DNA WG
Internet-Draft
Expires: January 19, 2006

JinHyeock Choi
Samsung AIT
DongYun Shin
Samsung Electronics
July 18, 2005

Fast Router Discovery with L2 support
draft-jinchoi-dna-frd-01.txt

Status of this Memo

Copyright Notice

Abstract

For efficient DNA, a host should quickly receive an RA upon a new link-layer connection. This draft presents a quick RA acquisition scheme with the support of a link-layer entity, PoA (Point of Attachment). Upon a new network attachment, the PoA may either trigger an AR (Access Router) to immediately send an unicast RA, "RA Triggering" or send such an RA for itself, "RA Proxying". We may put "RA Triggering" or "RA Proxying" functionality on a PoA to get the

optimized result without IPv6 standard change.

Table of Contents

1. Introduction

Upon establishing a new link-layer connection, a host should detect the identity of the currently attached link to ascertain the validity of the existing IP configuration. If the host is attached to a different link, it also needs to acquire the IP configuration for the new link [4].

An RA (Router Advertisement) message is necessary when the host has moved to a different link, so the number of messages needed for DNA can be minimized if the RA also can properly represent the link identity. Moreover to quickly check for link change, the host has to receive the RA without delay.

DNA solution should be able to 1) check for link change with a single RA message and 2) get the RA with minimum latency [5]. This draft presents only the second component, quick RA acquisition. But the proposed method can work with any link identify detection scheme based on unsolicited RA, such as linkid prefix in [13] or CompleteRA in [12].

There are several hindrances for sufficiently quick RA acquisition. First, Neighbor Discovery protocol [1] limits routers to a minimum interval of 3 seconds between sending multicast RA messages. Second, it SHOULD delay the transmission for a random amount of time before a host sends an initial RS (Router Solicitation) message. Third, a router MUST delay a response to a Router Solicitation by a random time too.

In cellular environments, it may not be cost-effective to broadcast the RA over wireless link. For DNA purpose, it's generally preferable to deliver the RA to the destination in unicast.

PoA (Point of Attachment) is the link endpoint of the link, such as 802.11 AP (Access Point) or 802.16 BS (Base Station). We propose a scheme which uses the link-layer entity, PoA, in such a way that an RA is delivered to the host in unicast just after L2 connection is made without any random delay.

When a host makes a new link-layer connection with a PoA, the PoA detects the new attachment. So at this moment, the PoA may either trigger an AR (Access Router) to immediately send a suitable RA or send such an RA for itself. For the latter case, the PoA needs to cache a suitable RA, such as 'RA optimized for DNA' defined in [5]

For example, if AR and PoA are in the same box, whenever a new host is attached, PoA module can deliver Link Up event to AR module so that AR module can immediately fire an RA. Or, if AR and PoA are

separated, PoA can cache a suitable RA and deliver it to a new host upon network attachment.

In this draft, we design a scheme for a PoA to trigger an RA, "RA Triggering" and another one for a PoA to proxy an RA, "RA Proxying". In RA Proxying, we present a way to cache a necessary RA and send the RA in unicast without any delay.

IEEE 802.21 (Media Independent Handover) standard develops a specification [21] that provides link layer intelligence and other related network information to upper layers to optimize handovers between heterogeneous media.

Utilizing the services defined in 802.21 MIH (Media Independent Handover) standard, we can put 'RA Triggering' or 'RA Proxying' functionality on a PoA to get the optimized result for quick RA acquisition without IPv6 standard change.

2. Terminology

Access Router (AR)

- An Access Network Router residing on the edge of an Access Network and offers IP connectivity to hosts.

Point of Attachment (PoA)

- The link endpoint on the link, such as 802.11 Access Point (AP) or 802.16 Base Station (BS), where a host may be connected.

Link Up

- An event provided by the link layer that signifies a state change associated with the interface becoming capable of communicating data frames.

Media Independent Handover Fuction (MIHF)

- The MIH Function provides asynchronous and synchronous services through well defined SAPs for lower layers and upper layers. The services provided include the Media Independent Event Service (MIES), the Media Independent Command Service (MICS), and the Media Independent Information Service (MIIS).

Media Independent Handover (MIH) Protocol

- The Media Independent Handover protocol defines frame formats for exchanging messages between peer MIH Function entities. These messages are based on the primitives which are part of MIES, MICS and MIIS. The MIHF Protocol allows peer MIH Function entities to interact with each other.

3. Proposal Overview

When a host establishes a link-layer connection, in the process, a link-layer entity, PoA (Point of Attachment), can detect the new attachment and get the necessary information to deliver an unicast L2 frame to the host, such as 802.11 MAC address or 802.16 CID (Connection Identifier) [19].

The PoA may forward the information to an AR (Access Router) and trigger the AR to immediately send in unicast a suitable RA, such as 'RA optimized for DNA' defined in [5].

Or the PoA itself may cache such an RA beforehand and deliver the cached RA to the host in unicast as soon as the link-layer connection is established.

In this draft, we refer the first scheme "RA Triggering" and the second "RA Proxying".

3.1 RA Triggering

In case PoA and AR are in the same box, when a new host is attached, link-layer (PoA module) can deliver Link UP event notification [7] to IP layer (AR module) to generate a suitable RA and immediately send the RA (in an unicast L2 frame with the host's MAC address).

In case PoA and AR are separated, upon a new network attachment, the PoA may deliver the AR the Link Up event notification with the information necessary to deliver an unicast RA. Upon receiving this notification, the AR can send a suitable RA in unicast without delay.

There are two ways for such a remote Link Up event notification. We may use the MIES (Media Independent Event Service) defined in IEEE 802.21 [21] or RS with TSLLAO (Tentative Source Link-Layer Address Option) [14].

3.2 RA Proxying

RA Proxying consists of "RA Caching" and "RA Delivery". RA Caching is to get a suitable RA and store it. RA Delivery is to immediately send the cached RA to a new host in unicast

There are several ways to cache the RA in a PoA. We may manually cache the RA in the PoA or use the scanning scheme. AR (Access Router)s periodically multicast a suitable RA, which goes through the PoA. So the PoA may scan incoming L2 frames and cache a necessary RA. The PoA can scan L2 frames either continuously or periodically to update the cached RA. Or PoA and AR may use a special information

service, such as the MICS (Media Independent Command Service) defined in IEEE 802.21 [21] in such a way that the AR can forward the PoA the information necessary to generate a suitable RA and permit it to porxy the RA.

For RA Delivery, PoA may put the cached RA into an unicast L2 frame with the host's MAC address (or CID for 802.16) and deliver it to the host in unicast immediately after link-layer connection is established.

4. RA Triggering

In case PoA and AR are in the same box, when a new host is attached, Link Up event notification with the information necessary to deliver an unicast RA, such as the host's MAC address, can be propagated upwards from the link-layer (PoA module) to the IP layer (AR module) within a local stack. Then IP layer (AR module) can immediately send a suitable RA in an unicast L2 frame with the new host's MAC address.

In case PoA and AR are separated, we may use 802.21 MIES (Media Independent Event Service) [21] to enable a PoA to trigger a remote AR to fire an immediate RA in unicast.

MIES (Media Independent Event Service) refers to the events sent from the lower layers to the higher layers. Events can also be sent from a local MIH entity to a peer MIH entity. Events may carry useful information. For example, Link Up event can carry a new host's MAC address.

When a new host is attached to a PoA, the PoA may use Link Up event and MIH Protocol to notify a remote AR the new attachment with the information necessary to deliver an unicast RA, such as the host's MAC address. Then the AR can immediately send a suitable RA in an unicast L2 frame with the new host's MAC address.

5. RA Proxying

RA Proxying is used only when AR and PoA are separated. If they are in the same box, we recommend to use RA Triggering instead.

5.1 RA Caching

We present 3 different ways to store a suitable RA in PoA.

5.1.1 Manual Configuration

In the simplest way, we can manually configure in PoA a suitable RA, such as RA with the linkid prefix in [13] or CompleteRA in [12]. In many cases, AR and PoA are under same administration and usually RA (Router Advertisement) message doesn't change so often.

5.1.2 Scanning

A PoA may scan incoming L2 frame for a suitable RA and store it.

First it scans L2 frame header to see whether it is a multicast frame. If not, the PoA sends that frame down link and scans a next L2 frame. If so, the PoA looks IP header to check whether it contains a suitable RA. If incoming L2 frame doesn't contain a suitable RA, the PoA sends that frame down link and scans a next L2 frame. When the PoA finds a suitable RA, it stores it and sends a copy down link.

A PoA can scan continuously, updating an old RA with a new RA. Or if it costs too much for the PoA to scan every incoming L2 frame, we can control the scanning rate. For example, we can set timer and execute scanning every T seconds. Or we can make the PoA to be able to send RS (Router Solicitation) message. Periodically the PoA sends an RS and an AR will reply a suitable RA and the PoA caches it. It is noted that the PoA doesn't need to have IP address since it can use unspecified address as its source address.

To help RA Caching, we may make it a rule that, whenever an AR changes its RA information, the AR advertises the new information several times, so that PoA can properly update its cached RA.

5.1.3 MICS (Media Independent Comment Service)

We may use 802.21 MICS (Media Independent Comment Service) and MIH (Media Independent Handover) Protocol [21] to enable an AR to send a suitable RA to a PoA and delegate the PoA to proxy the RA.

MICS (Media Independent Comment Service) refers to the commands sent

from the higher layers to the lower layers. Commands can also be sent from a local MIH entity to a peer MIH entity. These commands may carry the upper layer information to the lower layers on local device entity or at remote entity, and thus control the behavior of lower layers. For example, a new AR may send its IP address to old PoA with a Remote MIH Command, "MIH Network Address Information".

In a similar way, we may define a new Remote MIH Command, "MIH Router Advertisement Information" in 802.21 in such a way that 1) a PoA can use the command and MIP Protocol to request a suitable RA from an AR and permission to proxy the RA and 2) the AR can use the command and MIH Protocol to send a suitable RA to the PoA and delegate the PoA to deliver the RA to a new host upon network attachment

5.2 RA Delivery

We present a way to immediately deliver an RA in unicast upon network attachement for 802.11 and 802.16 respectively. The procedures describes in here can be extended to apply to other wireless technologies such as 3GPP and 3GPP.2.

5.2.1 802.11

In 802.11 Wireless LAN technology, when a new host arrives at an AP(Access Point), it should associate with the AP. The host sends an Association Request Message with its MAC address. Then the AP sends an Association Response Message to grant association.

As soon as association is made, the AP sends a cached RA to the host in an unicast 802.11 frame with the MAC address from the Association Request message. The host receives the unicast RA just after association is made, which is the earliest possible time in current standard.

5.2.2 802.16

IEEE 802.16 spec [19] is rather different from Ethernet or 802.11 and it's still unclear how to run IPv6 over 802.16. So we give a rough sketch of RA delivery over 802.16 and mention that further clarification is needed.

The 802.16 MAC is connection-oriented. All services, including inherently connectionless services, are mapped to a connection.

Connections are referenced with 16-bit connection identifiers (CIDs). Each 802.16 host has a standard 48-bit MAC address, but this serves mainly as an equipment identifier, since the primary addresses used during operation are the CIDs.

Upon entering the network, the host is assigned three management connections, the basic connection and the primary management connection and the secondary management connection.

The secondary management connection is used for the transfer of standards-based management messages such as Dynamic Host Configuration Protocol (DHCP). It is not decided yet but Neighbor Discovery messages, such as RS, RA, NS (Neighbor Solicitation) and NA (Neighbor Advertisement) may be delivered with this connection.

To establish a link layer connection, an 802.16 host performs Ranging to acquire the correct timing offset and power adjustment. The host sends the RNG-REQ message and the 802.16 BS (Base Station) replies RNG-RSP message to provide Basic and Primary Management CIDs for the host.

Afterwards the host performs Registration, which is the process by which the host is allowed entry into the network and receives its Secondary Management CID.

After Registration is completed, the 802.16 BS may send a cached RA to the host with the Secondary CID. The RA will be delivered in unicast 802.16 frame and the host will receive it with minimum latency.

We point out that it's not decided yet that the Secondary CID is used for RA message transfer. It's possible for RA to be delivered with a different CID.

6. IANA Considerations

No new message formats or services are defined in this document.

7. Security Considerations

Because DNA is based on Neighbor Discovery, its trust models and threats are similar to the ones presented in RFC 3756 [10]. Nodes connected over wireless interfaces may be particularly susceptible to jamming, monitoring and packet insertion attacks.

The threats specific to DNA are that an attacker might fool a node to detect attachment to a different link when it is in fact still attached to the same link, and conversely, the attacker might fool a node to not detect attachment to a new link.

In case PoA and AR are in the same box, there is no FRD specific security problem, because all procedures are executed within a local stack. In case PoA and AR are separated, FRD can be performed in secure manner, if there is a secure path between PoA and AR. For example, MIH (Media Independent Handover) services can be made available at L2 through secure port.

Even when there is no secure path between PoA and AR, FRD doesn't introduce a new security vulnerability. For the worst case, a host may reject the proxyed RA from PoA but will not make a false decision. Currently any node in a link can cache an RA and retransmit it. Use of [9] to secure Neighbor Discovery are important in achieving reliable detection of network attachment. DNA schemes SHOULD incorporate the solutions developed in IETF SEND WG if available, where assessment indicates such procedures are required.

DAN scheme should not result in excessive signaling. A PoA performs FRD procedures to generate an RA message only when a new host is attached to itself. Usually there is an upper bound for the number of hosts (wireless stations) that a PoA can support at a moment. So the number of RA messages from FRD procedure is also limited by this upper bound.

8. Acknowledgment

We gratefully acknowledge the generous assistance we received from Xiaoyu Liu, YounHee Han and James Kempf for notifying us the usability of 802.21 standard and clarifying the MIH Spec to us. We show our special gratitude to HeeJin Jang, Subba Reddy and Surekha Biruduraju for implementing and testing FRD scheme to provide enlightening insights. The authors wish to express our appreciation to Syam Madanapalli and Wable Ranjitsingh for valuable feedback. Thanks to Greg Daley, Brett Pentland, Nick Moore and YongGeun Hong for their contributions to this draft.

9. References

9.1 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] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[4] Choi, J., "Goals of Detecting Network Attachment in IPv6", draft-ietf-dna-goals-04 (work in progress), December 2004.

9.2 Informative References

[5] Choi, J. and E. Nordmark, "DNA solution framework", draft-ietf-dna-soln-frame-00 (work in progress), April 2005.

[6] Nordmark, E. and J. Choi, "DNA with unmodified routers: Prefix list based approach", draft-ietf-dna-cpl-01 (work in progress), July 2005.

[7] Yegin, A., "Link-layer Event Notifications for Detecting Network Attachments", draft-ietf-dna-link-information-01 (work in progress), February 2005.

[8] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[9] Arkko, J., Kempf, J., Sommerfeld, B., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", draft-ietf-send-ndopt-06 (work in progress), July 2004.

[10] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[11] Pentland, B., "An Overview of Approaches to Detecting Network Attachment in IPv6", draft-dnadt-dna-discussion-00 (work in progress), February 2005.

[12] Narayanan, S., "Detecting Network Attachment in IPv6 Networks (DNAv6)", draft-pentland-dna-protocol-00 (work in progress), May 2005.

[13] Choi, J., "DNA Solution: Link Identifier based approach",

draft-jinchoi-dna-protocol2-00 (work in progress), May 2005.

[14] Daley, G., "Tentative Source Link-Layer Address Options for IPv6 Neighbour Discovery", draft-daley-ipv6-tsllao-01 (work in progress), February 2005.

[15] Aboba, B., "Detecting Network Attachment (DNA) in IPv4", draft-ietf-dhc-dna-ipv4-13 (work in progress), June 2005.

[16] Nordmark, E., "MIPv6: from hindsight to foresight?", draft-nordmark-mobileip-mipv6-hindsight-00 (work in progress), November 2001.

[17] Kempf, J., Khalil, M., and B. Pentland, "IPv6 Fast Router Advertisement", draft-mkhalil-ipv6-fastra-05 (work in progress), July 2004.

[18] Daley, G. and J. Choi, "Movement Detection Optimization in Mobile IPv6", draft-daley-mobileip-movedetect-01 (work in progress), May 2003.

[19] IEEE 802.16-2001, "IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems," Apr. 8, 2002.

[20] IEEE 802.16 TGe Working Document (Draft Standard), "Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands", IEEE 802.16e/D8, May 2005.

[21] IEEE 802.21 Working Document (Draft Standard), "IEEE P802.21/D00.01: Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services," July, 2005.

Authors' Addresses

JinHyeock Choi
Samsung AIT
Communication & N/W Lab
P.O.Box 111 Suwon 440-600
KOREA

Phone: +82 31 280 9233
Email: jinchoe@samsung.com

DongYun Shin
Samsung Electronics
Device Solution Group
P.O.Box 111 Suwon 440-600
KOREA

Phone: +82 2 2191 4868
Email: yun7521@samsung.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.