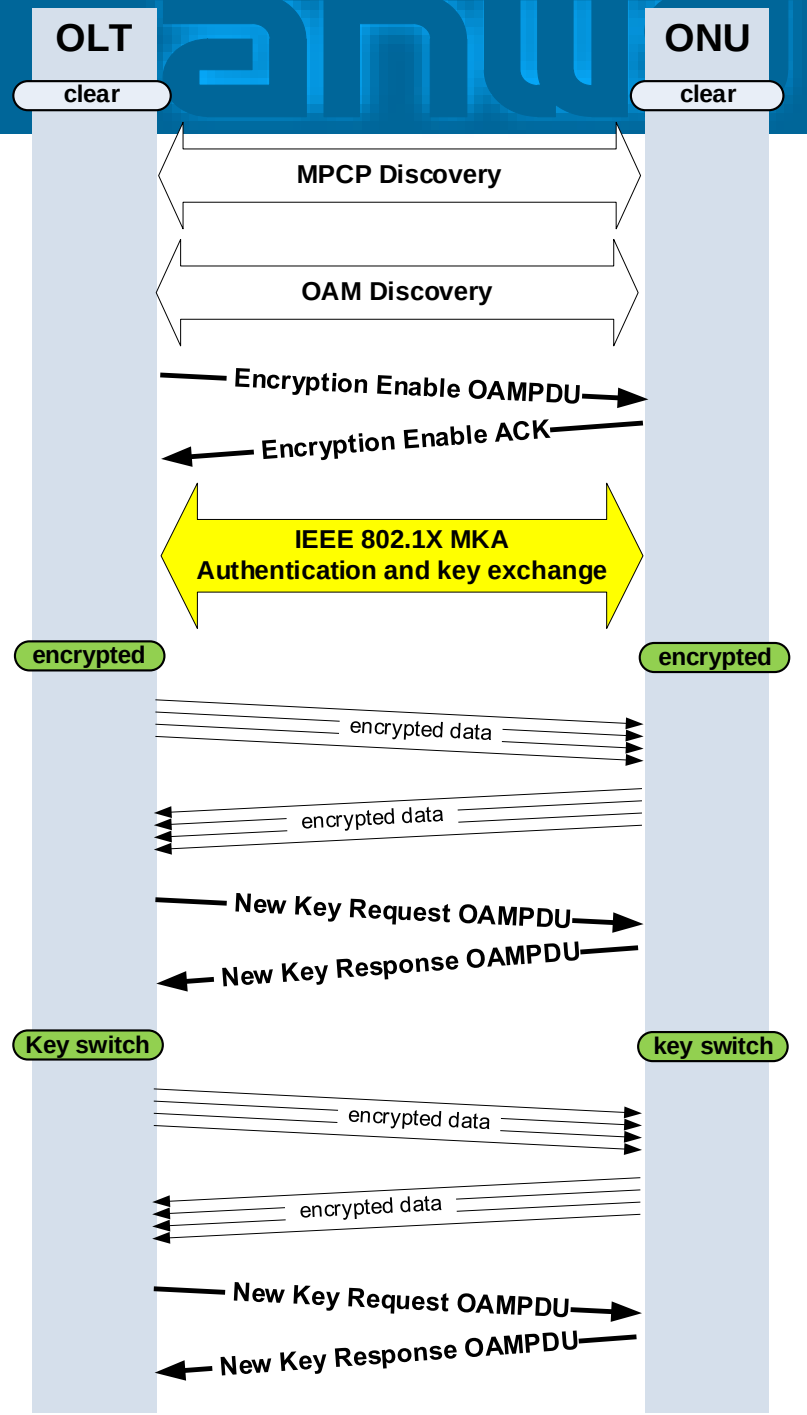
Key Exchange Protocol

Glen Kramer, Broadcom

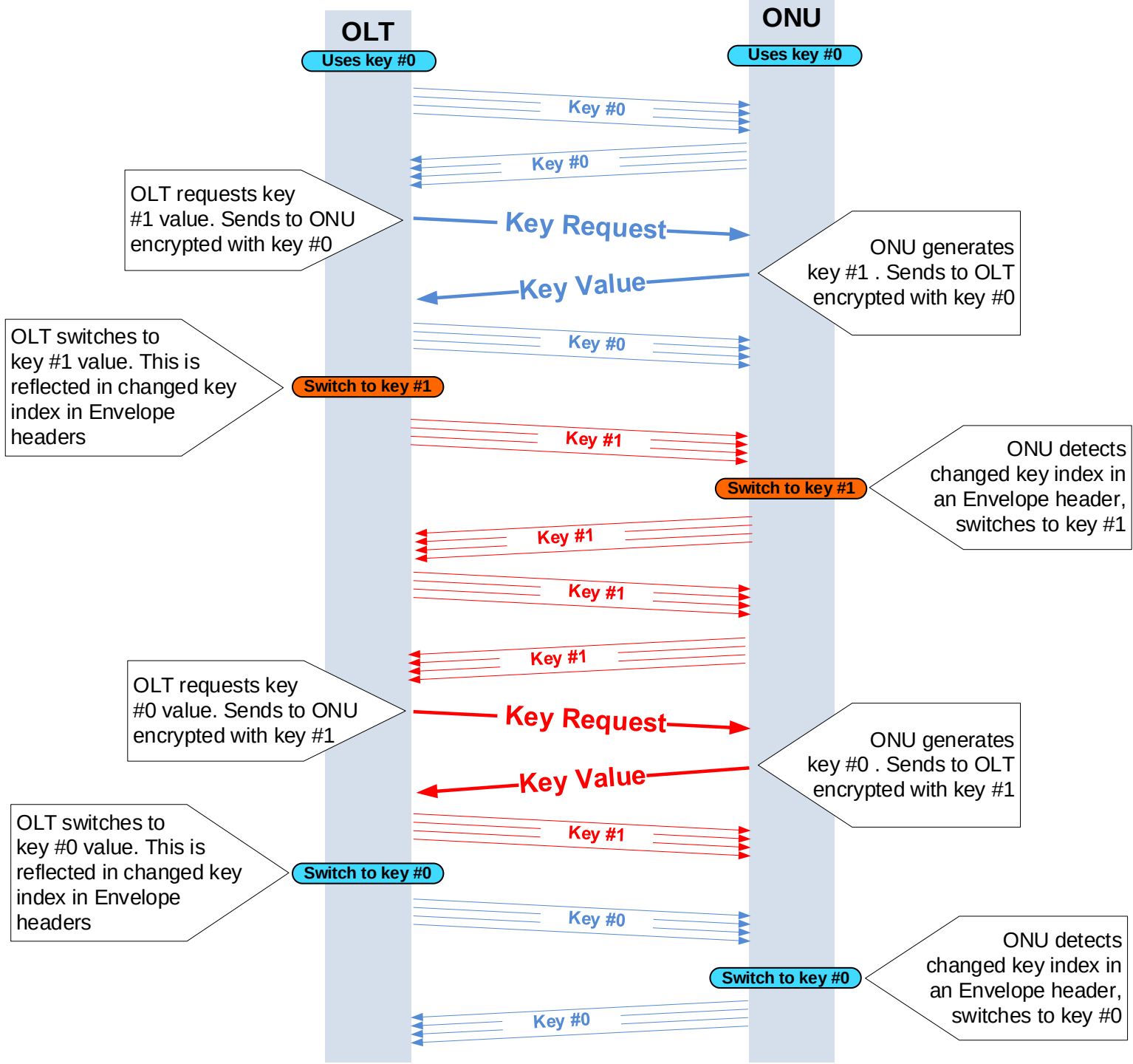
Encryption Initialization protocol

- The OLT and an ONU perform MPCP and OAM discovery.
  - At this time, only PLID and MLID are provisioned in the ONU
  - MPCP and OAM discovery is performed in the clear.
- OLT issues unicast *Encryption Enable* OAMPDU to enable encryption.
  - The OAMPDU includes Enable/Disable flag, 48-bit extended MPCP time, Key timeout interval
  - ONU synchronizes 48-bit MPCP time, sends ACK OAMPDU.
- OLT and ONU initiate MKA exchange to authenticate the ONU and perform the initial key negotiation.
- Once the key is exchanged, the PLID and MLID begin to carry encrypted traffic.
- At this time, the NMS may provision additional LLIDs (unicast and multicast ULIDs) using the encrypted MLID channel.
- All subsequent key exchanges are performed using New Key Request / New Key Response OAMPDUs



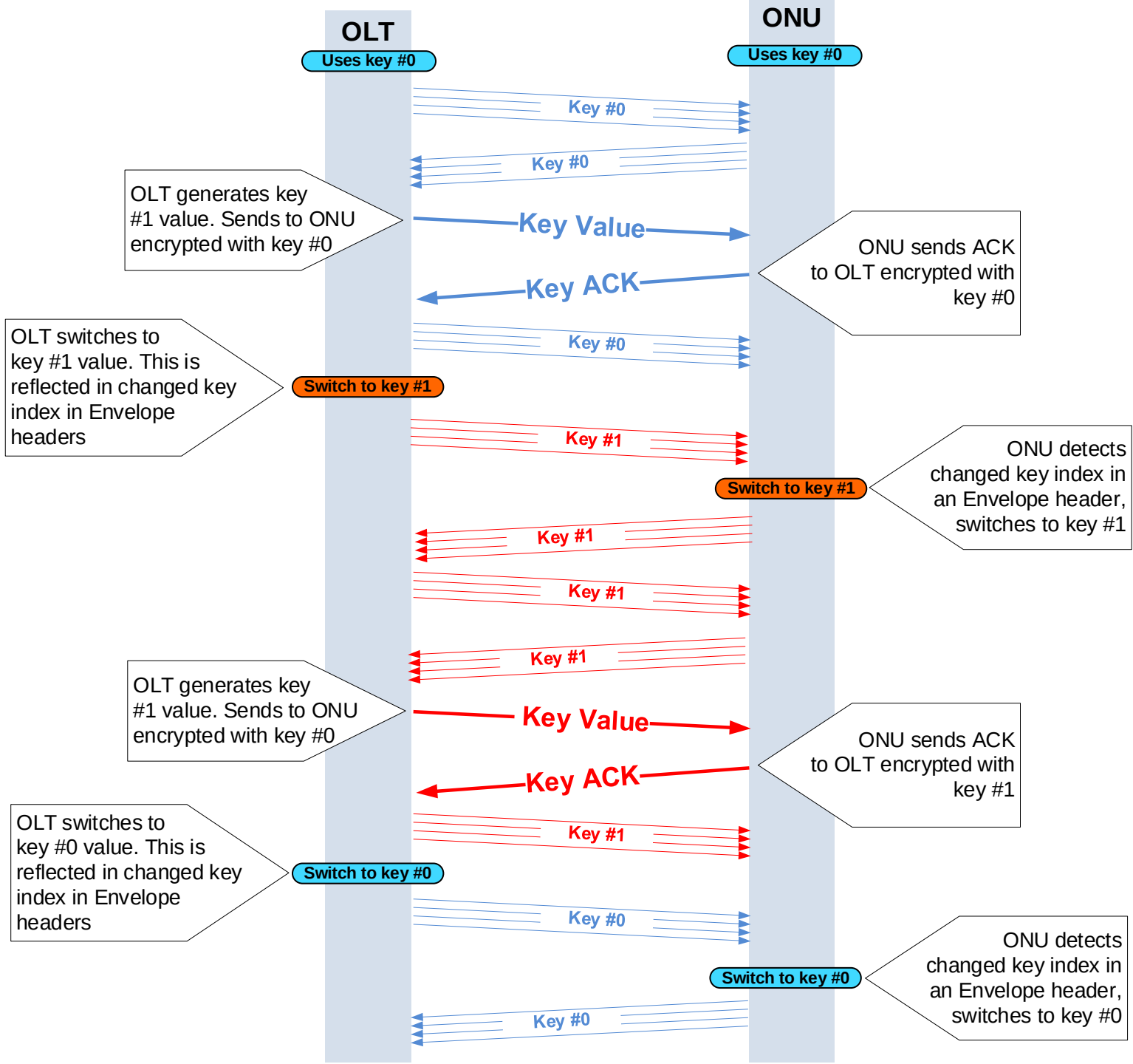
Key generated by ONU

- OLT requests new key from the ONU
- ONU generates a new key and sends it to the OLT, but does not switch to the new key yet
- OLT receives a new key and sometime later switches the downstream traffic to new key. OLT still uses the old key in the upstream.
- ONU detects the new key in the downstream and switches to the new key for the upstream.



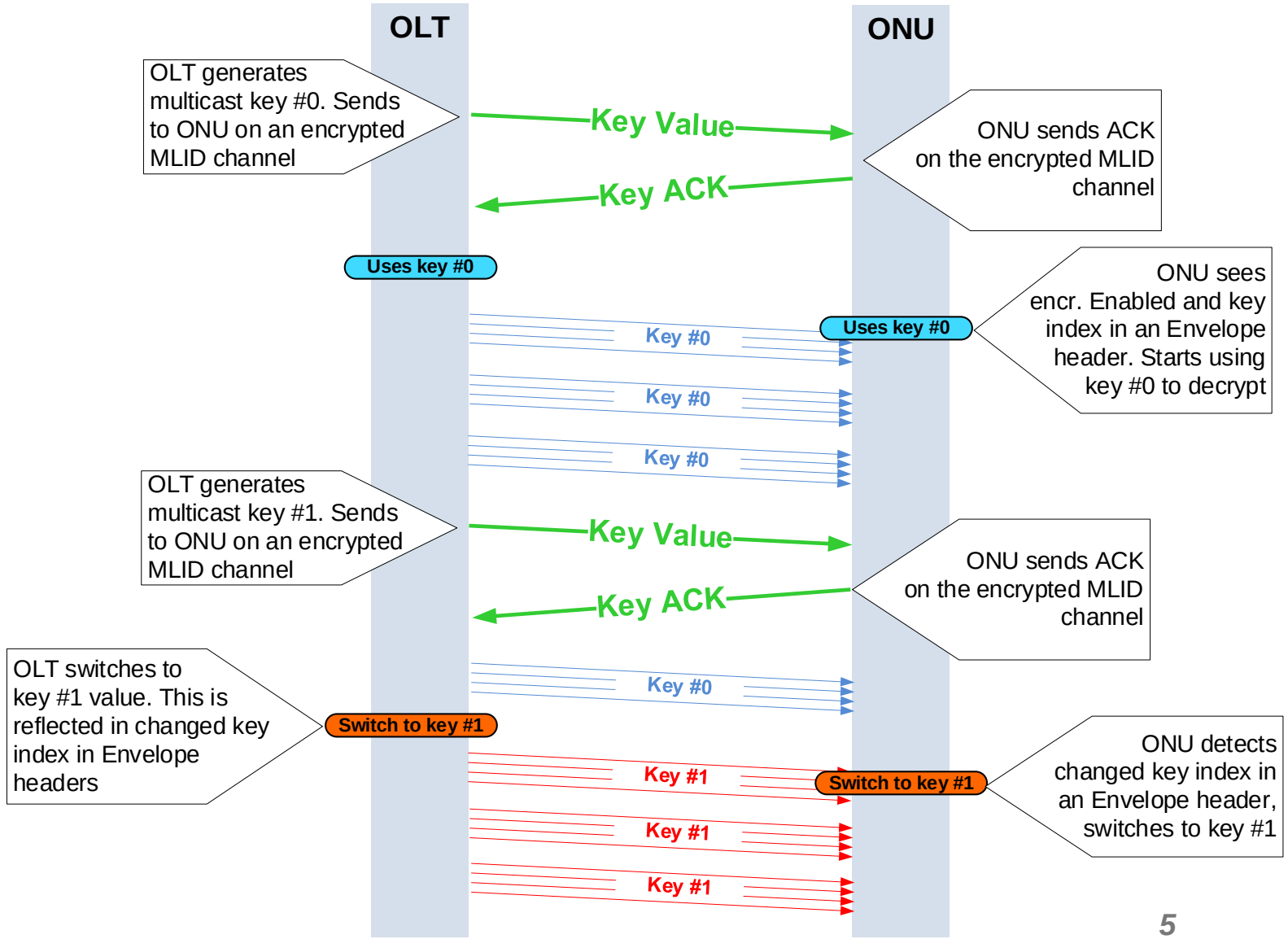
Key generated by OLT

- OLT requests new key from the ONU
- ONU generates a new key and sends it to the OLT, but does not switch to the new key yet
- OLT receives a new key and sometime later switches the downstream traffic to new key. OLT still uses the old key in the upstream.
- ONU detects the new key in the downstream and switches to the new key for the upstream.



Multicast LLID encryption

- NMS (multicast server) generates an encryption key for each multicast group
- Encryption key is delivered to each member of the group via previously encrypted MLID channel.
- Each ONU stores the next key, but doesn't activate it.
- All ONUs in a group switch to the next key when thy detect changed key index in the headers of the received multicast LLID envelopes



Key exchange messages and TLVs

- Currently, we have a special OAMPDU type (two sub-types) and two extended attributes dedicated to encryption

- **OAMPDUs:**
  - **eOAM_KeyExchange_Assign**
  - **eOAM_KeyExchange_ACK**

- **Attributes:**
  - ***aEncryptionKeyExpiration* (0xDB/0x04-01)**
  - ***aEncryptionMode* (0xDB/0x04-02)**

Table 13-10—eOAMPDUs and assignment of Opcode values

Opcode	eOAMPDUs	Defined in
0x01	*eOAM_Get_Request*	13.4.6.2
0x02	*eOAM_Get_Response*	13.4.6.3
0x03	*eOAM_Set_Request*	13.4.6.4
0x04	*eOAM_Set_Response*	13.4.6.5
0x08	*eOAM_KeyExchange*	13.4.6.7
0x09	*eOAM_Software*	13.4.6.6

Unclear what was the reason to allocate a special opcode to *eOAM_KeyExchange* OAMPDU instead of using a special attribute with regular *Set_Request/Set_Response* and *Get_Request/Get_Response* OAMPDUs

Attribute *aEncryptionKeyExpiration* (0xDB/0x04-01)

- What happens when this timer expires?
- Should ONU generate a new key and send it upstream to the OLT?
- Can the OLT drive this and request a new key from the ONU before the previous key expires?

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

This attribute represents the current value of the timeout for encryption keys used by the given L-ONU.

Attribute *aEncryptionKeyExpiration*:

Syntax:	Unsigned integer
Range:	0x00-00 to 0xFF-FF
Remote access:	Read/Write
Unit:	1 second
Default value:	0x00-00
Description:	This attribute indicates the duration of validity for the current encryption key used by the ONU.

The *aEncryptionKeyExpiration* attribute is associated with the LLID object (see 14.2.1). The Variable Container TLV for the *aEncryptionKeyExpiration* attribute shall be as specified in Table 14-158.

Table 14-158—*Encryption Key Expiry Time* TLV (0xDB/0x04-01)

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-01	Leaf identifier
1	Length	0x01 to 0x02	The size of TLV fields following the `Length` field
1..2	EncryptionKeyExpiration	Varies	Value of *aEncryptionKeyExpiration* attribute

Attribute *aEncryptionMode* (0xDB/0x04-02)

- This attribute selects an encryption mode
- Could there be different encryption modes in 1904.4?
- If encryption is enabled in an ONU, all unicast LLIDs in this ONU are encrypted in both directions.
- Multicast LLIDs are individually encrypted using a separate encryption enable / key assignment message

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

This attribute represents the current encryption mode configured on the given L-ONU. Individual encryption modes are defined in DPoE-SP-SEC.

Attribute *aEncryptionMode*:

Syntax: Enumeration
Default value: `none`
Remote access: Read/Write
Description: This attribute indicates the current encryption mode configured on the given L-ONU. The following values are defined:

- `none`: encryption is disabled.
- `1GD`: encryption is enabled; 1G-EPON downstream encryption is used.
- `10GD`: encryption is enabled; 10G-EPON downstream encryption is used.
- `10GB`: encryption is enabled; 10G-EPON bidirectional encryption is used.

The *aEncryptionMode* attribute is associated with the LLID object (see 14.2.1). The Variable Container TLV for the *aEncryptionMode* attribute shall be as specified in Table 14-159.

Table 14-159—*Encryption Mode* TLV (0xDB/0x04-02)

Size (octets)	Field (name)	Value	Notes
1	Branch	0xDB	Branch identifier
2	Leaf	0x04-02	Leaf identifier
1	Length	0x01	The size of TLV fields following the `Length` field
1	EncryptionMode	Varies	Value of *aEncryptionMode* attribute, defined as follows: `none`: 0x00 `1GD`: 0x01 `10GD`: 0x02 `10GB`: 0x03

Encryption-related messages/attributes

TLVs (messages) and their content if key is generated by the OLT
Encryption Config (Set_Request) 1) Encryption enabled/disabled 2) 48-bit extended MPCP clock
Key Assignment (Set_Request) 1) Next key index (1 bit) 2) Next key value (128 or 256 bits) Object context identifies target: multicast LLID or entire ONU for unicast key
Key Response (Set_Response) Regular *Return Code TLV*

- The *Key Assignment* message is used for both unicast and multicast key assignments
- All messages are exchanged only on the MLID channel

TLVs (messages) and their content if key is generated by the ONU
Encryption Config (Set_Request) 1) Encryption enabled/disabled 2) 48-bit extended MPCP clock 3) Key size: 128 or 256 bits
Key Request (Get_Request) Regular Variable Descriptor TLV
Key Response (Get_Response) 1) Next key index (1 bit) 2) Next key value (128 or 256 bits)
Multicast Key Assignment (Set_Request) 1) Next key index (1 bit) 2) Next key value (128 or 256 bits) Object context identifies the multicast LLID
Multicast Key Response (Set_Response) Regular *Return Code TLV*