Network Working Group   Kim Kinnear
INTERNET DRAFT   Mark Stapp
                                              Richard Johnson
                                              Jay Kumarasamy
                                                Cisco Systems

                                                   March 2002
                                        Expires August 2002

**VPN Identifier sub-option
for the Relay Agent Information Option**
<**draft-ietf-dhc-agent-vpn-id-01.txt**>

Status of this Memo

Copyright Notice

Abstract

   In some environments, a relay agent resides in a network element
   which also has access to one or more VPNs. If one DHCP server wishes
   to offer service to DHCP clients on those different VPNs the DHCP
   server needs to know the VPN on which each client resides. The vpn-
   id sub-option of the relay-agent-information option is used by the
   relay agent to tell the DHCP server the VPN 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.

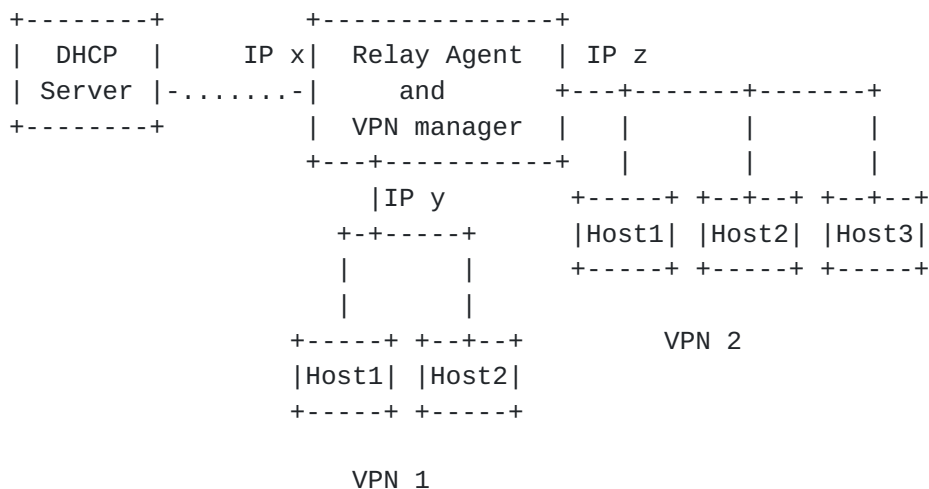**1**. **Introduction**

   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 this information in the relay-agent-
   information option in the client's DHCP requests. This document
   defines a sub-option for the relay-agent-information option which
   contains the vpn-id, and which allows the relay agent to communicate
   the VPN association to the DHCP server.

   When the DHCP server sends its response to the relay agent for for-
   warding back to the DHCP client, the relay agent will also need to
   use the vpn-id 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 vpn-id sub-option to the relay agent in the
   relay-agent-information option back to the relay agent.

   Consider the following architecture:


```
        +--------+          +---------------+
        |  DHCP  |    IP x|  Relay Agent  | IP z
        | Server |-........-|     and       +---+-------+-------+
        +--------+          |  VPN manager  |   |       |       |
                            +---+-----------+   |       |       |
                               |IP y           +-----+ +--+--+ +--+--+
                             +-+-----+          |Host1| |Host2| |Host3|
                             |       |          +-----+ +-----+ +-----+
                             |       |
                           +-----+ +--+--+           VPN 2
                           |Host1| |Host2|
                           +-----+ +-----+


                             VPN 1
```

In this architecture, the relay agent knows the VPN for each of the
DHCP clients, and inserts that information in the vpn-id sub-option
in every DHCP request it forwards onto 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 vpn-id
sub-option as well.

When the relay agent receives a DHCP reply packet from the server
with a vpn-id sub-option, it will forward the packet onto the proper
VPN based on the value of the vpn-id 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 confi-
     guration 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 dif-
     ferent 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 "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. **VPN identifier sub-option definition**

The vpn-id sub-option MAY be used by any DHCP relay agent which
desires to specify the VPN from which a DHCP client request was sent.

The vpn-id sub-option contains a generalized VPN identifier.

The format of the option is:

```
 SubOpt   Len   Type    VPN identifier
+------+------+------+------+------+------+---
| TBD  |   n  |   t  | id1  | id2  | id3  | ...
+------+------+------+------+------+------+---

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

There are two types of identifiers which can be placed in the vpn-id
sub-option. The first type of identifier which can be placed in the
vpn-id 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 vpn-id 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 vpn-id
sub-option is concerned).

A relay agent which recieves a DHCP request from a DHCP client on a
VPN SHOULD include a vpn-id 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 vpn-id 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 identical copy of the sub-
option in the relay-agent-info option to any relay-agent that sends
it.

In the event that a vpn-id option and a vpn-id sub-option are both
received in a particular DHCP client packet, the information from the
vpn-id sub-option MUST be used in preference to the information in
the vpn-id option.

Relay agents which include this sub-option when forwarding DHCP
client requests MUST discard DHCPOFFER or DHCPACK packets that do not
contain this sub-option in their associated relay-agent-info options.

In some cases, a DHCP server may use the vpn-id sub-option to inform
a relay agent that a particular DHCP client is associated with a par-
ticular VPN. It does this by sending the vpn-id 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 back to the DHCP client.

4. Security

DHCP currently provides no authentication or security mechanisms.
Potential exposures to attack are discussed is section 7 of the pro-
tocol specification [RFC2131]. The vpn-id sub-option could allow a
program masquerading as a relay agent to obtain addresses on other
VPNs than the one on which it resides, possibly aiding in an
address-pool exhaustion attack on that VPN.

This attack can be partially prevented by the relay agent not for-
warding 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 form of address-pool exhaustion.

Under the current DHCP security model there are no methods available
to completely circumvent this type of attack.

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 vpn-id
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 vpn-id option. The
type bytes and data formats of the vpn-id option and vpn-id sub-
option MUST always be identical.

6. Acknowledgments

None (yet).

7. 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 Identif-
    ier", Internet RFC 2685, September 1999.

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

8. Author's information

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

    Phone: (978) 497-8000

        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 intel-
lectual 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 stan-
dard. Please address the information to the IETF Executive Director.

10. **Full Copyright Statement**

such copies and derivative works. However, this document itself may not
be modified in any way, such as by removing the copyright notice or
references to the Internet Society or other Internet organizations,
except as needed for the purpose of developing Internet standards in
which case the procedures for copyrights defined in the Internet Stan-
dards process must be followed, or as required to translate it into
languages other than English.

The limited permissions granted above are perpetual and will not be
revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS
IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK
FORCE DISCLAIMS 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 FIT-
NESS FOR A PARTICULAR PURPOSE.