Internet Engineering Task Force (IETF)
Request for Comments: 6607
Updates: 3046
Category: Standards Track
ISSN: 2070-1721

K. Kinnear
R. Johnson
M. Stapp
Cisco Systems

April 2012

Virtual Subnet Selection Options for DHCPv4 and DHCPv6

Abstract

This memo defines a DHCPv4 Virtual Subnet Selection (VSS) option, a DHCPv6 VSS option, and the DHCPv4 VSS and VSS-Control sub-options carried in the DHCPv4 Relay Agent Information 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-options, this memo documents and extends existing usage as per RFC 3942. This memo updates RFC 3046 regarding details relating to the copying of sub-options (see Section 8).

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6607.

Table of Contents

1. Introduction

There is a growing use of Virtual Private Network (VPN) configurations. This 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 (also called a "Virtual Subnet Selector" or "VSS" in this document) from which an address, and other resources, should be allocated.

This memo defines a DHCPv4 Virtual Subnet Selection (VSS) option, a DHCPv6 VSS option, and two VSS sub-options carried in the DHCPv4 Relay Agent Information 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-options, 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 Agent Information sub-options 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 messages going between the DHCPv6 relay and server. In some cases, addresses or prefixes are being sought 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 [RFC3633] as well.

In the remaining text of this document, when the term "VSS sub-option" is used, it refers to the VSS sub-option carried in the DHCPv4 Relay Agent Information 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 [RFC2119].

This document uses the following terms:

- DHCP client

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

- DHCP proxy

  A DHCP proxy is a DHCP client that acquires IP addresses not for its own use but rather on behalf of another entity. There are a variety of ways that a DHCP proxy can supply the addresses it acquires to other entities that need them.

- DHCP relay agent

  A DHCP relay agent is an agent that transfers BOOTP and DHCP messages between clients and servers residing on different subnets, per [RFC951], [RFC1542], and [RFC3315].

- DHCP server

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

- DHCPv4 option

  A DHCPv4 option is an option used to implement a capability defined by the DHCPv4 RFCs ([RFC2131] [RFC2132]). This option has one-octet code and size fields.

- DHCPv4 sub-option

  As used in this document, a DHCPv4 sub-option refers to a sub-option of the Relay Agent Information option [RFC3046]. This sub-option has one-octet code and size fields.

- DHCPv6 option

  A DHCPv6 option is an option used to implement a capability defined by the DHCPv6 RFC [RFC3315]. This option has two-octet code and size fields.

- Global VPN

  This term indicates that the address being described belongs to the set of addresses not part of any VPN -- in other words, the normal address space operated on by DHCP. This includes private addresses -- for example, the 10.x.x.x addresses as well as the other private subnets that are not routed on the open Internet.

- NVT ASCII identifier

  A Network Virtual Terminal (NVT) identifier is an identifier containing only characters from the ASCII repertoire and using the Network Virtual Terminal encoding (see Appendix B of [RFC5198]).

- VSS information

  VSS information provides 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.

- VPN

  This term refers to a virtual private network. A VPN appears to the client to be a private network.

- VPN identifier

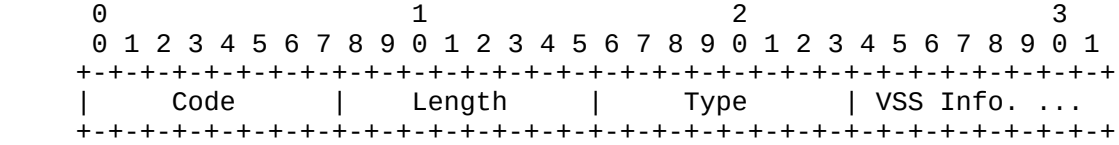
  The VPN-ID is defined by [RFC2685] to be a sequence of 7 octets.

3. Virtual Subnet Selection Options and Sub-Options: Definitions

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

3.1. DHCPv4 Virtual Subnet Selection Option

The format of the option is shown below.



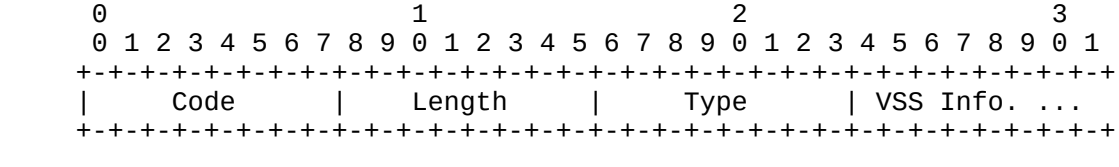
Code The option code (221).

Length The option length, minimum 1 octet.

Type and VSS Information -- see Section 3.5.

3.2. DHCPv4 Virtual Subnet Selection Sub-Option

This is a sub-option of the Relay Agent Information option [RFC3046]. The format of the sub-option is shown below.



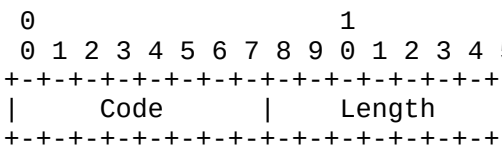
Code The sub-option code (151).

Length The sub-option length, minimum 1 octet.

Type and VSS Information -- see Section 3.5.

3.3. DHCPv4 Virtual Subnet Selection Control Sub-Option

This is a sub-option of the Relay Agent Information option [RFC3046]. The format of the sub-option is shown below.



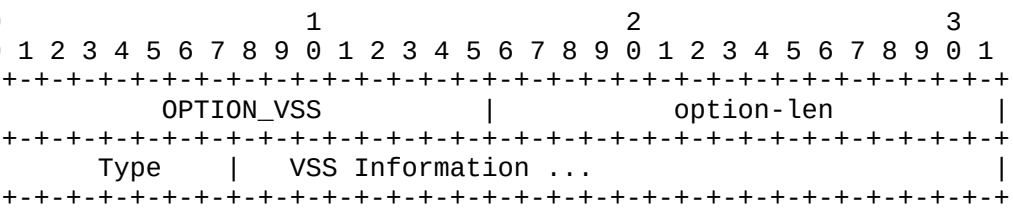
Code The sub-option code (152).

Length The sub-option length, 0.

This sub-option only appears in the DHCPv4 Relay Agent Information option. In a DHCP request, it indicates that a DHCPv4 VSS sub-option is also present in the Relay Agent Information option. In a DHCP reply, if it appears in the Relay Agent Information option, it indicates that the DHCP server did not understand any DHCPv4 VSS sub-option that also appears in the Relay Agent Information option.

3.4. DHCPv6 Virtual Subnet Selection Option

The format of the DHCPv6 VSS option is shown below. This option may be included by a client or relay agent (or both).



option-code OPTION_VSS (68).

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

Type and VSS Information -- see Section 3.5.

3.5. Virtual Subnet Selection Type and Information

All of the (sub-)options defined above that carry VSS information use identical payloads consisting of a Type value and additional VSS information, as follows:

Type	VSS Information Format
0	Network Virtual Terminal (NVT) ASCII VPN identifier
1	RFC 2685 VPN-ID
2-254	Unassigned
255	Global, default VPN

- Type 0 -- Network Virtual Terminal (NVT) ASCII VPN identifier

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

- Type 1 -- RFC 2685 VPN-ID

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

- 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 included in the VSS option or sub-option, and the length of the option or sub-option MUST be 1.

All other values of the Type field are unassigned.

4. Overview of Virtual Subnet Selection Usage

At the highest level, the VSS option or sub-option determines the VPN on which a DHCP client is supposed to receive an IP address. How the option or sub-option is entered and processed is discussed below, but the point of all of the discussion is to determine the VPN on which the DHCP client resides. This will affect a relay agent, in that it will have to ensure that DHCP packets sent to and received from the DHCP client flow over the correct VPN. This will affect the DHCP server in that it determines the IP address space used for the IP address allocation.

A DHCP server has as part of its configuration some IP address space from which it allocates IP addresses to DHCP clients. These allocations are typically for a limited time, and thus the DHCP client gets a lease on the IP address. In the absence of any VPN information, the IP address space is in the global or default VPN used throughout the Internet. When a DHCP server deals with VPN information, each VPN defines a new address space inside the server, one distinct from the global or default IP address space. A server that supports the VSS option or sub-option thereby supports allocation of IP addresses from multiple different VPNs. Supporting IP address allocation from multiple different VPNs means that the DHCP server must be prepared to configure multiple different address spaces (one per distinct VPN) and allocate IP addresses from these different address spaces.

These address spaces are typically independent, so that the same IP address (consisting of the same string of bytes) could be allocated to one client in the global, default VPN, and to a different client residing in a different VPN. There is no conflict in this allocation, since the clients have essentially different addresses, even though these addresses consist of the same string of bytes, because the IPv4 or IPv6 address is qualified by the VPN.

Thus, a VSS option or sub-option is a way of signaling the use of a VPN other than the global or default VPN. This brings up the question of who decides what VPN a DHCP client should be using.

There are three entities that can insert either a VSS option or sub-option into a DHCPv4 packet or DHCPv6 message: a DHCP client, a relay agent, or a DHCPv4 or DHCPv6 server. While all of these entities could include a different VSS option or sub-option in every request or response, this situation is neither typical nor useful. There are two known paradigms for use of the VSS option or sub-option; these are discussed below.

4.1. VPN Assignment by the DHCP Relay Agent

The typical use of the VSS option or sub-option is for the relay agent to know the VPN on which the DHCP client is operating. The DHCP client itself does not, in this approach, know the VPN on which it resides. The relay agent is responsible for mediating the access between the VPN on which the DHCP client resides and the DHCP server. In this situation, the relay agent will insert two DHCPv4 Relay Agent Information sub-options (one VSS sub-option, and one VSS-Control sub-option) into the Relay Agent Information option, or a DHCPv6 VSS option into the Relay-forward message of every request it

forwards from the DHCP client. The server will use the DHCPv6 VSS option or DHCPv4 VSS sub-option to determine the VPN on which the client resides and will use that VPN information to select the address space within its configuration from which to allocate an IP address to the DHCP client.

When, using this approach, a DHCPv4 relay agent inserts a VSS sub-option into the Relay Agent Information option, it MUST also insert a VSS-Control sub-option into the Relay Agent Information option. This is to allow the determination of whether or not the DHCPv4 server actually processes the VSS information provided by the DHCPv4 relay agent. If the DHCPv4 server supports the VSS capabilities described in this document, it will remove the VSS-Control sub-option from the Relay Agent Information option that it returns to the DHCPv4 relay agent. See Section 5 for more information.

In this approach, the relay agent might also send a VSS option or sub-option in either a DHCPv4 or DHCPv6 Leasequery request [RFC4388] [RFC5007], but in this case, it would use the VSS option in the Leasequery request to select the correct address space for the Leasequery. In this approach, the relay agent would be acting as a DHCP client from a leasequery standpoint, but it would not be as if a DHCP client were sending in a VSS option in a standard DHCP address allocation request, say a DHCPDISCOVER.

In this approach, only one relay agent would mediate the VPN access for the DHCP client to the DHCP server, and it would be the relay agent that inserts the VSS information into the request packet and that would remove it prior to forwarding the response packet.

The diagram below shows an example of a DHCPv4 client, DHCPv4 relay agent, and DHCPv4 server. The DHCPv6 situation is similar but uses the DHCPv6 VSS option.

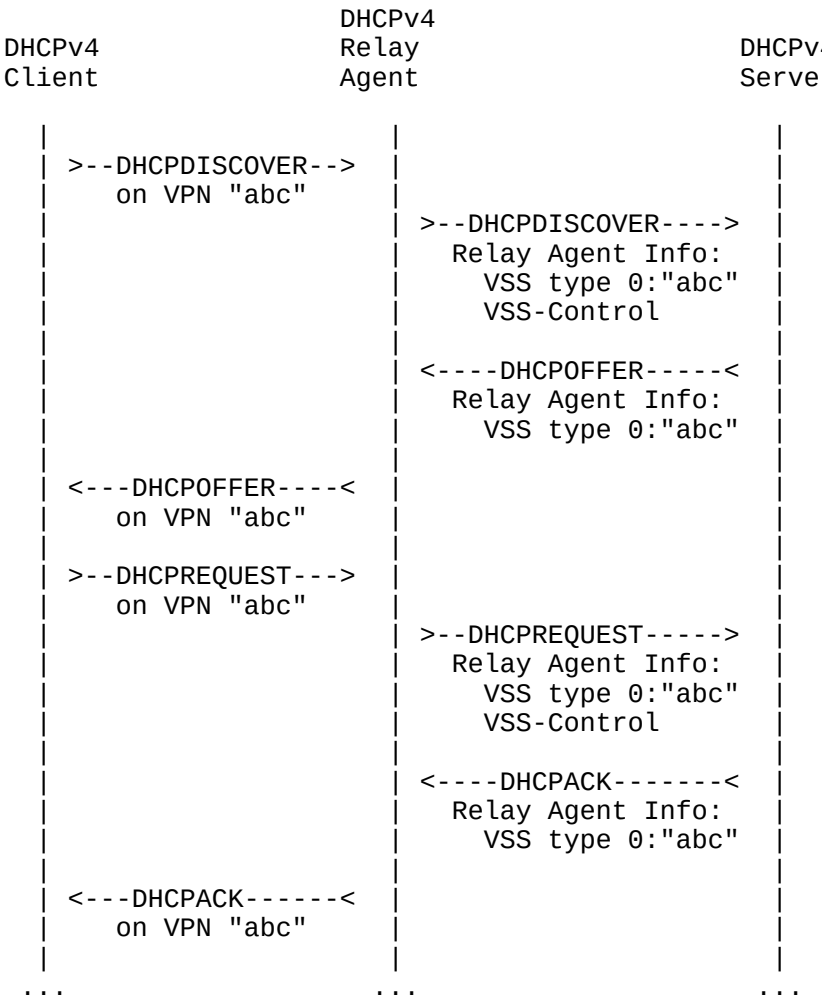


Figure 4.1-1: DHCPv4 - Relay Agent Knows VPN

The DHCP server would know that it should respond to VPN information specified in a VSS option or sub-option, and it would be configured with appropriate VPN address spaces to service the projected client requirements. Thus, in this common approach, the DHCP client knows nothing of any VPN access, the relay agent has been configured in some way that allows it to determine the VPN of the DHCP client and transmit that using a VSS option or sub-option to the DHCP server,

and the DHCP server responds to the VPN specified by the relay agent. There is no conflict between different entities trying to specify different VSS information -- each entity knows its role through policy or configuration external to this document.

If any misconfiguration exists, it SHOULD result in a DHCP client being unable to acquire an IP address. For instance, a relay agent that supports VPN access SHOULD couple transmission of VSS options or sub-options to the configuration of VPN support and not allow one without the other.

It is important to ensure that the relay agent and DHCP server both support the VSS option and sub-options (for DHCPv4) or the VSS option (for DHCPv6). Deploying DHCPv4 relay agents that support and emit VSS sub-options in concert with DHCPv4 servers that do not support the VSS option or sub-option as defined in this document SHOULD NOT be done, as such an ensemble will not operate correctly. Should this situation occur, however, the relay agent can detect the problem (since the VSS-Control sub-option will appear in the packets it receives from the DHCPv4 server, indicating the server did not effectively process the VSS sub-option), and it can issue appropriate diagnostic messages.

4.2. VPN Assignment by the DHCP Server

In this approach, the DHCP server would be configured in some way to know the VPN on which a particular DHCP client should be given access. The DHCP server would in this case include the VSS sub-option in the Relay Agent Information option for DHCPv4 or the VSS option in the Relay-reply message for DHCPv6. The relay agent responsible for mediating VPN access would use this information to select the correct VPN for the DHCP client. In the unusual event that there were more than one relay agent involved in this transaction, some external configuration or policy would be needed to inform the DHCPv6 server into which Relay-reply message the VSS option should go.

Once the relay agent has placed the DHCP client into the proper VPN, it SHOULD begin including VSS information in requests that it forwards to the DHCP server. Since this information does not conflict with the DHCP server’s idea of the proper VPN for the client, everything works correctly.

The diagram below shows this approach using DHCPv4. The DHCPv6 situation is similar but uses the DHCPv6 VSS option instead.

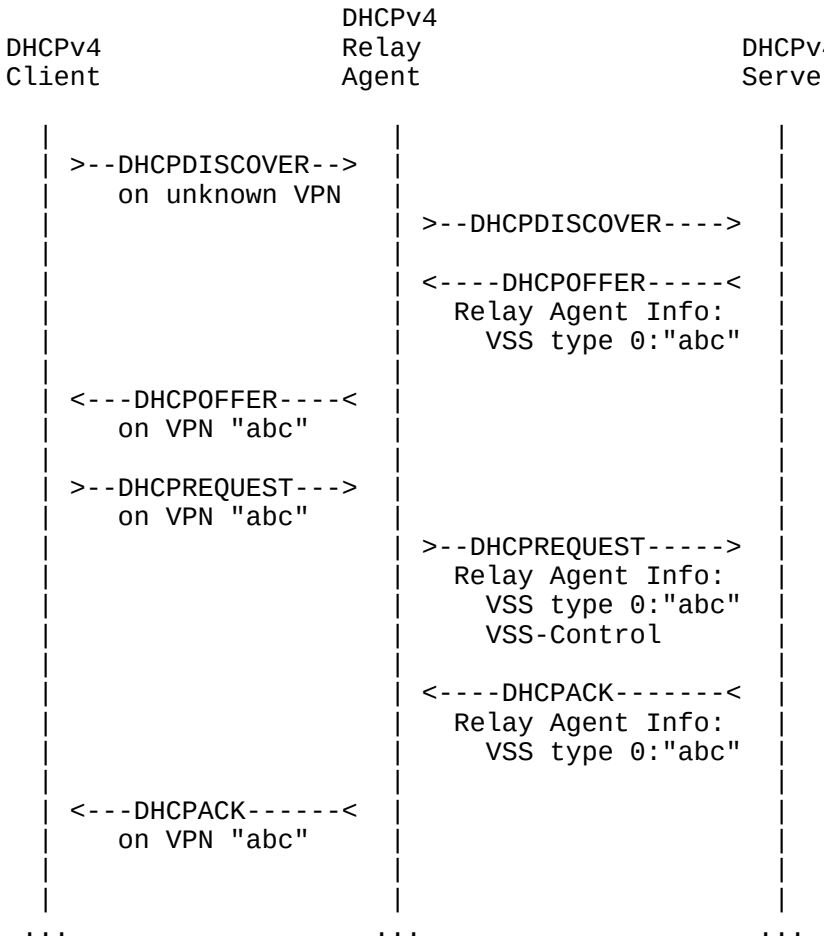


Figure 4.2-1: DHCPv4 - DHCPv4 Server Knows VPN

In this approach, the DHCP client is again unaware of any VPN activity. In this case, however, the DHCP server knows the VPN for the client, and the relay agent responds to the VSS information specified by the DHCP server. Similar to the previous approach, each entity knows its role through a means external to this document, and no two entities try to specify VSS information in conflict.

It is important that both the relay agent and the DHCP server support the VSS option and sub-options (for DHCPv4) and the VSS option (for DHCPv6). Deploying and configuring VPN support in one element and not in the other is not a practical approach.

4.3. Required Support

DHCP relay agents and servers MUST support the approach discussed in Section 4.1. DHCP relay agents and servers SHOULD support the approach discussed in Section 4.2. DHCP relay agents and servers SHOULD NOT be configured to operate with both approaches simultaneously.

4.4. Alternative VPN Assignment Approaches

There are many other approaches that can be created with multiple relay agents each inserting VSS information into different Relay-forward messages, relay agent VSS information conflicting with client VSS information, or DHCP server VSS information conflicting with relay agent and client VSS information. Since these approaches do not describe situations that are useful today, specifying precisely how to resolve all of these conflicts is not likely to be valuable in the event that these approaches actually become practical in the future.

The current use of the VSS option and sub-option requires that each entity know the part that it plays in dealing with VPN data. Each entity -- client, relay agent or agents, and server -- SHOULD know through some policy or configuration beyond the scope of this document whether it is responsible for specifying VPN information using the VSS option or sub-option or responsible for responding to VSS information specified by another entity, or whether it should simply ignore any VSS information that it might see.

Some simple conflict-resolution approaches are discussed below, in the hopes that they will cover simple cases that may arise from situations beyond those envisioned today. However, for more complex situations, or simple situations where appropriate conflict-resolution strategies differ from those discussed in this document, a document detailing the usage situations and appropriate conflict-resolution strategies SHOULD be created and submitted for discussion and approval.

5. Relay Agent Behavior

Implementers MAY provide a policy or configuration capability to enable or disable VSS support.

A relay agent that receives a DHCP request from a DHCP client on a VPN SHOULD include VSS information in the DHCP packet prior to forwarding the packet to the DHCP server unless inhibited from doing so by configuration information or policy to the contrary.

In this situation, a DHCPv4 relay agent MUST include a DHCPv4 VSS sub-option in a Relay Agent Information option [RFC3046], while a DHCPv6 relay agent MUST include a DHCPv6 VSS option in the Relay-forward message.

The value placed in the VSS sub-option or option would typically 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. In some cases, the information in the VSS sub-option or option might be an index to some internal table held in the relay agent, though this document places no requirement on a relay agent to have any such internal state.

A DHCPv4 relay agent MUST, in addition, include a DHCPv4 VSS-Control sub-option (which has a length of zero) in the Relay Agent Information option [RFC3046] whenever it includes a VSS sub-option in the Relay Agent Information option. The inclusion of the VSS sub-option and the VSS-Control sub-option in the Relay Agent Information option will allow the DHCPv4 relay agent to determine whether the DHCPv4 server actually processed the information in the VSS sub-option when it receives the Relay Agent Information option in the reply from the DHCPv4 server.

The reason to include this additional VSS DHCPv4 sub-option is that [RFC3046] specifies (essentially) that a DHCPv4 server should copy all sub-options that it receives in a Relay Agent Information option in a request into a corresponding Relay Agent Information option in the response. Thus, a server that didn't support the DHCPv4 VSS sub-option would normally just copy it to the response packet, leaving the relay agent to wonder if in fact the DHCPv4 server actually used the VSS information when processing the request.

To alleviate this potential confusion, a DHCPv4 relay agent instead sends in two sub-options: one VSS sub-option, and one VSS-Control sub-option. If both sub-options appear in the response from the DHCPv4 server, then the DHCPv4 relay agent MUST assume that the DHCPv4 server did not act on the VSS information in the VSS sub-option. If only the VSS sub-option appears in the response from

the DHCPv4 server and no VSS-Control sub-option appears in the response from the DHCPv4 server, then the relay agent SHOULD assume that the DHCPv4 server acted successfully on the VSS sub-option.

Any time a relay agent places a VSS option or sub-option in a DHCP request, it SHOULD send it only to a DHCP server that supports the VSS option or sub-option, and it MUST check the response to determine if the DHCP server actually honored the requested VSS information.

In the DHCPv6 case, the appearance of the option in the Relay-reply packet indicates that the DHCPv6 server understood and acted upon the contents of the VSS option in the Relay-forward packet. In the DHCPv4 case, as discussed above, the appearance of the VSS sub-option without the appearance of a VSS-Control sub-option indicates that the DHCPv4 server successfully acted upon the VSS sub-option.

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 option or sub-option 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 relay agent closer to the client or the client itself 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 or sub-option. In the DHCPv4 case, an additional VSS-Control sub-option would be required, as discussed above.

5.1. VPN Assignment by the DHCP Server

In some cases, a DHCP server may use the VSS 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 VSS 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 cannot respond correctly to the DHCP server's requirement to place the DHCP client into that VPN (perhaps

because it has not been configured with a VPN that matches the VSS information received from the DHCP server), it MUST drop the packet and not send it to the DHCP client.

In this situation, once the relay agent has placed the DHCP client into the VPN specified by the DHCP server, it will insert a VSS option or sub-option when forwarding packets from the client. The DHCP server in normal operation will echo this VSS information into the outgoing replies.

In the event that the relay agent doesn't include VSS information on subsequent requests after the DHCP server has included VSS information in a reply to the relay agent, the DHCP server can conclude that the relay agent doesn't support VSS processing, and the DHCP server SHOULD stop processing this transaction and not respond to the request.

5.2. DHCP Leasequery

A relay agent sometimes needs to submit a DHCP Leasequery [RFC4388] [RFC5007] packet to the DHCP server in order to recover information about existing DHCP-allocated IP addresses on networks 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 6 ("Client Behavior") should be followed to include the necessary VSS information.

6. Client Behavior

Typically, DHCPv4 and DHCPv6 clients have no interaction with VSS options or sub-options. The VSS information is handled by exchanges between a DHCPv4 or DHCPv6 relay agent and the corresponding DHCPv4 or DHCPv6 server.

However, there are times when an entity is acting as a DHCPv4 or DHCPv6 client in that it is communicating directly with a DHCPv4 or DHCPv6 server. In these instances -- where communication is occurring without employing the DHCPv4 Relay Agent Information option or the DHCPv6 Relay-forward or Relay-reply messages -- the entity is acting as a DHCPv4 or DHCPv6 client with regard to its communication with the DHCPv4 or DHCPv6 server, but not necessarily as a DHCP client that is requesting a DHCPv4 or DHCPv6 address for its own use.

The client, in this context, may be requesting an IP address for another entity, thus acting as a DHCP proxy. The client may be requesting information about another client-to-address binding, using the DHCPv4 [RFC4388] or DHCPv6 [RFC5007] leasequery protocol.

In the rest of this section, the term "client" refers to an entity communicating VSS information directly to a DHCPv4 or DHCPv6 server without using the DHCPv4 Relay Agent Information option or the DHCPv6 Relay-forward or Relay-reply messages, and there is no requirement that such a client be a traditional DHCPv4 or DHCPv6 client requesting an IP address binding for itself.

DHCPv4 or DHCPv6 clients 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 [RFC3633] 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. Thus, a client that places this option in a packet and doesn’t receive it or receives a different value in a returning packet SHOULD drop the packet, since the IP address that was allocated will not be in the requested VPN.

Clients should be aware that some DHCP servers will return a VSS option with different values than the values sent by the client. In addition, a client may receive a response from a DHCP server with a VSS option when none was sent 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.

7. 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 that 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 VSS 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 VSS 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 this situation, the relay agent will place the client in the proper VPN, and then it will insert a VSS option or sub-option in subsequent forwarded requests. The DHCP server will see this VSS information, and since it doesn't conflict in any way with the server's notion of the VPN on which the client is supposed to reside, it will process the requests based on the VPN specified in the VSS option or sub-option, and echo the same VSS information in the outgoing replies.

The relay agent receiving a reply containing a VSS option should support the VSS option. Otherwise, the relay agent will end up attempting to use the address as though it were a global address. Should this happen, the subsequent DHCPREQUEST will not contain any VSS information, in which case the DHCP server SHOULD NOT respond with a DHCPACK.

If a server uses a different VPN than what was specified in the VSS option or sub-option, it SHOULD send back the VPN information using the same type as the received type. It MAY send back a different type if it is not possible to use the same type (such as the RFC2685 VPN-ID if no ASCII VPN identifier exists).

A server that receives a VSS sub-option in the DHCPv4 Relay Agent Information option and does not receive a VSS-Control sub-option in the Relay Agent Information option MUST process the information specified in the VSS sub-option in the same fashion as it would have if it received both sub-options.

7.1. 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 is unable to support, is not configured to support, or does not implement support for VSS information in general or the requested VPN in particular.

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

The appearance of the DHCPv4 VSS option code in the DHCPv4 Parameter Request List option [RFC2132] should not change the processing or decision to return or not return the VSS option as specified in this document. The appearance of the DHCPv6 VSS option in the OPTION_ORO [RFC3315] or the OPTION_ERO [RFC4994] should not change the processing or decision to return (or not to return) the VSS option as specified in this document.

7.2. Returning the DHCPv4 Sub-Option

The case of the DHCPv4 sub-option is a bit more complicated. Note that [RFC3046] specifies that a DHCPv4 server that 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 understands the VSS sub-option.

In order to distinguish a DHCPv4 server that is simply copying Relay Agent Information option sub-options from an incoming to an outgoing Relay Agent Information option from a DHCPv4 server that

successfully acted upon the information in the VSS sub-option, DHCPv4 relay agents MUST include a VSS-Control sub-option in the Relay Agent Information any time that it includes a VSS sub-option in the Relay Agent Information option.

A DHCPv4 server that does not support the VSS sub-option will copy both sub-options into the outgoing Relay Agent Information option, thus signaling to the DHCPv4 relay agent that it did not understand the VSS sub-option.

A DHCPv4 server that supports the VSS sub-option

- MUST copy the VSS sub-option into the outgoing Relay Agent Information option
- MUST NOT copy the VSS-Control sub-option into the outgoing Relay Agent Information 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 the VSS sub-option that it returns to the DHCPv4 relay agent instead of the original VSS information it was given.

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 either sub-option into the outgoing Relay Agent Information option.

7.3. Making Sense of Conflicting VSS Information

It is possible for a DHCPv4 server to receive both a VSS option and VSS sub-options 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 outermost 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 general, relay agents SHOULD be aware through configuration or policy external to this document whether or not they should be including VSS information in packets that they forward, and so these relay agents should not specify any conflicting VSS information.

In situations where multiple VSS options or sub-options appear in the incoming packet or message, when the DHCP server constructs 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 only the VSS information that was used by the DHCP server to allocate the IP address (with, of course, the exception of a VSS-Control sub-option of a DHCPv4 Relay Agent Information option).

8. Update to RFC 3046

This document updates the specification of the Relay Agent Information option in Section 2.2 of RFC 3046, in the first sentence of the second paragraph, as follows:

- OLD:

  DHCP servers claiming to support the Relay Agent Information option SHALL echo the entire contents of the Relay Agent Information option in all replies.

- NEW:

  DHCP servers claiming to support the Relay Agent Information option SHALL echo the entire contents of the Relay Agent Information option in all replies, except if otherwise specified in the definition of specific Relay Agent Information sub-options.

9. Security Considerations

Message authentication in DHCPv4 for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in [RFC3118]. Potential exposures to attack are discussed in Section 7 of the DHCP protocol specification [RFC2131].

Implementations should consider using the DHCPv4 Authentication option [RFC3118] 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 [RFC4030] should be considered for DHCPv4 relay agents employing the sub-options defined in this document. Potential exposures to attack are discussed in Section 7 of the DHCP protocol specification [RFC2131].

For use of the VSS option by DHCPv6, the Security Considerations section of [RFC3315] details the general threats to DHCPv6, and thus to messages using the VSS option. The "Authentication of DHCP Messages" section of [RFC3315] 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 any VPN. 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 VSS options and the VSS sub-option should be aware of this possibility and use whatever techniques 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 agent 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.

10. IANA Considerations

IANA has assigned DHCPv4 option number 221 to the DHCPv4 Virtual Subnet Selection option defined in Section 3.1, in accordance with [RFC3942].

IANA has assigned sub-option number 151 to the DHCPv4 Virtual Subnet Selection sub-option defined in Section 3.2 from the DHCP Relay Agent Sub-options space [RFC3046], in accordance with the spirit of [RFC3942]. While [RFC3942] doesn’t explicitly mention the sub-option space for the DHCP Relay Agent Information option [RFC3046],

sub-option 151 is already in use by existing implementations of this sub-option, and this document is essentially upward-compatible with these current implementations.

IANA has assigned the value of 152 to the DHCPv4 Virtual Subnet Selection Control sub-option defined in Section 3.3.

IANA has assigned the value of 68 for the DHCPv6 Virtual Subnet Selection option defined in Section 3.4 from the DHCP Option Codes registry.

The Type byte defined in Section 3.5 defines a number space for which IANA has created and will maintain a new sub-registry entitled "VSS Type Options". This sub-registry needs to be related to both the DHCPv4 and DHCPv6 VSS options and the DHCPv4 Relay Agent Information option sub-option (all defined by this document), since the Type byte in these two options and the VSS sub-option MUST have identical definitions.

New values for the Type byte may only be defined by IETF Review, as described in [RFC5226]. Basically, this means that they are defined by RFCs approved by the IESG.

11. Acknowledgments

Jay Kumarasamy contributed to earlier versions of this document. Bernie Volz recommended consolidation of the DHCPv4 option and sub-option documents after extensive review of those former documents, and provided valuable assistance in structuring and reviewing this document. Alper Yegin expressed interest in the DHCPv6 VSS option, resulting in this combined document covering all three areas. Alfred Hoenes provided assistance with editorial review and also raised substantive protocol issues. David Hankins and Bernie Volz each raised important protocol issues that resulted in a clarified document. Josh Littlefield provided editorial assistance. Several IESG reviewers took the time to substantially review this document, resulting in much-improved clarity.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC2685] Fox, B. and B. Gleeson, "Virtual Private Networks Identifier", RFC 2685, September 1999.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[RFC4994] Zeng, S., Volz, B., Kinnear, K. and J. Brzozowski, "DHCPv6 Relay Agent Echo Request Option", RFC 4994, September 2007.

12.2. Informative References

[RFC951] Croft, W. and J. Gilmore, "Bootstrap Protocol", RFC 951, September 1985.

[RFC1542] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", RFC 1542, October 1993.

[RFC3118] Droms, R., Ed., and W. Arbaugh, Ed., "Authentication for DHCP Messages", RFC 3118, June 2001.

[RFC3942] Volz, B., "Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options", RFC 3942, November 2004.

[RFC4030] Stapp, M. and T. Lemon, "The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option", RFC 4030, March 2005.

[RFC4388] Woundy, R. and K. Kinnear, "Dynamic Host Configuration Protocol (DHCP) Leasequery", RFC 4388, February 2006.

[RFC5007] Brzozowski, J., Kinnear, K., Volz, B., and S. Zeng, "DHCPv6 Leasequery", RFC 5007, September 2007.

[RFC5198] Klensin, J. and M. Padlipsky, "Unicode Format for Network Interchange", RFC 5198, March 2008.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

Authors' Addresses

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

Phone: (978) 936-0000
EMail: kkinnear@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, MA 01719

Phone: (978) 936-0000
EMail: mjs@cisco.com