Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: September 15, 2016

H. Stenn
Network Time Foundation

March 14, 2016

Network Time Protocol Suggest REFID Extension Field
draft-stenn-ntp-suggest-refid-00

Abstract

NTP has been widely used through several revisions, with the latest being RFC 5905 [RFC5905]. A core component of the protocol and the algoritms is the Reference ID, or REFID, which is used to identify the source of time used for synchronization. Traditionally, when the source of time was another system the REFID was the IPv4 address of that other system. The purpose of the REFID is to prevent a one-degree timing loop, where if A has several timing sources that include B, if B decides to get its time from A we don't want A then deciding to get its time from B. The REFID is considered to be "public data" and is a vital core-component of the base NTP packet. If a system's REFID is the IPv4 address of its system peer, an attacker can try to use that information to send spoofed time packets to either or both the target or the target's server, attempting to cause a disruption in time service. This proposal is a backward-compatible way for a time source to tell its peers or clients "If you use me as your system peer, use this nonce as your REFID." This nonce SHOULD not be traceable to the original system, and if it is used as the REFID this type of attack is prevented.

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.

Table of Contents

1. Introduction

NTP has been widely used through several revisions, with the latest being RFC 5905 [RFC5905]. A core component of the protocol and the algoritms is the Reference ID, or REFID, which is used to identify the source of time used for synchronization. Traditionally, when the source of time was another system, the REFID was the IPv4 address of that other system. If the remote system was using IPv6 for its connection, a 4 octet digest value of the IPv6 address was used. The purpose of the REFID is to prevent a one-degree timing loop, where if A has several timing sources that include B, if B decides to get its time from A we don't want A then deciding to get its time from B. The REFID is considered to be "public data" and is a vital core-component of the base NTP packet. If a system's REFID is the IPv4 address of its system peer, an attacker can try to use that information to send spoofed time packets to either or both the target or the target's server, attempting to cause a disruption in time service. This proposal is a backward-compatible way for a time source to tell its peers or clients "If you use me as your system

peer, use this nonce as your REFID." This nonce, a Suggested REFID, SHOULD not be traceable to the sending system. If the receiving system uses this Suggested REFID nonce instead of the IPv4 address as its REFID, this type of attack and information disclosure is prevented.

The NTP protocol was designed with a mechanism that allowed for a depth-1 loop detection to avoid a simple "time loop". Recently, this mechanism was discovered to be a potential vulnerability exploit. The best way to mitigate this vulnerability is to decouple the IPv4 address of the server from its REFID. But there is no current way for a potential time source to tell the other party any other alternative to use as the REFID. This proposal creates an extension field to accomplish this.

1.1. 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. The REFID

The core reason for the REFID in the NTP Protocol is to prevent a timing loop of degree 1. Put another way, if servers A and B are exchanging time with each other and server B decides to follow A as its system peer, the REFID that B will use must be able to identify server A. The interpretation of a REFID is based on the stratum, as documented in RFC 5905 [RFC5905], section 7.3, "Packet Header Variables". At Stratum 2+, which will be the case if servers A and B are exchanging packets over IPv4, if server B follows A, then B will have A's IPv4 address as its REFID. When A asks B for its time, A will see that B is synchronized to A because B will tell A that its REFID is A's IPv4 address, so when A sees its IP address as B's REFID, A knows that if it were to follow B for its time then there would be a timing loop. In this case, A will not select B as a potential source of time.

3. The Suggested REFID Extension Field

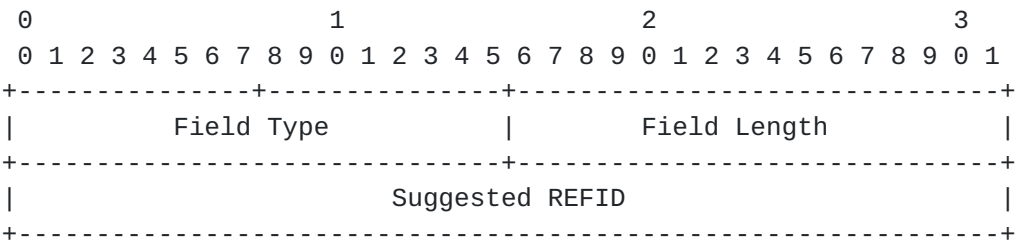
Since there is no way in the base NTP packet for "this" instance of an NTP server to tell the "other" instance what REFID it should use if the "other" instance decides to use "this" instance as its system peer, the best available way to convey this information is via an extension field.

If an incoming packet contains an unrecognized extension field, one of two things will happen. Either that extension field will be

ignored, or the entire packet will be dropped. If an extension field is present there ordinarily SHOULD be a MAC following the extension field. Some extension fields are unable to be "signed" by a MAC, regardless of whether or not that MAC is a traditional MAC or an extension field MAC.

The following paragraph is included for informational purposes. Another proposal is on its way that addresses and clarifies extension fields, perhaps in the form of an errata to https://datatracker.ietf.org/doc/draft-ietf-ntp-extension-field .

To assist in the validation of an NTP packet that contains extension fields, if the Field Type has the 0x2000 bit set in it, there MAY be a MAC after this extension field. If the Field Type does not have the 0x2000 bit set in it, there SHOULD be a MAC after this extension field.



NTP Extension Field: REFID Suggestion

Field Type: TBD (Recommendation for IANA: 0x0006 (Suggested REFID, MAC required), 0x2006 (Suggested REFID, MAC OPTIONAL))

Field Length: 0x0008

Suggested REFID: The 4 octets of the suggested REFID. This value SHOULD be 0xFDxxxxxx, where the bottom 3 octets SHOULD be random values.

Examples: When decoded as an IPv4 address, suggested REFIDs would decode as 253.0.0.0 thru 253.255.255.255.

4. Generating and Sending the Suggested REFID Extension Field

A system that decides to send a Suggested REFID extension field SHOULD generate a new Suggested REFID for each new association. It MAY generate a new Suggested REFID for any association in any response. In addition to remembering the IP-based REFID, the sender should also remember the Suggested REFID.

Since the core NTPv4 and earlier protocols do not contain any way to tell the recipient what to use as a REFID and RFC 5905 [RFC5905] uses the IPv4 address of the sender as the REFID if the association is effected over an IPv4 connection, this means that an attacker can simply send an NTP client request to a server knowing that server's system peer will be returned as the REFID in the response packet. At this point, an attacker can, if that REFID is an IPv4 address, begin to launch attacks at the target forging the putative IP of the target's time source, or the attacker can start forging packets to the putative time server claiming to be from the target, in an attempt to cause the time server to limit or deny time service to the target.

Using a nonce for the REFID that is only recognized by the sending machine effectively prevents this type of attack.

If servers S1, S2, and S3 are all exchanging time with each other, there is a 1 in 16,777,216 (2^24) chance that two different servers in the same group will happen to choose the same nonce, and that would produce a false-positive timing loop detection. If the Suggested REFID is never changed, this false-positive condition will occur for potentially a long time. This small risk can be reduced by periodically generating a new Suggested REFID.

5. Receiving a Suggested REFID Extension Field

An NTP server keeps track of the IP address it uses to talk to a client. If an NTP server chooses to send a Suggested REFID to an association, it MUST remember this value. When checking for a timing loop, the Suggested REFID must also be included in the list of tested values.

6. Acknowledgements

The author wishes to acknowledge the contributions of Martin Burnicki and Sam Weiler.

7. IANA Considerations

This memo requests IANA to allocate NTP Extension Field Types 0x0006 (Suggested REFID, MAC required), 0x2006 (Suggested REFID, MAC OPTIONAL) for this purpose.

8. Security Considerations

Additional information TBD

9. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <http://www.rfc-editor.org/info/rfc5905>.

[RFC7384] Mizrahi, T., "Security Requirements of Time Protocols in Packet Switched Networks", RFC 7384, DOI 10.17487/RFC7384, October 2014, <http://www.rfc-editor.org/info/rfc7384>.

Author's Address

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

Email: stenn@nwtime.org