EAP Authentication Extensions for the Dynamic Host Configuration Protocol for Broadband
draft-pruss-dhcp-auth-dsl-05

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 November 1, 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 Dynamic Host Configuration Protocol (DHCP)
extensions that provide for end-user authentication prior to configuration of the host. The primary applicability is within a Digital Subscriber Line (DSL) Broadband network environment in order to enable a smooth migration from the Point to Point Protocol (PPP).

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. Problem Statement ........................................... 3
4. Applicability Statement ...................................... 6
5. Protocol Operation ........................................... 6
   5.1. Protocol Operation for IPv4 ............................... 6
   5.2. Protocol Operation for IPv6 ............................... 12
6. DHCP Options ............................................... 15
   6.1. DHCPEAP Capability Vendor-identifying Vendor-specific Suboption .................................................. 15
   6.2. DHCPv6 DHCPEAP Capability Vendor-specific Suboption .... 16
7. DHCP Messages ............................................... 17
   7.1. DHCPv4 DHCPEAP Message type ............................... 17
   7.2. DHCPv6 DHCPEAP Message .................................... 18
8. Messages for EAP operation .................................. 19
   8.1. Messages for DHCPv4 ....................................... 19
     8.1.1. Client’s DHCPDISCOVER message .......................... 19
     8.1.2. DHCPEAP message ....................................... 20
   8.2. Messages for DHCPv6 ....................................... 21
     8.2.1. Client’s SOLICIT message ............................... 21
     8.2.2. DHCPEAP message type ................................... 22
9. Fragmentation ............................................... 23
10. Backwards Compatibility Considerations ..................... 24
11. Security Considerations ................................... 25
   11.1. Message Authentication .................................. 25
12. IANA Considerations ....................................... 25
13. Acknowledgements ......................................... 26
14. Notice .................................................... 26
15. References ................................................ 26
   15.1. Normative References .................................... 26
   15.2. Informative References .................................. 27
Authors’ Addresses .............................................. 29
1. Introduction

This document defines DHCP Options and procedures that allow for an Extensible Authentication Protocol (EAP) authentication exchange to occur in DHCP in order to enable smooth migration from Point-to-Point Protocol (PPP) [RFC1661] sessions to IP sessions in a DSL Broadband network environment. Primary goals are integration of authentication in such a way that it will operate seamlessly with existing RADIUS-based Authentication, Authorization and Accounting (AAA) infrastructure and Asynchronous Transfer Mode (ATM) or Ethernet based DSL Networks. As such, only the termination points of PPP in the DSL network are affected, both of which are devices that would logically need to be updated in any transition from PPP to IP sessions.

It should be noted that [RFC3118] defines a mechanism that provides authentication of individual DHCP messages. While this mechanism does provide a method of authentication for a DHCP Client based on a shared secret, it does not do so in a manner that can be seamlessly integrated with existing RADIUS-based AAA infrastructure.

2. Problem Statement

Digital Subscriber Line (DSL) broadband service providers are witnessing a shift in the "last-mile" aggregation technologies and protocols which have traditionally been relied upon. Two primary transitions are from ATM to Ethernet in the access network, and from the PPP for multi-protocol framing and dynamic endpoint configuration to direct encapsulation of IP and DHCP for dynamic endpoint configuration for some devices. The term used by the DSL Forum for the network state associated with an authorized subscriber (that is using DHCP and IP rather than PPP) is "IP session" [WT-146]. While these trends can be readily witnessed, neither are occurring overnight. In addition, they are not necessarily implemented in lock-step. Thus, one may find ATM-based and Ethernet-based access networks running a combination of PPP sessions and IP sessions at any given time, particularly during transition periods. This coexistence will even occur for the same service subscriber.

Removing PPP, Point-to-Point Protocol over ATM (PPPoA) [RFC2364], and Point-to-Point Protocol over Ethernet (PPPoE) [RFC2516] from the subscriber access network is relatively straightforward in that most of the properties that DSL providers are interested in going forward are already present in DHCP and IP sessions. Luckily, there are some capabilities of PPP which the market does not continue to demand. For example, the Dynamic configuration in PPP for IPX or NETBEUI, is no longer of concern. Neither are the multi-link bonding capabilities of PPP [RFC1990] commonly used on separate ISDN...
B-channels, and the myriad of other features that PPP developed as the "dial-based" access protocol of choice for framing, authentication, and dynamic configuration for IP and other network layer protocols. Missing from IP sessions and DHCP [RFC2131], however, are isomorphic methods for user authentication and session liveness probing (sometimes referred to as a session "keepalive"). For the latter, existence of a client using a given IP address can be detected by a number of means, including Address Resolution Protocol (ARP) [RFC0826], ICMP Echo/Echo Response [RFC0792], or Bidirectional Forwarding Detection (BFD) [I-D.ietf-bfd-base]. This leaves authentication as an open issue needing resolution. Specifically, authentication based on a username and secret password must be covered. This is something that in PPP always occurs before dynamic configuration of an IP address and associated parameters.

While most DSL deployments utilize a username and password to authenticate a subscriber and authorize access today, this is not the only method for authentication that has been adopted when moving to DHCP and IP sessions. "Option 82" [RFC3046] is commonly used with DHCP as a credential to authenticate a given subscriber line and authorize service. In this model, the DSL Access Node, which always sits between the DHCP Client and Server, snoops DHCP messages as they pass, and inserts pre-configured information for a given line (e.g., an ATM VPI/VCI, Ethernet VLAN, or other tag). That information, while provided in clear text, traverses what is considered a physically secured portion of the access network and is used to determine (typically via a request to an AAA server) whether the DHCP exchange can continue. This fits quite well with current DSL network architecture, as long as the subscriber line itself is all that needs be authorized. However, in some service models it is still necessary for the subscriber to provide credentials directly.

From the perspective of the Network Access Server (NAS) where the DHCP Server resides, the extensions defined in this document are analogous to the commonly available "Option 82" method. The primary difference between using Option 82 line configuration and a username and password is that the authentication credentials are provided by the subscriber rather than inserted by intervening network equipment. Providing credentials from the subscriber rather than intervening network equipment is particularly important for cases where subscriber line information is unavailable, untrusted, or due to the terms of the service changing at any time. Further, different devices in the home may have different policies and require different credentials. Migration scenarios where PPPoE and DHCP operate on the same network for a period of time lend well to models which utilize identical authentication and authorization credentials across the different data plane encapsulations.
3. Network Architecture and Terminology

The DSL Forum defines its ATM-based network architecture in [TR-059] and Ethernet-based network architecture in [TR-101]. The extensions for DHCP defined in this document are designed to work identically on Ethernet or ATM architectures. The diagram in Figure 1 and following terminology will be used throughout:

---

Figure 1: DSL Network Architecture

- **Access Node (AN):** Network device, usually located at a service provider central office or street cabinet, that terminates Access Loop connections from Subscribers. In case the Access Loop is a Digital Subscriber Line (DSL), this is often referred to as a DSL Access Multiplexer (DSLAM). The AN may support one or more Access Loop technologies and allow them to inter-work with a common aggregation network technology.

- **Network Access Server (NAS):** Network device that aggregates multiplexed Subscriber traffic from a number of Access Nodes. The NAS plays a central role in per-subscriber policy enforcement and QoS. Often referred to as a Broadband Network Gateway (BNG) or Broadband Remote Access Server (BRAS). A detailed definition of the NAS is given in [RFC2881].

- **The Home Gateway (HGW) connects the different Customer Premises Equipment (CPE) to the Access Node and the access network. In case of DSL, the HGW is a DSL Network Termination (NT) that could either operate as a layer 2 bridge or as a layer 3 router. In the latter case, such a device is also referred to as a Routing Gateway (RG).**
Referring to the DSL network architecture depicted in Figure 1, PPP (via PPPoA [RFC2364] or PPPoE [RFC2516]) operates over the DSL Access Network between the NAS and a device behind the HGW, or between the NAS and the HGW itself. The DHCP Client resides either on a home network device or the HGW, and the DHCP Server protocol state machine may reside fully on the NAS. The NAS obtains per-subscriber client configuration information either locally, relayed from a DHCP server or from the AAA infrastructure (which itself may consult external DHCP servers if necessary) after authentication is successfully completed.

4. Applicability Statement

The primary target for this extension is for DSL service provider networks where PPP is being phased out to be replaced by native IP and DHCP, or where new devices are being added which will not utilize PPP. Very specific assumptions have been made with respect to the security model, operational methods, and integration requirements for existing AAA mechanisms during the design. It is understood that this mechanism may not be generally applicable in this form for all network environments where DHCP is deployed, though perhaps elements of it may be used to develop a more generic approach while still meeting the specific requirements set out by the DSL network architecture. Earlier revisions of this document included a method to embed PPP CHAP [RFC1994] authentication as Options in existing DHCP messages. This method has been abandoned due to security vulnerabilities in CHAP, as well as a lack of extensibility. This document bases its authentication on EAP [RFC3748] which can be used with a large number of different authentication methods, including one backwards compatible with existing PPP CHAP.

5. Protocol Operation

This section describes the protocol operation for EAP within DHCPv4 [RFC2131] and DHCPv6 [RFC3315]. Options and message specifications used in these operation descriptions are detailed in later sections.

If multiple DHCP exchanges are occurring with multiple servers, both IPv4 and IPv6 each needs to authenticate separately.

5.1. Protocol Operation for IPv4

It is essential that the user/node authentication occurs before the assignment of an IP address and, further, that the assignment of the address depends upon the details of the successful authentication. DHCP [RFC2131] is widely used as an address assignment method (among
other things); EAP [RFC3748] has been widely adapted for authentication purposes, especially in those types of networks where DHCP is also used. This section describes how to combine the two in order to provide both strong authentication and authenticated address assignment in an efficient manner.

A Section 7.1 (using the DHCP Vendor-specific Message [I-D.volz-dhc-dhcpv4-vendor-message]) is used in the DHCP message flow to support the new EAP phase which occurs before a DHCPOFFER is sent by the Server. This message is used to integrate authentication methods supported by EAP, including CHAP and any other "in the clear" password mechanisms (for example, to support One-Time Password mechanisms), or to carry other EAP methods. EAP is widely used in other environments, outside of DSL Broadband, including 802.11 "Wi-Fi" access networks and 3GPP to name a few.

To request the assignment of an IPv4 address with authentication, a client first locates a DHCP server, then authenticates using EAP and then requests the assignment of an address and other configuration information from the server. The client sends a DHCPDISCOVER message with an option specifying that the client understands the DHCP User Authentication protocol using EAP, to find an available DHCP server. Any server that can authenticate and address it responds with a DHCPEAP message containing the first packet of the EAP protocol.

Servers which support DHCP User Authentication will respond with a DHCPEAP message. The client may receive one or more DHCPEAP messages from one or more DHCP Servers or DHCP relays. The Client may also receive one or more DHCPOFFER messages from other DHCP Servers which may not understand, or choose not to employ the DHCP User Authentication protocol. The Client chooses one server to reply to. If the selected server has sent a DHCPEAP message, then the Client will send a DHCPEAP message in reply. The DHCPEAP message contains EAP packets which facilitate the EAP authentication exchange. The exchange may occur between the DHCP Client and DHCP Server embedded within a NAS, or be carried transparently to the AAA Server. Upon successful completion of the authentication phase, the DHCP server sends a DHCPOFFER with the appropriate IP configuration for the authenticated user. The client then follows the normal DHCP procedures of a successful DHCP exchange by sending a DHCPEREQUEST, followed by a DHCPACK from the Server.

If the authentication phase fails the DHCP server may choose to either terminate all communication with a client or offer some default address possibly with some limited access policy. (Configuration policy for this is outside of the scope of this document).
The final EAP-Success or EAP-Failure message is always communicated using the DHCPEAP message type. If the Server will be sending a DHCPOFFER message, this message is sent immediately after the final DHCPEAP message.

A typical message flow proceeds as shown in Figure 2: The retransmission is handled by EAP as per Section 4.1 in [RFC3748].
DHCPDISCOVER -------->
(w/DHCP-auth-proto EAP)

<-------- DHCPEAP
(w/EAP Message)

DHCPEAP --------->
(w/EAP Message)

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

<-------- RADIUS
Access-Challenge (w/EAP Message)

<-------- DHCPEAP
(w/EAP Message)

DHCPEAP --------->
(w/EAP Message)

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

(The last four messages repeat until EAP Success or EAP fail)

<-------- RADIUS
Access-Accept (w/EAP Message)
(Access-Reject (w/EAP Message)
if unsuccessful)

<-------- DHCPEAP (w/EAP success Message)

(DHCP messages continue normally from
this point forward if successful)

<-------- DHCPOFFER (w/yiaddr)

DHCPREQUEST --------->

<-------- DHCPACK

Figure 2: DHCP Message Flow with DHCPEAP messages
The message exchange presented in Figure 2 is an example of simple one-way user authentication, e.g. the Server verifies the credentials of the HGW Client. The client indicates the ability to have an EAP exchange and the NAS (which takes on the EAP authenticator role) initiates the first EAP request to the DHCP Client (which takes on the EAP peer role).

When the NAS is acting as a DHCP Relay the BRAS may split the EAP Messages from DHCP and perform the AAA authentication with an AAA server. This allows use of existing DHCP servers and existing AAA servers.

An example message flow for DHCP Relay proceeds as shown in Figure 3: [RFC4014]

<table>
<thead>
<tr>
<th>(HGW)</th>
<th>(NAS)</th>
<th>(AAA)</th>
<th>(DHCP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Client</td>
<td>AAA Client</td>
<td>RADIUS Server</td>
<td>DHCP Server</td>
</tr>
</tbody>
</table>

DHCPDISCOVER -------->
(w/DHCP-auth-proto EAP)

<-------- DHCPEAP
(w/EAP Message)

DHCPEAP -------->
(w/EAP Message)

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

<-------- RADIUS
Access-Challenge
(w/EAP Message)

<-------- DHCPEAP
(w/EAP Message)

DHCPEAP -------->
(w/EAP Message)

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

(The last four messages repeat until EAP Success or EAP fail)

<-------- RADIUS
Access-Accept (w/EAP Message)

Access-Reject (w/EAP Message)
When the DHCP relay agent in the NAS receives a DHCP message from the client, it MAY append a DHCP Relay Agent Information option containing the RADIUS Attributes suboption, along with any other suboptions it is configured to supply. The RADIUS Attributes suboption is defined in [RFC4014].

DHCP Authentication uses one suboption inside the Vendor-identifying vendor-specific message option and makes use of the Vendor-specific Message option[I-D.volz-dhc-dhcpv4-vendor-message]:

- DHCPv4 DHCP-PEAP Capability Vendor-identifying Vendor-specific Suboption in the DHCPDISCOVER to specify the type of authentication exchange and makes use of a new DHCP Vendor-specific Message type

- DHCPv4 DHCP-PEAP Message type to carry the EAP data in the DHCP-PEAP messages.
5.2. Protocol Operation for IPv6

This section describes the protocol operation for extending Dynamic Host Configuration Protocol for IPv6 [RFC3315] for an EAP phase.

The same as the previous section on extending DHCP in IPv4 a new DHCP message, Section 7.2 is used to support EAP authentication before host configuration occurs. The mechanisms described here follow a similar methodology as that for DHCPv4 described in Section 5.1.

The client sends a Solicit message with an Option specifying the session authentication protocol as EAP to the All_DHCP_Relay_Agents_and_Servers address to find available DHCP servers. Any server that can authenticate and address it responds with a DHCPEAP message.

The client may receive one or more DHCPEAP messages from one or more DHCP Servers. The Client chooses one to reply to, and sends a DHCPEAP message, silently discarding DHCPEAP messages from other servers (As per the question above, is there some type of EAP message which can be sent to the other servers to stop EAP there?). The DHCPEAP messages contain EAP packets which facilitate the EAP authentication exchange. The exchange may occur between the DHCP Client and DHCP Server embedded within a NAS, or be carried transparently to the AAA Server. Upon successful completion of the authentication phase, the DHCP server sends a ADVERTISE with the appropriate configuration for the authenticated user. The client then follows the normal DHCP procedures of a successful DHCP exchange by sending a REQUEST, followed by an ACK from the Server.

If the authentication phase fails (e.g., the user does not provide appropriate credentials), then according to configured policy the DHCP Client is either denied any IP configuration with the DHCP Server sending a NAK accordingly, or the DHCP Client is given a "limited access" configuration profile and the DHCP exchange continues as if the authentication was successful.

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

<------ DHCPEAP
(w/EAP Message)

DHCP Client          DHCP Server/            RADIUS Server

(HGW)                (NAS)                   (AAA)

DHCPEAP --->>
(w/EAP Message)

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

<------ RADIUS
Access-Challenge (w/EAP Message)

<------ DHCPEAP
(w/EAP Message)

DHCPEAP --->>
(w/EAP Message)

RADIUS Access-Request ---->
(w/EAP Message)
(The last four messages repeat until EAP Success or EAP fail)

<------ RADIUS
Access-Accept (w/EAP Message)
(If unsuccessful)

<------ DHCPEAP (w/EAP success Message)
(DHCP messages continue normally from this point forward if successful)

<------ ADVERTISE
(DHCP messages continue normally from this point forward if successful)

REQUEST ----->

<------ REPLY
The retransmission is handled by EAP as per Section 4.1 in [RFC3748].

When the NAS is acting as a DHCPv6 Relay the BRAS may split the EAP Messages from DHCP and perform the AAA authentication with an AAA server. This allows use of existing DHCPv6 servers and existing AAA servers.

The message following this exchange is an ADVERTISE, sent unchanged by the Server. A typical message flow proceeds as shown in Figure 5:

```
(HGW)                (NAS)                (AAA)           (DHCP)
DHCP Client           AAA Client        RADIUS Server   DHCP Server

SOLICIT ------->
(w/DHCP-auth-proto EAP)

<-------- DHCPEAP
(w/EAP Message)

DHCPEAP ------->
(w/EAP Message)

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

<-------- RADIUS
Access-Challange (w/EAP Message)

<-------- DHCPEAP
(w/EAP Message)

DHCPEAP ------->
(w/EAP Message)

RADIUS Access-Request ------->
(w/EAP Message)
(The last four messages repeat until EAP Success or EAP fail)

<-------- RADIUS
Access-Accept (w/EAP Message)
(If unsuccessful)

<-------- DHCPEAP (w/EAP success Message)
(DHCP messages continue normally from
```
When the DHCP relay agent in the NAS receives a DHCP message from the client, it MAY append a DHCP Relay option or DHCP relay information suboption containing the RADIUS Attributes information, along with any other relay options or relay information suboptions it is configured to supply. The RADIUS Attributes suboption for DHCPv4 is defined in \[RFC4014\].

6. DHCP Options

One DHCP Vendor-specific suboption is defined in this section. The DHCPEAP Capability Vendor-identifying Vendor-specific Suboption is included into the client’s DHCPDISCOVER or SOLICIT message to specify that the client understand DHCPEAP messages, as defined below (see Section 8).

6.1. DHCPEAP Capability Vendor-identifying Vendor-specific Suboption

The DHCPv4 DHCPEAP-Capability Vendor-identifying Vendor-specific suboption is sent from the DHCPv4 Client to the DHCPv4 Server to indicate that the client is capable of understanding DHCPv4 DHCPEAP Messages. This suboption is defined using the DHCPv4 Vendor-identifying Vendor-specific option: 
Figure 6: DHCPv4 DHCP-EDAP Capability Vendor-identifying vendor-specific suboption

Opt-code: 125
Length: 7
Enterprise-ID: 9 (Cisco Systems)
Data-length: 2
Suboption: 14 (DHCP-EDAP Capability suboption)
Subopt-length: 0

6.2. DHCPv6 DHCP-EDAP Capability Vendor-specific Suboption

The DHCPv6 DHCP-EDAP-Capability Vendor-specific suboption is sent from the DHCPv6 Client to the DHCPv6 Server to indicate that the client is capable of understanding DHCPv6 DHCP-EDAP Messages. This suboption is defined using the DHCPv6 Vendor-specific option:

Figure 7: DHCPv6 DHCP-EDAP Capability Vendor-specific Suboption
OPTION_VENDOR_OPTS: 17
Length: 6
Enterprise-ID: 9 (Cisco Systems)
Suboption: 14 (DHCPEAP Capability suboption)
Subopt-length: 0

7. DHCP Messages

One new DHCPv4 message type and one new DHCPv6 message type are defined in order to carry the EAP messages between the client and the server. These messages make use of the Vendor-specific Message type and are defined using the Enterprise-ID for Cisco Systems.

7.1. DHCPv4 DHCPEAP Message type

The format of the DHCPEAP Message type for DHCPv4 follows the current draft [I-D.volz-dhc-dhcpv4-vendor-message], and is defined as follows:

```
+-----------------------------------------------+
| 53 | 1 |
|-----------------------------------------------+
| 254 |
|-----------------------------------------------+
```
...

```
+-----------------------------------------------+
|Vendor-msg=TBD | Length |
|-----------------------------------------------+
| Enterprise-ID=9 |
|-----------------------------------------------+
| Enterprise-ID (cont.) |
|-----------------------------------------------+
| Msg-type=1 | Suboption=1 |
|-----------------------------------------------+
| EAP-length | EAP msg ...
```

...
Figure 8: DHCPEAP Message type

Vendor-msg: TBD

Enterprise-ID: 9 (Cisco Systems)

Msg-type: 1 (DHCPEAP)

Suboption: 1 (DHCPEAP-Message)

EAP-length: (length of the EAP message)

Note that according to the current DHCPv4 Vendor-specific Message draft, a "vendor-msg-type" field is the first octet after the enterprise-ID, and after this octet all data should be in "code/length/value" fields "identical to the DHCP options field". Thus, the "vendor-msg-type" field ("Msg-type" in the figure above) is set to "1" and the next field is the suboption value, which is also set to "1", followed one octet specifying the length of the EAP message, followed by the EAP message itself.

The maximum size of a DHCP option is 255 octets. While in some cases (e.g., EAP MD5-Challenge [RFC3748]) a complete EAP message may fit in a single DHCP option, in general this is not the case. If an EAP message is too large to fit into a single DHCP Vendor-specific Message option, the method defined in [RFC3396] MUST be used to split the EAP message into separate options for transmission. Similarly, EAP assumes a minimum MTU of 1020 octets while the minimum DHCP packet size is 576 octets, including 312 octets reserved for options. A DHCP client including the EAP-Message option SHOULD also include the 'maximum DHCP message size' option [RFC2132] to set a suitable DHCP message size.

If a DHCP message is received containing more than one DHCPEAP Message type option, the method defined in [RFC3396] MUST be used to reassemble the separate options into the original EAP message. A DHCP server receiving an EAP message MAY forward it via a AAA protocol (such as RADIUS [RFC2865] [RFC3579] or Diameter [RFC3588] [RFC4072]).

7.2. DHCPv6 DHCPEAP Message

The format of the DHCPEAP Message type for DHCPv6 follows the current draft [I-D.volz-dhc-dhcpv6-vendor-message], and is defined as follows:
Figure 9: DHCP-EAP Message type

Note that according to the current DHCPv6 Vendor-specific Message draft, a "vendor-msg-type" field is the first octet after the enterprise-ID, and after this octet all data should be in "code/ length/value" fields "identical to the DHCPv6 options field". Thus, the "vendor-msg-type" field ("Msg-type" in the figure above) is set to "1" and the next field is the suboption value, which is also set to "1", followed two octets specifying the length of the EAP message, followed by the EAP message itself.

8. Messages for EAP operation

This section describes the overall DHCP message contents for all messages which are used in implementing the DHCP EAP User Authentication extensions.

8.1. Messages for DHCPv4

The authentication data in a DHCPv4 DHCP-EAP message is carried in a DHCP-EAP-Messsage type DHCPv4 DHCP-EAP Message type.

8.1.1. Client’s DHCPDISCOVER message

As shown in DHCP Message Flow with DHCP-EAP messages the DHCP Client starts the process by sending the DISCOVER to the MAC broadcast address. A client sending this EAP-Capability option in the DHCPDISCOVER is expected to be able to handle EAP messaging and the associated additional methods and fragmentation handling. The NAS that handles this request could be a DHCP server or a relay DHCP. As per [RFC3579] the NAS can send the initial EAP-Request to the client or the NAS can send an EAP-Start to the server. The diagrams in this draft assume the NAS sends the initial EAP-Request as [RFC3579] reads as if that is the recommended behaviour.
DHCP Header
Opcode: BOOTREQUEST (1)

Message-type option(53): DISCOVER
Vendor-identifying vendor-specific option (125):
Enterprise: 9 (Cisco Systems)
Suboption 14 (EAP-Capability option):

```
+---------------------+
| Opt-code=125 | Length=7 |
+---------------------+
| Enterprise-ID=9 |
```

Figure 10: Client’s DHCPDISCOVER message

8.1.2. DHCPEAP message

The NAS responds to DHCP Client by sending an initial DHCPEAP to the clients MAC address (unicast). Subsequent NAS DHCP messages would look the same; unicast response for these messages to avoid the EAP conversation being replicated to many downstream clients. As noted in [RFC3748], if an EAP packet is lost in transit between the authenticating peer and the NAS (or vice versa), the NAS will retransmit.
DHCP Header:
Opcode: BOOTREQUEST (1) or BOOTREPLY (2)

Message-type option (53): Vendor-specific-message-type (254)
Vendor-specific Message option (TBD)
(as described in draft-volz-dhc-dhcpv4-vendor-message):

+--------------------------------------------------+
| Vendor-msg=TBD  | Length |
+--------------------------------------------------+
| Enterprise-ID=9 |
+--------------------------------------------------+
| Enterprise-ID (cont.) |
+--------------------------------------------------+
| msg-type=1  | Suboption=1 |
+--------------------------------------------------+
| EAP-length   | Octets of EAP Message ... |
+--------------------------------------------------+

option-code=TBD
option-len=6
enterprise-number=9 (Cisco Systems)
vendor-message-data: (TLV format)
  Message-type code (1 octet): 1 (DHCP-EAP)
  Suboption code (1 octet): 1 (DHCP-EAP Message)

Figure 11: NAS DHCP-EAP message

8.2. Messages for DHCPv6

The DHCP-EAP messages for DHCPv6 follow the format for DHCP messages defined in RFC 2131 [RFC2131] and is identified by the presence of a vendor specific DHCP Message Type option as per [I-D.volz-dhc-dhcpv6-vendor-message], which encodes DHCP-EAP message type.

8.2.1. Client’s SOLICIT message

As shown in DHCP IPv6 with DHCP-EAP message the DHCP Client starts the process by sending the SOLICIT to the All_DHCP_Relay_Agents_and_Servers multicast address. The NAS that handles this request could be a DHCP server or a relay DHCP. A client sending this EAP-Capability option in the DHCPDISCOVER is expected to be able to handle EAP messaging and the associated additional methods and fragmentation handling. As per [RFC3579] the NAS can send the initial EAP-Request to the client or the NAS can send an EAP-Start to the server. The diagrams in this draft assume the NAS sends the initial EAP-Request as [RFC3579] reads as if that is the recommended behaviour.
DHCPv6 Message:

```
+-----------------------------------------------+
| SOLICIT | transaction-id |
+-----------------------------------------------+
.            options                   .
.              (variable)             .
+-----------------------------------------------+
| OPTION_VENDOR_OPTS | option-len |
+-----------------------------------------------+
| enterprise-number=9 |
+-----------------------------------------------+
| Suboption=14 | Subopt-length=0 |
+-----------------------------------------------+
```

Vendor-specific option (17):
Enterprise: 9 (Cisco Systems)
Suboption 14 (EAP-Capability option):

Figure 12: Client’s SOLICIT message

8.2.2. DHCPEAP message type

The NAS responds to DHCP Client by sending an initial DHCPEAP to the clients MAC address (unicast). Subsequent NAS DHCP messages would look the same; unicast response for these messages to avoid the EAP conversation being replicated to many downstream clients. As noted in [RFC2284][1], if an EAP packet is lost in transit between the authenticating peer and the NAS (or vice versa), the NAS will retransmit.
DHCPv6 Message

| Msg-type=TBD | Enterprise-ID=9 |
| Ent-ID (cont.) | Msg-type=1 | Suboption=1 |
| EAP-msg-length | Octets of EAP Msg ...

Enterprise: 9 (Cisco Systems)
Msg-type: 1 (DHCPEAP)
Suboption 1 (EAP-Message)

Figure 13: DHCPv6 DHCPEAP message

9. Fragmentation

Encapsulating EAP messages within DHCP raises the question of whether there are potential difficulties with respect to the MTU sizes of the EAP and DHCP messages, as well as the underlying link MTU.

EAP as defined in [RFC3748] Section 3.1 says:

[4] Minimum MTU. EAP is capable of functioning on lower layers that provide an EAP MTU size of 1020 octets or greater.

DHCP as defined in [RFC2131] Section 2 says:

... This requirement implies that a DHCP client must be prepared to receive a message of up to 576 octets, the minimum IP datagram size an IP host must be prepared to accept [3]. DHCP clients may negotiate the use of larger DHCP messages through the ‘maximum DHCP message size’ option. The options field may be further extended into the ‘file’ and ‘sname’ fields.

If we assume EAP MTU-sized packets, the overhead to pack an EAP packet into DHCP options is 2*(1020/255), or 8 octets. Adding the DHCP header (240 octets), UDP (8 octets), and the IP header (20 octets) gives 278 octets total overhead. Since the Ethernet effective MTU is 1500 octets, this 278 octet overhead leaves the DHCP
protocol with 1222 octets to carry EAP. This space is over 200 octets more than the EAP MTU of 1020 octets.

If we add the SNAME and CHADDR fields to the option pool, then there are nearly 400 octets available for DHCP options in an Ethernet MTU-sized DHCP packet, encapsulating EAP.

In short, when the ‘maximum DHCP message size’ option is used by the client, there is no problem carrying in EAP over DHCP. i.e. clients capable of performing EAP over DHCP should also advertise a maximum message that is capable of carrying EAP over DHCP.

10. Backwards Compatibility Considerations

This section is aimed at describing interoperability scenarios involving HGW and NAS with or without DHCP Authentication mechanism support in order to analyze compatibility issues that could be faced between newer and older products during the introduction of the DHCP Authentication functionally in current implemented network environments.

Scenario 1: Both HGW and NAS do not support DHCP Authentication

In this case the authentication process does not start, thus traditional DHCP message flow applies.

Scenario 2: HGW does not support DHCP Authentication and NAS supports DHCP Authentication

In this case the DHCP client does not start DHCP Authentication transaction, NAS MAY decide to respond to HGW without using DHCP Authentication, falling back to traditional DHCP message flow and assigning different network resources.

Scenario 3: HGW supports the DHCP Authentication and NAS does not support DHCP Authentication.

In this case the DHCP client inserts in the DHCPDISCOVER message sent to NAS, the DHCP Authentication Protocol Option described in the draft in order to communicate the NAS that it is able to perform authentication and for indicating the authentication algorithm preferred by the client. NAS on receiving a DHCPDISCOVER with unknown option silently discards unknown message. Alternatively NAS MAY ignore the unknown option, but still process the message and then reply to the DHCP client with traditional response. The HGW, that has upgraded software, realizes that the NAS does not support DHCP Authentication and can revert back to normal DHCP message flow.
Scenario 4 Both HGW and NAS support DHCP Authentication

In this case DHCP client inserts in the DHCPDISCOVER message sent to NAS, the DHCP Authentication Protocol Option in order to communicate the NAS that it is able to perform authentication and for indicating the authentication algorithm preferred by the client, NAS replies according to the message flow described in this draft.

The following table summarizes the behavior in the 4 described scenarios:

<table>
<thead>
<tr>
<th>Relay</th>
<th>Client</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No authentication</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>No authentication</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No authentication</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Authentication as per this document</td>
</tr>
</tbody>
</table>

11. Security Considerations

11.1. Message Authentication

RFC 3118 provides a mechanism to cryptographically protect DHCP messages using a key, K, shared between a DHCP client and Server, however no mechanism is defined to manage these keys. Authentication exchanges based on EAP have been built into authentication portions of network access protocols such as PPP, 802.1X, PANA, IKEv2, and now DHCP. EAP methods may provide for the derivation of shared key material, the MSK and the EMSK, on the EAP peer and EAP server. This dynamic key generation enables [RFC3118] protection and allows modes of operation where messages are protected from DHCP client to DHCP relay which previously would be difficult to manage.

A future document will look at how to derive the key, K, from the EMSK resulting from an EAP exchange and at how this mechanism interacts with the DHCP authentication or any EAP authentication prior to DHCP.

12. IANA Considerations

This specification requires three values to be assigned by IANA if non-Vendor message and option space is not use. Currently the draft needs no IANA specified number but this information is captured here incase that needs to change in the future.

The three numbers that could be assigned by IANA are:
Two are "BOOTP Vendor Extensions and DHCP Options"

TBA-1:  (DHCPAUTH-Protocol)

TBA-2:  (DHCPAUTH-Data)

Two DHCP Message Type 53 Values - per [RFC2132], for DHCPEAP message type.

13. Acknowledgements

Many thanks to Carlos Pignataro for help editing this document.

Thanks to Roberta Maglione for setting many of the requirements and network context for this work.

Thanks to Richard Johnson, Alan DeKok, Wojciech Dec, Eric Voit, Mark Townsley and Ralph Droms for help with this document.

Thanks to Amy Zhao and Yizhou Li for their work on DHCP Authentication and helping with laying the ground for this document.

14. Notice

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

15. References

15.1. Normative References


15.2.  Informative References

[I-D.ietf-bfd-base]  

[I-D.volz-dhc-dhcpv4-vendor-message]  

[I-D.volz-dhc-dhcpv6-vendor-message]  


[RFC2516]  Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D.,

Pruss & Zorn Expires November 1, 2009 [Page 27]


Authors’ Addresses

Richard Pruss
Cisco Systems
80 Albert Street
Brisbane, Queensland 4000
Australia

Phone: +61 7 3238 8228
Fax: +61 7 3211 3889
Email: ric@cisco.com

Glen Zorn
Network Zen
1310 East Thomas Street
#306
Seattle, Washington 98102
USA

Phone: +1 (206) 377-9035
Email: gwz@net-zen.net