Internet Engineering Task Force (IETF)
Request for Comments: 7283
Updates: 3315
Category: Standards Track
ISSN: 2070-1721

Y. Cui
Q. Sun
Tsinghua University
T. Lemon
Nominum, Inc.

July 2014

Handling Unknown DHCPv6 Messages

Abstract

DHCPv6 is not specific about handling messages with unknown types. This memo describes the problems associated with receiving DHCPv6 messages with unknown types, and defines how a DHCPv6 server, client, or relay agent should behave when receiving unknown DHCPv6 messages. This document also provides advice for authors of future documents that define new messages to be sent from DHCP servers to DHCP relay agents. This document updates RFC 3315.

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/rfc7283.

Table of Contents

1. Introduction 3
2. Requirements Language 3
3. Problem Statement 3
4. Relay Agent Behavior Update 3
4.1. A Valid Message for Constructing a New Relay-forward Message 4
4.2. Relaying a Message toward the Server 5
4.3. Relaying a Message toward the Client 5
5. Client and Server Behavior Update 5
6. Security Considerations 5
7. Contributors 6
8. Normative References 6

1. Introduction

DHCPv6 [RFC3315] provides a framework for conveying IPv6 configuration information to hosts on a TCP/IP network. But [RFC3315] is not specific about how to deal with messages with unrecognized types. This document describes the problems associated with receiving DHCPv6 messages with unknown types, and defines the behavior of a DHCPv6 server, client, or relay agent when handling unknown DHCPv6 messages.

2. 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].

3. Problem Statement

When a relay agent receives a message, it sends the message toward either the server or the client. The relay agent decides on the direction to forward based on the message type. Since RFC 3315 was published, new message types have been defined. Additional message types may be defined in the future. RFC 3315 does not specify what to do when a DHCP agent does not recognize the type of message it has received. This may lead to relay agents inappropriately dropping these messages and to other DHCP agents inappropriately processing these messages.

In addition, there is no specific requirement for dealing with unknown messages by the client or server in RFC 3315.

Note that it is expected that most future DHCPv6 messages will not be used to communicate directly with relay agents (though they may need to be relayed by relay agents).

4. Relay Agent Behavior Update

Relay agents relay messages toward servers and clients according to the message type. The Relay-reply message is sent toward the client. The Relay-forward message and other types of messages are sent toward the server.

We say "toward the client" and "toward the server" because relay agents may be chained together, so a relay message may be sent through multiple relay agents along the path to its destination. Relay-reply messages specify a destination address; the relay agent extracts the encapsulated message and sends it to the specified destination address. Any message other than a Relay-reply does not

have such a specified destination, so it follows the default forwarding path configured on the relay agent, which is always toward the server.

The sole purpose of requiring relay agents to relay unknown messages is to ensure that when legitimate new messages are defined in the protocol, relay agents (even if they were manufactured prior to the definition of these new messages) will, by default, succeed in relaying such messages.

4.1. A Valid Message for Constructing a New Relay-forward Message

Section 20.1 of [RFC3315] states that:

> When a relay agent receives a valid message to be relayed, it constructs a new Relay-forward message.

It does not define which types of messages are valid for constructing Relay-forward messages. In this document, we specify the definition as follows.

> The message is valid for constructing a new Relay-forward message:
>
> (a) if the message is a Relay-forward message, or
>
> (b) if the relay agent recognizes the message type and is not the intended target, or
>
> (c) if the relay agent does not recognize the message type.

New DHCP message types may be defined in the future that are sent, unsolicited, to relay agents. Relay agents that do not implement these messages will not recognize the messages as being intended for them. Therefore, a relay agent that implements this specification will forward such messages to the DHCP servers to which it is configured to relay client messages.

At this time, no such message types have been specified. If such a message is specified in the future, it is possible that this would result in needless load on DHCP servers. If such a message type is defined in a future specification, authors may need to consider a strategy for identifying non-conforming relays and not sending such messages to those relay agents.

However, since DHCP servers do not respond to unknown messages, this is unlikely to create significant load and is therefore likely to be unnecessary.

4.2. Relaying a Message toward the Server

If the relay agent receives a Relay-forward message, Section 20.1.2 of [RFC3315] defines the required behavior. If the relay agent receives messages other than Relay-forward and Relay-reply and the relay agent does not recognize its message type, it MUST forward them as described in Section 20.1.1 of [RFC3315].

4.3. Relaying a Message toward the Client

If the relay agent receives a Relay-reply message, it MUST process the message as defined in Section 20.2 of [RFC3315], regardless of the type of message encapsulated in the Relay Message option.

5. Client and Server Behavior Update

A client or server MUST silently discard any received DHCPv6 message with an unknown message type.

6. Security Considerations

This document creates no new security issues that are not already present in RFC 3315. By explicitly documenting the correct handling of unknown messages, this document, if implemented, reduces any security exposure that might result from incorrect handling of unknown messages. The following issues are already present with Section 23 of [RFC3315], but we discuss them in detail here as guidance for implementors.

As the relay agent will forward all unknown types of DHCPv6 messages, a malicious attacker can interfere with the relaying function by constructing fake DHCPv6 messages with an arbitrary type code. The same problem may occur in current DHCPv4 and DHCPv6 practice, where the attacker constructs the fake DHCP message with a known type code.

Clients and servers that implement this specification will discard unknown DHCPv6 messages. Since RFC 3315 did not specify relay agent, client, or server behavior in the presence of unknown messages, it is possible that some servers or clients that have not been updated to conform to this specification will become vulnerable to attacks through the relay agent as a result of this change.

For this reason, we recommend that relay agents, clients, and servers be updated to follow this new specification. However, in most deployment scenarios, it will be much easier to attack clients directly than through a relay agent. Furthermore, attacks using unknown message types are already possible on the local wire.

So, in most cases, if clients are not upgraded, there should be minimal additional risk. At sites where only servers and relay agents can be upgraded, the incremental benefit of doing so most likely exceeds any risk of vulnerable clients.

Nothing in this update should be construed to mean that relay agents may not be administratively configurable to drop messages based on the message type, for security reasons (e.g., in a firewall).

7. Contributors

Many thanks to Bernie Volz, Tomek Mrugalski, Sheng Jiang, Cong Liu, and Yuchi Chen for their contributions to the document.

8. Normative References

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

Yong Cui
Tsinghua University
Beijing 100084
P.R. China

Phone: +86-10-6260-3059
EMail: yong@csnet1.cs.tsinghua.edu.cn

Qi Sun
Tsinghua University
Beijing 100084
P.R. China

Phone: +86-10-6278-5822
EMail: sunqi@csnet1.cs.tsinghua.edu.cn

Ted Lemon
Nominum, Inc.
2000 Seaport Blvd
Redwood City, CA 94063
USA

Phone: +1-650-381-6000
EMail: Ted.Lemon@nominum.com