Mobility Extensions for IPv6
(mext)
Internet-Draft
Intended status: Informational
Expires: September 14, 2011

W. Haddad
Ericsson
C. Perkins
WiChorus Inc.

March 13, 2011

A Note on NAT64 Interaction with Mobile IPv6
draft-haddad-mext-nat64-mobility-harmful-02

Abstract

This memo discusses potential NAT64 technology repercussions for mobile nodes using Mobile IPv6. An ambiguity is identified related to the use of DNS during bootstrapping, which is likely to inhibit proper signaling between mobile node and home agent.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 14, 2011.

Copyright Notice

Table of Contents

1. Introduction

NAT64 technology, as described in [I-D.ietf-behave-v6v4-xlate-stateful], enables faster IPv4 network conversion to IPv6-only operation while maintaining contact with the remaining global IPv4 Internet. In this document, we are concerned with IPv6-only nodes attached to a network for which NAT64 provides connectivity with IPv4 networks.

This document aims to highlight potential NAT64 repercussions for mobile nodes using Mobile IPv6 ([I-D.ietf-mext-rfc3775bis]) and attached to a network behind a NAT64.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. NAT64 Incompatibility with Mobile IPv6

NAT technologies have from the very beginning exhibited numerous incompatibities with the Internet. Hence, the new incompatibility described in this document should not come as a surprise!

The NAT64 mechanism considered here complies with the DNS64 technology described in [I-D.ietf-behave-dns64] to provide the querying host with a synthetic DNS response in which, the queried FQDN is locally translated to an IPv6 address using the v6 prefix assigned to the NAT64 v6 interface. By inserting the translated IPv6 address in the synthetic DNS response, the querying node acts as if the destination is also using an IPv6 stack. This, in turn, enables the two nodes to establish a session during which, all exchanged packets are routed through the querying node's local NAT64 in order to reach their destinations.

As NAT64 technology is likely to be widely deployed, we consider its behavior in relationship to Mobile IPv6. For this purpose, suppose that a mobile node (MN) configured with an IPv6 home address (HoA) leaves its NAT64-serviced home network and attaches to a foreign network also serviced by NAT64, and configures a new IPv6 address, i.e., a care-of address (CoA). We analyze two scenarios which require using MIPv6 either to maintain a session, or to establish an optimal path to exchange the data packets, using MIPv6 route optimization (RO).

In the first scenario, suppose that before detaching from its home network, the MN has established a session with a corresponding node (CN) which is attached to an IPv4 network. Due to the NAT64 presence in the home network, the MN acts as if it were communicating with an IPv6-enabled CN. Hence, the MN decides upon attaching to the new NAT64-serviced foreign network, to run the MIPv6 return routability procedure with the CN by sending first a home test init (HoTI) message via its home agent. Such messages will be discarded either by the CN or by a more intelligent NAT64 -- in which case it would likely be followed by an ICMP message sent to the MN. In both cases, the MN can detect that the RR procedure is failing. Consequently, there is little harm to the MN's communications and no data packet loss since the MN will keep using MIPv6 bidirectional tunneling (BT) mode.

However, the situation worsens when we consider another scenario in which the MN decides to establish a session with the same CN from the foreign NAT64-serviced network. In such case, the MN will first obtain a synthetic DNS reply which presents the CN as being an IPv6-enabled node. Based on that, the MN may try to create a binding at the CN. The MN might first run the RR procedure which will

ultimately fail (for the same reasons as in the first scenario). More likely, the MN will initiate the session with the CN by using the BT mode then switching to the RO mode. In this case, the MN first tunnels its data packets to its HA without having them being intercepted by the foreign NAT64. However, after reaching the HA, the data packets will most likely be dropped at some point. This is due to the presence of the foreign NAT64 IPv6 prefix in the CN's IPv6 address.

4. Security Considerations

This document describes scenarios where a NAT64, using DNS64, can disrupt communications to a mobile node visiting the associated network. It does not introduce any new security vulnerabilities, provide any guidance about how to improve security, or describe any effects on existing security practices.

5. Acknowledgements

Thanks to Francis Dupont and Joel Halpern for reviewing the document at an early stage.

6. References

6.1. Normative References

[I-D.ietf-mext-rfc3775bis]
Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", draft-ietf-mext-rfc3775bis-13 (work in progress), March 2011.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

6.2. Informative References

[I-D.ietf-behave-dns64]
Bagnulo, M., Sullivan, A., Matthews, P., and I. Beijnum, "DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", draft-ietf-behave-dns64-11 (work in progress), October 2010.

[I-D.ietf-behave-v6v4-xlate-stateful]
Bagnulo, M., Matthews, P., and I. Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", draft-ietf-behave-v6v4-xlate-stateful-12 (work in progress), July 2010.

Authors' Addresses

Wassim Haddad
Ericsson
300 Holger Way
San Jose, CA 95134
US

Phone: +408 750 5667
Email: Wassim.Haddad@ericsson.com

Charles E. Perkins
WiChorus Inc.
3590 North, 1st Street, Suite 300
San Jose, CA 95134
US

Email: Charliep@computer.org