The following text describes changes that need to be made to Annex D of 802.1X-2001 in order to align it with the latest IETF draft on 802.1X and RADIUS guidelines (draft-congdon-radius-8021x-17.txt). This document should be published as an informational RFC soon.

In the following sections, a description of the change is provided as well as instructions on how to update Annex D. New text extracted from the IETF draft is included in a different font (Courier New). This text may need further updates to align it with IEEE editor's conventions and references.

D.1 Introduction

There has been a minor expansion of the opening paragraph to include further discussion on stand-alone mode and generalization about AAA clients. Consider replacing the 1st paragraph with the following three paragraphs.

IEEE 802.1X [13] provides "network port authentication" for IEEE 802 media; including Ethernet, Token Ring and 802.11 wireless LANS.

IEEE 802.1X does not require use of a backend authentication server, and thus can be deployed with stand-alone switches or access points, as well as in centrally managed scenarios.

In situations where it is desirable to centrally manage authentication, authorization and accounting (AAA) for IEEE 802 networks, deployment of a backend authentication and accounting server is desirable. In such situations, it is expected that IEEE 802.1X Authenticators will function as AAA clients.

D.2.1 Acct-Terminate-Cause

A discussion periodic re-authentication was added just after the paragraph discussing the re-authentication failure (20) termination cause. Insert the following paragraphs before the paragraph discussing Admin Reset (6).

Within 802.11 [22], periodic re-authentication may be useful in preventing reuse of an initialization vector with a given key. Since successful re-authentication does not result in termination of the session, accounting packets are not sent as a result of re-authentication unless the status of the session changes. For example:

a. The session is terminated due to re-authentication failure. In this case the Reauthentication Failure (20) termination cause is used.
b. The authorizations are changed as a result of a successful re-authentication. In this case, the Service Unavailable (15) termination cause is used. For accounting purposes, the portion of the session after the authorization change is treated as a separate session.

D.2.2 Acct-Multi-Session-Id

Clarification updates in the second paragraph. Replace the second paragraph with the following paragraph.

```
Where supported by the Access Points, the Acct-Multi-Session-Id
attribute is used to link together the multiple related sessions of a
roaming Supplicant.  In such a situation, if the session context is
transferred between access points, accounting packets may be sent
without a corresponding authentication and authorization exchange.
However, in such a situation it is assumed that the Acct-Multi-Session-
Id is transferred between the Access Points as part of the Inter-Access
Point Protocol.
```

The word ‘required’ is replaced with ‘recommended’ in the first sentence of the 4th paragraph.

An additional paragraph on encoding the Acct-Muilt-Session-Id was added at the end. Add the following paragraph to the end of section D.2.2

```
Since the Acct-Multi-Session-Id is of type String as defined in [5],
for use with IEEE 802.1X, it is encoded as an ASCII string of Hex
digits.
```

D.3 RADIUS authentication

In the opening paragraph, additional references are made to new documents. These will need to be augmented in the reference section of 802.1X as well. Replace the first paragraph with the following paragraph:

```
The following attributes defined in [4]-[6], [20], [21, [23] appear
most relevant for use in IEEE 802.1X authentication
```

IPv6 references are added for all IPv4 references in the list. After each IPv4 attribute, add the equivalent IPv6 attribute. Specifically, add NAS-IPv6-Address to item b) and add Framed-IPv6-Route to item I)

Framed-Pool is missing from the list and should be inserted after NAS-Port-ID as item z). This will make the letter notation role to aa) I guess? This attribute should include the IPv6 variant as well.

D.3.3 NAS-IP-Address

Add NAS-IPv6-Address to the clause heading, and replace the paragraph with the following text:

```
For use with IEEE 802.1X, the NAS-IP-Address contains the IPv4 address
of the bridge or Access Point acting as an Authenticator, and the NAS-
IPv6-Address contains the IPv6 address. If the IEEE 802.1X
authenticator has more than one interface, it may be desirable to use a
```

loopback address for this purpose so that the Authenticator will still be reachable even if one of the interfaces were to fail.

D.3.14 Framed-Route

Add NAS-IPv6-Route to the clause heading, and replace the paragraph with the following text:

The Framed-Route and Framed-IPv6-Route attributes provide routes that are to be configured for the supplicant. These attributes are therefore only relevant for IEEE 802.1X Authenticators that act as layer 3 devices, and cannot be understood by a bridge or Access Point.

D.3.16 Session-Timeout

This section appears to have undergone a considerable re-write. The first sentence also appears to be one that was added by 802.1X and may remain if desired. The next two paragraphs should be replaced with the following text:

When sent along in an Access-Accept without a Termination-Action attribute or with a Termination-Action attribute set to Default, the Session-Timeout attribute specifies the maximum number of seconds of service provided prior to session termination.

When sent in an Access-Accept along with a Termination-Action value of RADIUS-Request, the Session-Timeout attribute specifies the maximum number of seconds of service provided prior to re-authentication. In this case, the Session-Timeout attribute is used to load the reAuthPeriod constant within the Reauthentication Timer state machine of 802.1X. When sent with a Termination-Action value of RADIUS-Request, a Session-Timeout value of zero indicates the desire to perform another authentication (possibly of a different type) immediately after the first authentication has successfully completed.

As described in [6], when sent in an Access-Challenge, this attribute represents the maximum number of seconds that an IEEE 802.1X authenticator should wait for an EAP-Response before retransmitting. In this case, the Session-Timeout attribute is used to load the suppTimeout constant within the Backend state machine of IEEE 802.1X.

D.3.17 Idle-Timeout

A very minor change in the first sentence to reference the RADIUS RFC has been added. Insert the following sentence at the beginning of the first paragraph and fix the reference appropriately:

The Idle-Timeout attribute is described in [4].

D.3.18 Terminate-Action

The second sentence has been re-written and additional information about how to terminate the session when a default value is specified has been added. Replace all of the text in this clause with the following paragraph:

This attribute indicates what action should be taken when the service is completed. The value RADIUS-Request(1) indicates that re-authentication should occur on expiration of the Session-Time. The value Default (0) indicates that the session should terminate.

D.3.19 Called-Station-Id

A description of a special case for 802.11 access points has been added. The text in 802.1X differs from the original IETF draft because 802.1X references IEEE Std 802 for a description of Canonical format. This part of the text should remain, and if possible the IETF draft should be updated before going to RFC. Replace the text in this clause with the following paragraph

For IEEE 802.1X authenticators, this attribute is used to store the bridge or Access Point MAC address, represented as an ASCII character string in Canonical format (see IEEE Std 802). For Example: "00-10-A4-23-19-C0". For 802.11 Access Points, the 802.11 SSID SHOULD be appended to the Access Point MAC address, separated from the MAC address with a ":". Example "00-10-A4-23-19-C0:AP1".

D.3.29 Framed-Pool

Add Framed-IPv6-Pool to the clause heading and update the paragraph as needed. Change “this” to “these”.

D.3.30

The second paragraph has been split in an example of how this can be used has been inserted. After the first sentence of the second paragraph add the following sentence and break the following text into another paragraph:

This can be used, for example, to allow a wireless host to remain on the same VLAN as it moves within a campus network.

Additional comment text has existed in the IETF draft for some time that was not included in 802.1X. This text describes encoding the VLAN id field as a string. Consider adding the following paragraph as the last paragraph in this clause:

Note that the VLANID is 12-bits, taking a value between 0 and 4095, inclusive. Since the Tunnel-Private-Group-ID is of type String as defined in [20], for use with IEEE 802.1X, the VLANID is encoded as a string, rather than an integer.

D.4 Security considerations

Further clarification about NOT encapsulation of EAP packets in Access-Challenge requests has been added to the 3rd paragraph in this clause. Add the following text to the end of the 3rd paragraph:

Neither message should be encapsulated in an Access-Challenge because as described in RFC 2284, EAP-Success and EAP-Failure messages are not ACK'd. Since an Access-Challenge indicates a continuing EAP conversation and no client response is expected to these messages, encapsulating these messages within an Access-Challenge would constitute a contradiction.

The last paragraph in this clause has been re-written to flow with the above inserted text. Replace the last paragraph with the following text:

To address the possible corner conditions and ensure that access decisions made by IEEE 802.1X Authenticators conform to the wishes of the RADIUS server, it is necessary for the Authenticator to make the decision solely based on the authentication result (Accept/Reject) and NOT based on the contents of the EAP packet encapsulated in one or more EAP-Message attributes, if one is present at all.

D.5 Table of attributes

A whole new section has been added which includes a table of all the RADIUS attributes may be seen in 802.1X exchanges. Include the following text and table as a new clause D.5

The following table provides a guide to which attributes may be sent and received as part of IEEE 802.1X authentication. L3 denotes attributes that will be understood only by Authenticators implementing Layer 3 capabilities. For each attribute, the reference provides the definitive information on usage.

802.1X	#	**Attribute**
X	1	User-Name [4]
	2	User-Password [4]
	3	CHAP-Password [4]
X	4	NAS-IP-Address [4]
X	5	NAS-Port [4]
X	6	Service-Type [4]
	7	Framed-Protocol [4]
	8	Framed-IP-Address [4]
	9	Framed-IP-Netmask [4]
L3	10	Framed-Routing [4]
X	11	Filter-Id [4]
X	12	Framed-MTU [4]
	13	Framed-Compression [4]
L3	14	Login-IP-Host [4]
L3	15	Login-Service [4]
L3	16	Login-TCP-Port [4]
X	18	Reply-Message [4]

	19	Callback-Number [4]
	20	Callback-Id [4]
L3	22	Framed-Route [4]
L3	23	Framed-IPX-Network [4]
X	24	State [4]
X	25	Class [4]
X	26	Vendor-Specific [4]
X	27	Session-Timeout [4]
X	28	Idle-Timeout [4]
X	29	Termination-Action [4]
X	30	Called-Station-Id [4]
X	31	Calling-Station-Id [4]
X	32	NAS-Identifier [4]
X	33	Proxy-State [4]
	34	Login-LAT-Service [4]
	35	Login-LAT-Node [4]
	36	Login-LAT-Group [4]
L3	37	Framed-AppleTalk-Link [4]
L3	38	Framed-AppleTalk-Network [4]
L3	39	Framed-AppleTalk-Zone [4]
X	40	Acct-Status-Type [5]
X	41	Acct-Delay-Time [5]
X	42	Acct-Input-Octets [5]
X	43	Acct-Output-Octets [5]
X	44	Acct-Session-Id [5]
X	45	Acct-Authentic [5]
X	46	Acct-Session-Time [5]
X	47	Acct-Input-Packets [5]
X	48	Acct-Output-Packets [5]
X	49	Acct-Terminate-Cause [5]
X	50	Acct-Multi-Session-Id [5]
	51	Acct-Link-Count [5]
X	52	Acct-Input-Gigawords [6]
X	53	Acct-Output-Gigawords [6]
X	55	Event-Timestamp [6]
	60	CHAP-Challenge [4]
X	61	NAS-Port-Type [4]
	62	Port-Limit [4]
	63	Login-LAT-Port [4]
X	64	Tunnel-Type [20]
X	65	Tunnel-Medium-Type [20]
L3	66	Tunnel-Client-Endpoint [20]
L3	67	Tunnel-Server-Endpoint [20]
L3	68	Acct-Tunnel-Connection [21]
L3	69	Tunnel-Password [20]
	70	ARAP-Password [6]
	71	ARAP-Features [6]
	72	ARAP-Zone-Access [6]
	73	ARAP-Security [6]
	74	ARAP-Security-Data [6]
	75	Password-Retry [6]
	76	Prompt [6]
X	77	Connect-Info [6]
X	78	Configuration-Token [6]

X	79	EAP-Message [6]
X	80	Message-Authenticator [6]
X	81	Tunnel-Private-Group-ID [20]
L3	82	Tunnel-Assignment-ID [20]
X	83	Tunnel-Preference [20]
	84	ARAP-Challenge-Response [6]
X	85	Acct-Interim-Interval [6]
X	86	Acct-Tunnel-Packets-Lost [21]
X	87	NAS-Port-Id [6]
	88	Framed-Pool [6]
L3	90	Tunnel-Client-Auth-ID [20]
L3	91	Tunnel-Server-Auth-ID [20]
X	95	NAS-IPv6-Address [23]
	96	Framed-Interface-Id [23]
L3	97	Framed-IPv6-Prefix [23]
L3	98	Login-IPv6-Host [23]
L3	99	Framed-IPv6-Route [23]
L3	100	Framed-IPv6-Pool [23]

```
Key
===
802.1X    = May be used with IEEE 802.1X authentication
L3        = Implemented only by Authenticators with Layer 3
            capabilities
```

Other Stuff

Another reference was added to the IETF draft. It is related to the new IPv6 attributes included above. Consider adding to 802.1X the following reference:

[23] Aboba, B., Zorn, G., Mitton, D.,"RADIUS and IPv6", RFC 3162, August 2001.