Network Working Group
Request for Comments: 5107
Category: Standards Track

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

February 2008

DHCP Server Identifier Override Suboption

Status of This Memo

Abstract

This memo defines a new suboption of the DHCP relay information option that 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 2
2. Conventions 2
3. Terminology 2
4. Server Identifier Override Suboption Definition 3
5. Security Considerations 4
6. IANA Considerations 5
7. Intellectual Property Rights and Copyright 5
8. References 5
8.1. Normative References 5
8.2. Informative References 5

1. Introduction

There are many situations where a DHCP relay agent is involved, and it can easily insert a Relay Agent Information option [3] with appropriate suboptions into DHCPDISCOVER messages. Once the lease has been granted, however, future DHCPREQUEST messages sent by a client in RENEWING state are sent directly to the DHCP server, as specified in the Server Identifier option. In this case, the relay may not see these DHCPREQUEST messages (depending upon network topology) and thus cannot insert the Relay Agent Information option in the DHCPREQUEST messages.

This DHCP relay agent suboption, Server Identifier Override, allows the relay agent to tell the DHCP server what value to place into the Server Identifier option [5]. Using this, the relay agent can force a host in RENEWING state to send DHCPREQUEST messages to the relay agent instead of directly to the server. The relay agent then has the opportunity to insert the Relay Agent Information 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 DHCPDISCOVER message.

In short, this new suboption allows the DHCPv4 relay to function in the same fashion as the DHCPv6 relay [7] 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 [1].

3. Terminology

This document uses DHCP terminology as defined in section 1.5 of RFC 2131 [2], with the exception of the term "DHCP relay agent" replacing "BOOTP relay agent".

Other terms used in this document:

- RENEW DHCPREQUEST - a DHCPREQUEST message sent by a client in RENEWING state

4. Server Identifier Override Suboption Definition

The format of the suboption is:

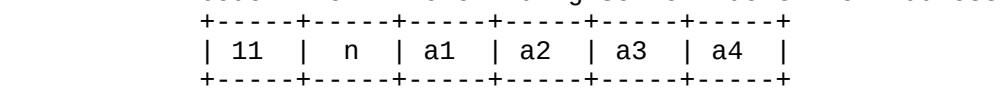

Figure 1

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

DHCP servers that implement this Relay Agent Information suboption MUST use this value, if present in a DHCP message received from a client, as the value to insert into the Server Identifier option in the corresponding response. The DHCP server must also record the address in the suboption for use in subsequent messages to the DHCP client until the next DHCP message is received from the DHCP relay agent.

If a DHCP server does not understand/implement this Relay Information suboption, it will ignore the suboption, and thus it will insert its own appropriate interface address in the Server Identifier option. In this case, the DHCP Relay will not receive RENEW DHCPREQUEST messages from the client. When configuring a DHCP relay agent to use this suboption, the administrator of the relay agent should take into account whether or not the DHCP server to which the message will be relayed will correctly understand this suboption.

When servicing a DHCPREQUEST message, 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 message contains a Server Identifier Override suboption, however, comparison should be made between the address in this suboption and the Server Identifier option. If both the Server Identifier Override suboption and the Server Identifier option specify the same address, then the server should accept the DHCPREQUEST message for processing, regardless of whether or not the Server Identifier option matches a DHCP server interface.

The DHCP relay agent should fill in the giaddr field when relaying the message, just as it normally would do.

In a situation where the DHCP relay agent is configured to forward messages to more than one server, the DHCP relay agent SHOULD forward all DHCP messages to all servers. This applies to RENEW DHCPREQUEST messages as well. The intent is that the DHCP relay agent should not need to maintain state information about the DHCP lease.

DHCP relay agents implementing this suboption SHOULD also implement and use the DHCPv4 Relay Agent Flags Suboption [4] in order to specify whether the DHCP relay agent received the original message as a broadcast or unicast. The DHCP server receiving a message containing the Server Identifier Override Suboption may use this additional information in processing the message.

Note that if the DHCP relay agent becomes inaccessible by the DHCP client or loses network access to the DHCP server, further RENEW DHCPREQUEST messages from the DHCP client may not be properly processed and the DHCP client's lease may time out.

5. Security Considerations

Message authentication in DHCP for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in [6]. Potential exposures to attack are discussed in Section 7 of the DHCP protocol specification in [2].

The DHCP Relay Agent Information option depends on a trusted relationship between the DHCP relay agent and the DHCP server, as described in Section 5 of RFC 3046. While the introduction of fraudulent DHCP relay agent information options can be prevented by a perimeter defense that blocks these options unless the DHCP relay agent is trusted, a deeper defense using the authentication suboption for DHCP relay agent information option [8] SHOULD be deployed as well.

If a rogue DHCP relay agent were inserted between the DHCP client and the DHCP server, it could redirect clients to itself using this suboption. This would allow such a system to later deny RENEW DHCPREQUESTs and thus force clients to discontinue use of their allocated addresses. 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. DHCP authentication [6] and/or DHCP Relay Agent Information option authentication [8] would address this case. (Note that, as is always the case, lack of DHCP authentication would allow a rogue DHCP relay agent to change the Server Identifier Override option in the DHCPOFFER and DHCPACK messages without detection. This threat is not new to the Server Identifier Override suboption.)

This document 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 relay agents between the client and server.

This relay suboption is not intended, by itself, to provide any additional security benefits.

6. IANA Considerations

IANA has assigned a suboption number (11) for the Server Identifier Override Suboption from the DHCP Relay Agent Information Option [3] suboption number space.

7. Intellectual Property Rights and Copyright

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.

8. References

8.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

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

[4] Kinnear, K., Normoyle, M., and M. Stapp, "The Dynamic Host Configuration Protocol Version 4 (DHCPv4) Relay Agent Flags Suboption", RFC 5010, September 2007.

8.2. Informative References

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

[6] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[7] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[8] Stapp, M. and T. Lemon, "The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option", RFC 4030, March 2005.

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