|  |  |
| --- | --- |
| Project | **IEEE 802.21 MIHS****<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **Suggested remedy for IEEE 802.21m draft** |
| DCN | 21-15-0050-03-REVP |
| Date Submitted | **May 13th, 2015** |
| Source(s) | Yoshikazu Hanatani (Toshiba) |  |
| Re: | Comments to IEEE 802.21m draft from IEEE 802 editor. |
| Abstract | This document describes suggested remedy for comments to IEEE 802.21m draft from IEEE SA editor. |
| Purpose | To create IEEE 802.21m draft |
| Notice | This document has been prepared to assist the IEEE 802.21 Working Group. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that IEEE 802.21 may make this contribution public. |
| Patent Policy | The contributor is familiar with IEEE patent policy, as stated in [Section 6 of the IEEE-SA Standards Board bylaws](http://standards.ieee.org/guides/opman/sect6.html#6.3) <[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://127.0.0.1:4664/cache?event_id=757737&schema_id=1&s=5X0vID10lu_E6yrIkWkNd4Wz2H8&q=hancock)> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/faq.pdf> |

**Comment [MT1]:** This has not been added yet, Amendment D, will be added post edit of the amendment.



 We will check the edited version draft.

**Comment [MT2]:** Verify this is the correct figure.



This comment is related to IEEE 802.21c.

 Problem: Figure 2 of D9.1 is from IEEE 802.21d D8.

 The original Figure 2 in 21 is Figure 3 of D9.1.

Suggested Remedy

 Change “Figure 2” to “Figure 3”.

 “Figure 2” in the second paragraph of 5.9.3 shall be changed to “Figure 3”.

**Comment [MT3]:** These may not be the correct clause numbers, inconsistencies with numbering in Amendment D, please check.



This comment is related to IEEE 802.21d.

Problem: Clause numbers in IEEE 802.21d D8 are already used in another annex.

 Suggested remedy:

Change the clause numbers in Table 3 of D9.1 as follows.

 7.4.30 to 7.4.34.

 7.4.31 to 7.4.35.

 7.4.32 to 7.4.36.

 7.4.33 to 7.4.37.

 7.4.34 to 7.4.38.

 7.4.35 to 7.4.39.

Add “7.4.30 **MIH\_Configuration\_Update** of D8” to D9.1 as 7.4.34.

Add “7.4.31 **MIH\_MN\_Group\_Manipulate** of D8” to D9.1 as 7.4.35.

 Add “7.4.32 **MIH\_Net\_Group\_Manipulate.request** of D8” to D9.1 as 7.4.36.

Add “7.4.33 **MIH\_Pull\_Certificate** of D8” to D9.1 as 7.4.37.

Add “7.4.34 **MIH\_Push\_Certificate** of D8” to D9.1 as 7.4.38.

Add “7.4.35 **MIH\_Revoke\_Certificate** of D8” to D9.1 as7.4.39.

**Comment [MT4]:** Inconsistencies with numbering Annex D, please fix.



This comment is related to IEEE 802.21d.

Problem: Clause numbers in IEEE 802.21d D8 are already used in another annex.

 Suggested remedy:

Change the clause numbers in Table 17 of D9.1 as follows.

 7.4.30 to 7.4.34.

 7.4.31 to 7.4.35.

 7.4.32 to 7.4.36.

 7.4.33 to 7.4.37.

 7.4.34 to 7.4.38.

 7.4.35 to 7.4.39.

**[MT5]:** Change as modified by 21d was not made here, this was confusing. The text did not match what was in the base nor modifications made by the previous amendments. Therefore I left text as is.



This comment is related to IEEE 802.21d.

Problem: Base texts in 7.4.16.1.4 (MIH\_Link\_Actions.request) of IEEE 802.21d D8 are from 7.4.15.2.4 (MIH\_Link\_Configure\_Tresholds.request) of IEEE 802.21 base specification.

Suggested remedy:

If the destination of the request is the local MIHF itself, the local MIHF issues a Link\_Action.request(s) to the specified ~~lower layer~~ link layer(s).

If the destination of the request is a remote MIHF, based on the ResponseFlag parameter, the local MIHF generates and sends an MIH \_Link \_Actions request message or an MIH\_Link\_Actions indication message to the remote MIHF. Upon the receipt of the message, the remote MIHF then issues Link\_Action.request(s) to the specified ~~lower layer~~ link layer(s). If Response Flag parameter is set, the remote MIHF also generates a response message for the sending MIHF.

Memo

 “indication.message” in 7.4.15.2.4 of D9.1 should be “indication message”.

**Comment [MT6]:** By default the numbering was changed based on modification in 802.21a, however I didn’t make any changes to Clause 8 (as modified by 21d (editorial intructions, are very unclear).



This comment is related to IEEE 802.21d.

Problem: Some instructions are unclear.

Suggested remedy:

Modify the instructions in D8 to instructions for D9.1 as follows.

 **8.4.2 Protected MIH protocol frame format**

***Change second paragraph of Clause 8.4.2 as follows:***

 A protected MIH PDU is an MIH PDU that has an MIH header with S bit set to one indicating that the MIH service specific TLVs in this PDU are ~~protected~~ encrypted and/or the PDU is digitally signed. When the MIH service specific TLVs in this PDU are encrypted, ~~Each~~each security association is defined for a pair or group of MIHFs and is identified by a security association identifier (SAID). ~~Therefore, for a protected MIH PDU, when a security association identifier is defined, the Source and Destination MIHF identifier TLVs may not be present. In this case, an MIH header is followed by an SAID TLV, which is followed by a security TLV. Figure 28a shows a protected MIH protocol frame, where the source and destination MIHF TLVs are optional.~~ In this case, an SAID TLV shall be carried in the PDU. Source and Destination MIHF Identifier TLVs may not be present when an SA is defined for a pair of MIHFs. When a PDU is digitally signed, a Signature TLV shall be carried in the PDU. A Signature TLV should be used for multicast MIH messages in order to provide source origin authentication for multicast MIH messages. Otherwise, a message alternation attack by an insider who has a GKB SA is possible even if the multicast MIH message is integrity protected by the group key corresponding to the GKB SA. Signature TLV is not needed for a message that is protected by a GKB SA for a two-member group. Figure 29 shows a protected MIH protocol frame. Table 4 shows valid combinations of S bit and security-related TLVs.

***Insert Table 4 of D8 to the end of 8.4.2.***

***Replace Figure 36 to Figure 29 of D8.***

**8.4.2.1 MIH PDU protected by (D)TLS**

***Add the following text at the end of Clause 8.4.2.1:***

A Signature TLV shall not be carried when MIH PDU is protected by (D)TLS (RFC 6347). Note that an MIH PDU protected by (D)TLS should only be used for unicast communication.

**8.4.2.2 MIH PDU protected through EAP-generated MIH SA**

***Add the following text at the end of Clause 8.4.2.2:***

 A Signature TLV shall not be carried when MIH PDU is protected through EAP-generated MIH SA.

***Add the following Clause at the end of 8.4.2.~~2~~3:***

 **8.4.2.~~4~~ MIH PDU protected through Group key generated MIH SA**

 When a GKB is used to distribute a MGK, the keys derived from MGK shall be used for a group MIH SA that is created for a group of MIHFs to encrypt Service Specific TLVs of an MIH PDU. The group MIH SA is identified by a security association identifier assigned by the PoS and carried in a SAID TLV. For integrity protection, a Signature TLV is carried in the MIH PDU. Figure 30 shows a protected MIH PDU for GKB-generated MIH SA. The protection procedure is specified in 9.6.2.

***Insert Figure 30 in D8 at the end of Clause 8.4.2.~~3~~4:***

**8.4.2.5 MIH PDU protected by digital signature only**

When an MIH PDU with the S bit set sent by a PoS is not encrypted, it is integrity protected by a digital signature. Figure 31 shows an MIH PDU protected by a digital signature only. The protection procedure is specified in 9.6.

***Insert Figure 31 in D 8at the end of Clause 8.4.2.4:***

**Comment [MT7]:** I have to figure out how to get this 2 closer to the parens.



Suggested remedy:

 IEEE SA editor can solve it.

**Comment [MT8]:** Check these last three rows, the modification in Amendment A, was unclear on where the insertions should go.

**Comment [MT9]:** Check for proper placement, based on Amendment B, it is unclear where the insertion should be.

Table D.1—Mapping MIH messages to reference points.



This comment is related to IEEE 802.21a and IEEE 802.21b.

Suggested remedy.

1. The placement of the four rows is correct.
2. Remove following two empty rows.
3. Change “MIH\_NET\_HO\_BCST\_Commit” in Table D.1 to “MIH\_Net\_HO\_Bcst\_Commit”.



Remove this row.

Remove this row.

**Comment [MT10]:** Check, for proper placement, Amendment C added this as item 5, however, the table already had the preceding information for 5.

Table F.4—Data types for links



This comment is related to IEEE 802.21c.

Problem: item 5 is already used by IEEE 802.21b.

Suggested remedy.

1. Insert the item 5 of Amendment C as item 14 to LINK\_PARAM\_GEN of Table F.4.
2. Change “14—255: (Reserved)” in LINK\_PARAM\_GEN of Table F.4 to “15—255: (Reserved)”.

**Comment [MT11]:** Review, this modification was added in Amended C, Bit 5: had already been added by a previous amendment.

Table F.20—Data type for MIH capabilities



This comment is related to IEEE 802.21c.

Problem: Bit 5 is already used by IEEE 802.21b.

Suggested remedy.

1. Insert the Bit 5 of Amendment C as Bit 6 to MIH\_CMD\_LIST of Table F.20.
2. Change “Bit 6-31: (Reserved)” in MIH\_CMD\_LIST of Table F.20 to “Bit 7-31: (Reserved)”.

**Comment [MT12]:** Check these three highlighted rows, the placement was not clear in Amendment A.

Table G.1 – Information element identifier values



This comment is related to IEEE 802.21a.

Suggested remedy:

1. The placement of the highlighted rows is correct.
2. Move two rows, IE\_PoS\_TUNN\_MGMT\_PRTO and IE\_PoS\_NAI, between IE\_PoS\_IP\_ADDR and IE\_CONTAINER\_LIST\_OF\_NETWORKS,as follows.



**Comment [MT13]:** Did not make changes as modified by Amendment A and Amemendment C (the instructions and information was conflicting in Amendment A and unclear, so left as is.



This comment is related to IEEE 802.21a and IEEE 802.21c.

Suggested remedy:

 Replace Annex H of D9.1 to Annex H of Amendment C.

# We need to verify with Yoshi.

**Comment [MT14]:** Review these modification, the previous row was added in a previous amendment, and according to Annex C, this information should be added, M.8.4.43 already existed. Fix discrepancy.

M.8.4 PDUs



This comment is related to IEEE 802.21c.

Problem: M.8.4.43 is already used by Amendment B.

Suggested remedy:

 Change M.8.4 as follows.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M.8.4.44 | MIH\_Prereg\_Xfer request | 8.6.3.24 | o | Yes [] No [] | PDU 44 |
| M.8.4.45 | MIH\_Prereg\_Xfer response | 8.6.3.25 | o | Yes [] No [] | PDU 45 |
| M.8.4.46 | MIH\_N2N\_Prereg\_Xfer request | 8.6.3.26 | o | Yes [] No [] | PDU 46 |
| M.8.4.47 | MIH\_N2N\_Prereg\_Xfer response | 8.6.3.27 | o | Yes [] No [] | PDU 47 |
| M.8.4.48 | MIH\_Prereg\_Ready request | 8.6.3.28 | o | Yes [] No [] | PDU 48 |
| M.8.4.49 | MIH\_Prereg\_Ready response | 8.6.3.29 | o | Yes [] No [] | PDU 49 |
| M.8.4.50 | MIH\_CTRL\_Transfer request | 8.6.3.30 | o | Yes [] No [] | PDU 50 |
| M.8.4.51 | MIH\_CTRL\_Transfer request | 8.6.3.31 | o | Yes [] No [] | PDU 51 |