

Network Working Group
INTERNET-DRAFT
Category: Proposed Standard
Expires: April 30, 2010
Updates: RFC [4072](#)

Bernard Aboba
Microsoft Corporation
Jouni Malinen
Devicescape Software
Paul Congdon
Hewlett Packard Company
Joseph Salowey
Cisco Systems
25 October 2009

RADIUS Attributes for IEEE 802 Networks
draft-aboba-radext-wlan-12.txt

Status of This Memo

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

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 April 30, 2010.

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

[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. The attributes defined in this document are usable both within RADIUS and Diameter.

Table of Contents

1.	Introduction	3
1.1	Terminology	3
1.2	Requirements Language	4
2.	RADIUS attributes	4
2.1	Allowed-Called-Station-Id	4
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	9
2.7	EAP-Lower-Layer	10
2.8	Network-Id-Name	11
2.9	Access-Status	12
3.	Table of attributes	13
4.	Diameter Considerations	14
5.	IANA Considerations	15
6.	Security Considerations	16
7.	References	16
7.1	Normative References	16
7.2	Informative References	17
	ACKNOWLEDGMENTS	18
	AUTHORS' ADDRESSES	18

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.

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-REV [[IEEE-802.1X-REV](#)], 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-REV](#)], 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-REV [[IEEE-802.1X-REV](#)]). 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.

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.

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.

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. EAP-Lower-Layer

Description

This Attribute provides information relating to the lower layer over which EAP is transported. This Attribute MAY be sent by the NAS to the RADIUS server in an Access-Request or an Accounting-Request packet. A summary of the EAP-Lower-Layer 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

TBD6

Length

6

Value

The field is 4 octets, containing a 32-bit unsigned integer with the following values:

- 1 - Wired IEEE 802.1X Version 1 (2001)
- 2 - Wired IEEE 802.1X Version 2 (2004) [[IEEE-802.1X](#)]
- 3 - Wired IEEE 802.1X Version 3 [[IEEE-802.1X-REV](#)]
- 4 - WPA
- 5 - WPA2 (no pre-authentication)
- 6 - WPA2, IEEE 802.1X pre-authentication
- 7 - IEEE 802.11r
- 8 - IEEE 802.11s
- 9 - IEEE 802.16e
- 10 - IKEv2
- 11 - PPP
- 12 - PANA (no pre-authentication)

[2.8.](#) Network-Id-Name

Description

The Network-Id-Name Attribute is utilized by implementations of IEEE-802.1X-REV [[IEEE-802.1X-REV](#)] 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-REV, 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

TBD7

Length

>=3

String

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

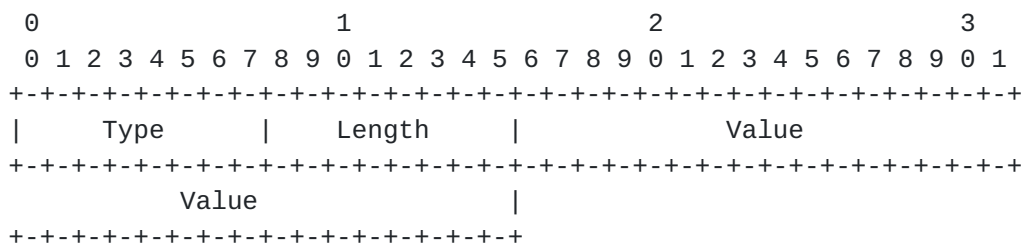
2.9. Access-Status

Description

The Access-Status Attribute is utilized by implementations of IEEE-802.1X-REV [[IEEE-802.1X-REV](#)] to specify the Status bits within an Access Information Type Length Value tuple (TLVs) sent to the user within MACsec Key Agreement (MKA) or EAPoL-Announcement frames.

A single Access-Status Attribute is permitted within a RADIUS Access-Accept or Accounting-Request packet.

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



Code

TBD8

Length

6

Value

The Value field is four octets containing a 32-bit unsigned integer. Since the Access status information field defined in [\[IEEE-802.1X-REV\] Section 11.12.2](#) 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.

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	EAP-Lower-Layer
0-1	0	0	0	TBD7	Network-Id-Name
0	0-1	0	0	TBD8	Access-Status

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	EAP-Lower-Layer
0	0-1	TBD7	Network-Id-Name
0-1	0-1	TBD8	Access-Status

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		P		V	Y		
Preauth-Timeout	Unsigned32	M	P		V	Y		
EAP-Lower-Layer	Unsigned32	M	P		V	Y		
Network-Id-Name	UTF8String	M	P		V	Y		
Access-Status	Unsigned32	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
EAP-Lower-Layer	TBD6
Network-Id-Name	TBD7
Access-Status	TBD8

This specification allocates the following decimal values for the EAP-Lower-Layer Attribute:

- 1 - Wired IEEE 802.1X Version 1 (2001)
- 2 - Wired IEEE 802.1X Version 2 (2004) [[IEEE-802.1X](#)]
- 3 - Wired IEEE 802.1X Version 3 [[IEEE-802.1X-REV](#)]
- 4 - WPA
- 5 - WPA2 (no pre-authentication)
- 6 - WPA2, IEEE 802.1X pre-authentication
- 7 - IEEE 802.11r
- 8 - IEEE 802.11s
- 9 - IEEE 802.16e
- 10 - IKEv2
- 11 - PPP
- 12 - PANA (no pre-authentication)

Additional values are allocated as described in "IANA Considerations

for RADIUS" [\[RFC3575\]](#) [Section 2.1](#) (Designated Expert).

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. 802.11-2007, 2007.
- [IEEE-802.11r] Draft Amendment to Standard for 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 2: Fast BSS Transition, IEEE P802.11r/D9.0, March 2008.
- [IEEE-802.1X-REV] Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control, D4.5, October 2009.
- [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.
- [RFC3575] Aboba, B., "IANA Considerations for RADIUS", [RFC 3575](#), July 2003.
- [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

- [IEEE-802.1X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004, December 2004.
- [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.
- [RFC3575] Aboba, B., "IANA Considerations for RADIUS", [RFC 3575](#), July 2003.
- [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. Roesse, "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

The authors would like to acknowledge Mick Seaman, 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

EMail: bernarda@microsoft.com
Phone: +1 425 706 6605
Fax: +1 425 936 7329

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

