DHCPv6 Option for Midcom Middlebox

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026. 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

Distribution of this document is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

The Dynamic Host Configuration Protocol version 6[RFC3315] provides a framework for passing configuration information to hosts on a TCP/IP network. Entities using the Midcom Protocol need to know the presence of Midcom middleboxes, such as firewalls and network address translators, in order to enable communication across these devices. A DHCPv6 option provides a means for these entities to determine the Midcom middleboxes IPv6 address or the domain name.
1 Terminology

Midcom agent: As defined in [RFC3303], MIDCOM agents are entities performing ALG functions, logically external to a middlebox. MIDCOM agents possess a combination of application awareness and knowledge of the middlebox function. This combination enables the agents to facilitate traversal of the middlebox by the application's packets.

Midcom middlebox: A Midcom middlebox is a middlebox capable of performing Midcom functionality as in [RFC3304].

Middlebox: As defined in [RFC3303], a middlebox is a network intermediate device that implements one or more of the middlebox services. A network address translation middlebox (NAT) is a middlebox implementing a NAT service. A firewall middlebox is a middlebox implementing a firewall service.

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119].

2 Introduction

Midcom as described in the RFCXXXX [MDCSEM], is a technique for dynamically configuring a middlebox. These are devices located in the path of two end-points which provide services such as firewall and network address translation. Midcom provides connectivity through Midcom middleboxes for protocols like a Session Initiation Protocol [RFC3261] which are normally broken when middleboxes are present in a network. In order to provide this connectivity, SIP entities can integrate a Midcom agent.

In a IPv6 network, a Midcom agent needs to know the IPv6 addresses or the domain name of the Midcom middleboxes present in the network in order to dynamically configure them. This document describes a DHCPv6 option intended for IPv6 networks which provides a means for Midcom agents to known the IPv6 addresses or the domain name of Midcom middleboxes.

3 Midcom Middlebox IP Address
A Midcom middlebox may have many IP addresses located in different domains as illustrated in figure 1. These addresses are defined in the Midcom semantics document [MDCSEM].

```
+----------+                                 +----------+
| internal | A0    A1 +-----------+ A2    A3 | external |
| endpoint +----------+ middlebox +----------+ endpoint |
+----------+          +-----------+          +----------+
```

Figure 1: Address tuples A0 - A3

- A0 - internal endpoint: address tuple A0 specifies a communication endpoint of a device within the internal network with respect to the middlebox.

- A1 - middlebox inside address: address tuple A1 specifies a virtual communication endpoint at the middlebox within the internal network. A1 is the destination address for packets passing from the internal endpoint to the middlebox, and is the source for packets passing from the middlebox to the internal endpoint.

- A2 - middlebox outside address: address tuple A2 specifies a virtual communication endpoint at the middlebox within the external network. A2 is the destination address for packets passing from the external endpoint to the middlebox, and is the source for packets passing from the middlebox to the external endpoint.

- A3 - external endpoint: address tuple A3 specifies a communication endpoint of a device within the external network with respect to the middlebox.

4 Midcom Middlebox DHCPv6 Option

The Midcom middlebox DHCPv6 option specifies a list of a 128-bit (binary) IPv6 addresses or, preferably, a DNS [RFC1035] domain name of the Midcom middleboxes that are present in a network. Midcom middlebox DHCPv6 option will thus use two DHCPv6 option numbers. No encoding mechanism will be used as in the DHCPv4 option for Midcom middlebox [DHCPV4MDC]. The first option is used to list Midcom middleboxes domain names and the second to list Midcom middleboxes IPv6 addresses. All implementations of the Midcom middlebox DHCPv6 option MUST implement both DHCPv6 option numbers.
4.1 Midcom Middlebox Domain Name List

Midcom middlebox DHCPv6 domain name list option (as illustrated in figure 1) specifies a list of Midcom middlebox domain names present in the network in order of preference.

The option number (OPTION_MIDCOM_DOMAIN) is TBD.

The parameter "option-length" is the length of the Midcom domain name list.

The "Midcom domain name list" contains a list of Midcom middlebox domain names present in the network which MUST be encoded following the section 3.1 of [RFC1035] and MUST NOT be stored in a compressed form according to section 4.1.4 of [RFC1035].

Domain names in messages are expressed in terms of a sequence of labels. Each label is represented as a one octet length field followed by that number of octets. Since every domain name ends with the null label of the root, a domain name is terminated by a length byte of zero. The high order two bits of every length octet must be zero, and the remaining six bits of the length field limit the label to 63 octets or less.

To simplify implementations, the total length of a domain name (i.e., label octets and label length octets) is restricted to 255 octets or less.

4.2 Midcom Middlebox IPv4 Address List

Dom
Midcom Middlebox DHCPv6 IPv6 address list option (as illustrated in figure 2) specifies a list of Midcom middlebox IPv6 addresses that are present in the network.

The option number (OPTION_MIDCOM_ADDR) is TBD.

The parameter "option-length" is the length of the Midcom middlebox IPv6 address list. This length MUST by a multiple of 16 (16*number of Midcom middlebox IPv6 Addresses).

The Midcom middlebox IPv6 address list is the list of Midcom middlebox IPv6 addresses that are present in the network. This list MUST define the addresses to use in order of preference.

5 Midcom Middlebox DHCPv6 Option Operation

Midcom middlebox DHCPv6 option defines two DHCPv6 options which MUST be implemented by DHCPv6 clients and servers. This section defines how these two options MUST interact.

5.1 Midcom Middlebox DHCPv6 Client Option Operation

A DHCPv6 client implementing a DHCPv6 Midcom middlebox option MUST be able to interpret both DHCPv6 options for Midcom middlebox domain name and IPv6 address list. This client MAY request either or both DHCPv6 "Option Request Option" (ORO) (see [RFC3315]) for Midcom middlebox domain names and IPv6 address list. In response to this request, a client MAY receive either or both DHCPv6 options for Midcom middlebox domain names and IPv6 addresses list. In the case where both lists are received, the client MUST use the domain name list first. It MAY only use the IPv6 address list in the case the Midcom middlebox domain can not be reached or resolved.
5.2 Midcom Middlebox DHCPv6 Server Option Operation

<table>
<thead>
<tr>
<th>Client request in ORO</th>
<th>Domain Name List</th>
<th>IPv6 Address List</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>SHOULD</td>
<td>MAY</td>
</tr>
<tr>
<td>Midcom Domain Name List</td>
<td>SHOULD</td>
<td>MAY</td>
</tr>
<tr>
<td>Midcom IPv6 Address List</td>
<td>MAY</td>
<td>MUST</td>
</tr>
<tr>
<td>Both options</td>
<td>SHOULD</td>
<td>MAY</td>
</tr>
</tbody>
</table>

Table 1: DHCPv6 server response to ORO

A DHCPv6 server implementing DHCPv6 Midcom middlebox option MUST be able to interpret the "Option Request Option" (ORO) for both DHCPv6 option for Midcom middlebox domain names and IPv6 addresses list. This server MAY send one or both of the Midcom middlebox domain names or IPv6 addresses list according to the response table 1.

6 Security Considerations

The security considerations in the DHCPv6 [RFC3315] apply.

There is the possibility of an attack of the type "man in the middle" which can modify the response from the DHCP server in order to change the Midcom middlebox address. This could lead a Midcom agent to contact a dumb middlebox and create a Denial of Service for the Midcom agent. This situation can then lead to a potential opening of a pinhole from the dumb middlebox using the information sent from the Midcom agent.

7 IANA Considerations

IANA has assigned the number TBD for the Midcom middlebox domain name DHCPv6 option and the number TBD for the Midcom middlebox IPv6 address name option.

8 Normative References


[RFC2119] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.


9 Informative References


10 Acknowledgments

This document was based on [RFC3319] written by H. Schulzrinne and B. Volz and [RFC3361] written by H. Schulzrinne.

11 Contributors

Pascal DorÉ“
M5T Centre d’excellence en Telecom inc.
Sherbrooke, Qc
Canada
e-mail: pdore@m5t.com
http://www.m5t.com

12 Authors’ Addresses

Joel Tran  
Dept. Genie Elect. & Genie Inf./Dep. Elect. & Comp. Engineering  
Universite de Sherbrooke  
Sherbrooke, Qc  
Canada  
e-mail: Joel.Tran@USherbrooke.ca

Soumaya Cherkaoui  
Dept. Genie Elect. & Genie Inf./Dep. Elect. & Comp. Engineering  
Universite de Sherbrooke  
Sherbrooke, Qc  
Canada  
e-mail: Soumaya.Cherkaoui@USherbrooke.ca

13 Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.