International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.988

Amendment 2
(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

ONU management and control interface (OMCI) specification

Amendment 2: Maintenance

Recommendation ITU-T G.988 (2010) – Amendment 2

ITU-T

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
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.988

ONU management and control interface (OMCI) specification

Amendment 2

Maintenance

Summary

Amendment 2 to Recommendation ITU-T G.988 (2010) continues the maintenance and evolution of the optical network unit management and control interface (OMCI) as defined in the Recommendation. A number of improvements in robustness are included, along with corrections of editorial errors. Significant feature extensions include added flexibility in the downstream virtual local area network (VLAN) tag treatment, provision for the Dynamic Host Configuration Protocol (DHCP) relay agent options in IPv4 and IPv6, and control of power over Ethernet capability.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.988	2010-10-07	15
1.1	ITU-T G.988 (2010) Amd. 1	2011-04-13	15
1.2	ITU-T G.988 (2010) Amd. 2	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/.

Recommendation ITU-T G.988

ONU management and control interface (OMCI) specification

Amendment 2

Maintenance

1 Scope

This amendment continues the maintenance and evolution of the optical network unit management and control interface (OMCI) as defined in Recommendation ITU-T G.988 (2010) as amended. A number of improvements in robustness are included, along with corrections of editorial errors. Significant feature extensions include added flexibility in the downstream virtual local area network (VLAN) tag treatment, provision for the Dynamic Host Configuration Protocol (DHCP) relay agent options in IPv4 and IPv6, and the control of power over Ethernet capability.

2 Changes to ITU-T G.988 (2010)

NOTE – In the remainder of this amendment, the headings of clauses are the same as the corresponding headers in ITU-T G.988 (2010), as modified by ITU-T G.988 Amendment 1 (2011).

4 Abbreviations and acronyms

Add the following abbreviations and acronyms to the list, in alphabetic order:

PD	Powered Device
PoE	Power over Ethernet
PSE	Power Sourcing Equipment

8 Protocol-independent MIB for the OMCI

8.1 Managed entities

Add the following new managed entities (MEs) to Table 8-1, in alphabetic order:

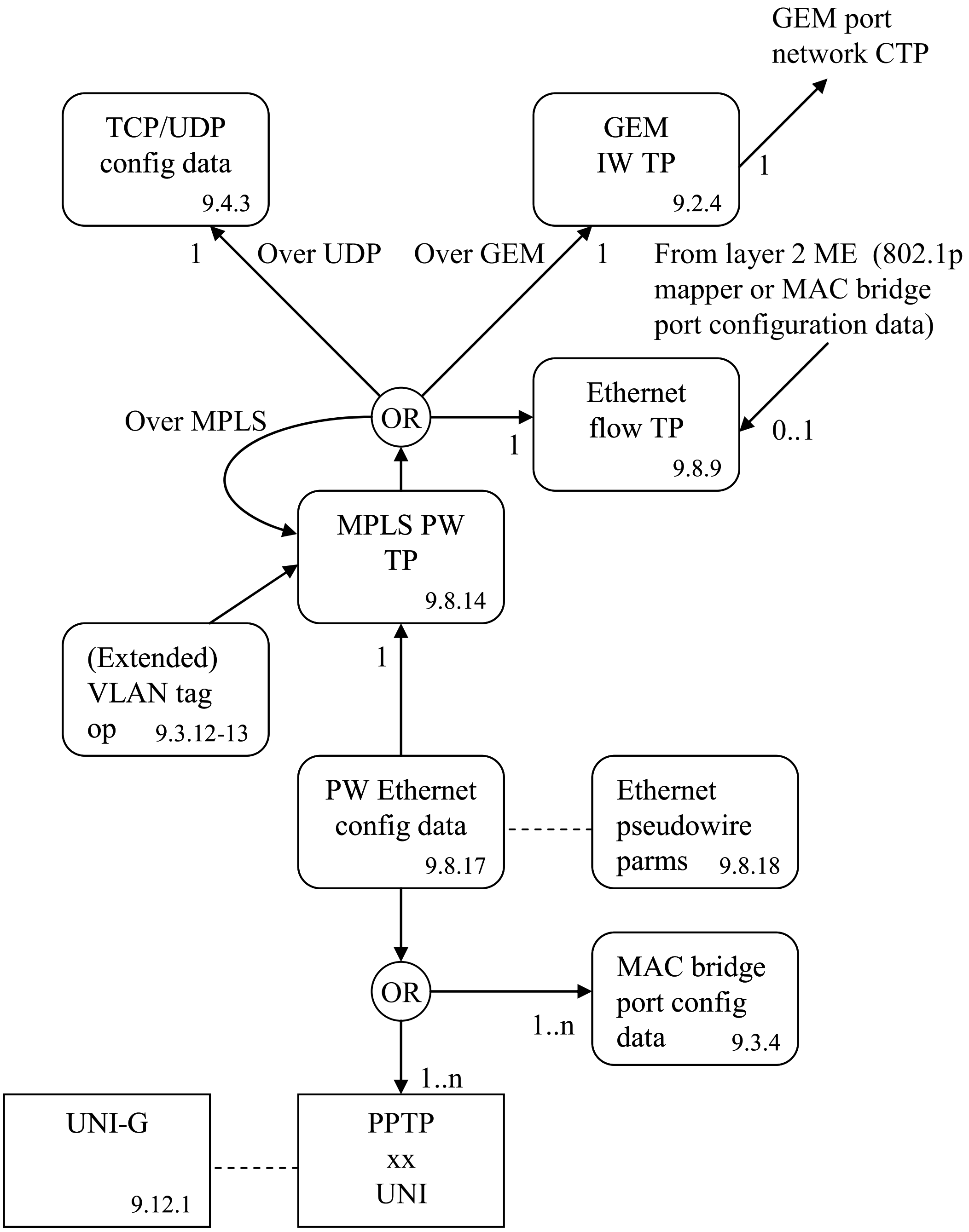
Table 8-1 – Managed entities of OMCI

Clause	Managed entity	ITU-T G.984 ITU-T G.987	ITU-T G.986	802.3 802.3av
9.5.6	PoE control			
9.8.18	Ethernet pseudowire parameters			

Delete the following line from Table 8-1 (it is an outline heading, not an ME):

Clause	Managed entity	ITU-T G.984 ITU-T G.987	ITU-T G.986	802.3 802.3av
9.14	Mid-span PON reach extender			

Replace Figure 8.2.9-3 with the following:



GEM port network CTP
TCP/UDP config data 9.4.3
GEM IW TP 9.2.4
1
1
Over UDP
Over GEM
1
From layer 2 ME (802.1p mapper or MAC bridge port configuration data)
Over MPLS
OR
1
Ethernet flow TP 9.8.9
0..1
MPLS PW TP 9.8.14
(Extended) VLAN tag op 9.3.12-13
1
PW Ethernet config data 9.8.17
Ethernet pseudowire parms 9.8.18
OR
MAC bridge port config data 9.3.4
1..n
1..n
UNI-G 9.12.1
PPTP xx UNI

9 MIB description

9.1.1 ONU-G

Add the following new attribute to the ONU-G in Rec. ITU-T G.988:

Extended TC-layer options: This attribute is meaningful in ITU-T G.984 systems only. It is a bit map that defines whether the ONU supports (1) or does not support (0) various optional TC-layer capabilities of ITU-T G.984.3. Bits are assigned as follows:

Bit	Meaning
1 (LSB)	ITU-T G.984.3 Annex C, PON-ID maintenance.
2	ITU-T G.984.3 Annex D, PLOAM channel enhancements: swift_POPUP and Ranging_adjustment messages.
3..16	Reserved

(R) (optional) (2 bytes)

Add the following alarms and note to this ME, and adjust the reserved space as shown:

Alarm number	Alarm	Description
13	Inv-Image	Software image is invalid (note)
14	PSE overload yellow	Indicates that the ONU is nearing its maximum ability to supply the known PoE demand of the attached PDs. The thresholds for declaring and clearing this alarm are vendor-specific.
15	PSE overload red	Indicates that the ONU is unable to supply all of the PoE demand of the attached PDs and has removed or reduced power to at least one PD.
16..207	Reserved	
NOTE – The ONU should declare this alarm only outside the software download process.		

9.1.2 ONU2-G

Add codepoints 0xA2 and 0xB2 as follows:

OMCC version: This attribute identifies the version of the OMCC protocol being used by the ONU. This allows the OLT to manage a network with ONUs that support different OMCC versions. Release levels of [ITU-T G.984.4] are supported with code points of the form 0x8y and 0x9y, where y is a hexadecimal digit in the range 0..F. Support for continuing revisions of this Recommendation is defined in the 0xAy range.

0x80 ITU-T G.984.4 (06/04)

NOTE – For historic reasons, this code point may also appear in ONUs that support later versions of ITU-T G.984.4.

0x81 ITU-T G.984.4 Amd.1 (06/05)

0x82 ITU-T G.984.4 Amd.2 (03/06)

0x83 ITU-T G.984.4 Amd.3 (12/06)

0x84 ITU-T G.984.4 2008 (2/08)

0x85 ITU-T G.984.4 2008 Amd.1 (06/09)

0x86 ITU-T G.984.4 2009 Amd.2 (2009). Baseline message set only, without the extended message set option

0x96 ITU-T G.984.4 2009 Amd.2 (2009). Extended message set option, in addition to the baseline message set

0xA0 ITU-T G.988 (2010). Baseline message set only, without the extended message set option

0xA1 ITU-T G.988 Amd.1 (2011). Baseline message set only

0xA2 ITU-T G.988 Amd.2 (2012). Baseline message set only

0xB0 ITU-T G.988 (2010). Baseline and extended message set

0xB1 ITU-T G.988 Amd.1 (2011). Baseline and extended message set

0xB2 ITU-T G.988 Amd.2 (2012). Baseline and extended message set

(R) (mandatory) (1 byte)

9.1.4 Software image

Add a new attribute to the software image ME, as follows:

Image hash: This attribute is an MD5 hash of the software image. It is computed at completion of the end download action. (R) (optional) (16 bytes)

9.3 Layer 2 data services

9.3.13 Extended VLAN tagging operation configuration data

Replace the downstream mode attribute description with the following:

Downstream mode: Regardless of its association, the rules of the received frame VLAN tagging operation table attribute pertain to upstream traffic. The downstream mode attribute defines the tagging action to be applied to downstream frames. In the downstream direction, the upstream default rules do not apply. For one-to-one VLAN mappings, the inverse is trivially defined. Many-to-one mappings are possible, however, and these are treated as follows.

- If an upstream many-to-one mapping results from multiple operation rules producing the same ANI-side tag configuration, then the first matching rule in the list defines the inverse operation. The meaning of *match* depends on the value of the downstream mode attribute.
- If the many-to-one mapping results from don't care fields in the filter being replaced with provisioned fields in the ANI side tags, then the inverse is defined to set the corresponding fields on the ANI side to their lowest legal value.

If the upstream rule merely copies (i.e., no explicit value is specified in the filter field) an inbound tag value to an outbound tag value, the comparison in the downstream direction applies to all tag values. This applies separately to the VID and p-bit fields. For example, with a downstream mode of 2 and an upstream rule that translates the VID while carrying forward the p-bit value, downstream frames that match the specified WAN-side VID will match any p-bit value and will translate the VID.

0 The operation performed in the downstream direction is the inverse of that performed in the upstream direction. Which treatment and filter fields are used for downstream filtering and the handling of unmatched frames are left to the implementation of the ONU.

1 Regardless of the filter rules, no operation is performed in the downstream direction. All downstream frames are forwarded unmodified.

2 Filter on VID and p-bit value. On a match, perform the inverse operation on both the VID and p-bit value. If no match is found, forward the frame unmodified.

3 Filter on VID only. On a match, perform the inverse VID operation only; pass the p bits through. If no match is found, forward the frame unmodified.

4 Filter on p-bit only. On a match, perform the inverse p-bit operation only; pass the VID through. If no match is found, forward the frame unmodified.

5 Filter on VID and p-bit value. On a match, perform the inverse operation on both the VID and p-bit value. If no match is found, discard the frame.

6 Filter on VID. On a match, perform the inverse operation on the VID only; pass the p bits through. If no match is found, discard the frame.

7 Filter on p-bit only. On a match, perform the inverse p-bit operation only; pass the VID through. If no match is found, discard the frame.

8 Regardless of the filter rules, discard all downstream traffic.

All other values are reserved. (R, W) (mandatory) (1 byte)

In the description of the Received frame VLAN tagging operation table attribute, replace the paragraph that reads:

When the table is created, the ONU should predefine three entries that list the default treatment (normal forwarding without filtering or modification) for untagged, single tagged, and double tagged frames. As an exception to the rule on ordered processing, these default rules are always considered as a last resort for frames that do not match any other rule. Best practice dictates that these entries not be deleted; however, they can be modified to produce the desired default behaviour.

with the following:

When the table is created, the ONU should autonomously predefine three entries that list the default treatment (normal forwarding without filtering or modification) for untagged, single tagged, and double tagged frames. As an exception to the rule on ordered processing, these default rules are always considered as a last resort for frames that do not match any other rule. Best practice dictates that these entries not be deleted by the OLT; however, they can be modified to produce the desired default behaviour.

It should be noted that downstream frame treatment is defined by the downstream mode attribute and is not affected by the upstream default rules.

Add the following text and Table 9.3.13-2 after Table 9.13.13-1 :

Table 9.3.13-2 illustrates the downstream behaviour for common deployment scenarios based on the downstream mode code point and the upstream rule. For brevity, the table omits a column for P-bit only, but the downstream action can be inferred from the VID only column.

In cases when the inner packet tag information is not available (i.e., in cases with more than one VID or VID+PBIT value in "VID-only" and "Both P and VID," such as "X and C" and "Px and Py and X and Y"), only outer tag information is used in the downstream filtering rule.

Table 9.3.13-2 – Case examples of downstream mode use

Upstream action type	Filter					Treatment					Downstream action				Notes
	Outer		Inner			Tags to remove	Outer		Inner						
	Priority	VID	Priority	VID	EtherType		Priority	VID	Priority	VID	Consider only …	VID only	Both P and VID	Action	
Untagged frames															
Insert 1 full tag (X): F → X-F	15	4096	15	4096	0	0	15	N/A	Px	X	Single tagged	X	Px and X	Strip tag	
Default case, do nothing	15	4096	15	4096	0	0	15	N/A	15	N/A	Untagged	–	–	Pass unmodified	
Insert 2 tags (X,Y): F → Y-X-F	15	4096	15	4096	0	0	Py	Y	Px	X	Double tagged	X and Y	Px and Py and X and Y	Strip two tags	
Single tagged frames															
Insert 1 full tag (X): C-F → X-C-F	15	4096	8	C	0	0	15	N/A	Px	X	Double tagged	X and C	X and Px and C	Strip outer tag	
Insert 1 tag (X), copy priority: C-F → X-C-F	15	4096	8	C	0	0	15	N/A	8	X	Double tagged	X and C	X and C	Strip outer tag, copy priority onto remaining tag	

Table 9.3.13-2 – Case examples of downstream mode use

Upstream action type	Filter					Treatment					Downstream action				
	Outer		Inner			Tags to remove	Outer		Inner						
	Priority	VID	Priority	VID	EtherType		Priority	VID	Priority	VID	Consider only …	VID only	Both P and VID	Action	Notes
Insert 2 tags (X,Y): C-F → Y-X-C-F	15	4096	8	C	0	0	Py	Y	Px	X	Triple tagged	X and Y and C	Px and Py and X and Y and C	Strip two outer tags	
Modify tag: C-F → X-F	15	4096	8	C	0	1	15	N/A	Px	X	Single tagged	X	Px and X	Replace X with C, retain Px	Use treatment specified in downstream mode definition for the set {C} if ambiguous
Modify tag, keep original priority: C-F → X-F	15	4096	8	C	0	1	15	N/A	8	X	Single tagged	X	Px and X	Replace X with C, retain Px	Use treatment specified in downstream mode definition for the set {C} if ambiguous
Modify and insert tag: C-F → Y-X-F	15	4096	8	C	0	1	Py	Y	Px	X	Double tagged	X and C	X and Px and C	Strip outer tag	
Remove tag: C-F → F	15	4096	8	C	0	1	15	N/A	15	N/A	Untagged	C	C	Add tag, VID = C, P = 0	

Table 9.3.13-2 – Case examples of downstream mode use

Upstream action type	Filter					Treatment					Downstream action				
	Outer		Inner			Tags to remove	Outer		Inner						
	Priority	VID	Priority	VID	EtherType		Priority	VID	Priority	VID	Consider only …	VID only	Both P and VID	Action	Notes
Insert two tags: C-F → Y-X-C-F	15	4096	8	C	0	0	Py	Y	Px	X	Triple tagged	X and Y and C	Px and Py and X and Y and C	Strip two outer tags	
Default case, do nothing	15	4096	14	4096	0	0	15	N/A	15	N/A	Single tagged	–	–	Pass unmodified	
Double tagged frames															
Insert 1 tag (X): S-C-F → X-S-C-F	8	S	8	C	0	0	15	N/A	Px	X	Triple tagged	X and S and C	X and Px and S and C	Strip outer tag	
Insert 1 tag (X), copy external priority: S-C-F → X-S-C-F	8	S	8	C	0	0	15	N/A	9	X	Triple tagged	X and S and C	X and S and C	Strip outer tag, copy priority onto resulting outer tag	
Insert 2 tags (X,Y): S-C-F → Y-X-S-C-F	8	S	8	C	0	0	Py	Y	Px	X	Quad tagged	X and Y and S and C	Px and Py and X and Y and S and C	Strip two outer tags	

Table 9.3.13-2 – Case examples of downstream mode use

Upstream action type	Filter					Treatment					Downstream action				
	Outer		Inner			Tags to remove	Outer		Inner						
	Priority	VID	Priority	VID	EtherType		Priority	VID	Priority	VID	Consider only …	VID only	Both P and VID	Action	Notes
Insert 2 tags (X,Y), copy external and internal priority: S-C-F → Y-X-S-C-F	8	S	8	C	0	0	9	Y	8	X	Quad tagged	X and Y and S and C	X and Y and S and C	Strip two outer tags, copy Px, Py onto remaining tags	
Modify external tag: S-C-F → X-C-F	8	S	8	C	0	1	15	N/A	Px	X	≥2 tags	X and C	Px and X and C	Replace X with S in outer tag	
Modify external tag, keep original priority: S-C-F → X-C-F	8	S	8	C	0	1	15	N/A	9	X	≥2 tags	X and C	X and C	Modify outer tag VID = S, retain priority	
Modify both tags: S-C-F → Y-X-F	8	S	8	C	0	2	Py	Y	Px	X	≥2 tags	X and Y	Px and Py and X and Y	Modify tags with S, C, retain priority	Use treatment specified in downstream mode definition for the sets {S} {C} if ambiguous
Modify both tags, keep original priorities: S-C-F → Y-X-F	8	S	8	C	0	2	9	Y	8	X	≥2 tags	X and Y	X and Y	Modify tags with Y, X, retain priority	Use treatment specified in downstream mode definition for the sets {S} {C} if ambiguous

Table 9.3.13-2 – Case examples of downstream mode use

Upstream action type	Filter					Treatment					Downstream action				
	Outer		Inner			Tags to remove	Outer		Inner						
	Priority	VID	Priority	VID	EtherType		Priority	VID	Priority	VID	Consider only …	VID only	Both P and VID	Action	Notes
Swap both tags: S-C-F → C-S-F	8	S	8	C	0	2	8	4096	9	4097	≥2 tags	S and C	S and C	Swap tags	
Remove outer tag: S-C-F → C-F	8	S	8	C	0	1	15	N/A	15	N/A	≥2 tags	S and C	S and C	Strip outer tag	
Remove both tags: S-C-F → F	8	S	8	C	0	2	15	N/A	15	N/A	≥2 tags	S and C	S and C	Strip both tags	
Default case, do nothing S-C-F → S-C-F	14	4096	14	4096	0	0	15	N/A	15	N/A	≥2 tags	–	–	Pass unmodified	

9.3.15 Dot1X configuration profile

Add the following attribute to this ME:

Calling station ID format: Radius messages initiated by the ONU contain a calling-station-ID field that is specified to be the supplicant's MAC address in upper-case ASCII form, with bytes separated by a delimiter. This attribute permits specification of the delimiter. (R, W) (optional) (2 bytes)

Value	Meaning
0	ONU's internal default
1	Hyphen (-) delimiter
2	Colon (:) delimiter
3	No delimiter
0x20 – 0x7E	Use this value as the delimiter
0xF0 – 0xFE	Vendor-specific use

Other values are reserved.

9.3.22 Dot1ag MEP

Modify the following attribute to read as follows (stricken through text is to be deleted):

MEP control: This attribute specifies some of the overall behavioural aspects of the MEP. It is interpreted as follows.~~ Ethernet AIS generation should not be enabled simultaneously with CCMs.~~

9.4.1 IP host config data

Add the following attribute to the IP host config data ME:

Relay agent options: This attribute is a pointer to a large string managed entity whose content specifies one or more DHCP relay agent options. (R, W) (optional) (2 bytes)

The content of the large string is parsed by the ONU and converted into text strings. Variable substitution is based on defined three-character groups, each of which begins with the '%' character. The string '%%' is an escape mechanism whose output is a single '%' character. When the ONU cannot perform variable substitution on a substring of the large string, it generates the specified option as an exact quotation of the provisioned substring value.

Provisioning of the large string is separate from the operation of setting the pointer in this attribute. It is the responsibility of the OLT to ensure that the large string contents are correct and meaningful.

Three-character variable definitions are as follows. The first variable in the large string must specify one of the option types. Both options for a given IP version may be present if desired, each introduced by its option identifier. Terminology is taken from [b-BBF TR-101], clause 3.9.3.

%01, %18

Specifies that the following string is for option 82 sub-option 1, agent circuit-ID (IPv4) or option 18, interface-ID (IPv6). The equivalence permits the same large string to be used in both IP environments.

%02, %37

Specifies that the following string is for option 82 sub-option 2, relay agent remote-ID (IPv4) or option 37, relay agent remote-ID (IPv6). The equivalence permits the same large string to be used in both IP environments.

%SL In TR-101, this is called a slot. In an ONU, this variable refers to a shelf. It would be meaningful if the ONU has multiple shelves internally or is daisy-chained to multiple equipment modules. The range of this variable is "0".. "99"

%SU In TR-101, this is called a sub-slot. In fact, it represents a cardholder. The range of this variable is "0".. "99"

%PO UNI port number. The range of this variable is "0".. "999"

%AE ATM or Ethernet. This variable can take on the values "atm" or "eth".

%SV S-VID for Ethernet UNI, or ATM VPI for ATM UNI, as it exists on the DHCP request received upstream across the UNI. Range "0".. "4096" for S-VID; range "0".. "255" for VPI. The value "4096" indicates no S-VID tag.

%CV C-VID (Q-VID) for Ethernet UNI, or ATM VCI for ATM UNI, as it exists on the DHCP request received upstream across the UNI. Range "0".. "4096" for C-VID; range "0".."65535" for VCI. The value "4096" indicates no C-VID tag.

Spaces in the provisioned string are significant.

Example: if the large string were provisioned with the value

%01%SL/%SU/%PO:%AE/%SV.%CV<null>,

then the ONU would generate the following DHCP option 82 agent circuit-ID string for an Ethernet UNI that sent a DHCP request with no S tag and C tag = 3210 on shelf 2, slot 3, port 4.

2/3/4:eth/4096.3210

With the same provisioning, the ONU would generate the following DHCP option 82 agent circuit-ID string for an ATM UNI that sent a DHCP request on VPI = 123 and VCI = 4567 on shelf 2, slot 3, port 4.

2/3/4:atm/123.4567

9.4.5 IPv6 host config data

Add the following attribute to the IPv6 host config data ME:

Relay agent options: This attribute is a pointer to a large string managed entity whose content specifies one or more DHCP relay agent options. (R, W) (optional) (2 bytes)

The meaning and interpretation of the large string's contents is identical to that described in the IP host config data definition in clause 9.4.1.

9.5 Ethernet services

Replace the introductory figure with the following:

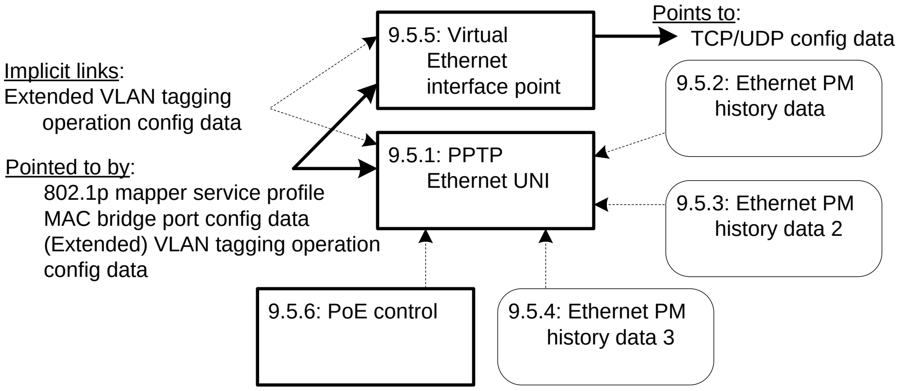

Points to:
TCP/UDP config data
9.5.5: Virtual Ethernet interface point
Implicit links:
Extended VLAN tagging operation config data
9.5.2: Ethernet PM history data
9.5.1: PPTP Ethernet UNI
Pointed to by:
802.1p mapper service profile
MAC bridge port config data
(Extended) VLAN tagging operation config data
9.5.3: Ethernet PM history data 2
9.5.6: PoE control
9.5.4: Ethernet PM history data 3

Figure 9.5-1 – Managed entities associated with Ethernet UNIs

9.5.1 Physical path termination point Ethernet UNI

Add the following note to the power control attribute:

Power control: This attribute controls whether power is provided to an external equipment over the Ethernet PPTP. The value 1 enables power over the Ethernet port. The default value 0 disables power feed. (R, W) (optional) (1 byte)

NOTE – This attribute is the equivalent of the acPSEAdminControl variable defined in [IEEE 802.3], clause 30.9.1.2.1. Other variables related to power over Ethernet appear in the PoE control ME.

9.5.5 Virtual Ethernet interface point

Revise the ME ID attribute of this managed entity to read as follows:

Managed entity id: This attribute uniquely identifies each instance of this managed entity. When used independently of a cardholder and circuit pack, the ONU should assign IDs in the sequence 1, 2,…. When used in conjunction with a cardholder and circuit pack, this two-byte number indicates the physical position of the VEIP. The first byte is the slot ID (defined in clause 9.1.5). The second byte is the port ID, with range 1..255. The values 0 and 0xFFFF are reserved. (R) (mandatory) (2 bytes)

9.5.6 Power over Ethernet (PoE) control

Add new clause 9.5.6 as follows:

9.5.6 Power over Ethernet (PoE) control

This managed entity represents the ability to monitor and control the power over Ethernet (PoE) capability of the ONU as a power-sourcing equipment (PSE) as defined in [IEEE 802.3], clauses 30.9 and 33.

An ONU that supports the enhanced PoE control feature automatically creates or deletes an instance of this managed entity whenever it creates or deletes the corresponding PPTP Ethernet UNI.

Administrative control of the PoE feature resides in the power control attribute of the PPTP Ethernet UNI ME.

Relationships

An instance of this managed entity is associated with each instance of a PPTP Ethernet UNI.

Attributes

Managed entity id: This attribute uniquely identifies each instance of this managed entity. Through an identical ID, this managed entity is implicitly linked to an instance of the physical path Ethernet UNI managed entity. (R) (mandatory) (2 bytes)

PoE capabilities: This attribute is a bit map that identifies the PoE capabilities of the port.

Bits are assigned as follows:

<u>Bit</u>	<u>Meaning</u>
1 (LSB)	When this bit is 1, the PSE pinout alternative may be changed through the power pair pinout control attribute. When the bit is 0, the PSE pinout alternative is fixed, and is described by the power pair pinout control attribute.
2..16	Reserved

(R) (mandatory) (2 bytes)

Power pair pinout control: If the PSE pinout is configurable, according to the PoE capabilities attribute, this attribute is used to configure the pinout. If the PSE pinout is fixed, this attribute is read-only. In either case, the value returned by a get operation indicates the actual configuration. The value 0 configures/indicates pinout alternative A (signal pairs); the value 1 configures/indicates pinout alternative B (spare pairs). Other values are reserved. This attribute corresponds to the aPSEPowerPairs variable defined in [IEEE 802.3]. (R, W) (mandatory) (1 byte)

Operational state: This attribute indicates whether or not the PPTP is capable of performing its function. Valid values are enabled (0) and disabled (1). (R) (mandatory) (1 byte)

Power detection status: This attribute is an enumeration that returns the current status of the port. It corresponds to the aPSEPowerDetectionStatus variable defined in [IEEE 802.3]. Its values are defined as follows:

0	PSE disabled
1	PSE searching
2	PSE delivering power
3	PSE test mode
4	PSE fault detected
5	PSE implementation specific fault detected

Other values are reserved.

(R) (mandatory) (1 byte)

Power classification status: This attribute is an enumeration that indicates the PD class of a detected PD. It is only valid when the power detection status attribute indicates PSE delivering power. The attribute corresponds to the aPSEPowerClassification variable defined in [IEEE 802.3]. Its values are defined as follows:

0	Undefined or feature not supported
1	Class 0 PD

2 Class 1 PD

3 Class 2 PD

4 Class 3 PD

5 Class 4 PD

Other values are reserved.

(R) (optional) (1 byte)

Power priority: This attribute controls the priority of the port from the point of view of a power management algorithm. The priority that is set by this attribute could be used by a control mechanism that prevents overcurrent situations by first disconnecting ports with lower power priority (higher numerical value). The attribute corresponds to the pethPsePortPowerPriority variable defined in [b-IETF RFC 3621]. Valid values are

1 critical

2 high

3 low

(R, W) (optional) (1 byte)

Invalid signature counter: This attribute increments when the [IEEE 802.3] Figure 33-6 PoE state machine enters the signature_invalid state, but not more than twice per second. The counter is never explicitly reset, but is not required to persist over ONU initialization. (R) (optional) (2 bytes)

Power denied counter: This attribute increments when the [IEEE 802.3] Figure 33-6 PoE state machine enters the power_denied state, but not more than twice per second. The counter is never explicitly reset, but is not required to persist over ONU initialization. (R) (optional) (2 bytes)

Overload counter: This attribute increments when the [IEEE 802.3] Figure 33-6 PoE state machine enters the error_delay_over state, but not more than twice per second. The counter is never explicitly reset, but is not required to persist over ONU initialization. (R) (optional) (2 bytes)

Short counter: This attribute increments when the [IEEE 802.3] Figure 33-6 PoE state machine enters the error_delay_short state, but not more than twice per second. The counter is never explicitly reset, but is not required to persist over ONU initialization. (R) (optional) (2 bytes)

MPS absent counter: This attribute increments when the [IEEE 802.3] Figure 33-6 PoE state machine goes from the state power_on to the idle state, but not more than twice per second. The counter is never explicitly reset, but is not required to persist over ONU initialization. (R) (optional) (2 bytes)

PsE class control: This attribute may be used to place specific limits on the class of power supported by this port. Valid code points for this attribute are:

0 Power feed enabled at the default level for this port

1 Power feed enabled at the class 0 power level

2 Power feed enabled at the class 1 power level

3 Power feed enabled at the class 2 power level

4 Power feed enabled at the class 3 power level

5 Power feed enabled at the class 4 power level

Other values are reserved. (R, W) (optional) (1 byte)

Actions

Get, set

Notifications

Attribute value change

Number	Attribute value change	Description
1..2	N/A	
3	Operational state	
4..12	N/A	
13..16	Reserved	

9.8 TDM services

9.8.14 MPLS pseudowire termination point

Add code point 4 to the TP type attribute, as shown:

TP type: This attribute specifies the type of ANI-side termination point associated with this managed entity.

…

4 MPLS pseudowire termination point

NOTE – If this instance of the MPLS PW TP is pointed to by another instance of the MPLS PW TP (i.e., whose TP type = 4), this instance represents a tunnelled MPLS flow, and the following attributes are not meaningful: MPLS PW direction, MPLS PW uplink label, MPLS PW downlink label, and MPLS PW TC. These attributes should be set to the proper number of 0x00 bytes by the OLT and ignored by the ONU.

Add the following two new attributes:

Administrative state: This attribute locks (1) and unlocks (0) the functions performed by the MPLS pseudowire TP. Administrative state is further described in clause A.1.6. (R, W) (optional) (1 byte)

Operational state: This attribute reports whether the managed entity is currently capable of performing its function. Valid values are enabled (0) and disabled (1). (R) (optional) (1 byte)

Notifications

Add the following table to the notifications section:

Attribute value change

Number	Attribute value change	Description
1..14	N/A	
15	Op state	Operational state
16	Reserved	

9.8.17 PW Ethernet configuration data

Add code point 13 to the TP type attribute, as follows:

TP type: This attribute identifies the type of UNI associated with this Ethernet PW. Valid values are:

…

13 MAC bridge port configuration data

9.8.18 Ethernet pseudowire parameters

Add the following new ME:

This managed entity contains the Ethernet pseudowire parameters. Instances of this managed entity are created and deleted by the OLT.

Relationships

An instance of this managed entity is associated with an instance of the PW Ethernet configuration data managed entity.

Attributes

Managed entity id: This attribute uniquely identifies each instance of this managed entity. Through an identical ID, this managed entity is implicitly linked to an instance of the PW Ethernet configuration data managed entity. (R, Set-by-create) (mandatory) (2 bytes)

MTU: This attribute identifies the maximum transmission unit (bytes) that can be received from the CPE in the upstream direction. Larger frames are discarded. (R, W, Set-by-create) (mandatory) (2 bytes)

Actions

Create, delete, get, set

Notifications

None

9.9 Voice services

9.9.7 RTP profile data

Modify the following attributes to read as follows (stricken through text is to be deleted):

Local port min: This attribute defines the base ~~RTP~~ UDP port that should be used by RTP for voice traffic. The recommended default is 50 000 (R, W, Set-by-create) (mandatory) (2 bytes)

Local port max: This attribute defines the highest ~~RTP~~ UDP port used by RTP for voice traffic. The value must be greater than local port min. The value 0 specifies that the local port max be equal to the local port min. (R, W, Set-by-create) (optional) (2 bytes)

Add the following new attribute at the end of the attributes list:

IP host config pointer: This optional pointer associates the bearer (voice) flow with an IP host config data or IPv6 host config data ME. If this attribute is not present or is not populated with a valid pointer value, the bearer flow uses the same IP stack that is used for signalling, indicated by the TCP/UDP pointer in the associated SIP agent or MGC config data. The default value is 0xFFFF, a null pointer. (R, W) (optional) (2 bytes)

9.12.1 UNI-G

Modify the following attributes to read as shown:

Deprecated: This attribute is not used. It should be set to 0 by the OLT and ignored by the ONU. (R, W) (mandatory) (2 bytes) ~~**Configuration option status**: This attribute holds the UNI configuration code field. The bit value 0 inhibits the specified alarm reporting function, while bit value 1 enables it. Bits are assigned as shown below:~~

~~**Bit**~~	~~**Name**~~	~~**Setting**~~
~~1 (LSB)~~	~~N/A~~	
~~2~~	~~Server trail fault propagation TC layer~~	~~TC layer alarm reporting through OMCC~~
~~3~~	~~Server trail fault propagation PHY layer~~	~~PHY layer alarm reporting through OMCC~~
4	~~Server trail fault propagation GAL layer~~	~~GAL layer alarm reporting through OMCC~~
~~5..16~~	~~Reserved~~	

~~(R, W) (mandatory) (2 bytes)~~

Administrative state: This attribute locks (1) and unlocks (0) the functions performed by this managed entity. Administrative state is further described in clause A.1.6. (R, W) (mandatory) (1 byte)

NOTE – PPTP MEs also have an administrative state attribute. The user port is unlocked only if both administrative state attributes are set to unlocked. It is recommended that this attribute not be used: that the OLT set it to 0 and that the ONU ignore it.

Add the following attribute to the UNI-G ME:

Relay agent options: This attribute is a pointer to a large string managed entity whose content specifies one or more DHCP relay agent options. (R, W) (optional) (2 bytes)

The content of the large string is parsed by the ONU and converted into text strings. Variable substitution is based on defined three-character groups, each of which begins with the '%' character. The string '%%' is an escape mechanism whose output is a single '%' character. When the ONU cannot perform variable substitution on a substring of the large string, it generates the specified option as an exact quotation of the provisioned substring value.

Provisioning of the large string is separate from the operation of setting the pointer in this attribute. It is the responsibility of the OLT to ensure that the large string contents are correct and meaningful.

Three-character variable definitions are as follows. The first variable in the large string must specify one of the option types. Both options for a given IP version may be present if desired, each introduced by its option identifier. Terminology is taken from [b-BBF TR-101] clause 3.9.3.

%01, %18
Specifies that the following string is for option 82 sub-option 1, agent circuit-ID (IPv4) or option 18, interface-ID (IPv6). The equivalence permits the same large string to be used in both IP environments.

%02, %37
Specifies that the following string is for option 82 sub-option 2, relay agent remote-ID (IPv4) or option 37, relay agent remote-ID (IPv6). The equivalence permits the same large string to be used in both IP environments.

%SL In TR-101, this is called a slot. In an ONU, this variable refers to a shelf. It would be meaningful if the ONU has multiple shelves internally or is daisy-chained to multiple equipment modules. The range of this variable is "0".. "99"

%SU In TR-101, this is called a sub-slot. In fact, it represents a cardholder. The range of this variable is "0".. "99"

%PO UNI port number. The range of this variable is "0".. "999"

%AE ATM or Ethernet. This variable can take on the values "atm" or "eth".

%SV S-VID for Ethernet UNI, or ATM VPI for ATM UNI, as it exists on the DHCP request received upstream across the UNI. Range "0".. "4096" for S-VID; range "0".. "255" for VPI. The value "4096" indicates no S-VID tag.

%CV C-VID (Q-VID) for Ethernet UNI, or ATM VCI for ATM UNI, as it exists on the DHCP request received upstream across the UNI. Range "0".. "4096" for C-VID; range "0".."65535" for VCI. The value "4096" indicates no C-VID tag.

Spaces in the provisioned string are significant.

Example: if the large string were provisioned with the value

%01%SL/%SU/%PO:%AE/%SV.%CV<null>,

then the ONU would generate the following DHCP option 82 agent circuit-ID string for an Ethernet UNI that sent a DHCP request with no S tag and C tag = 3210 on shelf 2, slot 3, port 4.

2/3/4:eth/4096.3210

With the same provisioning, the ONU would generate the following DHCP option 82 agent circuit-ID string for an ATM UNI that sent a DHCP request on VPI = 123 and VCI = 4567 on shelf 2, slot 3, port 4.

2/3/4:atm/123.4567

9.13 Miscellaneous services

Replace clause 9.13.11 in its entirety, with the following:

9.13.11 Enhanced security control

This managed entity contains the capabilities, parameters and controls of enhanced G-PON security features when they are negotiated via OMCI (Note). The attributes in this ME are intended to be used to implement a symmetric-key-based three step authentication process as described in the supplemental information section below.

NOTE – If an ITU-T G.987 system uses 802.1X authentication as defined in [ITU-T G.987.3], the only applicable attribute of this ME is the broadcast key table.

Relationships

One instance of this managed entity is associated with the ONU managed entity.

Attributes

Managed entity id: This attribute uniquely identifies each instance of this managed entity. There is only one instance, number 0. (R) (mandatory) (2 bytes)

OLT crypto capabilities: This attribute specifies the cryptographic mechanisms available at the OLT. It is written by the OLT during authentication step 1. It is formatted as a bit map, where a 1 bit indicates that the particular algorithm is supported, and a 0 bit indicates it is not supported.

Bit position	Algorithm
1 (LSB)	AES-CMAC-128 (support is mandatory)
2	HMAC-SHA-256
3	HMAC-SHA-512
4-128	Reserved

(W) (mandatory) (16 bytes)

OLT random challenge table: This attribute specifies the random challenge OLT_challenge issued by the OLT during authentication step 1. It is structured as a table, with each entry being 17 bytes. The first byte is the table row number, starting at 1, and the remaining 16 bytes are the content of the entry. OLT_challenge is the concatenation of all 16-byte content fields. In normal use, the OLT will write all the entries in the table, and then trigger the ONU's processing of the entire table using the OLT challenge status attribute. The table size is known by the maximum index set by the OLT. The OLT can clear the table with a set operation to row 0. (R, W) (mandatory) (17 * N bytes)

NOTE – It is assumed that the length of OLT_challenge is always an integer multiple of 16 bytes.

OLT challenge status: This Boolean attribute controls the completion of authentication step 1. This attribute behaves as follows:

When the OLT performs the first of possibly several set operations to the OLT crypto capabilities or the OLT random challenge table attributes, a side effect of the set operation is that the ONU sets the OLT challenge status attribute to false.

When the OLT completes the set operation(s) to the OLT crypto capabilities and the OLT random challenge table attributes, then it sets the OLT challenge status attribute to true. This triggers the ONU to process the OLT random challenge table, using its choice of the OLT's candidate cryptographic hash algorithms.

The ONU initializes this attribute to the value false. (R, W) (mandatory) (1 byte)

ONU selected crypto capabilities: This attribute specifies the cryptographic capability selected by the ONU in authentication step 2. Its value specifies one of the bit positions that has the value 1 in the OLT crypto capabilities attribute. (R) (mandatory) (1 byte)

ONU random challenge table: This attribute specifies the random challenge ONU_challenge issued by the ONU during authentication step 2. It is structured as a table, with each entry being 16 bytes of content. ONU_challenge is the concatenation of all 16-byte content fields in the table. Once the OLT triggers a response to be generated using the OLT challenge status attribute, the ONU generates the response and writes the table (in a single operation). The AVC generated by this attribute signals the OLT that the challenge is ready, so that the OLT can commence a get/get-next sequence to obtain the table's contents. (R) (mandatory) (16 * P bytes)

ONU authentication result table: (authentication step 2). This attribute contains the result of the authentication computation from the ONU (ONU_result), according to the ONU's selected crypto capabilities attribute.

ONU_result = SelectedHashFunction (PSK, (ONU_selected_crypto capabilities | OLT_challenge | ONU_challenge | 0x0000 0000 0000 0000)),

where "|" denotes concatenation.

This attribute is structured as a table, with each entry being 16 bytes of content. The number of rows Q is implicit in the choice of hash algorithm.

Once the OLT triggers a response to be generated using the OLT challenge status attribute, the ONU generates ONU_result and writes the table (in a single operation). The AVC generated by this attribute signals the OLT that the response is ready, so that the OLT can commence a get/get-next sequence to obtain the table's contents. (R) (mandatory) (16 * Q bytes)

OLT authentication result table: This attribute is used in authentication step 3. It contains OLT_result, the result of the authentication computation from the OLT.

OLT_result = SelectedHashFunction (PSK, (ONU_selected_crypto capabilities | ONU_challenge | OLT_challenge | ONU_serial_number)).

The ONU_serial_number is the serial number attribute of the ONU-G managed entity, 8 bytes.

This attribute is structured as a table, with each entry being 17 bytes. The first byte is the table row number, starting at 1; the remaining 16 bytes are content. OLT_result is the concatenation of all 16-byte content fields. The OLT writes all entries into the table, and then triggers the ONU's processing of the table using the OLT result status attribute. The number of rows R is implicit in the choice of hash algorithm. The OLT can clear the table with a set operation to row 0. (W) (mandatory) (17 * R bytes)

OLT result status: (authentication step 3). This Boolean attribute controls and reports the status of the OLT authentication result table attribute. This attribute behaves as follows:

> When the OLT performs the first of possibly several set operations to the OLT authentication result table attribute, a side effect of the set operation is that the ONU sets the OLT result status attribute to false.
>
> When the OLT completes the set operation(s) to the OLT authentication result table, then it sets the OLT result status attribute to true. This triggers the ONU to process the OLT authentication result table.

(R, W) (mandatory) (1 byte)

ONU authentication status: This attribute indicates the status of the authentication relationship from the perspective of the ONU. It has the following values:

0 Indeterminate. This initial value indicates that the OMCI authentication process has not yet completed, and may not even have been started.

1 Reserved.

2 Reserved.

3 Authentication success: the procedure has completed at least once and in its most recent execution, the ONU has authenticated the OLT

4 Authentication failure: the procedure has completed at least once, and either its most recent execution resulted in an error, or the ONU has failed to authenticate the OLT

5 Reserved.

When the ONU authentication status has the value 3, encryption keys exchanged in the TC layer will be encrypted using the master session key (ITU-T G.984 systems) or the key encryption key (ITU-T G.987 systems). The OLT should check the value of of this attribute before initiating a key switch.

(R) (mandatory) (1 byte)

Master session key name: Following successful authentication, this register contains the "name," or the hash signature, of the current master session key. The master session key is defined as:

> MSK = SelectedHashFunction (PSK, (OLT_challenge | ONU_challenge)).

The master session key name is defined as:

> MSKname = SelectedHashFunction (PSK, (ONU_challenge | OLT_challenge | 0x 3141 5926 5358 9793 3141 5926 5358 9793)).

If the selected hash function generates more than 128 bits, the result is truncated to the leftmost (most significant) 128 bits.

Upon the invalidation of a master session key (e.g., due to an ONU reset or deactivation, or due to an ONU-local decision that the master session key has expired), the ONU sets the master session key name to all zeros. (R) (mandatory) (16 bytes)

Broadcast key table: This attribute is defined only in ITU-T G.987 systems. It contains the broadcast key generated by the OLT. It is a table, each of whose rows is structured as follows:

Row control (1 byte): The two least significant bits of this byte determine the attribute's behaviour under the set action. They always read back as 0 under the get next action.

00 Set the specified row.

01 Clear the specified row.

10 Clear the entire table.

11 Reserved

The four most significant bits specify the length of the fragment, which is left-justified in the key fragment field. The value 0 indicates 16 bytes of key fragment.

The other two bits are reserved.

Row identifier (1 byte): The two most significant bits of this field are the key index, which appears in the header of encrypted multicast GEM frames. Key index 0 always indicates cleartext, and should therefore not appear in the identifier. The four least significant bits identify the key fragment number, starting with 0. The other two bits are reserved.

Key fragment (16 bytes): This field contains the specified fragment of the key (encrypted with AES-ECB using the KEK).

(R, W) (optional) (18N bytes)

Effective key length: This attribute specifies the maximum effective length, in bits, of keys generated by the ONU. (R) (optional) (2 bytes)

Actions

Get, set, get next

Notifications

Attribute value change

Number	Attribute value change	Description
1..4	Reserved	
5	ONU random challenge table	A new ONU challenge has been loaded into the table for the OLT to retrieve
6	ONU authentication result table	A new ONU response has been loaded into the table for the OLT to retrieve
7..8	Reserved	
9	ONU authentication status	The ONU authentication status has changed
10..16	Reserved	

Supplementary information

This managed entity contains the facilities to perform a conventional three step hash-based authentication sequence found in [ISO/IEC 9798-4] (used in DSL systems that employ MS-CHAPv2 and elsewhere) using get and set messages.

The logical structure of the conventional three step sequence is as follows. In the present situation, peer 1 is the OLT and peer 2 is the ONU:

Message 1: (Peer 1 → peer 2) my_cryptographic_capabilities | random_challenge_1

Message 2: (Peer 2 → peer 1): selected_cryptographic_capabilities | random_challenge_2 | MsgHash (PSK, (selected_cryptographic_capabilities | random_challenge_1 | random_challenge_2, peer_1_identity))

Message 3: (Peer 1 → peer 2): MsgHash (PSK, (selected_cryptographic_capabilities | random_challenge_2 | random_challenge_1 | peer_2_identity))

Where:

MsgHash () is a keyed hash function of the message

PSK is the pre-shared key known to the peers of the session

Peer_1_identity is always "0x0000 0000 0000 0000"

Peer_2_identity is the ONU serial number

The prerequisite is the availability of a pre-shared secret PSK. A PSK of 128 bits simplifies the application of security algorithms based on AES-128 (e.g., AES-CMAC-128). A PSK is associated with a particular ONU and is stored at that ONU and at the operator infrastructure. On the operator side, the PSK for a particular ONU might be stored in the physically-connected OLT, or at a central server that the OLT accesses during authentication. Configuration of the PSK into the ONU and into the operator infrastructure may be done in any manner that satisfies these requirements.

In OMCI, the authentication message sequence follows the steps illustrated in Figure 9.13.11-1.

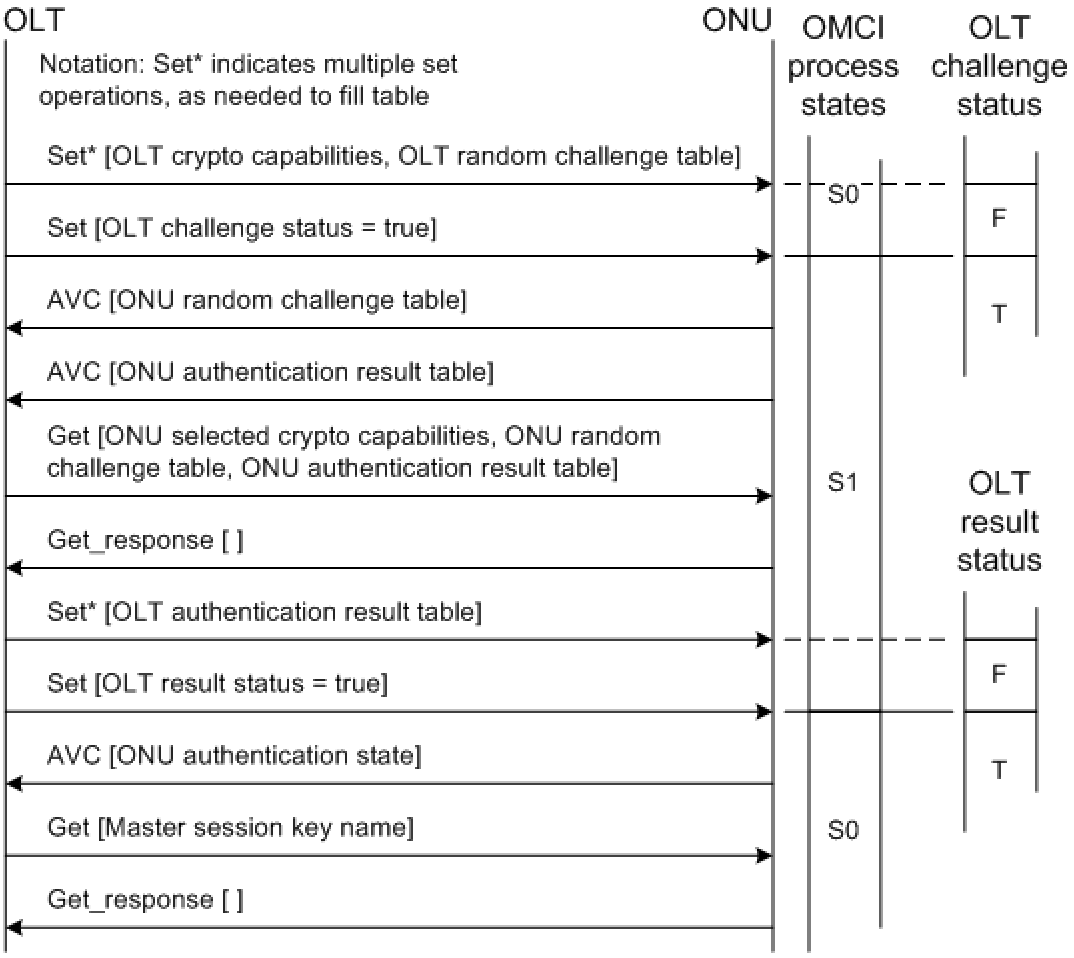

OLT
ONU
OMCI process states
OLT challenge status
Notation: Set* indicates multiple set operations, as needed to fill table
Set* [OLT crypto capabilities, OLT random challenge table]
Set [OLT challenge status = true]
AVC [ONU random challenge table]
AVC [ONU authentication result table]
Get [ONU selected crypto capabilities, ONU random challenge table, ONU authentication result table]
Get_response [ ]
Set* [OLT authentication result table]
Set [OLT result status = true]
AVC [ONU authentication state]
Get [Master session key name]
Get_response [ ]
S0
S1
S0
F
T
OLT result status
F
T

Figure 9.13.11-1 – Authentication message exchange sequence

States of the OMCI authentication process

When an ONU is in operation state O5, as defined in [ITU-T G.984.3] and [ITU-T G.987.3], it maintains an OMCI authentication process state machine that tracks the phase of the authentication-related OMCI message flow exchange. The OMCI authentication process state machine is driven by the OLT challenge and result status indications, and generates output that indicates the ONU authentication status.

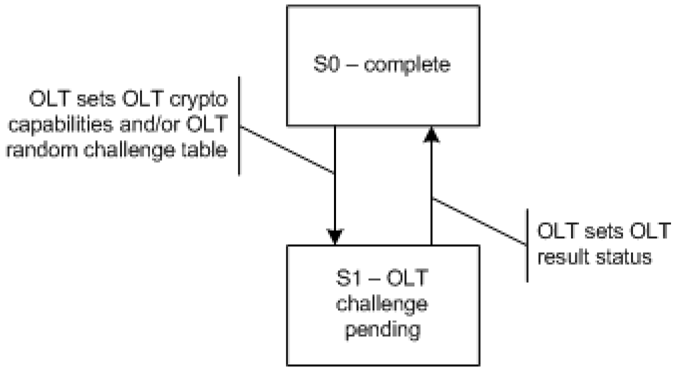

S0 – complete
OLT sets OLT crypto capabilities and/or OLT random challenge table
OLT sets OLT result status
S1 – OLT challenge pending

Figure 9.13.11-2 – ONU state diagram

Synchronization with TC layer and security considerations (ITU-T G.984 systems only)

When the ONU is in authenticated state, it uses its master session key to encrypt the key transmitted in the encryption_key PLOAM message.

The master session key is defined as:

MasterSessionKey = SelectedHashFunction (PSK, (OLT_challenge | ONU_challenge))

where SelectedHashFunction () is the hash function selected by the ONU in the ONU selected crypto capabilities attribute from the list supplied by the OLT.

The encryption of the encryption key is performed using AES-128 in electronic codebook (ECB) mode.

Since the encryption key carried in the encryption key PLOAM message is not protected against forgery, there is the possibility that the key can be forged or replayed by an attacker. Both forged and replayed keys can be detected with key synchronization mechanisms. A replay attack, however, could force the OLT to use an old encryption key, which would violate the security requirements of downstream data encryption. Consequently, an OLT designed to resist a replay attack should ensure that the ONU does not send a previously used encryption key between authentication cycles.

11 ONU management and control protocol

11.2.4 Managed entity identifier

Add the following new entries to Table 11.2.4-1 and adjust the reserved space accordingly.

Table 11.2.4-1 – Managed entity identifiers

Managed entity class value	Managed entity
349	PoE control
350-399	Reserved for vendor specific use
400	Ethernet pseudowire parameters
401-65279	Reserved for future standardization
65280-65535	Reserved for vendor specific use

Annex A

OMCI message syntax and common features

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

A.1 General

A.1.1 Result and reason

Add the following text at the end of this clause:

When the result-reason code in a response message indicates an exception (that is, its value is not 0), the response message is permitted to include vendor-specific additional information. The rules for additional error information are:

1. Additional error information is optional for the ONU to insert.
2. Additional information may or may not be represented in textual form.
3. The semantics of additional error information are specific to the ONU vendor.
4. The ONU must not rely on the OLT being able to detect or interpret additional error information.
5. Additional error information may occupy only padding bytes (baseline message set) or only uncommitted trailing bytes (extended message set).
6. In get, get current data and get next responses, the attribute mask controls the padding definition.
7. No additional error information is permitted in responses to start download and end download messages that are directed to multiple target MEs, as indicated by 0xFFFF in the target ME identifier.

These rules are defined with a view to maximizing the simplicity of an implementation.

A.2 Extended message set

A.2.21 Test

A.2.21.2 Format for IP host config data and IPv6 host config data entity classes

Revise the table to read as shown:

Field	**Byte**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**Comments**
Message contents length	9-10									Size of message contents field
Message contents	11	0	0	0	0	x	x	x	x	xxxx = select test 0001 Ping 0010 Traceroute 0011 Extended ping 0100..0111 Reserved 1000..1111 Vendor-specific use. The ICMP message is intended to be sent from the ONU upstream toward the network. See discussion related to the test result message.
	12-15									Option 1: IPv4 address of target (zero if byte 0 specifies extended ping test)

Field	Byte	8	7	6	5	4	3	2	1	Comments
	12-27									Option 2: IPv6 address of target (zero if byte 0 specifies extended ping test)
	28									Number of times to ping. This field pertains to both explicit and extended ping tests. The value 0 or the absence of this field selects the ONU's internal default.
	29-30									Pointer to large string ME that identifies the target via a DNS-parseable string. This field is used only for the extended ping test.

A.2.23 Start software download

Add the underlined text shown below:

Managed entity identifier	5-6									Entity class = software image
	7									MS byte of software image instance 0 ONU-G 1..254 slot number 255 download to multiple software image managed entities
	8									LS byte of software image instance 0 instance 0 1 instance 1 2..254 vendor-specific use 255 multiple download
Message contents length	9-10									Size of message contents field, bytes
Message contents	11									Window size – 1
	12-15									Image size in bytes
	16									Number of circuit packs to be updated in parallel (value 1...9)
	17-18									ME id of software image entity instance (first byte: slot number; second byte: instance 0..1 or 2..254 vendor-specific)
	19-20 etc.									Additional software image ME ids (same format as bytes 17..18) for additional simultaneous downloads.

Make the same changes, as applicable, to the following 19 clauses:

A.3.23 Start software download

A.2.24 A.3.24 Start software download response

A.2.25 A.3.25 Download section

A.2.26 A.3.26 Download section response

A.2.27 A.3.27 End software download

A.2.28 A.3.28 End software download response

A.2.29 A.3.29 Activate image

A.2.30 A.3.30 Activate image response

A.2.31 A.3.31 Commit image

A.2.32 A.3.32 Commit image response

A.2.39 Test result

A.2.39.4 Format for test action invoked against IP host config data and IPv6 host config data entity classes

Revise the first two tables and the intermediate text to read as shown:

Field	Byte	8	7	6	5	4	3	2	1	Comments
Message contents	11	0	0	0	0	0	x	x	x	xxx: Test result 000 Timed out, no response 001 ICMP echo responses attached 010 ICMP time exceeded responses attached 011 Unexpected ICMP response 100 Target address in large string ME could not be resolved 101..111 Reserved
	12..n									See following descriptions for the content of these bytes

If xxx = 001 (echo response – ping), the remainder of the message contains the following content. If the test message specifies the number of times to ping, the ONU should generate that number of echo requests; otherwise the number of echo requests generated is the ONU vendor's default. The resolution of the delay measurement is vendor-specific. The special value 0xFFFF indicates a lost response.

	12-27									In the extended ping test, these bytes contain the actual IP address that was pinged 4 bytes for IPv4, 16 bytes for IPv6. If the network address was not resolvable, the ONU should set these bytes to all zeroes. In the normal (non-extended ping test), delay measurements begin immediately in byte 12, according to the same pattern shown in bytes 28-29, etc.
	28-29									16-bit measurement of response delay n, expressed in ms.
	30-31									16-bit measurement of response delay n+1, expressed in ms.
	…									Etc.

A.3 Baseline message set

A.3.21 Test

A.3.21.2 Format for IP host config data and IPv6 host config data entity classes

Modify the table in the IP host config data entity class to read as shown:

Field	Byte	8	7	6	5	4	3	2	1	Comments
Message contents	9	0	0	0	0	x	x	x	x	xxxx = select test 0001 = Ping 0010 = Traceroute 0011 = Extended ping 0100..0111 Reserved 1000..1111 Vendor-specific use The ICMP message is intended to be from the ONU upstream toward the network. See discussion related to the test result message.
	10-13									Option 1: IPv4 address of target (zero if byte 0 specifies extended ping test)
	10-25									Option 2: IPv6 address of target (zero if byte 0 specifies extended ping test)
	26									Number of times to ping. This field pertains to both explicit and extended ping tests. The value 0 selects the ONU's internal default. NOTE – The number is bounded by the size of the test result message. It can be up to 15 for explicit ping and up to 7 for extended ping.
	27-28									Pointer to large string ME that identifies the target via a DNS-parseable string. This field is used only for the extended ping test.
	...40	0	0	0	0	0	0	0	0	Zero padding

A.3.39 Test result

A.3.39.4 Format for test action invoked against IP host config data and IPv6 host config data entity classes

Revise the first two tables and the intermediate text to read as shown:

Message contents	9	0	0	0	0	0	x	x	x	Test result: xxx = 000: timed out, no response xxx = 001: ICMP echo responses attached xxx = 010: ICMP time exceeded responses attached xxx = 011: Unexpected ICMP response xxx = 100: target address in large string ME could not be resolved xxx = 101-111: Reserved
	10	0	0	0	y	y	y	y	y	yyyyy: number of meaningful bytes in the remainder of the test result message. In the case of extended ping, this field is the number of bytes that contain delay measurement values.

If xxx = 001 (echo response – ping), the remainder of the message contains the following content. If the test message specifies the number of times to ping, the ONU should generate that number of echo requests; otherwise the number of echo requests generated is the ONU vendor's default. The resolution of the delay measurement is vendor-specific. The special value 0xFFFF indicates a lost response.

	11-12									16-bit measurement of response delay 1, expressed in ms
	13-14									16-bit measurement of response delay 2, expressed in ms
	…									Etc.
	25-40									For ping test 0001, these bytes can be either delay measurements or padding. For extended ping, these bytes contain the actual IP address that was pinged, 4 bytes for IPv4, 16 bytes for IPv6. If the network address was not resolvable, the ONU should set these bytes to all zeroes.

Bibliography

Add the following reference to the bibliography:

[b-IETF RFC 3621] IETF RFC 3621 (2003), *Power Ethernet MIB.*

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