Dynamic Host Configuration Working Group
Internet-Draft
Updates: 2131 (if approved)
Intended status: Standards Track
Expires: January 10, 2011

D. Hankins
ISC

July 9, 2010

Dynamic Host Configuration Protocol DHCPINFORM Message Clarifications
draft-ietf-dhc-dhcpinform-clarify-05

Abstract

The DHCPINFORM message within the DHCPv4 protocol has in operation diverged incompatibly from the current defined standard. This document seeks to provide clarification of actual behaviour and guidance for some situations that were previously omitted.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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 January 10, 2011.

Copyright Notice

Table of Contents

1. Introduction

The most recent DHCPv4 Standard [RFC2131] added a new DHCPv4 message: DHCPINFORM. The intent of the DHCPINFORM message was for clients that used manually entered fixed IPv4 addresses to still be able to get some configuration state dynamically. Since that time, however, we have seen this message used by normal DHCPv4 dynamically addressed clients; clients that have previously succeeded in receiving configuration through DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and finally DHCPACK messages.

These clients are attempting DHCPINFORM messages in order to obtain additional configuration state that was not present in their lease binding. The discovery is that DHCPINFORM can be used to reach extra DHCP servers, other than the one that gave an address, which may have more configuration options available but aren't in a position to give addresses. This extra configuration state is often required by applications that were not running at system startup, when the DHCP client was initialized, and supplied by servers or services bundled with a product that cannot easily be integrated with the network's existing DHCP infrastructure and so are provided separately.

Some of these DHCPINFORM clients have surfaced which run with stripped down user priveleges, but still perform some network related functions. This software does not have the capacity to determine its IPv4 address(es), nor does it know what interface(s) are present on the system, or their hardware addresses. But it can send and receive DHCP packets. Consequently, the 'ciaddr' and 'chaddr' fields have been witnessed to be empty, even though they appear to be required to be filled by RFC 2131. Clarification is sought for server behaviour when ciaddr is zero.

Another set of DHCP clients set the 'chaddr' field to a fixed magic value, rather than the client's hardware address, identifying them as part of a vendor's product. Although the 'chaddr' contents were never defined by any IETF RFC to be a valid place to store 'Vendor

Identifying Information', their implementors believed this field was unused by the DHCP protocol in specific regards to DHCPINFORM because a server would determine the client's hardware address through normal UDP unicast methods; IP forwarding leading to ARP [RFC0826] processing or similar.

We also wish to clarify a DHCPv4 server's behaviour when it receives a DHCPINFORM via a relay (when 'giaddr' is non-zero). Section 4.1 of the DHCPv4 specification [RFC2131] seems to include DHCPINFORM->DHCPACK exchanges by describing generic behaviour for all DHCPOFFER and DHCPACK replies, and it requires that if 'giaddr' is non-zero that it "MUST" be used. But this advice does not work in

practice (due to BOOTP Relay Agent [RFC1542] requirements to use 'yiaddr' field contents, which MUST be zero as also per [RFC2131]). Furthermore, this guidance conflicts with [RFC2131] Section 4.3.5, which directs that the server replies directly to the 'ciaddr' contents when responding to DHCPINFORM, and makes no other directions for other header fields. As a result, it also does not adequately describe current operational deployments of the DHCPINFORM message exchange which definitely direct replies directly to 'ciaddr' and may (it has not been concretely determined) direct replies to the 'giaddr' first.

2. Requirements Language

In this document, the key words "MAY", "MUST", "SHALL", "MUST NOT", "SHOULD", and "SHOULD NOT", are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

3. Client Behaviour

Clients are still required to fulfill the DHCPv4 requirements for DHCPINFORM messages ([RFC2131], Sections 4.4.1 and 4.4.3). But the following are clarified as in addition, or to overlay those requirements:

- Clients MUST set 'ciaddr' to a working IPv4 address which they can use to receive replies. This address SHOULD be an address that is currently assigned to the interface upon which the client is

transmitting its DHCPINFORM, except in the condition where the DHCP client is unable to determine a valid IP address for its host, in which case the client MUST set 'ciaddr' to all-zero.

- Clients MUST set 'chaddr', 'htype', and 'hlen' to the hardware address of the interface upon which the DHCPINFORM message is being transmitted, except in the condition where the DHCP client is unable to determine this address, in which case all three fields MUST be set all-zero.

- Clients MUST set the 'flags' field to zero. This means that the client MUST NOT set the 'BROADCAST' flag, and MUST be capable of receiving IP unicasts.

- Clients SHOULD direct their DHCPINFORM via unicast UDP to the IPv4 address contained in the Server Identifier [RFC2132] option, if they have a currently active binding from previous DHCPREQUEST message exchanges. It MAY be unicast to a known DHCP server, or otherwise broadcast to the appropriate IPv4 broadcast address on

the interface being configured.

4. Server Behaviour

DHCPv4 server behaviour in processing DHCPINFORM messages is a more difficult question to answer, due to inconsistent client behaviour and conflicting directions in RFC 2131. The following is intended to be a more complete reference.

First, upon receiving a DHCPINFORM, a DHCPv4 Server MUST determine the client's "relevant IPv4 address" according to the following in order of priority:

1. The Subnet Selection Option [RFC3011], if it is present.

2. The 'ciaddr' field, if it is non-zero.

3. The Relay Agent Link Selection Sub-Option [RFC3527], if it is present in a Relay Agent Information Option [RFC3046].

4. The 'giaddr' field, if it is non-zero.

5. The IPv4 source address field, if it is non-zero.

6. The DHCPv4 Server's address on the interface on which the DHCPINFORM was received.

The DHCPv4 server checks to see if the "relevant IPv4 address" is within a range or subnet over which it holds authority, or if it is configured to respond. It will manufacture a DHCPACK response with configuration values appropriate for the "relevant IPv4 address". If the "relevant IPv4 address" is from the 'ciaddr' field (because the Subnet Selection Option was not provided, and the 'ciaddr' field is non-zero), the server MAY also inspect that address's current lease in order to source configuration specific to the host, but MUST NOT modify the lease in any way.

In the DHCPACK reply:

- The 'htype', 'hlen', 'chaddr', 'ciaddr', 'xid', 'flags' (with the exception noted below), and 'giaddr' fields MUST be copied from the client's DHCPINFORM.

- The 'hops' field MUST be zero.

- The 'secs' field MUST be zero.

- The 'yiaddr' field MUST be zero.

- The 'siaddr' field MUST be zero.

- The 'sname' and 'file' fields MAY be used exclusively for 'option overloading', but MUST be all-zero otherwise.

- The 'options' field MUST be filled as described in RFC 2131 Section 4.3.1.

Next, the DHCPv4 server MUST determine the "reply address and port" according to the first of the following conditions it finds a valid reply address for, in order:

1. If the 'ciaddr' field is non-zero, the server selects its

contents as an IPv4 address and port 68 ('DHCP client').

2. If the 'giaddr' field is non-zero, the server selects its contents as an IPv4 address and port 67 ('DHCP server').

3. If the IPv4 source address field is non-zero, the server selects its contents as an IPv4 address and port 68 ('DHCP client')

4. The server selects the limited broadcast address (all-ones) and port 68 ('DHCP client').

At this point, the DHCPv4 server verifies that it holds configuration authority over the reply address (or link in case of limited broadcast address) it has selected to transmit the reply to. If the server has not been configured to hold authority over this address, it MUST NOT reply. It SHOULD increment a counter visible to the operator but SHOULD NOT log an error (unless a mechanism is used to suppress repeated log messages). See the Security section (Section 5) for the rationale behind this direction.

Note very carefully that a DHCPv4 server will send replies directly to a DHCPv4 client by way of 'ciaddr' even if the DHCPINFORM message was relayed. Note that this means DHCPINFORM processing is intentionally broken in deployments where the client's address space is unreachable by the DHCPv4 server. In such cases, the server should probably be configured not to reply to DHCPINFORMs.

Now, the server performs an exception to assist relay agents. If it selected the 'giaddr' as the destination address and port, then it MUST set the 'BROADCAST' bit in the flags field true, no matter what its value was in the client's DHCPINFORM message, without altering the other bits of the flag field. Otherwise, the response could not be delivered; a BOOTP Relay Agent [RFC1542] is required to direct

unicast server replies to the 'chaddr' and 'yiaddr' field contents, but 'chaddr' is not reliably filled, and 'yiaddr' is required to be all-zero. Setting the broadcast flag assists the relay agent in locating the client by informing it to perform a local limited broadcast.

Having selected a destination IPv4 address and port number, the last step is to select a destination link layer address.

For the all-ones limited broadcast address, the DHCPv4 server MUST use the all-ones broadcast hardware address.

For all other (unicast) destination selections, the DHCPv4 server MUST use its host operating system's usual methods to determine hardware addressing, as by IP forwarding and subsequent address resolution (such as through ARP [RFC0826]). Note that the DHCPv4 server MAY have seeded its ARP cache from a previous stateful exchange with the client (from 'chaddr' contents while processing a DHCPREQUEST message, due to the requirement of DHCPv4 servers to unicast some replies before clients will process ARP), and some DHCPv4 software MAY still use 'chaddr' contents to direct replies to directly connected clients. Consequently, DHCPINFORM can not be reasonably expected to instigate an immediate ARP broadcast, nor can 'chaddr' contents be used for any purpose other than to carry the unicast hardware address with which a client might reasonably be reached.

5. Security Considerations

As with all DHCP messages, DHCPINFORM and DHCPACK replies contain no capacity for encryption, and all packet contents must be presumed readable in the clear. In particular, and as outlined above, in some circumstances the packets may be broadcast and so more easily intercepted than most other messages.

Authentication for DHCPv4 Messages [RFC3118] does exist, but is not well deployed. Care should be taken in the degree to which configuration parameters provided by DHCPv4 are trusted, as the replies can be easily spoofed by any eavesdropper. Again noting that packets may be broadcast under some circumstances, the BOOTP header Transaction Id field ("XID") is insufficient protection from man-in-the-middle attacks.

A relay agent receives replies via unicast UDP messages from a DHCP server, and may broadcast these packets on the inside-facing network. If an outside attacker was aware of this relay agent and its unicast address, this facility could be used to produce broadcast storms on

the network. Care should be taken to ensure that the relay agent is

not open to this kind of attack, possibly making use of Relay Agent Authentication [RFC4030] to ensure that a DHCPv4 server can not be induced to sending bogus replies to the relay.

This protocol uses the 'ciaddr' field contents to direct replies, which may be set blindly by the client to any value, regardless of IP source address validation or related filter restrictions. If an attacker were to identify a number of DHCPv4 servers which reply to addresses not under their authority to configure, and those servers had enough large DHCPv4 options in configuration to request, it could represent a significant amplification vector in straight packet-load Denial-of-Service attacks. For this reason, servers MUST NOT make replies to addresses not explicitly configured under their authority to configure.

6. IANA Considerations

This document has no action for IANA.

7. Acknowledgements

This document has been reviewed and improved by the comments of several people, but the author would like to take a moment to thank Alfred Hoenes, who has submitted revised text for this document.

8. References

8.1. 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.

[RFC3011] Waters, G., "The IPv4 Subnet Selection Option for DHCP", RFC 3011, November 2000.

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

[RFC3527] Kinnear, K., Stapp, M., Johnson, R., and J. Kumarasamy, "Link Selection sub-option for the Relay Agent Information Option for DHCPv4", RFC 3527, April 2003.

8.2. Informative References

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[RFC1542] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, October 1993.

[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.

Author's Address

David W. Hankins
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
US

Phone: +1 650 423 1307
Email: David_Hankins@isc.org