DHC Working Group
Internet-Draft
Updates: 3315 (if approved)
Intended status: Standards Track
Expires: June 19, 2014

Y. Cui
Q. Sun
Tsinghua University
T. Lemon
Nominum, Inc.
December 16, 2013

Handling Unknown DHCPv6 Messages
draft-ietf-dhc-dhcpv6-unknown-msg-04

Abstract

DHCPv6 is not specific about handling messages with unknown types. This memo describes the problems and defines how a DHCPv6 server, client or relay agent should behave when receiving unknown DHCPv6 messages. This document updates RFC3315.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on June 19, 2014.

Copyright Notice

Table of Contents

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 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 decides to send the message either toward the server or toward the client. However, RFC 3315 does not explicitly describe how the relay agent can determine whether it should send a message toward the server or the client, although this is implied by the message definitions in RFC3315.

Another issue is that RFC3315 does not specify what a relay agent should do if it does not recognize a received message; the relay agent is not required to relay the message, nor advised to drop the message. If relaying an unknown message, the relay agent is given no guidance about whether to send it toward the server or the client.

In addition, there is no specific requirement for dealing with unknown messages by the client or server in RFC3315.

Note 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 receives the message for which it is not the target according to the message type.

In the case that a new type of message is sent by the server to a relay agent but the relay agent does not recognize it, the message is put into a Relay-forward message and sent to the server.

4.2. Relaying a Message toward 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 is described in Section 20.1.1 of [RFC3315].

4.3. Relaying a Message toward Client

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

5. Client and Server Behavior Update

There are chances that the client or server would receive DHCPv6 messages with unknown types. In this case, the client or server MUST silently discard the unrecognized messages.

6. Security Considerations

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 arbitrary type code. The same problem may happen 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 RFC3315 did not specify either 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 might be made vulnerable to

client attacks through the relay agent.

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 due to vulnerable clients.

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

7. IANA Considerations

This document does not include an IANA request.

8. Contributors List

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

9. 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