NTP Working Group
Internet Draft
Intended status: Standards Track
Updates: 5905
Expires: August 2016

T. Mizrahi
Marvell
D. Mayer
Network Time Foundation

February 9, 2016

The Network Time Protocol Version 4 (NTPv4) Extension Fields
draft-ietf-ntp-extension-field-07.txt

Abstract

The Network Time Protocol Version 4 (NTPv4) defines the optional usage of extension fields. An extension field, defined in RFC5905, is an optional field that resides at the end of the NTP header, and can be used to add optional capabilities or additional information that is not conveyed in the standard NTP header. This document updates RFC5905 by clarifying some points regarding NTP extension fields and their usage with Message Authentication Codes (MAC).

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 9, 2016.

Copyright Notice

Table of Contents

1. Introduction

The NTP header format consists of a set of fixed fields that may be followed by some optional fields. Two types of optional fields are defined, Message Authentication Codes (MAC), and extension fields, as defined in Section 7.5 of [RFC5905].

If a MAC is used, it resides at the end of the packet. This field can be either 24 octets long, 20 octets long, or a 4-octet crypto-NAK.

NTP extension fields were defined in [RFC5905] as a generic mechanism that allows to add future extensions and features without modifying the NTP header format (Section 16 of [RFC5905]).

The only currently defined extension fields are the ones used by the AutoKey protocol [RFC5906], and the Checksum Complement [NTPComp]. The AutoKey extension field is always followed by a MAC, and Section 10 of [RFC5906] specifies the parsing rules that allow a host to distinguish between an extension field and a MAC. However, a MAC is not mandatory after an extension field; an NTPv4 packet can include one or more extension fields without including a MAC (Section 7.5 of [RFC5905]).

This document updates [RFC5905] by clarifying some points regarding the usage of extension fields. These updates include changes to address errors found after the publication of [RFC5905] with respect to extension fields. Specifically, this document updates Section 7.5 of [RFC5905], clarifying the relationship between extension fields and MACs, and defining the behavior of a host that receives an unknown extension field.

2. Conventions Used in this Document

2.1. Terminology

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 [KEYWORDS].

2.2. Terms & Abbreviations

NTPv4	Network Time Protocol Version 4 [RFC5905]
MAC	Message Authentication Code

3. NTP Extension Fields - RFC 5905 Update

This document updates Section 7.5 of [RFC5905] as follows:

OLD:

7.5. NTP Extension Field Format

In NTPv4, one or more extension fields can be inserted after the header and before the MAC, which is always present when an extension field is present. Other than defining the field format, this document makes no use of the field contents. An extension field contains a request or response message in the format shown in Figure 14.

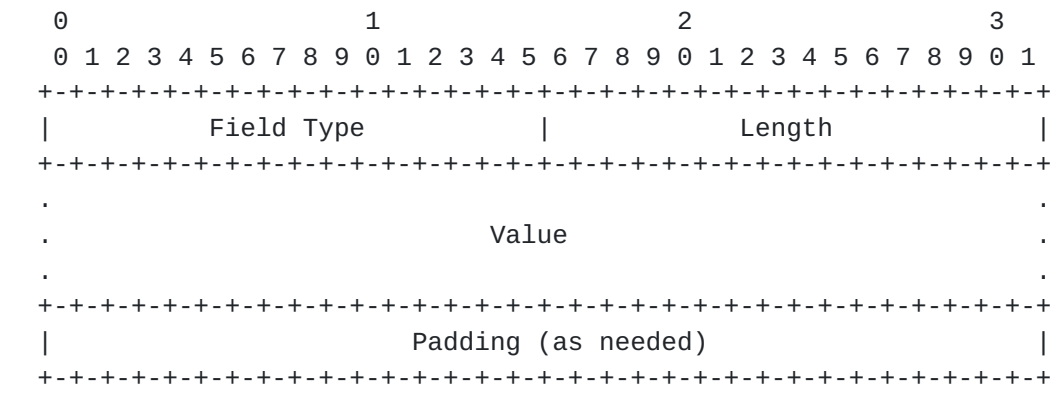

Figure 14: Extension Field Format

All extension fields are zero-padded to a word (four octets) boundary. The Field Type field is specific to the defined function and is not elaborated here. While the minimum field length containing required fields is four words (16 octets), a maximum field length remains to be established.

The Length field is a 16-bit unsigned integer that indicates the length of the entire extension field in octets, including the Padding field.

NEW:

7.5. NTP Extension Field Format

In NTPv4, one or more extension fields can be inserted after the header and before the MAC, if a MAC is present.

Other than defining the field format, this document makes no use of the field contents. An extension field contains a request or response message in the format shown in Figure 14.

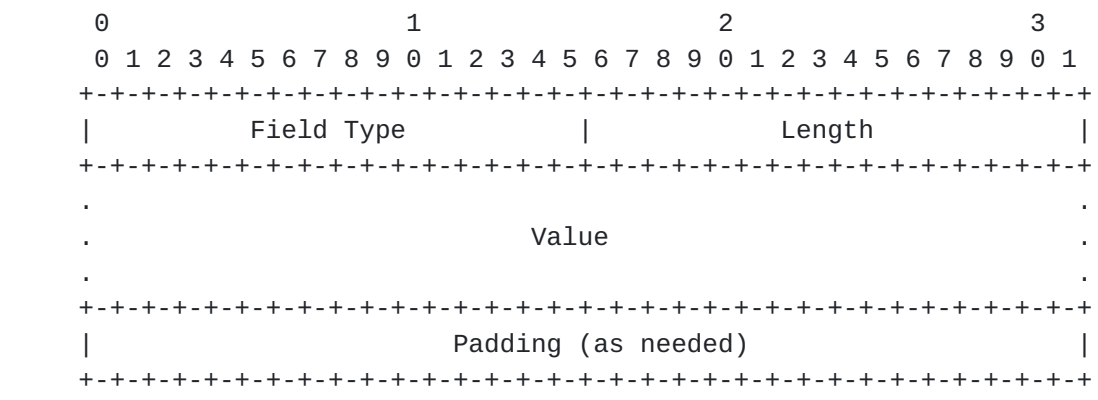

Figure 14: Extension Field Format

All extension fields are zero-padded to a word (four octets) boundary.

The Field Type, Value, and Padding fields are specific to the defined function and are not elaborated here; the Field Type value is defined in an IANA registry and its Length, Value and Padding are defined by the document referred to by the registry. If a host receives an extension field with an unknown Field Type, the host SHOULD ignore the extension field and MAY drop the packet altogether if policy requires it.

While the minimum field length containing required fields is four words (16 octets), the maximum field length cannot be longer than 65532 octets due to the maximum size of the length field.

The Length field is a 16-bit unsigned integer that indicates the length of the entire extension field in octets, including the Padding field.

7.5.1 Extension Fields and MACs

7.5.1.1 Extension Fields in the Presence of a MAC

An extension field can be used in an NTP packet that includes a MAC, for example, as defined in [RFC5906]. A specification that defines a new extension field MUST specify whether the extension field requires a MAC or not. If the extension field requires a MAC, the extension field specification MUST define the algorithm to be used to create the MAC and the length of the MAC thus created. An extension field MAY allow for more than one algorithm to be used in which case the information about which one was used MUST be included in the extension field itself.

7.5.1.2 Multiple Extension Fields with a MAC

If there are multiple extension fields that require a MAC they MUST all require use of the same algorithm and MAC length. Extension fields that do not require a MAC can be included with extension fields that do require a MAC.

An NTP packet MUST NOT be sent with two or more extension fields that require a MAC with different algorithms.

If an NTP packet is received with two or more extension fields that this receiver recognizes and those fields require a MAC with different algorithms, the packet MUST be discarded.

7.5.1.3 MAC in the absence of an Extension field

A MAC MUST NOT be longer than 24 octets if there is no extension field present, unless a longer MAC is agreed upon by both client and server. The client and server can negotiate this behavior using a previous exchange of packets with an extension field which defines the size and algorithm of the MAC transmitted in NTP packets.

7.5.1.4 Extension Fields in the Absence of a MAC

If a MAC is not present, one or more extension fields can be inserted after the header, according to the following rules:

- If the packet includes a single extension field, the length of the extension field MUST be at least 7 words, i.e., at least 28 octets.

- If the packet includes more than one extension field, the length of the last extension field MUST be at least 28 octets. The length of the other extension fields in this case MUST be at least 16 octets each.

4. Security Considerations

The security considerations of time protocols in general are discussed in [RFC7384], and the security considerations of NTP are discussed in [RFC5905].

Distributed Denial-of-Service (DDoS) attacks on NTP servers involve flooding a server with a high rate of NTP packets. Malicious usage of extension fields cannot amplify such DDoS attacks; such malicious attempts are mitigated by NTP servers, since the servers ignore unknown extension fields (as discussed in Section 3.), and only

respond, if needed, with known extension fields. Extension fields from incoming packets are neither propagated by NTP servers nor included in any response. NTP servers create their own extension fields if needed for a response. A large number of extension fields should be flagged by an NTP server as a potential attack. Large extension field sizes should also be flagged unless they are expected to be large.

Middleboxes such as firewalls MUST NOT filter NTP packets based on their extension fields. Such middleboxes should not examine extension fields in the packets since NTP packets may contain new extension fields that the middleboxes have not been updated to recognize.

5. IANA Considerations

There are no new IANA considerations implied by this document.

6. Acknowledgments

The authors gratefully acknowledge Dave Mills for his insightful comments. The authors also thank Tim Chown, Sean Turner, Miroslav Lichvar, Suresh Krishnan, and Jari Arkko for their thorough review and helpful comments.

This document was prepared using 2-Word-v2.0.template.dot.

7. References

7.1. Normative References

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

[RFC5905] Mills, D., Martin, J., Burbank, J., Kasch, W., "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

7.2. Informative References

[RFC5906] Haberman, B., Mills, D., "Network Time Protocol Version 4: Autokey Specification", RFC 5906, June 2010.

[RFC7384] Mizrahi, T., "Security Requirements of Time Protocols in Packet Switched Networks", RFC 7384, October 2014.

[NTPComp] Mizrahi, T., "UDP Checksum Complement in the Network Time Protocol (NTP)", draft-ietf-ntp-checksum-trailer (work in progress), October 2015.

Authors' Addresses

Tal Mizrahi
Marvell
6 Hamada St.
Yokneam, 20692 Israel

Email: talmi@marvell.com

Danny Mayer
Network Time Foundation
PO Box 918
Talent OR 97540

Email: mayer@ntp.org