Network Working Group
INTERNET-DRAFT
Category: Proposed Standard
<draft-aboba-radext-wlan-02.txt>
6 March 2006

Bernard Aboba
Microsoft

RADIUS Attributes for WLAN

Copyright Notice

Abstract

Although AAA support is optional within IEEE 802.11, it is expected that many IEEE 802.11 authenticators will function as AAA clients. This document proposes additional attributes for use by IEEE 802.11 authenticators. The attributes defined in this document are compatible with those used within Diameter EAP.

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, 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.

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

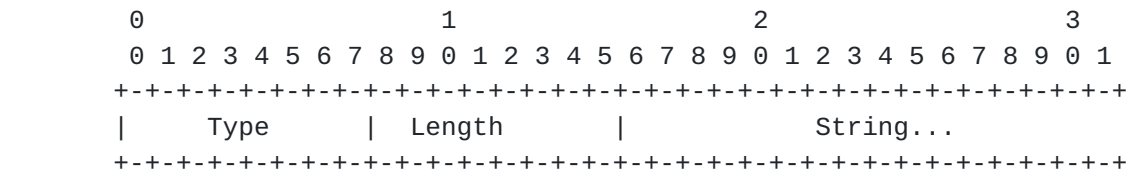
In this document, several words are used to signify the requirements of the specification. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. RADIUS Attributes

2.1. Allowed-SSID

Description

The Allowed-SSID attribute allows the RADIUS server to specify which SSIDs the user is allowed to access. One or more Allowed-SSID attributes MAY be included an Access-Accept or CoA-Request packet. This attribute is not allowed in other RADIUS packets. A summary of the Allowed-SSID Attribute format is shown below. The fields are transmitted from left to right.



Code

TBD

Length

>=3

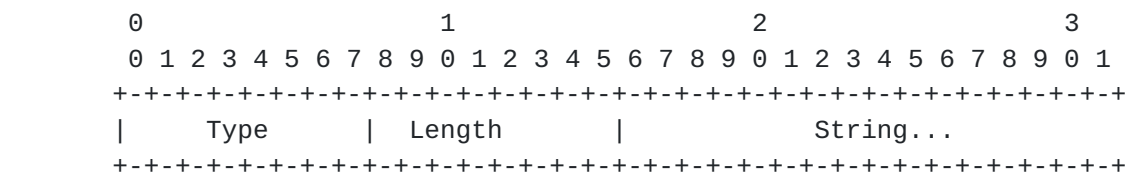
String

The String field contains one or more octets, encoding a single SSID, as defined in [IEEE-802.11]. If the SSID included in the Allowed-SSID attribute is not supported by the NAS, the attribute is silently discarded. UTF-8 encoded 10646 characters are recommended, but a robust implementation SHOULD support the field as undistinguished octets.

2.2. Allowed-Called-Station-ID

Description

The Allowed-Called-Station-ID attribute allows the RADIUS server to specify which Called-Station-IDs the user is allowed to access. More than one Allowed-Called-Station-ID attribute MAY be included in an Access-Accept or CoA-Request packet. This attribute is not allowed in other RADIUS packets. 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 terminated on. For details of the encoding, see [RFC2865] and [RFC3580]. Note that this attribute MUST NOT include the SSID. If the Called-Station-ID included in the Allowed-Called-Station-ID attribute does not describe a layer 2 endpoint of the NAS, the attribute is silently discarded. A robust implementation SHOULD support the field as undistinguished octets.

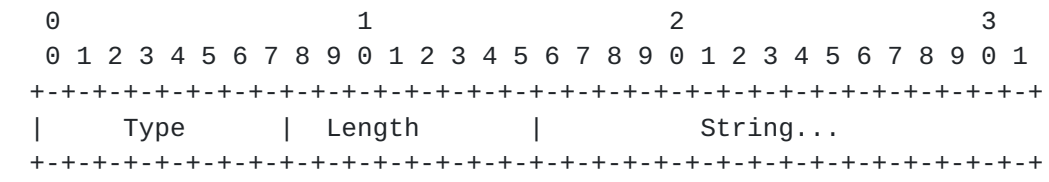
2.3. EAP-Key-Name

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 only 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 include this attribute in an Access-Accept or CoA-Request only if an EAP-Key-Name attribute was present in the Access-Request.

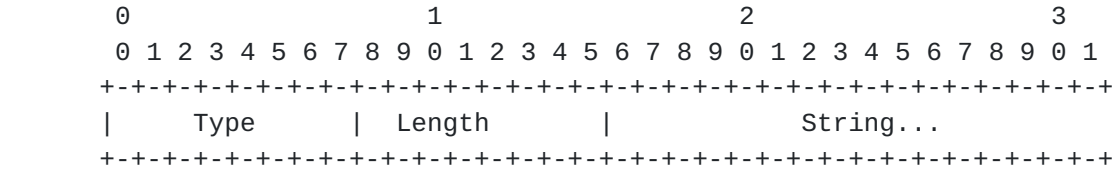
2.4. EAP-Peer-ID

Description

The EAP-Peer-ID Attribute contains an the 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 is only allowed in Access-Request and Access-Accept packets.

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 this attribute 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 the EAP Peer-ID exported by the EAP method. For details, see [KEYFRAME] Appendix A. A robust implementation SHOULD support the field as undistinguished octets.

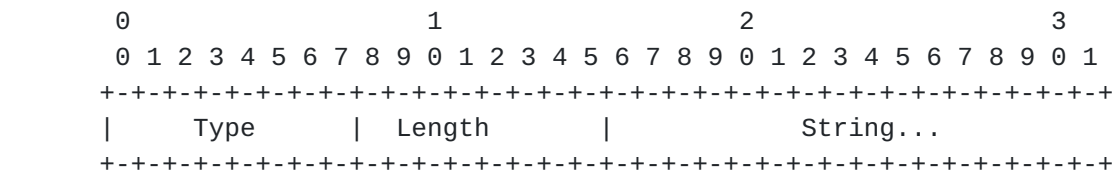
2.5. EAP-Server-ID

Description

The EAP-Server-ID Attribute contains the 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 and Access-Accept packets.

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

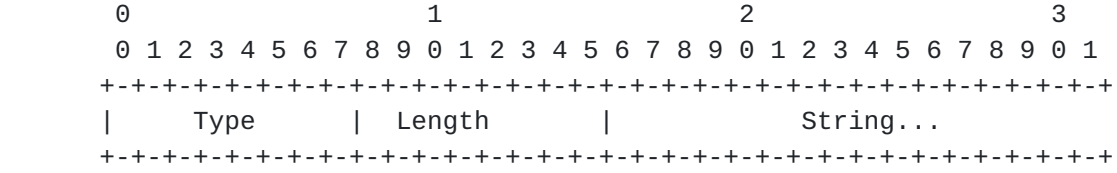
String

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.

2.6. 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.

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/Disconnect Req	#	Attribute
0	0+	0	0	0+	TBD	Allowed-SSID
0	0+	0	0	0+	TBD	Allowed-Called-Station-Id
0-1	0-1	0	0	0-1	102	EAP-Key-Name
0-1	0-1	0	0	0	TBD	EAP-Peer-ID
0-1	0-1	0	0	0	TBD	EAP-Server-ID
0-1	0	0	0	0	TBD	Mobility-Domain-ID

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 aready defined as a RADIUS attribute within Diameter EAP [RFC4072]. Diameter needs to define identical attributes with the same Type value for the Allowed-SSID, Allowed-Called-Station-ID, EAP-Peer-ID, EAP-Server-ID, and Mobility-Domain-ID. The Allowed-SSID, Allowed-Called-Station-ID, EAP-Peer-ID, EAP-Server-ID and Mobility-Domain-ID attributes should be available as part of the Diameter EAP application [RFC4072].

5. IANA Considerations

This specification requires assignment of a RADIUS attribute types for the following attributes:

Attribute	Type
Allowed-SSID	TBD
Allowed-Called-Station-Id	TBD
EAP-Peer-ID	TBD
EAP-Server-ID	TBD
Mobility-Domain-ID	TBD

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. 802.11-2003, 2003.

[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/D1.2, February 2006.

[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.

[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., Arkko, J., Eronen, P. and H. Levkowetz, "EAP Key Management Framework", draft-ietf-eap-keying-10.txt, March 2006.

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 Agere, and Ashwin Palekar of Microsoft.

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

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

Open issues

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

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