DHC Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 26, 2013

Y. Cui
Q. Sun
Tsinghua University
T. Lemon
Nominum, Inc.
April 24, 2013

Handling Unknown DHCPv6 Messages
draft-ietf-dhc-dhcpv6-unknown-msg-00

Abstract

Dynamic Host Configuration Protocol version 6 (DHCPv6) isn't specific about handling messages with unknown types. This document describes the problems and defines how a DHCPv6 function node should behave in this case. This document updates RFC3315.

Table of Contents

1. Introduction

Dynamic Host Configuration Protocol version 6 (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 message with unrecognized types. This document describe the problems and defines the behavior of a DHCPv6 function node in this case. This document updates [RFC3315].

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

The relay agent is bound to send a message either to the server or to the client. But RFC3315 doesn't specify how the relay agent can find out it should send a message towards the server or towards the client.

Another issue is that, there is no statement in RFC3315 about what a relay agent should do when receiving message types it doesn't recognize. The relay agent isn't required to relay the messages, nor advised to drop them.

In addition, there is no specific requirement of the client or server on dealing with an unknown message in RFC3315.

4. Relay Agent Behavior Update

A relay agent is responsible for relaying messages between the client and server. The Relay-reply message is meant to be sent to the client side (downlink), while the Relay-forward message and other types of message are meant to be sent to the server side (uplink). A relay agent should determine whether the message should be relayed towards the server or the client according to message types.

4.1. Definition of a Valid 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."

However it doesn't specify what a valid message is. In this document, we define that a message is valid for constructing a new Relay-forward message if it is not a Relay-reply message.

4.2. Relaying a Message towards Server

If the relay agent received a Relay-forward message, Section 20.1.2 of [RFC3315] defines the related behavior. If the relay agent received messages other than Relay-forward and Relay-reply, it MUST forward them as is described in Section 20.1.1 of [RFC3315].

4.3. Relaying a Message towards Client

If the relay agent received a Relay-reply message, it MUST unpack the message and forward it as is defined in Section 20.2 of [RFC3315], regardless of the message type in 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 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 has to construct the fake DHCP message with an known type code.

Clients and servers that implement this specification will discard unknown DHCPv6 messages. Since RFC3315 did not specify either relay, client or server behavior in the presence of unknown messages, it is possible that some server or client that has 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; 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 relays 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). 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.

7. IANA Considerations

This document does not include an IANA request.

8. Contributors List

Many thanks for Bernie Volz, Cong Liu and Yuchi Chen's contributions to the draft.

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
Department of Computer Science, Tsinghua University
Beijing 100084
P.R.China

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

Qi Sun

Tsinghua University
Department of Computer Science, 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: mellon@nominum.com