Network Working Group S. Russert, Ed.
Internet-Draft F. Templin, Ed.
Intended status: Standards Track Boeing Phantom Works
Expires: August 24, 2007 February 20, 2007

Hierarchical Mobility Anchor Points (HMAPs) for Network Localized Mobility Mangement (NETLMM)
draft-russert-netlmm-hmap-00.txt

Status of this Memo

Copyright Notice

Abstract

The Mobility Anchor Point (MAP) for Network Localized Mobility Management (NETLMM) is a single point of failure for the Localized Mobility Management Domain (LMMD) and a focal point for all mobile node (MN) traffic. These shortcomings can be addressed by distributing the MAP function equally among the Access Routers (ARs) in the LMMD and deploying hierarchically organized supporting nodes in the backhaul network. This document specifies a Hierarchical MAP

(HMAP) and its use in operational delployments that support traffic distribution and fault tolerance. Solutions for both IPv4 and IPv6 are given.

1. Introduction

This document specifies a Hierarchical Mobility Anchor Point (HMAP) that combines the DHCP [RFC2131][RFC3315] client, server, and relay functions together with a router function for Network-based Localized Mobility Management (NETLMM). HMAPs are deployed in a prefix delegation hierarchy that is automatically configured and/or operationally determined by the administrative authority for the Localized Mobility Management Domain (LMMD). The lowest level HMAPs in the prefix delegation hierarchy correspond to the Access Routers (ARs) in the NETLMM model represented in [I-D.templin-autoconf-netlmm-dhcp].

Each HMAP except the root for the LMMD has a delegating HMAP, and each delegating HMAP serves requesting HMAPs that it provisions with more-specific prefixes derived from its own prefixes. Each HMAP advertises the prefix(es) it aggregates via the LMMD's Interior Gateway Protocol (IGP).

HMAPs relay DHCP client messages to the authoritative HMAP for the address(es)/prefix(es) represented in the messages. HMAPs include the Classless Static Route (CSR) option in DHCP messages per ([I-D.templin-autoconf-netlmm-dhcp], Section 5.4) to update other HMAPs based on MN arrivals and departures.

2. Terminology

The terminology in the normative references applies; the following terms are defined within the scope of this document:

Hierarchical Mobility Anchor Point (HMAP)
: A backhaul network router that also configures the server, relay, and client functions of DHCP; as a server, the HMAP aggregates one or more prefixes.

delegating HMAP
: An HMAP that delegates prefixes per [I-D.ietf-dhc-subnet-alloc][RFC3633].

requesting HMAP
An HMAP that requests prefixes from a delegating HMAP per [I-D.ietf-dhc-subnet-alloc][RFC3633].

home HMAP
The HMAP that is authoritative for a particular MN, i.e., the HMAP that delegated the MN's addresses/prefixes.

visited HMAP
The HMAP that currently acts as Access Router (AR) for a roaming MN.

3. Model of Operation

HMAPs are configured to form a hierarchy based on prefix delegation, with each requesting HMAP in turn delegating progressively longer prefixes to form a chain of delegating/requesting HMAPs. The lowest level of the hierarchy delegates addresses/prefixes to MNs. (The same HMAP may both delegate prefixes to requesting HMAPs and delegate addresses/prefixes directly to MNs.)

Data packets destined for a MN are forwarded to the home HMAP (e.g., by standard IGP routing) which either delivers them to the MN on an attached access network or tunnels them to the MN's current visited HMAP. DHCP messages are relayed in the control plane to the authoritative HMAP for the MN's delegated address(es)/prefix(es).

Each HMAP has DHCP server, client, and relay functions. The client function allows the HMAP to request prefixes from a delegating HMAP, act as a DHCP proxy on behalf of a MN, and respond to server commands such as FORCERENEW (DHCPv4) and Reconfigure (DHCPv6). Server and relay functions interact; when an HMAP receives a client's DHCP message requesting renewal or confirmation of a MN's address(es)/ prefix(es) its server function begins processing the message to determine whether it is authoritative for the MN. If it is authoritative, it continues processing in server mode; otherwise, it shifts to relay-mode and forwards the message to the nexthop toward the authoritative HMAP.

4. HMAP Functional Specification

An HMAP serves as a home, visited, or relaying HMAP depending on its relationship to the MN's address(es)/prefix(es); an HMAP may perform all three functions concurrently on behalf of different MNs.

Each HMAP initializes, registers, and responds to the discovery of

new MNs as specified in ([I-D.templin-autoconf-netlmm-dhcp], Section 5) and in the following sections:

4.1. Home HMAP

When an HMAP receives a DHCP DISCOVER, REQUEST, INFORM (DHCPv4), Solicit, Request, or Information-request (DHCPv6) from a MN attached to one of its access links (or, when the HMAP acts as a DHCP proxy on behalf of a MN), it serves the request normally per [RFC2131][RFC3315].

For messages other than DISCOVER or Solicit, the home HMAP checks for route entries in its IP forwarding table to determine whether the MN is returning home from a visited HMAP. If the MN is returning home, the home HMAP creates a Classless Static Route Option (CSR) per ([I-D.templin-autoconf-netlmm-dhcp], Section 5), to inform the previously-visited HMAP that routes for the MN's address(es)/ prefix(es) should be deleted. It then sends a FORCERENEW (v4) or Reconfigure (v6) containing the CSR to the client function of the previously-visited HMAP.

When an HMAP receives a DHCP REQUEST, INFORM (DHCPv4), Request, or Information-request (DHCPv6) for which it is authoritative that has been relayed, it:

1. Forms a tunnel to the visited HMAP.

2. Creates IP forwarding table entries for the MN via the tunnel.

3. For DHCPv4, sends the DHCP ACK, including in the message a CSR option that adds a route for the MN with the visited HMAP as next-hop. This CSR is not intended for use at the MN, but is used by the visited HMAP to create a route entry for the roaming MN.

   For DHCPv6, sends the reply within a Relay-reply message including a CSR option that adds a route for the MN at the visited HMAP, with the visited HMAP as nexthop.

4.2. Visited HMAP

When an HMAP receives a REQUEST, INFORM (v4), Request, Confirm, or Information-Request (v6) concerning addresses/prefixes for which it is not authoritative, it relays the message to the nexthop in the path toward the authoritative server per standard DHCP relay behavior.

When a visited HMAP receives a server's DHCP message concerning a MN

that has roamed onto one of its access links, it updates its IP forwarding table according to information in CSR options attached to the message.

4.3. Relaying HMAP

HMAPs that are not authoritative for the address(es)/prefixe(es) represented in a specific client-server message relay the message to the nexthop in the path toward the authoritative server per standard DHCP relay behavior.

If an HMAP cannot relay the message, it sends a NAK (DHCPv4) or a Reply message with lifetimes for the IA set to 0 and a StatusCode option containing status code NotOnLink (DHCPv6) to the client. In response to these messages, a DHCPv4 client will restart the configuration process, and a DHCPv6 client will perform DHCP server solicitation and client-initiated reconfiguration.

4.4. HMAP Failover

When a delegating HMAP discovers that one of its requesting HMAPs has become unreachable (e.g., fails to renew its leases), it ceases to relay messages to it. The delegating HMAP also begins to respond to DHCP messages on behalf of the departed requesting HMAP.

5. IANA Considerations

This document has no actions for IANA.

6. Security Considerations

The security considerations in [I-D.templin-autoconf-netlmm-dhcp] apply also to this specification.

7. Acknowledgements

The following individuals have provided valuable input:

8. References

8.1. Normative References

[I-D.templin-autoconf-netlmm-dhcp]
Templin, F., "Network Localized Mobility Management using

DHCP", draft-templin-autoconf-netlmm-dhcp-04 (work in progress), October 2006.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

8.2. Informative References

[I-D.ietf-dhc-subnet-alloc]
Johnson, R., "Subnet Allocation Option", draft-ietf-dhc-subnet-alloc-04 (work in progress), October 2006.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

Authors' Addresses

Steven W. Russet (editor)
Boeing Phantom Works
P.O. Box 3707 MC 7L-49
Seattle, WA 98124
USA

Email: steven.w.russert@boeing.com

Fred L. Templin (editor)
Boeing Phantom Works
P.O. Box 3707 MC 7L-49
Seattle, WA 98124
USA

Email: fred.l.templin@boeing.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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