

Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document describes a new DHCPv6 option for passing a list of Simple Network Time Protocol (SNTP) server addresses to a client.

1. Introduction

This document describes a new option, called the SNTP [3] servers option, for passing information about SNTP servers in DHCPv6 [1].

2. Requirements

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in RFC 2119 [2].

3. Terminology

This document uses terminology specific to IPv6 and DHCPv6 as defined in the "Terminology" section of the DHCPv6 specification [1].

4. Simple Network Time Protocol (SNTP) Servers Option

The Simple Network Time Protocol servers option provides a list of one or more IPv6 addresses of SNTP [3] servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers. Clients MUST treat the list of SNTP servers as an ordered list. The server MAY list the SNTP servers in decreasing order of preference.

6. Security Considerations

The SNTP servers option may be used by an intruder DHCPv6 server to cause DHCPv6 clients to contact a rogue SNTP server, resulting in invalid synchronization of time in the client, finally leading to time-critical applications running inaccurately in the client machine. Time accuracy can be crucial to some security algorithms. For example, expired certificates may gain a new life, making the applications running on the client machine less secure. The inaccuracy can even cause clients to set their time incorrectly, making them vulnerable to replay attacks in protocols that use time stamps to detect replays.

To avoid attacks through these options, the DHCPv6 client SHOULD use authenticated DHCPv6 (see the "Authentication of DHCP messages" section in the DHCPv6 specification [1]).

7. IANA Considerations

The IANA has assigned an option code to the following from the option-code space defined in the "DHCPv6 Options" section of the DHCPv6 specification [1].

Option Name	Value	Described in
OPTION_SNTP_SERVERS	31	Section 4.

8. Acknowledgements

Thanks to the DHC Working Group for their time and input on the specification. In particular, thanks to (in alphabetical order) Bernie Volz, Jim Bound, Margaret Wasserman, Pekka Savola, Ralph Droms, Robert Elz, and Thomas Narten for their thorough review.

9. Normative References

- [1] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
- [2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

10. Informative References

- [3] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 2030, October 1996.
- [4] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

Author's Address

Vijayabhaskar A. Kalusivalingam
Cisco Systems (India) Private Limited,
No: 9, Brunton Road,
Bangalore - 560025
India

Phone: +91-80-51036615
EMail: vibhaska@cisco.com

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

