

Dynamic Host Configuration Protocol (DHCP-for-IPv4)
Option for Session Initiation Protocol (SIP) Servers

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

This document defines a Dynamic Host Configuration Protocol (DHCP-for-IPv4) option that contains a list of domain names or IPv4 addresses that can be mapped to one or more Session Initiation Protocol (SIP) outbound proxy servers. This is one of the many methods that a SIP client can use to obtain the addresses of such a local SIP server.

1. Terminology

DHCP client: A DHCP [1] client is an Internet host that uses DHCP to obtain configuration parameters such as a network address.

DHCP server: A DHCP server is an Internet host that returns configuration parameters to DHCP clients.

SIP server: As defined in RFC 3261 [2]. This server MUST be an outbound proxy server, as defined in [3]. In the context of this document, a SIP server refers to the host the SIP server is running on.

SIP client: As defined in RFC 3261. The client can be a user agent client or the client portion of a proxy server. In the context of this document, a SIP client refers to the host the SIP client is running on.

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 RFC 2119 [4].

2. Introduction

The Session Initiation Protocol (SIP) [2] is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. A SIP system has a number of logical components: user agents, proxy servers, redirect servers and registrars. User agents MAY contain SIP clients, proxy servers always do.

This document specifies a DHCP option [1,5] that allows SIP clients to locate a local SIP server that is to be used for all outbound SIP requests, a so-called outbound proxy server. (SIP clients MAY contact the address identified in the SIP URL directly, without involving a local SIP server. However in some circumstances, for example, when firewalls are present, SIP clients need to use a local server for outbound requests.) This is one of many possible solutions for locating the outbound SIP server; manual configuration is an example of another.

3. SIP Server DHCP Option

The SIP server DHCP option carries either a 32-bit (binary) IPv4 address or, preferably, a DNS (RFC 1035 [6]) fully-qualified domain name to be used by the SIP client to locate a SIP server.

The option has two encodings, specified by the encoding byte ('enc') that follows the code byte. If the encoding byte has the value 0, it is followed by a list of domain names, as described below (Section 3.1). If the encoding byte has the value 1, it is followed by one or more IPv4 addresses (Section 3.2). All implementations MUST support both encodings. The 'Len' field indicates the total number of octets in the option following the 'Len' field, including the encoding byte.

A DHCP server MUST NOT mix the two encodings in the same DHCP message, even if it sends two different instances of the same option. Attempts to do so would result in incorrect client behavior as DHCP processing rules call for the concatenation of multiple instances of an option into a single option prior to processing the option [7].

The code for this option is 120.

3.1 Domain Name List

If the 'enc' byte has a value of 0, the encoding byte is followed by a sequence of labels, encoded according to Section 3.1 of RFC 1035 [6], quoted below:

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.

RFC 1035 encoding was chosen to accommodate future internationalized domain name mechanisms.

The minimum length for this encoding is 3.

The option MAY contain multiple domain names, but these SHOULD refer to different NAPTR records, rather than different A records. The client MUST try the records in the order listed, applying the mechanism described in Section 4.1 of RFC 3263 [3] for each. The client only resolves the subsequent domain names if attempts to contact the first one failed or yielded no common transport protocols between client and server or denote a domain administratively prohibited by client policy.

Use of multiple domain names is not meant to replace NAPTR and SRV records, but rather to allow a single DHCP server to indicate outbound proxy servers operated by multiple providers.

Clients MUST support compression according to the encoding in Section 4.1.4 of "Domain Names - Implementation And Specification" [6].

Since the domain names are supposed to be different domains, compression will likely have little effect, however.

If the length of the domain list exceeds the maximum permissible within a single option (254 octets), then the domain list MUST be represented in the DHCP message as specified in [7].

The DHCP option for this encoding has the following format:

```

Code  Len   enc   DNS name of SIP server
+-----+-----+-----+-----+-----+-----+-----+-----+
| 120 |  n   |  0   |  s1 |  s2 |  s3 |  s4 |  s5 |  ...
+-----+-----+-----+-----+-----+-----+-----+-----+

```

As an example, consider the case where the server wants to offer two outbound proxy servers, "example.com" and "example.net". These would be encoded as follows:

```

+-----+-----+-----+-----+-----+-----+-----+-----+
|120|27 |  0 |  7 | 'e'|'x'|'a'|'m'|'p'|'l'|'e'| 3 | 'c'|'o'|'m'| 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+ | 7
| 'e'|'x'|'a'|'m'|'p'|'l'|'e'| 3 | 'n'|'e'|'t'| 0 | +-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+

```

3.2 IPv4 Address List

If the 'enc' byte has a value of 1, the encoding byte is followed by a list of IPv4 addresses indicating SIP outbound proxy servers available to the client. Servers MUST be listed in order of preference.

Its minimum length is 5, and the length MUST be a multiple of 4 plus one. The DHCP option for this encoding has the following format:

```

Code  Len   enc   Address 1           Address 2
+-----+-----+-----+-----+-----+-----+-----+-----+
| 120 |  n   |  1   | a1 | a2 | a3 | a4 | a1 |  ...
+-----+-----+-----+-----+-----+-----+-----+-----+

```

4. Security Considerations

The security considerations in RFC 2131 [1], RFC 2543 [2] and RFC 3263 [3] apply. If an adversary manages to modify the response from a DHCP server or insert its own response, a SIP user agent could be led to contact a rogue SIP server, possibly one that then intercepts call requests or denies service. A modified DHCP answer could also omit host names that translated to TLS-based SIP servers, thus facilitating intercept.

5. IANA Considerations

IANA has assigned a DHCP option number of 120 for the "SIP Servers DHCP Option" defined in this document.

6. Acknowledgements

Ralph Droms, Robert Elz, Wenyu Jiang, Peter Koch, Gautam Nair, Thomas Narten, Erik Nordmark, Jonathan Rosenberg, Kundan Singh, Sven Ubik, Bernie Volz and Dean Willis provided useful feedback through the evolution of this document.

7. Bibliography

- [1] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
- [2] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.
- [3] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.
- [4] Bradner, S., "Key words for use in RFCs to indicate requirement levels", BCP 14, RFC 2119, March 1997.
- [5] Alexander, S. and R. Droms, "DHCP options and BOOTP Vendor Extensions", RFC 2132, March 1997.
- [6] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.
- [7] Lemon, T. and S. Cheshire, "Encoding Long DHCP Options", Work in Progress.

8. Author's Address

Henning Schulzrinne
Dept. of Computer Science
Columbia University
1214 Amsterdam Avenue, MC 0401
New York, NY 10027
USA

EMail: schulzrinne@cs.columbia.edu

9. Full Copyright Statement

Copyright (C) The Internet Society (2002). 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.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

