Internet Engineering Task Force (IETF)
Request for Comments: 6842
Updates: 2131
Category: Standards Track
ISSN: 2070-1721

N. Swamy
Samsung India
G. Halwasia
P. Jhingran
Cisco Systems

January 2013

Client Identifier Option in DHCP Server Replies

Abstract

This document updates RFC 2131 "Dynamic Host Configuration Protocol" by addressing the issues arising from that document's specification that the server MUST NOT return the 'client identifier' option to the client.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6842.

Table of Contents

1. Introduction 2
1.1. Requirements Language 2
2. Problem Statement 2
3. Modification to RFC 2131 3
4. Security Considerations 4
5. Acknowledgments 4
6. Normative References 4

1. Introduction

The Dynamic Host Configuration Protocol (DHCP) defined in [RFC2131] provides configuration parameters to hosts on an IP-based network. DHCP is built on a client-server model, where designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured hosts.

The changes to [RFC2131] defined in this document clarify the use of the 'client identifier' option by the DHCP servers. The clarification addresses the issues (as mentioned in Problem Statement) arising out of the point specified by [RFC2131] that the server MUST NOT return the 'client identifier' option to the client.

1.1. Requirements Language

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].

2. Problem Statement

[RFC2131] specifies that a combination of 'client identifier' or 'chaddr' and assigned network address constitute a unique identifier for the client's lease and are used by both the client and server to identify a lease referred in any DHCP messages. [RFC2131] also specifies that the server MUST NOT return the 'client identifier' option in DHCPOFFER and DHCPACK messages. Furthermore, DHCP relay agents and servers implementing [RFC2131] MAY drop the DHCP packets in the absence of both the 'client identifier' and 'chaddr' option.

In some cases, a client may not have a valid hardware address to populate the 'chaddr' field and may set the field to all zeroes. One such example is when DHCP is used to assign an IP address to a mobile phone or a tablet and where the 'chaddr' field is set to zero in DHCP request packets. In such cases, the client usually sets the 'client

identifier' option field (to a value as permitted in [RFC2131]), and both the client and server use this field to uniquely identify the client with in a subnet.

Note that due to aforementioned recommendations in [RFC2131], valid downstream DHCP packets (DHCPOFFER, DHCPACK, and DHCPNAK) from the server MAY get dropped at the DHCP relay agent in the absence of the 'client identifier' option when the 'chaddr' field is set to zero.

The problem may get aggravated when a client receives a response from the server without 'client identifier' and with the 'chaddr' value set to zero, as it cannot guarantee that the response is intended for it. This is due to the fact that even though the 'xid' field is present to map responses with requests, this field alone cannot guarantee that a particular response is for a particular client, as 'xid' values generated by multiple clients within a subnet need not be unique.

Lack of the 'client identifier' option in DHCP reply messages also affects the scenario where multiple DHCP clients may be running on the same host sharing the same 'chaddr'.

This document attempts to address these problems faced by the DHCP relay agent and client by proposing modification to DHCP server behavior. The solution specified in this document is in line with DHCPv6 [RFC3315] where the server always includes the Client Identifier option in the Reply messages.

The requirement for DHCP servers not to return the 'client identifier' option was made purely to conserve the limited space in the packet. It is possible, though unlikely, that clients will drop packets that contain this formerly unexpected option. There are no known client implementations that will drop packets, but the benefit provided by this change outweighs any small risk of such behavior. More harm is being done by not having the 'client identifier' option present than might be done by adding it now.

3. Modification to RFC 2131

If the 'client identifier' option is present in a message received from a client, the server MUST return the 'client identifier' option, unaltered, in its response message.

The following table is extracted from Section 4.3.1 of [RFC2131] and relevant fields are modified accordingly to overcome the problems mentioned in this document.

Option	DHCPOFFER	DHCPACK	DHCPNAK
Client identifier (if sent by client)	MUST	MUST	MUST
Client identifier (if not sent by client)	MUST NOT	MUST NOT	MUST NOT

When a client receives a DHCP message containing a 'client identifier' option, the client MUST compare that client identifier to the one it is configured to send. If the two client identifiers do not match, the client MUST silently discard the message.

4. Security Considerations

This specification does not add any new security considerations other than the ones already mentioned in [RFC2131]. It is worth noting that DHCP clients routinely connect to different IP networks managed by different network providers. DHCP clients have no a priori knowledge of which network they are connecting to. Consequently, the client identifier will, by definition, be routinely shared with network operators and could be used in ways that violate the user's privacy. This is a problem that existed in [RFC2131]. This document does nothing to address this problem.

5. Acknowledgments

The authors would like to thank Bernie Volz, Ted Lemon, Barr Hibbs, Richard Johnson, Barry Leiba, Stephen Farrell, and Adrian Farrel for insightful discussions and review.

6. 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.

[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.

Authors' Addresses

Narasimha Swamy Nelakuditi
Samsung India
Block-B, Bagmane Lakeview,
66/1, Bagmane Tech Park,
Byrasandra, C.V. Raman Nagar, Bangalore, 560093
India

Phone: +91 80 4181 9999
EMail: nn.swamy@samsung.com

Gaurav Halwasia
Cisco Systems
SEZ Unit, Cessna Business Park
Sarjapur Marathalli Outer Ring Road
Bangalore, 560103
India

Phone: +91 80 4426 1321
EMail: ghalwasi@cisco.com

Prashant Jhingran
Cisco Systems
SEZ Unit, Cessna Business Park
Sarjapur Marathalli Outer Ring Road
Bangalore, 560103
India

Phone: +91 80 4426 1800
EMail: pjhingra@cisco.com