           Encapsulation of EAP Messages in CAPWAP Control Plane
                        draft-cao-capwap-eap-00

Abstract

   This document describes the scenario and requirement of encapsulating
   Extensible Authnetication Protocol (EAP) in the CAPWAP control plane.
   After the analysis and description, this document proposes the design
   of the new message types to encapsulate EAP messages.

described in the Simplified BSD License.

Table of Contents

1. Introduction

   Control and Provisioning of Wireless Access Points (CAPWAP) was
   designed as an interoperable protocol between the wireless access
   point and the access controller. This architecture makes it possible
   for the access controller to manage a huge number of wireless access
   points. With the goals and requirements established in[RFC4564] ,
   CAPWAP protocols were specified in [RFC5415] , [RFC5416]and
   [RFC5417].

   The specificaitons mentioned above mainly design the different
   control message types used by the AC to control multiple APs. The
   EAP messages, as key protocol exchange elements in the WLAN
   architecture also need to be encapsulated in the CAPWAP. However,
   the CAPWAP protocol does not specifies how to encapsulate the EAP
   message in its control plane. This situation makes it default to
   encapsulate the EAP messages in the CAPWAP-DATA plane.

   We found issues of encapsulating EAP in the CAPWAP-DATA plane in the
   scenario where there is a split betweent the CAPWAP-DATA and CAPWAP-
   CTL plane. This document describes such scenario and proposes a
   resolution to the problem.

1.1. Conventions used in this document

   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]

1.2. Terminology

   Access Controller (AP): The network entity that provides AP access to
   the network infrastructure in the data plane, control plane,
   management plane, or a combination therein.

   Access Point (AP): the same with Wireless Termination Point, The
   physical or network entity that contains an RF antenna and wireless
   Physical Layer (PHY) to transmit and receive station traffic for
   wireless access networks.

   CAPWAP Control Plane: A bi-directional flow over which CAPWAP Control
   packets are sent and received.

   CAPWAP Data Plane: A bi-directional flow over which CAPWAP Data
   packets are sent and received.

   EAP: Extensible Authentication Protocol, the EAP framework is
   specified in [RFC3748].

2. Scenario and Analysis

   The following figure shows where and how the problem arises. In many
   operators' network, the Access Controller is placed remotely at the
   central data center. In order to avoid the traffic aggregation at
   the AC, the data traffic from the AP is directed to the Access Router
   (AR). In this scenario, the CAPWAP-CTL plane and CAPWAP-DATA plane
   are separated from each other.

   Note: a powerful AC that aggregates the data flows is not a long-term
   solution to the problem. Because operators always plan the network
   capacity at a certain level, but with the air interface bandwidth
   increasing (e.g., from 11g to 11n and 11ac), and the increasing
   number of access requests on each AP, the powerful AC could not be
   "powerful" enough in the long run.

```
             CAPWAP-CTL +--------+
          ++============+   AC   |
         //             +--------+
        //
+-----+//   CAPWAP-DATA           +--------------+
| AP  |=========================| Access Router|
+-----+                          +--------------+
```
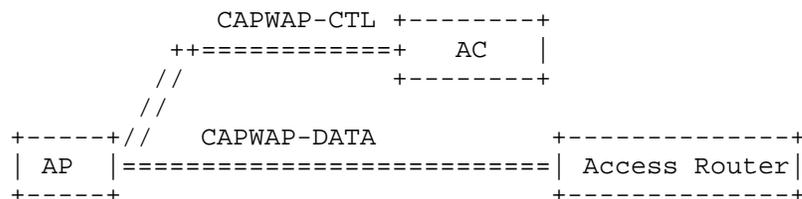
        Figure 1: Split between CAPWAP-CTL and CAPWAP-DATA Plane

   Because there are no explict message types to support the
   encapsulation of EAP packets in the CAPWAP-CTL plane, the EAP
   messages are tunneled via the CAPWAP-DATA plane to the AR. AR acts
   as authenticator in the EAP framework. After authentication, the AR
   receives the EAP keying message for the session. But AC is supposed
   to delieve these keying messages to the AP, and AR has no standard
   interface to ship them to the AP or the AC. This is unacceptable in
   the scenario of EAP-based auto-authentication.

3. Encapsulation of EAP in CAPWAP-CTL Plane

   In order to encapsulate EAP message in CAPWAP-CTL plane, we can reuse
   the control message header defined in RFC5415 and extend the message
   type to accommodate EAP messages.

   The CAPWAP Control message header is shown in Figure 2. Only 26
   message types have been defined in Section 4.5.5.1 of RFC5415. We
   can extend the message type here to encapsulate EAP messages.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Message Type                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Seq Num    |      Msg Element Length       |     Flags      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Msg Element [0..N] ...
+-+-+-+-+-+-+-+-+-+-+
```
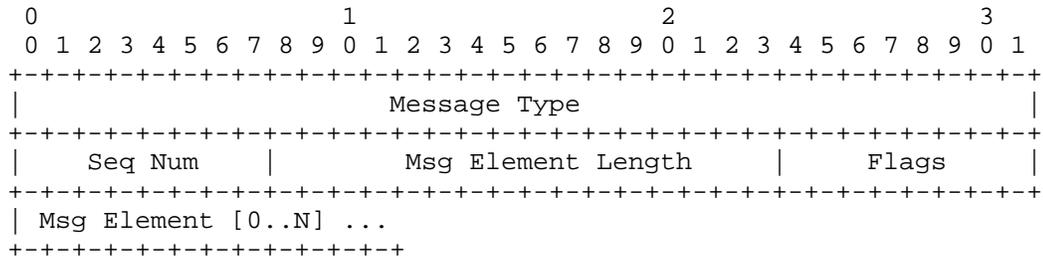
             Figure 2: The CAPWAP Control Message Header

3.1. Control Message Type for EAP

   This document defines a new control message type for EAP,
   i.e."AUTHENTICATION CONTROL". The message type value is to be
   defined by IANA.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Message Type = AUTHENTICATION CONTROL               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Seq Num    |      Msg Element Length       |     Flags      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Msg Element [0..N] ...
+-+-+-+-+-+-+-+-+-+-+
```
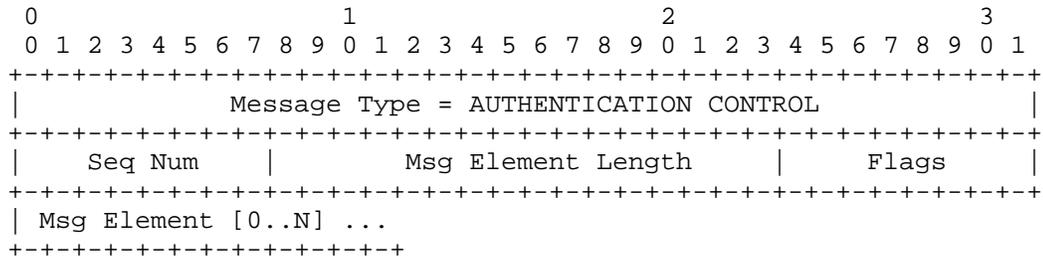
            Figure 3: The CAPWAP-EAP Control Message Header

   The Seq Num is design to match the response with the request for
   other control messages like "Discovery Request" and "Discovery
   Response". But this field is not useful for authentication control,
   because the EAP message encapsulated between the AP and AC is not
   handled in a request-response way. For AUTHENTICATION CONTROL
   messages, the AP and AC do not need to handle the 'Seq Num' field.

   Msg Element Length field indicates the number of bytes following the
   Sequence Number field.

   Flags field is left for future definition.

3.2. Message Element of the EAP

   The message element(s) carry the information pertinent to each of the
   control message types. Every control message in this specification
   specifies which message elements are permitted.

We define the message element of EAP message in the following figure.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type=Authentication Payload  |              Length           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Value ...   |
+-+-+-+-+-+-+-+-+
```
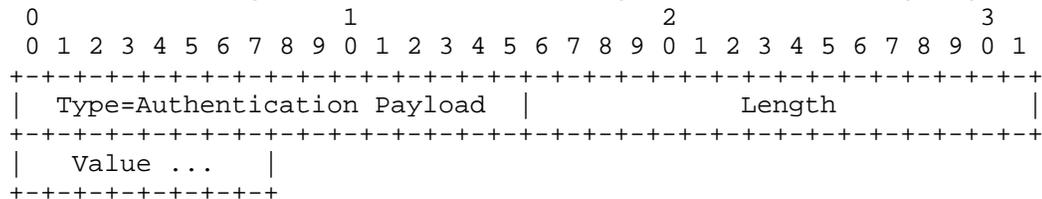
                     Message Element for EAP

Section 4.6 of RFC5415 defines the semantics of Message Element
Types. Type values from 1-49 have been used. An extended message
element type is requested by this document to carry the EAP
authentication payload.

4. IANA Considerations

This document has the following requests to the IANA.

CAPWAP Control Message Type Value for the EAP-AUTHENTICATION-CONTROL,
as defined in Section. 3.1 of this document.

CAPWAP Control Message Element Type Value for the EAP-AUTHENTICATION-
PAYLOAD, as defined in Section. 3.2 of this document.

5. Security Considerations

Security considerations for the CAPWAP protocol has been analyzed in
Section 12 of RFC5415. This document extends the CAPWAP CONTROL
Message Type and Control Message Element Type, and it does not
introduce other security issues besides what has been analyzed in
RFC5415.

6. Contributors

This document stems from the joint work of Hui Deng, Hong Liu, Yifan
Chen, Chunju Shao from China Mobile Research. Thank all the
contributors of this document.

7. References

7.1. Normative References

   [RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And
              Provisioning of Wireless Access Points (CAPWAP) Protocol
              Specification", RFC 5415, March 2009.

7.2. Informative 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.

   [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H.
              Levkowetz, "Extensible Authentication Protocol (EAP)",
              RFC 3748, June 2004.

   [RFC4564] Govindan, S., Cheng, H., Yao, ZH., Zhou, WH., and L. Yang,
              "Objectives for Control and Provisioning of Wireless
              Access Points (CAPWAP)", RFC 4564, July 2006.

   [RFC5416] Calhoun, P., Montemurro, M., and D. Stanley, "Control and
              Provisioning of Wireless Access Points (CAPWAP) Protocol
              Binding for IEEE 802.11", RFC 5416, March 2009.

   [RFC5417] Calhoun, P., "Control And Provisioning of Wireless Access
              Points (CAPWAP) Access Controller DHCP Option", RFC 5417,
              March 2009.

Authors' Addresses

   Rong Zhang
   China Telecom
   No.109 Zhongshandadao avenue
   Guangzhou,   510630
   China

   Phone:
   Fax:
   Email: zhangr@gsta.com
   URI:

      Zhen Cao
      China Mobile
      Xuanwumenxi Ave. No. 32
      Beijing,   100871
      China

      Phone: +86-10-52686688
      Email: zehn.cao@gmail.com, caozhen@chinamobile.com

      Haiyun Luo
      China Mobile
      United States

      Phone:
      Fax:
      Email: haiyunluo@chinamobile.com
      URI: