Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 4, 2007

H. Jeon
ETRI
M. Riegel
Siemens
S. Jeong
ETRI
Oct 2006

Transmission of IP Packets over Ethernet over IEEE 802.16
draft-riegel-16ng-ip-over-eth-over-80216-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes the behavior of the Ethernet emulation on top of IEEE 802.16 to efficiently support the transmission of IPv4 as well as IPv6 packets over IEEE 802.16 radio links. Due to resource constraints of radio transmission systems and the limitations of the IEEE 802.16 MAC layer for the emulation of Ethernet, the transmission

of IP over an emulated LAN on top of IEEE 802.16 may considerably benefit by adding IP specific support functions within the Ethernet emulation on top of IEEE 802.16.

Table of Contents

1. Introduction

IEEE 802.16 [IEEE802.16] defines a point-to-multipoint radio transmission system connecting a Base Station (BS) with multiple Subscriber Stations (SSs). IEEE 802.16e [IEEE802.16e] amends the base specification with PHY and MAC functions for supporting mobile terminals by adopting the same data link principles also for mobile networking systems.

This document provides a detailed description of the Ethernet emulation on top of IEEE 802.16 with additional functionalities for efficient support of IPv4 packets as well as IPv6 packets.

2. Requirements

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 [RFC2119].

3. Terminology

Description of following some terms is taken directly from [IEEE802.16] and [IEEE802.16e].

Base Station (BS): A generalized equipment set providing connectivity, management, and control of the subscriber station.

Subscriber Station (SS): A generalized equipment set providing connectivity between subscriber equipment and a base station. Within this document the term SS also represents the Mobile Subscriber Station introduced in IEEE 802.16e

Service-specific Convergence Sublayer (CS): Sublayer in IEEE 802.16 MAC layer which classifier external network data and associates them to the proper MAC service flow identifier and connection identifier.

Connection Identifier (CID): A 16 bit value that identifies a connection to equivalent peers in the MAC of the base station and subscriber station.

Source Node: Host which initiates an IPv6 Neighbor Discovery message using its own unique MAC address. A Source Node may be co-located with a SS or may be behind a SS, when the SS acts as a bridge.

Target Node: Host which is addressed by the target field in an IPv6 Neighbor Discovery message. The Target Node has its own unique MAC address and may be co-located with a SS or may be behind a SS, when the SS acts as a bridge

4. The IEEE 802.16 Link Model

4.1. Connection Oriented Air Interface

The IEEE 802.16 MAC provides connections between the BS and its associated SSs. Each of these connections is identified by a 16 bit CID number and has defined QoS capabilities. Multiple connections can be established between a BS and a SS, each with its particular QoS class and direction.

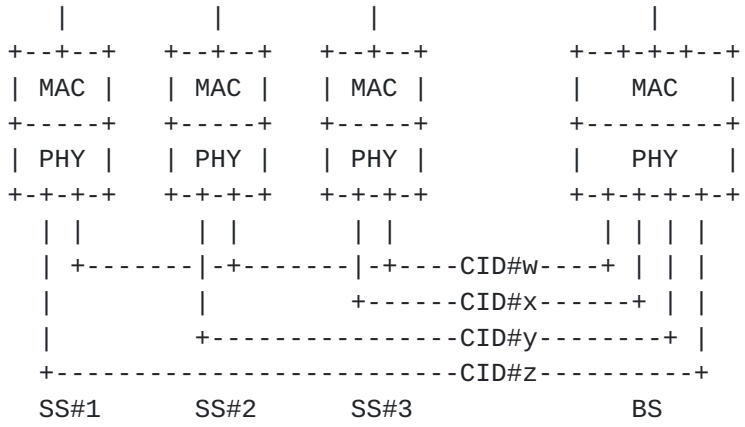

Figure 1. Basic IEEE 802.16 Link Model

While uplink connections provide only unicast transmission capabilities from a particular SS to the BS, downlink connections can be used for unicast transmission from the BS to a particular SS as well as for multicast transmissions to a group of SSs.

4.2. Convergence Sublayers

The assignment of higher layer packets to particular service flows and the related CIDs is performed within the IEEE 802.16 convergence sublayer by classifying the packets according to particular header fields. To enable the transmission of different kind of payloads over IEEE 802.16, multiple types of classification types are defined, each specific for one kind of upper layer protocol, like Ethernet, IPv4, IPv6 or even for encapsulated payload, like IPv4 over Ethernet or IPv6 over Ethernet.

Optionally the convergence sublayer performs a packet header

suppression reducing static parts of the header to a single byte value. With the application of the packet header suppression function there is mostly no difference in header overhead over the air for Ethernet encapsulated IP packets in comparison to plain IP packets.

4.3. Multicast and Broadcast Support in IEEE 802.16

Downlink connections can be shared among multiple SSs, enabling multicast channels with multiple SSs receiving the same information from the BS. Multicast is not enabled in the uplink but must be realized by an entity on top the IEEE 802.16 MAC sending packets received on a unicast uplink downstream on a multicast channel.

4.4. Solicitation of MAC addresses

The 48-bit unique MAC address of a SS is used during the initial ranging process for the identification of a SS and verified by the succeeding PKMv2 authentication phase. As a result, the BS establishes a list of solicited-node MAC addresses of all SSs connected to the BS. Note that there may be additional MAC addresses behind SSs when SSs act as bridge connecting networks behind the SSs. The additional MAC addresses may be also solicited when there is a controlled link state for the hosts behind the SS and the SS performs authentication of the link, e.g. by running IEEE 802.1X on the SS.

5. The IEEE 802.16 Network Model for Ethernet

5.1. IEEE 802.16 Ethernet Link Model

According to [I-D.ietf-ipv6-2461bis], an IP Link is defined as a communication facility or medium over which nodes can communicate at the link layer, i.e. the layer immediately below IP. IEEE 802.16 provides point-to-point connections between SSs and the BS without enabling any direct SS to SS connectivity. Ethernet is realized on top of IEEE 802.16 by implementing bridging between all SSs with IEEE 802.16 providing the links between the hosts and the bridge behind the BS like the twisted pair wires used in today's switched Ethernet.

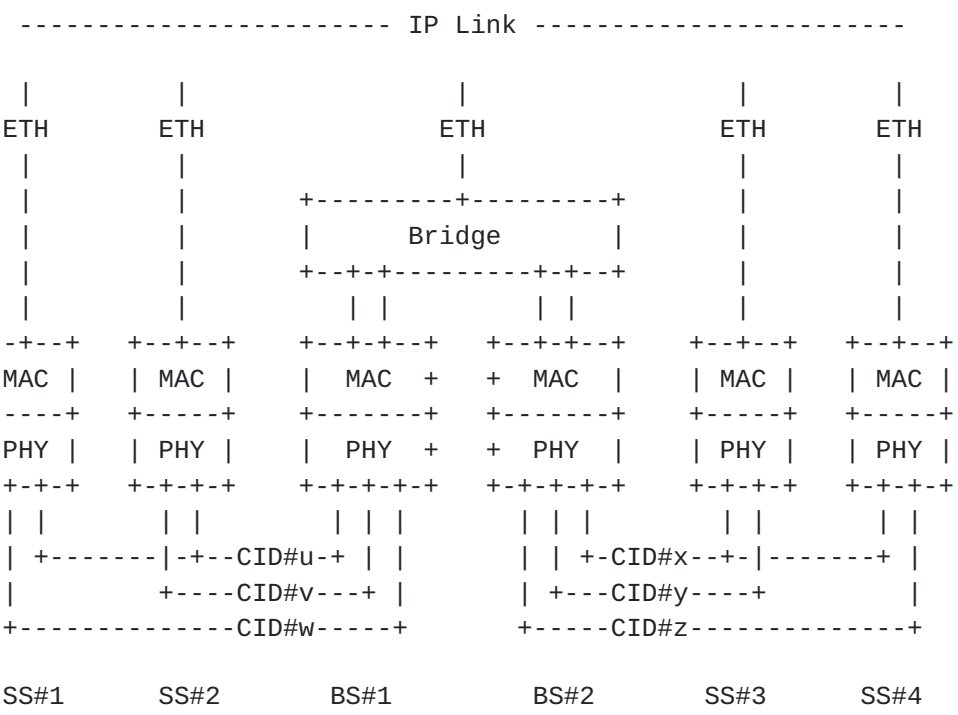

Figure 2. IEEE 802.16 IP over Ethernet Link Model

It is possible to control the size and coverage of IP links by segmenting the Ethernet and grouping particular links into VLANs. Such segmentation is mostly done between BSs, but it is also possible to extend the segmentation over IEEE802.16 links when multiple hosts are attached to a bridge at the SS.

5.2. Ethernet without Native Broadcast and Multicast Support

Ethernet is emulated on top of IEEE 802.16 without making use of MBS as defined in 6.3.23 of [IEEE802.16e] to allow full control over the reaction of SSs to broadcast messages. Instead of using MBS, broadcast and multicast messages are transferred in a unicast manner.

5.3. Default Processing of Ethernet Frames

If the SS performs a bridging function then it SHALL support Standard Learned Bridging between all its LAN ports and the airlink. The BS SHALL forward all the radio connections belonging to one SS to a port of a bridge performing Standard Learned Bridging between all ports on the radio side and the interfaces towards the network side.

When performing Standard Learned Bridging, the SS, when acting as a bridge, or the bridge behind the BSs shall learn all source MAC addresses originating from a port resulting in Dynamic Filtering Entries if the same MAC addresses are not already listed as Static

Filtering Entries. The accumulation of all learned MAC to port associations and all Static Filtering Entries derived from solicited-node MAC addresses constitute the Filtering Database. The Standard Learned Bridge shall automatically unlearn a Dynamic Filtering Entry MAC to port relationship after BRIDGETIMEOUT seconds have expired without any traffic from that MAC address.

When performing bridging, any packets destined for one of the addresses in the Filtering Database SHALL be forwarded directly to that port and all packets received from a port, for which the packet's destination MAC address is also an entry for that port in the Filtering Database, SHALL be silently discarded.

6. Deployment Scenarios for IP over Ethernet over IEEE 802.16

Figure 3 and 4 show possible deployment scenarios in case of IP over Ethernet over IEEE 802.16. In both figures, the AR is connected to a bridge, which is connected to all BSs. The bridge supports Static Filtering Entries and Standard Learned Bridging, as specified in Section 5.3. Multiple ARs can exist on a link, and a subnet (IP Link) consists of multiple hosts usually being co-located with a SS acting as bridge. The network behind a SS can support various access network technologies, e.g. 802.3, 802.11 or 802.15.

6.1. Public Access Scenario

Figure 3 depicts an IEEE 802.16 network deployment scenario without direct host-to-host communication. In the general public access case, direct communication between nodes is restricted because of security and accounting issues. In this scenario, the bridge SHALL forward all packets received from any radio side port to a network side port. Peer-to-peer communication is not supported by the bridge and all packets originated from a SS should be delivered to an AR.

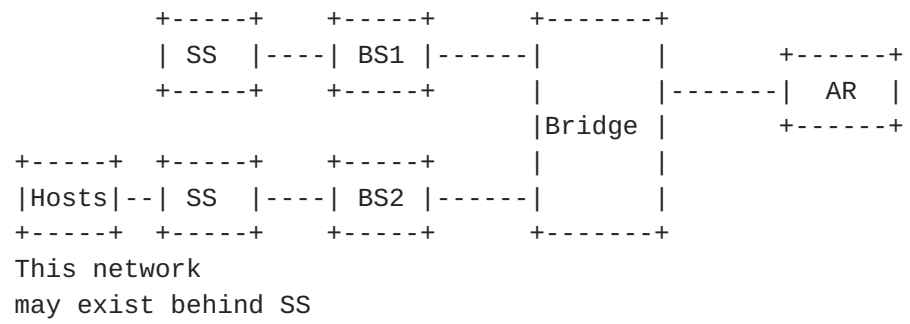

Figure 3. Network Model without direct host-to-host communication

6.2. VLAN Scenario

Figure 4 shows the VLAN scenario. Particular SSs grouped into a VLAN can directly communicate with each other when this mode is enabled for the VLAN. Otherwise, direct communication is prohibited and the VLAN shows the same behavior as the public access scenario case. The bridge has been extended to support VLAN capability and configurable direct host-to-host communication.

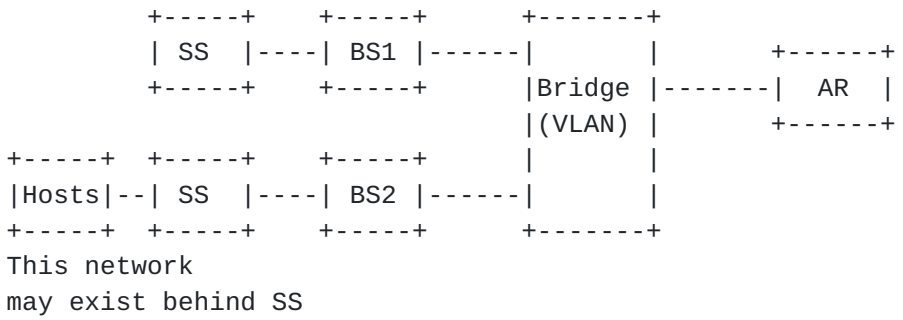

Figure 4. Network Model with direct host-to-host communication

7. Filtering and Forwarding

7.1. IP Broadcast and Multicast Support

As explained in 5.2, no native MBS support is used for emulation of the Ethernet behavior over IEEE 802.16 links. Only point-to-point connections are established between SSs and BS. Multiple connections belonging to the same SS are feeded into a single bridge port. Broadcast or all-nodes multicast data such as router advertisements are unicasted to intended SS via the point-to-point connection.

7.2. Packet Filtering

The bridge SHALL have the ability to enable or disable any filtering functionality defined herein. If a packet is filtered it SHALL be silently discarded. The filtering functionality is based on the information of the Identification Cache Table (ICT), which is an extension of the Filtering Database. Details of the ICT are given in Section 7.3.

The bridge SHALL support filtering of all packets received from a network side port to a destination MAC address not existing in the ICT.

The bridge SHALL support filtering of all packets received from a network side port to a broadcast or multicast MAC address.

If filtering is enabled the bridge SHALL permit all Address Resolution Protocol messages to pass to the ARP Proxy Agent and all Neighbor Discovery messages to pass to the Neighbor Discovery (ND) Relay Agent, as specified in following section.

All multicast and multicast control messages are forwarded according to [RFC4541]

7.3. Identification Cache Table

The bridge establishes and maintains information about each SS by the mean of an Identification Cache Table (ICT).

For IPv4 over Ethernet, the ICT contains for each MAC address, the lifetime if it is not Static Filtering Entry and one or more IPv4 addresses.

For IPv6 over Ethernet, the ICT contains for each MAC address, the lifetime if it is not Static Filtering Entry, the link-local address and one or more IPv6 addresses with associated Valid Flags.

The ARP Proxy Agent and the ND Relay Agent functions are based on information contained in the ICT.

IPv4 addresses can be learned by examining the source address of packets or DHCP Response message.

IPv6 link-local addresses can be derived from solicited-node MAC address. Note that Privacy Extension for IPv6 address [RFC3041] is not considered in the current version.

The IPv6 address is learned by extracting the Target field in the Neighbor Solicitation (NS) message for Duplicate Address Detection (DAD), if the tentative IPv6 address does not exist yet as a valid IPv6 address in the ICT. In this case, the Valid Flag is set to indicate the tentative IPv6 address has become valid. Otherwise, the IPv6 address in the Target field in a DAD NS message is stored as IPv6 address with Valid Flag is not set to identify the Source Node when the bridge relays the Neighbor Advertisement message from Target Node.

The lifetime of each entry follows the lifetime of the Learned Bridge Table. Figure 5 and Figure 6 show the ICT for IPv4 over Ethernet and IPv6 over Ethernet.

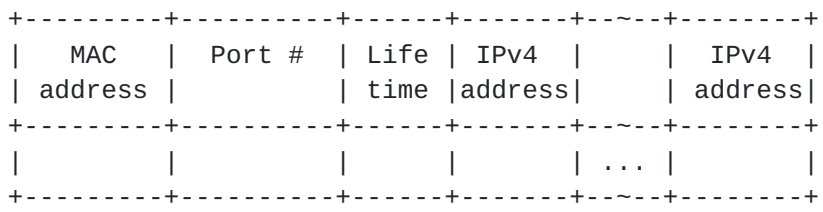

Figure 5. ICT on Bridge in case of IPv4 over Ethernet

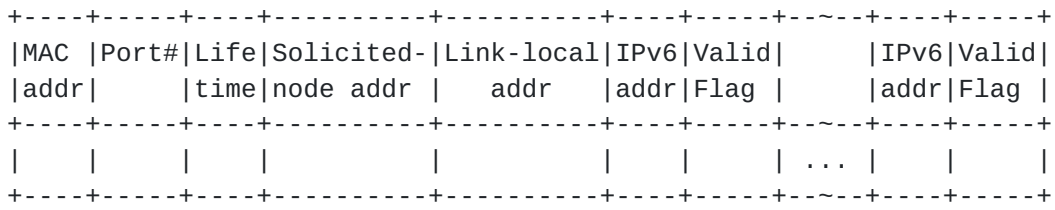

Figure 6. ICT on Bridge in case of IPv6 over Ethernet

7.4. Address Resolution Protocol Proxy Function

In the case of IPv4 over Ethernet, ARP requests can be responded by the ARP Proxy Agent of the bridge. (refer to Section 8.1.1 for more detail)

However, a proxy function in IPv6 over Ethernet is subjected to restriction because of security issues. Support of SeND [RFC3971] has been adopted in the IPv6 over Ethernet case.

7.5. Neighbor Discovery Relay Function

In the case of IPv6 over Ethernet, the AR sends periodically Router Advertisement and the Router Advertisement messages can be relayed by the ND Relay Agent of the bridge. The ND Relay Agent unicasts the Router Advertisement via all the already established a point-to-point connections between SSs and bridge.

Note that the relaying of Router Advertisement MUST NOT affect validness of SeND Timestamp.

When the bridge receives Neighbor Solicitation for DAD, the ND Relay Agent of the bridge performs the same operation as the Relay DAD. The ND Relay Agent looks up in the ICT to detect whether a tentative address in the Neighbor Solicitation message is in use or not. If the tentative address is not in use, the ND Relay Agent discards the

Neighbor Solicitation. Otherwise, the Neighbor Solicitation message is relayed only to the addressed Target Node.

When the bridge receives the DAD Neighbor Advertisement message from the Target Node, the ND Relay Agent of the bridge identifies the corresponding Source Node by the ICT and then unicasts the DAD Neighbor Advertisement message via the established point-to-point connection to the corresponding Source Node.

7.6. Access Router Behavior

The assignment of a common prefix to all SSs means locating them "on-link" in terms of IP packet transfer. According to [I-D.ietf-ipv6-2461bis], an IP node performs a longest prefix match against the prefix list in order to decide whether the destination of the IP packet is on-link or not. Therefore, SSs sharing a prefix can be said to be on-link IP nodes.

In the Public Access scenario, all unicast packets originated from a SS should be delivered to an AR even though the SS sends packets to on-link SSs. Therefore, it is necessary for the AR to relay the on-link packets.

The AR SHALL have packet-relay functionality. The AR relays packets destined for IP broadcast address and link-local scoped multicast addresses to incoming interface again.

When the AR relays packets destined for ab on-link host, the packet may be forwarded onto the incoming interface. It should be prevented that the AR transmits a Redirect message to sender when direct communication between on-link SSs occurs.

In the case of the VLAN scenario, direct communication between SSs may be enabled for all SSs belonging to a particular VLAN. In this case, no special handling is required.

8. Transmission of IP over Ethernet

8.1. IPv4 over Ethernet

[RFC0894] defines the transmission of IP packets over Ethernet networks. It contains the specification of the encapsulation of the IP packets into Ethernet frames as well as rules for mapping of IP addresses onto Ethernet MAC addresses. The use of ARP [RFC0826] is recommended for dynamic address resolution.

8.1.1. Address Resolution

The bridge SHALL support an ARP Proxy. The bridge SHALL have the ability to enable or disable the ARP Proxy.

If the ARP Proxy is disabled, the ARP Proxy Agent shall pass all ARP packets without discrimination or modification using bridging. The ARP Proxy Agent shall pass all ARP Response packets without discrimination or modification using bridging.

If the ARP Proxy is enabled, upon receiving an ARP Request from an radio side interface, the ARP Proxy Agent shall unicast an ARP Response back to the interface provided that the target address matches an entry in the ICT. Otherwise, the ARP Proxy Agent shall flood the ARP Request to all network side interfaces.

The ARP Proxy Agent shall silently discard any received self-ARP Requests. Those are requests for a target IP address, that when queried in the ICT results in a response MAC equal to the Request's source MAC address.

The ARP Proxy Agent shall issue a gratuitous ARP on the network side interfaces for any new addition to the ICT. An unsolicited broadcast ARP Response constitutes a gratuitous ARP.

8.2. IPv6 over Ethernet

The transmission of IPv6 Packets over Ethernet Networks is defined by [RFC2464] providing the frame format for encapsulation of IPv6 packets into Ethernet frames as well as the methods of forming IPv6 link-local addresses and statelessly autoconfigured addresses on Ethernet networks.

8.2.1. Router Discovery, Prefix Discovery and Parameter Discovery

Router Discovery, Prefix Discovery and Parameter Discovery procedures are achieved by receiving Router Advertisement (RA) messages. The RA is forwarded by using all-nodes IP multicast transmission.

This document assumes a point-to-point connection between each SS and bridge. The ND Relay Agent of the bridge unicast the RA from AR via the point-to-point connection.

Note that the RA has a long lifetime and minimum packet size which can be sent in IEEE 802.16 to the SSs being in sleep-mode during the periodic wakeup-time.

8.2.2. Address Configuration

8.2.2.1. Stateful Address Autoconfiguration

When the'M' flag in the received RA is set, a SS should perform stateful address configuration according to [RFC3315]. In this case, an AR supports DHCPv6 server or relay function.

8.2.2.2. Stateless Address Autoconfiguration

The global IPv6 addresses is derived based on prefix and EUI-64-derived interface identifier and then confirmed through Duplicate Address Detection (DAD) as specified in [RFC2462].

For DAD, the Source Node sends Neighbor Solicitation to the solicited-node MAC address corresponding to the generated global IPv6 address for DAD. The Neighbor Solicitation is passed to the ND Relay Agent when arriving at the bridge.

8.2.3. Address Resolution

The Source Node sends Neighbor Solicitation to the solicited-node address corresponding to the target address for address resolution.

Upon receiving the Neighbor Solicitation, the bridge retrieves the port corresponding to the solicited-node MAC address in its ICT and then forwards the Neighbor Solicitation via that port.

Finally the Target Node responds to the Neighbor Solicitation.

8.3. Maximum Transmission Unit Consideration

When stacked VLAN headers are transferred over GRE tunnels, the sizes of the VLAN headers and the GRE header need to be considered in setting the value of MTU of the transport path.

9. Security Considerations

[RFC3971] specifies security mechanisms for ND Protocol and defines means for securing ND Protocol messages. This document aims to fully support security mechanisms specified in [RFC3971].

10. Informative References

[I-D.ietf-ipv6-2461bis]
Narten, T., "Neighbor Discovery for IP version 6 (IPv6)",

draft-ietf-ipv6-2461bis-08 (work in progress), September 2006.

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

[IEEE802.16] IEEE Std 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 P802.16e-2005, "IEEE Standard for Local and metropolitan area networks, Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands", December 2005.

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[RFC0894] Hornig, C., "Standard for the transmission of IP datagrams over Ethernet networks", STD 41, RFC 894, April 1984.

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

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

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

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

[RFC3041] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 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.

Authors' Addresses

Hongseok Jeon
Electronics Telecommunications Research Institute
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-350
KOREA

Phone: +82-42-860-3892
Email: jeonhs@etri.re.kr

Max Riegel
Siemens
St-Martin-Str 76
Munich, 81541
Germany

Phone: +49-89-636-75194
Email: maximilian.riegel@siemens.com

Sangjin Jeong
Electronics Telecommunications Research Institute
161 Gajeong-dong, Yuseong-gu
Daejeon, 305-350
KOREA

Phone: +82-42-860-1877
Email: sjjeong@gmail.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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