A Simple Way of DHCP Authentication Extension For DSL Connection
draft-li-dhc-simple-dsl-auth-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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/1id-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 October 8, 2009.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document defines option extension of Dynamic Host Configuration Protocol (DHCP) to provide a simple EAP-based authentication for DSL connection. The DHCP client is triggered by short lease time for EAP
message exchanges.

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 RFC 2119 [RFC2119].

Table of Contents

1. Introduction ................................................... 3
2. DHCP Auth Option Format ........................................ 3
   2.1. DHCP Authentication Protocol Option ....................... 4
   2.2. DHCP EAP-Message Option ................................... 4
3. Protocol Operations .............................................. 4
   3.1. Message flow when DHCP server co-located with BNG ....... 4
   3.2. Message flow when DHCP server and BNG are separated ... 6
4. Re-authentication ............................................... 8
5. Retransmissions ................................................ 8
6. Security Considerations ......................................... 8
7. IANA Considerations ............................................ 9
8. References .................................................... 9
   8.1. Normative References ...................................... 9
   8.2. Informative References .................................... 9
Author’s Address .................................................. 10
1. Introduction

In Authentication Extensions for the Dynamic Host Configuration Protocol [I-D.pruss-dhcp-auth-dsl], problems of lacking of an EAP-based authentication method in the migration from PPP session to IP session[WT-146] in DSL world was stated. To recap the problem, Figure 1 shows the common architecture of DSL access network. IP session usually is created by DHCP process, and user authentication is a missing part in current IP session. There was a long debate regarding the draft of Authentication Extensions for the Dynamic Host Configuration Protocol [I-D.pruss-dhcp-auth-dsl], like whether DHCP is a right protocol to carry EAP payload, how new DHCP messages affect the operation of normal DHCP, whether all DHCP clients could be expected to support the new feature, etc. This draft is not going to tackle all the raised problems but wants to give a lightweight alternative solution. It makes use of the short lease time mechanism to naturally trigger DHCP client sending DHCP request with EAP payload. The DHCP state machine of client’s side is kept unchanged to the most extent.

```
+-----------+  +------------+
|   DHCP    |  | AAA/RADIUS  |
|  Server   |  |   Server    |
+-----------+  +------------+

Sub.     +-----+   +--------+       |         +-----+   +----------+
|            |            |            |         |     |          |
|            |            |            |         |     |          |
|            |            |            |         |     |          |
|            |            |            |         |     |          |
|            |            |            |         |     |          |

Home ---| HGW |---|        |       +---------|     |   |          |
|        |   | Access |                 |     |   |          |
|        |   |        |                 |     |   |          |
|        |   |        |                 |     |   |          |
|        |   |        |                 |     |   |          |
|        |   |        |                 |     |   |          |

Network +-----+   +--------+                 +-----+   +----------+

Sub.     +-----+   +--------+       |         +-----+   +----------+
|            |            |            |         |     |          |
|            |            |            |         |     |          |
|            |            |            |         |     |          |
|            |            |            |         |     |          |
|            |            |            |         |     |          |

Home ---| HGW |---|        |       +---------|     |   |          |
|        |   | Access |                 |     |   |          |
|        |   |        |                 |     |   |          |
|        |   |        |                 |     |   |          |
|        |   |        |                 |     |   |          |
|        |   |        |                 |     |   |          |

Network +-----+   +--------+                 +-----+   +----------+

-----------DSL Access Network -----------
```

Figure 1: DSL Network Architecture

2. DHCP Auth Option Format

This section reuses the new option defined in Authentication Extensions for the Dynamic Host Configuration Protocol (version 03)[I-D.pruss-dhcp-auth-dsl]. They are DHCP Authentication Protocol Option and DHCP EAP-Message Option. For easy reference, the option format is listed as follows.
2.1. DHCP Authentication Protocol Option

The DHCPAUTH-Protocol option is sent between DHCP Client to DHCP Server to indicate either party is able to support EAP authentication.

```
+----------------+------------+-----------------------+
| DHCP Code      | Length     | Authentication-Protocol |
+----------------+------------+-----------------------+
```

Figure 2: DHCP Authentication Protocol Option

DHCP Code: TBA-1 (DHCPAUTH-Protocol)
Length: 3
Authentication-Protocol
C227 (HEX) for Extensible Authentication Protocol (EAP)

2.2. DHCP EAP-Message Option

The format of the DHCP EAP-Message option is as follows:

```
+----------------+------------+-------------------------+
| DHCP Code      | Length     | EAP payload             |
+----------------+------------+-------------------------+
```

Figure 3: DHCP EAP-Message Option

The EAP-Message Option is carried by DHCPREQUEST and DHCPACK to transmit EAP payload.

3. Protocol Operations

In this section DHCP-based operations for user authentication are provided. We are trying to keep the change of client side state machine as minor as possible. No new message is introduced.

3.1. Message flow when DHCP server co-located with BNG

A typical message flow proceeds as shown in Figure 4:
1. DHCPDISCOVER ------->
   (w/DHCP-auth-proto EAP)

2. DHCPOFFER ------->
   (w/DHCP-auth-proto EAP)

3. DHCPREQUEST ------->
   (w/DHCP-auth-proto EAP)

4. DHCPACK ------->
   (w/EAP-Message/EAP-Request/Identity)

   (T1 expires)

5. DHCPREQUEST ------->
   (w/EAP-Message/EAP-Response/Identity)

6. RADIUS Access-Request ------->
   (w/EAP-Message)

7. RADIUS Access-Challenge
   (w/EAP-Message)

8. DHCPACK
   (w/EAP-Message/EAP-Request/)

   (repeating step 5-8)

9. DHCPREQUEST ------->
   (w/EAP-Message/EAP-Response)

10. RADIUS Access-Request ------->
    (w/EAP-Message)

11. RADIUS Access-Accept
    (w/EAP-Message)

    (Access-Reject
     if unsuccessful)

12. DHCPACK
    (DHCPNAK if unsuccessful)

Figure 4: Message Flow for DHCP server co-located with NAS

In step 2 DHCP client may collect more than one DHCPOFFERs. If there
is an DHCPOFFER does not require the client to perform the
authentication, the client may be willing to choose it. The message
flow presented in the figure makes use of the T1 timer expiration between step 4 and step 5. Section 4.4.5 in [RFC2131] talks about the timer expirations. T1 specifies the time at which the client tries to extend its lease. At time T1 the client moves to RENEWING state and sends (via unicast) a DHCPREQUEST message to the server to extend its lease. Value of T1 is configurable by the server through options. Its default value is (0.5 * duration_of_lease). In order to make the procedures more efficient, the coefficient can be set to a value less than the default 0.5 and duration of lease time should be short. By making T1 to be a very small value, DHCP client may trigger DHCPREQUEST carrying EAP message to be sent frequently enough for EAP exchange and such implementation is compliant with current client’s state machine. If the authentication is successful, DHCPACK will be sent to the client; otherwise DHCPNAK will be sent. The duration of lease carried in this DHCPACK is a normal DHCP lease duration.

3.2. Message flow when DHCP server and BNG are separated

In another deployment scenario, DHCP server may not be co-located with NAS. In this case, the message flow is depicted in Figure 5:
Figure 5: Message Flow with separated DHCP server and NAS
BNG serves as DHCP relay agent in this scenario. It relays DHCPDISCOVER and DHCPOFFER between the client and the server. By snooping DHCP-auth-proto option, relay agent is able to know an authentication procedure is expected. EAP-Message option is carried in DHCPREQUEST and DHCPACK between the client and the relay agent until the relay agent receives Access-Accept or Access-Reject from RADIUS server. Then the relay agent relays the DHCPREQUEST with RADIUS attributes suboption to the DHCP server.

4. Re-authentication

Re-authentication may be triggered from either client side or server side. BNG may require the DHCP client to reauthenticate to it due to administration or other purpose. In this case, BNG sends forcerenew message [RFC3203] with EAP-Message option to force the client perform the reauthentication procedures. If authentication was not required when the user first applies for an IP address via DHCP or it is known that client does not support dsl authentication feature, re-authentication should not be used by server side FORCERENEW message.

5. Retransmissions

In the section of Protocol Operations (Section 3), using the short lease time to trigger DHCPREQUEST carrying EAP-Message was introduced. The choice of T1 value is important. In order to make sure DHCPREQUEST reaches BNG before EAP itself time out, T1+RTT should be less than EAP RTO value.

DHCP clients are responsible for all DHCP message retransmissions as per [RFC2131]. When DHCP client does not receive the response for DHCPREQUEST, it will retransmit the message after certain timeout period. This may cause a duplicated EAP-Response in EAP-Message option to be carried in DHCPREQUEST to BNG. In order to avoid the timeout contention between EAP and DHCP, BNG should not give an immediate responding DHCPACK in this case. BNG should wait for a subsequent EAP request (either retransmited or brand new) to be passed from EAP layer and then carry it in DHCPACK to DHCP client. BNG always handles the retransmission pace.

6. Security Considerations

The client obtaining a short but valid lease time in each EAP round trip may bring extra security problems. The address obtained during authentication process should be only used for DHCP EAP exchange purpose. The address filter needs be properly set at access nodes.
The source address filter is normally established by snooping
DHCPACK. In order to make sure the address to be used unrestrictly
only after authentication succeeds, source address filter should
snoop DHCPACK with EAP-success instead of simply snoop DHCPACK.

7. IANA Considerations

This specification requires two values for new options to be assigned
by IANA.

TBA-1: (DHCPAUTH-Protocol)
TBA-2: (DHCPEAP-Message)

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

8.2. Informative References

[I-D.pruss-dhcp-auth-dsl]
Pruss, R. and G. Zorn, "Authentication Extensions for the
Dynamic Host Configuration Protocol",
draft-pruss-dhcp-auth-dsl-04 (work in progress),
March 2009.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5,
RFC 792, September 1981.

[RFC1661] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51,


[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson,
"Remote Authentication Dial In User Service (RADIUS)",
RFC 2865, June 2000.


