Internet Engineering Task Force
Internet Draft
Expiration: March 2005
File: draft-ietf-dhc-server-override-01.txt

Richard Johnson
Kim Kinnear
Mark Stapp
Jay Kumarasamy
Cisco Systems, Inc.

DHCP Server-ID Override Suboption
<draft-ietf-dhc-server-override-01.txt>

September 27, 2004

Status of this Memo

Copyright Notice

Abstract

This memo defines a new suboption of the DHCP relay information option [6] which allows the DHCP relay to specify a new value for the

Server-ID option, which is inserted by the DHCP Server. In some cases it is convenient for the DHCP relay to act as the actual DHCP server such that DHCP RENEWAL requests will come to the relay instead of going to the server directly. This gives the relay the opportunity to include the Relay Agent option with appropriate suboptions even on RENEWAL messages.

This new relay agent suboption allows the relay to tell the DHCP server what value to use in the Server-ID option [3]. If this suboption is not present, the server should build the Server-ID option in the normal fashion.

1.0 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-ID 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-ID override, allows the relay to tell the DHCP server what value to place into the Server-ID 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 request 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.

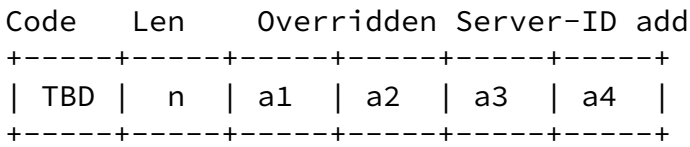
In short, this new suboption allows the DHCPv4 relay to function in the same fashion as the DHCPv6 relay currently does.

1.1 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].

2.0 Server-ID Override Suboption Definition

The format of the suboption is:



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

DHCP Servers SHOULD use this value, if present, as the value to insert into the Server-ID option whenever responding to a DHCP Client.

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

3.0 IANA Considerations

None.

4.0 Acknowledgements

This document is the result of work done within Cisco Systems. Thanks to Jay Kumarasamy, Kim Kinnear, and Mark Stapp for their work on this suboption definition and the other related work for which this is necessary.

5.0 Security Considerations

Message authentication in DHCP for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in RFC 3118 [5]. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification in RFC 2131 [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 requests 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 [5] or DHCP Relay Agent option authentication [4] would address this case.

6.0 Intellectual Property Rights and Copyright

"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.

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] Alexander, S. and Droms, R., "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[4] Stapp, M. "The Authentication Suboption for the DHCP

Relay Agent Option", draft-ietf-dhc-auth-suboption-00.txt, June 23, 2002

[5] Droms, R. "Authentication for DHCP Messages", RFC 3118, June 2001

[6] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001

Author Information:

Richard Johnson
Jay Kumarasamy
Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134

Phone: (408) 526-4000

EMail: jayk@cisco.com

raj@cisco.com

Kim Kinnear
Mark Stapp
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824

Phone: (978) 244-8000

EMail: kkinnear@cisco.com
mjs@cisco.com