Network Working Group
Internet-Draft
Expires: October 29, 2007

M-K. Shin, Ed.
ETRI
Y-H. Han
KUT
S-E. Kim
KT
D. Premec
Siemens Mobile
April 27, 2007

IPv6 Deployment Scenarios in 802.16 Networks
draft-ietf-v6ops-802-16-deployment-scenarios-04

Status of this Memo

Copyright Notice

Abstract

This document provides a detailed description of IPv6 deployment and integration methods and scenarios in wireless broadband access networks in coexistence with deployed IPv4 services. In this document we will discuss main components of IPv6 IEEE 802.16 access networks and their differences from IPv4 IEEE 802.16 networks and how IPv6 is deployed and integrated in each of the IEEE 802.16 technologies.

Table of Contents

1. Introduction

As the deployment of IEEE 802.16 access networks progresses, users will be connected to IPv6 networks. While the IEEE 802.16 standard defines the encapsulation of an IPv4/IPv6 datagram in an IEEE 802.16 MAC payload, a complete description of IPv4/IPv6 operation and deployment is not present. The IEEE 802.16 standards are limited to L1 and L2, so they may be used within any number of IP network architectures and scenarios. In this document, we will discuss main components of IPv6 IEEE 802.16 access networks and their differences from IPv4 IEEE 802.16 networks and how IPv6 is deployed and integrated in each of the IEEE 802.16 technologies.

This document extends the work of [RFC4779] and follows the structure and common terminology of that document.

1.1. Terminology

The IEEE 802.16 related terminologies in this document are to be interpreted as described in [I-D.ietf-16ng-ps-goals].

- Subscriber Station (SS): An end-user equipment that provides connectivity to the 802.16 networks. It can be either fixed/ nomadic or mobile equipment. In mobile environment, SS represents the Mobile Subscriber Station (MS) introduced in [IEEE802.16e].

- Base Station (BS): A generalized equipment sets providing connectivity, management, and control between the subscriber station and the 802.16 networks.

- Access Router (AR): An entity that performs an IP routing function to provide IP connectivity for subscriber station (SS or MS).

- Connection Identifier (CID): A 16-bit value that identifies a connection to equivalent peers in the 802.16 MAC of the SS(MS) and BS.

- Ethernet CS: It means 802.3/Ethernet CS specific part of the Packet CS defined in 802.16 STD.

- IPv6 CS: It means IPv6 specific subpart of the Packet CS, Classifier 2 (Packet, IPv6) defined in 802.16 STD.

2. Deploying IPv6 in IEEE 802.16 Networks

2.1. Elements of IEEE 802.16 Networks

The mechanism of transporting IP traffic over IEEE 802.16 networks is outlined in [IEEE802.16]. [IEEE802.16] only specifies the convergence sublayers and the ability to transport IP over the air interface. The details of IPv6 (and IPv4) operations over IEEE 802.16 are being discussed now in the 16ng WG.

Here are some of the key elements of an IEEE 802.16 network. Figure 1 illustrates the key elements of typical mobile 802.16 deployments.

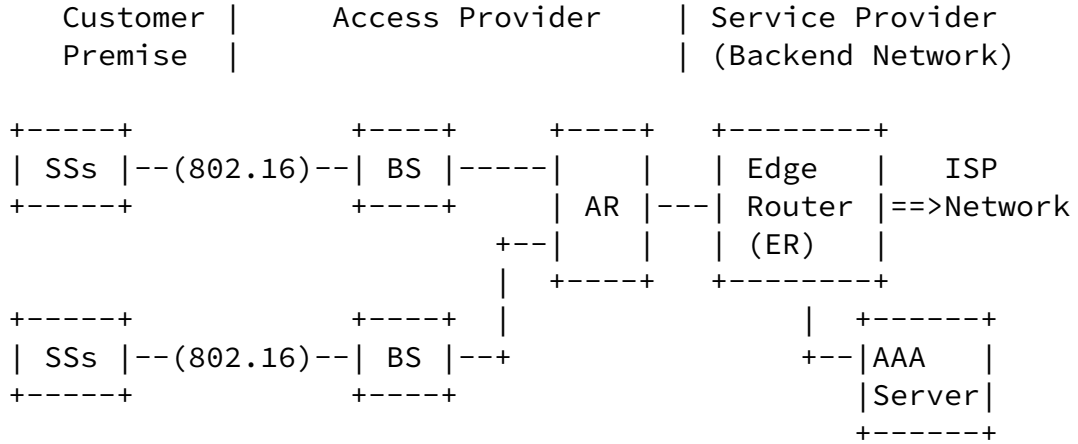


Figure 1: Key Elements of IEEE 802.16(e) Networks

2.2. Scenarios and IPv6 Deployment

[IEEE802.16] specifies two modes for sharing the wireless medium: point-to-multipoint (PMP) and mesh (optional). This document only focuses on the PMP mode.

Some of the factors that hinder deployment of native IPv6 core protocols are already introduced by [I-D.ietf-16ng-ps-goals].

There are two different deployment scenarios: fixed and mobile access deployment scenarios. A fixed access scenario substitutes for existing wired-based access technologies such as digital subscriber lines (xDSL) and cable networks. This fixed access scenario can provide nomadic access within the radio coverages, which is called Hot-zone model. A mobile access scenario exists for the new paradigm of transmitting voice, data and video over mobile networks. This scenario can provide high speed data rates equivalent to the wire-based Internet as well as mobility functions equivalent to cellular systems. The mobile access scenario can be classified into two different IPv6 link models: shared IPv6 prefix link model and point-

to-point link model.

2.2.1. Mobile Access Deployment Scenarios

Unlike IEEE 802.11, the IEEE 802.16 BS can provide mobility functions and fixed communications. [IEEE802.16e] has been standardized to provide mobility features on IEEE 802.16 environments. IEEE 802.16 BS might be deployed with a proprietary backend managed by an operator. Some architectural characteristics of IEEE 802.16 networks may affect the detailed operations of NDP [RFC2461], [RFC2462].

There are two possible IPv6 link models for mobile access deployment scenarios: shared IPv6 prefix link model and point-to-point link model [I-D.ietf-16ng-ipv6-link-model-analysis]. There is always a default access router in the scenarios. There can exist multiple hosts behind an MS (networks behind an MS may exist). The mobile access deployment models, Mobile WiMax and WiBro, fall within this deployment model.

1. Shared IPv6 Prefix Link Model

This link model represents the IEEE 802.16 mobile access network

deployment where a subnet consists of only single AR interfaces and multiple MSs. Therefore, all MSs and corresponding AR interfaces share the same IPv6 prefix as shown in Figure 2. The IPv6 prefix will be different from the interface of the AR.

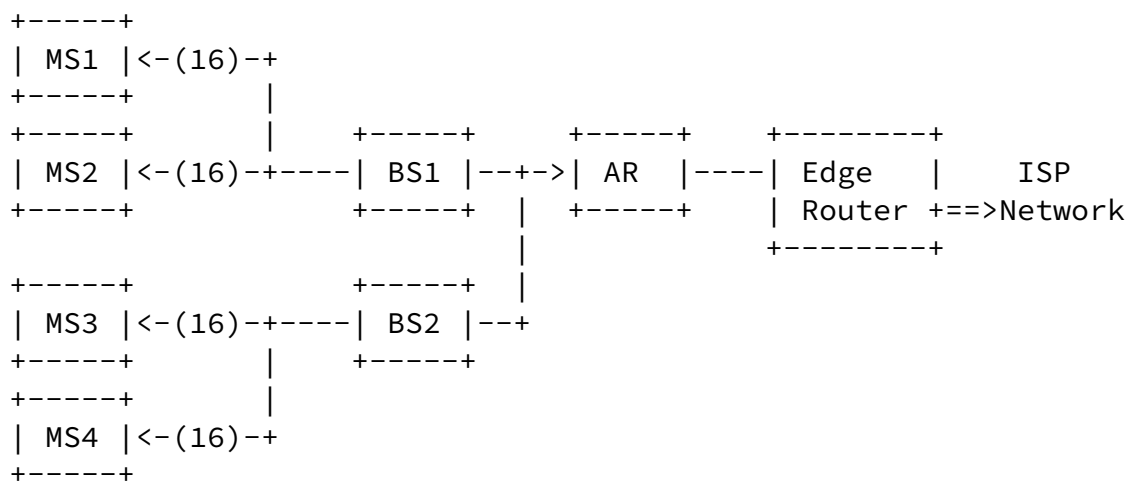
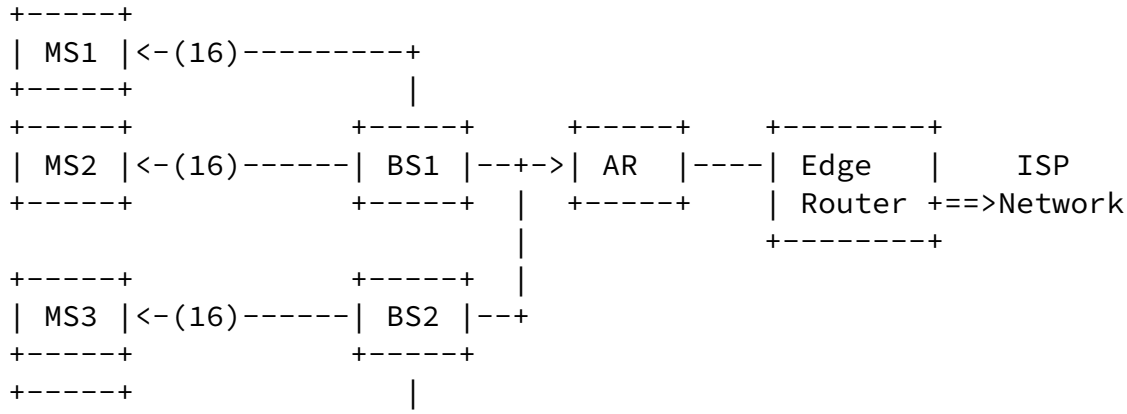


Figure 2: Shared IPv6 Prefix Link Model

2. Point-to-Point Link Model

This link model represents IEEE 802.16 mobile access network deployments where a subnet consists of only single AR, BS and MS. That is, each connection to a mobile node is treated as a single

link. Each link between the MS and the AR is allocated a separate, unique prefix or unique set of prefixes by the AR. The point-to-point link model follows the recommendations of [RFC3314].



```
| MS4 |<-(16)---------+
+-----+
```

Figure 3: Point-to-Point Link Model

2.2.1.1. IPv6 Related Infrastructure Changes

IPv6 will be deployed in this scenario by upgrading the following devices to dual-stack: MS, AR and ER. In this scenario, IEEE 802.16 BSs have only MAC and PHY layers without router functionality and operate as a bridge. The BS should support IPv6 classifiers as specified in [IEEE802.16]. However, if IPv4 stack is loaded to them for management and configuration purposes, it is expected that BS should be upgraded by implementing IPv6 stack, too.

2.2.1.2. Addressing

An IPv6 MS has two possible options to get an IPv6 address. These options will be equally applied to the other scenario below (Section 2.2.2).

1. An IPv6 MS can get the IPv6 address from an access router using stateless auto-configuration. In this case, router discovery and DAD operation should be properly operated over an IEEE 802.16 link.

2. An IPv6 MS can use DHCPv6 to get an IPv6 address from the DHCPv6 server. In this case, the DHCPv6 server would be located in the service provider core network and the AR should provide a DHCPv6 relay agent. This option is similar to what we do today in case of DHCPv4.

In this scenario, a router and multiple BSs form an IPv6 subnet and a single prefix is allocated to all the attached MSs. All MSs attached

to same AR can be on the same IPv6 link.

As for the prefix assignment, in case of the shared IPv6 prefix link model, one or more IPv6 prefixes are assigned to the link and hence shared by all the nodes that are attached to the link. In the point-to-point link model, the AR assigns a unique prefix or a set of unique prefixes for each MS. Prefix delegation can be required if networks exist behind an MS.

2.2.1.3. IPv6 Transport

In an IPv6 subnet, there are always two underlying links: one is the IEEE 802.16 wireless link between the MS and BS, and the other is a wired link between the BS and AR.

If stateless auto-configuration is used to get an IPv6 address, router discovery and DAD operation should be properly operated over IEEE 802.16 links. In case of the shared IPv6 prefix link model, the DAD [RFC2461] does not adapt well to the 802.16 air interface as there is no native multicast support. An optimization, called Relay DAD, may be required to perform DAD. However, in case of the point-to-point link model, DAD is easy since each connection to a MN is treated as a unique IPv6 link.

Note that in this scenario IPv6 CS [I-D.ietf-16ng-ipv6-over-ipv6cs] may be more appropriate than Ethernet CS [I-D.ietf-16ng-ip-over-ethernet-over-802.16] to transport IPv6 packets, since there is some overhead of Ethernet CS (e.g., Ethernet header) under mobile access environments. However, when PHS (Payload Header Suppression) is deployed it mitigates this overhead through the compression of packet headers.

Simple or complex network equipment may constitute the underlying wired network between the AR and the ER. If the IP-aware equipment between the AR and the ER does not support IPv6, the service providers can deploy IPv6-in-IPv4 tunneling mechanisms to transport IPv6 packets between the AR and the ER.

The service providers are deploying tunneling mechanisms to transport IPv6 over their existing IPv4 networks as well as deploying native IPv6 where possible. Native IPv6 should be preferred over tunneling mechanisms as native IPv6 deployment options might be more scalable and provide the required service performance. Tunneling mechanisms should only be used when native IPv6 deployment is not an option. This can be equally applied to other scenarios below (Section 2.2.2).

2.2.1.4. Routing

In general, the MS is configured with a default route that points to the AR. Therefore, no routing protocols are needed on the MS. The MS just sends to the AR using the default route.

The AR can configure multiple links to ER for network reliability. The AR should support IPv6 routing protocols such as OSPFv3 [RFC2740] or IS-IS for IPv6 when connected to the ER with multiple links.

The ER runs the IGP such as OSPFv3 or IS-IS for IPv6 in the service provider network. The routing information of the ER can be redistributed to the AR. Prefix summarization should be done at the ER.

2.2.1.5. Mobility

As for mobility management, the movement between BSs is handled by Mobile IPv6 [RFC3775], if it requires a subnet change. Also, in certain cases (e.g., fast handover [I-D.ietf-mipshop-fmipv6-rfc4068bis]) the link mobility information must be available for facilitating the layer 3 handoff procedure.

Mobile IPv6 defines that movement detection uses Neighbor Unreachability Detection to detect when the default router is no longer bidirectionally reachable, in which case the mobile node must discover a new default router. Periodic Router Advertisements for reachability and movement detection may be unnecessary because the IEEE 802.16 MAC provides the reachability by its Ranging procedure and the movement detection by the Handoff procedure.

IEEE 802.16 defines L2 triggers in case the refresh of an IP address is required during the handoff. Though a handoff has occurred, an additional router discovery procedure is not required in case of intra-subnet handoff. Also, faster handoff may occur by the L2 trigger in case of inter-subnet handoff.

Also, [IEEE802.16g] which is under-developed defines L2 triggers for link status such as link-up, link-down, handoff-start. These L2 triggers may make the Mobile IPv6 procedure more efficient and faster. In addition, Mobile IPv6 Fast Handover assumes the support from link- layer technology, but the particular link-layer information being available, as well as the timing of its availability (before, during or after a handover has occurred), differs according to the particular link-layer technology in use. This issue is also being discussed in [I-D.ietf-mipshop-fh80216e].

In addition, due to the problems caused by the existence of multiple

convergence sublayers [RFC4840], the mobile access scenarios need solutions about how roaming will work when forced to move from one CS to another (e.g., IPv6 CS to Ethernet CS). Note that, at this phase this issue is the out of scope of this document. It should be also discussed in the 16ng WG.

2.2.2. Fixed/Nomadic Deployment Scenarios

The IEEE 802.16 access networks can provide plain Ethernet end-to-end connectivity. Wireless DSL deployment model is an example of a fixed/nomadic IPv6 deployment of IEEE 802.16. Many wireless Internet service providers (Wireless ISPs) have planned to use IEEE 802.16 for the purpose of high quality broadband wireless services. A company can use IEEE 802.16 to build up a mobile office. Wireless Internet spreading through a campus or a cafe can be also implemented with it. The distinct point of this use case is that it can use the unlicensed (2.4 & 5 GHz) band as well as the licensed (2.6 & 3.5GHz) band. By using the unlicensed band, an IEEE 802.16 BS might be used just as a wireless switch/hub which a user purchases to build a private wireless network in his/her home or laboratory.

Under fixed access model, the IEEE 802.16 BS will be deployed using an IP backbone rather than a proprietary backend like cellular systems. Thus, many IPv6 functionalities such as [RFC2461], [RFC2462] will be preserved when adopting IPv6 to IEEE 802.16 devices.

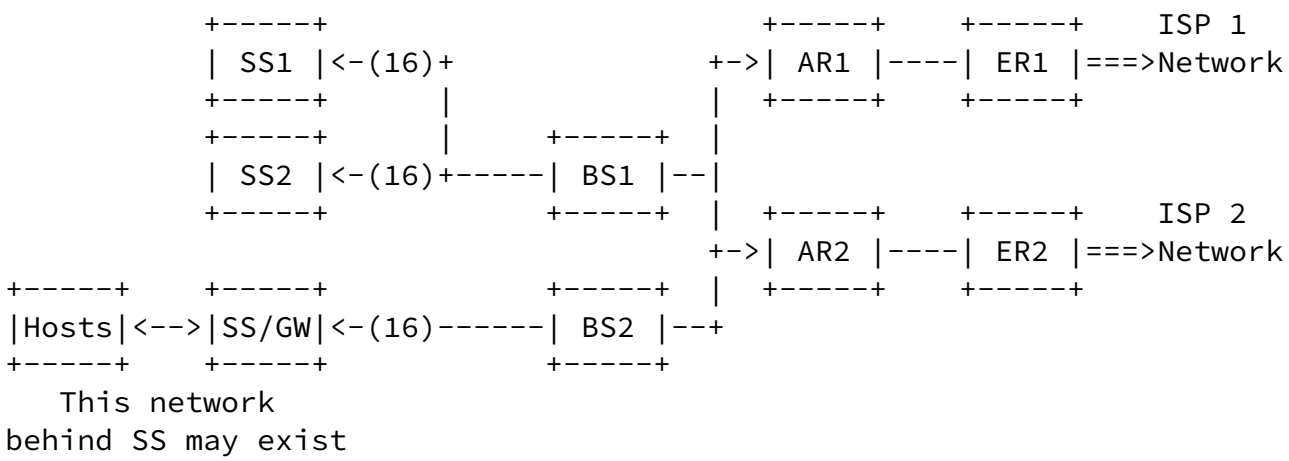


Figure 4: Fixed/Nomadic Deployment Scenario

This scenario also represents IEEE 802.16 network deployment where a subnet consists of multiple MSs and multiple interfaces of the multiple BSs. Multiple access routers can exist. There exist multiple hosts behind an SS (networks behind an SS may exist). When

802.16 access networks are widely deployed as in a WLAN, this case should be also considered. The Hot-zone deployment model falls

within this case.

While Figure 4 illustrates a generic deployment scenario, the following Figure 5 shows in more detail how an existing DSL ISP would integrate the 802.16 access network into its existing infrastructure.

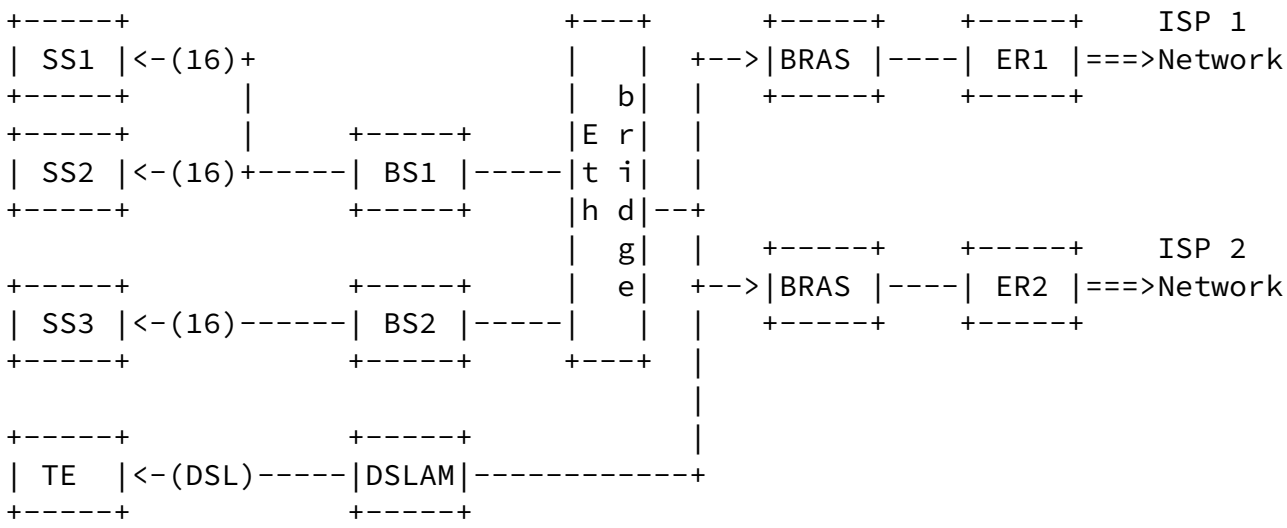


Figure 5: Integration of 802.16 access into DSL infrastructure

In this approach the 802.16 BS is acting as a DSLAM (Digital Subscriber Line Access Multiplexer). On the network side, the BS is connected to an Ethernet bridge which can be separate equipment or integrated into the BRAS (Broadband Remote Access Server).

2.2.2.1. IPv6 Related Infrastructure Changes

IPv6 will be deployed in this scenario by upgrading the following devices to dual-stack: MS, AR, ER, and the Ethernet Bridge. The BS should support IPv6 classifiers as specified in [IEEE802.16]. However, if a IPv4 stack is loaded to them for management and configuration purpose, it is expected that the BS should be upgraded by implementing an IPv6 stack, too.

The BRAS in Figure 5 is providing the functionality of the AR. An Ethernet bridge is necessary for protecting the BRAS from 802.16 link

layer peculiarities. The Ethernet bridge relays all traffic received through the BS to its network side port(s) connected to the BRAS. Any traffic received from the BRAS is relayed to the appropriate BS. Since the 802.16 MAC layer has no native support for multicast (and broadcast) in the uplink direction, the Ethernet bridge will implement multicast (and broadcast) by relaying the multicast frame received from the MS to all of its ports. The Ethernet bridge may also provide some IPv6 specific functions to increase link efficiency of the 802.16 radio link (see Section 2.2.2.3).

2.2.2.2. Addressing

One or more IPv6 prefixes can be shared to all the attached MSs. Prefix delegation can be required if networks exist behind the SS.

2.2.2.3. IPv6 Transport

Note that in this scenario Ethernet CS [I-D.ietf-16ng-ip-over-ethernet-over-802.16] may be more appropriate than IPv6 CS [I-D.ietf-16ng-ipv6-over-ipv6cs] to transport IPv6 packets, since the scenario needs to support plain Ethernet end-to-end connectivity. However, the IPv6 CS can also be supported. The MS and BS will consider the connections between the peer IP CSs at the MS and BS to form a point to point link. In the Ethernet CS case, an Ethernet bridge may provide implementation of an authoritative address cache and Relay DAD. An Authoritative address cache is a mapping between the IPv6 address and the MAC addresses of all attached MSs.

The bridge builds its authoritative address cache by parsing the IPv6 Neighbor Discovery messages used during address configuration (DAD). Relay DAD means that the Neighbor Solicitation message used in the DAD process will be relayed only to the MS which already has configured the solicited address as its own address (if such an MS exist at all).

2.2.2.4. Routing

In this scenario, IPv6 multi-homing considerations exist. For example, if there exist two routers to support MSs, a default router must be selected.

The Edge Router runs the IGP used in the SP network such as OSPFv3

[RFC2740] or IS-IS for IPv6. The connected prefixes have to be redistributed. Prefix summarization should be done at the Edge Router.

2.2.2.5. Mobility

No mobility functions are supported in the fixed access scenario. However, mobility can be supported in the radio coverage without any mobility protocol like WLAN technology. Therefore, a user can access Internet nomadically in the coverage.

2.3. IPv6 Multicast

In IEEE 802.16 air link, downlink connections can be shared among multiple MSs, enabling multicast channels with multiple MSs receiving the same information from the BS. Multicast and Broadcast Service

(MBS) may be used to efficiently implement multicast. However, it is not clear how to do this, as currently CID is assigned by BS, but in MBS it should be done at an AR and it's network scope. It is not clear how this mapping will happen for MBS, so MBS discussions have been postponed in WiMax for now. Note that it should be intensively researched later, since MBS will be one of the killer services in IEEE 802.16 networks.

In order to support multicast services in IEEE 802.16, Multicast Listener Discovery (MLD) [RFC2710] must be supported between the MS and AR. Also, the inter-working with IP multicast protocols and MBS should be considered.

MBS defines Multicast and Broadcast Services, but actually, MBS seems to be a broadcast service, not multicasting. MBS adheres to broadcast services, while traditional IP multicast schemes define multicast routing using a shared tree or source-specific tree to deliver packets efficiently.

In IEEE 802.16 networks, two types of access to MBS may be supported: single-BS access and multi-BS access. Therefore, these two types of services may be roughly mapped into Source-Specific Multicast.

2.4. IPv6 QoS

In IEEE 802.16 networks, a connection is unidirectional and has a QoS specification. The 802.16 supported QoS has different semantics from IP QoS (e.g., diffserv). Mapping CID to Service Flow IDentifier (SFID) defines QoS parameters of the service flow associated with that connection. In order to interwork with IP QoS, IP QoS (e.g., diffserv, or flow label for IPv6) mapping to IEEE 802.16 link specifics should be provided.

2.5. IPv6 Security

When initiating the connection, an MS is authenticated by the AAA server located at its service provider network. All the parameters related to authentication (username, password and etc.) are forwarded by the BS to the AAA server. The AAA server authenticates the MSs and when an MS is once authenticated and associated successfully with BS, IPv6 an address will be acquired by the MS through stateless autoconfiguration or DHCPv6. Note the initiation and authentication process is the same as used in IPv4.

IPsec is a fundamental part of IPv6. Unlike IPv4, IPsec for IPv6 may be used within the global end-to-end architecture. But, we do not have PKIs across organizations and IPsec is not integrated with IEEE 802.16 network mobility management.

IEEE 802.16 network threats may be different from IPv6 and IPv6 transition threat models [I-D.ietf-v6ops-security-overview]. It should be also discussed.

2.6. IPv6 Network Management

[IEEE802.16f] includes the management information base for IEEE 802.16 networks. For IPv6 network management, the necessary instrumentation (such as MIBs, NetFlow Records, etc) should be available.

Upon entering the network, an MS is assigned three management connections in each direction. These three connections reflect the three different QoS requirements used by different management levels. The first of these is the basic connection, which is used for the transfer of short, time-critical MAC management messages and radio link control (RLC) messages. The primary management connection is used to transfer longer, more delay-tolerant messages such as those

used for authentication and connection setup. The secondary management connection is used for the transfer of standards-based management messages such as Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Simple Network Management Protocol (SNMP).

IPv6 based IEEE 802.16 networks can be managed by IPv4 or IPv6 when network elements are implemented dual stack. For example, network management systems (NMS) can send SNMP messages by IPv4 with IPv6 related object identifiers. Also, an NMS can use IPv6 for SNMP requests and responses including IPv4 related OID.

3. IANA Considerations

This document requests no action by IANA.

4. Security Considerations

Please refer to Section 2.5 "IPv6 Security" technology sections for details.

5. Acknowledgements

This work extends v6ops work on [RFC4779]. We thank all the authors of the document. Special thanks are due to Maximilian Riegel, Jonne Soininen, Brian E Carpenter, Jim Bound, David Johnston, Basavaraj Patil, Byoung-Jo Kim, Eric Klein, Bruno Sousa, Jung-Mo Moon, Sangjin Jeong, and Jinhyeock Choi for extensive review of this document. We acknowledge Dominik Kaspar for proofreading the document.

6. References

6.1. Normative References

[RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC4779] Asadullah, S., Ahmed, A., Popoviciu, C., Savola, P., and J. Palet, "ISP IPv6 Deployment Scenarios in Broadband Access Networks", RFC 4779, January 2007.

6.2. Informative References

[RFC2740] Coltun, R., Ferguson, D., and J. Moy, "OSPF for IPv6", RFC 2740, December 1999.

[RFC3314] Wasserman, M., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4840] Aboba, B., Davies, E., and D. Thaler, "Multiple Encapsulation Methods Considered Harmful", RFC 4840, April 2007.

[I-D.ietf-16ng-ps-goals] Jee, J., "IP over 802.16 Problem Statement and Goals", draft-ietf-16ng-ps-goals-01 (work in progress), February 2007.

[I-D.ietf-16ng-ipv6-link-model-analysis]
Madanapalli, S., "Analysis of IPv6 Link Models for 802.16 based Networks", draft-ietf-16ng-ipv6-link-model-analysis-03 (work in progress), February 2007.

[I-D.ietf-16ng-ipv6-over-ipv6cs]
Patil, B., "IPv6 Over the IP Specific part of the Packet

Convergence sublayer in 802.16 Networks", draft-ietf-16ng-ipv6-over-ipv6cs-09 (work in progress), April 2007.

[I-D.ietf-16ng-ip-over-ethernet-over-802.16]
Jeon, H., "Transmission of IP over Ethernet over IEEE 802.16 Networks", draft-ietf-16ng-ip-over-ethernet-over-802.16-01 (work in progress), March 2007.

[I-D.ietf-mipshop-fmipv6-rfc4068bis]
Koodli, R., "Fast Handovers for Mobile IPv6", draft-ietf-mipshop-fmipv6-rfc4068bis-01 (work in progress), March 2007.

[I-D.ietf-mipshop-fh80216e]
Jang, H., "Mobile IPv6 Fast Handovers over IEEE 802.16e Networks", draft-ietf-mipshop-fh80216e-01 (work in progress), January 2007.

[I-D.ietf-v6ops-security-overview]
Davies, E., "IPv6 Transition/Co-existence Security Considerations", draft-ietf-v6ops-security-overview-06 (work in progress), October 2006.

[IEEE802.16]
"IEEE 802.16-2004, IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems", October 2004.

[IEEE802.16e]
"IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband

Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1", February 2006.

[IEEE802.16g]
"Draft Amendment to IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Management Plane Procedures and Services", January 2007.

[IEEE802.16f]
"Amendment to IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Management Information Base",

December 2005.

Authors' Addresses

Myung-Ki Shin
ETRI
161 Gajeong-dong Yuseng-gu
Daejeon, 305-350
Korea

Phone: +82 42 860 4847
Email: myungki.shin@gmail.com

Youn-Hee Han
KUT
Gajeon-Ri 307 Byeongcheon-Myeon
Cheonan-Si Chungnam Province, 330-708
Korea

Email: yhhan@kut.ac.kr

Sang-Eon Kim
KT
17 Woomyeon-dong, Seocho-gu
Seoul, 137-791
Korea

Email: sekim@kt.co.kr

Domagoj Premec
Siemens Mobile
Heinzelova 70a
10010 Zagreb
Croatia

Email: domagoj.premec@siemens.com

Full Copyright Statement

OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).