

February 2005
Expires July 2005

**Virtual Subnet Selection Sub-Option
for the Relay Agent Information Option**
<[draft-ietf-dhc-agent-vpn-id-03.txt](#)>

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

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/1id-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

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 one 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

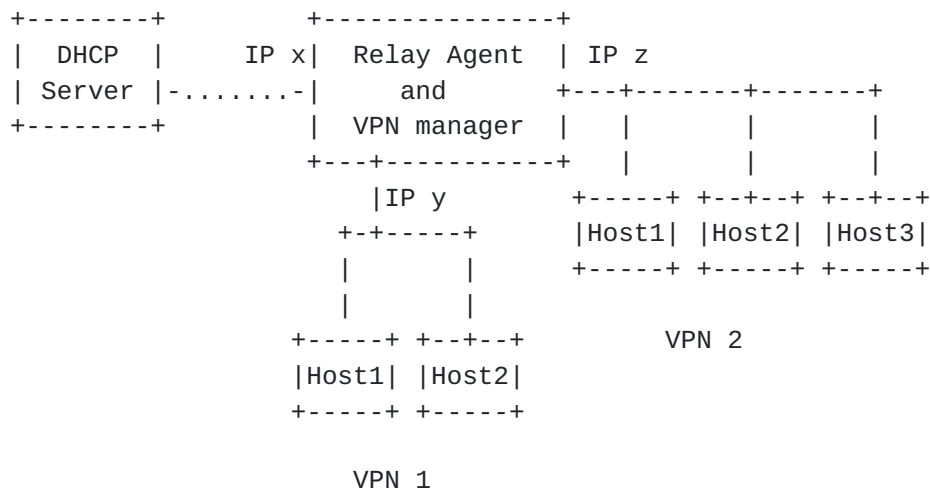
There exist situations where there are multiple VPNs serviced by one or more network elements which also contain relay agents. These VPNs contain DHCP clients, and there is a desire to allow one DHCP server to supply the full range of DHCP services to these DHCP clients.

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 over the relay-agent-information option from the request to the 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.

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 an Internet 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 an Internet 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 [[RFC2685](#)] to be a sequence of 14 hex digits.

### **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 typically 14 hex digits in length (though it can be any length as far as the virtual-subnet-selection sub-option is concerned).

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-info option to any relay-agent that sends it. 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.





Relay agents which include this sub-option when forwarding DHCP client requests MUST discard DHCP OFFER or DHCP ACK packets that do not contain this sub-option in their associated relay-agent-info options. This does not imply any memory of the particular packets forwarded with this sub-option included. Rather, the expectation is that the relay agent will use whatever algorithm that it used on the DHCP DISCOVER and DHCP REQUEST packets to decide to include this sub-option on the DHCP OFFER and DHCP ACK packets to decide if they MUST have this sub-option included in their relay-agent-info options.

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.

#### **4. Security**

Message authentication in DHCP 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].

The virtual-subnet-selection sub-option could be used by a client in order to obtain an IP address from a VPN other than the one on which it resides. This attack can be partially prevented by the relay agent not forwarding any DHCP packet which already contains a relay-agent-information option.

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 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](#).

This document defines a number space for the type byte of the virtual-subnet-selection sub-option. Certain allowable values for this byte are defined in this specification (see [Section 3](#)). New values 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 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., Droms, R., "DHCP Options and BOOTP Vendor Extensions", Internet [RFC 2132](#), March 1997.
- [RFC 2685] Fox, B., Gleeson, B., "Virtual Private Networks Identifier", Internet [RFC 2685](#), September 1999.
- [RFC 3046] Patrick, M., "DHCP Relay Agent Information Option", [RFC 3046](#), January 2001.
- [RFC 3118] Droms, R. "Authentication for DHCP Messages", [RFC 3118](#),



June 2001.

## **8. Author's information**

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

Phone: (978) 936-0000

EMail: kkinnear@cisco.com  
mjs@cisco.com

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

Phone: (408) 526-4000

EMail: jayk@cisco.com  
raj@cisco.com

## **9. Intellectual Property Statement**

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this



standard. Please address the information to the IETF Executive Director.

#### **10. Full Copyright Statement**

Copyright (C) The Internet Society (2005). 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 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.



