Key Exchange Protocol (take 2)

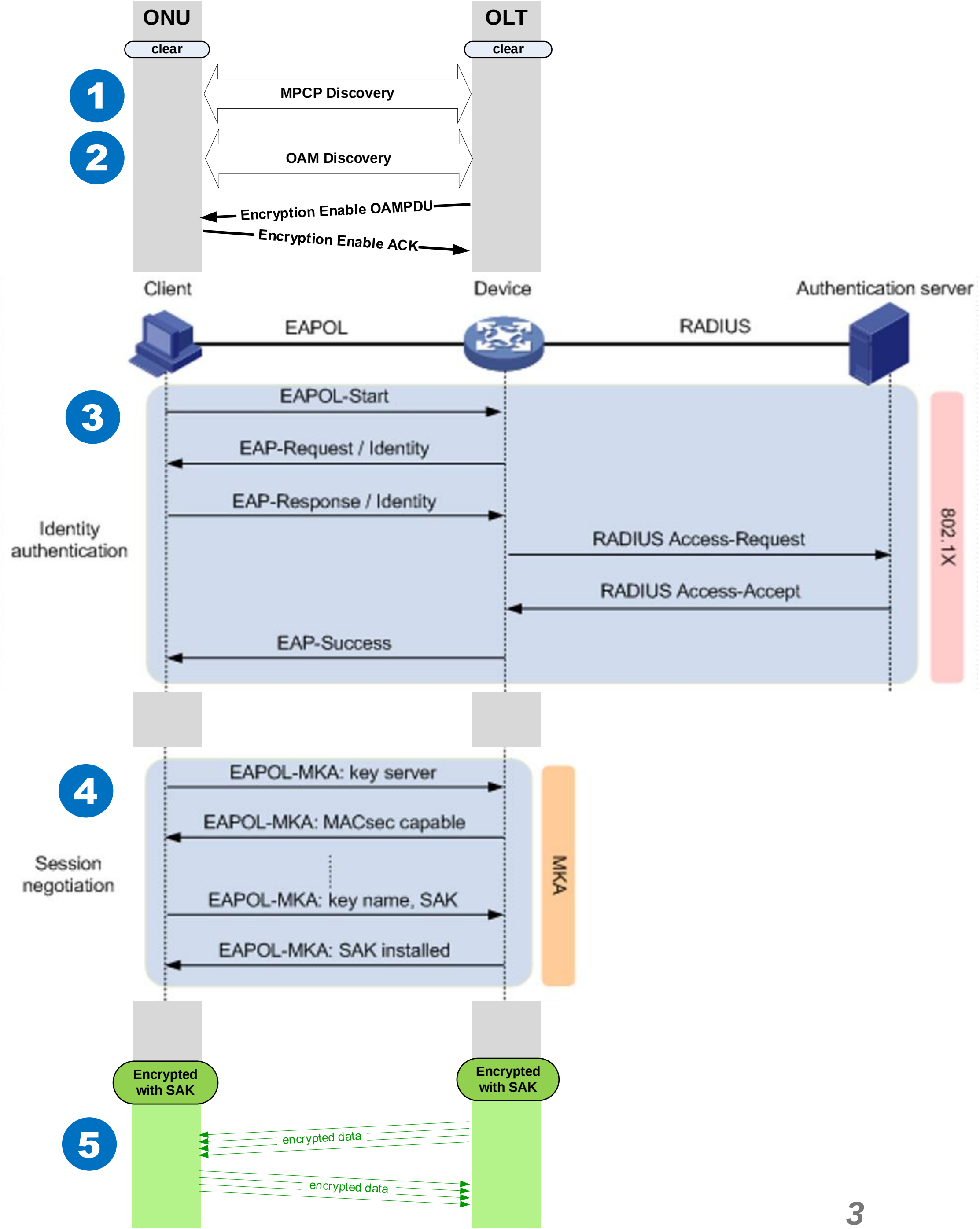
Glen Kramer, Broadcom

PON-specific encryption requirements

- Encryption is established only between the OLT and ONUs
  - Encryption is needed to protect each ONU’s traffic from being snooped by other ONUs (a problem created by broadcasting nature of PON medium)
  - Encryption must protect user traffic as well as PON control traffic between the OLT and ONUs (MPCPDUs, CCPDUs, OAMPDUs)
  - Generally, once encryption between the OLT and an ONU is stablished, it remains active until the ONU is reset/rebooted (i.e., months to years). Encryption sessions do not need to be re-negotiated every time a key is exchanged.
- Multicast groups must be encrypted to prevent non-members from snooping the multicast traffic
  - All ONU that are members of a given multicast group use the same encryption key. The key must be generated centrally (typically by the NMS or the OLT) and distributed to all member ONUs.
- Operators should be able to selectively enable/disable encryption per ONU or per multicast group for troubleshooting purposes

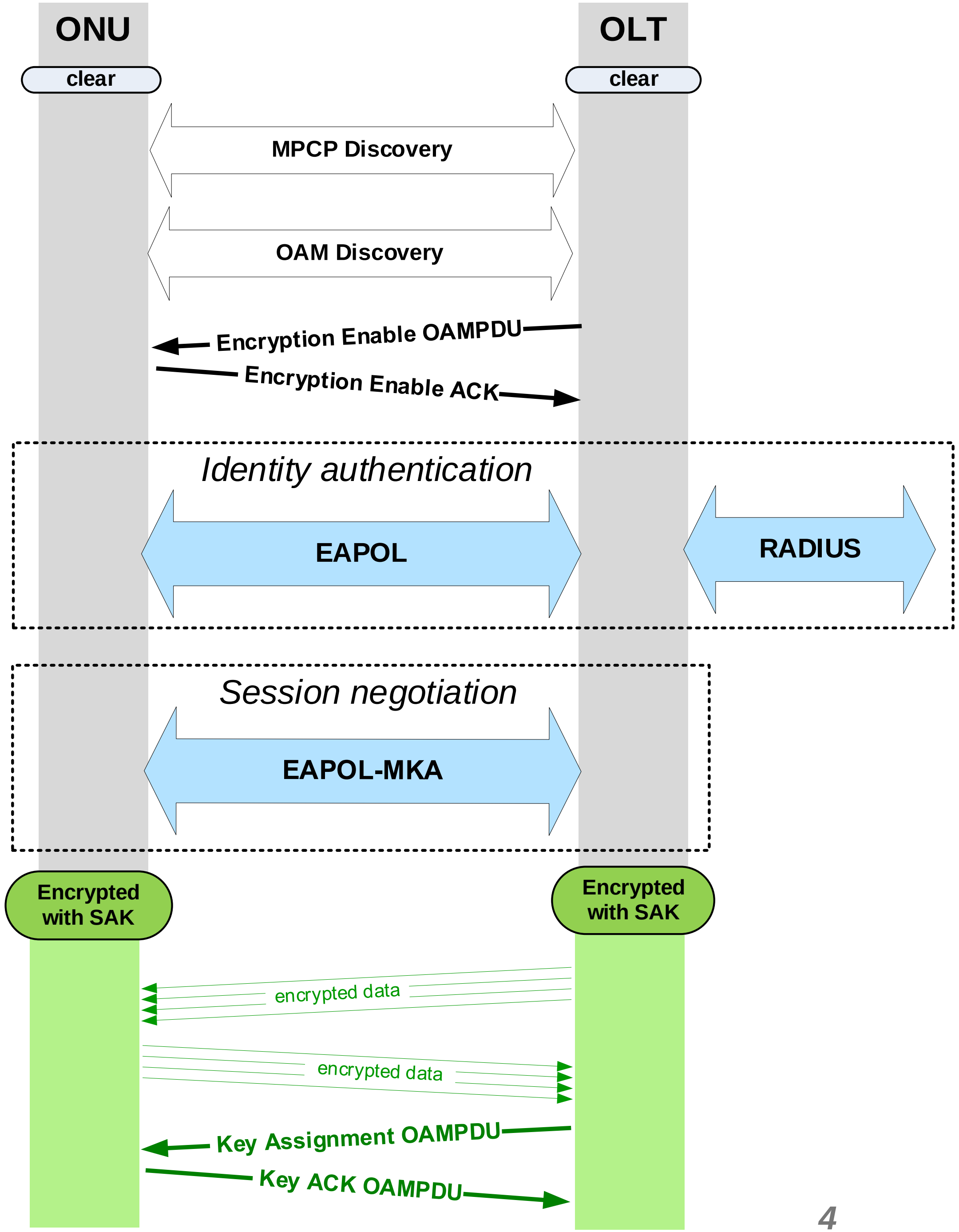
Encryption Initialization

1. 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.
2. 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.
3. OLT and ONU perform identity authentication using EAPOL/RADIUS
4. OLT and ONU perform session negotiation using EAPOL-MKA and exchange SAK
5. Once the SAK 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.



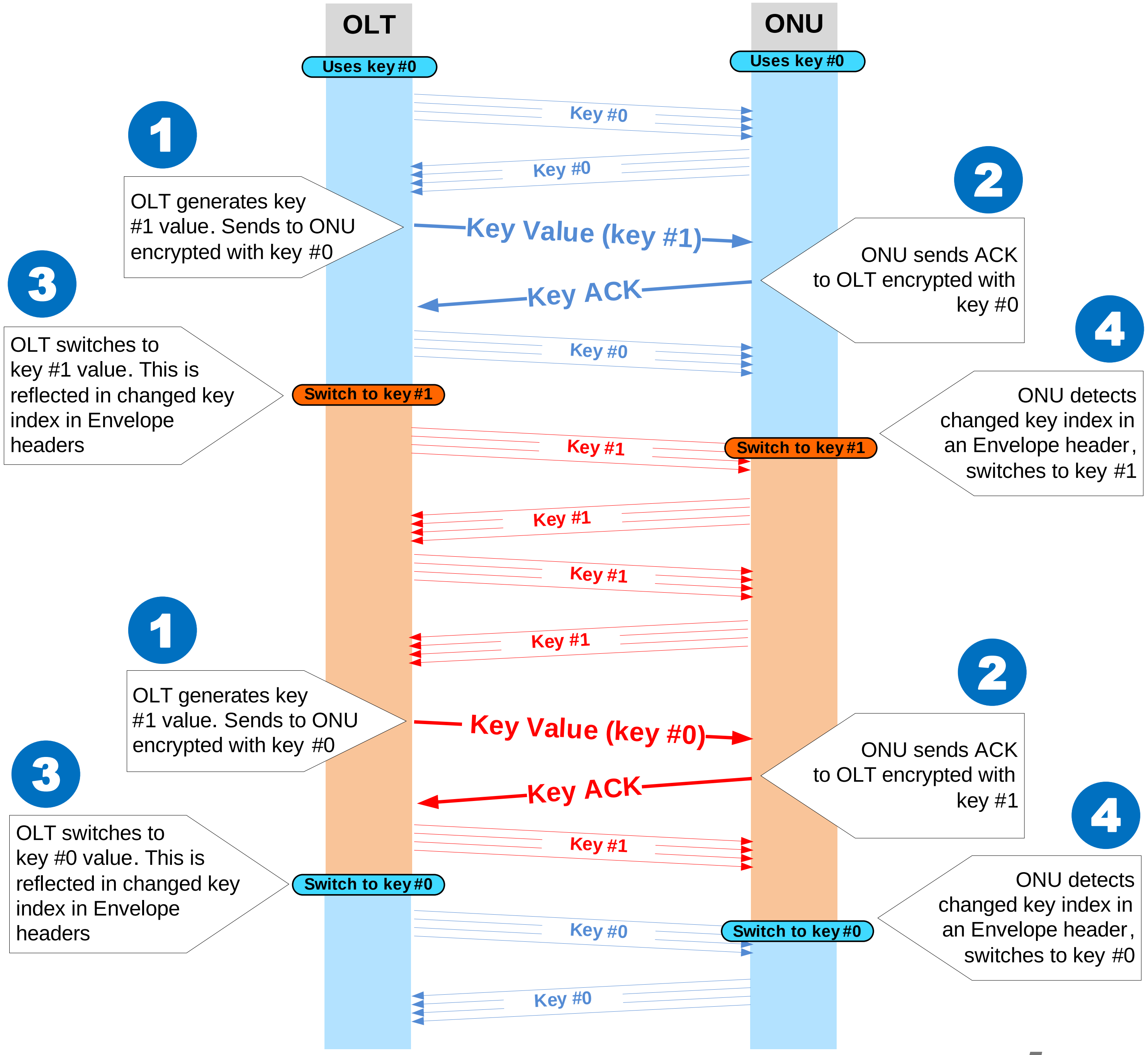
Subsequent key exchanges

- After the initial SAK exchange, the subsequent keys are generated by the NMS/OLT and delivered to ONUs using the ***Key Assignment*** OAMPDUs via their encrypted individual unicast MLID channels
- The key distribution mechanism is identical for the multicast and the unicast keys
- OLT maintains a key expiration timer and ensures that every ONU (a) receives a new key and (b) switches to the new key before its current key expires.
  - Probably enough to maintain a single key timer at the OLT and set the expiration time well in advance of the IV rollover time
  - All keys in all ONUs are updated when the key expiration timer times out.
  - An ONU that fails to accept a new key after a reasonable number of attempts is deregistered
- Example:
  - With 48-bit MPCP clock, the IV rollover period is ~200 hours
  - OLT key expiration timer can be set to 168 hours (one week).



Key assigned by OLT

1. Upon key timer expiration, the OLT generates a new key for every ONU and every multicast group.
   - This process can be paced to take several hours.
   - The new keys are sent in MLID channels encrypted using their currently-active keys.
2. ONUs acknowledge new unicast and multicast keys
3. After OLT receives an ACK from an ONU, it may start encryption unicast traffic to this ONU using the new key value.
   - New key activates synchronously with transmitting an envelope header. The key index in the envelope header is updated.
4. ONU detects the key switchover event by observing the change in key index value in the received envelope header.
   - ONU immediately switches to the new key value in order to decrypt the incoming data.



OLT generates key #1 value. Sends to ONU encrypted with key #0

ONU sends ACK to OLT encrypted with key #0

OLT switches to key #1 value. This is reflected in changed key index in Envelope headers

ONU detects changed key index in an Envelope header, switches to key #1

OLT generates key #1 value. Sends to ONU encrypted with key #0

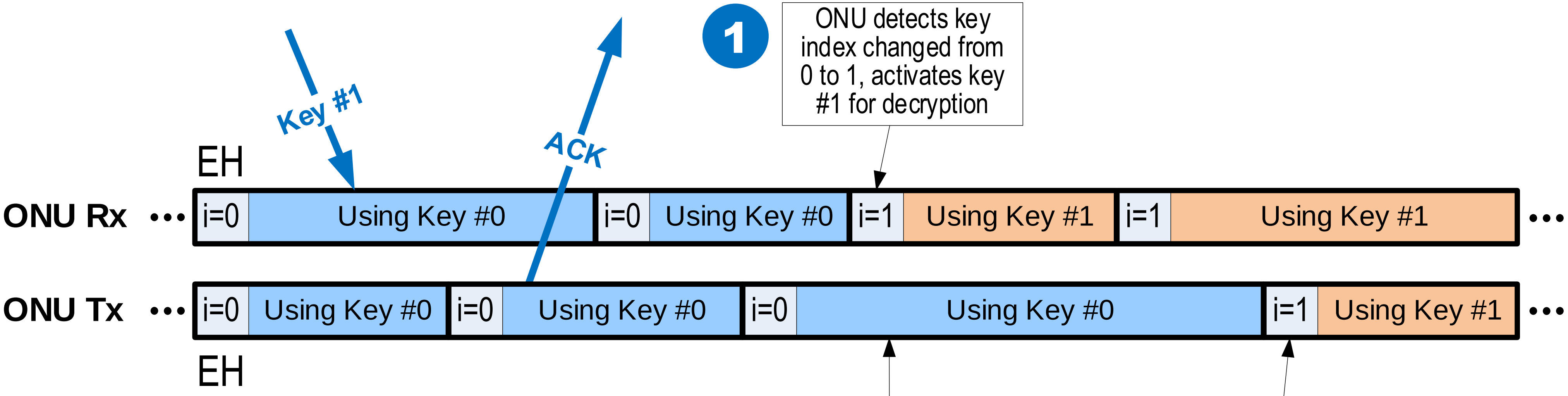
ONU sends ACK to OLT encrypted with key #1

OLT switches to key #0 value. This is reflected in changed key index in Envelope headers

ONU detects changed key index in an Envelope header, switches to key #0

Key switchover at the ONU

1. ONU detects the key switchover event by observing the change in key index value in the received envelope header.
   - ONU immediately switches to the new key value in order to decrypt the incoming data.
2. ONU keeps using the previous key for the encryption of the outgoing data until the end of the current envelope.
3. At the beginning of the next envelope, ONU switches to the new key and indicates this by updating the key index value in the outgoing envelope header.



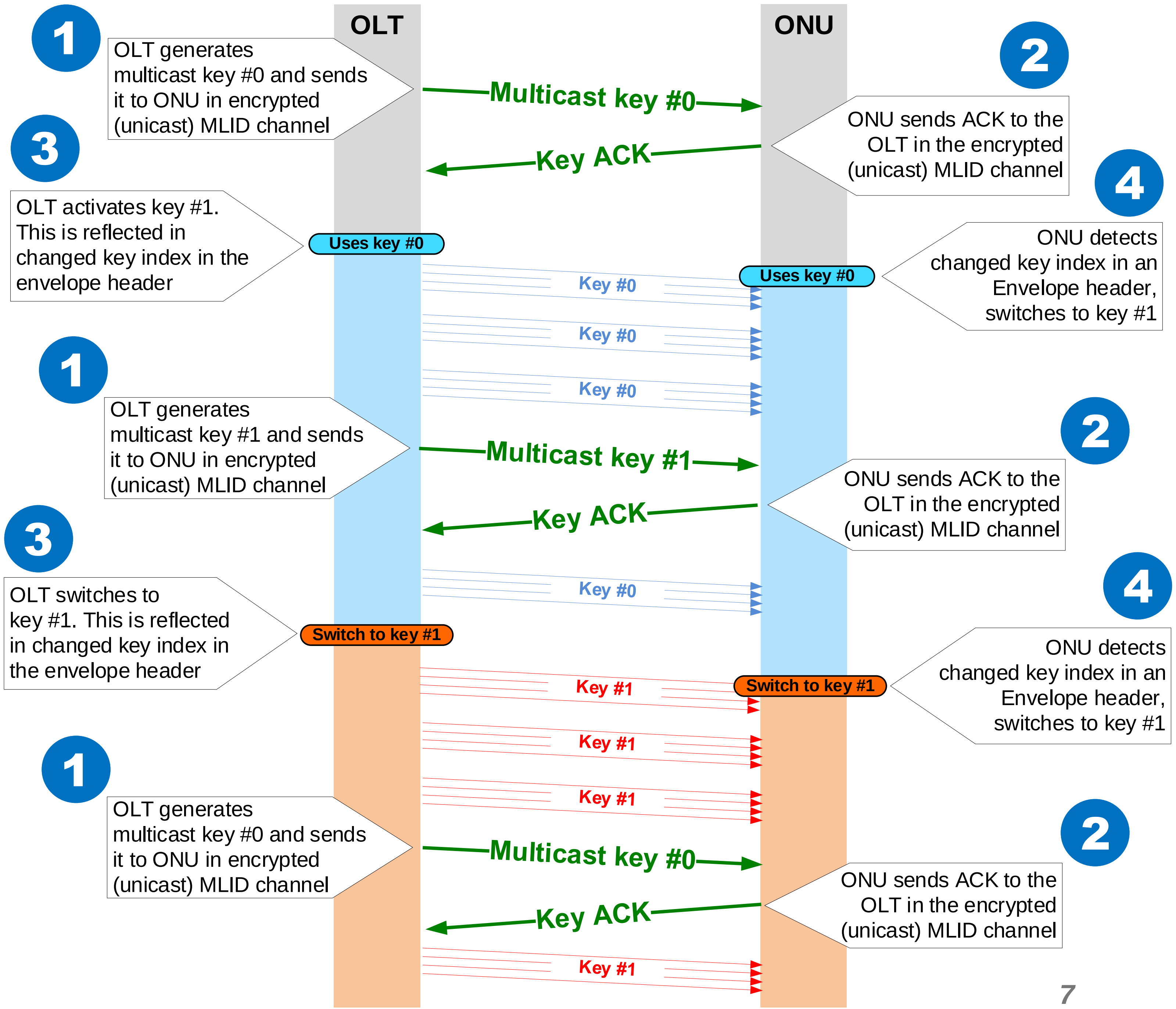
1 ONU detects key index changed from 0 to 1, activates key #1 for decryption

2 ONU continues using key #0 for encryption until the end of the current envelope

3 In the next envelope header, ONU changes key index from 0 to 1 and starts encrypting data with key #1

Multicast encryption

1. OLT or NMS (multicast server) generates an encryption key for each multicast group
2. Encryption key is delivered to each member of the group via previously encrypted MLID channels.
   - Each ONU stores the next key, but doesn't activate it.
3. OLT switches to the new key after it received ACKs <u>from all member ONUs</u>
4. All ONUs in a group switch to the next key when they detect changed key index in the headers of the received multicast LLID envelopes



OLT generates multicast key #0 and sends it to ONU in encrypted (unicast) MLID channel

ONU sends ACK to the OLT in the encrypted (unicast) MLID channel

OLT activates key #1. This is reflected in changed key index in the envelope header

ONU detects changed key index in an Envelope header, switches to key #1

OLT generates multicast key #1 and sends it to ONU in encrypted (unicast) MLID channel

ONU sends ACK to the OLT in the encrypted (unicast) MLID channel

OLT switches to key #1. This is reflected in changed key index in the envelope header

ONU detects changed key index in an Envelope header, switches to key #1

OLT generates multicast key #0 and sends it to ONU in encrypted (unicast) MLID channel

ONU sends ACK to the OLT in the encrypted (unicast) MLID channel

Encryption Configuration TLV

Context = ONU

Field size	Field value	Field description
1	0xDA	Identification branch
2	0x00-00	Object is ONU
1	1	Length
1	0	Instance (fixed)

Encryption Configuration TLV

Field size	Field value	Field description
1	0xDB	Extended Attributes branch
2	0x04-02	TLV Leaf value
1	7	Length
1	 0x00 0x10 0x20	Encryption Mode → None → AES-128 → AES-256
6	Various	48-bit value of extended MPCP clock at the time of this TLV/OAMPDU generation

- *Encryption Configuration* TLV replaces the *Encryption Mode* TLV (0xDB/0x04-02)

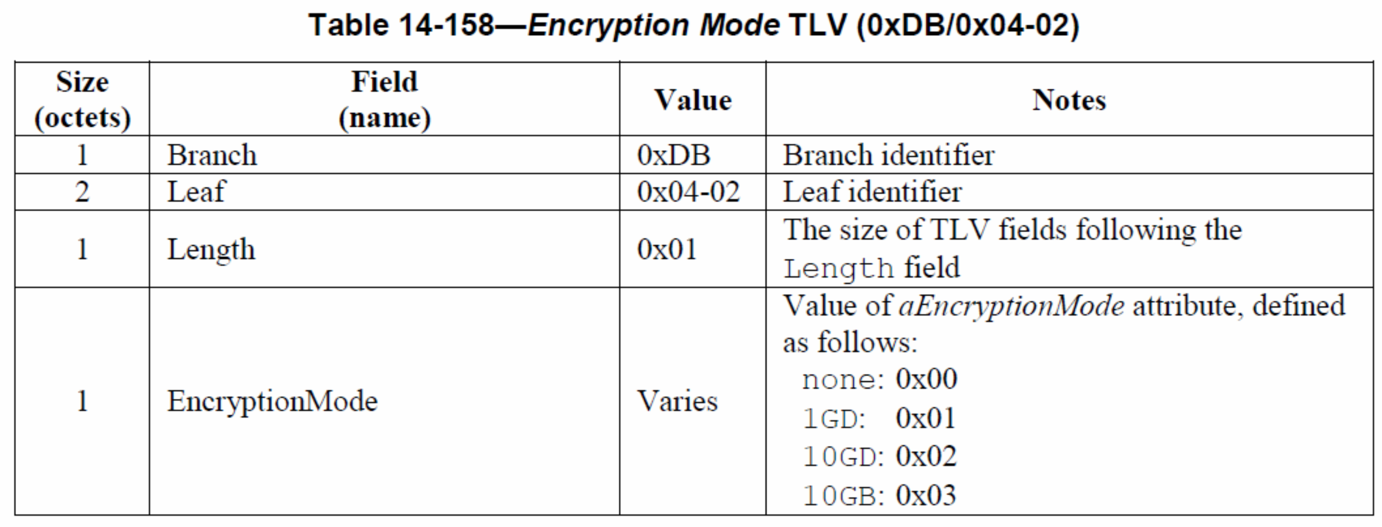


Table 14-158—*Encryption Mode* TLV (0xDB/0x04-02)

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

Key Assignment TLV

Context = ONU

Field size	Field value	Field description
1	0xDA	Identification branch
2	0x00-00	Object is ONU
1	1	Length
1	0	Instance (fixed)

Context = LLID

Field size	Field value	Field description
1	0xDA	Identification branch
2	0x00-02	Object is LLID
1	2	Length
2	Various	LLID value

One of these

followed by

one of these

Key Value TLV (128-bit key)

Field size	Field value	Field description
1	0xDB	Extended Attributes branch
2	0x04-03	TLV Leaf value
1	17	Length
1	0 or 1	Key Index (only bit 0 is used)
16	Various	Key Value

Key Value TLV (256-bit key)

Field size	Field value	Field description
1	0xDB	Extended Attributes branch
2	0x04-03	TLV Leaf value
1	33	Length
1	0 or 1	Key Index (only bit 0 is used)
32	Various	Key Value

- ❑ One *SetRequest* OAMPDU can assign multiple keys i.e., an OAMPDU can carry multiple *Key Value* TLVs, each under a different context object.
- ❑ When Context = LLID, the LLID value shall represent a unidirectional LLID provisioned in a target ONU. Otherwise, the ONU shall return the error 0xA5 (Invalid Context Object).

Discussion questions: Capability

1. Should ONUs mandatorily support both 128-bit and 256-bit keys or supporting only one size is ok?

2. If all ONUs support both 128-bit and 256-bit keys, shall all ONUs with encryption enabled always be configured to use the same key size? Or should the OLT support different key sizes for different ONUs?

Discussion questions: Operation (1/2)

1. Should we allow any ONU to operate with encryption disabled?
   a) Never
   b) Yes, but only temporarily for troubleshooting
   c) Yes, permanently

2. After a new ONU completed the MPCP Discovery/Registration and the OAM Discovery, how does it know whether it should start or not the EAP/Radius authentication and MKA key exchange?

3. Should we have an explicit message to enable or disable encryption per ONU?

4. Should each ONU support a mix of encrypted and unencrypted LLIDs?
   - Each envelope header contains 'Encryption enabled' bit. This makes it possible for ONUs to send a receive a mix of encrypted and unencrypted envelopes.

   a) ONU can detect 'Encryption enabled' bit in the incoming envelope headers for a given LLID and use the same mode for the transmission of this LLID.
   b) Alternatively, we can define a TLV to enable/disable encryption per LLID.

Discussion questions: Operation (2/2)

1. In PON, the OLT generally controls the key lifetime and is responsible for timely key renewals

2. Does the ONU also need to keep track of key expiration?

3. If ONU thinks the key has expired, but no new key was received from the OLT and the OLT continues to encrypt the data with the expired key, what shall ONU do?
   a) Follow the OLT lead and continue using the same expired key?
   b) Disable the encryption and start sending in the clear?
   c) Stop all transmissions and deregister?

4. Before the current key expires, the OLT delivers the next key. Can the next key be delivered encrypted using the current key or do we need double encryption just for the key value itself?
   a) What should be the lifetime of the Key Encryption Key (KEK)?
   b) How is KEK negotiated?
   c) How does the double encryption work?

Discussion questions: Multicast

1. A multicast flow shall either be sent in the clear, or else all member ONUs shall support the same key size <u>and have encryption enabled</u>.
   - If an ONU with encryption disabled joins an encrypted multicast group, it needs to receive the Key Assignment TLV with the multicast key. But it can only receive it over the unencrypted MLID channel, which will compromise the multicast key.

Thank you