Internet Engineering Task Force (IETF)
Request for Comments: 7268
Updates: 3580, 4072
Category: Standards Track
ISSN: 2070-1721

B. Aboba
Microsoft Corporation
J. Malinen
Independent
P. Congdon
Tallac Networks
J. Salowey
Cisco Systems
M. Jones
Azuca Systems

July 2014

RADIUS Attributes for IEEE 802 Networks

Abstract

RFC 3580 provides guidelines for the use of the Remote Authentication Dial-In User Service (RADIUS) within IEEE 802 local area networks (LANs). This document defines additional attributes for use within IEEE 802 networks and clarifies the usage of the EAP-Key-Name Attribute and the Called-Station-Id Attribute. This document updates RFCs 3580 and 4072.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7268.

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] provides guidelines for the use of the Remote Authentication Dial-In 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 entity that requires 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 entity that provides an authentication service to an authenticator. This service verifies the claim of identity made by the Supplicant using the credentials provided 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
: 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

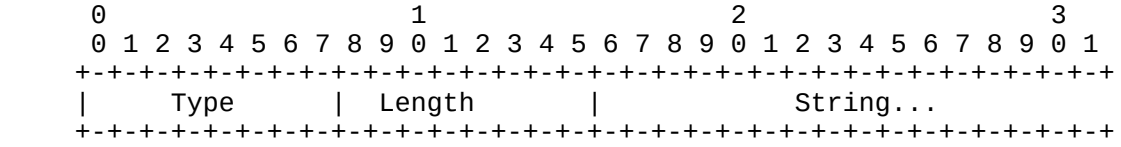
2.1. Allowed-Called-Station-Id

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, 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.



Type

174

Length

>=3

String

The String field is one or more octets, specifying a Called-Station-Id that the user MAY connect to; if the Called-Station-Id that the user connects to does not match one of the Allowed-Called-Station-Id Attributes, the Network Access Server (NAS) MUST NOT permit the user to access the network.

In the case of IEEE 802, the Allowed-Called-Station-Id Attribute is used to store the Medium Access Control (MAC) address, represented as an uppercase ASCII character string in Canonical format and with octet values separated by a "-", for 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 ":", for example, "00-10-A4-23-19-C0:AP1". Where no MAC address restriction is intended, the MAC address field MUST be omitted, but ":" and the network name field MUST be included, for example, ":AP1".

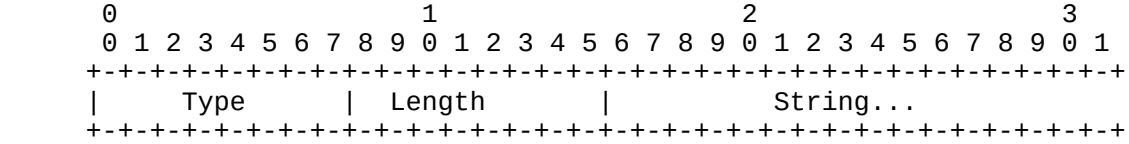
Within IEEE 802.11 [IEEE-802.11], the Service Set Identifier (SSID) constitutes the network name; within IEEE 802.1X [IEEE-802.1X] wired networks, the Network-Id Name (NID-Name) constitutes the network name. Since a NID-Name can be up to 253 octets in length, when used with [IEEE-802.1X] wired networks, there may not be sufficient room within the Allowed-Called-Station-Id Attribute to include both a MAC address and a network name. However, as the Allowed-Called-Station-Id Attribute is expected to be used largely in wireless access scenarios, this restriction is not considered serious.

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. 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.



Type

102 [RFC4072]

Length

>=3

String

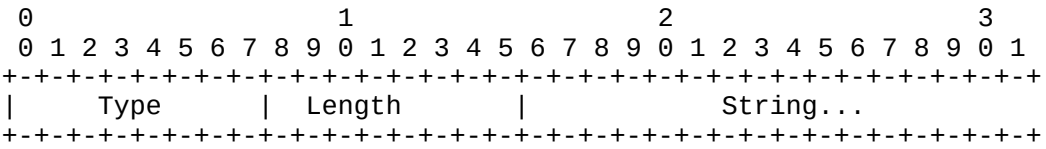
The String field is one or more octets, containing the EAP Session-Id, as defined in "Extensible Authentication Protocol (EAP) Key Management Framework" [RFC5247]. Since the NAS operates as a pass-through in EAP, it cannot know the EAP Session-Id before receiving it from the RADIUS server. As a result, 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 an 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. As noted in Section 6.2.2 of [IEEE-802.1X], the Connectivity Association Key Name (CKN) is derived from the EAP Session-Id, and, as described in Section 9.3.3 of [IEEE-802.1X], the CKN is subsequently used in the derivation of the Key Encrypting Key (KEK) and the Integrity Check Value Key (ICK), which protect the Secure Association Keys (SAKs) utilized by Media Access Control Security (MACsec). As a result, for the NAS to acquire information needed in the MACsec Key Agreement (MKA) exchange, it needs to include the EAP-Key-Name Attribute in the Access-Request and receive it from the RADIUS server in the Access-Accept.

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 with 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.



Type

175

Length

>=3

String

The String field is one or more octets, containing an EAP Peer-Id exported by the EAP method. For details, see Appendix A of [RFC5247]. A robust implementation SHOULD support the field as undistinguished octets. Only a single EAP Peer-Id may be included per attribute.

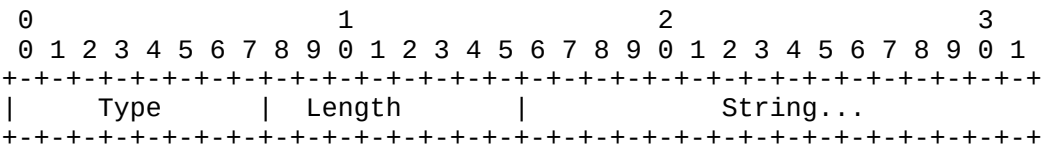
2.4. EAP-Server-Id

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 an Access-Request with 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 in 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.



Type

176

Length

>=3

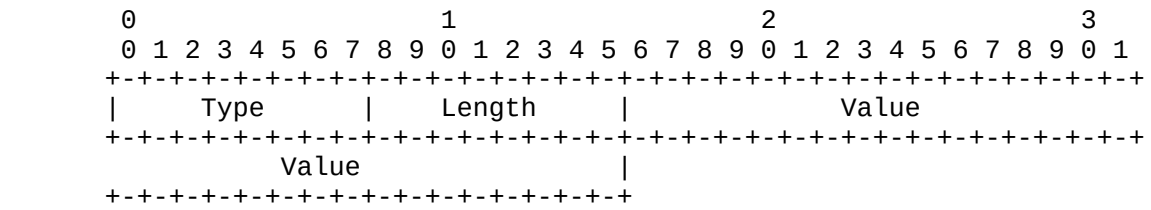
String

The String field is one or more octets, containing an EAP Server-Id exported by the EAP method. For details, see Appendix A of [RFC5247]. 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.



Type

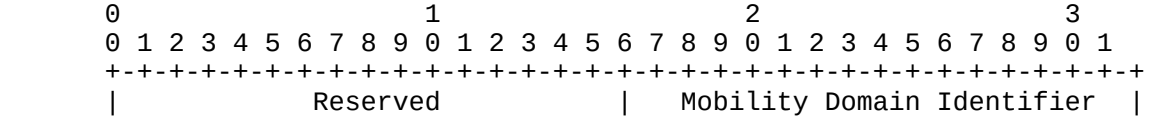
177

Length

6

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 Mobility Domain Identifier (MDID) defined in Section 8.4.2.49 of [IEEE-802.11].

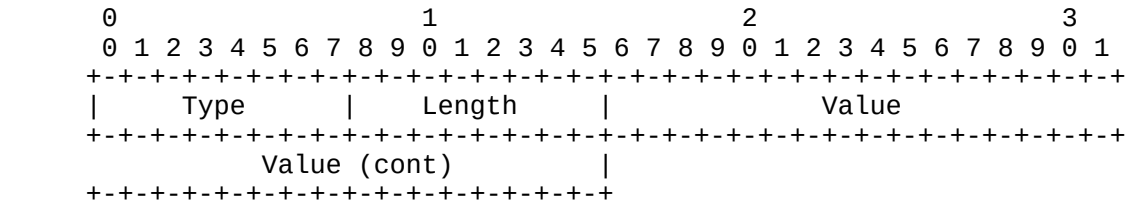


2.6. Preauth-Timeout

Description

This attribute sets the maximum number of seconds that 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 Pairwise Master Key (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.

A single Preauth-Timeout Attribute MAY be included within an Access-Accept or CoA-Request packet. A summary of the Preauth-Timeout Attribute format is shown below. The fields are transmitted from left to right.



Type

178

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

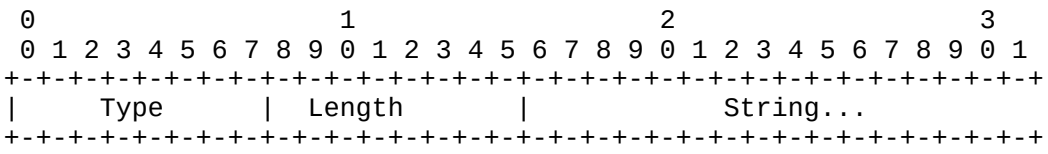
Description

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 MUST 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 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.



Type

179

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

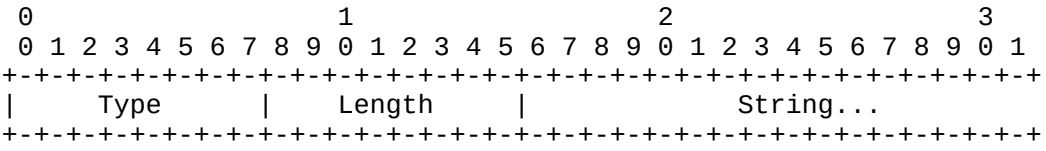
Description

The EAPoL-Announcement Attribute contains EAPoL-Announcement Type-Length-Value (TLV) tuples defined within Table 11-8 of IEEE-802.1X [IEEE-802.1X]. The acronym "EAPoL" stands for Extensible Authentication Protocol over Local Area Network.

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 packet, EAPoL-Announcement Attributes contain EAPoL-Announcement TLVs that the NAS is to send to the user in a unicast EAPoL-Announcement. When sent within an Accounting-Request packet, EAPoL-Announcement Attributes contain EAPoL-Announcement TLVs that the NAS has most recently sent to the user in a unicast EAPoL-Announcement.

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



Type

180

Length

>=3

String

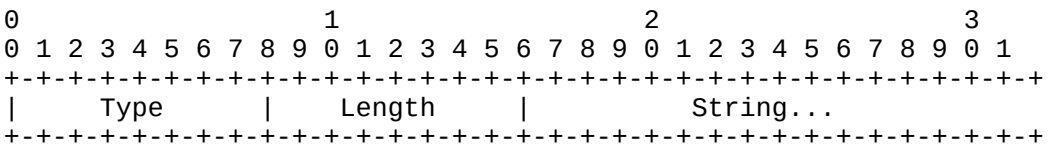
The String field is one or more octets, containing EAPoL-Announcement TLVs in the format defined in Figure 11-8 of Section 11.12 of [IEEE-802.1X]. Any EAPoL-Announcement TLV Type MAY be included within an EAPoL-Announcement Attribute, including Organizationally Specific TLVs. If multiple EAPoL-Announcement Attributes are present in a packet, their String fields MUST be concatenated before being parsed for EAPoL-Announcement TLVs; this allows EAPoL-Announcement TLVs longer than 253 octets to be transported by RADIUS. Similarly, EAPoL-Announcement TLVs larger than 253 octets MUST be fragmented between multiple EAPoL-Announcement Attributes.

2.9. WLAN-HESSID

Description

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 of [IEEE-802.11]. Zero or one WLAN-HESSID Attribute is permitted within an Access-Request or Accounting-Request packet.

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



Type

181

Length

19

String

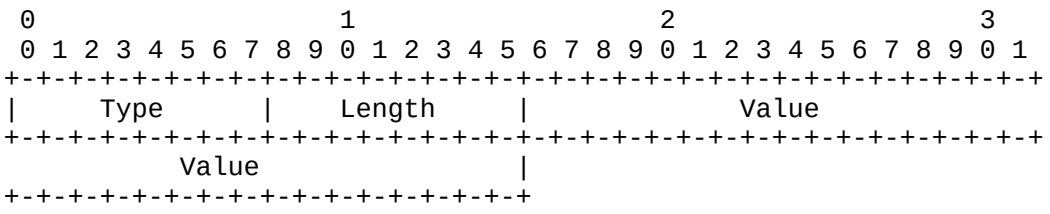
The String field is encoded in uppercase ASCII characters with the octet values separated by dash characters, as described in RFC 3580 [RFC3580], for example, "00-10-A4-23-19-C0".

2.10. WLAN-Venue-Info

Description

The WLAN-Venue-Info Attribute identifies the category of venue hosting the WLAN, as defined in Section 8.4.1.34 of [IEEE-802.11]. Zero or more WLAN-Venue-Info Attributes may be included in an Access-Request or Accounting-Request.

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



Type

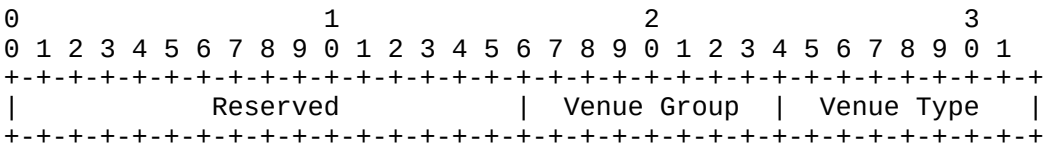
182

Length

6

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.



Venue Group

The Venue Group field is a single octet and describes the broad category of the venue, e.g., "Assembly". See Section 8.4.1.34 of [IEEE-802.11] for Venue Group codes and descriptions.

Venue Type

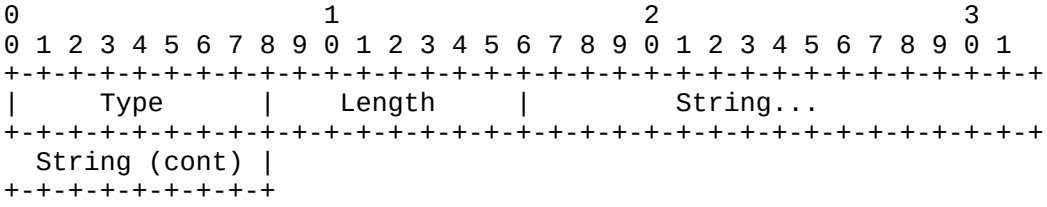
The Venue Type field is a single octet and describes the venue in a finer granularity within the Venue Group, e.g., "Library". See Section 8.4.1.34 of [IEEE-802.11] for Venue Type codes and descriptions.

2.11. WLAN-Venue-Language

Description

The WLAN-Venue-Language Attribute is a string encoded by ISO-14962-1997 [ISO-14962-1997] 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 or Accounting-Request, and each one indicates the language of the WLAN-Venue-Name Attribute that follows it.

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



Type

183

Length

4-5

String

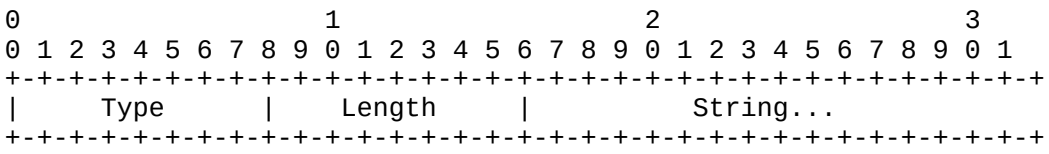
The String field is a two- or three-character language code selected from ISO-639 [ISO-639]. A two-character language code has a zero ("null" in ISO-14962-1997) appended to make it 3 octets in length.

2.12. WLAN-Venue-Name

Description

The WLAN-Venue-Name Attribute provides additional metadata on the Basic Service Set (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.



Type

184

Length

>=3

String

The String field is encoded in UTF-8 and contains the venue’s name. The maximum length of this field is 252 octets.

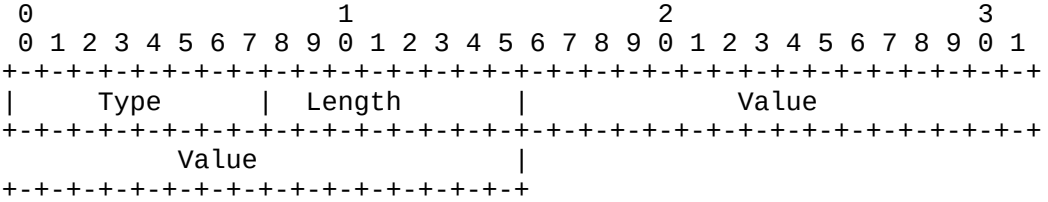
2.13. WLAN-Reason-Code

Description

The WLAN-Reason-Code Attribute contains information on the reason why a Station has been refused network access and has been disassociated or de-authenticated. This can occur due to policy or for reasons related to the user's subscription.

A WLAN-Reason-Code Attribute MAY be included within an Access-Reject or Disconnect-Request packet, as well as within an Accounting-Request packet. Upon receipt of an Access-Reject or Disconnect-Request packet containing a WLAN-Reason-Code Attribute, the WLAN-Reason-Code value is copied by the Access Point into the Reason Code field of a Disassociation or Deauthentication frame (see Clauses 8.3.3.4 and 8.3.3.12, respectively, in [IEEE-802.11]), which is subsequently transmitted to the Station.

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



Type

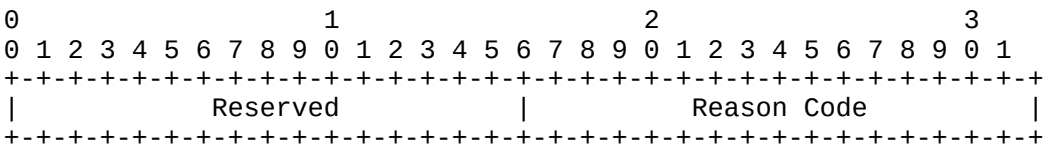
185

Length

6

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 Reason Code values defined in Table 8-36 of Section 8.4.1.7 of [IEEE-802.11].

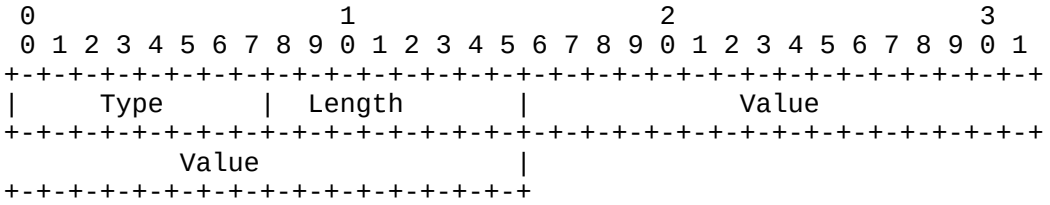


2.14. WLAN-Pairwise-Cipher

Description

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

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



Type

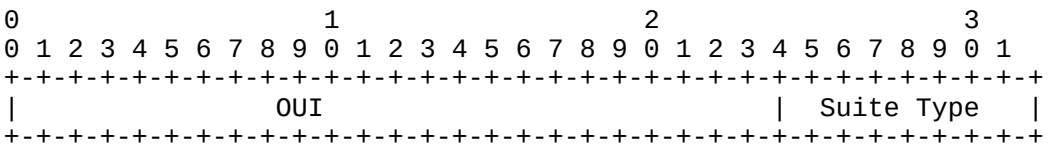
186

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.

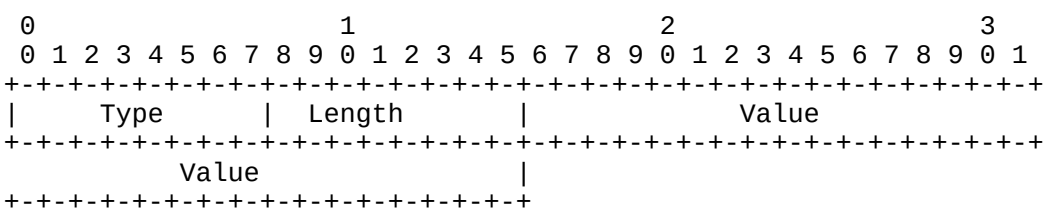


2.15. WLAN-Group-Cipher

Description

The WLAN-Group-Cipher Attribute contains information on the group ciphersuite 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.



Type

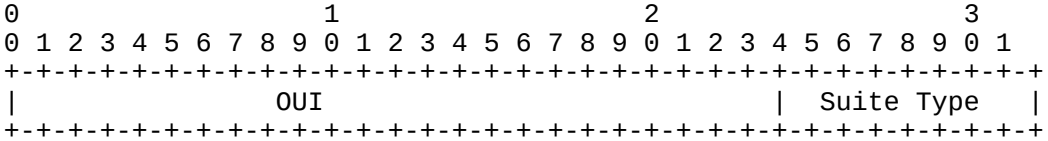
187

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.

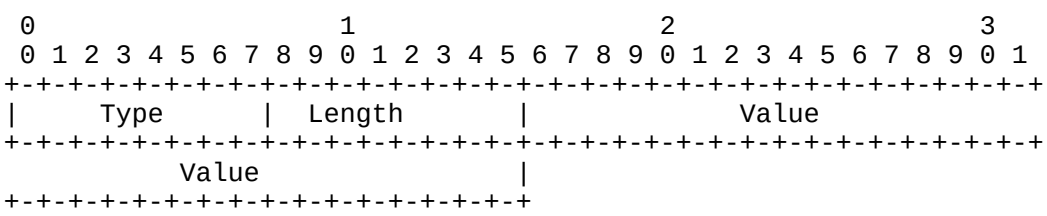


2.16. WLAN-AKM-Suite

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.



Type

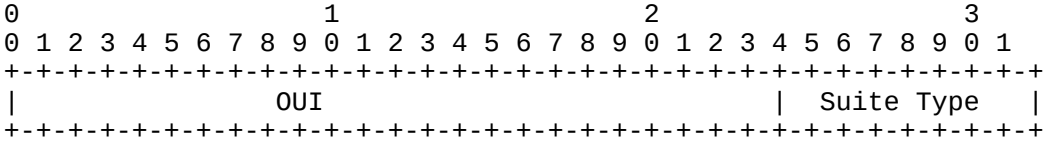
188

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:



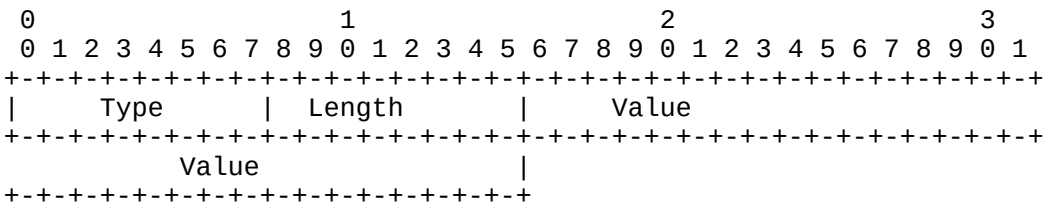
2.17. WLAN-Group-Mgmt-Cipher

Description

The WLAN-Group-Mgmt-Cipher Attribute contains information on the 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. The 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.



Type

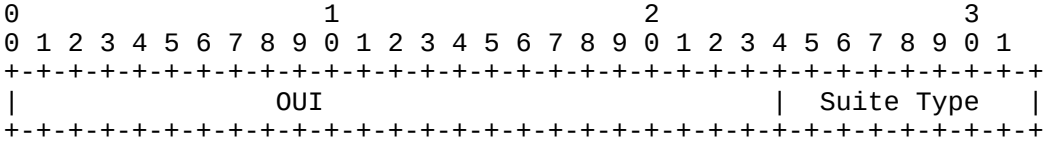
189

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:

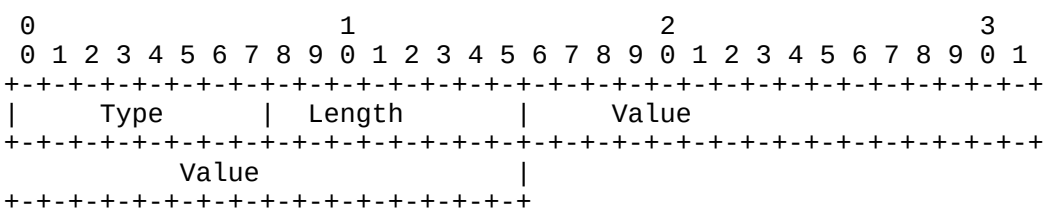


2.18. WLAN-RF-Band

Description

The WLAN-RF-Band Attribute contains information on the radio frequency (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.



Type

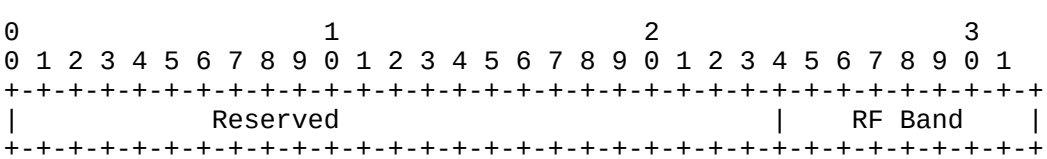
190

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 by the IEEE 802.11 Band ID field (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	174	Allowed-Called-Station-Id
0-1	0-1	0	0	102	EAP-Key-Name
0-1	0+	0	0	175	EAP-Peer-Id
0-1	0+	0	0	176	EAP-Server-Id
0-1	0	0	0	177	Mobility-Domain-Id
0-1	0-1	0	0	178	Preauth-Timeout
0-1	0	0	0	179	Network-Id-Name
0+	0+	0+	0+	180	EAPoL-Announcement
0-1	0	0	0	181	WLAN-HESSID
0-1	0	0	0	182	WLAN-Venue-Info
0+	0	0	0	183	WLAN-Venue-Language
0+	0	0	0	184	WLAN-Venue-Name
0	0	0-1	0	185	WLAN-Reason-Code
0-1	0	0	0	186	WLAN-Pairwise-Cipher
0-1	0	0	0	187	WLAN-Group-Cipher
0-1	0	0	0	188	WLAN-AKM-Suite
0-1	0	0	0	189	WLAN-Group-Mgmt-Cipher
0-1	0	0	0	190	WLAN-RF-Band

CoA-Req	Dis-Req	Acct-Req	#	Attribute
0+	0	0+	174	Allowed-Called-Station-Id
0-1	0	0	102	EAP-Key-Name
0	0	0+	175	EAP-Peer-Id
0	0	0+	176	EAP-Server-Id
0	0	0-1	177	Mobility-Domain-Id
0-1	0	0	178	Preauth-Timeout
0	0	0-1	179	Network-Id-Name
0+	0+	0+	180	EAPoL-Announcement
0	0	0-1	181	WLAN-HESSID
0	0	0-1	182	WLAN-Venue-Info
0	0	0+	183	WLAN-Venue-Language
0	0	0+	184	WLAN-Venue-Name
0	0-1	0-1	185	WLAN-Reason-Code
0	0	0-1	186	WLAN-Pairwise-Cipher
0	0	0-1	187	WLAN-Group-Cipher
0	0	0-1	188	WLAN-AKM-Suite
0	0	0-1	189	WLAN-Group-Mgmt-Cipher
0	0	0-1	190	WLAN-RF-Band

The following table defines 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>. Per this specification, RADIUS attribute types have been assigned for the following attributes:

Attribute	Type
Allowed-Called-Station-Id	174
EAP-Peer-Id	175
EAP-Server-Id	176
Mobility-Domain-Id	177
Preauth-Timeout	178
Network-Id-Name	179
EAPoL-Announcement	180
WLAN-HESSID	181
WLAN-Venue-Info	182
WLAN-Venue-Language	183
WLAN-Venue-Name	184
WLAN-Reason-Code	185
WLAN-Pairwise-Cipher	186
WLAN-Group-Cipher	187
WLAN-AKM-Suite	188
WLAN-Group-Mgmt-Cipher	189
WLAN-RF-Band	190

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]. In particular, when RADIUS traffic is sent in the clear, the attributes defined in this document can be obtained by an attacker

snooping the exchange between the RADIUS client and server. As a result, RADIUS confidentiality is desirable; for a review of RADIUS security and crypto-agility requirements, see [RFC6421].

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 ciphersuite 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, "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture. Amendment 2: Registration of Object Identifiers", ANSI/IEEE Std 802, 2001.

[IEEE-802.11] IEEE, "IEEE 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", IEEE Std 802.11-2012, 2012.

[IEEE-802.11ad]
IEEE, "IEEE 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 3: Enhancements for Very High Throughput in the 60 GHz Band", IEEE Std 802.11ad-2012, 2012.

[IEEE-802.1X]
IEEE, "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control", IEEE Std 802.1X-2010, February 2010.

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

[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", BCP 14, RFC 2119, March 1997.

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

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

[RFC5247] Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (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 (Remote Authentication Dial In User Service) 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, Ed., "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.

[RFC6421] Nelson, D., Ed., "Crypto-Agility Requirements for Remote Authentication Dial-In User Service (RADIUS)", RFC 6421, November 2011.

7. 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
US

EMail: bernard_aboba@hotmail.com

Jouni Malinen

EMail: j@w1.fi

Paul Congdon
Tallac Networks
6528 Lonetree Blvd.
Rocklin, CA 95765
US

Phone: +19167576350
EMail: paul.congdon@tallac.com

Joseph Salowey
Cisco Systems

EMail: jsalowey@cisco.com

Mark Jones
Azuca Systems

EMail: mark@azu.ca