ÉLECTRICITÉ RÉSEAU DISTRIBUTION FRANCE	**PLC G3 PROFILE SPECIFICATION**

TITLE

PLC G3 PROFILE SPECIFICATION

TYPE	SPECIFICATION	**PROJECT**	PLC G3 OFDM

SUMMARY

This document specifies the integration of the PHY and MAC layers in a complete communication profile for the purpose of metering.

CONTENTS

1. Purpose of the document

This document specifies the integration of the PHY (Physical) and MAC (Media Access Control) layers in a complete communication profile for metering purposes.

2. References

2.1. Standardizing references

2.1.1. PLC OFDM Specifications

[PHY]	PLC OFDM, "Physical (PHY) Layer Specification", October 2008.
[MAC-API]	PLC OFDM, "Specification of MAC Layer and its API (Application Programming Interface)", October 2008

2.1.2. IEEE Documents

[802-2001]	IEEE Computer Society, "IEEE 802-2001: IEEE Standard for Local and Metro Area Networks: Overview and Architecture", December 2001.
[802.15.4-2006]	IEEE Computer Society, "IEEE 802.15.4-2006: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)", September 2006.
[EUI64]	"GUIDELINES FOR 64-BIT GLOBAL IDENTIFIER (EUI-64) REGISTRATION AUTHORITY", IEEE http://standards.ieee.org/regauth/oui/tutorials/EUI64.html.

2.1.3. IETF Documents

[rfc0768]	Postel*, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.
[rfc1213]	McCloghrie, K. and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", RFC 1213, March 1991
[rfc1350]	Sollins, K., "The TFTP Protocol (Revision 2)", RFC 1350, July 1992
[rfc1952]	Deutsch, P., "GZIP file format specification version 4.3", RFC 1952, May 1996
[rfc2090]	Emberson, A., "TFTP Multicast Option", RFC 2090, February 1997
[rfc2347]	Malkin, G., and A. Harkin, "TFTP Option Extension", RFC 2347, May 1998
[rfc2348]	Malkin, G., and A. Harkin, "TFTP Blocksize Option", RFC 2348, May 1998
[rfc2349]	Malkin, G., and A. Harkin, "TFTP Timeout Interval and Transfer Size Options", RFC 2349, May 1998
[rfc2460]	Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
[rfc2578]	McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999
[rfc2579]	McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999
[rfc2863]	McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, June 2000
[rfc3416]	Presuhn, R., "Version 2 of Protocol Operations for the Simple Network Management Protocol (SNMP)", RFC 3416, December 2002
[rfc3418]	Presuhn, R., Case, J., Rose, M., and S. Waldbusser, "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", RFC 3418, December 2002

[rfc3584] Frye, R., Levi, D., Routhier, S. and B. Wijnen, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework", RFC 3584, August 2003

[rfc3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004

[rfc4113] Fenner, B.and J. Flick, "Management Information Base for the User Datagram Protocol (UDP)", RFC 4113, June 2005.

[rfc4194] Strombergson, J., Walleij, L. and P. Faltstrom, "The S Hexdump Format", RFC 4194, October 2005.

[rfc4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[rfc4293] Routhier, S., "Management Information Base for the Internet Protocol (IP)", RFC 4293, April 2006.

[rfc4764] Bersani, F. and H. Tschofenig, "The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method", RFC 4764, January 2007.

[rfc4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, August 2007.

[rfc4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[draft-load] IETF draft-daniel-6lowpan-load-adhoc-routing-03: “6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD)”

[draft-commissionning] IETF draft-6lowpan-commissioning-02: "Commissioning in 6LoWPAN”

[draft-6lowpan-mib] IETF draft-daniel-lowpan-mib-01: "6lowpan Management Information Base"

2.1.4. IEC Documents

[IEC 62056-47] "Electricity metering - Data exchange for meter reading, tariff and load control – Part 47: COSEM transport layers for IPv4 networks", November 2006

[IEC 62056-53] "Electricity metering - Data exchange for meter reading, tariff and load control – Part 53: COSEM application layer", February 2002

[IEC 62056-61] "Electricity metering - Data exchange for meter reading, tariff and load control – Part 61: Object Identification system (OBIS)", November 2006

[IEC 62056-62] "Electricity metering - Data exchange for meter reading, tariff and load control – Part 62: Interface Classes", November 2006

2.1.5. DLMS User Association Documents

[Blue Book] "Blue Book – 8th edition – Identification System and Interface Classes", DLMS UA 1000-1:2007

[dlms-security] dlms_015_security_05_GK080902, "DLMS/COSEM Contributions 015: Data security", September 2008

2.1.6. BroadBand Forum Documents

[TR-069] "CPE WAN Management Protocol v1.1", TR-069 Issue 1 Amendment 2, December 2007

[TR-106] "Data Model Template for TR-069-Enabled Devices v1.1", TR-069 Issue 1.1 Amendment 1, November 2006

2.2. REFERENCES FOR INFORMATION

2.2.1. IEEE DOCUMENTS

[802.1X-2004]	IEEE Computer Society, "IEEE 802.1X-2004: IEEE Standard for Local and Metro Area Networks: Port-Based Network Access Control", December 2004

2.2.2. IETF DOCUMENTS

[rfc0793]	Postel, J., " Transmission Control Protocol", STD 7, RFC 793, September 1981
[rfc2865]	Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.
[rfc3315]	Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003
[rfc3414]	Blumenthal, U. and B. Wijnen, "The User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002
[rfc3561]	Perkins, C., Belding-Royer, E. and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.
[rfc4861]	Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.
[rfc4862]	Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.
[rfc4995]	Jonsson, L-E., Pelletier, G. and K. Sandlund, "The RObust Header Compression (ROHC) Framework", RFC 4995, July 2007.
[rfc4996]	Pelletier, G., Sandlund, K., Jonsson, L-E. and M. West, "RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)", RFC 4996, July 2007.
[rfc5225]	Pelletier, G. and K. Sandlund, "RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite", RFC 5225, April 2008

3. DEFINITIONS, ABBREVIATIONS AND CONVENTIONS

3.1. DEFINITIONS

This specification uses the definitions proposed in [PHY] and [MAC-API]

3.2. ABBREVIATIONS

This specification uses the abbreviations proposed in [PHY] and [MAC-API]

3.3. CONVENTIONS

In this specification the status of an element in a reference document is noted using the following conventions:

- I = "Informative". The element is mentioned purely for information.
- N = "Normative". The element of the original document must be taken as a reference for this specification, without modifications or comments.
- M = "Normative with Modifications". The element of the original document must be taken as a reference for this specification with the modifications and comments noted subsequently.

- N/R = "Not Relevant". The element of the original document must be ignored in this specification. An explanation may be provided.
- A = "Additional". The element is not present in the original document and must be taken as a reference for this specification.

4. GENERAL PRESENTATION OF THE OFDM PLC COMMUNICATION PROFILE

The OFDM PLC (Orthogonal Frequency Division Multiplexing - Power Line Carrier) specifications are developed to meet the following aims:

- Robustness: the communication profile must be suited to severe environments
- Performance: it must take full advantage of the CENELEC A band
- Simplicity: it must be simple to implement, install (Plug and Play), operate and maintain
- Flexibility: it must be compatible with diverse applications and network topologies.
- Security: it must offer a safe environment for the promotion of Value Added services
- Openness: it must be based on open standards in order to support multi-supplier solutions.
- Compatibility: it must be able to function in a given network with earlier metering systems and existing Applications
- Scalability: it must support all future metering developments.

To this end, the OFDM PLC protocol stack aggregates several layers and sublayers that form the Transport layer:

- A robust high-performance PHY layer, based on OFDM and adapted to the PLC environment (CENELEC band A).
- A MAC layer of the IEEE type, well suited to low data rates
- IPv6, the new generation of IP (Internet Protocol), which widely opens the range of potential applications and services
- And to allow good IPv6 and MAC interoperability, an Adaptation sublayer taken from the Internet world and called 6LoWPAN.

The metering profile proposed herein remains compatible at COSEM application level with the profile adopted for the AMM pilot. Consequently the applications developed in the framework of the AMM pilot, at both meter level and data concentrator, can be reused with this profile.

Cohabitation between the two profiles is ensured at physical level. The carrier frequencies used by the AMM pilot profile are masked by the OFDM PLC profile, therefore there is no risk of one profile disturbing the other.

In the case of a random distribution of G1 (S-FSK) and G3 (OFDM) meters over a given low-voltage sub-network, the data concentrator situated at the MV/LV transformer station will have to manage the two profiles simultaneously: that is to say the two modulations (S-FSK and OFDM) as well as the intermediate protocol layers. The application at the concentrator level will be common.

The following figure gives an overall view of the OFDM PLC Communication Profile:

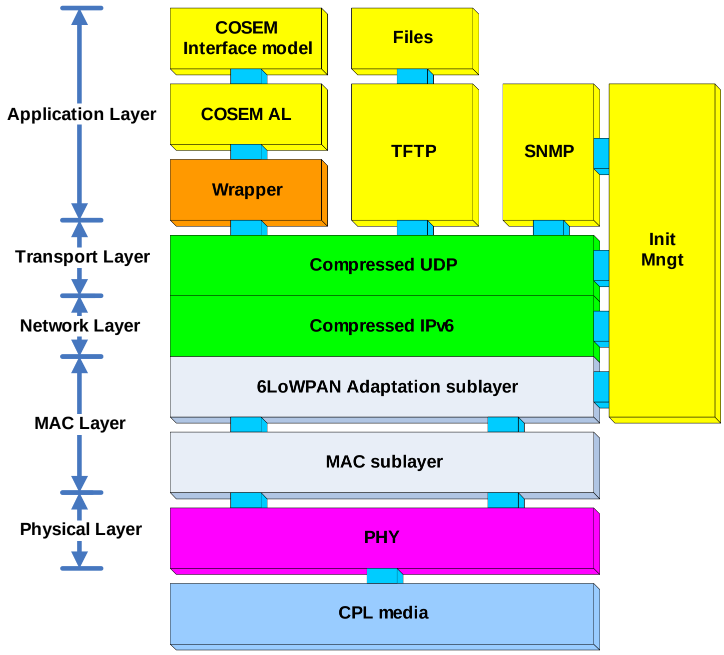

Figure 1 – OFDM PLC Communication Profile

The figure below gives the general format of the frames. It shows the headers for all the levels of the Transport layer (PHY, MAC, Adaptation 6LoWPAN, compressed IPv6 and compressed UDP):

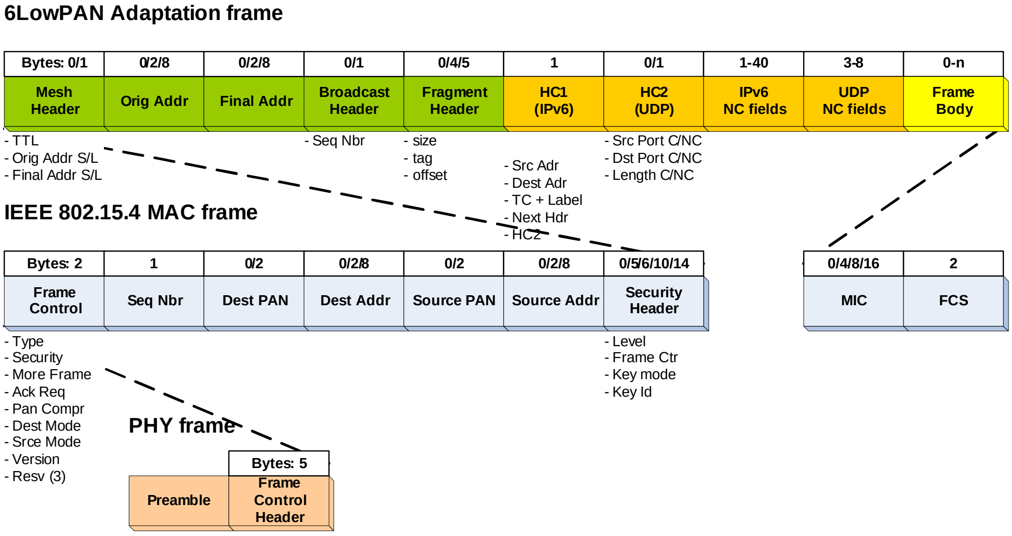

Figure 2 – General format of the frames

5. TRANSPORT STRATUM PROFILE (NORMATIVE)

5.1. PHYSICAL LAYER

The OFDM PLC PHY layer is specified in [PHY].

A description is given in §8.

5.2. OFDM PLC MAC LAYER

The OFDM PLC MAC layer is specified in [MAC-API]. It comprises two sublayers:

- The MAC sublayer derived directly from the MAC part of [802.15.4-2006]
- And the 6LoWPAN Adaptation sublayer derived directly from 6LoWPAN such as it is defined by [rfc4944] and the associated documents.

A description is provided in §9.

5.3. INTERNET AND TRANSPORT LAYERS

The proposed communication model natively integrates a network layer and an IP suite transport layer which opens the way to a vast range of Internet applications and ensures great flexibility in the system architecture. It provides the possibility of having:

- either a decentralized architecture, where the concentrator acts as an application relay, with more or less autonomy. The exchanges at transport level in this case are limited to the dialogue between the meters and the concentrators.
- or to have a more centralized architecture in which the concentrator simply acts as a network gateway and the meters dialogue directly with servers.

Mixed architectures are of course also possible. A centralized architecture can thus be used for the most sensitive functions, and distributed architecture used for the others.

The chosen Internet layer is based on the IPv6 protocol [rfc2460] to ensure the long-term continuity of the model.

The protocol used for the transport layer is UDP [rfc768] which provides unreliable transport to datagrams in non-connected mode. Reliability of exchanges within the PLC network is brought by the subjacent layers.

In order not to compromise the speed of the OFDM PLC links, the IPv6 and UDP headers are compressed. The 6LoWPAN specification [rfc4944] includes a simple and robust static compression which, for example, reduces the IPv6 and UDP headers from 48 bytes to 5 bytes.

There is no identified need for the TCP protocol [rfc793] which provides reliable transport in connected mode to flows of bytes produced by the Applications. This being said, there is nothing to prevent its introduction later on.

Likewise, other compression schemes shall be usable if necessary, such as adaptive ROHCv2 compression [rfc4995] with its specific profiles for TCP/IP [rfc4996] and UDP/IP [rfc5225]. In most cases ROHCv2 manages to reduce header size to 2 bytes. This compression is moreover extendable to other protocols.

6. Profile of the Applications stratum (Normative)

The Applications stratum covers layers 5 to 7 in the OSI model. The model proposed for metering (see Figure 1) is somewhat simplified and comprises two broad classes of Applications: the Metering Application proper and the Applications ensuring the Management of the meter in the broad sense.

It will be noted that all these applications rely natively on UDP, but there is nothing to prevent the future introduction of Applications that use TCP.

6.1. Metering application

In the OFDM PLC profile the COSEM Application strictly complies with the existing standards, namely:

- "COSEM Application Part" such as it is defined in [IEC 62056-61] and [IEC 62056-62]
- "COSEM Application Layer" such as it is defined in [IEC 62056-53]
- Security at Application level is ensured by the process defined in [Blue Book]. Other schemes are currently being specified [dlms-security]. They will integrate naturally into the profile.

Transport of the COSEM Application protocol by UDP requires the interpositioning of a "Wrapper" in accordance with [IEC 62056-47]. Although the title of the standard makes explicit reference to IPv4, it is applied with a few minor modifications to IPv6 and allows one to take advantage of the compression proposed by 6LoWPAN (see section 6.1.1). This is a very simple stateless protocol that enables the number of ports to be scaled down. The header it introduces should be able to be compressed in the future.

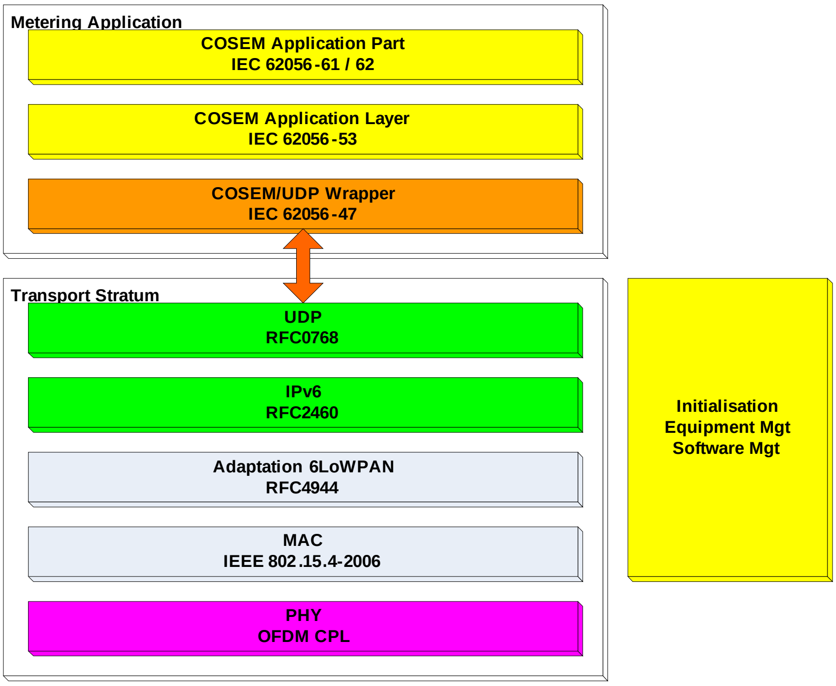

Figure 3 – Metering Application in the OFDM PLC profile

6.1.1. UDP/COSEM Wrapper for IPv6

The UDP/COSEM wrapper for IPv6 used in this specification is such as it is described in document [IEC 62056-47], supplemented by the following statements and modifications.

Clause	Title and remarks/modifications	Status
1	Area of application - Replace 'IPv4' by 'IPv6'	M
2	Normative references	N
3	Terms, definitions and abbreviations	N
3.1	Terms and definitions	N
3.2	Abbreviations	N
4	General presentation - Replace 'IPv4' by 'IPv6'	M
5	The COSEM connectionless transport layer based on UDP	N
5.1	General - Replace 'IPv4' by 'IPv6'	M
5.2	Service specification for the COSEM transport layer based on UDP	N
5.2.1	General	N
5.2.2	The UDP-DATA services	N
5.2.2.1	UDP-DATA.request - The UDP server port number used by the 'COSEM Server Application Layer' equals 61616 (0xF0B0). - The UDP client port number used by the 'COSEM Client Application Layer' can take any value between 1024 and 65535. Ideally this value will be between 61617 (0xF0B1) and 61631 (0xF0BF) in order to take full advantage of the compression of the UDP headers by the 6LoWPAN layer.	M
5.2.2.2	UDP-DATA.indication - The same remarks as for the UDP-DATA.request primitive apply for the 'Local_UDP_Port' and 'Remote_UDP_Port' parameters	M
5.2.2.3	UDP-DATA.confirm - The local generation of a UDP-DATA.confirm primitive does not provide a gain at functional level therefore it is ignored.	N/R
5.3	Protocol specification for the COSEM transport layer based on UDP	N
5.3.1	General	N
5.3.2	The wrapper protocol data unit (WPDU)	N
5.3.3	The COSEM transport layer data unit based on UDP	N
5.3.4	Reserved wrapper port numbers (wPorts) - The number of the wrapper port to use to access the COSEM public server (i.e. without ciphering of the data) is 0x0011 - The number of the wrapper port to use to access the COSEM administration server (i.e. with ciphering of the data at COSEM level) is 0x0012	M
5.3.5	Protocol state machine	N
6	The connection-oriented COSEM transport layer, based on TCP	N/R
6.1	General	N/R
6.2	Service specification for the COSEM transport layer based on TCP	N/R
6.2.1	General	N/R
6.2.2	The TCP-CONNECT services	N/R
6.2.2.1	TCP-CONNECT.request	N/R
6.2.2.2	TCP-CONNECT.indication	N/R
6.2.2.3	TCP-CONNECT.response	N/R
6.2.2.4	TCP-CONNECT.confirm	N/R
6.2.3	The TCP-DISCONNECT services	N/R
6.2.3.1	TCP-DISCONNECT.request	N/R
6.2.3.2	TCP-DISCONNECT.indication	N/R
6.2.3.3	TCP-DISCONNECT.response	N/R

Clause	Title and remarks/modifications	Status
6.2.3.4	TCP-DISCONNECT.confirm	N/R
6.2.4	The TCP-ABORT service	N/R
6.2.4.1	General	N/R
6.2.4.2	TCP-ABORT.indication	N/R
6.2.5	The TCP-DATA services	N/R
6.2.5.1	TCP-DATA.request	N/R
6.2.5.2	TCP-DATA.indication	N/R
6.2.5.3	TCP-DATA.confirm	N/R
6.3	Protocol specification for the COSEM transport layer based on TCP	N/R
6.3.1	General	N/R
6.3.2	The wrapper protocol data unit (WPDU)	N/R
6.3.3	The COSEM transport layer data unit based on TCP	N/R
6.3.4	Reserved wrapper port numbers	N/R
6.3.5	Definition of the procedures	N/R
6.3.5.1	Establishing the TCP connection	N/R
6.3.5.2	Interrupting the TCP connection	N/R
6.3.5.3	Abandoning the TCP connection	N/R
6.3.5.4	Communication of data using the TCP-DATA services	N/R
6.3.5.5	Wrapper sublayer high-level state transition diagram	N/R
Appendix A	Conversion of transport layer services of the OSI model to and from RFC-type TCP function calls	N/R

6.2. METER MANAGEMENT APPLICATIONS

The Meter Management Applications feature three large functional blocks:

- A Management Agent
- A software downloading system
- An Initialization and Supervision system

6.2.1. MANAGEMENT AGENT

The Management Agent operates under the supervision of a Manager function. Depending on the chosen architecture, it may be implemented in the Concentrator or centralized. Together, they must address the different functional domains:

- Configuration Management, which allows the loading and reading (GET/SET) of the parameters that control the functioning of the Meter. It will be noted that some of these parameters are also set by the LBP protocol during initial configuration.
- Fault and Alarm Management which ensures the supervision of functioning of the meter, the detection, recording and signalling of faults which are presented as Alarms
- Statistics Management, which counts and logs all the marking events

The protocol used for exchanges between Management Agent and Manager is SNMP *(Simple Network Management Protocol)* in its latest version [rfc3416]. Implementation must take into account the good practices defined by [rfc3584] to allow the coexistence of several versions of SNMP within a given network.

The security functions of SNMPv3 [rfc3414] turn out to be relatively difficult to use. To maintain simplicity of deployment, it is preferable not to activate them and to rely on the security functions offered by the OFDM PLC MAC level.

If a new need arises, later upgrading to the security model SNMPv3 [rfc3414] remains possible thanks to software downloading.

Other schemes well adapted to the management of a large number of objects like the CWMP protocol *(CPE WAN Management Protocol)* per specification [TR-069] of the BroadBand Forum, can also be used.

For the SNMP protocol, all the information is modelled in the form of an MIB *(Management Information Base)* as defined in §7.

6.2.2. SOFTWARE (FIRMWARE) DOWNLOADING SYSTEM

Teledistribution must be able to be total or incremental in order to optimize updating times.

The firmware memory images are stored in a File Server, which may be implemented in the Concentrator or be centralized, depending on the chosen architecture.

The recommended downloading protocol is TFTP *(Trivial File Transfer Protocol)* [rfc1350] and its options: [rfc2347], [rfc2348] and [rfc2349]. It is usually used for unicast downloading, but a multicast version [rfc2090] is also specified.

The downloading mechanism proper is that defined by the BroadBand Forum for the distribution of software in the residential equipment. It is specified in paragraphs 2.3.2, 3.4.3 and Appendix 3 of [TR-069]. It provides for two methods:

- Unmanaged downloading. The file server contacts the equipment directly by sending it a TFTP Write-Request (WRQ) message. In this case the transfer can only be unicast.
- Managed downloading: the Managers sets the necessary parameters in the equipment (URL of file to download, timeout, etc.) then gives the equipment the order to start the downloading. The equipment then contacts the file server by sending it a TFTP RRQ (*Read-Request*) message. Transfer can then take place in unicast or multicast mode after negotiation. The equipment can propose multicast mode by including an option in its request. The server can accept it by returning a TFTP OACK (*Option-Acknowledge*) message.

  Multicast mode is particularly effective when it is necessary to distribute a given software to an entire equipment pool.
- A variant of managed downloading appears during bootstrapping. The equipment receives the parameters necessary for a possible reloading via the LBP protocol. It checks whether proposed firmware version is more recent than that of the embedded firmware, and if it is, it contacts the file server by sending it an RRQ message as before.

The Memory Image files thus transferred must have the following characteristics:

- They must be natively in S format [rfc4194].
- They must be compressed to GZIP format [rfc1952].
- They must then be constituted in packets signed in accordance with Appendix E of [TR-069]. Each packet comprises:
  - A header including a preamble, the type of packet (version) and the lengths of the list of commands and of the payload.
  - A list of commands that contains the instructions necessary for the extraction and installation of the files contained in the packet: description, version, role of the file, actions on the file system (reformatting, erasure, addition, replacement, etc, with the version number taken into account or not), timeouts, bootstrap, etc.
  - A block of signatures
  - The payload which contains one or more files.

The overall security of the transfers depends on the security mechanisms at MAC level. Moreover, the meters must be able to check the authenticity and integrity of the downloaded files through signatures whose keys are transferred through the Protected Channel carried by EAP and defined earlier.

The downloading mechanism is of general usage. It will subsequently be able to be extended to file transfers in both directions: parameter setting files for the backing up / restoring of complete configurations, statistics files, trace files, etc.

6.2.3. Initialization and Supervision system

This system is responsible for sequencing the actions when bootstrapping the meter, such as "active scan", launching of the LBP/EAP/EAP-PSK protocol suite for authentication, distributing the keys and the initial configuration. Its specification is given in paragraphs 4.7 and 5.5.2 of [MAC-API].

It is moreover in relation with the SNMP agent and the different blocks and protocol layers for the aggregation of the information within the MIB.

7. STRUCTURE OF THE MIB (NORMATIVE)

All the information for the SNMP protocol is modelled as an MIB (Management Information Base) which groups:

- The MIB-II [rfc1213], updated, which is the common section of any SNMP MIB
- The information specific to each layer of the Transport stratum: PHY, MAC and Adaptation 6LoWPAN.
- The information specific to each of the blocks of the Applications stratum (apart from the COSEM Metering Application)

7.1. MIB-II AND ITS UPDATES

MIB-II [rfc1213] constitutes the trunk of the MIB associated with the "Metering" profile. It is made up of several Object Groups whose status for this specification is given in the following tables:

Table 1 – Status of the different Groups of the MIB-II [rfc1213]

Name of group and Remarks/Modifications	Status
System group - Group obsolete, redefined in [rfc3418]	N/R
Interface group - Group obsolete, redefined in [rfc2863]	N/R
Address Translation group - Group obsolete	N/R
IP group - Group obsolete, redefined in [rfc4293]	N/R
ICMP group - Group obsolete, redefined in [rfc4293]	N/R
TCP group - Group obsolete, redefined in [rfc4022]. - For possible future utilization	N/R
UDP group - Group obsolete, redefined in [rfc4113]	N/R
EGP group	N/R
Transmission group	N
SNMP group - Group obsolete, redefined in [rfc3418]	N/R

7.1.1.(IF-MIB)

Table 2 – Status of the different Groups of the Interfaces MIB [rfc2863]

Name of group and Remarks/Modifications	Status
ifGeneralInformationGroup	N
linkUpDownNotificationsGroup	N
ifFixedLengthGroup	N/R
ifHCFixedLengthGroup	N/R
ifPacketGroup	N
ifHCPacketGroup	N/R
ifVHCPacketGroup	N/R
ifCounterDiscontinuityGroup	N
ifStackGroup2	N/R

ifRcvAddressGroup	N/R

7.1.2.IP-ICMP MIB)

Table 3 – Status of the different Groups of the IP-ICMP MIB [rfc4293]

Name of group and Remarks/Modifications	Status
ipSystemStatsGroup	N
ipAddressGroup	N
ipNetToPhysicalGroup	N
ipDefaultRouterGroup	N
icmpStatsGroup	N
ipSystemStatsHCOctetGroup	N/R
ipSystemStatsHCPacketGroup	N/R
ipIfStatsGroup	N/R
ipIfStatsHCOctetGroup	N/R
ipIfStatsHCPacketGroup	N/R
ipv4GeneralGroup	N/R
ipv4IfGroup	N/R
ipv4SystemStatsGroup	N/R
ipv4SystemStatsHCPacketGroup	N/R
ipv4IfStatsGroup	N/R
ipv4IfStatsHCPacketGroup	N/R
ipv6GeneralGroup2	N
ipv6IfGroup	N
ipAddressPrefixGroup	N
ipv6ScopeGroup	N/R
ipv6RouterAdvertGroup	N/R
ipLastChangeGroup	N/R

7.1.3.UDP-MIB

Table 4 – Status of the different Groups of the UDP MIB [rfc4113]

Name of group and Remarks/Modifications	Status
udpBaseGroup	N
udpHCGroup	N/R
udpEndpointGroup	N

7.1.4.SNMP-MIB

Table 5 – Status of the different Groups of the SNMP MIB [rfc3418]

Name of group and Remarks/Modifications	Status
systemGroup	N
snmpGroup	N
snmpSetGroup	N
snmpBasicNotificationsGroup	N
snmpCommunityGroup	N/R
snmpWarmStartNotificationGroup	N/R

7.2. Transport stratum MIB

7.2.1. MAC/PHY PLC OFDM G3 MIB (PLC-G3-MIB)

The MAC Information Base (MAC PIB) is specified in paragraph 4.4 of [MAC-PHY].

The structure of the Neighbour Table is specified in paragraph 4.5.1 of [MAC-PHY].

The translation to SNMP MIB in accordance with SMIv2 [rfc2578] is provided in Appendix A.

7.2.2. IPV6LOWPAN-MIB ADAPTATION (IPV6LOWPAN-MIB)

The 6LoWPAN Application Information Base is specified in paragraph 5.2 of [MAC-PHY].

The translation to SNMP MIB is provided by the document [draft-6lowpan-mib] with the following remarks and modifications:

Table 6 – Status of the different elements of the 6LoWPAN MIB [draft-6lowpan-mib]

Name of group and Remarks/Modifications	Status
lowpanRoutingTable	N
lowpanNeighborTable Replaced by the NeighbourTable of PLC-G3-MIB	N/R
Other objects	N

If a given equipment item supports several OFDM PLC G3 interfaces, this MIB must be instantiated and form the subject of tables indexed by the interface number (ifIndex of IF-MIB).

7.3. Applications stratum MIBs

File Transfer Management complies with the specifications of the BroadBand Forum. The corresponding mechanisms are specified in [TR-069] and the Data Model in [TR-106].

The translation to SNMP MIB in accordance with SMIv2 [rfc2578] is provided in Appendix B.

8. Presentation of the OFDM PLC Physical layer (Informative)

8.1. Physical Layer Reference Model

The Physical Layer Reference Model is presented below:

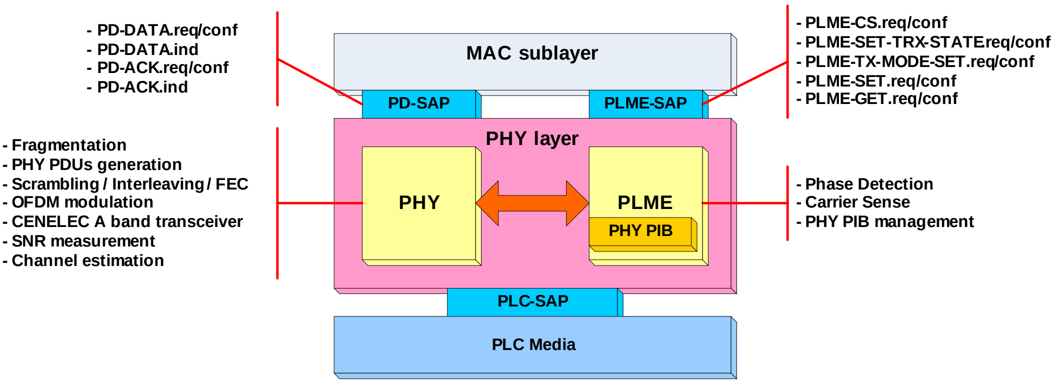

Figure 4 – Physical Layer Reference Model

This Reference Model reveals two functional blocks:

- The Physical processing block (PHY) in charge of emission and reception over the PLC medium
- The PHY Management Entity (PLME) responsible for managing the PHY layer. It relies in particular on the PHY Information Base (PHY PIB).

8.2. PHY Functions

The Physical processing block (PHY) comprises the following functions:

- Fragmentation: This function enables a MAC frame exchanged between two neighbours to be divided into segments whose length is optimized according to the negotiated modulation characteristics in order to limit stuffing.
- Generation of the PHY Protocol Data Units (PHY PDU): there are two types:
  - PHY Data frame. It adds to any MAC frame a preamble that enables the timing to be retrieved. It is followed by a header (FCH) that contains all the information necessary for the demodulation of the rest of the frame. This header is transmitted in ROBO mode. The very long range of this modulation prevents the hidden node phenomenon.
  - PHY Check frames. There are three check frames (ACK, NACK and FAIL) which are made up solely of a preamble followed by a short header (FCH) transmitted in ROBO mode.
- Scrambling / Interleaving / FEC: These functions allow effective correction of transmission errors. They combine convolutive coding (Viterbi) and block coding (Reed-Solomon).
- OFDM modulation. This is based on the dividing of the CENELEC A band into 70 tones (on the HTA network, it is possible to use a widened bandwidth as indicated in paragraph 5.2 of [PHY]). These tones can be modulated in either DBPSK (1 bit per tone), or DQPSK (2 bits per tone). The amplitude can be adapted by a pre-emphasis defined on 8 sub-bands. There is Automatic Gain Control (AGC) in reception.

Some of the 70 tones can be masked by configuration so as not to adversely affect other transmissions, while others can be eliminated because they are polluted by recurrent parasites.

For the ROBO mode, a spread spectrum is superimposed by repeating the information 4 times.

The order of size of the throughputs (70 tones, frames of about 240 bytes) is 30 kb/s for DQPSK, 15 kb/s for DBPSK and 3.5 kb/s for ROBO.

- Transmission in the CENELEC A band. Two types of coupling are planned for: low and medium voltage.
- Measurement of the Signal/Noise ratio: This measurement enables the Link Quality Index (LQI) to be deduced
- Channel estimation. This estimation aims to determine the optimum characteristics (tones, modulation, pre-emphasis) for transmission in one direction between two neighbouring nodes. It must be achieved independently for the two directions of communication to cope with any dissymmetry. If forms the subject of a procedure that associates PHY and MAC:
  - Between two nodes A and B, for the direction A → B, the estimation request is initiated by the MAC layer of emitter A by positioning a parameter of the PHY service primitive, PD-DATA.req.
  - This request is inserted in the PCH header of the PHY frame transmitted by A.
  - The PHY layer of receiver B starts to decode the PCH header, then proceeds with channel estimation further to the request. It stores the estimation parameters in its PHY PIB and associates them with a TMI (Tone Map Indicator) identifier. Then it transmits to its MAC layer a PD-DATA.ind primitive that takes up the request expressed by the MAC layer of the emitter.
  - The MAC layer of B retrieves the TMI via the PLME-GET.req primitives and the channel estimation parameters and transmits them to its counterpart A via a MAC Check frame.
  - On reception the MAC layer of A stores everything in its Neighbours Table. Henceforth all the exchanges in the A-to-B direction shall be made using the Channel Estimation parameters identified by this TMI.

8.3. PHY SERVICES PRIMITIVES

The PHY services are provided to the higher layer via PHY services primitives through a Services Access Point (PD-SAP):

- PD-DATA.request/indication/confirmation: they allow the transmission of a MAC frame by the PHY layer. Among the parameters are found some of those that will be included in the FCH header, including the TMI, the Estimation request and the Acknowledgement request.
- PD-ACK.request/indication/confirm: they process the acknowledgement by the neighbour.

8.4. PLME FUNCTIONS

The Physical Layer Management Entity (PLME) comprises the following functions:

- Carrier detection. This is one of the important elements of the CSMA/CA procedure. It concerns the detection of a signal in conformity with [PHY].

- Phase detection. It allows identification of the phase on which the meter transmits.
- Management of the PHY PIB Information Base

8.5. PLME Management Primitives

The PLME management services are provided to the higher layer via PLME management primitives through a Services Access Point (PLME-SAP):

- PLME-CS.request/confirm: These primitives activate carrier detection and record the result.
- PLME-SET-TRX-STATE.request/confirm: These primitives allow switching between emission and reception modes
- PLME-TX-MODE-SET.request/confirm: These primitives enable the MAC layer to set the transmission parameters (table of tone, etc.) before invoking a PD-DATA.request primitive.
- PLME-SET.request/confirm: These primitives set the information in the PHY PIB.
- PLME-GET.request/confirm: These primitives retrieve the information from the PHY PIB.

9. PRESENTATION OF THE OFDM PLC MAC LAYER (INFORMATIVE)

9.1. MAC SUBLAYER

9.1.1. REFERENCE MODEL OF THE MAC SUBLAYER

The Reference Model of the MAC sublayer is shown below:

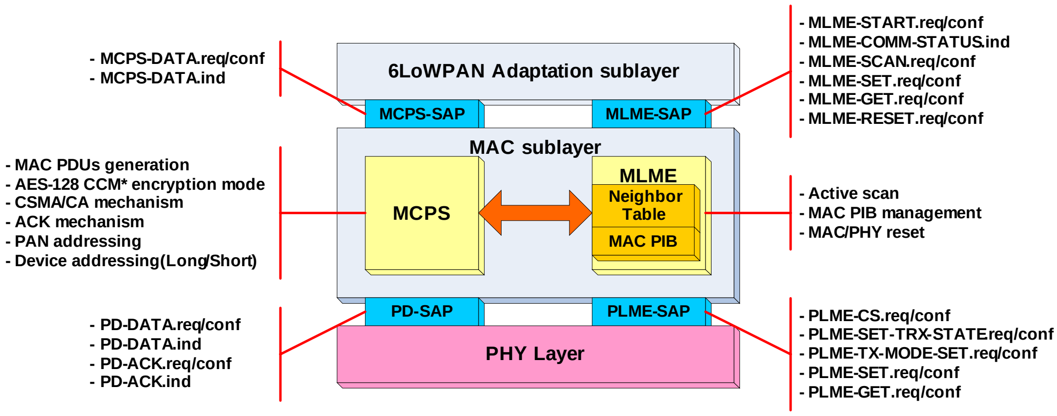

Figure 5 – Reference Model of the MAC sublayer

This Reference Model reveals two functional blocks:

- The MAC Common Part Sublayer (MCPS) responsible for communication with the neighbouring nodes
- The MAC Layer Management Entity (MLME) responsible for management of the MAC sublayer. It relies in particular on the MAC PAN Information Base (MAC PIB) whose main element is the Neighbour Table. This table contains all the information that the MAC and PHY levels need for bidirectional communication with the neighbours.

9.1.2. MCPS FUNCTIONS

The MAC Common Part Sublayer (MCPS) processing block comprises the following functions:

- Generation of the MAC Protocol Data Units (MAC PDU): there are three types:
  - MAC Data Frame. It adds a variable number of header fields to any 6LoWPAN frame:
    - Check frame (compulsory). It identifies the type of frame and its format, etc.
    - Sequence number (compulsory). It allows the elimination of duplicates when a frame is resent
    - Source and Destination Addressing for transfer between neighbours. The addresses can be short (16 bits) or long (EUI-64). They can be omitted when they are implicit. The PAN number allows several networks to coexist on the same given infrastructure.
    - Security Header (optional). It contains all the information relative to security (level of security, key identifier, CCM* encryption method counter, etc.)

        - Message Integrity Check (MIC) in the Security sense (optional). It verifies that the frame has not been maliciously modified or truncated.
        - Integrity Check in the transmission sense (compulsory). It verifies that the frame has not been modified further to a transmission disturbance.
    - MAC Check frames. These frames of a similar format enable requests or indications to be exchanged between neighbours: Discovery of the environment (active scan), Transfer of Channel Estimation parameters, etc.
    - Beacon Frame. The beacon frame is only emitted on request (active scan) and not cyclically as in other systems. It enables the basic characteristics of the neighbour nodes active on the network to be discovered: PAN number, MAC address, capacities (coordinator, encryption, etc.).

The following figure shows the format of typical MAC frames. The Data frame sent by a coordinator (no source address) directly to an end system, without the participation of a relay node (no Mesh 6LoWPAN header). The payload of the frame is encrypted with Integrity Check, hence the presence of the Security header and the MIC field.

Typical Data Frame

Bytes: 2	1	2	2	6	1	1	1	3	0-n	4	2
Frame Control	Seq Nbr	Dest PAN	Dest Addr (RA)	Security Header	HC1 (IPv6)	HC2 (UDP)	IPv6 NC fields	UDP NC fields	Frame Body	MIC	FCS

Beacon frame

Bytes: 2	1	2	2	2	2	1	1	2
Frame Control	Seq Nbr	Source PAN	Source Addr (TA)	FCS	Superframe Specif	GTS fields	Pending Address fields	FCS

MAC Command frame

Bytes: 2	1	2	2	2	1	0-m	2
Frame Control	Seq Nbr	Dest PAN	Dest Addr (RA)	Source Addr (TA)	Command Frame Id	Command Payload	FCS

- Association
- Dissociation
- etc.

- Ass Req/Resp
- Dis Notif
- etc.

Figure 6 – Format of typical MAC frames

- CSMA/CA Access Method: It is based on carrier detection by the PHY layer (PLME-CS.req/conf primitives). The conflict avoidance (CA) algorithm defines three time intervals at the end of emission of a frame:
    - A conflict-free time interval, reserved for the coordinator but who can temporarily delegate usage to another node.
    - A priority time interval within which a random delay mechanism avoids conflicts.
    - A non-priority time interval, with the same random delay mechanism.

  The treatment of Quality of Service (QoS) is therefore organized around the CSMA/CA access method.

- Reliable data transfer to the immediate neighbours (ACK mechanism). The ACK mechanism is checked by the MAC layer (PD-ACK.req/conf/ind primitives) and the frames belong to the PHY layer to avoid wasting bandwidth.

- Security: encryption in AES-128 CCM* mode, with selection from among 4 Group Session Keys and an Anti-Replay mechanism

- Network selection (PAN) and addressing of the different nodes: The MAC layer uses two types of MAC addresses to designate an equipment item:

  - A long address in EUI-64 format, deduced from the unique EUI-48 address assigned during manufacture of the equipment by adding two 0xFF bytes in its centre.

  - A short address on 16 bits assigned dynamically and in a centralized manner thanks to the LBP protocol (6LoWPAN Bootstrap Protocol) [draft-commissioning].

  The PAN number is assigned by configuration to its coordinator. It allows the sharing of the PLC infrastructure, including by crosstalk, between several logical OFDM PLC networks.

9.1.3.MCPS Services Primitives

The MCPS services are provided to the higher layer via MCPS services primitives through a Services Access Point (MCPS-SAP):

- MCPS-DATA.request/indication/confirmation: these primitives allow the MAC layer to transmit a 6LoWPAN frame. Among the parameters are found the MAC and PAN address information and the security parameters. The request primitive includes Quality of Service information and the indication primitive a Quality of Line indicator.

9.1.4.MLME Functions

The MAC Sublayer Management Entity (MLME) features the following functions:

- Active discovery (active scan) of neighbouring nodes. This is activated when a terminal equipment starts or after it has become detached from the network (failure, commanded detachment, etc.). The equipment sends a MAC discovery frame (active scan), to which all the active neighbouring nodes reply by emitting a Beacon frame. The equipment collates the replies (MAC address, PAN number, signal quality, etc.) and classifies them in order of interest. The remainder of the procedure is at 6LoWPAN level and implements the Bootstrap Protocol (LBP) which includes strong authentication, distribution of security keys and transmission of the initial configuration. The LBP dialogue is engaged with the first on the list. If this fails, it proceeds to the next on the list, and so on.

- Management of the MAC level parameters. These parameters constitute the MAC Information Base (MAC PIB), an integral part of the overall Management Information Base (MIB).

- Initialization/Reinitialization of the MAC and PHY layers.

9.1.5.MLME Management Primitives

The MLME management services are provided to the higher layer via MLME management primitives through a Services Access Point (MLME-SAP):

- MLME-START.request/confirm: these primitives initialize the MAC and PHY layers

- MLME-RESET.request/confirm: these primitives reinitialize the MAC and PHY layers.

- MLME-COMM-STATUS.indication: this primitive signals reception of an erroneous frame for maintenance purposes.

- MLME-SCAN.request/confirm: these primitives activate sending of the MAC discovery frame, gathering of the information carried by the Beacon frames and, after a programmable time period, the sending of a list of Neighbours with their main characteristics.
- MLME-SET.request/confirm: these primitives enable information to be set in the MAC PIB.
- MLME-GET.request/confirm: these primitives serve to retrieve information from the PHY PIB.

9.2. 6LOWPAN ADAPTATION SUBLAYER

9.2.1. REFERENCE MODEL OF THE 6LOWPAN ADAPTATION SUBLAYER

The Reference Model of the 6LoWPAN Adaptation sublayer is shown below:

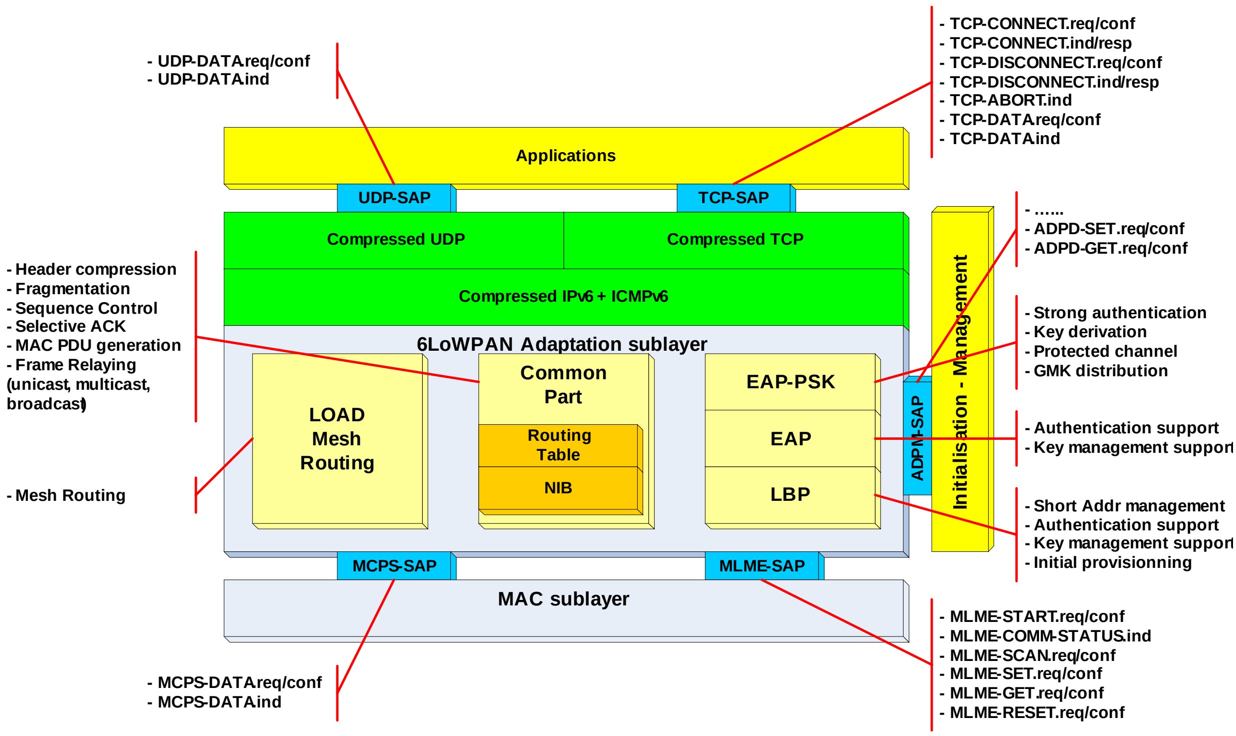

Figure 7 – Reference Model of the 6LoWPAN Adaptation Sublayer

This Reference Model reveals three functional blocks:

- The common processing operations block (Common Part) is responsible for end-to-end communication within the PLC local network (PLC LAN). It is based in particular on the 6LoWPAN Information Base (NIB), the main element of which is the Routing Table. This table contains the identifier of the neighbour node to which a packet is to be routed for each destination node identified by its short address on 16 bits.
- The routing function in Mesh mode. Its purpose is to constitute the routing table, and it does this using the LOAD protocol [draft-load], a compact version of the AODV protocol [rfc3561] that is adapted to 6LoWPAN.
- The Security and Initial Configuration function. It uses the LBP (6LoWPAN Bootstrap Protocol) [draft-commissioning] which appears as a grouping of the DHCPv6 [rfc3315] and EAPOL [802.1X-2004] protocols in a compressed version adapted to 6LoWPAN.

This protocol enables a terminal equipment to acquire its short MAC address on 16 bits, along with the parameters it needs in order to communicate effectively.

Beforehand, the terminal equipment must authenticate itself and receive the keys necessary for the security of the exchanges. To achieve this, LBP encapsulates the EAP authentication protocol [rfc3748]. This protocol is flexible and supports different methods. The method adopted for the needs of OFDM PLC is EAP-PSK [rfc4764]. It proposes strong authentication based on a secret shared on 128 bits, and a Protected Channel that allows the secure transmission of the session keys that can be used by all the layers.

9.2.2.6LoWPAN Functions

The 6LoWPAN common processing operations block comprises the following functions:

- Compression of Internet and Transport headers. See §5.3.
- Fragmentation: This function enables an Ipv6 datagram, whose size can reach 1260 bytes, to be divided into segments better adapted to transport across the PLC LAN.
- Generation of the 6LoWPAN PDUs: there are two types:
    - 6LoWPAN Data Frame: It adds varying numbers of headers to the Ipv6 datagram (or fragment in the case of a long datagram):
        - Fragmentation header in case of fragmentation or need for reliable transport
        - Transmission header in case of Broadcast or Multicast routing
        - Mesh header in case of relaying
    - Check frames corresponding to the LBP and LOAD protocols
- Packet reordering
- Reliable end-to-end data transfer (selective ACK mechanism)
- Relaying of MAC frames (unicast, multicast, broadcast). It is based on the information from the routing table and on the definition of the groups for multicast relaying.

9.2.3.Routing in Mesh mode

Calculation of the optimum route between two nodes A and B of the PLC LAN using the LOAD protocol is a decentralized process. It can be triggered either when there is a datagram to transmit, or preventively:

- Node A starts by broadcasting an RREQ message carrying a nil total cost.
- All the network nodes (x = C, D, E and F) capable of propagating this message start by adding their short address on 16 bits and incrementing the total cost of the route by the cost of the segment Ax. If node x already has a route to B, it propagates the RREQ message along that route. If not, the message is broadcast again.
- Node B of the destination thus receives several RREQ messages which have followed different routes whose path is stored in the body of the message. It chooses the route corresponding to the lowest cost and sends back an RREP message that will follow the reverse route to A.

- On reception of RREP, each node marks the route to B in its routing table.

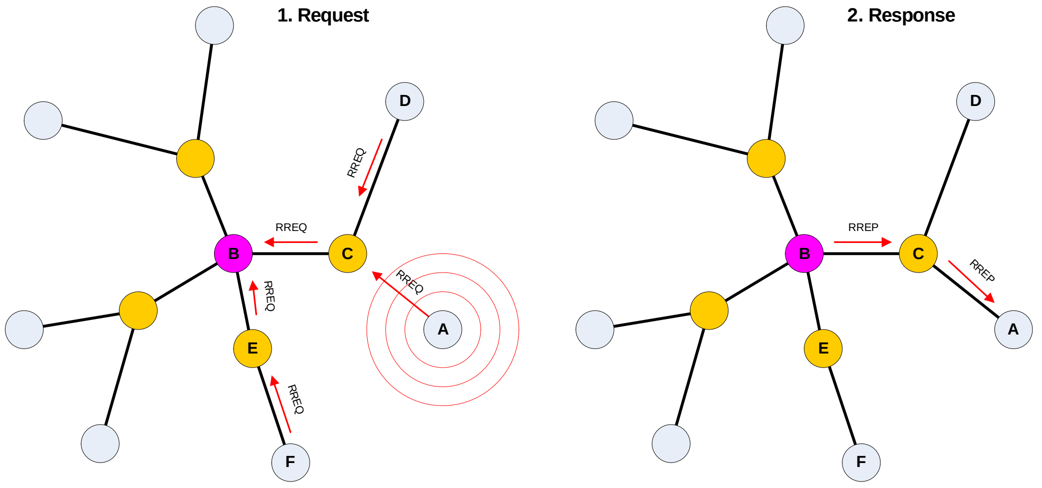

Figure 8 – Functioning of the LOAD protocol

A few remarks:

- An aging mechanism that enables the routes to be updated to take account of the appearance or disappearance of nodes and changes on the conditions of propagation.
- The LOAD protocol enables a route to be established between any pairs of nodes in the network.
- The cost function is determining in the choice of the optimum route. The route proposed is based on the transfer time (see [MAC-API] Appendix 2).

9.2.4. Security and Initial configuration

- Access control and Authentication:

  A Terminal Equipment (i.e. a meter) cannot access the PLC LAN without prior identification (including comparison with white or black lists) and a strong Authentication. Identification and Authentication are based on two parameters that personalize each Terminal Equipment:

  - An EUI-48 MAC address as defined in [802-2001]. This address can be easily converted to EUI-64 format as required by [802.15.4-2006] and the associated documents. It is considered to be public.
  - A secret shared on 128 bits (PSK) used as proof of identity during the authentication process. It is shared between the Equipment itself and an authentication server. The mutual authentication is based on proof that the other party knows PSK. It is of the utmost importance that PSK remains secret.

  The Identification and Authentication processes are activated when a Terminal Equipment restarts and can be initiated at any moment in accordance with the applicable Security policy. The corresponding equipment is transported by LBP (6LoWPAN Bootstrapping Protocol) which encapsulates EAP (Extensible Authentication Protocol).

  LBP and EAP have been specified to be relayed by intermediate nodes. Thus, during the bootstrap phase, when a Terminal Equipment that has not yet acquired a routable 16-bit address is situated one hop from the Coordinator, it can communicate with the coordinator directly. Otherwise it can use the services of an intermediate node situated one hop from that Terminal Equipment.

Furthermore, two different authentication architectures can be considered:

- The Authentication Server function is supported directly by the Coordinator, and in this case all the authentication material (access list, proof of identity, etc.) must be loaded into the Coordinator.

- The Authentication Server function is supported by a remote (and usually centralized) AAA server, and in this case the Coordinator is only responsible for transmitting the EAP messages to the AAA server by a standard AAA protocol (i.e. RADIUS [rfc2865]).

The Authentication process is fully dependent on the EAP method put in place. The EAP protocol is highly flexible and supports various EAP methods (EAP-MD5, EAP-AKA, EAP-TLS, etc.). Each method is characterized by its proof of identify (shared secret, certificate, SIM card, etc.) and by its signature and encryption algorithms.

The proposed method for the PLC LAN is EAP-PSK, for which the objectives are:

- Simplicity: it is based entirely on a unique proof of identity (a 128-bit shared secret) and a single cryptographic algorithm (AES-128).

- Security: it appears very conservative in its definition by following well known, tried and tested cryptographic schemes

- Scalability: in the case of OFDM PLC, it can be readily extended to support the distribution of group keys.

- Confidentiality and Integrity

  The Confidentiality and Integrity services are ensured at different levels:

  - At MAC level: as defined in [802.15.4-2006], a CCM* encryption is applied to each frame transmitted between the network nodes. It is a universal Confidentiality and Integrity Service (with Anti-Replay capacities). The MAC frames are encrypted and decrypted at each hop.

    The only exception concerns a few well verified frames in the first stages of the bootstrap process.

    To effectively support this service, all the network nodes receive the same Group Master Key (GMK). This key is distributed individually to each node in a secure manner thanks to the Protected Channel EAP-PSK.

  - At EAP-PSK level: as defined by [rfc4764], EAP-PSK provides Confidentiality and Integrity services (and Anti-Replay protection), also called Protected Channel (PCHANNEL) to the messages exchanged through EAP between Authentication Server and Terminal Equipment.

  - At the Applications level: as defined in §6.1 and §6.2.2.

- Anti-Replay and Prevention of Denial of Service (DoS)

It is always difficult to parry a DoS attack, and especially those targeting the Physical level, but their impact is limited by nature to a restricted zone.

The CCM* encryption mode is generalized at MAC level. It prevents the non-authenticated Equipment from accessing the network and performing malicious actions on the routing, the configuration or any other low-level process. The only exception is the Bootstrap process, which is well controlled.

In addition to this, the MAC layer includes an Anti-Replay mechanism.

- Generation and Distribution of Keys

  The following figure illustrates the key generation process as defined by EAP-PSK.

  The 128-bit Group Master Key (GMK) is generated by the Authentication server, then transmitted individually and securely to the different nodes via the Protected Channel EAP-PSK (PCHANNEL).

  GMK is assumed to be random but its mode of generation is considered to be purely dependent on the implementation.

  GMK is distributed to the nodes under two circumstances:

  - During the bootstrap process
  - During the key change process. The GMK lifetime is very long (several tens of years) because of the meter on 4 bytes included in the nonce. It is nevertheless a good policy to change the network keys regularly, or when a node leaves the network.

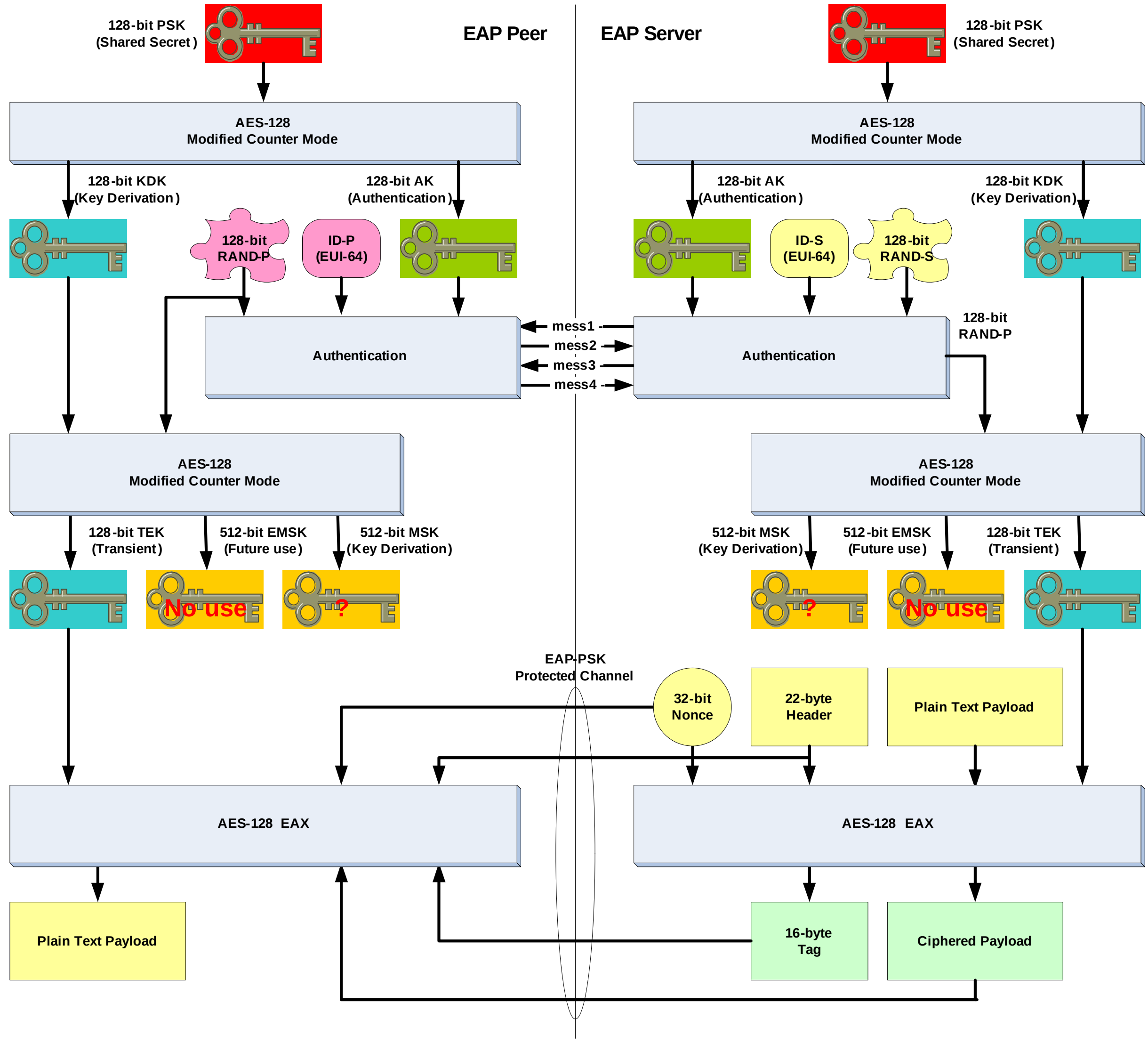

Figure 9 – Hierarchy of the keys in EAP-PSK

- Centralized allocation of short MAC addresses on 16 bits

  Rather like DHCPv6 would do, the LBP protocol offers the possibility of centralized assigning of an address to each node of the PLC LAN. In this case it is a short 16-bit MAC address. This address is assigned either at the end of the equipment bootstrapping process or when renumbering the network.

- Initial configuration

  Likewise, LBP can perform the initial configuring of a terminal equipment.

10. Positioning of the OFDM PLC profile compared with the AMM pilot profile (Informative)

10.1. Benefits brought by the OFDM PLC profile

- Data rates

  The OFDM PLC profile brings a clear advantage in terms of data rates, since the net data rate, after deducting the overheads introduced by the coding, is about 30 kb/s for DQPSK modulation, 15 kb/for DBPSK modulation and 3500 b/s for ROBO modulation, whereas the SFSK modulation used by the AMM pilot profile has raw data rates of 2400 b/s and 1200 b/s.

  Furthermore, the OFDM PLC profile has several mechanisms that enable maximum benefit to be drawn from the CENELEC A band at all times:

  - Configuration frequency masking in order to avoid disturbing other systems operating in the same frequency band
  - Unidirectional channel estimation in order to apply the most suitable modulation scheme between two neighbouring nodes
  - Mesh routing protocol capable of determining the optimum path between two remote nodes of the network

- Same metering applications (COSEM)

  The two profiles implement the same COSEM Application suites (IEC 62056-53], [IEC 62056-61] and [IEC 62056-62]) in order to give the operator a uniform picture of the information specific to the metering activity.

- MAC level Security

  Within a global Security policy, the introduction of MAC level Security services is the necessary complement to the mechanisms operating at the COSEM Application level.

  These MAC level services are based on known, tried and tested schemes. They are nevertheless simple, since they are based on a unique proof of identity (a 128-bit shared secret) and a single cryptographic algorithm (AES-128).

  They propose a strong Authentication and CCM* encryption which brings Confidentiality and Integrity. An Anti-Replay mechanism is also provided.

- Architecture diversity and openness (IP)

  The introduction of technologies from the world of the Internet into the OFDM PLC profile (IPv6 in this case, to guarantee the long-term continuity) opens up new possibilities in the architecture of the networks.

  Thus the AMM pilot profile in practice leads to the Concentrator being designed like a poorly transparent Application relay and the application intelligence to be distributed between the Central Information System, the Concentrator and the Meter.

  Without necessarily calling into question the concept, the OFDM PLC profile allows it to evolve. It thus becomes possible to put the Meter and the Information System in direct contact for certain functions such as Equipment Management, software downloading or Security.

- Open Equipment Management (SNMP)

The opening up to the technologies of the Internet world enables the metering domain to benefit from new tools such as Equipment Management by SNMP (Simple Network Management Protocol), which reduces the acquisition and operating costs, as is witnessed by its widespread adoption by Network operators.

But other schemes even better suited to the management of millions of terminal equipment items are reaching maturity, such as those based on the CWMP protocol of the BroadBand Forum (better known under the reference TR-069). Here they are based on very widely distributed Web technologies and are associated with a vast number of tools. The majority of them exists as freeware and is therefore free of charge.

- Software (Firmware) management (TFTP)

Another example of the benefits brought by the introduction of Internet technologies is the use of standard protocols and tools for the downloading and management of firmware.

This is an essential point since it guarantees the scalability and long-term continuity of the solution and the related equipment.

10.2. COHABITATION OF THE TWO PROFILES AND EVOLUTION SCENARIO

At the Physical level, the frequency masking possibilities provided by the OFDM PLC profile allow sharing of the CENELEC A band, and sharing of the PLC infrastructure over and beyond this.

Thus, meters coming from the two profiles can be made to cohabit in a given sector.

At Application level, the reference to the same standards enables the view of the Metering activity information provided to the Operator to be rendered uniform.

On the Concentrator side one can:

- Either juxtapose two concentrators that each treat their pool of meters and feed back the information independently to one and the same Information System.
- Or design a mixed concentrator that embeds the equipment necessary for the implementation of the PHY and MAC levels in the two technologies and the PLC communication profile up to the COSEM Application Layer.

In both cases, the pooling of elements other than Applications (e.g. the pooling of the LLC layer: IEC 61334-4-32) would not bring any decisive advantage and would slow down the evolution of the solution. This is why it has not been taken up again in the present specification.

11. APPENDIX A: MIB OF THE PHY AND MAC LEVELS: PLC-G3-MIB (NORMATIVE)

This appendix specifies the portion of the MIB, called PLC-G3-MIB, that is devolved to the management of the PHY and MAC levels of the OFDM G3 PLC interface.

11.1. RELATION WITH THE INTERFACES MIB

The Interfaces MIB [RFC2863] requires that all the MIBs that are added to it clarify certain points that are intentionally left vague in its definition. The following table provides the clarifications necessary for the case of the OFDM G3 PLC interface.

Table 7 – Relation with the Interfaces MIB [rfc2863]

Item IF-MIB	Application to the OFDM G3 PLC interface
Layering Model	No distinction is made between the PHY, MAC and 6LoWPAN layers and sublayers
Virtual Circuits	Not applicable
ifIndex	Each OFDM G3 PLC interface is represented by an ifEntry. The tables of the PLC-G3-MIB are indexed by ifIndex.
ifDescr	See [rfc2863]
ifType	Is provisionally set at 200. A value is to be requested from the IANA
ifMtu	Is set at 1280
ifSpeed	Not applicable
ifPhysAddress	The short 16-bit address the equipment uses to communicate in the PAN. If the equipment is the PAN coordinator, this value must be chosen before starting the PAN. Otherwise, the address is assigned during the Bootstrap procedure. The value 'FFFE'h indicates that the equipment is associated but the address has not been assigned to it. The value 'FFFF'h indicates that the equipment has no address.
ifAdminStatus	Not applicable
ifOperStatus	The operational status of the interface. The 'testing', 'dormant', and 'lowerLayerDown' statuses are not applicable
ifLastChange	See [rfc2863]
ifInOctets	The number of bytes received in valid MAC frames (Data + Command + Beacon) including the MAC header and the FCS.
ifInUcastPkts	The number of unicast packets received from the interface and transmitted to the higher layers or relayed
ifInDiscards	See [rfc2863].
ifInErrors	See [rfc2863]
ifInUnknownProtos	See [rfc2863]
ifOutOctets	The number of bytes transmitted in the valid MAC frames (Data + Command + Beacon) including the MAC header and the FCS.
ifOutUcastPkts	The number of unicast packets received from the higher layers or relayed and transmitted by the interface
ifOutDiscards	See [rfc2863]
ifOutErrors	See [rfc2863]
ifName	A name having a local meaning (i.e. 'Cpl0')
ifInMulticastPkts	The number of multicast packets received from the interface and transmitted to the higher layers or relayed
ifInBroadcastPkts	The number of broadcast packets received from the interface and transmitted to the higher layers or relayed
ifOutMulticastPkts	The number of multicast packets received from the higher

Item IF-MIB	Application to the OFDM G3 PLC interface
	layers or relayed and transmitted by the interface
ifOutBroadcastPkts	The number of broadcast packets received from the higher layers or relayed and transmitted by the interface
ifLinkUpDownTrapEnable	See [rfc2863]. The default value is 'disable'
ifHighSpeed	Is set to 0
ifPromiscuousMode	Is set to 'true'
ifConnectorPresent	Is set to 'true'
ifAlias	See [rfc2863]
ifCounterDiscontinuityTime	See [rfc2863]. A discontinuity affects the PLC-G3-MIB meters like those of the IF-MIB.
ifStackHigherLayer	Not applicable for this interface
ifStackLowerLayer	Ditto
ifStackStatus	Ditto
ifRcvAddressAddress	The table contains the short unicast, multicast and broadcast addresses from which this interface must accept the packets and transfer them to the higher layers. See *adpGroupTable* in [MAC-API].
ifRcvAddressStatus	Ditto
ifRcvAddressType	Ditto

11.2. DEFINITIONS

```
PLC-G3-MIB DEFINITIONS ::= BEGIN

   IMPORTS
      ifIndex
         FROM IF-MIB

      OBJECT-GROUP, MODULE-COMPLIANCE
         FROM SNMPv2-CONF
      mib-2, Integer32, Unsigned32, Counter32, OBJECT-TYPE,
      MODULE-IDENTITY
         FROM SNMPv2-SMI
      TruthValue, MacAddress, TEXTUAL-CONVENTION
         FROM SNMPv2-TC;


   cplg3MIB MODULE-IDENTITY
      LAST-UPDATED "200811120000Z"
      ORGANIZATION
         "Sagem Communications"
      CONTACT-INFO
         "Email: support@sagem.com"
      DESCRIPTION
         "The MIB module for management of PHY, MAC and 6LoWPAN
         Adaptation Layers in PLC OFDM metering devices.

         Copyright (C) Sagem Communications (2008).
         This information is internal and confidential to Maxim
         Integrated Products, Inc. and Sagem Communications SAS for
         ERDF"
      REVISION "200811120000Z"
      DESCRIPTION
```

```
          "Initial version, published as part of Metering Profile

          Specification."
       ::= { mib-2 201 }


--
-- Textual conventions
--

    Eui64Address ::= TEXTUAL-CONVENTION
       DISPLAY-HINT
          "2x:2x:2x:2x:2x:2x:2x:2x"
       STATUS current
       DESCRIPTION
          "A 64-bit MAC Address"
       SYNTAX OCTET STRING (SIZE (8))

    ShortAddress ::= TEXTUAL-CONVENTION
       DISPLAY-HINT
          "4x"
       STATUS current
       DESCRIPTION
          "A 16-bit MAC or 6LoWPAN short Address"
       SYNTAX OCTET STRING (SIZE (2))

    ToneArray ::= TEXTUAL-CONVENTION
       DISPLAY-HINT
          "18x"
       STATUS current
       DESCRIPTION
          "A 72-bit string.
          The 70 first bits referred each to an OFDM tone.
          The two last bits are meaningless"
       SYNTAX OCTET STRING (SIZE (9))


--
-- Node definitions
--

    cplg3Notifications OBJECT IDENTIFIER ::= { cplg3MIB 0 }
--   No TRAP in this MIB

    cplg3Objects OBJECT IDENTIFIER ::= { cplg3MIB 1 }

--
--   The MAC Layer objects
--
    cplg3Mac OBJECT IDENTIFIER ::= { cplg3Objects 1 }

--
--   MAC Statistics Table
--
    cplg3MacTable OBJECT-TYPE
```

```
   SYNTAX SEQUENCE OF Cplg3MacEntry
   MAX-ACCESS not-accessible
   STATUS current
   DESCRIPTION
      "MAC objects for a collection of OFDM PLC G3 interfaces
      attached to a particular system.
      There will be one row in this table for each OFDM PLC G3
      interface in the system."
   ::= { cplg3Mac 1 }

cplg3MacEntry OBJECT-TYPE
   SYNTAX Cplg3MacEntry
   MAX-ACCESS not-accessible
   STATUS current
   DESCRIPTION
      "MAC objects for a particular interface to PLC medium."
   INDEX { ifIndex }
   ::= { cplg3MacTable 1 }

Cplg3MacEntry ::=
   SEQUENCE {
      cplg3MacAssociationPermit
         TruthValue,
      cplg3MacAckWaitDuration
         Unsigned32,
      cplg3MacAssociatedPanCoord
         TruthValue,
      cplg3MacBsn
         Unsigned32,
      cplg3MacCoordShortAddress
         ShortAddress,
      cplg3MacPanCoordShortAddress
         ShortAddress,
      cplg3MacDsn
         Unsigned32,
      cplg3MacMaxBe
         Unsigned32,
      cplg3MacMaxCsmaBackoffs
         Unsigned32,
      cplg3MacMaxFrameTotalWaitTime
         Unsigned32,
      cplg3MacMaxFrameRetries
         Unsigned32,
      cplg3MacMinBe
         Unsigned32,
      cplg3MacPanId
         Unsigned32,
      cplg3MacResponseWaitTime
         Unsigned32,
      cplg3MacSecurityEnabled
         TruthValue,
      cplg3MacAddress
         MacAddress,
      cplg3MacHighPriorityWindowSize
         Unsigned32,
```

```
      cplg3MacToneMask
         ToneArray
    }

cplg3MacAssociationPermit OBJECT-TYPE
   SYNTAX TruthValue
   MAX-ACCESS read-write
   STATUS current
   DESCRIPTION
      "Indication of whether a coordinator (PAN coordinator or FFD) is
      currently allowing association. A value of true indicates that
      association is permitted.
      Not relevant for a RFD."
   REFERENCE
      "IEEE802.15.4, clause 7.4.2"
   DEFVAL { false }
   ::= { cplg3MacEntry 2 }

cplg3MacAckWaitDuration OBJECT-TYPE
   SYNTAX Unsigned32
   UNITS "symbols"
   MAX-ACCESS read-write
   STATUS current
   DESCRIPTION

      "The maximum number of symbols to wait for an acknowledgment
      frame to arrive following a transmitted data frame. "
   REFERENCE
      "IEEE802.15.4, clause 7.4.2"
   ::= { cplg3MacEntry 3 }

cplg3MacAssociatedPanCoord OBJECT-TYPE
   SYNTAX TruthValue
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "Indication of whether the device is associated to the
      PAN through the PAN coordinator. A value of true indicates
      the device has associated through the PAN coordinator.
      Otherwise, the value is set to false."
   REFERENCE
      "IEEE802.15.4, clause 7.4.2"
   DEFVAL { false }
   ::= { cplg3MacEntry 4 }

cplg3MacBsn OBJECT-TYPE
   SYNTAX Unsigned32 (0..255)
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "The sequence number added to the transmitted beacon frame
      MAC command frame.
      Not relevant for a RFD"
   REFERENCE
      "IEEE802.15.4, clause 7.4.2"
```

```
      ::= { cplg3MacEntry 5 }

   cplg3MacCoordShortAddress OBJECT-TYPE
      SYNTAX ShortAddress
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
         "The 16-bit short address assigned to the coordinator
         through which the device is associated. A value of
         'FFFE'h indicates that the coordinator (PAN coordinator or FFD)
         is only using its 64-bit extended address. A value of 'FFFF'h
         indicates that this value is unknown."
      REFERENCE
         "IEEE802.15.4, clause 7.4.2"
      DEFVAL { 'FFFF'h }
      ::= { cplg3MacEntry 6 }


   cplg3MacPanCoordShortAddress OBJECT-TYPE
      SYNTAX ShortAddress
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
         "The 16-bit short address assigned to the PAN coordinator
         A value of '0000'h indicates no PAN coordinator"
      REFERENCE
         "IEEE802.15.4, clause 7.4.2"
      DEFVAL { 'FFFF'h }
      ::= { cplg3MacEntry 7 }

   cplg3MacDsn OBJECT-TYPE
      SYNTAX Unsigned32 (0..255)
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
         "The sequence number added to the transmitted data or
         MAC command frame."
      REFERENCE
         "IEEE802.15.4, clause 7.4.2"
      ::= { cplg3MacEntry 8 }

   cplg3MacMaxBe OBJECT-TYPE
      SYNTAX Unsigned32 (3..8)
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
         "The maximum value of the backoff exponent (BE) in the
         CSMA-CA algorithm."
      REFERENCE
         "IEEE802.15.4, clause 7.4.2"
      DEFVAL { 5 }
      ::= { cplg3MacEntry 10 }

   cplg3MacMaxCsmaBackoffs OBJECT-TYPE
      SYNTAX Unsigned32 (0..5)
```

```
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
         "The maximum number of backoffs the CSMA-CA algorithm
         will attempt before declaring a channel access failure."
      REFERENCE
         "IEEE802.15.4, clause 7.4.2"
      DEFVAL { 4 }
      ::= { cplg3MacEntry 11 }

   cplg3MacMaxFrameTotalWaitTime OBJECT-TYPE
      SYNTAX Unsigned32
      UNITS "symbols"
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
         "The maximum number of symbols to wait for a frame
         intended as a response to a data request frame"
      REFERENCE
         "IEEE802.15.4, clause 7.4.2"
      ::= { cplg3MacEntry 12 }

   cplg3MacMaxFrameRetries OBJECT-TYPE
      SYNTAX Unsigned32 (0..7)
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
         "The maximum number of retries allowed after a
         transmission failure."
      REFERENCE
         "IEEE802.15.4, clause 7.4.2"

      DEFVAL { 3 }
      ::= { cplg3MacEntry 13 }

   cplg3MacMinBe OBJECT-TYPE
      SYNTAX Unsigned32 (0..8)
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
         "The minimum value of the backoff exponent (BE) in the
         CSMA-CA algorithm (must be less or equal cplg3MacMaxBe "
      REFERENCE
         "IEEE802.15.4, clause 7.4.2"
      DEFVAL { 3 }
      ::= { cplg3MacEntry 14 }

   cplg3MacPanId OBJECT-TYPE

      SYNTAX Unsigned32 (0..65535)
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
         "The 16-bit identifier of the PAN on which the device is
```

```
          operating. If this value is 'FFFF'h, the device is not

          associated.
          MAX-ACCESS is read-write for a PAN coordinator and read-only
          for a FFD or RFD."
       REFERENCE
          "IEEE802.15.4, clause 7.4.2"
       DEFVAL { 'FFFF'h }
       ::= { cplg3MacEntry 15 }

    cplg3MacResponseWaitTime OBJECT-TYPE
       SYNTAX Unsigned32 (2..64)
       UNITS "aBaseSuperframeDuration"
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
          "The maximum time, in multiples of aBaseSuperframeDuration,
          a device shall wait for a response command frame to be
          available following a request command frame."
       REFERENCE
          "IEEE802.15.4, clause 7.4.2"
       DEFVAL { 32 }
       ::= { cplg3MacEntry 16 }

    cplg3MacSecurityEnabled OBJECT-TYPE
       SYNTAX TruthValue
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
          "Indication of whether the MAC sublayer has security
          enabled.
          A value of 'true' indicates that security is enabled, while
          a value of 'false' indicates that security is disabled."
       REFERENCE
          "IEEE802.15.4, clause 7.4.2"
       DEFVAL { false }
       ::= { cplg3MacEntry 17 }

--
--   The 16-bit address that the device uses to communicate
--   in the PAN may be accessed via the IF-MIB.
--
    cplg3MacAddress OBJECT-TYPE
       SYNTAX MacAddress
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
          "The EUI-48 MAC address allocated to the device during the
          manufacturing process "
       ::= { cplg3MacEntry 18 }

    cplg3MacHighPriorityWindowSize OBJECT-TYPE
       SYNTAX Unsigned32 (0..7)
       UNITS "slots"
       MAX-ACCESS read-write
```

```
      STATUS current
      DESCRIPTION
         "The high priority contention window size in number of
         slots"
      DEFVAL { 7 }
      ::= { cplg3MacEntry 19 }

   cplg3MacToneMask OBJECT-TYPE
      SYNTAX ToneArray
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
         "The Tone Mask to use during symbol formation."
      DEFVAL { '3FFFFFFFFFFFFFFFF'h }
      ::= { cplg3MacEntry 20 }

   cpl3gMacStatsTable OBJECT-TYPE
      SYNTAX SEQUENCE OF Cpl3gMacStatsEntry
      MAX-ACCESS not-accessible
      STATUS current
      DESCRIPTION
         "MAC statistics for a collection of OFDM PLC G3 interfaces
         attached to a particular system.
         There will be one row in this table for each OFDM PLC G3
         interface in the system."
      ::= { cplg3Mac 2 }

   cpl3gMacStatsEntry OBJECT-TYPE
      SYNTAX Cpl3gMacStatsEntry
      MAX-ACCESS not-accessible
      STATUS current
      DESCRIPTION
         "MAC objects for a particular interface to PLC medium.

         Other counters may be accessed via the IF-MIB:
           * successfully transmitted unicast data packets
           * successfully received unicast data packets
           * successfully transmitted multicast packets
           * successfully received multicast packets
           * successfully transmitted broadcast packets
           * successfully received broadcast packets
           * packets discarded during transmission
           * packets in error during transmission
           * packets discarded during reception
           * packets in error during reception
           * received packets refering to an unknown protocol"
      INDEX { ifIndex }
      ::= { cpl3gMacStatsTable 1 }

   Cpl3gMacStatsEntry ::=
      SEQUENCE {
         cplg3MacStatsTxCmdPacketCount
            Counter32,
         cplg3MacStatsRxCmdPacketCount
            Counter32,
```

```
            cplg3MacStatsCsmaFailCount
               Counter32,
            cplg3MacStatsCsmaCollisionCount
               Counter32,
            cplg3MacStatsPanConflictCount
               Counter32
         }

      cplg3MacStatsTxCmdPacketCount OBJECT-TYPE
         SYNTAX Counter32
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of successfully transmitted command packets"
         ::= { cpl3gMacStatsEntry 1 }

      cplg3MacStatsRxCmdPacketCount OBJECT-TYPE
         SYNTAX Counter32
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of successfully received command packets"
         ::= { cpl3gMacStatsEntry 2 }

      cplg3MacStatsCsmaFailCount OBJECT-TYPE
         SYNTAX Counter32
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of failed CSMA transmit attempts"
         ::= { cpl3gMacStatsEntry 3 }

      cplg3MacStatsCsmaCollisionCount OBJECT-TYPE
         SYNTAX Counter32
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of collisions due to busy channel or
            failed transmission"
         ::= { cpl3gMacStatsEntry 4 }

      cplg3MacStatsPanConflictCount OBJECT-TYPE
         SYNTAX Counter32
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of frames received with a bad CRC"
         ::= { cpl3gMacStatsEntry 5 }

--
--    The Neighbor Table
--
      cplg3MacNeighborTable OBJECT-TYPE
         SYNTAX SEQUENCE OF Cplg3MacNeighborEntry
         MAX-ACCESS not-accessible
```

```
   STATUS current
   DESCRIPTION
      "The Neighbor table contains information on the way
      to transmit a frame to every neighbour device"
   ::= { cplg3Mac 27 }

cplg3MacNeighborEntry OBJECT-TYPE
   SYNTAX Cplg3MacNeighborEntry
   MAX-ACCESS not-accessible
   STATUS current
   DESCRIPTION
      "An entry (conceptual row) in the cplg3MacNeighborTable."
   INDEX { ifIndex, cplg3MacNeighborShortAddress }
   ::= { cplg3MacNeighborTable 1 }

Cplg3MacNeighborEntry ::=
   SEQUENCE {
      cplg3MacNeighborShortAddress
         ShortAddress,
      cplg3MacNeighborPanId
         Unsigned32,
      cplg3MacNeighborDeviceType
         INTEGER,
      cplg3MacNeighborIsParent
         TruthValue,
      cplg3MacNeighborToneMapIndex
         Unsigned32,
      cplg3MacNeighborModulation
         INTEGER,
      cplg3MacNeighborToneMap
         ToneArray,
      cplg3MacNeighborGain
         Unsigned32,
      cplg3MacNeighborPreemphasisGain
         Unsigned32,
      cplg3MacNeighborLqi
         Unsigned32,
      cplg3MacNeighborPhase
         Integer32,
      cplg3MacNeighborAge
         Unsigned32
    }

cplg3MacNeighborShortAddress OBJECT-TYPE
   SYNTAX ShortAddress
   MAX-ACCESS not-accessible
   STATUS current
   DESCRIPTION
      "The short address of the Neighbor"
   ::= { cplg3MacNeighborEntry 1 }

cplg3MacNeighborPanId OBJECT-TYPE
   SYNTAX Unsigned32 (0..65535)
   MAX-ACCESS read-only
   STATUS current
```

```
         DESCRIPTION
            "The PAN Identifier of the Neighbor"
         DEFVAL { 'FFFF'h }
         ::= { cplg3MacNeighborEntry 2 }


      cplg3MacNeighborDeviceType OBJECT-TYPE
         SYNTAX INTEGER
            {
            coordinator(0),
            router(1),
            endDevice(2)
            }
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The device type of the neighbor entry:
            (1) means PAN coordinator
            (2) means full function device
            (3) means reduced function device"
         DEFVAL { router }
         ::= { cplg3MacNeighborEntry 3 }

      cplg3MacNeighborIsParent OBJECT-TYPE
         SYNTAX TruthValue
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The value 'true' indicates that the neighbor is a topological parent of
the device"
         ::= { cplg3MacNeighborEntry 4 }

      cplg3MacNeighborToneMapIndex OBJECT-TYPE
         SYNTAX Unsigned32 (0..2047)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The Index of the Tone Map to use when transmitting
            a frame to the Neighbor"
         DEFVAL { 0 }
         ::= { cplg3MacNeighborEntry 5 }

      cplg3MacNeighborModulation OBJECT-TYPE
         SYNTAX INTEGER
            {
            robo(0),
            dbpsk(1),
            dqpsk(2)
            }
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The modulation type to use when transmitting a frame
            to the Neighbor"
```

```
   DEFVAL { robo }

   ::= { cplg3MacNeighborEntry 6 }

cplg3MacNeighborToneMap OBJECT-TYPE
   SYNTAX ToneArray
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "The Tone Map to use when transmitting a frame to the
      Neighbor"
   DEFVAL { '3FFFFFFFFFFFFFFFFF'h }
   ::= { cplg3MacNeighborEntry 7 }

cplg3MacNeighborGain OBJECT-TYPE
   SYNTAX Unsigned32 (0..63)
   MAX-ACCESS read-only
   STATUS current

   DESCRIPTION
      "The gain to use when transmitting a frame to the Neighbor"
   DEFVAL { 63 }
   ::= { cplg3MacNeighborEntry 8 }

cplg3MacNeighborPreemphasisGain OBJECT-TYPE
   SYNTAX Unsigned32
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "An array of eight times 4 bits to control the gain for
      each 10 kHz-wide spectrum band when transmitting a frame
      to the Neighbor"
   DEFVAL { 'FFFFFFFF'h }
   ::= { cplg3MacNeighborEntry 9 }

cplg3MacNeighborLqi OBJECT-TYPE
   SYNTAX Unsigned32 (0..255)
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "The Link Quality Indicator when transmitting a frame to the
      Neighbor"
   DEFVAL { 0 }
   ::= { cplg3MacNeighborEntry 10 }

cplg3MacNeighborPhase OBJECT-TYPE
   SYNTAX Integer32 (-180..180)
   UNITS "Degrees"
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "The Phase difference on the 50 Hz AC signal
      Delta_Ph = (local_Ph - neighbor_Ph)"
   ::= { cplg3MacNeighborEntry 11 }
```

```
cplg3MacNeighborAge OBJECT-TYPE
   SYNTAX Unsigned32 (0..255)
   UNITS "minutes"
   MAX-ACCESS read-only
   STATUS current
   DESCRIPTION
      "The remaining lifetime of this entry in minutes.
      Upon successful reception of a ToneMap.response, the value
      is set to adpMaxAgeTime. When it reaches 0, a ToneMap.request
      should be associated to the next frame sent to the Neighbor"
   DEFVAL { 0 }
   ::= { cplg3MacNeighborEntry 12 }

cplg3Conformance OBJECT IDENTIFIER ::= { cplg3MIB 2 }

cplg3Compliances OBJECT IDENTIFIER ::= { cplg3Conformance 1 }

cplg3Compliance MODULE-COMPLIANCE
   STATUS current
   DESCRIPTION
      "The compliance statement for Devices that implement PLC G3.
      All groups are mandatory."
   MODULE -- this module
      MANDATORY-GROUPS { cplg3MacObjectGroup, cplg3MacStatsGroup,
                         cplg3MacNeighborGroup }
   ::= { cplg3Compliances 1 }

cplg3Groups OBJECT IDENTIFIER ::= { cplg3Conformance 2 }

cplg3MacObjectGroup OBJECT-GROUP
   OBJECTS { cplg3MacAssociationPermit, cplg3MacAckWaitDuration,
             cplg3MacAssociatedPanCoord, cplg3MacBsn,
             cplg3MacCoordShortAddress, cplg3MacPanCoordShortAddress,
             cplg3MacDsn, cplg3MacMaxBe, cplg3MacMaxCsmaBackoffs,
             cplg3MacMaxFrameTotalWaitTime, cplg3MacMaxFrameRetries,
             cplg3MacMinBe, cplg3MacPanId, cplg3MacResponseWaitTime,
             cplg3MacSecurityEnabled, cplg3MacAddress,
             cplg3MacHighPriorityWindowSize, cplg3MacToneMask }
   STATUS current
   DESCRIPTION
      "A collection of objects for managing the PLC G3
      MAC layer."
   ::= { cplg3Groups 1 }

cplg3MacStatsGroup OBJECT-GROUP
   OBJECTS { cplg3MacStatsTxCmdPacketCount,
             cplg3MacStatsRxCmdPacketCount,
             cplg3MacStatsCsmaFailCount,
             cplg3MacStatsCsmaCollisionCount,
             cplg3MacStatsPanConflictCount }
   STATUS current
   DESCRIPTION
      "A collection of objects for managing the PLC G3
      MAC Statistics."
   ::= { cplg3Groups 2 }
```

```
   cplg3MacNeighborGroup OBJECT-GROUP
      OBJECTS { cplg3MacNeighborPanId, cplg3MacNeighborDeviceType,
                cplg3MacNeighborIsParent, cplg3MacNeighborToneMapIndex,
                cplg3MacNeighborModulation, cplg3MacNeighborToneMap,
                cplg3MacNeighborGain, cplg3MacNeighborPreemphasisGain,
                cplg3MacNeighborLqi, cplg3MacNeighborPhase,
                cplg3MacNeighborAge }
      STATUS current
      DESCRIPTION
         "A collection of objects for managing the Neighbor Table"
      ::= { cplg3Groups 3 }


END
```

12. APPENDIX B: FILE TRANSFER MANAGEMENT MIB: FLM-G3-MIB (NORMATIVE)

This appendix specifies the portion of the MIB, called FLM-G3-MIB, that is devolved to the management of File Transfers.

12.1. DEFINITIONS

```
FLM-G3-MIB DEFINITIONS ::= BEGIN

  IMPORTS
    OBJECT-GROUP, MODULE-COMPLIANCE
      FROM SNMPv2-CONF
    mib-2, Unsigned32, OBJECT-TYPE, MODULE-IDENTITY
      FROM SNMPv2-SMI
    DisplayString, DateAndTime, TruthValue
      FROM SNMPv2-TC;


  flmg3MIB MODULE-IDENTITY
    LAST-UPDATED "200811120000Z"
    ORGANIZATION
      "Sagem Communications"
    CONTACT-INFO
      "Email: support@sagem.com"
    DESCRIPTION
      "The MIB module for management of Files Transfers in PLC OFDM
      metering devices. It provides an SNMP SMIv2 version of
      BroadBand Forum CWMP-based File Management system.

      Copyright (C) Sagem Communications (2008).
      This information is internal and confidential to Maxim
      Integrated Products, Inc. and Sagem Communications SAS for
      ERDF"
    REVISION "200811120000Z"
    DESCRIPTION
      "Initial version, published as part of Metering Profile
      Specification."
    ::= { mib-2 200 }



--
-- Node definitions
--

--
--  Notifications
--
  flmg3Notifications OBJECT IDENTIFIER ::= { flmg3MIB 0 }
--    No TRAP in this MIB

  flmg3Objects OBJECT IDENTIFIER ::= { flmg3MIB 1 }

--
```

```
--   The Device Management objects
--
    flmg3Dev OBJECT IDENTIFIER ::= { flmg3Objects 1 }

    flmg3DevSerialNumber OBJECT-TYPE
      SYNTAX DisplayString (SIZE (64))
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
        " Serial number of the Device."
      REFERENCE
        "BBF TR-106, clause 3.4"
      ::= { flmg3Dev 1 }

    flmg3DevHardwareVersion OBJECT-TYPE
      SYNTAX DisplayString (SIZE (64))
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
        " A string identifying the particular Device model and
        version."
      REFERENCE
        "BBF TR-106, clause 3.4"
      ::= { flmg3Dev 2 }

    flmg3DevSoftwareVersion OBJECT-TYPE
      SYNTAX DisplayString (SIZE (64))
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
        " A string identifying the software version currently
        installed in the Device.
        To allow version comparisons, this element SHOULD be in the
        form of dot-delimited integers, where each successive integer
        represents a more minor category of variation. For example,
        3.0.21 where the components mean: Major.Minor.Build."
      REFERENCE
        "BBF TR-106, clause 3.4"
      ::= { flmg3Dev 3 }

    flmg3DevDateTime OBJECT-TYPE
      SYNTAX DateAndTime
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
        "The current date and time, with time zone information (if
        known).
        If the real data and time cannot be determined, this shall
        represent elapsed time from boot relative to the standard
        epoch '1970-1-1,0:0:0.0'.  In other words, if this agent has
        been up for 3 minutes and not been able to determine what the
        actual date and time are, this object will return the value
        '1970-1-1,0:03:0.0'."
      ::= { flmg3Dev 4 }
```

```
--
--   The File Transfer Control objects
--
     flmg3Ctl OBJECT IDENTIFIER ::= { flmg3Objects 2 }

--     Managed upgrades
     flmg3CtlUpgradesManaged OBJECT-TYPE
       SYNTAX TruthValue
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
         "Indicates whether or not the Manager will manage upgrades
         for the Device. If true, the Device must not accept unmanaged
         upgrades. If false, the Device should accept unmanaged
         upgrades."
       ::= { flmg3Ctl 1 }

     flmg3CtlAdminStatus OBJECT-TYPE
       SYNTAX INTEGER
         {
         running(1),
         upgradesNow(2),
         rebootNow(3)
         }
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
         "Indicates the desired state of the Device.
         When a Device initializes, it is placed in the running (1)
         state. If placed in the ugradeNow (2) state, the Device must
         launch an upgrade process as defined by the following objects.
         If placed in the rebootNow (3), the Device must reboot
         immediately"
       ::= { flmg3Ctl 2 }

     flmg3CtlCommandKey OBJECT-TYPE
       SYNTAX DisplayString (SIZE (64))
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
         " A string identifying a specific action to proceed.
         This object should be provisioned prior to the modification
         of flmg3CtlAdminStatus "
       REFERENCE
         "BBF TR-069, clause A.3.3"
       ::= { flmg3Ctl 3 }

     flmg3CtlFileType OBJECT-TYPE
       SYNTAX INTEGER { firmware(1) }
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
         "The type of the file to transfer.
         Initially, a single value is defined: firmware (1) indicating
         a firmware Upgrade Image.
```

```
    This object should be provisioned prior to the modification
    of flmg3CtlAdminStatus "
  REFERENCE
    "BBF TR-069, clause A.3.3"
  ::= { flmg3Ctl 4 }

flmg3CtlUrl OBJECT-TYPE
  SYNTAX DisplayString (SIZE (256))
  MAX-ACCESS read-write
  STATUS current
  DESCRIPTION
    "URL specifying the file location in the file server.
    It must be in the form:  tftp://host:port/path
    The host portion of the URL must be the IPv6 address of the
    file server in lieu of a host name.
    If the Device receives multiple Download requests with the
    same source URL, the Device MUST perform each download as
    requested, and MUST NOT assume that the content of the file
    to be downloaded is the same each time.
    This object should be provisioned prior to the modification
    of flmg3CtlAdminStatus "
  REFERENCE
    "BBF TR-069, clause A.3.3"
  ::= { flmg3Ctl 5 }

flmg3CtlFileSize OBJECT-TYPE
  SYNTAX Unsigned32
  MAX-ACCESS read-write
  STATUS current
  DESCRIPTION
    "The size of the file to be downloaded in bytes.
    The FileSize argument is intended as a hint to the Device,
    which the Device MAY use to determine if it has sufficient
    space for the file to be downloaded, or to prepare space to
    accept the file.
    The Manager MAY set this value to zero. The Device MUST
    interpret a zero value to mean that that the Manager has
    provided no information about the file size. In this case,
    the Device MUST attempt to proceed with the download under
    the presumption that sufficient space is available, though
    during the course of download, the Device might determine
    otherwise.
    The Manager SHOULD set the value of this parameter to the
    exact size of the file to be downloaded. If the value is
    non-zero, the Device MAY reject the Download request on the
    basis of insufficient space. If the Device attempts to
    proceed with the download based on the value of this object,
    but the actual file size differs from the value of this

    object, this could result in a failure of the download.
    However, the Device MUST NOT cause the download to fail
    solely because it determines that the value of this argument
    is inaccurate.
    This object should be provisioned prior to the modification
    of flmg3CtlAdminStatus "
```

```
      REFERENCE
        "BBF TR-069, clause A.3.3"
      ::= { flmg3Ctl 6 }

    flmg3CtlDeviceFileName OBJECT-TYPE
      SYNTAX DisplayString (SIZE (256))
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
        " The name of the file to be used on the Device file system.
        This argument MAY be left empty if the file name can be
        extracted from the downloaded file itself, or from the URL
        object, or if no file name is needed. If this value is
        specified, but the file name is also indicated by another
        source (for example, if it is extracted from the downloaded
        file itself), this object value MUST be ignored.

        If the file name is used, the downloaded file would replace
        any existing file of the same name.
        This object should be provisioned prior to the modification
        of flmg3CtlAdminStatus "
      REFERENCE
        "BBF TR-069, clause A.3.3"
      ::= { flmg3Ctl 7 }

    flmg3CtlDelaySeconds OBJECT-TYPE
      SYNTAX Unsigned32
      MAX-ACCESS read-write
      STATUS current
      DESCRIPTION
        " This argument has different meanings for Unicast and
        Multicast downloads. For Unicast downloads it is the number
        of seconds before the Device will initiate the download.
        For Multicast downloads the Device will initiate the download
        immediately and it is the number of seconds available for
        initiating, performing and applying the download.
        The Device MUST attempt to perform the download within the
        time window specified above even if the Device reboots one or
        more times prior to that time.
        This object should be provisioned prior to the modification
        of flmg3CtlAdminStatus "
      REFERENCE
        "BBF TR-069, clause A.3.3"
      ::= { flmg3Ctl 8 }

--    Transfer status
    flmg3CtlOperStatus OBJECT-TYPE
      SYNTAX INTEGER
        {
        inProgress(1),
        complete(2),
        failed(3),
        other(4)
        }
      MAX-ACCESS read-only
```

```
      STATUS current
      DESCRIPTION
        "Provides the current state of the Device:
        inProgress (1) indicates the action mentioned in ParameterKey
        is in progress
        complete (2) indicates its full completion
        failed (3) indicates the action has failed."
      ::= { flmg3Ctl 9 }

    flmg3CtlParameterKey OBJECT-TYPE
      SYNTAX DisplayString (SIZE (64))
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
        "A string identifying the last action."
      REFERENCE
        "BBF TR-106, clause 3.4"
      ::= { flmg3Ctl 10 }

    flmg3CtlStartTime OBJECT-TYPE
      SYNTAX DateAndTime
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
        "The date and time transfer was started in UTC. The Device
        SHOULD record this information and report it in this object,
        but if this information is not available, the value of this
        object MUST be set to the Unknown Time value:
        '1970-1-1,0:0:0.0'."
      REFERENCE
        "BBF TR-069, clause A.3.3"
      ::= { flmg3Ctl 11 }

    flmg3CtlCompleteTime OBJECT-TYPE
      SYNTAX DateAndTime
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
        "The date and time transfer was completed and applied in UTC.
        The Device SHOULD record this information and report it in
        this object, but if this information is not available, the
        value of this object MUST be set to the Unknown Time value:
        '1970-1-1,0:0:0.0'."
      REFERENCE
        "BBF TR-069, clause A.3.3"
      ::= { flmg3Ctl 12 }

--
--  Conformance statements
--
    flmg3Conformance OBJECT IDENTIFIER ::= { flmg3MIB 2 }

--
--  Compliances
--
```

```
    flmg3Compliances OBJECT IDENTIFIER ::= { flmg3Conformance 1 }

    flmg3Compliance MODULE-COMPLIANCE
      STATUS current
      DESCRIPTION
        "The compliance statement for Devices that implement
        the management of file transfers in PLC OFDM devices.
        All groups are mandatory."
      MODULE -- this module
        MANDATORY-GROUPS { flmg3DevObjectGroup, flmg3CtlObjectGroup }
      ::= { flmg3Compliances 1 }

--
--  Compliance groups
--
    flmg3Groups OBJECT IDENTIFIER ::= { flmg3Conformance 2 }

    flmg3DevObjectGroup OBJECT-GROUP
      OBJECTS { flmg3DevSerialNumber,
                flmg3DevHardwareVersion,
                flmg3DevSoftwareVersion,
                flmg3DevDateTime }
      STATUS current
      DESCRIPTION
        "A collection of objects for managing the main Device
        information."
      ::= { flmg3Groups 1 }

    flmg3CtlObjectGroup OBJECT-GROUP
      OBJECTS { flmg3CtlUpgradesManaged,
                flmg3CtlAdminStatus,
                flmg3CtlCommandKey,
                flmg3CtlFileType,
                flmg3CtlUrl,
                flmg3CtlFileSize,
                flmg3CtlDeviceFileName,
                flmg3CtlDelaySeconds,
                flmg3CtlOperStatus,
                flmg3CtlParameterKey,
                flmg3CtlStartTime,
                flmg3CtlCompleteTime }
      STATUS current
      DESCRIPTION
        "A collection of objects for controlling the file transfers
        in PLC OFDM devices."
      ::= { flmg3Groups 2 }


  END
```

13. APPENDIX C: INITIAL CONFIGURATION AND CONFIGURATION MANAGEMENT (INFORMATIVE)

This appendix defines the correspondence between the initial configuration parameters used by LBP and those contained in the MIB.

Table 8 – Correspondence between LBP parameters and MIB objects

LBP Parameter	Attr-ID	M	Description	MIB Object
PAN_ID	1	P	PAN identifier	cplg3MacPanId
PAN_type	2	P	Secured / closed / open. Normally 'secured' and never 'open' in the case of PLC G3	cplg3MacSecurityEnabled
Address_of_LBS	3	P	16-bit address of the PAN coordinator	cplg3MacPanCoordShortAddress
Join_Time	4	P	Indicates the moment at which the equipment must start the procedure to join the target PAN	Not used initially by PLC G3
Role_of_Device	5	D	Indicates whether the equipment must play the role of agent (and allow the association of other equipment items)	cplg3MacAssociationPermit
Allow_LBA_To_Send_PSI	6	P	Allows the equipment to add the PSIs	Not applicable in the MIB. Functioning internal to the LBP protocol
Short_Addr	7	D	16-bit address assigned to the equipment	ifPhysAddress
Short_Addr_Distribution	8	P	Centralized or distributed assignment of the 16-bit address	Not applicable. Always centralized for CPLG3.
Date_Time	32	P	The current time and date	flmg3DevDateTime
IPv6_Addr	33	D	Set of parameters relative to the assignment of the IPv6 address. See the IAADDR option of DHCPv6 [rfc3315]	ipAddressAddr
Router_Advertisement	34	P	Set of routing parameters. See the Router Advertisement Message of [rfc4861]	ipv6IpDefaultHopLimit ipAddressPrefixPrefix ipAddressPrefixLength ipAddressPrefixAdvPreferredLifetime ipAddressPrefixAdvValidLifetime ipDefaultRouterAddress
MAC_Attributes	35	P	Set of MAC configuration parameters	cplg3MacAckWaitDuration cplg3MacMaxBe cplg3MacMaxCsmaBackoffs cplg3MacMaxFrameTotalWaitTime cplg3MacMaxFrame retries cplg3MacMinBe cplg3MacResponseWaitTime cplg3MacHighPriorityWindowSize
ADP_Attributes	36	P	Set of 6LoWPAN configuration parameters	lowpanAckTimeout lowpanBroadcastRetries
SW_Attributes	37	P	Set parameters allowing the initial updating of the firmware	flmg3CtlUpgradesManaged flmg3CtlCommandKey flmg3CtlUrl flmg3CtlDelaySeconds
DHCPv6_Container	38	P	DHCPv6 options container [rfc3315]	
DHCPv4_Container	39	P	DHCPv4 options container	