Internet Engineering Task Force
Internet Draft
Expiration: March 2005
File: draft-ietf-dhc-vpn-option-03.txt

Richard Johnson
Kim Kinnear
Mark Stapp
Jay Kumarasamy
Cisco Systems, Inc.

DHCP VPN Information option

<draft-ietf-dhc-vpn-option-03.txt>

September 27, 2004

Status of this Memo

Copyright Notice

Abstract

This memo defines a new DHCP option for passing VPN information between the DHCP client and the DHCP server. It is intended for use primarily by DHCP proxy clients in situations where VPN information needs to be passed to the DHCP server for proper address allocation to take place.

1.0 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 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 VPN 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 VPN.

This memo defines a new DHCP [2] option, the VPN Information option, which allows the DHCP client to specify the VPN Information needed in order to allocate an address. If the receiving DHCP server understands the VPN 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.

1.1 Conventions

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 [3].

2.0 VPN Information Option Definition

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

The format of the option is:

```
    Code   Len   Type   VPN Information octets
   +-----+-----+------+-----+-----+-----+---
   | TBD |  n  |  t   | v1  | v2  | v3  | ...
   +-----+-----+------+-----+-----+-----+---
```

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

The option minimum length (n) is 2.

There are two types of identifiers which can be placed in the VPN Information Option. The first type of identifier which can be placed in the VPN 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 VPN 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 VPN 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 VPN options containing any other value than zero (0) or one (1) SHOULD be ignored.

Any VPN information contained in a DHCP Relay Suboption SHOULD override the information contained in this VPN 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 VPN Informmation Option and a VPN Information Relay Suboption are both received in a particular DHCP client packet, the information from the VPN Information Suboption MUST be used in preference to the information in the VPN 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].

3.0 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 VPN 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. 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 VPN Information Suboption, which would override the DHCP VPN 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 VPN 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 VPNs from which addresses may be requested.

4.0 IANA Considerations

IANA has assigned a value of TBD for the DHCP option code described in this document. 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 VPN Information Option. The type bytes and data formats of the VPN Information Option and VPN Information Suboption MUST always be identical.

5.0 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.

Copyright notice

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

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

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

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

Author Information:

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

Phone: (408) 526-4000

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

Kim Kinnear
Mark Stapp
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824

Phone: (978) 244-8000

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