DHCP Reconfigure Extension Option

draft-vinokour-dhcp-reconfigure-option-00

Vitali Vinokour
Wojciech Dec
James Bristow
David Miles

dhc WG meeting
IETF-72, 2008/07/29

Introduction

- RFC 3203 "DHCP reconfigure extension“ defines FORCERENEW message
- Allows the server to drive lease RENEWAL
- Applications:
  - Network reconfiguration
  - Change or interruption in subscriber service without waiting for lease expiration

Given wide deployment of DHCP based subscriber management, one would assume similarly wide usage of FORCERENEW in access networks.

But it is rarely used.

WHY?

Problem Statement

- There appear to be two issues with FORCERENEW:
  1. "The FORCERENEW message MUST be authenticated using the procedures as described in RFC 3118."
  2. Lack of FORCERENEW support in common DHCP stacks.
- Issue 2 is secondary in Service Provider circles since the DHCP stack is that of the RG which can be made to an SP's specification.
- Issue 1 is more serious. RFC3118 is not feasible in access networks because:
  - It assumes out-of-band exchange of a shared secret
  - It puts significant burden on aggregation equipment that needs to store keys and validate messages for tens and hundreds of thousands of DHCP sessions
  - It is superfluous in Broadband Forum TR-101 networks that provide native security mechanisms

Proposal

Relax strict authentication requirement for FORCERENEW messages:

Define a mechanism whereby DHCP server and client negotiate use of FORCERENEW without authentication.

Details

- Define new DHCP option TBD instructing client to enable processing of unauthenticated FORCERENEW messages:

```
 Code   Len  Value
+-----+-----+-----+
| TBD |  1  | 0/1 |
+-----+-----+-----+
```

- Client indicates support of the new functionality by inserting a Parameter List Request option containing option TBD in DHCPDISCOVER and DHCPREQUEST
- Server then inserts option TBD in DHCPOFFER and DHCPACK with value indicating whether to enable or disable processing of unauthenticated FORCERENEW

Discussion

- Default behavior is unchanged
- Network Admin or Service Provider control usage of unauthenticated FORCERENEW via DHCP server configuration
- Certain classes of networks (e.g. TR-101 access networks) have their own security mechanisms
- Unauthenticated FORCERENEW can be promptly disabled via the same mechanism that is used to enable it

Next Steps

- Adopt the draft as dhc WG item
- Approve new DHCP option