11 Security-oriented mechanisms

11.6 Session key activation protocol

11.6.1 Protocol overview

The key activation protocol defines a procedure of switching from the current encryption key to a new encryption key that has been previously distributed by the OLT to one or more ONUs using the session key distribution protocol (see 11.5).

The key activation protocol relies on encryption signaling fields embedded in envelope headers. These fields include the encryption enabled flag (*EncEnabled* field) and encryption key index (*EncKey* field). The *EncEnabled* and *EncKey* fields are described in IEEE Std 802.3, 143.3.2 and 143.3.3.4. The *EncKey* field takes on values of only 0 and 1.

11.6.1.1 Activation of a unicast (bidirectional) key

The unicast (bidirectional) key activation procedure consists of four sequential steps, as illustrated in Figure 11-10 ~~illustrates the procedure of a key activation, which consists of four sequential steps~~.

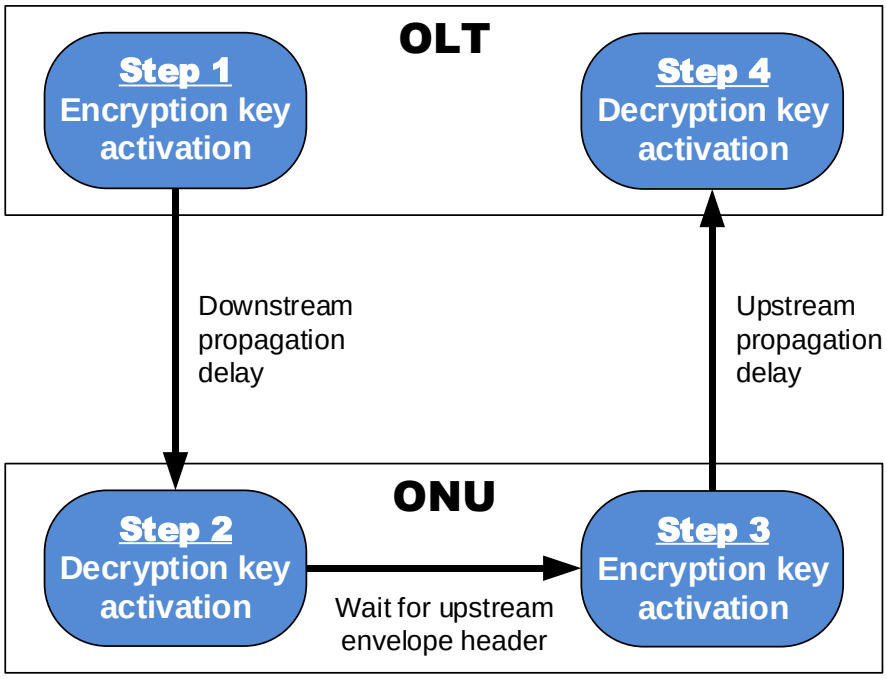

Figure 11-10–Four steps comprising the key activation procedure

Each of the above four steps is represented by an independent process that runs continuously within the secure Multi-Channel Reconciliation Sublayer (MCRS $_{SEC}$).

Step 1 ~~:~~ Encryption key activation at the OLT:

The process of encryption key activation at the OLT is defined in 11.6.2.4. The OLT activates the new encryption key upon the expiration of the key activation timer.

Generally, every encryption entity (i.e., ONUs and multicast LLIDs) maintains its own key activation timer and these timers may have different intervals and/or be set to expire at different

times. However, for practical considerations, it is allowed for all encryption entities to share the same key activation timer.

Once the key activation timer expired, the OLT waits for the next envelope header destined to the given encryption entity. The OLT indicates switching to the new key by toggling the value of the *EncKey* field in the envelope header. The envelope payload following this envelope header is encrypted using the new key.

Step 2 — : Decryption key activation at the ONU:

The process of decryption key activation at the ONU is defined in 11.6.2.5. For every received envelope, the ONU retrieves a key associated with the given encryption entity, identified by the LLID field in the envelope header, and the key index, identified by the *EncKey* field. Thus, toggling of the *EncKey* value by the OLT in Step 1 above caused the ONU to also retrieve the new key after it parsed and processed this envelope header.

Step 3 : — Encryption key activation at the ONU:

The process of encryption key activation at the ONU is defined in 11.6.2.6. ONU's activation of a new decryption key in Step 2 also serves as a trigger for activating the same key for the encryption of its upstream transmission. The ONU waits for the next envelope header from to the given encryption entity. The ONU indicates switching to the new key by toggling the value of the *EncKey* field in the envelope header. The payload following this envelope header is encrypted using the new key.

Step 4 : — Decryption key activation at the OLT:

The process of the decryption key activation at the OLT is identical to that process at the ONU, and is, in fact, described by the same state diagram (see 11.6.2.5). For every received envelope, the OLT retrieves a key associated with the given encryption entity, identified by the LLID field, and the key index, identified by the *EncKey* field. Thus, toggling of the *EncKey* value by the ONU in Step 3 above caused the OLT to also retrieve the new key after it parsed and processed this envelope header.

Optionally, the OLT may implement additional safety check of comparing that the retrieved decryption key matches the previously used encryption key. If implemented, such check shall be performed not earlier than a round-trip time after the activation of the new encryption key in step 1.

11.6.1.2 Activation of a mMulticast (unidirectional) key activation

The activation of the a multicast (unidirectional) key, i.e., the a key associated with a multicast LLIDs, involves only step 1 (see 11.6.1.1) and step 2 (see 11.6.1.1) because the multicast LLIDs carry traffic only in the downstream direction.

The activation of the encryption key by the OLT, as signaled by toggling of the *EncKey* field in the downstream envelope header, is detected by all ONUs that are members of the given multicast group. This causes all member ONUs to activate the new key for the decryption.

11.6.1.3 Location of key activation processes

The encryption and decryption key activation processes are located within the secure MCRS (MCRS $_{SEC}$) sublayer, as detailed in 11.2.2.

11.6.2 Definition of processes comprising the key activation protocol

<11.6.2 remains as is>