International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.9962

Amendment 1

(07/2020)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Access networks – In premises networks

Unified high-speed wire-line based home networking transceivers – Management specification

Amendment 1

Recommendation ITU-T G.9962 (2018) – Amendment 1

International Telecommunication Union

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999
Metallic access networks	G.9700–G.9799
Optical line systems for local and access networks	G.9800–G.9899
In premises networks	**G.9900–G.9999**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.9962

Unified high-speed wire-line based home networking transceivers – Management specification

Amendment 1

Summary

Recommendation ITU-T G.9962 specifies the physical and data link layer management for the ITU-T G.996x-series home networking transceiver specifications. It defines common management parameters and protocols for all ITU-T G.996x-series Recommendations for the purpose of device configuration, status and performance management, fault monitoring and diagnostics. It also provides management functionalities to coordinate multiple domains. It includes support for LCMP communication through the L1 and L6 interfaces.

Amendment 1 includes a new logical interface between the security controller entity and the domain master management entity.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.9962	2013-07-12	15	11.1002/1000/11901
1.1	ITU-T G.9962 (2013) Amd.1	2013-08-29	15	11.1002/1000/12005
2.0	ITU-T G.9962	2014-10-14	15	11.1002/1000/12084
2.1	ITU-T G.9962 (2014) Amd. 1	2016-04-13	15	11.1002/1000/12821
2.2	ITU-T G.9962 (2014) Cor. 1	2016-11-13	15	11.1002/1000/13114
3.0	ITU-T G.9962	2018-11-29	15	11.1002/1000/13777
3.1	ITU-T G.9962 (2018) Cor. 1	2020-03-15	15	11.1002/1000/14224
3.2	ITU-T G.9962 (2018) Amd. 1	2020-07-07	15	11.1002/1000/14225

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T G.9962

Unified high-speed wire-line based home networking transceivers – management specification

Amendment 1

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T G.9962 (2018) plus its Corrigendum 1.

1 Scope

This Recommendation specifies the physical and data link layer management for the ITU-T G.996x-series home networking transceiver specifications. It defines the management architecture, protocols and common management parameters, for all ITU-T G.996x-series Recommendations. More specifically, this Recommendation includes the following:

– Architecture and reference model for management layer;

– Management protocols defined in [ITU-T G.9980], [BBF TR-069], necessary for device configuration, status and performance management, fault monitoring, and diagnostics and security;

– Management parameters defined in [BBF TR-181 I2A8] for transparent integration with remote management functionality;

– Global master (GM) functionality that facilitates coordination of multiple ITU-T G.996x domains;

– Support for Layer 2 Configuration and Management Protocol (LCMP).

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.9960] Recommendation ITU-T G.9960 (2019), *Unified high-speed wire-line based home networking transceivers – System architecture and physical layer specification.*

[ITU-T G.9961] Recommendation ITU-T G.9961 (2019), *Unified high-speed wire-line based home networking transceivers – Data link layer specification.*

[ITU-T G.9963] Recommendation ITU-T G.9963 (2019), *Unified high-speed wire-line based home networking transceivers – Multiple input/multiple output specification.*

[ITU-T G.9964] Recommendation ITU-T G.9964 (2011), *Unified high-speed wire-line based home networking transceivers – Power spectral density specification*.

[ITU-T G.9980] Recommendation ITU-T G.9980 (2012), *Remote management of customer premises equipment over broadband networks – Customer premises equipment WAN Management Protocol*.

[BBF TR-069] Broadband Forum TR-069 (2013), *CPE WAN Management Protocol*.

[BBF TR-181 I2A8] Broadband Forum TR-181 Issue 2, Amendment 12 (2018), *Device data model for TR-069*[1].

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

Unless otherwise noted, the definitions in [ITU-T G.9960] and [ITU-T G.9961] shall apply.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 client: An application entity distinguished in the network by its unique address (e.g., MAC address).

3.2.2 global master (GM): A function that provides coordination between different domains (such as communication resources, priority setting, policies of domain masters and crosstalk mitigation). A global master may also convey management functions initiated by the remote management system (e.g., the Broadband Forum CPE WAN management protocol) to support broadband access.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AE Application Entity

DLL Data Link Layer

DM Domain Master

DME DLL Management Entity

DMME Domain Master Management Entity

GM Global Master

GME Global Master Entity

LCMP Layer 2 Configuration and Management Protocol

LLC Logical Link Control

LSB Least Significant Bit

MCS Management, Control and Security

MSB Most Significant Bit

NME Node Management Entity

NMS Network Management System

PHY Physical

PME PHY Management Entity

SC Security Controller

---

[1] See also http://www.broadband-forum.org/cwmp/tr-181-2-8-0.html for the root object definitions.

SCE Security Controller Entity

5 Conventions

5.1 Format of the primitive parameters

~~None.~~

Table 5-1 provides the possible format to be applied to the parameters used in the primitives described in this Recommendation.

Table 5-1 – MNGMT_TYPE.IND parameters

Format	Possible values
Binary(N)	N-bit concatenation
Boolean	True or False
EtherType	4 hexadecimal digits (digits 0-9, letters A-F or a-f). ([0-9A-Fa-f][0-9A-Fa-f]){4}
MAC Address	12 hexadecimal digits (digits 0-9, letters A-F or a-f) displayed as six pairs of digits separated by colons. ([0-9A-Fa-f][0-9A-Fa-f]:){5}([0-9A-Fa-f][0-9A-Fa-f])

6 Architecture and reference model

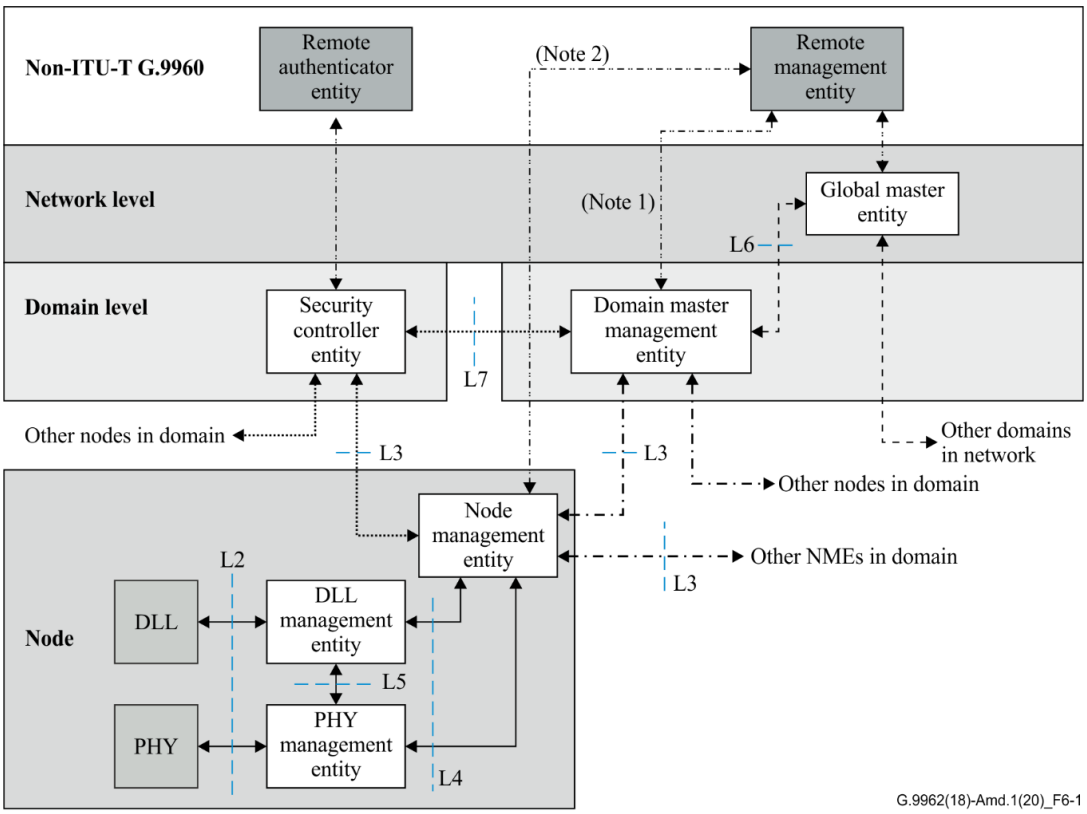
6.1 Architecture

A model of the [ITU-T G.9960] management, control, and security (MCS) architecture is depicted in Figure 6-1. The model consists of various entities located either within nodes, within a domain, or external to the domain. MCS entities provide management, control, and security of the layer they reside in as well as services and interfaces to enable MCS communications.

The structure of MCS begins with the layers of the node; the physical (PHY) layer and the data link layer (DLL). Each of these has a specific MCS entity. Above these in the MCS hierarchy, but still within Layer 2, is the node management entity (NME), which is responsible for managing the node's overall functions. Outside of the node are two entities that reside in the same domain as the node. These are the security controller entity (SCE) and the domain master management entity (DMME). These manage and control their specific areas of responsibility (e.g., security for the SCE) within the domain. These two entities are still within Layer 2 as they are solely functioning to facilitate Layer 2 activities. These two entities are considered to operate at the domain level, unlike the node located ones that operate at the node or device level. The next entity is the global master entity (GME). This entity is defined as external to the domain, performing management and control functions for all domains within a specific home network. Global master (GM) functions are logical and able to be distributed among its managed domain masters (DMs). As GM functions concern actions that span multiple domains within a common network, it is referenced as operating at the network level for logical representation of its place in the MCS hierarchy. This is an arbitrary assignment given the logical nature of the GM. Entities that perform functions above the security controller (SC) and the GM or, in its absence the DM, are considered to be non-ITU-T G.9960 entities and out of scope. They are described in summary here as they may exist and effect the operation of the entities lower than them in the hierarchy.

The SC and DM are depicted as separate entities as they might or might not be located within the same device and might or might not be associated with the same node.

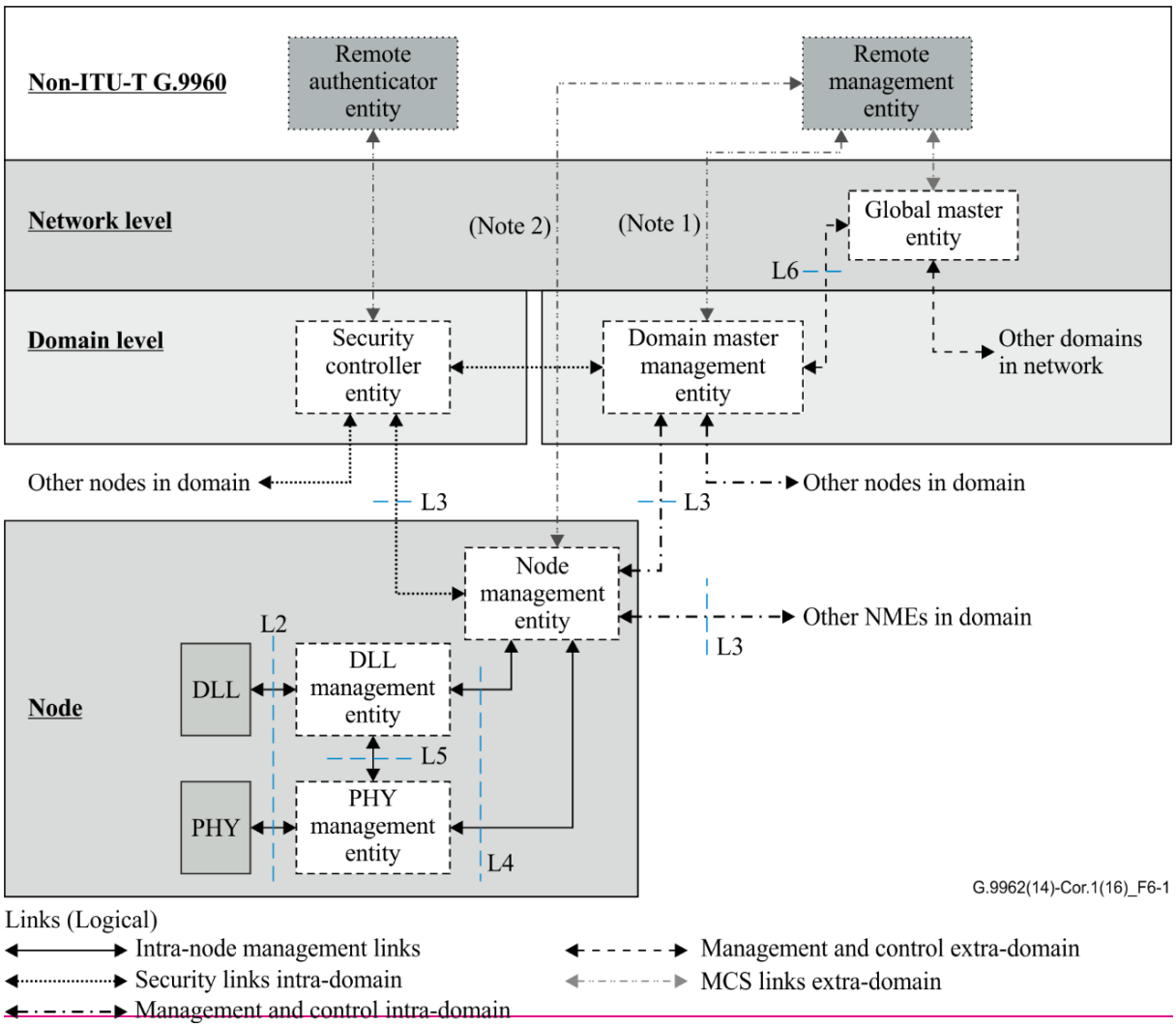
NOTE – the SC itself may be a proxy function versus a standalone entity, as it may be only a local presence of a remote authenticating system/entity that is out of scope of [ITU-T G.9960]. The internal operation and structure of the SC is as well out of scope, only its operations facing into the domain are within scope of [ITU-T G.9960], such operations as represented by its messaging and functions as described in clauses 8 and 9 of [ITU-T G.9961].



Links (Logical)

- Intra-node management links
- Security links intra-domain
- Management and control intra-domain
- Management and control extra-domain
- MCS links extra-domain

NOTE 1 – In the absence of a GME or when the GM functions are distributed, the DMME may communicate directly with the remote management entity.
NOTE 2 – The remote management entity may communicate with select nodes usings specific read/write functions.



~~NOTE 1 – In the absence of a GME or when the GM functions are distributed, the DMME may communicate directly with the remote management entity.~~

~~NOTE 2 – The remote management entity may communicate with select nodes using specific read/write functions.~~

Figure 6-1 – Architecture of management, control and security

At the device level within the same domain, management and control messages are exchanged between node NMEs and between node NMEs and Application Entities (AEs).

An AE may exchange management and control messages with the NME in its device or with another node's NME in the same domain (L1 interface) using the LCMP protocol (see clause 8.22 of [ITU-T G.9961]). Nodes exchange management and control messages between NMEs to facilitate communications between nodes (L3 interface). These interactions are illustrated in Figure 6-2 and discussed at length in clause 7 of [ITU-T G.9960] and clause 8 of [ITU-T G.9961].

Specific AE to AE communications are outside of scope of [ITU-T G.9960].

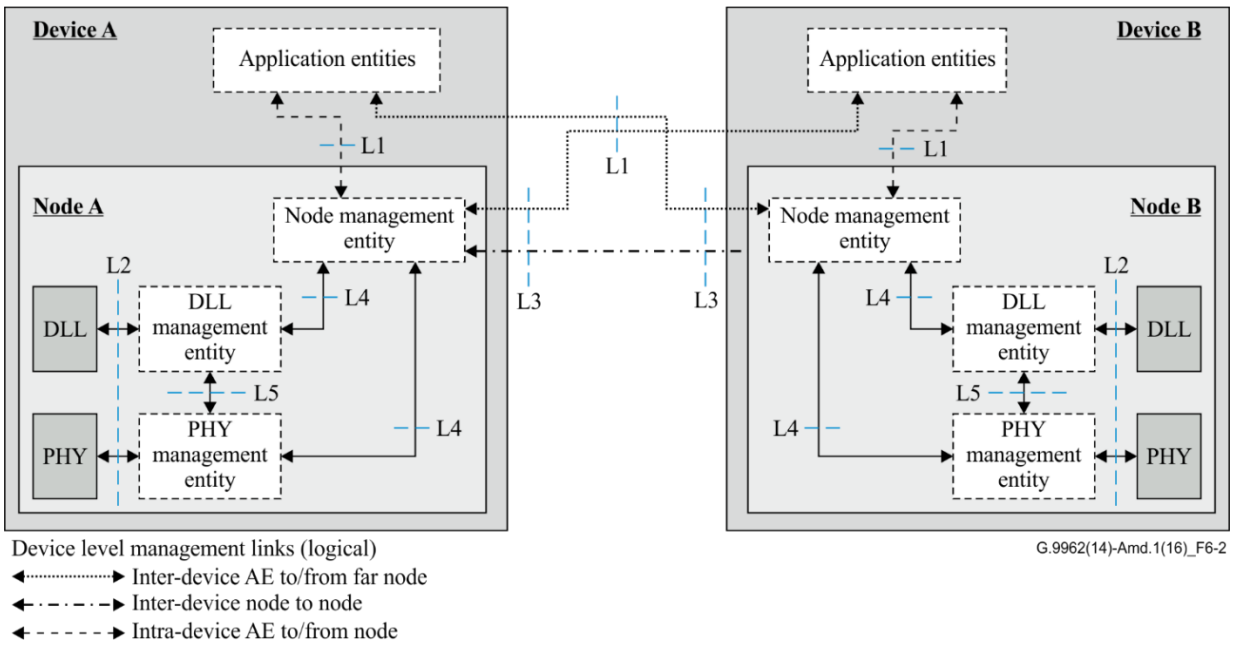


Figure 6-2 – Device level management links

6.1.1 Overall MCS structure

The MCS entities are associated with physical and network components of the [ITU-T G.9960] architecture. Each node has a PHY layer and a DLL, with each of these having its own management entity, the PHY management entity (PME) and the DLL management entity (DME), respectively. These entities are under control of the node management entity (NME). The NME is under control of the domain master management entity (DMME) as well it may receive commands from application entities above the node's A interface. Further, the node must be authenticated and its security status controlled by the security controller entity (SCE). The SCE and the DMME communicate between themselves for management of security in the network (e.g., node authentication failure notification to the DMME from SCE). The domain may be part of a larger [ITU-T G.9960] network consisting of itself and possibly several other [ITU-T G.9960] domains under control of a global master entity (GME). The GME may be under the control of a remote management entity while the SCE may be under the control of, or depend on functions located in, a remote authenticator entity. Neither the remote management entity nor the remote authenticator are defined within [ITU-T G.9960] other than as references to MCS services provided by entities that control entities defined within [ITU-T G.9960].

6.1.2 Management and control entities

The management and control functions and their interactions are as follows.

6.1.2.1 PHY management entity (PME)

The PME manages the node's PHY layer. The PME provides the PHY services to the DME and NME.

6.1.2.2 DLL management entity (DME)

The DME manages the node's DLL. The DME provides the DLL's services to the PME and NME.

6.1.2.3 Node management entity (NME)

The NME manages the node through the PME and DME while also providing domain-interfacing functions as needed for registration, authentication, and bandwidth control. The NME provides a node management service to the DME and PME while also providing a node service interface and client functions to the SCE and DMME.

6.1.2.3.1 L1 interface primitives

The following primitives describe the L_1 interface

Table 6-1 – Authentication primitives summary

Primitive type	Direction	Description
EA_AUTH.IND(MAC,Status)	AE → NME	External Authentication authentication status (see Table 6-2)
EA_SET_KEYS.IND(MAC, TK Seed, GTK Seed)	AE → NME	Key seeds to be used by the node to generate encryption keys when using external authentication (see Table 6-3)
MNGMT_TYPE.IND(EtherType, MAC)	AE → NME	Classify incoming APDUs with this EtherType and MAC as APDUs carrying management data (see Table 6-4)

Table 6-2 – AUTH.IND parameters

Parameter	Format (See clause 5.1)	Description
MAC	MAC Address	MAC address of the supplicant for which this authentication status indication is provided
Status	Boolean	Indicates the status of the authentication. True: Authentication granted False: Authentication not granted

Table 6-3 – EA_SET_KEYS.IND parameters

Parameter	Format (See clause 5.1)	Description
MAC	MAC Address	MAC address of the supplicant for which this authentication status indication is provided
TK Seed	Binary(128)	TK seed be used to generate encryption keys (see Annex D of [ITU-T G.9961])
GTK Seed	Binary(128)	GTK seed to be used to generate encryption keys (see Annex D of [ITU-T G.9961])

Table 6-4 – MNGMT_TYPE.IND parameters

Parameter	Format (See clause 5.1)	Description
EtherType	EtherType	Ethertype of the frames to be classified as carrying management information
MAC	MAC Address	Source MAC address of the frames that need to be classified

6.1.2.3.2 L7 interface primitives

The following primitives describe the L_7 interface

Table 6-4 – Authentication primitives summary

Primitive type	Direction	Description
EA_AUTH.IND(MAC,Status)	NME → SC	External Authentication authentication status (see Table 6-2)
REG_NEWNODE.IND(Device ID)	NME → SC	Convey the identity of a new registered node

6.1.2.3.31 Application entities and NME communication (L1 interface)

For the case when the application entity and the NME are physically separated, the messages passed between them shall use the LCMP protocol specified in clause 8.22 of [ITU-T G.9961] along with the LCMPValue field specified in Annex C.

NOTE – While it may occur with certain implementations that the application entity may reside in the same physical device as the NME, there remains the need to pass messages between these entities. In this case, the formats of these intra-device messages are vendor specific.

6.1.2.4 Domain master management entity (DMME)

The domain master management entity manages and controls the nodes in its domain through each node's NME by way of management messages and the MAP. The DMME also manages communications with neighbouring domains to address interference mitigation. The DMME provides the domain management services to each node within its domain as well as the SCE while providing domain-level service interface and client functions to the GME or a remote management entity if there is no GME.

6.1.2.5 Global master entity (GME)

The Global master manages all domains it is responsible for through the domains' individual DMME. The GME provides the network management services to each [ITU-T G.9960] domain within its network while providing network-level service interface and client functions to the remote management entity and the WAN its network is a part of.

6.1.2.5.1 DMME and GME communications (L6 interface)

For the case when the DMME and GME are physically separated, the messages passed between them may use the G.hn LCMP protocol as described in Annex B.

NOTE – While it may occur with certain implementations that the DMME and GME are located within the same physical device, there remains the need to pass messages between these entities. In this case, the formats of these intra-device messages are vendor specific.

6.1.2.6 Security controller entity (SCE)

The security controller (SC) manages security for the domain as specified in clause 9 (Security) of [ITU-T G.9961]. The SC may be under control of a remote authenticator entity. The SCE provides security services for the nodes in the domain as well as for the domain master.

6.1.2.6.1 DMME and SCE communications (L7 interface)

For the case when the DMME and SCE are physically separated (i.e., not in the same node), the messages passed between them are specified within clause 9 of [ITU-T G.9961].

NOTE – While it may occur with certain implementations that the DMME and SCE are located within the same physical device, there remains the need to pass messages between these entities. The formats of these intra-device messages are vendor specific.

6.2 Reference model

Figure 6-3 illustrates data-plane, control-plane and management-plane reference models for an [ITU-T G.9960/G.9961] transceiver. Data-plane and control-plane reference models are described in clause 5.3 of [ITU-T G.9960].

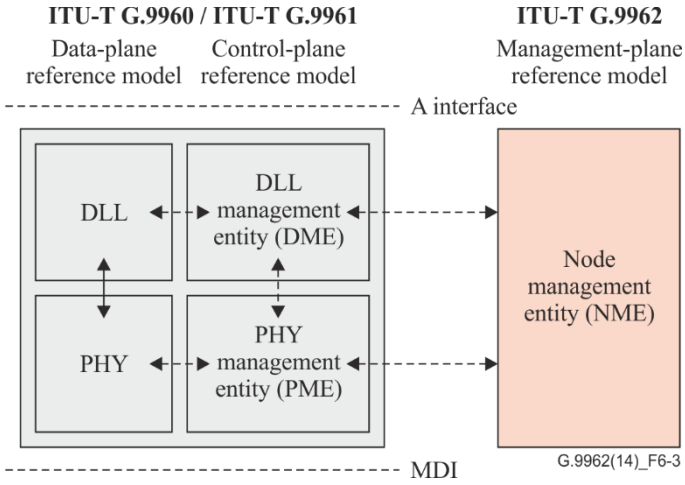


Figure 6-3 – ITU-T G.9962 reference model

7 ITU-T G.996x interface data model

ITU-T G.996x interface data model shall comply with [BBF TR-181 I2A5].

Annex A

LCMP communication through L1 interface

(This annex forms an integral part of this Recommendation.)

A.1 LCMP_CONTROL in L1 interface

LCMP frames conveying information via the L1 interface shall use 0_{16} as LCMP_CONTROL.

A.2 Data model for L1 interface

For further study.

Annex B

LCMP communication through L6 interface

(This annex forms an integral part of this Recommendation.)

B.1 LCMP_CONTROL in L6 interface

LCMP frames conveying information via the L6 interface shall use 5_{16} as LCMP_CONTROL.

B.2 Data model for L6 interface

For further study.

Annex C

G.hn LCMPValue field

(This annex forms an integral part of this Recommendation.)

C.1 LCMPValue field behaviour

The LCMP protocol defines a way for G.hn devices to communicate with external entities (see clause 8.22 of [ITU-T G.9961]).

This protocol is based on an exchange of LCMP messages that contain an LCMPValue field that shall be filled differently depending of the type of communication.

In particular, four actions can be performed using LCMP protocol. Table C.1 shows these actions and relates them to LCMP messages.

Table C.1 – List of defined actions

LCMP action	Description	Involved LCMP messages	Clause
WRITE	Write a parameter into the device	LCMP_WRITE.req; LCMP_WRITE.cnf	C.1.1
READ	Read a parameter from the device	LCMP_READ.req; LCMP_READ.cnf	C.1.1
CONTROL	Control the device	LCMP_CTRL.req; LCMP_CTRL.cnf	C.1.1
NOTIFY	Notify information	LCMP_NOTIFY.ind LCMP_NOTIFY.rsp	C.1.1

C.1.1 Embedding LCMP actions into LCMP

Figure C.1 shows the encapsulation of LCMPValue field within ITU-T LCMP protocol (see Table 8-129 of [ITU-T G.9961]).

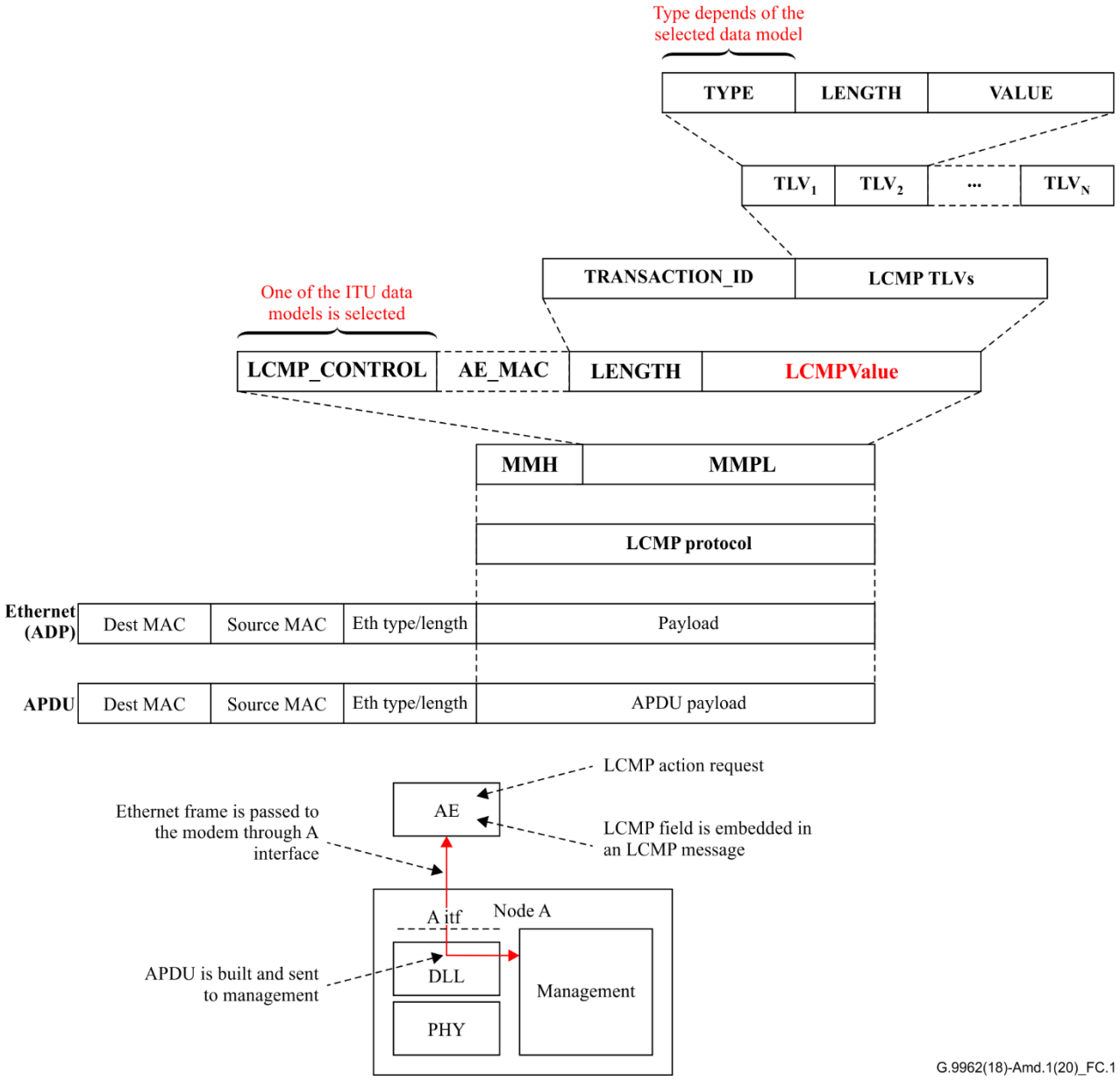


Figure C.1 – Encapsulation of LCMPValue field

The LCMP protocol uses the LCMP control codes reserved for ITU in LCMP protocol. The meaning of each of the control codes is specified in Table 8-129 of [ITU-T G.9961].

C.2 LCMP actions

LCMP actions are mapped to the corresponding [ITU-T G.9961] messages as shown in the following clauses.

The LCMP_CONTROL field the messages shall be set to the value corresponding to the data model being addressed (see clause C.3).

LCMP actions shall not be mixed in a single action (e.g., READ and WRITE actions shall not be conveyed in the same LCMP request).

Each action is marked with a specific transaction identification tag through the TRANSACTION_ID field of the payload (see clause C.4). The TRANSACTION_ID field contents of a confirmation shall be the same than the one received during the request.

The source of an action may decide to merge several petitions in a single action. However, the recipient of the action shall not merge different requests in a single answer.

C.2.1 LCMP WRITE action

An LCMP WRITE action allows writing a parameter into a device. The following diagram describes the sequence of elements.

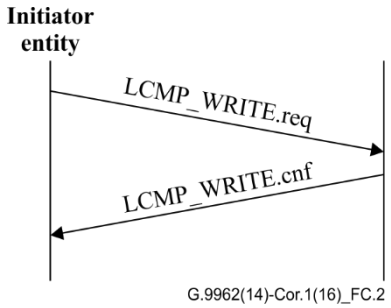


Figure C.2 – LCMP WRITE action

The LCMP TLV Field field of the LCMP_WRITE.req message shall contain:

– Zero or one INFO TLV

– One or more PARAMETER TLV

The LCMP TLV field of the LCMP_WRITE.cnf message shall contain:

– Zero or one INFO TLV

– One WRITE_PARAMETER_CONFIRM TLV

C.2.2 LCMP READ action

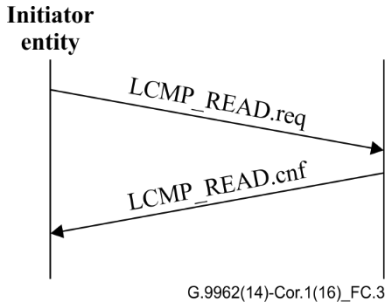


Figure C.3 – READ action

The LCMP TLV Field field of the LCMP_READ.req message shall contain:

– Zero or one INFO TLV

– One or more READ_PARAMETER TLV

The LCMP TLV Field field of the LCMP_READ.cnf message shall contain:

– Zero or one INFO TLV

– One or more PARAMETER TLV

C.2.3 CONTROL action

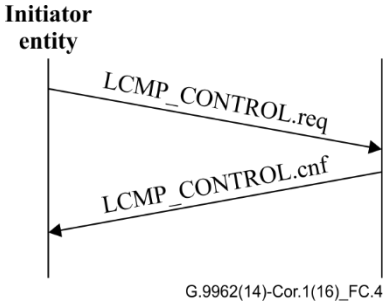


Figure C.4 – CONTROL action

The LCMP TLV Field field of the LCMP_CONTROL.req message shall contain:

– Zero or one INFO TLV

– One or more CONTROL TLV

The LCMP TLV Field field of the LCMP_CONTROL.cnf message shall contain:

– Zero or one INFO TLV

– One or more CONTROL_CONFIRM TLV

C.2.4 NOTIFY action

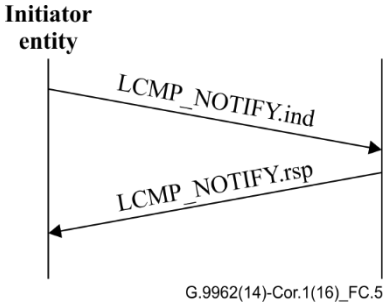


Figure C.5 – NOTIFY action

The LCMP TLV Field field of the LCMP_NOTIFY.ind message shall contain:

– Zero or one INFO TLV

– One or more_NOTIFY TLV

The LCMP_NOTIFY.rsp message shall only be sent when the NotificationAck bit of the received LCMP_NOTIFY.ind is set to one. In this case, the LCMP TLV Field of the LCMP_NOTIFY.rsp message shall contain:

– Zero or one INFO TLV

– One or more NOTIFY_CONFIRM TLV

C.3 Supported Data Models

Nodes shall support at least the following data models:

– **L1 interface data model**, including information exchanged through L1 interface (see clause 6.1 and Annex A).

– **L6 interface data model**, including information exchanged through L6 interface (see clause 6.1 and Annex B).

C.3.1 LCMP control codes

Field Data Model of LCMP_CONTROL field of LCMP messages shall be set to one of the values described in Table 8-129 of [ITU-T G.9961].

C.4 TRANSACTION_ID field

TRANSACTION_ID field is a 16-bit field that helps upper layer entities to track the transactions over LCMP.

The recipient of the action shall use the value of this field in the received message to fill the TRANSACTION_ID of the response message.

The source of the action should ensure that the TRANSACTION_IDs for different processes are distinct from each other (e.g., using the MSB of the TRANSACTION_ID).

NOTE – Using sequential numbers for TRANSACTION_IDs for a given process may help determining the order of messages on the receive side.

C.5 LCMP fields

C.5.1 TLV structure

TLVs follow the structure described in Table C.2.

Table C.2 – TLV structure

Field	Octet	Bits	Description
Type	0	[7:0]	Type of TLV. See Table C.3
Length	1-2	[15:0]	Length in octets of the value field
Value	Variable	Variable	Value corresponding to the TLV type. See Table C.3

C.5.2 TLVs

C.5.2.1 TLV types and values

Table C.3 – TLV type

TLV type	TLV type name	TLV type length (octets)	TLV type value
00_{16}	INFO	1	The Value field of this TLV shall be filled following clause C.5.2.1.8. This TLV, if it exists, shall be the first TLV to be transmitted.
01_{16}-$0F_{16}$	Reserved by ITU-T	N/A	Reserved by ITU-T
10_{16}	PARAMETER	Variable	Write/Read a parameter into/from the device. The value field of the TLV shall be filled following clause C.5.2.1.1
11_{16}	WRITE_PARAMETER_ CONFIRM	Variable	Confirmation of parameter writing. The value field of this TLV shall be filled as described in clause C.5.2.1.2
12_{16}	READ_PARAMETER	Variable	The value field of this TLV shall be filled following clause C.5.2.1.3
13_{16}	CONTROL	Variable	Control operation. The value field of the TLV shall be filled following clause C.5.2.1.4

Table C.3 – TLV type

TLV type	TLV type name	TLV type length (octets)	TLV type value
14_{16}	CONTROL_CONFIRM	Variable	Confirmation of writing of control information in the device. It shall be filled as described in clause C.5.2.1.5
15_{16}	NOTIFY	Variable	Notification. It shall be filled as described in clause C.5.2.1.6
16_{16}	NOTIFY_CONFIRM	Variable	Confirmation of a notification. It shall be filled as described in clause C.5.2.1.7
17_{16} to FF_{16}	Reserved by ITU-T	N/A	Reserved by ITU-T

C.5.2.1.1 PARAMETER TLV value field

The following table specifies the value field of PARAMETER TLV.

Table C.4 – PARAMETER TLV value field

Field	Octet	Bits	Description
ParameterType	0	[7:0]	ParameterId of the parameter to be written. It shall be filled according to: • Annex A in the case of accessing the L1 interface data model • Annex B in the case of accessing the L6 interface data model
ParameterValue	1	Variable	This field is parameter-dependent and shall be filled according to: • Annex A in the case of accessing L1 interface data model • Annex B in the case of accessing L6 interface data

C.5.2.1.2 WRITE_PARAMETER_CONFIRM TLV value field

The following table specifies the value field of WRITE_PARAMETER_CONFIRM TLV.

Table C.5 – WRITE_PARAMETER_CONFIRM TLV value field

Field	Octet	Bits	Description
NumberOfParameters	0	[7:0]	Number of parameters (N) for which the correct writing is confirmed
Parameter[0]	1	[7:0]	ParameterId of the first parameter to be confirmed for the accessed data model
…	…	…	…
Parameter[N-1]	N	[7:0]	ParameterId of the last parameter to be confirmed for the accessed data model

C.5.2.1.3 READ_PARAMETER TLV value field

The following table specifies the value field of READ_PARAMETER TLV.

Table C.6 – READ_PARAMETER TLV value field

Field	Octet	Bits	Description
ParameterId	0	[7:0]	ParameterId of the first parameter to be read. It shall be filled according to: • Annex A in the case of accessing L1 interface data model • Annex B in the case of accessing L6 interface data

C.5.2.1.4 CONTROL TLV value field

The following table specifies the value field of CONTROL TLV.

Table C.7 – CONTROL TLV value field

Field	Octet	Bits	Description
ControlType	0	[7:0]	ControlId of the control operation. It shall be filled according to: • Annex A in the case of accessing L1 interface data model • Annex B in the case of accessing L6 interface data
ControlValue	1	Variable	This field is parameter-dependent and shall be filled according to: • Annex A in the case of accessing L1 interface data model • Annex B in the case of accessing L6 interface data

C.5.2.1.5 CONTROL_CONFIRM TLV value field

The following table specifies the value field of CONTROL_CONFIRM TLV.

Table C.8 – CONTROL_CONFIRM TLV value field

Field	Octet	Bits	Description
NumberOfControlOps	0	[7:0]	Number of control operations (N) for which the correct writing is confirmed
ControlOp[0]	1	[7:0]	ControlId of the first control operation to be confirmed for the accessed data model
…	…	…	…
ControlOp[N-1]	N	[7:0]	ControlId of the last control operation to be confirmed for the accessed data model

C.5.2.1.6 NOTIFY TLV value field

The following table specifies the value field of NOTIFY TLV.

Table C.9 – NOTIFY TLV value field

Field	Octet	Bits	Description
NotifyType	0	[7:0]	NotifyID of the control operation. It shall be filled according to: • Annex A in the case of accessing L1 interface data model • Annex B in the case of accessing L6 interface data
NotifyValue	1	Variable	This field is parameter-dependent and shall be filled according to: • Annex A in the case of accessing L1 interface data model • Annex B in the case of accessing L6 interface data

C.5.2.1.7 NOTIFY_CONFIRM TLV Value field

The following table specifies the value field of NOTIFY_CONFIRM TLV.

Table C.10 – NOTIFY_CONFIRM TLV value field

Field	Octet	Bits	Description
NumberOfNotifies	0	[7:0]	Number of notification operations (N) for which the correct writing is confirmed
Notify[0]	1	[7:0]	NotifyId of the first control operation to be confirmed for the accessed data model
…	…	…	…
Notify[N-1]	N	[7:0]	NotifyId of the last control operation to be confirmed for the accessed data model

C.5.2.1.8 INFO TLV Value field

The following table specifies the value field of INFO TLV.

Table C.11 – INFO TLV value field

Field	Octet	Bits	Description
Reserved by ITU-T	0-4	[39:0]	Reserved by ITU-T (Note)
NOTE – Bits that are reserved by ITU-T shall be set to zero by the transmitter and ignored by the receiver			

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020