Network Working Group
INTERNET-DRAFT
Category: Proposed Standard
Expires: December 25, 2007

Bernard Aboba
Microsoft Corporation
Jouni Malinen
Devicescape Software
26 June 2007

RADIUS Attributes for WLAN
draft-aboba-radext-wlan-04.txt

This Internet-Draft will expire on December 25, 2007.

Abstract

This document proposes additional attributes for use by wireless LAN authenticators. The attributes defined in this document are usable both within RADIUS and Diameter.

Table of Contents

1. Introduction

In situations where it is desirable to centrally manage authentication, authorization and accounting (AAA) for IEEE 802.11 wireless LANs [IEEE-802.11], deployment of a backend authentication and accounting server is desirable. In such situations, it is expected that IEEE 802.11 authenticators will function as AAA clients. This document defines additional attributes suitable for usage by IEEE 802.11 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 802.11 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

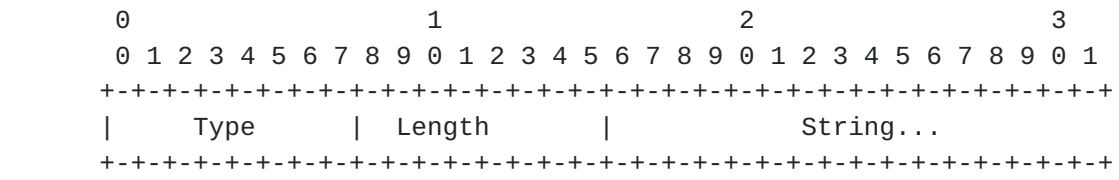
In this document, several words are used to signify the requirements of the specification. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. RADIUS attributes

2.1. Allowed-Called-Station-Id

Description

The Allowed-Called-Station-Id Attribute allows the RADIUS server to specify which Called-Station-Ids and SSIDs the user is allowed to access. 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.



Code

TBD

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 bridge or Access Point MAC address in ASCII format (upper case only), with octet values separated by a "-". Example: "00-10-A4-23-19-C0". In IEEE 802.11, where restrictions on both SSID and Access Point MAC address usage are intended, the SSID MUST be appended to the Access Point 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 ":" and SSID fields MUST be included. Example ":AP1".

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.

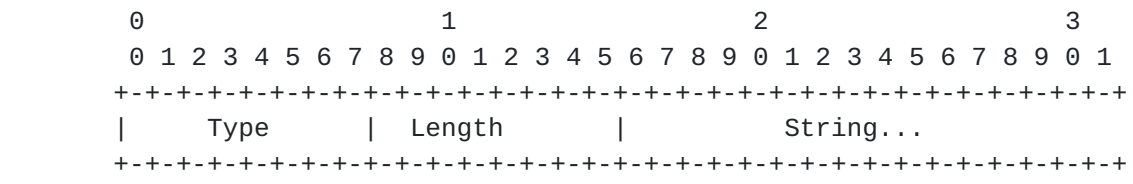
The Allowed-Called-Station-Id Attribute is useful in situations where users can connect to a NAS without an Access-Request being sent by the NAS to the RADIUS server (e.g. IEEE 802.11 PMK caching), or where pre-authentication may be supported (e.g. IEEE 802.11 pre-authentication) so it is possible that the SSID will not be included in a Called-Station-Id Attribute within the Access-Request. In these cases, it can be desirable for the RADIUS server to provide the NAS with usage restrictions.

2.2. EAP-Key-Name

Description

The EAP-Key-Name Attribute, defined in [RFC4072], contains the EAP Session-Id, as described in [KEYFRAME]. 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.



Code

102 [RFC4072]

Length

>=2

String

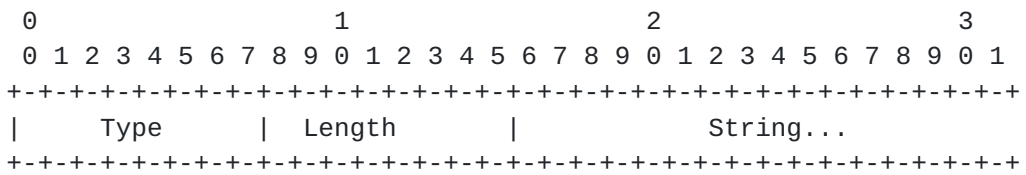
The String field, when present, is one or more octets, containing the EAP Session-Id, as defined in [KEYFRAME]. Since the NAS operates as a pass-through in EAP, it cannot know the EAP Session-Id before receiving it from the RADIUS server. As a result, an EAP-Key-Name Attribute sent in an Access-Request MUST NOT contain any data. A RADIUS server receiving an Access-Request with an EAP-Key-Name Attribute containing data MUST silently discard the Attribute. In addition, the RADIUS server SHOULD only include this Attribute in an Access-Accept or CoA-Request 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 [KEYFRAME] 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, 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 NOT contain any data. A home RADIUS server receiving an Access-Request an EAP-Peer-Id Attribute with non-empty data 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 empty 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.



Code

TBD

Length

>=2

String

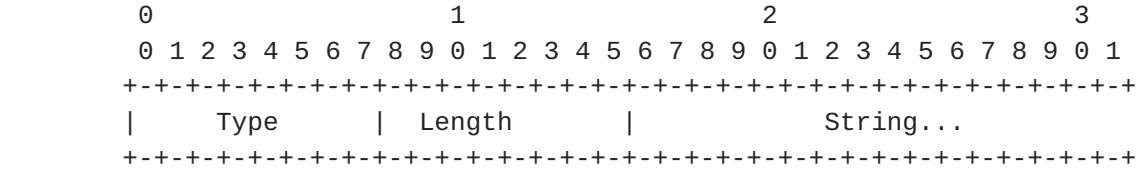
The String field, when present, is one or more octets containing a EAP Peer-Id exported by the EAP method. For details, see [KEYFRAME] Appendix A. A robust implementation SHOULD support the field as undistinguished octets.

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 [KEYFRAME] 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, 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 NOT contain any data. A home RADIUS server receiving in an Access-Request an EAP-Server-Id Attribute with non-empty data MUST silently discard the Attribute. In addition, the home RADIUS server SHOULD include this Attribute an Access-Accept only if an empty 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.



Code

TBD

Length

>=2

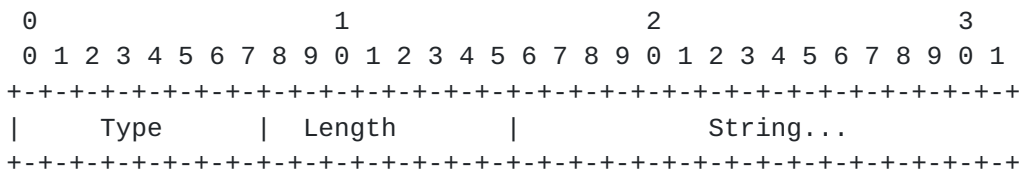
String

The String field, when present, is one or more octets, containing the EAP Server-Id exported by the EAP method. For details, see [KEYFRAME] 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, defined in [IEEE-802.11r]. A summary of the Mobility-Domain-Id Attribute format is shown below. The fields are transmitted from left to right.



Code

TBD

Length

>=3

String

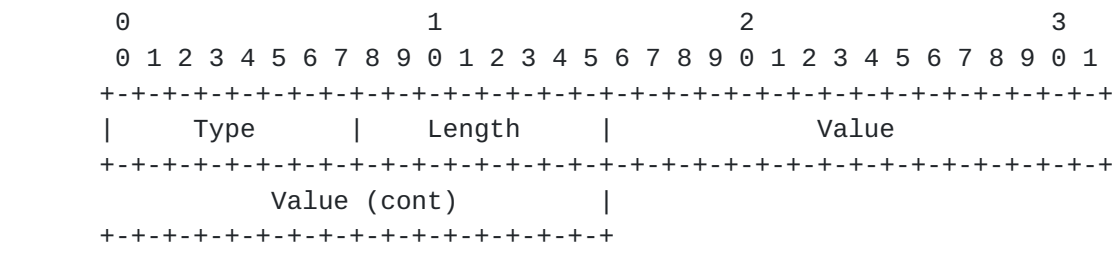
The String field contains one or more octets, encoding a single Mobility Domain Identifier as defined in [IEEE-802.11r]. UTF-8 encoded 10646 characters are recommended, but a robust implementation SHOULD support the field as undistinguished octets.

2.6. Preauth-Timeout

Description

This Attribute sets the maximum number of seconds which pre-authentication state is kept by the NAS. This Attribute MAY be sent by the server to the NAS in an Access-Accept. Where both Session-Timeout and Preauth-Timeout attributes are present in an Access-Accept, the Session-Timeout Attribute refers only to the

maximum session time after the station associates with the AP and is enabled to send data frames through it. A summary of the Preauth-Timeout Attribute format is shown below. The fields are transmitted from left to right.



Code

TBD

Length

6

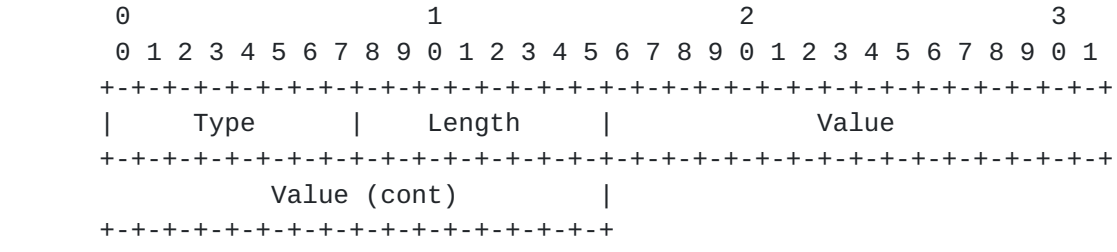
Value

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

2.7. EAP-Lower-Layer

Description

This Attribute indicates the lower layer over which EAP is transported. This Attribute MAY be sent by the NAS to the 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.



Code

TBD

Length

6

Value

The field is 4 octets, containing the following values:

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

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	CoA-Req	Acct-Req	#	Attribute
0	0+	0	0	0+	0	TBD	Allowed-Called-Station-Id
0-1	0-1	0	0	0-1	0	102	EAP-Key-Name
0+	0+	0	0	0	0+	TBD	EAP-Peer-Id
0+	0+	0	0	0	0+	TBD	EAP-Server-Id
0-1	0	0	0	0	0-1	TBD	Mobility-Domain-Id
0-1	0-1	0	0	0	0	TBD	Preauth-Timeout
0-1	0	0	0	0	0-1	TBD	EAP-Lower-Layer

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				
Attribute Name	Value Type	MUST	MAY	SHLD NOT	MUST 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	OctetString		P,M		V	Y
Preauth-Timeout	Unsigned32	M	P		V	Y
EAP-Lower-Layer	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 [RFC 3588] Section 4.1 and [RFC 4005] Section 9.

What this specification says about the applicability of the attributes for RADIUS Access-Request packets applies in Diameter to AA-Request [RFC 4005] or Diameter-EAP-Request [RFC 4072]. What is said about Access-Challenge applies in Diameter to AA-Answer [RFC 4005] or Diameter-EAP-Answer [RFC 4072] 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 [RFC 4005].

What is said about Accounting-Request applies to Diameter Accounting-Request [RFC 4005] 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	TBD
EAP-Peer-Id	TBD
EAP-Server-Id	TBD
Mobility-Domain-Id	TBD
Preauth-Timeout	TBD
EAP-Lower-Layer	TBD

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)
3 - WPA
4 - WPA2 (no pre-authentication)
5 - WPA2, IEEE 802.1X pre-authentication
6 - IEEE 802.11r
7 - IEEE 802.11s
8 - IEEE 802.11af
9 - IEEE 802.16e
10 - IKEv2
11 - PPP
12 - PANA (no pre-authentication)

Additional values are allocated as described in [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 WLANs, 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], [RFC3576], [RFC3579], and [RFC3580].

7. References

7.1. Normative references

[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/D6.0, June 2007.

[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.

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

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

[KEYFRAME]
Aboba, B., Simon, D., Eronen, P. and H. Levkowetz, "EAP Key Management Framework", draft-ietf-eap-keying-19.txt, June 2007.

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.

[RFC3575] Aboba, B., "IANA Considerations for RADIUS", RFC 3575, July 2003.

[RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, 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. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

Acknowledgments

The authors would like to acknowledge Dorothy Stanley of Aruba Networks, Yoshihiro Ohba of Toshiba, and the contributors to the IEEE 802.11 review of this document.

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

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

Open issues

Open issues relating to this specification are tracked on the following web site:

http://www.drizzle.com/~aboba/RADEXT/