Network Working Group   Bernard Aboba
INTERNET-DRAFT   Microsoft Corporation
Category: Proposed Standard   Jouni Malinen
Expires: October 2, 2012   Devicescape Software
Updates: 4072   Paul Congdon
                                         Hewlett Packard Company
                                                  Joseph Salowey
                                                   Cisco Systems
                                                      Mark Jones
                                                          Amdocs
                                                   4 April 2012

RADIUS Attributes for IEEE 802 Networks
draft-ietf-radext-ieee802ext-01.txt

Abstract

   RFC 3580 provides guidelines for the use of the Remote Authentication
   Dialin User Service (RADIUS) within IEEE 802 local area networks
   (LANs). This document proposes additional attributes for use within
   IEEE 802 networks, as well as providing clarifications on the usage
   of the EAP-Key-Name attribute, updating RFC 4072. The attributes
   defined in this document are usable both within RADIUS and Diameter.

Status of This Memo

   This Internet-Draft is submitted 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 2, 2012.

Table of Contents

1. Introduction

   In situations where it is desirable to centrally manage
   authentication, authorization and accounting (AAA) for IEEE 802
   [IEEE-802] networks, deployment of a backend authentication and
   accounting server is desirable. In such situations, it is expected
   that IEEE 802 authenticators will function as AAA clients.

   "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)
   Usage Guidelines" [RFC3580] defined guidelines for the use of the
   Remote Authentication Dialin User Service (RADIUS) within networks
   utilizing IEEE 802 local area networks. This document defines
   additional attributes suitable for usage by IEEE 802 authenticators
   acting as AAA clients. The attributes defined in this document are
   usable both within RADIUS and Diameter.

1.1. Terminology

This document uses the following terms:

Access Point (AP)
                A Station that provides access to the distribution
                services via the wireless medium for associated Stations.

Association   The service used to establish Access Point/Station
                mapping and enable Station invocation of the distribution
                system services.

authenticator   An authenticator is an entity that require authentication
                from the supplicant. The authenticator may be connected
                to the supplicant at the other end of a point-to-point
                LAN segment or wireless link.

authentication server
                An authentication server is an entity that provides an
                authentication service to an authenticator. This service
                verifies from the credentials provided by the supplicant,
                the claim of identity made by the supplicant.

Station (STA)   Any device that contains an IEEE 802.11 conformant medium
                access control (MAC) and physical layer (PHY) interface
                to the wireless medium (WM).

Supplicant   A supplicant is an entity that is being authenticated by
                an authenticator. The supplicant may be connected to the
                authenticator at one end of a point-to-point LAN segment
                or 802.11 wireless link.

1.2. Requirements Language

In this document, several words are used to signify the requirements
of the specification. 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].

2. RADIUS attributes

2.1. Allowed-Called-Station-Id

Description

The Allowed-Called-Station-Id Attribute allows the RADIUS server
to specify the authenticator MAC addresses and/or networks to
which the user is allowed to connect. One or more Allowed-Called-
Station-Id attributes MAY be included in an Access-Accept or CoA-
Request packet.

A summary of the Allowed-Called-Station-Id Attribute format is
shown below. The fields are transmitted from left to right.

```
 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      |    Length     |            String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

TBD1

Length

>=3

String

The String field is one or more octets, containing the layer 2
endpoint that the user's call is allowed to be terminated on, as
specified in the definition of Called-Station-Id in [RFC2865]
Section 5.30 and [RFC3580] Section 3.20. In the case of IEEE 802,
the Allowed-Called-Station-Id Attribute is used to store the
Medium Access Control (MAC) address in ASCII format (upper case
only), with octet values separated by a "-". Example:
"00-10-A4-23-19-C0". Where restrictions on both the network and
authenticator MAC address usage are intended, the network name

MUST be appended to the authenticator MAC address, separated from the MAC address with a ":". Example: "00-10-A4-23-19-C0:AP1". Where no MAC address restriction is intended, the MAC address field MUST be omitted, but the network name field MUST be included. Example: "AP1". Within IEEE 802.11 [IEEE-802.11], the SSID constitutes the network name; within IEEE 802.1X [IEEE-802.1X], the Network-Id Name (NID-Name) constitutes the network name. Since a NID-Name can be up to 253 octets in length, when used with [IEEE-802.1X], there may not be sufficient room within the Allowed-Called-Station-Id Attribute to include a MAC address.

If the user attempts to connect to the NAS from a Called-Station-Id that does not match one of the Allowed-Called-Station-Id attributes, then the user MUST NOT be permitted to access the network.

The Allowed-Called-Station-Id Attribute can be useful in the following situations:

[1]   Where users can connect to a NAS without an Access-Request being sent by the NAS to the RADIUS server (e.g. where key caching is supported within IEEE 802.11 or IEEE 802.1X [IEEE-802.1X]). To avoid elevation of privilege attacks, key cache entries are typically only usable within the network to which the user originally authenticated (e.g. the originally selected network name is implicitly attached to the key cache entry). Also, if it is desired that access to a network name not be available from a particular authenticator MAC address, then the authenticator can be set up not to advertise that particular network name.

[2]   Where pre-authentication may be supported (e.g. IEEE 802.1X pre-authentication). In this situation, the network name typically will not be included in a Called-Station-Id Attribute within the Access-Request, so that the RADIUS server will not know the network that the user is attempting to access. As a result, the RADIUS server may desire to restrict the networks to which the user can subsequently connect.

[3]   Where the network portion of the Called-Station-Id is present within an Access-Request, the RADIUS server can desire to authorize access to a network different from the one that the user selected.

2.2. **EAP-Key-Name**

   Description

      The EAP-Key-Name Attribute, defined in "Diameter Extensible
      Authentication Protocol (EAP) Application" [RFC4072], contains the
      EAP Session-Id, as described in "Extensible Authentication
      Protocol (EAP) Key Management Framework" [RFC5247]. Exactly how
      this Attribute is used depends on the link layer in question.

      It should be noted that not all link layers use this name and
      existing EAP method implementations do not generate it. An EAP-
      Key-Name Attribute MAY be included within Access-Request, Access-
      Accept and CoA-Request packets. A summary of the EAP-Key-Name
      Attribute format is shown below. The fields are transmitted from
      left to right.

```
    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      |    Length     |         String...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Code

      102 [RFC4072]

   Length

      >=3

   String

      The String field is one or more octets, containing the EAP
      Session-Id, as defined in "Extensible Authentication Protocol
      (EAP) Key Management Framework" [RFC5247]. Since the NAS operates
      as a pass-through in EAP, it cannot know the EAP Session-Id before
      receiving it from the RADIUS server. As a result, an EAP-Key-Name
      Attribute sent in an Access-Request MUST only contain a single NUL
      character. A RADIUS server receiving an Access-Request with an
      EAP-Key-Name Attribute containing anything other than a single NUL
      character MUST silently discard the Attribute. In addition, the
      RADIUS server SHOULD include this Attribute in an Access-Accept or
      CoA-Request only if an EAP-Key-Name Attribute was present in the
      Access-Request.

2.3.   **EAP-Peer-Id**

   Description

      The EAP-Peer-Id Attribute contains a Peer-Id generated by the EAP
      method. Exactly how this name is used depends on the link layer
      in question. See [RFC5247] for more discussion. The EAP-Peer-Id
      Attribute MAY be included in Access-Request, Access-Accept and
      Accounting-Request packets. More than one EAP-Peer-Id Attribute
      MUST NOT be included in an Access-Request; one or more EAP-Peer-Id
      attributes MAY be included in an Access-Accept.

      It should be noted that not all link layers use this name, and
      existing EAP method implementations do not generate it. Since the
      NAS operates as a pass-through in EAP [RFC3748], it cannot know
      the EAP-Peer-Id before receiving it from the RADIUS server. As a
      result, an EAP-Peer-Id Attribute sent in an Access-Request MUST
      only contain a single NUL character. A home RADIUS server
      receiving an Access-Request an EAP-Peer-Id Attribute containing
      anything other than a single NUL character MUST silently discard
      the Attribute. In addition, the home RADIUS server SHOULD include
      one or more EAP-Peer-Id attributes in an Access-Accept only if an
      EAP-Peer-Id Attribute was present in the Access-Request. A
      summary of the EAP-Peer-Id Attribute format is shown below. The
      fields are transmitted from left to right.

```
 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      |    Length     |             String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Code

      TBD2

   Length

      >=3

   String

      The String field is one or more octets containing a EAP Peer-Id
      exported by the EAP method. For details, see [RFC5247] Appendix
      A. A robust implementation SHOULD support the field as
      undistinguished octets.

2.4. **EAP-Server-Id**

   Description

      The EAP-Server-Id Attribute contains a Server-Id generated by the
      EAP method. Exactly how this name is used depends on the link
      layer in question. See [RFC5247] for more discussion. The EAP-
      Server-Id Attribute is only allowed in Access-Request, Access-
      Accept, and Accounting-Request packets. More than one EAP-Server-
      Id Attribute MUST NOT be included in an Access-Request; one or
      more EAP-Server-Id attributes MAY be included in an Access-Accept.

      It should be noted that not all link layers use this name, and
      existing EAP method implementations do not generate it. Since the
      NAS operates as a pass-through in EAP [RFC3748], it cannot know
      the EAP-Server-Id before receiving it from the RADIUS server. As
      a result, an EAP-Server-Id Attribute sent in an Access-Request
      MUST contain only a single NUL character. A home RADIUS server
      receiving in an Access-Request an EAP-Server-Id Attribute
      containing anything other than a single NUL character MUST
      silently discard the Attribute. In addition, the home RADIUS
      server SHOULD include this Attribute an Access-Accept only if an
      EAP-Server-Id Attribute was present in the Access-Request. A
      summary of the EAP-Server-Id Attribute format is shown below. The
      fields are transmitted from left to right.

```
        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      |    Length     |           String...
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Code

      TBD3

   Length

      >=3

   String

      The String field is one or more octets, containing a EAP Server-Id
      exported by the EAP method. For details, see [RFC5247] Appendix
      A. A robust implementation SHOULD support the field as
      undistinguished octets.

2.5. Mobility-Domain-Id

   Description

      A single Mobility-Domain-Id Attribute MAY be included in an
      Access-Request or Accounting-Request, in order to enable the NAS
      to provide the RADIUS server with the Mobility Domain Identifier
      (MDID), defined in IEEE 802.11 [IEEE-802.11]. A summary of the
      Mobility-Domain-Id Attribute format is shown below. The fields
      are transmitted from left to right.

```
 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      |    Length     |              Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
          Value                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Code

      TBD4

   Length

      6

   Value

      The Value field is four octets, containing a 32-bit unsigned
      integer. Since the Mobility Domain Identifier defined in IEEE
      802.11 [IEEE-802.11] is only two octets in length, the two most
      significant octets MUST be set to zero by the sender, and are
      ignored by the receiver; the two least significant octets contain
      the MDID value.

2.6. Preauth-Timeout

   Description

      This Attribute sets the maximum number of seconds which pre-
      authentication state is required to be kept by the NAS, without
      being utilized within a user session. For example, when
      [IEEE-802.11] pre-authentication is used, if a user has not
      attempted to utilize the PMK derived as a result of pre-
      authentication within the time specified by the Preauth-Timeout
      Attribute, the PMK MAY be discarded by the Access Point. However,
      once the session is underway, the Preauth-Timeout Attribute has no

bearing on the maximum session time for the user, or the maximum
time during which key state may be kept prior to re-
authentication. This is determined by the Session-Timeout
Attribute, if present.

This Attribute MAY be sent by the server to the NAS in an Access-
Accept. A summary of the Preauth-Timeout Attribute format is
shown below. The fields are transmitted from left to right.

```
 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      |    Length     |               Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           Value (cont)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

TBD5

Length

6

Value

The field is 4 octets, containing a 32-bit unsigned integer
encoding the maximum time in seconds that pre-authentication state
should be retained by the NAS.

2.7. Network-Id-Name

Description

The Network-Id-Name Attribute is utilized by implementations of
IEEE-802.1X [IEEE-802.1X] to specify the name of a Network-Id
(NID-Name).

Unlike the IEEE 802.11 SSID (which is a maximum of 32 octets in
length), the NID-Name may be up to 253 octets in length.
Consequently, if the MAC address is included within the Called-
Station-Id Attribute, it is possible that there will not be enough
remaining space to encode the NID-Name as well. Therefore when
used with IEEE 802.1X [IEEE-802.1X], the Called-Station-Id
Attribute SHOULD contain only the MAC address, with the Network-
Id-Name Attribute used to transmit the NID-Name. The Network-Id-
Name Attribute SHOULD NOT be used to encode the IEEE 802.11 SSID;

as noted in [RFC3580], the Called-Station-Id Attribute is used for this purpose.

Zero or one Network-Id-Name Attribute is permitted within a RADIUS Access-Request or Accounting-Request packet. When included within an Access-Request packet, the Network-Id-Name Attribute represents a hint of the NID-Name to which the Supplicant should be granted access. In order to indicate which network names the Supplicant is permitted to access, the Allowed-Called-Station-Id Attribute is provided within an Access-Accept. When included within an Accounting-Request packet, the Network-Id-Name Attribute represents the NID-Name to which the Supplicant has been granted access.

A summary of the Network-Id-Name Attribute format is shown below. The fields are transmitted from left to right.

```
 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      |    Length     |            String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

   TBD6

Length

   >=3

String

   The String field is one or more octets, containing a NID-Name. For details, see [IEEE-802.1X]. A robust implementation SHOULD support the field as undistinguished octets.
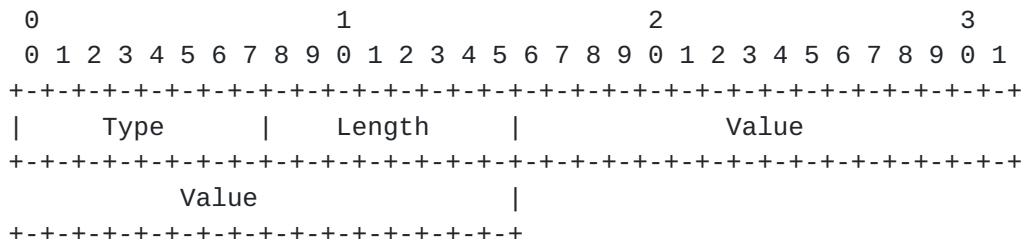
2.8. Access-Info

Description

   The Access-Info Attribute is utilized by implementations of IEEE-802.1X [IEEE-802.1X] to specify the Access status information field within an Access Information Type Length Value Tuple (TLV) to be sent to the user within MACsec Key Agreement (MKA) or EAPoL-Announcement frames.

   A single Access-Info Attribute is permitted within a RADIUS

   Access-Accept, Access-Challenge, Access-Reject or Accounting-
   Request packet.

   A summary of the Access-Info Attribute format is shown below. The
   fields are transmitted from left to right.

```
    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      |    Length     |              Value
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
            Value                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

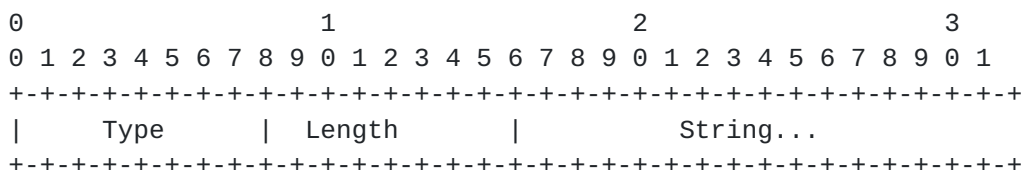   TBD7

Length

   6

Value

   The Value field is four octets containing a 32-bit unsigned
   integer. Since the Access status information field of the Access
   Information TLV defined in [IEEE-802.1X] Section 11.12.2 is only
   two octets in length, the two most significant octets of the Value
   field MUST be set to zero by the sender and are ignored by the
   receiver.

2.9. WLAN-SSID

Description

   The WLAN-SSID attribute contains the Service Set Identifier (SSID)
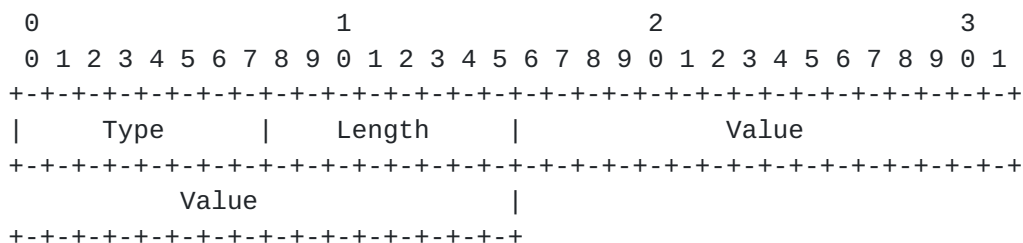   which identifies a specific 802.11 extended service set (ESS).

```
    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      |    Length     |          String...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

   TBD8

Length

   3 to 34

String

   The String field is between 1 and 32 octets in length. The actual
   format of the information is site or application specific, and a
   robust implementation SHOULD support the field as undistinguished
   octets.

2.10. WLAN-HESSID

Description

   The WLAN-HESSID attribute contains a 6-octet MAC address that
   identifies the Homogenous Extended Service Set. The HESSID is a
   globally unique identifier that in conjunction with the WLAN-SSID,
   may be used to provide network identification for a subscription
   service provider network (SSPN).

```
 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      |    Length     |          String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

   TBD9

Length

   19

String

   The String field is encoded in upper-case ASCII characters with
   the octet values separated by dash characters, as described in
   RFC3580 [RFC3580]. Example: "00-10-A4-23-19-C0".

2.11. WLAN-Venue-Info

Description

   The WLAN-Venue-Info attribute identifies the category of venue
   hosting the WLANi.

```
 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      |    Length     |              Value
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
            Value              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

   TBD10

Length

   4

Value

   The Value field is four octets, containing a 32-bit unsigned
   integer. The two most significant octets MUST be set to zero by
   the sender, and are ignored by the receiver; the two least
   significant octets contain the Venue-Group and Venue-Type fields.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Reserved           | Venue-Group   | Venue-Type    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
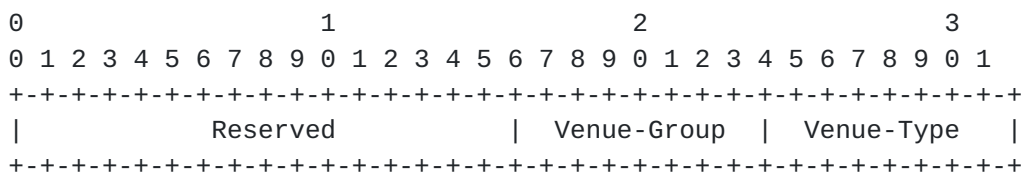
Venue-Group

   The Venue-Group field is a single octet and describes the broad
   category of the venue, e.g. "Assembly". See IEEE 802.11
   [IEEE-802.11] for Venue-Group codes and descriptions.

Venue-Type

   The Venue-Type field is a single octet and describes the venue in
   a finer granularity within the Venue-Group, e.g. "Library". See
   IEEE 802.11 [IEEE-802.11] for Venue-Type codes and descriptions.

2.12. WLAN-Venue-Language

Description

   The WLAN-Venue-Language attribute is an ISO-14962-1997
   [ISO-14962-1997] encoded string that defines the language used in
   the WLAN-Venue-Name attribute. Zero or more WLAN-Venue-Language

attributes may be included in an Access-Request and each one
indicates the language of the WLAN-Venue-Name attribute that
follows it.

```
 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      |     Length     |          String...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   String (cont) |
 +-+-+-+-+-+-+-+-+
```

Code

   TBD11

Length

   5

String

   The String field is a two or three character language code
   selected from ISO-639 [ISO-639]. A two character language code
   has a zero ("null" in ISO-14962-1997) appended to make it 3 octets
   in length.

2.13. WLAN-Venue-Name

Description

   The WLAN-Venue-Name attribute provides additional metadata on the
   BSS. For example, this information may be used to assist a user
   in selecting the appropriate BSS with which to associate. Zero or
   more WLAN-Venue-Name attributes may be included in an Access-
   Request in the same or different languages.

```
 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      |     Length     |          String...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code

   TBD12

Length

      >=3

   String

      The String field is a UTF-8 formatted field containing the venue's
      name. The maximum length of this field is 252 octets.

3. Table of attributes

   The following table provides a guide to which attributes may be found
   in which kinds of packets, and in what quantity.

Access-Request	Access-Accept	Access-Reject	Access-Challenge	#	Attribute
0	0+	0	0	TBD1	Allowed-Called-Station-Id
0-1	0-1	0	0	102	EAP-Key-Name
0-1	0+	0	0	TBD2	EAP-Peer-Id
0-1	0+	0	0	TBD3	EAP-Server-Id
0-1	0	0	0	TBD4	Mobility-Domain-Id
0-1	0-1	0	0	TBD5	Preauth-Timeout
0-1	0	0	0	TBD6	Network-Id-Name
0	0-1	0-1	0-1	TBD7	Access-Info
0-1	0	0	0	TBD8	WLAN-SSID
0-1	0	0	0	TBD9	WLAN-HESSID
0-1	0	0	0	TBD10	WLAN-Venue-Info
0-1	0	0	0	TBD11	WLAN-Venue-Language
0-1	0	0	0	TBD12	WLAN-Venue-Name

CoA-Req	Acct-Req	#	Attribute
0+	0	TBD1	Allowed-Called-Station-Id
0-1	0	102	EAP-Key-Name
0	0+	TBD2	EAP-Peer-Id
0	0+	TBD3	EAP-Server-Id
0	0-1	TBD4	Mobility-Domain-Id
0	0	TBD5	Preauth-Timeout
0	0-1	TBD6	Network-Id-Name
0-1	0-1	TBD7	Access-Info
0	0-1	TBD8	WLAN-SSID
0	0-1	TBD9	WLAN-HESSID
0	0-1	TBD10	WLAN-Venue-Info
0	0-1	TBD11	WLAN-Venue-Language
0	0-1	TBD12	WLAN-Venue-Name

   The following table defines the meaning of the above table entries.

      0   This Attribute MUST NOT be present in packet.
      0+   Zero or more instances of this Attribute MAY be

        present in the packet.
   0-1   Zero or one instance of this Attribute MAY be
         present in the packet.

4. **Diameter Considerations**

   The EAP-Key-Name Attribute is already defined as a RADIUS Attribute
   within Diameter EAP [RFC4072]. When used in Diameter, the other
   attributes defined in this specification can be used as Diameter AVPs
   from the Code space 1-255 (RADIUS Attribute compatibility space). No
   additional Diameter Code values are therefore allocated. The data
   types and flag rules for the attributes are as follows:

```
                                  +---------------------+
                                  |    AVP Flag rules   |
                                  |----+-----+----+-----|----+
                                  |    |     |SHLD| MUST|    |
   Attribute Name        Value Type  |MUST| MAY | NOT|  NOT|Encr|
   ----------------------------------------|----+-----+----+-----|----|
   Allowed-Called-                  |    |     |    |     |    |
   Station-Id            UTF8String | M  |  P  |    |  V  | Y  |
   EAP-Peer-Id           UTF8String | M  |  P  |    |  V  | Y  |
   EAP-Server-Id         UTF8String | M  |  P  |    |  V  | Y  |
   Mobility-Domain-Id    Unsigned32 | M  |  P  |    |  V  | Y  |
   Preauth-Timeout       Unsigned32 | M  |  P  |    |  V  | Y  |
   Network-Id-Name       UTF8String | M  |  P  |    |  V  | Y  |
   Access-Info           Unsigned32 | M  |  P  |    |  V  | Y  |
   WLAN-SSID             UTF8String | M  |  P  |    |  V  | Y  |
   WLAN-HESSID           UTF8Strin  | M  |  P  |    |  V  | Y  |
   WLAN-Venue-Info       Unsigned32 | M  |  P  |    |  V  | Y  |
   WLAN-Venue-Language   UTF8Strin  | M  |  P  |    |  V  | Y  |
   WLAN-Venue-Name       UTF8String | M  |  P  |    |  V  | Y  |
   ----------------------------------------|----+-----+----+-----|----|
```

   The attributes in this specification have no special translation
   requirements for Diameter to RADIUS or RADIUS to Diameter gateways;
   they are copied as is, except for changes relating to headers,
   alignment, and padding. See also [RFC3588] Section 4.1 and [RFC4005]
    Section 9.

   What this specification says about the applicability of the
   attributes for RADIUS Access-Request packets applies in Diameter to
   AA-Request [RFC4005] or Diameter-EAP-Request [RFC4072]. What is said
   about Access-Challenge applies in Diameter to AA-Answer [RFC4005] or
   Diameter-EAP-Answer [RFC4072] with Result-Code AVP set to
   DIAMETER_MULTI_ROUND_AUTH.

   What is said about Access-Accept applies in Diameter to AA-Answer or

Diameter-EAP-Answer messages that indicate success. Similarly, what
is said about RADIUS Access-Reject packets applies in Diameter to AA-
Answer or Diameter-EAP-Answer messages that indicate failure.

What is said about COA-Request applies in Diameter to Re-Auth-Request
[RFC4005]. What is said about Accounting-Request applies to Diameter
Accounting- Request [RFC4005] as well.

5. **IANA Considerations**

This document uses the RADIUS [RFC2865] namespace, see
<http://www.iana.org/assignments/radius-types>. This specification
requires assignment of a RADIUS attribute types for the following
attributes:

```
Attribute                      Type
=========                      ====
Allowed-Called-Station-Id      TBD1
EAP-Peer-Id                    TBD2
EAP-Server-Id                  TBD3
Mobility-Domain-Id             TBD4
Preauth-Timeout                TBD5
Network-Id-Name                TBD6
Access-Info                    TBD7
WLAN-SSID                      TBD8
WLAN-HESSID                    TBD9
WLAN-Venue-Info               TBD10
WLAN-Venue-Language           TBD11
WLAN-Venue-Name               TBD12
```

6. **Security Considerations**

Since this document describes the use of RADIUS for purposes of
authentication, authorization, and accounting in IEEE 802 networks,
it is vulnerable to all of the threats that are present in other
RADIUS applications. For a discussion of these threats, see
[RFC2607], [RFC2865], [RFC3162], [RFC3579], [RFC3580] and [RFC5176].

[7](). References

[7.1](). Normative references

[IEEE-802] IEEE Standards for Local and Metropolitan Area Networks:
          Overview and Architecture, ANSI/IEEE Std 802, 1990.

[IEEE-802.11]
          Information technology - Telecommunications and information
          exchange between systems - Local and metropolitan area
          networks - Specific Requirements Part 11: Wireless LAN
          Medium Access Control (MAC) and Physical Layer (PHY)
          Specifications, IEEE Std. 802.11-2012, 2012.

[IEEE-802.1X]
          IEEE Standard for Local and Metropolitan Area Networks -
          Port-Based Network Access Control, IEEE 802.1X-2010, February
          2010.

[ISO-639] ISO, "Codes for the Representation of Names of Languages".

[ISO-14962-1997]
          ISO, "Space data and information transfer systems - ASCII
          encoded English", 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", RFC 2119, March, 1997.

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

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J.
          Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC4072] Eronen, P., Hiller, T. and G. Zorn, "Diameter Extensible
          Authentication Protocol (EAP) Application", RFC 4072, August
          2005.

[RFC5247] Aboba, B., Simon, D. and P. Eronen, "EAP Key Management
          Framework", RFC 5247, August 2008.

[7.2](). Informative references

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy
          Implementation in Roaming", RFC 2607, June 1999.

[RFC3162]   Aboba, B., Zorn, G. and D. Mitton, "RADIUS and IPv6", RFC
            3162, August 2001.

[RFC3579]   Aboba, B. and P. Calhoun, "RADIUS Support for Extensible
            Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3580]   Congdon, P., Aboba, B., Smith, A., Zorn, G. and J. Roese,
            "IEEE 802.1X Remote Authentication Dial In User Service
            (RADIUS) Usage Guidelines", RFC 3580, September 2003.

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

[RFC4005]   Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter
            Network Access Server Application", RFC 4005, August 2005.

[RFC5176]   Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba,
            "Dynamic Authorization Extensions to Remote Authentication
            Dial In User Service (RADIUS)", RFC 5176, January 2008.

Acknowledgments

Authors' Addresses

   Bernard Aboba
   Microsoft Corporation
   One Microsoft Way
   Redmond, WA 98052

   EMail: bernard_aboba@hotmail.com

   Jouni Malinen
   Devicescape Software, Inc.
   900 Cherry Avenue
   San Bruno, CA 94066

   EMail: jkm@devicescape.com
   Phone: +1 650 829 2600
   Fax: +1 650 829 2601

   Paul Congdon
   Hewlett Packard Company
   HP ProCurve Networking
   8000 Foothills Blvd, M/S 5662
   Roseville, CA 95747

   Phone: +1 916 785 5753
   Fax: +1 916 785 8478
   EMail: paul_congdon@hp.com

   Joseph Salowey
   Cisco Systems

   EMail: jsalowey@cisco.com

   Mark Jones
   Amdocs

   EMail: mark@azu.ca