Network Working Group
INTERNET-DRAFT
Category: Informational
<draft-congdon-radius-8021x-17.txt>
12 November 2001

Paul Congdon
Hewlett Packard Company
Bernard Aboba
Tim Moore
Ashwin Palekar
Microsoft
Andrew Smith
Extreme Networks
Glen Zorn
Dave Halasz
Cisco Systems
Andrea Li
Albert P. Young
3Com
John Roese
Enterasys

IEEE 802.1X RADIUS Usage Guidelines

Abstract

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

This document provides suggestions on RADIUS usage by IEEE 802.1X Authenticators. An earlier version of this specification is included in a non-normative Appendix of the IEEE 802.1X specification. It is currently being revised within the IEEE 802.1X Revision PAR effort and is being presented to the IETF for informational purposes.

1. Introduction

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.

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.

This document is currently being revised as part of the IEEE 802.1X Revision PAR effort, and is being presented to the IETF for informational purposes.

1.1. Terminology

This document uses the following terms:

Authenticator
: An Authenticator is an entity that require authentication from the Supplicant. The Authenticator may be connected to the Supplicant at the other end of a point-to-point LAN segment or 802.11 wireless link.

Authentication Server
: An Authentication Server is an entity that provides an Authentication Service to an Authenticator. This service verifies from the credentials provided by the Supplicant, the claim of identity made by the Supplicant.

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.

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, the key words "MAY", "MUST, "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT", are to be interpreted as described in RFC 2119 [3].

2. RADIUS accounting attributes

With a few exceptions, the RADIUS accounting attributes defined in [5] and [6] 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 [5]. As described in [13], IEEE 802.1X defines the following termination cause values, which are shown with their RADIUS equivalents in the following table:

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. For example, if the Supplicant disconnects a point-to-point LAN connection, or moves out of range of an 802.11 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 reauthentication timer or explicit reauthentication request by management action.

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.

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 IEEE 802.1X does not act on aggregated ports, it is possible for a Supplicant roaming between IEEE 802.11 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 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.

If Acct-Multi-Session-Id were not unique between Access Points, then it is possible that the chosen Acct-Multi-Session-Id might 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, it is recommended that the Acct-Multi-Session-Id attribute be unique among all the 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 Access-Point MAC Address | Supplicant MAC Address | NTP Timestamp

Here the original Access-Point MAC Address is the MAC address of the Access Point (in binary form) at which the session started, and the 32-bit NTP timestamp indicates the beginning of the original session. In order to provide for consistency of the Acct-Multi-Session-Id between **802.11 roaming sessions, the multi-session-id may be moved between** Access Points as part of an inter-access point protocol.

The use of 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 [5], for use with IEEE 802.1X, it is encoded as an ASCII string of Hex digits.

2.3. Acct-Link-Count

Since IEEE 802.1X does not act on aggregated ports, there is no equivalent to PPP multi-link bundles, and this attribute is not useful for IEEE 802.1X authenticators.

3. RADIUS authentication

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

- User-Name
- NAS-IP-Address, NAS-IPv6-Address
- NAS-Port
- Service-Type
- Framed-Routing
- Filter-Id
- Framed-MTU
- Reply-Message
- Framed-Route, Framed-IPv6-Route
- State
- Class
- Vendor-Specific
- Session-Timeout
- Idle-Timeout
- Termination-Action
- Called-Station-ID
- Calling-Station-ID
- NAS-Identifier
- Proxy-State
- NAS-Port-Type
- Password-Retry
- Connect-Info
- EAP-Message
- Message-Authenticator
- NAS-Port-Id
- Tunnel-attributes

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 [4].

Alternatively, where Service-Type=Call Check, the User-Name attribute contains 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 802.11 Access Point does not have physical ports, it does assign a unique "association ID" to every mobile station upon a successful association exchange. As a result, for an 802.11 Access Point, the NAS-Port attribute will contain the association ID, which is a 16-bit unsigned integer.

3.5. Service-Type

For use with IEEE 802.1X, only the Framed (2), Authenticate Only (8), and Call Check (10) values have meaning.

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 [4], 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 [4] 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 802 media, the Framed-Protocol attribute is not used by IEEE 802.1X authenticators.

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

Since IEEE 802.1X does not provide a mechanism for IP address assignment, the Framed-IP-Address and Framed-IP-Netmask attributes are not used by IEEE 802.1X authenticators.

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 for the supplicant. For use with an IEEE 802.1X authenticator, it may be used to indicate either layer 2 or layer 3 filters.

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. 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

3.11. Framed-Compression

IEEE 802.1X does not include compression support so that this attribute is not understood by 802.1X Authenticators.

3.12. Reply-Message

This attribute is used to indicate text which MAY be displayed to the user. An IEEE 802.1X authenticator receiving this attribute includes the String within an EAP-Request/Notification message sent to the supplicant.

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, Vendor-Specific, Proxy-State

These attributes are used for the same purposes as described in [4].

3.16. 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.

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.

3.17. Idle-Timeout

The Idle-Timeout attribute is described in [4]. 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 802.11. It is possible for an 802.11 device to wander out of range of all access points. In this case, the Idle-Timeout attribute indicates the maximum time that an 802.11 device may remain idle.

3.18. 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.

3.19. Called-Station-Id

For IEEE 802.1X authenticators, this attribute is used to store the bridge or Access Point MAC address in ASCII format, with octet values separated by a "-". 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".

3.20. Calling-Station-Id

For IEEE 802.1X authenticators, this attribute is used to store the supplicant MAC address in ASCII format, with octet values separated by a "-". Example: "00-10-A4-23-19-C0".

3.21. NAS-Identifier

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

3.22. 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.

3.23. Port-Limit

This attribute has no meaning when sent to an IEEE 802.1X Authenticator.

3.24. 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.

3.25. 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.

3.26. EAP-Message

Since IEEE 802.1X provides for encapsulation of EAP as described in [1] and [13], the EAP-Message attribute is used to encapsulate EAP packets for transmission from the IEEE 802.1X Authenticator to the Authentication Server.

3.27. Message-authenticator

As noted in [6], the Message-Authenticator attribute MUST be used to protect all packets containing an EAP-Message attribute.

3.28. 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.

3.29. Framed-Pool, Framed-IPv6-Pool

Since IEEE 802.1X does not support address assignment, these attributes have no meaning to IEEE 802.1X Authenticators.

3.30. Tunnel attributes

Reference [20] defines RADIUS tunnel attributes used for authentication and authorization, and reference [21] 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) 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 sent:

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

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.

4. Security considerations

Since this draft 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, with one exception. For a discussion of these threats, see [6].

Since IEEE 802.1X does not support PAP or CHAP authentication, the RADIUS User-Password hiding mechanism is not utilized to hide user passwords. As noted in [18], there are doubts about the security of this mechanism.

Note that RFC 2869 [6] does not require that the EAP packet encapsulated in an EAP-Message attribute agree with the outcome of the authentication, or even that an EAP-Message attribute be included in an Access-Accept or Access-Reject. For example, an EAP-Success can be encapsulated in an Access-Reject, or an EAP-Failure can be encapsulated within an Access-Accept. 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.

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.

5. 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 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]
802.1X	#	Attribute

802.1X	#	Attribute
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]
802.1X	#	Attribute

802.1X	#	Attribute
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]
802.1X	#	Attribute

Key
===

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

6. References

[1] Blunk, L., Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[2] Rivest, R., Dusse, S., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March, 1997.

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

[5] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[6] Rigney, C., Willats, W., Calhoun, P., "RADIUS Extensions", RFC 2869, June 2000.

[7] IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, ANSI/IEEE Std 802, 1990.

[8] ISO/IEC 10038 Information technology - Telecommunications and information exchange between systems - Local area networks - Media Access Control (MAC) Bridges, (also ANSI/IEEE Std 802.1D- 1993),

1993.

[9] ISO/IEC Final CD 15802-3 Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3:Media Access Control (MAC) bridges, (current draft available as IEEE P802.1D/D15).

[10] IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1Q/D8, January 1998.

[11] 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.

[12] IEEE Standards for Local and Metropolitan Area Networks: Demand Priority Access Method, Physical Layer and Repeater Specification For 100 Mb/s Operation, IEEE Std 802.12-1995.

[13] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.

[14] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[15] Yergeau, F., "UTF-8, a transformation format of Unicode and ISO 10646", RFC 2044, October 1996.

[16] Aboba, B., Beadles, M., "The Network Access Identifier", RFC 2486, January 1999.

[17] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[18] Dobbertin, H., "The Status of MD5 After a Recent Attack." CryptoBytes Vol.2 No.2, Summer 1996.

[19] Atkinson, R., "Security Architecture for the Internet Protocol", RFC 1825, August 1995.

[20] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., Goyret, I., "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[21] Zorn, G., Mitton, D., Aboba, B., "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867, June 2000.

[22] 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.

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

7. 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)

Acknowledgments

The authors would like to acknowledge Bob O'Hara of Informed Technology and Dave Bagby of 3Com for contributions to this document.

Authors' Addresses

Paul Congdon
Hewlett Packard Company
HP ProCurve Networking
3000 Hanover Street
Palo Alto, CA 94304

Phone: +1 916 785 5753
Fax: +1 916 785 5949
Email: PAUL_CONGDON@hp.com

Andrew Smith
Allegro Networks
6399 San Ignacio Ave.
San Jose, CA 95119

Fax: +1 415 345 1827
Email: andrew@allegronetworks.com

Albert P. Young
3Com Corporation
5400 **Bayfront Plaza**
P.O. Box 58145, M/S: 4204
Santa Clara CA 95052-8145

Phone: +1 408 326 6435
Fax: +1 408 326 5855
Email: Albert_Young@3com.com

Andrea Li
3Com Corporation
10545 **Willows Rd. NE**
M/S: Suite 110 - First Floor
Redmond, WA 98052

Phone: +1 425 498 8213
Fax: +1 425 498 8201
Email: Andrea_Li@3com.com

John Roese
Enterasys

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

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

Dave Halasz
Cisco Systems

Email: dhala@cisco.com

Bernard Aboba
Ashwin Palekar
Tim Moore
Microsoft Corporation
One Microsoft Way

Redmond, WA 98052

EMail: {bernarda, ashwinp, timmoore}@microsoft.com
Phone: +1 425 882 8080
Fax: +1 425 936 7329

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.

Full Copyright Statement

INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

Expiration Date

This memo is filed as <draft-congdon-radius-8021x-17.txt>, and expires May 22, 2002.