Network Working Group
Request for Comments: 5181
Category: Informational

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

May 2008

IPv6 Deployment Scenarios in 802.16 Networks

Status of This Memo

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 the 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 Media Access Control (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 the 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 [RFC5154].

- 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 a mobile environment, SS represents the Mobile Subscriber Station (MS) introduced in [IEEE802.16e].

- Base Station (BS): A generalized equipment set 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 a 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 (Convergence Sublayer): 802.3/Ethernet CS-specific part of the Packet CS defined in 802.16 STD.

- IPv6 CS (Convergence Sublayer): 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

[IEEE802.16e] is an air interface for fixed and mobile broadband wireless access systems. [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 defined in the 16ng WG. The IPv6 over IPv6 CS definition is already an approved specification [RFC5121]. IP over Ethernet CS in IEEE 802.16 is defined in [IP-ETHERNET].

Figure 1 illustrates the key elements of typical mobile 802.16 deployments.

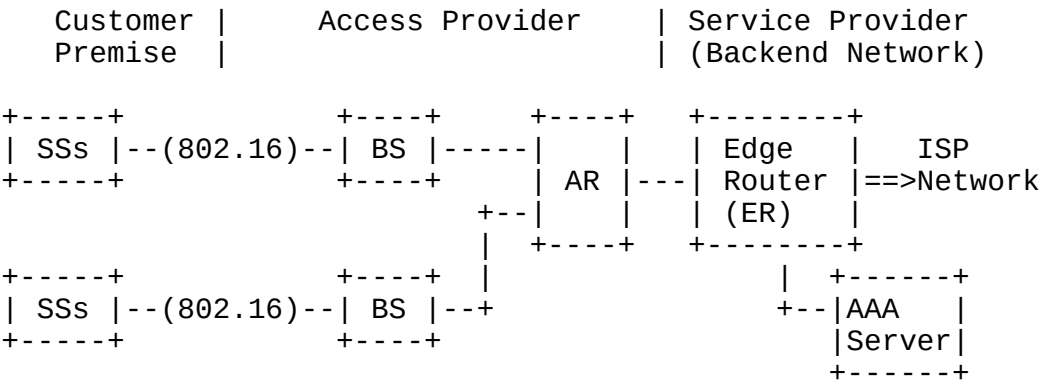

Figure 1: Key Elements of IEEE 802.16(e) Networks

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 [RFC5154].

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 the 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. There are the different IPv6 impacts on convergence sublayer type, link model, addressing, mobility, etc. between fixed and mobile access deployment scenarios. The details will be discussed below. 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.

There are two possible IPv6 link models for mobile access deployment scenarios: shared IPv6 prefix link model and point-to-point link model [RFC4968]. 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.

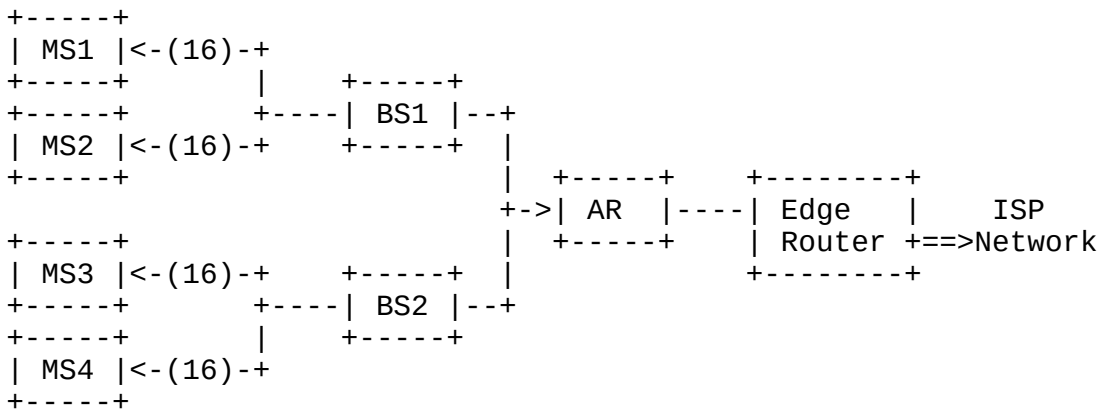

Figure 2: Shared IPv6 Prefix Link Model

(2) Point-to-Point Link Model

This link model represents IEEE 802.16 mobile access network deployments where a subnet consists of only a 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 a set of unique prefixes by the AR. The point-to-point link model follows the recommendations of [RFC3314].

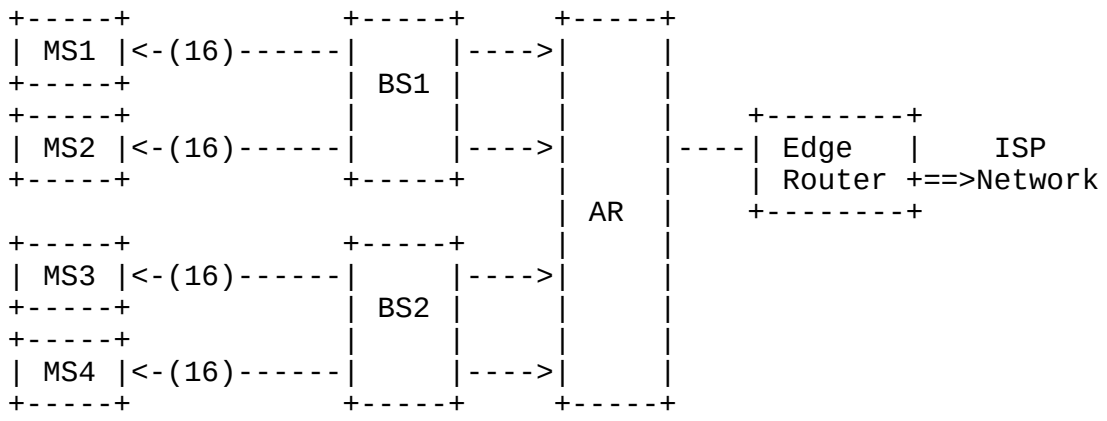

Figure 3: Point-to-Point Link Model

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 (Physical Layer) layers without router functionality and operate as a bridge. The BS should support IPv6 classifiers as specified in [IEEE802.16].

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 Duplicate Address Detection (DAD) operation should be properly operated over an IEEE 802.16 link.

(2) An IPv6 MS can use Dynamic Host Configuration Protocol for IPv6 (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 the same AR can be on the same IPv6 link.

As for the prefix assignment, in the case of the shared IPv6 prefix link model, one or more IPv6 prefixes are assigned to the link and are 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.

IPv6 packets can be sent and received via the IP-specific part of the packet convergence sublayer. The Packet CS is used for the transport of packet-based protocols, which include Ethernet and Internet Protocol (IPv4 and IPv6). Note that in this scenario, IPv6 CS may be more appropriate than Ethernet CS 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. The details of IPv6 operations over the IP-specific part of the packet CS are defined in [RFC5121].

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

The ER runs the Interior Gateway Protocol (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

There are two types of handovers for the IEEE 802.16e networks: link layer handover and IP layer handover. In a link layer handover, BSs involved in the handover reside in the same IP subnet. An MS only needs to reestablish a link layer connection with a new BS without changing its IP configuration, such as its IP address, default router, on-link prefix, etc. The link layer handover in IEEE 802.16e is by nature a hard handover since the MS has to cut off the connection with the current BS at the beginning of the handover process and cannot resume communication with the new BS until the handover completes [IEEE802.16e]. In an IP layer handover, the BSs involved reside in different IP subnets, or in different networks. Thus, in an IP layer handover, an MS needs to establish both a new link layer connection, as in a link layer handover, and a new IP configuration to maintain connectivity.

IP layer handover for MSs is handled by Mobile IPv6 [RFC3775]. 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.

Mobile IPv6 alone will not solve the handover latency problem for the IEEE 802.16e networks. To reduce or eliminate packet loss and to reduce the handover delay in Mobile IPv6, therefore, Fast Handover for Mobile IPv6 (FMIPv6) [RFC4068] can be deployed together with MIPv6. To perform predictive packet forwarding, the FMIPv6's IP layer assumes the presence of handover-related triggers delivered by

the IEEE 802.16 MAC layers. Thus, there is a need for cross-layering design to support proper behavior of the FMIPv6 solution. This issue is also discussed in [MIPSHOP-FH80216E].

Also, [IEEE802.16g] defines L2 triggers for link status such as link-up, link-down, and handoff-start. These L2 triggers may make the Mobile IPv6 or FMIPv6 procedure more efficient and faster.

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.

2.2.2. Fixed/Nomadic Deployment Scenarios

The IEEE 802.16 access networks can provide plain Ethernet end-to-end connectivity. This scenario represents a deployment model using Ethernet CS. A 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 also be implemented with it.

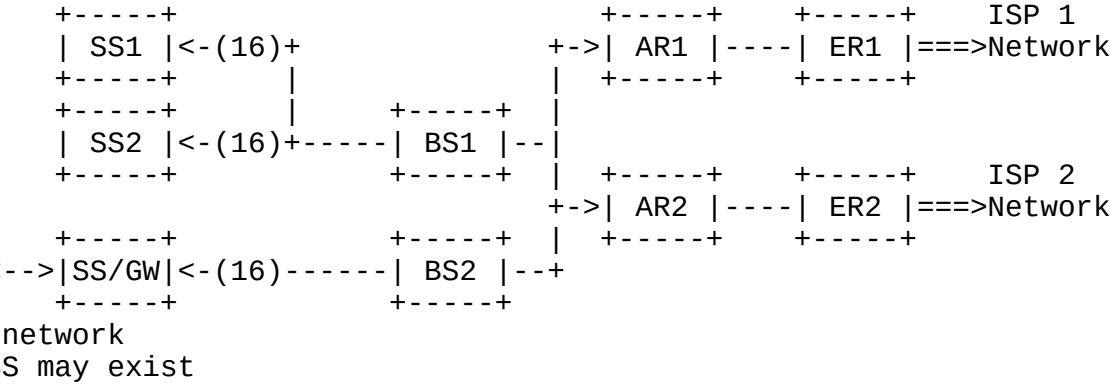

Figure 4: Fixed/Nomadic Deployment Scenario

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 Wireless Local Area Network (WLAN), this case should also be 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.

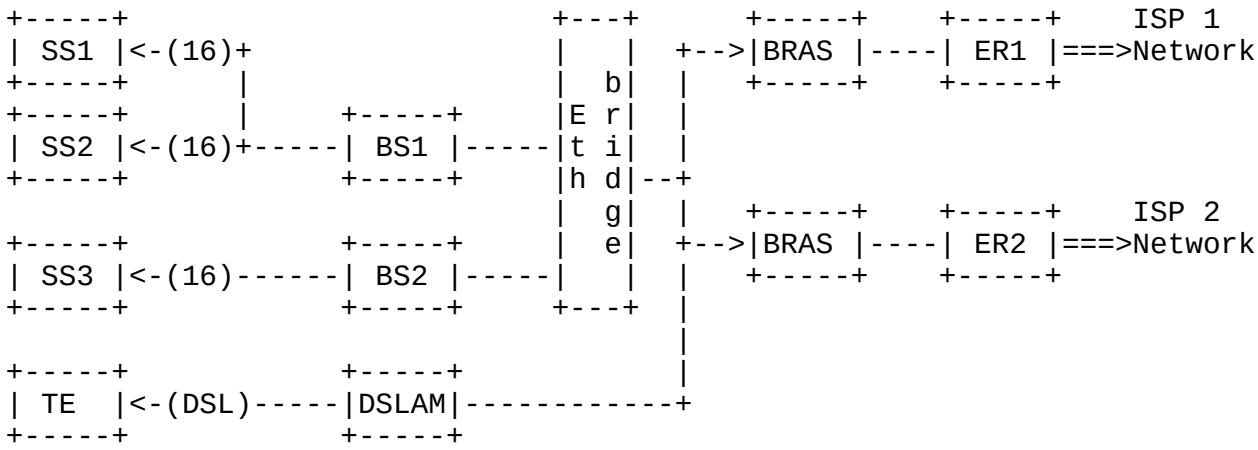

Figure 5: Integration of 802.16 Access into the DSL Infrastructure

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].

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

Transmission of IPv6 over Ethernet CS follows [RFC2464] and does not introduce any changes to [RFC4861] and [RFC4862]. However, there are a few considerations in the viewpoint of operation, such as preventing periodic router advertisement messages from an access router and broadcast transmission, deciding path MTU size, and so on. The details about the considerations are described in [IP-ETHERNET].

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 of Layer 2 and Layer 3 are supported in the fixed access scenario. Like WLAN technology, however, nomadicity can be supported in the radio coverage without any mobility protocol. So, a user can access Internet nomadically in the coverage.

Sometimes, service users can demand IP session continuity or home address reusability even in the nomadic environment. In that case, Mobile IPv6 [RFC3775] may be used in this scenario even in the absence of Layer 2's mobility support.

2.3. IPv6 Multicast

[IP-ETHERNET] realizes IPv6 multicast support by Internet Group Management Protocol/Multicast Listener Discovery (IGMP/MLD) proxying [RFC4605] and IGMP/MLD snooping [RFC4541]. Additionally, it may be possible to efficiently implement multicast packet transmission among the multicast subscribers by means of IEEE 802.16 Multicast CIDs. However, such a protocol is not yet available and under development in WiMAX Forum.

2.4. IPv6 QoS

In IEEE 802.16 networks, a connection is unidirectional and has a Quality of Service (QoS) specification. Each connection is associated with a single data service flow, and each service flow is associated with a set of QoS parameters in [IEEE802.16]. The QoS-related parameters are managed using the Dynamic Service Addition (DSA) and Dynamic Service Change (DSC) MAC management messages specified in [IEEE802.16]. The [IEEE802.16] provides QoS differentiation for the different types of applications by five scheduling services. Four scheduling services are defined in 802.16: Unsolicited Grant Service (UGS), real-time Polling Service (rtPS), non-real-time Polling Service (nrtPS), and Best Effort (BE). A fifth scheduling service is Extended Real-time Polling Service (ertPS), defined in [IEEE802.16e]. It is required to define IP layer quality of service mapping to MAC layer QoS types [IEEE802.16], [IEEE802.16e].

2.5. IPv6 Security

When initiating the connection, an MS is authenticated by the Authentication, Authorization, and Accounting (AAA) server located at its service provider network. To achieve that, the MS and the BS use Privacy Key Management [IEEE802.16],[IEEE802.16e], while the BS communicates with the AAA server using a AAA protocol. Once the MS is authenticated with the AAA server, it can associate successfully with the BS and acquire an IPv6 address through stateless auto-configuration or DHCPv6. Note that the initiation and authentication process is the same as the one used in IPv4.

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. SNMP messages can be carried by either IPv4 or IPv6.

3. Security Considerations

This document provides a detailed description of various IPv6 deployment scenarios and link models for IEEE 802.16-based networks, and as such does not introduce any new security threats. No matter what the scenario applied is, the networks should employ the same link layer security mechanisms defined in [IEEE802.16e] and IPv6 transition security considerations defined in [RFC4942]. However, as already described in [RFC4968], a shared prefix model-based mobile access deployment scenario may have security implications for protocols that are designed to work within the scope. This is the concern for a shared prefix link model wherein private resources cannot be put onto a public 802.16-based network. This may restrict the usage of a shared prefix model to enterprise environments.

4. 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.

5. References

5.1. Normative References

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

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

5.2. Informative References

[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.

[IEEE802.16f] "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.

[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.

[IP-ETHERNET] Jeon, H., Riegel, M., and S. Jeong, "Transmission of IP over Ethernet over IEEE 802.16 Networks", Work in Progress, April 2008.

[MIPSHOP-FH80216E] Jang, H., Jee, J., Han, Y., Park, S., and J. Cha, "Mobile IPv6 Fast Handovers over IEEE 802.16e Networks", Work in Progress, March 2008.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[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.

[RFC4068] Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[RFC4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, May 2006.

[RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.

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

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

[RFC4942] Davies, E., Krishnan, S., and P. Savola, "IPv6 Transition/Co-existence Security Considerations", RFC 4942, September 2007.

[RFC4968] Madanapalli, S., "Analysis of IPv6 Link Models for 802.16 Based Networks", RFC 4968, August 2007.

[RFC5121] Patil, B., Xia, F., Sarikaya, B., Choi, JH., and S. Madanapalli, "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", RFC 5121, February 2008.

[RFC5154] Jee, J., Madanapalli, S., and J. Mandin, "IP over IEEE 802.16 Problem Statement and Goals", RFC 5154, April 2008.

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.com

Domagoj Premec
Siemens Mobile
Heinzelova 70a
10010 Zagreb
Croatia

EMail: domagoj.premec@siemens.com

Full Copyright Statement

Intellectual Property