Forcerenew Key Authentication

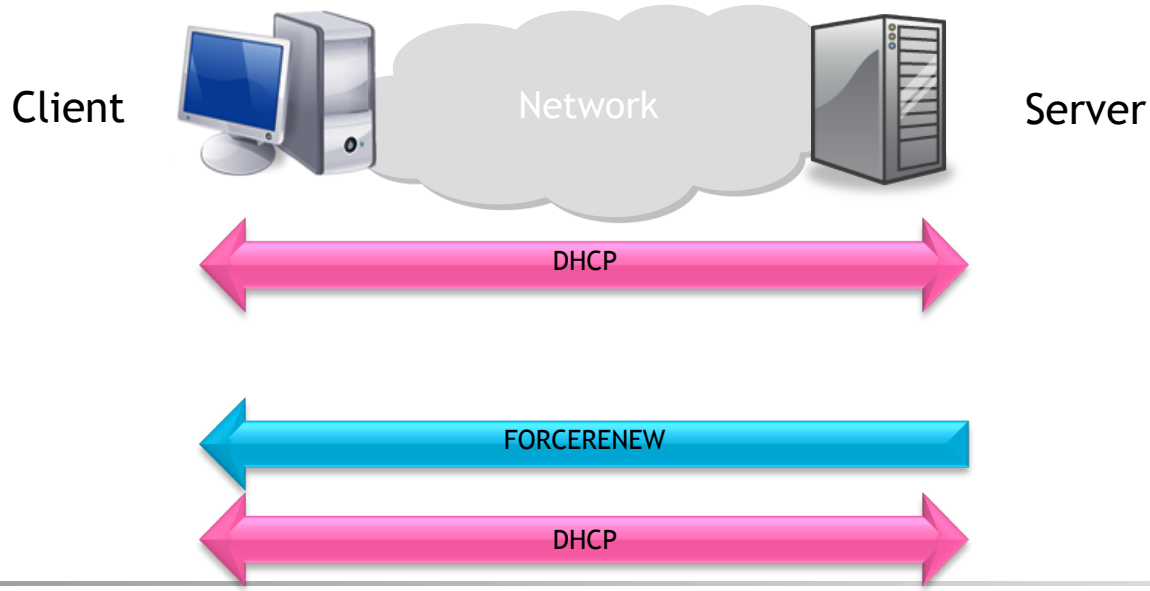
draft-miles-dhc-forcerenew-key-01

David Miles david.miles@alcatel-lucent.com
Wojciech Dec wdec@cisco.com
James Bristow james.bristow@swisscom.com
Roberta Maglione roberta.maglione@telecomitalia.it

IETF 74 – DHC Working Group

Problem Statement

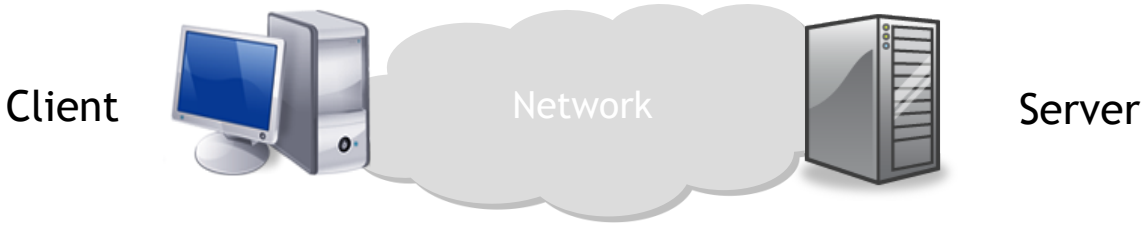
- Forcerenew is used to set the DHCP client to the RENEW state and change host parameters
- Current forcerenew (RFC 3203) requires token authentication from DHCP server to client
- The current authentication (RFC 3118) scheme uses shared secrets distributed out-of-band – not always practical to deploy in advance



Proposal

- Define an extension to Authentication for DHCP[v4] Messages (RFC 3118)
- Define the use of Forcerenew Key Authentication to exchange a key with the DHCP client during initial DHCP exchange
- The key is used by the client to validate a server forcerenew message is valid
- Clients indicate their capability through a new zero length option: Forecrenew_Key_Capable
- Mirrors the functionality in DHCPv6 (RFC 3315) – equivalent to the Reconfigure Key Authentication protocol
- Parameters to change are not sent in the Forcerenew message – RFC 3203 defines that the server shall NAK a renewing client in order to change parameters – forces the client into INIT state

Initial DHCP Exchange



DHCP Discover
w/ Forcerenew-Key-Capable option

DHCP Offer
w/ Forcerenew-Key-Capable option

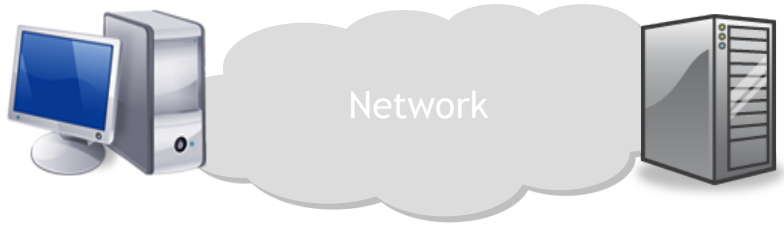
DHCP Request
w/ Forcerenew-Key-Capable option

Commit Configuration
Generate 128-bit Forcerenew Key

DHCP Ack
Authentication-Protocol: Forcerenew Key Protocol
Type: Key
Value: *<128-bit key>*

Commit Configuration
Client stores Forcerenew Key

Forcerenew Operation



Forcerenew
Retrieve 128-bit Forcerenew Key
HMAC-MD5 entire Forcerenew message

DHCP Force
Authentication-Protocol: Forcerenew Key Protocol
Type: HMAC-MD5 Digest
Value: *<128-bit digest>*

Retrieve Key
Client retrieves Forcerenew Key
Calculates HMAC-MD5 Digest & compares

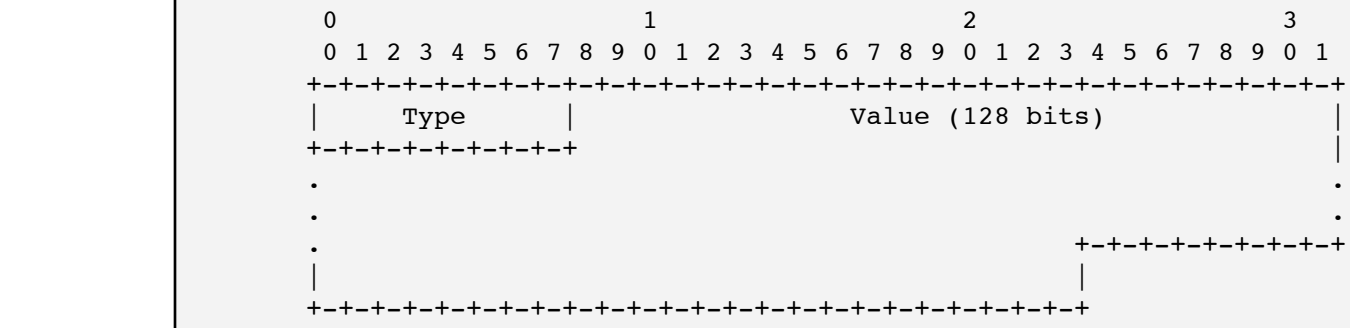
DHCP Request
w/ Forcerenew-Key-Capable option

Commit Configuration
Generate 128-bit Forcerenew Key

DHCP Ack
Authentication-Protocol: Forcerenew Key Protocol
Type: Key
Value: *<128-bit key>*

New Things

```
protocol  <TBD (IANA)>
algorithm  1
RDM  0
```




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

             1   Forcerenew Key value (used in ACK message).

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

  Value   Data as defined by field.
```

```
 The FORCERENEW_KEY_CAPABLE option is a zero length option with code
of <TDB> and format as follows:
       Code   Len
      +-----+-----+
      | TBD |  0  |
      +-----+-----+
```