#11 Type: TR TF: TF4 Clause: 7.2.1 Page: 59 Line: 16 Commenter: Glen Kramer / Broadcom

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

Current draft includes VLAN modes from all three packages in 1904.1. Some of these modes have contradictory requirements: 7.2.1.1.1: The OLT preserves the last provisioned configuration for VLAN mode and VLAN IDs in the nonvolatile memory. Upon the power-up, reset, or restart caused by local or remote signaling, the OLT shall use the last provisioned VLAN mode and VLAN IDs for all LLIDs. 7.2.2.2.6: Upon power-up, reboot, or restart caused by local or remote signaling, the OLT shall be configured to use the Transparent VLAN mode for all ESPs associated with the active ONUs. The same contradiction exists for the ONU requirements. Both The Device-Based VLAN modes and Port-based VLAN modes rely on OAM attributes that are not defined in 1904.4.

Delete sub-clauses 7.2.1 except 7.2.1.3. Elevate 7.2.1.3 to L3 header.

-

#2 Type: TR TF: TF4 Clause: 11 Page: 136 Line: 1 Commenter: Glen Kramer / Broadcom

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

The contribution submitted with comment #24 against D2.0 had an introductory text that for some reason didn't make it into D2.1

Add the following text under the L1 header: "Clause 11 introduces the security-related mechanisms, focusing in particular on ONU identity and various aspects of access management (see 11.2) and data encryption / decryption (see 11.3), achieved in an interoperable manner."

-

#3 Type: T TF: TF4 Clause: 11.1.3.1 Page: 140 Line: 6 Commenter: Glen Kramer / Broadcom

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

Cross-reference is TBD.

Replace TBD with 11.2.2.1.4

-

#10 Type: E TF: TF4 Clause: 11.2.2.1.3 Page: 141 Line: 30 Commenter: Glen Kramer / Broadcom

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

11.2.2.1.3, line 30: "...extension with a value of “1” (dac). (see 11.2.2.1.2)" 11.2.2.1.4, line 35: "...extension with a value of “2 (nac)” (see 11.2.2.1.2)."

1) Remove quotation marks around "1" and "2 (nac)" 2) Remove the text "(dac)" and "(nac)" 3) On page 141 line 30, move the dot to the end of sentence

-

#6 Type: T TF: TF4 Clause: 11.2.2.1.3 Page: 142 Line: 4 Commenter: Glen Kramer / Broadcom

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

"The certificate does not include any extensions marked “critical” unless required by RFC-5280 or required above." The above sentence places burden on a reader to search what critical certificates are required above or by the RFC 5280. Looking at what is "required above" - the specification does not list any critical extensions. The RFC-5280 does not indicate which critical extensions must appera in DAC. The example DAC in Annex 11A shows just one critical extension (BasicConstraints). So, it is very confusing for the standrad user to figure out what critical extensions must be included. This decision should be done at the time of writing the standard, not left to users.

State directly what critical extension(s) are included in DAC. For example: "The certificate does not include any extensions marked “critical”, except the BasicConstraints extension."

-

#8 Type: T TF: TF4 Clause: 13.4.6.7.1 Page: 207 Line: 17 Commenter: Glen Kramer / Broadcom

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

This NAC example in 11A.3.1 shows the bare manimum NAC and intermediate certificates, with no operator-defined metadata, except the subscriber-id. And already these two certificates together take 1441 bytes in PEM format. This is very close to our combined limit of 1489 bytes for the NAC together with all intermediate certificates. The limit comes from the earlier decision to carry NAC + intermediates together in one OAMPDU.

Should we revise it and make separate OAMPDU opcodes for carrying NAC and for carrying intermediate certificates? This way, each individual certificate can be up to 1489 bytes long. Also, it would be possible to install more than one intermediate certificate into the ONU. This comment is to prompt a discussion. No specific draft changes are proposed.

-

#5 Type: T TF: TF4 Clause: 4A.2.6 Page: 392 Line: - Commenter: Glen Kramer / Broadcom

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

Subclause 4A.2.6 is titled 'ONU Authentication", but it covers both authentication and authorization PICS. The same is with OLT PICS in 4A.3.6 PICS U-AU0 and T-AU0 say "...implements ONU authentication function per 11.2", but 11.2 includes both authentication and authorization procedures.

1) In Table 5-1, row "AU", change the feature name to "ONU authentication and authorization". (Keep the acronym "AU" or change to "AAU"?) 2) Change titles of 4A.2.6 and 4A.3.6 to "ONU authentication and authorization" 3) Change Value/Comment of PICS U-AU0 and T-AU0 to "...performs ONU authentication and authorization procedures per 11.2"

-

#1 Type: T TF: TF4 Clause: 4A.2.15 Page: 423 Line: 1 Commenter: Marek Hajduczenia / Charter

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

Update multicast connectivity PICS for ONU and OLT

Use tf4_2408_hajduczenia_1.docx (and pdf) for reference on the changes to 4A.2.15, 4A.3.15, and 4A.3.16

-

#4 Type: E TF: TF4 Clause: 4A.3.6 Page: 433 Line: - Commenter: Glen Kramer / Broadcom

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

In Value/Comment field of T-AU5, the word "that" is repeated twice

Correct, per comment,

-

#7 Type: E TF: TF4 Clause: 9A Page: 461 Line: 1 Commenter: Glen Kramer / Broadcom

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

Annex 9A and Annex 11A do not show line numbers

per comment

-

#9 Type: TR TF: TF4 Clause: 11A Page: 464 Line: 1 Commenter: Glen Kramer / Broadcom

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

Several issues with Annex 11A: Per 11.2.2.1.1, the DAK shall be generated using SECP384R1, but the anenx example shows it generated with SECP256R1 curve. Anenx shows first the PEM-encoded result of certificate generation, then the parsed (human-readable) certificate, only then the code used to generate it. The annex organization could be imporved. The code generating the certificates lumps together the geroic function that could be applicable to generate any certificate with a specific example parameters that are used for illustration only. It is better to separate the two. The examples generate a new random keypair and a new NEC serial number on every execution. This makes the examples not very useful as they are not reproducible by vendors. Examples need to rely on static parameters where possible.

Replace Annex 11A with a revised text provided in tf4_2408_kramer_annex11a_2.pdf. (Note that the contribution does not have the correct header numbering. Editor's assistance is required.) On page 141, line 34, change the text “CN=SIEPON4_ONU_0A7FB49E2CF1” to "CN=SIEPON4_ONU_58D08F123456", to match the new annex (using SIEPON OUI)

-