

Network Working Group
Request for Comments: 3993
Category: Standards Track

R. Johnson
T. Palaniappan
M. Stapp
Cisco Systems, Inc.
March 2005

Subscriber-ID Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This memo defines a new Subscriber-ID suboption for the Dynamic Host Configuration Protocol's (DHCP) relay agent information option. The suboption allows a DHCP relay agent to associate a stable "Subscriber-ID" with DHCP client messages in a way that is independent of the client and of the underlying physical network infrastructure.

Table of Contents

1. Introduction	2
2. Requirements Terminology	2
3. The Subscriber-ID Suboption	2
3.1. Suboption Format	3
4. Relay Agent Behavior	3
5. DHCP Server Behavior	4
6. Security Considerations	4
7. IANA Considerations	5
8. Acknowledgements	5
9. References	5
9.1. Normative References	5
9.2. Informative References	5
Authors' Addresses	6
Full Copyright Statement	7

1. 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 such as DOCSIS data-over-cable and xDSL, it has proven useful for the relay agent to add information to the DHCP message before forwarding it, by 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 service provider environments, it is desirable to associate some provider-specific information with clients' DHCP messages. This is often done by using the relay agent information option. RFC 3046 defines Remote-ID and Circuit-ID suboptions that are used to carry such information. The values of those suboptions, however, are usually based on a 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. If a client connects to the service provider network through different paths, different values are carried in network-dependent suboptions.

2. 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].

3. The Subscriber-ID Suboption

In complex service provider environments, connecting a customer's DHCP configuration and administrative information is necessary. The Subscriber-ID suboption carries a value that can be independent of the physical network configuration through which the subscriber is connected. This value complements, and might well be used in addition to, the network-based relay agent option suboptions discussed in Section 2. The "subscriber-id" assigned by the provider is intended to be stable as customers connect through different paths, and as network changes occur.

The Subscriber-ID information allows the service provider to assign/activate subscriber-specific actions; e.g., assignment of host IP address and subnet mask, DNS configuration, or trigger accounting. This suboption is de-coupled from the access network's physical structure, so subscriber moves from one access-point to another, for example, would not require reconfiguration at the service provider's DHCP servers.

The Subscriber-ID is an ASCII string; the encoding of the string is defined in Section 3.1. The semantic contents of the Subscriber-ID string are, of course, provider-specific. This specification does not establish any semantic requirements on the data in the string.

3.1. Suboption Format

This memo defines a new DHCP relay agent option suboption that carries a "Subscriber-ID" value. The value is an ASCII string. The suboption takes a form similar to that of many other relay information option suboptions:

```

0      1      2      3      4      5
+-----+-----+-----+-----+-----+
|Code | Len | Subscriber-ID string ...
+-----+-----+-----+-----+-----+

```

The Code for the suboption is 6.

The one-octet Len field is the length of the ID string, in octets. The minimum length of the ID string is 1 octet.

The "Subscriber-ID" is an NVT ASCII [4] string. The string MUST NOT be NULL terminated, as the length is specified in the "Len" field.

4. Relay Agent Behavior

DHCP relay agents MAY be configured to include a Subscriber-ID suboption if they include a relay agent information option in relayed DHCP messages. The subscriber-id strings themselves are assigned and configured through mechanisms that are outside the scope of this memo.

5. DHCP Server Behavior

This suboption provides additional information to the DHCP server. If it is configured to support this option, the DHCP server 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.

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 attacks 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 fields in a DHCP message conveying 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 identifier selected, the Subscriber-ID 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 Subscriber-ID suboptions should be careful to use identifiers 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 6 from the DHCP Relay Agent Information Option [3] suboption codes for the Subscriber-ID Suboption described in this document.

8. Acknowledgements

This document is the result of work done within Cisco Systems. Thanks especially to Andy Sudduth for his review comments.

9. References

9.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, 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] Postel, J. and J. Reynolds, "Telnet Protocol Specification", STD 8, RFC 854, May 1983.

9.2. 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", Work in Progress.
- [7] Droms, R., "Authentication of Relay Agent Options Using IPSec", Work in Progress.

Authors' Addresses

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

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

Phone: 978.936.0000
EMail: mjs@cisco.com

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

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

