DHC Working Group
Internet-Draft
Expires: July 29, 2004

M. Stapp
R. Johnson
T. Palaniappan
Cisco Systems, Inc.

January 29, 2004

Vendor-Specific Suboption for the DHCP Relay Agent Option

<draft-stapp-dhc-vendor-suboption-00.txt>

Status of this Memo

Copyright Notice

Abstract

This memo defines a new Vendor-Specific suboption for the Dynamic Host Configuration Protocol's (DHCP) relay agent information option. The suboption allows a DHCP relay agent to include vendor-specific information in DHCP messages it forwards, as configured by its administrator.

Table of Contents

1. Requirements 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[1].

2. Introduction

DHCP (RFC 2131[2]) provides IP addresses and configuration information for IPv4 clients. It includes a relay agent capability, in which processes within the network infrastructure receive broadcast messages from clients and forward them to DHCP servers as unicast messages. In network environments like DOCSIS data-over-cable and xDSL, for example, it has proven useful for the relay agent to add information to the DHCP message before forwarding it, using the relay agent information option (RFC 3046[3]).

Servers that recognize the relay agent option echo it back in their replies, and some of the information that relays add may be used to help an edge device efficiently return replies to clients. The information that relays supply can also be used in the server's decision making about the addresses and configuration parameters that the client should receive.

In many environments it's desirable to associate some vendor- or provider-specific information with clients' DHCP messages. This is often done using the relay agent information option. RFC 3046 defines Remote-ID and Circuit-ID sub-options that are used to carry such information. The values of those suboptions, however, are usually based on some network resource, such as an IP address of a network access device, an ATM Virtual Circuit identifier, or a DOCSIS cable-modem identifier. As a result, the values carried in these suboptions are dependent on the physical network configuration. The Vendor-Specific suboption allows administrators to associate other useful data with relayed DHCP messages.

3. The Vendor-Specific Suboption

This memo defines a new DHCP relay agent option suboption that carries vendor-defined data. The suboption takes a form similar to many other relay information option suboptions.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Code      |    Length     |         Enterprise Number     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                               |     Type      |               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               +
   .                                                               .
   .                         Suboption Data                        .
   .                                                               .
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Code for the suboption is <TBD>.

The one-byte Length field is the length of the data carried in the suboption, in bytes. The length includes the length of the Enterprise Number; the minimum length is 4 bytes.

The "Enterprise Number" is the vendor's Enterprise Number as registered with IANA[4]. It is a four-byte integer value in network byte-order.

The one-byte Type value can be used to distinguish among a vendor's uses of different data in different configurations, or among multiple instances of the suboption which carry different types of data.

The Data is an arbitrary sequence of bytes.

The Vendor-Specific suboption includes an Enterprise Number and carries a sequence of bytes. The Type byte can be used to distinguish among different types of data if a single relay vendor is able to generate different types of suboptions. The Type codes are defined by the vendor identified in the Enterprise Number field; the Type codes are not IANA-assigned or -managed. A relay MAY include more than one Vendor-Specific suboption.

The Vendor-Specific data are of course provider-specific. This specification does not establish any requirements on the data in the suboption. Vendors who make use of this suboption are encouraged to document their usage in order to make interoperability possible.

4. Relay Agent Behavior

DHCP relay agents MAY be configured to include Vendor-Specific suboptions if they include a relay agent information option in relayed DHCP messages. The suboptions' types and data are assigned and configured through mechanisms that are outside the scope of this

memo.

Relay implementors are encouraged to offer their administrators some means of configuring what data can be included in this suboption, and to document what they are capable of.

5. DHCP Server Behavior

This suboption provides additional information to the DHCP server. The DHCP server, if it is configured to support this suboption, may use this information in addition to other relay agent option data and other options included in the DHCP client messages in order to assign an IP address and/or other configuration parameters to the client. There is no special additional processing for this suboption.

DHCP server vendors are encouraged to offer their administrators some means of configuring the use of data from incoming Vendor-Specific suboptions in DHCP decision-making.

6. Security Considerations

Message authentication in DHCP for intradomain use where the out-of-band exchange of a shared secret is feasible is defined in RFC 3118[5]. Potential exposures to attack are discussed in section 7 of the DHCP protocol specification in RFC 2131[2].

The DHCP relay agent option depends on a trusted relationship between the DHCP relay agent and the server, as described in section 5 of RFC 3046. Fraudulent relay agent option data could potentially lead to theft-of-service or exhaustion of limited resources (like IP addresses) by unauthorized clients. A host that tampered with relay agent data associated with another host's DHCP messages could deny service to that host, or interfere with its operation by leading the DHCP server to assign it inappropriate configuration parameters.

While the introduction of fraudulent relay agent options can be prevented by a perimeter defense that blocks these options unless the relay agent is trusted, a deeper defense using authentication for relay agent options via the Authentication Suboption[6] or IPSEC[7] SHOULD be deployed as well.

There are several data in a DHCP message that convey information that may identify an individual host on the network. These include the chaddr, the client-id option, and the hostname and client-fqdn options. Depending on the type of data included, the Vendor-Specific suboption may also convey information that identifies a specific host or a specific user on the network. In practice, this information isn't exposed outside the internal service-provider network, where DHCP messages are usually confined. Administrators

who configure data that's going to be used in DHCP Vendor-Specific suboptions should be careful to use data that are appropriate for the types of networks they administer. If DHCP messages travel outside the service-provider's own network, or if the suboption values may become visible to other users, that may raise privacy concerns for the access provider or service provider.

7. IANA Considerations

IANA has assigned a value of <TBD> from the DHCP Relay Agent Information Option[3] suboption codes for the Vendor-Specific Suboption described in this document.

8. Acknowledgements

The authors are grateful to Andy Sudduth, Josh Littlefield, and Kim Kinnear for their review and comments.

Normative References

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

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

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

[4] IANA, , "Private Enterprise Numbers (http://www.iana.org/assignments/enterprise-numbers.html)".

Informative References

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

[6] Stapp, M., "The Authentication Suboption for the DHCP Relay Agent Option", draft-ietf-dhc-auth-suboption-02.txt (work in progress), October 2003.

[7] Droms, R., "Authentication of Relay Agent Options Using IPSEC", draft-ietf-dhc-relay-agent-ipsec-01.txt (work in progress), November 2003.

Authors' Addresses

Mark Stapp
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

Phone: 978.936.0000
EMail: mjs@cisco.com

Richard Johnson
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
USA

Phone: 408.526.4000
EMail: raj@cisco.com

Theyn Palaniappan
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
USA

Phone: 408.526.4000
EMail: athenmoz@cisco.com

Full Copyright Statement

Acknowledgement

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