

Network Working Group
Internet-Draft
Expires: April 24, 2006

R. Johnson
J. Jumarasamy
K. Kinnear
M. Stapp
Cisco Systems, Inc.
October 21, 2005

DHCP Server Identifier Override Suboption
draft-ietf-dhc-server-override-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 24, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This memo defines a new suboption of the DHCP relay information option which allows the DHCP relay to specify a new value for the Server Identifier option, which is inserted by the DHCP Server. This allows the DHCP relay to act as the actual DHCP server such that RENEW DHCPREQUESTs will come to the relay instead of going to the server directly. This gives the relay the opportunity to include the

Internet-Draft

Server ID Override Suboption

October 2005

Relay Agent option with appropriate suboptions even on DHCP RENEW messages.

Table of Contents

1.	Introduction	3
2.	Conventions	4
3.	Server Identifier Override Suboption Definition	5
4.	Security Considerations	6
5.	IANA Considerations	7
6.	Intellectual Property Rights and Copyright	8
7.	References	8
	Authors' Addresses	9
	Intellectual Property and Copyright Statements	10

1. Introduction

There are many situations where the DHCP relay is involved and can insert a relay agent option with appropriate suboptions easily into DHCP DISCOVER messages. Once the lease has been granted, however, future DHCP RENEWAL messages are sent directly to the DHCP Server as specified in the Server Identifier option. This means that the relay may not see the DHCP RENEWAL messages (depending upon network topology) and thus can not provide the same relay agent option information in the RENEWAL messages.

This new DHCP relay agent suboption, Server Identifier override, allows the relay to tell the DHCP server what value to place into the Server Identifier option. Using this, the relay agent can force RENEWAL messages to come to it instead of the server. The relay may then insert the relay agent option with appropriate suboptions and relay the DHCPREQUEST to the actual server. In this fashion the DHCP server will be provided with the same relay agent information upon renewals (such as Circuit-ID, Remote-ID, Device Class, etc.) as was provided in the initial DISCOVER message. In effect, this makes a RENEWAL into a REBINDING.

This new suboption could also be used by the DHCP relay in order to allow the relay to appear as the actual DHCP server to the client. This has the advantage that the relay can more easily keep up-to-date information about leases granted, etc.

In short, this new suboption allows the DHCPv4 relay to function in the same fashion as the DHCPv6 relay currently does.

2. Conventions

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](#) [1].

[3.](#) Server Identifier Override Suboption Definition

The format of the suboption is:

Code	Len	Overriding Server Identifier address			
+-----+	+-----+	+-----+	+-----+	+-----+	+-----+
TBD	n	a1	a2	a3	a4
+-----+	+-----+	+-----+	+-----+	+-----+	+-----+

Figure 1

The option length (n) is 4. The octets "a1" through "a4" specify the value which MUST be inserted into the Server Identifier option by the DHCP Server upon reply.

DHCP Servers which implement this Relay Suboption MUST use this value, if present, as the value to insert into the Server Identifier option whenever responding to a DHCP Client.

If a DHCP Server does not understand/implement this Relay Suboption, it will ignore the Suboption, and thus will insert it's own

appropriate interface address as the Server Identifier address. In this case, the DHCP Relay will not receive RENEW DHCPREQUEST packets from the client. When configuring a DHCP Relay to use this Suboption, the administrator of the Relay should take into account whether or not the DHCP Server to which the packet will be relayed will correctly understand this Suboption.

When servicing a DHCPREQUEST packet the DHCP Server would normally look at the Server Identifier option for verification that the address specified there is one of the addresses associated with the DHCP Server, silently ignoring the DHCPREQUEST if it does not match a configured DHCP Server interface address. If the DHCPREQUEST packet contains a Server Identifier Override Suboption, however, comparison should be made between this suboption and the Server Identifier option. If both of the Server Identifier Override Suboption and the Server Identifier Option specify the same address, then the Server should accept the DHCPREQUEST packet for processing, regardless of whether or not the Server Identifier Option matches a DHCP Server interface.

The DHCP Relay should fill in the giaddr field when relaying the packet just as it normally would do.

[4.](#) Security Considerations

Message authentication in DHCP for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in [\[3\]](#). Potential exposures to attack are discussed in [section 7](#) of the DHCP protocol specification in [\[2\]](#).

The DHCP Relay Agent option depends on a trusted relationship between the DHCP relay agent and the server, as described in section 5 of [RFC 3046](#). While the introduction of fraudulent relay-agent options can be prevented by a perimeter defense that blocks these options unless the relay agent is trusted, a deeper defense using the authentication option for relay agent options [\[4\]](#) SHOULD be deployed as well.

If a rogue DHCP relay were inserted between the client and the

server, it could redirect clients to it using this suboption. This would allow such a system to later deny RENEW DHCPREQUEST and thus force clients to discontinue use of their allocated address. This interception, however, would need to be done during the initial DISCOVER and OFFER phase, since the suboption value SHOULD be ignored by the server during RENEWAL state. Either DHCP Authentication [3] or DHCP Relay Agent option authentication [4] would address this case.

5. IANA Considerations

IANA is requested to assign a suboption number for the Server Identifier Override Suboption from the DHCP Relay Agent Information Option [3] suboption number space. None.

The IETF has been notified of intellectual property rights claimed in regard to some or all of the specification contained in this document. For more information consult the online list of claimed rights.

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.

7. References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), [BCP 14](#), March 1997.
- [2] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [3] Droms, R., "Authentication for DHCP Messages", [RFC 3118](#), June 2001.
- [4] Stapp, M., "The Authentication Suboption for the DHCP Relay Agent Option", [RFC 4030](#), March 2005.
- [5] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [RFC 2434](#), October 1998.
- [6] Patrick, M., "DHCP Relay Agent Information Option", [RFC 3046](#), November 2004.

Authors' Addresses

Richard A. Johnson
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
US

Phone: +1 408 526 4000
Email: raj@cisco.com

Jay Kumarasamy
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
US

Phone: +1 408 526 4000
Email: jayk@cisco.com

Kim Kinnear
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
US

Phone: +1 408 526 4000
Email: kkinnear@cisco.com

Mark Stapp
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
US

Phone: +1 408 526 4000
Email: mjs@cisco.com

Internet-Draft

Server ID Override Suboption

October 2005

Intellectual Property Statement

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.

Disclaimer of Validity

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.

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.

Acknowledgment

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

Johnson, et al.

Expires April 24, 2006

[Page 10]