Network Working Group
Internet-Draft
Expires: August 10, 2005

R. Johnson
J. Kumarasamy
K. Kinnear
M. Stapp
Cisco

February 9, 2005

Virtual Subnet Selection Option
draft-ietf-dhc-vpn-option-04.txt

Status of this Memo

This Internet-Draft will expire on August 10, 2005.

Copyright Notice

Abstract

This memo defines a new DHCP option for passing Virtual Subnet Selection (VSS) information between the DHCP client and the DHCP server. 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 RFC-3942[7] , 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

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 Subject 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 suboption could be included. In some cases, however an IP address is being sought by a DHCP proxy on behalf of a client (would 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 addresses are acquired via DHCP and then given to the remove customer system via IPCP. 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 [2] 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. VSS Information Definition

The VSS Information option is a DHCP option [3]. The option contains generalized VSS information in one of two formats: NVT ASCII VPN identifier, or RFC2685 VPN-ID [4].

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 [4], which is typically 14 hex digits 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 [4] as a VPN Identifier, typically 14 hex digits.

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.

Any VSS information contained in a DHCP Relay Suboption SHOULD override the information contained in this VSS Information option

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. Clients using this option MUST discard DHCPOFFER or DHCPACK packets that do not contain this option.

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 configure 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 VSS Informmation Option and a VSS Information Relay Suboption are both received in a particular DHCP client packet, the information from the VSS Information Suboption MUST be used in preference to the information in the VSS Information Option.

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 will discard the DHCPOFFER or DHCPACK. 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. In this case the client will discard the DHCPOFFER or DHCPACK. In other words, this option MUST NOT appear in a DHCPOFFER from a server unless it was used by the server in making the address allocation requested.

This option SHOULD NOT be used without also making use of the DHCP Authentication option [5].

3. Security Considerations

Message authentication in DHCP for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in [5]. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification in [2].

The VSS Information option could be used by a client in order to obtain an IP address from a VSS other than the one where it should. DHCP relays MAY choose to remove the option before passing on DHCPDISCOVER packets. Another possible defense would be for the DHCP relay to insert a Relay option containing a VSS Information Suboption, 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.

4. IANA Considerations

No assignment of values for the type field need be made at this time. New values may only be defined by IETF Consensus, as described in [6]. 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 Suboption MUST always be identical.

5. Acknowledgements

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.

6 References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997.

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

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

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

[5] Droms, R., "Authentication for DHCP Messages", RFC 3118, June 2001.

[6] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 2434, October 1998.

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

Authors' Addresses

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

Intellectual Property Statement

Disclaimer of Validity

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.

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.