Network Working Group
Request for Comments: 3319
Category: Standards Track

H. Schulzrinne
Columbia University
B. Volz
Ericsson

July 2003

Dynamic Host Configuration Protocol (DHCPv6) Options 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 (2003). All Rights Reserved.

Abstract

This document defines a Dynamic Host Configuration Protocol version 6 (DHCPv6) option that contains a list of domain names or IPv6 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

This document uses the DHCP terminology defined in [1].

A SIP server is 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 outbound SIP proxy server is running on.

A SIP client is defined in RFC 3261 [2]. 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 BCP 14, 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 two DHCPv6 options [1] that allow 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, such as when firewalls are present, or local dialing plans, local emergency and other services need to be provided, 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 DHCPv6 Option

This document defines two DHCPv6 options that describe a local outbound SIP proxy: one carries a list of domain names (Section 3.1), the other a list of 128-bit (binary) IPv6 addresses (Section 3.2).

> Since DHCPv6 does not suffer from a shortage of option codes, we avoid the encoding byte found in the IPv4 DHCP option for SIP servers [6]. This makes the option shorter, easier to parse, simplifies appropriate word alignment for the numeric addresses and allows the client to request either numeric or domain name options using the "option request option".

An implementation implementing this specification MUST support both options.

3.1 SIP Servers Domain Name List

The option length is followed by a sequence of labels, encoded according to Section 3.1 of RFC 1035 [5], 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 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. Domain names MUST be listed in order of preference.

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

The DHCPv6 option has the format shown in Fig. 1.

option-code: OPTION_SIP_SERVER_D (21)

option-length: Length of the 'SIP Server Domain Name List' field in octets; variable.

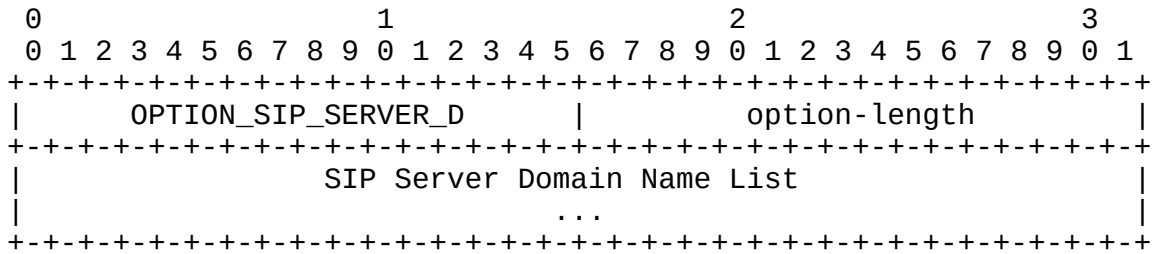
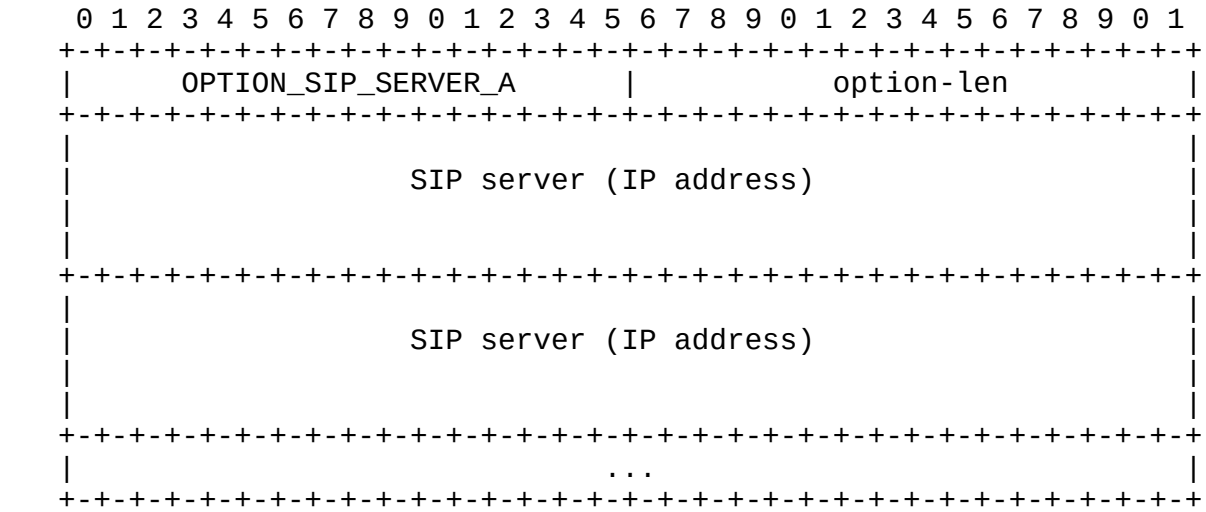


Figure 1: DHCPv6 option for SIP Server Domain Name List

SIP Server Domain Name List: The domain names of the SIP outbound proxy servers for the client to use. The domain names are encoded as specified in Section 8 ("Representation and use of domain names") of the DHCPv6 specification [1].

3.2 SIP Servers IPv6 Address List

This option specifies a list of IPv6 addresses indicating SIP outbound proxy servers available to the client. Servers MUST be listed in order of preference.



option-code: OPTION_SIP_SERVER_A (22)

option-length: Length of the 'options' field in octets; must be a multiple of 16.

SIP server: IPv6 address of a SIP server for the client to use. The servers are listed in the order of preference for use by the client.

4. Client Operation

A client may request either or both of the SIP Servers Domain Name List and SIP Servers IPv6 Address List options in an Options Request Option (ORO) as described in [1],

If a client receives both the SIP Servers Domain Name List and SIP Servers IPv6 Address List options, it SHOULD use the SIP Servers Domain Name List option. Only if no server in the SIP Servers Domain Name List can be resolved or reached, the client MAY use the SIP Servers IPv6 Address List option.

5. Server Operation

A server MAY send a client one or both of the SIP Servers Domain Name List and SIP Servers IPv6 Address List options.

If a client requests both options and the server is configured for both, the server MAY send a client only one of these options and SHOULD send the SIP Servers Domain Name List.

A server configured with the SIP Servers IPv6 Address List option MUST send a client the SIP Servers IPv6 Address List option if that client requested the SIP Servers IPv6 Address List option and not the SIP Servers Domain Name List option in an ORO (see [1]).

The following table summarizes the server's response:

Client sends in ORO	Domain Name List	IPv6 Address List
Neither option	SHOULD	MAY
SIP Servers Domain Name List	SHOULD	MAY
SIP Servers IPv6 Address List	MAY	MUST
Both options	SHOULD	MAY

6. Security Consideration

The security considerations in RFC 3315 [1], RFC 3261 [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.

7. IANA Considerations

The IANA has assigned a DHCPv6 option number of 21 for the "SIP Servers Domain Name List" and the DHCPv6 option number of 22 for the "SIP Servers IPv6 Address List" defined in this document.

8. Acknowledgements

Erik Nordmark and Alex Zinin provided helpful comments.

9. Normative References

[1] Droms, R., Editor, Bounds, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[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] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

10. Informative References

[6] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers," RFC 3361, August 2002.

11. Authors' Addresses

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

EMail: schulzrinne@cs.columbia.edu

Bernie Volz
116 Hawkins Pond Road
Center Harbor, NH 03226-3103
USA

EMail: volz@metrocast.net

12. Full Copyright Statement

Copyright (C) The Internet Society (2003). 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.