DHC
Internet-Draft
Intended status: Standards Track
Expires: October 25, 2007

K. Kinnear
M. Normoyle
M. Stapp
Cisco Systems, Inc.
April 23, 2007

DHCPv4 Relay Agent Flags Suboption
draft-ietf-dhc-relay-agent-flags-03.txt

Status of this Memo

Copyright Notice

Abstract

This memo defines a new suboption of the DHCP relay agent information option that allows the DHCP relay to specify flags for the forwarded packet. One flag is defined to indicate whether the DHCP relay received the packet via a unicast or broadcast packet. This information may be used by the DHCP server to better serve clients based on whether their request was originally broadcast or unicast.

Table of Contents

1. Introduction

Any time a client's DHCP packet is broadcast, a local DHCP relay will process its request and forward it on to the DHCP server. When the DHCP relay performs this function, it can be configured to use the DHCP relay agent information option to forward additional information to the DHCP server, which the server may then use to alter its processing algorithms. Once the lease has been granted, however, future DHCP DHCPREQUEST/RENEWAL messages are unicast directly to the DHCP Server. [RFC2131] [RFC2132] [RFC3046]

In general, DHCP servers may also make subtle (and sometimes not so subtle) changes in their processing algorithms depending on whether or not the DHCP server received the message as a unicast packet from the DHCP client directly, a broadcast packet from the DHCP client on a locally connected network, or a unicast packet from a DHCP Relay Agent which has forwarded on a packet broadcast from a DHCP client connected to a network local to the DHCP Relay Agent.

In some situations, DHCP Clients may unicast their DHCPREQUEST/RENEW packets to the DHCP Relay Agent, which will forward the packet on to the DHCP server. In these cases, the DHCP server cannot tell whether the packet was broadcast or unicast by the DHCP client, and so it may be unable to process the DHCP client packets in the manner that it would if it knew whether the original DHCP packet was broadcast or unicast. For example, a server might be willing to NAK a client in the REBINDING state based on a determination that the client's address does not match its location in the network, but might not be willing to do so if the client is in the RENEWING state.

The purpose of the suboption described in this document is to allow the DHCP relay to specify flags for the forwarded packet. These flags can be used to describe DHCP client attributes that are useful to the DHCP server, but can only be detected by the local DHCP relay. The DHCP server can use the information provided by the DHCP relay to improve its processing algorithms.

One flag is defined to indicate whether the DHCP relay received the packet via a unicast or broadcast packet. This allows the DHCP server to know if a packet forwarded on by a DHCP Relay Agent was broadcast or unicast to the DHCP Relay Agent.

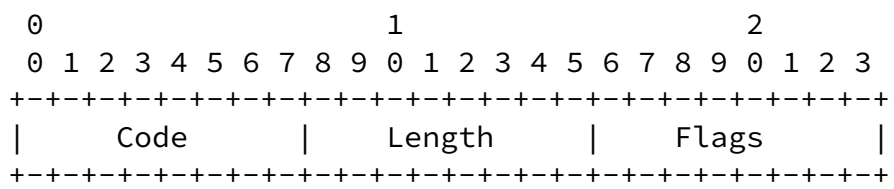
2. Requirements Terminology

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].

3. The Flags Suboption

The Flags suboption provides an extensible suboption definition for several possible flags. The first flag defined is the unicast flag.

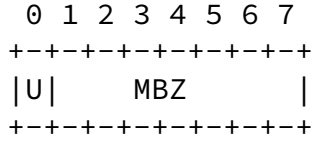
The format of the suboption is:



Code The suboption code. (TBD, to be assigned by IANA).

Length The suboption length, 1 octet.

Flags The Relay Agent flags for this forwarded packet.



U: UNICAST flag

unicast = 1
broadcast = 0

MBZ: MUST BE ZERO (reserved for future use)

4. DHCP Relay Agent Behavior

A DHCP relay agent that claims to conform to this specification MUST include this suboption in every Relay Agent Information Option [RFC3046] it adds to a forwarded DHCP request. In this way, the DHCP server can distinguish a request forwarded from a DHCP relay agent that does not support the relay-agent-flags suboption from a request forwarded by a DHCP relay agent that supports the relay-agent-flags suboption and which received the request that is being forwarded in a broadcast packet.

To put this another way, A DHCP relay agent which supports the relay-agent-flags suboption MUST always include it in every relay-agent-information-option that it inserts into packets which it forwards on to the DHCP server, whether the packet it is forwarding was received as a broadcast or as a unicast. This is because the DHCP server will

be dealing with DHCP relay agents that support the relay-agent-flags suboption as well as DHCP relay agents that do not support the relay-agent-flags suboption.

5. DHCP Server Behavior

This option provides additional information to the DHCP server. The DHCP server MAY use this information to make processing decisions regarding the DHCP Client's packet which it is processing. For instance, knowledge of the broadcast or unicast reception of a packet by a DHCP relay agent could be used when making the processing decisions required to implement Load Balancing [RFC3074]. A load-balancing server may be willing to respond to a REBINDING client, but the server cannot determine the client's state without this additional indication.

The option length is one octet. If the DHCP server receives a relay-agent-flags suboption that is longer than one octet, it MUST evaluate the first octet.

Note to implementors: In specifying the behavior of new flags bits in

the future, careful attention must be paid to compatibility with earlier implementations. If additional flags values are defined in the future, it will not always be possible to distinguish between messages from relay agents who understand the new value and set its value to 'zero', and relay agents who are simply setting a series of unassigned bits to 'zero'. It would be a mistake to specify significant behavior changes based on 'zero' values of flags specified in the future.

6. 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]. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification in [RFC2131].

The DHCP Relay Agent option depends on a trusted relationship between the DHCP relay agent and the server, as described in section 5 of [RFC3046]. 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] SHOULD be deployed as well.

7. IANA Considerations

IANA is requested to assign a suboption number for the Flags Suboption from the DHCP Relay Agent Information Option [RFC3046] suboption number space.

8. Acknowledgements

Thanks to David Hankins for realizing the problems created by the server-id-override option draft and for helping us understand the value of finally solving this problem in a way that has general applicability.

9. References

9.1. Normative References

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

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[RFC4030] Stapp, M. and T. Lemon, "The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option", RFC 4030, March 2005.

9.2. Informative References

[RFC3074] Volz, B., Gonczi, S., Lemon, T., and R. Stevens, "DHC Load Balancing Algorithm", RFC 3074, February 2001.

Authors' Addresses

Kim Kinnear
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
US

Phone: +1 978 936 0000
Email: kkinnear@cisco.com

Marie Normoyle
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
US

Phone: +1 978 936 0000
Email: mnormoyle@cisco.com

Mark Stapp
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
US

Phone: +1 978 936 0000
Email: mjs@cisco.com

Full Copyright Statement

Intellectual Property

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.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).