

RADEXT Working Group
INTERNET-DRAFT
Category: Proposed Standard
Expires: July 20, 2014
Updates: [3580](#), [4072](#)

Bernard Aboba
Microsoft
Jouni Malinen
Devicescape Software
Paul Congdon
Hewlett Packard Company
Joseph Salowey
Cisco Systems
Mark Jones
Azuca Systems
21 January 2014

RADIUS Attributes for IEEE 802 Networks
draft-ietf-radext-ieee802ext-10.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 clarifying the usage of the EAP-Key-Name attribute and the Called-Station-Id attribute. This document updates [RFC 3580](#) as well as [RFC 4072](#).

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 July 20, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](http://trustee.ietf.org/license-info) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

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.

Table of Contents

1.	Introduction	4
1.1	Terminology	4
1.2	Requirements Language	5
2.	RADIUS attributes	5
2.1	Allowed-Called-Station-Id	5
2.2	EAP-Key-Name	6
2.3	EAP-Peer-Id	7
2.4	EAP-Server-Id	8
2.5	Mobility-Domain-Id	9
2.6	Preauth-Timeout	10
2.7	Network-Id-Name	11
2.8	EAPoL-Announcement	12
2.9	WLAN-HESSID	13
2.10	WLAN-Venue-Info	14
2.11	WLAN-Venue-Language	15
2.12	WLAN-Venue-Name	16
2.13	WLAN-Reason-Code	17
2.14	WLAN-Pairwise-Cipher	18
2.15	WLAN-Group-Cipher	19
2.16	WLAN-AKM-Suite	20
2.17	WLAN-Group-Mgmt-Cipher	20
2.18	WLAN-RF-Band	21
3.	Table of attributes	23
4.	IANA Considerations	24
5.	Security Considerations	24
6.	References	25
6.1	Normative References	25
6.2	Informative References	26
	ACKNOWLEDGMENTS	26
	AUTHORS' ADDRESSES	27

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](#)] provides 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.

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.

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].

2.1. Allowed-Called-Station-Id

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, CoA-Request or Accounting-Request packet.

The Allowed-Called-Station-Id Attribute can be useful in situations where pre-authentication is supported (e.g. IEEE 802.11 pre-authentication). In these scenarios, a Called-Station-Id Attribute typically will not be included within the Access-Request so that the RADIUS server will not know the network that the user is attempting to access. The Allowed-Called-Station-Id enables the RADIUS server to restrict the networks and attachment points to which the user can subsequently connect.

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	2	3	4	5	6	7	8	9
+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-
				Type										Length																			String...						
+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-

Code

TBD1

Length

 ≥ 3

String

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	2	3	4	5	6	7	8	9
+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-
				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. Since a NAS will typically only include a EAP-Key-Name Attribute in an Access-Request in situations where the Attribute is required to provision service, if an EAP-Key-Name Attribute is included in an Access-Request but is not present in the Access-Accept, the NAS SHOULD treat the Access-Accept as though it were an Access-Reject. If an EAP-Key-Name Attribute was not present in the Access-Request but is included in the Access-Accept, then the NAS SHOULD silently discard the EAP-Key-Name Attribute.

[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. If a NAS receives EAP-Peer-Id Attribute(s) in an Access-Accept without having included one in an Access-Request, the NAS SHOULD silently discard the Attribute(s). 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. Only a single EAP Peer-Id may be included per Attribute.

[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 Section 8.4.2.49 of [[IEEE-802.11](#)]. A summary of the Mobility-Domain-Id Attribute format is shown below. The fields are transmitted from left to right.

Zero or one Network-Id-Name Attribute is permitted within an Access-Request, Access-Challenge, Access-Accept 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. When included within an Access-Accept packet, the Network-Id-Name Attribute represents the NID-Name to which the Supplicant is to be granted access. 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. EAPoL-Announcement

Description

The EAPoL-Announcement Attribute contains EAPoL-Announcement Type Length Value Tuples (TLVs) defined within Table 11-8 of IEEE-802.1X [[IEEE-802.1X](#)].

Zero or more EAPoL-Announcement attributes are permitted within an Access-Request, Access-Accept, Access-Challenge, Access-Reject, Accounting-Request, CoA-Request or Disconnect-Request packet.

When included within an Access-Request packet, EAPoL-Announcement attributes contain EAPoL-Announcement TLVs that the user sent in an EAPoL-Announcement. When included within an Access-Accept, Access-Challenge, Access-Reject, CoA-Request or Disconnect-Request

The WLAN-HESSID attribute contains a MAC address that identifies the Homogenous Extended Service Set. The HESSID is a globally unique identifier that in conjunction with the SSID, encoded within the Called-Station-Id Attribute as described in [RFC3580], may be used to provide network identification for a subscription service provider network (SSPN), as described in [Section 8.4.2.94](#)

Code

A summary of the WLAN-Venue-Language 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...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
      String (cont) |
+---+---+---+---+---+

```

Code

TBD10

Length

4-5

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.

[2.12.](#) 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 or Accounting-Request in the same or different languages.

A summary of the WLAN-Venue-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

TBD11

Length

The Value field is four octets, containing a 32-bit unsigned integer. The two most significant octets MUST be set to zero by

The Value field is four octets, containing a 32-bit unsigned integer, in Suite selector format as specified in Figure 8-187 within Section 8.4.2.27.2 of [IEEE-802.11], with values of OUI and Suite type drawn from Table 8-99.


```

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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               OUI                               | Suite Type |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

2.15. WLAN-Group-Cipher

Description

The WLAN-Group-Cipher Attribute contains information on the group cipher suite used to establish the robust security network association (RSNA) between the AP and mobile device. A WLAN-Group-Cipher Attribute MAY be included within Access-Request and Accounting-Request packets.

A summary of the WLAN-Group-Cipher 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

TBD14

Length

6

Value

The Value field is four octets, containing a 32-bit unsigned integer, in Suite selector format as specified in Figure 8-187 within Section 8.4.2.27.2 of [[IEEE-802.11](#)], with values of OUI and Suite type drawn from Table 8-99.

```

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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               OUI                               | Suite Type |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

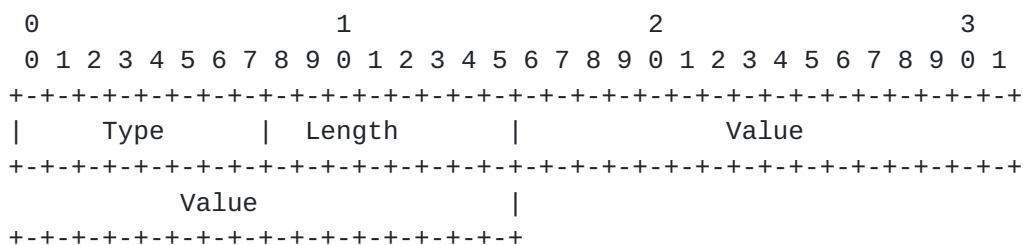
```


2.16. WLAN-AKM-Suite

Description

The WLAN-AKM-Suite Attribute contains information on the authentication and key management suite used to establish the robust security network association (RSNA) between the AP and mobile device. A WLAN-AKM-Suite Attribute MAY be included within Access-Request and Accounting-Request packets.

A summary of the WLAN-AKM-Suite Attribute format is shown below. The fields are transmitted from left to right.



Code

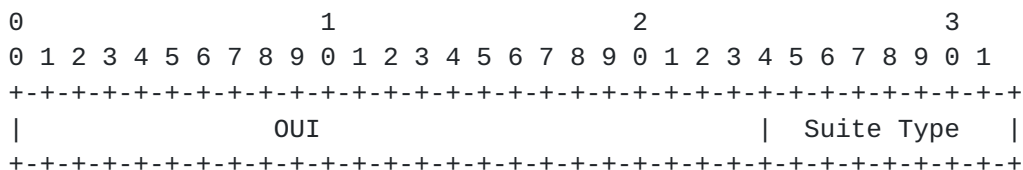
TBD15

Length

6

Value

The Value field is four octets, containing a 32-bit unsigned integer, in Suite selector format as specified in Figure 8-187 within Section 8.4.2.27.2 of [IEEE-802.11], with values of OUI and Suite type drawn from Table 8-101:



2.17. WLAN-Group-Mgmt-Cipher

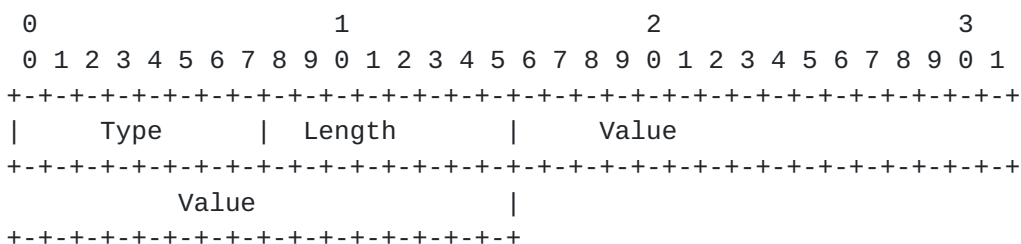
Description

The WLAN-Group-Mgmt-Cipher Attribute contains information on group management cipher used to establish the robust security network

association (RSNA) between the AP and mobile device.

Zero or one WLAN-Group-Mgmt-Cipher Attribute MAY be included within Access-Request and Accounting-Request packets. Presence of the attribute indicates that the station negotiated to use management frame protection during association.

A summary of the WLAN-Group-Mgmt-Cipher Attribute format is shown below. The fields are transmitted from left to right.



Code

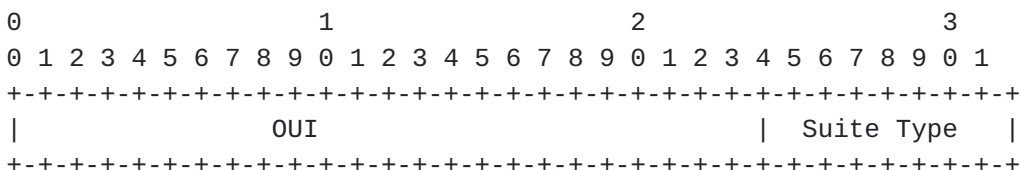
TBD16

Length

6

Value

The Value field is four octets, containing a 32-bit unsigned integer, in Suite selector format as specified in Figure 8-187 within Section 8.4.2.27.2 of [[IEEE-802.11](#)], with values of OUI and Suite type drawn from Table 8-99:

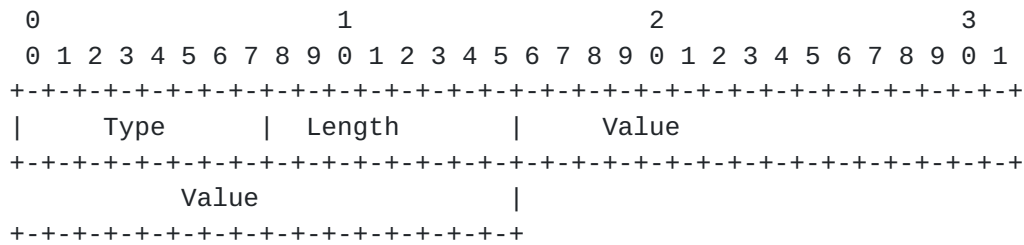


2.18. WLAN-RF-Band

Description

The WLAN-RF-Band Attribute contains information on the RF band used by the Access Point for transmission and reception of information to and from the mobile device. Zero or one WLAN-RF-Band Attribute MAY be included within an Access-Request or Accounting-Request packet.

A summary of the WLAN-RF-Band Attribute format is shown below.
The fields are transmitted from left to right.



Code

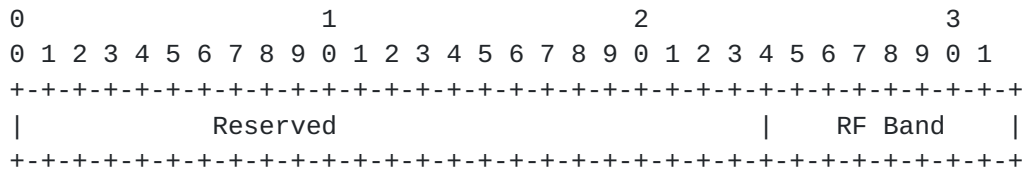
TBD17

Length

6

Value

The Value field is four octets, containing a 32-bit unsigned integer. The three most significant octets MUST be set to zero by the sender, and are ignored by the receiver; the least significant octet contains the RF Band field, whose values are defined in Table 8-53a of [[IEEE-802.11ad](#)].



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+	0+	0+	TBD7	EAPoL-Announcement
0-1	0	0	0	TBD8	WLAN-HESSID
0-1	0	0	0	TBD9	WLAN-Venue-Info
0+	0	0	0	TBD10	WLAN-Venue-Language
0+	0	0	0	TBD11	WLAN-Venue-Name
0	0	0-1	0	TBD12	WLAN-Reason-Code
0-1	0	0	0	TBD13	WLAN-Pairwise-Cipher
0-1	0	0	0	TBD14	WLAN-Group-Cipher
0-1	0	0	0	TBD15	WLAN-AKM-Suite
0-1	0	0	0	TBD16	WLAN-Group-Mgmt-Cipher
0-1	0	0	0	TBD17	WLAN-RF-Band

CoA-Req	Dis-Req	Acct-Req	#	Attribute
0+	0	0+	TBD1	Allowed-Called-Station-Id
0-1	0	0	102	EAP-Key-Name
0	0	0+	TBD2	EAP-Peer-Id
0	0	0+	TBD3	EAP-Server-Id
0	0	0-1	TBD4	Mobility-Domain-Id
0-1	0	0	TBD5	Preauth-Timeout
0	0	0-1	TBD6	Network-Id-Name
0+	0+	0+	TBD7	EAPoL-Announcement
0	0	0-1	TBD8	WLAN-HESSID
0	0	0-1	TBD9	WLAN-Venue-Info
0	0	0+	TBD10	WLAN-Venue-Language
0	0	0+	TBD11	WLAN-Venue-Name
0	0-1	0-1	TBD12	WLAN-Reason-Code
0	0	0-1	TBD13	WLAN-Pairwise-Cipher
0	0	0-1	TBD14	WLAN-Group-Cipher
0	0	0-1	TBD15	WLAN-AKM-Suite
0	0	0-1	TBD16	WLAN-Group-Mgmt-Cipher
0	0	0-1	TBD17	WLAN-RF-Band

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. 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
EAPoL-Announcement	TBD7
WLAN-HESSID	TBD8
WLAN-Venue-Info	TBD9
WLAN-Venue-Language	TBD10
WLAN-Venue-Name	TBD11
WLAN-Reason-Code	TBD12
WLAN-Pairwise-Cipher	TBD13
WLAN-Group-Cipher	TBD14
WLAN-AKM-Suite	TBD15
WLAN-Group-Mgmt-Cipher	TBD16
WLAN-RF-Band	TBD17

Since this specification relies entirely on values assigned by IEEE 802, no registries are established for maintenance by the IANA.

5. 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](#)].

While it is possible for a RADIUS server to make decisions on whether to Accept or Reject an Access-Request based on the values of the WLAN-Pairwise-Cipher, WLAN-Group-Cipher, WLAN-AKM-Suite, WLAN-Group-Mgmt-Cipher and WLAN-RF-Band Attributes the value of doing this is

limited. In general, an Access-Reject should not be necessary, except where Access Points and Stations are misconfigured so as to enable connections to be made with unacceptable values. Rather than rejecting access on an ongoing basis, users would be better served by fixing the misconfiguration.

Where access does need to be rejected, the user should be provided with an indication of why the problem has occurred, or else they are likely to become frustrated. For example, if the values of the WLAN-Pairwise-Cipher, WLAN-Group-Cipher, WLAN-AKM-Suite or WLAN-Group-Mgmt-Cipher Attributes included in the Access-Request are not acceptable to the RADIUS server, then a WLAN-Reason-Code Attribute with a value of 29 (Requested service rejected because of service provider cipher suite or AKM requirement) SHOULD be returned in the Access-Reject. Similarly, if the value of the WLAN-RF-Band Attribute included in the Access-Request is not acceptable to the RADIUS server, then a WLAN-Reason-Code Attribute with a value of 11 (Disassociated because the information in the Supported Channels element is unacceptable) SHOULD be returned in the Access-Reject.

6. References

6.1. 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-802.11ad]
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, Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band, IEEE Std. 802.11ad-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.
- [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.

[6.2.](#) 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.
- [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

The authors would like to acknowledge Maximilian Riegel, Dorothy Stanley, Yoshihiro Ohba, and the contributors to the IEEE 802.1 and IEEE 802.11 reviews of this document, for useful discussions.

Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

E-Mail: bernard_aboba@hotmail.com

Jouni Malinen
E-Mail: j@w1.fi

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
E-Mail: paul_congdon@hp.com

Joseph Salowey
Cisco Systems
E-Mail: jsalowey@cisco.com

Mark Jones
Azuca Systems
E-Mail: mark@azu.ca

