Honeywell

THE POWER OF CONNECTED

KSMW-PA2502 - Companion Standard

G3-PLC Implementation Guide

Revision 1.1

18.09.2018

Copyright

Disclaimer

Table OF CONTENTS

1. INTRODUCTION

This document is an implementation guide required for the development of a G3-PLC communication infrastructure.

It is a complementary document to the ITU-T G.9901 and G.9903 standards, describing the physical and data link layers.

1.1 REVISIONS HISTORY

Version	Revisions	Date	Author
0.0	Initial Draft Version	16.11.2017	R. Thor
0.1	1st Draft Release	20.12.2017	R. Thor
0.2	Update according: KSMW PA2502 Companion Standard Review List Rev 0.2.xlsx	29.01.2018	R. Thor
0.3	Update according: KSMW PA2502 Companion Standard Review List Rev 0.3.xlsx	22.02.2018	R. Thor
0.4	Update according: KSMW PA2502 Companion Standard Review List Rev 0.4.xlsx	06.03.2018	R. Thor
0.5	Update according: KSMW PA2502 Companion Standard Review List Rev 0.5.xlsx	19.03.2018	R. Thor
0.6	Update according: KSMW PA2502 Companion Standard Review List Rev 0.6.xlsx	06.04.2018	R. Thor
1.0	Update according: KSMW PA2502 Companion Standard Review List Rev 1.0.xlsx	03.07.2018	R. Thor
1.1	Update according: KSMW PA2502 Companion Standard Review List Rev 1.1.xlsx	18.09.2018	R. Thor

2. OVERVIEW

2.1 SCOPE

In addition to the Companion Standard and the G3-PLC physical and data link layer specifications, the present “Implementation Guidelines” come as a companion document defining the G3-PLC metering profile, from transport layer down to the physical layer:

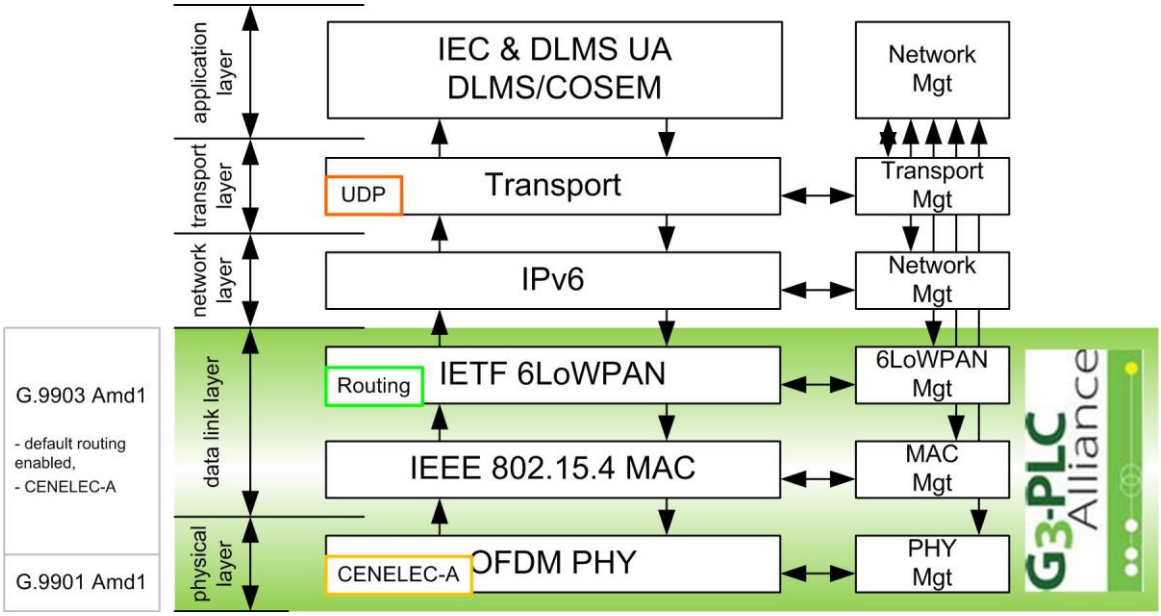

Fig. 1: G3-PLC-based metering profile

2.2 PURPOSE

This document precisely describes the features of the whole G3-PLC-based communication stack for metering, shown in Fig. 1. This stack being built with several standards, this document aims to specify which clauses shall be implemented, with or without modifications, and which clauses shall not be implemented.

The DLMS/COSEM application layer definitions are covered by a separate document, as multiple interfaces will access this layer.

2.3 RESTRICTIONS

The basis for this document was provided by Enedis (LINKY-GENEP1-GUIDE-CPL-G3, rev 1.6, release 01.09.2017)

3. NORMATIVE REFERENCES

[1] Recommendation ITU-T G.9901 (06/2017): *Narrowband Orthogonal Frequency Division Multiplexing Power Line Communication Transceivers – Power Spectral Density Specification* – available at *http://www.itu.int/rec/T-REC-G.9901/en*

[2] Recommendation ITU-T G.9903 (08/2017): *Narrowband Orthogonal Frequency Division Multiplexing Power Line Communication Transceivers for G3-PLC networks – available at https://www.itu.int/rec/T-REC-G.9903/en*

[3] not referenced anymore

[4] not referenced anymore

[5] IEEE 802.15.4: *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)* – 2006

[6] RFC 768: *User Datagram Protocol* – J. Postel – 1980

[7] RFC 8200: *Internet Protocol, Version 6 (IPv6) Specification* – S. Deering, R. Hinden – 2017

[8] RFC 4291: *IP Version 6 Addressing Architecture* – R. Hinden, S. Deering – 2006

[9] RFC 4193: *Unique Local IPv6 Unicast Addresses* – R. Hinden, B. Haberman – 2005

[10] RFC 4944: *Transmission of IPv6 Packets over IEEE 802.15.4 Networks* – G. Montenegro, N. Kushalnagar, D. Culler – 2007

[11] RFC 6282: *Compression format for IPv6 Datagrams over IEEE 802.15.4-Based Networks* – J. Hui, P. Thubert – 2011

[12] RFC 6775: *Neighbour Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)* – Z. Shelby, S. Chakrabarti, E. Nordmark, C. Bormann – 2012

[13] RFC 4861: *Neighbour Discovery for IP version 6* – T. Narten, E. Nordmark, W. Simpson, H. Soliman – 2007

[14] draft-clausen-lln-loadng-15: *The Lightweight On-demand Ad hoc Distance-vector Routing Protocol – Next Generation (LOADng)* – T. Clausen, A. Colin de Verdiere, J. Yi, A. Niktash, Y. Igarashi, H. Satoh, U. Herberg, C. Lavenu, T. Lys, C. Perkins, J. Dean – 2017

[15] EN 50065-1: *Signaling on low-voltage electrical installations in the frequency range 3 kHz to 148,5 kHz – Part 1: General requirements, frequency bands and electromagnetic disturbances* – 2011

[16] not referenced anymore

[17] RFC 2474: *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* – K. Nichols, S. Blake, F. Baker, D. Black – 1998

[18] RFC 4443: *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification* – A. Conta, S. Deering, M. Gupta – 2006

[19] EN50065-7: Signaling on low voltage electrical installations in the frequency range 3kHz to 148,5 kHz – Part 7 : Equipment Impedance

[20] RFC 6980: Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery – F. Gont - 2013

[21] RFC7112: Implications of Oversized IPv6 Header Chains – F. Gont, V. Manral, R. Bonica - 2014

4. ACRONYMS

6CO	6LoWPAN Context Option
6LoWPAN	IPv6 Low power Wireless Personal Area Network
6LBR	6LoWPAN Border Router
AARE	Application Association RElease
AARQ	Application Association ReQuest
ACSE	Application Control Service Element
AMI	Advanced Metering Infrastructure
AP	Application Process
API	Application Programming Interface
ASO	Application Service Object
ARQ	Automatic Repeat request
COSEM	COmpanion Specification for Energy Metering
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
D8PSK	Differential 8 Phase Shift Keying
DBPSK	Differential Binary Phase Shift Keying
DHCP	Dynamic Host Configuration Protocol
DLMS	Device Language Message Specification
DoS	Denial of Service
DQPSK	Differential Quadrature Phase Shift Keying
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EAP-PSK	EAP – Pre Shared Key
EUI	Extended Unique Identifier
FEC	Forward Error Correction
GMK	Group Master Key
IANA	Internet Assigned Numbers Authority
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFFT	Inversed Fast Fourier Transform
ITU	International Telecommunication Union
LBA	LoWPAN Bootstrapping Agent
LBD	LoWPAN Bootstrapping Device
LBP	LoWPAN Bootstrapping Protocol
LBS	LoWPAN Bootstrapping Server
LN	Logical Name
LOADng	6LOWPAN Ad-hoc on-Demand distance vector routing new generation

LV	Low Voltage
MAC	Medium Access Control
MIB	Management Information Base
MV	Medium Voltage
NAN	Neighbourhood Area Network
NDP	Neighbour Discovery Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PDU	Protocol Data Unit
QoS	Quality of Service
RA	Router Advertisement
RS	Router Solicitation
TCP	Transmission Control Protocol
ULA	Unique Local Address
UDP	User Datagram Protocol
WAN	Wide Area Network

5. CONVENTIONS

Some sections of the present document are referring to other reference documents in order to specify more precisely the requirements to be fulfilled by the implementations. The status of each clause of the reference document is given using the following convention:

- I = “Informative”: the statements of the reference document are provided for information only.
- M = “Mandatory”: the statements of the reference document shall apply without modifications or remarks.
- S = “Selection”: the statements of the reference document shall apply with the selections and/or the modifications specified.
- E = “Extension”: the statements of the reference document shall apply with the extensions specified.
- N/R = “Not Relevant”: the statements of the reference document do not apply.

6. G3-PLC MODEM ELECTRICAL SPECIFICATIONS

6.1 OUTPUT LEVEL FOR CENELEC-A

G3-PLC modems working in the Cenelec-A band shall conform to the definition in ITU-9901 [1] concerning the output specification relating to the 3 kHz–148.5 kHz band.

Conformance with EN50065-1

G3-PLC modems have to conform to EN 50065-1 [15] transmitter output voltage and disturbance limits requirements. In addition, devices shall emit at the maximum output level allowed by EN 50065-1 [15].

Additional tests

G3-PLC modems shall meet the following requirements:

- According to ITU-T G.9901 [1], no individual carrier shall have average power outside of the range ±5 dB with respect to the average power in all of the subcarriers (when set to transmit equal transmit power level). This measurement is done with a CISPR-16 LISN.
- Single-phase transmitters are required to emit at an output power level higher than 114 dBµVrms measured in a bandwidth equal or greater than the bandwidth of the transmitter. This test is performed using a 2-ohm artificial mains network (as shown in Figure 2).
- Three-phase devices emitting simultaneously on all phases are required to emit at an output power level higher than 108 dBµVrms (between phases and ground) measured in a bandwidth equal or greater than the bandwidth of the transmitter. This test is performed using a 2-ohm artificial mains network (as shown in Figure 2).
- For single and three-phase transmitters, no individual carrier shall have average power outside of the range ±5 dB with respect to the average power in all of the subcarriers (when set to transmit equal transmit power level). This test is performed using a 2-ohm artificial mains network (as shown in Figure 2).

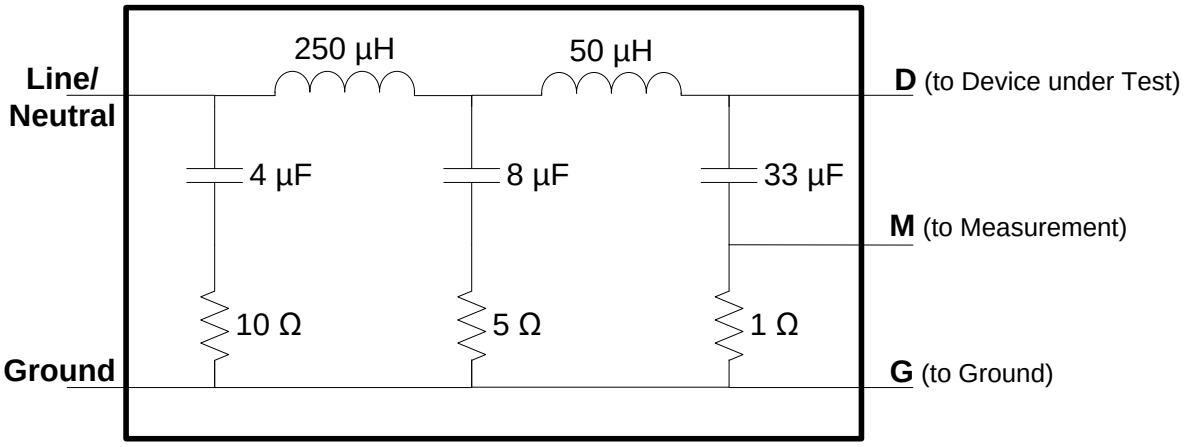

Fig. 2: A 2-ohms artificial mains network cell

6.2 OUTPUT LEVEL FOR FCC

G3-PLC modems working in the FCC band shall conform to the definition in ITU-9901 [1] concerning the output specification relating to the 148.5 kHz–535 kHz band

6.3 RECEPTION INPUT IMPEDANCE

Couplers and analog front end components for the communication part should be selected carefully to maintain, when in receive mode, its input impedance modulus above 50 ohms in the frequency range [35 kHz - 500 kHz] measured at mains plane.

When a meter is located in a place where several meters are connected to the same phase, a large part of the signal is drained off due to the receiver input impedance presented by the meters that are connected to the same phase nearby. Keeping the impedance of the coupling at this fairly high impedance eases extending the range of the signal.

Measurement may be done using the test setup described in clause 5 of EN 50065-7 [19].

7. PHYSICAL AND DATA LINK LAYERS

The G3-PLC communication is based on those two documents:

- [1] Recommendation ITU-T G.9901 (06/2017) Narrowband Orthogonal Frequency Division Multiplexing Power Line Communication Transceivers – Power spectral density specification.
- [2] Recommendation ITU-T G.9903 (08/2017): Narrowband Orthogonal Frequency Division Multiplexing Power Line Communication Transceivers for G3-PLC networks –

.

7.1 G3-PLC PHYSICAL LAYER

The G3-PLC physical layer is given in ITU-T G.9901 [1] for the frequency bandplan definition and on ITU-T G.9903 [2] for the PHY operational description.

Frequency bandplan and physical parameters

G3-PLC devices implementing the G3-PLC profile defined in this document operate in the CENELEC-A and FCC bandplan according to ITU-T G.9901 [1]:

Bandplan	Number of subcarriers	First subcarrier (kHz)	Last subcarrier (kHz)
CENELEC-A	36	35.9375	90.625
FCC	72	154.6875	487.500

In addition, the G3-PLC physical layers are based on the following system parameters, as defined in ITU-T G.9901 [1]:

	CENELEC-A	FCC
Number of FFT points	N = 256	N = 256
Number of overlapped samples	$N_0 = 8$	$N_0 = 8$
Number of cyclic prefix samples	$N_{CP} = 30$	$N_{CP} = 30$
Number of FCH symbols	$N_{FCH} = 13$	$N_{FCH} = 12$
Sampling Frequency	$F_s = 0.4$ MHz	$F_s = 1.2$ MHz
Number of symbols in preamble	$N_{pre} = 9.5$	$N_{pre} = 9.5$

7.1.1 Conformance with ITU-T G.9903 [2]

Clause	Title and remarks/modifications	Statement
1	Scope	M
2	References	M
3	Conventions and Definitions	M
3.1	Conventions	M
3.2	Terms defined elsewhere	M
3.3	Terms defined in this Recommendation	M
4	Abbreviations and Acronyms	M

5	Introduction to OFDM and the power line channel	M
6	General Description	I
6.1	Overall Infrastructure	I
6.2	Coexistence with other PLC Networks	N/R
6.2.1	Frequency division coexistence mechanism	N/R
6.2.2	Preamble-based coexistence mechanism	N/R
7	Physical Layer Specification	M
7.1	Introduction	M
7.2	System Parameters	M
7.3	Data Rate, Reed Solomon Block Size and Maximum PSDU Length	M
7.3.1	Data Rate Calculation and RS Block Size	I
7.3.1.1	CENELEC A Bandplan	M
7.3.1.2	CENELEC B Bandplan	N/R
7.3.1.3	FCC Bandplan	M
7.3.2	Maximum PSDU Length Calculation	M
7.4	Frame Structure	M
7.5	Preamble	M
7.6	Frame Control Header	M
7.6.1	CENELEC Bandplans	M
7.6.1.1	FCH for a data frame	M
7.6.1.2	FCH for ACK/NACK frame	M
7.6.1.3	CRC5	M
7.6.2	FCC Bandplan	M
7.6.2.1	FCH for a data frame	M
7.6.2.2	FCH for ACK/NACK frame	M
7.6.2.3	CRC8	M
7.7	Payload of PHY Frame	M
7.8	Scrambler	M
7.9	FEC Coding	M
7.9.1	Reed-Solomon Encoder	M
7.9.2	Convolutional Encoder	M
7.9.2.1	Encoding 2 Reed-Solomon Blocks	N/R
7.9.3	Robust and Super Robust Modes	M

7.9.3.1	Repetition Coding by 4 (RC4)	M
7.9.3.2	Repetition Coding by 6 (RC6)	M
7.10	Interleaver	M
7.10.1	Elementary Interleaver	M
7.10.2	Full block Interleaver	M
7.11	Mapping for DBPSK/DQPSK/D8PSK	M
7.12	Frequency Domain Pre-Emphasis	M
7.13	OFDM Generation (IFFT and CP Addition)	M
7.14	Windowing	M
7.15	Tone Masking and Tone Mapping	M
7.15.1	PN Modulating Unused Subcarriers	M
7.16	Coherent Modulation Scheme	M
7.16.1	Frame Structure – Coherent Modulation Scheme	M
7.16.2	Preamble – Coherent Modulation Scheme	M
7.16.3	Frame Control Header – Coherent Modulation Scheme	M
7.16.4	CRC – Coherent Modulation Scheme	M
7.16.5	Data Scrambler – Coherent Modulation Scheme	M
7.16.6	FEC Coding – Coherent Modulation Scheme	M
7.16.7	Payload Padding – Coherent Modulation Scheme	M
7.16.8	Interleaver – Coherent Modulation Scheme	M
7.16.9	Coherent Mapping for BPSK, QPSK, 8PSK, 16QAM and Robust Modes – Coherent Modulation Scheme	M
7.16.9.1	Mapping for BPSK and Robust Modulations – Coherent Modulation Scheme	M
7.16.9.2	Mapping for QPSK and Robust Modulations – Coherent Modulation Scheme	M
7.16.9.3	Mapping for 8PSK and Robust Modulations – Coherent Modulation Scheme	M
7.16.9.4	Mapping for 16QAM and Robust Modulations – Coherent Modulation Scheme	M
7.16.10	Pilot Tones – Coherent Modulation Scheme	N
7.16.10.1	Example of pilot tone assignment	I
7.16.11	Frequency Domain Pre-Emphasis – Coherent Modulation Scheme	M

7.16.12	OFDM Generation (IFFT and CP Addition) – Coherent Modulation Scheme	M
7.16.13	Windowing – Coherent Modulation Scheme	M
7.16.14	Adaptive Tone Mapping and Transmit Power Control – Coherent Modulation Scheme	M
7.17	PHY Primitives	M
7.17.1	Data Primitives	M
7.17.1.1	PD-DATA.request	M
7.17.1.2	PD-DATA.confirm	M
7.17.1.3	PD-DATA.indication	M
7.17.1.4	PD-ACK.request	M
7.17.1.5	PD-ACK.confirm	M
7.17.1.6	PD-ACK.indication	M
7.17.2	Management Primitives	M
7.17.2.1	PLME-SET.request	M
7.17.2.2	PLME-SET.confirm	M
7.17.2.3	PLME-GET.request	M
7.17.2.4	PLME-GET.confirm	M
7.17.2.5	PLME-SET-TRX-STATE.request	M
7.17.2.6	PLME-SET-TRX-STATE.confirm	M
7.17.2.7	PLME-CS.request	M
7.17.2.8	PLME-CS.confirm	M
8	Transmitter Specifications	M
8.1	Output Level Measurement	M
8.2	Transmit Spectrum Mask	M
8.3	Transmitter attenuation	M
8.4	Spurious Transmission	M
8.5	System Clock Frequency Tolerance	M
8.6	Transmitter Constellation	M
8.6.1	Transmitter Constellation Error	M
8.6.2	Transmit Modulation Accuracy Test	M
8.6.3	Error Vector Magnitude Limits	M
8.7	Transmitter Spectral Flatness	M

8.8	Crossing MV/LV Transformer	I
8.9	MV Coupler	I
8.10	AC Phase Detection	M

7.2 G3-PLC MAC LAYER

7.2.1 Conformance with ITU-T G.9903 [2]

Clause	Title and remarks/modifications	Statement
9	Data Link Layer Specifications	M
9.1	Introduction	M
9.2	Conventions	M
9.3	MAC Sublayer Specification	M
9.3.1	Channel Access	M
9.3.1.1	Overview	M
9.3.1.2	Inter-Frame (IFS) Spacing	M
9.3.1.3	CSMA-CA	M
9.3.1.4	Priority	M
9.3.1.5	ARQ	M
9.3.1.6	Segmentation and Reassembly Overview	M
9.3.2	MAC Acknowledgement	M
9.3.2.1	ACK Generation	M
9.3.2.2	NACK Generation	M
9.3.2.3	NACK Generation Avoidance	M
9.3.2.4	ACK and NACK Validity	M
9.3.2.5	Segment Retransmission	M
9.3.2.6	Subsequent Segment Collision Avoidance	M
9.3.3	MAC Sublayer Service Specification	M
9.3.3.1	Selections	M
9.3.3.2	Extensions	M
9.3.4	MAC Frame Formats	M
9.3.4.1	Selections	N
9.3.4.2	Extensions	M
9.3.5	MAC Command Frames	M
9.3.5.1	Selections	M
9.3.5.2	Extensions	M
9.3.5.2.1	MAC Command Frames Supported	M
9.3.5.2.2	Tone Map Response	E

	Payload Modulation Scheme field is set accordingly to macCoherentTransmission value: • If macCoherentTransmission is set to 0, Payload Modulation Scheme field is set to 0. • If macCoherentTransmission is set to 1, Payload Modulation Scheme field is set to 1. • If macCoherentTransmission is set to 2, the node chooses which modulation scheme is the most appropriate.	
9.3.6	MAC Constants and PIB Attributes	M
9.3.6.1	Selections	M
9.3.6.2	Extensions	S
9.3.6.2.1	Additional MAC Sublayer Constants	M
9.3.6.2.2	macBadCRCCount Statistic counter of the number of frames received with bad CRC which MAC destination address is either the address of device or the broadcast address. Additional MAC Sublayer Attributes - A new MAC attribute shall be implemented to set modulation scheme for transmission.***macCoherentTransmission*** is an integer. 0: Only differential modulation scheme shall be set in tone map response, 1: Only coherent modulation scheme shall be set in tone map response, 2: Either differential or coherent modulation scheme may be set in tone map response. By default, this attribute is set to 0.	S, E
9.3.6.2.3	MAC Sublayer Attributes and their Associated ID	M
9.3.7	MAC Functional Description	M
9.3.7.1	Selections In clauses 7.5.8.1 and 7.5.8.1.2, the Device Table is used.	S
9.3.7.2	Extensions	M
9.3.7.2.1	POS Table	M
9.3.7.2.2	Neighbour Table	M
9.3.8	MAC Security Suite Specifications	M
9.3.9	Message Sequence Chart Illustrating MAC – PHY	M
9.3.9.1	Selections	M
9.3.9.2	Extensions	M
9.3.9.2.1	PAN Start Message Sequence Chart for PAN Coordinators	M

9.3.9.2.2	Active Scan Message Sequence Chart	M
9.3.9.2.3	Data Transmission Message Sequence Chart	M
9.3.9.2.4	Channel Estimation Message Sequence Chart	M
9.3.10	MAC Annexes	M
9.3.11	Modified MAC Sublayer Data Primitives	M
9.3.11.1	MCPS-DATA.request	M
9.3.11.2	MCPS-DATA.indication	M

7.2.2 Implementation requirements

Remote firmware update (for bug corrections or specification evolution) shall be made available for data link and upper layers.

Requirements for a data concentrator / border router

- The Device Table shall allow at least 1000 entries
- The Neighbour Table shall allow at least 500 entries
- The POS Table shall allow at least 1000 entries

Requirements for a meter

- The Device Table shall allow at least 250 entries
- The Neighbour Table shall allow at least 75 entries
- The POS Table shall allow at least 250 entries

Neighbour and POS table behaviour

In case the Table is full and the node must store a new entry, the entry corresponding to the shortest valid time is removed.

7.3 G3-PLC ADAPTATION LAYER

7.3.1 Conformance with ITU-T G.9903 [2]

Clause	Title and remarks/modifications	Statement
9.4	IPv6 Adaptation Sublayer Specifications	M
9.4.1	Information Base Attributes	M
9.4.1.1	General adpMetricType is a read/write attribute	S
9.4.1.2	Routing, Broadcast and Blacklisted Neighbour Table Description	M
9.4.2	Data Frame Format, Datagram Transmission and Addressing	M

9.4.2.1	Selections from IETF RFC 4944	M
9.4.2.2	Selections from IETF RFC 6282	M
9.4.2.3	Extensions	M
9.4.2.3.1	Command Frame Header	M
9.4.2.3.2	Security Processing for Adaptation Layer Frames	M
9.4.3	Mesh Routing	M
9.4.3.1	Selections from Annex D	M
9.4.3.2	Extensions to Annex D	M
9.4.3.2.1	Unicast Packet Routing	M
9.4.3.2.2	Multicast/Broadcast	M
9.4.3.2.2.1	Packet Routing	M
9.4.3.2.2.2	Groups	M
9.4.3.2.3	Route Discovery	M
9.4.3.2.3.1	Manual Route Discovery	M
9.4.3.2.3.2	Automatic Route Discovery	M
9.4.3.2.3.3	RREQ RERR Generation Frequency Limit	M
9.4.3.2.4	Path Discovery	M
9.4.3.2.4.1	Operation	M
9.4.3.2.5	Route Repair and route Error	E
9.4.3.2.6	Link Cost Computation	M
9.4.3.2.7	Routing Packet and Message Formats	M
9.4.3.2.7.1	General Packet Format	M
9.4.3.2.7.2	Route request (RREQ) and route reply (RREP) message format	M
9.4.3.2.7.3	Route error (RERR) message format	M
9.4.3.2.7.4	Path Request (PREQ) Message Format	M
9.4.3.2.7.5	Path Reply (PREP) Message Format	M
9.4.3.2.7.6	RLCREQ Message Format	M
9.4.3.2.7.7	RLCREP Message Format	M
9.4.4	Commissioning of New Devices	M
9.4.4.1	Selections from Annex E	M
9.4.4.2	Extensions to Annex E	M
9.4.4.2.1	6LoWPAN Bootstrapping Protocol (LBP) Message Format	M
9.4.4.2.1.1	General	M

9.4.4.2.1.2	Embedded EAP Message	M
9.4.4.2.1.3	Configuration Parameters	M
9.4.4.2.2	6LoWPAN Bootstrapping Procedures	M
9.4.4.2.2.1	Overview	M
9.4.4.2.2.2	Discovering Phase	M
9.4.4.2.2.3	Access Control Phase	M
9.4.4.2.2.4	Authentication and Key Distribution Phase	M
9.4.4.2.2.5	Authorization and Initial Configuration Phase	M
9.4.4.2.2.6	Joining a PAN for any Node Except Coordinator	M
9.4.4.2.2.7	Leaving a PAN – Removal of a Device by the PAN Coordinator	M
9.4.4.2.2.8	Leaving a PAN – Removal of a Device by Itself	M
9.4.5	Sniffer Mode (optional mode)	N/A
9.4.6	Adaptation Sublayer Service Primitives	M
9.4.6.1	ADP Data Primitives	M
9.4.6.1.1	Overview	M
9.4.6.1.2	ADPD-DATA.request	M
9.4.6.1.2.1	Semantics of the service primitive	M
9.4.6.1.2.2	When generated	M
9.4.6.1.2.3	Effect on receipt	M
9.4.6.1.3	ADPD-DATA.confirm	M
9.4.6.1.3.1	Semantics of the service primitive	M
9.4.6.1.3.2	When generated	M
9.4.6.1.3.3	Effect on receipt	M
9.4.6.1.4	ADPD-DATA.indication	M
9.4.6.1.4.1	Semantics of the service primitive	M
9.4.6.1.4.2	When generated	M
9.4.6.1.4.3	Effect on receipt	M
9.4.6.2	ADP management service	M
9.4.6.2.1	Overview	M
9.4.6.2.2	ADPM-DISCOVERY.request	M
9.4.6.2.2.1	Semantics of the service primitive	M
9.4.6.2.2.2	When generated	M
9.4.6.2.2.3	Effect on receipt	M

9.4.6.2.3	ADPM-DISCOVERY.confirm	M
9.4.6.2.3.1	Semantics of the service primitive	M
9.4.6.2.3.2	When generated	M
9.4.6.2.3.3	Effect on receipt	M
9.4.6.2.4	ADPM-NETWORK-START.request	M
9.4.6.2.4.1	Semantics of the service primitive	M
9.4.6.2.4.2	When generated	M
9.4.6.2.4.3	Effect on receipt	M
9.4.6.2.5	ADPM-NETWORK-START.confirm	M
9.4.6.2.5.1	Semantics of the service primitive	M
9.4.6.2.5.2	When generated	M
9.4.6.2.5.3	Effect on receipt	M
9.4.6.2.6	ADPM-NETWORK-JOIN.request	M
9.4.6.2.6.1	Semantics of the service primitive	M
9.4.6.2.6.2	When generated	M
9.4.6.2.6.3	Effect on receipt	M
9.4.6.2.7	ADPM-NETWORK-JOIN.confirm	M
9.4.6.2.7.1	Semantics of the service primitive	M
9.4.6.2.7.2	When generated	M
9.4.6.2.7.3	Effect on receipt	M
9.4.6.2.8	ADPM-NETWORK-LEAVE.request	M
9.4.6.2.8.1	Semantics of the service primitive	M
9.4.6.2.8.2	When generated	M
9.4.6.2.8.3	Effect on receipt	M
9.4.6.2.9	ADPM-NETWORK-LEAVE.indication	M
9.4.6.2.9.1	Semantics of the service primitive	M
9.4.6.2.9.2	When generated	M
9.4.6.2.9.3	Effect on receipt	M
9.4.6.2.10	ADPM-NETWORK-LEAVE.confirm	M
9.4.6.2.10.1	Semantics of the service primitive	M
9.4.6.2.10.2	When generated	M
9.4.6.2.10.3	Effect on receipt	M
9.4.6.2.11	ADPM-RESET.request	M

9.4.6.2.11.1	Semantics of the service primitive	M
9.4.6.2.11.2	When generated	M
9.4.6.2.11.3	Effect on receipt	M
9.4.6.2.12	ADPM-RESET.confirm	M
9.4.6.2.12.1	Semantics of the service primitive	M
9.4.6.2.12.2	When generated	M
9.4.6.2.12.3	Effect on receipt	M
9.4.6.2.13	ADPM-GET.request	M
9.4.6.2.13.1	Semantics of the service primitive	M
9.4.6.2.13.2	When generated	M
9.4.6.2.13.3	Effect on receipt	M
9.4.6.2.14	ADPM-GET.confirm	M
9.4.6.2.14.1	Semantics of the service primitive	M
9.4.6.2.14.2	When generated	M
9.4.6.2.14.3	Effect on receipt	M
9.4.6.2.15	ADPM-SET.request	M
9.4.6.2.15.1	Semantics of the service primitive	M
9.4.6.2.15.2	When generated	M
9.4.6.2.15.3	Effect on receipt	M
9.4.6.2.16	ADPM-SET.confirm	M
9.4.6.2.16.1	Semantics of the service primitive	M
9.4.6.2.16.2	When generated	M
9.4.6.2.16.3	Effect on receipt	M
9.4.6.2.17	ADPM-NETWORK-STATUS.indication	M
9.4.6.2.17.1	Semantics of the service primitive	M
9.4.6.2.17.2	When generated	M
9.4.6.2.17.3	Effect on receipt	M
9.4.6.2.18	ADPM-ROUTE-DISCOVERY.request	M
9.4.6.2.18.1	Semantics of the service primitive	M
9.4.6.2.18.2	When generated	M
9.4.6.2.18.3	Effect on receipt	M
9.4.6.2.19	ADPM-ROUTE-DISCOVERY.confirm	M
9.4.6.2.19.1	Semantics of the service primitive	M

9.4.6.2.19.2	When generated	M
9.4.6.2.19.3	Effect on receipt	M
9.4.6.2.20	ADPM-PATH-DISCOVERY.request	M
9.4.6.2.20.1	Semantics of the service primitive	M
9.4.6.2.20.2	When generated	M
9.4.6.2.20.3	Effect on receipt	M
9.4.6.2.21	ADPM-PATH-DISCOVERY.confirm	M
9.4.6.2.21.1	Semantics of the service primitive	M
9.4.6.2.21.2	When generated	M
9.4.6.2.21.3	Effect on receipt	M
9.4.6.2.22	ADPM-LBP.request	M
9.4.6.2.22.1	Semantics of the service primitive	M
9.4.6.2.22.2	When generated	M
9.4.6.2.22.3	Effect on receipt	M
9.4.6.2.23	ADPM-LBP.confirm	M
9.4.6.2.23.1	Semantics of the service primitive	M
9.4.6.2.23.2	When generated	M
9.4.6.2.23.3	Effect on receipt	M
9.4.6.2.24	ADPM-LBP.indication	M
9.4.6.2.24.1	Semantics of the service primitive	M
9.4.6.2.24.2	When generated	M
9.4.6.2.24.3	Effect on receipt	M
9.4.6.2.25	ADPM-BUFFER.indication	M
9.4.6.2.25.1	Semantics of the service primitive	M
9.4.6.2.25.2	When generated	M
9.4.6.2.25.3	Effect on receipt	M
9.4.6.3	Behaviour to MAC indications	M
9.4.6.3.1	Overview	M
9.4.6.3.2	MCPS-DATA.indication	M
9.4.6.3.3	MLME-ASSOCIATE.indication	M
9.4.6.3.4	MLME-DISASSOCIATE.indication	M
9.4.6.3.5	MLME-BEACON-NOTIFY.indication	M
9.4.6.3.6	MLME-GTS.indication	M

9.4.6.3.7	MLME-ORPHAN.indication	M
9.4.6.3.8	MLME-COMM-STATUS.indication	M
9.5	Functional description	M
9.5.1	Network formation	M
10	Security	M
10.1	Access control and authentication	M
10.2	Confidentiality and integrity	M
10.3	Anti-replay and DoS prevention	M
10.4	Authentication and key distribution protocol – Selections from IETF RFC 3748	M
10.5	EAP method	M
10.5.1	Overview of EAP-PSK	M
10.5.2	Group key distribution	M
10.5.3	Configuration extension format	M
10.5.4	Peer side procedure	M
10.5.5	Server side procedure	M
Annex A	Protocol implementation conformance statement	M
A.1	Overview	M
A.2	PICS proforma tables	M
A.2.1	Functional device types (from Annex D.7.1 of [IEEE 802.15.4])	M
A.2.2	PHY functions (from Annex D.7.2.1 of [IEEE 802.15.4])	M
A.2.3	PHY packet (from Annex D.7.2.2 of [IEEE 802.15.4])	M
A.2.4	Radio frequency (from Annex D.7.2.3 of [IEEE 802.15.4])	M
A.2.5	MAC sublayer functions (from Annex D.7.3.1 of [IEEE 802.15.4])	M
A.2.6	MAC frames (from Annex D.7.3.2 of [IEEE 802.15.4])	M
Annex B	Routing Cost The same metric (adpMetricType) is intended to be used in a PAN. There is no intention to mix different metrics within a PAN.	M
B.1	Composite metric method	M
Annex C	Device Starting Sequence of messages	M
Annex D	The Lightweight On-demand Ad hoc Distance-vector Routing Protocol – Next Generation	M
D.1	Introduction	M
D.2	Terminology and Notation	M

D.2.1	Message and Message Field Notation	M
D.2.2	Variable Notation	M
D.2.3	Other Notation	M
D.2.4	Terminology	M
D.3	Applicability Statement	M
D.4	Protocol Overview and Functioning	M
D.4.1	Overview	M
D.4.2	LOADng Routers and LOADng Interfaces	M
D.4.3	Information Base Overview	M
D.4.4	Signaling Overview	M
D.5	Protocol Parameters	M
D.5.1	Protocol and Port Numbers	M
D.5.2	Router Parameters	M
D.5.3	Interface Parameters	M
D.5.4	Constants	M
D.6	Protocol Message Content	M
D.6.1	Route Request (RREQ) Messages	M
D.6.2	Route Reply (RREP) Messages	M
D.6.3	Route Reply Acknowledgement (RREP_ACK) Messages	N/R
D.6.4	Route Error (RERR) Messages	M
D.7	Information Base	M
D.7.1	Routing Set	M
D.7.2	Local Interface Set	M
D.7.3	Blacklisted Neighbour Set	M
D.7.4	Destination Address Set	M
D.7.5	Pending Acknowledgement Set	N/R
D.8	LOADng Router Sequence Numbers	M
D.9	Route Maintenance	M
D.10	Unidirectional Link Handling	M
D.10.1	Blacklist Usage	M
D.11	Common Rules for RREQ and RREP Messages	M
D.11.1	Identifying Invalid RREQ or RREP Messages	M
D.11.2	RREQ and RREP Message Processing	M

D.12	Route Requests (RREQs)	M
D.12.1	RREQ Generation	M
D.12.2	RREQ Processing	M
D.12.3	RREQ Forwarding	M
D.12.4	RREQ Transmission	M
D.13	Route Replies (RREPs)	M
D.13.1	RREP Generation	M
D.13.2	RREP Processing	M
D.13.3	RREP Forwarding	M
D.13.4	RREP Transmission	M
D.14	Route Errors (RERRs)	M
D.14.1	Identifying Invalid RERR Messages	M
D.14.2	RERR Generation	M
D.14.3	RERR Processing	M
D.14.4	RERR Forwarding	M
D.14.5	RERR Transmission	M
D.15	Route Reply Acknowledgements (RREP_ACKs)	N/R
D.15.1	Identifying Invalid RREP_ACK Messages	N/R
D.15.2	RREP_ACK Generation	N/R
D.15.3	RREP_ACK Processing	N/R
D.15.4	RREP_ACK Forwarding	N/R
D.15.5	RREP_ACK Transmission	N/R
D.16	Metrics	M
D.16.1	Specifying New Metrics	M
D.17	Security Considerations	M
D.17.1	Confidentiality	M
D.17.2	Integrity	M
D.17.3	Channel Jamming and State Explosion	M
D.17.4	Interaction with External Routing Domains	M
Annex E	Commissioning in 6LoWPAN	M
E.1	Introduction	M
E.2	Terminology	M
E.2.1	Requirement Notation	M

E.3	Bootstrapping	M
E.3.1	Resetting the device	M
E.3.2	Scanning through channels	M
E.3.3	LoWPAN Bootstrapping Mechanism	M
E.3.3.1	LoWPAN Bootstrapping Protocol message format	M
E.3.3.1.1	LBP message	M
E.3.3.2	LoWPAN Bootstrapping Information Base	M
E.3.3.3	LBA discovering phase	M
E.3.3.4	LoWPAN Bootstrapping Protocol (LBP)	M
E.3.3.5	LBP in secured 6LoWPAN	M
E.3.3.6	Role of Entities in LBP	M
E.3.4	Assigning the short address	M
E.3.5	Obtaining IPv6 address - RA_WAIT_TIME corresponds to RSRetryWaitTime	M
E.3.6	Configuration Parameters	M
E.4	IANA Considerations	I
E.5	Security Considerations	M
Annex F	Regional requirements for Japan	N/R
F.1	Overview	N/R
F.2	Physical layer specifications for ARIB bandplan	N/R
F.2.1	System fundamental parameters for ARIB bandplan	N/R
F.3	Data link layer specifications	N/R
F.3.1	TM (Tone Map)	N/R
F.3.2	CIFS	N/R
F.3.3	LBP Joining Procedure	N/R
Annex G	Regional requirements for the USA	N/R
Appendix I	Examples on encoding and decoding	I
I.1	Example for data encoding	I
I.2	Example for data decoding	I
Appendix II	Test Vectors for cryptographic building blocks	I
II.1	Introduction	I
II.1.1	Short Frame Ciphering	I
II.1.2	Long Frame Ciphering	I

	Bibliography	I

7.3.2 Implementation requirements

Requirements for a data concentrator / border router

- The Routing Table shall allow at least 1200 entries
- The Broadcast Log Table shall allow at least 64 entries
- The Blacklisted Neighbour Table shall allow at least 64 entries
- The Group Table shall allow at least 16 entries
- The Context Information Table shall allow 16 entries

Requirements for a meter

- The Routing Table shall allow at least 150 entries
- The Broadcast Log Table shall allow at least 32 entries
- The Blacklisted Neighbour Table shall allow at least 32 entries
- The Group Table shall allow at least 16 entries
- The Context Information Table shall allow 16 entries
- The Prefix Table shall allow at least 4 entries

Routing, Broadcast Log and Blacklisted Neighbour table behaviour

In case the Table is full and the node must store a new entry, the entry corresponding to the shortest valid time is removed.

8. IPV6 AND 6LOWPAN CONSIDERATIONS

For security purposes, regarding IPv6 layer, features reported in this section - and only them - shall be implemented.

This section describes how IPv6 is supported over the G3-PLC physical and data link layers. If the IPv6 protocol has to be implemented in conformance with RFC 2460 [7] and the appropriate updates to the protocol, the following clause defines the IPv6 addressing plan meeting architectural considerations guaranteeing overall scalability and enabling IP end-to-end communications (direct IP communication between the information system and the meters). Additional clauses specify IPv6 address provisioning, routing and ICMP features.

8.1 INBOUND COMMUNICATIONS

8.1.1 Unicast IPv6 Addresses

Link-local type addresses, consisting in the static prefix FE80::/64 and an interface identifier as defined in RFC 4291 [8], are not routable addresses:

Link-local type IPV6 address structure:	
64 bits	64 bits
Static prefix: FE80::/64	Interface ID

These IPv6 addresses are only valid within one IP hop, or in other words, within the G3-PLC PAN.

On the other hand ULA addresses, defined in RFC 4193 [9] as follows, have an extended scope:

ULA type IPV6 address structure:				
7 bits	1 bit	40 bits	16 bits	64 bits
Static prefix: FC/7	L: 1	Global ID	Subnet ID	Interface ID

These addresses are valid outside the G3-PLC PAN and can be routed on a larger domain defined by the end-user. Thus, the use of ULA addresses allows the information system to directly reach a G3-PLC communication node (meter) with its IPv6 ULA address.

ULA type addresses shall be used for end-to-end communication between external IP hosts and devices belonging to the PAN in addition to the **link-local addresses, which use is restricted to local communication between devices belonging to the PAN**.

8.1.2 Multicast IPv6 Addresses

IPv6 multicast addresses are also supported and shall follow the structure defined in RFC 4291 [8]:

IPV6 multicast address structure:			
8 bits	4 bit	4 bits	112 bits
Static prefix: FF/8	Flag	Scope	Group ID

The “scope” field follows IANA recommendations. It is set to 2 for link-local scope, to 5 for site-local scope and to 8 for organization-local scope.

Consequently, the link-local scope IPv6 multicast address used by default in the G3-PLC metering profile equals **0xFF02::0001** (group 0x80**01** is carried in the mesh header).

Moreover, a G3-PLC device may subscribe to additional multicast addresses by a management entity (DLMS/COSEM client, firmware…) subsequently. Practically, the management entity updates the adaptation layer group table attribute and advertises context information if needed (see 8.4). The group table may contain up to 16 addresses.

Note: while the most efficient compression scheme is reached with groups 0x8000 to 0x80FF for a link-local scope (possible IPv6 addresses match 0xFF02::00XX), the groups 0x8100 to 0x9FFF require a different and less efficient compression scheme independently from the desired scope (possible IPv6 addresses match 0xFFXX::00XX:XXXX in the best case). See 8.4 and RFC 6282 [11] for more details.

For each meter, the COSEM configuration object “IPv6Setup” is listing the valid multicast addresses in attribute 5: “multicast_IPv6_addresses” which is reflecting the possible combinations derived from the group table entries and, eventually, relevant context information.

8.2 ENABLING OUTBOUND COMMUNICATIONS

The ULA address, which allows IP communication with external entities, is built from its static prefix 0xFC/7, the local bit, the Global ID and the Subnet ID fields (see 8.1.1).

Global ID and Subnet ID fields are stored in each data concentrator. The ULA prefixes of the data concentrator / border router and the associated meters are derived from these fields.

Fig. 3 shows a ULA-addressed network allowing IP end-to-end communication:

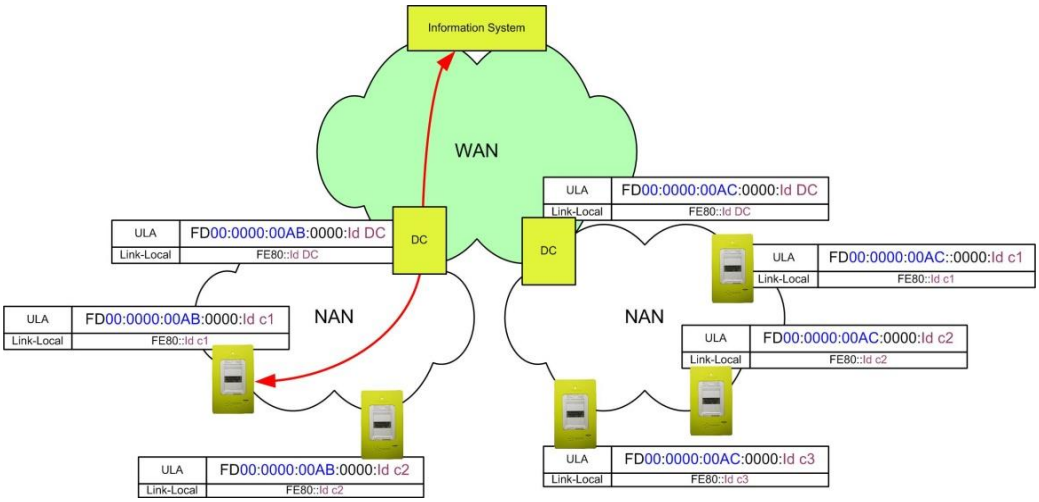

Fig. 3: A ULA-addressed network

For each meter, both LLA and ULA addresses are stored in attribute 4: “IPv6_addresses” of the COSEM configuration object “*IPv6Setup*”.

According to Enedis’ current AMI requirements, each G3-PLC device has two IPv6 interfaces, resulting in the provisioning of one link-local address and one ULA address (the IPv6 address composed with the modem’s interface identifier and the PAN’s ULA prefix). These addresses are strictly configured using IP layer mechanisms, and if the device is a meter, the corresponding COSEM object is updated.

8.2.1 Border Router Features

The data concentrator, when configured as a border router, allows G3-PLC packets to be routed to an external entity (external to the G3-PLC network) and vice versa.

For the meters, 2 modes are defined:

- Autoconfiguration: the meter is not able to generate packets to external hosts and is not proactively learning its ULA prefix.
- Neighbour Discovery Protocol (NDP): the meter is able to generate packets to hosts outside the PAN and is proactively learning its ULA prefix.

	Meter / 6LN		Data Concentrator / Border Router / 6LBR	
	Capability in Autoconfiguration mode	Capability in NDP mode	Capability when Border Router is disabled	Capability when Border Router is enabled
Store/Update its own ULA prefix	Yes	Yes	Yes	Yes
Store/Update entries of its Context Table	Yes	Yes	Yes	Yes
Send a RS if no PIO/6CO is sent following the bootstrapping	No	Yes	N/R	N/R
Forward a router solicitation/ advertisement	Yes	Yes	N/R	N/R
Forward a packet from/to external entities	Yes	Yes	No	Yes
Generate a packet with a ULA as source address.	No	Yes	No	Yes
Generate a packet with a ULA as destination address.	No	Yes	No	Yes
Receive a packet with a destination address matching the device's ULA (if known).	No The LOADng router will reject any packet with its own ULA as destination address	Yes	No The LOADng router will reject any packet with its own ULA as destination address	Yes

8.2.2 Border Router Activation Procedure

Given the initial conditions below:

- the Border Router is disabled;

- Global ID and Subnet ID fields are empty;
- meters are set to Autoconfiguration mode.

For the meters that may be accidentally configured in NDP mode, the RA messages sent by the data concentrator upon solicitation (i.e. upon receipt of RS messages) are empty.
The procedure to initiate outbound communications follows:

- Global ID, Subnet ID and possibly context information are sent to the data concentrator by the information system. Starting from this, the border router periodically advertises prefix and context information within the PAN using multicast RA packets carrying appropriate PIO and 6CO options as specified in 8.5.4.
- All the meters (being configured either in NDP or Autoconfiguration mode) build their own ULA IPv6 addresses according to the Global ID and Subnet ID carried in the PIO option received as specified in 8.3.
- After a given time, the information system configures the data concentrator as border router. The data concentrator then configures its own ULA IPv6 address and accepts packets carrying its own address as destination address.

8.3 IPV6 ADDRESS PROVISIONING

In order to meet the architectural requirements outlined previously, two major steps lead to G3-PLC device IPv6 address provisioning: the G3-PLC PAN joining procedure and the ULA IPv6 address assignment.

8.3.1 G3-PLC PAN Joining Procedure

When a new device joins a G3-PLC PAN, the procedure specified in ITU-T G.9903 [2] is applied as stated in section 7.3.1 (LoWPAN Bootstrapping Protocol). This commissioning procedure is resulting in the secure delivery of an IPv6 link-local address composed of the link-local prefix (FE80::/10) and a 64-bit interface identifier derived from the 16-bit PAN ID and the 16-bit short address allocated by the coordinator (Stateless Address Autoconfiguration).

The interface identifier matches the following format: **0xYYYY:00FF:FE00:XXXX**, where YYYY is the 16-bit PAN ID (chosen as described in clause 9.4.2.1 of ITU-T G.9903 [2]), and XXXX the 16-bit short address.

The short addresses shall be provisioned as described in the following table:

Device type	Valid range
Coordinator (data concentrator)	0x0000
PAN device (meter)	0x0001 – 0x7FFF
Multicast addresses	0x8000 – 0x9FFF
Reserved addresses	0xA000 – 0xFFFE
Broadcast addresses	0xFFFF

8.3.2 ULA IPv6 Address Assignment

Once the device successfully joined the network a second phase consists in the assignment of an IPv6 ULA address to the device, composed of a prefix meeting the requirements of section 8.1.1 and a 64-

bit interface identifier corresponding to the interface identifier of the previously provisioned IPv6 link-local address.

The prefix is deduced from the received RA carrying the ULA prefix to be used within the NAN managed by the PAN coordinator as specified in 8.5.4.

8.4 IPV6 ADDRESS COMPRESSION FEATURES

As described in clause 7.3.1, IPv6 header compression specified in RFC 6282 [11] shall be supported for both link-local and ULA addresses.

8.4.1 CID Extension Field

If the compression of link-local addresses does not require any further data to be transmitted in addition to the 16-bit short address, the optimal compression of ULA addresses which allow IP communication with external entities (outside the considered G3-PLC PAN) is done through the prior transmission of context information.

When the CID field of the 6LoWPAN PDU is set (CID = 1), an additional 8-bit context identifier extension field composed of two nibbles (4-bit SCI and DCI fields) is carried in line as specified in RFC 6282 [11].

Both nibbles SCI (Source Context Identifier) and DCI (Destination Context Identifier) specify the prefixes of both source and destination addresses carried by the 6LoWPAN PDU.

8.5 PREFIX AND CONTEXT ADVERTISEMENT

8.5.1 IPv6 Neighbour Discovery over G3-PLC

The Neighbour Discovery protocol for IPv6 (RFC 4861 [13]) was developed for IPv6 nodes to discover each other's presence and to determine link-local network parameters enabling outbound communication. RFC 4861 [13] defines the IPv6 nodes' behavior and signalling to achieve the following basic operations:

- Router and prefix discovery
- Address resolution and neighbour unreachability detection
- Redirect function

In addition, RFC 6775 [12] specifies how IPv6 Neighbour Discovery is optimized and extended for constrained 6LoWPAN networks. It introduces:

- Multihop prefix and context distribution
- Multihop duplicate address detection
- Address Registration

Application of IPv6 Neighbour Discovery to G3-PLC networks is limited to router and prefix context discovery and distribution.

Due to the centralized assignment of IEEE 802.15.4 [5] short addresses as specified in ITU-T G.9903 [2] (LoWPAN Bootstrapping Protocol), duplicate address detection is not relevant. In addition, address registration is not required at IP level since G3-PLC provides periodically updated neighbour tables.

IPv6 Neighbour Discovery over G3-PLC networks is limited to the use of Router Advertisements and Router Solicitations carrying the following options:

- Prefix Information Option (PIO)
- Context Information Option (6CO)

According to RFC 6775 [12], the two abovementioned options shall be carried in solicited and unsolicited Router Advertisement messages to allow G3-PLC nodes to be aware of the prefix(es) and contexts used within the G3-PLC PAN.

Note: In this G3-PLC metering profile (mesh-under topology), the PAN-specific information is only advertised by the 6LBR (i.e. the PAN coordinator). Since all G3-PLC nodes are located one IP hop away from the 6LBR, the ABRO option is not needed and must not be included in the Router Advertisements.

Note: see 8.5.5 for details describing which parts of RFC 6775 [12] are required for an implementation following the guidelines given in this document.

8.5.2 Prefix Information Option (PIO)

According to RFC 6775, valid prefix(es) have to be advertised for the nodes to configure their ULA address(es). This information is carried by a Router Advertisement message in a “Prefix Information Option” as defined in RFC 4861 [13]:

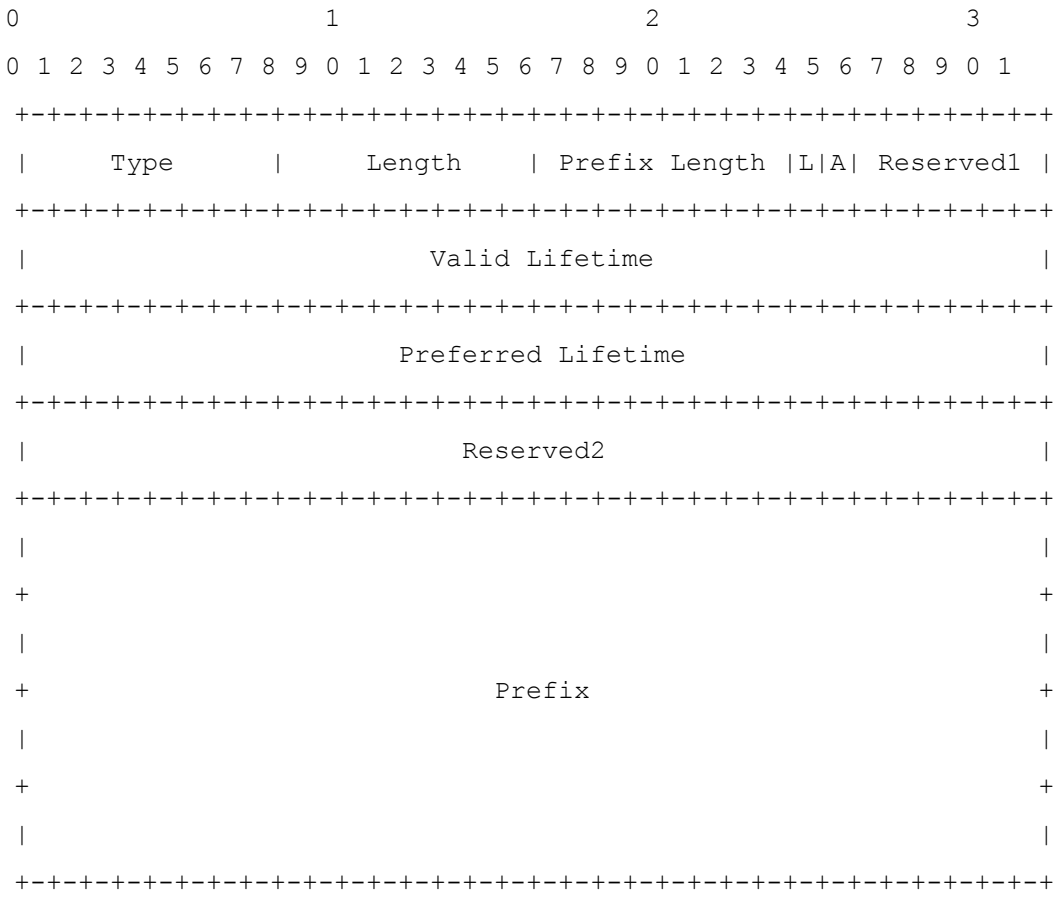

Fig. 4: Prefix Information Option

The values of the fields transmitted within a PIO option are recalled in the following table:

Field	Length	Default value	Description
Type	8 bits	3	As stated in the IANA Considerations clause of RFC 4861, the type value 3 is used for the PIO option.
Length	8 bits	4	Length in units of 8 bytes

Prefix Length	8 bits	Variable	Number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.
L	1 bits	Variable	1-bit on-link flag
A	1 bit	Variable	1-bit autonomous address-configuration flag
Reserved1	6 bits	0	The field is unused
Valid Lifetime	32 bits	Variable	Length of time in seconds during which the prefix is valid for the purpose of on-link determination
Preferred Lifetime	32 bits	Variable	Length of time in seconds during which addresses generated from the prefix via remain preferred
Reserved2	32 bits	0	The field is unused
Prefix	Prefix Length	Variable	IPv6 address or a prefix of an IPv6 address

8.5.3 6LoWPAN Context Option (6CO)

Context information has to be advertised prior to using any ULA address-based communication scheme. It is carried in “6LoWPAN Context Option” (6CO) fields as specified in RFC 6775 [12]:

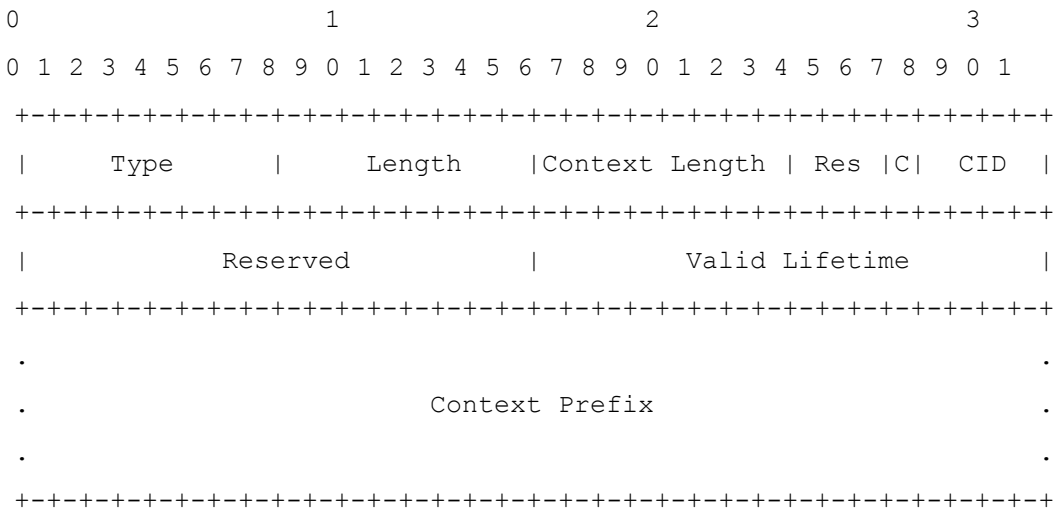

Fig. 5: 6LoWPAN Context Option

The values of the fields transmitted within a 6CO message are defined in the following table:

Field	Length	Default value	Description
Type	8 bits	34	As stated in the IANA Considerations clause of RFC 6775 [12], the type value 34 is used for 6CO advertisements.
Length	8 bits	2	Length in units of 8 bytes
Context Length	8 bits	Variable	Up to 128-bit contexts may be carried (IPv6 ULA prefixes are 64-bit context, multicast contexts length are variable).
Res	3 bits	0b000	Reserved for future use
C	1 bit	Variable	Indicates the validity of the CID for compression purposes. The recommendations stated in clause 7.2 of RFC 6775 [12] shall be followed (see 8.5.4).
CID	4 bits	See 8.4.1	This CID field corresponds to the 4-bit context information used for source and destination addresses (SCI, DCI).
Reserved	16 bits	0x0000	Reserved for future use
Valid Lifetime	16 bits	Variable	This field corresponds to the lifetime of the sent context. Upon reception of a new 6CO advertisement for an existing context identified by its CID, its associated time to live is updated with the specified Valid Lifetime.
Context Prefix	Context Length	Variable	Context information (64 bit ULA prefixes, multicast information for stateful context based compression as defined in RFC 6282 [11]…). Upon reception of a new 6CO advertisement for an existing context identified by its CID, context information shall be overwritten if different.

8.5.4 Prefix and Context Information Distribution

Practically, the relevant context information is initially advertised to communication nodes just after a successful joining procedure:

- After a communication node successfully performs the LBP procedure, the PAN coordinator shall generate a Router Advertisement (RA) ICMP packet that carries one or more PIO and 6CO (up to 16) options as specified in RFC 6775 [12]. If no RA packet is received within **RSRetryWaitTime**, a Router Solicitation (RS) packet (see RFC 4861 [13]) shall be transmitted to the PAN coordinator every RSRetryWaitTime seconds until reception of the expected RA packet. Up to **RSMaxRetry** RS packets may be transmitted.

Within an already established PAN, prefix and context information distribution is triggered by the higher layers:

- The 6LBR (PAN coordinator) shall send periodic multicast RA packets carrying the complete set of context information available for the PAN (one or more PIO and 6CO options). The duration of the period is set by the **RASendPeriod** parameter which must be chosen taking into account the advertised information valid lifetime(s). If long term validity is desired for a given piece of PAN-specific information, this parameter shall be chosen much smaller than its valid lifetime.
- The PAN coordinator shall send a multicast RA packet every time the prefix and/or the context information to be distributed within the PAN is updated.

Note: if for any reason, context information has not been provided to the 6LBR, periodic RA packet transmission is not performed and the 6LBR shall only respond to RS packets with unicast RA packets carrying no option.

In addition, as stated in clause 7.2 of RFC 6775 [12], the following recommendations shall be followed, regardless of the distribution mechanism used (RS triggered, higher layers triggered):

- When a piece of context information (one 6CO field) is advertised for the first time, the “C” field of the related 6LoWPAN Context Option shall be set to 0, such as the context is not initially used for compression (devices can only use it for decompression purposes).

  After a waiting time (given by the parameter **RAContextActivationWaitTime**) corresponding to the estimated time needed for all devices of a PAN to update their context information tables, the “C” field is set to 1, such as the use of the aforementioned piece of context information is now allowed.
- After a piece of context information is not valid anymore within a PAN, the 6LBR shall continue advertising it for an additional duration (given by the parameter **RAContextDesactivationWaitTime**), such as the “C” field of the 6LoWPAN Context Option is set to 0. The context is not used for compression anymore (devices can only use it for decompression purposes).

8.5.5 Selections from RFC 6775

Clause	Title and remarks/modifications	Statement
1	Introduction	I
1.1	The Shortcomings of IPv6 Neighbor Discovery	I
1.2	Applicability	I
1.3	Goals and Assumptions	I
1.4	Substitutable Features	I
2	Terminology	M

	- regular G3-PLC nodes are considered as 6LoWPAN Nodes (6LN) and the PAN coordinator is considered as the 6LoWPAN Border Router (6LBR).	
3	Protocol Overview	I
3.1	Extensions to RFC 4861	I
3.2	Address Assignment - Address assignment is performed as described in ITU-T G.9903 [2].	N/R
3.3	Host-to-Router Interaction - Address registration, neighbor unreachability detection and neighbor cache entries are not supported.	S
3.4	Router-to-Router Interaction - Duplicate address detection and neighbor cache entries are not supported.	S
3.5	Neighbor Cache Management - G3-PLC manages neighbor-specific information in a Neighbor Table at MAC level.	N/R
4	New Neighbor Discovery Options and Messages	M
4.1	Address Registration Option	N/R
4.2	6LoWPAN Context Option	M
4.3	Authoritative Border Router Option	N/R
4.4	Duplicate Address Messages	N/R
5	Host Behavior - The host behavior is modified as specified in 8.5.1 and 8.5.4.	S
5.1	Forbidden Actions	M
5.2	Interface Initialization - Host interface initialization preceding the transmission of the first RS message is fully described in ITU-T G.9903 [2].	S
5.3	Sending a Router Solicitation - The SLLAO is not needed since the RA message will be sent in unicast using IPv6 destination address field with the soliciting node's link-local IPv6 address. - MAX_RTR_SOLICITATIONS corresponds to the attribute **RSMaxRetry** specified in 8.10 (default value = 3). - RTR_SOLICITATIONS_INTERVAL corresponds to the attribute **RSRetryWaitTime** specified in 8.10 (default value = 10s).	S
5.4	Processing a Router Advertisement	M
5.4.1	Address Configuration	M
5.4.2	Storing Contexts	M
5.4.3	Maintaining Prefix and Context Information	M
5.5	Registration and Neighbor Unreachability Detection - Address registration, neighbor unreachability detection and neighbor cache entries are not supported.	N/R
5.5.1	Sending a Neighbor Solicitation	N/R
5.5.2	Processing a Neighbor Advertisement	N/R

5.5.3	Recovering from Failures	N/R
5.6	Next-Hop Determination	N/R
5.7	Address Resolution	N/R
5.8	Sleeping	N/R
5.8.1	Picking an Appropriate Registration Lifetime	N/R
5.8.2	Behavior on Wakeup	N/R
6	Router Behavior for 6LRs and 6LBRs - The router behavior is modified as specified in 8.5.1 and 8.5.4.	S
6.1	Forbidden Actions	M
6.2	Interface Initialization - The recommendations specified for clause 5.2 of RFC 6775 apply during the non-router configuration phase.	S
6.3	Processing a Router Solicitation - The SLLAO is not needed since the RA message will be sent in unicast using IPv6 destination address field with the soliciting node's link-local IPv6 address.	S
6.4	Periodic Router Advertisements - In case periodic multicast RAs are sent, **RASendPeriod** specified in 8.5.4 determines the advertisement period.	S
6.5	Processing a Neighbor Solicitation	N/R
6.5.1	Checking for Duplicates	N/R
6.5.2	Returning Address Registration Errors	N/R
6.5.3	Updating the Neighbor Cache	N/R
6.5.4	Next-Hop Determination	N/R
6.5.5	Address Resolution between Routers	N/R
7	Border Router Behavior - The border router behavior is modified as specified in 8.5.1 and 8.5.4.	S
7.1	Prefix Determination	M
7.2	Context Configuration and Management - See extensions specified in 8.5.4.	S
8	Substitutable Feature Behavior	M
8.1	Multihop Prefix and Context Distribution	M
8.1.1	6LBRs Sending Router Advertisements	M
8.1.2	Routers Sending Router Solicitations	M
8.1.3	Routers Processing Router Advertisements	M
8.1.4	Storing the Information	M
8.1.5	Sending Router Advertisement	M
8.2	Multihop Duplicate Address Detection	N/R
8.2.1	Message Validation for DAR and DAC	N/R
8.2.2	Conceptual Data Structures	N/R
8.2.3	6LR Sending a Duplicate Address Request	N/R

8.2.4	6LBR Receiving a Duplicate Address Request	N/R
8.2.5	Processing a Duplicate Address Confirmation	N/R
8.2.6	Recovering from Failures	N/R
9	Protocol Constants	I
10	Examples	I
10.1	Message Examples	I
10.2	Host Bootstrapping Example	N/R
10.2.1	Host Bootstrapping Messages	N/R
10.3	Router Interaction Example	N/R
10.3.1	Bootstrapping a Router	N/R
10.3.2	Updating the Neighbor Cache	N/R
11	Security Considerations	I
12	IANA Considerations	M
13	Interaction with Other Neighbor Discovery Extensions	N/R
14	Guidelines for New Features	N/R
15	Acknowledgements	N/R
16	References	M
16.1	Normative References	M
16.2	Informative References	I

8.6 ROUTING FEATURES

The default LOADng routing algorithm, specified in Annex D of ITU-T G.9903 [2] (based on draft-clausen-lln-loadng-10 [14]), operates at the data link layer as a mesh-under routing protocol.

However, the metering profile described in this document specifies how IPv6 ULA addresses are used to allow IP end-to-end communications. At first, following RFC2460, a node must be able to accept a fragmented packet that, after reassembly, is as large as 1500 octets. Secondly, devices having joined a given G3-PLC PAN can interact with other IP hosts located outside of this PAN. From a data link perspective, it means that frames carrying IP packets sent from an external originator or sent to an external destination shall be routed towards the appropriate destination within the PAN.

Practically, the IP headers of these packets are compressed as defined in 8.4, resulting in 6LoWPAN frames carrying specific context information within the context identifier extension field. On the other hand, LOADng uses only 6LoWPAN 16-bit short addresses. Thus, the following rules shall be observed:

- If both originator and destination belong to the same PAN (**local communication**).

  If the route is not already installed in its routing table, the originator initiates a route discovery procedure by generating an RREQ message such as:

  <originator> = 6LoWPAN 16-bit short address of the originator

  <destination> = 6LoWPAN 16-bit short address of the destination

- If the originator does not belong to the G3-PLC PAN (**the originator is an external entity**). Upon reception of the originator's packet, the border router shall send it to the destination.

If the route is not already installed in its routing table, the border router initiates a route discovery procedure by generating an RREQ message such as:

<originator> = 6LoWPAN 16-bit short address of the border router

<destination> = 6LoWPAN 16-bit short address of the destination

- If the destination does not belong to the G3-PLC PAN (**the destination is an external entity**). The originator shall send its packet to the border router, which will send it towards the destination.

  If the route is not already installed in its routing table, the originator initiates a route discovery procedure by generating an RREQ message such as:

  <originator> = 6LoWPAN 16-bit short address of the originator

  <destination> = 6LoWPAN 16-bit short address of the border router

Note: if the destination address is not part of the PAN, a LOADng router shall not try to find the matching 16-bit short address in its routing table. The data packet shall be forwarded to the MAC address matching the route towards the border router.

Note 2: the destination address set offered by the G3-PLC specification is unused for the Linky AMI.

8.7 INTERACTIONS WITH EXTERNAL HOSTS

As defined in 8.3, the interface identifier of a G3-PLC device is derived from its 6LoWPAN 16-bit short address that has been allocated by the coordinator such as it is unique within the PAN. Nevertheless, in an IP end-to-end communication scheme, external IPv6 hosts may not have an adequate interface identifier.

To ensure efficient compression and correct delivery of IP datagrams using G3-PLC, external entities' IPv6 addresses shall be constructed with the prefix related to the appropriate context identifier extension and an interface identifier conformant with the following format:

- **0xYYYY:00FF:FE00:XXXX**, where YYYY always equals 0x0000 and XXXX is chosen within the range 0x0000 – 0xFFFF among the reserved short address range defined in 8.3.

This will allow the border router[1] to compress external IPv6 addresses in the exact same way it is done for devices that belong to the G3-PLC PAN.

Note: this clause is informational and is only intended to give a system overview on this aspect without having a direct impact on the G3-PLC communication stack implementation.

8.8 ICMPV6 REQUIREMENTS

As defined in the IPv6 specification (see RFC 2460 [7] chapter 1), the implementation of ICMPv6 as defined in RFC 4443 [18] is mandatory for all G3-PLC devices. ICMPv6 is used as a building block to support distribution of prefix and context information (see §8.4.4) and ping functionality.

The following table summarizes how the statements of RFC 4443 [18] apply:

Clause	Title and remarks/modifications	Statement
1	Introduction	I

[1] A border router is a device that establishes connectivity between the G3-PLC PAN and another network (possibly another G3-PLC PAN). In an IP end-to-end communication scheme between the information system and a meter, the data concentrator may be the border router.

2	ICMPv6 (ICMP for IPv6)	M
2.1	Message General Format	M
2.2	Message Source Address Determination	M
2.3	Message Checksum Calculation	M
2.4	Message Processing Rules	M
3	ICMPv6 Error Messages	M
3.1	Destination Unreachable Message	M
3.2	Packet Too Big Message	M
3.3	Time Exceeded Message	M
3.4	Parameter Problem Message	M
4	ICMPv6 Informational Messages	M
4.1	Echo Request Message	M
4.2	Echo Reply Message An Echo Reply should be sent in response to an Echo Request message sent to an IPv6 unicast address and not to a multicast address.	S
5	Security Considerations	I
5.1	Authentication and Confidentiality of ICMP Messages *Note: the G3-PLC MAC layer security features provide the protection needed for the ICMPv6 messages transmitted over the PAN*	I
5.2	ICMP Attacks	I
6	IANA Considerations	M
6.1	Procedure for New ICMPV6 Type and Code Value Assignment	I
6.2	Assignments for This Document	M
7	References	M
7.1	Normative References	M
7.2	Informative References	I
8	Acknowledgements	N/R
Appendix A	Changes since RFC 2463	N/R

8.9 SECURITY CONSIDERATIONS

8.9.1 Neighbour Discovery Fragmentation

Following RFC 6980, to avoid NDP-based attacks, Neighbour Discovery messages (Router Solicitation and Router Advertisement) must not use fragmentation. Fragmented Neighbour Discovery messages received by nodes must then be discarded silently.

The following table summarizes how the statements of RFC 6980 [20] apply:

Clause	Title and remarks/modifications	Statement
1	Introduction	I
2	Traditional Neighbour Discovery and IPv6 Fragmentation	I
3	Secure Neighbor Discovery (SEND) and IPv6 Fragmentation	N/R
4	Rationale for Forbidding IPv6 Fragmentation in Neighbour Discovery	I
5	Specification	N
6	Operational Advice	N/R
7	Security Considerations	N/R
8	Acknowledgements	I
9	References	I
Appendix A	Message Size When Carrying Certificates	N/R

8.9.2 Oversized IPv6 Header

Following RFC 7112[21], a node that receives a first IPv6 fragment that does not contain the entire Header Chain of the IPv6 packet must be discarded silently.

The following table summarizes how the statements of RFC 7112 [21] apply:

Clause	Title and remarks/modifications	Statement
1	Introduction	I
2	Requirements Language	I
3	Terminology	I
4	Motivation	I
5	Updates to RFC 2460 ICMPv6 error message is not sent : A host that receives a first fragment that does not satisfy the above-stated requirement should discard the packet and DOES NOT send an ICMPv6 error message to the source address of the offending packet.	S
6	IANA Considerations	N/R
7	Security Considerations	I
8	Acknowledgments	I
9	References	I

8.10 LIST OF THE NEW PARAMETERS DEFINED IN THIS CHAPTER

The following table provides a precise description of the complete set of parameters defined in this chapter:

Parameter	PAN Coord.	PAN Device	Length	Range	Description	Default value
RSMaxRetry	No	Yes	8 bits	0 – 255	Maximum number of RS retries	3
RSRetryWaitTime	No	Yes	16 bits	1000 – 65535	Waiting time between two RS retries (in milliseconds)	10000
RASendPeriod	Yes	No	16 bits	0 – 65535	RA transmission period (in minutes)	1440
RAContext ActivationTime	Yes	No	16 bits	0 – 65535	Waiting time in minutes for an advertised context to be activated for compression purposes	Context specific
RAContext DesactivationTime	Yes	No	16 bits	0 – 65535	Duration in minutes for a context to be advertised only for decompression purposes before being not advertised anymore	Context specific

9. UDP TRANSPORT LAYER SETTINGS

This section focuses on the use of the UDP protocol [6] within the G3-PLC metering profile.

9.1 UDP PORT NUMBERING

“COSEM Client Application Layer” must be in the range between 1024 and 65535 and UDP port shall be chosen between 61617 and 61631 to benefit from the best compression of 6LoWPAN adaptation layer.

9.2 UDP HEADER COMPRESSION

UDP header compression shall be conformant with RFC 6282 [11].

10.QUALITY OF SERVICE

In order to handle different QoS levels for different services, priority level mapping has to be ensured at all levels.

At the DLMS/COSEM application level, the applicable services are tagged with a Priority parameter, which allows two levels of priority: FALSE (normal priority) and TRUE (high priority).

Quality of service shall however be supported for experimental purposes.

ICMP Echo will be sent with normal priority.

G3-PLC messages (routing, bootstrapping, RA,,...) shall be sent with normal priority.

At the IPv6 network level, priority tagging shall be enforced using the traffic class field. For instance, the 3 most significant bits of the 6-bit DSCP (Differentiated Services Code Point – see RFC 2474 [17]) part of the 8-bit traffic class field shall be used. Consequently, the traffic class field may take a value among 0x00 (normal priority) and 0x20 (high priority). A DLMS/COSEM service tagged with Priority set to FALSE corresponds to a 0x00 traffic class. When Priority is set to TRUE, a 0x20 traffic class is used.

At the 6LoWPAN adaptation layer, the traffic class is directly mapped into the ADPD-DATA.request QualityOfService parameter.

Finally, at the G3-PLC MAC layer, the ADPD-DATA.request triggers the generation of a MCPS-DATA.request with the QualityOfService parameter set to the carried value. The quality of service is then carried as Channel Access Priority (CAP field) in the Segment Control (MAC Header) and propagated by this mean.

The following table indicates the required QoS mapping:

Priority level	DLMS/COSEM	IP	ADP layer	MAC layer
	Priority Parameter	Traffic Class	QualityofService	QualityofService
Normal priority	FALSE	0x00	0x00	0x00
High priority	TRUE	0x20	0x01	0x01

When receiving a packet from the data concentrator with a high priority at MAC layer, the nodes shall propagate the QoS associated to this request all along the route up to the final destination. If a response is sent back, the answer shall set its priority to the same level.

In addition, each 6loWPAN PDU shall be routed within a 100 ms timeframe starting from end of ACK received frame and ending at the beginning of the relayed frame transmission (over an idle media).

11. DATA LINK LAYER SECURITY

Data link security is specified in clause 10 of ITU-T G.9903 [2].

11.1 ANTI-REPLAY MECHANISM

As defined in 0, an anti-replay mechanism based on the Device Table defined in IEEE 802.15.4 [5] is supported (see clauses 9.3.8 of ITU-T G.9903 [2] for details).

11.2 FRAME COUNTER HANDLING

The MAC layer frame counter must not be reset upon reception of a new GMK key (during the bootstrapping procedure). A reset of the frame counter may create communication issues if a device bootstraps alternately on two PLC network (due to crosstalk for example).

11.3 EAP-PSK CRYPTOGRAPHIC OPERATIONS

It is important to note that the LoWPAN Bootstrapping Protocol encapsulating the EAP message modifies the first byte of the EAP content.

As a result, all EAP-PSK cryptographic operations (in particular the Protected Channel ciphering) must be done on the EAP message before encapsulation in a LBP message. If this constraint is not taken into account, the EAP-PSK computation will be erroneous and the transport of the EAP message over another protocol (UDP, RADIUS…) will be impossible.

11.4 KEY MANAGEMENT OVERVIEW

The PAN coordinator manages the PAN's GMK key and provides it to the devices during bootstrapping. The GMK key remains the same after a PAN coordinator reboot.

The PAN coordinator also acts as an EAP authentication server to the devices. In order to perform the EAP-PSK bootstrapping exchanges with the devices, the PAN coordinator downloads the device's PSK key from the information system.

11.5 RE-KEYING OPERATION

To perform a GMK key change, the following operations are performed by the PAN coordinator:

- The PAN coordinator generates a new GMK key and chooses an identifier (KeyId-new), which is different from the identifier of the current GMK. GMK key identifier values can only be set to 0 or 1.
- Then, the PAN coordinator carries out an EAP-PSK authentication procedure with every device of the PAN. This procedure starts with an EAP-PSK message 1. The next steps follow the normal EAP-PSK message exchanges.
- The device keeps sending messages according to the previously assigned policy until the receipt of an LBP ACCEPTED message embedding a GMK-Activation parameter.
- Then, it acknowledges the message with an LBP JOINING message embedding a Parameter-result and starts sending frames using the new GMK.
- Note that a device may keep receiving messages encrypted with the previous GMK during a transient period. The previous GMK may be deleted after receipt of an LBP message including a GMK-remove parameter.

12.INITIALIZATION, BOOTSTRAPPING AND KEEP ALIVE

12.1 PAN COORDINATOR

The data concentrator's behavior initializes its G3-PLC modem as described in clause 9.3.9.2.1of ITU-T G.9903 [2] and with the additions detailed in the following figure:

- *Initialization – step 1:* reset of the G3-PLC modem.
- *Initialization – step 2:* configuration of the modem in PAN Coordinator mode (see adpDeviceType attribute).
- *Initialization – step 3:* the modem's EUI-64 MAC address is read and compared to the address stored within the applicative part of the device. If it is different to the modem's parameter, the applicative part of the device reconfigures it with all the attributes.
- *Initialization – step 4:* a discovery procedure is started as defined in ITU-T G.9903 [2]. The duration of the active scan is set to ActiveScanDuration when ADPM-DISCOVERY.request is called. The MAC active scan procedure returns a PANDescriptor list.
- *Initialization – step 5:* a network start procedure is performed as defined in ITU-T G.9903 [2]. By default, as stated in 8.3.1, the coordinator's short address is set to 0x0000. The choice of the network's PAN ID is out of the scope of this document.

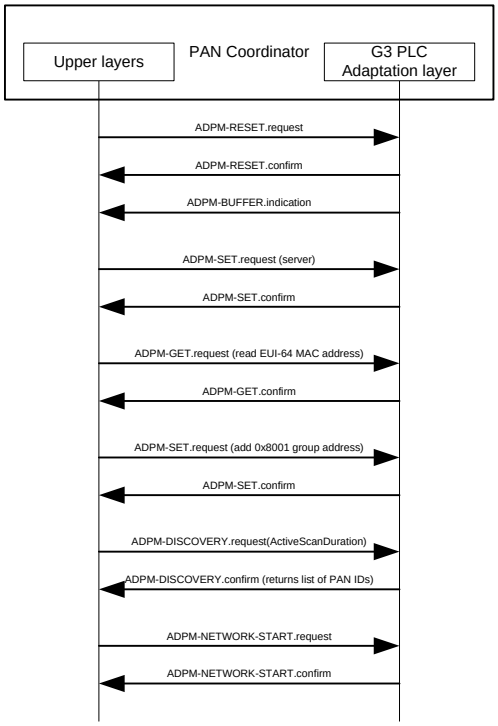

Fig. 7: Server initialization

12.2 PAN DEVICES

Standard devices (meters) shall initialize their modems and carry out the bootstrapping procedure described hereunder:

- *Initialization – step 1:* reset of the G3-PLC modem.
- *Initialization – step 2:* configuration of the modem in PAN device (see adpDeviceType attribute).
- *Initialization – step 3:* the modem's EUI-64 MAC address is read and compared to the address stored within the applicative part of the device. If it is different to the modem's parameter, the applicative part of the device reconfigures it with all the attributes.
- *Initialization – step 4:* a discovery procedure is started as defined in ITU-T G.9903 [2]. The duration of the active scan is set to ActiveScanDuration when ADPM-DISCOVERY.request is called. The MAC active scan procedure returns a PANDescriptor list.
- *Bootstrapping – step 1:* the LBP procedure is performed as defined in ITU-T G.9903 [2] in order to join a PAN.

After the discovery procedure, the PAN descriptor list is available. First of all (to avoid crosstalk cases), the PAN chosen is the one among the neighbours providing the best link quality (LQI) with the local node. Once the PAN is identified, the LBA chosen is the node providing the lowest route cost toward the PAN-selected coordinator, including the link cost toward the LBA chosen. The route cost computation is similar to a standard route discovery. Based on all beacons received during the active scan, the node computes the link cost toward each possible LBA according to the metric in use, and adds it to the RC_COORD received in the beacon. The node shall set the Weak Link Count to 1 in case the LQI of the link to the LBA is below adpWeakLQIValue. Similar to the G3-PLC protocol, the best route is defined by the lowest route cost among the lowest number of Weak Link computed. This way, the node is able to select the LBA providing the best route toward the coordinator. Note that LBA is not selected if its LQI with the local node is below JoinLQIThreshold.

Once the bootstrap is completed successfully, if the attribute adpDefaultCoordRouteEnabled is set to TRUE then a route discovery with the unicast RREQ flag set to TRUE is issued to confirm the route to the Pan Coordinator (whatever is the value of the attribute adpUnicastRREQGenEnabled).

The following algorithm shall be applied for a device to join a PAN:

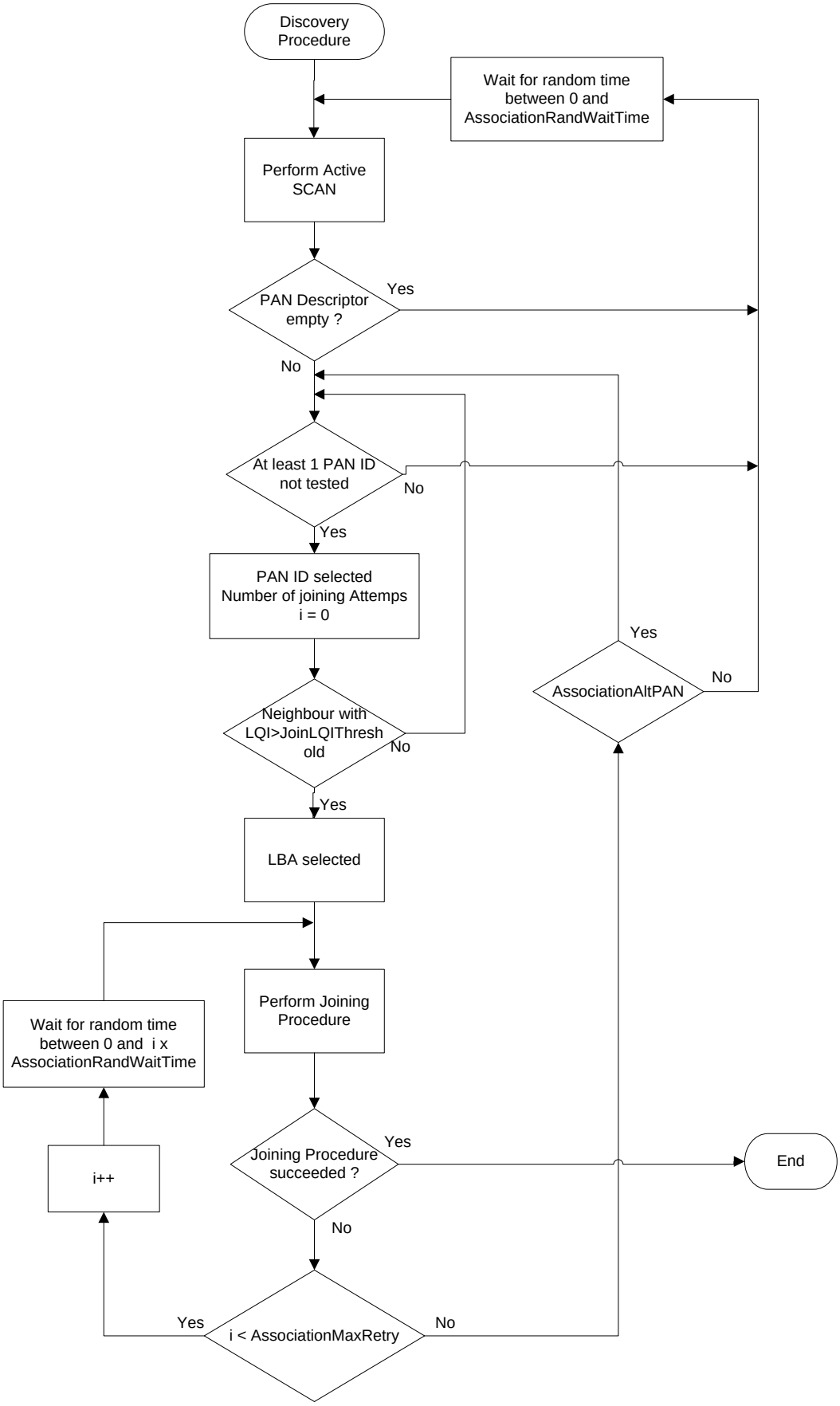

Fig. 8: PAN association procedure from "discovery" to "route discovery"

The first discovery attempt is done immediately after the start.

If the **AssociationAltPAN** parameter is set to TRUE and when all association attempts to join the same PAN have failed, the device shall initiate an association procedure with another PAN selected as previously specified among the remaining PANs of the PANDescriptor list.

If **AssociationAltPAN** is set to FALSE or if all association attempts with the remaining PANs of the PANDescriptor list have failed, the device shall not initiate association procedures with any other PAN (only the first selected PAN is considered).

If no association has been accomplished with one of the PANs of the PANDescriptor list, the device shall return in *Initialization – step 4* (another active scan is performed before initiating a new bootstrapping procedure).

- *Bootstrapping – step 2:* a route is established between the new communication node and the PAN coordinator.

A G3-PLC device may be configured using NDP-like configuration (NDP mode according to the DLMS/COSEM data model) or Stateless Address Autoconfiguration (AUTO_CONFIGURATION mode according to the DLMS/COSEM data model). While NDP configuration allows both ULA and link-local addresses to be used, as well as both stateless and stateful multicast, Stateless Address Autoconfiguration only allows the use of link-local addresses and stateless multicast.

Consequently, the following steps are performed only if NDP configuration is enabled (NDP configuration is enabled by default):

- *Bootstrapping – step 3:* the device receives a Router Advertisement from the coordinator carrying the context information. Router Solicitation is sent if no Router Advertisement has been received according to 8.5.4.
- *Bootstrapping – step 4:* the device autoconfigures its full ULA IPv6 address based on the received context information.
- *Keep alive:* when a device is operating within a PAN, a keep alive mechanism shall be supported (regardless of the NDP configuration) in order to maintain the device's association with the aforementioned PAN.

These messages:

- Path Request (6loWPAN level),
- ICMP Echo Request, ICMP Echo Reply (IP level),
- OPEN request, RELEASE request, GET request, SET request, ACTION request (COSEM level),

when sent in unicast by the PAN coordinator shall reset the PLCG3TimeOut timer to timeout_not_addressed value. Before the device's G3-PLC timeout expires, precisely after a duration indicated by **KeepAliveStartTime**, it sends periodic ICMP Echo requests intended for the PAN coordinator at a rate provided by the **KeepAliveSendPeriod** parameter. This mechanism may be disabled in setting the **KeepAliveEnable** parameter to FALSE.

The following sequence chart is illustrating a device's initialization and bootstrapping procedure:

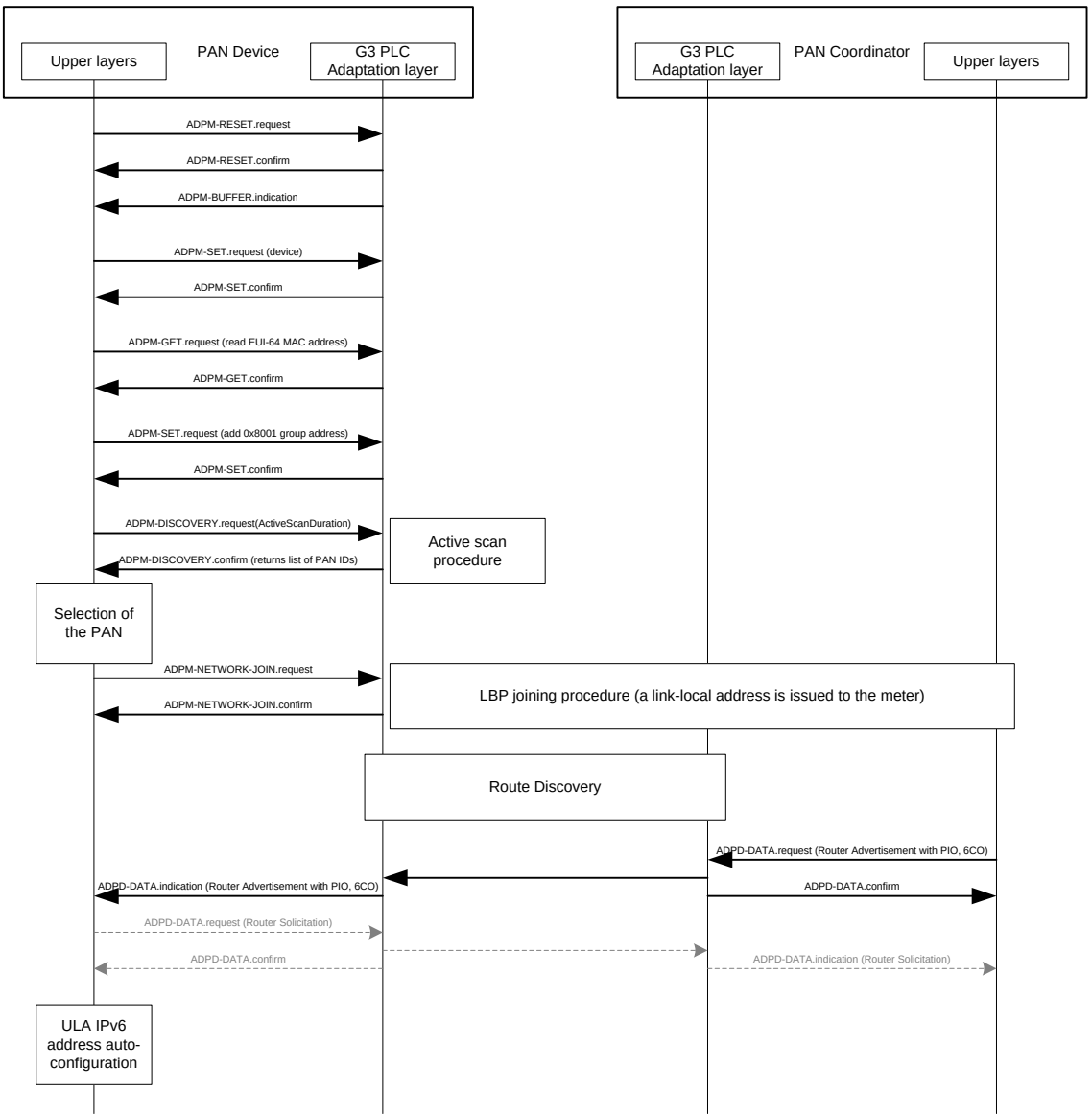

Fig. 9: Device initialization and bootstrapping

12.3 LIST OF THE NEW PARAMETERS DEFINED IN THIS CHAPTER

The following table provides a precise description of the complete set of parameters defined in this chapter:

Parameter	PAN Coord.	PAN Device	Length	Range	Description	Default value
ActiveScanDuration	Yes	Yes	8 bits	0 - 255	This attribute specifies the duration in seconds of the active scan.	15
AssociationMaxRetry	No	Yes	8 bits	1 – 255	Maximum number of association retries	8

AssociationRandWaitTime	No	Yes	8 bits	0 – 255	Maximum waiting time in minutes between two association retries for the same PAN	15
AssociationAltPAN	No	Yes	1 bit (Boolean)	TRUE FALSE	Indicates if the device tries to join an alternate PAN after reaching AssociationMaxRetry retries	TRUE
JoinLQIThreshold	No	Yes	8 bits	0 – 255	LQI threshold value to be used for LBA and PAN selection	52
KeepAliveStartTime	No	Yes	16 bits	0 – 65535	Indicates the time in minutes to wait before starting periodic emission of ICMP Echo requests	1380
KeepAliveSendPeriod	No	Yes	8 bits	1 – 255	Indicates the time in minutes between two successive keep alive ICMP Echo requests	10
KeepAliveEnable	No	Yes	1 bit (Boolean)	TRUE FALSE	Indicates whether the keep alive mechanism is enabled or not	FALSE

13. DLMS/COSEM COMMUNICATION PROFILES AND SERVICES

The DLMS/COSEM communication via the LAN interface is based on UDP over the IPv6 stack in combination with the G3-PLC transport layer.

13.1 UDP/IP PROFILE

The DLMS COSEM application connects to the TCP/IP or UDP/IP layer using and additional sublayer called the DLMS/COSEM wrapper.

The UDP/IP channel is configured and managed via the following COSEM objects:

Object / Attribute Name	Class	Ver.	OBIS code
TCP-UDP setup	41	0	0-0:25.0.0.255
IPv6 setup	48	0	0-0:25.7.0.255

Table 1: UDP/IP Objects

The UDP client port number used by the “COSEM Client Application Layer” shall be set between 61617 (0xF0B1) and 61631 (0xF0BF).
The UDP server port number used by the “COSEM Server Application Layer” shall be set 61616 (0xF0B0).

The following table summarizes the valid UDP port numbers for the DLMS/COSEM metering application:

Application	Server UDP ports Ports applying for packets emitted by the server to the client		Client UDP ports Ports applying for packets emitted by the client to the server	
	Source	Destination	Source	Destination
DLMS/COSEM	61616	61617-61629	61617-61629	61616

Other port numbers are reserved for future services

13.2 G3 INTERFACE SETUP

The G3 channel is configured and managed via the following COSEM objects:

Object / Attribute Name	Class	Ver.	OBIS code
MAC address setup	43	0	0-0:25.2.0.255
G3-PLC 6LoWPAN adaptation layer setup	92	1	0-0:29.2.0.255
G3-PLC MAC setup	91	1	0-0:29.1.0.255
G3-PLC MAC layer counters	90	1	0-0:29.0.0.255
PLCG3_Bandplan	1	0	0-0:94.43.128.255
PLCG3_Bandplan scheduler	22	0	0-0:94.43.129.255
PLCG3_Bandplan script table	9	0	0-0:94.43.130.255

Table 2: G3 Interface Objects

MAC address setup
The MAC address setup holds the EUI-48 address of the PLC G3 Modem.

G3-PLC 6LoWPAN adaptation layer setup
This object holds the necessary parameters to set up the 6LoWPAN adaptation sub-layer and provides access to information settings and tables that might be necessary for the network management:

- Routing Table
- Prefix Table
- Context Information Table
- Blacklist Table
- …

G3-PLC MAC setup
This object holds the necessary parameters to set up the MAC IEEE 802.15.4 sub-layer and provides access to information settings and tables that might be necessary for the network management:
- Neighbour Table
- ….

G3-PLC MAC counters
This object stores the counters relating to exchanges between PHY and MAC. The purpose of these counters is to provide statistical information for maintenance.
Note: when a counter reaches its maximum value (0xFFFFFFFF), it is automatically reset.

PLCG3_Bandplan
This object allows the identification of the current bandplan in use.
The supported bandplans are
0 = CENELEC-A band
3 = FCC band
Switching between Cenelec A and FCC band must be possible by either FW upgrade or configuration change:
⇨ In case of using a FW upgrade, this object shall be declared as readable only and displays the currently bandplan in use.
⇨ In case of using a configuration change, this object shall be declared as readable and writable and allows changing the current bandplan in use.

PLCG3_Bandplan scheduler and script table
These objects allow switching the bandplan from CENELE-A to FCC and vice versa at a scheduled date and time.

13.3 G3 NETWORK MANAGEMENT

The G3-PLC network requires some specific features for the establishment and maintenance of connections to the PAN device.
There is no description of these parameters in the IDIS specification [D] but they are important for the fine-tuning and maintenance of the G3-PLC network.

The G3 network is configured and managed via the following COSEM objects:

Object / Attribute Name	Class	Ver.	OBIS code
Auto connect	29	2	0-0:2.1.0.255
PLCG3_PSK_KEK	1	0	0-0:94.43.133.255
PLCG3_PSK	1	0	0-0:94.33.128.255
PLCG3TimeOut	1	0	0-0:94.33.10.255
PLCG3KeepAlive	1	0	0-0:94.33.11.255
AdpLBPAssociationSetup	1	0	0-0:94.33.14.255
AdpLQIRange	1	0	0-0:94.33.16.255
AdpRREPWait	1	0	0-0:94.33.15.255
AdpDefaultCoordRouteEnabled	1	0	0-0:94.43.135.255
MacCoherentTransmission	1	0	0-0:94.33.12.255
MacDeviceTable	1	0	0-0:94.33.13.255
MacPOSTableEntryTTL	1	0	0-0:94.43.136.255
MacPOSTable	1	0	0-0:94.43.137.255
MacBroadcastMaxCWEnabled	1	0	0-0:94.43.138.255
MacTransmitAtten	1	0	0-0:94.43.139.255
InitiatorElectricalPhase	1	0	0-0:96.62.0.255
DeltaElectricalPhase	1	0	0-0:96.62.1.255
AlternatePANId	1	0	0-0:94.33.55.255
AlternatePANIdLog	7	1	0-0:94.33.9.255
PAN connection status	1	0	0-0:94.43.131.255

PAN connection status profile	7	1	0-0:94.43.132.255

Table 3: G3 Network Objects

Auto connect
The network connectivity of the meter is controlled by the auto connect object
The following auto connect modes are supported:
- (101) The meter is permanently connected to the IP network and can be reached by the HES via its known IP address.

PLCG3_PSK_KEK
This object allows changing the PSK Key Encryption Key (128 bits / 16 octets) of the meter.
The new PSK_KEK is wrapped by the AES-128 key wrap algorithm, using the current PSK_KEK as the wrapping key.

PLCG3_PSK
This object allows changing the PSK (128 bits / 16 octets) of the meter.
The new PSK is wrapped by the AES-128 key wrap algorithm, using the dedicated PSK KEK as the wrapping key.
After the successful change of the PSK (confirmation to the DLMS client), the meter returns to the non associated state and re-starts it's joining process for the reconnection to the PAN coordinator.

PLCG3TimeOut
This data defines the time, in minutes, after which a meter that has not been individually addressed (meaning the meter has not received any Path Discovery message, ICMP ping, nor unicast DLMS APDU) returns to the non associated state and loses its PAN coordinator. A value equal to 0 is equivalent to cancel the use of the related time-out-not-addressed counter.

PLCG3KeepAlive
This object defines the parameters used by the "keep alive" mechanism.

AdpLBPAssociationSetup
This attributes contains parameters for Bootstrapping procedure setup.

AdpLQIRange
The LQI range defines the lower and higher LQI value used for the metric computation

AdpRREPWait
This object defines the delay for an RREP frame to wait in seconds before being generated after either the arrival of the first RREQ or the transmission of the latest RREP.

AdpDefaultCoordRouteEnabled
The adaptation layer adds a default route to the PAN coordinator after successful completion of the bootstrapping procedure if enabled. Otherwise, no default route will be created.

MacCoherentTransmission
This object indicates the specific modulation scheme to set in the tone map response.

MacDeviceTable
This object describes a table of Device-Descriptor entries.

MacPOSTableEntryTTL
Time to live for an entry in the POS table in minutes

MacPOSTable
The POS table contains information about devices in the POS of the device.

MacBroadcastMaxCWEnabled

Allows MAC to use the maximum contention window for broadcast frames if enabled.

MacTransmitAtten
Attenuation of the output level in dB

InitiatorElectricalPhase
This object indicates the phase number to which the client system is connected.

DeltaElectricalPhase
This object indicates the phase difference between the client system's connecting phase and the meter's connecting phase.

AlternatePANid
This object stores the detected PANid for capturing into the AlternatePANIdLog
The data contains the alternate PAN Id that has been indicated by the MLME-COMM-STATUS.indication with Status = ALTERNATE_PANID_DETECTION.

AlternatePANid log
This object logs the « alternate PAN Id » detected by the meter.
Everytime the MLME-COMM-STATUS.indication primitive is called with Status = ALTERNATE_PANID_DETECTION, the meter checks if there is already an entry with the same PAN-ID in the buffer:
• If it is the case, this entry is updated with the current date and time, and moved to the end of the buffer (i.e. it becomes the latest element of the array);
• If not, a new entry is added with the alternate PAN-Id value and the current date and time.
When the buffer is full, the oldest entry is deleted to allow the storage of a new entry.

min capacity:	5 entries
structure:	clock.time, value
capture_period:	0 (externally triggered)
captured objects:	clock.time; alternate PAN ID
buffer encoding:	normal: clock with every entry
selective access:	by range and by entry
sorted method:	unsorted (FIFO)

PAN connection status
This object contains the network status information for the connection of the end device to the PAN coordinator.
The connection status information is based on the
- Routing table entry of the 'PAN coordinator' and
- Neighbour table entry of the 'Next Hop'

```
PAN_connection_status ::= structure
        {
                routing_table_entry ::= structure;
                neighbour_table_entry ::= structure
        }

routing table entry to PAN coordinator
routing_table ::= structure
        {
                destination_address: long-unsigned,
                next_hop_address: long-unsigned,
                route_cost: long-unsigned,
                hop_count: unsigned,
                weak_link_count: unsigned,
                valid_time: long-unsigned
        }
```

neighbor table entry of next hop
neighbour_table ::= structure
{
short_address: long-unsigned,
payload_modulation_scheme: boolean,
tone_map: bit-string,
modulation: enum,
tx_gain: integer,
tx_res: enum,
tx_coeff: bit-string,
lqi: unsigned,
phase_differential integer,
TMR_valid_time: unsigned,
neighbour_valid_time: unsigned
}

PAN connection status profile
This object allows monitoring the network status for the connection of the end device to the PAN coordinator by recoding the PAN connection status in a regular interval.

capacity:	7 days with hourly entries, 3 captured objects (min. 168 entries)
structure:	clock.time, value
capture_period:	default 60 minutes (3600 seconds), allowed range 1,5,10,15,60 min or daily
captured objects:	clock.time, PAN connection status
buffer encoding:	normal: clock with every entry
selective access:	by range and by entry
sorted method:	unsorted (FIFO)