IPv6 in WiMAX Networks – Challenges for Broadband Wireless

Prateek Kapadia and Abhay Karandikar

TTSL IIT Bombay Center for Excellence in Telecom

Department of Electrical Engineering, IIT Bombay Powai, Mumbai 400076

Abstract

Broadband wireless access is one of the ways to enable widespread broadband Internet access in India. Worldwide Interoperability for Microwave Access (WiMAX) is a proven technology choice for providing broadband wireless access. An Indian operator offering broadband in India today, by default, uses an IPv4 network. However, country-wide wireless broadband (several thousands of homes, and millions of mobile users) requires an addressing capacity that cannot be met by IPv4 addressing.

This article presents a review of the challenges in using IPv6 in a WiMAX network, and discusses focus areas for deployments and standards.

Introduction

WiMAX specifications are managed by the WiMAX Forum. These specifications include, by reference, the IEEE 802.16 Wireless Metropolitan Area Network set of specifications for the air-interface. IPv6 is specified by the Internet Engineering Task Force (IETF). The use of IPv6 in a WiMAX network is standardized both by the WiMAX Forum and IETF in cross-related and cross-referenced documentation (see [1], [2]).

WiMAX and Wireless MAN Standards

The Wireless MAN standard is developed by the IEEE's 802.16 Working Group. This standard defines protocols and technologies for an air-interface for broadband wireless access. The specifications include the physical (PHY) and medium access control (MAC) layers.

The 802.16 standard has evolved significantly since its inception in 1999. It was originally designed to support stationary, enterprise-class deployments. The long-term goal was to enhance the standard (along with developing technology) to the point at which it could be economically feasible to move deeper into the access towards the user. In 2003, an enhanced standard - with technology suitable for residential class applications – was released. Work had also began then to evolve the technology further, towards systems that could support mobile as well as stationary terminals, which then became part of the IEEE802.16e amendment.

The timeline below shows the evolution of the standard:

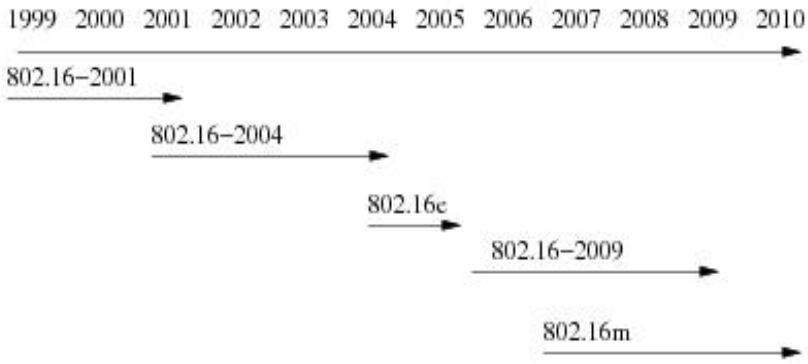

Figure 1: 802.16 Development History

The WiMAX Forum, through successive releases, adopts a particular 802.16 standard revision as its air-interface.

What is IPv6?

IPv6 is a network layer standard specified by the Internet engineering Task Force (IETF). Some of its salient features are:

1. *Large Address Space*: IPv6 extends the 32-bit IPv4 address range to 128 bits.

2. *Auto-configuration*: A device can obtain its IPv6 address by *stateless auto-configuration,* supported by the *neighbor discovery protocol* described in RFC 2461 (see [3]). The neighbor discovery protocol defines procedures for important functions, such as *Duplicate Address Detection* (DAD), address prefix discovery, next-hop discovery, *Router Discovery*, etc. The device obtains an IPv6 address in three steps: it first generates a *link local address* based on its hardware identity, then ensures uniqueness of this address using DAD*,* and finally obtains its network prefix by router discovery*.*

3. *Mobility:* Mobility is supported in IPv6 through the IETF MobileIPv6 standards (see RFC 3775, [4] and RFC 5213, [10]).

4. *Security:* IPv6 mandates use of the IPSec security protocol (see RFC 4301, [5]).

The case for IPv6 in next-generation Indian broadband access

The next-generation telecom customer will use all network services on TCP/IP. These services include peer-to-peer services, like voice, gaming, and video-conferencing. The scarcity of publicly routable IPv4 addresses would imply the use of *network address translation* (NAT)*.* However, some of these new applications may not be compatible with NAT. Thus, a large public address space will be required. This can only be fulfilled by migrating to IPv6. Further, the explosive growth of the Internet to all devices, homes and offices cannot be met with the IPv4 public address space.

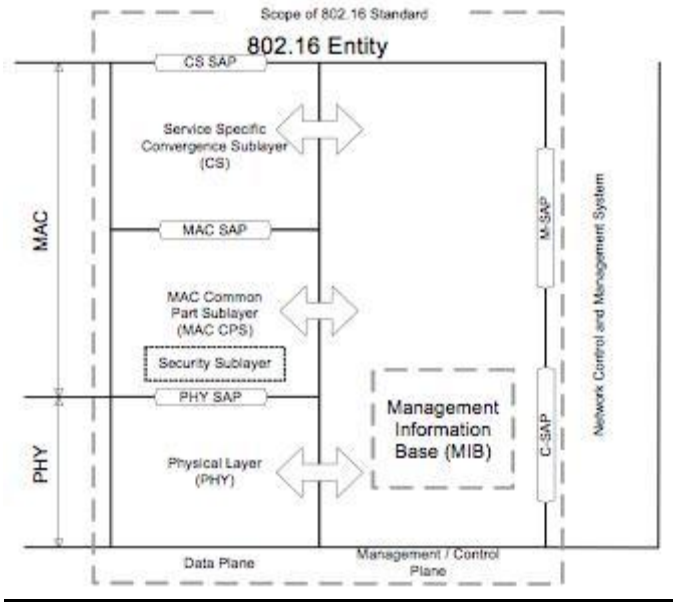

Figure 2: 802.16 Protocol Reference Model

IPv6 in a WiMAX Network

The IEEE 802.16 specifications include a *Protocol Reference Model* (Figure 2, from 802.16-2009 [6]) that defines the interfaces between the 802.16 MAC and PHY layers, and between the MAC and a *Convergence Sublayer* (CS). These interfaces are called *Service Access Points* (SAP). The CS SAP defines the interface between the MAC layer and a network layer protocol - viz. IPv4, IPv6, or ATM. The specification allows two choices for interfacing IPv6 with 802.16: either through the IPv6-over-Ethernet CS, or directly as an IPv6 CS.

The path of a packet through the CS SAP and the MAC is summarized below:

1. The IP packet is mapped to a MAC service flow.

2. The packet header is compressed, and a MAC header is appended to the packet.

3. The MAC frame is scheduled and transmitted through the PHY.

4. The MAC frame is received through PHY and decoded by MAC.

5. Packet headers are restored, by decompression and removal of the MAC header.

6. The packet is passed to the network layer.

Some other intrinsic MAC features are:

1. Radio resource management and radio link control.

2. Security for MAC layer data and control

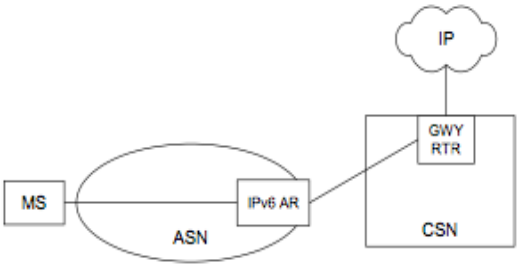

Figure 3: IPv6 in WiMAX Network Architecture

The WiMAX Forum Network Architecture, shown in Figure 3 above, shows the use of IPv6 within the WiMAX network. The IPv6 Access Router (AR) is the next-hop router for the IPv6 Mobile Station (MS). Thus, IP address and network prefix configuration is negotiated with the ASN (Access Services Network) hosting this AR.

Challenges in Deploying IPv6 over 802.16

Several reports (see Ksentini [7], Lee et al [8], RFC 5154 [9]) have identified challenges in implementing IPv6 over the 802.16 air-interface. The current working draft of the WiMAX Forum Network Architecture Release 1.5 (see [2]) attempts to overcome these challenges and incorporates some solutions from these reports.

Some of the important challenges are:

1. IPv6 CS: Neighbor discovery packets need to be sent *before* an IP address is assigned to the MS. Since there is no destination MAC address in 802.16, and the source 6-byte MAC is not sent on each frame, a special procedure needs to be devised.

2. IPv6 CS: The 802.16 is a point-to-point MAC on the uplink. Thus, each MS and AR pair is a separate subnet. This implies that router advertisements need to be unicast to each MS.

3. IPv6-over-Ethernet CS: Multicast *Neighbor Discovery*, *Duplicate Address Discovery*, and *Router Discovery* messages can be exchanged in this CS; however, it is advisable to filter multicast messages so that MS that do not require these messages are not woken from idle or sleep mode.

These issues have been addressed to a large extent by the current set of standards. The state-of-art issues in implementing IPv6 in the WiMAX network are as below:

1. IPv6 CS and IPv6-over-Ethernet CS are *optional* in the present network architecture (see [2]). IPv6 CS needs to be mandated, IPv6-over-Ethernet CS may be optional. RFC 5121 (see [1]) also mandates that the WiMAX network support IPv6 packet transfers between MS and BS, if both MS and BS want to use IPv6.

2. *Initial Service Flow* (ISF) establishment procedures allow for router advertisement and solicitation. However, the use for *Duplicate Address Detection* (DAD) for IPv6 CS is not clear. Standards should perhaps include mechanisms to exclude DAD from point-to-point links.

3. The requirement for filters for downlink multicasts is specified. However, the filtering procedures and messages that must be filtered for proper use of IPv6-over-Ethernet are yet to be specified.

Conclusion

IPv6 operation in a WiMAX network needs to be carefully implemented in the standards. Subsequently, the Indian operator must carefully validate its choice of equipment to ensure that an interoperable IPv6 network can be rolled out to meet the capacity and application demands of the near future.

References

[1] "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", RFC 5121, February 2008

[2] "WiMAX Forum Network Architecture Release 1.5", November 2009

[3] "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998

[4] "Mobility Support in IPv6", RFC 3775, June 2004

[5] "Security Architecture for the Internet Protocol", RFC 4301, December 2005

[6] "802.16-2009 IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems", September 2009

[7] Adlen Ksentini, "IPv6 over IEEE 802.16 (WiMAX) networks: Facts and challenges", *Journal of Communications* (*Vol. 3, No. 3*), July 2008

[8] Lee, Han, Shin, Jang and Kim, "Considerations of Neighbor Discovery Protocol over IEEE 802.16 Networks", *International Conference on Advanced Communication Technology*, 2006

[9] "IP over IEEE 802.16 Problem Statement and Goals", RFC 5154, April 2008

[10] "Proxy Mobile IPv6", RFC 5213, August 2008

Author Biographies:

Prateek Kapadia is Senior Manager at TTSL-IITB Centre for Excellence in Telecom at IIT Bombay. He is a

voting member in 802.16, and an active contributor to the 802.16m MAC layer. He is also pursuing his PhD in Computer Science on Analytical Models for Wireless Coverage. From 2003 to 2009, Prateek was employed as General Manager at Reliance Communications, where he contributed to planning, engineering and operations management of wireless packet data networks. From 1997 to 2002, Prateek designed and implemented cryptographic security layers in firewalls, VPN devices and mobile applications platforms.

Abhay Karandikar earned his MTech. and PhD degrees in Electrical Engineering from the Indian Institute

of Technology, Kanpur in 1988 and 1994, respectively. From 1994-97, he worked at the Center for Development of Advanced Computing (C-DAC), As Team Coordinator, he led the team on high-speed interconnection network design of the PARAM 9000 supercomputer, and several other high-speed networking projects in C-DAC. He joined the Department of Electrical Engineering, IIT Bombay in April 1997, where he is currently Professor. At IIT Bombay, he started many technology development projects, including the one on Open Source MPLS and Linux based MPLS emulator. He co-founded the venture backed company Eisodus Networks focusing on Metro Ethernet. He is leading TTSL-IIT Bombay Center for Excellence in Telecom. Dr Karandikar has supervised many PhD and Masters theses and published in several international and national journals and conferences. His research group at IIT Bombay is currently focused on resource allocation in wireless networks. He is a working group member of IEEE 802 and has recently made several contributions to IEEE 802.1 Carrier Ethernet and 802.16m WiMAX standard. Dr Karandikar has lectured extensively in various international forums and given tutorials in IEEE GLOBECOM, MILCOM. He has been awarded with Best Teacher award of IIT Bombay.