

Network Working Group
Request for Comments: 3580
Category: Informational

P. Congdon
Hewlett Packard Company
B. Aboba
Microsoft
A. Smith
Trapeze Networks
G. Zorn
Cisco Systems
J. Roese
Enterasys
September 2003

IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)
Usage Guidelines

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This document provides suggestions on Remote Authentication Dial In User Service (RADIUS) usage by IEEE 802.1X Authenticators. The material in this document is also included within a non-normative Appendix within the IEEE 802.1X specification, and is being presented as an IETF RFC for informational purposes.

Table of Contents

1.	Introduction	3
1.1.	Terminology.	3
1.2.	Requirements Language.	4
2.	RADIUS Accounting Attributes	5
2.1.	Acct-Terminate-Cause	5
2.2.	Acct-Multi-Session-Id.	6
2.3.	Acct-Link-Count.	7
3.	RADIUS Authentication.	7
3.1.	User-Name.	8
3.2.	User-Password, CHAP-Password, CHAP-Challenge	8
3.3.	NAS-IP-Address, NAS-IPv6-Address	8
3.4.	NAS-Port	8
3.5.	Service-Type	8
3.6.	Framed-Protocol.	9
3.7.	Framed-IP-Address, Framed-IP-Netmask	9
3.8.	Framed-Routing	9
3.9.	Filter-ID.	9
3.10.	Framed-MTU	9
3.11.	Framed-Compression	10
3.12.	Displayable Messages	10
3.13.	Callback-Number, Callback-ID	10
3.14.	Framed-Route, Framed-IPv6-Route.	11
3.15.	State, Class, Proxy-State.	11
3.16.	Vendor-Specific.	11
3.17.	Session-Timeout.	11
3.18.	Idle-Timeout	12
3.19.	Termination-Action	12
3.20.	Called-Station-Id.	12
3.21.	Calling-Station-Id	12
3.22.	NAS-Identifier	12
3.23.	NAS-Port-Type.	12
3.24.	Port-Limit	13
3.25.	Password-Retry	13
3.26.	Connect-Info	13
3.27.	EAP-Message.	13
3.28.	Message-Authenticator.	13
3.29.	NAS-Port-Id.	13
3.30.	Framed-Pool, Framed-IPv6-Pool.	14
3.31.	Tunnel Attributes.	14
4.	RC4 EAPOL-Key Descriptor	15
5.	Security Considerations.	18
5.1.	Packet Modification or Forgery	18
5.2.	Dictionary Attacks	19
5.3.	Known Plaintext Attacks.	19
5.4.	Replay	20
5.5.	Outcome Mismatches	20

5.6.	802.11 Integration	20
5.7.	Key Management Issues.	21
6.	IANA Considerations.	22
7.	References	22
7.1.	Normative References	22
7.2.	Informative References	23
8.	Table of Attributes.	25
9.	Intellectual Property Statement	28
10.	Acknowledgements	28
11.	Authors' Addresses	29
12.	Full Copyright Statement	30

1. Introduction

IEEE 802.1X enables authenticated access to IEEE 802 media, including Ethernet, Token Ring, and 802.11 wireless LANs. Although Remote Authentication Dial In User Service (RADIUS) support is optional within IEEE 802.1X, it is expected that many IEEE 802.1X Authenticators will function as RADIUS clients.

IEEE 802.1X [IEEE8021X] provides "network port authentication" for IEEE 802 [IEEE802] media, including Ethernet [IEEE8023], Token Ring and 802.11 [IEEE80211] wireless LANs.

IEEE 802.1X does not require use of a backend Authentication Server, and thus can be deployed with stand-alone bridges 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.

This document provides suggestions on RADIUS usage by IEEE 802.1X Authenticators. Support for any AAA protocol is optional for IEEE 802.1X Authenticators, and therefore this specification has been incorporated into a non-normative Appendix within the IEEE 802.1X specification.

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 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 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.

Port Access Entity (PAE)

The protocol entity associated with a physical or virtual (802.11) Port. A given PAE may support the protocol functionality associated with the Authenticator, Supplicant or both.

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. These words are often capitalized. 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 Accounting Attributes

With a few exceptions, the RADIUS accounting attributes defined in [RFC2866], [RFC2867], and [RFC2869] have the same meaning within IEEE 802.1X sessions as they do in dialup sessions and therefore no additional commentary is needed.

Attributes requiring more discussion include:

Acct-Terminate-Cause
Acct-Multi-Session-Id
Acct-Link-Count

2.1. Acct-Terminate-Cause

This attribute indicates how the session was terminated, as described in [RFC2866]. [IEEE8021X] defines the following termination cause values, which are shown with their RADIUS equivalents in the table on the next page.

IEEE 802.1X dot1xAuthSessionTerminateCause Value	RADIUS Acct-Terminate-Cause Value
-----	-----
SupplicantLogoff(1)	User Request (1)
portFailure(2)	Lost Carrier (2)
SupplicantRestart(3)	Supplicant Restart (19)
reauthFailed(4)	Reauthentication Failure (20)
authControlForceUnauth(5)	Admin Reset (6)
portReInit(6)	Port Reinitialized (21)
portAdminDisabled(7)	Port Administratively Disabled (22)
notTerminatedYet(999)	N/A

When using this attribute, the User Request (1) termination cause corresponds to the situation in which the session terminated due to an EAPOL-Logoff received from the Supplicant. When a session is moved due to roaming, the EAPOL state machines will treat this as a Supplicant Logoff.

A Lost Carrier (2) termination cause indicates session termination due to loss of physical connectivity for reasons other than roaming between Access Points. For example, if the Supplicant disconnects a point-to-point LAN connection, or moves out of range of an Access Point, this termination cause is used. Lost Carrier (2) therefore equates to a Port Disabled condition in the EAPOL state machines.

A Supplicant Restart (19) termination cause indicates re-initialization of the Supplicant state machines.

A Reauthentication Failure (20) termination cause indicates that a previously authenticated Supplicant has failed to re-authenticate successfully following expiry of the re-authentication timer or explicit re-authentication request by management action.

Within [IEEE80211], 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.

Where IEEE 802.1X authentication occurs prior to association, accounting packets are not sent until an association occurs.

An Admin Reset (6) termination cause indicates that the Port has been administratively forced into the unauthorized state.

A Port Reinitialized (21) termination cause indicates that the Port's MAC has been reinitialized.

A Port Administratively Disabled (22) termination cause indicates that the Port has been administratively disabled.

2.2. Acct-Multi-Session-Id

The purpose of this attribute is to make it possible to link together multiple related sessions. While [IEEE8021X] does not act on aggregated ports, it is possible for a Supplicant roaming between Access Points to cause multiple RADIUS accounting packets to be sent by different Access Points.

Where supported by the Access Points, the Acct-Multi-Session-Id attribute can be 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,

provided that Association has occurred. 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 (IAPP).

If the Acct-Multi-Session-Id were not unique between Access Points, then it is possible that the chosen Acct-Multi-Session-Id will overlap with an existing value allocated on that Access Point, and the Accounting Server would therefore be unable to distinguish a roaming session from a multi-link session.

As a result, the Acct-Multi-Session-Id attribute is unique among all the bridges or Access Points, SupPLICants and sessions. In order to provide this uniqueness, it is suggested that the Acct-Multi-Session-Id be of the form:

Original AP MAC Address | SupPLICant MAC Address | NTP Timestamp

Here "|" represents concatenation, the original AP MAC Address is the MAC address of the bridge or Access Point at which the session started, and the 64-bit NTP timestamp indicates the beginning of the original session. In order to provide for consistency of the Acct-Multi-Session-Id between roaming sessions, the Acct-Multi-Session-Id may be moved between Access Points as part of IAPP or another handoff scheme.

The use of an Acct-Multi-Session-Id of this form guarantees uniqueness among all Access Points, SupPLICants and sessions. Since the NTP timestamp does not wrap on reboot, there is no possibility that a rebooted Access Point could choose an Acct-Multi-Session-Id that could be confused with that of a previous session.

Since the Acct-Multi-Session-Id is of type String as defined in [RFC2866], for use with IEEE 802.1X, it is encoded as an ASCII string of Hex digits. Example: "00-10-A4-23-19-C0-00-12-B2-14-23-DE-AF-23-83-C0-76-B8-44-E8"

2.3. Acct-Link-Count

The Acct-Link-Count attribute may be used to account for the number of ports that have been aggregated.

3. RADIUS Authentication

This section describes how attributes defined in [RFC2865], [RFC2867], [RFC2868], [RFC2869], [RFC3162] and [RFC3579] are used in IEEE 802.1X authentication.

3.1. User-Name

In IEEE 802.1X, the Supplicant typically provides its identity via an EAP-Response/Identity message. Where available, the Supplicant identity is included in the User-Name attribute, and included in the RADIUS Access-Request and Access-Reply messages as specified in [RFC2865] and [RFC3579].

Alternatively, as discussed in [RFC3579] Section 2.1., the User-Name attribute may contain the Calling-Station-ID value, which is set to the Supplicant MAC address.

3.2. User-Password, CHAP-Password, CHAP-Challenge

Since IEEE 802.1X does not support PAP or CHAP authentication, the User-Password, CHAP-Password or CHAP-Challenge attributes are not used by IEEE 802.1X Authenticators acting as RADIUS clients.

3.3. NAS-IP-Address, NAS-IPv6-Address

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.

3.4. NAS-Port

For use with IEEE 802.1X the NAS-Port will contain the port number of the bridge, if this is available. While an Access Point does not have physical ports, a unique "association ID" is assigned to every mobile Station upon a successful association exchange. As a result, for an Access Point, if the association exchange has been completed prior to authentication, the NAS-Port attribute will contain the association ID, which is a 16-bit unsigned integer. Where IEEE 802.1X authentication occurs prior to association, a unique NAS-Port value may not be available.

3.5. Service-Type

For use with IEEE 802.1X, the Framed (2), Authenticate Only (8), and Call Check (10) values are most commonly used.

A Service-Type of Framed indicates that appropriate 802 framing should be used for the connection. A Service-Type of Authenticate Only (8) indicates that no authorization information needs to be returned in the Access-Accept. As described in [RFC2865], a

Service-Type of Call Check is included in an Access-Request packet to request that the RADIUS server accept or reject the connection attempt, typically based on the Called-Station-ID (set to the bridge or Access Point MAC address) or Calling-Station-ID attributes (set to the Supplicant MAC address). As noted in [RFC2865], it is recommended that in this case, the User-Name attribute be given the value of Calling-Station-Id.

3.6. Framed-Protocol

Since there is no value for IEEE 802 media, the Framed-Protocol attribute is not used by IEEE 802.1X Authenticators.

3.7. Framed-IP-Address, Framed-IP-Netmask

IEEE 802.1X does not provide a mechanism for IP address assignment. Therefore the Framed-IP-Address and Framed-IP-Netmask attributes can only be used by IEEE 802.1X Authenticators that support IP address assignment mechanisms. Typically this capability is supported by layer 3 devices.

3.8. Framed-Routing

The Framed-Routing attribute indicates the routing method for the Supplicant. It is therefore only relevant for IEEE 802.1X Authenticators that act as layer 3 devices, and cannot be used by a bridge or Access Point.

3.9. Filter-ID

This attribute indicates the name of the filter list to be applied to the Supplicant's session. For use with an IEEE 802.1X Authenticator, it may be used to indicate either layer 2 or layer 3 filters. Layer 3 filters are typically only supported on IEEE 802.1X Authenticators that act as layer 3 devices.

3.10. Framed-MTU

This attribute indicates the maximum size of an IP packet that may be transmitted over the wire between the Supplicant and the Authenticator. IEEE 802.1X Authenticators set this to the value corresponding to the relevant 802 medium, and include it in the RADIUS Access-Request. The RADIUS server may send an EAP packet as large as Framed-MTU minus four (4) octets, taking into account the additional overhead for the IEEE 802.1X Version (1), Type (1) and Body Length (2) fields. For EAP over IEEE 802 media, the Framed-MTU values (which do not include LLC/SNAP overhead) and maximum frame length values (not including the preamble) are as follows:

Media	Framed-MTU	Maximum Frame Length
=====	=====	=====
Ethernet	1500	1522
802.3	1500	1522
802.4	8174	8193
802.5 (4 Mbps)	4528	4550
802.5 (16 Mbps)	18173	18200
802.5 (100 Mb/s)	18173	18200
802.6	9191	9240
802.9a	1500	1518
802.11	2304	2346
802.12 (Ethernet)	1500	1518
802.12 (Token Ring)	4502	4528
FDDI	4479	4500

NOTE - the Framed-MTU size for IEEE 802.11 media may change as a result of ongoing work being undertaken in the IEEE 802.11 Working Group. Since some 802.11 stations cannot handle an MTU larger than 1500 octets, it is recommended that RADIUS servers encountering a NAS-Port-Type value of 802.11 send EAP packets no larger than 1496 octets.

3.11. Framed-Compression

[IEEE8021X] does not include compression support. Therefore this attribute is not understood by [IEEE8021X] Authenticators.

3.12. Displayable Messages

The Reply-Message attribute, defined in section 5.18 of [RFC2865], indicates text which may be displayed to the user. This is similar in concept to the EAP Notification Type, defined in [RFC2284]. As noted in [RFC3579], Section 2.6.5, when sending a displayable message to an [IEEE8021X] Authenticator, displayable messages are best sent within EAP-Message/EAP-Request/Notification attribute(s), and not within Reply-Message attribute(s).

3.13. Callback-Number, Callback-ID

These attributes are not understood by IEEE 802.1X Authenticators.

3.14. Framed-Route, Framed-IPv6-Route

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.

3.15. State, Class, Proxy-State

These attributes are used for the same purposes as described in [RFC2865].

3.16. Vendor-Specific

Vendor-specific attributes are used for the same purposes as described in [RFC2865]. The MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes, described in section 2.4 of [RFC2548], MAY be used to encrypt and authenticate the RC4 EAPOL-Key descriptor [IEEE8021X, Section 7.6]. Examples of the derivation of the MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes from the master key negotiated by an EAP method are given in [RFC2716]. Details of the EAPOL-Key descriptor are provided in Section 4.

3.17. Session-Timeout

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.

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.

3.18. Idle-Timeout

The Idle-Timeout attribute is described in [RFC2865]. For IEEE 802 media other than 802.11 the media are always on. As a result the Idle-Timeout attribute is typically only used with wireless media such as IEEE 802.11. It is possible for a wireless device to wander out of range of all Access Points. In this case, the Idle-Timeout attribute indicates the maximum time that a wireless device may remain idle.

3.19. Termination-Action

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.

3.20. Called-Station-Id

For IEEE 802.1X Authenticators, this 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 the SSID is known, it SHOULD be appended to the Access Point MAC address, separated from the MAC address with a ":". Example "00-10-A4-23-19-C0:AP1".

3.21. Calling-Station-Id

For IEEE 802.1X Authenticators, this attribute is used to store the Supplicant MAC address in ASCII format (upper case only), with octet values separated by a "-". Example: "00-10-A4-23-19-C0".

3.22. NAS-Identifier

This attribute contains a string identifying the IEEE 802.1X Authenticator originating the Access-Request.

3.23. NAS-Port-Type

For use with IEEE 802.1X, NAS-Port-Type values of Ethernet (15) Wireless - IEEE 802.11 (19), Token Ring (20) and FDDI (21) may be used.

3.24. Port-Limit

This attribute has no meaning when sent to an [IEEE8021X] Authenticator.

3.25. Password-Retry

In IEEE 802.1X, the Authenticator always transitions to the HELD state after an authentication failure. Thus this attribute does not make sense for IEEE 802.1X.

3.26. Connect-Info

This attribute is sent by a bridge or Access Point to indicate the nature of the Supplicant's connection. When sent in the Access-Request it is recommended that this attribute contain information on the speed of the Supplicant's connection. For 802.11, the following format is recommended: "CONNECT 11Mbps 802.11b". If sent in the Accounting STOP, this attribute may be used to summarize statistics relating to session quality. For example, in IEEE 802.11, the Connect-Info attribute may contain information on the number of link layer retransmissions. The exact format of this attribute is implementation specific.

3.27. EAP-Message

Since IEEE 802.1X provides for encapsulation of EAP as described in [RFC2284] and [IEEE8021X], the EAP-Message attribute defined in [RFC3579] is used to encapsulate EAP packets for transmission from the IEEE 802.1X Authenticator to the Authentication Server. [RFC3579] Section 2.2. describes how the Authentication Server handles invalid EAP packets passed to it by the Authenticator.

3.28. Message-Authenticator

As noted in [RFC3579] Section 3.1., the Message-Authenticator attribute MUST be used to protect packets within a RADIUS/EAP conversation.

3.29. NAS-Port-Id

This attribute is used to identify the IEEE 802.1X Authenticator port which authenticates the Supplicant. The NAS-Port-Id differs from the NAS-Port in that it is a string of variable length whereas the NAS-Port is a 4 octet value.

3.30. Framed-Pool, Framed-IPv6-Pool

IEEE 802.1X does not provide a mechanism for IP address assignment. Therefore the Framed-Pool and Framed-IPv6-Pool attributes can only be used by IEEE 802.1X Authenticators that support IP address assignment mechanisms. Typically this capability is supported by layer 3 devices.

3.31. Tunnel Attributes

Reference [RFC2868] defines RADIUS tunnel attributes used for authentication and authorization, and [RFC2867] defines tunnel attributes used for accounting. Where the IEEE 802.1X Authenticator supports tunneling, a compulsory tunnel may be set up for the Supplicant as a result of the authentication.

In particular, it may be desirable to allow a port to be placed into a particular Virtual LAN (VLAN), defined in [IEEE8021Q], based on the result of the authentication. This can be used, for example, to allow a wireless host to remain on the same VLAN as it moves within a campus network.

The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept. However, the IEEE 802.1X Authenticator may also provide a hint as to the VLAN to be assigned to the Supplicant by including Tunnel attributes within the Access-Request.

For use in VLAN assignment, the following tunnel attributes are used:

```
Tunnel-Type=VLAN (13)
Tunnel-Medium-Type=802
Tunnel-Private-Group-ID=VLANID
```

Note that the VLANID is 12-bits, taking a value between 1 and 4094, inclusive. Since the Tunnel-Private-Group-ID is of type String as defined in [RFC2868], for use with IEEE 802.1X, the VLANID integer value is encoded as a string.

When Tunnel attributes are sent, it is necessary to fill in the Tag field. As noted in [RFC2868], section 3.1:

The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. Valid values for this field are 0x01 through 0x1F, inclusive. If the Tag field is unused, it MUST be zero (0x00).

For use with Tunnel-Client-Endpoint, Tunnel-Server-Endpoint, Tunnel-Private-Group-ID, Tunnel-Assignment-ID, Tunnel-Client-Auth-ID or Tunnel-Server-Auth-ID attributes (but not Tunnel-Type, Tunnel-Medium-Type, Tunnel-Password, or Tunnel-Preference), a tag field of greater than 0x1F is interpreted as the first octet of the following field.

Unless alternative tunnel types are provided, (e.g. for IEEE 802.1X Authenticators that may support tunneling but not VLANs), it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLANID, the tag field SHOULD be set to zero (0x00) in all tunnel attributes. Where alternative tunnel types are to be provided, tag values between 0x01 and 0x1F SHOULD be chosen.

4. RC4 EAPOL-Key Frame

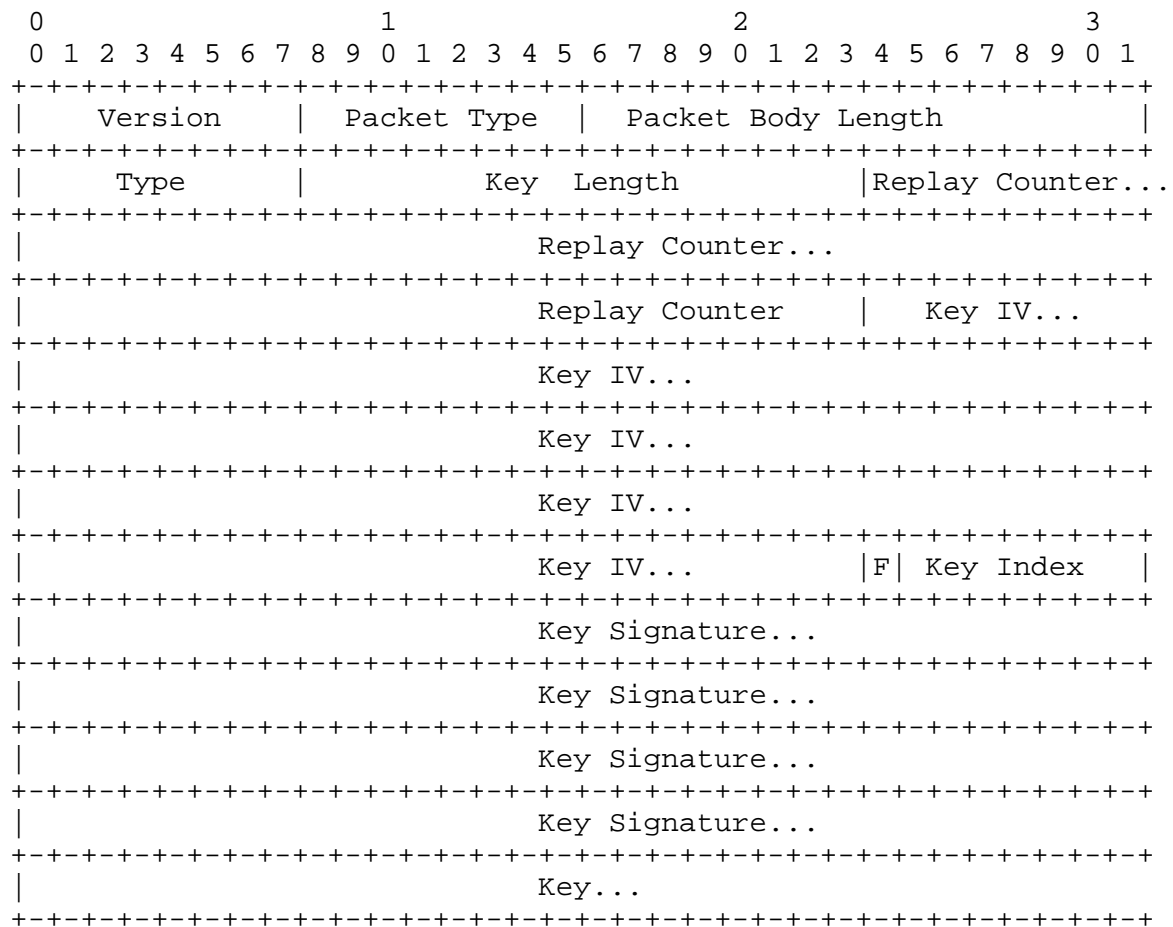
The RC4 EAPOL-Key frame is created and transmitted by the Authenticator in order to provide media specific key information. For example, within 802.11 the RC4 EAPOL-Key frame can be used to distribute multicast/broadcast ("default") keys, or unicast ("key mapping") keys. The "default" key is the same for all Stations within a broadcast domain.

The RC4 EAPOL-Key frame is not acknowledged and therefore the Authenticator does not know whether the Supplicant has received it. If it is lost, then the Supplicant and Authenticator will not have the same keying material, and communication will fail. If this occurs, the problem is typically addressed by re-running the authentication.

The RC4 EAPOL-Key frame is sent from the Authenticator to the Supplicant in order to provision the "default" key, and subsequently in order to refresh the "default" key. It may also be used to refresh the key-mapping key. Rekey is typically only required with weak ciphersuites such as WEP, defined in [IEEE80211].

Where keys are required, an EAP method that derives keys is typically selected. Therefore the initial "key mapping" keys can be derived from EAP keying material, without requiring the Authenticator to send an RC4 EAPOL-Key frame to the Supplicant. An example of how EAP keying material can be derived and used is presented in [RFC2716].

While the RC4 EAPOL-Key frame is defined in [IEEE8021X], a more complete description is provided on the next page.



Version

The Version field is one octet. For IEEE 802.1X, it contains the value 0x01.

Packet Type

The Packet Type field is one octet, and determines the type of packet being transmitted. For an EAPOL-Key Descriptor, the Packet Type field contains 0x03.

Packet Body Length

The Packet Body Length is two octets, and contains the length of the EAPOL-Key descriptor in octets, not including the Version, Packet Type and Packet Body Length fields.

Type

The Type field is a single octet. The Key descriptor is defined differently for each Type; this specification documents only the RC4 Key Descriptor (Type = 0x01).

Key Length

The Key Length field is two octets. If Packet Body Length = 44 + Key Length, then the Key Field contains the key in encrypted form, of length Key Length. This is 5 octets (40 bits) for WEP, and 13 octets (104 bits) for WEP-128. If Packet Body Length = 44, then the Key field is absent, and Key Length represents the number of least significant octets from the MS-MPPE-Send-Key attribute [RFC2548] to be used as the keying material. Note that the MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes are defined from the point of view of the Authenticator. From the Supplicant point of reference, the terms are reversed. Thus the MS-MPPE-Recv-Key on the Supplicant corresponds to the MS-MPPE-Send-Key on the Authenticator, and the MS-MPPE-Send-Key on the Supplicant corresponds to the MS-MPPE-Recv-Key on the Authenticator.

Replay Counter

The Replay Counter field is 8 octets. It does not repeat within the life of the keying material used to encrypt the Key field and compute the Key Signature field. A 64-bit NTP timestamp MAY be used as the Replay Counter.

Key IV

The Key IV field is 16 octets and includes a 128-bit cryptographically random number.

F

The Key flag (F) is a single bit, describing the type of key that is included in the Key field. Values are:

- 0 = for broadcast (default key)
- 1 = for unicast (key mapping key)

Key Index

The Key Index is 7 bits.

Key Signature

The Key Signature field is 16 octets. It contains an HMAC-MD5 message integrity check computed over the EAPOL-Key descriptor, starting from the Version field, with the Key field filled in if present, but with the Key Signature field set to zero. For the computation, the 32 octet (256 bit) MS-MPPE-Send-Key [RFC2548] is used as the HMAC-MD5 key.

Key

If Packet Body Length = 44 + Key Length, then the Key Field contains the key in encrypted form, of length Key Length. If Packet Body Length = 44, then the Key field is absent, and the least significant Key Length octets from the MS-MPPE-Send-Key attribute is used as the keying material. Where the Key field is encrypted using RC4, the RC4 encryption key used to encrypt this field is formed by concatenating the 16 octet (128 bit) Key-IV field with the 32 octet MS-MPPE-Recv-Key attribute. This yields a 48 octet RC4 key (384 bits).

5. Security Considerations

Since this document describes the use of RADIUS for purposes of authentication, authorization, and accounting in IEEE 802.1X-enabled 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], and [RFC3576].

Vulnerabilities include:

- Packet modification or forgery
- Dictionary attacks
- Known plaintext attacks
- Replay
- Outcome mismatches
- 802.11 integration
- Key management issues

5.1. Packet Modification or Forgery

RADIUS, defined in [RFC2865], does not require all Access-Requests to be authenticated or integrity protected. However, IEEE 802.1X is based on EAP. As described in [3579], Section 3.1.:

The Message-Authenticator attribute MUST be used to protect all Access-Request, Access-Challenge, Access-Accept, and Access-Reject packets containing an EAP-Message attribute.

As a result, when used with IEEE 802.1X, all RADIUS packets MUST be authenticated and integrity protected. In addition, as described in [3579], Section 4.2.:

To address the security vulnerabilities of RADIUS/EAP, implementations of this specification SHOULD support IPsec [RFC2401] along with IKE [RFC2409] for key management. IPsec ESP [RFC2406] with non-null transform SHOULD be supported, and IPsec ESP with a non-null encryption transform and authentication

support SHOULD be used to provide per-packet confidentiality, authentication, integrity and replay protection. IKE SHOULD be used for key management.

5.2. Dictionary Attacks

As discussed in [RFC3579] Section 4.3.3., the RADIUS shared secret is vulnerable to offline dictionary attack, based on capture of the Response Authenticator or Message-Authenticator attribute. In order to decrease the level of vulnerability, [RFC2865], Section 3 recommends:

The secret (password shared between the client and the RADIUS server) SHOULD be at least as large and unguessable as a well-chosen password. It is preferred that the secret be at least 16 octets.

In addition, the risk of an offline dictionary attack can be further mitigated by employing IPsec ESP with a non-null transform in order to encrypt the RADIUS conversation, as described in [RFC3579], Section 4.2.

5.3. Known Plaintext Attacks

Since IEEE 802.1X is based on EAP, which does not support PAP, the RADIUS User-Password attribute is not used to carry hidden user passwords. The hiding mechanism utilizes MD5, defined in [RFC1321], in order to generate a key stream based on the RADIUS shared secret and the Request Authenticator. Where PAP is in use, it is possible to collect key streams corresponding to a given Request Authenticator value, by capturing RADIUS conversations corresponding to a PAP authentication attempt using a known password. Since the User-Password is known, the key stream corresponding to a given Request Authenticator can be determined and stored.

The vulnerability is described in detail in [RFC3579], Section 4.3.4. Even though IEEE 802.1X Authenticators do not support PAP authentication, a security vulnerability can still exist where the same RADIUS shared secret is used for hiding User-Password as well as other attributes. This can occur, for example, if the same RADIUS proxy handles authentication requests for both IEEE 802.1X (which may hide the Tunnel-Password, MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes) and GPRS (which may hide the User-Password attribute).

The threat can be mitigated by protecting RADIUS with IPsec ESP with a non-null transform, as described in [RFC3579], Section 4.2. In addition, the same RADIUS shared secret MUST NOT be used for both IEEE 802.1X authentication and PAP authentication.

5.4. Replay

As noted in [RFC3579] Section 4.3.5., the RADIUS protocol provides only limited support for replay protection. Replay protection for RADIUS authentication and accounting can be provided by enabling IPsec replay protection with RADIUS, as described in [RFC3579], Section 4.2.

As with the Request Authenticator, for use with IEEE 802.1X Authenticators, the Acct-Session-Id SHOULD be globally and temporally unique.

5.5. Outcome Mismatches

[RFC3579] Section 2.6.3. discusses the issues that arise when the EAP packet encapsulated in an EAP-Message attribute does not agree with the RADIUS Packet Type. For example, an EAP Success packet might be encapsulated within an Access-Reject; an EAP Failure might be sent within an Access-Accept; or an EAP Success or Failure might be sent within an Access-Challenge.

As described in [RFC3579] Section 2.6.3., these conflicting messages are likely to cause confusion. To 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 (Access-Accept/Reject) and not based on the contents of EAP-Message attributes, if present.

5.6. 802.11 Integration

[IEEE8021X] was developed for use on wired IEEE 802 networks such as Ethernet, and therefore does not describe how to securely adapt IEEE 802.1X for use with 802.11. This is left to an enhanced security specification under development within IEEE 802.11.

For example, [IEEE8021X] does not specify whether authentication occurs prior to, or after association, nor how the derived keys are used within various ciphersuites. It also does not specify ciphersuites addressing the vulnerabilities discovered in WEP, described in [Berkeley], [Arbaugh], [Fluhrer], and [Stubble]. [IEEE8021X] only defines an authentication framework, leaving the definition of the authentication methods to other documents, such as [RFC2716].

Since [IEEE8021X] does not address 802.11 integration issues, implementors are strongly advised to consult additional IEEE 802.11 security specifications for guidance on how to adapt IEEE 802.1X for use with 802.11. For example, it is likely that the IEEE 802.11

enhanced security specification will define its own IEEE 802.11 key hierarchy as well as new EAPOL-Key descriptors.

5.7. Key Management Issues

The EAPOL-Key descriptor described in Section 4. is likely to be deprecated in the future, when the IEEE 802.11 enhanced security group completes its work. Known security issues include:

- [1] Default key-only support. IEEE 802.1X enables the derivation of per-Station unicast keys, known in [IEEE80211] as "key mapping keys." Keys used to encrypt multicast/broadcast traffic are known as "default keys". However, in some 802.11 implementations, the unicast keys, derived as part of the EAP authentication process, are used solely in order to encrypt, authenticate and integrity protect the EAPOL-Key descriptor, as described in Section 4. These implementations only support use of default keys (ordinarily only used with multicast/broadcast traffic) to secure all traffic, unicast or multicast/broadcast, resulting in inherent security weaknesses.

Where per-Station key-mapping keys (e.g. unicast keys) are unsupported, any Station possessing the default key can decrypt traffic from other Stations or impersonate them. When used along with a weak cipher (e.g. WEP), implementations supporting only default keys provide more material for attacks such as those described in [Fluhrer] and [Stubble]. If in addition, the default key is not refreshed periodically, IEEE 802.1X dynamic key derivation provides little or no security benefit. For an understanding of the issues with WEP, see [Berkeley], [Arbaugh], [Fluhrer], and [Stubble].

- [2] Reuse of keying material. The EAPOL-Key descriptor specified in section 4 uses the same keying material (MS-MPPE-Recv-Key) both to encrypt the Key field within the EAPOL-Key descriptor, and to encrypt data passed between the Station and Access Point. Multi-purpose keying material is frowned upon, since multiple uses can leak information helpful to an attacker.
- [3] Weak algorithms. The algorithm used to encrypt the Key field within the EAPOL-Key descriptor is similar to the algorithm used in WEP, and as a result, shares some of the same weaknesses. As with WEP, the RC4 stream cipher is used to encrypt the key. As input to the RC4 engine, the IV and key are concatenated rather than being combined within a mixing function. As with WEP, the IV is not a counter, and therefore there is little protection against reuse.

As a result of these vulnerabilities, implementors intending to use the EAPOL-Key descriptor described in this document are urged to consult the 802.11 enhanced security specification for a more secure alternative. It is also advisable to consult the evolving literature on WEP vulnerabilities, in order to better understand the risks, as well as to obtain guidance on setting an appropriate re-keying interval.

6. IANA Considerations

This specification does not create any RADIUS attributes nor any new number spaces for IANA administration. However, it does require assignment of new values to existing RADIUS attributes. These include:

Attribute =====	Values Required =====
NAS-Port-Type	Token-Ring (20), FDDI (21)
Tunnel-Type	VLAN (13)
Acct-Terminate-Cause	Supplicant Restart (19) Reauthentication Failure (20) Port Reinitialized (21) Port Administratively Disabled (22)

7. References

7.1. Normative References

- [RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2284] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.
- [RFC2865] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.
- [RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.
- [RFC2867] Zorn, G., Aboba, B. and D. Mitton, "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867, June 2000.

- [RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.
- [RFC2869] Rigney, C., Willats, W. and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.
- [RFC3162] Aboba, B., Zorn, G. and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.
- [RFC3280] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.
- [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 (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.
- [IEEE8021X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.

7.2. Informative References

- [RFC2104] Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.
- [RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.
- [RFC2548] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.
- [RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.
- [RFC2716] Aboba, B. and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

- [MD5Attack] Dobbertin, H., "The Status of MD5 After a Recent Attack." CryptoBytes Vol.2 No.2, Summer 1996.
- [IEEE802] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.
- [IEEE8021Q] IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1Q, January 1998.
- [IEEE8023] ISO/IEC 8802-3 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, (also ANSI/IEEE Std 802.3- 1996), 1996.
- [IEEE80211] 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. 802.11-1999, 1999.
- [Berkeley] Borisov, N., Goldberg, I. and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", ACM SIGMOBILE, Seventh Annual International Conference on Mobile Computing and Networking, July 2001, Rome, Italy.
- [Arbaugh] Arbaugh, W., Shankar, N. and J.Y.C. Wan, "Your 802.11 Wireless Network has No Clothes", Department of Computer Science, University of Maryland, College Park, March 2001.
- [Fluhrer] Fluhrer, S., Mantin, I. and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Eighth Annual Workshop on Selected Areas in Cryptography, Toronto, Canada, August 2001.
- [Stubble] Stubblefield, A., Ioannidis, J. and A. Rubin, "Using the Fluhrer, Mantin and Shamir Attack to Break WEP", 2002 NDSS Conference.

8. Table of Attributes

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 require layer 3 capabilities, and thus may not be supported by all Authenticators. For each attribute, the reference provides the definitive information on usage.

802.1X	#	Attribute
X	1	User-Name [RFC2865]
	2	User-Password [RFC2865]
	3	CHAP-Password [RFC2865]
X	4	NAS-IP-Address [RFC2865]
X	5	NAS-Port [RFC2865]
X	6	Service-Type [RFC2865]
	7	Framed-Protocol [RFC2865]
L3	8	Framed-IP-Address [RFC2865]
L3	9	Framed-IP-Netmask [RFC2865]
L3	10	Framed-Routing [RFC2865]
X	11	Filter-Id [RFC2865]
X	12	Framed-MTU [RFC2865]
	13	Framed-Compression [RFC2865]
L3	14	Login-IP-Host [RFC2865]
L3	15	Login-Service [RFC2865]
L3	16	Login-TCP-Port [RFC2865]
	18	Reply-Message [RFC2865]
	19	Callback-Number [RFC2865]
	20	Callback-Id [RFC2865]
L3	22	Framed-Route [RFC2865]
L3	23	Framed-IPX-Network [RFC2865]
X	24	State [RFC2865]
X	25	Class [RFC2865]
X	26	Vendor-Specific [RFC2865]
X	27	Session-Timeout [RFC2865]
X	28	Idle-Timeout [RFC2865]
X	29	Termination-Action [RFC2865]
X	30	Called-Station-Id [RFC2865]
X	31	Calling-Station-Id [RFC2865]
X	32	NAS-Identifier [RFC2865]
X	33	Proxy-State [RFC2865]
	34	Login-LAT-Service [RFC2865]
	35	Login-LAT-Node [RFC2865]
	36	Login-LAT-Group [RFC2865]
802.1X	#	Attribute

802.1X	#	Attribute
L3	37	Framed-AppleTalk-Link [RFC2865]
L3	38	Framed-AppleTalk-Network [RFC2865]
L3	39	Framed-AppleTalk-Zone [RFC2865]
X	40	Acct-Status-Type [RFC2866]
X	41	Acct-Delay-Time [RFC2866]
X	42	Acct-Input-Octets [RFC2866]
X	43	Acct-Output-Octets [RFC2866]
X	44	Acct-Session-Id [RFC2866]
X	45	Acct-Authentic [RFC2866]
X	46	Acct-Session-Time [RFC2866]
X	47	Acct-Input-Packets [RFC2866]
X	48	Acct-Output-Packets [RFC2866]
X	49	Acct-Terminate-Cause [RFC2866]
X	50	Acct-Multi-Session-Id [RFC2866]
X	51	Acct-Link-Count [RFC2866]
X	52	Acct-Input-Gigawords [RFC2869]
X	53	Acct-Output-Gigawords [RFC2869]
X	55	Event-Timestamp [RFC2869]
	60	CHAP-Challenge [RFC2865]
X	61	NAS-Port-Type [RFC2865]
	62	Port-Limit [RFC2865]
	63	Login-LAT-Port [RFC2865]
X	64	Tunnel-Type [RFC2868]
X	65	Tunnel-Medium-Type [RFC2868]
L3	66	Tunnel-Client-Endpoint [RFC2868]
L3	67	Tunnel-Server-Endpoint [RFC2868]
L3	68	Acct-Tunnel-Connection [RFC2867]
L3	69	Tunnel-Password [RFC2868]
	70	ARAP-Password [RFC2869]
	71	ARAP-Features [RFC2869]
	72	ARAP-Zone-Access [RFC2869]
	73	ARAP-Security [RFC2869]
	74	ARAP-Security-Data [RFC2869]
	75	Password-Retry [RFC2869]
	76	Prompt [RFC2869]
X	77	Connect-Info [RFC2869]
X	78	Configuration-Token [RFC2869]
X	79	EAP-Message [RFC3579]
X	80	Message-Authenticator [RFC3579]
X	81	Tunnel-Private-Group-ID [RFC2868]
L3	82	Tunnel-Assignment-ID [RFC2868]
X	83	Tunnel-Preference [RFC2868]
	84	ARAP-Challenge-Response [RFC2869]
802.1X	#	Attribute

802.1X	#	Attribute
X	85	Acct-Interim-Interval [RFC2869]
X	86	Acct-Tunnel-Packets-Lost [RFC2867]
X	87	NAS-Port-Id [RFC2869]
L3	88	Framed-Pool [RFC2869]
L3	90	Tunnel-Client-Auth-ID [RFC2868]
L3	91	Tunnel-Server-Auth-ID [RFC2868]
X	95	NAS-IPv6-Address [RFC3162]
	96	Framed-Interface-Id [RFC3162]
L3	97	Framed-IPv6-Prefix [RFC3162]
L3	98	Login-IPv6-Host [RFC3162]
L3	99	Framed-IPv6-Route [RFC3162]
L3	100	Framed-IPv6-Pool [RFC3162]
X	101	Error-Cause [RFC3576]
802.1X	#	Attribute

Key

===

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

9. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

10. Acknowledgments

The authors would like to acknowledge Bob O'Hara of Airespace, David Halasz of Cisco, Tim Moore, Sachin Seth and Ashwin Palekar of Microsoft, Andrea Li, Albert Young and Dave Bagby of 3Com for contributions to this document.

11. Authors' Addresses

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

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

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

Andrew Smith
Trapeze Networks
5753 W. Las Positas Blvd.
Pleasanton, CA 94588-4084

Fax: +1 415 345 1827
EMail: ah_smith@acm.org

John Roese
Enterasys

Phone: +1 603 337 1506
EMail: jjr@enterasys.com

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500
Bellevue, WA 98004

Phone: +1 425 438 8218
Fax: +1 425 438 1848
EMail: gwz@cisco.com

12. Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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

