Abstract

RFC 5905 [RFC5905], section 7.3, "Packet Header Variables", defines the value to be used as the REFID for network associations. For IPv4 associations the IPv4 address is used, and for IPv6 associations four octets of the MD5 hash of the IPv6 are used. Often, the REFID is simplistically and incorrectly used to identify upstream servers. While this works in an IPv4 network, it doesn’t work for IPv6 associations and may have other problems in an environment with mixed use of IPv4 and IPv6. Specifically, the NTP Project has received a report where the generated IPv6 hash decoded to the IPv4 address of a different machine on the system peer’s network.

This proposal offers a way for a system to generate a REFID for a system peer that communicates over IPv6 that does not conflict with a valid IPv4-based REFID.

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 15, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction ........................................ 2
   1.1. Requirements Language ............................. 3
2. Augmenting the IPv6 REFID Hash ........................ 3
3. Potential Problems .................................... 3
4. Questions ............................................ 4
5. Acknowledgements ...................................... 4
6. IANA Considerations ................................... 4
7. Security Considerations ............................... 4
8. Normative References .................................. 4
Author’s Address ......................................... 4

1. Introduction

RFC 5905 [RFC5905], section 7.3, "Packet Header Variables", defines
the value to be used as the REFID for network associations. It says:

    If using the IPv4 address family, the identifier is the four-octet
IPv4 address. If using the IPv6 family, it is the first four
octets of the MD5 hash of the IPv6 address. ...

Often, the REFID is simplistically and incorrectly used to identify
upstream servers. While this works in an IPv4 network, it doesn’t
work for IPv6 associations and may have other problems in an
environment with mixed use of IPv4 and IPv6. Specifically, the NTP
Project has received a report where the generated IPv6 hash decoded
to the IPv4 address of a different machine on the system peer’s
network.

This proposal offers a way for a system to generate a REFID for a
system peer that communicates over IPv6 that does not conflict with a
valid IPv4-based REFID.
1. Requirements Language

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 RFC 2119 [RFC2119].

2. Augmenting the IPv6 REFID Hash

When generating a REFID based on a network system peer, the NTPv4 specification says:

If using the IPv4 address family, the identifier is the four-octet IPv4 address. If using the IPv6 family, it is the first four octets of the MD5 hash of the IPv6 address. ...

This means that the IPv4 representation of the IPv6 hash would be: b1.b2.b3.b4. The proposal is that the system MAY also use 255.b2.b3.b4 as its REFID.

When using the REFID to check for a timing loop for an IPv6 association, if the code that checks the first four-octets of the hash fails to match then the code must check again, using 0xFF as the first octet of the hash.

3. Potential Problems

There is a 1 in 16,777,216 chance that the REFID hashes of two IPv6 addresses will be identical, producing a false-positive loop detection. With a sufficient number of servers, the risk of this problem becomes a non-issue. The use of the "REFID Suggestion" extension field is also a way to mitigate this potential situation.

Unrealistically, if only two instances of NTP are communicating via IPv6 and one side implements this new IPv4 REFID hash and the other side does not, the "other side" will not be able to detect this loop condition. In this case, the two machines will slowly increase their Stratum until they reach S16 and become unsynchronized. This situation is considered to be unrealistic because the only current way this could happen would be for there to only be these two instances of NTP available as time sources in a misconfigured "orphan mode" setup. There is no risk of this happening in an NTP network with 3 or more time sources, or in a properly-configured "time island" setup.
4. Questions

Should we ask IANA to allocate a pseudo Extension Field Type of 0xFFFF (for example) so the proposed "I-Do" exchange can report whether or not the "IPv6 REFID Hash" is supported?

5. Acknowledgements

The author wishes to acknowledge Dan Mahoney (and perhaps others) for suggesting the idea of using an "impossible" first-octet value to indicate an IPv6 refid hash. The author wishes to acknowledge the contributions of Joey Saccadonuts.

6. IANA Considerations

This memo makes no requests of IANA.

7. Security Considerations

Additional information TBD

8. Normative References


Author’s Address

Harlan Stenn
Network Time Foundation
P.O. Box 918
Talent, OR 97540
US

Email: stenn@nwtime.org