

dhc Working Group
Internet Draft
Intended Status: Standards Track
Expires: August 22, 2008

Kim Kinnear
Richard Johnson
Mark Stapp
Jay Kumarasamy
Cisco Systems
February 22, 2008

Virtual Subnet Selection Options for DHCPv4 and DHCPv6
<[draft-ietf-dhc-vpn-option-08.txt](#)>

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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>.

This Internet-Draft will expire on August 22, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

This memo defines a Virtual Subnet Selection (VSS) option for DHCPv4 and DHCPv6, and a DHCPv4 relay-agent-information sub-option. These are intended for use by DHCP clients, relay agents, and proxy clients in situations where VSS information needs to be passed to the DHCP server for proper address or prefix allocation to take place.

For the DHCPv4 option and relay-agent-information sub-option, this memo documents existing usage as per [RFC 3942](#).

Table of Contents

1.	Introduction.....	2
2.	Terminology.....	3
3.	Virtual Subnet Selection Option and Sub-Option Definitions...	4
3.1.	DHCPv4 Virtual Subnet Selection Option.....	5
3.2.	DHCPv4 Virtual Subnet Selection Sub-Option.....	5
3.3.	DHCPv6 Virtual Subnet Selection Option.....	5
3.4.	Virtual Subnet Selection Type and Information.....	6
4.	Relay Agent Behavior.....	7
4.1.	VPN assignment by the DHCP server.....	8
4.2.	DHCP Leasequery.....	9
5.	Client Behavior.....	9
6.	Server Behavior.....	10
6.1.	Returning the DHCPv4 or DHCPv6 Option.....	11
6.2.	Returning the DHCPv4 Sub-Option.....	11
6.3.	Making sense of conflicting VSS information.....	12
7.	Security.....	12
8.	IANA Considerations.....	13
9.	Acknowledgments.....	14
10.	Normative References.....	14
11.	Informative References.....	14
12.	Authors' Addresses.....	15
13.	Full Copyright Statement.....	16
14.	Intellectual Property.....	16
15.	Acknowledgment.....	17

[1.](#) Introduction

There is a growing use of Virtual Private Network (VPN) configurations. The growth comes from many areas; individual client systems needing to appear to be on the home corporate network even when traveling, ISPs providing extranet connectivity for customer companies, etc. In some of these cases there is a need for the DHCP server to know the VPN (hereafter called a "Virtual Subnet Selector" or "VSS") from which an address, and other resources, should be allocated.

This memo defines a Virtual Subnet Selection (VSS) option for DHCPv4 and DHCPv6, and a DHCPv4 relay-agent-information sub-option. These are intended for use by DHCP clients, relay agents, and proxy clients in situations where VSS information needs to be passed to the DHCP server for proper address or prefix allocation to take place. If the

receiving DHCP server understands the VSS option or sub-option, this information may be used in conjunction with other information in determining the subnet on which to select an address as well as other information such as DNS server, default router, etc.

If the allocation is being done through a DHCPv4 relay, then the relay sub-option defined here should be included. In some cases, however an IP address is being sought by a DHCPv4 proxy on behalf of a client (which may be assigned the address via a different protocol). In this case, there is a need to include VSS information relating to the client as a DHCPv4 option.

If the allocation is being done through a DHCPv6 relay, then the DHCPv6 VSS option defined in this document should be included in the Relay-forward and Relay-reply message going between the DHCPv6 relay and server. In some cases, addresses or prefixes are being sought for by a DHCPv6 proxy on behalf of a client. In this case, there is a need for the client itself to supply the VSS information using the DHCPv6 VSS option in the messages that it sends to the DHCPv6 server.

In the remaining text of this document, when a DHCPv6 address is indicated the same information applies to DHCPv6 Prefix Delegation [[RFC 3633](#)] as well.

2. Terminology

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 [RFC 2119](#) [[RFC 2119](#)].

This document uses the following terms:

- o "DHCP client"

A DHCP client is a host using DHCP to obtain configuration parameters such as a network address.

- o "DHCP relay agent"

A DHCP relay agent is a third-party agent that transfers BOOTP and DHCP messages between clients and servers residing on different subnets, per [[RFC 951](#)] and [[RFC 1542](#)].

- o "DHCP server"

A DHCP server is a host that returns configuration parameters to DHCP clients.

- o "DHCPv4 option"

An option or used to implement a capability defined by the DHCPv4 RFCs [[RFC 2131](#)][RFC 2132]. These options have one octet code and size bytes.

- o "DHCPv4 sub-option"

As used in this document, a DHCPv4 sub-option refers to a sub-option of the relay-agent-information option [[RFC 3046](#)]. These sub-options have one octet code and size bytes.

- o "DHCPv6 option"

An option used to implement a capability defined by the DHCPv6 RFC [[RFC 3315](#)]. These options have two octet code and size bytes.

- o "downstream"

Downstream is the direction from the access concentrator towards the subscriber.

- o "upstream"

Upstream is the direction from the subscriber towards the access concentrator.

- o "VSS information"

Information about a VPN necessary to allocate an address to a DHCP client on that VPN and necessary to forward a DHCP reply packet to a DHCP client on that VPN.

- o "VPN"

Virtual private network. A network which appears to the client to be a private network.

- o "VPN Identifier"

The VPN-ID is defined by [[RFC 2685](#)] to be a sequence of 7 octets.

3. Virtual Subnet Selection Option and Sub-Option Definitions

The Virtual Subnet Selection options and sub-option contains a

generalized way to specify the VSS information about a VPN. There are two options and one sub-option defined in this section. The actual VSS information is identical in each.

3.1. DHCPv4 Virtual Subnet Selection Option

The format of the option is:

```

      0                               1                               2                               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Code   |   Length   |   Type   | VSS Info ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Code The option code (221).

Length The option length, minimum 1 octets.

Type and VSS Information -- see [Section 3.4](#)

3.2. DHCPv4 Virtual Subnet Selection Sub-Option

This is a sub-option of the relay-agent-information option [RFC 3046]. The format of the sub-option is:

```

      0                               1                               2                               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Code   |   Length   |   Type   | VSS Info. ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Code The sub-option code (151).

Length The option length, minimum 1 octets.

Type and VSS Information -- see [Section 3.4](#)

3.3. DHCPv6 Virtual Subnet Selection Option

The format of the DHCPv6 Virtual Subnet Selection option is shown below. This option may be included by a client or relay-agent (or

both).

```

      0               1               2               3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|               OPTION_VSS               |               option-len       |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|               Type               | VSS Information ...                   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

option-code OPTION_VSS (TBD).

option-len The number of octets in the option, minimum 1.

Type and VSS Information -- see [Section 3.4](#)

[3.4.](#) Virtual Subnet Selection Type and Information

All of the (sub)options defined above carry identical payloads, consisting of a type and additional VSS information as follows:

Type	VSS Information format:
0	NVT ASCII VPN identifier
1	RFC2685 VPN-ID
2-254	Not Allowed
255	Global, default VPN.

o Type 0 -- NVT ASCII VPN identifier

Indicates that the VSS information consists of a NVT ASCII string. It MUST NOT be terminated with a zero byte.

o Type 1 -- [RFC2685](#) VPN-ID

Indicates that the VSS information consists of an [RFC2685](#) VPN-ID [[RFC 2685](#)], which is defined to be 7 octets in length.

o Type 255 -- Global, default VPN

Indicates that there is no explicit, non-default VSS information

but rather that this option references the normal, global, default address space. In this case, there MUST NOT be any VSS Information and the length of the VSS option MUST be 1.

All other values of the Type field are invalid as of this memo and a VSS option with a Type field containing any value other than zero (0), one (1), or 255 SHOULD be ignored.

4. Relay Agent Behavior

A relay agent which receives a DHCP request from a DHCP client on a VPN should include Virtual Subnet Selection information in the DHCP packet prior to forwarding the packet on to the DHCP server.

A DHCPv4 relay agent SHOULD include a DHCPv4 VSS sub-option in a relay-agent-information option [[RFC 3046](#)], while a DHCPv6 relay agent SHOULD include a DHCPv6 VSS option in the Relay-forward message.

The value placed in the Virtual Subnet Selection sub-option or option SHOULD be sufficient for the relay agent to properly route any DHCP reply packet returned from the DHCP server to the DHCP client for which it is destined.

Since this option or sub-option is placed in the packet in order to change the VPN on which an IP address is allocated for a particular DHCP client, one presumes that an allocation on that VPN is necessary for correct operation. If this presumption is correct, then a relay agent which places this option in a packet and doesn't receive it (or receives a different value than that sent to the server) in the returning packet should drop the packet since the IP address that was allocated will not be in the correct VPN. If an IP address that is not on the requested VPN is not required, then the relay agent is free to accept the IP address that is not on the VPN that was requested.

The converse, however, is more complicated. In the DHCPv6 case, the appearance of the option in the Rely-reply packet does indeed indicate that the DHCPv6 server understood and acted upon the contents of the VSS option in the Relay-forward packet. In the DHCPv4 case, however, the appearance of the sub-option in the relay-agent-information option received by the relay agent does not necessarily indicate that the DHCPv4 server even understood, let alone acted correctly upon, the VSS sub-option that it received.

The reason is that [[RFC 3046](#)] specifies that a DHCPv4 server which supports the relay-agent-information option SHALL copy all sub-options received in a relay-agent-information option into any outgoing relay-agent-information option. Because of these

requirements, even a DHCPv4 server which doesn't implement support for Virtual Subnet Selection sub-option will almost certainly copy it into the outgoing relay-agent-information option. This means that the appearance of the Virtual Subnet Selection sub-option in a relay-agent-information option doesn't indicate support for the Virtual Subnet Selection sub-option.

There are only two pieces of information which can be determined from the appearance or lack of appearance of the DHCPv4 Virtual Subnet Selection sub-option in a relay-agent-information option received by a relay agent from a DHCPv4 server. First, if the Virtual Subnet Selection sub-option does not appear, then the server was able to support this sub-option but chose not to do so. Second, if the Virtual Subnet Selection sub-option appears and has a different value than the one originally included in the relay-agent-information option, then the DHCP server was able to support this sub-option and allocated an address using different VSS information than was originally provided by the relay agent.

Thus, if a DHCPv4 relay agent has a requirement to determine if the address allocated by a DHCPv4 server is on a particular VPN, it must use some other approach than the appearance of the VSS sub-option in the reply packet to make this determination.

This document does not create a requirement that a relay agent remember the contents of a VSS DHCPv4 sub-option or VSS DHCPv6 option sent to a DHCP server. In many cases, the relay agent may simply use the value of the VSS returned by the DHCP server to forward the response to the DHCP client. If the VSS information, the IP address allocated, and the VPN capabilities of the relay agent all interoperate correctly, then the DHCP client will receive a working IP address. Alternatively, if any of these items don't interoperate with the others, the DHCP client will not receive a working address.

Note that in some environments a relay agent may choose to always place a VSS option or sub-option into packets and messages that it forwards in order to forestall any attempt by a downstream relay agent or client to specify VSS information. In this case, a type field of 255 is used to denote the global, default VPN. When the type field of 255 is used, there MUST NOT be any additional VSS Information in the VSS option.

4.1. VPN assignment by the DHCP server

In some cases, a DHCP server may use the Virtual Subnet Selection sub-option or option to inform a relay agent that a particular DHCP client is associated with a particular VPN. It does this by sending the Virtual Subnet Selection sub-option or option with the

appropriate information to the relay agent in the relay-agent-information option for DHCPv4 or the Relay-reply message in DHCPv6. If the relay agent is unable to honor the DHCP server's requirement to place the DHCP client into that VPN it MUST drop the packet and not send it to the DHCP client.

4.2. DHCP Leasequery

Sometimes a relay-agent needs to submit a DHCP Leasequery [[RFC 4388](#)] [[RFC 5007](#)] packet to the DHCP server in order to recover information about existing DHCP allocated IP addresses on other than the normal, global VPN. In the context of a DHCP Leasequery the relay agent is a direct client of the DHCP server and is not relaying a packet for another DHCP client. Thus, the instructions in [Section 5](#) on Client Behavior should be followed to include the necessary VSS information.

5. Client Behavior

A DHCPv4 or DHCPv6 client will employ the VSS option to communicate VSS information to their respective servers. This information MUST be included in every message concerning any IP address on a different VPN than the global or default VPN. A DHCPv4 client will place the DHCPv4 VSS option in its packets, and a DHCPv6 client will place the DHCPv6 VSS option in its messages.

A DHCPv6 client that needs to place a VSS option into a DHCPv6 message SHOULD place a single VSS option into the DHCPv6 message at the same level as the Client Identifier option. A DHCPv6 client MUST NOT include different VSS options in the same DHCPv6 message.

Note that, as mentioned in [Section 1](#), throughout this document when a DHCPv6 address is indicated the same information applies to DHCPv6 Prefix Delegation [[RFC 3633](#)] as well.

Since this option is placed in the packet in order to change the VPN on which an IP address is allocated for a particular DHCP client, one presumes that an allocation on that VPN is necessary for correct operation. If this presumption is correct, then a client which places this option in a packet and doesn't receive it or receives a different value in the returning packet should drop the packet since the IP address that was allocated will not be in the correct VPN. If an IP address that is not on the requested VPN is not required, then the client is free to accept the IP address that is not on the VPN that the was requested.

Client's should be aware that some DHCP servers will return a VSS option with different values than that which was sent in. In addition, a client may receive a response from a DHCP server with a

VSS option when none was sent in by the Client.

Note that when sending a DHCP Leasequery request, a relay agent is acting as a DHCP client and so it should include the respective DHCPv4 or DHCPv6 VSS option in its DHCPv4 or DHCPv6 Leasequery packet if the DHCP Leasequery request is generated for other than the default, global VPN. It should not include a DHCPv4 sub-option in this case.

6. Server Behavior

A DHCP server receiving the VSS option or sub-option SHOULD allocate an IP address (or use the VSS information to access an already allocated IP address) from the VPN specified by the included VSS information.

In the case where the type field of the VSS option or sub-option is 255, the VSS option denotes the global, default VPN. In this case, there is no explicit VSS information beyond the type field.

This document does not prescribe any particular address allocation policy. A DHCP server may choose to attempt to allocate an address using the VSS information and, if this is impossible, to not allocate an address. Alternatively, a DHCP server may choose to attempt address allocation based on the VSS information and, if that is not possible, it may fall back to allocating an address on the global or default VPN. This, of course, is also the apparent behavior of any DHCP server which doesn't implement support for the VSS option and sub-option. Thus, DHCP clients and relay agents SHOULD be prepared for either of these alternatives.

In some cases, a DHCP server may use the Virtual Subnet Selection sub-option or option to inform a relay agent that a particular DHCP client is associated with a particular VPN. It does this by sending the Virtual Subnet Selection sub-option or option with the appropriate information to the relay agent in the relay-agent-information option for DHCPv4 or the Relay-reply message in DHCPv6.

In a similar manner, a DHCP server may use the Virtual Subnet Selection option to inform a DHCP client that the address (or addresses) it allocated for the client is on a particular VPN.

In either case above, care should be taken to ensure that a client or relay agent receiving a reply containing a VSS option will correctly understand the VSS option. Otherwise, the client or relay agent will end up using the address as though it were a global address.

6.1. Returning the DHCPv4 or DHCPv6 Option

DHCPv4 or DHCPv6 servers receiving a VSS option (for sub-option processing, see below) MUST return an instance of this option in the reply packet or message if the server successfully uses this option to allocate an IP address, and it MUST NOT include an instance of this option if the server was unable to or not configured to support the requested VPN.

If they echo the option (based on the criteria above), servers SHOULD return the an exact copy of the option unless they desire to change the VPN on which a client was configured.

6.2. Returning the DHCPv4 Sub-Option

The case of the DHCPv4 sub-option is a bit more complicated. Note that [[RFC 3046](#)] specifies that a DHCPv4 server which supports the relay-agent-information option SHALL copy all sub-options received in a relay-agent-information option into any outgoing relay-agent-information option. Thus, the default behavior for any DHCPv4 server is to return any VSS sub-option received to the relay agent whether or not the DHCPv4 server understand the VSS sub-option. A server which implements the VSS sub-option MUST include the VSS sub-option in the relay-agent-information option in the reply packet if it successfully acted upon the VSS information in the incoming VSS sub-option.

Moreover, if a server uses different VSS information to allocate an IP address than it receives in a particular DHCPv4 sub-option, it MUST include that alternative VSS information in a sub-option that it returns to the DHCPv4 relay agent.

If a DHCPv4 server supports this sub-option and for some reason (perhaps administrative control) does not honor this sub-option from the request then it MUST NOT echo this sub-option in the outgoing relay-agent-information option.

Note that the appearance of the VSS sub-option in a reply packet from a DHCPv4 server to a relay-agent does not communicate any useful information about whether or not the server used the VSS sub-option in its processing. However, the absence of a VSS sub-option in a reply from a DHCPv4 server when a VSS sub-option was included in a request to the DHCPv4 server is significant, and means that the server did not use the VSS information present in the sub-option in its processing.

6.3. Making sense of conflicting VSS information

It is possible for a DHCPv4 server to receive both a VSS option and a VSS sub-option in the same packet. Likewise, a DHCPv6 server can receive multiple VSS options in nested Relay-forward messages as well as in the client message itself. In either of these cases, the VSS information from the relay agent closest to the DHCP server SHOULD be used in preference to all other VSS information received. In the DHCPv4 case, this means that the VSS sub-option takes precedence over the VSS option, and in the DHCPv6 case, this means that the VSS option from the outer-most Relay-forward message in which a VSS option appears takes precedence.

The reasoning behind this approach is that the relay-agent closer to the DHCP server is almost certainly more trusted than the DHCP client or more distant relay agents, and therefore information in the relay-agent-information option or the Relay-forward message is more likely to be correct.

In these situations where multiple VSS option or sub-options appear in the incoming packet or message, when constructing the response to be sent to the DHCP client or relay agent, all existing VSS options or sub-options MUST be replicated in the appropriate places in the response and MUST contain the VSS information that was used by the DHCP server to allocate the IP address.

7. Security

Message authentication in DHCPv4 for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in [RFC 3118]. Potential exposures to attack are discussed in [section 7](#) of the DHCP protocol specification in [RFC 2131].

Implementations should consider using the DHCPv4 Authentication option [RFC 3118] to protect DHCPv4 client access in order to provide a higher level of security if it is deemed necessary in their environment.

Message authentication in DHCPv4 relay agents as defined in [RFC 4030] should be considered for DHCPv4 relay agents employing this sub-option. Potential exposures to attack are discussed in [section 7](#) of the DHCP protocol specification in [RFC 2131].

For DHCPv6 use of the VSS option, the "Security Considerations" section of [RFC 3315] details the general threats to DHCPv6, and thus to messages using the VSS option. The "Authentication of DHCP Messages" section of [RFC 3315] describes securing communication between relay agents and servers, as well as clients and servers.

The VSS option could be used by a client in order to obtain an IP address from a VPN other than the one where it should. This option would allow a client to perform a more complete address-pool exhaustion attack since the client would no longer be restricted to attacking address-pools on just its local subnet.

A DHCP server that implements these options and sub-option should be aware of this possibility and use whatever techniques that can be devised to prevent such an attack. Information such as the giaddr in DHCPv4 or link address in the Relay-forward DHCPv6 message might be used to detect and prevent this sort of attack.

One possible defense would be for the DHCP relay to insert a VSS option or sub-option to override the DHCP client's VSS option.

Servers that implement the VSS option and sub-option MUST by default disable use of the feature; it must specifically be enabled through configuration. Moreover, a server SHOULD provide the ability to selectively enable use of the feature under restricted conditions, e.g., by enabling use of the option only from explicitly configured client-ids, enabling its use only by clients on a particular subnet, or restricting the VSSs from which addresses may be requested.

8. IANA Considerations

IANA is requested to assign DHCPv4 option number 221 for the DHCPv4 VSS option defined in [Section 3.1](#), in accordance with [\[RFC 3942\]](#).

IANA is requested to assign sub-option number 151 for the DHCPv4 sub-option defined in [Section 3.2](#) from the DHCP Relay Agent Sub-options space [\[RFC 3046\]](#), in accordance with the spirit of [\[RFC 3942\]](#). While [\[RFC 3942\]](#) doesn't explicitly mention the sub-option space for the DHCP Relay Agent Information option [\[RFC 3046\]](#), sub-option 151 is already in use by existing implementations of this sub-option and the current draft is essentially compatible with these current implementations.

IANA has assigned the value of TBD for the DHCPv6 VSS option defined in [Section 3.3](#).

While the type byte defined in [Section 3.4](#) defines a number space that could be managed by IANA, expansion of this number space is not anticipated and so creation of a registry of these numbers is not required by this document. In the event that additional values for the type byte are defined in subsequent documents, IANA should at that time create a registry for these type bytes. New values for the type byte may only be defined by IETF Consensus, as described in [\[RFC 2434\]](#). Basically, this means that they are defined by RFCs

approved by the IESG.

9. Acknowledgments

Bernie Volz recommended consolidation of the DHCPv4 option and sub-option drafts after extensive review of the former drafts, and provided valuable assistance in structuring and reviewing this document. Alper Yegin expressed interest in the DHCPv6 VSS option, resulting in this combined draft covering all three areas.

10. Normative References

- [RFC 2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997.
- [RFC 2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [RFC 2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), March 1997.
- [RFC 2685] Fox, B., Gleeson, B., "Virtual Private Networks Identifier", [RFC 2685](#), September 1999.
- [RFC 3046] Patrick, M., "DHCP Relay Agent Information Option", [RFC 3046](#), January 2001.
- [RFC 3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC 3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", [RFC 3633](#), December 2003.

11. Informative References

- [RFC 951] Croft, B. and J. Gilmore, "Bootstrap Protocol", [RFC 951](#), September 1985.
- [RFC 1542] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", [RFC 1542](#), October 1993.
- [RFC 2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997.

- [RFC 2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 1998.
- [RFC 3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", [RFC 3118](#), June 2001.
- [RFC 3942] Volz, B., "Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options", [RFC 3942](#), November 2004.
- [RFC 4030] Stapp, M. and T. Lemon, "The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option", [RFC 4030](#), March 2005.
- [RFC 4388] Woundy, R. and K. Kinneer, "Dynamic Host Configuration Protocol (DHCP) Leasequery", [RFC 4388](#), February 2006.
- [RFC 5007] Brzozowski, J., Kinneer, K., Volz, B., and S. Zeng, "DHCPv6 Leasequery", [RFC 5007](#), September 2007.

12. Authors' Addresses

Kim Kinneer
Cisco Systems
1414 Massachusetts Ave.
Boxborough, Massachusetts 01719

Phone: (978) 936-0000

EMail: kkinneer@cisco.com

Richard Johnson
Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134

Phone: (408) 526-4000

EMail: raj@cisco.com

Mark Stapp
Cisco Systems
1414 Massachusetts Ave.
Boxborough, Massachusetts 01719

Phone: (978) 936-0000

EMail: mjs@cisco.com

Jay Kumarasamy
Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134

Phone: (408) 526-4000

EMail: jayk@cisco.com

13. Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

14. Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at

<http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

15. Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).