Network Working Group	R. Gayraud	
Internet-Draft	None	
Intended status: Standards Track	B. Lourdelet	
Expires: September 7, 2009	Cisco Systems, Inc.	
	March 06, 2009	

TOC

Network Time Protocol (NTP) Server Option for DHCPv6
draft-ietf-ntp-dhcpv6-ntp-opt-03.txt

Status of this Memo

Copyright Notice

Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

The NTP Server Option for DHCPv6 provides NTP (Network Time Protocol version 4) configuration information to DHCPv6 hosts.

Table of Contents

1. Requirements notation
2. Introduction
    2.1. Related Work and Usage Model
3. NTP Server Option for DHCPv6
    3.1. NTP Server Address Suboption
    3.2. NTP Multicast Address Suboption
    3.3. NTP Server FQDN Suboption
4. Examples of use
5. Appearance of this Option
6. Security Considerations
7. IANA Considerations
8. References
    8.1. Normative References
    8.2. Informative References
§ Authors' Addresses

---

1. Requirements notation

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

2. Introduction

TOC

This document defines a DHCPv6 option and associated suboptions to provide Network Time Protocol version 4 [draft-ntpv4] or greater configuration information to DHCPv6 hosts.

2.1. Related Work and Usage Model

TOC

[RFC4075] (Kalusivalingam, V., “Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6,” May 2005.) (SNTP Configuration Option for DHCPv6) provides some degree of automatic time server configuration for IPv6, as it specifies how to transmit SNTP [RFC4330] (Mills, D., “Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI,” January 2006.) servers addresses through DHCPv6. However this approach is not suitable for all NTP deployments. It is not an extensible mechanism and introduces some semantic confusion throught 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 a FQDN (Fully Qualified Domain Name) as well.

The NTP service is publicly offered on the Internet by a number of organizations. Those servers can be used but not abused, so any method which 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 device with a hardcoded configuration, this configuration MUST NOT include server location that is not part of the organization that distribute 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 an 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 unexisting IPv6 address 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 then restricted to server location.

---

3. NTP Server Option for DHCPv6

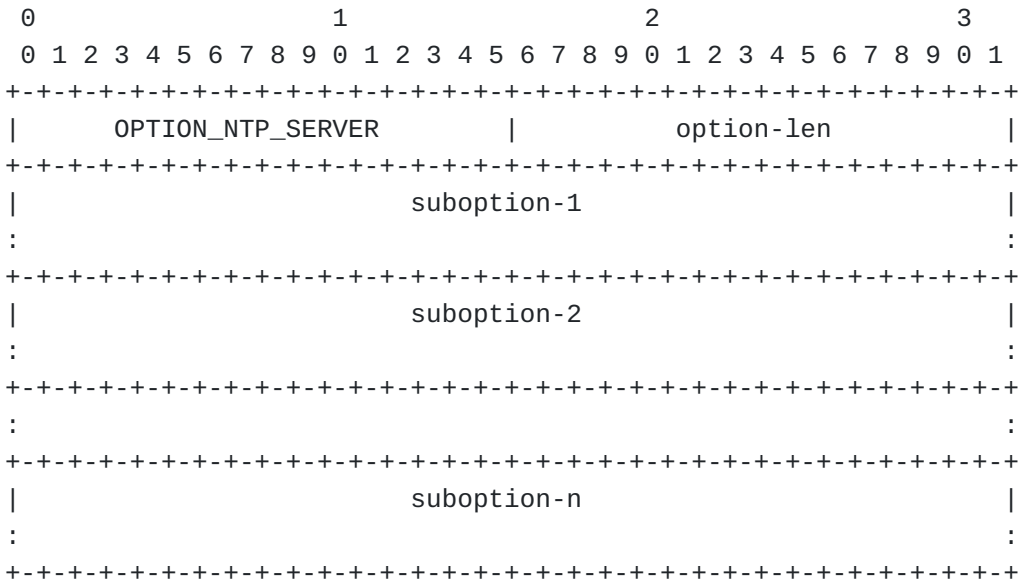
TOC

This option serves as a container for all the information related to one NTP server. This option can appear multiple times in a DHCPv6 message. Each instance of this option is to be considered by the NTP 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 configuration information.

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, NTP_OPTION_SRV_FQDN. It carries the NTP server location, as a unicast or multicast IPv6 address or as an NTP 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 dependancy to DNS is not desirable.
If the NTP 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 (TBD_IANA),

option-len: Total length of the included suboptions.

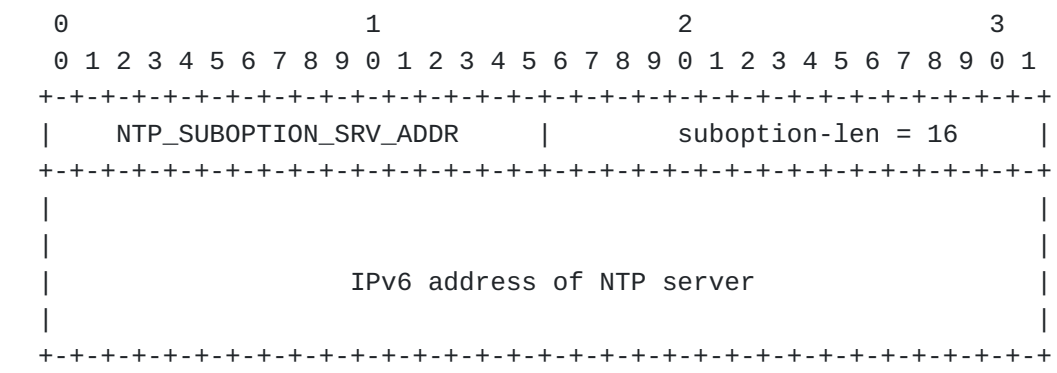
This document does not define any priority between the client's embedded configuration and the NTP servers discovered via this option. In particular, the client is allowed to simultaneously use its own configured NTP servers and the servers discovered via DHCP.

3.1. NTP Server Address Suboption

TOC

This suboption is intended to appear inside the OPTION_NTP_SERVER option. It specifies the IPv6 unicast address of an NTP server available to the client. An example of use is present in Section 4 (Examples of use).

The format of the NTP Server Address Suboption is:



suboption-code: NTP_SUBOPTION_SRV_ADDR (1),

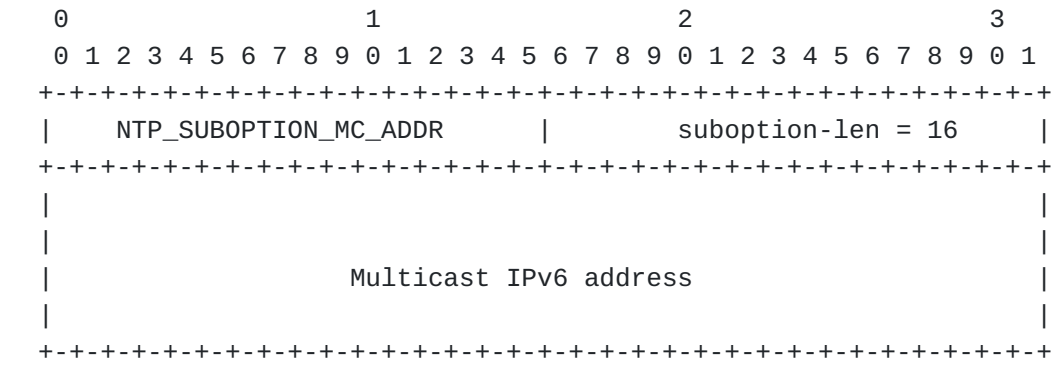
suboption-len: 16.

3.2. NTP Multicast Address Suboption

TOC

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. An example of use is present in Section 4 (Examples of use).

The format of the NTP Multicast Address Suboption is:



suboption-code: NTP_SUBOPTION_MC_ADDR (2),

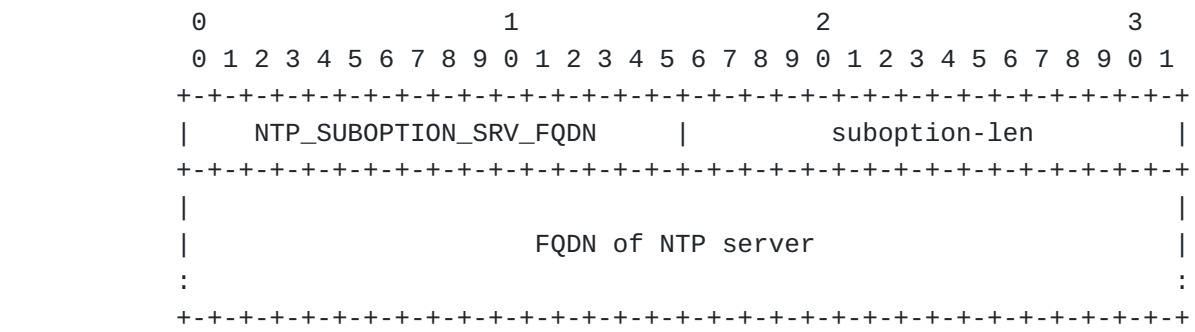
suboption-len: 16.

TOC

3.3. NTP Server FQDN Suboption

This suboption is intended to appear inside the OPTION_NTP_SERVER option. It specifies the FQDN of an NTP server 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,

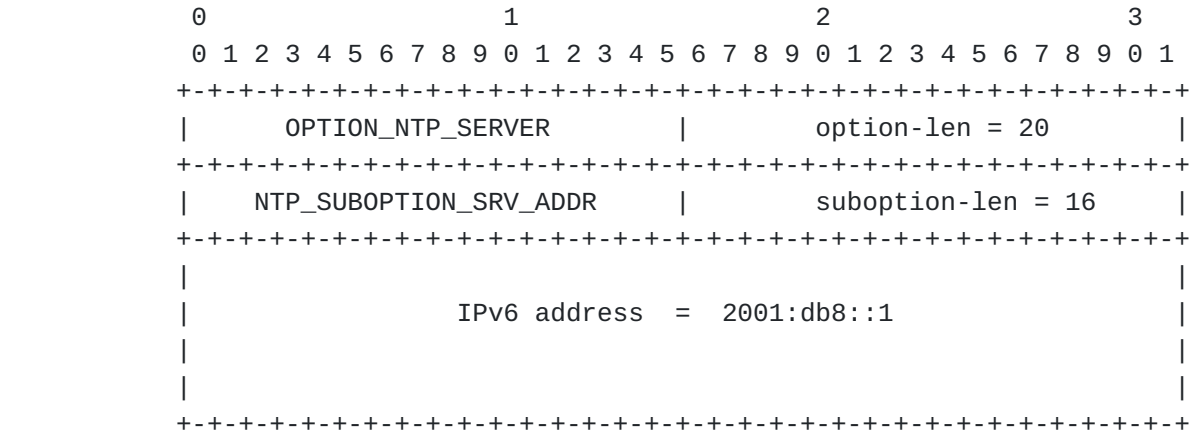
FQDN: Fully Qualified Domain Name of the NTP server. This field MUST be encoded as described in [RFC3315], section 8.

---

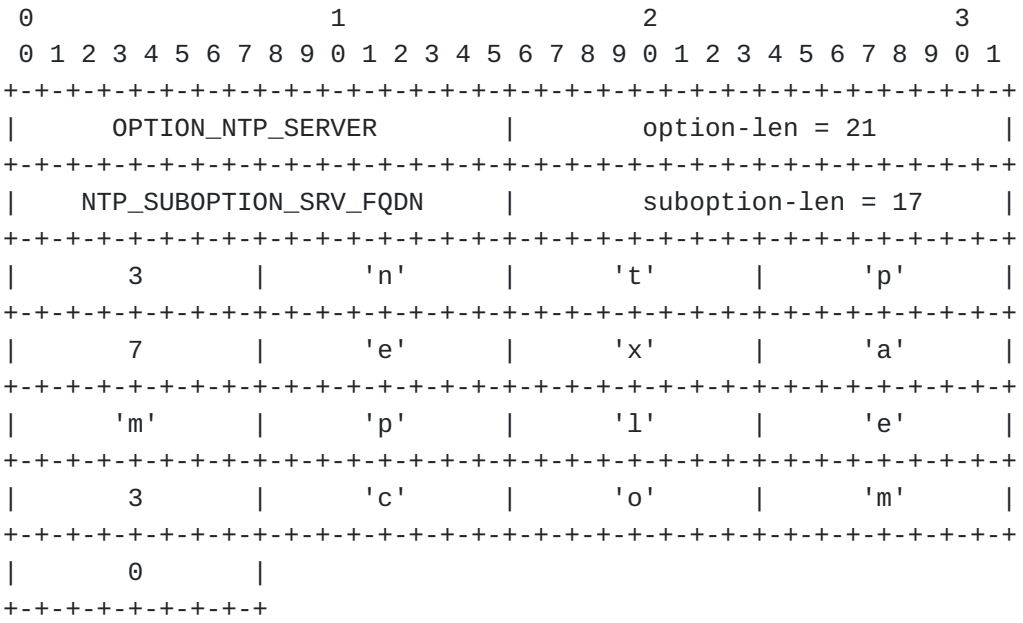
4. Examples of use

TOC

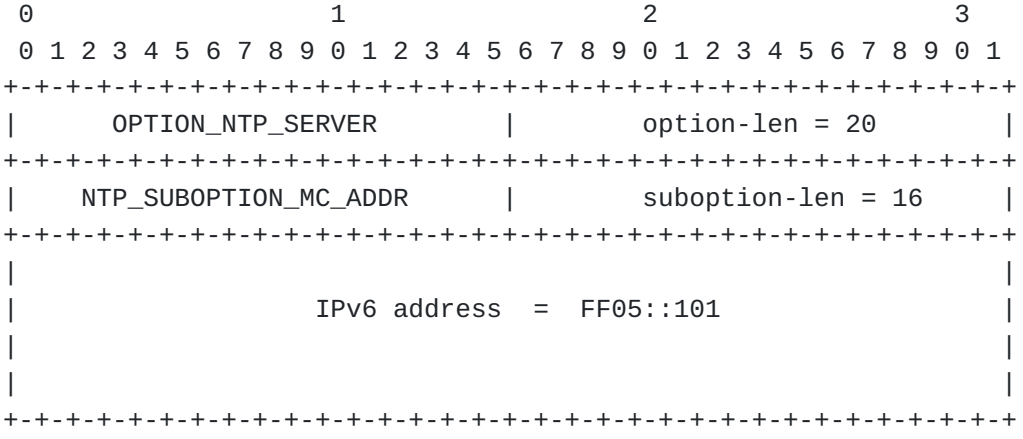
To instruct a client to use an NTP server located at address 2001:db8::1, a DHCP server shall use the following format:



To to enable a client to use the 'ntp.example.com' server, a DHCP server shall use the following format:



To instruct a client to join the FF05::101 NTP multicast group, a DHCP server shall use the following format:



---

5. Appearance of this Option

TOC

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 prefered 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] (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” July 2003.) 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

TOC

This option could be used by an intruder to advertise the address of a malicious NTP 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] (Arkko, J., Kempf, J., Zill, B., and P. Nikander, “SEcure Neighbor Discovery (SEND),” March 2005.), simply by affecting the clock on these nodes.
To prevent these attacks, it is strongly advisable to secure the use of this option either by:

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

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

---

7. IANA Considerations

TOC

When this document is published, the IANA is requested to assign an option code from the "DHCPv6 Options Codes" registry for OPTION_NTP_SERVER.

---

8. References

TOC

8.1. Normative References

TOC

[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 (TXT).
[draft-ntpv4]	Burbank, J., Kasch, W., Martin, J., and D. Mills, "Network Time Protocol Version 4 Protocol And Algorithms Specification," draft-ietf-ntp-ntpv4-proto-11 (work in progress), September 2008.
[draft-autokey]	Haberman, B. and D. Mills, "Network Time Protocol Version 4 Autokey Specification," draft-ietf-ntp-autokey-04 (work in progress), August 2008.

8.2. Informative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3971]	Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," RFC 3971, March 2005 (TXT).
[RFC4075]	Kalusivalingam, V., "Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6," RFC 4075, May 2005 (TXT).
[RFC4330]	Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI," RFC 4330, January 2006 (TXT).

Authors' Addresses

TOC

	Richard Gayraud
	None
Email:	richard.gayraud@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