softwire	D. Miles
Internet-Draft	Alcatel-Lucent
Intended status: Standards Track	W. Dec
Expires: September 11, 2011	Cisco Systems
	J. Bristow
	Swisscom Schweiz AG
	R. Maglione
	Telecom Italia
	March 10, 2011

Forcerenew Nonce Authentication
draft-ietf-dhc-forcerenew-nonce-01

Abstract

DHCP Forcerenew allows for the reconfiguration of a single host by forcing the DHCP client into a Renew state on a trigger from the DHCP server. In Forcerenew Nonce Authentication the server exchanges a nonce with the client on the initial DHCP ACK that is used for subsequent validation of a Forcerenew message.

Status of this Memo

Copyright Notice

Table of Contents

*1. Introduction

*2. Requirements Language

*3. Message authentication

*3.1. Forcerenew Nonce Authentication

*3.1.1. Forcerenew Nonce Protocol Capability Option

*3.1.2. Forcerenew Nonce Protocol

*3.1.3. Server considerations for Forcerenew Nonce Authentication

*3.1.4. Client considerations for Forcerenew Nonce Authentication

*4. Acknowledgements

*5. IANA Considerations

*6. Security Considerations

*6.1. Protocol vulnerabilities

*7. References

*7.1. Normative References

*7.2. Informative References

*Authors' Addresses

1. Introduction

The DHCP Reconfigure Extension defined in [RFC3203] is a useful mechanism allowing dynamic reconfiguration of a single host triggered by the DHCP server. Its application is currently limited by a requirement that FORCERENEW message is always authenticated using procedures as described in [RFC3118]. Authentication for DHCP [RFC3118]

is mandatory for Forcerenew, however as it is currently defined [RFC3118] requires distribution of constant token or shared-secret out-of-band to DHCP clients. The mandatory authentication was originally motivated by a legitimate security concern whereby in some network environments a FORCERENEW message can be spoofed. However, in some networks native security mechanisms already provide sufficient protection against spoofing of DHCP traffic. An example of such network is a DSL Forum TR-101 [TR-101] compliant access network. In such environments the mandatory coupling between FORCERENEW and DHCP Authentication [RFC3118] can be relaxed. This document defines extensions to Authentication for DHCP(v4) Messages [RFC3118] to create a new authentication protocol for DHCPv4 Forcerenew [RFC3203] messages; this method does not require out-of-band key distribution to DHCP clients. The Forcerenew Nonce is exchanged between server and client on initial DHCP ACK and is used for verification of any subsequent Forcerenew message.

2. Requirements Language

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 [RFC2119].

3. Message authentication

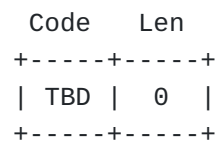
The FORCERENEW message must be authenticated using either [RFC3118] or the proposed Forcerenew Nonce Authentication protocol.

3.1. Forcerenew Nonce Authentication

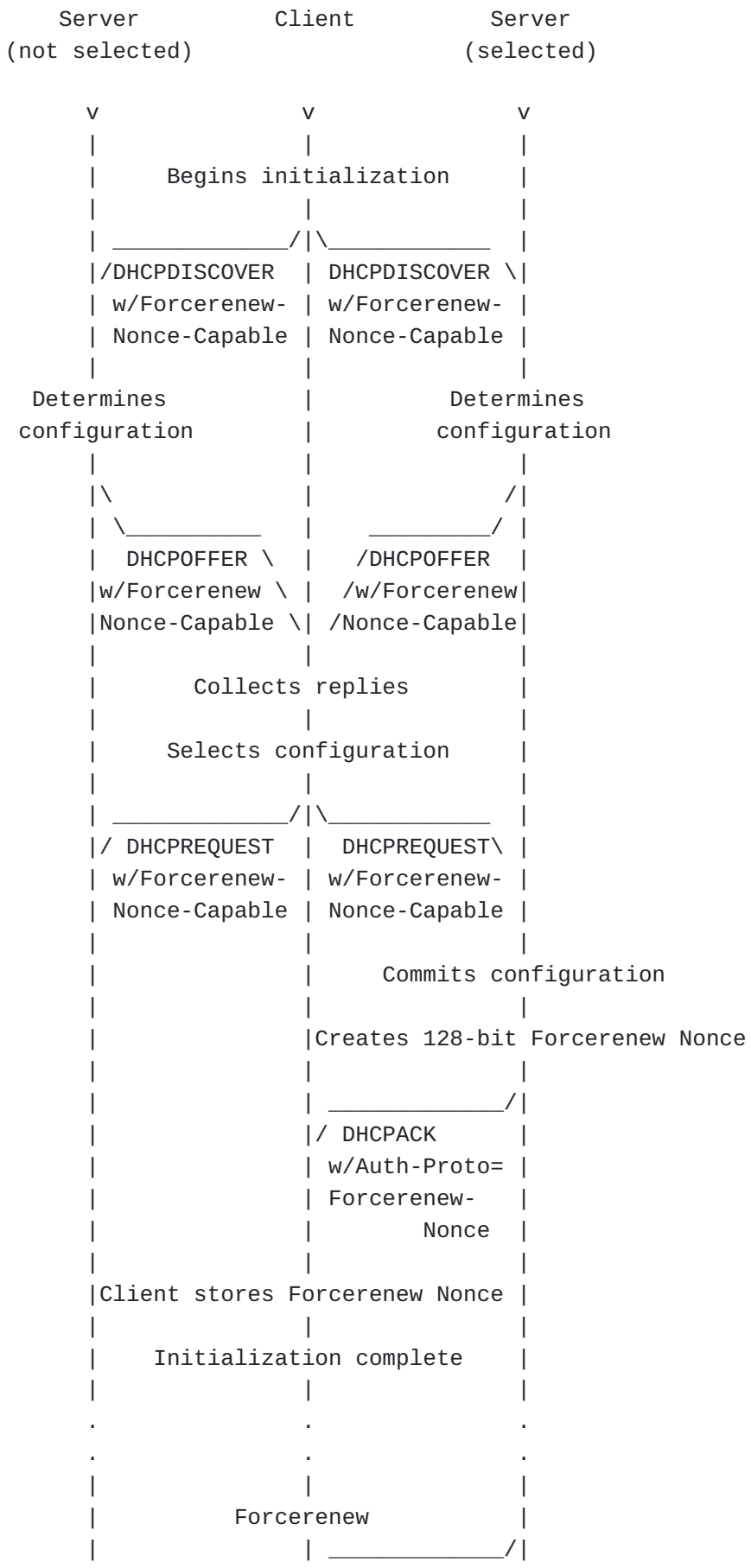
The Forcerenew nonce authentication protocol provides protection against misconfiguration of a client caused by a Forcerenew message sent by a malicious DHCP server. In this protocol, a DHCP server sends a Forcerenew nonce to the client in the initial exchange of DHCP messages. The client records the Forcerenew nonce for use in authenticating subsequent Forcerenew messages from that server. The server then includes an HMAC computed from the Forcerenew nonce in subsequent Forcerenew messages.
Both the Forcerenew nonce sent from the server to the client and the HMAC in subsequent Forcerenew messages are carried as the Authentication information in a DHCP Authentication option. The format of the Authentication information is defined in the following section.
The Forcerenew nonce protocol is used (initiated by the server) only if the client and server are not using any other authentication protocol and the client and server have negotiated to use the Forcerenew Nonce Authentication protocol.

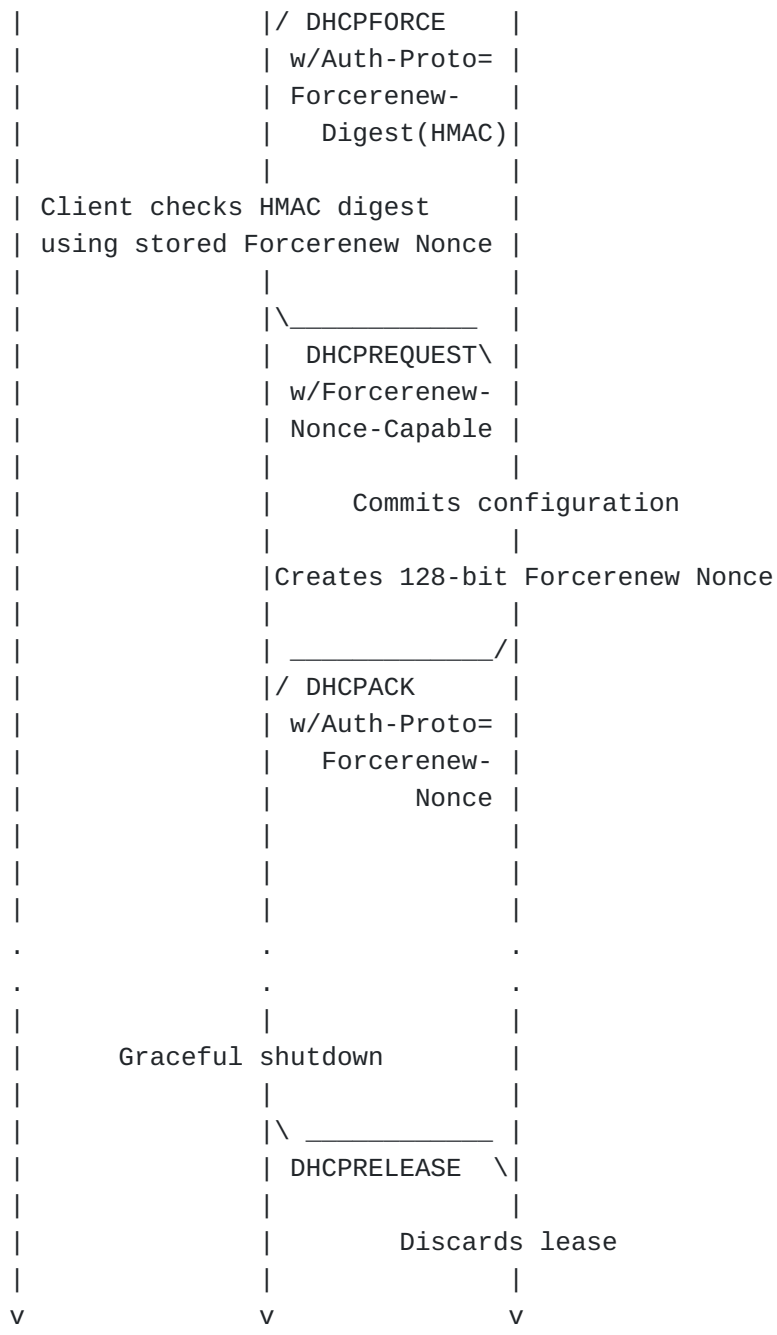
3.1.1. Forcerenew Nonce Protocol Capability Option

A DHCP client indicates DHCP Forcerenew Nonce Protocol capability by including a FORCERENEW_NONCE_CAPABLE(<TBD>) option in DHCP Discover and Request messages sent to the server.
A DHCP server that does not support Forcerenew Nonce Protocol authentication should ignore the FORCERENEW_NONCE_CAPABLE(<TBD>) option. A DHCP server indicates DHCP Forcerenew Nonce Protocol preference by including a FORCERENEW_NONCE_CAPABLE(<TBD>) option in any DHCP Offer messages sent to the client.
A DHCP client MUST NOT send DHCP messages with authentication options where the protocol value is Forcerenew Nonce Authentication(<TBD>).
The FORCERENEW_NONCE_CAPABLE option is a zero length option with code of <TDB> and format as follows:



The client would indicate that it supports the functionality by inserting the FORCERENEW_NONCE_CAPABLE option in the DHCP Discover and Request messages. If the server supports Forcerenew nonce authentication and is configured to require Forcerenew nonce authentication, it will insert the FORCERENEW_NONCE_CAPABLE option in the DHCP Offer message.


Server
(not selected)
Client
Server
(selected)
Begins initialization
DHCPDISCOVER w/Forcerenew-Nonce-Capable
DHCPDISCOVER w/Forcerenew-Nonce-Capable
Determines configuration
Determines configuration
DHCPOFFER w/Forcerenew Nonce-Capable
DHCPOFFER w/Forcerenew Nonce-Capable
Collects replies
Selects configuration
DHCPREQUEST w/Forcerenew-Nonce-Capable
DHCPREQUEST w/Forcerenew-Nonce-Capable
Commits configuration
Creates 128-bit Forcerenew Nonce
DHCPACK w/Auth-Proto= Forcerenew-Nonce
Client stores Forcerenew Nonce
Initialization complete
Forcerenew



3.1.2. Forcerenew Nonce Protocol

[RFC3118] defined an extensible DHCPv4 authentication option which supports multiple protocols. The Forcerenew Nonce Protocol makes use of the DHCP authentication option defined in [RFC3118] re-using the option format.

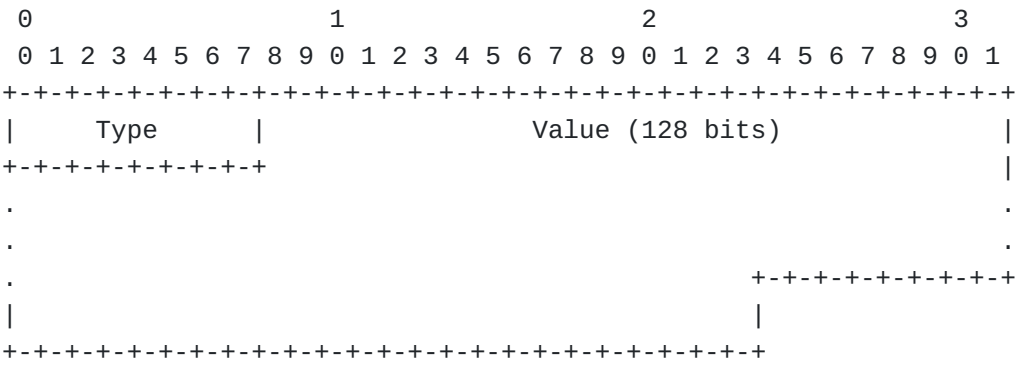
The following fields are set in an DHCP authentication option for the Forcerenew Nonce Authentication Protocol:

protocol <TBD (IANA)>

algorithm 1

RDM 0

The format of the Authentication information for the Forcerenew Nonce Authentication Protocol is:



Type Type of data in Value field carried in this option:

1 Forcerenew Nonce value (used in ACK message)

2 HMAC-MD5 digest of the message (FORCERENEW message)

Value Data as defined by field

3.1.3. Server considerations for Forcerenew Nonce Authentication

The use of Forcerenew Nonce Protocol is dependent on the client indicating its capability through the FORCERENEW_NONCE_CAPABLE(<TBD>) DHCP option in any DHCP Discover or Request messages. The DHCP Discovery or Request message from the client MUST contain the FORCERENEW_NONCE_CAPABLE(<TBD>) option if the Forcerenew Nonce Protocol is to be used by the server. The absence of the FORCERENEW_NONCE_CAPABLE(<TBD>) option indicates to the server that the Forcerenew Nonce Authentication protocol is not supported and thus the server MUST NOT include a Forcerenew Nonce Protocol Authentication option in the DHCP Ack.
The server indicates its support of the Forcerenew Nonce Protocol authentication by including the DHCP FORCERENEW_NONCE_CAPABLE(<TBDP>) option in the DHCP Offer message. The server SHOULD NOT include this option unless the client has indicated its capability in a DHCP Discovery message . The presence of the FORCERENEW_NONCE_CAPABLE(<TDB>) option in the DHCP offer may be used by clients to prefer Forcerenew nonce Protocol authentication-capable DHCP servers over those servers which do not support such capability.

The server selects a Forcerenew nonce for a client only during Request/ Ack message exchange. The server records the Forcerenew nonce and transmits that nonce to the client in an Authentication option in the DHCP Ack message.
The Forcerenew nonce is 128 bits long, and MUST be a cryptographically strong random or pseudo-random number that cannot easily be predicted. The nonce is imbedded as a 128-bit value of the Authentication information where type is set to 1 (Forcerenew nonce Value).
To provide authentication for a Forcerenew message, the server selects a replay detection value according to the RDM selected by the server, and computes an HMAC-MD5 of the Forcerenew message using the Forcerenew nonce for the client. The server computes the HMAC-MD5 over the entire DHCP Forcerenew message, including the Authentication option; the HMAC-MD5 field in the Authentication option is set to zero for the HMAC-MD5 computation. The server includes the HMAC-MD5 in the authentication information field in an Authentication option included in the Forcerenew message sent to the client with type set to 2 (HMAC-MD5 digest).

3.1.4. Client considerations for Forcerenew Nonce Authentication

The client MUST indicate Forcerenew nonce Capability by including the FORCERENEW_NONCE_CAPABLE(<TBD>) DHCP option (Section 2.1.1) in all DHCP Discover and Request messages. DHCP servers that support Forcerenew nonce Protocol authentication MUST include the DHCP Forcerenew Nonce protocol authentication option in DHCP Offers with type set to zero(0), allowing the client to use this capability in selecting DHCP servers should multiple Offers arrive.
A DHCP server has indicates its support through the inclusion of the FORCERENEW_NONCE_CAPABLE(<TBD>) option in the DHCP Offer. The client MUST validate the DHCP Ack message contains a Forcerenew Nonce in a DHCP authentication option. If the server has indicated capability for Forcerenew Nonce Protocol authentication in the DHCP Offer and a subsequent Ack omits a valid DHCP authentication option for the Forcerenew Nonce Protocol, the client MUST send a DHCP Decline message and return to the DHCP Init state.
The client will receive a Forcerenew Nonce from the server in the initial DHCP Ack message from the server. The client records the Forcerenew Nonce for use in authenticating subsequent Forcerenew messages.
To authenticate a Forcerenew message, the client computes an HMAC-MD5 over the DHCP Forcerenew message, using the Forcerenew Nonce received from the server. If this computed HMAC-MD5 matches the value in the Authentication option, the client accepts the Forcerenew message.

4. Acknowledgements

Comments are solicited and should be addressed to the DHC WG mailing list (dhcwg@ietf.org) and/or the authors. This contribution is based on

work by Vitali Vinokour. Major sections of this draft use modified text from [RFC3315]. The authors wish to thank Ted Lemon and Bernie Volz for their support.

5. IANA Considerations

This document requests IANA to allocate an option code for the newly defined DHCP option FORCERENEW_NONCE_CAPABALE as described in the text.
This document requests IANA to allocate a DHCP Authentication Option(90) protocol number be assigned for Forcerenew Nonce Authentication, per [RFC3118].
This document requests IANA to create a new namespace associated with the Forcerenew Nonce Authentication protocol: algorithm, per [RFC3118].

6. Security Considerations

As in some network environments FORCERENEW can be used to snoop and spoof traffic, the FORCERENEW message MUST be authenticated using the procedures as described in [RFC3118] or this proposal. In this proposal any party able intercept the nonce exchange could impersonate a server and thus offers no protection from man-in-the- middle attacks.
FORCERENEW messages failing the authentication should be silently discarded by the client.

6.1. Protocol vulnerabilities

The mechanism described in this document is vulnerable to a denial of service attack through flooding a client with bogus FORCERENEW messages. The calculations involved in authenticating the bogus FORECERENEW messages may overwhelm the device on which the client is running.
The mechanism described provides protection against the use of a FORCERENEW message by a malicious DHCP server to mount a denial of service or man-in-the-middle attack on a client. This protocol can be compromised by an attacker that can intercept the initial message in which the DHCP server sends the nonce to the client.

7. References

7.1. Normative References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC3118]	Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.
[RFC3203]	T'Joens, Y., Hublet, C. and P. De Schrijver, "DHCP reconfigure extension", RFC 3203, December 2001.

7.2. Informative References

[TR-101]	Cohen et al, , "Architecture & Transport: "Migration to Ethernet Based DSL Aggregation, DSL Forum TR-101", 2005.
[RFC3315]	Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

Authors' Addresses

David Miles Miles Alcatel-Lucent L3 / 215 Spring St Melbourne, Victoria 3000, Australia Phone: +61 3 9664 3308 EMail: david.miles@alcatel-lucent.com

Wojciech Dec Dec Cisco Systems Haarlerbergpark Haarlerbergweg 13-19 Amsterdam, NOORD-HOLLAND 1101 CH Netherlands EMail: wdec@cisco.com

James Bristow Bristow Swisscom Schweiz AG Zentweg 9 Bern, 3050, Switzerland EMail: James.Bristow@swisscom.com

Roberta Maglione Maglione Telecom Italia Via Reiss Romoli 274 Torino, 10148 Italy EMail: roberta.maglione@telecomitalia.it