DHCP Server Identifier Override Suboption
draft-ietf-dhc-server-override-05.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/1id-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 May 20, 2008.

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

Table of Contents

1. Introduction   [TOC](#)

There are many situations where the DHCP relay is involved and can insert a relay agent option [RFC3046] (Patrick, M., "DHCP Relay Agent Information Option," January 2001.) 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 [RFC2132] (Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions," March 1997.). 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 [RFC3315] (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," July 2003.) currently does.

[TOC](#)

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 [RFC2119] (Bradner, S.,
"Key words for use in RFCs to Indicate Requirement Levels,"
March 1997.).

---

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 matchs a DHCP Server interface.
The DHCP Relay should fill in the giaddr field when relaying the packet just as it normally would do.
In a situation where the DHCP Relay is configured to forward packets to more than one server, the DHCP Relay should forward all DHCP packets to all servers. This applies to DHCP RENEW packets as well. The intent is that the DHCP Relay should not need to maintain state information about the DHCP lease.
DHCP Relays using this suboption SHOULD also implement and use the DHCPv4 Relay Agent Flags Suboption [RFC5010] (Kinnear, K., Normoyle, M., and M. Stapp, "The Dynamic Host Configuration Protocol Version 4 (DHCPv4) Relay Agent Flags Suboption," September 2007.) in order to specify whether the DHCP Relay received the original packet as a broadcast or unicast. The DHCP Server receiving a packet containing the Server Identifier Override Suboption may use this additional information in processing the packet.
Note that if the DHCP Relay becomes inaccessible by the DHCP Client or loses network access to the DHCP Server, further DHCP RENEW packets from the DHCP Client may not be properly processed and the DHCP Client's lease may time out.

---

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 [RFC3118] (Droms, R. and W. Arbaugh, "Authentication for DHCP Messages," June 2001.). Potential exposures to attack are discussed in section 7 of the DHCP protocol specification in [RFC2131] (Droms, R., "Dynamic Host Configuration Protocol," March 1997.).
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 [RFC4030] (Stapp, M. and T. Lemon, "The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option," March 2005.) 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. It could also allow the rogue relay to change, insert, or delete DHCP options in DHCPACK messages and extend leases beyond what the server has allowed. 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. DHCP Authentication [RFC3118] (Droms, R. and W. Arbaugh, "Authentication for DHCP Messages," June 2001.) and/or DHCP Relay Agent option authentication [RFC4030] (Stapp, M. and T. Lemon, "The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option," March 2005.) would address this case. (Note that, as is always the case, lack of DHCP Authentication would allow a rogue DHCP relay to change the Server-ID option in the DHCPOFFER and DHCPACK packets without detection. This threat is not new to the Server-ID-Override suboption.) This draft does not add any new vulnerabilities that were not already present, except in the case where DHCP authentication is already in place and DHCP clients require its use. It is suggested that DHCP Authentication and DHCP Relay Agent Option Authentication SHOULD be deployed when this option is used, or protection should be provided against the insertion of rogue DHCP relays and server.
This relay sub-option is not intended, by itself, to provide any additional security benefits.

---

5. IANA Considerations   TOC

IANA is requested to assign a suboption number for the Server Identifier Override Suboption from the DHCP Relay Agent Information Option [RFC3046] (Patrick, M., "DHCP Relay Agent Information Option," January 2001.) suboption number space.

---

6. Intellectual Property Rights and Copyright   TOC

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.

---

7. References   TOC

7.1. Normative References
                                                              TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).

[RFC2131]	Droms, R., "Dynamic Host Configuration Protocol," RFC 2131, March 1997 (TXT, HTML, XML).
[RFC3046]	Patrick, M., "DHCP Relay Agent Information Option," RFC 3046, January 2001 (TXT).
[RFC5010]	Kinnear, K., Normoyle, M., and M. Stapp, "The Dynamic Host Configuration Protocol Version 4 (DHCPv4) Relay Agent Flags Suboption," RFC 5010, September 2007 (TXT).

7.2. Informative References

[RFC2132]	Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions," RFC 2132, March 1997 (TXT, HTML, XML).
[RFC3118]	Droms, R. and W. Arbaugh, "Authentication for DHCP Messages," RFC 3118, June 2001 (TXT).
[RFC3315]	Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 3315, July 2003 (TXT).
[RFC4030]	Stapp, M. and T. Lemon, "The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option," RFC 4030, March 2005 (TXT).

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

Full Copyright Statement

Intellectual Property