TOC

Network Working Group	R. Johnson
Internet-Draft	J. Kumarasamy
Expires: May 20, 2008	K. Kinnear
	M. Stapp
	Cisco
	November 17, 2007

Virtual Subnet Selection Option
draft-ietf-dhc-vpn-option-07.txt

Status of this Memo

Abstract

This memo defines existing usage for the Virtual Subnet Selection (VSS) information option. It is intended for use primarily by DHCP proxy clients in situations where VSS information needs to be passed to the DHCP server for proper address allocation to take place.

The option number currently in use is 221. This memo documents the current usage of the option in agreement with [RFC3942] (Volz, B., “Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options,” November 2004.), which declares that any pre-existing usages of option numbers in the range 128 - 223 should be documented and the working group will try to officially assign those numbers to those options.

Table of Contents

1. Introduction

TOC

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.

If the allocation is being done through a DHCP relay, then a relay sub-option could be included. In some cases, however an IP address is being sought by a DHCP 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 DHCP option.

A good example might be a dial-in aggregation device where PPP [RFC1661] (Simpson, W., “The Point-to-Point Protocol (PPP),” July 1994.) addresses are acquired via DHCP and then given to the remote customer system via IPCP [RFC1332] (McGregor, G., “The PPP Internet Protocol Control Protocol (IPCP),” May 1992.). In a network where such a device is used to aggregate PPP dial-in from multiple companies, each company may be assigned a unique VSS.

This memo defines a new DHCP [RFC2131] (Droms, R., “Dynamic Host Configuration Protocol,” March 1997.) option, the VSS Information option, which allows the DHCP client to specify the VSS Information needed in order to allocate an address. If the receiving DHCP server understands the VSS Information 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.

2. Conventions

TOC

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 [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).
This document also uses the following terms:

DHCP Client DHCP Client or "Client" is an Internet host using DHCP to obtain configuration parameters such as a network address.

DHCP Server A DHCP Server or "Server" is an Internet host that returns configuration parameters to DHCP Clients.

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 [RFC951] (Croft, B. and J. Gilmore, “Bootstrap Protocol (BOOTP),” September 1985.) and [RFC1542] (Wimer, W., “Clarifications and Extensions for the Bootstrap Protocol,” October 1993.).

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

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

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.

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

VPN Identifier The VPN-ID is defined by [RFC2685] (Fox, B. and B. Gleeson, “Virtual Private Networks Identifier,” September 1999.) to be a sequence of 7 octets.

3. VSS Information Definition

TOC

The VSS Information option is a DHCP option [RFC2132] (Alexander, S. and R. Droms, “DHCP Options and BOOTP Vendor Extensions,” March 1997.).
The option contains generalized VSS information in one of two formats:

NVT ASCII VPN identifier, or RFC2685 VPN-ID [RFC2685] (Fox, B. and B. Gleeson, “Virtual Private Networks Identifier,” September 1999.).

The format of the option is:

```
      Code   Len   Type   VSS Information octets
     +-----+-----+------+-----+-----+-----+---
     | 221 |  n  |  t   | v1  | v2  | v3  | ...
     +-----+-----+------+-----+-----+-----+---

     Type:   0       NVT ASCII VPN identifier
             1       RFC2685 VPN-ID
             2-255   Not Allowed
```

Figure 1

The option minimum length (n) is 2.

There are two types of identifiers which can be placed in the VSS Information Option. The first type of identifier which can be placed in the VSS Information 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 VSS Information Option is an RFC2685 VPN-ID [RFC2685] (Fox, B. and B. Gleeson, “Virtual Private Networks Identifier,” September 1999.), which is typically 7 octets (3 of VPN OUI followed by 4 of VPN index) in length (though it can be any length as far as the VSS Information Option is concerned).

If the type field is set to zero (0), it indicates that all following bytes of the option contain a NVT ASCII string. This string MUST NOT be terminated with a zero byte.

If the type field is set to one (1), it indicates that all following bytes should be interpreted in agreement with RFC2685 as a VPN Identifier, typically 7 octets.

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

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 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.

Servers configured to support this option MUST return an identical copy of the option to any client that sends it, regardless of whether or not the client requests the option in a parameter request list.

This option provides the DHCP server additional information upon which to make a determination of address to be assigned. The DHCP server, if it is configured to support this option, should use this information in addition to other options included in the DHCPDISCOVER packet in order to assign an IP address for DHCP client.

In the event that a Virtual Subnet Selection option and a Virtual Subnet Selection sub-option [I-D.ietf-dhc-agent-vpn-id] (Kinnear, K., “Virtual Subnet Selection Sub-Option for the Relay Agent Information Option for DHCPv4,” November 2007.) 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.

Servers that do not understand this option will allocate an address using their normal algorithms and will not return this option in the DHCPOFFER or DHCPACK. In this case the client should consider discarding the DHCPOFFER or DHCPACK, as mentioned above. Servers that understand this option but are administratively configured to ignore the option MUST ignore the option, use their normal algorithms to allocate an address, and MUST NOT return this option in the DHCPOFFER or DHCPACK such that the client will know that the allocated address is not in the VPN requested and will consider this information in deciding whether or not to accept the DHCPOFFER. In other words, this option MUST NOT appear in a DHCPOFFER or DHCPACK from a server unless it was used by the server in making or updating the address allocation requested.

---

4. Security Considerations

TOC

Message authentication in DHCP for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in [RFC3118] (Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” June 2001.). Potential exposures to attack are discussed in section 7 of the DHCP protocol specification in [RFC2131] (Droms, R., “Dynamic Host Configuration Protocol,” March 1997.).

The VSS Information option could be used by a client in order to obtain an IP address from a VPN other than the one where it should. Another possible defense would be for the DHCP relay to insert a Relay option containing a VSS Information Relay Sub-option, which would override the DHCP VSS Information option.

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.
Servers that implement the VSS Information 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.
Implementations should consider using the DHCP Authentication option [RFC3118] (Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” June 2001.) in order to provide a higher level of security if it is deemed necessary in their environment.

5. IANA Considerations

TOC

IANA is requested to assign DHCP option number 221 for this option, in accordance with [RFC3942] (Volz, B., “Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options,” November 2004.).
While the type byte of the Virtual Subnet Selection 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 [RFC2434] (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” October 1998.). 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 VSS Information Option. The type bytes and data formats of the VSS Information Option and VSS Information Relay Sub-option MUST always be identical.

6. Acknowledgements

TOC

This document is the result of work done within Cisco Systems. Thanks to Kim Kinnear, Mark Stapp, and Jay Kumarasamy for their work on this option definition and the other related work for which this is necessary.

7. References

TOC

7.1. Normative References

TOC

[RFC951]	Croft, B. and J. Gilmore, “Bootstrap Protocol (BOOTP),” RFC 951, September 1985 (TXT).
[RFC1542]	Wimer, W., “Clarifications and Extensions for the Bootstrap Protocol,” RFC 1542, October 1993 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2131]	Droms, R., “Dynamic Host Configuration Protocol,” RFC 2131, March 1997 (TXT, HTML, XML).
[RFC2132]	Alexander, S. and R. Droms, “DHCP Options and BOOTP Vendor Extensions,” RFC 2132, March 1997 (TXT, HTML, XML).
[RFC2685]	Fox, B. and B. Gleeson, “Virtual Private Networks Identifier,” RFC 2685, September 1999 (TXT).
[RFC2434]	Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” BCP 26, RFC 2434, October 1998 (TXT, HTML, XML).
[RFC3942]	Volz, B., “Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options,” RFC 3942, November 2004 (TXT).

7.2. Informative References

TOC

[RFC1332]	McGregor, G., “The PPP Internet Protocol Control Protocol (IPCP),” RFC 1332, May 1992 (TXT).
[RFC1661]	Simpson, W., “The Point-to-Point Protocol (PPP),” STD 51, RFC 1661, July 1994 (TXT).
[RFC3118]	Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” RFC 3118, June 2001 (TXT).
[I-D.ietf-dhc-agent-vpn-id]	Kinnear, K., “Virtual Subnet Selection Sub-Option for the Relay Agent Information Option for DHCPv4,” draft-ietf-dhc-agent-vpn-id-05 (work in progress), November 2007 (TXT).

Authors' Addresses

TOC

	Richard A. Johnson

Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134
US
Phone: +1 408 526 4000
Email: raj@cisco.com

Jay Kumarasamy
Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134
US
Phone: +1 408 526 4000
Email: jayk@cisco.com

Kim Kinnear
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824
US
Phone: +1 978 244 8000
Email: kkinnar@cisco.com

Mark Stapp
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824
US
Phone: +1 978 244 8000
Email: mjs@cisco.com

Full Copyright Statement

TOC

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.