International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:7, 2011

NGN and WiMAX: Putting the Pieces Together

Mohamed K. Watfa, Khaled Abdel Naby , Chetan Govind Bhatia

***Abstract*—**With the exponential rise in the number of multimedia applications available, the best-effort service provided by the Internet today is insufficient. Researchers have been working on new architectures like the Next Generation Network (NGN) which, by definition, will ensure Quality of Service (QoS) in an all-IP based network [1]. For this approach to become a reality, reservation of bandwidth is required per application per user. WiMAX (Worldwide Interoperability for Microwave Access) is a wireless communication technology which has predefined levels of QoS which can be provided to the user [4]. IPv6 has been created as the successor for IPv4 and resolves issues like the availability of IP addresses and QoS. This paper provides a design to use the power of WiMAX as an NSP (Network Service Provider) for NGN using IPv6. The use of the Traffic Class (TC) field and the Flow Label (FL) field of IPv6 has been explained for making QoS requests and grants [6], [7]. Using these fields, the processing time is reduced and routing is simplified. Also, we define the functioning of the ASN gateway and the NGN gateway (NGNG) which are edge node interfaces in the NGN-WiMAX design. These gateways ensure QoS management through built in functions and by certain physical resources and networking capabilities.

***Keywords*—**WiMAX, NGN, QoS, IPv6, Flow Label, ASN Gateway

I. Introduction

MULTIMEDIA applications on the Internet like VoIP and Video on Demand require guaranteed QoS which the current best-effort service cannot provide. There is a big hurdle in the current TCP/IP layer for providing guaranteed real time QoS. TCP (Transmission Control Protocol) causes delay with its handshake requirement. An application requiring QoS will experience degradation of service (higher delay, jitter, etc.) by the process of acknowledging packets and retransmitting lost packets. UDP (User Datagram Protocol) does not guarantee packet delivery. IPv4 (Internet Protocol) has no policing or flow control. Also, telecommunications technologies which guarantee QoS are still in research or have been implemented only in the testing stage.

IPv6 is a solution as it provides 2^{128} different IP addresses which are way more than ever required. Another point to consider is that, in IPv4, features to provide QoS have not been implemented. The IPv6 header has two fields, TC and FL, which can be used to make QoS requests and get accurate responses [5]. This results in reduction in processing time and routing is also simplified.

M.Watfa is an Associate professor at the University of Wollongong in Dubai, UAE (e-mail: MohamedWatfa@uowdubai.ac.ae).

Khaled Abdel Naby & Chetan Govind Bhatia are graduate students in the faculty of computer science and engineering at the university of Wollongong in dubai, Dubai, UAE (email: MohamedWatfa@uowdubai.ac.ae).

Seamless connectivity to the Internet with guaranteed QoS is the demand of today. Any user who is fixed or mobile should be able to access the Internet irrespective of speed and location. WiMAX (IEEE 802.16) [3] is a telecommunications technology that provides wireless broadband internet access and is a replacement to wire line services like xDSL and Cable Modems. It is a packet-based i.e. an end-to-end all-IP technology which ensures that QoS is guaranteed. It provides better range (upto 50Km) and higher frequencies when compared with Wi-Fi which allows the same service without location constraints.

With the overburdening of protocols at all layers of the TCP/IP protocol stack, Internet designers are looking towards a single network based on IP technology. NGN is an all-IP network architecture which makes use of multiple broadband and guarantees QoS and generalized mobility. NGN has been conceptualized on the PSTN (Public Switched Telephone Network) [2] where the source dials a number of a receiver of choice and when a connection has been established, QoS has been enabled between the two parties. In this paper, we begin by explaining why it makes sense to use WiMAX as the communications technology for NGN. Section 3 defines an architectural framework for NGN-WiMAX and describes components which are used in this framework. The alteration and functioning of the IPv6 header to request QoS has been explained in Section 4. Section 5 explains the functions of the ASN gateway and the NGNG for QoS management. Section 6 describes the interfaces standardized in WiMAX which can be used in NGN. Section 7 provides an ideal scenario for implementing the gateways. We end with the conclusion and comparisons with related work.

II. WiMAX over NGN: Sensibility

There are many advantages of using WiMAX as the communications technology for providing wireless broadband Internet in the futuristic NGN architecture:

1) Wider Access Scope:
WiMAX adopts the orthogonal frequency division multiplexing which allows non-line-of-sight propagation of signals to provide broadband access upto 15 Km without any degradation of service and last mile access upto 50 Km. In areas where wire line resources are scarce and of poor quality, the advantage of WiMAX is particularly apparent. This will be very beneficial to the NGN architecture.

2) Competitive Costs:
WiMAX is based on the IEEE 802.16 standard. This makes it simpler for manufacturers to develop products and ensure interoperability between them. Participation of chipmakers like Intel [9] in this development process will greatly reduce the cost of WiMAX products. In addition, WiMAX being a wireless technology, it does not require operators to invest in

cable installation. Short installation period and easy capacity expansion allow operators to cut capital investment, quicken capital turnover and recovery, protect investments and cut business risks. NGN plans to replace all forms of communication and so the costs have to managed well.

3) Higher Bandwidth:

WiMAX ensures bandwidth which is higher than other conventional access modes. This makes it more suitable for application in high-traffic hotspots such as hotels, hospitals and shopping malls. WiMAX is also more suitable for providing real time services and multimedia applications like VoD and video conferencing. NGN is an all-IP architecture and requires powerful speeds on demand.

4) QoS:

WiMAX is the first wireless communications technology to ensure QoS. It has 5 levels of QoS defined for different requests and different real time applications. NGN implements a unified service network platform for providing voice, data, mobile and multimedia services. In order to provide all these applications together at the same time and also ensure that all requests for QoS are answered, WiMAX becomes an obvious choice. With the communication technology defined, designers and researchers can work on further development of NGN.

III. A Framework for The NGN-WiMAX Architecture

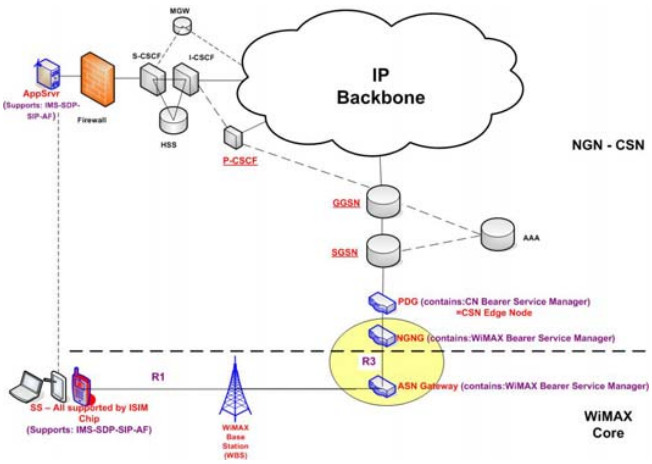

Fig. 1: A design for a framework required for integrating WiMAX in NGN

The NGN architecture [2] should contain 3 fundamental domains: the application domain, the session service domain and the transport domain. The application domain interacts with the end user application and forwards requests made by the user to the transport domain. The transport domain is responsible for all the addressing required to ensure end to end communication in the NGN. The session service domain is an intermediate between the application domain and the transport domain and is responsible for proper session establishment and translation.

The architectural framework of the NGN-WiMAX network model should consist of the WiMAX Access Service Network (ASN) and the Connectivity Service Network (CSN) which connects NGN elements like routers, AAA proxy/servers, user databases, Policy servers and Service Selection gateways (Figure 1).

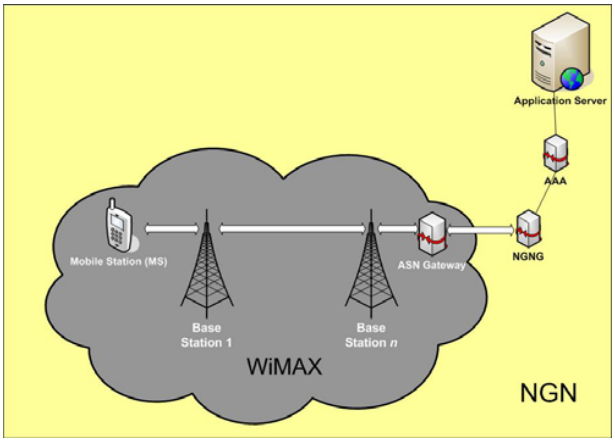

Fig. 2: WiMAX-NGN practical Architecture

We briefly describe all the important and required components below:

1) Access Service Network (ASN):

It defines a set of network functions that provide required signals to a WiMAX subscriber. An ASN is comprised of base stations (one or more base stations), and ASN Gateway(s). The ASN typically provides functions such as network discovery and selection, connectivity service between the Mobile Station (MS) and Connectivity Services network (CSN), Radio Resource Management, Multicast and Broadcast Control, Intra-ASN mobility, Paging and Location Management.

2) Information exchange between the ASN and WiMAX subscribers is based on the IEEE 802.16 (‘d’ for fixed and ‘e’ for mobile subscribers).

3) Network Access Provider (NAP):

It is a business entity that provides WiMAX radio access infrastructure to one or more WiMAX Network Service Providers (NSPs). A NAP implements this infrastructure using one or more ASNs.

4) Connectivity Service Network (CSN):

It is a set of network functions that provide IP connectivity to WiMAX subscriber(s). With the emergence of all-IP end-to-end mobile networks (viz. NGN), there is a need for an all-IP Broadband Access Gateway (NGNG). Both the NGNG and the ASN gateway share intelligence between the Base Station (BS) and the IP network. All radio independent control is done through the NGNG and the ASN gateway, while all radio dependent control is the responsibility of the WiMAX BS.

5) WiMAX is standards-based wireless technology that offers

high speed broadband connection over long distances. It can be used for a number of applications, including “last mile” broadband connections, fixed and mobile cellular service, hotspots and cellular backhaul, and high-speed enterprise connectivity for business.

6) It is also *important* to note that there is seperation between NSP and the ASP (Access Service Provider). The ASN gateway is a part of the NSP which provides the infrastructure for end to end connectivity. The ASP is responsible for billing the user and providing the required level of QoS according to its predefined policies.

Figure 2 shows a practical architecture of integrating WiMAX in an NGN network.

IV. IPv6 Functioning in the WiMAX-NGN Framework

The TC field and the FL field of IPv6 allow marking of packets, identification of flow and requests and grants of QoS. The 8 bit TC field contains a value negotiated with the application domain about the QoS level requested.

The 20 bit FL field in IPv6 has been created to provide QoS management. Its functioning has not been clear and is still under research [7]**.** RFC 3697 describes the FL field as follows:

- It is used by the source to label packets belonging to a particular flow.
- FL value zero indicates that that particular packet is not part of any particular flow.
- The FL value once chosen by the source, it cannot be changed by any intermediate routing device or the destination w.r.t. a particular flow.
- The source address, the destination address and the FL value is enough to define which flow a packet belongs to.

We explain 4 scenarios which should help in achieving end to end QoS. The 20 bit FL field is divided into 2 parts: first 2 bits of Label Type (LT) and remaining 18 bits of Random Label Number (LN).

2 bits	18 bits
Label type	**Randomly generated Label Number**

Fig. 3: Flow Label Field

The Label Type value can be one of 4 values. [8] defines these values as:

Type	Meaning
00	Requested by source
01	Response by receiver
10	Data transmission
11	End session

Fig. 4: LT proposed values

Figure 5 shows the table used at the base stations. It records the label number, source address, destination address and the ToS that has been requested for classifying all flows separately. Figure 5 shows the table defined at the ASN gateway. It helps in defining the next hop for each flow required to get to the required NGN.

LN	S	D	ToS
Random Label No. A	S_1	D_1	rtPS

Fig. 5: Table defined at the WiMAX base stations

LN	D	Next Hop
Random Label No. A	D_1	----------

Fig. 6: Table defined at the ASN gateway

The request and grant of QoS are explained in the following 4 steps:

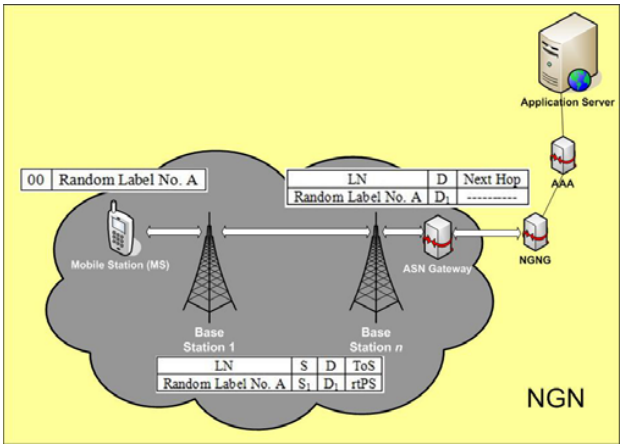

Fig. 7: Request

1. The smart phone, SP_1, generates a random LN (figure 7). Here, LT=00 and LN=Random Label No. A. This is the request made by the source. The ToS requested is rtPS (real time polling service) [4] which is standardized by WiMAX. When the closest base station receives packets, there is a confirmation made to check is the LN is a unique value. If confirmed, the source IP, Destination IP, LN and the ToS is entered into its table. If the LN is not unique, the host is requested for a new LN. When this information is received by the edge routing device i.e. the ASN gateway, it does a similar check like the base stations (LT, LN and ToS). It selects the next hop which will lead to the required NGNG. The ASN gateway records the Destination IP, LN and the next hop. This request packet is forwarded to the next core router and the process is continued till the required NGNG has been reached. Finally the request is forwarded to the Web server.

2. After receiving the request, the web server replies with a response message with the same LN i.e. Random Label No. A and LT=01 along the same path back to the smart phone, SP_1. This is based on the core routers which contain the same LN value. When SP_1 receives this packet, a connection has been established between the 2 parties. (Figure 8).

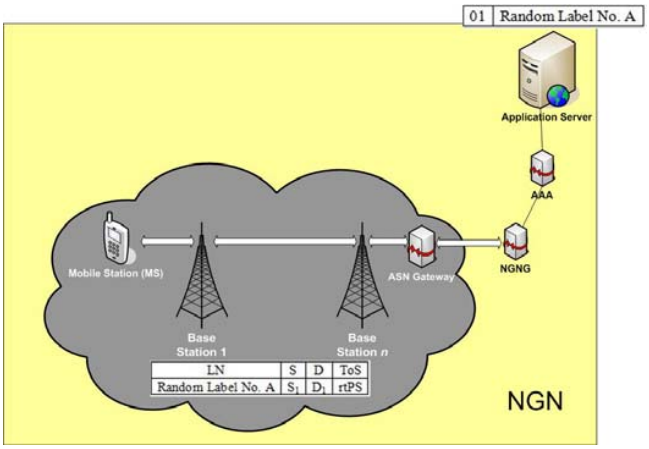

Fig. 8: Response

3. As shown in Figure 9, once the data connection has been established, an exchange of data packets can occur between source and destination. This exchange is confirmed by the LT=10 value and LN= Random Label No. A. The ToS value is more important now as exchange of data will occur according to the requested QoS.

4. When SP_1 sends out a termination message with the LT=11 and LN=Random Label No. A, the base stations and the ASN gateway deletes the matching LN values (figure 10).

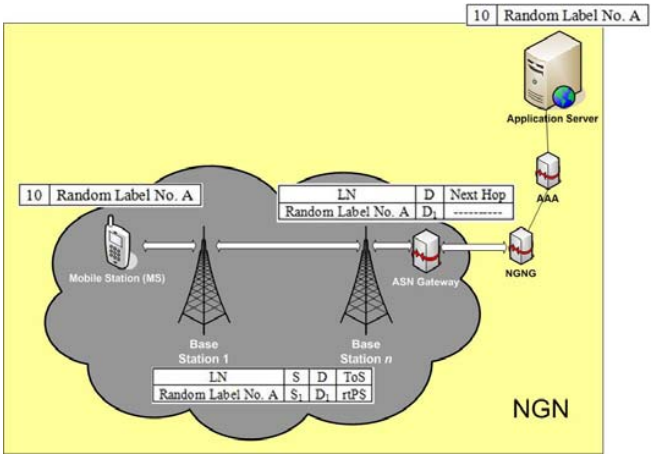

Fig. 9: Data Exchange

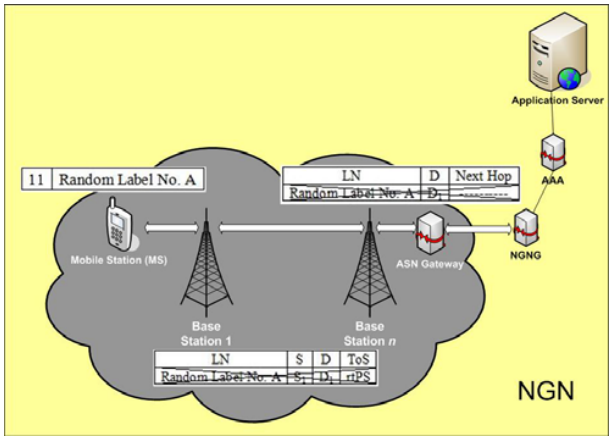

Fig. 10: Termination

V. ASN Gateway and the NGNG

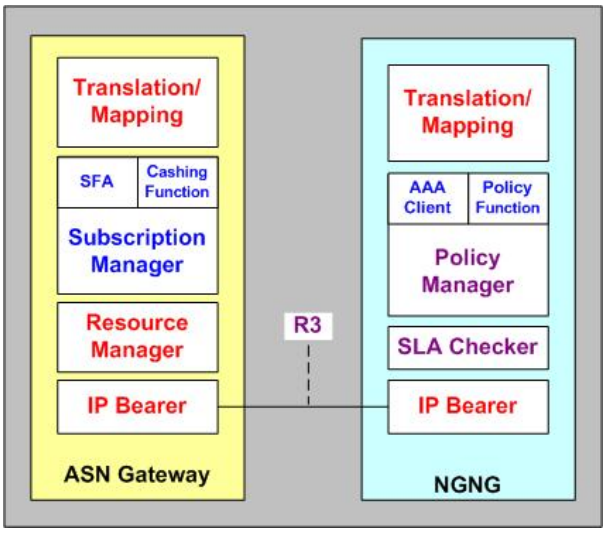

Fig. 11: Functioning of the ASN Gateway and the NGNG

The ASN Gateways provides local mobility anchor capabilities. Using this feature, users can move between base-stations. The ASN Gateway also caches authentication and security identification to accommodate fast roaming of users across base-stations or between other ASN Gateways. It is also the key for IP mobility. It provides the termination of the mobility function across base-stations and the foreign agent function.

The ASN Gateway maps the radio bearer to the NGNG through IP. Then NGNG works with the CSN and the policy servers to control user requests as per its policies. Additionally, The ASN Gateway acts as an IP gateway for the IP host function that is located on the base station, as standardized in [10], including end-to-end QoS service.

The following is a pseudo code which explains the functioning of the ASN gateway when the end user makes a QoS request:

1) *Start*
2) ***Translate*** *signals from analogue to digital*
3) ***Check Subscription Status***

4) *If (User subscribed i.e. if SFA exists)*
5) *Create SLA*
6) *Goto 9*
7) *Else request user to subscribe to service*
8) *Goto End*
9) ***Reserve BW** as per the user requirement defined in the TC field of the IPv6 header*
10) *If (Requested BW <= Available BW)*
11) *Reserve BW*
12) *Available BW = Available BW – Requested BW*
13) *Goto 16*
14) *Else queue request for n trials (n is predefined by NSP)*
15) *When timer t expires, Goto 10*
16) ***Flow label number and the destination address entered** in the ASN table and IPv6 datagram packet forwarded to NGNG*
17) *End*

When the ASN gateway receives the IPv6 datagram packet, it first translates the analogue signal to digital data to understand the information received. The first 2 bits of the 20 bit FL field determines whether the datagram packet is a request for QoS or not. The first check involves figuring out whether the end user has been subscribed with the NSP. User subscription is confirmed by the SFA (service flow agreement). If yes, an SLA is created. If the gateway finds that the user has not been subscribed, the packet is dropped and the user is requested to subscribe to the NSP. The gateway checks if the requested bandwidth (according to the TC field in the IPv6 header) is less than or equal to the available bandwidth, the requested bandwidth is reserved for the user. If the bandwidth requested is not available, the request is queued till a timer expires and the check for bandwidth is done again. Once bandwidth is reserved, the LN value, Destination address and next hop is recorded and the request is forwarded to the next core router. This information is recorded in all core routers leading to the NGNG. The LN value is from the FL field in the IPv6 header.

The NGNG will perform in the following order when it receives a request from the ASN gateway:
1) *Start*
2) ***Translate** signals from analogue to digital*
3) ***Check** if the user request conforms with the predefined policies within the network*
4) *If (request conforms with policies)*
5) *Goto 8*
6) *Else deny user request*
7) *Goto End*
8) ***Confirm validity** of the SLA defined by the ASN Gateway*
9) *If (valid SLA confirmed)*
10) *Goto 13*
11) *Else deny user request*
12) *Goto End*
13) ***Negotiate Policy Functions** with Subscription manager of the ASN gateway*
14) *Forward request to Application Server*
15) *End*

The first step is similar to that of the ASN gateway i.e. translation from analogue signal to bits of information representing the IPv6 datagram packet containing the request for QoS. The NGNG along with the ASP checks if the request conforms to the predefined policies like culture, etc. If it does, a security check occurs to confirm the validity of the SLA as defined by the corresponding ASN gateway. Once this is complete, a negotiation occurs between the subscription manager of the ASN gateway and the NGNG about issues like availability of bandwidth in NGN. Also, the request packet is forwarded to the application server.

VI. Interfaces Standardized for WiMAX

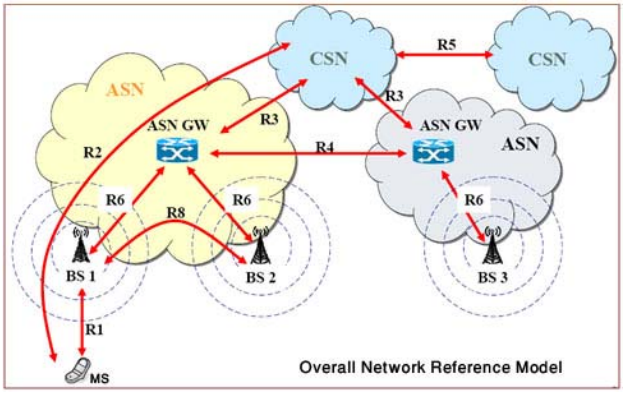

Fig. 12: Interfaces illustrated for NGN-WiMAX interconnection

All connection interfaces (R's) have been standardized in a few RFCs from the WiMAX Forum [10]. From these interfaces, some R's are explained as follows:

- **R3** consists of a set of control plane protocols between the ASN and the CSN to support AAA, policy enforcement and mobility management capabilities. It encompasses the bearer plane methods (e.g., tunneling) to transfer user data between the ASN and the CSN.
- **R4** consists of the set of Control and Bearer plane protocols originating/terminating in various functional entities of an ASN that coordinate MS mobility between ASNs and ASN-GWs. R4 is the only interface interoperable between similar or heterogeneous ASNs.
- **R6** consists of the set of control and bearer plane protocols for communication between the BS and the ASN-GW. The bearer plane consists of an intra-ASN data path between the BS and ASN gateway. The control plane includes protocols for data path establishment, modification, and release control in accordance with the MS mobility events. R6, in combination with R4, may serve as a conduit for exchange of MAC states information between BSs that cannot interoperate with R8.

VII. Ideal Scenario for the NGNG and the ASN Gateway

Both the NGNG and ASN Gateways are major infrastructure elements in the NGN-WiMAX network model. The WiMAX Forum defined several baseline requirements for ASN Gateways:

- L2 (Layer 2) connectivity with user devices.
- Discovery of available WiMAX networks and the customer's preferred operator.
- Relay functionality for establishing L3 (Layer 3) connectivity with devices.
- Radio resource management.

NGNG and ASN Gateways also can be developed to support tasks such as:

- Accounting agent functions
- Tunneling
- DHCP
- Header compression, in order to maximize radio resources

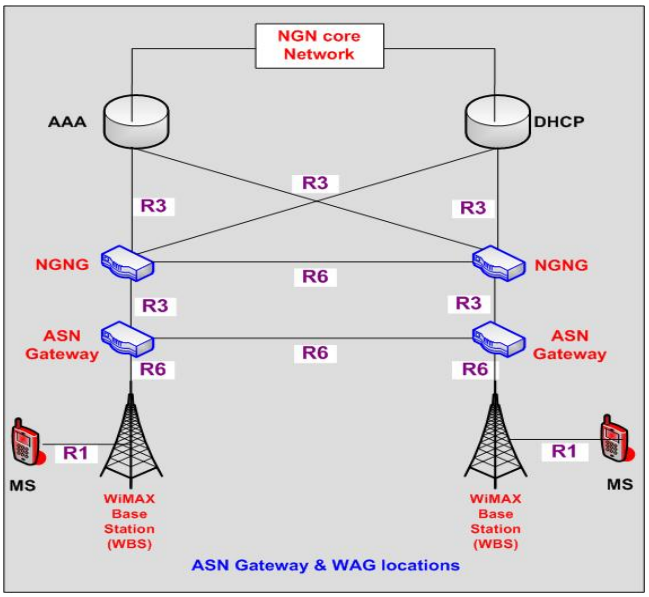

Fig. 13: The location of an NGNG and the ASN gateway in a service provider network

AAA Accounting Support:

The Policy Manager will have a built in AAA client function which makes the NGNG sends the following messages to the AAA server to establish proper accounting of the user which has been granted the service:

Accounting Start: The NGNG sends this message to the AAA server when a new service flow is created.

Accounting Interim Update: The NGNG generates an Accounting Update message if periodic accounting update message is configured. The accounting updates are based on a time trigger, and when configured.

Accounting Stop: The NGNG sends an Accounting Stop message when the service flow is deleted or when the end user requests termination.

The ideal NGNG and ASN Gateways also should be highly flexible. For example, as processors become more powerful, the gateway's design should allow CPU cards to be easily removed and replaced with faster models. This is popular with the newer Cisco networking devices. This ability is important as the ASN Gateway's requirements for QoS will require a lot of processing power. These gateways should also use solutions based on 10-Gigabit Ethernet or more. This is necessary for having ample bandwidth to accommodate growth of subscribers.

The NGNG and ASN Gateways must support several real-world benefits:

- Easy installation and management
- Standard interface supporting NGNG and ASN Gateway reference points.
- Integrated fast path (IP-over-IP tunneling over R3 interfaces).
- Optimal cost point for staged roll-out, with scalability from hundreds of base stations at launch to thousands of sites in a mature network
- Support for an optimal ratio of registered users
- Support for security (accelerators for encryption: IPSec).
- Fast and predictable handovers
- IPv4 routing

VIII. Conclusion

This paper provides a design for the functional architecture in where WiMAX and NGN can coexist. The design shows and explains all the required components to provide end to end QoS. The paper also shows how IPv6 can use the TC and FL fields to request the required level of QoS from the NSP. Another important aspect is the required gateways i.e. NGNG and ASN, to provide this end to end connectivity. A brief algorithm of its functionalities of both the ASN gateway and the NGN has been explained. The estimated results show the expected throughput values over time.

References

[1] ITU-T, "General Overview of NGN", ITU-T Recommendation Y.2001, 2004.
[2] A. Modarressi, S. Mohan, "Control and Management in Next-Generation Networks: Challenges and Opportunities", IEEE Communications Magazine, 2000, pp. 94-102.
[3] H. Cordova, P. Boets, L. Biesen, "Insight Analysis into WiMAX Standard and its trends", 2005.
[4] B. Li, Y. Qin, C. Low, C. Gwee, "A Survey on Mobile WiMAX", IEEE Communications Magazine, 2007, pp. 70-75.
[5] S. Deering, R. Hinden, "Internet Protocol, version 6", IETF Network Working Group RFC 2460, 1998.
[6] K. Nichols, S. Blake, F. Baker, D. Black "Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers", IETF Network Working Group RFC 2474, 1998.
[7] J. Rajahalme, A. Conta, B. Carpenter, S. Deering, "IPv6 Flow Label Specification", IETF Network Working Group RFC 3697, 2004, pp.2-6.
[8] Chuan-Neng Lin, Pei-Chen Tseng, Wen-Shyang Hwang, "End-to-End QoS Provisioning by Flow Label in IPv6", 2006.
[9] Intel, "Broadband Wireless: The New Era in Communications", white paper, 2004.
[10] WiMAX Forum, WiMAX End-to-End Network System Architecture (Stage 2: Architecture Tenets, Reference Model and Reference Points).