Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 10, 2010

JC. Zuniga
M. Perras
InterDigital Communications, LLC
T. Melia
Alcatel-Lucent Bell Labs
C. Bernardos
Universidad Carlos III de Madrid
November 06, 2009

Support of Proxy MIP in the context of WiMAX Networks
draft-zuniga-netext-wimax-mn-ar-if-00

Abstract

This ID documents the support of Proxy MIP in the context of WiMAX networks (WiMAX-to-WiMAX using PMIP). The main goal is to support the Netext working group in the discussions regarding how RFC 5213 [RFC5213] has been deployed by other SDOs.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

Copyright Notice

Table of Contents

1. Terminology

This document uses the following terminology:

A-DPF	ASN-GW DPF
ASN	Access Service Network
CSN	Connectivity Service Network
DPF	Data Path Function
FA	Foreign Agent
HA	Home Agent
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
NAS	Network Access Server
NSP	Network Service Provider

2. Introduction

The WiMAX Forum specified the WiMAX Network Architecture. Figure 1 introduces the network reference model that shows several interoperability reference points.

```
                                  R2
   |--------------------------------------------------------------|
   |                                      R3                      |
   |                 |-----------------------------------------|  |
   |          _______|______         _____________        _____|__|____
   |         |      NAP     |       |     V_NSP   |      |     H_NSP   |
   |         |              |       |             |      |             |
+--|--+      | +----------+ |       | +---------+ |      | +---------+ |
|     |      | |      ASN | |       | |     CSN | |      | |     CSN | |
| MS  |  R1  | |          | |   R3  | |         | |  R5  | |         | |
|     |------| |  ASN GW  | |-------| | AAA     | |------| | AAA     | |
|     |      | |          | |       | | proxy   | |      | | home    | |
|     |      | |  FA/MAG  | |       | |         | |      | |         | |
+-----+      | |          | |       | |         | |      | | HA/LMA  | |
             | |  NAS     | |       | +---------+ |      | +---------+ |
             | +----------+ |       |_____________|      |_____________|
             |       |      |                                   |
             |       | R4   |                                   |
             |       |      |                                   |
             | +----------+ |                                   |
             | |      ASN | |                                   |
             | |          | |                                   |
             | |  ASN GW  | |                                   |
             | |          | |                                   |
             | |  FA/MAG  | |                                   |
             | |          | |                                   |
             | |  NAS     | |                             |-----|
             | +----------+ |                             |
             |______________|                       _.----|-----.
                                                ,-''             `--._
                                               /                      \
                                              (        Internet        )
                                               \                      /
                                                `--.             _.--'
                                                    `----------''

   Legend of lines:
     control plane    ---------
```

Figure 1: Network Reference Model with HA in home NSP

Figure 1 shows the WiMAX Reference Model. Reference Point R1 consists of the protocols and procedures between MS and ASN as per the air interface specifications. Reference Point R2 consists of protocols and procedures between the MS and CSN associated with Authentication, Services Authorization and IP Host Configuration management. Reference Point R3 consists of the set of Control Plane

protocols between the ASN and the CSN to support AAA, policy enforcement and mobility management capabilities. It also encompasses the Bearer Plane methods (e.g., tunneling) to transfer user data between the ASN and the CSN. Reference Point R4 consists of the set of Control and Bearer Plane protocols originating/terminating in various functional entities of an ASN that coordinate MS mobility between ASNs and ASN-GWs. Reference Point R5 consists of the set of Control Plane and Bearer Plane protocols for internetworking between the CSN operated by the home NSP and that operated by a visited NSP.

In PMIPv6 supported network, in order to provide the IP mobility service connectivity to MS that does not have mobility capability, LMA in CSN will assign a home prefix or an IPv4 MN-HoA to the MS (if not statically allocated from the AAA server). Depending on the network configuration, the home prefix(es) could be assigned by either V-LMA (if VCSN exists) or H-LMA. Authentication, authorization and accounting information as well as policy control are handled by the home NSP over R3 and/or R5 reference points.

In the remainder of this document we assume PMIPv6 is the selected mobility management protocol.

3. Differences between PMIP in WiMAX and IETF specifications

The WiMAX network architecture is specified in [WMF-T32-002-R010v04 Part 1]. The PMIPv6 protocol support in WiMAX is specified in [WiMAX Forum Network Working Group Proxy MIPv6 support Stage 2]. The main differences between the PMIPv6 protocol specified in [RFC5213] and the PMIPv6 protocol specified by WiMAX Forum are listed here and described in more details in the following sub-sections. These differences are mainly: 1) the introduction of new parameters used to indicate the IP service capability of the ASN and VCSN, 2) the introduction of the Authenticator/NAS function and 3) the in-band protocol security applied by the MAG/LMA to the PBU/PBA.

3.1. New parameters introduced to indicate IP service capability

The new parameters named ASN IP Service Capabilities and VCSN IP Service Capabilities are used to indicate the IP service capability of the ASN and VCSN and are introduced in the WiMAX network.

It should be noted that these parameters are conveyed from ASN (VCSN) to (H)CSN through AAA request message. Once the MS is successfully authenticated by the HAAA and HCSN has authorized one or more IP Services, the Authorized IP Services and Authorized Anchor Location attributes are passed to ASN through AAA Response message.

These parameters are not specified in the PMIP specifications [RFC5213]

3.2. Authenticator/NAS function introduced

The Authenticator/NAS negotiates the PMIPv6 security mode with the HAAA and makes that information available to the MAG. If the negotiated security mode is in-band, then the Authenticator/NAS facilitates authentication and authorization functions with the aim to acquire, store and distribute keys and related security information required for PMIPv6 operation. Authenticator interworks with MAG in the process of establishing the LMA trust relationships and appropriately securing mobility signaling.

The Authenticator/NAS functionally is specific to the WiMAX specifications. What is specified in [RFC4285] is only concerning the authentication and AAA server: "The network entities in the Proxy Mobile IPv6 domain, while serving a mobile node, will have access to the mobile node's policy profile and these entities can query this information using RADIUS [RFC2865] or DIAMETER [RFC3588] protocols".

3.3. In-band protocol security applied between MAG/LMA

There are two mandatory-to-implement and optional-to-use security modes for PMIP6: One using [RFC4285] (in-band security), and the other not using any PMIP6-specific security but relying on the R3/R5 control plane security (lower-layer security). NSP and NAP decide which mode to operate based on their local policy and the dynamic negotiation during the network access authentication of the MS. MAG learns the negotiated mode from the authenticator in order to generate the PBU and process the PBA accordingly.

Proxy MIPv6 [RFC5213] specifies IPsec as a mandatory-to-implement security mechanism. It also specifies that the use of IPsec for protecting a mobile node's data traffic is optional. Additionally, it specifies that other documents may specify alternative for securing Proxy Mobile IPv6 signaling messages. In WiMAX networks, the PMIPv6 signaling messages are secured using the security mode defined in [RFC4285] (use of AE in the PBU/PBA).

4. PMIPv6 support - CSN anchored mobility management

As stated before we focus here on the use of PMIPv6. We summarize in the following sections the attachment procedures, PMIPv6 connection setup, CSN-anchored mobility handover and detachment procedures focusing on the PMIPv6 usage and MAG, Authenticator, LMA functions.

4.1. Network attachment

CSN anchored mobility management based on PMIPv6 is transparent to the MS. At the time of the network entry, MS undergoes the regular attachment procedures without directly participating in mobility signaling; selects the network, performs the network entry and proceeds by configuring the IP address. For a given MS, the network determines whether to use PMIPv6 or not.

4.1.1. Network Service Capability Negotiation

Simple IP, CMIP and PMIP services for IPv4 as well as IPv6 may be simultaneously provided by a network. Such network configuration provides coexistence of Simple IP service and MIP service support on a per user basis. Whether the Simple IP service or PMIP or CMIP service is invoked by the network for a given user will depend on the user profile, network capabilities negotiation between ASN, VCSN and HCSN along with the operator policy.

4.1.1.1. Selection Scheme

The Network Service Capability Negotiation and Selection scheme expands the network access authentication and authorization process adding capability to negotiate the appropriate IP service among ASN, VCSN (when exists) and HCSN. Two new RADIUS attributes named ASN IP Service Capability and V-CSN IP Service Capabilities have been defined to indicate IP service capabilities of ASN and VCSN, respectively.

These parameters are conveyed from ASN (VCSN) to (H)CSN through AAA request message. Once the MS is successfully authenticated by the HAAA and HCSN has authorized one or more IP Services, the Authorized IP Services and Authorized Anchor Location attributes are passed to ASN through AAA Response message.

Depending on the outcome of this capability negotiation, ASN offers only one of authorized Simple IP, PMIP or CMIP services to the mobile. When multiple IP services are authorized it is the ASN network that makes the final decision of whether or not to allow MS request and assign the appropriate IP service support for this MS.

4.1.1.2. Selection Flow

During MS authentication phase, the AAA Request message is sent by the ASN to the H-AAA of the MS (may be sent via the AAA Proxy at the VCSN). In particular, ASN includes the ASN IP Service Capabilities attribute in the AAA Request to provide current ASN IP service capability information of this ASN to the HAAA.

After receiving AAA Request message, the VCSN adds VCSN IP Service Capabilities attribute to this message and forward the message to HAAA Server at the HCSN.

Once the HAAA Server successfully authenticates and authorizes the MS services, the HAAA returns the AAA Response message to the NAS in ASN via the AAA Proxy at the VCSN. Together with other MS subscriber and IP configuration parameters, the Authorized IP Services (and Visited Authorized IP Services if VCSN anchoring is permitted) attribute are also included in the AAA Response message.

The AAA Proxy in VCSN relays this AAA Response message to ASN. The ASN extracts out the Authorized IP Services and Visited Authorized IP Services information, stores them locally and makes it available to use by the appropriate IP service function entities within ASN. Depending on the outcome of the capability negotiation, the ASN selects among the authorized services and offers a single IP service to the MS.

4.1.2. IP address configuration

WiMAX network supports both stateless and stateful IPv6 address autoconfiguration methods within the PMIPv6 scope. Depending on the configuration and preferences, MS can try to configure an IPv4 address by DHCPv4, one or more IPv6 addresses by DHCPv6 or stateless address autoconfiguration.

If for any reason the network needs to enforce a specific configuration method it must set the particular address configuration flags in the RA messages (ManagedFlag and OtherConfigFlag) to do so.

The HNP for the PMIPv6 MN-HoA may be allocated from two sources, the LMA or the AAA server.

- Prefix/HoA can be bootstrapped from the dedicated AAA server during the network authentication process.

- PMIPv6 LMA assigns the unique/64 IPv6 prefix in response to the PBU message from the AR/MAG (ASN) with Home Prefix option set to ALL_ZERO, when HNP has not been obtained through network authentication.

4.2. PMIPv6 connection setup

The network authentication enables the ASN/NAS to negotiate and boostrap the necessary PMIPv6 mobility parameters and network configuration, including the assigned IP address or IPv6 prefix, security related settings, authorized address configuration mode(s),

etc.

The PMIPv6 connection setup takes place after the initial network entry and access authentication is completed. The prerequisite for the procedure is the network decision to assign the network-based PMIPv6 service for MS IP session. The mobility binding registration from the AR/MAG can occur at any moment following the access authentication response that brought the required IP capabilities and services authorization from the H/VCSN to the ASN where MS is attaching.

The connection setup procedures are differentiated by the address configuration process the MS undergoes. For an IPv6 MS the WiMAX network should provide both stateful and stateless address (auto)configuration modes with per-MS unique prefix assignment, while for IPv4 MS, the DHCPv4 support is needed to distribute the IPv4 MN-HoA to the MS.

The MS is not involved in PMIPv6 mobility procedures and only required to perform the common address acquisition and configuration procedure to obtain IP mobility management via PMIPv6.

4.3. PMIPv6 CSN-anchored mobility handover

PMIPv6 mobility handover comes as a result of the A-DPF handover and R3 path relocation to the new serving ASN. There are no specific requirements towards the MS for the case of PMIPv6 handover. The new serving ASN(b) SHOULD assure the appropriate link configuration and the same address of the first-hop AR/MAG get consistently advertised to the MS after the HO, to hide the actual change of the attaching link.

If not performed during the Idle Mode, the process is preceded by regular ASN-MM procedures where the PMIPv6 MAG remains anchored at the previous serving ASN-GW/ASN(a) until the Push/Pull A-DPF HO is triggered. In course of the process the new ASN-GW/ASN(b) obtains all mobility and security wise session information from the serving ASN(a) and Anchor Authenticator, and is able to register the MS new location at the LMA. Successful PMIPv6 registration from the new MAG (new Proxy CoA) results with a refresh to binding cache at the LMA, extension to MS PMIPv6 session and an update to MS forwarding tunnel now redirected towards the new serving MAG at the ASN(b).

In case of idle mode, when the MS has established the data path on the new serving ASN(b), triggered by one of the HO events, the serving ASN(b) may initiate PMIPv6 HO by sending the Anchor_DPF_HO_Trigger message to the anchor ASN(a) for PULL handover mode. The anchor ASN(a) either responds or self-initiates the

handover (PUSH mode) by sending the Anchor_DPF_HO_Req to the serving ASN(b). The message contains the relevant information associated with the specific PMIPv6 session; allocated HNP or IPv4 HoA, LMA IP address, protocol configuration details such as DHCP and security mode (if applicable), etc. The target ASN(b) sends an Anchor_DPF_Relocate_Req message to the anchor Authenticator requesting a PMIP6 HO. If the ongoing PMIPv6 session requires in-band protocol security, the target ASN(b) requests the keying information from the anchor Authenticator needed to protect the forthcoming PMIPv6 signaling exchange with the LMA.

In case that target AR/MAG in ASN(b) receives Anchor_DPF_Relocate_Rsp message from the anchor Authenticator, it triggers PBU/PBA procedure to register MS new location and create the PMIPv6 tunnel between itself and the LMA. the target ASN(b) updates the anchor Authenticator with new AR/MAG location by sending the Anchor_DPF_Relocate_Ack message with success code. The target ASN(b) also informs the ASN(a) of the PBU registration result by sending an Anchor_DPF_HO_Rsp with an appropriate result code.

Target AR/MAG performs the PBU registration procedure following the guidelines specified in [RFC5213] . The PBU MUST contain the MN ID, HNP or IPv6 HoA options, the Access Technology Type (set to value WIMAX), the Handoff Indicator option (set to value of 3) as well as the Link-local Address option (set to value ALL_ZERO, requesting the LMA to provide current in-use AR downlink address).

The LMA updates the MS binding cache entry with the new location information storing the new Proxy-CoA address. Upon successfully updating the MS BCE, the LMA establishes PMIPv6 tunnel towards the new AR/MAG together and installs the corresponding forwarding rules, and simultaneously tears down the tunnel towards the previous AR/MAG (old Proxy-CoA). If the AAA indicates in-band protocol security is needed for the ongoing PMIPv6 session (i.e., use of AE in PBA/PBU), the LMA requires and derives the necessary security parameters as to protect the PBA before it is sent to the target AR/MAG.

Upon receiving PBA from the LMA indicating registration success, the new AR/MAG in ASN(b) updates its local MS context and mobility binding with the information obtained, creates PMIPv6 transport tunnel towards the LMA and install the needed forwarding rules.

4.4. PMIPv6 session termination

MS self-initiates PMIPv6 session termination when detaching from the network with graceful network exit, or simply performing the IP/DHCP release procedure for its IP session. The designated network entities may also initiate the IP session termination if discovering

the MS has detached/lost connectivity, prohibited from continuing the service or for some other operative or administrative reason. The ASN-GW/A-DPF, LMA or the AAA server induce the path deregistration by issuing a corresponding trigger message towards the serving ASN-GW/ ASN. Session termination SHALL follow the common NWG procedures and signaling exchange to achieve R4/R6 (R6 is the interface between the BS and MAG in the ASN) path release, MS state change and accounting stop. If applicable, the network-initiated session termination includes PMIPv6 De-registration at the LMA as well as IP/DHCP release on the MS side.

5. Security Considerations

For constructing the PBU and processing PBA response from the LMA, the AR/MAG follows requirements from [RFC5213] on MS attachment and initial binding registration, and receiving the PBA section, with one key difference. Inline with PMIPv6 service authorization results from the Access-Accept, the AR/MAG must apply in-band protocol security to the PBU sent to the LMA. When lower-layer transport security is requested by the HCSN, AR/MAG abandons explicit protection of PMIPv6 control plane. In any case, trust relationship MUST be established between LMA and its corresponding MAGs.

When in-band security is enabled (use of AE in the PBU/PBA), the LMA retrieves all necessary keying information from the AAA. Then the PBU includes a valid MAG-LMA derivation in the MN-HA mobility message authentication option [RFC4285].

The received PBU that entails signaling protection in form of valid authentication option MUST be replied a PBA using the same protection mechanism. The PBUs received without embedded signaling protection is processed and acknowledged only if the source MAG is considered trusted and use of AE options is not enforced for that PMIPv6 peer.

In case MS handovers from one ASN where R3 security is present to another ASN where it is not present and the target ASN wants to initiate change of PMIPv6 security mode, a re-authentication has to take place in order to change the negotiated security mechanism upon the handover. This change is feasible only to the LMA that supports the change of the security mechanism from in-band to lower-layer, or vice-versa, for the same MS upon an R3 handover.

When the negotiated mechanism is the lower-layer security, then the MAG/LMA does not include Mobility Message Authentication Option [RFC4285] in the PBU/PBAs, and MAG/LMA does not drop any incoming PBU/PBA which carries that option.

6. IANA Considerations

This document makes no request of IANA.

7. Acknowledgements

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

8.2. Informative References

[RFC4285] IETF, "Authentication Protocol for Mobile IPv6", January 2006.

[WMF-T32-002-R010v04 Part 1] WiMAX Forum Network Architecture, "WiMAX Forum Network Architecture Stage 2 Part 1", Stage 2 R010v04, February 2009.

[WiMAX Forum Network Working Group Proxy MIPv6 support Stage 2] WiMAX Forum Network Working Group, "Proxy MIPv6 support", Stage 2 1.0.0, January 2009.

Authors' Addresses

Juan Carlos Zuniga
InterDigital Communications, LLC

Email: JuanCarlos.Zuniga@InterDigital.com

Michelle Perras
InterDigital Communications, LLC

Email: Michelle.Perras@InterDigital.com

Telemaco Melia
Alcatel-Lucent Bell Labs

Email: telemaco.melia@alcatel-lucent.com

Carlos J. Bernardos
Universidad Carlos III de Madrid

Email: cjbc@it.uc3m.es