DNA WG
Internet-Draft
Expires: January 10, 2005

JinHyeock Choi
DongYun Shin
Samsung AIT

July 12, 2004

Fast Router Discovery with RA Caching
draft-jinchoi-dna-frd-00.txt

Status of this Memo

Copyright Notice

Abstract

This document presents RA Caching in AP for Fast Router Discovery. For seamless handoff, a mobile node MUST quickly discover its new access router. In our proposal an AP caches a Router Advertisement message and sends it to a new mobile node as soon as new L2 association is made. We present a way for an AP to cache a suitable RA. By putting 'RA Caching' and 'AP Notification' functionality on AP, we get the optimized result without IPv6 standard change.

Table of Contents

1. Introduction

The primary movement detection mechanism for Mobile IPv6 defined in [8] uses the facilities of IPv6 Neighbor Discovery [4], including Router Discovery and Neighbor Unreachability Detection. A mobile node MUST quickly detect when it moves to a link served by a new access router, so that it can acquire a new care-of address and send Binding Updates quickly. A mobile node MUST receive Router Advertisement from a new access router as soon as possible.

There are several hindrances for sufficiently fast Router Discovery. First, Neighbor Discovery protocol [4] limits routers to a minimum interval of 3 seconds between sending unsolicited multicast Router Advertisement messages. Second, it SHOULD delay the transmission for a random amount of time before a mobile node sends an initial Router Solicitation. Third, a router MUST delay a response to a Router Solicitation by a random time too. Though solutions are proposed by [8], [11], they require IPv6 standard [4] change.

In our proposal AP (Access Point) caches a suitable RA (Router Advertisement) message , for example 'RA optimized for DNA' defined in [10], and sends it to a new mobile node as soon as L2 association is made. We present a way for an AP to cache a suitable RA. By putting 'RA Caching' and 'AP Notification' functionality on an Access Point, we get the optimized result without IPv6 standard change. In our scheme, mobile node receives Router Advertisement just after L2 association is made which is the earliest possible time under the current standard.

2. Terminology

Access Router (AR)

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

Access Point (AP)

An L2 entity that has station functionality and provides access to the distribution services, via the wireless medium for associated stations.

3. Proposal Overview

In 802.11 b Wireless LAN technology, when an MN (mobile node) arrives at a new link, it should associate with a new AP.

In our proposal, an AP caches an RA message beforehand and sends it to a mobile node as soon as L2 association is made.

We can cache an RA in an AP manually or use the following scheme. An AR (Access Router) periodically multicasts an unsolicited RA, which goes through an AP. So the AP can scan incoming L2 frames and cache a necessary RA. the AP scans L2 frames either continuously or periodically to update a stored RA. Moreover if an AR and an AP are under same network administration, they can be configured such that an AP caches an RA efficiently.

4. Operation Description

Our proposal consists of 'RA Caching' and 'AP Notification', RA Caching periodically scans incoming L2 frames for an unsolicited RA and stores it. AP Notification sends a stored RA to a new MN as soon as L2 association is made.

4.1 RA Caching

An AP scans incoming L2 frame for an unsolicited RA.

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

An AP can scan continuously, updating an old RA with a new RA. Or if it costs too much for the AP 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 AP to be able to send Router Solicitation message. Periodically the AP sends Router Solicitation. Then an AR will reply an RA and the AP caches it. It is noted that the AP doesn't need to have IP address since it can use unspecified address as its source address.

4.2 AP Notification

When a new MN arrives at an AP, it sends an Association Request Message with its MAC address. Then the AP grants association by sending an Association Response Message. As soon as association is made, the AP sends a stored RA to a new MN with MAC address in Association Request message. The MN receives an RA just after association is made which is the earliest possible time in current standard.

5. IANA Considerations

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

6. Security Considerations

Since our proposal is based on Neighbor Discovery, its trust models and threats are similar to the ones presented in [4].

If higher layer notification of connectivity is not available, and eager handoff strategies are in place, any node or router which advertises an RA with a false prefix will cause mobile nodes to perform spurious handover signalling and DAD operations.

But above threats are inherent to all schemes which depends exclusively on Router Discovery for movement detection. Our proposal doesn't incur any additional threats. We will incorporate the solutions [12] developed in IETF SEND Working Group when available.

7. References

7.1 Normative References

[1] Bradner, S., "IETF Rights in Contributions", BCP 78, RFC 3667, February 2004.

[2] Bradner, S., "Intellectual Property Rights in IETF Technology", BCP 79, RFC 3668, February 2004.

[3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

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

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

[7] Choi, J., "Detecting Network Attachment in IPv6 Goals", draft-ietf-dna-goals-00 (work in progress), June 2004.

7.2 Informative References

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

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

[13] Choi, J. and E. Nordmark, "DNA solution framework" draft-jinchoi-dna-soln-frame-00.txt (work in progress), July 2004.

[11] Kempf, J., Khalil, M. and B. Pentland, "IPv6 Fast Router Advertisement", draft-mkhalil-ipv6-fastra-02 (work in progress), October 2002.

[12] Arkko, J., Kempf, J., Sommerfeld, B., Zill, B. and P. Nikander, "SEcure Neighbor Discovery (SEND)", draft-ietf-send-ndopt-05 (work in progress), April 2004.

Authors' Addresses

JinHyeock Choi
Samsung AIT
i-Networking Lab
P.O.Box 111 Suwon 440-600
KOREA

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

DongYun Shin
Samsung AIT
i-Networking Lab
P.O.Box 111 Suwon 440-600
KOREA

Phone: +82 31 280 8321
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.