Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 20, 2007

M-K. Shin
ETRI
Y-H. Han
KUT
S-E. Kim
KT
D. Premec
Siemens Mobile
January 16, 2007

IPv6 Deployment Scenarios in 802.16(e) Networks
draft-ietf-v6ops-802-16-deployment-scenarios-02

Abstract

This document provides 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 network and its differences from IPv4 IEEE 802.16 networks and how IPv6 is deployed and integrated in each of the IEEE 802.16 technologies using tunneling mechanisms and native IPv6.

Table of Contents

1. Introduction

As the deployment of IEEE 802.16(e) access network progresses, users will be connected to IPv6 networks. While the IEEE 802.16 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. In this document, we will discuss main components of IPv6 IEEE 802.16 access network and its differences from IPv4 IEEE 802.16 networks and how IPv6 is deployed and integrated in each of the IEEE 802.16 technologies using tunneling mechanisms and native IPv6.

This document extends works of [I-D.ietf-v6ops-bb-deployment-scenarios] and follows the structure and common terminology of the document.

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 16ng WG.

Here are some of the key elements of an IEEE 802.16 network. The terminologies in this document "SS(MS)", "BS", and "AR" are to be interpreted as described in [I-D.ietf-16ng-ps-goals].

- o 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 IEEE 802.16e specification.

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

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

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

```
       Customer |     Access Provider    | Service Provider
       Premise  |                        | (Backend Network)

    +------+           +-----+     +-----+   +--------+
    | SSs |--(802.16)--| BS |-----|     |   | Edge   |   ISP
    +------+           +-----+     | AR |---| Router |==>Network
                                +--|     |   | (ER)   |
                                |  +-----+   +--------+
    +------+           +-----+  |                |  +-------+
    | SSs |--(802.16)--| BS |--+                +--|AAA    |
    +------+           +-----+                      |Server|
                                                    +-------+
```

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 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 substitudes for existing wired-based access technologies such as digital subscriber line (xDSL) and cable network. This fixed access scenario can provide nomadic access within the radio coverages, which is called Hot-zone model. A mobile access scenario is for new paradigm for voice, data and video over mobile network. This scenario can provide high speed data rate equalivent to wire-based Internet as well as mobility function equivalent to cellular system. 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, IEEE 802.16 BS can offer mobility function as well as fixed communication. [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 alwayes a default access router in the scenarios. There 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 IEEE 802.16 mobile access network deployment where a subnet consists of only single interface of AR and multiple MSs. Therefore, all MSs and corresponding interface of AR share the same IPv6 prefix as shown in Figure 2. IPv6 prefix will be different from the interface of AR.

```
+-----+
| MS1 |<-(16)-+
+-----+       |
+-----+       |    +-----+     +-----+    +---------+
| MS2 |<-(16)-+----| BS1 |--+->| AR  |----| Edge    |    ISP
+-----+            +-----+  |  +-----+    | Router +==>Network
                            |             +---------+
+-----+            +-----+  |
| MS3 |<-(16)-+----| BS2 |--+
+-----+       |    +-----+
+-----+       |
| MS4 |<-(16)-+
+-----+
```

Figure 2: Shared IPv6 Prefix Link Model

2. Point-to-Point Link Model

This link model represents IEEE 802.16 mobile access network deployment 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].

```
+-----+
| MS1 |<-(16)---------+
+-----+               |
+-----+            +-----+     +-----+    +---------+
| MS2 |<-(16)------| BS1 |--+->| AR  |----| Edge    |    ISP
+-----+            +-----+  |  +-----+    | Router +==>Network
                            |             +---------+
+-----+            +-----+  |
| MS3 |<-(16)------| BS2 |--+
+-----+            +-----+
+-----+               |
| 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 function and operates as a bridge. The BS does not need to support IPv6. However, if IPv4 stack is loaded to them for management and configuration purpose, it

is expected that BS should be upgraded by implementing IPv6 stack, too.

2.2.1.2. Addressing

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. 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 IEEE 802.16 link.

2. 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 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 same IPv6 link.

As for the prefix assignment, in case of 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 point-to-point link model, the AR assigns a unique prefix or set of unique prefixes for each MS. Prefix delegation can be required if networks can exist behind MS.

2.2.1.3. IPv6 Transport

In a subnet, there are always two underlying links: one is the IEEE 802.16 wireless link between MS and BS, and the other is a wired link between BS and AR. The IPv6 packet should be classified by IPv6 source/destination addresses, etc. BS generates the flow based on the classification. It also decides where to send the packet or just forward the packet to the ACR, since IEEE 802.16 connection always ends at BS while IPv6 connection terminates at the AR. This operation may be dependent on IPv6 subnet models.

If stateless auto-configuration is used to get an IPv6 address, router discovery and DAD operation should be properly operated over IEEE 802.16 link. In case of 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 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 may be more appropriate than Ethernet CS to transport IPv6 packets, since there are some overhead of Ethernet CS (e.g., Ethernet header) under mobile access environments. However PHS (Packet Header Compression), if deployed, mitigates much of this overhead.

Simple or complex network equipments may constitute the underlying wired network between the AR and the ER. If the IP aware equipments between the AR and the ER do 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 option might be more scalable and provide required service performance. Tunneling mechanisms should only be used when native IPv6 deployment is not an option. This can be equally applied to other scenario below (Section 2.2.2).

2.2.1.4. Routing

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

The AR can configure multiple link to ER for network reliability. The AR should support IPv6 routing protocol 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 layer 3 handoff procedure.

Mobile IPv6 defines that movement detection uses Neighbor Unreachability Detection to detect when the default router is no longer bi-directionally 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 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 whether 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 be occurred by the L2 trigger in case of inter-subnet handoff.

Also, IEEE 802.16g which is under-developed defines L2 triggers for link status such as link-up, link-down, handoff-start. These L2 triggers may make 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 [I-D.iab-link-encaps], the mobile access scenarios need solutions about how roaming will work when forced to move from one CS to another. Note that, at this phase this issue is the out of scope of this draft. It should be also discussed in 16ng WG.

2.2.2. Fixed/Nomadic Deployment Scenarios

The IEEE 802.16 access networks can provide plain Ethernet connectivity end-to-end. 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 service. A company can use IEEE 802.16 to build up 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 unlicensed (2.4 & 5 GHz) band as well as 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.

This scenario also represents IEEE 802.16 network deployment where a

subnet consists of multiple MSs and multiple interface 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 like WLAN, this case should be also considered. Hot-zone deployment model falls within this case.

```
            +-----+                         +-----+    +-----+    ISP 1
            | SS1 |<-(16)+              +->| AR1 |----| ER1 |===>Network
            +-----+      |              |  +-----+    +-----+
            +-----+      |     +-----+  |
            | SS2 |<-(16)+-----| BS1 |--|
            +-----+            +-----+  |  +-----+    +-----+    ISP 2
                                        +->| AR2 |----| ER2 |===>Network
 +-----+    +-----+            +-----+  |  +-----+    +-----+
 |Hosts|<-->|SS/GW|<-(16)------| BS2 |--+
 +-----+    +-----+            +-----+
    This network
 behind SS may exist
```

Figure 4: Fixed/Nomadic Deployment Scenario

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.

```
 +-----+                        +---+      +-----+    +-----+    ISP 1
 | SS1 |<-(16)+                 |   |  +-->|BRAS |----| ER1 |===>Network
 +-----+      |                 |  b|  |   +-----+    +-----+
 +-----+      |     +-----+     |E r|  |
 | SS2 |<-(16)+-----| BS1 |-----|t i|  |
 +-----+            +-----+     |h d|--+
                                |  g|  |   +-----+    +-----+    ISP 2
 +-----+            +-----+     |  e|  +-->|BRAS |----| ER2 |===>Network
 | SS3 |<-(16)------| BS2 |-----|   |  |   +-----+    +-----+
 +-----+            +-----+     +---+  |
                                       |
 +-----+            +-----+            |
 | TE  |<-(DSL)-----|DSLAM|------------+
 +-----+            +-----+
```

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 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 and ER. In this scenario, IEEE 802.16 BSs have only MAC and PHY layers without router function and operates as a bridge. The BS does not need to support IPv6. However, if IPv4 stack is loaded to them for management and configuration purpose, it is expected that BS should be upgraded by implementing IPv6 stack, too.

The BRAS in Figure 5 is providing the functionality of the AR. The Ethernet bridge is necessary for protecting the BRAS from 802.16 link layer peculiarities. The Ethernet bridge relays all traffic received through BS to its network side port(s) connected to BRAS. Any traffic received from BRAS is relayed to appropriate BS. Since 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 can exist behind SS.

2.2.2.3. IPv6 Transport

Note that in this scenario Ethernet CS may be more appropriate than IPv6 CS to transport IPv6 packets, since the scenario need to support plain Ethernet connectivity end-to-end. 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 authoritative address cache and Relay DAD. 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 DAD process will be relayed only to the MS which already has configured the solicited address as its own address (if such 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, 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 fixed access scenario. However, mobility can support 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. 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. For MBS how this mapping will happen is not clear, 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 Multicast and Broadcast Service (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 QoS has different semantics with 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 once authenticated. When an MS is once authenticated and associated successfully with BS, IPv6 address will be acquired by the MS with 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 don't have PKIs across organizations and IPsec isn't 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

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 network can be managed by IPv4 or IPv6 when

network elements are implemented dual stak. For example, network management system (NMS) can send SNMP message by IPv4 with IPv6 related object identifier. Also, an NMS can use IPv6 for SNMP request and response 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 works on [I-D.ietf-v6ops-bb-deployment-scenarios]. 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 and Jung-Mo Moon for extensive review of this 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.

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

6.2. Informative References

[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.

[I-D.ietf-16ng-ps-goals]
Jee, J., "IP over 802.16 Problem Statement and Goals", draft-ietf-16ng-ps-goals-00 (work in progress), October 2006.

[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-02 (work in progress), January 2007.

[I-D.ietf-mipshop-fmipv6-rfc4068bis]
Koodli, R., "Fast Handovers for Mobile IPv6", draft-ietf-mipshop-fmipv6-rfc4068bis-00 (work in progress), May 2006.

[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.

[I-D.ietf-v6ops-bb-deployment-scenarios]
Asadullah, S., "ISP IPv6 Deployment Scenarios in Broadband Access Networks", draft-ietf-v6ops-bb-deployment-scenarios-05 (work in progress), June 2006.

[I-D.iab-link-encaps]
Aboba, B., "Multiple Encapsulation Methods Considered Harmful", draft-iab-link-encaps-05 (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 Std. 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.

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

Acknowledgment

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