#1 Type: TR TF: TF4 Clause: 11.2.3 Page: 193 Line: 7 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

The Encryption and Decryption functions operate on units of Eqs. However, Figures 11-2 and 11-3 and the associated text all talk about control characters, which are octets, according to 802.3, 142.2.1). Also, there is local text that would serve as a better cross-reference than pointing back to 802.3.

Modify the text and figures in 11.2.3 and 11.2.4 as shown in tf4_2312_kramer_block_diagrams_1_diff.pdf.

-

#16 Type: E TF: TF4 Clause: 11.2.6 Page: 199 Line: 3 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

Various lists in D1.6 use different format.

Apply the format similar to that shown in tf4_2312_kramer_key_activation_8_clean.pdf to the list of 6 steps on pages 199-200.

-

#3 Type: E TF: TF4 Clause: 11.3 Page: 201 Line: 18 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

Grammar

Add "a" before "compliant"

-

#17 Type: TR TF: TF4 Clause: 11.3 Page: 201 Line: 34 Commenter: Craig Pratt / CableLabs

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

Split up text into subsections 11.3.1-11.3.3

-

-

#18 Type: TR TF: TF4 Clause: 11.3 Page: 201 Line: 34 Commenter: Craig Pratt / CableLabs

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

Added section 11.3.4 - Symmetric key derivation using HKDF. This specifies how the symmetric key is derived from the DHE shared secret.

-

-

#4 Type: T TF: TF4 Clause: 11.5.1 Page: 206 Line: 28 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

The first DHE key negotiated between the OLT and ONU is called the "Initial key" everywhere in the draft. But in one place it is still called SAK (Security Association Key). This 802.1x term is not applicable here.

Replace "After the initial SAK exchange …" with "After the initial key exchange…" Remove SAK entry from 3.2 Acronyms and Abbreviations Discuss if a better name can be used for the initial key. If yes, replace it throughout the drat.

-

#2 Type: E TF: TF4 Clause: 11.5.1 Page: 207 Line: 1 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

Hashed pattern in Figure 11-9 does not transfer into pdf well. Also, the distinction between using key 0 and using key 1 relies on color (green, blue). This distinction will be lost when the figure is viewed in B&W.

Replace the figure 11-9 with the one shown in the attached tf4_2312_kramer_key_distrib_fig_2.pdf

-

#15 Type: T TF: TF4 Clause: 11.6.1 Page: 209 Line: 13 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

Sub-clause 11.6.1 needs to better differentiate activation of bidirectional (unicast) key from the activation of a unidirectional (multicast) key. There is no need to break individual steps of the key activation procedure into individual sub-clauses.

Apply changes to the sub-clause 11.6.1 as shown in tf4_2312_kramer_key_activation_8_diff.pdf

-

#6 Type: T TF: TF4 Clause: 11.6.2.2 Page: 213 Line: 18 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

Cross-reference is TBD. D1.6 now has a corresponding sub-clause

Change TBD to 11.7.4.2. Make the link live.

-

#7 Type: T TF: TF4 Clause: 11.7.3 Page: 218 Line: 17 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

"This mask is AND-ed with the output of the AES block cipher, resulting in the unencrypted control characters being placed in the plaintext blocks." The description is not very precise. It needs to be explained that the control characters are received unencrypted, therefore no need for decryption.

Replace "...resulting in the unencrypted control characters being placed in the plaintext blocks." with "…resulting in the unencrypted control characters being transfered from the ciphertext blocks into the plaintext blocks."

-

#8 Type: TR TF: TF4 Clause: 11.7.4 Page: 219 Line: 4 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

"To encrypt a message, the IV is calculated by the encryption key activation processes at the OLT (see 3 Figure 11-11) and at the ONU (see Figure 11-13) when an Envelope Start Header (ESH) is observed in the 4 transmit path of the MCRSSEC sublayer." The IV is calculated whenever either ESH or the ECH is observed. The text implies that only ESH causes the IV calculation.

On line 4 and on line 7, replace "…when an Envelope Start Header (ESH) is observed…" with "… when an envelope header (ESH or ECH) is observed …"

-

#12 Type: TR TF: TF4 Clause: 11.7.4.1 Page: 220 Line: 26 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

"Because the OLT CipherClock and the ONU TxCipherClock extend their respective MPCP clocks, they preserve their relative shift, ensuring that the MessageTime value used to construct the IV for the encryption at the OLT matches the MessageTime value used to construct the IV for the decryption at the ONU." The above sentence referes to the upstream transmission, which means ONU does the encryption and the OLT does the decryption. But the last part of the sentence says "...encryption at the OLT ...<and> ... decryption at the ONU."

Swap "OLT" and "ONU" at the end of the sentence. The correcter sentence reads: "Because the OLT CipherClock and the ONU TxCipherClock extend their respective MPCP clocks, they preserve their relative shift, ensuring that the MessageTime value used to con

-

#14 Type: TR TF: TF4 Clause: 11.7.4.1.3 Page: 221 Line: 32 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

The contents of the sub-clause 11.7.4.1.3 Initial cipher clock synchronization are missing

Add the sub-clause text as shown in tf4_2312_kramer_cipher_clock_sync_6.pdf. The described cipher clock synchronization procedure requires a new eOAM action. Add the action shown in tf4_2312_kramer_cipher_clock_action_7.pdf as a new sub-clause 14.6.5.2

-

#10 Type: TR TF: TF4 Clause: 13.3.1 Page: 233 Line: 1 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

Figure 3-1 is highlighted as needing an update. This figure references the MPCP Discovery and Registration processes associated with 1G-EPON and 10G-EPON. Also the figure shows OAM discovery and eOAM discovery as one combined procedure, contradicting the text in 13.3.2.3, which states: "The OLT starts the eOAM discovery process immediately after the completion of the OAM discovery process."

Use the new figure as shown in tf4_2312_kramer_figure_13-1_5.pdf. The new figure shows the OAM discovery and eOAM discovery as separate processes. The figure is drawn in the same style as figure 11-4.

-

#11 Type: T TF: TF4 Clause: 13.3.2.3 Page: 234 Line: 23 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

When we describe a protocol (or a message exchange), we usually don't designate each message as a separate step of the protocol. Rather steps represent a phase of the protocol, such as capability discovery phase or configuration phase. For example, see Figure 11-4. But the message flow during the eOAM discovery designates each OAMPDU as a separate step. Also, it would be nice if Figure 13-2 style matched the Figure 11-5 style.

Modify section 13.3.2.3 as shown in tf4_2312_kramer_eoam_discovery_4_clean.pdf and tf4_2312_kramer_eoam_discovery_4_diff.pdf General text improvements are made, as well as figure style changed to match Figure 11-5.

-

#9 Type: TR TF: TF4 Clause: 14.4.5.1 Page: 365 Line: 15 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

"The minimum value of 2 denotes the two methods that are mandatory to support (see 11.3)." The definition of the attribute aInitialKeyCapability refers to two encryption methods that are mandatory, but the sub-clause 11.3 doesn't mention such methods.

Add 4 additional sub-clauses under the 11.3 to cover the key establishment method requirements and the initial key lifetime. The existing subclause 11.3 becomes 11.3.3. The exact changes are illustrated in tf4_2312_kramer_ecdh_requirements_3.pdf

-

#13 Type: T TF: TF4 Clause: 14.4.5.1 Page: 366 Line: 4 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

"...indicates that the corresponding sIdentifier[i] is defined by the IANA TLS Supported Groups registry (see [IANA TLS Groups])" Missing normative reference entry for IANA

Add the following to the clause 2 Normative References: IANA, “TLS Supported Groups”, https://www.iana.org/assignments/tls-parameters.

-

#5 Type: T TF: TF4 Clause: 4A.2.7 Page: 436 Line: 1 Commenter: Glen Kramer / Broadcom

Comment Status: New Response Status: None Commenter Satisfaction: None Category: -

In D1.6 in Table 5-1, the feature "Management" was refined as "Management MessAGE Structure". The corresponding PICS were renamed from MG-xxx to MMS-xxx. But the subclause titles were not updated.

Change titles of 4A.2.7 and 4A.3.7 from "Management" to ""Management message structure"

-