

dhc Working Group  
Internet Draft  
Intended Status: Standards Track  
Expires: June 18, 2008

Kim Kinnear  
Mark Stapp  
Richard Johnson  
Jay Kumarasamy  
Cisco Systems  
December 18, 2007

**Virtual Subnet Selection Sub-Option  
for the Relay Agent Information Option for DHCPv4  
<[draft-ietf-dhc-agent-vpn-id-06.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 May 16, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

In some environments, a relay agent resides in a network element which also has access to one or more virtual private networks (VPNs). If a DHCP server wishes to offer service to DHCP clients on those different VPNs the DHCP server needs to know information about the VPN on which each client resides. The Virtual Subnet Selection sub-

option of the relay-agent-information option is used by the relay agent to tell the DHCP server important information about the VPN (called the Virtual Subnet Selection information, or VSS) for every DHCP request it passes on to the DHCP server, and is also used to properly forward any DHCP reply that the DHCP server sends back to the relay agent.

## **1. Introduction**

There exist situations where there are multiple VPNs serviced by one or more network elements which also contain relay agents. These VPNs contain DHCP clients, and there is a desire to allow a DHCP server to supply the full range of DHCP services to these DHCP clients.

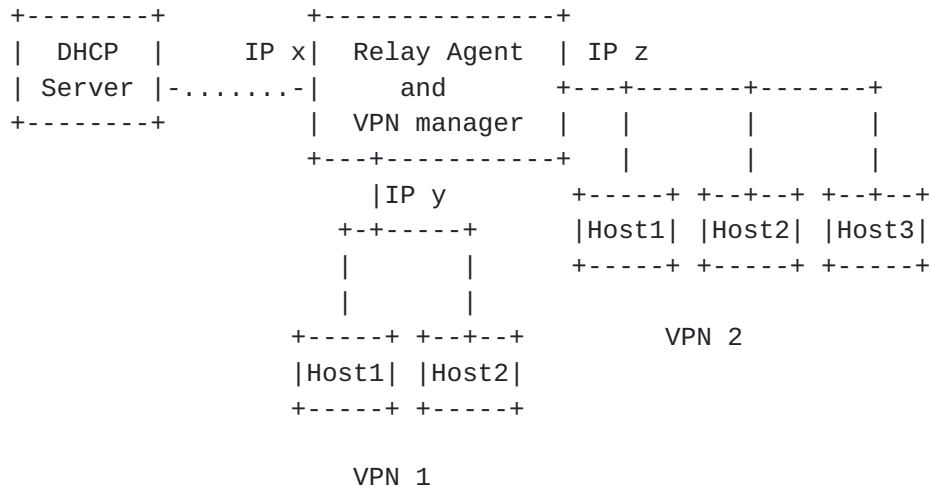
The network element which contains the relay agent typically is also the network element which knows about the VPN association of the DHCP client and could include information about the VPN in the relay-agent-information option in the client's DHCP requests. This information about the VPN is called the Virtual Subnet Selection information, or VSS information. This document defines a sub-option for the relay-agent-information option which contains this VSS information, and which allows the relay agent to communicate the VSS information to the DHCP server.

When the DHCP server sends its response to the relay agent for forwarding back to the DHCP client, the relay agent will also need to use the Virtual Subnet Selection sub-option to determine to which VPN to send the DHCP response.

This sub-option can also be used by the DHCP server to inform a relay agent that a particular DHCP client is associated with a particular VPN by sending the Virtual Subnet Selection sub-option in the relay-agent-information option back to the relay agent.



Consider the following architecture:



In this architecture, the relay agent knows the VPN for each of the DHCP clients, and inserts the VSS information about the VPN in the Virtual Subnet Selection sub-option in every DHCP request it forwards on to the DHCP server.

When the DHCP server copies the relay-agent-information option from the incoming packet into the server's reply packet, it will copy over the Virtual Subnet Selection sub-option as well.

When the relay agent receives a DHCP reply packet from the server with a Virtual Subnet Selection sub-option, it will forward the packet onto the proper VPN based on the VSS information in the Virtual Subnet Selection sub-option.

## 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 "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 Sub-Option Definition**

The Virtual Subnet Selection sub-option MAY be used by any DHCP relay agent which desires to specify the VSS information about a VPN from which a DHCP client request was sent.

The Virtual Subnet Selection sub-option contains a generalized way to specify the VSS information about a VPN.

The format of the option is:



SubOpt	Len	Type	VPN identifier			
+-----+	+-----+	+-----+	+-----+	+-----+	+-----+	+-----+
TBD	n	t	id1	id2	id3	...
+-----+	+-----+	+-----+	+-----+	+-----+	+-----+	+-----+

Type:	0	NVT ASCII VPN identifier
	1	<a href="#">RFC2685</a> VPN-ID
	2-255	Not Allowed

There are two types of identifiers which can be placed in the Virtual Subnet Selection sub-option. The first type of identifier which can be placed in the Virtual Subnet Selection sub-option is an NVT ASCII string. It MUST NOT be terminated with a zero byte.

The second type of identifier which can be placed in the Virtual Subnet Selection sub-option is an [RFC2685](#) VPN-ID [[RFC 2685](#)], which is defined to be 7 octets in length.

All other values of the type field are invalid as of this memo and VSS sub-options containing any other value than zero (0) or one (1) SHOULD be ignored.

A relay agent which receives a DHCP request from a DHCP client on a VPN SHOULD include a Virtual Subnet Selection sub-option in the relay-agent-information option that it inserts in the DHCP packet prior to forwarding it on to the DHCP server.

The value placed in the Virtual Subnet Selection sub-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. Servers supporting this sub-option MUST return an instance of this sub-option in the relay-agent-information option to any relay-agent that sends it if the server successfully uses this sub-option to allocate the IP address and SHOULD NOT include this sub-option in the relay-agent-information option if the server was unable or not configured to support the requested VPN. If they echo the sub-option, servers SHOULD return the an exact copy of the sub-option unless they desire to change the VPN on which a client was configured, which would typically be a very unusual thing to do.

In the event that a Virtual Subnet Selection option and a Virtual Subnet Selection sub-option are both received in a particular DHCP client packet, the information from the Virtual Subnet Selection sub-option MUST be used in preference to the information in the





Virtual Subnet Selection option. This reasoning behind this approach is that the relay-agent is almost certainly more trusted than the DHCP client, and therefore information in the relay-agent-information option that conflicts with information in the packet generated by the DHCP client is more likely to be correct.

Note that [[RFC 3046](#)] specifies that a DHCP server which supports the relay-agent-information option SHALL copy all suboptions received in a relay-agent-information option into any outgoing relay-agent-information option. In the case of the Virtual Subnet Selection sub-option, if the server supports this sub-option and for some reason (perhaps administrative control) does not honor this sub-option from the request then it SHOULD NOT echo this sub-option in the outgoing relay-agent-information option.

Because of the requirements of [[RFC 3046](#)], even a 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.

The only information which can be determined from the appearance or lack of appearance of the Virtual Subnet Selection sub-option in a relay-agent-information option received by a relay agent from a DHCP server is that 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.

Since this 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. The relay agent may choose to try to determine whether or not the IP address that was allocated was from the correct VPN (and drop the packet if it was not) or to simply pass the packet along to the DHCP client and let the client operate to the extent possible.

In some cases, a DHCP server may use the Virtual Subnet Selection sub-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 with the appropriate information to the relay agent in the relay-agent-information option. 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.

This sub-option SHOULD NOT be used without also making use of some form of authentication for relay-agent-information option.



While this sub-option is the way that a relay-agent can insert VPN information into a DHCP client packet that it is forwarding, when a relay-agent needs to submit a DHCP Leasequery packet to the DHCP server in order to recover information about existing DHCP allocated IP addresses on other than the normal, global VPN, it SHOULD NOT use this sub-option. Instead, it SHOULD use the Virtual Subnet Selection option, since in the context of a DHCP Leasequery the relay agent is the client and is not relaying a packet for another DHCP client.

#### **4. Security**

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

The Virtual Subnet Selection sub-option could be used by a DHCP client masquerading as a relay agent in order to obtain an IP address from a VPN other than the one on which it resides. The DHCP server processing for this sub-option should be aware of this possibility and use whatever techniques it can devise to prevent such an attack. Information such as the giaddr might be used to detect and prevent this sort of attack, as well as the use of The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option [\[RFC 4030\]](#).

Any program which unicasts a DHCP packet to the DHCP server with a relay-agent-information option in it with a vpn-id for a different VPN would cause the DHCP server to allocate an address from that different VPN, but since the DHCP server cannot (in general) communicate directly back to the program that sent in the malicious DHCP packet, the entire cycle of creating a lease will not be completed. Certainly many leases could be offered, which would result in a temporary form of address-pool exhaustion.

Servers that implement the Virtual Subnet Selection 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 VPNs from which addresses may be requested.

#### **5. IANA Considerations**

IANA is requested to assign sub-option number 151 for this sub-option in 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, 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 VPN Identifier sub-option from the DHCP Relay Agent Sub-options space [\[RFC 3046\]](#) for the VPN Identifier sub-option defined in [Section 3](#).

While the type byte of the Virtual Subnet Selection sub-option 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.

Moreover, any changes or additions to the type byte codes MUST be made concurrently in the type byte codes of the Virtual Subnet Selection option. The type bytes and data formats of the Virtual Subnet Selection option and Virtual Subnet Selection sub-option MUST always be identical.

## **[6.](#) Acknowledgments**

None.

## **[7.](#) Normative 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 2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), 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 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 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.

## **8. Authors' Addresses**

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

Phone: (978) 936-0000

EMail: [kkinnear@cisco.com](mailto:kkinnear@cisco.com)

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

Phone: (408) 526-4000

EMail: [raj@cisco.com](mailto:raj@cisco.com)

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

Phone: (978) 936-0000

EMail: [mjs@cisco.com](mailto:mjs@cisco.com)





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

Phone: (408) 526-4000

EMail: jayk@cisco.com

## **9. Full Copyright Statement**

Copyright (C) The IETF Trust (2007).

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.

## **10. 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](mailto:ietf-ipr@ietf.org).

## **11. Acknowledgment**

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