Annex B: PLOAM and OMCI security-related messages

PLOAM

PLOAM uses simple messages with a message type and structured content to exchange configuration data. In the table below, a flow represents the succession of downstream (OLT) and upstream (ONU) PLOAM messages that achieve the described operation.

Flow	Description	PON version
1. (Upstream) Serial_Number_ONU	The ONU sends its serial number during the initialisation process in response to a serial number grant (the OLT grants the ONU an upstream opportunity to send the serial number). Used as a first identifier and in the OMCI-based authentication protocol.	All
1. (Downstream) Request_Password 2. (Upstream) Password (three times)	The (PLOAM) password is one of the identifiers the OLT can request from the ONU in GPON. It's just another identifier.	GPON
1. (Downstream) Request_Registration 2. (Upstream) Registration	Request the ONU's *Registration_ID*, to use in *Registration_ID* authentication for instance.	XG(S)-PON, NG-PON2 and 50G-PON
1. (Downstream) Key_Control 2. (Upstream) Key_Report (repeated)	The OLT requests a new data encryption key or wants to confirm an existing key. The ONU sends the key in 32-byte fragments. The required key length is provided by the *Key_Length* field. (50G-PON only) The OLT request contains up to two random 128-bit numbers that should be used in the data encryption key generation.	XG(S)-PON, NG-PON2 and 50G-PON
1. (Downstream) Request_Key 2. (Upstream) Encryption key (three times for each 8-byte fragment)	The OLT requests a new AES key or wants to confirm an existing key. Superseded by *Key_Control*/*Key_Report* in later PON specifications.	GPON
1. (Downstream) Key_Switching_Time	GPON uses PLOAM to synchronize the moment when	GPON

Flow	Description	PON version
2. (Upstream) Acknowledge	a new AES key will start being used. Newer versions have a slot system and a state-machine to manage how encryption keys are renewed.	
1. (Downstream) Encrypted_Port-ID 2. (Upstream) Acknowledge	GPON does not use OMCI for enabling encryption on GEM ports; instead, a PLOAM message is used.	GPON

OMCI

OMCI differs from PLOAM: messages are mostly exchanged to update a database called MIB (Management Information Base). The MIB is separated into Management Entities (ME) with attributes, and it is synced between the OLT and the ONU (the OLT centralizes the MIBs of all its ONUs). Some fields are writable only by the ONU and others only by the OLT.

OMCI Management Entity	Attributes	Description
ONU-G	• Logical ONU ID (LOID) • Logical password (LOID PW) • Credentials status	*LOID/LOID PW* are one mechanism that can be used for ONU identification. Some manufacturers use vendor-specific Management Entities which themselves seem to use similar identifiers (LOID/LOID PW). *Credential status*: allows the OLT to indicate to the ONU if the LOID identification was successful and if not, why.
ONU2-G	• Security capability • Security mode	*Security capability* allows the ONU to broadcast which block cipher (used for data encryption) it supports. *Security mode* is used by the OLT to select one of the block ciphers reported in *Security capability*. It is shared by all (X)GEM ports, and defaults to AES-128.
GEM port network CTP	• Encryption state • Encryption key ring	*Encryption state* indicates the state of encryption of the targeted (X)GEM port. *0* indicates an unencrypted port while the other values are

OMCI Management Entity	Attributes	Description
		taken from the *Security mode* attribute of ONU2-G. *Encryption key ring* enables encryption, either unicast in both directions, unicast in downstream only, multicast (broadcast) or unencrypted.
Enhanced security control	• Several fields related to the OMCI authentication mode. • Broadcast key table • Effective key length	Outside of fields related to the OMCI authentication mode, the *Broadcast key table* contains the multicast (broadcast) keys that are available in XG(S)-PON and above, and generated on the OLT. *Effective key length* reports the maximum effective key size in bits of the encryption keys generated by the ONU.
Dot1X OLT/ONU authentication termination point	• OLT Admin State • ONU Admin State • Operational Status	*OLT Admin State* and *ONU Admin State* respectively assert whether the OLT mandates the use of the IEEE 802.1X authentication and if the ONU mandates it. If they do, they will respectively drop upstream and downstream XGEM frames. *Operational Status* reflects whether the link between the ONU and the OLT is currently authenticated using IEEE 802.1X or not.