Network Working Group
Request for Comments: 4977
Category: Informational

G. Tsirtsis
Qualcomm
H. Soliman
Elevate Technologies

August 2007

Problem Statement: Dual Stack Mobility

Status of This Memo

Abstract

This document discusses the issues associated with mobility management for dual stack mobile nodes. Currently, two mobility management protocols are defined for IPv4 and IPv6. Deploying both in a dual stack mobile node introduces a number of problems. Deployment and operational issues motivate the use of a single mobility management protocol. This document discusses such motivations. The document also discusses requirements for the Mobile IPv4 (MIPv4) and Mobile IPv6 (MIPv6) protocol so that they can support mobility management for a dual stack node.

Table of Contents

1. Terminology

This document uses the following terms as defined in Stateless IP/ ICMP Translation (SIIT) [RFC2765]: IPv4-capable node, IPv4-enabled node, IPv6-capable node, IPv6-enabled node.

The following terms are introduced in this document:

- MIPv4-capable node:

  A node that supports MIPv4 [RFC3344] in its implementation. This allows the mobile node to configure a home address (statically or dynamically) and use such address in its Mobile IPv4 signaling. A MIPv4-capable node may also be IPv6-capable or IPv6-enabled and must be IPv4-capable.

- MIPv6-capable node:

  A node that supports MIPv6 [RFC3775] by configuring a home address and using such address in its Mobile IPv6 signaling. A MIPv6-enabled node may also be IPv4-capable or IPv4-enabled and must be IPv6-capable.

2. Introduction and Motivation

A MIPv4-capable node can use Mobile IPv4 [RFC3344] to maintain connectivity while moving between IPv4 subnets. Similarly, a MIPv6-capable node can use Mobile IPv6 [RFC3775] to maintain connectivity while moving between IPv6 subnets.

One of the ways of migrating to IPv6 is to deploy nodes that are both IPv4 and IPv6 capable. Such nodes will be able to get both IPv4 and IPv6 addresses and thus can communicate with the current IPv4 Internet as well as any IPv6 nodes and networks as they become available.

A node that is both IPv4 and IPv6 capable can use Mobile IPv4 for its IPv4 stack and Mobile IPv6 for its IPv6 stack so that it can move between IPv4 and IPv6 subnets. While this is possible, it does not ensure connectivity since that also depends on the IP version support of the network accessed. Supporting Mobile IPv4 and Mobile IPv6 is also more inefficient since it requires:

- Mobile nodes to be both MIPv4 and MIPv6 capable.

- Mobile nodes to send two sets of signaling messages on every handoff.

- Network Administrators to run and maintain two sets of mobility management systems on the same network, with each of these systems requiring its own set of optimizations.

This document discusses the potential inefficiencies, IP connectivity problems, and operational issues that are evident when running both mobility management protocols simultaneously. It also proposes a work area to be taken up by the IETF on the subject and discusses requirements for appropriate solutions.

3. Problem Description

Mobile IP (v4 and v6) uses a signaling protocol (Registration requests in MIPv4 [RFC3344] and Binding updates in MIPv6 [RFC3775]) to set up tunnels between two end points. At the moment, Mobile IP signaling is tightly coupled to the address family (i.e., IPv4 or IPv6) used, in the connections it attempts to manipulate. There are no fundamental technical reasons for such coupling. If Mobile IP were viewed as a tunnel-setup protocol, it should be able to set up IP in IP tunnels, independently of the IP version used in the outer and inner headers. Other protocols -- for example, SIP [RFC3261] -- are able to use either an IPv4- or IPv6-based signaling plane to manipulate IPv4 and IPv6 connections.

A node that is both MIPv4 and MIPv6 capable, will require the following to roam within the Internet:

- The network operator needs to ensure that the home agent supports both protocols or that it has two separate Home Agents supporting the two protocols, each requiring its own management.

- Double the amount of configuration in the mobile node and the home agent (e.g., security associations).

- IP-layer local network optimizations for handovers will also need to be duplicated.

We argue that all of the above will make the deployment of Mobile IPv6, as well as any dual stack solution in a mobile environment, harder. We will discuss some of the issues with the current approach separately in the following sections.

3.1. The Impossibility of Maintaining IP Connectivity

Even if a mobile node is both MIPv4 and MIPv6 capable, connectivity across different networks would not, in fact, be guaranteed since that also depends on the IPv4/IPv6 capabilities of the networks the mobile is visiting; i.e., a node attempting to connect via a IPv4-only network would not be able to maintain connectivity of its IPv6 applications and vice versa. This is potentially the most serious problem discussed in this document.

3.2. Implementation Burdens

As mentioned above, a node that is IPv4 and IPv6 capable must also be MIPv4 and MIPv6 capable to roam within the Internet. The ability to employ both IP versions from one mobility protocol makes it possible to implement just that one protocol, assuming the protocol choice is known. However, in situations where the mobile node must be capable of working in any network, it may still need two protocols.

3.3. Operational Burdens

As mentioned earlier, deploying both protocols will require managing both protocols in the mobile node and the home agent. This adds significant operational issues for the network operator. It would certainly require the network operator to have deep knowledge in both protocols, which is something an operator may not be able to justify due to the lack of substantial gains.

In addition, deploying both protocols will require duplication of security credentials on mobile nodes and home agents. This includes IPsec security associations, keying material, and new authentication protocols for Mobile IPv6, in addition to the security credentials and associations required by Mobile IPv4. Depending on the security mechanisms used and with some further work, it might be possible to rely on one set of common credentials. Assuming nothing else changes, however, such duplication is again significant with no gain to the operator or the mobile node.

3.4. Mobility Management Inefficiencies

Suppose that a mobile node is moving within a dual stack access network. Every time the mobile node moves, it needs to send two mobile IP messages to its home agent to allow its IPv4 and IPv6 connections to survive. There is no reason for such duplication. If local mobility optimizations were deployed (e.g., Hierarchical Mobile IPv6 (HMIPv6) [RFC4140], Fast handovers for Mobile IPv4 [RFC4068]), the mobile node will need to update the local agents running each protocol. Ironically, one local agent might be running both HMIPv6

and local MIPv4 home agent. Clearly, it is not desirable to have to send two messages and complete two sets of transactions for the same fundamental optimization.

Hence, such parallel operation of Mobile IPv4 and Mobile IPv6 will complicate mobility management within the Internet and increase the amount of bandwidth needed at the critical handover time for no apparent gain.

3.5. IPv4 to IPv6 Transition Mechanisms

The IETF has standardized a number of transition mechanisms to allow networks and end nodes to gain IPv6 connectivity while the Internet is migrating from IPv4 to IPv6. However, while some transition mechanisms can be combined with Mobile IPv4 or Mobile IPv6, none of the known mechanisms have been shown to assist with the issues described in this document.

4. Conclusions and Recommendations

The points above highlight the tight coupling in both Mobile IPv4 and Mobile IPv6 between signaling and the IP addresses used by upper layers. Given that Mobile IPv4 is currently deployed and Mobile IPv6 is expected to be deployed, there is a need for gradual transition from IPv4 mobility management to IPv6. Running both protocols simultaneously is inefficient and has the problems described above. The gradual transition can be done when needed or deemed appropriate by operators or implementers. In the meantime, it is important to ensure that the problems listed above can be avoided. Hence, this section lists some actions that should be taken by the IETF to address the problems listed above, without mandating the use of two mobility management protocols simultaneously.

The Mobile IPv6 Working Group has reached the view that to allow for a gradual transition based on current standards and deployment, the following work areas would be reasonable:

- It should be possible to run one mobility management protocol that can manage mobility for both IPv4 and IPv6 addresses used by upper layers. Both Mobile IPv4 and Mobile IPv6 should be able to perform such tasks. It may not be possible to support route optimization for Mobile IPv6 in all cases; however, mobility management and session continuity can be supported.

- It should be possible to create IPv4 extensions to Mobile IPv6 so that an IPv4 and IPv6 capable mobile node can register its IPv4 and IPv6 home addresses to an IPv4- and IPv6-enabled Home Agent using MIPv6 signaling only.

- It should be possible to create IPv6 extensions to Mobile IPv4 so that an IPv4 and IPv6 capable mobile node can register its IPv4 and IPv6 home addresses to an IPv4- and IPv6-enabled Home Agent using Mobile IPv4 signaling only.

- It should also be possible to extend MIPv4 [RFC3344] and MIPv6 [RFC3775] so that a mobile node can register a single care-of address (IPv4 or IPv6) to which IPv4 and/or IPv6 packets can be tunneled.

If the IETF chooses to pursue all these paths, a vendor could choose to support one mobility management protocol while avoiding the incompatibility and inefficiency problems listed in this document. Similarly, operators could decide to continue using one mobility management protocol throughout the period of IPv4 and IPv6 coexistence. However, a mobile node would be forced to choose one approach or the other, or nevertheless to install both and use one or the other according to circumstances.

5. Security Considerations

This document is a problem statement that does not by itself introduce any security issues.

6. References

6.1. Normative References

[RFC2765] Nordmark, E., "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765, February 2000.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

6.2. Informative References

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC4068] Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[RFC4140] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, August 2005.

Authors' Addresses

George Tsirtsis
Qualcomm

Phone: +908-443-8174
EMail: tsirtsis@qualcomm.com

Hesham Soliman
Elevate Technologies

Phone: +614-111-410-445
EMail: hesham@elevatemobile.com

Full Copyright Statement

Intellectual Property