IPv6 over IEEE 802.16 (WiMAX) networks: Facts and challenges

Adlen Ksentini
IRISA, University of Rennes 1, Rennes, France
Email: {adlen.ksentini}@irisa.fr

Abstract— **Deploying the new generation "Internet Protocol" (IPv6) over 802.16-based wireless networks is facing an important challenge as the IEEE 802.16 standard is failing to support IPv6 functionalities. In fact, unlike the other 802 standards, the IEEE 802.16 is based on a point-to-multipoint (PMP) communication model, where no direct connection (at the MAC layer) is possible between two stations, all communications pass through the Base Station. As a result, the 802.16 standard is unable to handle any form of IP multicast (group) communication, and hence it can not sustain the new functionality of IPv6, namely auto-configuration mechanism, which particularly relies on IP multicast communication.**
In this paper, we present different architectures to consider when deploying IPv6 over wireless broadband network, such as WiMAX. Also, we point out challenges and solutions related to this deployment, by focusing particularly on solutions proposed by the 16ng IETF group, which aims to establish an Internet RFC on deploying IPv6 over IEEE 802.16.

Index Terms— **IPv6, IEEE 802.16, IEEE 802.16e, Multicast, WiMAX**

I. INTRODUCTION

Wireless communication has known a huge development since the last decade. Different technologies have emerged to propose connection to the Internet through wireless communications such as IEEE 802.11 (WiFi), 3G and IEEE 802.16 (WiMAX). Among these technologies, IEEE 802.16 [1] is "defacto" standard for broadband wireless communication. It is considered as the missing link for the "last mile" connection in Wireless Metropolitan Area Networks (WMAN). It represents a serious alternative to the wired network, such as DSL and cable-modem. Besides Quality of Service (QoS) support, the IEEE 802.16 standard is currently offering a nominal data rate up to 100 Mega Bit Per Second (Mbps), and a covering area around 50 kilometres. Thus, a deployment of multimedia services such as Voice over IP (VoIP), Video on Demand (VoD) and video conferencing is now possible, which will open new markets and business opportunities for vendors and service providers.

Meanwhile, the growth of the wireless industry (both cellular and wireless network) has been nothing short of phenomenal. From the carriers' perspective, especially those supporting multiple media access types (e.g. 3G and WiMax), leveraging IP as the method of transporting and routing packets makes sense. Cell phones and PDAs can already access the Internet, play games with other users, make phone calls, and even stream video content. Instead of supporting all of these functions using different transport protocols and creating intermediary applications to facilitate communications, it is far more efficient to leverage the existing network infrastructure of the Internet and a company's network. However, the fact that these new technologies use IP for maintaining connectivity, increases the problem of scarcity of IP addresses. Actually, the IPv4 address space is not sufficient to connect all the new devices (PDA, Cell phones, ..) introduced by the wireless industry. To solve this constraint, IPv6 is designed to replace IPv4 and extends the address space from 32 bits to 128 bits, providing an IP address for every grain of sand on the planet. IPv6 is not only extending the address space, but it is also considered as a new protocol designed to handle the growth rate of the Internet and to cope with the demanding requirements on services, mobility, and end-to-end security. Perhaps the most interesting new feature of IPv6 is its stateless autoconfiguration mechanism, known as the Neighbor Discovery Protocol (NDP). When a booting device comes up and asks for its network prefix, it can get one or more network prefixes from an IPv6 router on its link. By using this prefix information, it can autoconfigure for one or more valid global IP addresses by using either its MAC identifier or a private random number to build a unique IP address. It is worth mentioning that NDP procedures rely on the lower layers' capacity to handle multicast communication, which is a technique to establish communication from one to many over an infrastructure. Multicast mechanism uses the network resources efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers.

IEEE 802.16 network is different form existing IEEE 802.X standards by the fact that it is based on a point-to-multipoint architecture, where no direct communication is authorized (at the MAC layer) between two stations, all communications start and end at the Base Station (BS). Therefore, multicast communication is not supported by the IEEE 802.16, which bothers the deployment of IPv6 procedures (NDP) over WiMAX architecture. According to the IEEE 802.16 standard, there is no description of the IPv6 operations over WiMAX, rather only specification on how to encapsulate IP packet in a 802.16 frame is provided. Since IPv6 is an IETF (Internet Engineering Task Force) specifications, a special group namely 16ng

This work was supported in part by FP6 IST Anemone Project

was formed to tackle the challenge of supporting IPv6 over WiMAX. Beside the lack of multicast support, the 16ng group depicted other issues that prevent from deploying IPv6 and NDP procedures over 802.16 such as: subnet model, the BS architecture, and the initial Suscriber Station (SS) connections.

The challenge of deploying IPv6 over WiMAX has also interested the WiMAX forum, which is constituted by a consortium of industrials [2] that aims to certificate WiMAX products. The WiMAX forum has contributed to this topic by proposing a model for deploying IPv6 over WiMAX. The proposed architecture gives specification on how SS, BS and Access Router (AR) interact at IPv6 level as well as WiMAX level. Our purpose in this paper is to show how the 802.16 standard can be effectively utilized to successfully deploy and support IPv6 procedures. In this context, we will review proposed network architectures as well as research activity done by the 16ng group and the network community.

The remainder of this paper is organized as follows: Section 2 introduces the background materials concerning the 802.16 MAC layer and the IPv6 autoconfiguration mechanism. Problems rising from deploying IPv6 over 802.16-based networks are presented and analyzed in section 3. Besides describing and analyzing the proposed solution, particularly those of the 16ng group, we give some directions that are still open for discussion in section 4. Finally, Section 5 concludes this paper.

II. Background and Related Work

A. The IEEE 802.16 standard

Like the other IEEE 802 standards, the 802.16 gives specifications for the MAC and Physical layer functionalities. The Physical layer of IEEE 802.16 operates in 10-66 GHz (IEEE 802.16) or 2-11 GHz (IEEE 802.16a) band and supports data rate in the range of 32-130 Mbps depending on the bandwidth of operation as well as the modulation and coding schemes. In the 10-66 GHz band, the signal propagation between BS and SS should be line-of-sight and single carrier modulation is used. WirelessMAN-SC is the air interface specification for IEEE 802.16 operating in this frequency band. In contrast, IEEE 802.16a operates in the 2-11 GHz band and supports nonline-of-sight communication. In the 10-66 GHz band, channel bandwidth of 20, 25, or 28 MHz can be used. For modulation, Quadrature Phase-Shift Keying (QPSK), 16-QAM and 64-QAM can be used depending on the channel quality (i.e., signal-to-noise ratio (SNR) at the receiver). The system uses a frame size of 0.5, 1, or 2 ms for transmission and a frame is divided into subframes for downlink and uplink transmissions.

At the MAC layer, the IEEE 802.16 network is viewed as a point-to-multipoint connection where all data communications, for both transport and control, are in unidirectional connection. The BS grants resources to the SS on demand. For this purpose the wireless medium is divided into uplink and downlink frames. The MAC-layer has support for both TDD (Time Division Duplex) and FDD (Frequency Division Duplex) framing, where TDD separates uplink and downlink in time and FDD separates them by frequency. Figure 1 shows how physical slots make a general TDD frame structure. The frame size can be varied in accordance to different physical profiles. The partition of the frame between uplink and downlink can also be adjusted. The downlink frame goes from the BS to SS, so there is no need for sharing these time slots among the different SS as only the BS sends data. In this frame, the BS announces the schedule of the upcoming uplink frame through the Uplink Map (UL-MAP) messages. That is, the set of SS allowed to transmit on uplink direction. The uplink frame on the other hand, contains information sent from the SS. Therefore, there is no direct connection between two SS belonging to the same cell.

Besides, the SS has the possibility to send a bandwidth request per connection. This can be done through the introduction of a Connection Identifier (CID), ensuring thus an identification of the traffic per connection rather than per station. Even though all data in IEEE 802.16 are broadcasted to air shared to all SS, only SS associated with the CID included in the transmitted frame can access to the content. At the BS, SS's traffic is handled per CID and hence there is no need to use the MAC address for identifying destination, which constitutes a major difference by report to the other 802.X standards.

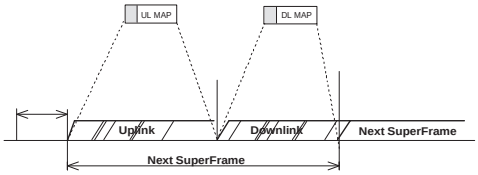

Figure 1. The IEEE 802.16 superframe - TDD fashion

Concerning QoS support, the 802.16 standard proposes to classify, at the MAC layer, the applications according to their QoS service requirement (real time applications with stringent delay requirement, best effort applications with minimum guaranteed bandwidth) as well as their packet arrival pattern (fixed / variable data packets at periodic / aperiodic intervals). For this aim, the initial standard proposes four classes of traffic, and the 802.16e [3] amendment adds another class:

- Unsolicited grant service (UGS): supports Constant Bit Rate (CBR) services, such as T1/E1 emulation and VoIP without silence suppression.
- Real-time polling service (rtPS): supports real-time services with variable size data on a periodic basis, such as MPEG and VoIP with silence suppression.
- Extended rtPS : recently introduced by the 802.16e standard, it combines UGS and rtPS. That is, it guaranties periodic unsolicited grants, but the grant size can be changed by request. It was specially introduced to support VoIP traffics [3], [4].
- Non Real-Time Polling service (nrtPS): supports non real-time services that require variable size data bursts on regular basis, such as File Transport Pro-

tocol (FTP) service.
- Best effort (BE): for applications that do not require QoS such as Hyper Text Transfer Protocol (HTTP).

Each SS requiring a connection has to include its needs on QoS by specifying which class will be used. The 802.16

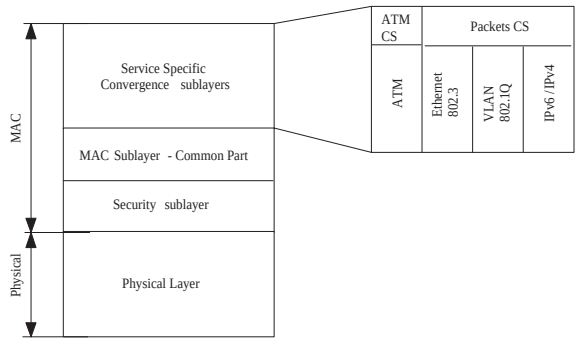

Figure 2. The IEEE 802.16 MAC layer

MAC layer is constituted by two sublayers: the convergence sublayer and the common part sublayer (as depicted in 2). The convergence sublayer maps the transport-layer-specific traffic into the core MAC common part sublayer. As the name implies, the convergence sublayer handles the convergence of Asynchronous Transfer Mode (ATM) cells and IP packets, so the MAC layer can support both ATM services and packet services, such as IPv4, IPv6, Ethernet, and Virtual Local Area Network (VLAN) services. It is worth mentioning that most predominant CS sublayers in today's WiMAX products are the IP CS and Ethernet CS. The common part sublayer is independent of the transport mechanism, and is responsible for fragmentation and segmentation of the Service Data Units (SDUs) into MAC protocol data units (PDUs), QoS control, and scheduling and retransmission of MAC PDUs. The convergence sublayer classifies the incoming SDUs by their type of traffic (voice, web surfing, ATM CBR,) and assigns them to a service flow using a 32-bit Service Flow ID (SFID). Here, if the IP CS is used, then the SDUs are classified according to: (i) IP addresses (destination and source); (ii) Transport (TCP or UDP) Ports (destination and source); (iii) Type of service field. If the Ethernet CS is used, then the SDUs are classified according to: (i) Ethernet addresses (source and destination); (ii) user field priority. When the service flow is admitted or active, it is mapped to a MAC connection that can handle its QoS requirements using a unique 16-bit CID. A service flow is characterized by a QoS Parameter Set that describes its latency, jitter and throughput assurances. With Adaptive Burst Profiling, each service flow is assigned a PHY layer configuration (i.e. modulation scheme, Forward Error Correction scheme, etc) to handle the service.

Once the service flow is assigned a CID, it is forwarded to the appropriate queue. Uplink packet scheduling is done by the BS through signalling to the SS. At the SS, the packet scheduler will retrieve the packets from the queues and transmit them to the network in the appropriate time

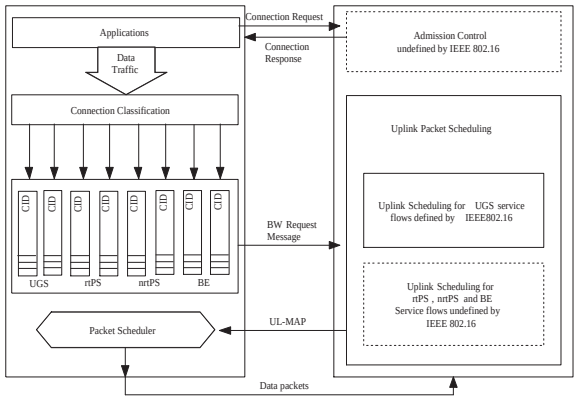

Figure 3. MAC procedures

slots as defined by the UL-MAP sent by the BS. This is illustrated in Figure 3.

B. IPv6 and Auto-configuration

IPv6 is the *next generation* protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 (IPv4). IPv6 fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses. It also adds many improvements to IPv4 in areas such as:

- Stateless address autoconfiguration
- Native multicast support
- Network layer security by integrating IPsec (IP security) in the protocol specification
- Native mobility support through MIPv6 (Mobil IPv6)

IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during a transition period.

Auto-configuration is one of new functionalities introduced by IPv6 [5]; it allows an automatic setting of Host's IP address. This mechanism in fact, enables a plug-and-play networking of hosts while avoiding the administration overhead. IP addresses are allocated to each network interface of a node. An interface using IPv6 usually gets a link-local address and a global address, which are allocated at least. Link-local address is used for control functions, while global address is used for usual data communications. In IPv4, only one address is allocated for one interface as a basic rule. But in IPv6 there is no such limitation.

In IPv6, 128 bit IP address is constituted by two identifiers: network prefix, which identifies network, and interface ID, which identifies a node (interface). Interface ID is configured by the node on its own, and prefix is notified by the network (usually router). The combination of this information constitutes an IPv6 address.

In the following, we present the actual procedure used by IPv6 to auto-configure address:

- The new entering node on the network generates link local address and allocates it to the interface. Link-local address has the following form: fe80::/64.

- The node confirms that generated link local address is not already used on the same network, by employing the Duplicate Address Detection (DAD) procedure. At first, the node transmits Neighbor Solicitation (NS) message on the network. If another node is already using the same address, this node sends Neighbor Advertisement (NA) message. If no NA is received after a certain time, the node that transmitted NS message will use the original link-local address. Otherwise, if the new node is notified of the duplicate address situation, it will not allocate the link-local address and terminates the interface.
- By using the allocated link-local address, the new node sends the Router Solicitation (RS) message to request information. Here, the RS message transmission is trivial, so the node can passively wait for next step.
- The node that received RS message (usually a router) sends back Router Advertisement (RA) message. RA message is transmitted periodically, so nodes do not necessarily have to send RS message.
- The node receives RA and gets IPv6 address prefix.
- Finally, the node forms the global IPv6 address by combining prefix and interface ID, just as it did for link-local address.

It should be noted that RA sender, such as router, only sends fixed prefix allocated to the network. In other words, RA sender does not care to whom it sent information. It does not maintain such records. Therefore, if two routers exist on the same network and advertise different prefixes with RAs, receiving node automatically gets both RA to allocate different address on the same interface.

III. Deploying IPv6 over IEEE 802.16

One of the originality introduced by IPv6 is the station's ability to set up automatically an IP address, thanks to the NDP procedures that allows this autoconfiguration. However, when considering IPv6 over a wireless broadband architecture such as 802.16, there are some challenges to fix. These challenges are particularly related to the fact that IEEE 802.16 standard is failing to support NDP procedures. Further, other reasons can block the deployment of IPv6 over WiMAX such as: (i) the IP multicast support; (ii) the IPv6 subnet model to consider; (iii) BS and AR interaction; (iv) the transport connection for IPv6 signalling. In this section, we review the main problems introduced by the IEEE 802.16 architecture that prevents deploying NDP procedures and hence IPv6 over such networks.

Before presenting the above issues, we introduce the key elements constituting the IEEE 802.16.

- SS or Mobile Station (MS): A mobile station is always a SS which must provide mobility function.
- BS: Generalized equipment set providing management and control of SS-BS connections. A transport connection is unidirectional mapping between BS and SS MAC peers for the purpose of transporting a service flow's traffic.
- AR: Generalized equipment set providing IP connectivity between BS and IP based network. An AR performs first hop routing function to all SS.

A. Multicast support

Most of the NDP procedures such as address configuration and Router Discovery are based on multicast communication. These procedures use multicast addresses rather than broadcast addresses in order to reach a group of users. Since 802.16 follows the PMP architecture without bi-directional connection, there is no native support of multicast without an explicit support on the network side (BS). Multicast communication is possible only in the downlink frame. Hence, the SS have not the ability to use multicast addressing on the uplink frame, only the BS can send multicast packet associated with a multicast CID. Unlike other 802-based standard such as Ethernet, the 802.16 is not able to map directly the IP multicast addresses into layer 2 multicast addresses. By consequence, there is a need for a procedure to associate multicast IPv6 addresses with a CID at the 802.16 MAC layer. Further, as NDP uses multiples multicast addresses (Router Solicitation, Router Advertisement, Prefix user), the BS must handle multiple multicast connections.

B. Subnet or Link Model

The IPv6 subnet or model to consider has an important impact on the NDP functionalities. Depending on how the SS, BS and AR are organized on IP subnet, some NDP functionalities are obsolete. Here, by IP Subnet we mean a topological area that uses the same IPv6 address prefix, where that prefix is not further subdivided except into individual addresses. Accordingly, we distinguish two IPv6 prefix assignment procedures: (i) per station prefix; (ii) shared prefix.

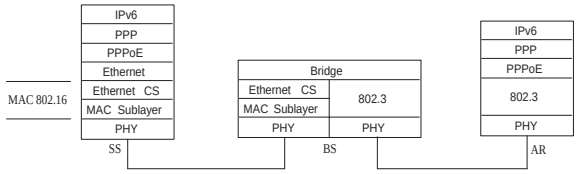

Figure 4. Point-to-point link model based on Ethernet CS

1) Per station IPv6 prefix: This link model is usually known as the point-to-point link model. In this case, each SS under a BS resides on different IP subnets. Hence, only a SS and an AR exist under an IPv6 subnet and IPv6 packets with destination address of link local scope are delivered only within the point-to-point link between a SS and an AR. For this link model's deployment, one solution is to use the PPP (Point-To-Point Protocol) protocol, which was widely employed for this kind of point-to-point link. However, the direct use of PPP is not possible on the 802.16 network, since the 802.16 does not define a CS sublayer that can encapsulate and decapsulate PPP frames. Consequently, in case of IPv6 CS sublayer,

using this link layer model needs another mechanism to provide a point-to-point link between a SS and an AR. The second option is to utilize the PPP over Ethernet by using the Ethernet CS, which implies the use of the PPPoE stack [6]. Figure 4 shows an example of the point-to-point architecture and its network stacks when using the Ethernet CS.

2) Shared IPv6 prefix: In this link model, all SS are assumed under an AR and reside on the same IP subnet, even when SS are connected with different BS. To implement this model there are two solutions, the first one consists of using the IPv6 CS sublayer and the second one employs the Ethernet CS sublayer. Figure 5 illustrates a high level view of this link model based on IPv6 CS. The link between the SS and the AR at the IPv6 layer is viewed as a shared link, and lower link between the SS and BS is a point-to-point link. This point-to-point link between the SS and BS is extended all the way to the AR when the granularity of the tunnel between the BS and AR is on a per station basis. The

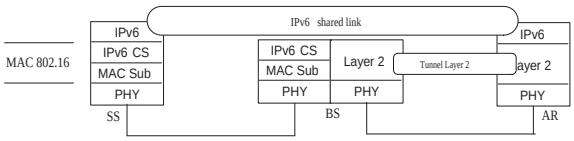

Figure 5. Shared IPv6 prefix based on IPv6 CS

second way of establishing this link model is to use the Ethernet CS. This model is known as the Ethernet like link model. It assumes that underlying link layer provides the equivalent functionality like Ethernet, for example, native broadcast and multicast. Further, the BS in this model has to implement Bridge functionality. We show in Figure 6 the architecture of the Ethernet like model. There

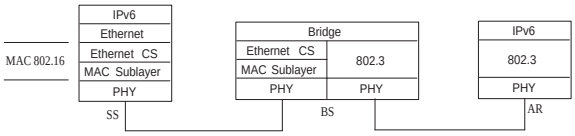

Figure 6. Shared IPv6 prefix based on Ethernet CS (Ethernet like link)

exists however, a discrepancy between the assumption from the Ethernet like link model and the 802.16's MAC feature which is connection-oriented and not providing multicast and broadcast connection for IP packet transfer. Furthermore, the frequent IPv6 multicast signalling within the IPv6 subnet like Ethernet results in the problem of waking up dormant SS.

3) IPv6 functionalities according to the CS layer: Depending on which CS sublayer is deployed at the 802.16 MAC layer, many IPv6 functionalities are employed with difficulty, whereas others functionalities are deployed easily. Here, we consider that 802.16 link models are based on either:

- IP sublayer, in case of point-to-point link like model.
- Ethernet sublayer, in case of Ethernet link like model.

Figure 7 shows the main IPv6 functionalities required when considering both link models. If the deployed model is a point-to-point connection, like 3G, separate prefix are assigned to each SS. Thus, the DAD is completely trivial as there is no need to check the duplication of an IPv6 address. Further, the address resolution process is not essential, since the 802.16 MAC cache is not used as a part of the 802.16 frame. Although that Network Unreachability Detection (NUD) is not trivial, nonetheless it can be used to verify the AR survivability. Here, the point that needs some enlightenment is the Router Discovery procedure. Actually, it is not clear whether source link layer address need to be carried in the RS. The RS may need to have source IPv6 address specified so that the RA can be sent back. For sending periodic RA messages, the AR has to send them by using separate IPv6 prefix through a unicast manner for each SS explicitly.
When considering Ethernet CS, the IPv6 prefix is obviously shared between the SS. In this case, all the IPv6 functionalities must be employed.

- Address Resolution: this mechanism is needed, since there is a mapping between the Ethernet address and the IPv6. Although this mapping is not essential for the 802.16, the BS can use the encapsulated MAC address in order to reach the destination when this one is not in the same network (in case of Bridge). In case, when the destination IP address has the same prefix, the Ethernet address is a part of the Ethernet header (as the destination address). To obtain this address, the NDP procedure is needed.
- NUD: this procedure is deployed to check all the addresses used in the IPv6 network (SS with the same prefix), including all the SS and the AR.
- Address Auto-configuration: As a part of this procedure, the DAD is highly required in this configuration. In fact, it is important to check the existence of duplicate addresses, as the IPv6 prefix is shared between the SS.
- Router Discovery: This procedure is strictly required, but its activation can cause some problems. These problems are linked to the energy dissipation constraint, which constitutes an important issue in case of mobile environment. In fact, the DAD procedure uses all-node multicast address, therefore the dormant SS have to wake-up and handle the periodic DAD messages, which introduce a problem of energy consumption.

4) Multilink issue: The IPv6 prefix link model eventually results in multi-link subnet problems [7]. In fact, this problem rises when either a procedure or a protocol assumes that a relationship exists between the Time To Live (TTL) and the number of hop. Many applications (or protocols) use the TTL to give the scope of the packet. For instance, if the TTL is equal to 1, the packet is considered for a local scope. In case when this packet is passing through a router the TTL is decremented, changing thus

Figure 7. IPv6 required functionalities according to the link model

Link Model	CS sublayer	Address Resolution	Router Discovery	NUD	Address Autoconf
Point-to-POint	IP	No, 802.16 Neighbor cache is not used in a part of 802.16 frame	Not clear	Only to check the AR	DAD is not trivial
Ethernet	Ethernet	Yes, needs an address resolution	Periodically an AR is sent	Required for all the SS as well as the AR	Required

the scope of the packet. Now, if we assume that BS assigns separate 802.16 connections for SS, then these SS will be regarded as located on different links. In this situation, distributing shared IPv6 prefix for SS that are placed on the different links implies that all packets must go through the AR in order to reach other SS (no direct communication is allowed between two SS), which cause the multi-link subnet problems (as the AR decrements the TTL, changing thus the scope of the packet). This is valid for IP CS and even to the Ethernet CS if any bridging functionality is not implemented on top of BS or between BS and AR.

5) Connection set-up: Another important think to consider when deploying IPv6 over IEEE 802.16, is how a SS enters the networks and auto-configure its IPv6 address. In IEEE 802.16, when a SS enters the networks it gets three CID connections to set-up its global configuration. The first CID is usually used for transferring short, sensitive MAC and radio link control messages, like those relating to the choice of the physical modulations. The second CID is more tolerant connection, it is considered as the primary management connection. With this connection, authentication and connection set-up messages are exchanged between SS and BS. Finally, the third CID is dedicated to the secondary management connection. This connection is employed to deploy service such as Dynamic Host Configuration Protocol (DHCP) and Trivial FTP (TFTP). From the IPv6 point of view, there is no indication about which CID is dedicated to the NDP procedures. IPv6 needs different connections since there are different management messages to transmit like: DAD, Router Solicitation as well as Router Advertisement.

IV. Issues and directions

In order to resolve the problems arose from deploying IPv6 over 802.16, the 16ng group has identified different points to tackle, and it give some directions to follow for solving these points. In this section, we present the solutions currently presented as well as the remaining open issues regarding the deployment of IPv6 over 802.16-based networks.

A. Multicast/Broadcast

From the points depicted in the above section, it is obvious that there is a strong need for using multicast communications when deploying IPv6, particularly for the NDP procedures. Thereby, it is desirable to have a model for IP multicast as well as IP broadcast in 802.16. The solution actually proposed in the 16ng group consists of using a CID dedicated to multicast, namely mCID [8]. For this aim the original CID field is replaced by mCID format as depicted in Figure 8. mCID consists of mCID prefix, CS, and scope field. The mCID prefix is used to indicate that a multicast packet is embedded in an IEEE 802.16 frame. CS field determines which CS sublayer is used (1 if IP CS, 0 if Ethernet CS). However, the actual version of the draft does not indicate how the mCID is initiated and distributed to the SS participating to a multicast group. Besides the solution proposed by the 16ng group, there

Figure 8. Multicast CID

are others solutions proposed in the literature. In [9] the authors propose to use an intermediate layer between the IP layer (or Ethernet) and the 802.16 Convergence Sublayer (CS), namely Multicast Relaying Part (MRP). This layer is dedicated to NDP procedures and introduced in the SS stations as well as the AR (see Figure 9). When a multicast packet is issued either at IPv6 layer or Ethernet layer, the MRP layer captures this packet and sent it to the AR. The AR's MRP layer checks the mapping table and sent this multicast packet to the SS involved in this address through a repeated unicast transmission. However, the weakness of such solution is the overhead introduced when a multicast packet is replaced by a repeated unicast transmission, which eliminate the benefit of using multicast. In [10], an emulation of the multicast procedure is

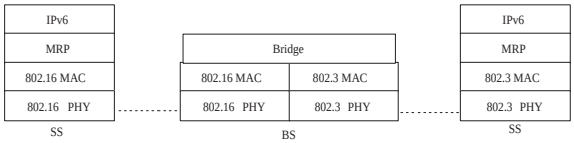

Figure 9. MRP architecture

presented. The authors propose to concentrate at the BS all procedures related to handling and managing multicast packets (centralized fashion). Thus, when receiving a multicast packet, the BS has to decide if there is a need to apply a selective decision in order to optimize the air resource. Here, the selective decisions are:

- Some types of multicast traffic may be filtered off and be dropped by the BS
- Some types of multicast traffic such as all-nodes multicast may be delivered in a unicast manner to all SS
- Some types of traffic such as solicited-node or routers multicast may be delivered in a unicast manner to the some of nodes (its members).
- Some types of traffic may be forwarded to as specific node.
- Some types of traffic may be delivered by using a shared CID.

Although these solutions work well, they do not consider the multilink problem as well as the heterogeneity of the CS sublayer. In fact, all these solutions assume that the same CS sublayer is used by all SS, which is not realistic since each SS selects locally the CS sublayer. This problem will be discussed in section 4.3.

B. BS and AR architecture

1) Common architectures: Another point which is not clear yet, is the interaction between the Base Station and the AR. In fact, there are two predominant solutions.

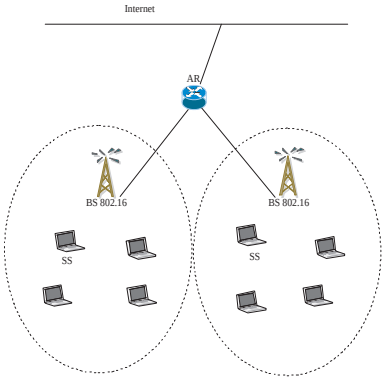

Figure 10. BS and AR are separated

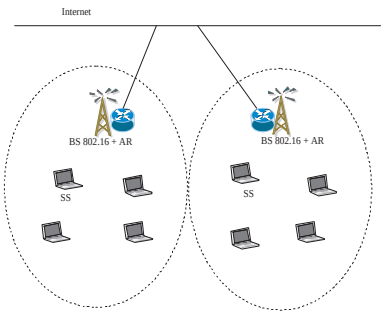

Figure 11. BS and AR are located in the same box

- The BS and the AR are separated (Figure 10): In this case, it is important to consider the link between the AR and the BS, and how the BS can act as a gateway between the 802.16 network and the AR (at the link layer). This would be very challenging if we consider that the link between the AR and BS is Ethernet-based. Unlike 802.11 where the AP can act as a gateway by implementing a Logical Link Control (LLC) layer that permits to translate 802.11 frames to 802.3 frames. In 802.16 there is no LLC layer, so it is not easy to convert 802.16 frame to 802.3 frame directly. In addition to this, the BS can not directly see the destination Ethernet address of the uplink packets.
- The BS and the AR are located at the same box (Figure 11): In this case, a subnet consists of only one single router and single BS. This alternative is very useful as all IPv6 functionalities can be implemented without consideration about the underlying network implementation. The AR/BS is always the end-point at both IP and 802.16 levels.

By taking into account these two solutions, it is not very realistic and not optimal to tell the 802.16 Network providers to use the second solution as the cost will be very high. So, most implementation separates the BS from the AR, and use a single AR that covers a set of interconnected BS. For more details about the different scenarios and architectures to consider reader can refer to [11].

C. WiMAX forum Architectures

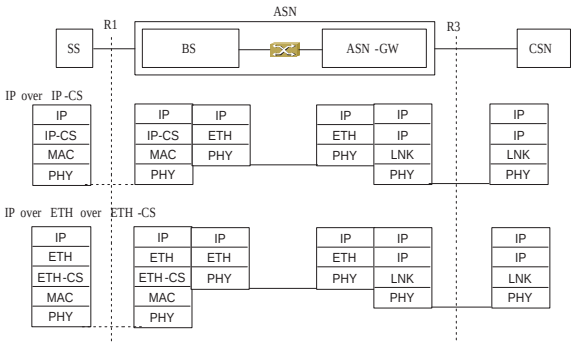

Figure 12. BS and AR are connected by a Switch

The WiMAX forum has recently described specifications for different architectures in order to deploy IPv6 over WiMAX. The WiMAX forum proposes to regroup the BS and AR into one entity named the Access Service Network (ASN). It has a complete set of functions such as AAA (Authentication, Authorization, Accounting), Mobile IP Foreign agent, Paging controller, and Location Register to provide radio access to a WiMAX Subscriber. The Connectivity Service Network (CSN) offers connectivity to the internet. In the ASN, the BS and AR (or ASN-Gateway) are connected by using either a Switch or Router. Figure 12 shows the case of connecting the AR and BS by an Ethernet Switch. In this architecture the ASN has to: (i) support Bridging between all its R1 interfaces and the interfaces towards the network side; (ii) forward all packets received from any R1 to a network side port; (iii) flood any packet received from

a network side port destined for a MAC broadcast or multicast address to all its R1 interfaces. Furthermore, direct communication between SSs is not available by the Bridging in the ASN. Figure 13 represents the case

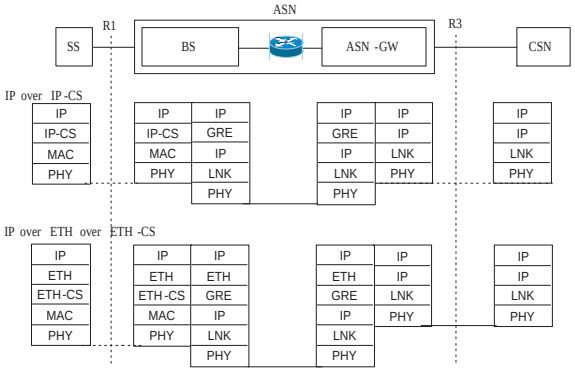

Figure 13. BS and AR are connected by a Router

of connecting the BS and AR in the ASN through a router. Here, a Generic Routing Encapsulation (GRE) tunnel is used between the BS and AR in order to establish a point-to-point connection (at IPv6 level) between the SS and AR. This architecture is based on shared IPv6 link model and all the SS are connected by point-to-point links to the AR. At this point, the SS can not communicate directly; all the traffic goes through the AR. Emulation of shared link behaviour is done by an Authoritative Address Cache and Relay DAD.

D. Subnet Model

There are some issues concerning the subnet model, which are not fixed yet. In fact, it is very important to develop link model solution without being related to a CS sublayer. Since the choice of the CS sublayer is locally decided at the SS station, probably we can found in the same 802.16 network SS using IP CS and other using Ethernet CS. One solution will consist in introducing a negotiation between the BS and SS to choose a common CS layer for all SS belonging to this BS, or to propose a default CS sublayer that must be implemented by all WiMAX producets (and others CS can be implemented optionally). Another problem rising from the subnet model choice is the multilink problem. That is, two SS having connection to the same BS and can be viewed as two physical links. One solution is to filter at the AR the packets with link local destination addresses and relay them to the destination without decrementing the TTL.

E. Mobility

By introducing the 802.16e amendment, SS are now considered mobile and can roam across different cell covered by different BS. This mobility support leverages the 802.16-based networks, allowing them to be a direct concurrent to the 3G networks.

Meanwhile, IPv6 handles mobility through the Mobile IPv6 procedures. These procedures track node mobility by using the DAD mechanism, which permit to detect that the default router is no longer bi-directionally reachable (in case of moving from one subnet to another). In this case, the mobile node must discover a new default router. These procedures however, introduce a high latency since the mobility information are handled at the IP layer. To tackle this issue the Fast handover procedure (FMIPv6) is introduced [12]. It deals with some handover process, such as the configuration of Care of Addresses (CoA) and DAD, in advance so that handover latency can be reduced. Nonetheless, the Mobile IPv6 is usually initiated after the completion of layer 2 handover.

When deploying IPv6 over 802.16e-based networks it is important to take advantage from the information available at the MAC 802.16e layer, such reachability and SS movement detection in order to ensure efficient handover at the IPv6 layer. Thereby, it is useful to combine FMIPv6 and IEEE 802.16e amendment by introducing a set of trigger between layer 2 and layer 3 as done in IEEE 802.21 draft [13]. Actually, the MIPSHOP[1] draft [14] tackling the IPv6 mobility over IEEE 802.16e proposes to use an integrated handover procedure of both layer 2 and layer 3. This procedure uses four IEEE 802.21 triggers in order that : (i) the layer 2 informs the layer 3 about the process of link handover; (ii) layer 3 orders layer 2 to execute a link handover. In addition, the proposed solution can deal with both Mobile IPv6 solutions, as to know predictive mode and active mode. However, the 16ng proposition suffers from the fact that layer 3 procedures have to be performed after the completion of layer 2 handover, which increase the duration of the disconnection time. In [15], the authors introduce a cross layer design for handling handover in 802.16 with Mobile IPv6. Rather than separating each layer handover's messages, the authors propose to integrate correlated messages. Besides reducing the number of message exchanged before the handover, the proposed solution decreases the handover latency as the two involved layers are completely synchronized.

F. Dormant SS

Since SS are now considered as mobile (MS), the support for dormant mode is now critical and a necessary feature. Paging capability and optimizations possible for paging an MS are neither enhanced nor handicapped by the link model itself. However, the multicast capability within a link may cause for an MS to wake up for an unwanted packet. One solution can consist in filtering the multicast packets and delivering the packets to only for MS that are listening for particular multicast packets. As shared IPv6 prefix model does not have the multicast capability and the point-to-point link model has only one node on the link, neither have any effect on the dormant mode. The Ethernet-like link model may have

[1]Mobility for IP: Performance, Signaling and Handoff Optimization, IETF draft

the multicast capability, which requires filtering at the BS to support the dormant mode for the MS.

G. Others issues

Through the above sections we have depicted the major issues to tackle when deploying IPv6 over 802.16-based network. However, it still exist minor issues that are not treated yet. In the following we depict the remaining issues:

- The Maximum Transmission Unit (MTU) size is not defined for IEEE 802.16. When using Ethernet CS, one can consider that MTU size is equal to 1500 bytes. When using IPv6 CS however, the MTU size is unknown, which can affect seriously the IP fragmentation process.
- In case of using Point-to-Point link model it is important to block the unuseful NDP functionalities. This can be done at the SS in case of using IP CS for instance. However, the implementation of such solution is still unclear.
- In case of using Diffserv QoS procedure at the IPv6 layer, it is important to introduce a mapping mechanism at the CS sublayer in order to associate the different Diffserv QoS classes with those proposed by the MAC 802.16 layer.

V. Conclusion

The need of deploying IPv6 is now a reality, however if we consider this deployment over wireless broadband networks such IEEE 802.16, there are many challenges to fix before. In fact, these challenges are particularly related to the lack of IP multicast support in 802.16-based network. Thereby, in this paper we have introduced the challenges that prevent deploying IPv6 over 802.16. After that, we have surveyed the solutions proposed by the 16ng group as well as those proposed by the research community and WiMAX forum. Finally, we have pointed out the remaining open issues regarding this deployment. At this point, the 16ng group is continuing its activities on proposing solutions to deploy IPv6 over IEEE 802.16 by tackling different aspects. Further, the solutions presented in this paper are still in progress, so other drafts and solutions are emerging in the 16ng group as well as in the research community when writing this paper.

References

[1] IEEE standard for local and metropolitan area networks, Part 16: Air Interface for fixed broadband wireless access systems, IEEE Standard 802.16, October 2004.
[2] WiMAX Forum, www.wimaxforum.org.
[3] IEEE 802.16e, "IEEE Standard for local and Metropolitan Area Networks - Part 16: Air Interface for fixed broadband wireless access systems - Amendment for Physical and Medium Access Control Layers for combined Fixed and Mobile Operation in Licensed Bands," 2005.
[4] H. Lee, T. Kwon and D-H. Cho, "Extended-rtPS algorithm for VoIP Services in IEEE 802.16 systems", in Proc. IEEE ICC 2006, Turkey, 2006.
[5] T. Narten, "Neighbor Discovery for IP version 6 (IPv6)", in RFC 2461on IETF. Dec 1998.
[6] L. Mamakos, K. Lidl, J. Varts, D. Carrel, D. Simone and R. Wheeler, "A method for transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.
[7] T. Narten, "Issues with protocols proposing multilink subnets", IETF Draft, draft-thaler-intarea-multilink-subnet-issues-00, March 2006.
[8] Jeong, Jang, "IPv6 Multicast Packet Delivery over IEEE 802.16 Networks", IETF Draft, draft-Jeong-16ng-multicast-delivery-01.
[9] J-C. Lee, Y-H. Han, M-K Shin, H-J Jang and H-J. Kim, "Considerations of Neighbor Discovery Protocol over IEEE 802.16 Networks", in Proc. IEEE ICACT 2006, Republic of Korea, 2006.
[10] H. Jeon and J. Jee, "IPv6 Neighbor Discovery Protocol for Common Prefix Allocation in IEEE 802.16", in Proc. IEEE ICACT 2006, Republic of Korea, 2006.
[11] M-K. Shin, Y-H. Han, S-E. Kim and D. Premec, "IPv6 Deployement Scenarios in 802.16 Networks", IETF Draft, draft-ietf-v6ops-802-16-deployement-scenarios-03.
[12] R. Koodli, "Fast Handovers for Mobile IPv6", IETF RFC-4068, July 2005.
[13] V. Gupta, "IEEE 802.21 Standard and Metropolitain Area Networks: Meida Independent Handover Services", Draft P802.21/D00.05", January 2006.
[14] H. Jang, "Mobile IPv6 Fast Handovers over IEEE 802.16e Networks", IETF Draft, draft-ietf-mipshopfh80216e-00, April 2006.
[15] Y-W Chen and F-Y. Hsieh, "A Cross Layer Design for Handover in 802.16e Networks with IPv6 Mobility", in Proc. IEEE WCNC 2007, Honk kong.
[16] J. Jee, S. Madanapalli, J. Mandi, G. Montenegro, S. Park and M. Riegel, "IP over 802.16 Problem Statement and Goals", IETF Draft , draft-ietf-16ng-ps-goal-01.txt.

Adlen Ksentini received the MS degree in telecommunications and multimedia networking from the University of Versailles and the PhD degree in computer science in 2005 from the University of Cergy, Pontoise. His PhD dissertation focused on QoS provisioning in IEEE 802.11-based networks. He is an associate professor at the University of Rennes 1, Rennes, France, where he is also a member of the IRISA Laboratory. He is involved in several industrial projects and the FP6 IST-ANEMONE, which aim at realizing a largescale testbed supporting mobile user on heterogeneous wireless technologies. His research interests include mobility and QoS support in IEEE 802.16, QoS support in the newly IEEE 802.11s mesh networks, and multimedia transmission. He is a coauthor of more than 20 technical journal papers and international conference proceedings. He is a member of the IEEE.