DHC
Internet-Draft
Intended status: Standards Track
Expires: September 1, 2016

E. Lear
R. Droms
Cisco Systems

February 29, 2016

# Manufacturer Usage Description URI and DHCP Option
# draft-lear-ietf-dhc-mud-option-01

Abstract

The ability of smart objects to protect themselves will vary. A good source of information about a device's capabilities is the manufacturer. This document specifies a means by which devices can communicate a URI that the network can use to retrieve simple network-relevant information.

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 September 1, 2016.

Table of Contents

1. Introduction . . . . . 2
2. The MUD URI DHCP Option . . . . . 3
3. How the Option Is Processed . . . . . 3
3.1. Client Behavior . . . . . 3
3.2. Server Behavior . . . . . 4
3.3. Relay Requirements . . . . . 4
4. Security Considerations . . . . . 4
5. IANA Considerations . . . . . 5
6. Acknowledgments . . . . . 5
7. References . . . . . 5
7.1. Normative References . . . . . 5
7.2. Informative References . . . . . 6
Authors' Addresses . . . . . 7

## 1. Introduction

A Manufacturer Usage Description (mud) refers to a YANG-based XML file that is intended for use by a management station or controller, but is very close to directly parsable by a NETCONF-enabled device.[RFC6020],[RFC6241]. The basic concept is that a device will emit a uniform resource identifier (URI) [RFC3986] that is associated with that file, and the network may do various things with that knowledge, including apply access lists or quality of service policies. A complete overview of MUD can be found in [I-D.lear-mud-framework].

In this memo a single means is defined to emit the MUD URI, which is a DHCP option[RFC2131],[RFC3315] that the DHCP client uses to inform the DHCP server. The DHCP server may take further actions, such as retrieve the URI or otherwise pass it along to network management system or controller.

The format of the mud URI is specified in [I-D.lear-ietf-netmod-mud].

An example would be as follows:

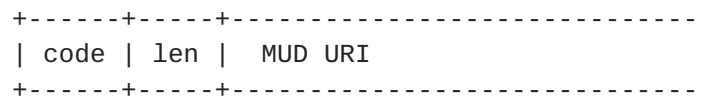
https://www.vendor.example.com/.well-known/mud/v1/BudsLight/m2000

Figure 1: URI example

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].

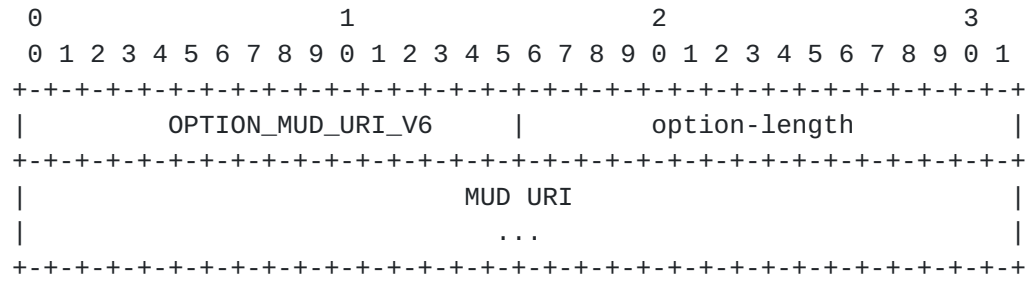
## 2. The MUD URI DHCP Option

The IPv4 MUD URI client option has the following format:




Code OPTION_MUD_URI_V4 (TBD) is assigned by IANA. len is a single octet that indicates the length of the URI in octets. MUD URI is a URI. The length of a MUD URI does not exceed 255 bytes.

The IPv6 MUD URI client option has the following format:




OPTION_MUD_URI_V6 (TBD; assigned by IANA).

option-length contains the length of the URI in octets. The length MUST NOT exceed 255 octets.

The MUD URI is a URI.

## 3. How the Option Is Processed

The intent of this option is to provide both a new classifier to the network as well as some recommended configuration to the routers that implement policy. However, it is entirely the purview of the network system as managed by the network administrator to decide what to do with this information. The key function of this option is simply to identify the type of device to the network in a structured way such that the policy can be easily found with existing toolsets.

### 3.1. Client Behavior

A client MAY emit a DHCP v4 or DHCPv6 option or both. This is a singleton option, as specified in [RFC7227]. Because clients are intended to have at most one MUD URI associated with them, they may emit at most one MUD URI option via DHCPv4 and one MUD URI option via

DHCPv6. In the case where both v4 and v6 DHCP options are emitted, the same URI MUST be used.

Clients SHOULD log or otherwise report improper acknowledgments from servers, but they MUST NOT modify their MUD URI configuration based on a server's response. The server's response is only an acknowledgment that the server has processed the option, and promises no specific network behavior to the client. In particular, it may not be possible for the server to retrieve the file associated with the MUD URI, or the local network administration may not wish to use the usage description. Neither of these situations should be considered in any way exceptional.

### 3.2. Server Behavior

DHCP servers MAY ignore or process the option. For purposes of debugging, if a server successfully parses the option and the URI, it MUST return the option with the same URI as an acknowledgment. Even in this circumstance, no specific network behavior is guaranteed. When a server consumes this option, it will either forward the URI and relevant client information to a network management system (such as the giaddr), or it will retrieve the usage description by resolving the URI.

DHCP servers may implement MUD functionality themselves or they may pass along appropriate information to a network management system or controller. The server that does process the MUD URI MUST adhere to the process specified in [RFC2818] and [RFC5280] to validate the TLS certificate of the web server hosting the MUD file. Those servers will retrieve the file, process it, create and install the necessary configuration on the relevant gateway. Servers SHOULD monitor the gateway for state changes on a given interface. DHCP servers that are NOT providing MUD functionality themselves will forward to the network management system(s) that are any RELEASEs they receive for any DHCPREQUESTs that they previously processed, so that the network management systems may then retire any lingering state.

### 3.3. Relay Requirements

There are no additional requirements for relays.

## 4. Security Considerations

Emission of a MUD URI will provide an interloper with knowledge about a device. However, an interloper may gain most of this same information through classical fingerprinting techniques. That is, device behavior patterns are generally easy to determine. In environments where this would be a concern, use of devices with this

option is NOT RECOMMENDED. Instead other more secure means should be considered.

It may be possible for a man in the middle to modify the DHCP request so that a different URI is queried. To address this threat, controllers SHOULD NOT query a site based on the authority component of the MUD URI when it has noted that the authority section has changed. For example, if the MAC address is the same and the authority portion of the URI is different from the last query, something probably has gone wrong. Such a situation SHOULD be logged and reported. As of this writing, one of the authors is aware of ongoing work to address DHCP message integrity protection[I-D.ietf-dhc-sedhcpv6].

A malicious device could emit a URI to malware. Servers or other network management systems should only process valid MUD URIs, and MUST apply strict validation rules to the content that is returned, making use of the Accept: header, and rejecting any content that does not have an acceptable type. In addition, servers MAY ignore URIs to unknown manufacturers. In order to prevent modification of content in flight, all communication to web sites MUST make use of TLS, and all certificates MUST be validated.

## 5. IANA Considerations

IANA is requested to allocated the DHCPv4 and v6 options as specified in Section 2.

## 6. Acknowledgments

The authors thank Bernie Volz for his helpful suggestions.

## 7. References

### 7.1. Normative References

[I-D.lear-ietf-netmod-mud]
Lear, E., "Manufacturer Usage Description YANG Model", draft-lear-ietf-netmod-mud-00 (work in progress), January 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <http://www.rfc-editor.org/info/rfc2131>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <http://www.rfc-editor.org/info/rfc2818>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

## 7.2. Informative References

[I-D.ietf-dhc-sedhcpv6]
Jiang, S., Li, L., Cui, Y., Jinmei, T., Lemon, T., and D. Zhang, "Secure DHCPv6", draft-ietf-dhc-sedhcpv6-10 (work in progress), December 2015.

[I-D.lear-mud-framework]
Lear, E., "Manufacturer Usage Description Framework", draft-lear-mud-framework-00 (work in progress), January 2016.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <http://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <http://www.rfc-editor.org/info/rfc6241>.

[RFC7227] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", BCP 187, RFC 7227, DOI 10.17487/RFC7227, May 2014, <http://www.rfc-editor.org/info/rfc7227>.

## Authors' Addresses

Eliot Lear
Cisco Systems
Richtistrasse 7
Wallisellen CH-8304
Switzerland

Phone: +41 44 878 9200
Email: lear@cisco.com

Ralph Droms
Cisco Systems
55 Cambridge Parkway
Cambridge 1057
United States

Phone: +1 617 621 1904
Email: rdroms@cisco.com