Transmission of IPv4 packets over IEEE 802.16's IP Convergence Sublayer

draft-ietf-16ng-ipv4-over-802-dot-16-ipcs-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 15, 2009.

Abstract

IEEE 802.16 is an air interface specification for wireless broadband access. IEEE 802.16 has specified multiple service specific convergence sublayers for transmitting upper layer protocols. The packet CS (Packet Convergence Sublayer) is used for the transport of 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 the 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 the IP-specific part of the Packet Convergence Sublayer of IEEE 802.16.

Table of Contents

1. Introduction .................................................. 3
2. Terminology .................................................. 3
3. Typical Network Architecture for IPv4 over IEEE 802.16 ...... 3
   3.1. IEEE 802.16 IPv4 Convergence sub-layer support .......... 4
4. IPv4-CS link in 802.16 Networks ............................... 5
   4.1. IPv4-CS link establishment .............................. 5
   4.2. Frame Format for IPv4 Packets ............................ 6
   4.3. Maximum Transmission Unit ............................... 7
5. Subnet Model and IPv4 Address Assignment ...................... 8
   5.1. IPv4 Unicast Address Assignment and Router Discovery ... 8
   5.2. Address Resolution Protocol .............................. 9
   5.3. IP Multicast Address Mapping ............................. 9
6. Handling Multicast and Broadcast packets in IPv4 CS .......... 9
7. Security Considerations ........................................ 10
8. IANA Considerations ........................................... 10
9. Acknowledgements ............................................. 10
10. References .................................................. 10
   10.1. Normative References ................................... 10
   10.2. Informative References .................................. 11
Appendix A. Multiple Convergence Layers - Impact on Subnet Model ........................................... 12
Appendix B. Sending and Receiving IPv4 Packets .................. 12
Appendix C. Wimax IP-CS MTU size ............................... 13
Appendix D. Thoughts on handling multicast-broadcast IP packets ........................................... 13
Authors’ Addresses ................................................. 14
Intellectual Property and Copyright Statements .................... 16
1. Introduction

IEEE 802.16 [XREF_10] is a connection oriented access technology for the last mile. The IEEE 802.16 specification includes the PHY and MAC details. The MAC includes various convergence sublayers (CS) for transmitting higher layer packets including IPV4 packets [RFC5154].

The scope of this specification is limited to the operation of IPv4 over the IP-specific part of the packet CS (referred to as "IPv4 CS" or simply "IP CS" in this document).

This document specifies a method for encapsulating and transmitting IPv4 [RFC0791] packets over the IP CS of IEEE 802.16. This document also specifies the MTU and address assignment method for the IEEE 802.16 based networks using IP CS.

This document also discusses ARP (Address Resolution Protocol) and Multicast Address Mapping whose operation is similar to any other point-to-point link model.

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].

2. Terminology

The terminology in this document is based on the definitions in [RFC5154].

3. Typical Network Architecture for IPv4 over IEEE 802.16

The network architecture follows what is described in [RFC5154] and [RFC5121]. In a nutshell, 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. From the layer 3 perspective, MS and AR are connected by a point-to-point link. The figure below illustrates the network architecture for convenience.
3.1. IEEE 802.16 IPv4 Convergence sub-layer support

As described in [RFC5154] section 3.3, an IP specific subpart classifier carries either IPv4 or IPv6 payloads. In this document, we are focussing on IPv4 over IP Convergence sublayer.

The convergence sublayer maintains an ordered "classifier table". Each entry in the classifier table includes a classifier and a target CID. In case of IP convergence sub-layer, the base-station performs the mapping between CID or service-flow ID and a corresponding GRE key for a particular IP-CS session. Also the classification takes place in Access Router based on the GRE key per service-flow and/or IP-address of the MS.

The other classifiers in Packet CS are IPv6 CS and Ethernet CS [RFC5154]. The classifiers used by IP CS, enable the differentiation of IPv4 and IPv6 packets and their mapping to specific transport connections over the air interface.

The figure below shows the IPv4 user payload over IP transport over the packet CS of IEEE 802.16:
In this document we have defined IPv4 CS link as a point-to-point link between the MS and the AR using a set of service flows consisting of MAC transport connections between a MS and BS, and L2 tunnel(s) between between a BS and AR. It is recommended that a tunnel be established between the AR and a BS based on ‘per MS’ or ‘per service flow’ (An MS can have multiple service flows which are identified by a service flow ID). Then the tunnel(s) for an MS, in combination with the MS’s MAC transport connections, forms a single point-to-point link. Each MS belongs to a different link and is assigned an unique IPv4 address per recommendations in [RFC4968]. In summary:

- IPv4-CS uses the IPv4 header fields to classify the packets and map to appropriate CID.
- Point-to-point link between MS and AR is established.

4.1. IPv4-CS link establishment

In order to enable the sending and receiving of IPv4 packets between the MS and the AR, the link between the MS and the AR via the BS needs to be established. This section explains the link establishment procedures following section 6.2 of [RFC5121]. Steps 1-4 are same as indicated in 6.2 of [RFC5121]. In step 5, support for IPv4 is indicated. In step 6, an initial service flow is created.
that can be used for exchanging IP layer signaling messages, e.g., address assignment procedures using DHCP.

The address assignment procedure depends on the MS mode - i.e., whether it is acting as a Mobile IPv4 client or a Proxy Mobile IP client or a Simple IP client. In the most common case, the MS requests an IP address using DHCP.

4.2. Frame Format for IPv4 Packets

IPv4 packets are transmitted in Generic IEEE 802.16 MAC frames in the data payloads of the 802.16 PDU (see section 3.2 of [RFC5154]).

```
0                   1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
H|E| TYPE |R|C|EKS|R|LEN |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| LEN LSB | CID MSB |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| CID LSB | HCS |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| IPv4     |
+-         +
| header   |
+-         +
| and      |
+-         +
/ payload  /
+-         +
|          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|CRC (optional) |
+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: 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

4.3. Maximum Transmission Unit

The MTU value for IPv4 packets on an IEEE 802.16 link is configurable. The default MTU for IPv4 packets over an IEEE 802.16 link is 1400 bytes. This default value accommodates for the overhead of the GRE tunnel used to transport IPv4 packets between the BS and AR and the IP-transport header. The choice of default MTU value in IPv4-CS link is determined by the present deployment of IEEE 802.16 network specifications and the legacy IPv4 client implementations where they do not typically ask for MTU configuration of the link, while DHCP servers are required to provide the MTU information only when requested. The default MTU value ensures that no packet loss happens at the L2 level due to the low-capacity IP CS link-MTU in order to accommodate the GRE encapsulation over IP-transport between the AR and BS.

However, if the deployment offers higher link MTU (1500 bytes or more), the IPv4 CS client host SHOULD configure the link-MTU before starting the IP-level communication. The following paragraph discusses different approaches through which the IPv4 CS client finds out the available link-MTU value. The discovery and configuration of a proper link MTU value ensures adequate usage of the network bandwidth and resource.

- The IEEE is currently revising 802.16 (see 802.16Rev2 [802_16REV2]) to reproduce capabilities to inform the Service Data Unit or MAC MTU in the IEEE 802.16 SBC-REQ/SBC-RSP phase, such that future IEEE 802.16 compliant clients can configure the negotiated MTU size for IP-CS link. However, the implementation must communicate the negotiated MTU value to the IP layer to adjust the IP Maximum payload size for proper handling of fragmentation. Note that this method is useful when MS is directly connected to the BS. If there is a bridge between the MS and the BS, then the negotiated MTU value will only be valid for the link between the MS and the bridge. In the bridged scenario, the default MTU (1400 bytes) is safe to use.
Configuration and negotiation of MTU size at the network-layer by using DHCP interface MTU option [RFC2132].

This document recommends that all future implementations of IPv4 and IPv4-CS clients SHOULD implement DHCP interface MTU option [RFC2132] in order to configure its interface MTU according to the access network in order to maximize the capacity of the bandwidth of the network.

Consequently, the clients are encouraged to run PMTU[RFC 1191] or PPMTUD[RFC 4821]. However, PMTU mechanism has inherent problems of packet loss due to ICMP messages not reaching the sender and IPv4 routers not fragmenting the packets due to DF bit being set in the IP packet. The above mentioned path MTU mechanisms will take care of the MTU size between the MS and its correspondent node across different flavors of convergence layers in the WiMAX networks, IEEE 802.16 networks and other types of networks such as Wi-Fi, Ethernet or 3G networks.

5. Subnet Model and IPv4 Address Assignment

The Subnet Model recommended for IPv4 over IEEE 802.16 using IP CS is based on the point-to-point link between MS and AR [RFC4968], hence each MS shall be assigned an address with 32bit prefix-length or subnet-mask. The point-to-point link between MS and AR is achieved using a set of IEEE 802.16 MAC connections (identified by CIDs) and a L2 tunnel (usually a 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.

5.1. IPv4 Unicast Address Assignment and Router Discovery

DHCP [RFC2131] SHOULD be used for assigning IPv4 address for the MS. DHCP messages are transported over IEEE 802.16 MAC connection to and from the BS and relayed to the AR. In case DHCP server does not reside in the AR, the AR SHOULD implement DHCP relay Agent [RFC1542]. Please refer to the MTU section of this document for requirements of DHCP interface-MTU option for the new IPv4 CS MS implementation.

Although DHCP is the recommended method of address assignment, it is possible that the MS could be a pure Mobile-IPv4 [RFC3344] device or Wimax Mobile-IPv4 client which will be offered an IP-address from its home-network after successful Mobile-IP [RFC3344] registration. In such situation, the mobile-client implementation SHOULD use the default link MTU in order to avoid any link-layer packet loss due to larger than supported packet size in the IP CS link.
Router discovery messages [RFC1256] contain router solicitation and router advertisements. The Router solicitation messages (multicast or broadcast) are directly delivered to AR via BS from the MS through the point-to-point link. The BS SHOULD map the all-router multicast nodes or broadcast nodes for router discovery to the AR’s IP-address and delivered directly to the AR. Similarly for router-advertisement to the all-node multicast nodes will be either unicast to each MS by the BS separately or put onto a multicast connection to which all MSs are listening to. If no multicast connection exists, and the BS does not have the capability to aggregate and de-aggregate the messages from and to the MS hosts, then the AR implementation must take care of sending unicast messages to the corresponding individual MS hosts within the set of broadcast or multicast recipients. However, this specification simply assumes that the multicast service is provided. How the multicast service is implemented in IEEE 802.16 Packet CS network, is out of scope of this document.

The ‘Next-hop’ IP-address of the IP CS MS is always the IP-address of the AR, because MS and AR are attached with a point-to-point link.

5.2. Address Resolution Protocol

The IP CS does not allow for transmission of ARP [RFC0826] packets. Furthermore, in a point-to-point link model, address resolution is not needed.

5.3. IP Multicast Address Mapping

IPv4 multicast packets are carried over the point-to-point link between the AR and the MS (via the BS). The IPv4 multicast packets are classified normally at the IP CS if the IEEE 802.16 MAC connection has been setup with a multicast IP address as a classification parameter for the destination IP address. The IPv4 multicast address may be mapped into multicast CID defined in IEEE 802.16 specification, but the mapping mechanism at the BS or efficiency of using multicast CID as opposed to simulating multicast by generating multiple unicast messages are out of scope of this document. However, it has been studied that the use of multicast CID for realizing multicast transmissions reduces transmission efficiency when the multicast group is small, due to the nature of wireless network (IEEE 802.16) [ETHCS].

6. Handling Multicast and Broadcast packets in IPv4 CS

In the IP-CS link model, two different approaches can work - 1) BS maps the multicast or Broadcast IP-addresses into different multicast CIDs of the MSs or 2) AR maps the multicast IP-addresses to different
unicast IP-addresses and send the packets directly to each MS separately.

However as mentioned earlier, handling a mechanism of multicast or broadcast IP CS packets are out of scope of this document. Please refer to Appendix section for some thoughts and suggestions.

7. 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 [XREF_10]. 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 [XREF_11].

8. IANA Considerations

This document has no actions for IANA.

9. Acknowledgements

The authors would like to acknowledge the contributions of Bernard Aboba, Dave Thaler, Jari Arkko, Bachet Sarikaya, Basavaraj Patil, Paolo Narvaez, and Bruno Sousa for their review and comments. The working group members Burcak Beser, George Weseley, Max Riegel and DJ Johnston helped shape the MTU discussion for IPv4-CS link. Thanks to many other members of the 16ng working group who commented on this document to make it better. The authors of this document offer special thanks to Gabriel Montenegro for the review of the document and providing alternative texts to many sections of this document.

10. References

10.1. Normative References


10.2. Informative References


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 [RFC4040].

Appendix B. 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 C. Wimix IP-CS MTU size

The current architecture of IPv4CS in IEEE 802.16 networks is defined in the WiMAX (Worldwide Interoperability for Microwave Access) forum [WMF]. The addressing and operation of IPv4-CS described in this document are applicable to the WiMAX networks as well. The WiMAX forum [WMF] has specified the Max SDU size as 1522 octets. However, it specifies that IP-payload in WiMAX architecture [WMF] specified network is 1400 bytes.

Hence if a IPV4-CS MS is configured for 1500 bytes it will have to be communicated by the access router (AR) about the default link MTU (1400 bytes) in WiMAX network. However, currently in IPv4 client architecture a node is not required to ask for MTU option in its DHCP messages nor the IPv4 router-advertisements are required to advertise link MTU option when the link does not support 1500 byte de-facto MTU size. An IPV4-CS client is not capable of doing ARP probing either to find out the link MTU. Thus current specifications of WiMAX network access routers cannot communicate its link MTU to the IPV4-CS MS. On the other hand, it is imperative for an MS to know the link MTU size if it is not the default MTU value for de-facto standard in order to successfully send packets in the network towards the first hop. This document can not also assume that the legacy IPv4 client implementation with IEEE 802.16 layer 2 support, would be able to dynamically sense IPV4-CS WiMAX network and adjust their MTU size accordingly.

Thus for IPV4-CS over IEEE 802.16 the default MTU size is 1400 bytes.

Appendix D. Thoughts on handling multicast-broadcast IP packets

Although this document does not directly specify details of multicast or broadcast packet handling, here are some suggestions:
While uplink connections from the MSs to the BS provide only unicast transmission capabilities, downlink connections can be used for multicast transmission to a group of MSs as well as unicast transmission from the BS to a single MS. For all-node IP-addresses, the AR or BS should have special mapping and the packets should be distributed to all active point-to-point connections by the AR or by the BS. All-router multicast packets and any broadcast packets from a MS will be forwarded to the AR by the BS. If BS and MS are co-located, then the first approach is more useful. If the AR and BS are located separately then the second approach SHOULD be implemented. An initial capability exchange message should be performed between BS and AR (if they are not co-located) to determine who would perform the distribution of multicast/broadcast packets. Such mechanism should be part of L2 exchange during the connection setup and is out of scope of this document. In order to save energy of the wireless end-devices in the IEEE 802.16 wireless network, it is recommended that the multicast and broadcast from network side to device side should be reduced. Only DHCP, IGMP, Router-advertisements packets are allowed on the downlink for multicast and broadcast IP-addresses. Other protocols using multicast and broadcast IP-addresses should be permitted through local AR/BS configuration.

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
IP Infusion
1100 Arques Avenue
Sunnyvale, CA
USA

Email: samitac@ipinfusion.com
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT 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.