

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: June 22, 2012

M. Bhatia  
Alcatel-Lucent  
X. Chen  
D. Zhang  
Huawei  
December 20, 2011

## **IPv6 Router Advertisement Option for NTP Server Configuration draft-bcd-6man-ntp-server-ra-opt-00**

### Abstract

This document specifies a new IPv6 Router Advertisement option to allow IPv6 routers to advertise Network Time Protocol version 4 or greater server location information to IPv6 hosts.

### 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](#)].

### 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 June 22, 2012.

### Copyright Notice

Copyright (c) 2011 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

<a href="#">1.</a>	<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Overview</a>	<a href="#">4</a>
<a href="#">3.</a>	<a href="#">Neighbor Discovery Extension</a>	<a href="#">4</a>
<a href="#">3.1.</a>	<a href="#">NTP Server Unicast Address Suboption</a>	<a href="#">5</a>
<a href="#">3.2.</a>	<a href="#">NTP Server Multicast Address Suboption</a>	<a href="#">6</a>
<a href="#">3.3.</a>	<a href="#">NTP Server FQDN Suboption</a>	<a href="#">7</a>
<a href="#">4.</a>	<a href="#">Security Considerations</a>	<a href="#">7</a>
<a href="#">5.</a>	<a href="#">IANA Considerations</a>	<a href="#">8</a>
<a href="#">6.</a>	<a href="#">Acknowledgements</a>	<a href="#">8</a>
<a href="#">7.</a>	<a href="#">References</a>	<a href="#">8</a>
<a href="#">7.1.</a>	<a href="#">Normative References</a>	<a href="#">8</a>
<a href="#">7.2.</a>	<a href="#">Informative References</a>	<a href="#">8</a>
	<a href="#">Authors' Addresses</a>	<a href="#">9</a>

## 1. Introduction

NTP [[RFC5905](#)] servers form a core component of the Internet infrastructure. They are used to provide time and synchronization services for hosts and routers in a network, which is critical for many applications (event logging, security mechanisms and other services). In order to synchronize the time, all routers and hosts need to be configured to point to a NTP server that will provide clocking to all the devices. This ensures accurate and synchronized time among all devices. It is usually recommended to choose among several NTP servers in case one of the servers becomes unreachable or its clock becomes unreliable.

Neighbor Discovery (ND) for IP Version 6 and IPv6 Stateless Address Autoconfiguration provide ways to configure either fixed or mobile nodes with one or more IPv6 addresses, default routers and some other parameters like the link-layer address of the interface from which the Router Advertisement is sent, link MTU [[RFC4861](#)], IP address of the DNS servers [[RFC5006](#)], etc.

This document proposes a new mechanism which uses a new IPv6 Router Advertisement (RA) option to allow IPv6 routers to advertise NTP server addresses to IPv6 hosts.

RA-based NTP configuration is a useful, optional alternative in networks where an IPv6 host's address is autoconfigured through IPv6 stateless address autoconfiguration, and where the delays in acquiring server addresses and communicating with the servers are critical. RA-based NTP configuration allows the host to acquire the nearest server addresses on every link. Furthermore, it learns these addresses from the same RA message that provides configuration information for the link, thereby avoiding an additional protocol run. This can be beneficial in some mobile environments, such as with Mobile IPv6.

The NTP Server Option that this document proposes is an extension of Router Advertisement. It does not change the basic function of the existing ND/SLAAC mechanisms.

Information that an IPv6 host or a router needs to run the basic Internet applications (such as the Clock Synchronization, Timestamp Verification, Certificate Expiration check, etc.) can be obtained with the addition of this option to Neighbor Discovery and address autoconfiguration.

This mechanism works over a broad range of scenarios and leverages IPv6 Neighbor Discovery. This works well on links that are high performance (e.g., Ethernet LANs) and low performance (e.g., cellular



networks). In the latter case, by combining the NTP server information (that this draft proposes) with the other information in the Router Advertisement, the IPv6 devices can learn all the information needed to use most Internet applications in a single transaction. This not only saves bandwidth, but also minimizes the delay needed to learn the NTP server information.

## **2. Overview**

This document defines a new ND option called NTP Server option that contains the addresses of the NTP servers. Existing ND transport mechanisms (i.e., Advertisements and Solicitations) are used. This works in the same way that hosts learn about routers and prefixes. An IPv6 host can configure the IPv6 addresses of one or more NTP servers via RA messages periodically sent by a router or solicited by Router Solicitation (RS) messages.

This approach requires NTP Server information to be configured in the routers sending the advertisements. The configuration of NTP server addresses in the routers can be done by manual configuration. The automatic configuration of NTP server addresses in routers is out of scope for this document.

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).

## **3. Neighbor Discovery Extension**

The IPv6 NTP configuration mechanism in this document defines a new ND option in Neighbor Discovery - the NTP Server (NTPS) option. 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 RA 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. 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 (NTPS) Option is:

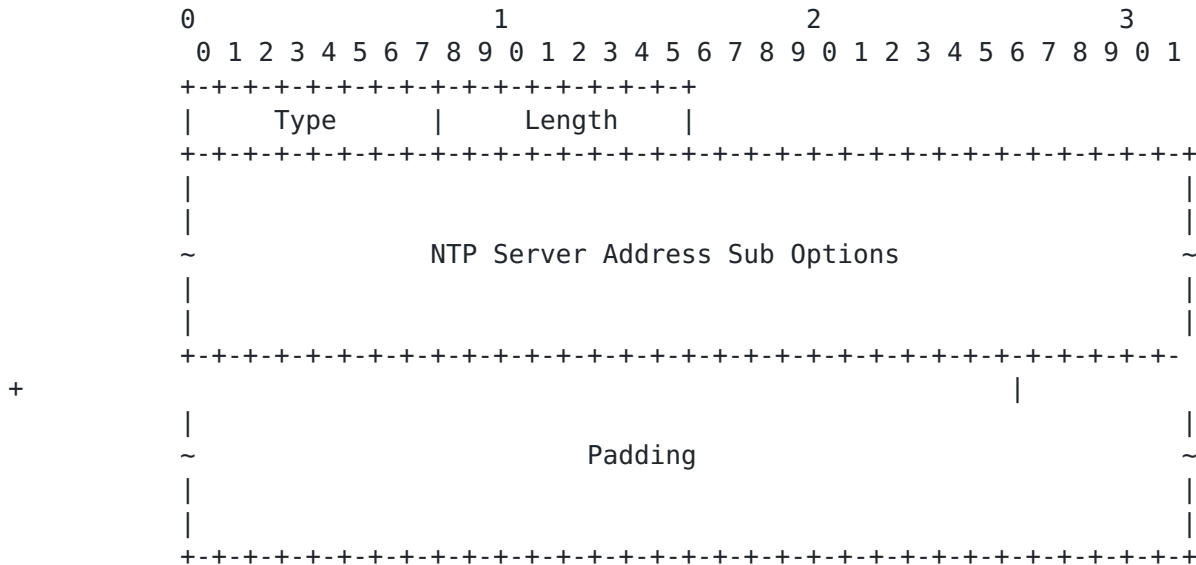


Figure 1: NTP Server Option in the RA

Fields:

Type: 8 bit identifier of the NTP Server option type in the RA message - To be assigned by IANA.

Length: 8 bit unsigned integer. Total length of the included sub options (including the Type and Length fields) is in units of 8 octets.

NTP Server Address Sub Options : List of NTP server addresses sub options

Padding: It is optional and is used, if required, to preserve IPv6 8-octet alignment.

### 3.1. NTP Server Unicast Address Suboption

This suboption is intended to appear inside the NTP Server Option within the RA message. It specifies the IPv6 unicast address of an NTP server or SNTP server available to the client.





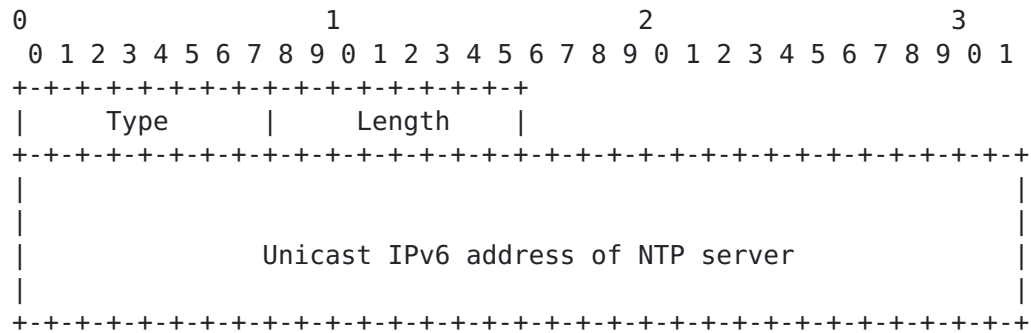


Figure 2: NTP Server Unicast Address Suboption

Fields:

Type: 8 bit identifier of the NTP Server Unicast Address Suboption - To be assigned by IANA.

Length: 8 bit unsigned integer. Total length of the sub options (including the Type and Length fields) in octets. Its set to 18

Unicast IPv6 address of NTP server: An IPv6 Address

### 3.2. NTP Server Multicast Address Suboption

This suboption is intended to appear inside the NTP Server Option within the RA message. It specifies the IPv6 Multicast Group address of an NTP server or SNTP server available to the client.

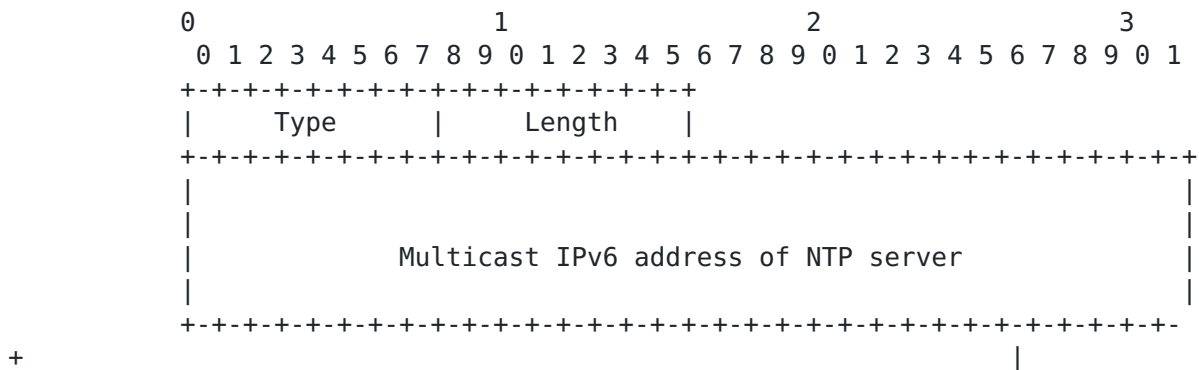


Figure 2: NTP Server Multicast Address Suboption

Fields:

Type: 8 bit identifier of the NTP Server Multicast Address Suboption - To be assigned by IANA.



Length: 8 bit unsigned integer. Total length of the sub options (including the Type and Length fields) in octets. Its set to 18

Multicast IPv6 address of NTP server: An IPv6 Address

### 3.3. NTP Server FQDN Suboption

This suboption is intended to appear inside the NTP Server Option within the RA message. It specifies the FQDN of an NTP server or SNTP server available to the client.

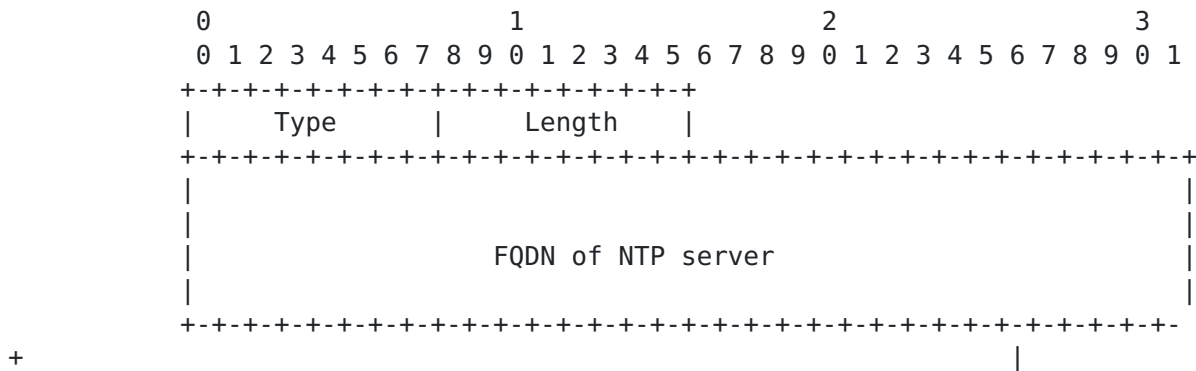


Figure 2: NTP Server FQDN Suboption

Fields:

Type: 8 bit identifier of the NTP Server FQDN Suboption - To be assigned by IANA.

Length: 8 bit unsigned integer. Total length of the FQDN field and including the Type and Length fields in octets.

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

## 4. Security Considerations

Because NTPS option does not change the base functions of existing ND/SLAAC mechanism, it can be claimed that the NTP Server option for RA has vulnerabilities similar to those existing in current mechanisms. If the Secure Neighbor Discovery (SEND) protocol is used as a security mechanism for ND, all the ND options including the NTP Server option are automatically included in the signatures [\[RFC3971\]](#), and the NTPS transport is integrity-protected.



## **5. IANA Considerations**

IANA needs to assign an option code for the NTP Server Option that will be used in the Router Advertisements.

IANA is required to maintain a new number space of NTP Server suboptions as defined in this document. IANA should assign future NTP time source suboptions with an "IETF Consensus" policy as described in [[RFC5226](#)].

## **6. Acknowledgements**

This document is built upon [draft-chen-ntp-ra-opt-00](#) which expired eons ago.

## **7. References**

### **7.1. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [RFC5905] Mills, D., Martin, J., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", [RFC 5905](#), June 2010.

### **7.2. Informative References**

- [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.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [RFC4330] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", [RFC 4330](#), January 2006.
- [RFC5006] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Option for DNS Configuration", [RFC 5006](#), September 2007.

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

#### Authors' Addresses

Manav Bhatia  
Alcatel-Lucent

Email: [manav.bhatia@alcatel-lucent.com](mailto:manav.bhatia@alcatel-lucent.com)

Xu Chen  
Huawei

Email: [zhangdacheng@huawei.com](mailto:zhangdacheng@huawei.com)

Dacheng Zhang  
Huawei

Email: [zhangdacheng@huawei.com](mailto:zhangdacheng@huawei.com)