

dhc
Internet-Draft
Updates: [3203](#) (if approved)
Intended status: Standards Track
Expires: August 17, 2012

D. Miles
Google
W. Dec
Cisco Systems
J. Bristow
Swisscom Schweiz AG
R. Maglione
Telecom Italia
February 14, 2012

Forcerenew Nonce Authentication
draft-ietf-dhc-forcerenew-nonce-04

Abstract

Dynamic Host Configuration Protocol (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 sends a nonce to the client on the initial DHCP ACK that is used for subsequent validation of a FORCERENEW message. This document updates [RFC 3203](#).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on August 17, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Requirements Language	3
3.	Message authentication	3
3.1.	Forcerenew Nonce Authentication	3
3.1.1.	Forcerenew Nonce Protocol Capability Option	4
3.1.2.	Forcerenew Nonce Protocol	6
3.1.3.	Server considerations for Forcerenew Nonce Authentication	8
3.1.4.	Client considerations for Forcerenew Nonce Authentication	9
4.	Acknowledgements	10
5.	IANA Considerations	10
6.	Security Considerations	10
6.1.	Protocol vulnerabilities	11
7.	References	11
7.1.	Normative References	11
7.2.	Informative References	11
	Authors' Addresses	12

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 DHCP messages can be spoofed and an attacker could more accurately guess the timing of DHCP renewal messages by first sending a FORCERENEW message. However, in some networks native security mechanisms already provide sufficient protection against spoofing of DHCP traffic. An example of such network is a Broadband Forum TR-101 [\[TR-101i2\]](#) compliant access network. In such environments the mandatory coupling between FORCERENEW and DHCP Authentication [\[RFC3118\]](#) can be relaxed and a lighter authentication mechanism can be used for the FORCERENEW message. This document defines extensions to Authentication for DHCPv4 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. This document updates [\[RFC3203\]](#)

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 the authentication mechanism specified in [[RFC3118](#)] 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>).

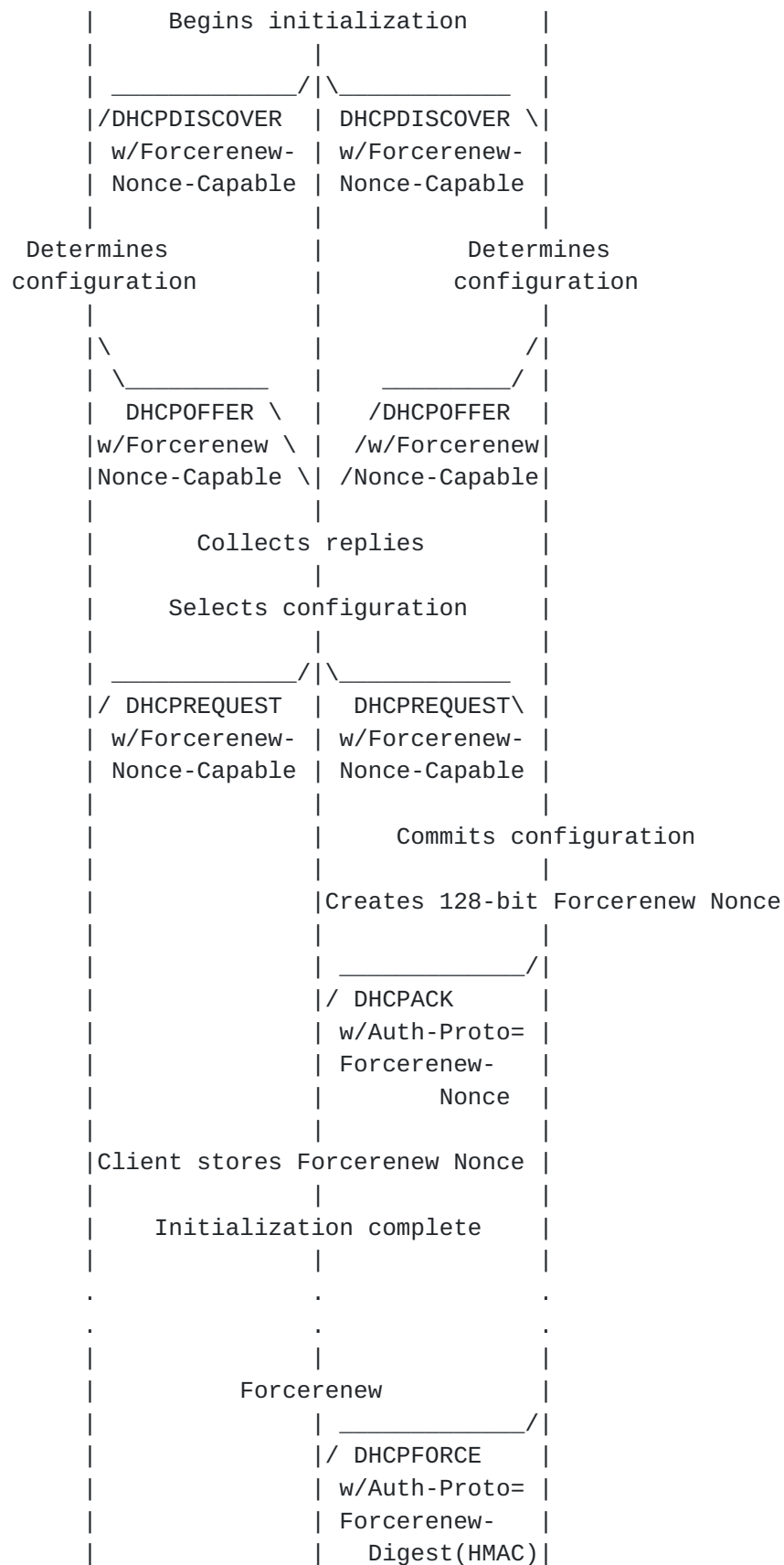
The FORCERENEW_NONCE_CAPABLE option is a zero length option with code of <TBD> and format as follows:

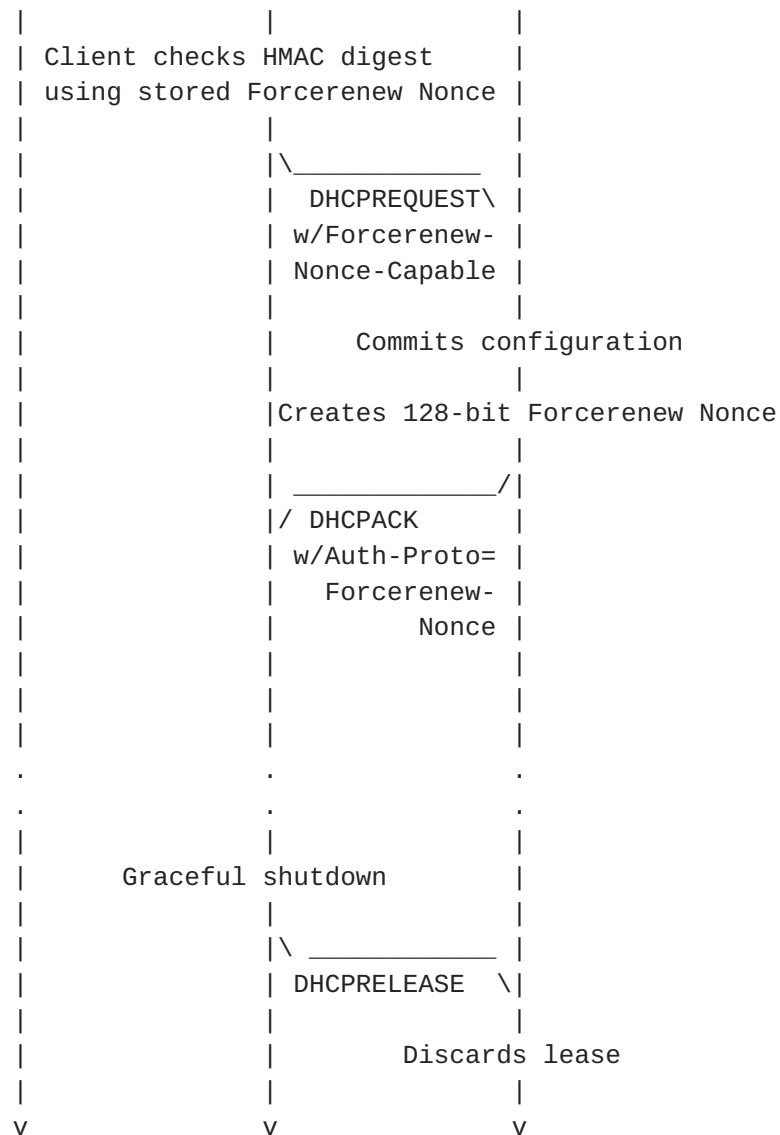
```

Code    Len
+-----+-----+
| TBD |  0  |
+-----+-----+
```

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 requires Forcerenew nonce authentication, it will insert the FORCERENEW_NONCE_CAPABLE option in the DHCP Offer message.

Server (not selected)	Client	Server (selected)
v	v	v





3.1.2. Forcerenew Nonce Protocol

The Forcerenew Nonce Protocol makes use of both the DHCP authentication option defined in [\[RFC3118\]](#) re-using the option format and of the Reconfigure Key Authentication Protocol defined in [\[RFC3315\]](#).

The following diagram defines the format of the DHCP authentication option:


```

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   |   Protocol   |   Algorithm   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   RDM     | Replay Detection (64 bits) |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  Replay cont. |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|  Replay cont. |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
|           Authentication Information
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

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

code 90

length field contains the length of the protocol

protocol 3

algorithm 1

Replay Detection field is per the Replay Detection Method (RDM)

Replay Detection Method (RDM) 0

Authentication Information: specified below

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

option in the DHCP Ack message.

The server SHOULD NOT include the nonce in an ACK when responding to a renew unless a nonce was generated. This minimizes the number of times the nonce is sent over the wire.

If the server to which the DHCP Request message was sent at time T1 has not responded, the client enters the REBINDING state and attempts to contact any server. The new Server receiving the DHCP message MUST generate a new nonce.

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 embedded 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, based on the procedure specified in [section 21.5 of \[RFC3315\]](#), using the Forcerenew nonce for the client. The server computes the HMAC-MD5, based on the procedure specified in [section 21.5 of \[RFC3315\]](#), 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

A client that supports this mechanism MUST indicate Forcerenew nonce Capability by including the FORCERENEW_NONCE_CAPABLE(<TBD>) DHCP option defined in [Section 3.1.1](#) in all DHCP Discover and Request messages. DHCP servers that support Forcerenew nonce Protocol authentication MUST include the FORCERENEW_NONCE_CAPABLE(<TBD>) DHCP option in all DHCP Offers, allowing the client to use this capability in selecting DHCP servers should multiple Offers arrive.

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 the subsequent ACK received by the client while in the selecting state omits a valid DHCP authentication option for the Forcerenew Nonce Protocol, the client MUST discard the message and return to the INIT stat

The client MUST record the Forcerenew Nonce from any valid ACK it receives, if the ACK contains one.

To authenticate a Forcerenew message, the client computes an HMAC-MD5, based on the procedure specified in [section 21.5 of \[RFC3315\]](#), 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, Matthew Ryan and Bernie Volz for their support.

5. IANA Considerations

This document requests IANA to assign the following new DHCPv4 option code from the registry "BOOTP Vendor Extensions and DHCP Options" maintained at <http://www.iana.org/assignments/bootp-dhcp-parameters>:

Tag: TBD

Name: FORCERENEW_NONCE_CAPABALE

Data length: 1

Description: Forcerenew Nonce Capable

Reference: this document

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.

The mechanism in [\[RFC3315\]](#) for DHCPv6, which this document mirrors for DHCPv4, uses a nonce to prevent an off-link attacker from successfully triggering a renewal on a client by sending DHCPFORCERENEW; since the attacker is off-link, it doesn't have the nonce, and can't force a renewal.

An on-link attacker can always simply watch the DHCP renewal message go out and respond to it, so this mechanism is useless for preventing on-link attacks, and hence the security of the nonce in the case of on-link attacks isn't relevant. Any party able to 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 FORCERENEW 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.
- [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.

7.2. Informative References

- [TR-101i2] Anschutz, T., "Migration to Ethernet-Based Broadband Aggregation Broadband Forum TR-101 Issue 2", July 2011.

Authors' Addresses

David Miles
Google

Phone:
Fax:
Email:
URI:

Wojciech Dec
Cisco Systems
Haarlerbergpark Haarlerbergweg 13-19
Amsterdam, NOORD-HOLLAND 1101 CH
Netherlands

Phone:
Fax:
Email: wdec@cisco.com
URI:

James Bristow
Swisscom Schweiz AG
Zentweg 9
Bern, 3050,
Switzerland

Phone:
Fax:
Email: James.Bristow@swisscom.com
URI:

Roberta Maglione
Telecom Italia
Via Reiss Romoli 274
Torino 10148
Italy

Phone:
Email: roberta.maglione@telecomitalia.it

