de 2 octets et indique le nombre de liaisons libérées;

- d) Link ID 1 to N (ID de liaison 1 à N, où N = nombre de liaisons) de la table de liaisons: chacun de ces ID de liaison a une longueur de 2 octets, ce qui correspond aux identificateurs des liaisons libérées.

Le paquet de réponse de libération de liaison est utilisé pour retourner les résultats d'exécution de la libération de liaison. Le format du paquet de réponse de libération de liaison est décrit au Tableau 155.

Tableau 155 – Format du paquet de réponse de libération de liaison

	Format de paquet de réponse de libération de liaison		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 19 (ID de commande = 19)	Execution result (résultat d'exécution)

Le paquet de réponse de libération de liaison comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 19;
- Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de réponse de libération de liaison. Si le processus de réponse réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.13 Demande d'ajout de supertrame et réponse

Le paquet de demande d'ajout de supertrame est utilisé par le NM pour ajouter une nouvelle supertrame à un appareil de routage et il est également utilisé par l'appareil de routage pour ajouter une nouvelle supertrame à un appareil de terrain. Après avoir reçu ce paquet de commande, il convient que l'appareil de routage ou l'appareil de terrain ajoute un enregistrement dans sa table de supertrames.

Le format du paquet de demande d'ajout de supertrame est décrit au Tableau 156.

Tableau 156 – Format du paquet de demande d'ajout de supertrame

	Format de paquet de demande d'ajout de supertrame		
Longueur en octet(s)	14/16	1	12
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 20 (ID de commande = 20)	Superframe table item (élément de table de supertrames)

Le paquet de demande d'ajout de supertrame comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 20;
- Superframe table item (élément de table de supertrames): ce champ a une longueur de 12 octets et indique les informations détaillées de la supertrame ajoutée (voir Tableau 16).

Le paquet de réponse d'ajout de supertrame est utilisé pour retourner les résultats d'exécution de l'ajout de supertrame. Le format du paquet de réponse d'ajout de supertrame est décrit au Tableau 157.

Tableau 157 – Format du paquet de réponse d'ajout de supertrame

	Format de paquet de réponse d'ajout de supertrame		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 21 (ID de commande = 21)	Execution result (résultat d'exécution)

Le paquet de réponse d'ajout de supertrame comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 21;
- Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de réponse d'ajout de supertrame. Si le processus de réponse réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.14 Demande de mise à jour de supertrame et réponse

Le paquet de demande de mise à jour de supertrame est utilisé par le NM pour mettre à jour une supertrame existante d'un appareil de routage et est également utilisé par l'appareil de routage pour mettre à jour une supertrame existante d'un appareil de terrain. Après avoir reçu ce paquet de commande, il convient que l'appareil de routage ou l'appareil de terrain mette à jour un enregistrement dans sa table de supertrames.

Le format du paquet de demande de mise à jour de supertrame est décrit au Tableau 158.

Tableau 158 – Format du paquet de demande de mise à jour de supertrame

	Format de paquet de demande de mise à jour de supertrame		
Longueur en octet(s)	14/16	1	12
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 22 (ID de commande = 22)	Superframe table item (élément de table de supertrames)

Le paquet de demande de mise à jour de supertrame comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 22;
- Superframe table item (élément de table de supertrames): ce champ a une longueur de 12 octet et indique les informations détaillées de la supertrame mise à jour (voir Tableau 16).

Le paquet de réponse de mise à jour de supertrame est utilisé pour retourner les résultats d'exécution de la mise à jour de supertrame. Le format du paquet de réponse de mise à jour de supertrame est décrit au Tableau 159.

Tableau 159 – Format du paquet de réponse de mise à jour de supertrame

	Format de paquet de réponse de mise à jour de supertrame		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 23 (ID de commande = 23)	Execution result (résultat d'exécution)

Le paquet de réponse de mise à jour de supertrame comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 23;
- c) Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de réponse de mise à jour de supertrame. Si le processus de réponse réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.15 Demande de libération de supertrame et réponse

La trame de commande de demande de libération de supertrame est utilisée par le NM pour libérer une supertrame existante d'un appareil de routage et est également utilisée par l'appareil de routage pour libérer une supertrame existante d'un appareil de terrain. Après avoir reçu ce paquet de commande, il convient que l'appareil de routage ou l'appareil de terrain libère un enregistrement dans sa table de supertrames.

Le format du paquet de demande de libération de supertrame est décrit au Tableau 160.

Tableau 160 – Format du paquet de demande de libération de supertrame

	Format de paquet de demande de libération de supertrame		
Longueur en octet(s)	14/16	1	2
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 24 (ID de commande = 24)	Superframe ID (ID de supertrame)

Le paquet de demande de libération de supertrame comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 24;
- c) Superframe ID (ID de supertrame): ce champ a une longueur de 2 octets et indique l'identificateur de la supertrame à libérer (voir Tableau 16).

Le paquet de réponse de libération de supertrame est utilisé pour retourner les résultats d'exécution de la libération de supertrame. Le format du paquet de réponse de libération de supertrame est décrit au Tableau 161.

Tableau 161 – Format du paquet de réponse de libération de supertrame

	Format de paquet de réponse de libération de supertrame		
Longueur en octet(s)	14/16	1	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 25 (ID de commande = 25)	Execution result (résultat d'exécution)

Le paquet de réponse de libération de supertrame comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 25;

- c) Execution result (résultat d'exécution): ce champ a une longueur de 1 octet et indique le résultat du processus de réponse de libération de supertrame. Si le processus de réponse réussit, la valeur de ce champ est 0; sinon, la valeur de ce champ est 1 (voir Tableau 134).

9.6.4.16 Demande de rapport sur la condition des appareils

Le paquet de demande de rapport sur la condition des appareils est utilisé pour rapporter à distance les conditions des appareils. Le format du paquet de demande de rapport sur la condition des appareils est décrit au Tableau 162.

Tableau 162 – Format du paquet de demande de rapport sur la condition des appareils

Format du paquet de demande de rapport sur la condition des appareils				
Longueur en octet(s)	14/16	1	1	Longueur variable
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 26 (ID de commande = 26)	Number of devices (nombre d'appareils)	Items of device condition information (éléments d'informations sur la condition des appareils)

Le paquet de demande de rapport sur la condition des appareils comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 26;
- Number of devices (nombre d'appareils): ce champ a une longueur de 1 octet et indique le nombre d'appareils rapportés;
- Items of device condition information (éléments d'informations sur la condition des appareils): le format détaillé du champ d'informations sur la condition des appareils est décrit au Tableau 163. Ce champ a une longueur de $N \times 11$ octets, où N = nombre d'appareils.

Tableau 163 – Format du champ d'informations sur la condition des appareils

Format du champ d'informations sur la condition des appareils							
Longueur en octet(s)	2	2	2	2	1	2	4
Nom de champ	Device short address (adresse courte de l'appareil)	Number of packets transmitted after last report (nombre de paquets émis après le dernier rapport)	Number of packets terminated in this device after last report (nombre de paquets terminés dans cet appareil après le dernier rapport)	Number of packets with MAC MIC failure after last report (nombre de paquets avec défaillance de MIC MAC après le dernier rapport)	Battery level (niveau de la batterie)	Restart count of device after last report (nombre de redémarrages de l'appareil après le dernier rapport)	Uptime (durée de fonctionnement)

Le champ d'informations sur la condition des appareils comporte les sous-champs suivants (voir Tableau 22):

- a) Device short address (adresse courte de l'appareil): ce sous-champ a une longueur de 2 octets et indique l'adresse courte de l'appareil rapporté;
- b) Number of packets transmitted after last report (nombre de paquets émis après le dernier rapport): ce sous-champ a une longueur de 2 octets et indique le nombre de paquets émis depuis le dernier rapport de l'appareil rapporté;
- c) Number of packets terminated in this device after last report (nombre de paquets terminés dans cet appareil après le dernier rapport): ce sous-champ a une longueur de 2 octets et indique le nombre de paquets reçus depuis le dernier rapport de l'appareil rapporté;
- d) Number of packets with MAC MIC failure after last report (nombre de paquets avec défaillance de MIC MAC après le dernier rapport): ce sous-champ a une longueur de 2 octets et indique le nombre de paquets avec défaillance de MIC MAC depuis le dernier rapport;
- e) Battery level (niveau de la batterie): ce sous-champ a une longueur de 1 octet et indique le niveau de puissance résiduelle;
- f) Restart count of device after last report (nombre de redémarrages de l'appareil après le dernier rapport): ce sous-champ a une longueur de 2 octets et indique le nombre de redémarrages depuis le dernier rapport;
- g) Uptime (durée de fonctionnement): ce sous-champ a une longueur de 4 octets et indique la durée de fonctionnement d'un appareil.

9.6.4.17 Demande de rapport sur la condition des canaux

Le paquet de demande de rapport sur la condition des canaux est utilisé pour rapporter à distance l'état de qualité des canaux de communication. Le format du paquet de demande de rapport sur la condition des canaux est décrit au Tableau 164.

Tableau 164 – Format du paquet de demande de rapport sur la condition des canaux

Format de paquet de demande de rapport sur la condition des canaux				
Longueur en octet(s)	14/16	1	1	Longueur variable
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 27 (ID de commande = 27)	Number of channels (nombre de canaux)	Items of channel quality information (éléments d'informations sur la qualité des canaux)

Le paquet de demande de rapport sur la condition des canaux comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 27;
- c) Number of channels (nombre de canaux): ce champ a une longueur de 1 octet et indique le nombre de canaux rapportés;
- d) Channel quality information (informations sur la qualité des canaux): ce champ a une longueur variable;
- e) Items of channel quality information (éléments d'informations sur la qualité des canaux): le format détaillé du champ d'informations sur la qualité des canaux est décrit au Tableau 165. Ce champ a une longueur de $N \times 5$ octets, où N = nombre de canaux.

Tableau 165 – Format du champ d'informations sur la qualité des canaux

	Format du champ d'informations sur la qualité des canaux			
Longueur en octet(s)	1	1	2	1
Nom de champ	Channel index (indice de canal)	Link quality (qualité de liaison)	Packet loss rate (taux de perte de paquets)	Number of retries (nombre de nouvelles tentatives)

Le champ d'informations sur la qualité des canaux comporte les sous-champs suivants:

- Channel index (indice de canal): ce champ a une longueur de 1 octet et indique le numéro séquentiel du canal;
- Link quality (qualité de liaison): ce champ a une longueur de 1 octet et indique la valeur LQI de chaque canal;
- Packet loss rate (taux de perte de paquets): ce champ a une longueur de 2 octets et indique le taux de perte de paquets de chaque canal;
- Number of retries (nombre de nouvelles tentatives): ce champ a une longueur de 1 octet et indique le nombre de retransmissions de chaque canal.

9.6.4.18 Demande de rapport sur la défaillance des chemins

Le paquet de demande de rapport sur la défaillance des chemins est utilisé par les appareils de routage pour rapporter la défaillance d'un chemin. Le format du paquet de demande de rapport sur la défaillance des chemins est décrit au Tableau 166.

Tableau 166 – Format du paquet de demande de rapport sur la défaillance des chemins

	Format de paquet de demande de rapport sur la défaillance des chemins		
Longueur en octet(s)	14/16	1	2
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 28 (ID de commande = 28)	ID d'itinéraire

Le paquet de demande de rapport sur la défaillance des chemins comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 28;
- Route ID (ID d'itinéraire): ce champ a une longueur de 1 octet et indique l'identificateur de l'itinéraire rapporté.

9.6.4.19 Demande d'obtention d'attribut

Le paquet de demande d'obtention d'attribut est utilisé pour demander à un appareil spécifié de rapporter les attributs de sa base MIB. Le format du paquet de demande d'obtention d'attribut est décrit au Tableau 167.

Tableau 167 – Format du paquet de demande d'obtention d'attribut

Format du paquet de demande d'obtention d'attribut						
Longueur en octet(s)	14/16	1	1	1	2	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 29 (ID de commande = 29)	Attribute ID (ID d'attribut)	Attribute member ID (ID d'élément d'attribut)	First storage index of multiple attribute values (premier indice de stockage des multiples valeurs d'attribut)	Number of attributes (nombre d'attributs)

Le paquet de demande d'obtention d'attribut comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 29;
- Attribute ID (ID d'attribut): ce champ a une longueur de 1 octet et indique l'indice de l'attribut demandé;
- Attribute member ID (ID d'élément d'attribut): ce champ a une longueur de 1 octet et indique l'indice de l'élément d'attribut demandé;
- First storage index of multiple attribute values (premier indice de stockage des multiples valeurs d'attribut): ce champ a une longueur de 2 octets et indique le premier indice de stockage des multiples valeurs d'attribut;
- Number of attributes (nombre d'attributs): ce champ a une longueur de 1 octet; il indique le nombre de valeurs d'attributs ou de valeurs d'éléments d'attributs.

9.6.4.20 Réponse d'obtention d'attribut

Le paquet de réponse d'obtention d'attribut est utilisé pour répondre à la demande d'obtention d'attribut; il convient de retourner les valeurs des attributs. Le format du paquet de réponse d'obtention d'attribut est décrit au Tableau 168.

Tableau 168 – Format du paquet de réponse d'obtention d'attribut

Format du paquet de réponse d'obtention d'attribut								
Longueur en octet(s)	14/16	1	1	1	1	2	1	Longueur variable
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 30 (ID de commande = 30)	Statut	Attribute ID (ID d'attribut)	Attribute member ID (ID d'élément d'attribut)	First storage index of multiple attribute values (premier indice de stockage des multiples valeurs d'attribut)	Number of attributes (nombre d'attributs)	Attribute value (valeur d'attribut)

Le paquet de réponse d'obtention d'attribut comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 30;

- c) Status (état): ce champ a une longueur de 1 octet et indique le résultat du processus d'obtention d'attribut; la valeur 0 indique que le processus d'obtention a réussi et la valeur 1 indique que l'attribut demandé n'est pas pris en charge; sinon, ce champ est réservé (voir Tableau 122);
- d) Attribute ID (ID d'attribut): ce champ a une longueur de 1 octet et indique l'indice de l'attribut demandé;
- e) Attribute member ID (ID d'élément d'attribut): ce champ a une longueur de 1 octet et indique l'indice de l'élément d'attribut demandé;
- f) First storage index of multiple attribute values (premier indice de stockage des multiples valeurs d'attribut): ce champ a une longueur de 2 octets et indique le premier indice de stockage des multiples valeurs d'attribut;
- g) Number of attributes (nombre d'attributs): ce champ a une longueur de 1 octet; il indique le nombre de valeurs d'attributs ou de valeurs d'éléments d'attributs.
- h) Attribute values (valeurs d'attributs): ce champ a une longueur variable et indique les valeurs d'attributs demandées.

9.6.4.21 Demande d'établissement d'attribut

Le paquet de demande d'établissement d'attribut est utilisé pour demander à un appareil d'ajouter ou de modifier la valeur d'attribut dans sa base MIB. Le format du paquet de demande d'établissement d'attribut est décrit au Tableau 169.

Tableau 169 – Format du paquet de demande d'établissement d'attribut

Format du paquet de demande d'établissement d'attribut							
Longueur en octet(s)	14/16	1	1	1	2	1	Longueur variable
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 31 (ID de commande = 31)	Attribute ID (ID d'attribut)	Attribute member ID (ID d'élément d'attribut)	First storage index of multiple attribute values (premier indice de stockage des multiples valeurs d'attribut)	Number of attributes (nombre d'attributs)	Attribute value (valeur d'attribut)

Le paquet de demande d'établissement d'attribut comporte les champs suivants:

- a) Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- b) Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 31;
- c) Attribute ID (ID d'attribut): ce champ a une longueur de 1 octet et indique l'indice de l'attribut demandé;
- d) Attribute member ID (ID d'élément d'attribut): ce champ a une longueur de 1 octet et indique l'indice de l'élément d'attribut demandé;
- e) First storage index of multiple attribute values (premier indice de stockage des multiples valeurs d'attribut): ce champ a une longueur de 2 octets et indique le premier indice de stockage des multiples valeurs d'attribut;
- f) Number of attributes (nombre d'attributs): ce champ a une longueur de 1 octet; il indique le nombre de valeurs d'attributs ou de valeurs d'éléments d'attributs.
- g) Attribute values (valeurs d'attributs): ce champ a une longueur variable et indique les valeurs d'attributs à établir.

9.6.4.22 Réponse d'établissement d'attribut

Le paquet de réponse d'établissement d'attribut est utilisé pour répondre à la demande d'établissement d'attribut. Le format du paquet de réponse d'établissement d'attribut est décrit au Tableau 170.

Tableau 170 – Format du paquet de réponse d'établissement d'attribut

	Format du paquet de réponse d'établissement d'attribut						
Longueur en octet(s)	14/16	1	1	1	1	2	1
Nom de champ	Network layer header (en-tête de couche réseau)	Command ID = 32 (ID de commande = 32)	Statut	Attribute ID (ID d'attribut)	Attribute member ID (ID d'élément d'attribut)	First storage index of multiple attribute values (premier indice de stockage des multiples valeurs d'attribut)	Number of attributes (nombre d'attributs)

Le paquet de réponse d'établissement d'attribut comporte les champs suivants:

- Network layer header (en-tête de couche réseau): la définition de l'en-tête de couche réseau est identique à celle donnée dans le Tableau 128;
- Command ID (ID de commande): ce champ a une longueur de 1 octet et sa valeur est égale à 32;
- Status (état): ce champ a une longueur de 1 octet et indique le résultat du processus d'établissement d'attribut; la valeur 0 indique que le processus d'établissement a réussi et la valeur 1 indique que l'attribut demandé n'est pas pris en charge; sinon, ce champ est réservé (voir Tableau 126);
- Attribute ID (ID d'attribut): ce champ a une longueur de 1 octet et indique l'indice de l'attribut demandé;
- Attribute member ID (ID d'élément d'attribut): ce champ a une longueur de 1 octet et indique l'indice de l'élément d'attribut demandé;
- First storage index of multiple attribute values (premier indice de stockage des multiples valeurs d'attribut): ce champ a une longueur de 2 octets et indique le premier indice de stockage des multiples valeurs d'attribut;
- Number of attributes (nombre d'attributs): ce champ a une longueur de 1 octet; il indique le nombre de valeurs d'attributs ou de valeurs d'éléments d'attributs.

10 Application layer, couche d'application

10.1 Vue d'ensemble

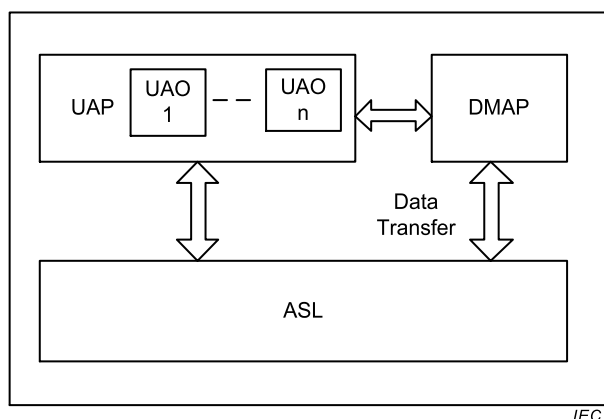
10.1.1 Généralités

La couche application (AL) du réseau WIA-PA est composée du processus d'application utilisateur (UAP) et de la sous-couche application (ASL). La couche AL définit les objets d'application qui interagissent avec les processus industriels. Elle définit aussi les services de communication qui prennent en charge les communications entre plusieurs objets pour les applications industrielles réparties.

Les opérations locales entre les objets UAO ne sont pas spécifiées dans le présent document.

10.1.2 Structure de la couche AL

La structure de la couche application (AL) est représentée à la Figure 71.



Anglais	Français
Date Transfer	Transfert de données

Figure 71 – Structure de la couche application (AL)

Les applications réparties des processus industriels peuvent être mises en œuvre par des objets UAP. Un UAP est constitué d'un ou de plusieurs UAO. Dans un appareil, tous les UAO peuvent interagir les uns avec les autres. Les objets UAO dans des appareils différents peuvent interagir les uns avec les autres via les services de communication fournis par la couche application (AL).

La sous-couche application (ASL) fournit des services transparent d'émission de données: entre la sous-couche application (ASL) et les processus d'application utilisateur (UAP).

10.1.3 Fonctions de l'UAP

Un processus d'application utilisateur (UAP) a les fonctions suivantes:

- recueil des données de processus, telles que les données de processus température, pression et débit;
- traitement des données de processus recueillies, comme par exemple conversion, linéarisation, compensation et filtrage;
- calcul et génération des données de sortie en se basant sur les données traitées de l'appareil ou celles d'autres appareils;
- contrôle du processus;
- génération et report d'une alarme: il convient que le processus UAP rapporte un événement d'alarme, par exemple lorsque les données de processus sont au-delà des limites, que l'état des objets UAO change, etc.
- Interfonctionnement entre les appareils du réseau WIA-PA

10.1.4 Fonctions de la sous-couche application (ASL)

La sous-couche application (ASL) fournit des services de données et de gestion comme suit:

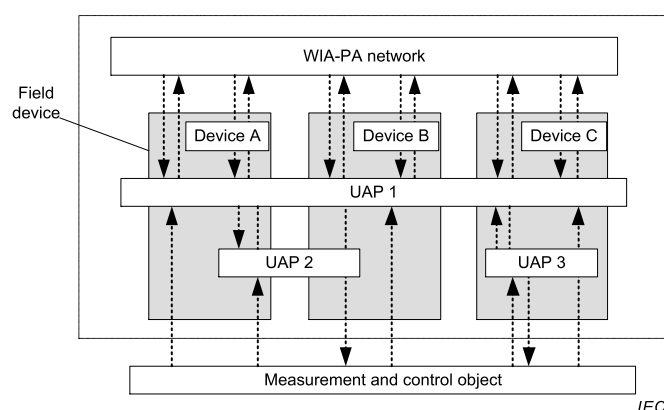
- services de transfert de données: la sous-couche application (ASL) fournit des services transparents de transfert de données de bout en bout pour le processus d'application utilisateur (UAP) et prend en charge les transmissions de données C/S, P/S et R/S; et
- les services de gestion de la sous-couche application (ASL) ne sont pas définis dans le présent document.

10.2 UAP

10.2.1 Généralités

Le processus d'application utilisateur (UAP) est une unité de traitement de l'information pour des applications spécifiques et est utilisé pour la mise en œuvre des applications réparties résidant au sein de réseau WIA-PA.

Un processus UAP peut être conçu comme un processus d'application selon l'IEC 61499-1 et l'IEC 61499-2 ou l'IEC 61804-2. Un processus UAP peut également être un processus d'application défini par des utilisateurs. La mise en œuvre d'un processus UAP peut être réalisée à l'aide de blocs fonctionnels ou d'autres approches (voir Figure 72).



Anglais	Français
WIA-PA network	Réseau WIA-PA
Field device	Appareil de terrain
Device A	Appareil A
Device B	Appareil B
Device C	Appareil C
Measurement and control object	Objet de mesure et de commande

Figure 72 – Processus d'application utilisateur (UAP)

Un processus UAP peut être constitué de plusieurs objets UAO au sein d'un même appareil, référencé UAP 3 à la Figure 72. Un processus UAP peut également être constitué de plusieurs objets UAO résidant dans des appareils différents, référencés UAP 1 et UAP 2 à la Figure 72.

10.2.2 UAO

10.2.2.1 Généralités

Un objet d'application utilisateur (UAO) est défini selon différentes fonctions, qui peuvent être définies comme blocs fonctionnels par d'autres approches.

Pour prendre en charge l'interopérabilité entre différents appareils, chaque objet UAO possède ses propres attributs. Les attributs de l'objet UAO sont utilisés pour décrire les profils d'application que les objets d'application doivent suivre.

Chaque objet UAO doit être identifié par un ID d'objet et un ID d'instance. Si certains attributs de l'objet UAO peuvent fonctionner à distance, ils doivent également être accessibles à partir de l'identificateur d'attribut.

10.2.2.2 Fonctions de l'UAO

Dans un réseau WIA-PA, les objets d'application utilisateur (UAO) recueillent et traitent les données issues de processus industriels (telles que la température, la pression et le débit) en utilisant différents types de capteurs et contrôlent également le processus au moyen d'actionneurs. Les fonctions d'un objet UAO sont décrites ci-dessous.

a) Mise à l'échelle d'une plage

La mise à l'échelle de plage est une transformation linéaire qui convertit les données de processus d'une unité dans une autre unité afin de simplifier les mesures et calculs ultérieurs. Par exemple, les signaux de 4 mA ~ 20 mA peuvent être convertis en signaux de 0 Kpa à 10 Kpa. La mise à l'échelle peut également convertir les données comportant des unités en données dépourvues d'unités, telles qu'un pourcentage.

b) Linéarisation

Les caractéristiques des capteurs sont majoritairement non linéaires voire irrégulières. C'est pourquoi il est nécessaire d'effectuer une linéarisation lorsqu'il s'agit de traiter des données de capteurs.

c) Compensation

Les valeurs mesurées de capteurs peuvent présenter une dérive linéaire en raison de l'influence de l'environnement, si bien qu'il est nécessaire d'effectuer une compensation.

d) Filtrage

Dans le processus industriel, les capteurs peuvent subir des interférences, ce qui se traduit par un saut relativement abrupt des valeurs mesurées. Afin d'éviter une telle situation, le filtrage est utilisé pour éliminer l'influence des signaux de saut.

e) Entreposage

Le stockage consiste à copier les données dans une zone de stockage temporaire afin qu'elles puissent être renvoyées en cas de perte des données d'origine.

f) Conversion en unités techniques

La conversion en unités techniques consiste à convertir les unités des signaux d'entrée dans d'autres unités pouvant être identifiées par les sous-systèmes d'entrée/sortie (E/S).

g) Référence temporelle des mesures

L'heure courante est ajoutée comme référence temporelle aux données mesurées.

L'objet UAO n'est pas spécifié dans le présent document. Pour un exemple d'objet UAO, voir Annexe C.

10.2.3 Définition des méthodes

10.2.3.1 Généralités

Le Tableau 171 spécifie les méthodes utilisées pour traiter les paramètres des objets d'application utilisateur (UAO).

Tableau 171 – Définition des méthodes pour les objets d'application utilisateur (UAO)

Méthode	Identificateur de méthode	Domaine d'application		Description
		Objet	Instance	
READ	demande: 0x00	Obligatoire	Obligatoire	Lecture des attributs d'objets UAO
	réponse: 0x80	Obligatoire	Obligatoire	Réponse de la lecture des attributs d'objets UAO
WRITE	demande: 0x01	Non pris en charge	Facultatif	Ecriture des attributs d'objets UAO
	réponse: 0x81	Non pris en charge	Facultatif	Réponse de l'écriture des attributs d'objets UAO
PUBLISH	demande: 0x02	Non pris en charge	Facultatif	Publication des attributs d'objets UAO
REPORT	demande: 0x03	Non pris en charge	Facultatif	Report des données d'alarme et d'événement
REPORT ACK	demande: 0x04	Non pris en charge	Facultatif	Acquittement d'alarme

10.2.3.2 Format de la méthode READ

Le format de demande de la méthode READ est décrit au Tableau 172.

Tableau 172 – Format de demande de la méthode READ

	Format de demande de la méthode READ		
Longueur en octet(s)	1	1	1
Nom de champ	Object identifier (identificateur d'objet)	Object instance identifier (identificateur d'instance d'objet)	Object attribute identifier (identificateur d'attribut d'objet)

Le format de demande de la méthode READ comporte les champs suivants:

- Object identifier (identificateur d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un UAO;
- Object instance identifier (identificateur d'instance d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'une instance d'objet;
- Object attribute identifier (identificateur d'attribut d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un attribut d'objet; lorsque l'identificateur d'attribut d'objet est égal à 0, il convient que tous les attributs de l'instance soient lus.

Le format de réponse de la méthode READ est décrit au Tableau 173.

Tableau 173 – Format de réponse de la méthode READ

	Format de réponse de la méthode READ				
Longueur en octet(s)	1	1	1	1	Longueur variable
Nom de champ	Object identifier (identificateur d'objet)	Object instance identifier (identificateur d'instance d'objet)	Object attribute identifier (identificateur d'attribut d'objet)	Data length (longueur des données)	Données

Le format de réponse de la méthode READ comporte les champs suivants:

- a) Object identifier (identificateur d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un UAO;
- b) Object instance identifier (identificateur d'instance d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'une instance d'objet;
- c) Object attribute identifier (identificateur d'attribut d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un attribut d'objet; lorsque l'identificateur d'attribut d'objet est égal à 0, il convient que tous les attributs de l'instance soient lus.
- d) Data length (longueur des données): ce champ a une longueur de 1 octet et indique la longueur des données de l'attribut d'objet; une valeur de Data length égale à 0 indique l'échec de l'opération de lecture.
- e) Data (données): ce champ a une longueur variable et indique les données de l'attribut d'objet. Si la valeur de Data length est égale à 0, ce champ doit être ignoré.

10.2.3.3 Format de la méthode WRITE

Le format de demande de la méthode WRITE est décrit au Tableau 174.

Tableau 174 – Format de demande de la méthode WRITE

	Format de demande de la méthode WRITE				
Longueur en octet(s)	1	1	1	1	Longueur variable
Nom de champ	Object identifier (identificateur d'objet)	Object instance identifier (identificateur d'instance d'objet)	Object attribute identifier (identificateur d'attribut d'objet)	Data length (longueur des données)	Données

Le format de demande de la méthode WRITE comporte les champs suivants:

- a) Object identifier (identificateur d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un UAO;
- b) Object instance identifier (identificateur d'instance d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'une instance d'objet;
- c) Object attribute identifier (identificateur d'attribut d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un attribut d'objet; lorsque l'identificateur d'attribut d'objet est égal à 0, il convient que tous les attributs de l'instance soient écrits.
- d) Data length (longueur des données): ce champ a une longueur de 1 octet et indique la longueur des données de l'attribut d'objet.
- e) Data (données): ce champ a une longueur variable et indique les données de l'attribut d'objet.

Le format de réponse de la méthode WRITE est décrit au Tableau 175.

Tableau 175 – Format de réponse de la méthode WRITE

	Format de réponse de la méthode WRITE			
Longueur en octet(s)	1	1	1	1
Nom de champ	Object identifier (identificateur d'objet)	Object instance identifier (identificateur d'instance d'objet)	Object attribute identifier (identificateur d'attribut d'objet)	Statut

Le format de réponse de la méthode WRITE comporte les champs suivants:

- a) Object identifier (identificateur d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un UAO;

- b) Object instance identifier (identificateur d'instance d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'une instance d'objet;
- c) Object attribute identifier (identificateur d'attribut d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un attribut d'objet;
- d) Status (état): ce champ a une longueur de 1 octet et est utilisé pour indiquer le résultat de l'opération WRITE; la valeur 0 indique que le processus a réussi et la valeur 1 indique que le processus a échoué.

10.2.3.4 Format de la méthode PUBLISH

Le format de la méthode PUBLISH est décrit au Tableau 176.

Tableau 176 – Format de la méthode PUBLISH

Format de la méthode PUBLISH					
Longueur en octet(s)	1	1	1	1	Longueur variable
Nom de champ	Object identifier (identificateur d'objet)	Object instance identifier (identificateur d'instance d'objet)	Object attribute identifier (identificateur d'attribut d'objet)	Data length (longueur des données)	Données

Le format de la méthode PUBLISH comporte les champs suivants:

- a) Object identifier (identificateur d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un UAO;
- b) Object instance identifier (identificateur d'instance d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'une instance d'objet;
- c) Object attribute identifier (identificateur d'attribut d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un attribut d'objet; lorsque l'identificateur d'attribut d'objet est égal à 0, il convient que tous les attributs de l'instance soient publiés.
- d) Data length (longueur des données): ce champ a une longueur de 1 octet et indique la longueur des données de l'attribut d'objet publié.
- e) Data (données): ce champ a une longueur variable et indique les données de l'attribut d'objet publié.

10.2.3.5 Format de la méthode REPORT

Le format de la méthode REPORT est décrit au Tableau 177.

Tableau 177 – Format de la méthode REPORT

Format de la méthode REPORT					
Longueur en octet(s)	1	1	1	1	Longueur variable
Nom de champ	Object identifier (identificateur d'objet)	Object instance identifier (identificateur d'instance d'objet)	Object attribute identifier (identificateur d'attribut d'objet)	Data length (longueur des données)	Données

Le format de la méthode REPORT comporte les champs suivants:

- a) Object identifier (identificateur d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un UAO;
- b) Object instance identifier (identificateur d'instance d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'une instance d'objet;

- c) Object attribute identifier (identificateur d'attribut d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un attribut d'objet; lorsque l'identificateur d'attribut d'objet est égal à 0, il convient que tous les attributs de l'instance soient rapportés.
- d) Data length (longueur des données): ce champ a une longueur de 1 octet et indique la longueur des données de l'attribut d'objet rapporté.
- e) Data (données): ce champ a une longueur variable et indique les données de l'attribut d'objet rapporté.

10.2.3.6 Format de la méthode REPORT ACK

Le format de la méthode REPORT ACK est décrit au Tableau 178.

Tableau 178 – Format de la méthode REPORT ACK

	Format de la méthode REPORT ACK			
Longueur en octet(s)	1	1	1	1
Nom de champ	Object identifier (identificateur d'objet)	Object instance identifier (identificateur d'instance d'objet)	Object attribute identifier (identificateur d'attribut d'objet)	Statut

Le format de la méthode REPORT ACK comporte les champs suivants:

- a) Object identifier (identificateur d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un UAO;
- b) Object instance identifier (identificateur d'instance d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'une instance d'objet;
- c) Object attribute identifier (identificateur d'attribut d'objet): ce champ a une longueur de 1 octet et indique l'identificateur d'un attribut d'objet rapporté;
- d) Status (état): ce champ a une longueur de 1 octet et indique le résultat du processus REPORT; la valeur 0 indique d'effacer l'événement d'alarme et la valeur 1 indique de maintenir l'événement d'alarme.

10.3 Sous-couche application

10.3.1 Généralités

La sous-couche application (ASL) fournit des services de communication de données entre des objets UAO dans le réseau WIA-PA.

10.3.2 Entité de données de la sous-couche application (ASLDE)

10.3.2.1 Généralités

La sous-couche application (ASL) définit l'entité de données de la sous-couche application (ASLDE), qui fournit des interfaces transparentes pour l'envoi et la réception des données entre la couche ASL et la couche réseau (NL). L'entité ASLDE prend en charge le transport des unités APDU entre deux objets UAO.

La sous-couche application (ASL) prend en charge trois modes de communication: le mode C/S, le mode P/S et le mode R/S:

- a) le mode C/S prend en charge l'émission en monodiffusion de données dynamiques et apériodiques;
- b) le mode P/S prend en charge l'émission en monodiffusion et en multidiffusion de données périodiques;
- c) le mode R/S prend en charge l'émission en monodiffusion et en multidiffusion de données apériodiques, telles que les alarmes, alertes ou événements.

Ces modes de communication sont pris en charge par les types correspondants de VCR.

Il convient que les services de données de la couche AL soient pris en charge par trois primitives: ASLDE-DATA.request, ASLDE-DATA.confirm et ASLDE-DATA.indication.

10.3.2.2 ASLDE-DATA.request

La couche supérieure envoie des données à la couche ASL en utilisant la primitive ASLDE-DATA.request.

La sémantique de cette primitive est décrite comme suit:

```
ASLDE-DATA.request (
    VcrID,
    Priority,
    MethodIdentifier
    AsduLength,
    Asdu
)
```

Le Tableau 179 spécifie les paramètres de la primitive ASLDE-DATA.request.

Tableau 179 – Paramètres de ASLDE-DATA.request

Nom	Type de données	Plage valide	Description
VcrID	Unsigned16	0 à 65 535	VCR utilisée pour l'émission
Priorité	Unsigned8	0 à 255	Priorité des données UAO
MethodIdentifier	Unsigned8	0 à 255	Identificateur de la méthode (voir Tableau 171)
AsduLength	Unsigned16	0 à 65 535	Nombre d'octets constituant l'unité ASDU devant être transférée
Asdu	Octetstring		Ensemble d'octets constituant l'unité ASDU devant être transférée

Lorsque la sous-couche application (ASL) reçoit une demande de données issue de la couche supérieure, il convient qu'elle encapsule l'unité ASDU en fonction du format de paquet ASL et qu'elle la transporte à la couche NL. Après avoir transporté les données, il convient que la sous-couche ASL produise une ASLDE-DATA.confirm pour la couche supérieure avec le paramètre Status (état) mis à la valeur d'état retournée par la couche NL.

10.3.2.3 ASLDE-DATA.confirm

La primitive ASLDE-DATA.confirm est invoquée pour indiquer le résultat de l'émission. Lorsque les données ont été transférées avec succès, il convient que le paramètre Status (état) de cette primitive soit établi sur la valeur SUCCESS. Autrement, il convient que le paramètre Status (état) soit établi sur le code d'erreur correspondant pour indiquer la raison de l'échec.

La sémantique de cette primitive est décrite comme suit:

```
ASLDE-DATA.confirm(
    VcrID,
    Statut
)
```

Le Tableau 180 spécifie les paramètres pour la primitive ASLDE-DATA.confirm.

Tableau 180 – Paramètres de ASLDE-DATA.confirm

Nom	Type de données	Plage valide	Description
VcrID	Unsigned16	0 à 65 535	Identificateur unique de la VCR utilisé pour cette émission
Statut	Unsigned8	0 à 255	Etat de la demande correspondante: 0 = SUCCESS (succès) 1 = INVALID_ADDRESS (adresse invalide) 2 = FAIL (échec) Les autres valeurs sont réservées.

10.3.2.4 ASLDE-DATA.indication

Après avoir reçu des paquets de la NL, la sous-couche application (ASL) transfère les données utilisateur à la couche supérieure par la primitive ASLDE-DATA.indication et la couche supérieure exécute l'opération correspondante et traite les données utilisateur en fonction des différents types de service.

La sémantique de cette primitive est décrite comme suit:

```
ASLDE-DATA.indication(
    MethodIdentifier,
    Priority,
    AsduLength,
    Asdu
)
```

Le Tableau 181 spécifie les paramètres pour la primitive ASLDE-DATA.indication.

Tableau 181 – Paramètres de ASLDE-DATA.indication

Nom	Type de données	Plage valide	Description
MethodIdentifier	Unsigned8	0 à 255	Identificateur de la méthode (voir Tableau 171)
Priorité	Unsigned8	0 à 255	Priorité du paquet
AsduLength	Unsigned16	0 à 65 535	Nombre d'octets constituant l'unité ASDU reçue
Asdu	Octetstring		Ensemble d'octets constituant l'unité ASDU reçue

10.3.2.5 ASLDE-AGG.request

La primitive ASLDE-AGG.request est invoquée par le DMAP pour demander à la sous-couche ASL d'envoyer le paquet agrégé.

La sémantique de cette primitive est décrite comme suit:

```
ASLDE-AGG.request(
    VcrID,
    SrcAddr,
    GatewayAddr,
    Priority,
    AggPacketFlag,
    AggRouteID,
    AggPayload
)
```


Le Tableau 182 spécifie les paramètres pour la primitive ASLDE-AGG.request.

Tableau 182 – Paramètres de ASLDE-AGG.request

Nom	Type de données	Plage valide	Description
VcrID	Unsigned16	0 à 65 535	Identificateur unique de la VCR utilisé pour cette émission
SrcAddr	Unsigned16	0 à 65 535	Adresse réseau de la source
GatewayAddr	Unsigned16	0 à 65 535	Adresse réseau de l'appareil de passerelle
Priorité	Unsigned8	0 à 255	Priorité des données de processus
AggPacketFlag	Unsigned8	0 à 255	Indique si ce paquet est un paquet de données ou un paquet d'agrégation: 0 = paquet de données 1 = paquet d'agrégation
AggRouteID	Unsigned16	0 à 65 535	Identificateur d'itinéraire pour les données d'agrégation
AggPayload	Octetstring		Paquet agrégé de DMAP

10.3.2.6 ASLDE-DAG.indication

La primitive ASLDE-DAG.indication est invoquée par la sous-couche ASL pour demande au DMAP de désagréger le paquet.

La sémantique de cette primitive est décrite comme suit:

```
ASLDE-DAG.indication (
    AggPayload
)
```

Le Tableau 183 spécifie les paramètres pour la primitive ASLDE-DAG.indication.

Tableau 183 – Paramètres de ASLDE-DAG.indication

Nom	Type de données	Plage valide	Description
AggPayload	Octetstring		Paquet agrégé

10.3.2.7 Modes de communication

10.3.2.7.1 Généralités

La sous-couche application (ASL) fournit trois modes de communication de données pour les services de transmission de données: le mode C/S, le mode P/S et le mode R/S.

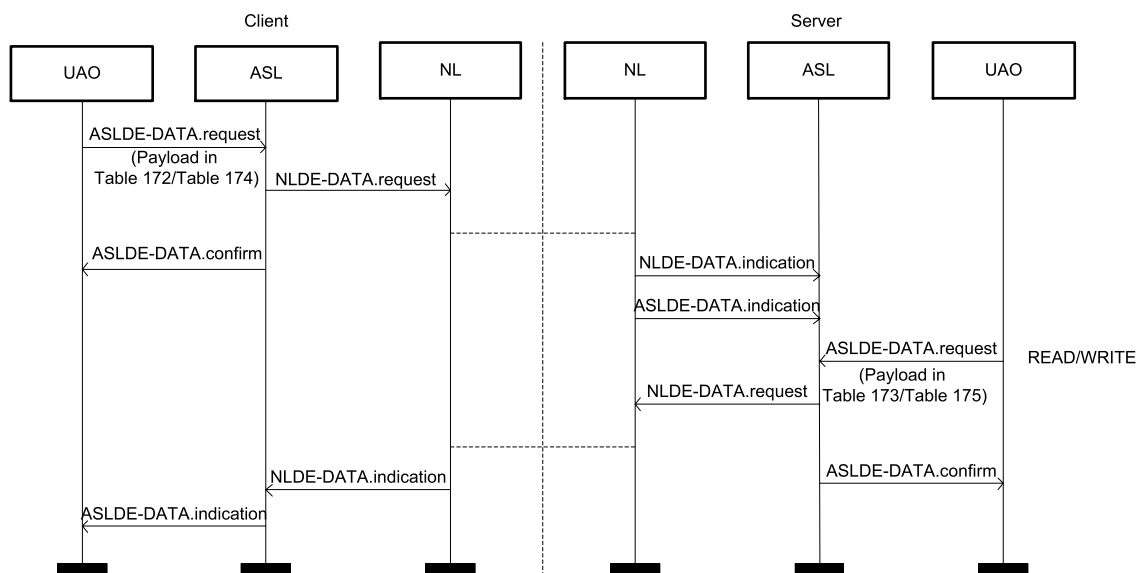
10.3.2.7.2 Mode Client/Serveur

La sous-couche application (ASL) fournit le mode C/S pour lire ou écrire des objets UAO et leurs attributs afin de prendre en charge les opérations d'obtention ou d'établissement d'informations. Le mode C/S est pris en charge par les VCR C/S.

Il convient que l'application utilisateur Client envoie une demande de lecture ou d'écriture à l'application utilisateur Serveur. Il convient que l'objet UAO Serveur exécute l'opération correspondante sur ses attributs en fonction des différents types de service et qu'il retourne ensuite le résultat comme réponse à l'objet UAO Client demandeur.

Il convient que la sous-couche ASL Client maintienne un numéro séquentiel pour chaque demande d'envoi, qui est utilisé pour faire correspondre la réponse et l'acquittement du serveur.

Le processus de communication C/S est représenté à la Figure 73.



IEC

Anglais	Français
Client	Client
Server	Serveur
(Payload in Table 172/Table 174)	(charge utile décrite au Tableau 172/Tableau 174)
(Payload in Table 173/Table 175)	(charge utile décrite au Tableau 173/Tableau 175)
READ/WRITE	READ/WRITE

Figure 73 – Processus de communication C/S

10.3.2.7.3 Mode Publisher/Subscriber (éditeur/abonné)

La sous-couche application (ASL) fournit le mode P/S pour prendre en charge l'émission de données périodiques des objets UAO. Le mode P/S est pris en charge par des VCR P/S.

Dans l'éditeur (Publisher), les VCR correspondantes ont des attributs pour définir l'heure d'envoi des données périodiques (DataUpdateRate) et il convient que le gestionnaire de réseau (NM) ainsi que la tête de groupe allouent des ressources de communication à l'appareil en fonction de son attribut. Dans l'abonné (Subscriber), les VCR correspondantes ont des attributs incluant les informations d'adresse respectives des données d'éditeur et des objets UAO d'abonné. Il convient que les données publiées soient transférées aux objets UAO correspondants.

Le processus de communication P/S est représenté à la Figure 74 et à la Figure 75. La Figure 74 représente le processus de communication P/S lorsque les appareils désactivent la fonction d'agrégation. La Figure 75 représente le processus de communication P/S lorsque les appareils activent la fonction d'agrégation.

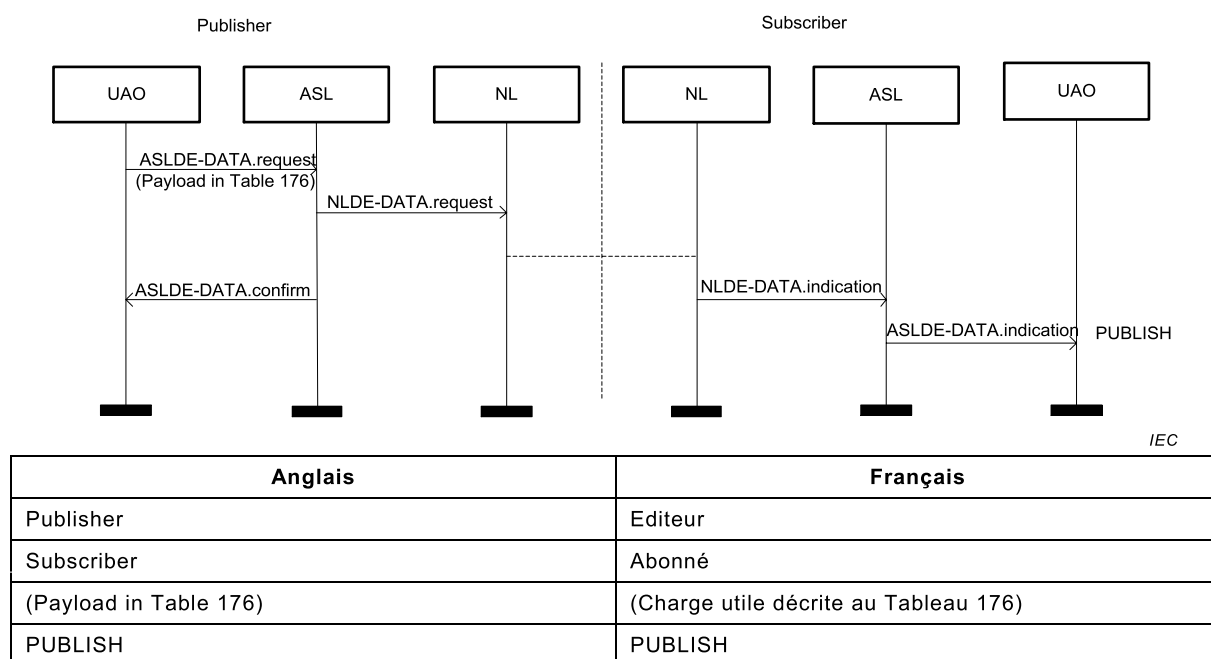


Figure 74 – Processus de communication P/S (fonction d'agrégation désactivée)

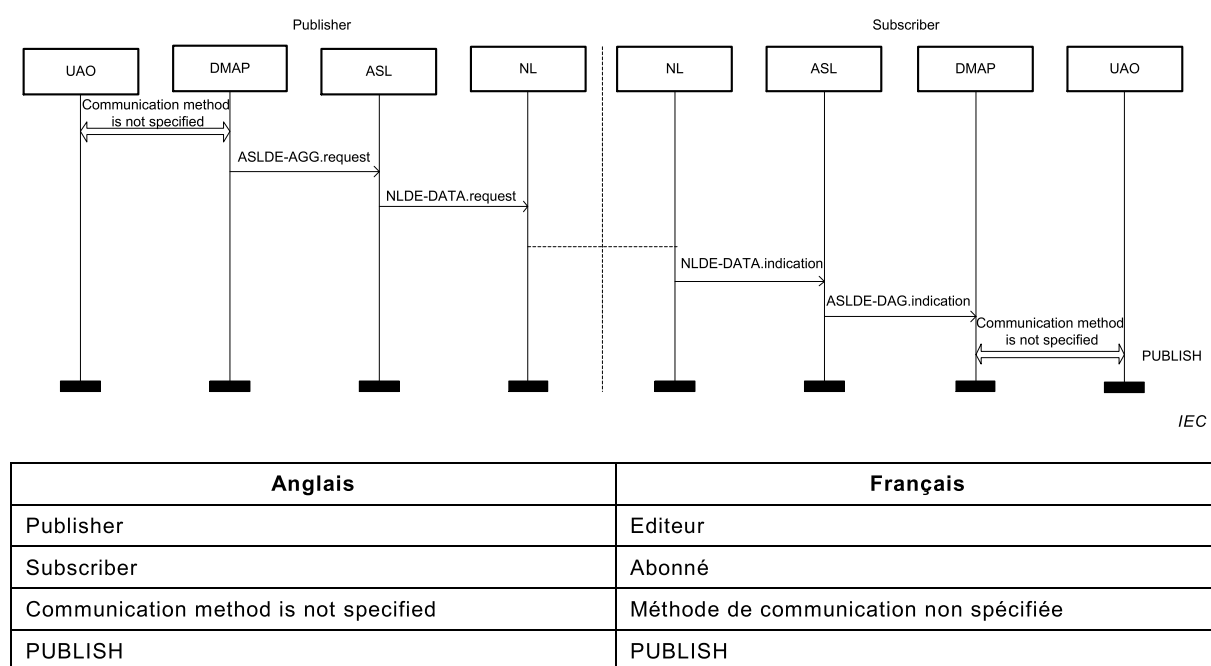


Figure 75 – Processus de communication P/S (fonction d'agrégation activée)

10.3.2.7.4 Mode de communication Report source/Sink (source/puits de rapport)

La sous-couche application (ASL) fournit le mode R/S pour prendre en charge les rapports sur les alarmes ou les événements alarmes aperiodiques et rapporter les acquittements des objets UAO. Le mode R/S est pris en charge par les VCR R/S.

En mode R/S, il convient que l'objet UAO envoie l'alarme ou l'événement qu'il a produit via une VCR R/S allouée. En R/S, il convient que l'alarme ou l'événement reçu soit transféré aux objets UAO correspondants.

Le processus de communication R/S est représenté à la Figure 76.

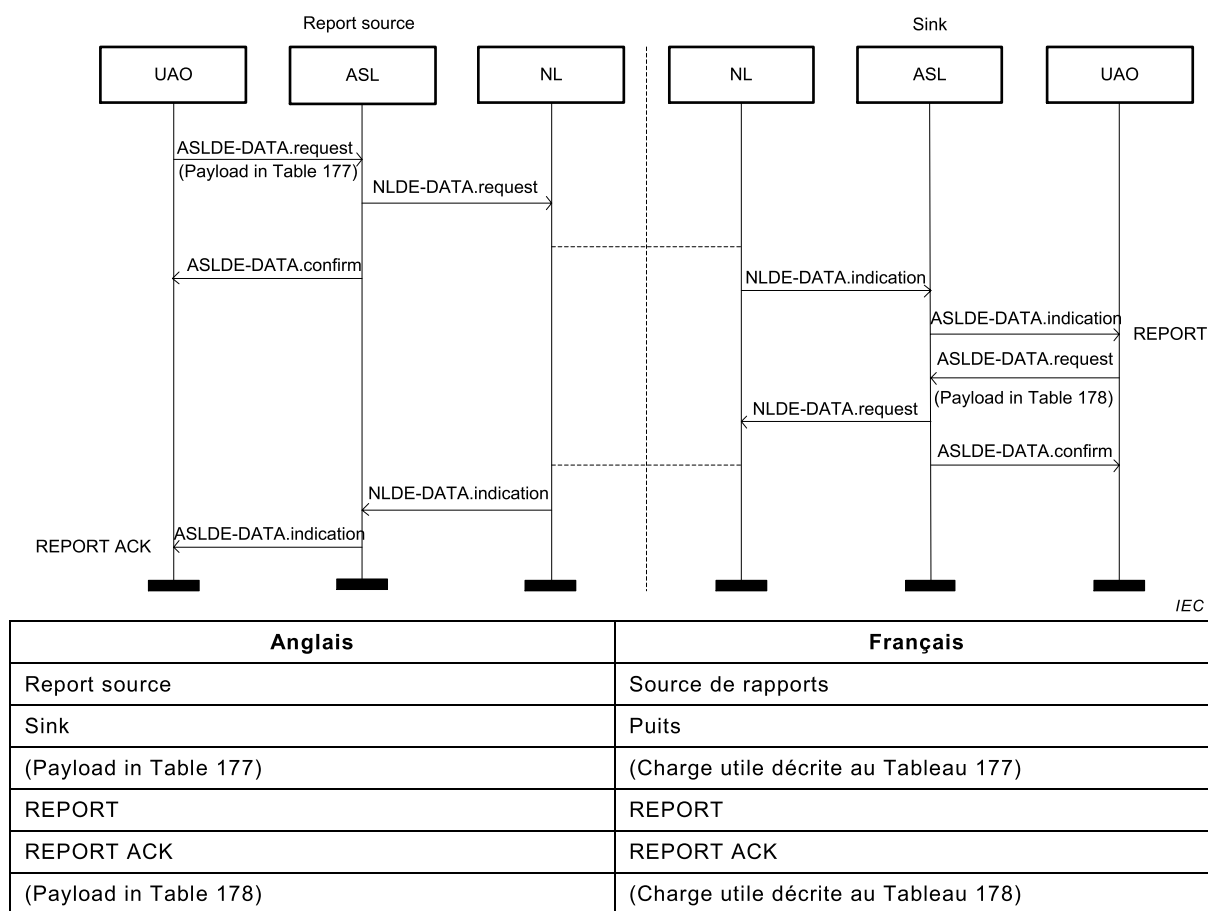


Figure 76 – Processus de communication R/S

10.4 Formats des paquets de la sous-couche application (ASL)

10.4.1 Généralités

La présente partie spécifie les formats des paquets de la sous-couche application (ASL). Chaque paquet de la sous-couche application (ASL) comprend deux parties:

- En-tête de paquet de la sous-couche application (En-tête ASL): il comprend les champs Packet control (contrôle de paquet), Sequence number (numéro séquentiel), Method identifier (identificateur de méthode) et Payload length (longueur de charge utile);
- Charge utile de paquet de la sous-couche application (Charge utile ASL): sa longueur est variable.

10.4.2 Format de paquet général ASL

10.4.2.1 Généralités

Le format du paquet général ASL est indiqué au Tableau 184.

Tableau 184 – Format de paquet général de la sous-couche application (ASL)

	Format de paquet général ASL				
	EN-tête ASL				ASL payload (charge utile ASL)
Longueur en octet(s)	1	1	1	2	Longueur variable
Nom de champ	Paquet contrôle	Sequence Number (numéro séquentiel)	Method identifier (identificateur de méthode)	Payload length (longueur de charge utile)	Payload (charge utile)

Le paquet général ASL comporte les champs ou sous-champs suivants:

- a) ASL packet head (en-tête de paquet ASL), dont les sous-champs suivants:
- Packet control (contrôle de paquet): ce sous-champ a une longueur de 1 octet et est décrit dans le Tableau 185;
 - Sequence number (numéro séquentiel): ce sous-champ a une longueur de 1 octet et indique le numéro séquentiel du paquet ASL;
 - Method identifier (identificateur de méthode): ce sous-champ a une longueur de 1 octet et indique l'identificateur de la méthode (voir 10.2.3);
 - Payload length (longueur de charge utile): ce sous-champ a une longueur de 2 octets et est utilisé pour indiquer la longueur de charge utile de la sous-couche application (ASL);
- b) ASL payload (charge utile ASL): ce sous-champ a une longueur variable et est utilisé pour remplir les données de la sous-couche application (ASL).

10.4.2.2 Champ contrôle de paquet ASL

10.4.2.2.1 Généralités

La longueur du champ contrôle de paquet est de 8 bits. Le format du champ contrôle de paquet est donné au Tableau 185.

Tableau 185 – Format du champ contrôle de paquet

Longueur en bit(s)	Format du champ contrôle de paquet			
	2	1	1	4
Nom de sous-champ	Packet type (type de paquet)	Security (sécurité)	ACK	Réservé

Le champ Packet control (contrôle de paquet) comporte les sous-champs Packet type (type de paquet), Security (sécurité), ACK ainsi que des sous-champs Reserved (réservés) qu'il convient de décrire dans les paragraphes suivants.

10.4.2.2.2 Sous-champ Packet type (type de paquet)

La longueur du sous-champ Packet type (type de paquet) est de 2 bits. Sa valeur est donnée au Tableau 186.

Tableau 186 – Valeur du sous-champ Packet type (type de paquet)

Valeur de type de paquet b0b1	Nom du type de paquet
00	Données
01	Réservé
10	Acquittement
11	Paquet agrégé

10.4.2.2.3 Sous-champ Security (sécurité)

La longueur du sous-champ Security (sécurité) est de 1 bit. Le sous-champ Security (sécurité) sert à contrôler si, oui ou non; la couche application (AL) utilise la fonction de sécurité lors de l'émission de données. Si le sous-champ Security (sécurité) (à savoir b2) est mis à 0, il indique que l'AL n'utilise pas d'opération de sécurité; si b2 est 1, il indique que l'AL utilise l'opération de sécurité pour chiffrer la partie charge utile de données du paquet d'application.

10.4.2.2.4 Sous-champ Acknowledgement (acquittement)

La longueur du sous-champ Acknowledgement (acquittement) est de 1 bit. Il est utilisé pour indiquer si, oui ou non, l'acquittement de paquet d'application est nécessaire. Si le sous-champ Acknowledgement (acquittement) (à savoir b3) est mis à 0, il indique que l'acquittement n'est pas nécessaire; si ce bit a pour valeur 1, il indique que l'acquittement est nécessaire.

10.4.2.3 Champ Sequence number (numéro séquentiel)

La longueur du champ Sequence number (numéro séquentiel) est de 1 octet. Il convient que la sous-couche ASL maintienne le numéro séquentiel des paquets. Si elle émet un paquet AL, il convient que le numéro séquentiel soit augmenté de la valeur 1. Pour le paquet de données de réponse émis dans le mode de communication C/S, son numéro séquentiel reste cohérent avec le paquet de demande correspondant. Le numéro séquentiel est utilisé pour faire concorder le paquet d'acquittement de la demande/réponse. Lorsque le numéro séquentiel atteint sa valeur maximale, il convient de la redéfinir sur la valeur 0.

10.4.2.4 Champ Method identifier (identificateur de méthode)

La longueur du champ Method identifier (identificateur de méthode) est de 1 octet (voir Tableau 171).

10.4.2.5 Champ Payload length (longueur de charge utile)

La longueur du champ Payload length (longueur de charge utile) est de 1 octet. Ce champ est utilisé pour indiquer la longueur de la charge utile ASL en octets.

10.4.2.6 ASL payload (charge utile ASL)

La longueur de la charge utile ASL est variable.

10.4.3 Formats de paquet

10.4.3.1 Généralités

Deux types de formats de paquet sont définis dans la sous-couche application (ASL): le paquet de données ASL et le paquet d'acquittement ASL.

10.4.3.2 Paquet de données ASL

10.4.3.2.1 Généralités

Le format du paquet de données ASL est indiqué au Tableau 187.

Tableau 187 – Format du paquet de données ASL

	Format du paquet de données ASL				
	En-tête ASL				ASL payload (charge utile ASL)
Longueur en octet(s)	1	1	1	2	Longueur variable
Nom de champ	Packet control (contrôle de paquet) (Packet type = 0b00) (type de paquet = 0b00)	Sequence Number (numéro séquentiel)	Method identifier (identificateur de méthode)	Payload length (longueur de charge utile)	Data payload (charge utile de données)

L'en-tête ASL du paquet de données comporte les sous-champs Packet control (contrôle de paquet), Sequence number (numéro séquentiel), Method identifier (identificateur de méthode) et Payload length (longueur de charge utile). Des descriptions détaillées de ces sous-champs sont données dans les Paragraphes 10.4.3.2.2 à 10.4.3.2.3.

10.4.3.2.2 Champ ASL header (en-tête ASL) du paquet de données

L'en-tête ASL du paquet de données comporte les champs Packet control (contrôle de paquet), Sequence number (numéro séquentiel), Method identifier (identificateur de méthode) et Payload length (longueur de charge utile). Il convient de définir le sous-champ Packet type (type de paquet) du champ Packet control (contrôle de paquet) sur la valeur 0b00 pour indiquer s'il s'agit d'un paquet de données ASL. Il convient de définir les autres champs en fonction de la primitive ASLDE-DATA.request de la sous-couche application (ASL).

Une fois que la couche application (AL) a émis un paquet de couche application, il convient d'augmenter son numéro séquentiel de la valeur 1. Le numéro séquentiel du paquet de données de réponse qui est émis dans le mode de communication C/S reste cohérent avec le paquet de données de demande correspondant.

10.4.3.2.3 Champ ASL payload (charge utile ASL)

Le champ ASL payload (charge utile ASL) inclut les données de demande de la couche supérieure (voir 10.3.2).

10.4.3.3 Paquet d'acquiescement ASL

L'acquiescement est utilisé pour confirmer si oui ou non l'appareil de destination a reçu le paquet. Si l'acquiescement n'est pas retourné au bout d'une certaine durée (configurable par EtoEACKTimeout, voir 6.9.1.2.1), il convient que l'appareil source tente à nouveau d'émettre le paquet précédent.

Pour le paquet de données envoyé par le mode P/S, le paquet de diffusion et le paquet d'acquiescement, la sous-couche application (ASL) n'a pas besoin d'être acquittée et le sous-champ Acknowledgement (acquiescement) du champ Packet control (contrôle de paquet) est mis à la valeur 0.

La sous-couche ASL indique que le paquet courant a besoin d'être acquitté en mettant le sous-champ Acknowledgement (acquiescement) du champ Packet control (contrôle de paquet) à la valeur 1.

Après avoir reçu le paquet AL nécessitant être acquitté, il convient que la sous-couche ASL locale le confirme en retournant un paquet d'acquiescement. Il convient que le numéro de séquence du paquet d'acquiescement soit le même que celui dans le paquet de demande correspondant.

Le format du paquet d'acquiescement est décrit au Tableau 188.

Tableau 188 – Format du paquet d'acquiescement ASL

	Format du paquet d'acquiescement ASL			
	ASL header (en-tête ASL)			
Longueur en octet(s)	1	1	1	2
Nom de champ	Packet control (contrôle de paquet) (Packet type = 0b10) (type de paquet = 0b10)	Sequence Number (numéro séquentiel)	Method identifier (identificateur de méthode)	Payload length (longueur de charge utile)

The acknowledgement packet has only the ASL header, which includes the following subfields.

- Packet control (contrôle de paquet): ce sous-champ a une longueur de 1 octet et est décrit dans le Tableau 185. Il convient de définir le sous-champ Packet type (type de paquet) du champ Packet control (contrôle de paquet) sur la valeur 0b10 pour indiquer s'il s'agit d'un paquet d'acquiescement. Si la sécurité est utilisée, il convient de définir le sous-champ Security (sécurité) sur la valeur 1; sinon, il convient de le définir sur la valeur 0.
- Sequence number (numéro séquentiel): ce sous-champ a une longueur de 1 octet et indique le numéro séquentiel du paquet d'acquiescement ASL; il convient que le sous-champ Sequence number (numéro séquentiel) soit identique à celui figurant dans le paquet de demande reçu correspondant.
- Method identifier (identificateur de méthode): ce sous-champ a une longueur de 1 octet et indique l'identificateur de la méthode (voir 10.2.3); l'identificateur de méthode du paquet d'acquiescement est 0b04.
- Payload length (longueur de charge utile): ce sous-champ a une longueur de 2 octets et est utilisé pour indiquer la longueur de charge utile de la sous-couche application (ASL); la longueur de charge utile du paquet d'acquiescement est 0.

11 Sécurité

11.1 Généralités

Avant d'établir les stratégies de sécurité et les mesures de sécurité pour le réseau WIA-PA, il convient d'analyser les exigences de sécurité, les principes de sécurité et les objectifs de sécurité du réseau WIA-PA. Pour connaître la recommandation concernant l'analyse du risque lié à la sécurité du réseau WIA-PA, les principes de sécurité et les objectifs de la sécurité, voir les Articles A.1 à A.3.

La couche MAC du réseau WIA-PA applique les services de sécurité définis dans la couche MAC de l'IEEE 802.15.4-2011. Les couches supérieures du réseau WIA-PA fournissent les services de sécurité suivants:

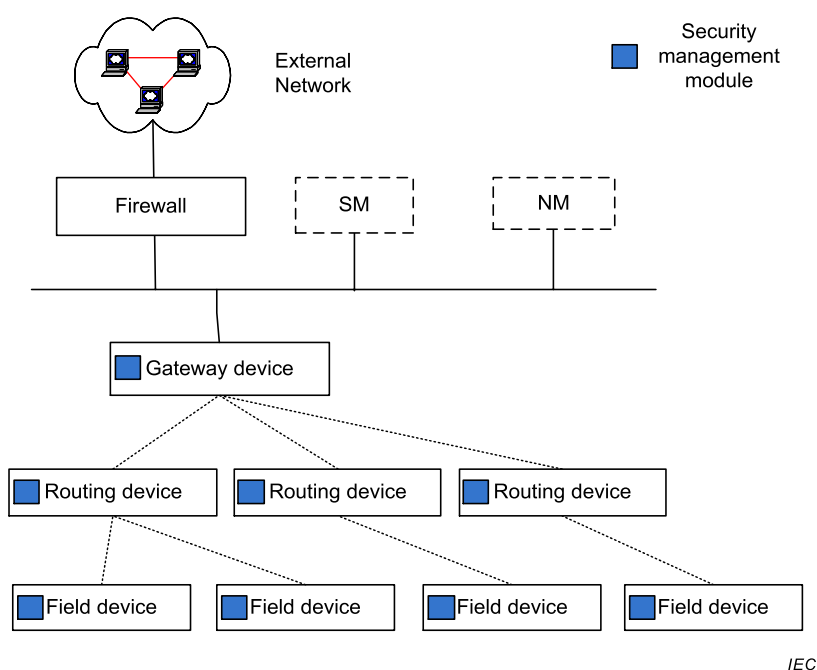
- Intégrité des données. Le service de vérification de l'intégrité des données est fourni dans la couche AL et la sous-couche DLSL. Un appareil source génère un code de contrôle à l'aide d'un algorithme de vérification; l'appareil de destination vérifie le code de contrôle et juge si le paquet reçu a été compromis ou non.
- Confidentialité des données. Le service de confidentialité des données est fourni dans la couche AL et la sous-couche DLSL. Un appareil source chiffre les paquets en utilisant un algorithme à clé symétrique et envoie les paquets chiffrés. L'appareil de destination déchiffre les paquets chiffrés en utilisant le même algorithme à clé symétrique.

- c) Authentification d'appareil. Le SM utilise les renseignements de sécurité pour authentifier un appareil. Les renseignements de sécurité sont générés par la clé de rattachement (KJ) et l'adresse longue. Il convient qu'il soit irréversible.

La définition de l'algorithme de vérification et de l'algorithme à clé symétrique n'est pas couverte dans le présent document.

11.2 Cadre de travail de gestion de la sécurité

Compte tenu de l'exigence de temps réel et des ressources limitées des appareils, le réseau WIA-PA a besoin de stratégies de sécurité et de mesures différentes qui doivent être réalisées dans des couches différentes. Pour connaître la recommandation concernant les mesures graduées et stratifiées du système et les mesures graduées des paquets sûrs, voir l'Article A.4. Le cadre de travail de la gestion de la sécurité pour le réseau WIA-PA est représenté à la Figure 77.



Anglais	Français
External network	Réseau extérieur
Security management module	Module de gestion de la sécurité
Firewall	Pare-feu
SM	Gestionnaire de sécurité (SM)
NM	Gestionnaire de réseau (NM)
Gateway device	Appareil passerelle
Routing device	Appareil de routage
Field device	Appareil de terrain

Figure 77 – Cadre de travail de la gestion de la sécurité pour le réseau WIA-PA

Comme indiqué à la Figure 77, le cadre de travail de la gestion de la sécurité est constitué d'un gestionnaire de sécurité (SM) et de modules de gestion de la sécurité figurant dans l'appareil de passerelle, les appareils de routage et les appareils de terrain.

Le cadre de travail de la gestion de la sécurité interagit avec des réseaux extérieurs par l'intermédiaire du pare-feu. Il protège la frontière du réseau WIA-PA tout entier et garantit les

opérations normalisées du réseau WIA-PA. Le pare-feu n'est pas spécifié dans le présent document.

Il convient que le gestionnaire de sécurité (SM) configure les mesures de sécurité du réseau WIA-PA, gère les clés et authentifie les appareils. Il assure les fonctions suivantes:

- a) configurer les stratégies de sécurité du système et les mesures de sécurité du réseau WIA-PA en fonction d'applications spécifiques;
- b) configurer et surveiller l'appareil de passerelle et les appareils de routage selon les applications spécifiques et les stratégies de sécurité du système;
- c) autoriser les appareils de routage et appareils de terrain qui tentent de se rattacher au réseau WIA-PA;
- d) assurer la gestion des clés, y compris la création de clés, la distribution de clés, la récupération de clés et la mise à jour de clés.

Le module de gestion de la sécurité de l'appareil de passerelle assure les fonctions suivantes:

- a) gérer ses propres mesures de sécurité;
- b) assumer les fonctions du module de gestion de la sécurité dans les appareils de routage.

Le module de gestion de la sécurité de l'appareil de routage assure les fonctions suivantes:

- a) gérer les clés utilisées par le groupe et transférer les clés allouées par le SM;
- b) mettre en œuvre les mesures de sécurité de chiffrement des données, de déchiffrement et de vérification de l'intégrité des données;
- c) envoyer la demande d'authentification.

Le module de gestion de la sécurité de l'appareil de terrain assure les fonctions suivantes:

- a) gérer les mesures de sécurité de la sous-couche DLSL et de la sous-couche ASL;
- b) mettre en œuvre les mesures de sécurité de chiffrement des données, de déchiffrement et de vérification de l'intégrité des données;
- c) gérer les clés.

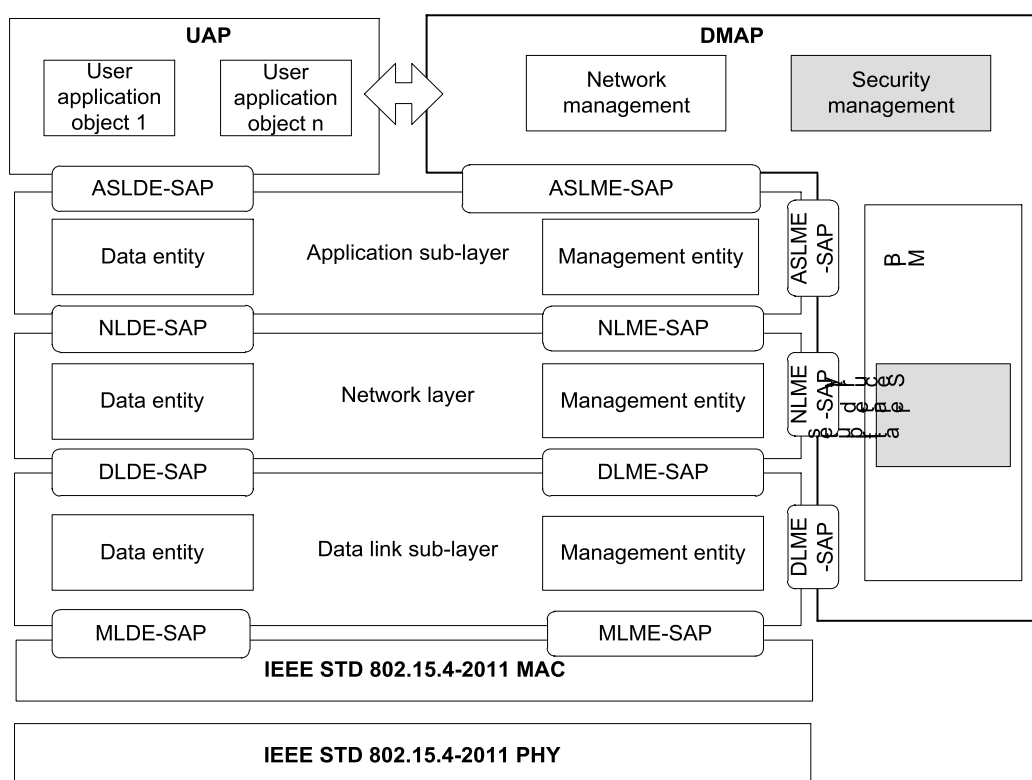
Les appareils de routage et les appareils de terrain fournissent également une fonction de rapport sur l'alerte. Lorsque le nombre d'attaques atteint la valeur MaxAttackedCnt ou que le paramètre KeyAttackCnt atteint la valeur MaxKeyAttackedCnt, il convient que les appareils de routage/appareils de terrain rapportent une alerte à l'appareil de passerelle en utilisant le service NLME_INFO_SET.

Les appareils redondants se connectent par câbles aux appareils principaux. L'appareil redondant possède la même clé de rattachement (KJ) que l'appareil principal. Lorsqu'une authentification de sécurité est nécessaire, l'appareil principal utilise l'adresse longue de l'appareil redondant et la clé de rattachement (KJ) pour authentifier le second.

11.3 Pile de protocole de communications sécurisées

11.3.1 Généralités

La pile de protocole de communications sécurisées inclut les mesures de sécurité pour chaque couche. Les clés sont stockées dans la base MIB (voir Tableau 23). En coordination avec le SM, le module de gestion de la sécurité du DMAP assure également la gestion et la maintenance des clés (voir 11.4). La sous-couche DLSL et la sous-couche ASL gèrent le transport sécurisé de manière indépendante. La pile de protocole de communications sécurisées est indiquée à la Figure 78, les modules gris étant liés à la sécurité. Les attributs relatifs à la sécurité dans la base MIB sont définis en tant que base d'informations de gestion de la sécurité. Le module de gestion de la sécurité utilise les services d'établissement des attributs de réseau pour régler la base d'informations de gestion de la sécurité.



IEC

Anglais	Français
User application object 1	Objet d'application utilisateur 1
User application object n	Objet d'application utilisateur n
Network management	Gestion de réseau
Security management	Gestion de sécurité
Data entity	Entité de données
Application sub-layer	Sous-couche application (ASL)
Management entity	Entité de gestion
MIB	Base d'informations de gestion (MIB)
Network layer	Couche réseau (NL)
Security related attributes	Attributs relatifs à la sécurité
Data link sub-layer	Sous-couche liaison de données (DLSL)
IEEE STD 802.15.4-2011 MAC	MAC selon l'IEEE 802.15.4-2011
IEEE STD 802.15.4-2011 PHY	PHY selon l'IEEE 802.15.4-2011

Figure 78 – Pile de protocole de communication en sécurité

11.3.2 Sécurité de la sous-couche liaison de données

11.3.2.1 Généralités

Les mesures de sécurité sont fournies par la sous-couche DLSL dans le réseau WIA-PA. La sécurité de la couche MAC est désactivée. La sous-couche DLSL utilise le chiffrement de données et le code d'intégrité de message (MIC) CCM pour garantir la sécurité du transport point à point, où le compteur de trames est remplacé par le nombre d'intervalles de temps absolu (ASN). Le MIC est généré avec les clés DLSL, l'en-tête DLSL et la charge utile DLSL. Il sert à la vérification de l'intégrité des messages. Le chiffrement des données est utilisé pour la confidentialité des données. L'obtention de clé de chiffrement est mise en œuvre par les services d'obtention d'attribut de réseau (voir 9.5.13).

Le gestionnaire de sécurité peut configurer ou lire la clé des appareils en utilisant le service NLME_INFO_SET ou NLME_INFO_GET.

11.3.2.2 Sécurité des trames de la sous-couche liaison de données

Le format d'une DLPDU de sécurité est indiqué au Tableau 189.

Tableau 189 – Format d'une DLPDU de sécurité

	Format d'une DLPDU de sécurité			
Longueur en octet(s)	1	1	Longueur variable	0/4/8/16
Nom de sous-champ	DLSL frame control (contrôle de trame DLSL)	DLSL security header (en-tête de sécurité DLSL)	DLSL payload (charge utile DLSL)	MIC

Si le sous-champ Security enabled (sécurité activée) du champ DLSL frame control (contrôle de trame DLSL) est mis à 1, il convient d'utiliser l'en-tête de sécurité DLSL (voir Tableau 190).

Tableau 190 – Format de l'en-tête de sécurité DLSL

	Format de l'en-tête de sécurité DLSL		
Longueur en bit(s)	3	2	3
Nom de sous-champ	Security control (contrôle de sécurité)	Security material control (contrôle des renseignements de sécurité)	Réservé

La taille du champ Security control (contrôle de sécurité) est de 3 bits (voir Tableau 191). Le champ Security control (contrôle de sécurité) définit les attributs de sécurité.

Tableau 191 – Structure du champ Security control (contrôle de sécurité) dans l'en-tête de sécurité DLSL

Champ Security control (contrôle de sécurité) b2b1b0	Attributs de sécurité
000	Aucune
001	MIC-32
010	MIC-64
011	MIC-128
100	ENC
101	ENC-MIC-32
110	ENC-MIC-64
111	ENC-MIC-128

Si le chiffrement et la vérification du MIC sont fournis, l'émetteur calcule d'abord le MIC et chiffre ensuite les trames. Par ailleurs, il convient que le destinataire déchiffre les trames et vérifie ensuite le MIC.

Le champ Security material control (contrôle des renseignements de sécurité) définit le type de paquet du service des renseignements de sécurité de l'appareil (voir Tableau 192).

Tableau 192 – Structure du champ Security material control (contrôle des renseignements de sécurité) dans l'en-tête de sécurité DLSL

Champ Security material control (contrôle des renseignements de sécurité) b1b0	Attributs de sécurité
00	Paquet de données
01	Paquet de demande d'obtention des renseignements de sécurité de l'appareil
10	Paquet de réponse d'obtention des renseignements de sécurité de l'appareil
11	Réservé

11.3.3 Sécurité de la sous-couche application (ASL)**11.3.3.1 Généralités**

La sécurité de la sous-couche application (ASL) met en œuvre la sécurité du transport de données de bout en bout. La sous-couche ASL utilise le chiffrement de données et le code d'intégrité de message (MIC) CCM pour garantir la sécurité du transport de bout en bout, où le compteur de trames est remplacé par le nombre d'intervalles de temps absolu (ASN). La sous-couche ASL établit et gère les clés dans la base d'informations de gestion de la sécurité. Le MIC est généré avec les clés ASL et la charge utile ASL. Il sert à la vérification de l'intégrité des messages.

11.3.3.2 Sécurité des paquets de la sous-couche application (ASL)

La structure d'une APDU de sécurité est décrite au Tableau 193.

Tableau 193 – Structure d'une APDU de sécurité

	Structure d'une APDU de sécurité			
Longueur en octet(s)	5	1	Longueur variable	0/4
Nom de champ	ASL header (en-tête ASL)	ASL security header (en-tête de sécurité ASL)	ASL payload (charge utile ASL)	MIC

Si le sous-champ Security enabled (sécurité activée) du champ Packet control (contrôle de paquet) de l'en-tête ASL est mis à 1, il convient d'utiliser l'en-tête de sécurité DLSL (voir Tableau 194).

Tableau 194 – Structure du champ ASL security header (en-tête de sécurité ASL)

Bits: 0 à 1	2 à 7
00 = NONE (aucun) 01 = ENC 10 = MIC-32 11 = ENC-MIC-32	Réservé

Si le chiffrement et la vérification du MIC sont fournis, l'émetteur calcule d'abord le MIC et chiffre ensuite les trames. Par ailleurs, il convient que le destinataire déchiffre les trames et vérifie ensuite le MIC.

11.4 Gestion de clés

11.4.1 Type de clé

Le gestionnaire de sécurité (SM) et les modules de gestion de la sécurité gèrent les clés utilisées dans le réseau WIA-PA. Les clés cryptographiques suivantes sont définies.

a) Clé de rattachement (KJ)

Il s'agit d'une clé provisoire utilisée lors du rattachement d'un appareil. La clé KJ est établie durant le processus de mise en service. Elle est distribuée par le gestionnaire de sécurité (SM) par l'intermédiaire des appareils tenus à la main. Elle est utilisée pour chiffrer l'adresse longue 64 bits du nouvel appareil afin de produire les renseignements de sécurité. Lorsque l'appareil a réussi à se rattacher au réseau, la clé KJ sert également à protéger la clé de chiffrement de clé (KEK) lorsque la clé KEK est distribuée pour la première fois.

b) Clé de partage (KS)

Il s'agit d'une clé de partage possédant une valeur unifiée. La clé KS est établie durant le processus de mise en service. Elle est distribuée par le gestionnaire de sécurité (SM) par l'intermédiaire des appareils tenus à la main. Elle est utilisée pour chiffrer la trame balise et la trame de diffusion. Durant le processus de rattachement, le gestionnaire de sécurité (NM) retournera le résultat du rattachement; lors du dernier saut, la clé KS est utilisée pour chiffrer la réponse de rattachement par l'appareil de routage en ligne ou l'appareil de passerelle.

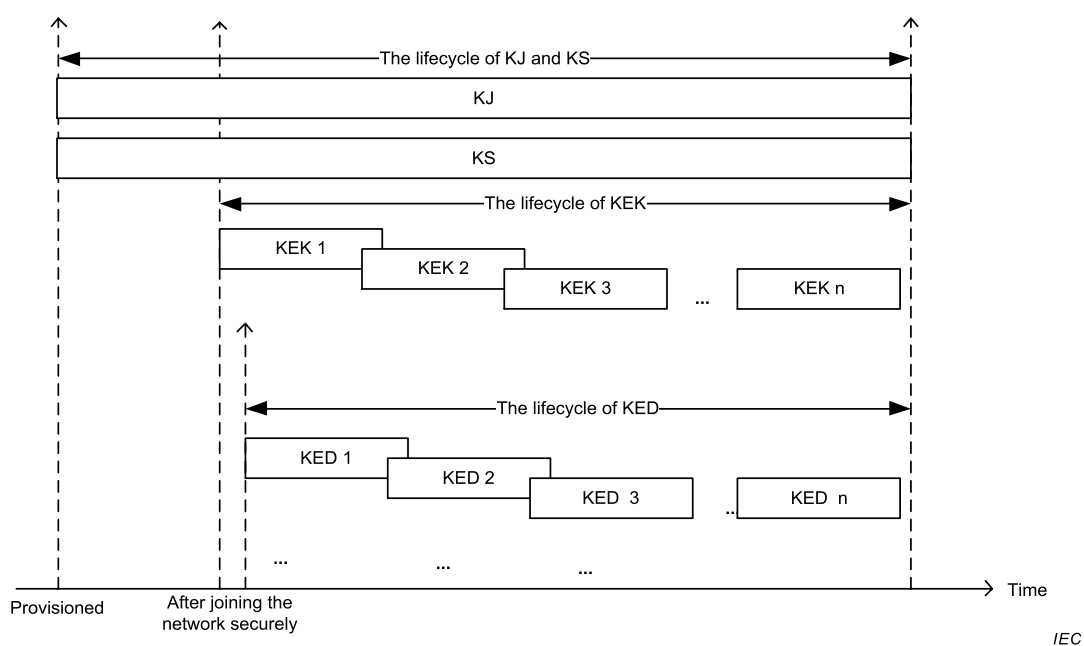
c) Clé de chiffrement de clé (KEK)

La clé KEK est distribuée par le gestionnaire de sécurité (SM) après qu'un appareil ait rejoint le réseau WIA-PA. Elle est utilisée pour chiffrer les autres clés. Lorsque le gestionnaire de sécurité (SM) distribue la clé KEK pour la première fois, la clé KEK est protégée par une clé de rattachement (KJ). Après quoi, la nouvelle clé KEK est protégée par la clé KEK qui est actuellement utilisée lors de sa période de mise à jour.

d) Clé de chiffrement de données (KED)

La clé KED est distribuée par le gestionnaire de sécurité (SM) après qu'un appareil ait rejoint le réseau WIA-PA, ce qui inclut la clé de chiffrement DLSL et la clé de chiffrement AL. Elle est utilisée pour protéger les données et vérifier l'intégrité lors de la transmission des données. La clé KED est protégée par la clé de chiffrement de clé (KEK) lors de ses périodes de distribution et mise à jour.

Le cycle de vie des clés est représenté à la Figure 79.



IEC

Anglais	Français
The lifecycle of KJ and KS	Cycle de vie des clés KJ et KS
The lifecycle of KEK	Cycle de vie des clés KEK
The lifecycle of KED	Cycle de vie des clés KED
Provisioned	Mise en service
After joining the network securely	Après rattachement sécurisé au réseau
Time	Temps

Figure 79 – Cycle de vie des clés

Les clés KEK et KED ont besoin d'être mises à jour régulièrement par le gestionnaire de sécurité (SM) en réglant les paramètres de clé dans la base MIB (voir Tableau 23).

11.4.2 Distribution de clés

Avant qu'un appareil ne rejoigne le réseau, il convient que la clé KJ soit distribuée à l'appareil. Il convient que la clé KJ soit directement distribuée par les appareils tenus à la main.

Après qu'un appareil ait rejoint le réseau WIA-PA, il convient que les clés KEK et KED soient distribuées aux appareils rattachés par le gestionnaire de sécurité (SM). La distribution de clés est mise en œuvre par les services d'établissement d'attribut de réseau (voir 9.5.14).

11.4.3 Mise à jour de clé

Lorsque le gestionnaire de sécurité (SM) a besoin de mettre à jour une clé d'appareil, il convient de générer une nouvelle clé. Ensuite, la nouvelle clé est chiffrée par la clé KEK et la nouvelle clé chiffrée est distribuée à l'appareil WIA-PA SM en utilisant les services d'établissement d'attribut de réseau (voir 9.5.14).

Une fois la nouvelle clé distribuée, il convient que l'appareil déchiffre la nouvelle clé chiffrée avec sa clé de chiffrement de clé (KEK) et mette à jour sa clé.

Le cycle de mise à jour de clés est déterminé par les utilisateurs en fonction de leurs exigences et il convient qu'il ne dépasse pas 24 h.

La nouvelle clé exige les propriétés suivantes.

- a) Il convient que la nouvelle clé soit différente des clés utilisées par d'autres appareils du réseau WIA-PA.
- b) Il convient que la nouvelle clé soit garantie comme étant la plus récente.
- c) Il convient que la nouvelle clé soit envoyée aux appareils associés dans les temps.

11.4.4 Etat de clé

De son établissement à son abolition, il convient que la clé passe par les états suivants:

- a) **BACKUP**: cet état est défini dès lors que la clé a été établie, mais n'a pas été utilisée pour le fonctionnement normal;
- b) **USING**: cet état est défini dès lors qu'une clé est en cours d'utilisation;
- c) **INVALID**: cet état est défini dès lors qu'une clé n'est pas disponible.

Lorsque le paramètre KeyActiveTime (voir Tableau 23) d'une clé à l'état BACKUP est atteint, la clé passe de l'état BACKUP à l'état USING. Parallèlement, la clé à l'état USING (s'il en existe une) passe à l'état INVALID.

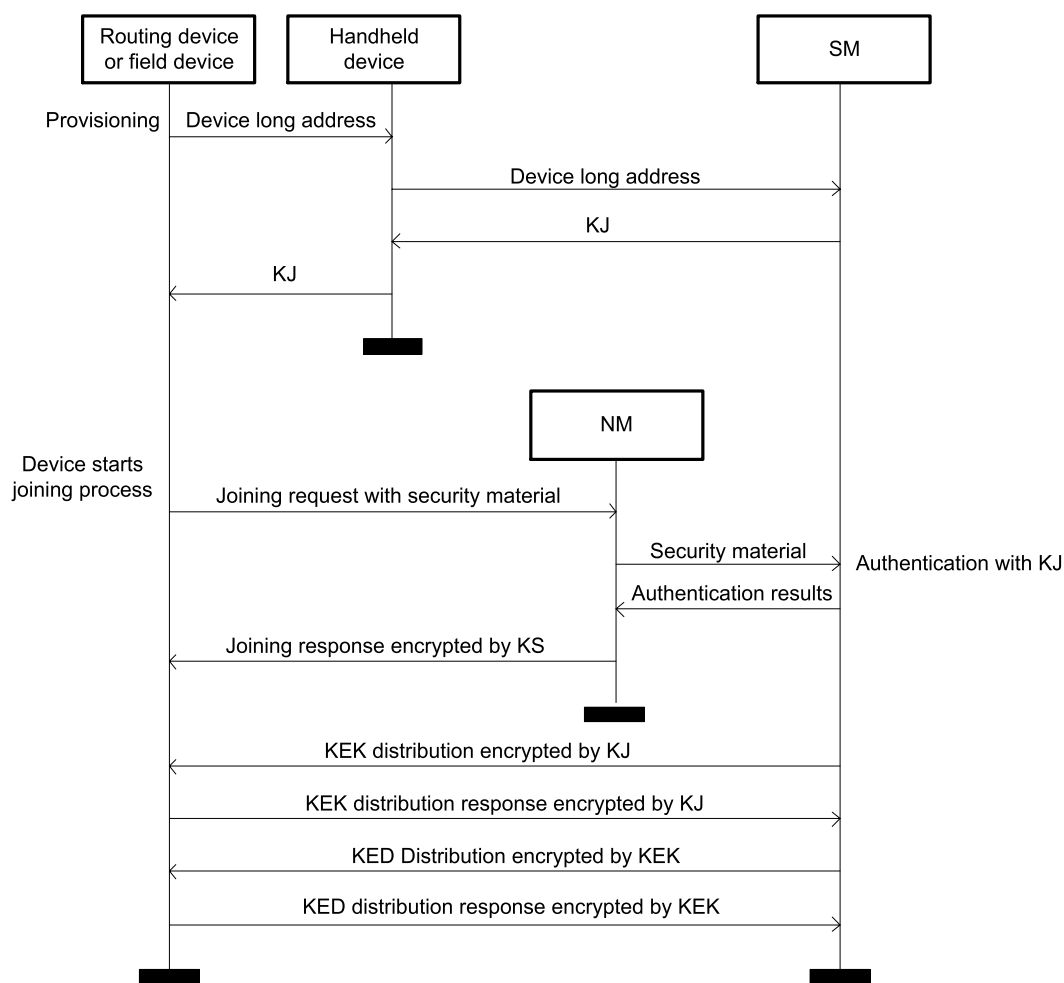
11.5 Processus de rattachement sécurisé

11.5.1 Processus de rattachement sécurisé d'un nouvel appareil WIA-PA

Lorsqu'un nouvel appareil de terrain ou qu'un nouvel appareil de routage se rattache au réseau WIA-PA, il convient que le gestionnaire de sécurité (SM) authentifie le nouvel appareil de terrain ou le nouvel appareil de routage.

Il convient qu'un nouvel appareil soit doté de la clé de rattachement (KJ) et d'une adresse longue de 64 bits avant de se rattacher au réseau WIA-PA. Il convient que la clé de rattachement (KJ) soit écrite par des appareils tenus à la main.

Le processus de rattachement sécurisé d'un nouvel appareil WIA-PA est représenté à la Figure 80.



IEC

Anglais	Français
Routing device or field device	Appareil de routage ou appareil de terrain
Handheld device	Appareil tenu à la main
SM	Gestionnaire de sécurité (SM)
Provisioning	Mise en service
Device long address	Adresse longue de l'appareil
Device starts joining process	L'appareil débute le processus de rattachement.
NM	Gestionnaire de réseau (NM)
Joining request with security material	Demande de rattachement avec renseignements de sécurité
Security material	Renseignements de sécurité
Authentication results	Résultats de l'authentification
Authentication with KJ	Authentification avec la clé KJ
Joining response encrypted by KS	Réponse de rattachement chiffrée par la clé KS
KEK distribution encrypted by KJ	Distribution de clé KEK chiffrée par la clé KJ
KEK distribution response encrypted par KJ	Réponse de distribution de clé KEK chiffrée par clé KJ
KED distribution encrypted by KEK	Distribution de clé KES chiffrée par la clé KEK
KED distribution response encrypted par KEK	Réponse de distribution de clé KED chiffrée par clé KEK

Figure 80 – Processus de rattachement sécurisé d'un nouvel appareil WIA-PA

Il convient qu'un nouvel appareil souhaitant rejoindre le réseau WIA-PA procède comme suit:

- a) Avant que le nouvel appareil ne rejoigne le réseau WIA-PA, l'appareil tenu à la main lit l'adresse longue 64 bits du nouvel appareil et la transmet au gestionnaire de sécurité (SM). Le gestionnaire de sécurité (SM) génère la clé de rattachement (KJ) pour le nouvel appareil tandis que l'appareil tenu à la main transmet la clé de rattachement (KJ) au nouvel appareil.
- b) Le nouvel appareil doté de la clé de rattachement (KJ) continue de balayer les canaux disponibles afin de recevoir des balises provenant des appareils de routage en ligne ou de l'appareil de passerelle.
- c) Le nouvel appareil choisit un appareil de routage en ligne ou l'appareil de passerelle comme tête de groupe, puis se synchronise au réseau conformément à la balise reçue.
- d) Le nouvel appareil génère les renseignements de sécurité à partir de l'adresse longue et de la clé de rattachement (KJ), puis les envoie à la tête de groupe. La tête de groupe envoie une demande de rattachement incluant les renseignements de sécurité au gestionnaire de réseau (NM) pour le nouvel appareil.
- e) Lorsque le gestionnaire de réseau (NM) reçoit la demande de rattachement, il convient qu'il transmette les renseignements de sécurité au gestionnaire de sécurité (SM). Le gestionnaire de sécurité (SM) vérifie les renseignements de sécurité. Si l'authentification échoue, le gestionnaire de réseau (NM) retournera la réponse d'échec. Si l'authentification réussit, le gestionnaire de réseau (NM) retournera la réponse de réussite.
- f) Lorsque l'appareil achève le processus de rattachement, il convient que le gestionnaire de sécurité (SM) génère la clé de chiffrement de clé (KEK) pour le nouvel appareil et distribue la clé de chiffrement de clé (KEK) chiffrée par la clé de rattachement (KJ). Il convient ensuite que le gestionnaire de sécurité (SM) génère la clé de chiffrement de données (KED) pour le nouvel appareil et distribue la clé de chiffrement de données (KED) chiffrée par la clé de chiffrement de clé (KEK).

11.5.2 Services d'obtention des renseignements de sécurité de l'appareil

11.5.2.1 DLME-SEC.request

Les appareils de routage utilisent la primitive DLME-SEC.request pour demander les renseignements de sécurité.

La sémantique de DLME-SEC.request est décrite comme suit:

DLME-SEC.request (

DstPhyAddr
)

Le Tableau 195 spécifie les paramètres pour DLME-SEC.request.

Tableau 195 – Paramètres de DLME-SEC.request

Nom	Type de données	Plage valide	Description
DstPhyAddr	Unsigned64	0 à ($2^{64}-1$)	Adresse physique 64 bits du nouvel appareil

11.5.2.2 DLME-SEC.indication

A la réception d'un paquet de demande d'obtention des renseignements de sécurité de l'appareil, la DLSL du nouvel appareil invoquera la primitive DLME-SEC.indication et informera le DMAP.

La sémantique de DLME-SEC.indication est décrite comme suit:

DLME-SEC.indication (
 DstPhyAddr
)

Le Tableau 196 spécifie les paramètres pour DLME-SEC.request.

Tableau 196 – Paramètres de DLME-SEC.indication

Nom	Type de données	Plage valide	Description
DstPhyAddr	Unsigned64	0 à $(2^{64}-1)$	Adresse physique 64 bits du nouvel appareil

11.5.2.3 DLME-SEC.response

Le DMAP du nouvel appareil invoque la primitive DLME-SEC.response pour fournir ses renseignements de sécurité.

La sémantique de DLME-SEC.response est décrite comme suit:

DLME-SEC.response (
 ProxyAddr,
 PhyAddr,
 SecMaterial,
 Statut
)

Le Tableau 197 spécifie les paramètres pour DLME-SEC.response.

Tableau 197 – Paramètres de DLME-SEC.response

Nom	Type de données	Plage valide	Description
ProxyAddr	Unsigned16	0 à 65 535	Adresse de l'appareil de routage choisie par le nouvel appareil (adresse de monodiffusion)
PhyAddr	Unsigned64	0 à $(2^{64}-1)$	Adresse physique 64 bits du nouvel appareil
SecMaterial	Unsigned32	0 à $(2^{32}-1)$	Renseignements de sécurité de l'appareil. Ils sont générés à partir de l'adresse 64 bits chiffrée par la clé KJ. Utilisation des bits 0 à 31
Statut	Unsigned8	0 à 255	Résultat d'exécution de la demande: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

11.5.2.4 DLME-SEC.confirm

A la réception d'un paquet de réponse d'obtention des renseignements de sécurité de l'appareil, la DLSL du nouvel appareil invoquera la primitive DLME-SEC.confirm et informera le DMAP.

La sémantique de DLME-SEC.confirm est décrite comme suit:

DLME-SEC.confirm (

PhyAddr,
SecMaterial,
Statut

)

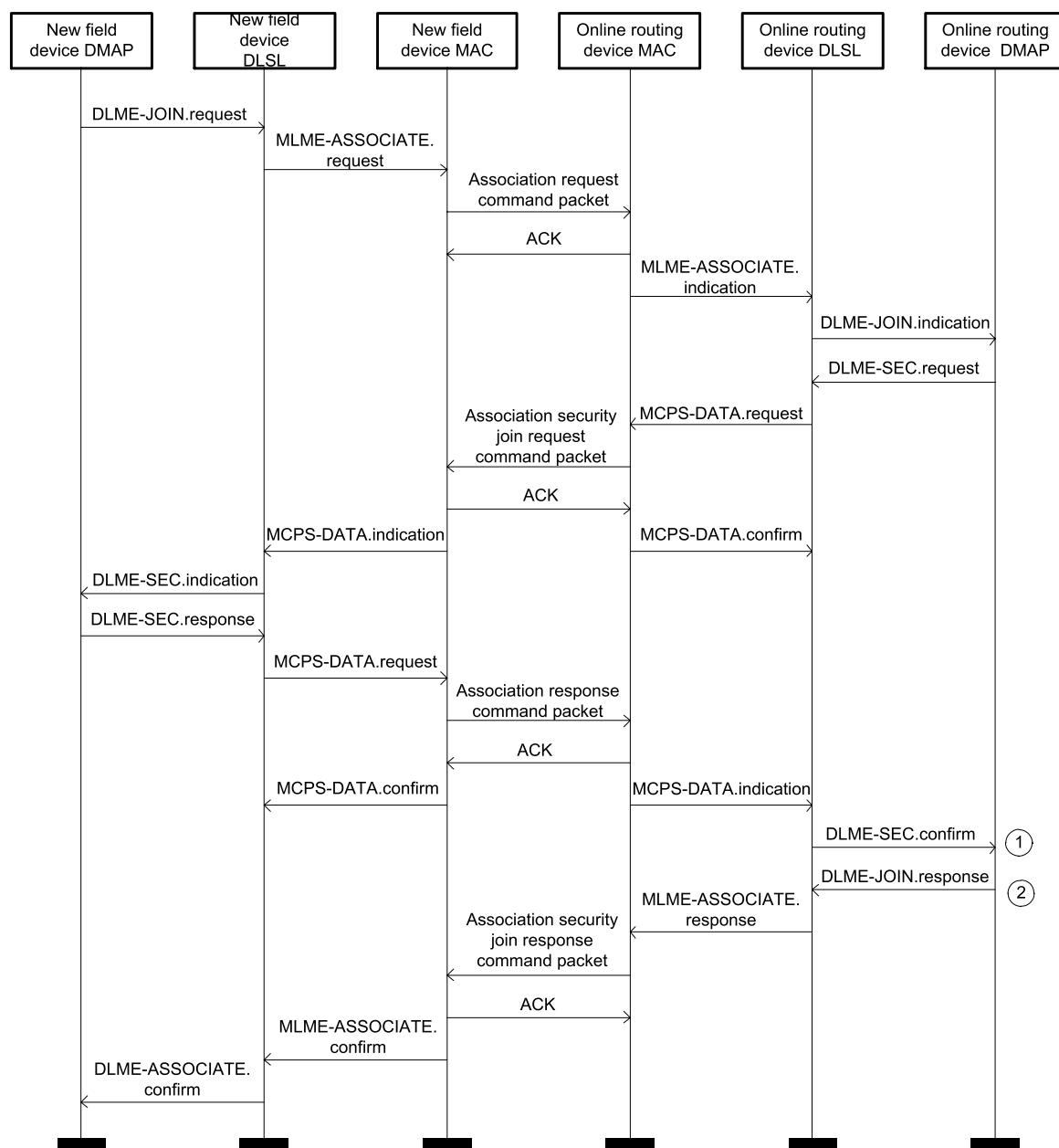
Le Tableau 198 spécifie les paramètres pour DLME-SEC.confirm.

Tableau 198 – Paramètres de DLME-SEC.confirm

Nom	Type de données	Plage valide	Description
PhyAddr	Unsigned64	0 à $(2^{64}-1)$	Adresse de l'appareil de routage choisie par le nouvel appareil (adresse de monodiffusion)
SecMaterial	Unsigned32	0 à $(2^{32}-1)$	Renseignements de sécurité de l'appareil. Ils sont générés à partir de l'adresse 64 bits chiffrée par la clé KJ. Utilisation des bits 0 à 31
Statut	Unsigned8	0 à 255	Résultat d'exécution de la demande: 0 = SUCCESS (succès) 1 = FAILURE (échec) Les autres valeurs sont réservées.

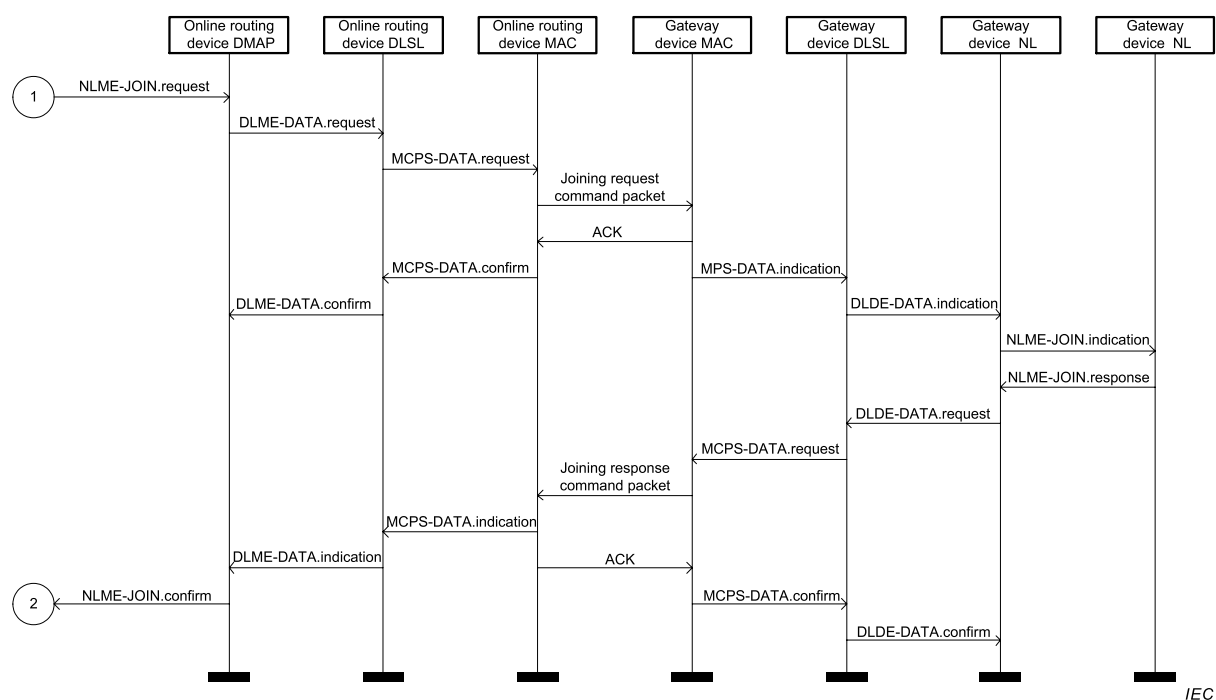
11.5.2.5 Séquence temporelle pour le rattachement sécurité d'appareil

Dans l'architecture en étoile et maillée, si SecEnableFlag = 1 (voir 6.9.1.2.1), la Figure 81 et la Figure 82 représentent des exemples de processus de rattachement sécurisé pour les appareils de terrain.



Anglais	Français
New field device DMAP	DMAP du nouvel appareil de terrain
New field device DLSL	DLSL du nouvel appareil de terrain
New field device MAC	MAC du nouvel appareil de terrain
Online routing device MAC	MAC de l'appareil de routage en ligne
Online routing device DLSL	DLSL de l'appareil de routage en ligne
Online routing device DMAP	DMAP de l'appareil de routage en ligne
Online routing device NL	NL de l'appareil de routage en ligne
Association request command packet	Paquet de commande de demande d'association
Association security join request command packet	Paquet de commande de demande de rattachement sécurisé d'association
Association response command packet	Paquet de commande de réponse d'association
Association security join response command packet	Paquet de commande de réponse de rattachement sécurisé d'association

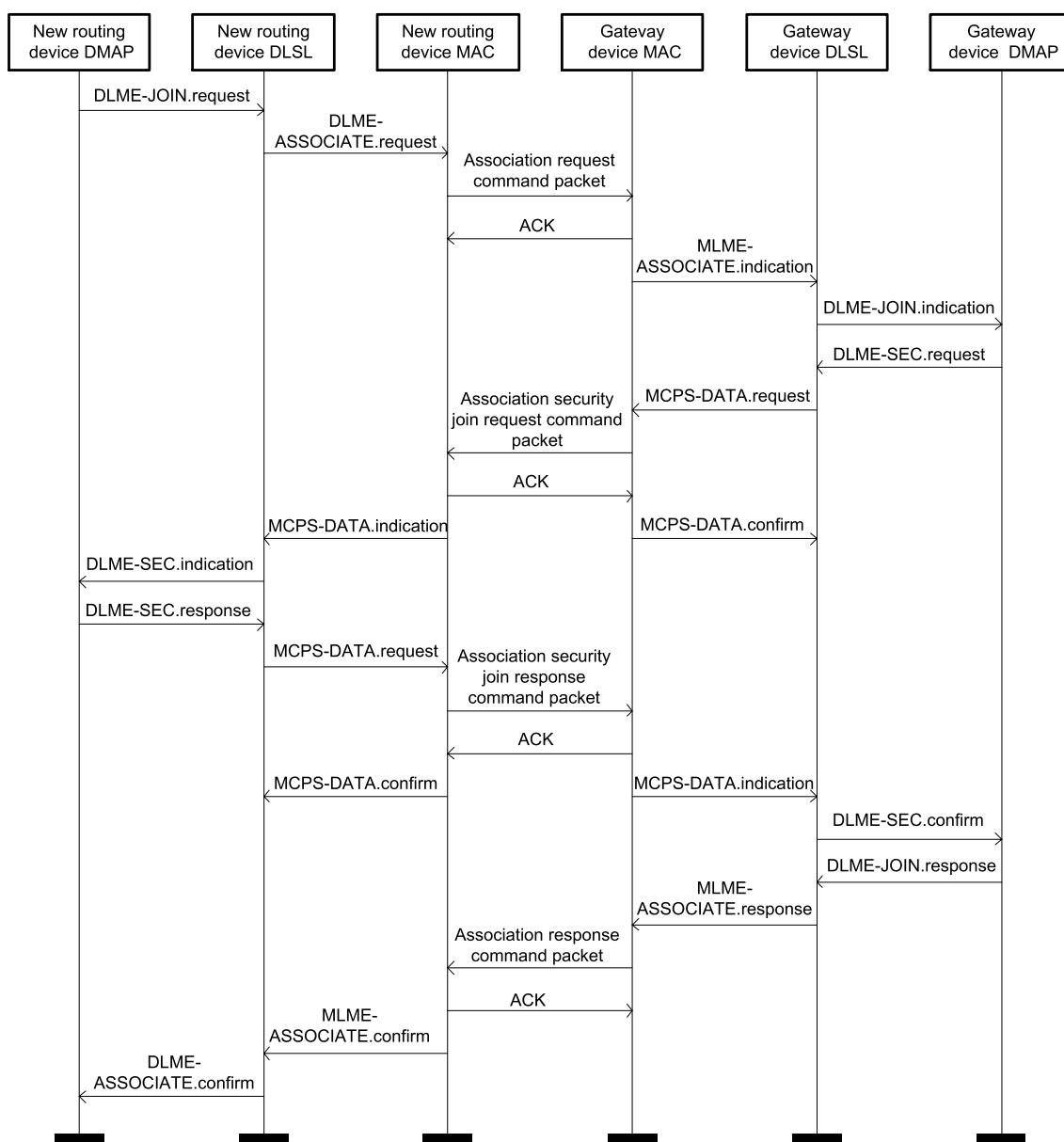
Figure 81 – Séquence temporelle pour le rattachement d'un appareil de terrain (appareil de terrain vers appareil de routage)



Anglais	Français
Online routing device DMAP	DMAP de l'appareil de routage en ligne
Online routing device DLSL	DLSL de l'appareil de routage en ligne
Online routing device MAC	MAC de l'appareil de routage en ligne
Gateway device MAC	MAC de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Joining request command packet	Paquet de commande de demande de rattachement
Joining response command packet	Paquet de commande de réponse de rattachement

Figure 82 – Séquence temporelle pour le rattachement d'un appareil de terrain (appareil de routage vers appareil de passerelle)

La Figure 83, la Figure 84 et la Figure 85 représentent des exemples de processus de rattachement pour un appareil de routage.



IEC

Anglais	Français
New routing device DMAP	DMAP du nouvel appareil de routage
New routing device DLSL	DLSL du nouvel appareil de routage
New routing device MAC	MAC du nouvel appareil de routage
Gateway device MAC	MAC de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device DMAP	DMAP de l'appareil passerelle
Association request command packet	Paquet de commande de demande d'association
Association security join request command packet	Paquet de commande de demande de rattachement sécurisé d'association
Association security join response command packet	Paquet de commande de réponse de rattachement sécurisé d'association
Association response command packet	Paquet de commande de réponse d'association

Figure 83 – Processus de rattachement en un saut d'un appareil de routage

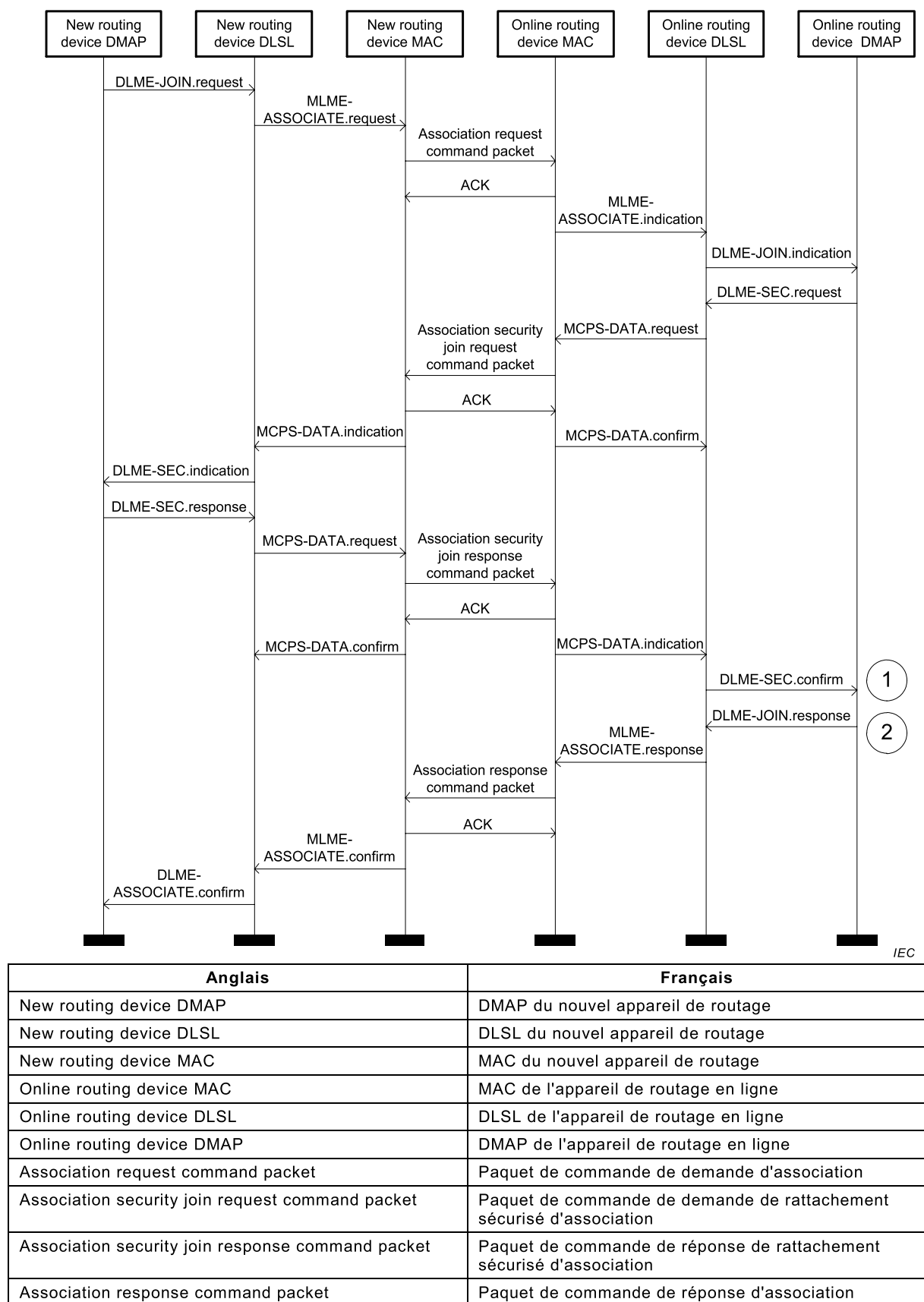
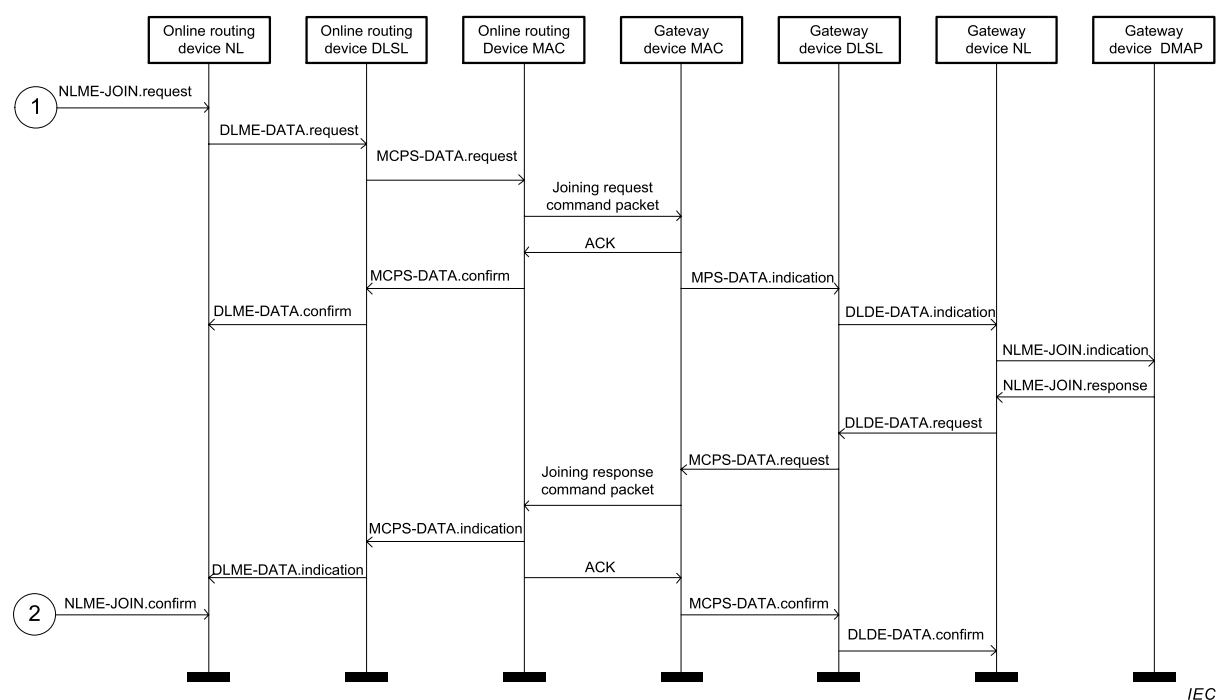


Figure 84 – Processus de rattachement multisaut d'un appareil de routage (nouvel appareil de routage vers appareil de routage)



Anglais	Français
Online routing device NL	NL de l'appareil de routage en ligne
Online routing device DLSL	DLSL de l'appareil de routage en ligne
Online routing device MAC	MAC de l'appareil de routage en ligne
Gateway device MAC	MAC de l'appareil passerelle
Gateway device DLSL	DLSL de l'appareil passerelle
Gateway device NL	NL de l'appareil passerelle
Gateway device DMAP	DMAP de l'appareil passerelle
Joining request command packet	Paquet de commande de demande de rattachement
Joining response command packet	Paquet de commande de réponse de rattachement

Figure 85 – Processus de rattachement multisaut d'un appareil de routage (appareil de routage vers appareil de passerelle)

11.6 Transport sécurisé

11.6.1 Processus de transport sécurisé entre un appareil de terrain et l'ordinateur de configuration d'hôte

Si les fonctions d'agrégation des appareils de routage et de l'appareil de terrain ne sont pas prises en charge, le processus de transport sécurisé entre un appareil de terrain et l'ordinateur de configuration d'hôte inclut les étapes suivantes.

- a) Selon SecMode et SecLevel dans la base MIB, le module de gestion de la sécurité du DMAP dans l'appareil de terrain chiffre la charge utile ASL, obtient le code d'intégrité (MIC) dans la couche application (AL) et l'envoie à la couche réseau (NL). Selon SecMode et SecLevel dans la base MIB, le module de gestion de la sécurité du DMAP dans l'appareil de terrain chiffre la charge utile DLSL et récupère le code d'intégrité (MIC). Puis, il est envoyé à l'appareil de routage.
- b) Lorsque l'appareil de routage reçoit le paquet, il déchiffre la trame de données et vérifie l'intégrité avec le code d'intégrité (MIC) dans la sous-couche DLSL, puis utilise la clé DLSL de prochain saut pour obtenir le code d'intégrité (MIC) et chiffrer la charge utile DLSL. Le paquet sera ensuite transmis à l'appareil de passerelle.

- c) Lorsque l'appareil de passerelle reçoit le paquet, le module de gestion de la sécurité déchiffre le paquet et vérifie le code d'intégrité (MIC) dans les sous-couches DLSL et ASL. L'appareil de passerelle envoie ensuite ces données à l'ordinateur de configuration d'hôte.

Si la fonction d'agrégation d'un appareil de terrain est prise en charge, le processus de transport sécurisé entre un appareil de terrain et l'ordinateur de configuration d'hôte inclut les étapes suivantes.

- a) Si l'appareil de terrain prend en charge l'agrégation des données, il chiffre les charges utiles des données de processus multiples en provenance d'objets d'application utilisateur (UAO) multiples. Selon SecMode et SecLevel dans la base MIB, le module de gestion de la sécurité du DMAP dans l'appareil de terrain chiffre la charge utile ASL, obtient le code d'intégrité (MIC) dans la couche application (AL) et l'envoie à la couche réseau (NL). Selon SecMode et SecLevel dans la base MIB, le module de gestion de la sécurité du DMAP dans l'appareil de terrain chiffre la charge utile DLSL et récupère le code d'intégrité (MIC). Le paquet chiffré est ensuite envoyé à l'appareil de routage.
- b) Si la fonction d'agrégation d'un appareil de routage n'est pas prise en charge, l'appareil de routage reçoit le paquet. L'appareil de routage vérifie le code d'intégrité (MIC) et déchiffre le paquet de données sur la sous-couche DLSL. Selon SecMode et SecLevel dans la base MIB, le module de gestion de la sécurité du DMAP dans l'appareil de routage chiffre la charge utile DLSL et récupère le code d'intégrité (MIC). Le paquet sera ensuite transmis à l'appareil de passerelle.
- c) Si la fonction d'agrégation d'un appareil de routage est prise en charge, la couche réseau (NL) informe le DMAP d'agréger ces charges utiles et obtient un nouveau paquet. Selon SecMode et SecLevel dans la base MIB, le module de gestion de la sécurité du DMAP dans l'appareil de routage commence par chiffrer la charge utile ASL et obtient le code d'intégrité (MIC); le module de gestion de la sécurité du DMAP dans l'appareil de routage chiffre ensuite la charge utile DLSL et récupère le code d'intégrité (MIC) dans la sous-couche DLSL. Le paquet chiffré sera ensuite transmis à l'appareil de passerelle.
- d) Lorsque l'appareil de passerelle reçoit le paquet, le module de gestion de la sécurité vérifie le code d'intégrité (MIC) et déchiffre le paquet dans les sous-couches DLSL et ASL. Le paquet est désagréé et est envoyé à l'ordinateur de configuration d'hôte.

11.6.2 Processus de transport sécurisé entre l'ordinateur de configuration d'hôte et un appareil de terrain

Ce processus est l'inverse du processus de transport entre un appareil de terrain et l'ordinateur de configuration d'hôte.

Annexe A (informative)

Stratégie de sécurité pour le réseau WIA-PA

A.1 Analyse du risque pour le réseau WIA-PA

En tant que système ouvert, le réseau WIA-PA présente des risques potentiels de sécurité. En fonction des sources, ces risques peuvent provenir de réseaux internet ou d'autres réseaux intranet d'une entreprise ou des réseaux WIA-PA internes. Le réseau WIA-PA peut subir un certain nombre de menaces, telles que l'invasion, la destruction de données et les attaques par réinsertion.

Par conséquent, il convient de prendre certaines mesures de sécurité pour assurer les opérations de sécurité par les utilisateurs du réseau WIA-PA, protéger les sources internes et maintenir les opérations normales du système. Les principaux objectifs de la sécurité du réseau WIA-PA sont de protéger les opérations normales du système, trouver les attaques et adopter des méthodes correspondantes dès que possible, limiter le dommage au niveau le plus bas et ramener le réseau à son état normal dès que possible après une attaque.

A.2 Principes de sécurité pour le réseau WIA-PA

Conformément aux caractéristiques du réseau WIA-PA, il convient d'adopter les mesures de sécurité et les principes de sécurité qui suivent:

- a) déploiement et utilisation faciles;
- b) être facultatif pour les mesures de sécurité et les services liés à la sécurité;
- c) réduire le plus possible les opérations manuelles;
- d) réduire le plus possible la transmission d'informations de sécurité;
- e) utilisation de technologies de chiffrement basées sur le matériel;
- f) utilisation de technologies de chiffrement et d'authentification existantes en plus de la norme publiée.

A.3 Objectifs de sécurité pour le réseau WIA-PA

Les objectifs de sécurité dans le réseau WIA-PA comprennent:

- a) protection des frontières: elle fournit la protection des frontières pour le réseau physique;
- b) disponibilité du système: elle permet aux utilisateurs légitimes d'accéder aux ressources du système lorsqu'ils en ont besoin;
- c) intégrité des données: elle garantit la cohérence des informations et empêche les utilisateurs illégitimes du système de modifier les données;
- d) authenticité des appareils: elle permet d'authentifier l'identité des appareils dans le réseau WIA-PA;
- e) confidentialité: elle permet de s'assurer que le matériel, les logiciels et les données du système peuvent uniquement être utilisés par les utilisateurs légitimes;
- f) gestion de clés: elle fournit les fonctions de mise à jour et de gestion des clés de sécurité.

A.4 Système de sécurité gradué et stratifié

En fonction de leurs métiers, types de services et objets de service, les utilisateurs emploient différentes méthodes et mesures de sécurité pour affronter les risques de sécurité, les niveaux de risques et les niveaux de sécurité exigés. En ce qui concerne les limitations des

ressources de calcul et les aptitudes de calcul des appareils de terrain, il convient d'accorder plus d'attention à la sécurité aux frontières du réseau WIA-PA.

Le système de sécurité gradué et détaillé par couches est décrit au Tableau A.1.

Tableau A.1 – Mesures de sécurité graduées et stratifiées pour réseau WIA-PA

WIA-PA Niveau de sécurité du réseau	Niveau 0	Niveau 1	Niveau 2
Protection de frontières	Passerelle de filtrage de message	Passerelle de conversion de protocole et de filtrage de message	Passerelle de conversion IPsec et de filtrage de message
Mesure de sécurité	Authentification Contrôle d'intégrité	Authentification Contrôle d'accès Contrôle d'intégrité Chiffrement XOR	Authentification Contrôle d'accès Contrôle d'intégrité Chiffrement

Les sous-couches DLSL et AL du réseau WIA-PA peuvent toutes les deux établir des connexions sécurisées. Lorsqu'un appareil de routage transmet des paquets de données, les niveaux de sécurité des paquets de données d'origine ne peuvent pas baisser. Les niveaux de sécurité des paquets de données sont établis conformément au Tableau A.2.

Tableau A.2 – Niveaux de sécurité des paquets de données

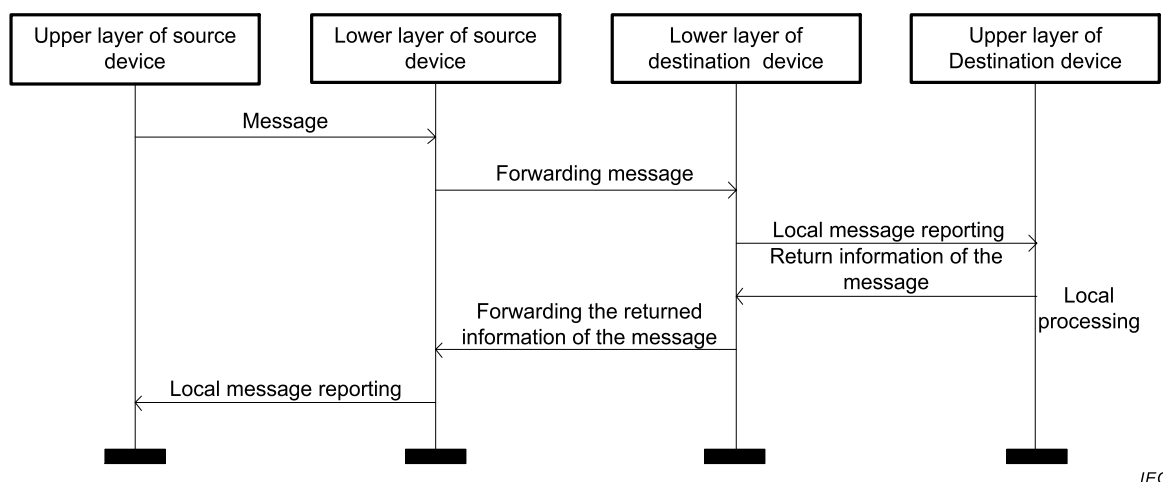
Niveau de sécurité de flux entrant	Niveau de sécurité de flux sortant			
	Non-vérification et non-chiffrement	Chiffrement et non-vérification	Vérification et non-chiffrement	Chiffrement et vérification
Non-vérification et non-chiffrement	autorisés	autorisés	autorisés	autorisés
Chiffrement et non-vérification	non autorisés	autorisés	non autorisés	autorisés
Vérification et non-chiffrement	non autorisés	non autorisés	autorisés	autorisés
Chiffrement et vérification	non autorisés	non autorisés	non autorisés	autorisés

Annexe B (informative)

Description de format

B.1 Diagramme de séquence temporelle

La Figure B.1 est un diagramme de séquence temporelle. Il représente une interaction qui s'intéresse à la séquence des messages entre les couches empilées des appareils du réseau WIA-PA sur les lignes de vie.



Anglais	Français
Upper layer of source device	Couche supérieure de l'appareil source
Lower layer of source device	Couche inférieure de l'appareil source
Lower layer of destination device	Couche inférieure de l'appareil de destination
Upper layer of destination device	Couche supérieure de l'appareil de destination
Message	Message
Forwarding message	Transmission de message
Local message reporting	Production de rapport de message local
Local processing	Traitement local
Return information of the message	Retour des informations du message
Forwarding the returned information of the message	Transmission des informations de message retournées

Figure B.1 – Diagramme de séquence temporelle

Les couches empilées des appareils du réseau WIA-PA sont représentées par des blocs rectangulaires. Le temps est représenté par des lignes verticales. Un message est représenté par une flèche. Dans le présent document, une flèche pleine est utilisée pour représenter l'occurrence générale d'un message indépendamment de la gestion synchrone ou asynchrone du message. La séquence des messages est définie par l'ordre des messages en partant du haut du diagramme.

B.2 Format de paquet ou de trame

Les définitions d'un paquet et d'une trame ont la même structure. La principale différence est leur plage fonctionnelle. Le format de paquet est utilisé pour la couche réseau (NL) et la sous-couche application (ASL) tandis que le format de trame est utilisé pour la couche de contrôle d'accès au support (MAC) et la sous-couche liaison de données (DLSL).

Le format de champ en octet(s) d'un paquet ou d'une trame est décrit au Tableau B.1.

Tableau B.1 – Format de paquet ou de trame en octet(s)

	Format de paquet ou de trame en octet(s)			
Longueur en octet(s)	X_1	X_2	...	X_N
Nom de champ	Champ 1	Champ 2	...	Champ N

Comme indiqué au Tableau B.1, la valeur de X_i ($i=1,2,\dots, N$) décrit la longueur en octet(s) du champ de paquet/trame correspondant. Il convient que l'émission d'un paquet ou d'une trame s'effectue de l'octet de poids faible jusqu'à l'octet de poids fort, autrement dit il convient d'émettre en premier l'octet de poids faible du Champ 1.

Un champ peut comporter plusieurs longueurs dans différents contextes. Dans ces cas, il convient d'utiliser les valeurs $X_{i1}/\dots/X_{iM}$ au lieu de X_i pour spécifier la longueur du champ i .

Un champ peut comporter plusieurs sous-champs. Le Tableau B.2 spécifie la définition du format des sous-champs si un champ faisant 1 octet de longueur est subdivisé en plusieurs sous-champs en bit(s).

Tableau B.2 – Format des sous-champs en bit(s)

	Format des sous-champs en bit(s)			
Longueur en bit(s)	X_1	X_2	...	X_N
Nom de sous-champ	Sous-champ 1	Sous-champ 2	...	Sous-champ m

Comme indiqué au Tableau B.2, la valeur de X_i ($i=1,2,\dots, N$) décrit le nombre de bits occupés par le sous-champ correspondant, qui est défini de 1 à 8. La somme de X_1 , X_2 , ... et X_N est fixée à 8. Les sous-champs de gauche à droite sont alloués du bit 0 au bit 7. Il convient que l'émission du format des sous-champs s'effectue du bit de poids faible jusqu'au bit de poids fort, autrement dit il convient d'émettre en premier le bit de poids faible du Sous-champ 1.

Annexe C (informative)

Exemple d'objet d'application utilisateur (UAO)

C.1 Généralités

Le présent document spécifie les objets d'application utilisateur (UAO) en utilisant une approche orientée objet. Un UAO a ses propres attributs et méthodes. Les attributs comprennent le nom d'objet, le nom d'attribut, l'identificateur d'attribut et le type de données de l'attribut. Les méthodes fournies par les UAO sont utilisées pour réaliser les opérations de ces attributs.

Les UAO peuvent inclure les objets d'entrée analogiques (AIO, Analog Input Object), les objets de sortie analogiques (AOO, Analog Output Object), les objets d'entrée numériques (DIO, Digital Input Object) et les objets de sortie numériques (DOO, Digital Output Object). Il convient de définir ces objets dans les profils d'application. Ce document utilise l'objet AIO comme exemple pour spécifier l'utilisation des UAO. Par ailleurs, les objets DAGO, PAGO et DGO sont considérés comme des objets UAO spéciaux.

C.2 Objet d'entrée analogique

C.2.1 Vue d'ensemble

Un objet AIO est utilisé pour échantillonner le processus industriel et convertir la valeur mesurée en la valeur de données ayant des dimensions physiques. Les méthodes prises en charge par l'AIO sont indiquées au Tableau 171.

C.2.2 Attribut de classe de l'AIO

Le Tableau C.1 spécifie l'attribut de classe de l'AIO.

Tableau C.1 – Attribut de classe de l'AIO

Nom d'attribut	Identificateur d'attribut	Type de données	Méthode associée	Description
Object identifier (identificateur d'objet)	0	Unsigned8	Read (Lecture)	Identificateur unique d'un objet qui est utilisé pour l'adressage d'objet

C.2.3 Attribut d'instance de l'AIO

Le Tableau C.2 spécifie les attributs d'instance de l'AIO.

Tableau C.2 – Attributs d'instance de l'AIO

Identificateur d'attribut	Nom d'attribut	Type de données	Méthode de prise en charge	Description
1	Instance ID	Unsigned8	READ	Identificateur unique d'une instance d'objet
2	ProcessValue	Float	READ	Variable processus industriel
3	OutValue	Float	READ PUBLISH REPORT	Valeur de sortie basée sur ProcessValue
4	SimulateValue	Float	READ/WRITE	Valeur écrite par l'opérateur pour simuler l'attribut OutValue
5	DefaultValue	Float	READ/WRITE	Valeur par défaut de l'attribut OutValue si une panne de capteur ou d'électronique capteur est détectée
6	HighWarning	Float	READ/WRITE	Valeur limite haute d'avertissement
7	HighHighAlm	Float	READ/WRITE	Valeur limite haute d'alarme
8	LowWarning	Float	READ/WRITE	Valeur limite basse d'avertissement
9	LowLowAlm	Float	READ/WRITE	Valeur limite basse d'alarme
10	EngineeringUnit	Unsigned16	READ/WRITE	Unité technique pour toutes les valeurs
10	Action	Unsigned8	READ/WRITE	Lancement/arrêt du processus de mesurage
11	SamplePeriod	Unsigned32	READ/WRITE	Sert à régler le cycle d'échantillonnage
12	Alarme	Unsigned8	READ	0 = Normal 1 = HighWarning 2 = LowWarning 3 = HighAlarm 4 = LowAlarm 5 à 255 = Réservés.
13 à 19	Réservé			Réservé pour une utilisation ultérieure
100 à 255	Spécifique constructeur au			Attributs spécifiques au fabricant

Annexe D (informative)

Configurations spécifiques à un pays et spécifiques à une région

Le support de terrain WIA-PA utilise une interface physique largement utilisée et admise; il est donc approprié à une utilisation dans un grand nombre de régions géographiques du monde. Cependant, certaines régions ont des considérations spéciales qui peuvent imposer des exigences réglementaires différentes. Même si un produit est conçu pour satisfaire à ces exigences réglementaires, son utilisation n'est souvent pas légalement autorisée tant qu'il n'a pas été soumis à des essais de conformité et que tous les éventuels permis ou certificats locaux exigés n'ont pas été délivrés par les organismes de réglementation spécifiques à un pays.

Le présent document est conçu pour prendre en charge l'exploitation au sein d'une zone géographique fixe qui fonctionne sous des réglementations uniformes. A ce titre, il est censé prendre en charge le fonctionnement n'importe où dans le monde (voir 8.4.11).

Le présent document ne spécifie pas les certifications ou permis réglementaires dont a besoin un produit conforme au présent document; il est de la responsabilité du fabricant du produit et de l'utilisateur final de les déterminer. Un produit peut avoir des certifications pour l'exploitation dans plusieurs pays ou régions.

Pour plus d'informations sur les dispositions spécifiques qui ont été prises dans le présent document pour prendre en charge l'approbation réglementaire des systèmes et équipements en lieux fixes, voir Annexe E.

Les règlements des radiocommunications exigent souvent des appareils de fonctionner à des niveaux contraints de puissance, et ce, à tout moment, y compris pendant la configuration par liaison radio. Quelques seuils de PIRE identifiés sont: 10 mW/MHz (Japon); 10 dBm (Chine); 10 dBm, 10 dBm/MHz, ou 20 dBm (CE dans la bande ISM de 2,4 GHz); 36 dBm avec un gain d'antenne maximal de 6 dBi (US FCC).

Dans certains pays, tels que la France, les niveaux d'émission sur certains canaux peuvent avoir besoin d'être affaiblis. Dans d'autres pays, tels que la Corée, le nombre et la plage de canaux ont besoin d'être contraints.

Annexe E (informative)

Modifications régionales pour conformité aux normes ETSI

E.1 Généralités

WIA-PA limite l'utilisation du spectre à la bande ISM de 2,4 GHz (voir Article 7).

Des exigences supplémentaires s'appliquent en Europe en ce qui concerne les équipements de transmission de fréquences radio à large bande fonctionnant dans cette bande ISM de 2,4 GHz. Certaines de ces exigences européennes peuvent être satisfaites en se conformant aux deux Normes harmonisées de l'ETSI, à savoir l'EN 300 328 et l'EN 300 440-2.

La présente Annexe E fournit des exigences supplémentaires concernant la conformité des appareils WIA-PA (IEC 62601) fonctionnant dans la bande ISM de 2,4 GHz à ces deux normes ETSI:

- L'EN 300 440-2 s'applique aux équipements (appareils) présentant une puissance d'émission maximale de PIRE comprise entre 0 dBm et 10 dBm (voir Article E.2);
- L'EN 300 328 s'applique aux équipements (appareils) présentant une puissance d'émission maximale de PIRE comprise entre 10 dBm et 100 dBm (voir Article E.3).

NOTE Dans l'Annexe E, le terme "appareils" se réfère à l'électronique des équipements radioélectriques fonctionnant conformément à la norme applicable; ils incluent, mais sans s'y limiter, les appareils de passerelle, les appareils de routage et les appareils de terrain.

E.2 Conformité à l'EN 300 440-2

Le Tableau E.1 spécifie les exigences supplémentaires qui permettent aux appareils WIA-PA de fonctionner dans la bande ISM de 2,4 GHz afin de satisfaire aux exigences de limitation de puissance d'émission de l'EN 300 440-2.

NOTE L'EN 300 440-2 est répertoriée en tant que norme harmonisée en vertu de la Directive 2014/53/UE relative aux équipements radioélectriques.

Tableau E.1 – Liste des exigences applicables de l'EN 300 440-2

Paramètre	Exigences EN 300 440-2	Exigences supplémentaires
Puissance d'émission maximale	PIRE de 10 dBm (10 mW)	Les appareils doivent être configurés pour émettre une PIRE de moins de 10 dBm, ce qui signifie moins de 10 dBm de puissance électrique avec un gain d'antenne de 0dBi. Si le gain d'antenne est différent de 0dBi, la PIRE résultant doit être inférieur à 10 dBm via un réglage de puissance électrique adéquat. Cette exigence remplace l'exigence relative à la puissance électrique donnée en 7.3.6.

E.3 Conformité à l'EN 300 328

Le Tableau E.2 spécifie les exigences supplémentaires qui permettent aux appareils WIA-PA de fonctionner dans la bande ISM de 2,4 GHz afin de satisfaire aux différentes exigences de l'EN 300 328.

NOTE L'EN 300 328 V1.9.1 est répertoriée en tant que norme harmonisée en vertu de la Directive 2014/53/UE relative aux équipements radioélectriques.

Tableau E.2 – Liste des exigences applicables de l'EN 300 328

Paramètre	Exigences EN 300 328 V1.9.1	Exigences supplémentaires
Puissance d'émission maximale	PIRE de 20 dBm (100 mW)	Les appareils doivent être configurés pour émettre une PIRE de moins de 10 dBm $\pm$ 3 dBm selon 7.3.6.
Densité spectrale de puissance maximale	PIRE de 10 mW/MHz	Compte tenu de la nature de DSSS (voir l'IEEE 802.15.4-2011, Article 10), une PIRE maximale de 13 dBm donne lieu à une densité spectrale en-dessous de 10 mW/MHz comme exigé.
Facteur d'utilisation, séquence d'émission, écart d'émission	Pour les équipements non adaptatifs avec une PIRE maximale supérieure à 10 dBm: Le facteur d'utilisation doit être inférieur ou égal à la valeur maximale déclarée par le fournisseur. Temps séquence d'émission $\leq$ 10 ms. Le temps d'un écart d'émission minimal suivant une séquence d'émission doit être égal à la durée de cette séquence d'émission en cours, avec une valeur minimale de 3,5 ms.	Aucune exigence supplémentaire n'est nécessaire. Les exigences sont satisfaites par les caractéristiques suivantes. Le temps d'une séquence d'émission maximal pour un paquet WIA-PA s'élève à 4,256 ms dans un intervalle de 10 ms selon le Tableau E.3, (T_{maxPHY}), tandis que le temps de transmission pour un ACK WIA-PA s'élève à 352 μs selon le Tableau E.3 (T_{ACK}). Le temps d'une séquence d'émission maximal pour un paquet WIA-PA est identique au temps de transmission maximal; le temps d'un écart d'émission minimal pour un paquet WIA-PA est identique au temps de transmission maximal.
Limite d'utilisation du support	Pour les équipements non adaptatifs avec une PIRE maximale supérieure à 10 dBm: Facteur maximal d'utilisation du support = 10 %.	Le cycle de service d'un appareil WIA-PA ne peut pas dépasser 43 % en se basant sur un intervalle de 10 ms et un temps de transmission maximal pour un paquet WIA-PA de 4,256 ms dans un intervalle de 10 ms selon le Tableau E.3. Cela donne lieu à un facteur maximal d'utilisation inférieur à 10 % comme exigé. PIRE de MU = 13 dBm $\times$ 43 % $<$ 9 %

Tableau E.3 – Définitions et calculs de la temporisation des intervalles de temps

Symbole	Valeur de temporisation	Base de calcul
T_{maxPHY}	4 256 μ s	Pour la bande de fréquences 2 400 à 2 483,5 MHz et un débit de 250 Kbit/s, le temps de transmission maximal d'un paquet PHY s'élève à 4 256 μ s, ce qui inclut un préambule de 128 μ s (voir Tableau 71 de l'IEEE 802.15.4-2011), un délimiteur de début de trame (SFD) de 32 μ s (voir Tableau 71 de l'IEEE 802.15.4-2011) et une charge utile PHR/PHY de 4 096 μ s (voir Tableau 70 de l'IEEE 802.15.4-2011)
T_{ACK}	352 μ s	Les appareils WIA-PA doivent utiliser l'ACK selon l'IEEE 802.15.4-2011. La longueur totale de l'ACK est de 11 octets (voir Figure 47 et Figure 67 de l'IEEE 802.15.4-2011) et le temps de transmission d'un ACK s'élève à 352 μ s pour la bande de fréquences 2 400 – 2 483, 5 MHz et un débit de 250 Kbit/s.
T_{Offset}	2 120 μ s	Début de l'intervalle de temps où le récepteur doit effectuer l'écoute
T_{Delay}	1 000 μ s	Fin de la trame au début de l'acquittement

Bibliographie

ISO/IEC/IEEE 60559:2011, *Information technology – Microprocessor Systems – Floating-Point arithmetic* (disponible en anglais seulement)

IEC 61804-2, *Blocs fonctionnels (FB) pour les procédés industriels – Partie 2: Spécification du concept de FB*

IEC 61499-1, *Blocs fonctionnels – Partie 1: Architecture*

IEC 61499-2, *Blocs fonctionnels – Partie 2: Exigences pour les outils logiciels*

IEC TR 62390:2005, *Common automation device – Profile guideline* (disponible en anglais seulement)

ISO/IEC 7498-1, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Modèle de référence de base: Le modèle de base*

ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher* (disponible en anglais seulement)

ISO/IEC 9797-2:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function* (disponible en anglais seulement)

ISO 3166-1, *Codes pour la représentation des noms de pays et de leurs subdivisions – Partie 1: Codes de pays*

ISO 10181-2:1996, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Cadres de sécurité pour les systèmes ouverts: Cadre d'authentification*

ISO 10181-4:1997, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Cadres de sécurité dans les systèmes ouverts: Cadre de non-répudiation*

ISO 10181-5:1996, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Cadres de sécurité pour les systèmes ouverts: Cadre de confidentialité*

ISO 10181-6:1996, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Cadres de sécurité pour les systèmes ouverts: Cadre d'intégrité*

ISO/IEC 15408-1, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model* (disponible en anglais seulement)

ISO/IEC 15408-2, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional c* (disponible en anglais seulement)

ISO/IEC TR 10000-1:1998, *Information technology – Framework and taxonomy of International Standardized Profiles – Part 1: General principles and documentation framework* (disponible en anglais seulement)

ISO/IEC 17799:2005¹, *Information technology – Security techniques – Code of practice for information security management* (disponible en anglais seulement)

ETSI EN 300 328 V1.8.1 (2012-06), *Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive* (disponible en anglais seulement)

ETSI EN 300 440-2, V1.4.1 (2010-08), *Electromagnetic compatibility and Radio spectrum Matters (ERM); Short range devices; Radio equipment to be used in the 1 GHz to 40 GHz frequency range; Part 2: Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive* (disponible en anglais seulement)

Directive 1999/5/CE de la Commission européenne relative aux ,équipements hertziens et, équipements terminaux de télécommunications et à la reconnaissance mutuelle de leur conformité, disponible à l'adresse: http://ec.europa.eu/enterprise/sectors/rtte/index_en.htm

Directive 2014/53/UE du Parlement européen et du Conseil relative aux équipements radioélectriques (Directive 1999/5/CE abrogative), disponible à l'adresse: http://ec.europa.eu/enterprise/sectors/rtte/index_en.htm

IEEE 64, *Guidelines for 64-bit Global Identifier (EUI-64™)* (disponible en anglais seulement)

IEEE 754:2008, *Standard for floating-point arithmetic* (disponible en anglais seulement)

¹ Retirée.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch