Internet Engineering Task Force (IETF)
Request for Comments: 5908
Category: Standards Track
ISSN: 2070-1721

R. Gayraud
Unaffiliated
B. Lourdelet
Cisco Systems, Inc.

June 2010

Network Time Protocol (NTP) Server Option for DHCPv6

Abstract

The NTP Server Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) provides NTPv4 (Network Time Protocol version 4) server location information to DHCPv6 hosts.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5908.

Table of Contents

1. Introduction

This document defines a DHCPv6 option and associated suboptions to provide Network Time Protocol version 4 [RFC5905] or greater server location information to DHCPv6 hosts.

2. Requirements Notation

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. Related Work and Usage Model

The NTP service is publicly offered on the Internet by a number of organizations. Those servers can be used but should not be abused, so any method that is tasked to disseminate locations of NTP servers must act responsibly in a manner that does not lead to public server overloading. When using DHCPv6 to offer NTP server location, and if there is a need to distribute a host with a hardcoded configuration, this configuration MUST NOT include server location that is not part of the organization that distributes this device. Typical usage of this option is to specify an NTP server that is part of the organization that operates the DHCPv6 server.

The location of the NTP service, like any other Internet service, can be specified by an IP address or a Fully Qualified Domain Name (FQDN). By design, DHCP offers information to multiple devices and is prone to amplification of mistakes, so great care must be taken to define its configuration. Specification of the NTP service by FQDN offers a level of indirection that works as a possible mitigation

tool in case of misconfiguration. DNS can be used to redirect misconfigured clients to an IPv6 address that is not configured on any host instead of having to change the address of the NTP server itself.

While the NTP specification defines a comprehensive set of configuration parameters, modification of those parameters is best left to the decision of the client itself. The DHCPv6 option for NTP is therefore restricted to server location.

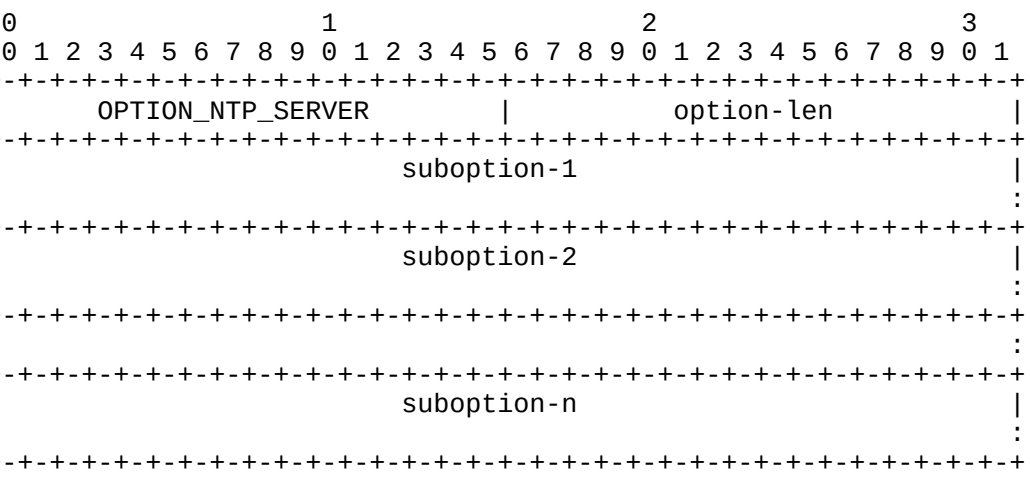
4. NTP Server Option for DHCPv6

This option serves as a container for server location information related to one NTP server or Simple Network Time Protocol (SNTP) [RFC4330] server. This option can appear multiple times in a DHCPv6 message. Each instance of this option is to be considered by the NTP client or SNTP client as a server to include in its configuration.

The option itself does not contain any value. Instead, it contains one or several suboptions that carry NTP server or SNTP server location. This option MUST include one, and only one, time source suboption. The currently defined time source suboptions are NTP_OPTION_SRV_ADDR, NTP_OPTION_SRV_MC_ADDR, and NTP_OPTION_SRV_FQDN. It carries the NTP server or SNTP server location as a unicast or multicast IPv6 address or as an NTP server or SNTP server FQDN. More time source suboptions may be defined in the future. While the FQDN option offers the most deployment flexibility, resiliency as well as security, the IP address options are defined to cover cases where a DNS dependency is not desirable.

If the NTP server or SNTP server location is an IPv6 multicast address, the client SHOULD use this address as an NTP multicast group address and listen to messages sent to this group in order to synchronize its clock.

The format of the NTP Server Option is:



option-code: OPTION_NTP_SERVER (56),

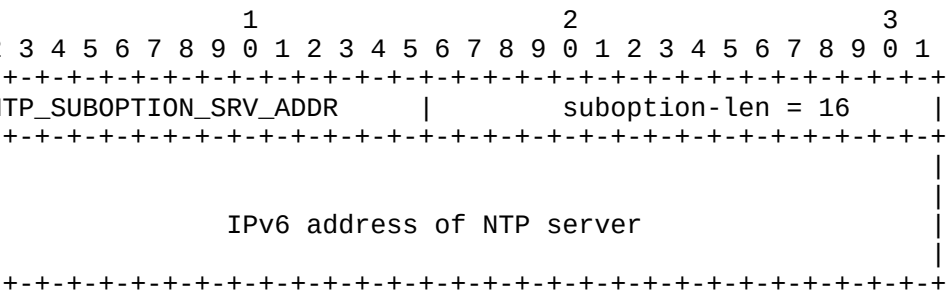
option-len: Total length of the included suboptions.

This document does not define any priority relationship between the client's embedded configuration (if any) and the NTP or SNTP servers discovered via this option. In particular, the client is allowed to simultaneously use its own configured NTP servers or SNTP servers and the servers discovered via DHCP.

4.1. NTP Server Address Suboption

This suboption is intended to appear inside the OPTION_NTP_SERVER option. It specifies the IPv6 unicast address of an NTP server or SNTP server available to the client.

The format of the NTP Server Address Suboption is:



IPv6 address of the NTP server: An IPv6 address,

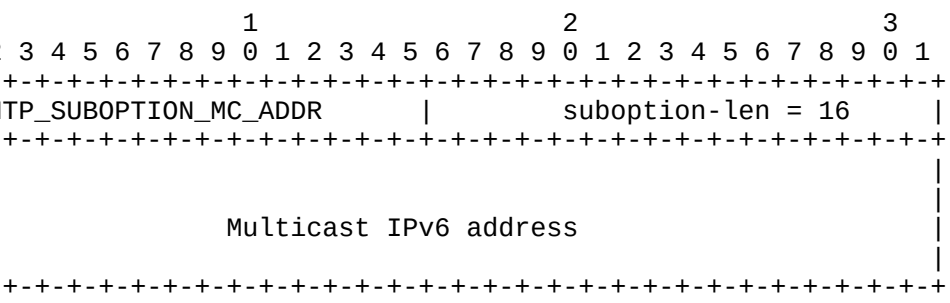
suboption-code: NTP_SUBOPTION_SRV_ADDR (1),

suboption-len: 16.

4.2. NTP Multicast Address Suboption

This suboption is intended to appear inside the OPTION_NTP_SERVER option. It specifies the IPv6 address of the IPv6 multicast group address used by NTP on the local network.

The format of the NTP Multicast Address Suboption is:



Multicast IPv6 address: An IPv6 address,

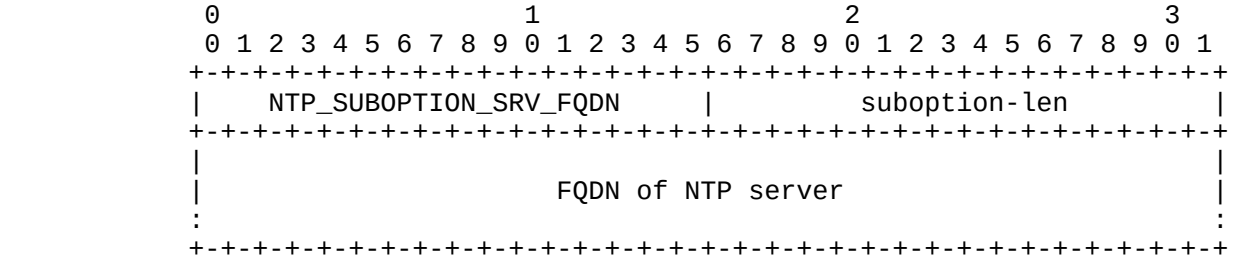
suboption-code: NTP_SUBOPTION_MC_ADDR (2),

suboption-len: 16.

4.3. NTP Server FQDN Suboption

This suboption is intended to appear inside the OPTION_NTP_SERVER option. It specifies the FQDN of an NTP server or SNTP server available to the client.

The format of the NTP Server FQDN Suboption is:



suboption-code: NTP_SUBOPTION_SRV_FQDN (3),

suboption-len: Length of the included FQDN field,

FQDN: Fully-Qualified Domain Name of the NTP server or SNTP server. This field MUST be encoded as described in [RFC3315], Section 8. Internationalized domain names are not allowed in this field.

5. Appearance of This Option

The OPTION_NTP_SERVER option can appear multiple times in a DHCPv6 message. The order in which these options appear is not significant. The client uses its usual algorithms to determine which server(s) or multicast group(s) should be preferred to synchronize its clock.

The OPTION_NTP_SERVER option MUST NOT appear in messages other than the following: Solicit, Advertise, Request, Renew, Rebind, Information-Request, and Reply. If this option appears in messages other than those specified above, the receiver MUST ignore it.

The option number for this option MAY appear in the "Option Request" option [RFC3315] in the following messages: Solicit, Request, Renew, Rebind, Information-Request, and Reconfigure. If this option number appears in the "Option Request" option in messages other than those specified above, the receiver SHOULD ignore it.

6. Security Considerations

This option could be used by an intruder to advertise the address of a malicious NTP server or SNTP server and adversely affect the clock of clients on the network. The consequences of such an attack can be critical, because many security protocols depend on time synchronization to run their algorithms. As an example, an attacker could break connectivity between SEND-enabled nodes [RFC3971], simply by affecting the clock on these nodes.

To prevent these attacks, it is strongly advisable to secure the use of this option by either:

- using the NTPv4 Autokey public key authentication, as defined in [RFC5906] or,

- using authenticated DHCP as described in [RFC3315], Section 21.

7. RFC 4075 Deprecation

"Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6" [RFC4075] provides some degree of automatic time server configuration for IPv6, as it specifies how to transmit SNTP [RFC4330] server addresses through DHCPv6. However, this approach is not suitable for all NTP deployments. It is not an extensible mechanism and introduces some semantic confusion through the use of the "SNTP" acronym. Additionally, the approach of only offering IPv6 addresses to specify server location does not meet NTP requirements that make use of an FQDN (Fully-Qualified Domain Name) as well. For all the abovementioned reasons, this document makes [RFC4075] deprecated.

8. IANA Considerations

IANA has assigned 56 as an option code from the "DHCPv6 Options Codes" registry for OPTION_NTP_SERVER.

IANA is required to maintain a new number space of NTP time source suboptions, located in the BOOTP-DHCP Parameters Registry. The initial suboptions are described in Section 4 of this document. IANA assigns future NTP time source suboptions with an "IETF Consensus" policy as described in [RFC5226]. Future proposed suboptions are to be referenced symbolically in the documents that describe them, and shall be assigned numeric codes by IANA when approved for publication as an RFC.

9. References

9.1. Normative References

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

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

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

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

9.2. Informative References

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC4075] Kalusivalingam, V., "Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6", RFC 4075, May 2005.

[RFC4330] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 4330, January 2006.

Authors' Addresses

Richard Gayraud
Unaffiliated

EMail: richardgayraud@free.fr

Benoit Lourdelet
Cisco Systems, Inc.
Village ent. GreenSide, Bat T3,
400, Av de Roumanille,
06410 BIOT - Sophia-Antipolis Cedex
France

Phone: +33 4 97 23 26 23
EMail: blourdel@cisco.com