16ng Working Group
Internet-Draft
Intended status: Informational
Expires: August 23, 2007

S. Madanapalli, Ed.
LogicaCMG

February 19, 2007

# Analysis of IPv6 Link Models for 802.16 based Networks
## draft-ietf-16ng-ipv6-link-model-analysis-03.txt

Status of this Memo



Copyright Notice



Abstract

This document provides different IPv6 link models that are suitable for 802.16 based networks and provides analysis of various considerations for each link model and the applicability of each link model under different deployment scenarios. This document is result of a Design Team that was formed to analyze the IPv6 link models for 802.16 based networks.

Table of Contents

## 1. Introduction

802.16 [4] [5] is a point-to-multipoint connection oriented access technology for the last mile without bi-directional native multicast support. 802.16 has defined only downlink multicast support. This leads to two methods for running IP protocols that traditionally assume the availability of multicast at the link layer. One method is to use bridging e.g. 802.1D [6] to support bi-directional multicast, another method is to treat the 802.16 MAC transport connections between an MS and BS as point-to-point IP link, so that, the IP protocols (e.g. ARP, IPv6 Neighbor Discovery) can be run without any problems.

This is further complicated by the definition of commercial network models like WiMAX, which defines the WiMAX transport connection that extend the 802.16 MAC transport connection all the way to an access router by using a tunnel between the base station and the access router. This leads to multiple ways of deploying IP over 802.16 based networks.

This document looks at various considerations in selecting a link model for 802.16 based networks and provides an analysis of the various possible link models. And finally this document provides a recommendation for choosing one link model that best suits for the deployment.

## 2. Terminology

The terminology in this document is based on the definitions in [6], in addition to the ones specified in this section.

Access Router (AR): An entity that performs an IP routing function to provide IP connectivity for Mobile Stations. In WiMAX Networks, the AR is an Access Service Network Gateway.

Access Service Network (ASN) - The ASN is defined as a complete set of network functions needed to provide radio access to a WiMAX subscriber. The ASN is the access network to which the MS attaches. The IPv6 access router is an entity within the ASN. The term ASN is specific to the WiMAX network architecture.

Dormant Mode: A state in which a mobile station restricts its ability to receive normal IP traffic by reducing monitoring of radio channels. This allows the mobile station to save power and reduces signaling load on the network. In the dormant mode, the MS is only listening at scheduled intervals to the paging channel. The network (e.g. the AR) maintains state about an MS which has transitioned to

dormant mode and can page it when needed.

## 3. IPv6 Link Models for 802.16 based Networks

This section discusses various IPv6 link models for 802.16 based networks and provides their operational considerations in practical deployment scenarios.

### 3.1. Shared IPv6 Prefix Link Model

In this model, all MSs attached to an AR share one or more prefixes for constructing their global IPv6 addresses, however this model does not any multicast capability. The following figures illustrates high level view of this link model wherein one more prefixes advertised on the link would be used by all the MSs attached to the IPv6 link.

```
     +-----+
     | MS1 |-----+
     +-----+     |
                 |
                 |
     +-----+     |     +-----+          +---------+
     | MS2 |-----+-----| BS1 |----------|   AR    |-------Internet
     +-----+     |     +-----+          +---------+
        .        |           ____________
        .        |          ()__________()
     +-----+     |            L2 Tunnel
     | MSn |-----+
     +-----+
```

Figure 1. Shared IPv6 Prefix Link Model

The above figure shows the case where the BS and AR exist as separate entities. In this case a tunnel exists between the BS and AR per MS basis.

In this link model, the link between the MS and the AR at the IPv6 layer is viewed as a shared link and the lower layer link between the MS and BS is a point-to-point link. This point-to-point link between the MS and BS is extended all the way to the AR when the granularity of the tunnel between the BS and AR is on per MS basis. This is illustrated in the following figure below.

```
          MS
        +----+                                      +----+
        |    |      IPv6 (Shared link)              |    |
        | L3 |======================================|    |
        |    |                                      |    |
        |----|   PTP conn. +----+   L2 Tunnel       | AR |---Internet
        | L2 |-------------| BS |===================|    |
        |    |             |    |                   |    |
        +----+             +----+                   |    |
                                                    |    |
                           +----+   L2 Tunnel       |    |
                           | BS |===================|    |
                           |    |                   |    |
                           +----+                   +----+
```

Figure 2. Shared IPv6 Prefix Link Model - Layered View

In this link model, an AR can serve one or more BSs. All MSs connected to BSs that are served by an AR are on the same IPv6 link. This model is different from Ethernet Like Link model wherein the later model provides Ethernet link abstraction and multicast capability to IPv6 layer, whereas the Shared IPv6 Prefix Link Model defined here does not provide native link layer multicast and broadcast capabilities.

#### 3.1.1. Prefix Assignment

One or more IPv6 prefixes are assigned to the link and hence shared by all the nodes that are attached to the link. The prefixes are advertised with autonomous flag (A-Flag) set and the On-link flag (L-flag) reset for address autoconfiguration so that the nodes may not make an on-link assumption for the addresses in those prefixes.

#### 3.1.2. Address Autoconfiguration

The standard IPv6 address autoconfiguration mechanisms, which are specified in [2] [3] are used.

#### 3.1.3. Duplicate Address Detection

The DAD procedure as specified in [2] does not adapt well to the 802.16 air interface as there is no native multicast support. The DAD can be performed with MLD snooping [7] and the AR relaying the DAD probe to the address owners in case if the address is duplicate, called Relay DAD. In this method, the MS behavior is same as

specified in [2] and the optimization is achieved with the support of AR, which maintains MLD table for a list of multicast addresses and the nodes that joined the multicast address. The relay DAD works as below:

1. An MS constructs a Link Local Address as specified in [2].
2. The MS constructs a solicited node multicast address for the corresponding Link Local Address and sends an MLD Join request for the solicited node multicast address.
3. The MS starts verifying address uniqueness by sending a DAD NS on the initial MAC transport connection.
4. The AR consults the MLD table for who joined the multicast address. If the AR does not find any entry in the MLD table, the AR silently discards the DAD NS. If the AR founds a match, the AR relays the DAD NS to the address owner.
5. The address owner defends the address by sending DAD NA, which is relayed to the DAD originating MS via the AR.
6. If the DAD originating MS does not receive any response (DAD NA) to its DAD NS, the MS assigns the address to its interface. If the MS receives the DAD NA, the MS discards the tentative address and behaves as specified in [2].

### 3.1.4. Considerations

#### 3.1.4.1. Reuse of existing standards

The shared IPv6 prefix model uses the existing specification and does not require any protocol changes or any new protocols. However this model requires implementation changes for DAD optimization on the AR.

#### 3.1.4.2. On-link Multicast Support

No native on-link multicast is possible with this method. However the multicast can be supported with using a backend process in AR that maintains the multicast members list and forwards the multicast packets to the MSs belonging to a particular multicast group in unicast manner. MLD snooping [7] should be used for maintaining the multicast members list.

#### 3.1.4.3. Consistency in IP Link Definition

The definition of IPv6 link is consistent for all procedures and functionalities except for the support of native on-link multicast support.

#### 3.1.4.4. Packet Forwarding

All the packets travel to the AR before being delivered to the final destination as the layer 2 transport connection exists between the MS

and AR. The AR handles the packets with external IPv6 addresses normally. However the packets with link local destination addresses are relayed by the AR to destination without decrementing the hop-limit.

#### 3.1.4.5. Changes to Host Implementation

This link model does not require any implementation changes for the host implementation.

#### 3.1.4.6. Changes to Router Implementation

This link model requires MLD snooping in the AR for supporting Relay DAD.

### 3.1.5. Applicability

This model is good for providing shared on-link services in conjunction with IP convergence sublayar with IPv6 classifiers. However in public access networks like cellular networks, this model cannot be used for the end users to share any of their personal devices/services with the public.

This link model was also under consideration of the WiMAX Forum Network Working Group for using with IPv6 CS access.

## 3.2. Point-to-point Link Model

In this model, a set of MAC transport connections between an MS and the AR are treated as a single link. The point-to-point link model follows the recommendations of [8]. In this model, each link between an MS and the AR is allocated a separate, unique prefix or a set of unique prefixes by the AR. No other node under the AR has the same prefixes on the link between it and the AR. The following diagram illustrates this model.

```
                          +----+                    +----+
          +-----+         |    |       Tunnel       |    |
          | MS1 |-------------|....|===================|    |
          +-----+         |    |                    |    |
                          |    |                    |    |
          +-----+         |    |       Tunnel       |    |
          | MS2 |-------------|....|===================|    |---Internet
          +-----+         |    |                    | AR |
                          | BS |                    |    |
          +-----+         |    |       Tunnel       |    |
          | MS3 |-------------|....|===================|    |
          +-----+         |    |                    |    |
                          +----+                    +----+
```

Figure 3. Point-to-point Link Model

There are multiple possible ways that the point-to-point link between the AR and the MS can be implemented.

1. One way to accomplish this is to run PPP on the link [8]. Running PPP requires that the 802.16 link use the Ethernet CS and PPP over Ethernet [9]. Since the IPv6 CS does not support PPP, whether PPP can be run depends on the network architecture.
2. If the actual physical medium is shared, like Ethernet, but PPP is not run, the link can be made point to point between the MS and AR by having each MS on a separate VLAN [11].
3. If neither PPP nor VLAN is used, the set of 802.16 connections can be viewed as a virtual point-to-point link.

### 3.2.1. Prefix Assignment

Prefixes are assigned to the link using the standard [1] Router Advertisement mechanism. The AR assigns a unique prefix or set of unique prefixes for each MS. In the prefix information options, both the A-flag and L-flag are set to 1, as they can be used for address autoconfiguration and the prefixes are on link.

### 3.2.2. Address Autoconfiguration

MSs perform link local as well as global address autoconfiguration exactly as specified in [2], including duplicate address detection. Because there is only one other node on the link, the AR, there is only a possibility of an address conflict with the AR, so collisions are statistically very unlikely, and easy to fix if they should occur.

If DHCP is used for address configuration ('M=1' in the Router Advertisement), the DHCP server must provide addresses with a separate prefix per MS. The prefix must of course match a prefix the ASN Gateway has advertised to the MS (if any).

### 3.2.3. Considerations

#### 3.2.3.1. Reuse of existing standards

This solution reuses RFC 2461, 2462, and if PPP is used, RFC 2472 and RFC 2516. No changes in these protocols are required, the protocols must only be configured properly.

If PPP is not used, any VLAN solution, such as IEEE 802.1Q [9], or any L2 tunnel can be used.

#### 3.2.3.2. On-link Multicast Support

Since the link between the MS and the AR is point to point, any multicast can only be sent by one or the other node. Link local multicast between other nodes and the AR will not be seen.

#### 3.2.3.3. Consistency in IP Link Definition

The IP link is fully consistent with a standard IP point-to-point link, without exception.

#### 3.2.3.4. Packet Forwarding

The MS always sends all packets to the AR, because it is the only other node on the link. Link local unicast and multicast packets are also forwarded only between the two.

#### 3.2.3.5. Changes to Host Implementation

Host implementations follow standard IPv6 stack procedures. No changes needed.

#### 3.2.3.6. Changes to Router Implementation

If PPP is used, no changes in router implementations are needed. If PPP is not used, the AR must be capable of doing the following:

1. Each MS is assigned a separate VLAN when 802.1X [12] or each MS must have an L2 tunnel to the AR to aggregate all the connections to the MS and present these set of connections as an interface to the IPv6 layer.

2. The AR must be configured to include a unique prefix or set of prefixes for each MS. This unique prefix or set of prefixes must be included in Router Advertisements every time they are sent, and if DHCP is used, the addresses leased to the MS must include only the uniquely advertised prefixes.

Note that, depending on the router implementation, these functions may or may not be possible with simple configuration. No protocol changes are required, however.

#### 3.2.4. Applicability

In enterprise networks, shared services including printers, fax machines, and other such on-line services are often available in on the local link. These services are typically discovered using some kind of link local service discovery protocol. The unique prefix per MS model is not appropriate for these kinds of deployments, since it is not possible to have shared link services in the ASN.

The p2p link model is applicable to deployments where there are no shared services in the ASN. Such deployments are typical of service provider networks like cellular network which provide public access to wireless network.

### 3.3. Ethernet Like Link Model

This model describes a scheme for configuration and provisioning of an IEEE 802.16 networks so that it emulates a broadcast link in a manner similar to Ethernet. Figure 4 illustrates an example of the Ethernet model. This model essentially functions like an Ethernet link, which means the model works as described in [1], [2].

One way to construct an Ethernet like link is to implement bridging [13] between BSs and AR like switched Ethernet. In the Figure 4, bridging performs link aggregation between BSs and AR. Bridging also supports multicast packet filtering.

```
              +-----+                 +---+       +----+
              | MS1 |---+             |   |   +---|AR1 |---Internet
              +-----+   |             |  S|   |   +----+
              +-----+   |   +-----+   |E w|   |
              | MS2 |---+---| BS1 |---|t i|   |
              +-----+       +-----+   |h t|---+
                                      |  c|   |   +----+
     +-----+  +-----+       +-----+   |  h|   +---|AR2 |---Internet
     |Hosts|--|MS/GW|-------| BS2 |---|   |       +----+
     +-----+  +-----+       +-----+   +---+
     A network
     may exists behind
     MS/GW
```

Figure 4: Ethernet Like Link Model

### 3.3.1. Prefix Assignment

Prefixes are assigned as specified in [1], [2].

### 3.3.2. Address Autoconfiguration

It is the same as described in [2].

### 3.3.3. Duplicate Address Detection

It is the same as described in [2].

### 3.3.4. Considerations

#### 3.3.4.1. Reuse of existing standards

All the IPv6 standards can be preserved or reused in this model.

#### 3.3.4.2. On-link Multicast Support

On-link multicast can be emulated in unicast manner by efficiently bridging between all BSs with IEEE 802.16 providing the links between the MSs and the bridge on top of the BS.  MLD snooping should be used for efficient forwarding of multicast packets as specified in [7]. Nevertheless, in case of bridging, direct inter-MSs communication may not be not allowed due to restrictions from the service providers.

#### 3.3.4.3. Consistency in IP Link Definition

This model is consistent with the IP link definition.

#### 3.3.4.4. Packet Forwarding

When properly configured and assisted by simple bridging, IEEE 802.16 can emulate a simple broadcast network like Ethernet.

#### 3.3.4.5. Changes to Host Implementation

No special impact on host implementation.

#### 3.3.4.6. Changes to Router Implementation

No special impact on router implementation under a separated AR-BS model, if the bridging is implemented in BS. Some networks e.g. WiMAX networks may require bridging be implemented in the AR (ASN Gateway).

### 3.3.5. Applicability

This model works with the Ethernet CS and is chosen for fixed/nomadic WiMAX networks by the WiMAX Forum Network Working Group.

## 4. Renumbering

If the downstream prefixes managed by the AR are involved in renumbering, it may be necessary to renumber each link under the AR. [10] discusses recommended procedures for renumbering.

If the prefixes are advertised in RAs, the AR must withdraw the existing prefixes and advertise the new ones. Since each MS irrespective of the link model is on a separate point-to-point link at the MAC level because of the 802.16 connection oriented architecture, the AR must send an RA withdrawing the old prefix and advertising the new one to each link. In point-to-point link model, the number of RAs sent is equal to the number of nodes the AR serves, whereas in the other two models, the AR sends a single RA to BS that is sent to all the MSs as separate RAs.

If DHCP is used to assign addresses, either the DHCP address lease lifetime may be reduced prior to the renumbering event to encourage MSs to renew their addresses quickly or a DHCP Reconfigure message may be sent to each of the MSs by the server to cause them to renew their addresses.

In conclusion, the amount of traffic on the air-interface is same for all link models. However the number of RAs sent by the AR to BS can be more compared to the other two models.

## 5. Effect on Dormant Mode

If the network needs to deliver packets to an MS, which is in dormant mode, the AR pages the MS. The MS that is monitoring the paging channel receives the page and transitions out of the dormant mode to active mode. It establishes connectivity with the network by requesting and obtaining the radio resources. The network is then able to deliver the packets to the MS. In many networks, packets destined to an MS in dormant mode are buffered at the AR in the network until connectivity is established.

Support for dormant MSs is critical in mobile networks and hence it is a necessary feature. Paging capability and optimizations possible for paging an MS are not either enhanced or handicapped by the link model itself. However the multicast capability within a link may cause for an MS to wake up for unwanted packet. This can be avoided by filtering the multicast packets and delivering the packets to only for MSs that are listening for particular multicast packets. As the Shared IPv6 Prefix model does not have the multicast capability and point-to-point link model has only one node on the link, they do not have any effect on the dormant mode. The Ethernet like link model may have the multicast capability, which requires filtering at the BS to support the dormant mode for the MSs.

## 6. Conclusions and Relevant Link Models

Ethernet Like Link model would be used when the deployment requires the use of Ethernet CS as this is the only model being proposed for the Ethernet CS and running IPv6 over Ethernet is well understood.

For IP CS with IPv6 classifiers, point-to-point link model appears to the choice because of its simplicity for performing the DAD and does not break any existing applications or require defining any new protocol. However the IPv6 shared prefix model would be defined if there is any interest from service provider community.

## 7. Security Considerations

This document provides the analysis of various IPv6 link models for 802.16 based networks and this document as such does not introduce any new security threats.

## 8. IANA Considerations

This document has no actions for IANA.

## 9. Acknowledgements

This document is a result of discussions in v6subnet design team for IPv6 Prefix Model Analysis. The members of this design team in alphabetical order were: Dave Thaler, David Johnston, Junghoon Jee, Max Riegel, Myungki Shin and Syam Madanapalli. The discussion in the DT was benefited from the active participation of James Kempf, Behcet Sarikaya, Basavaraj Patil and JinHyeock Choi in the DT mailing list. The DT thanks the chairs (Gabriel Montenegro and Soohong Daniel Park) and Shepherding AD (Jari Arkko) for their active participation and motivation.

## 10. Contributors

The members who provided the text based on the DT discussion are:

Myung-Ki Shin
ETRI
myungki.shin@gmail.com

James Kempf
DoCoMo Communications Labs USA
kempf@docomolabs-usa.com

Soohong Daniel Park
Samsung Electronics
soohong.park@samsung.com

Dave Thaler
Microsoft
dthaler@microsoft.com

JinHyeock Choi
Samsung Advanced Institute of Technology
jinchoe@samsung.com

Behcet Sarikaya
Huawei USA
sarikaya@ieee.org

## 11. References

### 11.1. Normative References

[1] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[2] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[3] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

### 11.2. Informative References

[4] "IEEE 802.16-2004, IEEE standard for Local and metropolitan area networks, Part 16:Air Interface for fixed broadband wireless access systems", October 2004.

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

[6] Jee, J., "IP over 802.16 Problem Statement and Goals", October 2006, <http://www.ietf.org/internet-drafts/draft-ietf-16ng-ps-goals-00.txt>.

[7] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, May 2006.

[8] Wasserman, M., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.

[9] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.

[10] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, September 2005.

[11] "IEEE, Virtual Bridged Local Area Networks, IEEE 802.1Q", May 2003.

[12] "IEEE, Port-based Network Access Control, IEEE 802.1X", December 2004.

[13] "IEEE Std 802.1D-2004, "IEEE Standard for Local and metropolitan area networks, Media Access Control (MAC) Bridges"", June 2004.

## Author's Address

Syam Madanapalli (editor)
LogicaCMG
Global Innovation Center
125 Yemlur P.O.
Bangalore 560037
India

Email: smadanapalli@gmail.com

## Full Copyright Statement



## Intellectual Property



## Acknowledgment

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