**IEEE P802.21
Media Independent Handover Services**

|  |
| --- |
| **Proposed Remedy for the 802.21d LB7 comment #159** |
| **Date:** 2013-09-14 |
| **Author(s):** |
| **Name** | **Affiliation** | **Address** | **Phone** | **Email** |
| Yoshikazu Hanatani | Toshiba |  |  | yoshikazu.hanatani@ toshiba.co.jp |

Abstract

This document contains proposed remedy for “the 802.21d ballot 7 comment #159 about a team of “divided GKB.”

**Remedy for the 802.21d LB7 comment #159**

9.4.2 Secure group manipulation with group key distribution

Figure 45 illustrates group manipulation command distribution initiated by a Command center via a multicast channel. The MIH User of the Command center generates an MIH\_Net\_Group\_Manipulate.request, described in 7.4.32, and then it passes the request to the MIHF of the Command center. Upon receiving the request, the MIHF generates MIH\_Net\_Group\_Manipulate indication (Note that the decision on sending an indication message or a request message depends on the ResponseFlag parameter of the MIH\_Net\_Group\_Manipulate.request primitive), described in 0, and sends it to the MNs via multicast mechanisms. When an MN receives the MIH\_Net\_Group\_Manipulate indication message, the MIHF of the MN processes the message. After processing the message, the MIHF sends MIH\_Group\_Manipulate.indication to the MIH User of the MN.



1. —Example of group manipulation distribution using multicast mechanisms

###### 9.4.2.1 MIH User of a PoS

In a typical example, an MIH User of a Command center generates MIH\_Net\_Group\_Manipulate.request described in 7.4.32 as follows:

1. Define a group to manipulate. If it is a new group, choose a TargetIdentifier which is not currently in use by consulting with the Group Management Database. Then, decide group members, i.e. MNs, of the group and a master group key for the group. For new groups, the master group key is chosen uniformly at random. For an already existing group, new members to be added to the group are added to the group members, and members to be removed from the group are removed from the group members. Group membership is registered at the Group Management Database and managed by the Group manager.
2. Send to the GKB Generator all the Device Keys, the Leaf Numbers of the group members determined in a) and the group key. Then, the MIH User receives from the GKB generator a GKB or a set of GKBs: A GKB contains a CompleteSubtree field, a GroupKeyData field and optionally a SubgroupRange field. A SubgroupRange is a pair of Leaf Numbers and defines a range of Leaf Numbers. A simple example which shows how to make those fields is given in **Error! Reference source not found.**. A GKB contains a SubgroupRange field if it is one of fragmented GKBs. Note that one MIH\_Net\_Group\_Manipulate.request contains one and only one GKB. Plural GKBs result in plural requests.
3. (Optional) Construct the UserSpecificData field.
4. Choose a DestinationIdentifier. A DestinationIdentifier is a Group MIHF ID which represents an existing group. The SubgroupRange indicates the MNs which are the distribution targets of the GKB. If an MN is in the range, it should receive the fragmented GKB. At least, an MIHF Broadcast Identifier is assumed to exist. Other initial groups may exist though they are out of the scope of this specification.
5. Generate an MIH\_Net\_Group\_Manipulate.request from the DestinationIdentifier, the TargetIdentifier, the SubgroupRange (an option), the VerifyGroupKey (an option), the UserSpecificData (an option), the CompleteSubtree and the GroupKeyData (an option). Set the GroupKeyUpdateFlag if the group key of the group designated by the TargetIdentifier should be updated. Send it to the local MIHF.
6. Update the Group Management Database. If the target group of manipulation is an existing group, add/remove members (MIHF IDs, Device Keys and Leaf Numbers) and update its group key. If the target group is a new one, add a new Group MIHF ID (= TargetIdentifier) with its new members and its new group key to the Group Management Database.

Insert following text to an appropriate part.

If a data size of a GKB is greater than the upper bound of the MIH command, an MIH User of PoS shall fragment the GKB. Each fragmented GKB shall contain a SubgroupRange to correctly manipulate a group. The expected behavior of a fragmented GKB recipient depends on (1) whether the recipient is covered by CompletedSubtree, and and (2) whether the recipient is covered by SubGroupRange when SubGroupRange is contained in the GKB, as described in Table XX.

Table XX Expected Behavior of Recipient of Fragmented GKB

|  |  |  |
| --- | --- | --- |
| Covered by CompleteSubtree? | Covered by SubGroupRange? | Expected behavior |
| No | No | Ignore |
| No | Yes | Leave |
| Yes | No | Ignore |
| Yes | Yes | Join |