14 Management entities

14.1 Introduction

14.2 Branch 0xDA “identification”

14.3 Branch 0x07 “basic attributes”

14.4 Branch 0xDB “extended attributes”

14.4.1 ONU management

14.4.2 Bridging

14.4.3 Statistics and counters

14.4.4 Alarms

14.4.5 Encryption

14.4.5.1 Attribute *aInitialKeyMethods* (0xDB/0x04-01)

This attribute represents the list of key establishment methods (KEM) supported by the given ONU. Each KEM is identified by a 16-bit KEM ID value There could be various organizations providing their own KEM definitions and KEM ID enumerations.

The *aInitialKeyMethods* attribute consists of the following sub-attributes: *sKemCount*, *sKemId[sKemCount]*, and *sKemDomainId[sKemCount]*.

Sub-attribute *aInitialKeyMethods.sKemCount*:

Syntax:	Unsigned integer
Range:	0x02 to 0xFF
Remote access:	Read-Only
Description:	This sub-attribute represents the number of KEMs supported by the ONU.

Sub-attribute *aInitialKeyMethods.sKemDomainId[sKemCount]*:

Syntax: Enumeration
Remote access: Read-Only
Description: Each element of this array identifies the KEM domain, i.e., an organization that defines and maintains the KEM ID enumaration system. The following KEM domain ID values are defined:

`tls_groups`: indicates that the corresponding *sKemId[i]* is defined by the IANA *TLS Supported Groups* registry (see [IANA TLS Groups]) .

All other values are reserved for future use.

Sub-attribute *aInitialKeyMethods.sKemId[sKemCount]*:

Syntax:	Unsigned integer
Range:	0x00-00 to 0xFF-FF
Remote access:	Read-Only
Description:	Each element of this array identifies a KEM supported by the ONU. The *sKemId[i]* value is interpreted within the context of the KEM domain.

At a minimum, the ONU shall support the following KEMs (*sKemDomainId[i]* / *sKemId[i]*):

- **secp256r1**: (`tls_group` / 23)
- **x25519**: (`tls_group` / 29)

The ONU should support the following KEMs:

- **secp384r1**: (`tls_group` / 24)
- **x448**: (`tls_group` / 30)

The *aInitialKeyMethods* attribute is associated with the ONU object (see 14.2.1). The Variable Container TLV for the *aInitialKeyMethods* attribute shall be as specified in Table 14-xx.

Table 14-xx—*Initial Key Methods Mode* TLV (0xDB/0x04-01)

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-01	Leaf identifier
1	Length	1+3×*N*	The size of TLV fields following the `Length` field
1	KemCount	*N*	Value of the *sKemCount* sub-attribute
1	KemDomainId[0]	Varies	Value of the *sKemDomainId[0]* sub-attribute, encoded as follows: `tls_groups`: 0x01
2	KemId[0]	Varies	Value of the *sKemId[0]* sub-attribute
…	…	…	…
1	KemDomainId[*N*-1]	Varies	Value of the *sKemDomainId[N-1]* sub-attribute. (See *sKemDomainId[0]* for encoding.)
2	KemId[*N*-1]	Varies	Value of the *sKemId[N-1]* sub-attribute

14.4.5.2 Attribute *aInitialKeyParameters* (0xDB/0x04-02)

14.4.5.3 Attribute *aEncryptionMode* (0xDB/0x04-03)