16ng Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 21, 2008

S. Madanapalli
Ordyn Technologies
Soohong D. Park
Samsung Electronics
S. Chakrabarti
Azaire Networks
November 18, 2007

Transmission of IPv4 packets over IEEE 802.16's IP Convergence Sublayer
draft-ietf-16ng-ipv4-over-802-dot-16-ipcs-01.txt

Status of this Memo

Copyright Notice

Abstract

IEEE 802.16 is an air interface specification for wireless broadband access. IEEE has specified the service specific convergence sublayers (CS) in the IEEE 802.16 MAC to be used by upper layer protocols. Asynchronous Transfer Mode Convergence Sublayer (ATM CS) and Packet Convergence Sublayer (Packet CS) represent the two main

service specific convergence sublayers for the IEEE 802.16. The packet CS is used for transport for all packet-based protocols such as Internet Protocol (IP), IEEE 802.3 (Ethernet) and IEEE 802.1Q (VLAN). The IP specific part of the Packet CS enables transport of IPv4 packets directly over the IEEE 802.16 MAC.

This document specifies the frame format, the Maximum Transmission Unit (MTU) and address assignment procedures for transmitting IPv4 packets over IP Convergence Sublayer (IPCS) of the IEEE 802.16. This document also provides the details of why the ARP cannot be sent over the IEEE 802.16 links using IPCS and a recommendation for this.

Table of Contents

1. Introduction

IEEE 802.16 [7] is a connection oriented access technology for the last mile without bi-directional native multicast support. IEEE 802.16 has only downlink multicast support and there is no mechanisms defined for mobile stations to be able to send multicast packets that can be mapped to downlink multicast connection. And also IEEE 802.16 MAC does not use the Source and Destination MAC addresses, instead it uses the Connection Identifiers (CIDs), which are assigned dynamically while setting up the MAC connections, for transmitting the IEEE 802.16 frames between a Mobile Station (MS) and a Base Station (BS).

This document specifies a method for encapsulating and transmitting IPv4 [2] and Address Resolution Protocol (ARP) packets over IP CS of IEEE 802.16. This document also specifies the MTU and address assignment method for the IEEE 802.16 based networks using IPCS. As the IEEE 802.16 MAC does not use the source and destination MAC addresses for the frame transmission, this document recommends avoiding ARP and Mapping of multicast IP address to MAC address.

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 [1].

2. Terminology

The terminology in this document is based on the definitions in [10], in addition to the ones specified in this section.

Access Router (AR): An entity that performs an IP routing function to provide IP connectivity for Mobile Stations.

3. Typical Network Architecture for IPv4 over IEEE 802.16

In a network that utilizes the IEEE 802.16 air interface, each MS is attached to an Access Router (AR) through a Base Station (BS), a layer 2 entity. The AR can be an integral part of the BS or the AR could be an entity beyond the BS within the access network. IPv4 packets between the MS and BS are carried over a point-to-point MAC transport connection which has a unique connection identifier (CID). The packets between BS and AR are carried using L2 tunnel (typically GRE tunnel) so that MS and AR are seen as layer 3 peer entities. At least one L2 tunnel is required for each MS, so that IP packets can be sent to MSs before they acquire IP addresses. The figure below illustrates the network architecture.

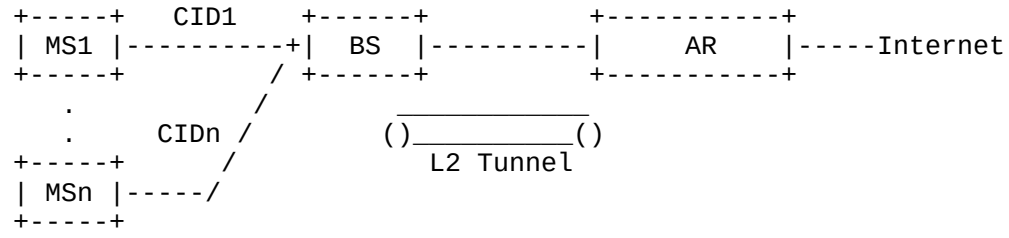

Figure 1: Typical Network Architecture for IPv4 over IEEE 802.16

The above network model serves as an example and is shown to illustrate the point to point link between the MS and the AR. The L2 tunnel is not required if BS and AR are integrated into a single box.

4. Frame Format for IPv4 Packets

IPv4 packets are transmitted in Generic IEEE 802.16 MAC frames as shown in the following figure.

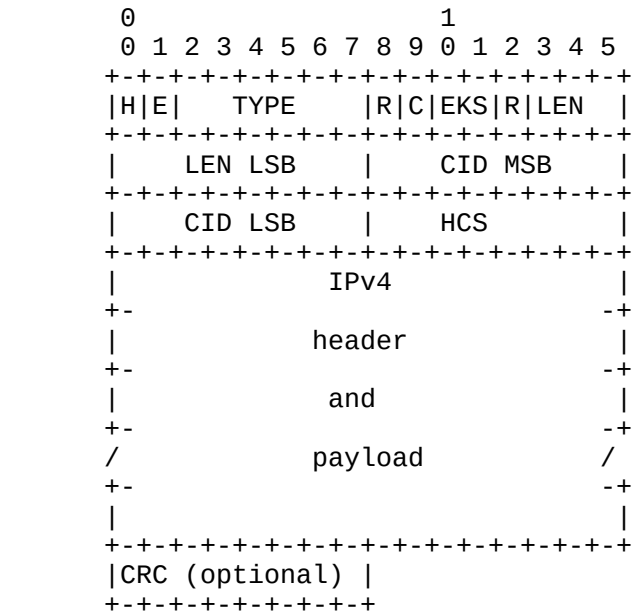

Figure 2: IEEE 802.16 MAC Frame Format for IPv4 Packets

H: Header Type (1 bit). Shall be set to zero indicating that it is a Generic MAC PDU.
E: Encryption Control. 0 = Payload is not encrypted; 1 = Payload is encrypted.
R: Reserved. Shall be set to zero.
C: CRC Indicator. 1 = CRC is included, 0 = 1 No CRC is included
EKS: Encryption Key Sequence
LEN: The Length in bytes of the MAC PDU including the MAC header and the CRC if present (11 bits)
CID: Connection Identifier (16 bits)
HCS: Header Check Sequence (8 bits)
CRC: An optional 8-bit field. CRC appended to the PDU after encryption.
TYPE: This field indicates the subheaders (Mesh subheader, Fragmentation Subheader, Packing subheader etc and special payload types (ARQ) present in the message payload

5. Maximum Transmission Unit

The Length parameter of IEEE 802.16 MAC frame has a size of 11 bits. Hence the total PDU size is 2048 bytes. The IPv4 payload can be a maximum value of 2038 bytes (Total PDU size (2048) - (MAC Header (6) + CRC (4)), which is the maximum possible MTU. The minimum MTU required for IPv4 is 576 bytes [4]. The default MTU value for IPCS is 1440 bytes. The default IPCS MTU is chosen based on 1500 bytes ethernet MTU size;it is less than 1500 bytes because of two reasons - 1) GRE tunnel between the AR and BS ethernet network, 2)avoiding IP fragmentation as much as possible when transmitting packets from IEEE 802.16 IPCS network to a different access network using IPSec tunnel over ethernet or IEEE 802.11 wireless network. The actual MTU value can be set by the Path MTU Discovery [9] or by static configuration of each MS. The IPCS link of the AR SHOULD also set the default MTU value as 1440 bytes.

6. Subnet Model and IPv4 Address Assignment

The Subnet Model recommended for IPv4 over IEEE 802.16 using IP CS is based on point-to-point link between MS and AR, hence each MS shall be on different IP subnet. The point-to-point link between MS and AR is achieved using a set of IEEE 802.16 MAC connections (identified by CIDs) and at least an L2 tunnel (usually GRE tunnel) per MS between BS and AR. If the AR is co-located with the BS then the set of IEEE 802.16 MAC connections between the MS and BS/AR represent the point-to- point connection.

DHCP [5] SHOULD be used for assigning IPv4 address for the MSs. DHCP

messages are transported over IEEE 802.16 MAC transported connection to and from the AR. In case DHCP server does not reside in AR, the AR SHOULD implement DHCP relay Agent [6].

7. Address Resolution Protocol

The IEEE 802.16 frame header does not contain the source and destination MAC addresses, instead it uses the Connection Identifier (CID) for the delivery of MAC frames. This makes classical Address Resolution Protocol (ARP) [3] trivial and unnecessary. > Also, IEEE 802.16 IPCS cannot classify the ARP packets as ARP runs directly over Ethernet and does not contain IP header. Thus ARP packets are not transmitted over IEEE 802.16 air interface when using IPCS.

8. IP Multicast Address Mapping

In IEEE 802.16, MAC address is not used for delivering the frames as well as there is no concept of multicast MAC address. Hence, the Mapping of multicast IP address to an IEEE 802.16 MAC address is not required. The IPv4 multicast packets are classified normally at the IPCS if the IEEE 802.16 MAC connection has been setup with a multicast IP address as a classification parameter for the destination IP address.

9. Security Considerations

This document specifies transmission of IPv4 packets over IEEE 802.16 networks with IPv4 Convergence Sublayer and does not introduce any new vulnerabilities to IPv4 specifications or operation. The security of the IEEE 802.16 air interface is the subject of [7]. In addition, the security issues of the network architecture spanning beyond the IEEE 802.16 base stations is the subject of the documents defining such architectures, such as WiMAX Network Architecture [8].

10. IANA Considerations

This document has no actions for IANA.

11. Acknowledgements

The authors would like to acknowledge the contributions of Bachet Sarikaya, Basavaraj Patil, Paolo Narvaez, Bruno Sousa and Bernard Aboba, Dave Thaler and Jari Arkko for their review and comments.

Thanks to Jongtaek Oh for providing texts on multicast address mapping and mentioning of NAT in appendix for completeness.

12. References

12.1. Normative References

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

[2] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[3] 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.

[4] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[5] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[6] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, October 1993.

12.2. Informative References

[7] "IEEE 802.16e, IEEE standard for Local and metropolitan area networks, Part 16:Air Interface for fixed and Mobile broadband wireless access systems", October 2005.

[8] "WiMAX End-to-End Network Systems Architecture Stage 2-3 Release 1.0.0, http://www.wimaxforum.org/technology/documents", March 2007.

[9] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, November 1990.

[10] Jee, J., "IP over 802.16 Problem Statement and Goals", February 2007, <http://www.ietf.org/internet-drafts/draft-ietf-16ng-ps-goals-01.txt>.

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

Appendix A. Multiple Convergence Layers - Impact on Subnet Model

Two different MSs using two different convergence sublayers (e.g. an MS using Ethernet CS only and another MS using IP CS only) cannot communicate at data link layer and requires interworking at IP layer. For this reason, these two nodes must be configured to be on two different subnets. For more information refer [11].

Appendix B. Consideration for ARP Implementation

A node may trigger ARP for address resolution when there is no corresponding entry in ARP cache, in such cases, the node should synthesize the ARP response locally for smooth operation of IP layer.

Appendix C. Sending and Receiving IPv4 Packets

IEEE 802.16 MAC is a point-to-multipoint connection oriented air-interface, and the process of sending and receiving of IPv4 packets is different from multicast capable shared medium technologies like Ethernet.

Before any packets being transmitted, IEEE 802.16 transport connection must be established. This connection consists of IEEE 802.16 MAC transport connection between MS and BS and an L2 tunnel between BS and AR. This IEEE 802.16 transport connection provides a point-to-point link between MS and AR. all the packets originated at the MS always reach AR before being transmitted to the final destination.

IPv4 packets are carried directly in the payload of IEEE 802.16 frames when the IPv4 CS is used. IPv4 CS classifies the packet based on upper layer (IP and transport layers)header fields to put the packet on one of the available connections identified by the CID. The classifiers for the IPv4 CS are source and destination IPv4 addresses, source and destinations ports, Type-of-Service and IP protocol field. The CS may employ Packet Header Suppression (PHS) after the classification.

The BS tunnels the packet that has been received on a particular MAC connection to the AR. BS reconstructs the payload header if the PHS is in use before the packet is tunneled to the AR. Similarly the packets received on a tunnel interface from the AR, would be mapped to a particular CID using IPv4 classification mechanism.

AR performs normal routing for the packets that it receives and forwards the packet based on its forwarding table. However the DHCP

relay agent in the AR, MUST maintain the tunnel interface on which it receives DHCP requests, so that it can relay the DHCP responses to the correct MS. One way of doing this is to have a mapping between MAC address and Tunnel Identifier.

Appendix D. Network Address Translation

There is not enough IPv4 address available, private IP address domain has been used in deployment. If mobiles are assigned private IP addresses from the DHCP server located in the access network, there would be a NAT function in the Access router (AR) for address and port translation;this is a generic requirement for private IPv4 address deployment model.

Authors' Addresses

Syam Madanapalli
Ordyn Technologies
1st Floor, Creator Building, ITPL
Bangalore - 560066
India

Email: smadanapalli@gmail.com

Soohong Daniel Park
Samsung Electronics
416 Maetan-3dong, Yeongtong-gu
Suwon 442-742
Korea

Email: soohong.park@samsung.com

Samita Chakrabarti
Azaire Networks
3121 Jay Street
Santa Clara, CA
USA

Email: samitac2@gmail.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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