



BSI Standards Publication

Electricity metering data exchange — The DLMS/COSEM suite

Part 8: SMITP B-PSK PLC communication profile for neighbourhood networks — Including: The Original-SMITP PLC B-PSK communication profile, The Original-SMITP Local data exchange profile and The Original-SMITP IP communication profile

National foreword

This Published Document is the UK implementation of CLC/TS 50568-8:2015.

The UK participation in its preparation was entrusted to Technical Committee PEL/13, Electricity Meters.

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 2015.

Published by BSI Standards Limited 2015

ISBN 978 0 580 85915 1

ICS 35.240.60; 91.140.50

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2015.

Amendments/corrigenda issued since publication

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

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CLC/TS 50568-8

April 2015

ICS 35.240.60; 91.140.50

English Version

Electricity metering data exchange - The DLMS/COSEM suite -
Part 8: SMITP B-PSK PLC communication profile for
neighbourhood networks - Including: The Original-SMITP PLC B-
PSK communication profile, The Original-SMITP Local data
exchange profile and The Original-SMITP IP communication
profile

This Technical Specification was approved by CENELEC on 2014-11-11.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

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



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

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

CONTENTS

Foreword	9
Introduction.....	10
1 Scope.....	11
2 Normative references	12
3 Acronyms and abbreviations, terms, definitions and notations	13
3.1 Acronyms and abbreviations	13
3.2 Terms and definitions	14
3.3 Notations.....	15
4 The DLMS/COSEM SMITP B-PSK PLC profile.....	16
4.1 Structure of the profile	16
4.2 Physical layer	17
4.3 Data link layer	17
4.4 Application to data link convergence layer	17
4.5 Application layer	27
4.6 Application process	27
4.7 PLC network management.....	28
4.8 Addressing	31
4.9 System variables	32
5 The Original-SMITP B-PSK PLC profile	33
5.1 Overview	33
5.2 Structure of the profile	33
5.3 Physical layer	34
5.4 Data Link layer	35
5.5 Application layer	35
5.6 SMITP Data model	35
5.7 Application process	35
6 The Original-SMITP IP profile	43
6.1 Overview	43
6.2 Structure of profile.....	43
6.3 Physical and data link layers	44
6.4 Transport and network layers	44
6.5 Application layer	48
6.6 SMITP Data model	48
7 Original-SMITP Local Optical interface profile	49
7.1 Overview	49
7.2 Physical layer	49
7.3 Data transmission protocol	50
7.4 Packet's protocol format	51
7.5 Data Link Layer	53
8 Discovery and registration services	55
8.1 DLMS/COSEM over B-PSK discovery and registration services	55
8.2 Original-SMITP over B-PSK discovery and registration services	68

9	The Original-SMTP AL Services	75
9.1	Application messages exchanged in distribution line networks.....	75
9.2	Application messages exchanged in telecommunication public networks	107
9.3	Encryption, Authentication and Playback Attacks Protection	131
9.4	Encoding examples	136
9.5	TCP/IP encapsulation example of SMTP TB Application layer message.....	141
10	The Original-SMTP Data model	144
10.1	Introduction	144
10.2	Internal parameters	145
10.3	Total energies	148
10.4	Daily energies	149
10.5	Load profiles and setting parameters	150
10.6	Communication address and keys of authentication	153
10.7	Meter identification information	156
10.8	Temporal information	157
10.9	Billing period information	160
10.10	Software, Hardware and Security information	162
10.11	Supply contract information	165
10.12	Weekly tariff information	169
10.13	Annual tariff information	179
10.14	Public holidays programming	181
10.15	Load modulation parameters	182
10.16	Voltage interruption information	185
10.17	Voltage variation information	191
10.18	Control information	197
10.19	Normal Status Word	200
10.20	Extended Status Word	202
10.21	Cut-off device control information	204
10.22	Display management	206
10.23	Download parameters	208
10.24	Measurand profiles and parameters	211
10.25	Synchronized measurand registers	215
10.26	Event log management	219
10.27	Billing data information	221
10.28	Virtual billing data registers	237
10.29	Time stamp of maximum power demand	246
10.30	Measurand information	252
10.31	Reading mode management	255
10.32	Management of log's events	256
Annex A (informative)	Node discovery procedure example using the DLMS/COSEM SMTP B-PSK PLC profile	261
A.1	Node Discovery	261
A.1.1	Discover nodes directly accessible from the Concentrator	261
A.1.2	Enable L1 meters to discover nodes not directly accessible from the Concentrator	263
A.1.3	Gathering discovered nodes from L1 meters	263

A.1.4	Repeating the process with L1 meters until no new meters are discovered	265
A.2	Registration and routing management	268
Annex B (informative)	Node discovery procedure example using the Original-SMITP over B-PSK PLC profile	270
B.1	Node Discovery	270
B.1.1	Discover nodes directly accessible from the Concentrator.....	272
B.1.2	Enable L1 meters to discover nodes not directly accessible from the Concentrator	272
B.1.3	Gathering discovered nodes from L1 meters	272
B.1.4	Repeating the process with L1 meters until no new meters are discovered	274
B.2	Registration and routing management	278
Annex C (informative)	SMITP specific definitions	280
C.1	Management of reserved elements	280
C.2	ECTL structure	280
Annex D (normative)	MIB and COSEM Set-up class interface	281
D.1	General	281
D.2	Types definition	281
D.3	SMITP configuration attributes.....	281
D.4	SMITP statistical attributes	284
Annex E (informative)	Specification of communication mode F for direct local data exchange.....	285
E.1	Introduction	285
E.2	Mode F for direct local data exchange	285
E.2.1	General.....	285
E.2.2	Sign-on flow.....	285
E.2.3	Physical layer primitives.....	286
E.2.4	Timers	287
E.3	Sign on example.....	287
E.3.1	Identifier request -300 baud- (TP)	287
E.3.2	Meter identifier response from meter -300 baud-.....	287
E.3.3	Work mode selection -300 baud- (HHU)	288

List of figures

Figure 1	Document structure of CLC/TS 50568-8	11
Figure 2	The DLMS/COSEM SMITP B-PSK PLC communication profile	16
Figure 3	Services of the COSEM to B-PSK convergence layer	18
Figure 4	Type 1 CLPDU format	20
Figure 5	Type 2 CLPDU format	20
Figure 6	Control field format	21
Figure 7	Sequence chart of a CL transfer not requiring segmentation	22
Figure 8	sequence chart of a CL transfer requiring segmentation at both sides	23
Figure 9	sequence chart of a CL transfer requiring segmentation using the unconfirmed service.....	25

Figure 10 – Meter's state diagram.....	31
Figure 11 – Reference communication architecture.....	32
Figure 12 – Protocol stack for SMITP on PLC.....	33
Figure 13 – Meter's state diagram.....	36
Figure 14 – Synchronization without protection.....	37
Figure 15 – Synchronization with protection.....	37
Figure 16 – Individual registers reading.....	37
Figure 17 – Table registers reading.....	38
Figure 18 – Individual registers writing.....	38
Figure 19 – Table registers writing.....	38
Figure 20 – Download procedure.....	40
Figure 21 – Reference communication architecture.....	43
Figure 22 – Protocol stack for SMITP on IP.....	44
Figure 23 – Connection Opening.....	47
Figure 24 – Data exchange.....	47
Figure 25 – Connection Closing.....	48
Figure 26 – Optical interface protocol stack.....	49
Figure 27 – Messages sequence in connection procedure between meter and HHU.....	50
Figure 28 – Connection request message.....	52
Figure 29 – Identification response message.....	52
Figure 30 – Acknowledgement message.....	53
Figure 31 – MAC frame structure.....	53
Figure 32 – Discover messages exchange.....	58
Figure 33 – DiscoverReport messages exchange.....	59
Figure 34 – TCTset messages exchange.....	60
Figure 35 – DiscoverForward messages exchange.....	61
Figure 36 – DiscoverForwardReport messages exchange.....	63
Figure 37 – Status messages exchange.....	64
Figure 38 – Register messages exchange.....	65
Figure 39 – RegisterReport messages exchange.....	66
Figure 40 – Deregister messages exchange.....	67
Figure 41 – Ping.request messages exchange.....	68
Figure 42 – Ping.response messages exchange.....	68
Figure 43 – Subnets of the network.....	75
Figure 44 – Request A-Node to transmit data to B-Node.....	97
Figure 45 – Request A-Node to transmit data to B-Node: B-Node does not answer.....	98
Figure 46 – Structure of messages exchanged in telecommunication networks.....	108
Figure 47 – Structure of Message Header.....	109
Figure 48 – Structure of Message Data.....	109
Figure 49 – TB messages exchange in the On-Line transaction.....	113
Figure 50 – Error condition during the transaction.....	114

Figure 51 – TB messages exchange in the Off-Line transaction	115
Figure 52 – Messages to cancel a transaction required by AMM system	115

List of tables

Table 1 – Convergence layer error management scheme	26
Table 2 – Example of message structure to be displayed	42
Table 3 – Standard ASCII control characters	51
Table 4 – Baud Rate coded values	53
Table 5 – Discover service	58
Table 6 – Discover service arguments	58
Table 7 – DiscoverReport service	59
Table 8 – DiscoverReport service arguments	59
Table 9 – TCTset service	60
Table 10 – TCTSet service arguments	60
Table 11 – DiscoverForward service	61
Table 12 – DiscoverForward service arguments	61
Table 13 – DiscoverForwardReport service	62
Table 14 – DiscoverForwardReport service arguments	62
Table 15 – Status service	63
Table 16 – Status service arguments	63
Table 17 – Register service	64
Table 18 – Register service arguments	64
Table 19 – RegisterReport service	65
Table 20 – RegisterReport service arguments	65
Table 21 – Deregister service	66
Table 22 – Deregister service arguments	66
Table 23 – Ping service	67
Table 24 – Ping service arguments	67
Table 25 – Chl.Req 112 message	69
Table 26 – Chl.Resp 113 message	69
Table 27 – Address.Req 090 message	70
Table 28 – TCT_Set.Req 092 message	71
Table 29 – ReqAddr.Req 094 message	71
Table 30 – Address.Resp 091 message	72
Table 31 – ReqAddr.Resp 095 message	73
Table 32 – Structure of Struct Address.Resp	73
Table 33 – NACK.RESP 247 message	74
Table 34 – Application messages in distribution line network	77
Table 35 – Write.Req 004 message for clock synchronization	79
Table 36 - Write.Req 004 message for general parameter writing	79
Table 38 – WriteTab.Req 010 message	81

Table 39 – WriteTab.Req 110 message	82
Table 40 – SetTab.Req 014 message	83
Table 41 – SetTab.Req 114 message	84
Table 42 – Example of a table set command.....	85
Table 43 – ResetTab.Req 016 message	85
Table 44 – ResetTab.Req 116 message	86
Table 45 – Read.Req 002 message	87
Table 46 – Read.Resp 003 message	87
Table 47 – ReadTab.Req 006 message	88
Table 48 – ReadTab.Resp 007 message.....	88
Table 49 – ReadTab.Req 008 message (block read).....	89
Table 50 – ReadTab.Resp 009 message (block read)	89
Table 51 – GetTab.Req 030 message	90
Table 52 – GetTab.Resp 031 message	91
Table 53 – Authenticated Read.Req 102 message	91
Table 54 – Authenticated Read.Resp 103 message	92
Table 55 – Authenticated ReadTab.Req 106 message	93
Table 56 – Authenticated ReadTab.Resp 107 message	93
Table 57 – Authenticated ReadTab.Req 108 message (block read).....	94
Table 58 – Authenticated ReadTab.Resp 109 message (block read).....	95
Table 59 – Authenticated GetTab.Req 130 message.....	95
Table 60 – Authenticated GetTab.Resp 131 message	96
Table 61 – SetIc.Req 040 message.....	97
Table 62 – Authenticated SetIc.Req 140 message	98
Table 63 – WriteTabIc.Req 042 message	99
Table 64 – Authenticated WriteTabIc.Req 142 message	100
Table 65 – Reprog 100 message (local programming)	101
Table 66 – Reprog 101 message (broadcast programming)	101
Table 67 – Command 018 message	102
Table 68 – Authenticated Command 118 message.....	102
Table 69 – A-Node ACK 253 message	103
Table 70 – Authenticated A-Node ACK 243 message.....	104
Table 71 – A-Node NACK 255 message.....	104
Table 72 – Authenticated A-Node NACK 245 message	104
Table 73 – Coding of field Value in A-Node Nack messages	105
Table 74 – Coding of sub field SSAP in LLC frame	105
Table 75 – B-Node ACK 251 message	106
Table 76 – Authenticated B-Node ACK 241 message.....	106
Table 77 – B-Node NACK 249 message.....	106
Table 78 – Authenticated B-Node NACK 239 message	107
Table 79 – Coding of field Value in B-Node Nack messages	107

Table 80 – Relationship between Message Code, Prot and Action fields	110
Table 81 – General description of a message using SMITP references	110
Table 82 – TB Message example 1	111
Table 83 – PLC translation of previous TB message	111
Table 84 – TB Message example 2	111
Table 85 – PLC translation of previous TB message	111
Table 86 – TB application messages in telecommunication public network.....	111
Table 87 – TB Write.Req 004 message (single programming of one parameter).....	116
Table 88 – TB Write.Req 004 message (single programming of more parameters).....	116
Table 89 – TB Sinc.Req 034 message	117
Table 90 – TB WriteTab.Req 010 message	118
Table 91 – TB SetTab.Req 014 message	119
Table 92 – TB ResetTab 016 message	119
Table 93 – TB GetTab.Req 030 message.....	120
Table 94 – TB GetTab.Resp 031 message	121
Table 95 – TB Read.Req 002 message	121
Table 96 – TB Read.Resp 003 message	122
Table 97 – TB ReadTab.Req 006 message	123
Table 98 – TB ReadTab.Resp 007 message	123
Table 99 – TB ReadTab.Req 008 message (entire table)	124
Table 100 – TB ReadTab.Resp 009 message (entire table).....	124
Table 101 – TB Command 018 message	125

Foreword

This document (CLC/TS 50568-8:2015) has been prepared by CLC/TC 13, "Electrical energy measurement and control".

The following date is fixed:

- latest date by which the existence of (doa) 2015-07-24
this document has to be announced
at national level

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

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

The European Committee for Electrotechnical Standardization (CENELEC) draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of a maintenance service concerning the stack of protocols on which the present Technical Specification CLC/TS 50568 is based.

The CENELEC takes no position concerning the evidence, validity and scope of this maintenance service.

The provider of the maintenance service has assured the CENELEC that he is willing to provide services under reasonable and non-discriminatory terms and conditions for applicants throughout the world. In this respect, the statement of the provider of the maintenance service is registered with the CENELEC. Information may be obtained from:

Meters and More Open Technologies
Brussels/Belgium
www.metersandmore.eu

Introduction

This Technical Specification is based on the results of the European OPEN Meter project, Topic Energy 2008.7.1.1, Project no.: 226369, www.openmeter.com.

1 Scope

This Technical Specification contains 4 profile specifications

- the DLMS/COSEM SMITP B-PSK PLC Profile (clause 4)
- the Original-SMITP B-PSK PLC Profile (clause 5)
- the Original-SMITP IP Profile (clause 6)
- the Original-SMITP Local data exchange profile (clause 7)

The **DLMS/COSEM SMITP B-PSK profile** (see Clause 4) defines the use of the CLC/TS 50568-4 communication protocol and methods to access and exchange data modelled by the COSEM objects of EN 62056-6-2 via the EN 62056-5-3 application layer. This clause is in line with the DLMS/COSEM suite as described in EN 62056-1-0.

The **Original-SMITP Profiles** (Clauses 5, 6 and 7) define the use of the CLC/TS 50568-4 communication protocol and methods to access and exchange data modelled by the Original-SMITP Data Model (clause 10) via the Original-SMITP Application Layer (Clause 9). These clauses are not part of the DLMS/COSEM suite as described EN 62056-1-0.

NOTE The expression Original-SMITP refers to the open Smart Metering Information and Telecommunication Protocol originally developed and maintained by the Meters and More Association (see Foreword). The Original SMITP specifications were developed prior to the availability of the DLMS/COSEM SMITP B-PSK profile.

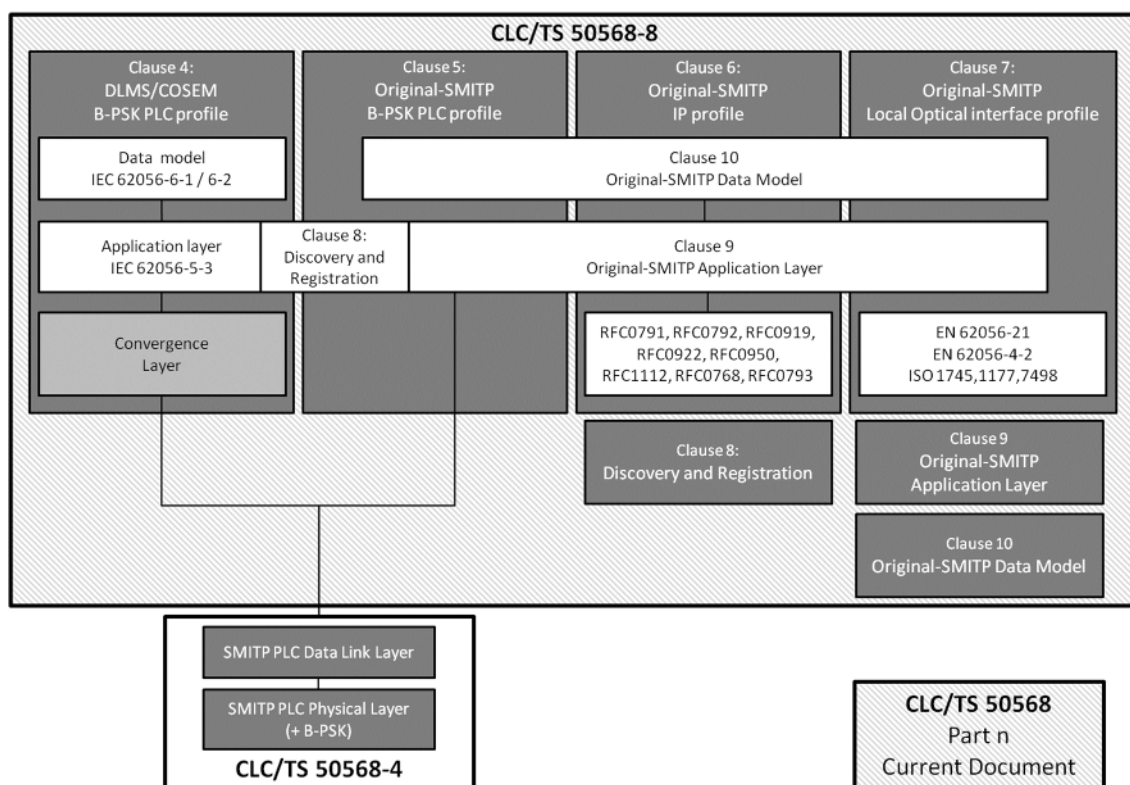


Figure 1 – Document structure of CLC/TS 50568-8

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.

CLC/TS 50568-4:2015, *Electricity metering data exchange — The Smart Metering Information and Telecommunication Protocols (SMITP) suite — Part 4: Physical layer based on B-PSK modulation + Data Link Layer*

EN 62056-21, *Electricity metering — Data exchange for meter reading, tariff and load control — Direct local data exchange (IEC 62056-21)*

EN 62056-42, *Electricity metering — Data exchange for meter reading, tariff and load control — Part 42: Physical layer services and procedures for connection-oriented asynchronous data exchange (IEC 62056-42)*

EN 62056-5-3, *Electricity metering data exchange – The DLMS/COSEM Suite - Part 5-3: DLMS/COSEM application layer (IEC 62056-5-3)*

EN 62056-6-2, *Electricity metering data exchange – The DLMS/COSEM Suite - Part 6-2: COSEM Interface classes (IEC 62056-6-2)*

SP 800-38A, Morris Dworkin, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques, December 2001*

NIST SP 800-38B, Morris Dworkin, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005*

ISO 1745, *Information processing — Basic mode control procedures for data communication systems*

ISO 1177, *Information processing — Character structure for start/stop and synchronous character oriented transmission*

ISO 7498, *Information processing systems — Open systems interconnection — Basic reference model*

3 Acronyms and abbreviations, terms, definitions and notations

3.1 Acronyms and abbreviations

For the purpose of this document, the following acronyms and abbreviations apply.

AA:	Application Association
ACA:	Absolute Communication Address
ACK:	Acknowledgement
AES:	Advanced Encryption Standard
AES-CMAC:	Advanced Encryption Standard – Cipher-based Message Authentication Code
AES-CTR:	Advanced Encryption Standard – Counter Mode Encryption
AES-ECB:	Advanced Encryption Standard – Electronic Codebook
AL:	Application Layer
AMM:	Automatic Metering Management
AP:	Application Process
APDU:	Application Protocol Data Unit
ATTR:	Attribute of SMTP message
AV:	Any Value
A-XDR:	Adapted eXtended Data Representation
bcd:	Binary Coded Decimal
B-PSK:	Binary Phase Shift Keying
CF:	Control Function
COSEM:	Companion Specification for Energy Metering
CT:	Current Transformer
DCS:	Digital Cross-connect System
DLMS:	Device Language Messaging Specification
DM:	Data Model
DSAP:	Destination Service Access Point
DST:	Daylight Saving Time
GPRS:	General Packet Radio Service
GSM:	Group Special Mobile
HES:	Head End System
HHU:	Hand Held Unit
IC:	Interface Class
IP:	Internet Protocol
Len:	Length (in bytes)
LLC:	Logical Link Control
LMON:	Last Message Order Number
ECTL:	Link Service Access Point
LSb:	Least Significant bit
LSB:	Least Significant Byte

LV:	Low Voltage
MAC:	Media Access Control
MBZ:	Must Be Zero
MDF:	More Data Follow
MU:	Measurement Unit
NA:	Not Applicable
NACK:	Negative Acknowledgement
NNAP:	Neighbourhood Network Access Point
NN:	Neighbourhood Networks
NTW:	Network
OBIS:	Object Identification System
OPA:	Optical Powerline Access
PLC:	Power Line Carrier
PQ:	Power Quality
RES:	Reserved
RTC:	Real Time Clock
SAP:	Service Access Point
SCA:	Section Communication Address
SEQ:	Sequence
SSAP:	Source Service Access Point
STD:	Standard Time
TB:	Tele-management from AMM system
TCP:	Transmission Control Protocol
TCR:	Silencing level threshold
TCT:	Silencing level parameter
TMAC:	Truncated MAC
ULP:	Upper Layer Protocol
UMTS:	Universal Mobile Telecommunications System
WAN:	Wide Area Network

3.2 Terms and definitions

For the purpose of this document the following terms and definitions apply:

3.2.1

concentrator section

identification code of the network managed by the concentrator

3.2.2

node subsection

identification code of the sub network within the network identified by concentrator section

3.2.3

node progressive

unique node ID within the node subsection

3.3 Notations

For the purpose of this document the following notations apply:

- 1 byte = 8 bits;
- fields and bytes naming: capital alphanumeric characters;
- transmission bit order of byte/field relative to the representative mode: first right bit = first transmitted bit;
- transmission bit order of byte/field relative to their weight: least significant bit = first transmitted bit.

4 The DLMS/COSEM SMITP B-PSK PLC profile

4.1 Structure of the profile

The reference model of the DLMS/COSEM SMITP B-PSK PLC communication profile is shown in figure below. It is based on a simplified – or collapsed – three layer OSI architecture. The layers are the physical layer, the data link layer, the convergence layer and the application layer. The data link layer is split into the MAC sub layer and the LLC sub layer.

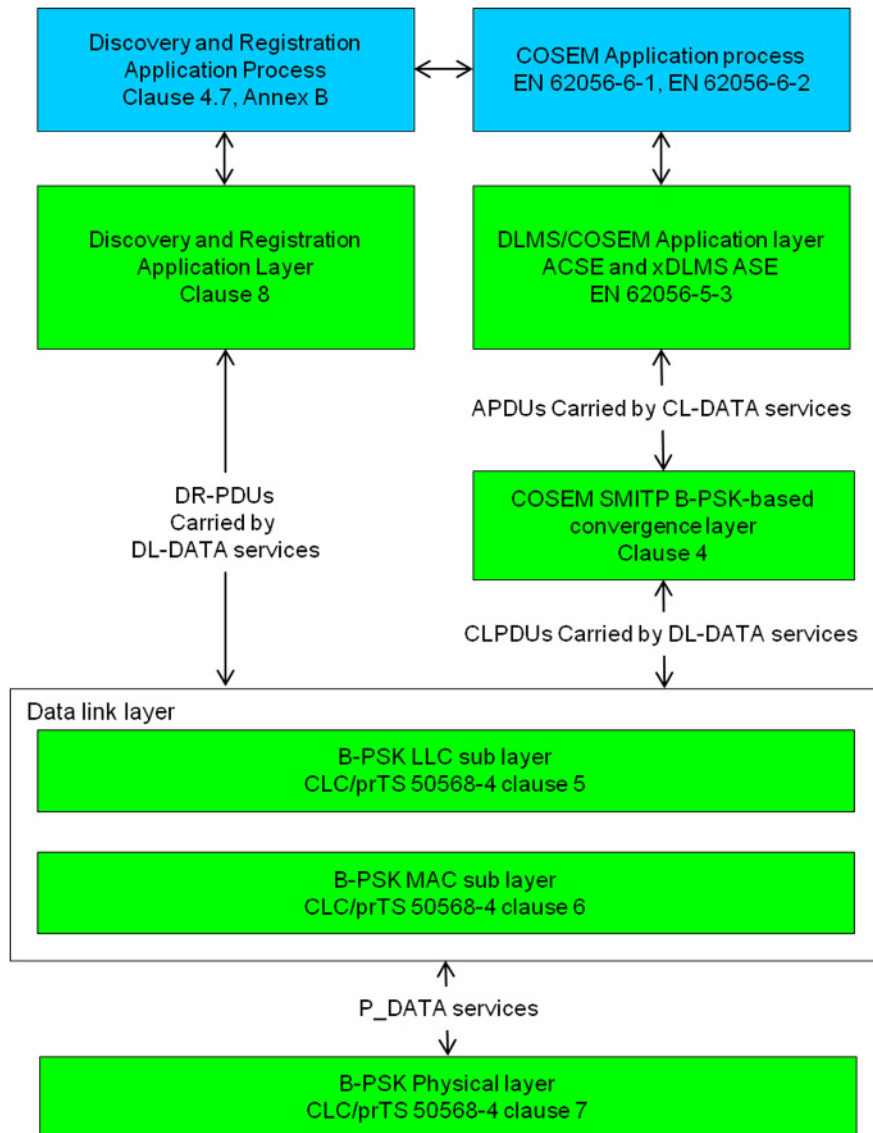


Figure 2 – The DLMS/COSEM SMITP B-PSK PLC communication profile

4.2 Physical layer

The Physical layer provides the interface between the equipment and the physical transmission medium, that is the distribution network. It transports binary information from the source to the destination.

The Physical Layer is specified in CLC/TS 50568-4:2015, Clause 7. It provides to the MAC sub-layer P_DATA services to transfer MPDUs to a peer MAC sub layer entity(ies) using the distribution network as the transport medium.

4.3 Data link layer

4.3.1 General

The data link layer consists of two sub layers: the Medium Access Control (MAC) and the Logical Link Control (LLC) sub layer.

The MAC sub layer handles access to the physical medium and provides physical device addressing. The decision to access the medium is made by the initiator, directly for its own MAC sub layer, or indirectly for other MAC sub layers that are requested to transmit a response to a request sent previously by the initiator.

The LLC sub layer controls the logical links.

4.3.2 The MAC sub layer

The MAC sub layer of the DLMS/COSEM SMITP B-PSK PLC communication profile is specified in CLC/TS 50568-4:2015, Clause 6. It provides the following services to its service user LLC sub layer:

- the MA_DATA services. These services allow the LLC sub layer entity to exchange LLC data units with peer LLC sub layer entities;
- the MA_EVENT.indication service. The usage of this service is specified in CLC/TS 50568-4:2015, Clause 6.

4.3.3 The LLC sub layer

The LLC sub layer is as specified in CLC/TS 50568-4:2015, Clause 5. It provides to the upper layers the DL_DATA services. These services allow the application layer entity to exchange application data with peer application entity(ies), either directly or through the convergence layer.

Management of ECTL field in LPDU is as follows:

- DSAP field shall be fixed to:
 - 0000 if the LPDU is used to transport CLPDUs;
 - 0001 if the LPDU is used to transport DR-PDUs ;
- SSAP field shall be always 0000.

4.4 Application to data link convergence layer

4.4.1 General

The B-PSK-based Data Link provides to the DLMS/COSEM application layer the basic data services required: unicast and multicast data transfer. In order to cover all the COSEM application layer requirements additional features are implemented in this convergence layer, in particular:

- Segmentation and Reassembly;
- SAP management.

4.4.2 Service specification for the DLMS/COSEM SMITP B-PSK-based convergence layer

4.4.2.1 General

The DLMS/COSEM SMITP B-PSK convergence layer provides unbalanced service between Master and Slave, meaning that the slave cannot spontaneously initiate a communication. In fact it is only allowed to transmit data to the Master via a .response service that can be issued after an .indication service only..

The DLMS/COSEM SMITP B-PSK convergence layer provides only data communication services in connection-less mode

Both confirmed and unconfirmed services are supported by this convergence layer, confirmed services shall make use of RA and RB service classes when invoking DL-DATA services, unconfirmed services shall make use of S service class when invoking DL-DATA services.

The .request, .response and .indication service primitives are mandatory; the implementation of .confirm service, which is a local service primitive, is optional.

NOTE DSAP and SSAP referenced in this clause have no relationship with the DSAP sub-field described in 4.3.3 and in CLC/TS 50568-4:2015, Clause 5. DSAP and SSAP referenced in this clause are transparently passed between the communication endpoint systems Application Layers, any description of these fields or this usage is out of the scope of this document.

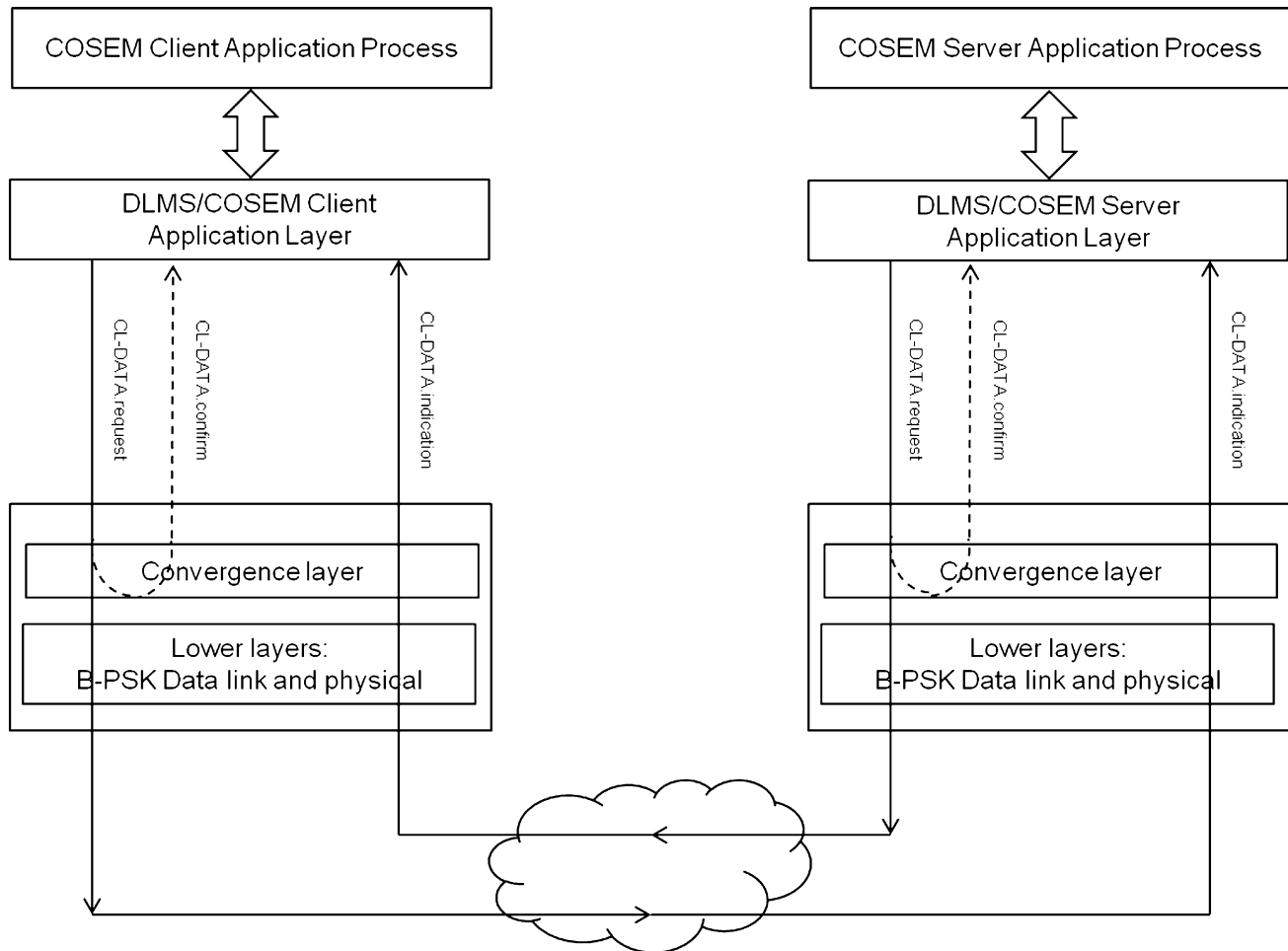


Figure 3 – Services of the DLMS/COSEM to B-PSK convergence layer

4.4.2.2 CL-DATA.request

Function

This service primitive is invoked by the Client service user DLMS/COSEM application layer to request the transmission of an APDU to the Server DLMS/COSEM application layer.

Service parameters

```
CL-DATA.request {
    Data_link_communication_parameters,
    SSAP,
```

```

    DSAP,
    Data_length,
    Data
}

```

Data_Link_communication_parameters are transparently passed to the DL-DATA.request; definition of these parameters is given in CLC/TS 50568-4:2015, Clause 5.

SSAP is the Service Access Point of the originating entity; it is used to indicate which application entity generated the APDU.

DSAP is the Service Access Point of the destination entity; it is used to indicate to which application entity the APDU shall be delivered.

Data_Length is the length of the APDU to be transferred to the server application layer entity.

Data is the APDU to be transferred to the server application layer entity.

Use

The CL-DATA.request primitive is invoked by the client DLMS/COSEM application layer to request sending an APDU to a single peer application layer, or, in the case of multi- or broadcasting, to multiple peer application layers. The same primitive is also invoked by the server DLMS/COSEM application layer, as a response to an CL-DATA.indication event in case the application layer requested a confirmed service.

The invocation of this service primitive shall cause the convergence layer to segment the APDU if needed, to assemble the convergence layer PDU (see clause 4.4.3), and then to call the DL_DATA.request with the properly formed CLPDUs.

4.4.2.3 CL-DATA.confirm

Function

This optional service primitive is invoked by the convergence layer to confirm to the service user DLMS/COSEM application layer the result of the previous CL-DATA.request service. The service represents a local confirmation only.

Service parameters

```

CL-DATA.confirm {
    Data_link_communication_parameters,
    Transmission_status
}

```

Data_Link_communication_parameters are transparently passed from the DL-DATA.confirm; definition of these parameters is given in CLC/TS 50568-4:2015, Clause 5.

Transmission_status is local confirmation of transmission status, *Transmission_status* == OK means that the PDU has been correctly transmitted. No indication on the reception status of the peer entity is given.

Use

If implemented, this service primitive is used to confirm the result of a previous CL-DATA.request. It is locally generated and indicates that the complete *Data* of the .request primitive could be correctly sent or not. In case of segmentation, the confirm is invoked after sending the last segment.

An CL-DATA.confirm with Result == OK means only that the Data has been sent, and does not mean that the Data has been (or will be) successfully delivered to the destination.

4.4.2.4 CL-DATA.indication

Function

This service primitive is invoked by the DLMS/COSEM application Layer to indicate to the service user DLMS/COSEM application layer that an APDU has been received from a remote application layer.

Service parameters

CL-DATA.indication {

SSAP,

DSAP,

Data_length,

Data

}

SSAP is the Service Access Point of the originating entity, it is transparently passed to the peer application layer entity.

DSAP is the Service Access Point of the destination entity, it is transparently passed to the peer application layer entity.

Data_Length is the length of the APDU to be transferred to the peer application layer entity.

Data is the APDU to be transferred to the peer application layer entity.

Use

The CL-DATA.indication service primitive is used to indicate to the service user DLMS/COSEM application layer that an APDU from the peer layer entity has been received.

The primitive is generated following the reception of all the segments composing an APDU by the B-PSK Data Link layer. If not all the segments have been correctly received the APDU is discarded.

4.4.3 Protocol specification for the DLMS/COSEM SMITP B-PSK-based transport layer

4.4.3.1 The convergence layer protocol data unit (CLPDU)

There are two CLPDU formats, the Type 1, depicted in Figure 4, is used to transfer the first segment of each APDU, the Type 2, depicted in Figure 5, is used for the following segments if any.

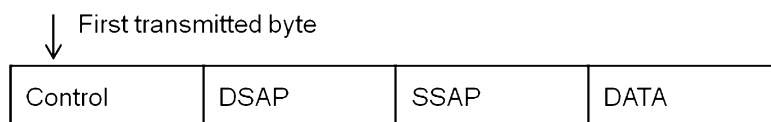


Figure 4 – Type 1 CLPDU format

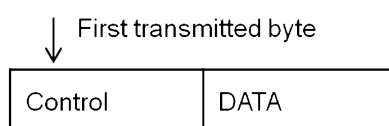


Figure 5 – Type 2 CLPDU format

DSAP

The DSAP address field identifies the service access point for which the data field is intended.

SSAP

The SSAP address field identifies the specific service access point from which the Data field was initiated.

Control Field

The Control field consists of one byte; it is formatted as indicated in Figure 6

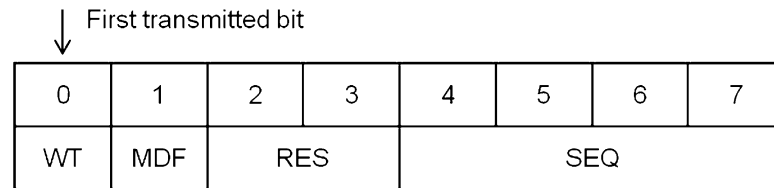


Figure 6 – Control field format

WT (CLPDU Type) can assume two different values:

- WT=0 in frames using Type 1 format;
- WT=1 in frames using Type 2 format.

MDF (More Data Follow) can assume two different values:

- MDF=0 if the frame is the last one in a sequence in this direction;
- MDF=1 if there are other APDU segments which needs to be sent in the same direction.

RES is a 2 bit field of value 00.

SEQ is the sequence number of the current segment, the numbering always starts from 0. In case the APDU is accommodated in only one frame the SEQ field assumes value 0.

Data

Data is the APDU segment to be transferred to the peer application entity.

4.4.3.2 Maximum transfer unit size and segment size

The theoretical maximum transfer unit (MTU) size is composed of 16 segments of the maximum length, one with Type 1 header and 15 with Type 2 header. It is possible for an implementation to limit the MTU to a lower value, given that the minimum allowed size is 242 bytes.

Given that the complete APDU shall accommodate in no more than 16 segments, the decision about the number of segments and the size of each segment is left to the transmitter side implementation.

Provided the minimum size specified above, the MTU size is implementation dependant, and it is noticed to the AL using the CL_mtu_size variable (see Annex D).

4.4.3.3 Exchange of frames not requiring segmentation (confirmed service)

4.4.3.3.1 General

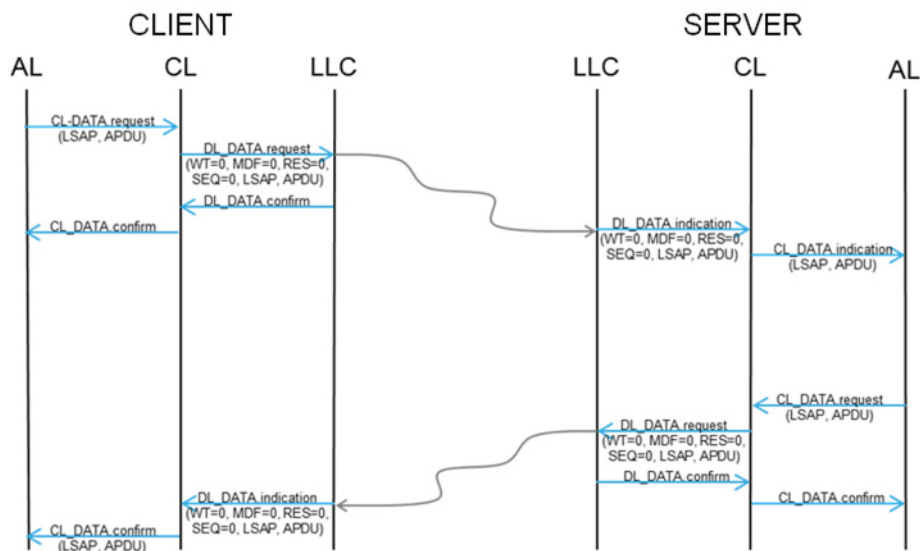


Figure 7 – Sequence chart of a CL transfer not requiring segmentation

4.4.3.3.2 Client transmitting phase

At client side, upon reception of a CL-DATA.request from the application layer entity, a single CLPDU is generated. Type 1 frame is used where control field has the following format:

(WT = 0, MDF = 0, RES = 0 SEQ = 0)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters (see CLC/TS 50568-4:2015, Clause 5):

(ECTL = 0x00, Service_class = RA or RB, Max_resp_len = CL_mtu_size)

CL_mtu_size specified in the DLDATA.request invocation is the one of the addressed server, and not the one specified in the client.

At the reception of DL-DATA.confirm an optional CL-DATA.confirm can be generated.

4.4.3.3.3 Server transmitting phase

At Server side the reception of a DL-DATA.indication triggers a CL-DATA.indication, the convergence layer is put in a state on which it waits for a CL-DATA.request issued by the application layer entity.

At the reception of the CL-DATA.request primitive the convergence layer generates a CLPDU. Type 1 frame is used where the control field has the following format:

(WT = 0, MDF = 0, RES = 0 SEQ = 0)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x00)

The resulting frame exchange is showed in Figure 7.

4.4.3.4 Exchange of frames requiring segmentation (unconfirmed service)

4.4.3.4.1 General

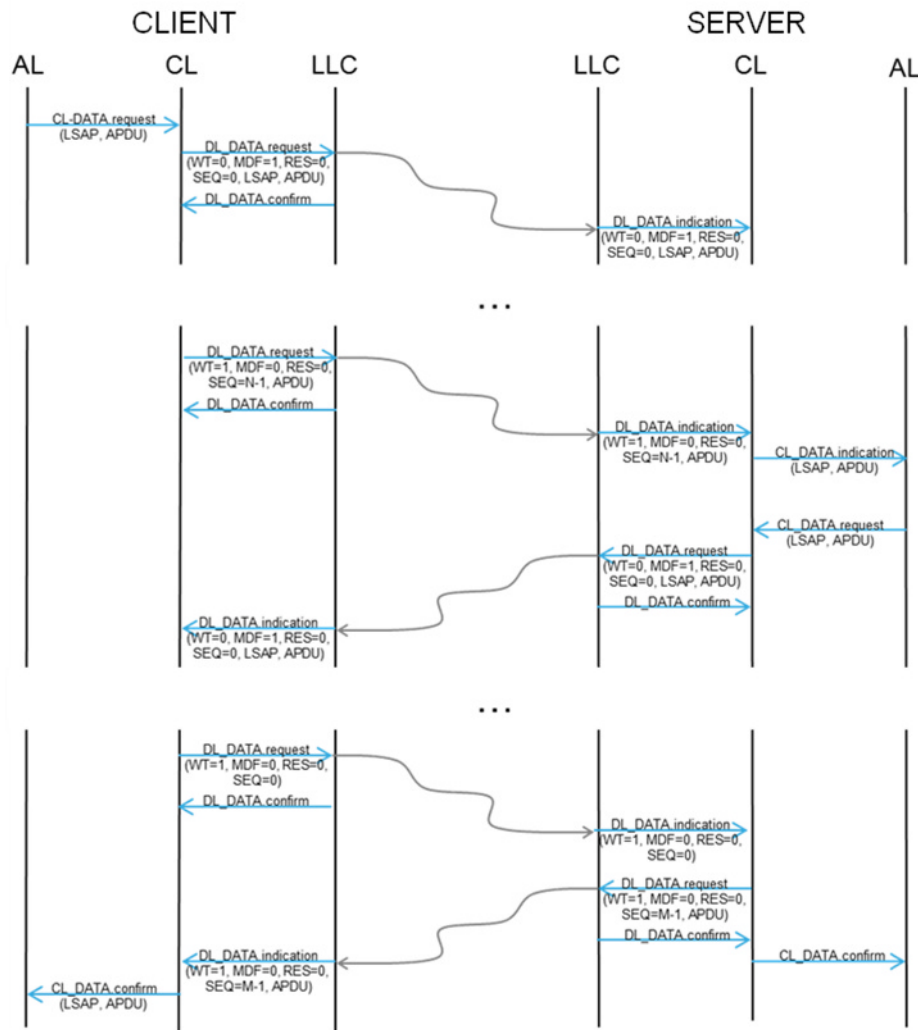


Figure 8 – sequence chart of a CL transfer requiring segmentation at both sides

At client side, upon reception of a CL-DATA.request from the application layer entity, the APDU is segmented in N segments, the resulting data exchange is described below and showed in Figure 8 .

Provided that DL layer already provides a procedure to ensure point to point reliable communication, based on acknowledge and retransmission mechanisms, no lost segment recovery mechanism is provided with this specification.

The behaviour of the Client and Server systems in case of loss of segments is described in 4.4.3.6.

4.4.3.4.2 Client in transmitting phase

At first the client side convergence layer generates a CLPDU with the first segment to be sent, CLPDU shall use frame type 1 where control field has the following format:

(WT = 0, MDF = 1, RES = 0 SEQ = 0)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000, Service_class = RA or RB, Max_resp_len = CL_mtu_size)

At the reception of the DL-DATA.indication, the server side convergence layer generates a CLPDU with no data (this is used to acknowledge the reception of a segment to the client), the CLPDU shall use type 2 where control field has the following format:

(WT = 1, MDF = 0, RES = 0 SEQ = 0)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000)

At client side, at the reception of the DL-DATA.indication a CLPDU containing the second segment of data is generated. CLPDU shall use frame type 2 is used where the control field has the following format:

(WT = 1, MDF = 1, RES = 0 SEQ = 1)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000, Service_class = RA or RB, Max_resp_len = 1)

The server side generates again a CLPDU with no data and the same format as before.

After the transmission of the N-1th segment, at the reception of the DL-DATA.indication, the client convergence layer generates the last CLPDU of this transaction. The CLPDU shall use frame type 2 where control field has the following format:

(WT = 1, MDF = 0, RES = 0 SEQ = N-1)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000, Service_class = RA or RB, Max_resp_len = CL_mtu_size)

4.4.3.4.3 Server in transmitting phase

At the reception of the last segment, which can be verified by checking the value of MDF field in the control byte, the server side convergence layer issues a CL-DATA.indication to the application layer entity passing the re-assembled ADPU.

Upon reception of a CL-DATA.request the APDU is segmented in M segments.

The convergence layer generates a CLPDU with the first APDU segment. The CLPDU shall use frame type 1, where control field has the following format:

(WT = 0, MDF = 1, RES = 0 SEQ = 0)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000)

At the reception of the DL-DATA.indication the client side convergence layer, basing on the MDF bit of control field, generates a CLPDU with no data. The CLPDU shall use frame type 2 where control field has the following format:

(WT = 1, MDF = 1, RES = 0 SEQ = 0)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000, Service_class = RA or RB, Max_resp_len = CL_mtu_size)

After the transmission of the M-1th segment, at the reception of a DL-DATA.indication, the server side convergence layer generates the last CLPDU of the transaction and optionally issues a CL-DATA.confirm to the application layer entity. The CLPDU shall use frame format 2 where control field has the following format:

(WT = 1, MDF = 0, RES = 0 SEQ = M-1)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000)

Upon reception of the corresponding DL-DATA.indication the client side convergence layer issues a CL-DATA.indication to the application layer entity passing the re-assembled APDU.

4.4.3.5 Exchange of frames requiring segmentation (unconfirmed service)

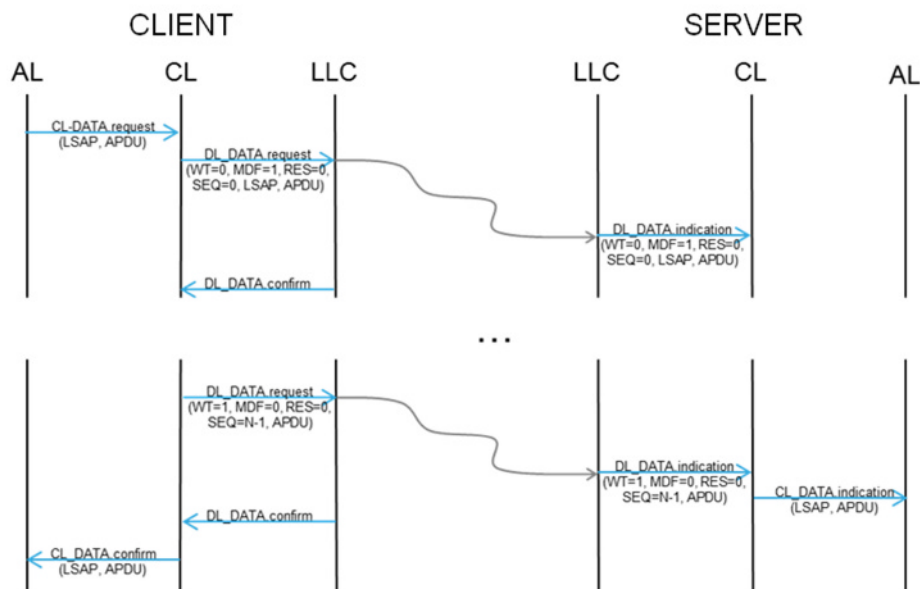


Figure 9 – sequence chart of a CL transfer requiring segmentation using the unconfirmed service

At client side, upon reception of a CL-DATA.request from the application layer entity, the APDU is segmented in N segments, the resulting data exchange is described below and showed in Figure 9.

At first the client side convergence layer generates a CLPDU with the first segment to be sent, CLPDU shall use frame type 1 where control field has the following format:

(WT = 0, MDF = 1, RES = 0, SEQ = 0)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000, Service_class = S)

Since DL is using an unconfirmed service (Service Class S), postponed confirmation is used, so as soon as the client DL issues the corresponding DL-DATA.confirm primitive the CL can transmit the next segment of the APDU, so a CLPDU containing the second segment of data is generated. CLPDU shall use frame type 2 is used where the control field has the following format:

(WT = 1, MDF = 1, RES = 0, SEQ = 1)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000, Service_class = S)

After the transmission of the N-1th segment, at the reception of the DL-DATA.confirm, the client convergence layer generates the last CLPDU of this transaction. The CLPDU shall use frame type 2 where control field has the following format:

(WT = 1, MDF = 0, RES = 0, SEQ = N-1)

CL invokes a DL-DATA.request passing the CLPDU formed as above mentioned, using the following parameters:

(ECTL = 0x0000, Service_class = S)

4.4.3.6 Management of errors in the procedure

In case a malformed CLPDU is received or a DL-DATA.confirm with negative result is issued by the data link, the transaction shall be terminated, whether this event is notified to the application layer entity and how is summarized in the table below.

Table 1 – Convergence layer error management scheme

Side	Status	Event	Actions
Client	Transmitting/receiving	DL-DATA.confirm with negative result	Optionally issues a CL-DATA.confirm with negative result. Abort transaction
Client	Transmitting/receiving	Reception of a malformed CLPDU	Optionally issues a CL-DATA.confirm with negative result. Abort transaction
Server	Transmitting/receiving	DL-DATA.confirm with negative result	Optionally issues a CL-DATA.confirm with negative result. Abort transaction
Server	Transmitting/receiving	Reception of a malformed CLPDU	Optionally issues a CL-DATA.confirm with negative result. Abort transaction.

A CLPDU is considered malformed if:

- The control field is not consistent with what described in 4.4.3.1:
- The SEQ number is different from what was expected.

In case a malformed CLPDU is received at Server side, where the CLPDU can be interpreted as the initial segment of a new transaction (SEQ == 0), the Server system can decide whether to ignore this CLPDU or to consider it as new transaction having aborted the previous one.

4.5 Application layer

The application layer is the DLMS/COSEM application layer as specified in EN 62056-5-3. It provides services to the COSEM application process (AP) and uses the services of the convergence layer.

4.6 Application process

4.6.1 General

On the server side, the COSEM device- and object model – as specified in EN 62056-6-2 applies. Each logical device represents an AP.

The client side APs make use of the resources of the server side AP. A physical device may host one or more client APs.

4.6.2 Establishing application association

The AAs can only be established with server systems properly registered to the NNAP. By a communication point of view a server node is properly registered when it is configured within the client system that is the master node of the sub network, and the MAC layer address is assigned to the server node by the master node itself.

A pre-established AA can also be used once the registration procedure has been successfully completed.

The mechanisms for discovery and registering of server nodes are described in the following 4.7.

4.6.3 Releasing application association

As the LLC sublayer supporting the DLMS/COSEM application layer is connectionless, the COSEM-Release service may be invoked with the Use_RLRQ_RLRE option = TRUE to release an AA.

To secure the RLRQ APDU against denial-of-service attacks – executed by unauthorized releasing of the AA – the user-information field of the RLRQ APDU may contain the xDLMS InitiateRequest APDU, authenticated and encrypted using the AES-GCM-128 algorithm, the global unicast encryption key and the authentication key (the same as in the AARQ APDU).

4.6.4 Service parameters of the COSEM-OPEN, -RELEASE and -ABORT services

No specific features / constraints apply related to the usage of COSEM-OPEN, -ABORT and -RELEASE services.

4.6.5 Transporting messages

Unsolicited services are not supported in this profile,, no other specific features / constraints apply related to the usage of DLMS/COSEM client/server services.

4.6.6 Transporting long messages

In the SMITP B-PSK profile, the LLC sub layer imposes a limitation on the length of the payload that can be transported. To remove this constraint, segmentation can be applied at the convergence layer and application layer block transfer is available.

4.6.7 Broadcasting

Broadcast messages can be sent by the data NNAP (concentrator), acting as a client, to servers using broadcast addresses as specified in in CLC/TS 50568-4:2015, Clause 6.

4.7 PLC network management

4.7.1 Introduction

PLC network management is provided by the Discovery and Registration Services, as described in Clause 8 of this document.

The discovery and registration services are the following:

- The Discover service;
- The Register service;
- The Deregister service
- The DiscoverForward service;
- The DiscoverReport service;
- The DiscoverForwardReport service;

- The RegisterReport service;
- The TCTset service;
- The Status service;
- The Ping service.

4.7.2 The Discover services

The Discover service is used to discover new meters. It is possible to use Discover service to discover meters which are already registered, in case they require an alternative route to improve the communication link, this is done properly managing the TCT value of the meters and the TCR parameter in the primitives.

The Discover services are used only when the active initiator is the concentrator, in those cases where the concentrator delegates a server to act as an active initiator, the DiscoverForward services shall be used.

The Discover service primitive shall provide the parameters as shown in 8.1.1.2. The concentrator shall issue a DL_DATA.request using multicast destination address and RCx Discipline without repeaters.

In order to guarantee the network communication stability the Client is allowed, at any time, to find alternate routes to reach a meter, even if it is already registered; for this reason the meter unit shall be able to answer to a DiscoverPDU even in case it is already registered; the allowance to answer to a DiscoverPDU is based uniquely in the filtering parameters specified for the Discover service. In case the meter is already registered it will accept DiscoverPDUs only if they originate from the Concentrator that has registered the meter.

4.7.3 The Register service

The Register service is used to perform meter configuration. It assigns a MAC address (the SCA) to an unregistered meter.

The Register service primitive shall provide the parameters as shown in 8.1.1.8. The concentrator shall issue a DL_DATA.request using unicast address and SAx Discipline.

4.7.4 The Deregister service

The deregister service is used to force a registered meter to become unregistered, the previously assigned SCA is no more valid and the concentrator can re-assign it to a newly registered meter other than the deregistered one.

The Deregister service primitive shall provide the parameters as shown in 8.1.1.10. The concentrator shall issue a DL_DATA.request using unicast address and RAx Discipline.

4.7.5 The DiscoverForward service

The DiscoverForward service is used to discover meters which are not reachable by the concentrator, or when the communication link with the concentrator is not reliable. Using this service the concentrator delegates a meter to become an active initiator, providing a remote discover service originating from the selected meter.

The meter which receives a DiscoverForwardService issues a DiscoverPDU equivalent to the one generated by the Concentrator.

The DiscoverForward service primitive shall provide the parameters as shown in 8.1.1.5. The concentrator shall issue a DL_DATA.request using unicast address of the receiver as repeater address, multicast address as destination address, and RCx Discipline with repeaters

4.7.6 The DiscoverReport service

The DiscoverReport service is used as a response to the Discover service at meter side, only meters matching the filtering criteria specified by the Discover service (TCR, AddToAddress and RightShiftAdd) shall use this service.

The DiscoverReport service primitives shall provide the parameters as shown in 8.1.1.3. The meter shall issue a DL_DATA.request using unicast address and Sx Discipline.

4.7.7 The DiscoverForwardReport service

The DiscoverForwardReport service is used as a response to the DiscoverForward service at meter side; only meters matching the filtering criteria specified by the DiscoverForward service (TCR, AddToAddress and RightShiftAdd) shall use this service.

The DiscoverForwardReport service primitive shall provide the parameters as shown in 8.1.1.6. The meter (which is the destination system of a previously issued DiscoverForward service) shall issue a DL_DATA.request using unicast address and Sx Discipline.

4.7.8 The RegisterReport service

The RegisterReport service is used as a response to the Register service at meter side.

The RegisterReport service primitive shall provide the parameters as shown in 8.1.1.9. The meter shall issue a DL_DATA.request using unicast address and Sx Discipline.

4.7.9 The TCTset service

The TCTset service is used by the concentrator to silence a meter which has been already discovered, to prevent that it answers to the following discover requests. Its value has only a relative meaning, since it defines the maximum level of TCR (see 8.1.1.2 and 8.1.1.5) at which a meter is allowed to answer a Discover or a DiscoverForward request.

The TCTset service primitive shall provide the parameters as shown 8.1.1.4. The concentrator shall issue a DL_DATA.request using unicast address and Rx Discipline.

4.7.10 The Status Service

The Status service is used to acknowledge the TCTset, the DiscoverForward, the Deregister and the Ping services.

The Status service primitive shall provide the parameters as shown in 8.1.1.7. The meter shall issue a DL_DATA.request using unicast address and Sx Discipline.

4.7.11 The Ping service

The Ping service is used to check that a meter is already registered and still present on the network. It also allows verifying that the right physical device is linked to the right MAC address. It also prevents the time_out_no_activity timer to expire.

The process starts with a Ping.request service primitive issued by the concentrator. The service contains the ACA of the physical device pinged.

The Ping service primitive shall provide the parameters as shown in 8.1.1.11. The originating system shall issue a DL_DATA.request using unicast address and Rx Discipline.

4.7.12 Applying filtering criteria to Discovery procedure

The Discover and the DiscoverForward services allow a pre-selection on the meters which are allowed to answer with the appropriate Report service, this filtering action can be applied to the phase where the PLC modem of the meter is connected to, the ACA address of the meter or to an internal parameter, the so called TCT.

If requested by the initiator only the meters which have the PLC modem connected to the phase used for the transmission of the message containing the Discover, or DiscoverForward, service shall answer to the request and perform the discovery process.

Filtering on ACA address is performed through two parameters (AddToAddress and RightShiftAdd) in this way: the receiver adds to its ACA the AddToAddress parameter, then it divides the result by $2^{RightShiftAdd}$, if the remainder of this division is zero then the meter is allowed to answer to the request and perform the discovery process.

Filtering on TCT is used to prevent already discovered meters from answering to the discovery requests. Every meter has an internal parameter, the so called TCT, which has a default value of 255, a system is allowed to answer to the request only if TCR parameter specified on it is lower than its TCT value. The TCT value of each node can be changed using the TCTset service.

4.7.13 Meter discovery procedure

4.7.13.1 General

Since the B-PSK DL is managed following a strict master-slave policy, the Concentrator (that is the master of the network) keeps the control of the entire procedure.

NOTE The implementation of such a procedure is up to Concentrator manufacturer, so that, using the Discovery and Register services, it can build the procedure with the best performance.

Discovery and Register services are described in Clause 8 of the document.

An example of meter discovery procedure is shown in Annex A.

4.7.13.2 Routing table updating

Preliminary remarks:

- meter discovery procedure can run periodically in background on the Concentrator, in order to monitor any new meter installed on the network or any meter that become “unregistered” (after Activity_timeout seconds without any activity on the PLC);
- when a meter is not polled from the Concentrator for an adequate and configurable amount of time, it sets to zero the value of his SCA address (ad-hoc modelled timeout register). In this way it declares itself unregistered.

Case A: a new meter is discovered.

When a Concentrator, during the discovery procedure, finds a new meter, it communicates to AMM system its ACA address in order to receive the authorization to register it.

Case B: a meter became inaccessible.

When the Concentrator is not able to communicate with a meter, following an adequate algorithm it executes a certain number of retries.

Any Concentrator manufacturer is free to build and optimize such a procedure. A configurable inaccessibility timeout should be implemented within the Concentrator in order to monitor the connection with each PLC node. When such a timeout expires the Concentrator could notify the problem to the AMM system that verifies if a lost meter has been, for example, associated to another Concentrator (in case of high level network reconfiguration due to maintenance works). In this case, the AMM could ask to the first Concentrator to unregister that meter from its database. Otherwise it could require the Concentrator to perform again the discover procedure or set it in local maintenance addressed to field operators.

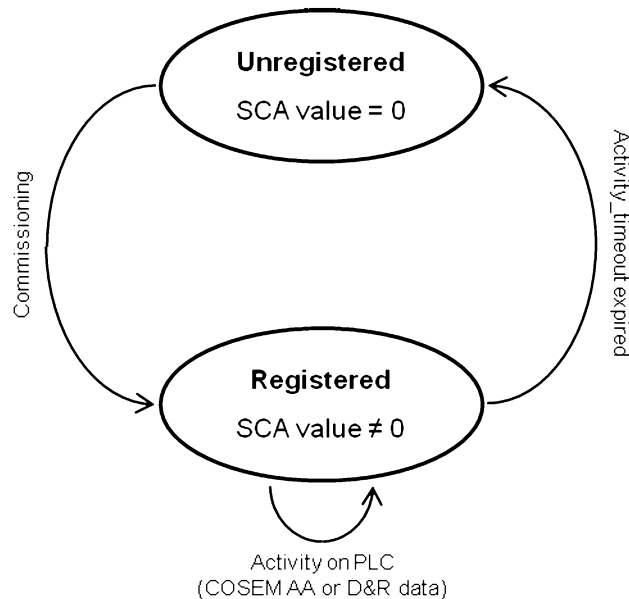


Figure 10 – Meter's state diagram

Changes on the network topology, moving more meters from one Concentrator to another one (e.g. in case of maintenance activities during a long period) is performed automatically when a Concentrator is turned off. In fact, when a concentrator is turned off, it stops polling his meters; in this way the meters turn themselves to unregistered state and they become available to respond to a meter discovery procedure started by another Concentrator.

4.8 Addressing

Each node in the PLC network can be addressed using either an absolute communication address (ACA) or a section communication address (SCA). ACA is fixed and globally unique for each node and, in general, it is used during the network initialization phase. SCA is assigned by the network controller, which guarantees its uniqueness in every PLC network. ACA and SCA addresses are managed at MAC layer level.

ACA is a unicast address.

SCA provides two-level addressing inside the PLC network, which are identified by:

- Node subsection;
- Node progressive.

It is possible to define SCA multicast addresses at node subsection level and SCA broadcast addresses. Details on the addressing scheme are given in CLC/TS 50568-4:2015, Clause 6.

4.9 System variables

CL_MTU_Size is the maximum transfer unit size (in bytes) the system can manage through CL-DATA services.

Timeout_no_activity is the amount of time a system should wait from the last activity on the PLC before re-setting its TCT value to the default value of 255.

TCT is the silencing level of the node, any request of discovery having a TCR level higher than the TCT level of the system shall be ignored.

5 The Original-SMITP B-PSK PLC profile

5.1 Overview

The PLC profile based on B-PSK modulation is used for remote data exchange on Neighbourhood Networks (NN) between Neighbourhood Network Access Points (NNAP) and End Devices using B-PSK power line technology over the low voltage electricity distribution network as a communication medium.

End devices – typically electricity meters – comprise application function and communication functions. They may be connected directly to the NNAP via the C interface.

The NNAP device, also known as Concentrator, is connected upstream to the Metering Head End System (HES) through interface G.

The reference architecture is shown in Figure 11.

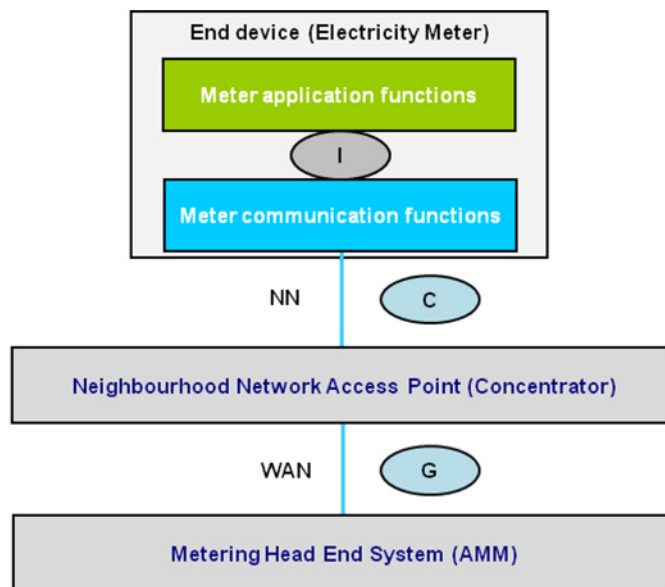


Figure 11 – Reference communication architecture

5.2 Structure of the profile

The protocol stack for PLC profile based on B-PSK modulation is shown in Figure 12.

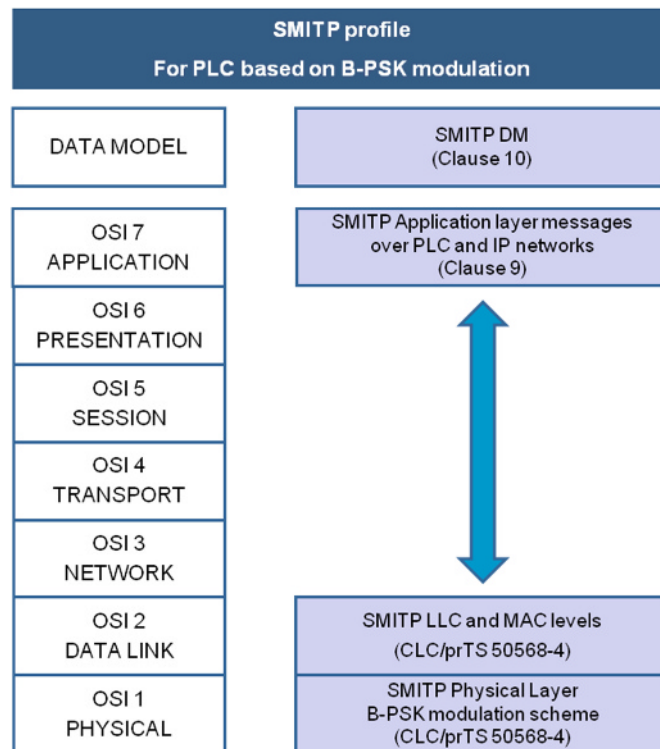


Figure 12 – Protocol stack for SMITP on PLC

5.3 Physical layer

5.3.1 Introduction

The SMITP Physical layer is described in CLC/TS 50568-4:2015.

The physical layer provides the interface between the equipment and the physical transmission medium. It transports binary information from the source to the destination.

In transmission it performs the coding and encapsulation of the payload in a physical frame, the 32 bit CRC calculation and the modulation in Binary Phase Shifting Key (B-PSK) at 4800 bps.

In reception it performs bit, byte and frame synchronization, the demodulation of the frame (B-PSK), the decoding of the payload and CRC checking. It makes a signal to noise ratio (SNR) estimation.

5.3.2 Crosstalk management

In the SMITP system, the Concentrator initiates the communication to the meters, which have been detected by the discovery mechanism (see par.5.7.1). The Concentrator is connected to all three phases, which are managed independently for communications, and since the phase of the meter is known, it establishes communications to each meter over this specific phase. Nevertheless, there are particular cases where a Concentrator cannot reach a meter in a direct way over the correct phase, but only via a crosstalk connection to another phase; in this case, the Concentrator recognizes during the discovery process that the meter is not reachable through its corresponding phase, but via another phase, and then manages the connection via cross talk correctly.

Concerning cross talk with other Concentrators, each Concentrator manages only the meters that are present in its Meter addresses table, established during the discovery procedure, and no others, so it will never try to reach a meter that is out of its domain. In this way the crosstalk (which is always possible in a Power Line Network) does not introduce any interference problem between a Concentrator and a meter bound by another one.

5.3.3 Communication performance assessment and management

Communication performance related to a meter is assessed by a Concentrator, for example counting the percentage of responses of the meter to the Concentrator's requests. If the percentage of responses is under a predefined threshold, it is up of the Concentrator to find a better path to reach it, using the mechanism of the meter discovery procedure (see 5.7.1).

5.4 Data Link layer

The SMITP Data Link layer is described in CLC/TS 50568-4:2015.

It consists of two sublayers: the Medium Access Control (MAC) sublayer and the Logical Link Control (LLC) sublayer.

The MAC sublayer handles the access to the physical medium and provides physical device addressing. It provides repetition and physical interfacing functionalities.

The repetition functions are:

- an end-to-end connectionless service between master node and all the net slave nodes;
- timers management related to net busy condition in master nodes and repeaters.

The physical interfacing functions are:

- frame encapsulation;
- received frames filtering, on the basis of a single or grouped address;
- frame errors detection. Wrong frames are rejected (no error recovery);
- electric phase connectivity detection.

The access mode to the physical medium is half-duplex.

LLC sub-layer interfaces the Application layer on the upper side and the MAC sub-layer on the lower side; it shall perform the following functions:

- it is responsible about the execution of end-to-end exchange procedures to guarantee a correct access procedure that avoids any possible collision on the net (in any moment a single node can ask a transmission request on MAC level); it manages access times to the LV communication on the master node;
- it operates end-to-end between the master node and all the net slave nodes; it offers a connectionless-type service to equipment applications, according to the kind of exchange procedure required;
- in the master node, it indicates net availability to application; user can request transmission of another message, upon reception of this indication;
- in the master nodes it manages re-transmissions (retry) on exchanges with expected answer. The mechanism of retransmission is vendor specific.

LLC sub-layer does not check the correctness of the disciplines used by the application layer; it is applications care to use discipline properly.

5.5 Application layer

The SMITP Application layer is described in Clause 9.

It provides the set of messages exchanged between the nodes present on the low voltage net. Three different types of nodes are foreseen:

- Concentrator: is the master of the net; there is always one and only one Concentrator for each section (identifier of the network managed by Concentrator).
- A-Node: is a peripheral unit which can communicate with the Concentrator (in this case it acts as slave) or with an associated B-Node (in this case it acts as master). The A-nodes are typically the meters.

- B-Node: is a peripheral unit which can communicate with the Concentrator or with an associated A-Node; it always acts as slave. It is typically the end customer device.

The application layer provides the services needed to manage meters and end customer devices:

- parameters programming activity, with access to SMITP data model;
- data exchange activity, with access to SMITP data model;
- software download;
- acknowledgements of requests or actions;
- remote command execution;
- encryption and authentication.

It also provides the services to manage the network.

NOTE For the identification codes of the mentioned messages in the following clauses, please, refer to Clause 9.

5.6 SMITP Data model

The SMITP Data model is described in Clause 10.

By an abstract point of view, the SMITP Data Model consists of data grouped in tables, each table representing an homogeneous set of parameters (registers). Each parameter can be accessed with specific rights (writable/not writable and readable/not readable) depending of the nature of the data.

These data can be retrieved individually, in sets of logically bound data (entire tables) or by user defined sets of data (Custom tables), allowing a fast and flexible scheme of data access.

Data retrieving is possible through Table ID, which is used to identify uniquely a SMITP table, and Register ID, which is used to identify uniquely a register within a SMITP table.

5.7 Application process

5.7.1 Meter discovery procedure

Because the SMITP network is managed following a strict master-slave policy, the Concentrator (that is the master of the network) keeps the control of the entire procedure. The implementation of such a procedure is up to Concentrator manufacturer, so that, using the features and messages available in the protocol (application layer) , he can build the procedure with the best performance.

Discovery services are described in Clause 8 of the document.

An example of meter discovery procedure is showed in Annex B.

5.7.2 Routing table updating

Preliminary remarks:

- meter discovery procedure can run periodically in background on the Concentrator, in order to monitor any new meter installed on the network or any meter that become “orphan” (ad-hoc modelled timeout register).
- when a meter is not polled from the Concentrator for an adequate and configurable amount of time, it sets to zero the value of his SCA address (ad-hoc modelled timeout register). In this way it declares itself orphan.

Case A: a new meter is discovered.

When a Concentrator, during the discovery procedure, finds a new meter, it communicate to AMM system its ACA address in order to receive the authorization to register it.

Case B: a meter became inaccessible.

When the Concentrator is not able to communicate with a meter, following an adequate algorithm (any Concentrator manufacturer is free to build and optimize such a procedure) it executes a certain number of retries.

Only in case of a long time inaccessibility, the Concentrator could notify the problem to the AMM system. When the AMM system receives this kind of alert from a Concentrator, it verifies if the lost meter was, for example, associated to another Concentrator (in case of high level network reconfiguration due to maintenance works). In this case, the AMM could ask to the first Concentrator to delete the meter from its routing table. Otherwise it could translate the Concentrator's message in a local maintenance request addressed to field operators.

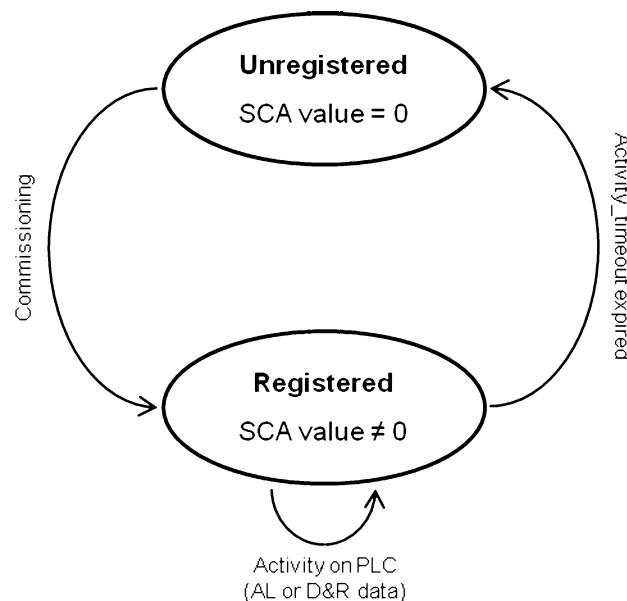


Figure 13 – Meter's state diagram

Changes on the network topology, moving more meters from one Concentrator to another one (e.g. in case of maintenance activities during a long period) is performed automatically turning off a Concentrator. In fact, when a concentrator is turned off, it stops polling his meters; in this way the meters turn themselves to orphan state and they become available to respond to a meter discovery procedure started by another Concentrator.

5.7.3 Meter's clock synchronization

For the correct operation of the system, all registered meters should be synchronized with an external temporal reference that comes from the Central System or AMM system. The Concentrators store this reference for their own synchronization and it should be sent periodically to the meters.

The meters store the current date and time that can be modified through a writing message WRITE.REQ (without/with protection).

The WRITE.REQ message without protection can only be used in the following cases:

- the node clock has never been synchronized;
- node lost every temporal reference (i.e. power fail, HW fail ...);
- the deviation between the Concentrator time and the node time is smaller than a predetermined value.

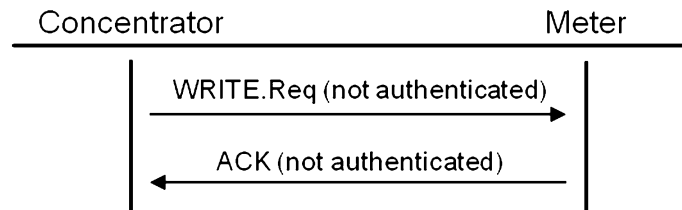


Figure 14 – Synchronization without protection

If any of the described conditions is fulfilled, the writing of the register should be done through a protected message WRITE.REQ.

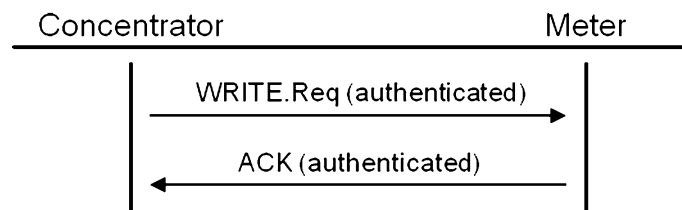


Figure 15 – Synchronization with protection

5.7.4 Reading and writing operations

5.7.4.1 Primitives for SMITP data model

It is possible to execute reading and writing operations on meter registers from the Concentrator via a sequence of application layer messages. Meter registers are organized in tables and to access a register (both for reading and writing) a 2 byte code is needed (1 byte for Table ID and 1 byte for Row ID).

Reading and writing operations can be authenticated, so each primitive has an equivalent version in case the authentication mechanism is active.

5.7.4.2 Reading operations

A reading operation is made through the primitive READ.REQ for individual registers (002 without protection, 102 with protection), READTAB.REQ (006/106) specific for several registers belonging to the same table and READTAB.REQ (008/108) for entire table data.

In case the reading is satisfactory, the Concentrator receives from the meter the response messages READ.RESP (003/103), READTAB.RESP (007/107) and READTAB.RESP (009/109) containing the requested data inside the payload.

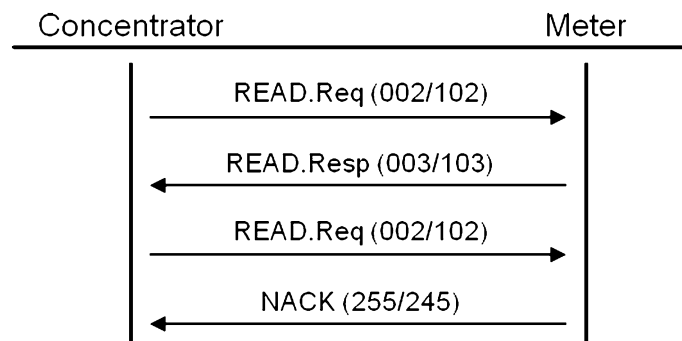


Figure 16 – Individual registers reading

If there is any problem on the reading operation, the meter will respond with a NACK message (255 without authentication, 245 with authentication) indicating the corresponding error code.

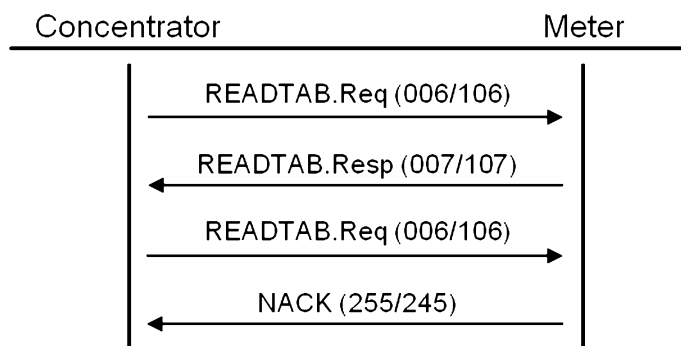


Figure 17 – Table registers reading

5.7.4.3 Writing operations

A writing operation is made through the primitive WRITE.REQ (004/104) for individual registers, WRITETAB.REQ (010/110) for several registers belonging to the same table.

In case the writing operation is satisfactory, the Concentrator receives from the meter an ACK message (253/243). Otherwise, if there is any problem on the writing, it receives a NACK message (255/245) with the corresponding error code.

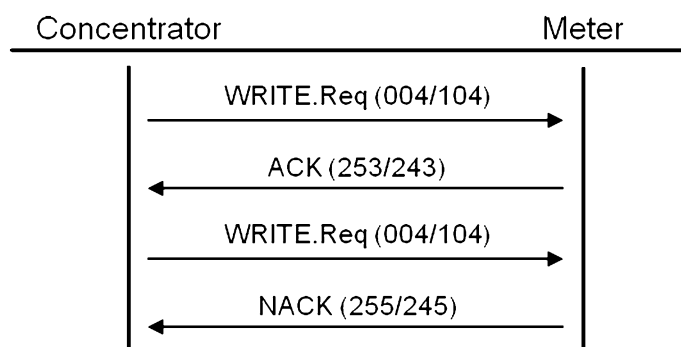


Figure 18 – Individual registers writing

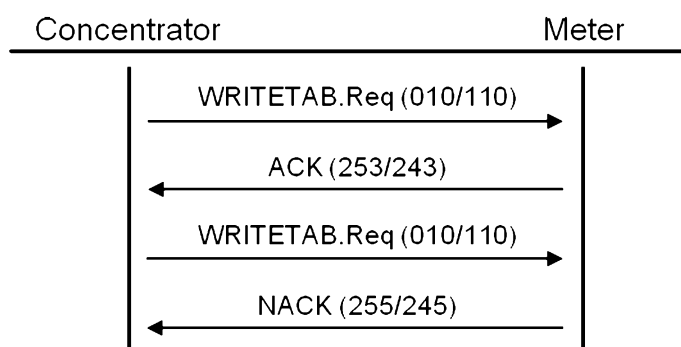


Figure 19 – Table registers writing

5.7.5 Download procedure

The meter software update is possible due to the available messages at the application layer for the control of this task. The stored/handled information is the following (acronyms are for used for concision of description):

- FRFPN: Final packet number. It shows the last packet of firmware that the meter should receive.

- SWOT: Switchover time. It shows the date at which the meter will proceed to activate the firmware loaded through the procedure.
- FRAD: Digest of the entire firmware. It is used by the meter to check the integrity of the received firmware.
- FRCW: to control and monitor the download procedure in case of writing or reading. While for writing it works as a way of sending commands to control the downloading procedure, on reading gives a sequence of status indicators (mask of bits) of the procedure so that the written values cannot be recovered again. The values to be considered on the mentioned information are:
 - WRITE:
 - STARTLOAD: it starts the procedure of charge. Activate the INPROGRESS bit and delete the remaining control bits.
 - ABORTLOAD: it aborts the procedure of charge. It deletes all the control bits.
 - READ:
 - INPROGRESS: it indicates if there is a procedure of load in execution. It is deleted when a STARTLOAD is received or a SWITCHREADY is activated.
 - RECEIVEDALL: it indicates that all the packets have been received and that activation date can be written. It is deleted when the STARTLOAD or ABORTLOAD commands are written.
 - DIGESTERR: it indicates that it has been detected an error in the digest firmware calculation regarding the FRAD value. It is deleted when the STARTLOAD or ABORTLOAD commands are written.
 - SWITCHREADY: ready to launch the switchover. It is activated after RECEIVEDALL activation and digest checking against FRAD value. It is deleted when the STARTLOAD or ABORTLOAD commands are written.
 - SWITCHDONE: it indicates that the switchover was done correctly.

The firmware update procedure consists of the following steps:

- 1) Update of the FRFPN and FRAD info indicating the final packet number and the complete firmware digest;
- 2) Update of the FRCW info with the command STARTLOAD corresponding value. If FRCW is read we will receive the INPROGRESS flag;
- 3) sending firmware packets using application layer REPROG messages to update a node. These messages are sent using SCA addressing, so meters have to be registered in the Concentrator. In case of broadcast programming, when the Concentrator finishes sending all the packets, it checks in each meter if some packets has not been received. Then Concentrator continues sending REPROG messages transporting those firmware packets still not received. In case of local programming, if the packet is received correctly on the meter, it sends the corresponding ACK (not authenticated) message. Otherwise the meter sends no acknowledge message or a NACK (not authenticated) message and the Concentrator will send again the REPROG message with the same firmware packet;
- 4) once all firmware packets have been received correctly by the meter, the Concentrator updates SWOT with the desired date and time to activate the new firmware.

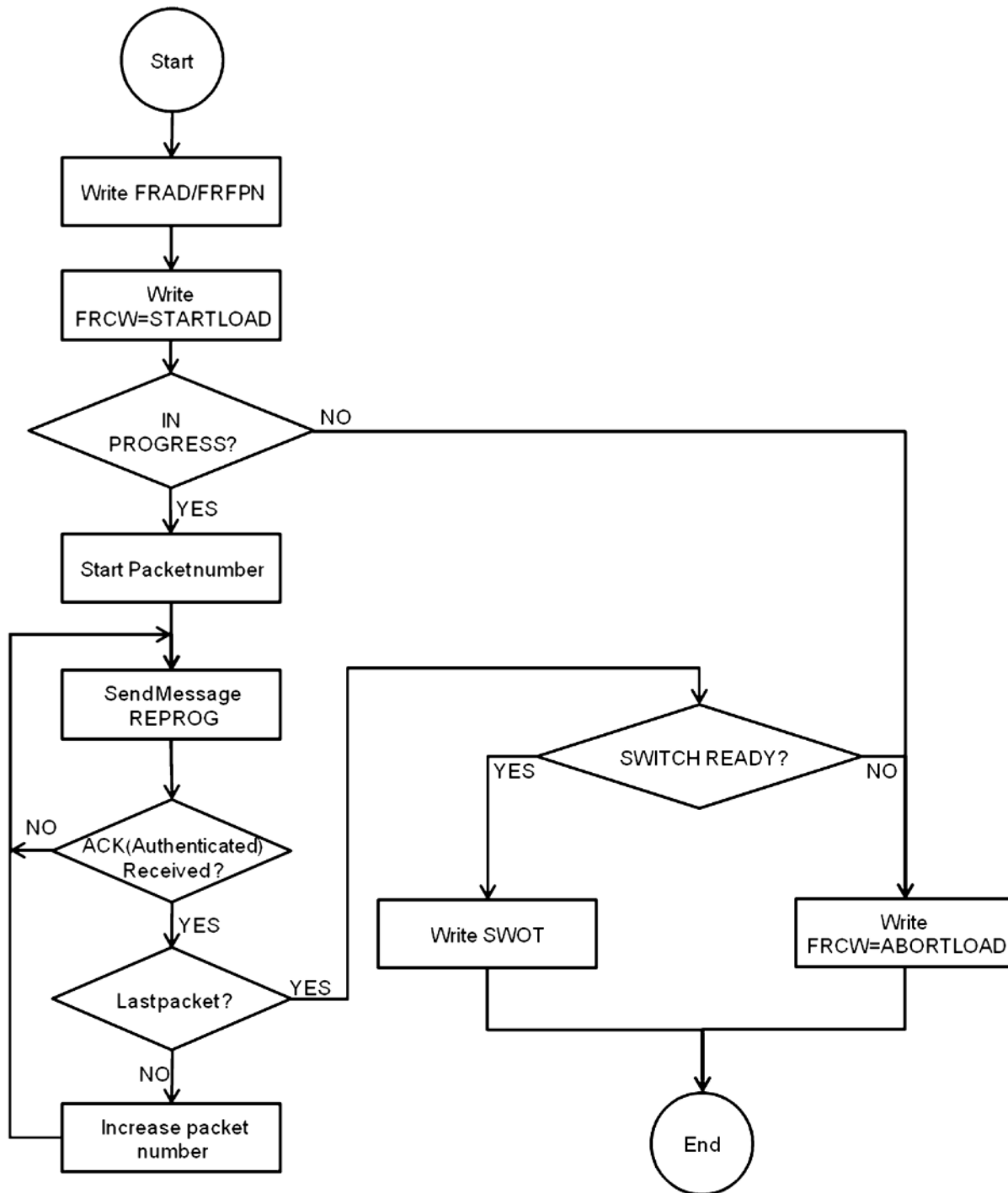


Figure 20 – Download procedure

5.7.6 Display management

5.7.6.1 Introduction

The meter shall display information of interest to the customer on a LCD module composed of 16 alphanumeric characters (5 x 7 dots) x 1 line and icons (special symbols or operating indicators).

The display is divided in two totally independent areas:

- Register Area (RegA): this area is used to show meter data. All the data elements contain:

- register Code Identifier (text label that may be assigned to the data registers to be identified on the display);
 - register Data Value;
 - register Data Measurement Unit.
- Operating Indicators Area (icons).

The operating indicators may be shown and refreshed in any moment, whatever data is being displayed in Register Area.

The Operating Indicators Area can indicate simultaneously the following information:

- quadrant in use;
- data unit for active and reactive energy/power;
- per phase: voltage and current presence;
- alarm condition indicator;
- PLC communication indicator;
- primary verification led in “reactive” mode;
- cut-off element open (this indication is placed at the most right-bottom position).

The control of the quadrant icons is based on the active (A) and reactive (R) energy measurements; therefore the highlighted icon shall be updated every change of the sign of A or R. At the start up of the meter the highlighted icon is based on the last measurement.

The active tariffs (one for each contract) are identified by means of a specific symbol that is placed close to the right side of the register Code Identifier when the related active energy register is shown in LCD idle mode. In any other LCD mode, this identification solution has not to be performed. This process will be performed only if a multi-tariff structure is active.

5.7.6.2 Display mode management

The meter handles and stores up to 240 messages. Each message is composed by 16 alpha-numeric symbols and by a set of control information used to define the related special characteristics described in the sections below.

The set of handled messages is shown on the LCD module of the meter according to the display configuration set by the operator. The way the messages are displayed is configured and is associated to the following transition events:

- Timeout event. Messages are shown after a programmable timeout. Four different timeouts can be defined (the configured value is readable) and assigned to specific info.
- Short press button event. Messages are shown when the front panel button is pushed for less than a programmable period of time.
- Long press button event. Messages are shown when the front panel button is pushed for more than a programmable period of time.

The meter implements special messages to be used in order to optimize the visualization of data related to measurements of different tariffs.

An example message structure is described below:

Table 2 – Example of message structure to be displayed

DSP						
DSP_SYM	DSP_CODING	MSG_ID	DSP_TEXT	DSP_SM	DSP_DIVIDE	DSP_SI

DSP_SYM: a set of flags corresponding to each special symbol to be displayed. When a flag bit is 1, the associated symbol is displayed.

DSP_CODING: code number of the data to be displayed.

MSG_ID: an unique message identification code assigned by the AMM system to each message structure in the table.

DSP_TEXT: contains the actual text to be displayed and it is comprised of 16 ASCII characters. A special character '}' is used to indicate where in the message the selected register has to be placed.

DSP_SM: if non-zero, it gives the number of one of the 104 special messages. They are pre-defined messages that are used in order to optimize the visualization of data related to measurements of different tariffs. An example would be a message to display the active tariff in conjunction with its associated value of the total consumption.

DSP_DIVIDE: number (power of 10) by which the absolute value held in the register is divided for.

DSP_SI: set of flags indicating special instructions for the message. These may include instructions to display the specified register as text or maybe to display leading zeroes.

6 The Original-SMITP IP profile

6.1 Overview

The PLC profile based on B-PSK modulation is used for remote data exchange on Neighbourhood Networks (NN) between Neighbourhood Network Access Points (NNAP) and End Devices using B-PSK power line technology over the low voltage electricity distribution network as a communication medium.

End devices – typically electricity meters – comprise application function and communication functions. They may be connected directly to the NNAP via the C interface.

The NNAP device, also known as Concentrator, is connected upstream to the Metering Head End System (HES) through interface G, via IP enabled networks.

The reference architecture is shown in Figure 21.

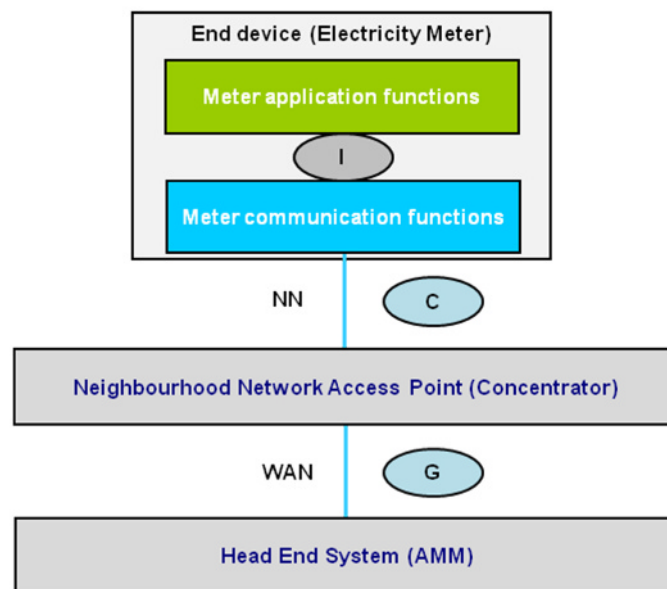


Figure 21 – Reference communication architecture

6.2 Structure of profile

Figure 22 shows the SMITP protocol stack on IP profile for the communication on a public network between the Central System and the Concentrator.

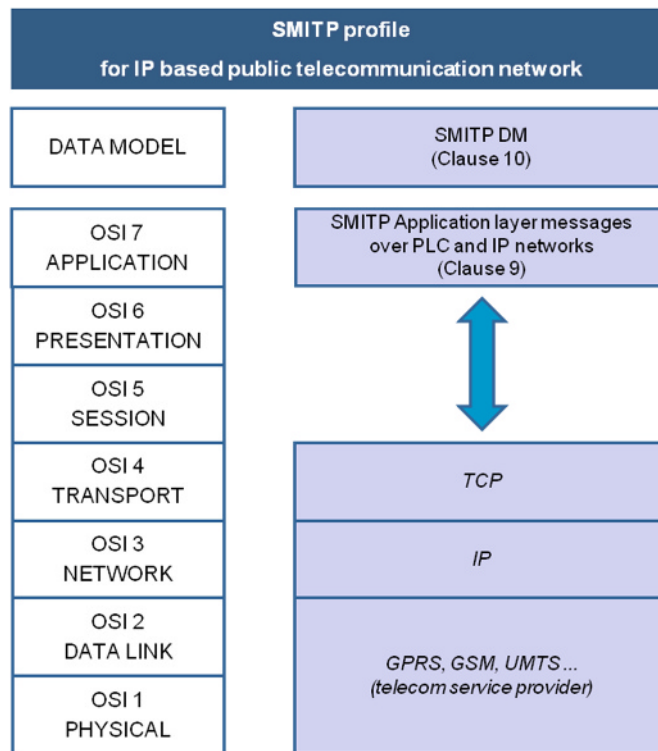


Figure 22 – Protocol stack for SMITP on IP

6.3 Physical and data link layers

The lower layers for this interface provide the physical medium to communicate the central system and the Concentrator, the medium access control and the addressing.

Due to the geographical dispersion of the Concentrators, and the lack of private communications networks among them, public telecommunication networks will be used where available: GPRS, UMTS, GSM, PSTN.

The services provided by these layers will be those supported by the public networks used, mainly error free data transportation.

6.4 Transport and network layers

6.4.1 General

The SMITP Application Layer uses the transport layer always in a connection-oriented mode, based on the connection-oriented Internet transport protocol, called Transmission Control Protocol or TCP STD0005, STD0006 and STD0007.

TCP is an end-to-end reliable protocol. This reliability is ensured by a conceptual “virtual circuit”, using a method called “Positive Acknowledgement with Retransmission” or PAR. It provides acknowledged data delivery, error detection, data re-transmission after an acknowledgement time-out, etc., therefore is dealing with lost, delayed, duplicated or erroneous data packets. In addition, TCP offers an efficient flow control mechanism and full duplex operation, too.

TCP, as a connection-oriented transfer protocol, involves three phases: connection establishment, data exchange and connection release. These phases are performed by a logical TCP management entity that uses standard ULP/TCP services. Any message of the SMITP Application Layer to be encapsulated in TCP packets is managed by this entity. This task could be implemented through the use of any standard TCP management library. 9.5 reports an example explaining the TCP/IP encapsulation of a SMITP TB Application layer message.

In the connection procedure, the client (AMM system) shall to send the requests toward the server (Concentrator) TCP port 50000, and the server (Concentrator) shall send the responses using its TCP port 50001.

6.4.2 TCP Service Request Primitives

6.4.2.1 UNSPECIFIED-PASSIVE-OPEN.request

Parameters: source-port, [timeout], [timeout-action], [precedence], [security-range]

Description: this primitive is used to listen for connection attempt at specified security range and precedence from any remote destination.

6.4.2.2 FULLY-SPECIFIED-PASSIVE-OPEN.request

Parameters: source-port, destination-port, destination-address, [timeout], [timeout-action], [precedence], [security-range]

Description: this primitive is used to listen for connection attempt at specified security range and precedence from specified destination.

6.4.2.3 ACTIVE-OPEN.request

Parameters: source-port, destination-port, destination-address, [timeout], [timeout-action], [precedence], [security]

Description: this primitive is used to request a connection at a particular security and precedence to a specified destination.

6.4.2.4 ACTIVE-OPEN-WITH-DATA.request

Parameters: source-port, destination-port, destination-address, [timeout], [timeout-action], [precedence], [security], data, data-length, PUSH-flag, URGENT-flag

Description: this primitive is used to request a connection at a particular security and precedence to a specified destination and transmit data together.

6.4.2.5 SEND.request

Parameters: local-connection-name, data, data-length, PUSH-flag, URGENT-flag, [timeout], [timeout-action].

Description: this primitive is used to transfer data across named connection.

6.4.2.6 ALLOCATE.request

Parameters: local-connection-name, data-length.

Description: this primitive is used to issue incremental allocation for data to be received.

6.4.2.7 CLOSE.request

Parameters: local-connection-name.

Description: this primitive is used to close connection in regular way.

6.4.2.8 ABORT.request

Parameters: local-connection-name.

Description: this primitive is used to close connection immediately.

6.4.2.9 Status.request

Parameters: local-connection-name.

Description: this primitive is used to query connection status.

6.4.3 TCP Service Response Primitives:

6.4.3.1 OPEN-ID.confirm

Parameters: local-connection-name, source-port, destination-port, destination-address.

Description: this primitive is used to inform TCP user about the connection name assigned to pending connection requests in an Open Primitive.

6.4.3.2 OPEN-FAILURE.confirm

Parameters: local-connection-name.

Description: this primitive is used to report failures of an Active Open request.

6.4.3.3 OPEN-SUCCESS.confirm

Parameters: local-connection-name.

Description: this primitive is used to report completion of a pending Open request.

6.4.3.4 DELIVER.indication

Parameters: local-connection-name, data, data-length, URGENT-flag.

Description: this primitive is used to report arrival of data.

6.4.3.5 CLOSING.indication

Parameters: local-connection-name.

Description: this primitive is used to report that remote TCP user has issued a Close and that all data sent by remote user have been delivered.

6.4.3.6 TERMINATE.confirm

Parameters: local-connection-name, description.

Description: this primitive is used to report that the connection has been terminated; a description of the reason for termination is provided.

6.4.3.7 STATUS-RESPONSE.confirm

Parameters: local-connection-name, source-port, source-address, destination-port, destination-address, connection-state, receive-window, send-window, amount-awaiting-ACK, amount-awaiting-receipt, urgent-state, precedence, security, timeout.

Description: this primitive is used to report current status of connection.

6.4.3.8 ERROR.indication

Parameters: local-connection-name, error description.

Description: this primitive is used to report service-request or internal error.

6.4.4 Example of primitives working

The following figures describe the use of TCP-ULP primitives in case of the ULP of an TCP connection opening request by a client (see Figure 21), a data exchange (see Figure 24) and a TCP connection closing request by a server (see Figure 25). The client is always the AMM system and the server is the Concentrator.

NOTE Primitives between TCP and IP protocols are inserted in order to detail the behaviour within the system but they are out of scope in this document.

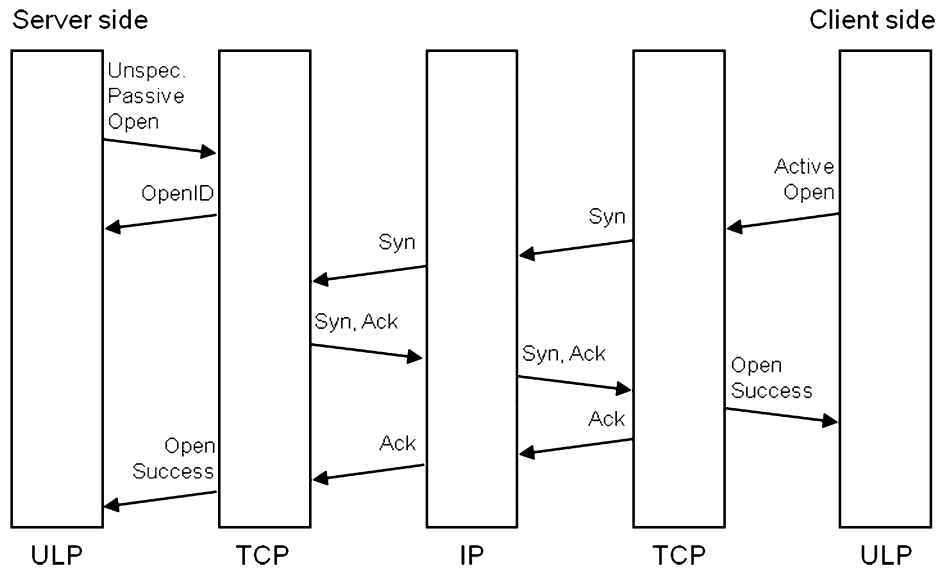


Figure 23 – Connection Opening

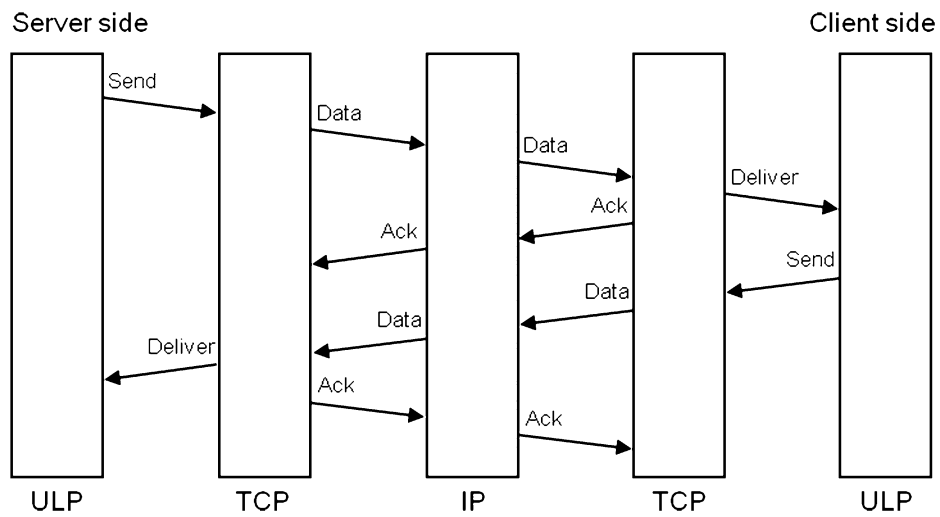


Figure 24 – Data exchange

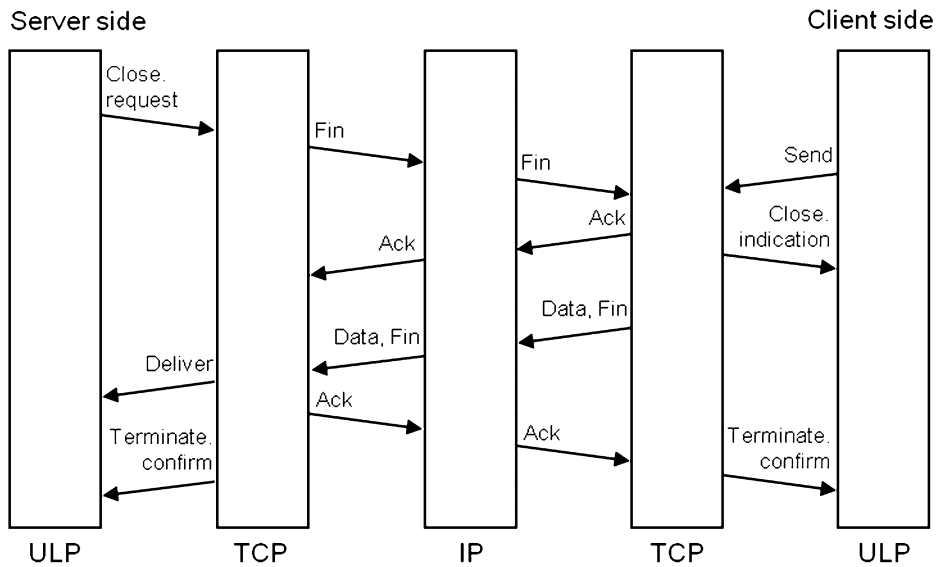


Figure 25 – Connection Closing

6.5 Application layer

The SMITP Application layer is described in Clause 9.

It provides the set of messages exchanged between AMM system and the Concentrator, through the public telecommunication networks (GSM, DCS, PSTN, GPRS etc).

The SMITP Application layer provides the services to handle LV network pattern and Concentrator management.

These services are:

- Requests to Concentrators to manage meters and end customer devices (programming, data exchange, software download, etc.);
- Concentrator and network management (programming, synchronization, software download, command execution, acknowledgements, events handling, etc).

6.6 SMITP Data model

The SMITP Data model is described in Clause 10.

By an abstract point of view, the SMITP Data Model consists of data grouped in tables, each table representing an homogeneous set of parameters (registers). Each parameter can be accessed with specific rights (writable/not writable and readable/not readable) depending of the nature of the data.

These data can be retrieved individually, in set of logically bound data (entire tables) or by user defined sets of data (Custom tables), allowing a fast and flexible scheme of data access.

Data retrieving is possible through Table ID, which is used to identify uniquely a SMITP table, and Register ID, which is used to identify uniquely a register inside a SMITP table.