

Network Information Service (NIS)
Configuration Options for
Dynamic Host Configuration Protocol for IPv6 (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 (2004).

Abstract

This document describes four options for Network Information Service (NIS) related configuration information in Dynamic Host Configuration Protocol for IPv6 (DHCPv6): NIS Servers, NIS+ Servers, NIS Client Domain Name, NIS+ Client Domain name.

1. Introduction

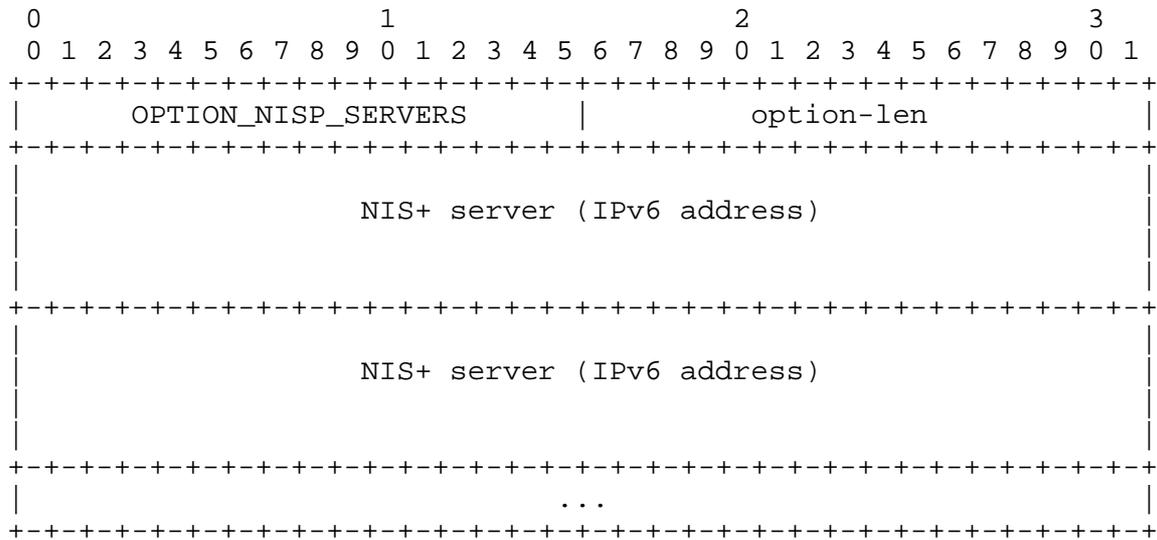
This document describes four options for passing configuration information related to Network Information Service (NIS) [3] in DHCPv6 (RFC 3315 [1]).

The options defined in this document can only be used to configure information about NIS servers that can be reached using IPv6. The DHCP option to configure information about IPv4 NIS servers can be found in RFC 2132 [4]. Mechanisms for configuring IPv4/IPv6 dual-stack applications are being considered, but are not specified in this document.

2. 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 BCP 14, RFC 2119 [2].

The format of the Network Information Service V2 (NIS+) Servers option is as shown below:



option-code: OPTION_NISP_SERVERS (28)

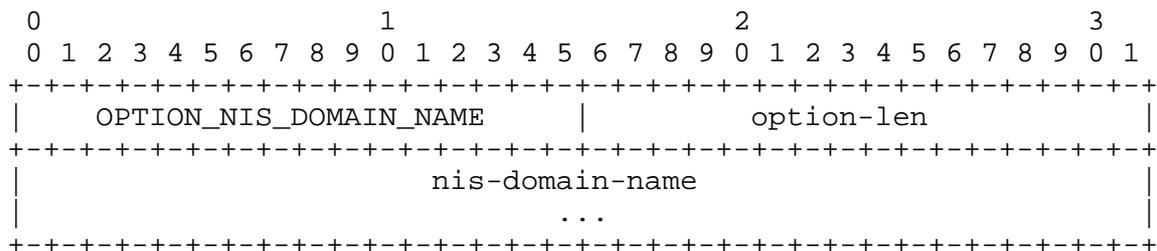
option-len: Length of the 'NIS+ server' fields in octets; It must be a multiple of 16

NIS+ server: IPv6 address of NIS+ server

5. Network Information Service (NIS) Domain Name Option

The Network Information Service (NIS) Domain Name option is used by the server to convey client's NIS Domain Name info to the client.

The format of the NIS Domain Name option is as shown below:



option-code: OPTION_NIS_DOMAIN_NAME (29)

option-len: Length of the 'nis-domain-name' field in octets

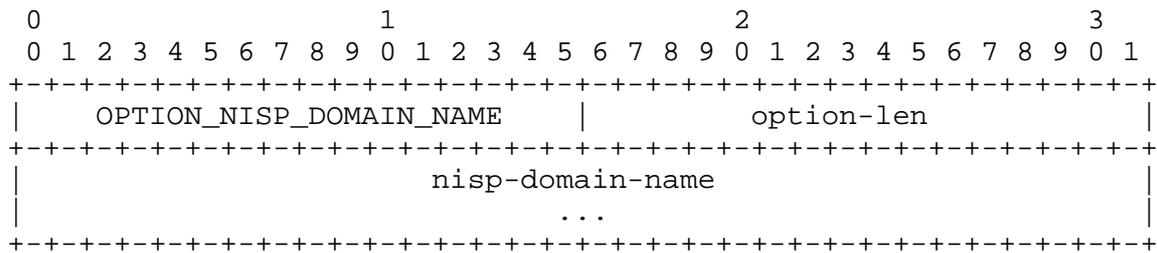
nis-domain-name: NIS Domain name for client

The 'nis-domain-name' MUST be encoded as specified in section "Representation and Use of domain names" of the DHCPv6 specification [1].

6. Network Information Service V2 (NIS+) Domain Name Option

The Network Information Service V2 (NIS+) Domain Name option is used by the server to convey client's NIS+ Domain Name info to the client.

The format of the NIS+ Domain Name option is as shown below:



option-code: OPTION_NISP_DOMAIN_NAME (30)

option-len: Length of the 'nisp-domain-name' field in octets

nisp-domain-name: NIS+ Domain name for client

The 'nisp-domain-name' MUST be encoded as specified in section "Representation and Use of domain names" of the DHCPv6 specification [1].

7. Appearance of these Options

The NIS servers, NIS+ servers, NIS domain name and NIS+ domain name options MUST NOT appear in other than the following messages: Solicit, Advertise, Request, Renew, Rebind, Information-Request and Reply.

The option number for these options MAY appear in the Option Request Option [1] in the following messages: Solicit, Request, Renew, Rebind, Information-Request and Reconfigure.

8. Security Considerations

The NIS servers, NIS+ servers, NIS domain name and NIS+ domain name options may be used by an intruder DHCPv6 server to assign invalid NIS parameters, resulting in clients unable to use NIS service.

The NIS servers and NIS+ servers options may be used by an intruder DHCPv6 server to cause the DHCPv6 clients to send their queries to an intruder NIS/NIS+ server. This misdirected searches may be used to spoof NIS/NIS+ names.

The NIS domain name and NIS+ domain name options may be used by an intruder DHCPv6 server to cause the DHCPv6 clients to search through invalid domains for incompletely specified domain names. The results of these misdirected searches may be used to spoof NIS/NIS+ names.

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

9. IANA Considerations

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

Option Name	Value	Described in
OPTION_NIS_SERVERS	27	Section 3
OPTION_NISP_SERVERS	28	Section 4
OPTION_NIS_DOMAIN_NAME	29	Section 5
OPTION_NISP_DOMAIN_NAME	30	Section 6

10. References

10.1. Normative References

- [1] Droms, R., Ed., 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.

10.2. Informative References

- [3] Sun Microsystems, "System and Network Administration", March 1990.
- [4] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

Acknowledgements

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

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 (2004).

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 IETF's procedures with respect to rights in IETF 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.

