International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.984.3
Amendment 3
(04/2012)

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

Digital sections and digital line system – Optical line systems for local and access networks

---

Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification

Amendment 3

Recommendation ITU-T G.984.3 (2008) – Amendment 3

ITU-T

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
General	G.900–G.909
Parameters for optical fibre cable systems	G.910–G.919
Digital sections at hierarchical bit rates based on a bit rate of 2048 kbit/s	G.920–G.929
Digital line transmission systems on cable at non-hierarchical bit rates	G.930–G.939
Digital line systems provided by FDM transmission bearers	G.940–G.949
Digital line systems	G.950–G.959
Digital section and digital transmission systems for customer access to ISDN	G.960–G.969
Optical fibre submarine cable systems	G.970–G.979
Optical line systems for local and access networks	**G.980–G.989**
Access networks	G.990–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

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

Recommendation ITU-T G.984.3

Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification

Amendment 3

Summary

Amendment 3 to Recommendation ITU-T G.984.3 (2008) aligns gigabit-capable passive optical network (G-PON) security with the enhanced security control features supported in Recommendation ITU-T G.988. It also introduces a new PON-ID maintenance capability, as well as new physical layer operations, administrations and maintenance (PLOAM) functions: broadcast POPUP to Operation state, and relative equalization delay adjustment.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.984.3	2004-02-22	15
1.1	ITU-T G.984.3 (2004) Amd. 1	2005-07-14	15
1.2	ITU-T G.984.3 (2004) Amd. 2	2006-03-29	15
1.3	ITU-T G.984.3 (2004) Amd. 3	2006-12-14	15
2.0	ITU-T G.984.3	2008-03-29	15
2.1	ITU-T G.984.3 (2008) Amd. 1	2009-02-13	15
2.2	ITU-T G.984.3 (2008) Amd. 2	2009-11-13	15
2.3	ITU-T G.984.3 (2008) Amd. 3	2012-04-22	15

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

		Page
1)	Clause 2, References	1
2)	Clause 4, Abbreviations and acronyms	1
3)	Enhanced security capabilities	1
4)	New Annex B	3
5)	New Annex C	5
6)	New Annex D	7
7)	Bibliography	10

Introduction

This amendment aligns gigabit-capable passive optical network (G-PON) security with the enhanced security control features supported in [ITU-T G.988], and introduces a new PON-ID maintenance capability, as well as new physical layer operations, administrations and maintenance (PLOAM) functions: broadcast POPUP to Operation state and relative equalization delay adjustment.

Recommendation ITU-T G.984.3

Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification

Amendment 3

1) Clause 2, References

In clause 2, add the following references:

– *After line item [ITU-T G.984.2], insert the following line item:*

[ITU-T G.988] Recommendation ITU-T G.988 (2010), *ONU management and control interface (OMCI) specification*.

– *After line item [FIPS 140-2], insert the following line item:*

[NIST SP800-38A] NIST Special Publication 800-38A (2001), *Recommendation for Block Cipher Modes of Operation – Methods and Techniques.*

2) Clause 4, Abbreviations and acronyms

In clause 4, Abbreviations and acronyms, insert the following items in alphabetic order:

AVC Attribute Value Change

ECB Electronic CodeBook

MSK Master Session Key

PIT PON-ID type

PSK Pre-shared Secret Key

TOL Transmit Optical Level

3) Enhanced security capabilities

3.1) Restructuring of clause 12.3, Key exchange and switch-over

For the sake of reference only, partition clause 12.3 into the following two new clauses.

Replace clause 12.3 with the following:

12.3 Data encryption key exchange

We presume that the OLT and ONU have already configured a Port-ID for encrypted behaviour, and that they have established a key to use. Both the ONU and OLT store the key material in their active_key_registers, and it is this register that the encryption algorithm uses.

The key exchange is initiated by the OLT. The OLT does so by sending the Request_Key message in the PLOAM channel. The ONU responds by generating, storing and sending the key. The ONU stores the new key in the shadow_key_register. The ONU should generate a cryptographically unpredictable key. For guidance in achieving this, see [FIPS 140-2]. Because the PLOAM message is limited in length, the key is sent in two pieces, using the fragmentation field to indicate which part of the key is being sent. Both parts of the key are sent three times for extra redundancy. All ONU transmissions of a particular key have the same value of Key_Index, so that the OLT can definitively confirm that all transmissions are from the same key. The Key_Index is incremented for each key that the ONU generates upon request from the OLT.

If the OLT is unsuccessful in receiving either part of the key all three times it is transmitted, then the OLT will ask the ONU to generate another key by issuing a new Request_Key message. If the key transmission fails three times, then the OLT should declare a loss of key synchronization (LOKi) condition and deactivate the ONU.

Once the OLT successfully receives the key, it stores the validated key in its shadow_key_register. Now the system is prepared for key switch-over.

Add the following new clause 12.4:

12.4 Data encryption key switch-over

The OLT chooses a frame number in the future to be the first frame to use the new key. It transmits the super-frame number of this frame to the ONU using the Key_Switching_Time message. This message is sent three times, and the ONU need only receive one correct copy to know the time to switch.

The Key_Switching_Time message requires an acknowledgment by the ONU. If, after three message loss of acknowledgment LOAi condition and deactivate the ONU.

If after the ONU has acknowledged a Key_Switching_Time message but before the key switch is executed, the ONU receives a new Request_Key message, it generates a new key, overwriting the value previously stored in the shadow_key_register, and discards the previously chosen superframe number associated with the overwritten key. A new superframe number should be communicated to the ONU by a subsequent Key_Switching_Time message.

At the beginning of the chosen frame, the OLT will copy the contents of the shadow_key_register into the active_key_register, and the ONU will copy its shadow_key_register into the active_key_register. In this way, both the OLT and ONU begin using the new key at precisely the same frame boundary for any new PDUs (frames) that they exchange.

Note that the AES algorithm requires the generation of a series of round keys based on a single key. This key scheduling operation takes time, and so it must be done in anticipation of the key switch. At the moment the key_switch bit is changed, both OLT and ONU must be ready to use the new key.

In some rare cases, an ONU may experience an intermittent LOS/LOF condition that interferes with a scheduled key switch. To ensure graceful recovery in such cases, it is recommended that the OLT restart the key exchange and switch-over procedure with an ONU that has been transitioned from the POPUP state (O6) to the Operation state (O5) immediately upon issuing a directed POPUP message to that ONU.

4) New Annex B

Add new Annex B, specifying the enhanced security capability.

Annex B

Enhanced Security Capabilities

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

The implementation of this annex is optional. The ITU-T G.984 G-PON systems, OLTs, or ONUs that are required to support the provision of this annex are herein referred to as compliant.

B.1 Introduction

This annex describes a G-PON system that supports the Enhanced Security Control ME (see clause 9.13.11 of [ITU-T G.988]) and hence achieves a higher level of security through secure mutual authentication and encrypted transmission of the data encryption key.

B.2 Secure mutual authentication and data key encryption

B.2.1 Pre-shared secret

A compliant G-PON system shall support a pre-shared secret key (PSK) that is associated with a particular ONU and is stored at that ONU and in the operator infrastructure. On the operator side, the pre-shared secret for a particular ONU might be stored in the physically-connected OLT, or at a central server that the OLT accesses during authentication. The PSK is a 128-bit value. It may be provisioned into the ONU and into the operator infrastructure in any manner that satisfies these requirements. Specification of how exactly the PSK is provisioned is beyond the scope of this Recommendation.

B.2.2 Master session key

As described in clause 9.13.11 of [ITU-T G.988], the compliant OLT and ONU may execute a mutual authentication procedure, in the course of which both the OLT and the ONU compute the 128-bit master session key (MSK), a session-specific shared secret. Whenever the ONU is successfully authenticated, as indicated by the value of the ONU Authentication status attribute, the MSK is used to encrypt data encryption keys that are transmitted upstream.

For the duration of the execution of the secure mutual authentication procedure, the OLT refrains from initiating data encryption key exchanges.

The new MSK, obtained in the course of execution of the secure mutual authentication procedure, is committed as active by the ONU at the moment the AVC on authentication status attribute is transmitted, and is committed as active by the OLT at the moment that the AVC on the ONU's authentication status attribute is received.

B.2.3 Data encryption key exchange

For a compliant system the content of this clause replaces the content of clause 12.3.

Key exchange is initiated by the OLT. The OLT does so by sending the Request_Key message in the PLOAM channel. The ONU responds to the Request_Key message by generating, storing, possibly encrypting, and sending the data encryption key upstream. The ONU stores the new key in the shadow_key_register. The ONU should generate a cryptographically unpredictable key. For guidance in achieving this, see [FIPS 140-2]. Because the PLOAM message is limited in length, the key is sent in two pieces, using the fragmentation field to indicate which part of the key is being sent. Both parts of the key are sent three times for extra redundancy. All ONU transmissions of a particular key have the same value of Key_Index, so that the OLT can definitively confirm that all transmissions are from the same key. The Key_Index field is incremented for each key that the ONU generates upon request from the OLT.

The ONU encrypts the data encryption key transmitted upstream in the Encryption_Key PLOAM message, if at the time of Request_Key message processing there exists a valid secure mutual association between the OLT and the ONU as indicated by the value of the ONU authentication status attribute. The data encryption key is encrypted using the MSK with the AES-128 block cipher [FIPS-197] in the Electronic Codebook mode (AES-ECB), as specified in [NIST SP800-38A]. In AES-ECB encryption, the forward AES-128 function is applied directly and independently to each block of plaintext using a secret key to produce a block of ciphertext. Specifically,

$$C = \text{AES-ECB}(MSK, P)$$

Here P is a plaintext data key, C is a ciphertext data key, MSK is the key used for data key encryption.

If the OLT is unsuccessful in receiving either part of the key all three times it is transmitted, then the OLT asks the ONU to generate another key by issuing a new Request_Key message. If the key transmission fails three times, then the OLT should declare a loss of key synchronization (LOKi) condition.

Once the OLT successfully receives the key, it may have to decrypt it. The OLT decrypts the key if there exists a valid secure mutual association between the OLT and the ONU. In AES-ECB decryption, the inverse AES-128 function is applied directly and independently to each block of ciphertext with the same secret key to restore the original block of plaintext. Specifically,

$$P = \text{AES-ECB}^{-1}(MSK, C)$$

The receiver stores the validated key in its shadow_key_register. Now the system is prepared for key switch-over.

B.3 G-PON systems with reduced data encryption strength

Clause B.3.1 introduces the concept of effective key length. Clause B.3.2 contains conditional requirements that are mandatory only for the G-PON systems with the specified effective key length less than 128 bits.

B.3.1 Effective key length

The standard key size used for AES data encryption in G-PON is 128 bits. Per operator requirements, a G-PON system may optionally employ a data encryption system of reduced strength by replacing a part of the key with a well-defined bit pattern. The number of randomly generated bits of the key is referred to as the effective key length.

B.3.2 Data encryption key format

In a G-PON system with reduced data encryption strength, the effective key length L_{eff} is a multiple of 8 bits. Each network element responsible for data encryption key generation replaces the (128 – L_{eff})/8 most significant octets of the 128-bit key with the value 0x55, as shown in Figure B.1.

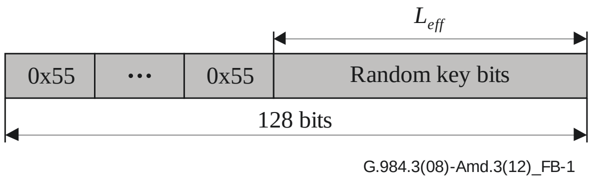

Figure B.1 – Format of a data encryption key with reduced effective length

In a G-PON system with reduced data encryption strength, a network element responsible for the generation of a data encryption key should be able to report the effective key length to the element management system, using the Effective key length attribute of the Enhanced security control ME defined in clause 9.13.11 of [ITU-T G.988].

5) New Annex C

Add new Annex C, specifying the PON-ID maintenance functionality.

Annex C

PON-ID maintenance

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

The implementation of this annex is optional. The ITU-T G.984 G-PON systems, OLTs, or ONUs that are required to support the provision of this annex are herein referred to as compliant. An ONU's compliance with this annex can be discovered via the enhanced TC layer options attribute of the ONU-G managed entity defined in clause 9.1.1 of [ITU-T G.988].

C.1 Introduction

This annex contains provisions enabling the field personnel to retrieve a PON port identifier and an indication of the launched power on the network, adapted from the optical layer supervision concept defined in [b-ITU-T G.984.2 Amd.2]. The specified method introduces an additional downstream PLOAM message. Comparison of the locally measured optical power and the image of the source launched power coded in the PLOAM message should give operators a means to differentiate fibre plant loss from variations in launched power. Coding commonality with existing power measurements in [ITU-T G.988] is intended, as well as alignment with [b-SFF SFF8472], which defines the information available at the RSSI interface of opto-electrical converters of interest in OLT implementations.

C.2 PON-ID PLOAM message

A system compliant with this annex shall support a PON-ID PLOAM message according to the following definition. A compliant OLT generates the PON-ID message only when provisioned to do so.

C.2.1 New downstream message type

A new PLOAM message type is defined in addition to the message types specified in the table of clause 9.2.1.

	Message name	Function	Trigger	Times sent	Effect of receipt
19	PON-ID	To name tag an OLT PON interface and broadcast a digital image of the estimated launched power	Periodic at approx. 1 second intervals	1	This message has no effect on the ONU behaviour but may be stored by the ONU to be accessed via a monitoring terminal

C.2.2 PON-ID message description

The PON-ID message consists of three elements, two statically provisioned by the operator, one dynamic with cyclic update from OLT system data:

– PON-ID type (1 byte, static, provisioned by the operator): an indication of the ODN architecture, the source of the reported launch power and the ODN class;

– PON-Identifier (7 bytes, static, provisioned by the operator): any value of interest to the operator, which may, for example, reflect the established logical address plan;

– TOL (2 bytes, dynamic, maintained by the OLT): transmit optical level, an indication of the current transceiver launch power of the appropriate network element. The coding is adapted to support the full suite of specified G-PON ODN classes (A, B, B+, C, C+) and reach extender options (see [b-ITU-T G.984.6]), covering the transceiver launch power range from 0 dBm to +9 dBm.

PON-ID message		
Octet	**Content**	**Description**
1	11111111	Broadcast message to all ONUs.
2	00010101	Message identification "PON-ID"
3	ACCCpppp	PON-ID Type. A bit: 0 – TOL reports the OLT's power level; 1 – TOL reports RE's power level. CCC bits encode the budget class of the system/plant in the ODN section 000 represents Class A 001 represents Class B 010 represents Class B+ 011 represents Class C 100 represents Class C+ other codepoints reserved pppp bits are reserved for future use set to 0000 unless otherwise specified
4	bbbbbbbb	PON-Identifier Byte 1.
…	…	…
10	bbbbbbbb	PON-Identifier Byte 7.
11-12	Tx optical level	Transmit optical level (TOL). This two-byte attribute reports the current measurement of the mean optical launch power of the appropriate network element. Its value is an integer referred to 1 μW (i.e., the zero value represents –30 dBm), with 0.1 dB granularity. The 0xFFFF default value indicates that TOL is not supported on the given PON interface.

6) New Annex D

Add new Annex D, specifying enhancements to the G-PON PLOAM channel: broadcast POPUP to the Operation state, and relative equalization delay adjustment.

Annex D

PLOAM channel enhancements

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

The implementation of this annex is optional. The ITU-T G.984 G-PON systems, OLTs, or ONUs that are required to support the provision of this annex, are herein referred to as compliant. An ONU's compliance with this annex can be discovered via the Extended TC-layer options attribute of the ONU-G ME defined in clause 9.1.1 of [ITU-T G.988]. The OLT can rely on functionality specified herein, in communication with the compliant ONUs only.

D.1 Introduction

The new extended PLOAM channel functionality includes broadcast POPUP to the Operation state (O5) and relative equalization delay adjustment. To ensure backward compatibility, both functionalities are implemented with new PLOAM message types.

A system compliant with this annex shall support Swift_POPUP and Ranging_Adjustment PLOAM messages according to the following definitions.

D.2 New downstream PLOAM message types

Two new downstream PLOAM message types are defined in addition to the message types specified in clause 9.2.1.

	Message name	Function	Trigger	Times sent	Effect of receipt
20	Swift_ POPUP	The OLT forces all ONUs that are in POPUP state and have cleared LOS/LOF defect to execute a transition directly to Operation state (O5).	At the OLT's discretion, to facilitate ONUs' transition to O5	3	The ONU transitions to Operation state (O5)
21	Ranging_ Adjustment	To provide incremental correction to the previously established equalization delay either to individual ONUs, or to all active ONUs simultaneously	At the OLT's discretion in the course of in-service EqD adjustment	1	If in O4, discard. If in O5 update the equalization delay register with this value; if unicast, send Acknowledgement

D.3 New downstream PLOAM message descriptions

D.3.1 Swift_POPUP message

Swift_POPUP message		
Octet	**Content**	**Description**
1	11111111	Broadcast message to all ONUs.
2	00010110	Message identification "Swift_POPUP"
3-12	Padding	Set to 0x00 by transmitter; treated as "don't care" by receiver.
NOTE – An ONU in the POPUP state (O6) that receives a Swift_POPUP message moves directly to Operation state (O5) while keeping its equalization delay and TC layer configuration.		

D.3.2 Ranging_Adjustment message

Ranging_Adjustment message		
Octet	**Content**	**Description**
1	ONU-ID or 11111111	Directed message to one ONU or broadcast message to all ONUs. As a broadcast to all ONUs, ONU-ID = 0xFF.
2	00010111	Message identification "Ranging_Adjustment"
3	000000S0	Bit S = 0-Positive: increase the current EqD by the specified value. Bit S = 1-Negative: decrease the current EqD by the specified value
4	dddddddd	First (most significant) byte of the incremental equalization delay value
5	dddddddd	Second byte of the incremental equalization delay value
6	dddddddd	Third byte of the incremental equalization delay value
7	dddddddd	Fourth (least significant) byte of the incremental equalization delay value
8-12	Padding	Set to 0x00 by transmitter; treated as "don't care" by receiver.
NOTE – The equalization delay increment is represented in bit times with respect to the nominal upstream line rate.		

D.4 Modified activation state diagram

In addition to the state transitions specified in clause 10.2, a compliant ONU supports a transition from the POPUP state (06) to the Operation state (O5) upon receipt of a Swift_POPUP message.

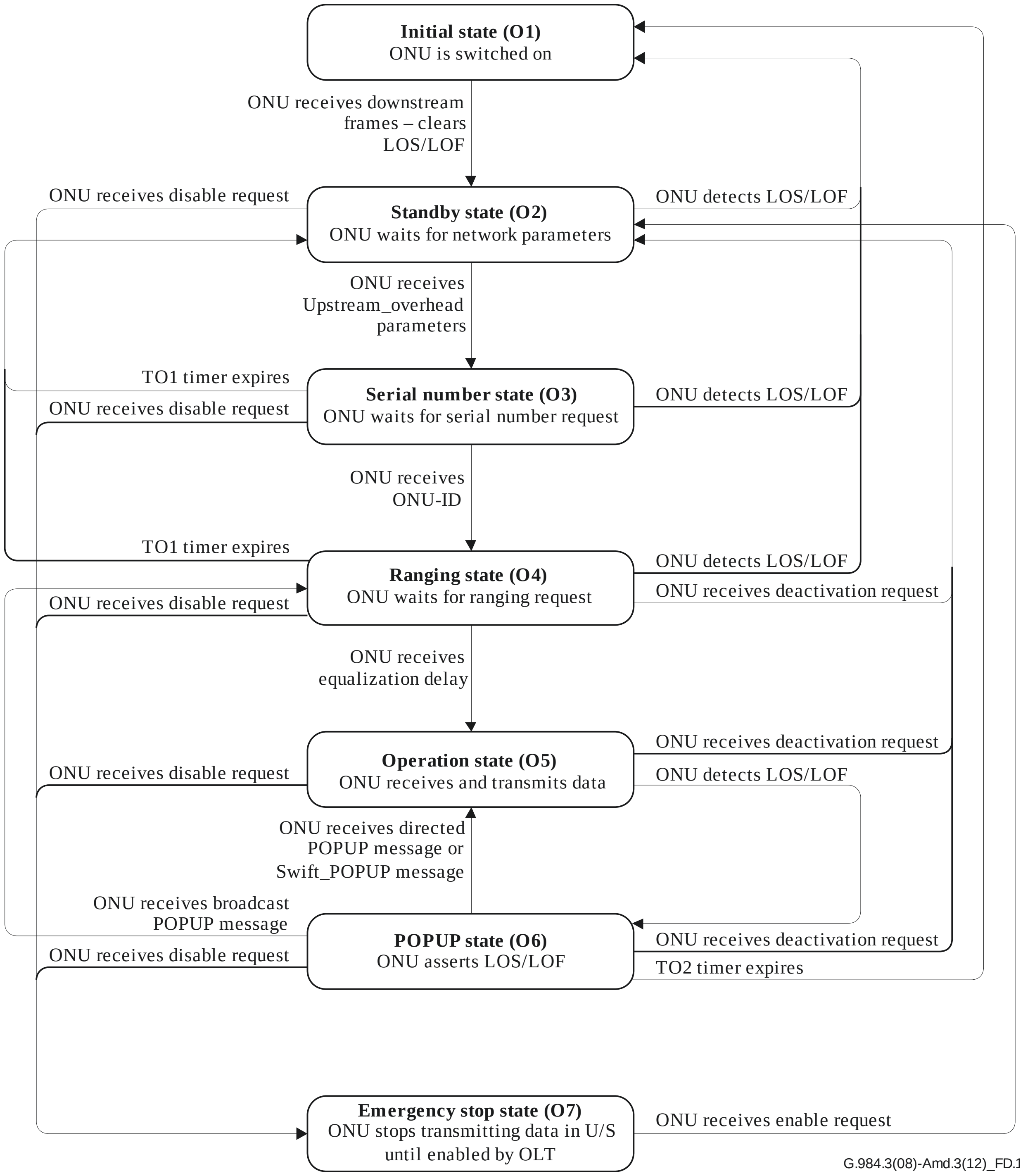

Figure D.1 – Modified state diagram of the ONU

7) Bibliography

Add the following references to the bibliography:

[b-ITU-T G.984.2 Amd.2] Recommendation ITU-T G.984.2 (2003) Amd.2 (2008), *Gigabit-capable passive optical networks (G-PON): Physical media dependent (PMD) layer specification*.

[b-ITU-T G.984.6] Recommendation ITU-T G.984.6 (2008), *Gigabit-capable passive optical networks (G-PON):Reach extension*.

[b-SFF SFF8472] SFF Committee Specification SFF8472 (2010), *Diagnostic Monitoring Interface for Optical Transceivers*. Rev. 11.0.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012