NETEXT WG S. Gundavelli
Internet-Draft B. Pularikkal
Intended status: Standards Track R. Koodli
Expires: April 24, 2014 Cisco
October 21, 2013

Applicability of Proxy Mobile IPv6 for Service Provider Wi-Fi Deployments
draft-gundavelli-netext-pmipv6-wlan-applicability-06.txt

Abstract

Proxy Mobile IPv6 is a network-based mobility management protocol. The protocol is designed for providing mobility management support to a mobile node, without requiring its participation in any IP mobility related signaling. The base protocol is defined in an access technology independent manner, it identifies the general requirements from the link-layer for supporting the protocol operation. However, it does not provide any specific details on how it can be supported on a specific access technology. This specification identifies the key considerations for supporting Proxy Mobile IPv6 protocol on the widely deployed wireless LAN access architectures, based on IEEE 802.11 standards. It explores the current dominant wireless LAN deployment models and provides the needed interworking details.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Proxy Mobile IPv6 is a network-based mobility management protocol specified in [RFC5213]. The protocol can be used for providing mobility management support to a mobile node within a localized domain, without requiring its participation in any IP mobility related signaling.

The core functional entities in the Proxy Mobile IPv6 domain are the local mobility anchor (LMA) and the mobile access gateway (MAG). The local mobility anchor is responsible for maintaining the mobile node's reachability state and is the topological anchor point for the mobile node's home network. The mobile access gateway is the entity that performs the mobility management on behalf of a mobile node, and it resides on the access link where the mobile node is anchored. The mobile access gateway is responsible for detecting the mobile node's movements to and from the access link and for initiating binding registrations to the mobile node's local mobility anchor.

There are numerous protocol extensions defined to Proxy Mobile IPv6 protocol, for supporting various features. These features include support for IPv4 transport and addressing support [RFC5844], GRE Key negotiation support [RFC5845], Binding Revocation support [RFC5846]. Diameter support [RFC5779], RADIUS support [I-D.draft-ietf-netext-radius-pmip6] and Proxy Mobile IPv6 MIB [I-D.draft-ietf-netlmm-pmipv6-mib]. All of these features give the protocol a completeness for being adopted as a network-based mobility management protocol within a micro-mobility domains, based on WLAN access architectures.

This specification identifies the key considerations for supporting Proxy Mobile IPv6 protocol in micro-mobility domains, such as in wireless LAN access architectures, based on IEEE 802.11 standards.

2. Conventions & Terminology

2.1. Conventions

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].

2.2. Terminology

All the mobility related terms used in this document are to be interpreted as defined in the Proxy Mobile IPv6 specifications [RFC5213], [RFC5844], [RFC5845] and [RFC5846]. Additionally, this document uses the following abbreviations:

- WLAN (Wireless Local Area Network) - A wireless network.

- WTP (Wireless Termination Point): The entity that functions as the termination point for the network-end of the IEEE 802.11 based air interface from the mobile node. It is also knows as the Wireless Access Point.

- WLC (Wireless LAN Controller): The entity that provides the centralized forwarding, routing function for the user traffic. All the user traffic from the mobile nodes attached to the WTP's is typically tunneled to this centralized WLAN access controller.

3. WLAN as an access technology and the related considerations

WLAN as wireless access technology has experienced significant adoption in both Enterprise and Service Provider Deployments. Enterprises leverage WLAN networks to provide Mobile access to their employees and partners to the enterprise network resources. Service Providers leverage WLAN for providing wireless Access to their subscribers by deploying indoor and outdoor Wi-Fi hotspots. These PWLAN deployments allow the service providers with additional revenue generation opportunities through the deployment of various use cases, which leverage the WLAN access. PWLAN networks typically deploy two types of SSIDs, Open and Secured. Open SSIDs are typically used along with some web portal based authentication and provides complimentary, pre-paid or subscription based Wi-Fi access to Internet. Secure SSIDs are typically used for Mobile Data Offload scenarios, which will use SIM card based authentication for the Mobile subscribers.

For the WLAN access network deployment, three models are available- a) Controller based WLAN Access Network with Converged CP-DP, b) Controller based WLAN Access Network with Split CP-DP & c) WLAN Access Network with Autonomous APs. Since these two options can be applied to various models, the Access Network section will be covered first followed by the detailed overview of various Deployment Models.

3.1. Controller based WLAN Access Network - Central Switched

This is a split MAC model with CAPWAP where 802.11 control plane functions are divided between AP and the WLC. WLC also handles AP provisioning, management and RRM. In this model, end user data traffic is always switched through the WLC via a CAPWAP data plane tunnel. From the PMIPv6 implementation perspective, the MAG functionality resides on the controller. This WLAN access network model is illustrated in Figure 1 below.

```
+-------+    CAPWAP CNTRL     +-------------+
|       +---------------------+             |  PMIPv6 towards LMA
|  AP   |                     |   WLC + MAG |+------------------->
|       +---------------------+             |
+-------+    CAPWAP DATA      +-------------+
```

Figure 1: WLAN Access - Central Switched

3.2. Controller based WLAN Access Network - Local Switched

This is a split MAC model with CAPWAP where 802.11 control plane functions are divided between AP and the WLC. WLC also handles AP provisioning, management and RRM. In this model, end user data traffic locally switched by the AP and does not reach the WLC. From the PMIPv6 implementation perspective, the MAG functionality resides on the AP. WLC does not play a role in the end user data traffic forwarding. This WLAN access network model is illustrated in Figure 2 below.

```
                              +----------+
          CAPWAP CNTRL        |          |
       +----------------------+   WLC    |
       |                      |          |
       |                      +----------+
       |
       |
       |
  +----+------+
  |           |     PMIPv6 towards LMA
  | AP + MAG  +---------------------------->
  |           |
  +-----------+
```

Figure 2: WLAN Access - Local Switched

3.3. WLAN Access Network with Autonomous APs

In this Access network model, WLCs will not be used. APs will perform all aspects of the 802.11 control plane and signaling. From the PMIPv6 implementation perspective, the MAG functionality will reside on the AP. This WLAN access model is illustrated in Figure 3 below.

```
   +------------+
   |            |   PMIPv6 towards LMA
   |  AP + MAG  |-------------------------->
   |            |
   +------------+
```

Figure 3: WLAN Access - with Autonomous APs

3.4. Comparison between WLAN Access Network Models

In general a controller-based architecture brings several advantages over autonomous AP deployments. The standards based split-mac model where many 802.11 functions are offloaded to the controller from the AP allows more lightweight and hence cost effective access point implementation. Also controller based architecture offers more flexible and scalable provisioning and operational management of the APs. Controllers may also support sophisticated Wi-Fi Radio Resource Management. No effective RRM implementation options are available in autonomous AP deployments. Another advantage of the controller based implementation model is the ability to localize the mobility events between the APs at the controller.

For the controller-based models, whether to use central switched or local switched depends up on the particular deployment models and the AP, Controller capabilities. In the central switched model, the mobility events between the APs are masked from the Wi-Fi aggregation gateway. However it will require the controller to handle all the end user data traffic, which may not scale in some cases. This will also put restrictions on the location of the controllers in a network, since the controllers will always need to be installed closer to the APs to ensure optimized forwarding path for the Wi-Fi end user traffic. Local switched mode may be suited in deployments where Wi-Fi gateways can handle high rate of mobility events and it is desirable to place controllers in a centralized location.

4. Deployment Models

There are numerous "field of use" cases around Service Provider Wi-Fi deployments; some of the key use cases are listed below:

Metro Wi-Fi model indoor and outdoor Wi-Fi deployments

Mobile Data Offload

Hospitality Wi-Fi

Community Wi-Fi

Whole Sale Deployment Model

Municipal Wi-Fi

PMIPv6 can be leveraged as the underlying architecture for any of these deployment use cases. The built in Network Based Mobility Management support available on PMIPv6 along with the rich set of protocol extensions make it a well suited standards based protocol of choice for SP Wi-Fi deployments.

Various "field of use cases" in Service Provider Wi-Fi can be mapped to one of the deployment models described in the section. For all of these deployment models, any of the WLAN access network implementation options described earlier in section 3 can be leveraged. For the sake of simplicity, discussions in this section will use the Controller based central switched option on the access network side for illustrative purposes.

4.1. Flat Model Deployments (Single PMPv6 Domains)

In this deployment model, PMIPv6 MAG functionality resides on the access network element (typically on AP or WLC) and the PMIPv6 LMA functionality resides either on a Wi-Fi Subscriber Aggregation Gateway (WAG) or a PDN Gateway. LMA on WAG will be used for the deployment scenarios, which does not require Mobile data offload. LMA function on PDN Gateway will be used for the packet core integration use cases where one or more SSIDs on the WLAN access network side are enabled for Mobile Data Offload. Flat model deployments are described in detail in the next two sub-sections.

4.1.1. Flat Model with LMA on WAG

This model is illustrated below in Figure 4. In this model, the Wi-Fi access network may leverage open SSIDs or secured SSIDs. If the open SSID is in use, subscriber access will always be controlled

by some sort of Web portal based authentication or MAC address based automatic login or a combination of both. Secured SSID may leverage non-SIM based authentication scenarios such as EAP-TLS or EAP-TTLS. WAG is the subscriber management element, which acts as the policy enforcement point for the Wi-Fi subscribers. WAG works in conjunction with an external PCRF. Interconnect between the PCRF and WAG in this model use either RADIUS or Diameter and in some cases may rely on some proprietary protocol. WAG uses either a RADIUS or diameter interface to forward the billing related information to an external billing entity. Two common subscriber billing options are pre-paid and post paid.

```
                     +-------+           +-----+
                     |BILLING+----+      |PCRF |
                     +-------+    |      +--+--+
                                  |         |
                             RADIUS/      RADIUS/
                             DIAMETER     DIAMETER
                                  |         |
                                  |         |
                                  +         |
                +-----+      +-------+      |
    +---+ CAPWAP|WLC | PMIPv6| LMA  |       |
    |AP |+------+ +  +--------+  +   +-------+
    +---+       |MAG |       | WAG  |
                +-----+      +--+---+
                                |
                                |
                                |
                              _----_
                            _(      )_
                           ( Internet )
                                    (_      _)
                              '----'
```

Figure 4: Flat Model with LMA on WAG

4.1.2. Flat Model with LMA on P-GW

This model is illustrated below in figure 5. In this model, LMA resides on a P-GW, which is part of a 3GPP Evolved Packet Core. S2a Mobility over PMIPv6 is part of 3GPP standard and allows trusted WLAN to EPC integration. Since the Wi-Fi access network is considered trusted, the solution always assumes the SSID is secured. SSID will be typically enabled for one of the SIM based authentication options such as EAP-SIM, EAP-AKA or EAP-AKA'. In this model, P-GW handles

the subscriber policy enforcement. P-GW acts as a PCEF and talks to an external PCRF over diameter interface. P-GW supports diameter based billing interface for offline and or online charging. Two common subscriber-billing options are pre-paid and post paid.

From an authentication perspective the WLAN will have a diameter or RADIUS interface to a 3GPP AAA server. This interface may be directly between the AP/WLC or in some cases with a proxy AAA server in the WLAN network side.

```
                   +                  +--------+
 WLAN Access NW    |   Packet Core +--+BILLING |
                   |               |  +--------+
                   |  +-------+    |
                   |  | 3GPP |     |          +----+
               ++-----+ AAA  |   DIAMETER     |PCRF|
               |   |  +-------+    |          +-+--+
            DIAMETER/              |            |
             RADIUS|               |            |
               |   |               +            |
            +--+--+|           +--------+  DIAMETER
+---+ CAPWAP| WLC ||  PMIPv6   |  LMA   |       |
|AP +--------+  +  +------------+   +    +-------+
+---+       | MAG ||           |  P-GW  |
            +-----+|           +----+---+
                   |                 |
                   |                 |
                                  _----_
                                _(      )_
                               ( Internet )
                                        (_      _)
                                  '----'
```

Figure 5: Flat Model with LMA on P-GW

4.2. Hierarchical Deployments with Domain Chaining

Domain chaining may be suited for some large scale SP Wi-Fi deployments and hybrid solutions which supports which supports open and secured SSIDs with or without Seamless Data Offload for Mobile operators. Domain chaining allows localization of mobility events at the chaining point for the first level domain. This is model is suited for inter-operator roaming scenarios as well.

There are two types of chaining models, both of which are described in the following sub-sections.

4.2.1. PMIPv6 to PMIPv6 chaining with RFC compatible Level-1 and Level-2 MAG and LMA functions

This model assumes that there are no requirements for packet core integration. The primary motivation behind chaining would be to introduce simplicity and scalability though the two level domain hierarchy. The chaining point not only allows for the localization of mobility events in a particular region, but can act as the SIPTO offload point for traffic which need to be selectively offloaded. SIPTO may happen at per subscriber level or per traffic flow level for a given subscriber. Another advantage, the chaining model introduces is the reduced scaling requirements around data plane tunnels. For example, with hierarchical model, simultaneous number of data plane tunnels need to be supported at a level LMA or level 2 LMA would be significantly lower compared the requirements on the LMA function in a flat deployment model. This model is illustrated in Figure 6.

```
                             +------+      +---------+
                             |PCRF  |      |BILLING  |
                             +---+--+      +-----+---+
                                 |               |
                                 |               |
                                 |               |
                                 +----------+    |
                                            |    |          x xxxxx
                                            |    |        xx      xxx
                                            |    |       xx         xx
                +----+      +------+       ++----+-+     x           xx
    +--+ CAPWAP |WLC |PMIPv6|L1-LMA|PMIPv6 |       |    xx            x
    |AP+--------+ +  +------|  +   +-------+L2-LMA +---+x CENTRALIZED xx
    +--+        |MAG |      |L2-MAG|       |       |    x              x
                +----+      +---+--+       +---+---+    x  SERVICES    x
                          SIPTO |                       x              x
                             xxx+xxxxx                  x             x
                            xx       xx                  xx          x
                           xx          x                     xxxxxx
                           x           xx
                          xx            x
                          x LOCALIZED  xx
                          x SERVICES   xx
                          x             x
                          xx            x
                           xxx       xxx
                             xxxxxxxxx
```

Figure 6: PMIPv6 to PMIPv6 Chaining

In this model per subscriber policy enforcement is expected to happen at level-1 LMA and level-2 LMA. Depending up on the deployment use case, interaction between PCRF may be done either just at the level-2 LMA or at both the chaining point as well as level-2 LMA. Charging support may or may not be a requirement at the chaining point and will depend up on whether SIPTO is enabled.

4.2.2. PMIPv6 to S2a Chaining with RFC compatible Level-1 LMA & s2a (PMIPv6 or GTPv2) towards 3GPP EPC

In this model, the chaining point provides a 3GPP complaint S2a interface towards the packet core for trusted WLAN to EPC integration. S2a interface may use either PMIPv6 or GTPv2 protocol. In the model, for the secured WLANs (SSIDs), which are configured for SIM, based authentication for Mobile offload, the level-1 gateway, which performs the chaining, may act as the 3GPP AAA proxy as well. Alternatively some deployments may use an out of band authentication model and the intermediate gateway does not perform and AAA proxy functions. The ability for the intermediate gateway to perform AAA proxy functions are more relevant when diameter based authentication support is required for packet core integration. For this scenario, the WLC will be forwarding EAP messages over RADIUS and the intermediate gateway will provide a diameter AAA interface towards a 3GPP AAA server. This model is illustrated in Figure 7. This model can simultaneously support a combination of mobile data offload and non-offload scenarios as described below:

Open SSID and Web Portal based authentication: Intermediate gateway, which will also be the WAG, will have an interface towards a local PCRF and may use RADIUS or DIAMETER interface. IP address assignment will be managed by the intermediate gateway.

Secured SSID and NSWO: For this use case, Mobile operator's subscribers will get authenticated using one of the SIM based authentication methods, but UE data will not be offloaded to the packet core. Instead the intermediate gateway will perform SIPTO of all the subscriber traffic. UE address assignment will be managed by the intermediate gateway.

Secured SSID and Packet Core Integration: For this use case, Mobile operator's subscribers will get authenticated using one of the SIM based authentication methods and S2a (over PMIPv6 or GTPv2) will be used to tunnel the UE traffic towards a P-GW in the packet core. Some deployments also may implement flow based SIPTO for the UE traffic at the intermediate gateway. UE address assignment will be managed by the P-GW.

```
                                 +----+     +-------+
                                 |PCRF|     |BILLING|
                                 +-+--+     +--+----+
                                   |           |
                                   |           |
                                   |           |            xxx
                                   +---------+ |          xx  xxx
                                             | |         xx     xx
                                             | |       xx         xx
                                             | |       x           xx
               +------+      +---+          ++++-+     x            x
   +--+ CAPWAP | WLC  |PMIPv6|LMA| S2a      |    |    xx  MOBILE    x
   |AP+--------+  +   +------+ + +---------+|P-GW+----+     NW      x
   +--+        | MAG  |      |MAG| PMIPv6 / |    |    xx            x
               +------+      +-+-+  GTPv2   +----+     x  RESOURCES x
                               |                       xx           x
                             NSWO/                      xxx        x
                             SIPTO                       xxxx  xxx
                               |                             xxx
                            xxx+xxxxx
                           xx       xxx
                          xx          x
                          x           xx
                          x LOCALIZED  x
                          x  SERVICES  x
                          x            x
                          xx          xx
                           xxxx     xxx
                              xxxxxxx
```

Figure 7: PMIPv6 to S2a Chaining

5. Deployment Considerations

This section covers deployment considerations for PMIPv6 based SP Wi-Fi Architecture Models. Key areas are covered in the following sub-sections.

5.1. IP addressing Considerations

PMIPv6 supports IPv4, IPv6 and dual stack addressing for UEs. For all deployment models, LMA manages the address assignment for the UEs. For the chaining scenarios, depending up on the deployment use cases, the address assignment may be handled by the intermediate gateways (level 1 LMAs) or the level-2 gateway (LMA and or P-GW). LMA may either use a locally defined pool or it works with an external DHCP server for address assignment.

For IPv4 addressing, the MAG acts as a DHCP server and completes the LMA assigned IP address to the UE via DHCP messages. It is important to provide protocol configuration options (PCOs) such as domain name, DNS server address etc. to the UE. LMA can provide these PCOs in the PBA message and MAG in turn can pass the same to the UE via DHCP message along with the client IP address.

For IPv6 addressing, it is a general practice in SP Wi-Fi deployments to assign a dedicated prefix per UE. In order for this dedicated prefix assignment to work, MAG must support unicast RA as defined in RFC 6085. MAG may use either DHCPv6 or SLAAC for prefix assignment. SLAAC is the preferred option since it is universally supported by various UEs compared to DHCPv6. If SLAAC is the option used for prefix assignment, MAG should use "Recursive DNS Server" Option and "DNS Search List" Options, specified in RFC 6106 for providing the DNS configuration using IPv6 messages.

5.2. Access Authentication & User Identity

As briefly mentioned in the previous section, the access authentication mechanisms depend up on the particular deployment use case. For metro Wi-Fi model deployments and other indoor / outdoor Wi-Fi deployments, web portal based authentication is very commonly used. A common web portal based authentication scenario is an existing subscriber presenting the user id and the password credential to a web login page before he can access the Internet. There are various to this model out there such as new user accessing the network and signing up for subscription based or one time usage services, or users leveraging vouchers for access which will impose time and or quota limit etc.

Another common user authentication scenario implemented in many metro

Wi-Fi deployments is automatic authentication based up on mac address. This model allows an existing subscriber to register one or more mac-addresses for automatic access When the subscriber tries access the Wi-Fi network for the first time from a UE device subscriber will have to go through a portal based authentication and the system captures the mac-address of the device at that time so that the subsequent access will allow automatic access from that UE device.

For secured SSIDs an 802.1X based authentication mechanism will be in place. Even though most of the Wi-Fi deployments out there rely on open SSIDs except for Mobile data offload use cases, it is the intent of the industry to move towards secured SSIDs and implement some EAP based authentication mechanisms. 802.1x based authentication will be requirement for Hotspot 2.0 compliance. For mobile data offload scenarios, secure SSIDs with SIM card based authentication will be in use.

PMIPv6 protocol allows the access network to pass the user identity such as mac-address, NAI, IMSI etc. towards the network side GW (LMA/WAG or LMA/P-GW) through the PMIPv6 control messages. With this standardized user identity presentation, there is no need to rely on alternative proprietary options.

5.3. Policy Provisioning & Enforcement

Policy provisioning systems referred to as PCRF in the 3GPP terminology is the entity which decides what kind of services a specific subscriber can get and for what duration, what kind of charging polices are applicable to the subscriber etc. Depending up on the deployment model, the gateways talk to the PCRF entity either using diameter interface (typically Gx) or RADIUS interface. RADIUS interface is more common in WAG deployments, which do not handle 3GPP packet core integration, and diameter is typically used in 3GPP packet core elements such as P-GW. Use of diameter for PCRF integration in non-3GPP deployments is also possible even though not common. WAG/LMA or P-GW acts as the policy enforcement point and works in conjunction with PCRF.

5.4. Charging Considerations

Accounting and Charging in service provider Wi-Fi deployments fall under two broad categories a) Diameter based and b) RADIUS based. Diameter based charging will be leveraged for Architecture models, which use one or more 3GPP, network elements. RADIUS based charging will be leveraged for the deployment models, which typically does not involve packet core integration.

Diameter based charging leverages diameter protocol for the charging interfaces. Diameter based charging architecture and the associated interfaces are defined in 3GPP standards. Charging in 3GPP can be broadly classified into two categories a) Offline Charging and b) Online Charging. In offline charging, resource usage is reported by the network element to the billing system after the resource usage has occurred. For online charging, authorization for the network resource usage, must be obtained by the network prior to the actual resource usage will be allowed.

Online charging maps to pre-paid charging use cases and offline charging maps to post-paid charging use cases. Pre-paid and post-paid charging is supported by RADIUS based charging models as well. Charging information can be collected from various points in the Wi-Fi network such as WLAN access network, MAG, chaining point LMA/ P-GW etc. The type of charging and the required charging interfaces will depend up on the particular use case model.

5.5. Legal Intercept

Legal Intercept stands for legally authorized capture & delivery of subscriber communications data by a communications provider to a law enforcement agency (LEA). The communications data, which the LEA will intercept as part of the target subscriber surveillance, is classified into two types, Communication Content (CC) and Intercept Related Information (IRI). CC is the bearer data exchanged to and from the subscriber. IRI provides the relevant context information for the CC. IRI is a loosely defined term and the scope varies for different end user applications.

In most of the countries, there are legal obligations for Service Providers to facilitate the intercept of any subscriber's communication, if requested by law enforcement agencies. Communications Assistance for Law Enforcement Act (CALEA), the United States wiretapping law passed in 1994 is an example for such legal mandates.

For various SP Wi-Fi deployment models covered in this document, legal intercept will be a requirement and one or more network elements in the system should support the Intercept and forwarding or IRI, CC or both to the LI mediation systems which in turn will provide the intercepted information to law enforcement agencies

5.6. SIPTO Considerations

Depending up on the deployment use case, SIPTO may be desirable use case for flat as well as hierarchical models. For the flat models, SIPTO can be implemented at the MAG itself. With chaining model

SIPTO can be done either at the level-1MAG or the intermediate gateway doing the chaining.

6. IANA Considerations

This specification does not require any IANA actions.

7. Security Considerations

All the security considerations from the base Proxy Mobile IPv6 specifications, [RFC5213] and [RFC5844], apply equally well to Proxy Mobile IPv6 domains supporting IEEE 802.11-based access networks. The support for IEEE 802.11-based access networks does not require any new security considerations and does not introduce any new security vulnerabilities known at this time.

8. Acknowledgements

The author of this document thanks the members of the NETLMM working group for all the discussions related to this topic.

9. References

9.1. 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.

[RFC5779] Korhonen, J., Bournelle, J., Chowdhury, K., Muhanna, A., and U. Meyer, "Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server", RFC 5779, February 2010.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

[RFC6085] Gundavelli, S., Townsley, M., Troan, O., and W. Dec, "Address Mapping of IPv6 Multicast Packets on Ethernet", RFC 6085, January 2011.

9.2. Informative References

[I-D.liebsch-netext-pmip6-authiwk]
Gundavelli, S., Liebsch, M., and P. Seite, "PMIPv6 inter-working with WiFi access authentication", draft-liebsch-netext-pmip6-authiwk-05 (work in progress), September 2012.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

[RFC5845] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung, "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6", RFC 5845, June 2010.

[RFC5846] Muhanna, A., Khalil, M., Gundavelli, S., Chowdhury, K., and P. Yegani, "Binding Revocation for IPv6 Mobility", RFC 5846, June 2010.

[RFC6224] Schmidt, T., Waehlisch, M., and S. Krishnan, "Base Deployment for Multicast Listener Support in Proxy Mobile

IPv6 (PMIPv6) Domains", RFC 6224, April 2011.

[RFC6475] Keeni, G., Koide, K., Gundavelli, S., and R. Wakikawa, "Proxy Mobile IPv6 Management Information Base", RFC 6475, May 2012.

[RFC6572] Xia, F., Sarikaya, B., Korhonen, J., Gundavelli, S., and D. Damic, "RADIUS Support for Proxy Mobile IPv6", RFC 6572, June 2012.

Authors' Addresses

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

Byju Pularikkal
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: byjupg@cisco.com

Rajeev Koodli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: rcoodli@cisco.com