

DHCP Options for Novell Directory Services

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 (1997). All Rights Reserved.

Abstract

This document defines three new DHCP options for delivering configuration information to clients of the Novell Directory Services. The first option carries a list of NDS servers. The second option carries the name of the client's NDS tree. The third carries the initial NDS context. These three options provide an NDS client with enough information to connect to an NDS tree without manual configuration of the client.

1. Introduction

Novell Directory Services is a distributed, replicated, hierarchical database of objects representing network resources such as nodes, services, users, and applications. An NDS client must be able to locate an NDS server in order to authenticate itself to the network and gain access to the database. In addition, the node's user is better served if the NDS client's attention is focused on the area of the NDS database likely to be of the most interest to the user. This specification describes DHCP options [1] that carry NDS information to TCP/IP clients of NDS. The first option, the NDS Servers Option, carries a list of NDS servers. The other two options, the NDS Tree Name Option and the NDS Context Option, provide the client with a default context within the NDS database.

The NDS Tree Name Option and the NDS Context Option carry 16-bit Unicode text encoded into an octet stream using UTF-8 [4]. A complete DHCP implementation can represent of the entire Unicode character set supported by NDS. At the same time, 7-bit ASCII text is unchanged by the UTF-8 transformation. In environments where the NDS tree name and context are restricted to the range of 7-bit ASCII characters, ASCII-only DHCP clients and servers can support these options by using the ASCII text as the UTF-8 encoded data.

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. [2]

2. NDS Servers Option

This option specifies one or more NDS servers for the client to contact for access to the NDS database. Servers SHOULD be listed in order of preference.

The code for this option is 85. The minimum length of this option is 4 octets, and the length MUST be a multiple of 4.

Code	Len	Address 1				Address 2				
85	n	a1	a2	a3	a4	a1	a2	a3	a4	...

3. NDS Tree Name Option

This option specifies the name of the NDS tree the client will be contacting. NDS tree names are 16-bit Unicode strings. For transmission in the NDS Tree Name Option, an NDS tree name is transformed into octets using UTF-8. The string should NOT be zero terminated.

The code for this option is 86. The maximum possible length for this option is 255 bytes.

Code	Len	NDS Tree Name				
86	n	c1	c2	c3	c4	...

4. NDS Context Option

This option specifies the initial NDS context the client should use. NDS contexts are 16-bit Unicode strings. For transmission in the NDS Context Option, an NDS context is transformed into octets using UTF-8. The string should NOT be zero terminated.

A single DHCP option can only contain 255 octets. Since an NDS context name can be longer than that, this option can appear more than once in the DHCP packet. The contents of all NDS Context options in the packet should be concatenated as suggested in the DHCP specification [3, page 24] to get the complete NDS context. A single encoded character could be split between two NDS Context Options.

The code for this option is 87. The maximum length for each instance of this option is 255, but, as just described, the option may appear more than once if the desired NDS context takes up more than 255 octets. Implementations are discouraged from enforcing any specific maximum to the final concatenated NDS context.

Code	Len	Initial	NDS	Context
+-----+	+-----+	+-----+	+-----+	+-----+
87	n	c1	c2	c3 c4 ...
+-----+	+-----+	+-----+	+-----+	+-----+

5. References

- [1] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC-2132, March 1997.
- [2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC-2119, March 1997.
- [3] Droms, R., "Dynamic Host Configuration Protocol", RFC-2131, March 1997.
- [4] Yergeau, F., "UTF-8, a transformation format of Unicode and ISO 10646", RFC-2044, October 1996

6. Security Considerations

DHCP currently provides no authentication or security mechanisms. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification [3]. In particular, these DHCP options allow an unauthorized DHCP server to misdirect an NDS client to a nonexistent NDS server or even a spoof NDS server. These threats are similar to what NDS faces during normal operations in its native IPX environment.

7. Author's Address

**Don Provan
Novell, Inc.
2180 Fortune Drive
San Jose, California, 95131**

Phone: +1 408 577 8440

EMail: donp@Novell.Com

8. Full Copyright Statement

Copyright (C) The Internet Society (1997). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.