Subnet Selection sub-option
for the Relay Agent Information Option
<draft-ietf-dhc-agent-subnet-selection-01.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

Abstract

In RFC2131, the giaddr specifies both the subnet on which a DHCP client resides as well as an IP address which can be used to communicate with the relay agent. The subnet selection option [RFC 3011] allows these functions of the giaddr to be split so that when one entity is performing as a DHCP proxy, it can specify the subnet from which to allocate an IP address which is different from the IP address with which it desires to communicate with the DHCP server.
Analogous situations exist where the relay agent needs to specify the subnet on which a DHCP client resides which is different from an IP address which can be used to communicate with the relay agent. The subnet-selection sub-option (specified here) of the relay-agent-information option allows a relay agent to do this.

1. Introduction

In RFC2131, the giaddr specifies both the subnet on which a DHCP client resides as well as an IP address which can be used to communicate with the relay agent. The subnet selection option [RFC 3011] allows these functions of the giaddr to be split so that when one entity is performing as a DHCP proxy, it can specify the subnet from which to allocate an IP address which is different from the IP address with which it desires to communicate with the DHCP server.

Analogous situations exist where the relay agent needs to specify the subnet on which a DHCP client resides which is different from an IP address which can be used to communicate with the relay agent. Consider the following architecture:

```
+--------+         +---------------+
|  DHCP  |     IP x|               |IP y
| Server |-.......-|  Relay Agent |----+------------+
+--------+         |               |    |            |
+---------------+    |         +------+
|         |Modem |
|         +------+
|          |    |    |
+-----+  +-----+ +-----+  +-----+
|Host1|  |Host2| |Host3|
+-----+  +-----+ +-----+  +-----+
```

In the usual approach, the relay agent would put IP address Y into the giaddr of any packets that it forwarded to the DHCP server. However, if for any reason IP address Y is not accessible from the DHCP server, then this usual approach will fail. There are several reasons why IP y might be inaccessible from the DHCP server:

1. IP y might not be unique for this subnet, but might instead be shared as a gateway address by multiple subnets.

2. There might be some firewall capability in the network element
in which the relay agent resides that does not allow the DHCP
server to access the relay agent via IP y.

3. There might not be an IP y. An example would be the case where
there was only one host and this was a point to point link.

In any of these or other cases, the relay agent needs to be able to
communicate to the DHCP server the subnet from which to allocate an
IP address. The IP address which will communicate to the DHCP server
the subnet information cannot be used as a way to communicate between
the DHCP server and the relay agent.

Since the relay agent can modify the client’s DHCP DHCPREQUEST in
only two ways: the giaddr and the relay-agent-info option, there is
thus a need to extend the relay-agent-info option with a new sub-
option, the subnet-selection sub-option, to allow separation of the
specification of the subnet from the IP address to use when communi-
cating with the relay agent.

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 [RFC 2119].

This document uses the following terms:

- "DHCP client"
  A DHCP client is an Internet host using DHCP to obtain config-
  uration parameters such as a network address.

- "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].

- "DHCP server"
  A DHCP server is an Internet host that returns configuration
  parameters to DHCP clients.

3. Subnet selection sub-option definition

The subnet-selection sub-option MAY be used by any DHCP relay agent
which desires to specify a subnet for a DHCP client request that it
is relaying but needs the subnet specification to be different from
the IP address the DHCP server should use when communicating with the
relay agent.

The sub-option contains a single IP address that is the address of a
subnet. The value for the subnet address is determined by taking any
IP address on the subnet and ANDing that address with the subnet mask
(i.e.: the network and subnet bits are left alone and the remaining
(address) bits are set to zero). When the DHCP server is allocating
an address and this option is present then the DHCP server MUST allo-
cate the address on either:

- the subnet specified in the subnet selection option, or;
- a subnet on the same network segment as the subnet specified in
  the subnet selection option.

The format of the option is:

```
SubOpt   Len      subnet IP address
+-------------+----------+---------------+---------------+---------------+---------------+---------------+
|    TBD     |      4   |   a1          |   a2          |   a3          |   a4          |
+-------------+----------+---------------+---------------+---------------+---------------+
```

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. Relay agents using this sub-option MUST discard DHCPOFFER
or DHCPACK packets that do not contain this option in their associ-
ated relay-agent-info options.

This option does not require changes to operations or features of the
DHCP server other than to select the subnet on which to allocate an
address. For example, the handling of DHCPDISCOVER for an unknown
subnet should continue to operate unchanged.

In the event that a DHCP server receives a packet which contains both
a subnet selection option [RFC 3011] as well as a subnet selection
sub-option, the information contained in the subnet selection sub-
option MUST be used to control the allocation of an IP address in
preference to the information contained in the subnet selection
option.

When this option is present and the server supports this option, the
server MUST NOT offer an address that is not on the requested subnet or network segment.

The IP address to which a DHCP server sends a reply MUST be the same as it would chose when this option is not present.

4. Security

DHCP currently provides no authentication or security mechanisms. Potential exposures to attack are discussed in section 7 of the protocol specification [RFC 2131]. The subnet selection sub-option allows a relay agent to specify the subnet on which to allocate an address for a DHCP client. Given that the subnet selection option already exists [RFC 3011], no new security issues are raised by the existence of the subnet selection sub-option specified in this document. The existence of either the subnet selection option or subnet selection sub-option documented here would allow a malicious DHCP client to perform a more complete address-pool exhaustion attack than could be performed without the use of these options, since the client would no longer be restricted to attacking address-pools on just its local subnet. Under the current DHCP security model there are no methods available to circumvent this type of attack.

5. IANA Considerations

IANA has assigned the value of TBD for the relay-agent-info option sub-option code for this sub-option.

6. Acknowledgments

Eric Rosen contributed to helping the authors to understand the need for this sub-option. Much of the text of this document was borrowed with only minimal modifications from the document describing the subnet selection option [RFC 3011].

7. References


8. Author’s information

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

Phone: (978) 244-8000
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. Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and