

BS IEC 62601:2011



BSI Standards Publication

Industrial communication networks — Fieldbus specifications — WIA-PA communication network and communication profile

bsi.

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

National foreword

This British Standard is the UK implementation of IEC 62601:2011. It supersedes DD IEC/PAS 62601:2009 which is withdrawn.

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

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

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

© The British Standards Institution 2014.
Published by BSI Standards Limited 2014

ISBN 978 0 580 68579 8
ICS 25.040.40; 35.100.05

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

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

Amendments/corrigenda issued since publication

Amd. No.	Date	Text affected
----------	------	---------------



INTERNATIONAL STANDARD



**Industrial communication networks – Fieldbus specifications – WIA-PA
communication network and communication profile**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE

XJ

ICS 25.040.40; 35.100.05

ISBN 978-2-88912-788-7

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 Specification of data types.....	21
4.1 Representation of boolean type	21
4.2 Representation of unsigned integer type	21
4.3 Representation of octet type.....	21
4.4 Representation of floating point number type.....	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.....	25
6.1 General.....	25
6.2 Framework of system management	27
6.3 Joining process	28
6.3.1 Joining process of routing device.....	28
6.3.2 Joining process of field device	30
6.3.3 Addressing and address assignment	31
6.4 Virtual Communication Relationship (VCR).....	31
6.4.1 Definition.....	31
6.4.2 Protocol support for VCR.....	32
6.4.3 VCR establishment.....	33
6.4.4 VCR release	33
6.5 Routing configuration and communication resource allocation	33
6.5.1 Routing configuration.....	33
6.5.2 Framework of communication resource allocation	33
6.5.3 DLPDU priority and scheduling rules	34
6.5.4 Communication resource allocation to routing device	35
6.5.5 Communication resource allocation to field device.....	35
6.6 Aggregation and disaggregation	36
6.6.1 Aggregation	36
6.6.2 Disaggregation	38
6.6.3 An example of the two level aggregation process	39
6.6.4 Management of aggregation and disaggregation objects.....	41
6.7 Performance monitoring	43
6.7.1 Path failure report.....	43
6.7.2 Device status report	43
6.7.3 Channel condition report.....	44
6.8 Leaving process	44
6.8.1 General	44
6.8.2 Leaving process of routing device.....	44

6.8.3	Leaving process of field device	46
6.9	Management information base and services	47
6.9.1	Management information base	47
6.9.2	MIB services	59
7	Physical Layer	61
8	Data link layer	62
8.1	General	62
8.2	Protocol stack	62
8.3	MAC overview and function extension	62
8.3.1	MAC overview	62
8.3.2	MAC function extension	63
8.4	DLSL function description	66
8.4.1	General	66
8.4.2	Coexistence	67
8.4.3	Timeslot communication	67
8.4.4	WIA-PA superframe	68
8.4.5	Frequency hopping	68
8.4.6	Transmission of long cycle data	70
8.4.7	Retry strategy	71
8.4.8	Management service	71
8.4.9	Radio link quality and channel condition measurement	71
8.4.10	Security	71
8.4.11	DLSL state machine	71
8.5	Data link sub-layer data services	73
8.5.1	General	73
8.5.2	DLDE-DATA.request	73
8.5.3	DLDE-DATA.confirm	74
8.5.4	DLDE-DATA.indication	75
8.5.5	Time sequence of DLSL data service	76
8.6	Data link sub-layer management services	77
8.6.1	General	77
8.6.2	Network discovery services	77
8.6.3	Device joining services	79
8.6.4	Device leaving services	81
8.6.5	DLME-CHANNEL-CONDITION.indication	82
8.6.6	DLME-NEIGHBOR-INFO.indication	83
8.6.7	DLME-COMM-STATUS.indication	83
8.6.8	Keep-alive services	84
8.6.9	Time synchronization services	85
8.7	DLSL frame formats	86
8.7.1	General frame format	86
8.7.2	Data frame format	86
8.7.3	Command frame format	87
9	Network layer	87
9.1	General	87
9.2	Protocol stack	87
9.3	Function description	88
9.3.1	General	88
9.3.2	Addressing	88

9.3.3	Routing.....	89
9.3.4	Packet lifecycle management	89
9.3.5	Joining and leaving network of device	89
9.3.6	End-to-end network performance monitoring.....	89
9.3.7	Fragmentation and reassembly.....	90
9.3.8	Network layer state machine.....	90
9.4	Network layer data services	91
9.4.1	General	91
9.4.2	NLDE-DATA.request.....	91
9.4.3	NLDE-DATA.confirm	91
9.4.4	NLDE-DATA.indication	92
9.4.5	Time sequence of NL data services	92
9.5	Network layer management services	93
9.5.1	General	93
9.5.2	Network communication status report services	93
9.5.3	Network joining services	95
9.5.4	Network leaving services	101
9.5.5	Cluster member report services	107
9.5.6	Neighbor information report services	109
9.5.7	Route allocation services.....	110
9.5.8	Communication resource allocation services	116
9.5.9	Aggregation and disaggregation services	131
9.5.10	Device status report services.....	132
9.5.11	Channel condition report services.....	134
9.5.12	Failure path report services	136
9.5.13	Network attribute getting services.....	137
9.5.14	Network attribute setting services	140
9.6	Network layer packet formats	143
9.6.1	Common packet format.....	143
9.6.2	Data packet format	144
9.6.3	Aggregated packet format.....	144
9.6.4	Command packet format.....	145
10	Application Layer.....	160
10.1	Overview	160
10.1.1	General	160
10.1.2	AL structure.....	160
10.1.3	Functions of UAP.....	161
10.1.4	Functions of ASL	161
10.2	UAP	161
10.2.1	General	161
10.2.2	UAO	162
10.2.3	Method definition	163
10.3	Application sub-layer	166
10.3.1	General	166
10.3.2	Application sub-layer data entity	166
10.4	Application sub-layer packet formats	171
10.4.1	General	171
10.4.2	ASL general packet format	172
10.4.3	Packet formats	172

11 Security	175
11.1 General	175
11.2 Security management framework	175
11.3 Secure communication protocol stack	176
11.3.1 General	176
11.3.2 MAC layer security	177
11.3.3 Data link sub-layer security	177
11.3.4 Application sub-layer security	179
11.4 Key management	180
11.4.1 Key type	180
11.4.2 Key distribution	181
11.4.3 Key update	181
11.4.4 Key status	182
11.5 Secure joining process	182
11.5.1 Secure joining process of a new WIA-PA device	182
11.5.2 Device security material getting services	183
11.6 Secure transportation	187
11.6.1 Process of secure transportation from field device to host configuration computer	187
11.6.2 Process of secure transportation from host configuration computer to field device	188
Annex A (informative) Security strategy for WIA-PA network	189
Annex B (informative) Format description for WIA-PA standard	191
Annex C (informative) Example of UAO	193
Bibliography	195
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	29
Figure 9 – Joining process of field device through a gateway device	30
Figure 10 – Joining process of field device through a routing device	30
Figure 11 – Long address structure of device	31
Figure 12 – Short address structure of routing device	31
Figure 13 – Short address structure of field device	31
Figure 14 – An example of resource allocation	34
Figure 15 – Allocation process of routing device's communication resources	35
Figure 16 – Allocation process of field device's communication resources	36
Figure 17 – Example of aggregation and disaggregation	40
Figure 18 – Process of path failure report	43
Figure 19 – Device status report process of field device	43
Figure 20 – Device status report process of routing device	43

Figure 21 – Process of channel condition report	44
Figure 22 – Active leaving process of routing device	45
Figure 23 – Passive leaving process of routing device	45
Figure 24 – Active leaving process of field device (leaving from gateway device).....	46
Figure 25 – Active leaving process of field device (leaving from routing device).....	46
Figure 26 – Passive leaving process of field device (leaving from gateway device)	47
Figure 27 – Passive leaving process of field device (leaving from routing device)	47
Figure 28 – WIA-PA DLL protocol stack	62
Figure 29 – WIA-PA DLSL reference model	67
Figure 30 – WIA-PA superframe	68
Figure 31 – R1, R2 and R3 superframe structures	70
Figure 32 – An example of long cycle data transmission	70
Figure 33 – DLSL state machine	72
Figure 34 – Time sequence of data service.....	76
Figure 35 – Time sequence of network discovery.....	79
Figure 36 – General frame format	86
Figure 37 – WIA-PA network layer protocol stack.....	87
Figure 38 – WIA-PA Network layer reference model.....	88
Figure 39 – Network layer state machine	90
Figure 40 – Time sequence of NL data services.....	93
Figure 41 – Time sequence for field device joining through routing device	98
Figure 42 – One-hop joining process for routing device.....	99
Figure 43 – Multi-hop join process of routing device	100
Figure 44 – Active leaving process of field device (leaving routing device).....	103
Figure 45 – Passive leaving of field device	104
Figure 46 – Active leaving process of routing device	105
Figure 47 – Passive leaving process of routing device	106
Figure 48 – Cluster member reporting process.....	108
Figure 49 – Neighbor information reporting process	110
Figure 50 – Time sequence for route adding	112
Figure 51 – Time sequence for route updating	114
Figure 52 – Time sequence for route deleting	116
Figure 53 – Adding a link originated from gateway device to routing device	119
Figure 54 – Adding a link originated from routing device to field device.....	119
Figure 55 – Updating a link originated by gateway device to routing device	121
Figure 56 – Updating a link originated from routing device to field device	121
Figure 57 – Releasing a link originated from gateway device to routing device.....	123
Figure 58 – Releasing a link originated from routing device to field device.....	124
Figure 59 – Adding a superframe originated from gateway device to routing device	126
Figure 60 – Adding a superframe originated from routing device to field device	126
Figure 61 – Updating a superframe originated from gateway device to routing device	128
Figure 62 – Updating a superframe originated from routing device to field device	128
Figure 63 – Releasing a superframe originated from gateway device to routing device	130

Figure 64 – Releasing a superframe originated from routing device to field device	130
Figure 65 – Device status reporting process from field device to routing device	133
Figure 66 – Device status reporting process from routing device to gateway device	134
Figure 67 – Channel condition reporting process from field device to routing device	135
Figure 68 – Channel condition reporting process from routing device to gateway device	136
Figure 69 – Failure path reporting process	137
Figure 70 – Network layer common packet format	143
Figure 71 – Network layer data packet format	144
Figure 72 – Aggregated packet format	144
Figure 73 – Format of NL command packet	145
Figure 74 – AL structure	160
Figure 75 – User application process	161
Figure 76 – C/S communication process	169
Figure 77 – P/S communication process (disable aggregation function)	170
Figure 78 – P/S communication process (enable aggregation function)	171
Figure 79 – R/S communication process	171
Figure 80 – Application sub-layer general packet format	172
Figure 81 – ASL data packet format	173
Figure 82 – Acknowledgement packet format	174
Figure 83 – Security management framework of WIA-PA network	175
Figure 84 – Security communication protocol stack	177
Figure 85 – MPDU structure	177
Figure 86 – Security DLPDU structure	178
Figure 87 – Security APDU structure	179
Figure 88 – Key lifecycle	181
Figure 89 – Secure joining process of WIA-PA device	182
Figure 90 – Time sequence for field device joining (Field device to routing device)	185
Figure 91 – Time sequence for field device joining (Routing device to gateway device)	185
Figure 92 – One-hop joining process for routing device	186
Figure 93 – Multi-hop join process of routing device (new routing device to routing device)	186
Figure 94 – Multi-hop join process of routing device (routing device to gateway device)	187
Figure B.1 – Time sequence diagram	191
Table 1 – Protocol support for VCR	32
Table 2 – Relations between VCR and aggregation function	37
Table 3 – Format of aggregated data followed by field device's DAGO	38
Table 4 – Format of aggregated packet followed by routing device's PAGO	38
Table 5 – DAGO class attributes	41
Table 6 – DAGO instance attributes	41
Table 7 – MEM_STRUCT structure	42
Table 8 – PAGO class attributes	42
Table 9 – PAGO instance attributes	42

Table 10 – DGO class attributes	42
Table 11 – DGO instance attributes	43
Table 12 – Unstructured attributes	48
Table 13 – Structured attributes	51
Table 14 – NLRoute_Struct structure	52
Table 15 – Superframe_Struct structure	52
Table 16 – Link_Struct structure	53
Table 17 – Neighbor_Struct structure	54
Table 18 – ChanCon_Struct structure	54
Table 19 – Device_struct structure	55
Table 20 – VCR_Struct structure	57
Table 21 – DevConRep_Struct structure	58
Table 22 – Key_Struct structure	58
Table 23 – ObjList_Struct structure	59
Table 24 – DMAP-MIB-GET.request parameters	59
Table 25 – DMAP-MIB-GET.confirm parameters	60
Table 26 – DMAP-MIB-SET.request parameters	61
Table 27 – DMAP-MIB-SET.confirm parameters	61
Table 28 – MAC extended PIB attributes	63
Table 29 – MAC extended command frame	63
Table 30 – MLME-KEEP-LIVE.confirm parameters	64
Table 31 – MLME-KEEP-LIVE.indication parameters	64
Table 32 – MLME-TIME-SYN.request parameters	64
Table 33 – MLME-TIME-SYN.confirm parameters	65
Table 34 – MLME-TIME-SYN.indication parameters	65
Table 35 – Beacon payload	65
Table 36 – Format of keep-alive command frame	66
Table 37 – Format of time synchronization command frame	66
Table 38 – Hopping mechanisms	69
Table 39 – DLSE state transitions	72
Table 40 – DLDE-DATA.request parameters	74
Table 41 – DLDE-DATA.confirm parameters	75
Table 42 – Status table	75
Table 43 – DLDE-DATA.indication parameters	76
Table 44 – DLME-DISCOVERY.request parameters	77
Table 45 – DLME-DISCOVERY.confirm parameters	78
Table 46 – Network descriptor list	78
Table 47 – DLME-JOIN.request parameters	79
Table 48 – DLME-JOIN.indication parameters	80
Table 49 – DLME-JOIN.response parameters	80
Table 50 – DLME-JOIN.confirm parameters	81
Table 51 – DLME-LEAVE.request parameters	81
Table 52 – DLME-LEAVE.indication parameters	82

Table 53 – DLME-LEAVE.confirm parameters	82
Table 54 – DLME-CHANNEL-CONDITION.indication parameters	83
Table 55 – DLME-NEIGHBOR-INFO.indication parameters	83
Table 56 – DLME-COMM-STATUS.indication parameters	84
Table 57 – DLME -KEEP-LIVE.confirm parameters	84
Table 58 – DLME -KEEP-LIVE.indication parameters	85
Table 59 – DLME-TIME-SYN.request parameters	85
Table 60 – DLME -TIME-SYN.confirm parameters	85
Table 61 – DLME-TIME-SYN.indication parameters	86
Table 62 – DLSL frame control field	86
Table 63 – Date frame format	87
Table 64 – General command frame format	87
Table 65 – DLSL command frame	87
Table 66 – Example of a routing table	89
Table 67 – Network layer states	90
Table 68 – NL state transitions	90
Table 69 – NLDE-DATA.request parameters	91
Table 70 – NLDE-DATA.confirm parameters	92
Table 71 – NLDE-DATA.indication parameters	92
Table 72 – NLME-COMM-STATUS.request parameters	93
Table 73 – NLME-COMM-STATUS.indication parameters	94
Table 74 – NLME-COMM-STATUS.confirm parameters	94
Table 75 – NLME-JOIN.request parameters	95
Table 76 – NLME-JOIN.indication parameters	96
Table 77 – NLME-JOIN.response parameters	96
Table 78 – NLME-JOIN.confirm parameters	97
Table 79 – NLME-LEAVE.request parameters	101
Table 80 – NLME-LEAVE.indication parameters	101
Table 81 – NLME-LEAVE.response parameters	101
Table 82 – NLME-LEAVE.confirm parameters	102
Table 83 – NLME-RPT-CLRMEM.request parameters	107
Table 84 – NLME-RPT-CLRMEM.confirm parameter	107
Table 85 – NLME-RPT-CLRMEM.response parameters	108
Table 86 – NLME-NEIGHBOR-INFO.request parameters	109
Table 87 – NLME-NEIGHBOR-INFO.confirm parameter	110
Table 88 – NLME-ADD_ROUTE.request parameters	110
Table 89 – NLME-ADD_ROUTE.confirm parameters	111
Table 90 – NLME-UPDATE_ROUTE.request parameters	112
Table 91 – NLME-UPDATE_ROUTE.confirm parameter	113
Table 92 – NLME-UPDATE_ROUTE.request parameters	114
Table 93 – NLME-DELETE_ROUTE.confirm parameters	115
Table 94 – NLME-ADD-LINK.request parameters	117
Table 95 – NLME-ADD-LINK.confirm parameters	118

Table 96 – NLME-UPDATE-LINK.request parameters	120
Table 97 – NLME-UPDATE-LINK.confirm parameters	120
Table 98 – NLME-RELEASE-LINK.request parameters	122
Table 99 – NLME-RELEASE-LINK.confirm parameters	122
Table 100 – NLME-ADD-SFR.request parameters.....	124
Table 101 – NLME-ADD-SFR.confirm parameters.....	125
Table 102 – NLME-UPDATA-SFR.request parameters	127
Table 103 – NLME-UPDATE-SFR.confirm parameters	127
Table 104 – NLME-RELEASE-SFR.request parameters	129
Table 105 – NLME-RELEASE-SFR.confirm parameters	129
Table 106 – NLME-AGG.indication parameters	131
Table 107 – NLME-AGO-SEND.request parameters.....	131
Table 108 – NLME-DAG.indication parameter.....	132
Table 109 – NLME- DEVICE -STATUS.request parameters	132
Table 110 – NLME- DEVICE -STATUS.indication parameters	133
Table 111 – NLME- DEVICE -STATUS.confirm parameter	133
Table 112 – NLME-CHANNEL-CONDITION.request parameters	134
Table 113 – NLME-CHANNEL-CONDITION.indication parameters	135
Table 114 – NLME-CHANNEL-CONDITION.confirm parameter	135
Table 115 – NLME-PATH_FAILURE.request parameters	136
Table 116 – NLME-PATH_FAILURE.indication parameters	137
Table 117 – NLME-PATH_FAILURE.confirm parameters	137
Table 118 – NLME-INFO_GET.request parameters.....	138
Table 119 – NLME-INFO_GET. indication parameters	139
Table 120 – NLME-INFO_GET.response parameters	139
Table 121 – NLME-INFO_GET.response parameters	140
Table 122 – NLME-INFO_SET.request parameters	141
Table 123 – NLME-INFO_SET.indication parameters.....	141
Table 124 – NLME-SET. response parameters	142
Table 125 – NLME-SET.confirm parameters	143
Table 126– Control field format.....	143
Table 127 – Network layer command packet.....	146
Table 128 – Execution results of commands	147
Table 129 – Format of joining request packet.....	147
Table 130 – Format of joining response packet.....	147
Table 131 – Format of communication status report request packet.....	148
Table 132 – Format of leaving request packet.....	148
Table 133 – Value of leaving reason	148
Table 134 – Format of leaving response packet.....	149
Table 135 – Format of cluster member report request packet.....	149
Table 136 – Format of cluster member report response packet	149
Table 137 – Format of neighbor information report request packet.....	150
Table 138 – Format of route adding request packet	150

Table 139 – Format of route adding response packet.....	150
Table 140 – Format of route update request packet	151
Table 141 – Format of route update response packet.....	151
Table 142 – Format of route deleting request packet	151
Table 143 – Format of route deleting response packet.....	152
Table 144 – Format of link adding request packet	152
Table 145 – Format of link adding response packet	152
Table 146 – Format of link update request packet.....	153
Table 147 – Format of link update response packet	153
Table 148 – Format of link release request packet.....	154
Table 149 – Format of link release response packet	154
Table 150 – Format of superframe adding request packet.....	154
Table 151 – Format of superframe adding response packet	155
Table 152 – Format of superframe update request packet.....	155
Table 153 – Format of superframe update response packet	155
Table 154 – Format of superframe release request packet.....	156
Table 155 – Format of superframe release response packet	156
Table 156 – Format of device condition report request packet.....	156
Table 157 – Format of device condition information	157
Table 158 – Format of channel condition report request packet	157
Table 159 – Format of channel quality information	157
Table 160 – Format of path failure report request packet	158
Table 161 – Format of attribute getting request packet	158
Table 162 – Format of attribute getting response packet.....	159
Table 163 – Format of attribute setting request packet.....	159
Table 164 – Format of attribute setting response packet	160
Table 165 – Method definition.....	163
Table 166 – Request format of READ	163
Table 167 – Response format of READ method	163
Table 168 – Request format of WRITE method	164
Table 169 – Response format of WRITE method.....	164
Table 170 – Format of PUBLISH method	165
Table 171 – Format of REPORT method	165
Table 172 – Format of REPORT ACK method.....	165
Table 173 – ASLDE-DATA.request parameters	167
Table 174 – ASLDE-DATA.confirm parameters	167
Table 175 – ASLDE-DATA.indication parameters.....	168
Table 176 – ASLDE-AGG.request parameters	168
Table 177 – ASLDE-DAG.indication parameters	169
Table 178 – Packet control field format.....	172
Table 179 – Packet type subfield value	172
Table 180 – Structure of DLSL security header	178
Table 181 – Structure of security control field in DLSL security header.....	179

Table 182 – Structure of security material control field in DLSL security header.....	179
Table 183 – Structure of ASL security header field	180
Table 184 – DLME-SEC.request parameters.....	183
Table 185 – DLME-SEC.indication parameters	183
Table 186 – DLME-SEC.response parameters	184
Table 187 – DLME-SEC.confirm parameters.....	184
Table A.1 – Graded and layered security measures for WIA-PA network.....	190
Table A.2 – Security levels of data packets.....	190
Table B.1 – Packet or frame format in octet(s)	191
Table B.2 – Subfield format in bit(s).....	192
Table C.1 – AIO Class Attribute	193
Table C.2 – AIO Instance Attributes	194

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
 FIELDBUS SPECIFICATIONS –
 WIA-PA COMMUNICATION NETWORK
 AND COMMUNICATION PROFILE**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC 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 standard cancels and replaces IEC/PAS 62601 published in 2009. This first edition constitutes a technical revision.

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

FDIS	Report on voting
65C/663/FDIS	65C/671/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 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 COMMUNICATION NETWORKS – FIELDBUS SPECIFICATIONS – WIA-PA COMMUNICATION NETWORK AND COMMUNICATION PROFILE

1 Scope

This International Standard specifies the system architecture and the communication protocol of Wireless networks for Industrial Automation – Process Automation (WIA-PA) built on IEEE STD 802.15.4-2006.

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.

IEC/TS 61804-2: 2006, *Function blocks (FB) for process control – Part 2: Specification of FB concept*

IEEE STD 802.15.4-2006, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (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. Its value increases by one, and does not decrease. Its current value is always the sequence number of the current timeslot. Its maximum value is $(2^{48}-1)$. After the maximum value, it re-counts from zero

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

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

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**cluster head**

manager in a cluster, performed by the routing device

3.1.12**cluster member**

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 These networks may or may not have the same set of rules.

3.1.14**communication resources**

channels and timeslots used to transport frames

3.1.15**WIA-PA configuration software**

software tools for configuring the WIA-PA network and devices

3.1.16**data link sub-layer**

upper layer of the IEEE STD 802.15.4-2006 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 installed 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

[IEEE STD 802.15.4-2006]

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 neighbor devices in one network transaction without the participation of any other devices in the WIA-PA network

NOTE 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**interoperability**

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

[ISO/IEC TR 10000-1: 1998, 3.2.1, modified]

3.1.26**joining**

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

3.1.27**link**

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

NOTE It includes source/destination address, timeslot, channel, direction, and link type.

3.1.28**mesh**

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

NOTE One routing device may connect to the gateway device and more than one other routing device.

3.1.29**multicast**

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

3.1.30**network address**

16-bit unsigned integer uniquely identifying the device in the WIA-PA network; also called short address

NOTE The most significant 8 bits of the network address, assigned by the network manager, identify different clusters.

3.1.31**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

3.1.32**packet**

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

[IEEE STD 802.15.4-2006, 3.31]

3.1.33**packet lifecycle**

maximal packet survival time from being generated to being dropped

3.1.34**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

3.1.35**physical address**

EUI-64 bits uniquely identifying the device in the WIA-PA network; also called long address

NOTE A physical address is assigned by the manufacturers.

3.1.36**routing device**

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

3.1.37**security manager**

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

3.1.38**superframe**

collection of timeslots repeating over time

NOTE It specifies the transmitting or receiving time of periodic communication.

3.1.39**timeslot**

basic time unit of data exchange

NOTE Its duration is configurable in the WIA-PA network.

3.1.40**timeslot hopping**

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

3.1.41**unicast**

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

3.1.42**virtual communication relation**

communication paths and communication resources between two user application objects

3.1.43**WIA-PA device**

device in the WIA-PA network, e.g. the 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	ASLDE Service Access Point
ASLME	Application Sub-Layer Management Entity
ASLME-SAP	ASLME Service Access Point
ASLPDU	Application Sub-Layer Protocol Data Unit
ASN	Absolute timeSlot Number
CAP	Contention Access Period
CFP	Contention Free 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
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
KP	Provision 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
SMK	Symmetric Master Key
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 Specification of data types

4.1 Representation of boolean type

```
Boolean :: = BOOLEAN           -- non 0: TRUE
```

```
-- 0: FALSE
```

4.2 Representation of unsigned integer type

```
Unsigned8 ::= INTEGER(0..255) -- integer range:  $0 \leq i < 2^8$ 
```

```
Unsigned16 :: = INTEGER(0..65 535)           -- integer range:  $0 \leq i < 2^{16}$ 
```

```
Unsigned24 :: = INTEGER(0.. 224-1)           -- integer range: 0 <= i <= 224-1
```

```
Unsigned32 :: = INTEGER(0.. 232-1)           -- integer range: 0 <= i <= 232-1
```

```
Unsigned40 ::= INTEGER(0.. 240-1)           -- integer range: 0 <= i <= 240-1
```

```
Unsigned48 ::= INTEGER(0.. 248-1)           -- integer range: 0 <= i <= 248-1
```

```
Unsigned64 ::= INTEGER(0.. 264-1)           -- integer range: 0 <= i <= 264-1
```

4.3 Representation of octet type

```
Octetstring ::= OCTET STRING -- 8-bit string
```

4.4 Representation of floating point number type

```
Float ::= BIT STRING SIZE (4) -- single precision, range references to
```

IEEE STD 754 Short Real Number (32 Bit)

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 start-up time of a redundant device is not later than that of the primary device. Redundant devices do not start up their radio modules. When the information of primary devices is changed, the primary devices should timely backup the changed information to their redundant devices in the wired manner. The wired manner is not specified in this document.

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.

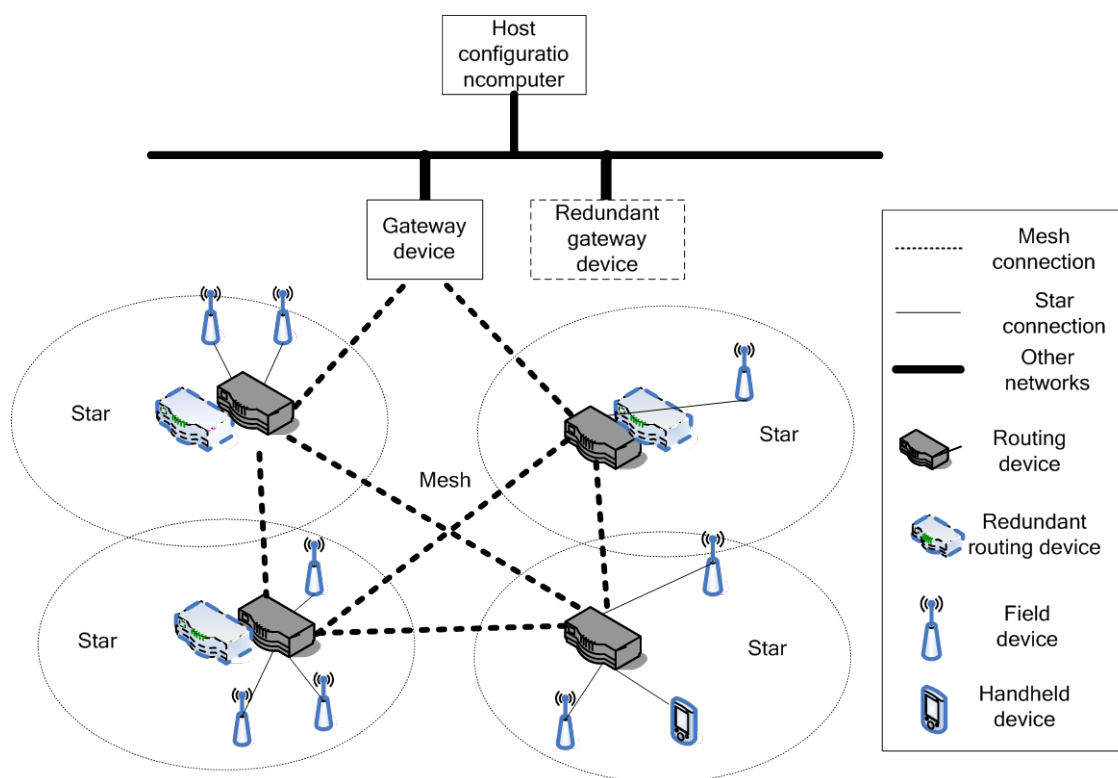


Figure 1 – Example of WIA-PA physical topology (combination of star and mesh)

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.

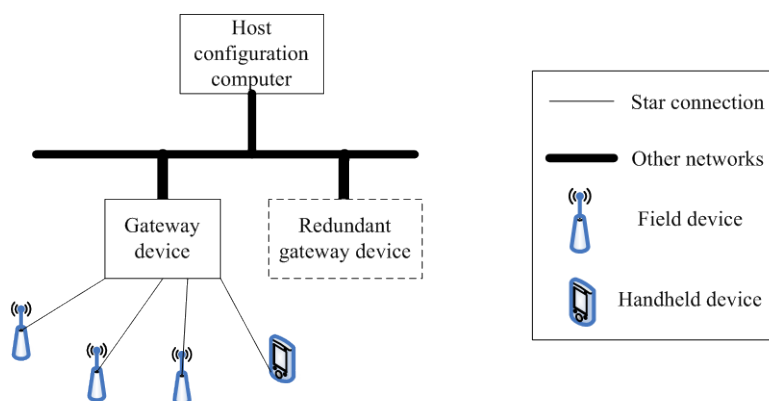


Figure 2 – Example of WIA-PA physical topology (star-only)

NOTE 1 The star-only network is a special case of the hierarchical network. In the rest of this document, the specification of the hierarchical network covers that of the star-only network. Therefore, the specification of the star-only network will not be specially described.

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.

NOTE 2 The primary device is marked by the parameter "PrimaryDevAddr" and the redundant device is marked by the parameter "RedundantDevFlag" in Table 19.

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 802.15.4-2006.

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 802.15.4-2006 MAC
Physical	Mechanical / electrical connection. Transmits raw bit stream	PHY (IEEE STD 802.15.4-2006-based radios)

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.

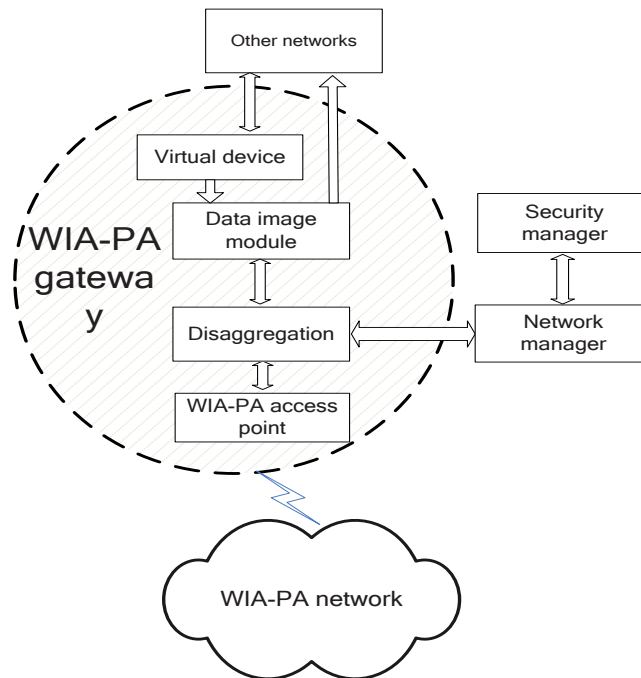


Figure 4 – The architecture of WIA-PA gateway

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.

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...

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.

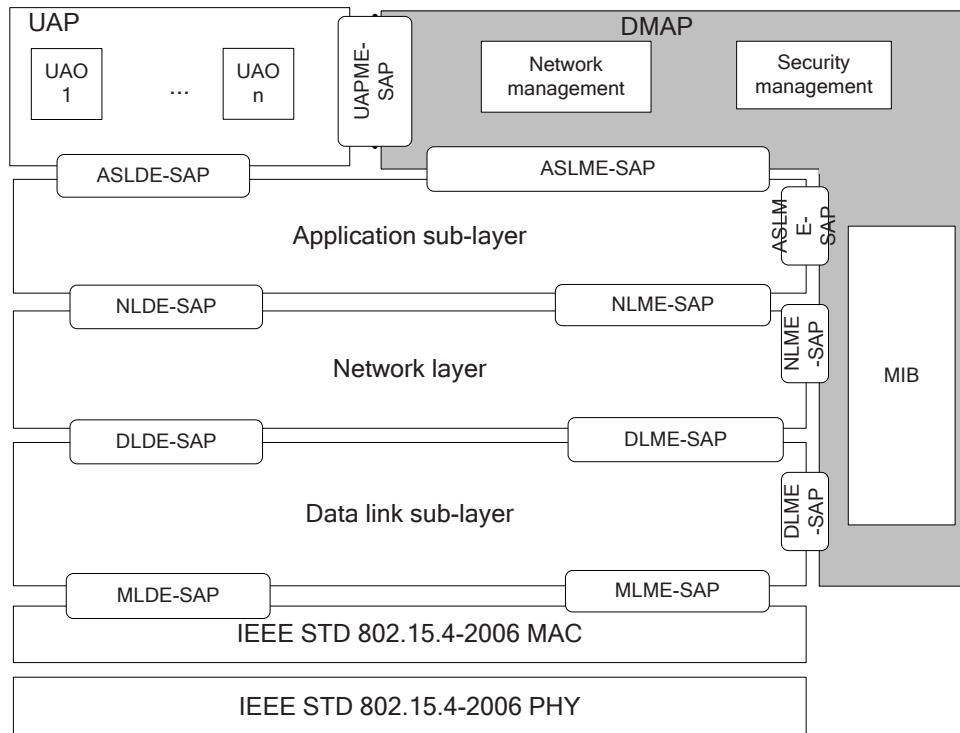


Figure 5 – DMAP in system management

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 routing device is assigned by the NM. The short address of each field device is assigned by the routing device.

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 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 10.1 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.

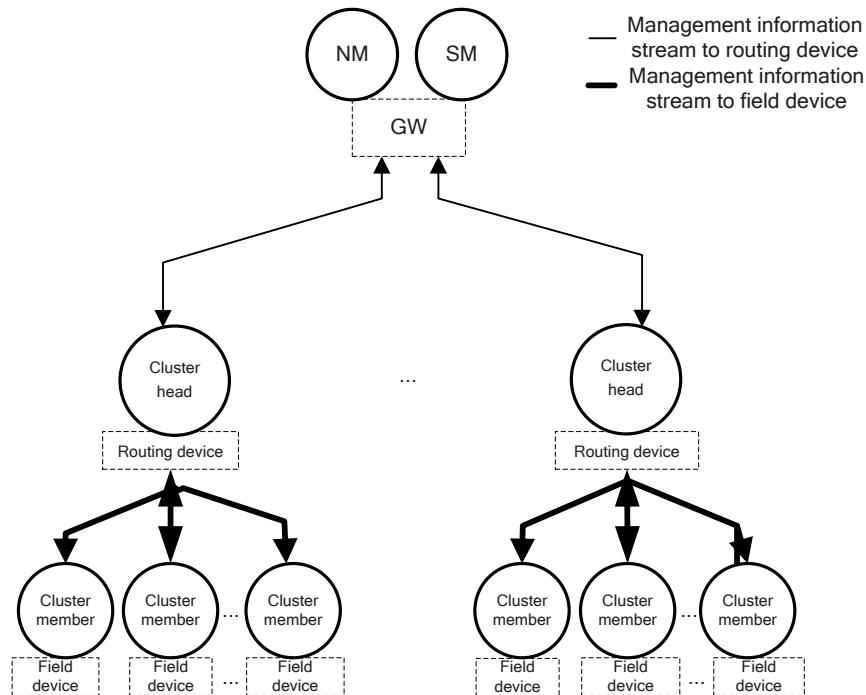


Figure 6 – Hybrid centralized and distributed system management scheme

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 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.

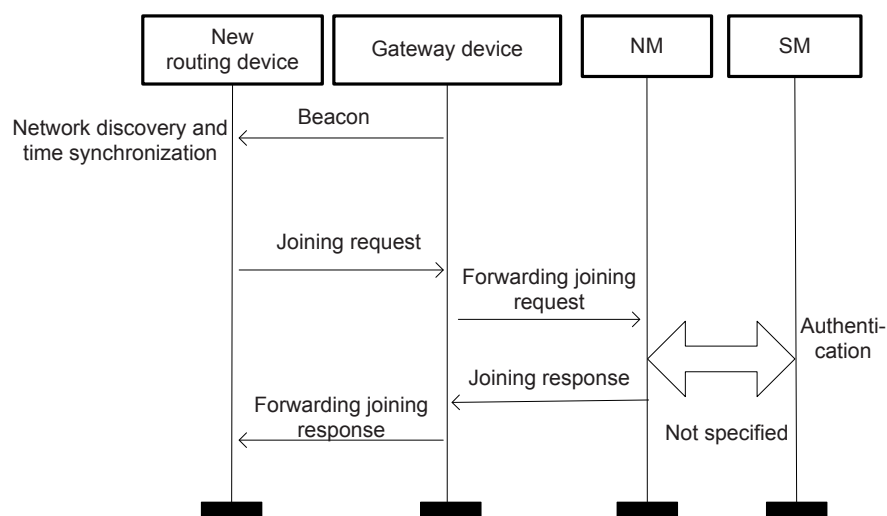


Figure 7 – Joining process of routing device through the gateway device

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

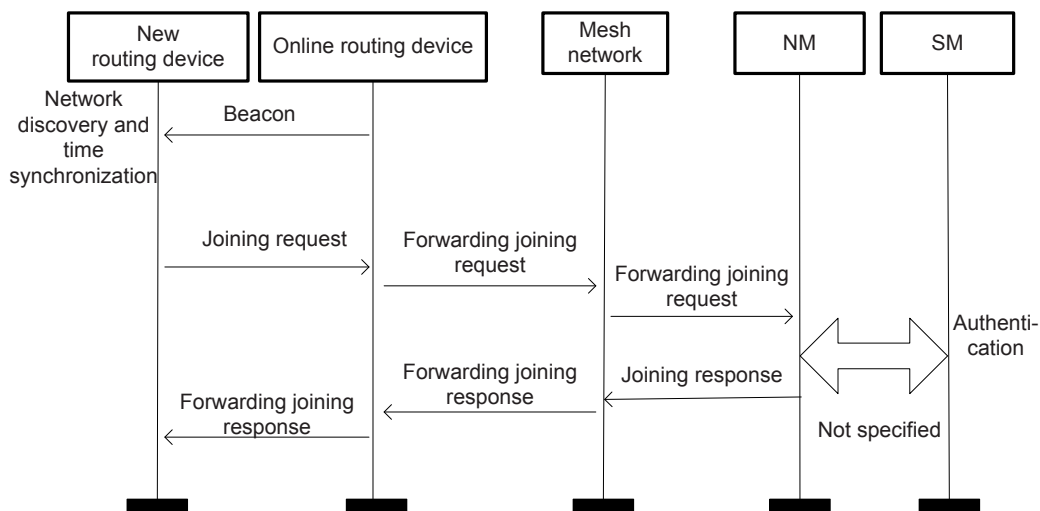


Figure 8 – Joining process of routing device through an online routing device

See 9.5.8 for the allocation of communication resources.

6.3.2 Joining process of field device

When a field 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 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 Table 49 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 one 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.

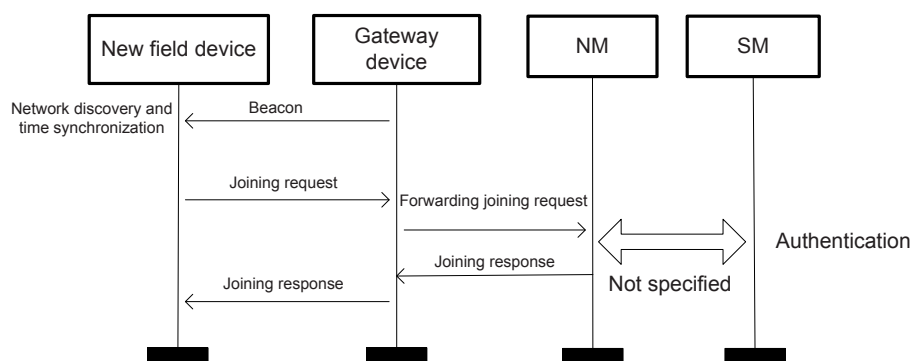


Figure 9 – Joining process of field device through a gateway device

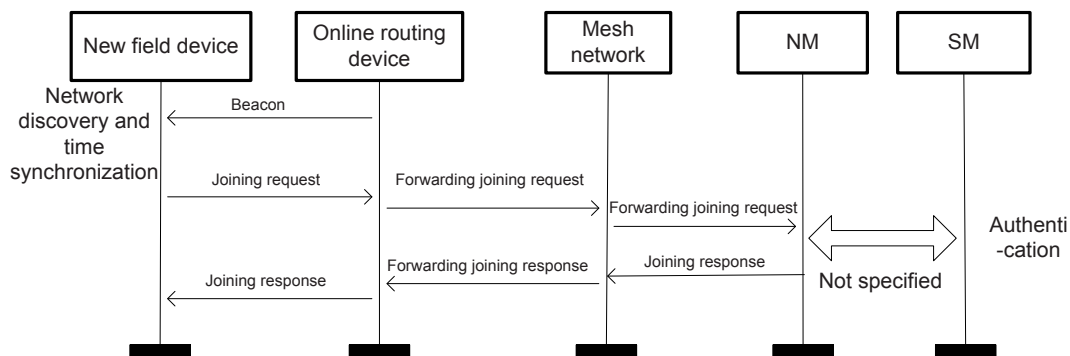


Figure 10 – Joining process of field device through a routing device

NOTE 1 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.

NOTE 2 See clause 11 for detailed information about security.

6.3.3 Addressing and address assignment

In the WIA-PA network, each 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.

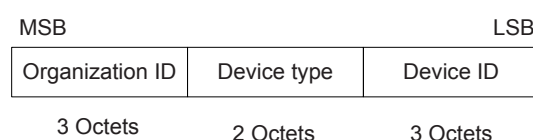


Figure 11 – Long address structure of device

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.

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.

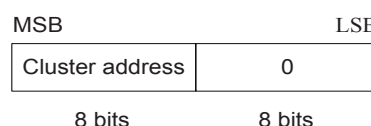


Figure 12 – Short address structure of routing device

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. The intra-cluster address is assigned by the cluster head.

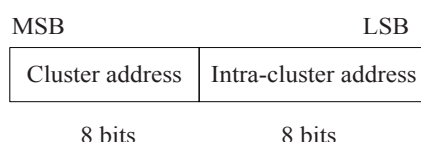


Figure 13 – Short address structure of field device

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, UAO ID at destination side, addresses of source device/destination device, VCR type, valid scope, etc (see Table 20).

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

- Publisher/Subscriber (P/S) VCR, which is used to publish periodic data;
- Report source /Sink (R/S) VCR, which is used to support aperiodic events and trend reports;
- 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 cluster head. 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.

NOTE PAGOs, DGOs, and DAGOs are three special UAOs. See 6.6.1 for DAGOs.

6.4.2 Protocol support for VCR

The protocol supports for VCRs are listed in Table 1.

Table 1 – Protocol support for VCR

Protocol layer support			VCR types		
			P/S VCR	R/S VCR	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:

- a) 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).
- b) 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 20 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 14. 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.

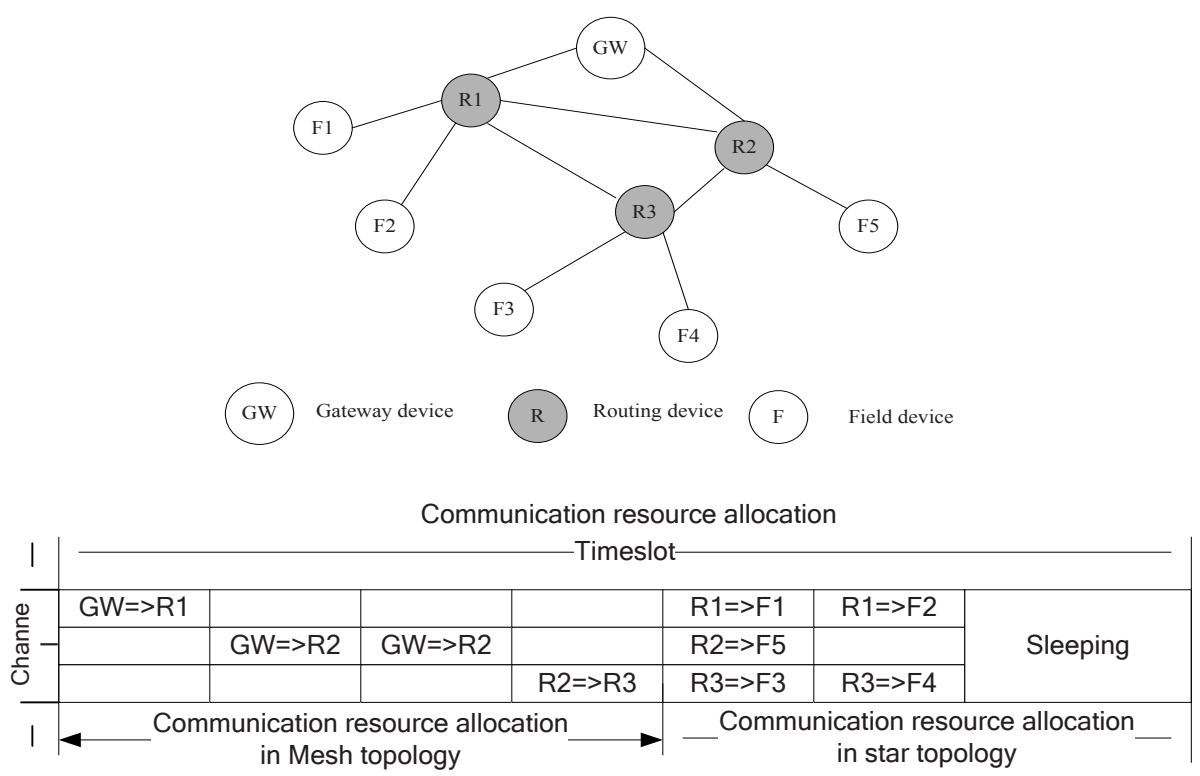


Figure 14 – An example of resource allocation

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 employed for allocating communication resources:

- a) First allocating channels to the beacon frame and active period;
- b) First allocating timeslots to the devices with the fastest update rate;
- c) First allocating resources to the packet with the earliest generating time in multi-hop situations;
- d) First 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 neighbor devices on each channel and report the neighbor information to the NM. After receiving the neighbor 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.

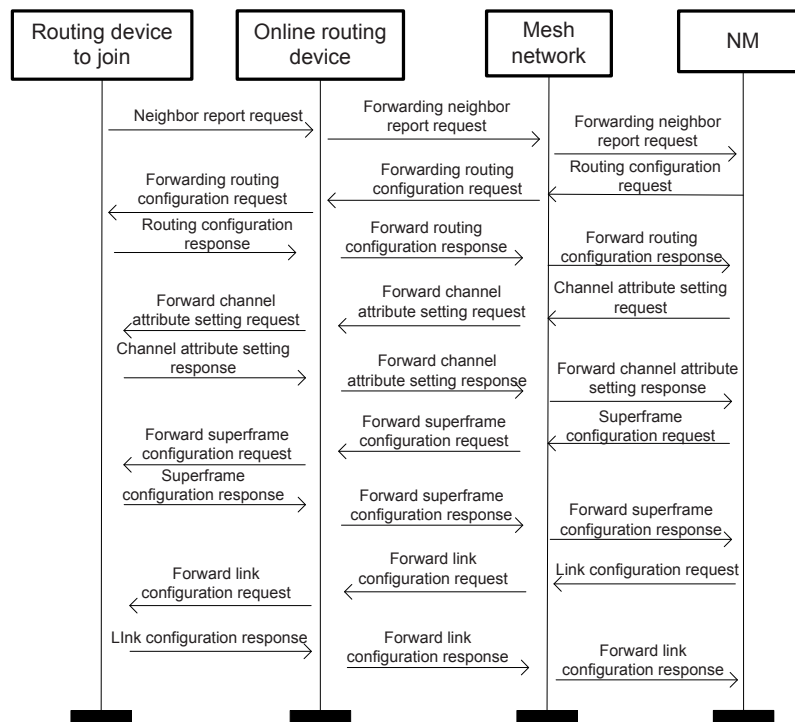


Figure 15 – Allocation process of routing device's communication resources

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.



6.6.1 Aggregation

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

- 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:

- a) A field device supports the aggregation function, while its routing device does not.
- b) A routing device supports the aggregation function, while its field device does not.
- c) Both, a field device and its routing device support the aggregation function.
- d) 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 2.

Table 2 – Relations between VCR and aggregation function

	Field device DAGO (Aggregation function)		Routing device PAGO (Aggregation function)		Gateway device DGO (Disaggregation function)	
	Disenable	Enable	Disenable	Enable	Disenable	Enable
Non-aggregation VCR	X		X		—	—
Data aggregation VCR		X	X ^a			X
		X		X ^b		X
Packet aggregation VCR	— ^c	— ^c		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:

- a) NM should read the AGGSupportFlag to verify whether devices support the aggregation function.
- b) 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 20) of its field devices in the cluster. When aggregation duration expires, the routing device aggregates all its packets and sends the aggregated packet out.
- c) 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 20) 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 3. 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 *Flagment* flat 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 *Flagment* 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 a superframe cycle. Once *AggPeriod* (see 6.9.1.2.1) expires, the PAGO aggregates the packets according to the format that is shown in Table 4, and searches the *RouteID* related to the packet aggregation VCR. The aggregated packet, packet aggregation VCR, and the related *RouteID* are then sent to the NL; the NL should send this aggregated packet to the gateway device through the related *RouteID*. 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 *RouteID*.

Table 3 – 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 4 – Format of aggregated packet 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 19). If the gateway device supports the disaggregation mechanism, the NM sets the aggregation and disaggregation enable flag *AGGEnableFlag* to 1 (see Table 19).

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 1s, and the data update rates of b1 and b2 are configured to 4s. 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 1s. 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.

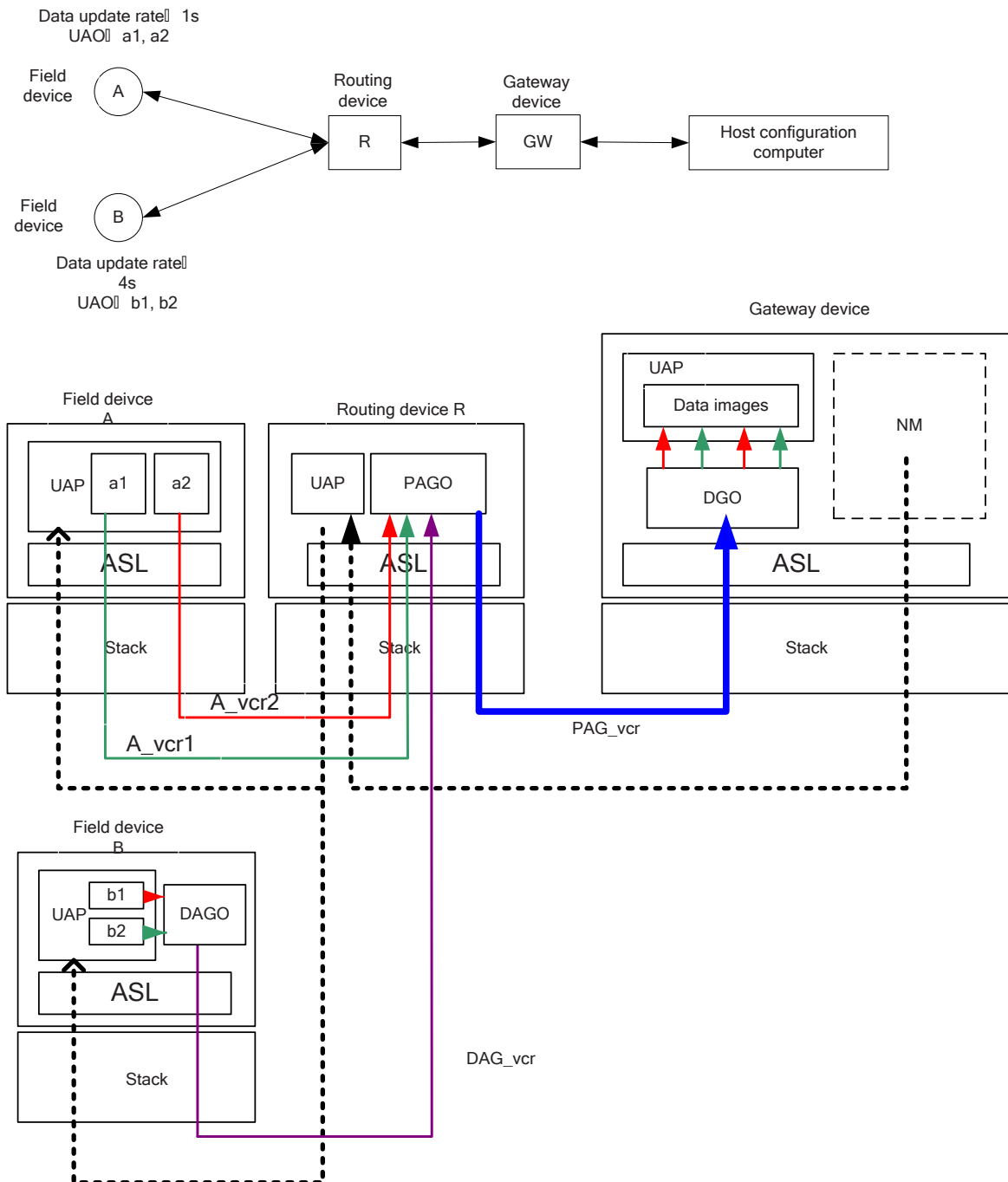


Figure 17 – Example of aggregation and disaggregation

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 4s, 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 1s. 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 5.

Table 5 – 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 6.

Table 6 – 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 7)		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 10.2.3 Table 165.

The definition of the MEM_STRUCT structure is shown in Table 7.

Table 7 – MEM_STRUCT structure

Attribute ID	Name	Data type	Description
0	AppObjID	Unsigned8	The identifier of the UAO
1	AppObjInstID	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 8.

Table 8 – 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 9.

Table 9 – PAGO instance attributes

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	PagoInstID	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 10.2.3 Table 165.

The attributes of the DGO class are shown in Table 10.

Table 10 – 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 11.

Table 11 – DGO instance attributes

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

The methods supported by the DGOs are shown in 10.2.3 Table 165.

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 for more details.

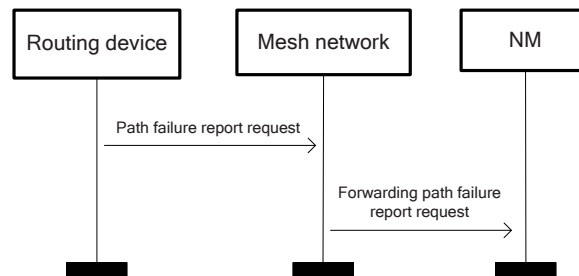


Figure 18 – Process of path failure report

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 neighboring 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 for more details.

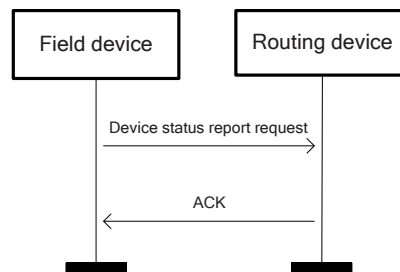


Figure 19 – Device status report process of field device

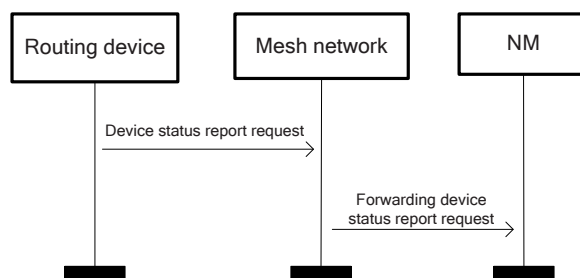


Figure 20 – Device status report process of routing device

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 for more details.

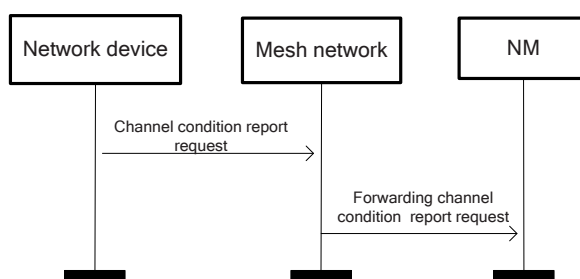


Figure 21 – Process of channel condition report

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 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 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.

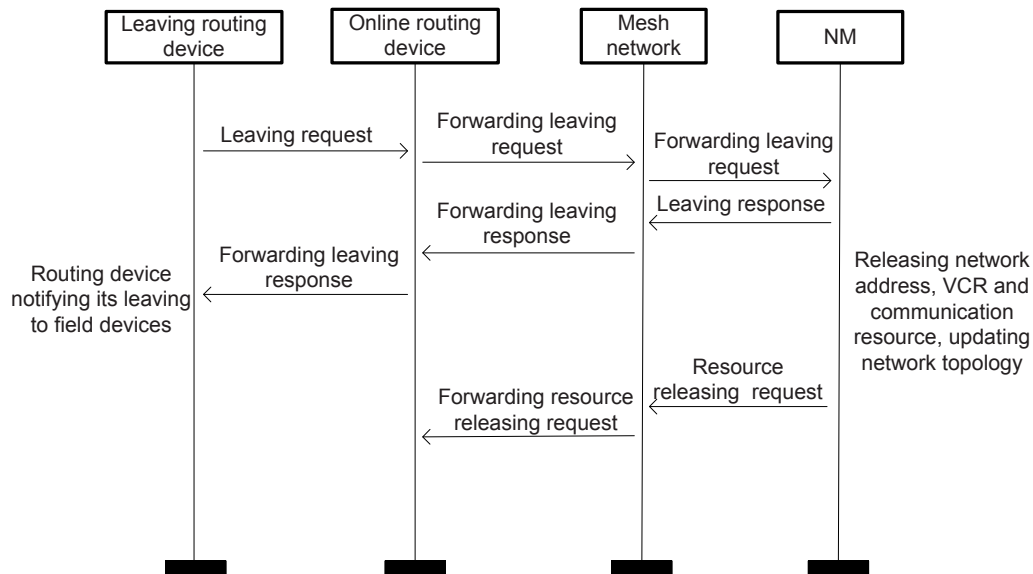


Figure 22 – Active leaving process of routing device

The passive leaving process of a routing device is shown in Figure 23.

- The NM sends the leaving request to a routing device.
- The routing device sends a leaving response to the NM after receiving the leaving request.
- The routing device notifies its leaving to the field devices. After passive leaving of field devices, the routing device leaves the network.
- 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.

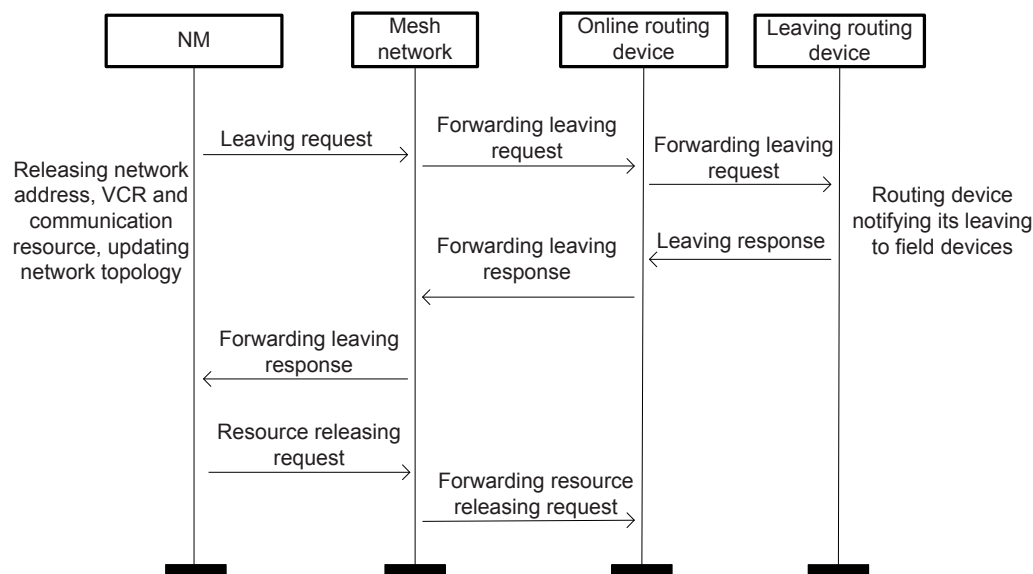


Figure 23 – Passive leaving process of routing device

6.8.3 Leaving process of field device

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

The active leaving process of a field device is 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.

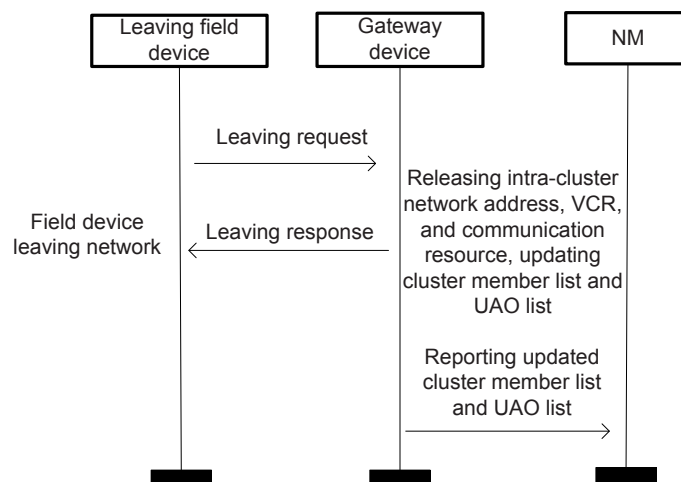


Figure 24 – Active leaving process of field device (leaving from gateway device)

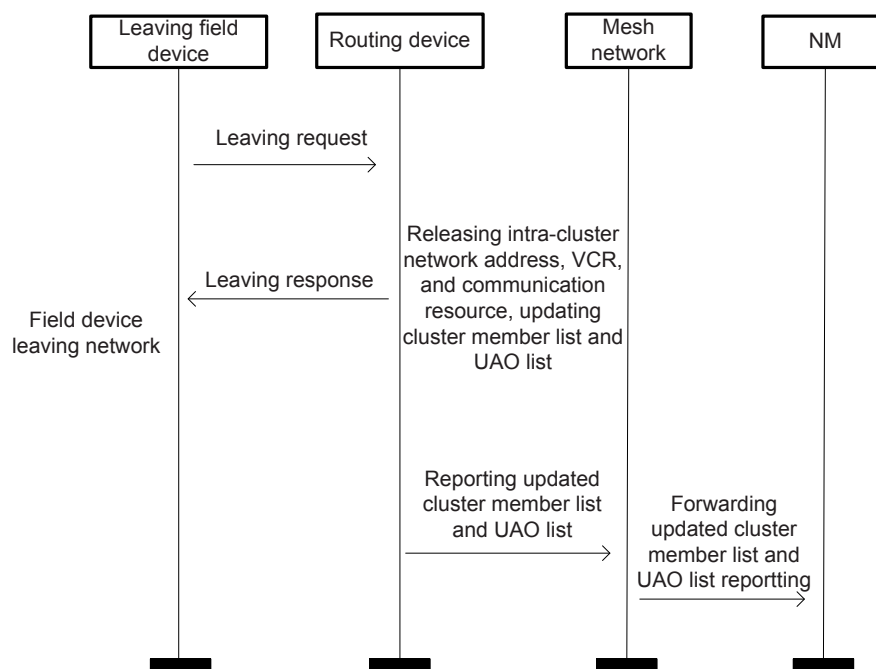


Figure 25 – Active leaving process of field device (leaving from routing device)

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

- a) The routing device or the gateway device sends the leaving request to a field device.
- b) The field device returns the leaving response to the routing device or the gateway device.
- c) 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.

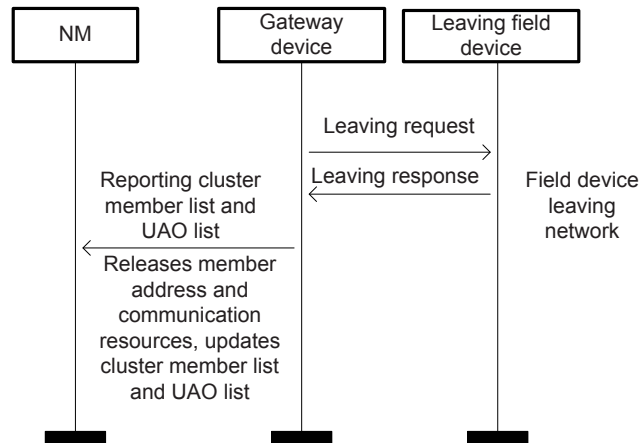


Figure 26 – Passive leaving process of field device (leaving from gateway device)

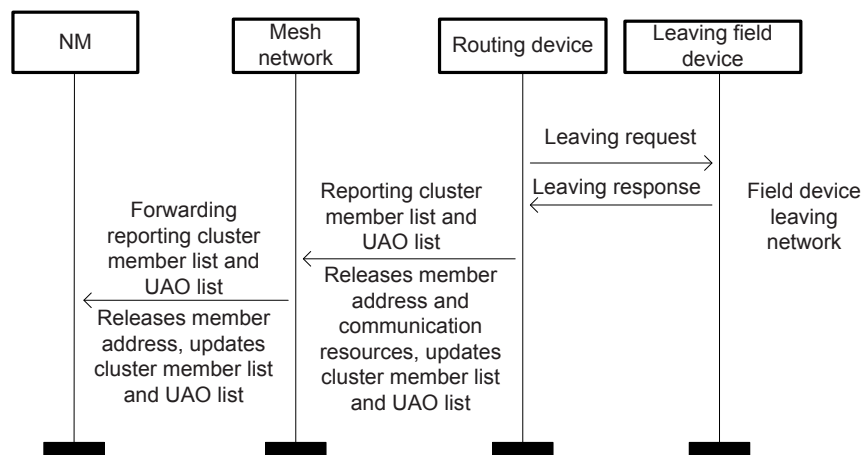


Figure 27 – Passive leaving process of field device (leaving from routing device)

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 the attributes in the MIB:

- a) R (Read), which means the values of the attribute may be read by other devices in WIA-PA network; and
- b) W (Write), which means 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 12. The values of attributes numbered 0 to 20 are identical in the entire network; and the values of attributes numbered 21 to 28 are device specific.

Table 12 – Unstructured attributes

ID	Name	Data type	Valid range	Access type	Storage type	Default value	Description
0	NetworkID	Unsigned8	0 to 255	R/W	Static	0	Network identifier, used for multiple networks coexisting
1	StatisticsDuration	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 neighbor tables.
2	MaxNSDUSize	Unsigned8	0 to 255	R	Static	N/A	Maximum size of service data unit supported by the NL
3	BitMap ^a	Unsigned32	32 bits	R/W	Dynamic	0	Indicating if a channel can be used: 0 = Not used; 1 = Used. The value of bit <i>i</i> indicates the usage status of channel <i>i</i> . <i>i</i> is related to the IEEE 802.15.4 channel number.
4	KeepAliveDuration	Unsigned24	0 to (2 ²⁴ -1)	R/W	Static	0	Duration between two keep-alive frames (in milliseconds)