

Network Working Group
Internet-Draft
Expires: December 6, 2003

M. Stapp
Cisco Systems, Inc.
T. Lemon
Nominum, Inc.
R. Droms
Cisco Systems, Inc.
June 7, 2003

The Authentication Suboption for the DHCP Relay Agent Option
<[draft-ietf-dhc-relay-agent-auth-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/lid-abstracts.txt>.

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

This Internet-Draft will expire on December 6, 2003.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

The DHCP Relay Agent Information Option ([RFC 3046](#)) conveys information between a DHCP relay agent and a DHCP server. This specification defines two mechanisms for securing the messages exchanged between a relay agent and a server. The first mechanism defines a new authentication suboption for the Relay Agent Information Option that supports source entity authentication and data integrity for relayed DHCP messages. The authentication suboption contains a cryptographic signature in a payload derived

from the option used in DHCP Authentication ([RFC 3118](#)). The second mechanism uses IPsec ([RFC 2401](#)) to protect messages exchanged between relay agents and servers.

Table of Contents

1.	Requirements Terminology	3
2.	DHCP Terminology	3
3.	Introduction	3
4.	Relay Agent Option Authentication Sub-option	4
4.1	Suboption Format	5
4.2	Replay Detection	6
4.3	The Relay Identifier Field	6
4.4	Computing Authentication Information	7
4.4.1	The HMAC-MD5 Algorithm	7
4.5	Procedures for Sending Messages	9
4.5.1	Replay Detection	9
4.5.2	Packet Preparation	9
4.5.3	Signature Computation	9
4.5.4	Sending the Message	9
4.6	Procedures for Processing Incoming Messages	9
4.6.1	Initial Examination	9
4.6.2	Replay Detection Check	10
4.6.3	Signature Check	10
4.7	Relay Agent Behavior	10
4.7.1	Receiving Messages from Other Relay Agents	11
4.7.2	Sending Messages to Servers	11
4.7.3	Receiving Messages from Servers	11
4.8	DHCP Server Behavior	11
4.8.1	Receiving Messages from Relay Agents	12
4.8.2	Sending Reply Messages to Relay Agents	12
5.	Use of IPsec to secure DHCP messages	12
6.	IANA Considerations	13
7.	Security Considerations	13
7.1	Authentication sub-option Protocol Considerations	13
7.2	IPsec Considerations	14
8.	Acknowledgements	14
	References	14
	References	14
	Authors' Addresses	15
	Full Copyright Statement	16

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. DHCP Terminology

This document uses the terms "DHCP server" (or "server") and "DHCP client" (or "client") as defined in [RFC 2131](#). The term "DHCP relay agent" refers to a "BOOTP relay agent" as defined in [RFC 2131](#).

3. Introduction

DHCP ([RFC 2131](#) [[8](#)]) provides IP addresses and configuration information for DHCP clients. It includes a relay agent capability ([RFC 951](#) [[9](#)], [RFC 1542](#) [[10](#)]), in which processes within the network infrastructure receive broadcast messages from clients and forward them to 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](#) [[2](#)]. The kind of information that a relay agent adds is often used in the server's decision making about the addresses and configuration parameters that the client should receive. The way that the relay agent data is used in server decision-making tends to make that data very important, and highlights the importance of the trust relationship between the relay agent and the server.

The existing DHCP Authentication specification ([RFC 3118](#)) [[11](#)] only secures communication between the DHCP client and server. Because relay agent information is added after the client has signed its message, the DHCP Authentication specification explicitly excludes relay agent data from that authentication.

The goals of this specification is to define methods that a relay agent can use to:

1. protect the integrity of the data that the relay adds
2. provide replay protection for that data
3. leverage existing mechanisms such as DHCP Authentication and IPsec

The first mechanism defined to meet these goals specifies a new relay agent suboption, the Authentication suboption. The format of this suboption is very similar to the format of the DHCP Authentication

option, and the specification of the cryptographic methods and signature computation for the suboption are also similar to that option's specification.

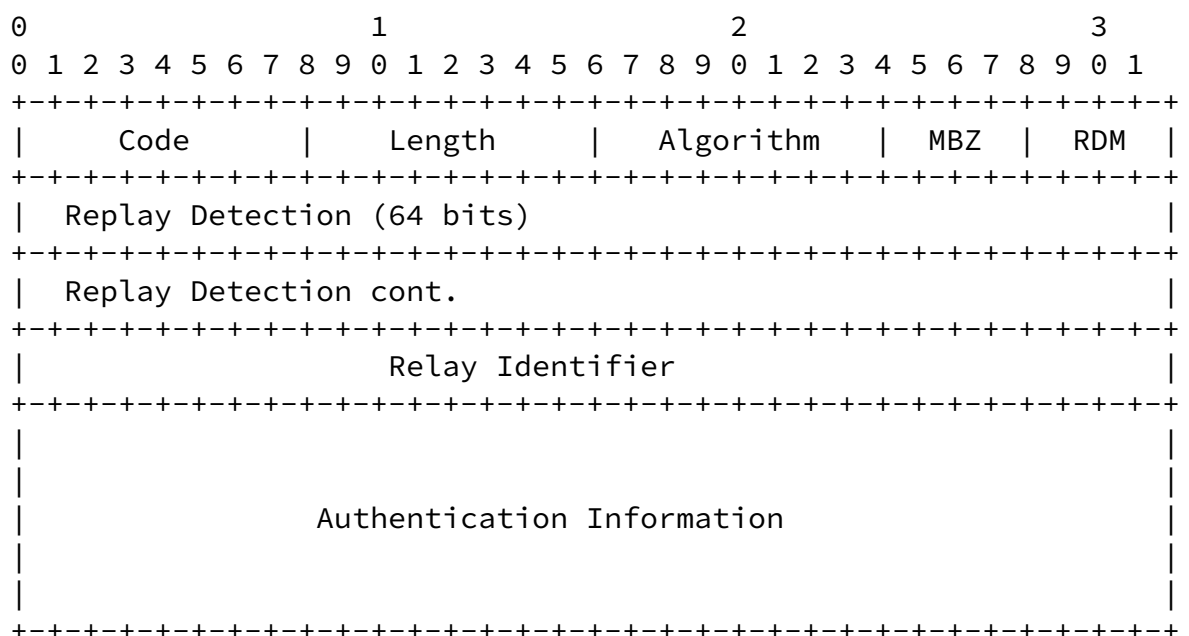
The Authentication suboption is included by relay agents that wish to ensure the integrity of the data they include in the Relay Agent option. These relay agents are configured with the parameters necessary to generate cryptographically strong signatures of the data in the DHCP messages which they forward to DHCP servers. A DHCP server configured to process the Authentication suboption uses the information in the suboption to validate the signature in the suboption, and continues processing the relay agent information option only if the signature is valid. If the DHCP server sends a response, it includes an Authentication suboption in its response message, signing the data in its message. Relay agents check the signatures in DHCP server responses and decide whether to forward the responses based on the signatures' validity.

The second mechanism specifies the use of IPsec between relay agents and servers to authenticate the identity of the source and contents of messages carrying relay agent options.

[4.](#) Relay Agent Option Authentication Sub-option

The Relay Agent Option Authentication Sub-option, described in this section of the document, provides identity authentication, detection of modification of message contents and protection against message replay.

[4.1](#) Suboption Format



The code for the suboption is TBD. The length field includes the lengths of the algorithm, RDM, and all subsequent suboption fields in octets.

The Algorithm field defines the algorithm used to generate the authentication information.

Four bits are reserved for future use. These bits SHOULD be set to zero, and MUST be ignored when the suboption is processed.

The Replay Detection Method (RDM) field defines the method used to generate the Replay Detection Data.

The Replay Detection field contains a value used to detect replayed messages, interpreted according to the RDM.

The Relay Identifier field is used by relay agents that do not set giaddr, as described in [RFC 3046](#) [2], Section 2.1.

The Authentication Information field contains the data required to communicate algorithm-specific parameters, as well as the signature. The signature is usually a digest of the data in the DHCP packet computed using the method specified by the Algorithm field.

[4.2](#) Replay Detection

The replay-detection mechanism is based on the notion that a receiver can determine whether or not a message has a valid replay token value. The default RDM, with value 1, specifies that the Replay Detection field contains an increasing counter value. The receiver associates a replay counter with each sender, and rejects any message containing an authentication suboption with a Replay Detection counter value less than the last valid value. DHCP servers MAY identify relay agents by giaddr value or by other data in the message (e.g. data in other relay agent suboptions). Relay agents identify DHCP servers by source IP address. If the message's replay detection value is valid, and the signature is also valid, the receiver updates the its notion of the last valid replay counter value associated with

the sender.

All implementations MUST support the default RDM. Additional methods may be defined in the future, following the process described in [Section 6](#).

Receivers SHOULD perform the replay-detection check before validating the signature. The authentication hash calculation is likely to be much more expensive than the replay-detection value check.

DISCUSSION:

This places a burden on the receiver to maintain some run-time state (the most-recent valid counter value) for each sender, but the number of members in a DHCP agent-server system is unlikely to be unmanageably large.

[4.3](#) The Relay Identifier Field

The Relay Agent Information Option [\[2\]](#) specification permits a relay agent to add a relay agent option to relayed messages without setting the giaddr field. In this case, the eventual receiver of the message needs a stable identifier to use in order to associate per-sender state such as Key ID and replay-detection counters.

A relay agent that adds a relay agent information option and sets giaddr MUST NOT set the Relay ID field. A relay agent that does not set giaddr MAY be configured to place a value in the Relay ID field. If the relay agent is configured to use the Relay ID field, it MAY be configured with a value to use, or it MAY be configured to generate a value based on some other data, such its MAC or IP addresses. If a relay agent generates a Relay ID value it SHOULD select a value that

it can regenerate reliably, e.g. across reboots.

Servers that process an Authentication Suboption SHOULD use the giaddr value to identify the sender if the giaddr field is set. Servers MAY be configured to use some other data in the message to identify the signer. If giaddr is not set, the server SHOULD use the Relay ID field if it is non-zero. If neither the giaddr nor the

Relay ID field is set, the server MAY be configured to use some other data in the message, or it MAY increment an error counter.

[4.4](#) Computing Authentication Information

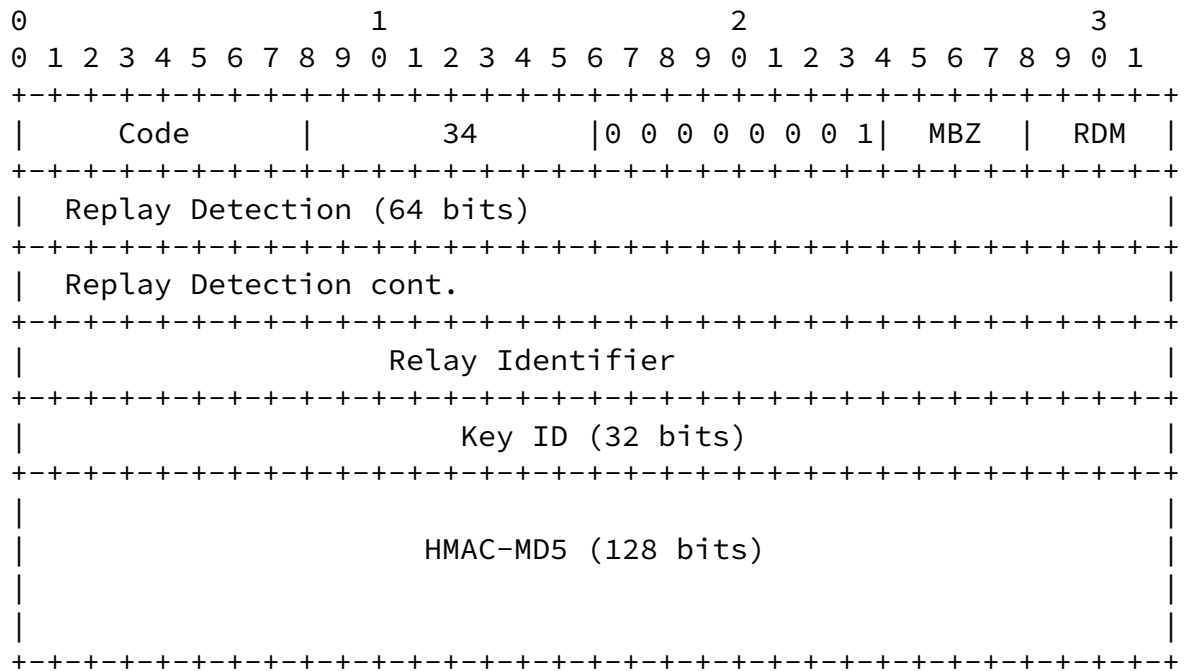
The Authentication Information field contains a computed signature, generated by the sender. All algorithms are defined to process the data in the DHCP messages in the same way. The sender and receiver compute the signature across a buffer containing all of the bytes in the DHCP message, including the fixed DHCP message header, the DHCP options, and the relay agent suboptions, with the following exceptions. The value of the 'hops' field MUST be set to zero for the computation, because its value may be changed in transmission. The value of the 'giaddr' field MUST also be set to zero for the computation because it may be modified in networks where one relay agent adds the relay agent option but another relay agent sets 'giaddr' (see [RFC 3046, section 2.1](#)). In addition, because the relay agent option itself is included in the computation, the 'signature' part of the 'authentication information' field in the Authentication suboption is set to all zeroes. The relay agent option length, the Authentication suboption length and other Authentication suboption fields are all included in the computation.

All implementations MUST support Algorithm 1, the HMAC-MD5 algorithm. Additional algorithms may be defined in the future, following the process described in [Section 6](#).

[4.4.1](#) The HMAC-MD5 Algorithm

Algorithm 1 is assigned to the HMAC [\[3\]](#) protocol, using the MD5 [\[4\]](#) hash function. This algorithm requires that a shared secret key be configured at the relay agent and the DHCP server. A 32-bit Key Identifier is associated with each shared key, and this identifier is carried in the first 4 bytes of the Authentication Information field of the Authentication suboption. The HMAC-MD5 computation generates a 16-byte signature, which is placed in the Authentication Information field after the Key ID.

The format of the Authentication suboption when Algorithm 1 is used is:



The suboption length is 34. The RDM and Replay Detection fields are as specified in [Section 4.2](#). The Relay ID field is set as specified in [Section 4.3](#). The Key ID is set by the sender to the ID of the key used in computing the signature, as an integer value in network byte-order. The HMAC signature follows the Key ID.

The Key ID exists only to allow the sender and receiver to specify a shared secret in cases where more than one secret is in use among a network's relays and DHCP servers. The Key ID values are entirely a matter of local configuration; they only need to be locally unique. This specification does not define any semantics or impose any requirements on this algorithm's Key ID values.

DISCUSSION:

We specify a four-byte Key ID, following the example of the DHCP Authentication RFC. Other authentication protocols, like DNS TSIG [\[12\]](#), use a key name. A key name is more flexible and potentially more human-readable than a key id. DHCP servers may well be configured to use key names for DNS updates using TSIG, so it might simplify DHCP server configuration if some of the key-management for both protocols could be shared.

On the other hand, it is crucial to minimize the size expansion caused by the introduction of the relay agent information option. Named keys would require more physical space, and would entail more complex suboption encoding and parsing implementations.

These considerations have led us to specify a fixed-length Key ID instead of a variable-length key name.

[4.5](#) Procedures for Sending Messages

[4.5.1](#) Replay Detection

The sender obtains a replay-detection counter value to use, based on the RDM it is using. If the sender is using RDM 1, the default RDM, the value **MUST** be greater than any previously-sent value.

[4.5.2](#) Packet Preparation

The sender sets the 'giaddr' field and the 'hops' field to all zeroes. The sender appends the relay agent information option to the client's packet, including the Authentication suboption. The sender selects an appropriate Replay Detection value. The sender places its identifier into the Relay ID field, if necessary, or sets the field to all zeroes. The sender sets the suboption length, places the Replay Detection value into the Replay Detection field of the suboption, and sets the algorithm to the algorithm number that it is using. If the sender is using HMAC-MD5, it sets the Key ID field to the appropriate value. The sender sets the field which will contain the signature to all zeroes. Other algorithms may specify additional preparation steps.

[4.5.3](#) Signature Computation

The sender computes the signature across the entire DHCP message, using the algorithm it has selected. The sender places the result of the computation into the signature field of the Authentication suboption.

[4.5.4](#) Sending the Message

The sender restores the values of the 'hops' and 'giaddr' fields, and sends the message.

[4.6](#) Procedures for Processing Incoming Messages

[4.6.1](#) Initial Examination

The receiver examines the message, the value of the giaddr field, and determines whether the packet includes the relay agent information option. The receiver uses its configuration to determine whether it should expect an Authentication suboption. The receiver MAY be configured to drop incoming messages that do not contain a valid

relay agent information option and Authentication suboption.

If the receiver determines that the Authentication suboption is present and that it should process the suboption, it uses the data in the message to determine which algorithm, key, and RDM to use in validating the message. If the receiver cannot determine which algorithm, key, and RDM to use, or if it does not support the value indicated in the message, it SHOULD drop the message. Because this situation could indicate a misconfiguration which could deny service to clients, receivers MAY attempt to notify their administrators or log an error message.

[4.6.2](#) Replay Detection Check

The receiver examines the RDM field. Receivers MUST discard messages containing RDM values that they do not support. Because this may indicate a misconfiguration at the sender, an attempt SHOULD be made to indicate this condition to the administrator, by incrementing an error counter or writing a log message. If the receiver supports the RDM, it examines the value in the Replay Detection field using the procedures in the RDM and in [Section 4.2](#). If the Replay value is not valid, the receiver MUST drop the message.

Note that the receiver MUST NOT update its notion of the last valid Replay Detection value for the sender at this point. Until the signature has been checked, the Replay Detection field cannot be trusted. If the receiver trusts the Replay Detection value without checking the signature, a malicious host could send a replayed message with a Replay Detection value that was very high, tricking the receiver into rejecting legitimate values from the sender.

[4.6.3](#) Signature Check

The receiver prepares the packet in order to check the signature. The receiver sets the 'giaddr' and 'hops' fields to zero, and sets the signature field of the Authentication suboption to all zeroes.

Using the algorithm and key associated with the sender, the receiver computes a hash of the message. The receiver compares the result of its computation with the value sent by the sender. If the signatures do not match, the receiver MUST drop the message. Otherwise, the receiver updates its notion of the last valid Replay Detection value associated with the sender, and processes the message.

[4.7](#) Relay Agent Behavior

DHCP Relay agents are typically configured with the addresses of one or more DHCP servers. A relay agent that implements this suboption requires an algorithm number for each server, as well as appropriate

Stapp, et al.

Expires December 6, 2003

[Page 10]

Internet-Draft

Authentication Suboption

June 2003

credentials (i.e. keys) to use. Relay implementations SHOULD support configuration which indicates that all relayed messages should include the authentication suboption. Use of the authentication suboption SHOULD be disabled by default. Relay agents MAY support configuration that indicates that certain destination servers support the authentication suboption, while other servers do not. Relays MAY support configuration of a single algorithm number and key to be used with all DHCP servers, or they MAY support configuration of different algorithms and keys for each server.

[4.7.1](#) Receiving Messages from Other Relay Agents

There are network configurations in which one relay agent adds the relay agent option, and then forwards the DHCP message to another relay. For example, a layer-2 switch might be directly connected to a client, and it might forward messages to an aggregating router, which sets giaddr and then forwards the message to a DHCP server. When a DHCP relay which implements the Authentication suboption receives a message, it MAY use the procedures in [Section 4.6](#) to verify the source of the message before forwarding it.

[4.7.2](#) Sending Messages to Servers

When the relay agent receives a broadcast packet from a client, it determines which DHCP servers (or other relay agents) should receive copies of the message. If the relay agent is configured to include the Authentication suboption, it determines which Algorithm and RDM to use, and then it performs the steps in [Section 4.5](#).

[4.7.3](#) Receiving Messages from Servers

When the relay agent receives a message, it determines from its configuration whether it expects the message to contain a relay agent information option and an Authentication suboption. The relay agent MAY be configured to drop response messages that do not contain the Authentication suboption. The relay agent then follows the procedures in [Section 4.6](#).

[4.8](#) DHCP Server Behavior

DHCP servers may interact with multiple relay agents. Server implementations MAY support configuration that associates the same algorithm and key with all relay agents. Servers MAY support configuration which specifies the algorithm and key to use with each relay agent individually.

Stapp, et al.

Expires December 6, 2003

[Page 11]

Internet-Draft

Authentication Suboption

June 2003

[4.8.1](#) Receiving Messages from Relay Agents

When a DHCP server which implements the Authentication suboption receives a message, it performs the steps in [Section 4.6](#).

[4.8.2](#) Sending Reply Messages to Relay Agents

When the server has prepared a reply message, it uses the incoming request message and its configuration to determine whether it should include a relay agent information option and an Authentication suboption. If the server is configured to include the Authentication suboption, it determines which Algorithm and RDM to use, and then performs the steps in [Section 4.5](#).

DISCUSSION:

This server behavior represents a slight variance from [RFC 3046](#) [2], Section 2.2. The Authentication suboption is not echoed back from the server to the relay: the server generates its own suboption.

[5.](#) Use of IPsec to secure DHCP messages

Relay agents and servers that exchange messages securely can use IPsec mechanisms [\[5\]](#) as described in this section. Relay agents and servers MUST support manual configuration and installation of static keys. If a client message is relayed through multiple relay agents, each of the relay agents must have established independent, pairwise trust relationships. That is, if messages from client C will be relayed by relay agent A to relay agent B and then to the server, relay agents A and B must be configured to use IPsec for the messages they exchange, and relay agent B and the server must be configured to use IPsec for the messages they exchange.

Relay agents and servers that support secure relay agent to server or relay agent to relay agent communication, MUST include an IPsec implementation with the following restrictions:

- o The IPsec implementation MUST use ESP [\[6\]](#)
- o Packet authentication MUST be applied
- o Encryption MAY be applied (i.e., NULL encryption can be used)

[6.](#) IANA Considerations

[Section 4.1](#) defines a new suboption for the DHCP relay agent option, called the Authentication Suboption. IANA is requested to allocate a new suboption code from the relay agent option suboption number space.

This specification introduces two new number-spaces for the Authentication suboption's 'Algorithm' and 'Replay Detection Method' fields. These number spaces are to be created and maintained by IANA.

The Algorithm identifier is a one-byte value. Algorithm value 0 is reserved. Algorithm value 1 is assigned to the HMAC-MD5 signature as defined in [Section 4.4.1](#). Additional algorithm values will be

allocated and assigned through IETF consensus, as defined in [RFC 2434 \[7\]](#).

The RDM identifier is a four-bit value. RDM value 0 is reserved. RDM value 1 is assigned to the use of a monotonically increasing counter value as defined in [Section 4.2](#). Additional RDM values will be allocated and assigned through IETF consensus, as defined in [RFC 2434 \[7\]](#).

[7](#). Security Considerations

This specification describes two mechanisms that can be used to provide authentication and message integrity protection to the messages between DHCP relay agents and DHCP servers.

The use of the authentication sub-option protocol imposes a new computational burden on relay agents and servers, because they must perform cryptographic hash calculations when they send and receive messages. This burden may add latency to DHCP messages exchanges. Because relay agents are involved when clients reboot, periods of very high reboot activity will result in the largest number of messages which have to be signed and verified. During a cable MSO head-end reboot event, for example, the time required for all clients to be served may increase.

[7.1](#) Authentication sub-option Protocol Considerations

Because DHCP is a UDP protocol, messages between relays and servers may be delivered in a different order than the order in which they were generated. The replay-detection mechanism will cause receivers to drop packets which are delivered 'late', leading to client retries. The retry mechanisms which most clients implement should not cause this to be an enormous issue, but it will cause senders to

do computational work which will be wasted if their messages are re-ordered.

The authentication sub-option protocol requires configuration of relay agents and servers with shared secret keys.

[7.2](#) IPsec Considerations

The use of IPsec for securing relay agent options in DHCP messages requires the existence of an IPsec implementation available to the relay agents and DHCP servers. It also requires manual configuration of the participants, including manual distribution of keys.

8. Acknowledgements

The need for this specification was made clear by comments made by Thomas Narten and John Schnizlein, and the use of the DHCP Authentication option format was suggested by Josh Littlefield, at IETF 53.

Normative references

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997.
- [2] Patrick, M., "DHCP Relay Agent Information Option", [RFC 3046](#), January 2001.
- [3] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", [RFC 2104](#), February 1997.
- [4] Rivest, R., "The MD5 Message Digest Algorithm", [RFC 1321](#), April 1992.
- [5] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.
- [6] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.
- [7] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [RFC 2434](#), October 1998.

Informative References

- [8] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.

- [9] Croft, B. and J. Gilmore, "Bootstrap Protocol", [RFC 951](#),

September 1985.

- [10] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol", [RFC 1542](#), October 1993.
- [11] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", [RFC 3118](#), June 2001.
- [12] Vixie, P., Gudmundsson, O., Eastlake, D. and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", [RFC 2845](#), May 2000.

Authors' Addresses

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

Phone: 978.936.1535
EMail: mjs@cisco.com

Ted Lemon
Nominum, Inc.
950 Charter St.
Redwood City, CA 94063
USA

EMail: mellon@nominum.com

Ralph Droms
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

Phone: +1 978.936.1674
EMail: rdroms@cisco.com

Full Copyright Statement

Copyright (C) The Internet Society (2003). 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 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all 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 Standards 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 FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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

Stapp, et al.

Expires December 6, 2003

[Page 16]