Network Working Group
INTERNET-DRAFT
Category: Proposed Standard
<draft-ietf-radext-vlan-01.txt>
22 March 2006

Paul Congdon
Mauricio Sanchez
Hewlett-Packard Company
Bernard Aboba
Microsoft Corporation

RADIUS Attributes for Virtual LAN and Priority Support

Copyright Notice

Abstract

This document proposes additional RADIUS (Remote Authentication Dial In User Service) attributes for dynamic Virtual LAN assignment and prioritization, for use by IEEE 802.1X authenticators. These attributes are usable within either RADIUS or Diameter.

Table of Contents

1. Introduction

IEEE 802.1X [IEEE-802.1X] provides "network port authentication" for IEEE 802 [IEEE-802] media, including Ethernet [IEEE-802.3], Token Ring and 802.11 wireless LANs [IEEE-802.11i].

This document describes Virtual LAN (VLAN) and re-prioritization attributes that may prove useful for provisioning of access to IEEE 802 local area networks with the Remote Authentication Dialin User Service (RADIUS).

While [RFC3580] enables support for VLAN assignment based on the tunnel attributes defined in [RFC2868], it does not provide support for a more complete set of VLAN functionality as defined by [IEEE-802.1Q]. The attributes defined in this document provide support within RADIUS analogous to the management variables supported in [IEEE-802.1Q] and MIB objects defined in [RFC4363]. In addition, this document enables support for a wider range of [IEEE-802.1X] configurations.

1.1. Terminology

This document uses the following terms:

Authenticator
: The end of the link initiating EAP authentication. The term authenticator is used in [RFC3748] and [IEEE-802.1X], and has the same meaning in this document.

backend authentication server
: A backend authentication server is an entity that provides an authentication service to an authenticator. When used, this server typically executes EAP methods for the authenticator. This terminology is also used in [IEEE-802.1X].

Network Access Server (NAS)
: A device that provides an access service for a user to a network.

Supplicant
: The end of the link that responds to the authenticator in [IEEE-802.1X].

1.2. Requirements Language

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].

1.3. Attribute Interpretation

If a NAS conforming to this specification receives an Access-Accept packet containing an attribute defined in this document which it cannot apply, it MUST act as though it had received an Access-Reject.

Similarly, [RFC3576] requires that a NAS receiving a CoA-Request containing an unsupported attribute reply with a CoA-NAK. It is recommended that an Error-Cause attribute with value set to "Unsupported Attribute" (401) be included in the packet. As noted in [RFC3576], authorization changes are atomic so that this situation does not result in session termination and the pre-existing configuration remains unchanged. As a result, no accounting packets should be generated.

2. Attributes

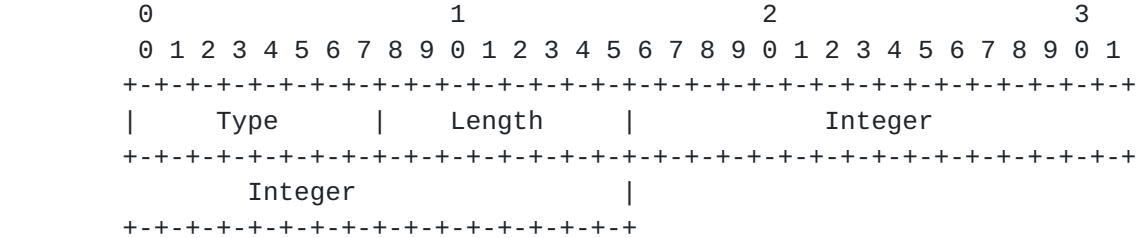
2.1. Egress-VLANID

Description

The Egress-VLANID attribute represents an allowed IEEE 802 Egress VLANID for this port, indicating if the VLANID is allowed for tagged or untagged packets as well as the VLANID.

Multiple Egress-VLANID attributes MAY be included in an Access-Request, Access-Accept or CoA-Request packet; this attribute MUST NOT be sent within an Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, or CoA-NAK. Each attribute adds the specified VLAN to the list of allowed egress VLANs for the port.

The Egress-VLANID attribute is shown below. The fields are transmitted from left to right:



Type

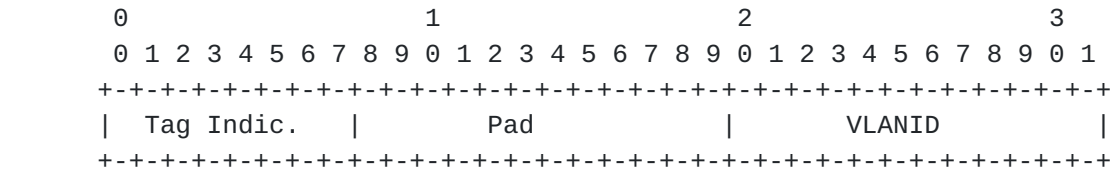
TBD

Length

6

Integer

The Integer field is four octets in length. The format is described below:



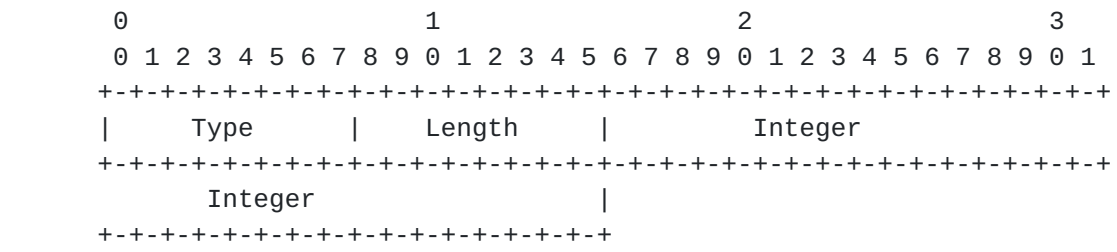
The Tag Indication field is one octet in length, and indicates whether the frames on the VLAN are tagged (0x31) or untagged (0x32). The Pad field is 12-bits in length and MUST be 0 (zero). The VLANID is 12-bits in length and contains the [IEEE-802.1Q] VLAN VID value.

2.2. Ingress-Filters

Description

The Ingress-Filters attribute corresponds to Ingress Filter per-port variable defined in [IEEE-802.1Q] clause 8.4.5. When the attribute has the value "Enabled", the set of VLANs that are allowed to ingress a port must match the set of VLANs that are allowed to egress a port. Only a single Ingress-Filters attribute MAY be sent within an Access-Request, Access-Accept or CoA-Request packet; this attribute MUST NOT be sent within an Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, or CoA-NAK.

The Ingress-Filters attribute is shown below. The fields are transmitted from left to right:



Type

TBD

Length

6

Integer

Supported values include:

1 - Enabled
2 - Disabled

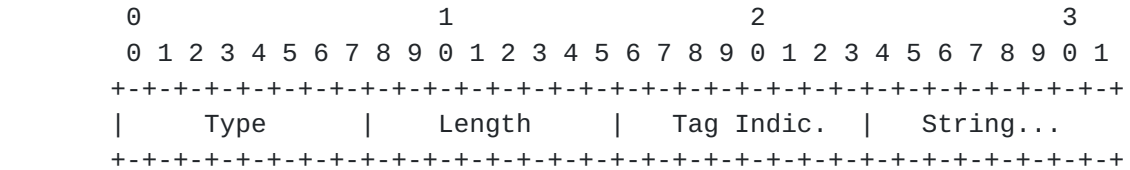
2.3. Egress-VLAN-Name

Description

Clause 12.10.2.1.3 (a) in [IEEE-8021.Q] describes the administratively assigned VLAN Name associated with a VLAN-ID defined within an IEEE 802.1Q bridge. The Egress-VLAN-Name attribute represents an allowed VLAN for this port. It is similar to the Egress-VLANID attribute, except that the VLAN-ID itself is not specified or known; rather the VLAN name is used to identify the VLAN within the system.

The Egress-VLAN-Name attribute contains two parts; the first part indicates if frames on the VLAN for this port are to be represented in tagged or untagged format, the second part is the VLAN name.

Multiple Egress-VLAN-Name attributes MAY be included within an Access-Request, Access-Accept or CoA-Request packet; this attribute MUST NOT be sent within an Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, or CoA-NAK. Each attribute adds the named VLAN to the list of allowed egress VLANs for the port. The Egress-VLAN-Name attribute is shown below. The fields are transmitted from left to right:



Type

TBD

Length

>=4

Tag Indication

The Tag Indication field is one octet in length, and indicates whether the frames on the VLAN are tagged (0x31) or untagged (0x32).

String

The String field is at least one octet in length, and contains the the VLAN Name as defined in [IEEE-802.1Q] clause 12.10.2.1.3 (a). [RFC3629] UTF-8 encoded 10646 characters are RECOMMENDED, but a robust implementation SHOULD support the field as undistinguished octets.

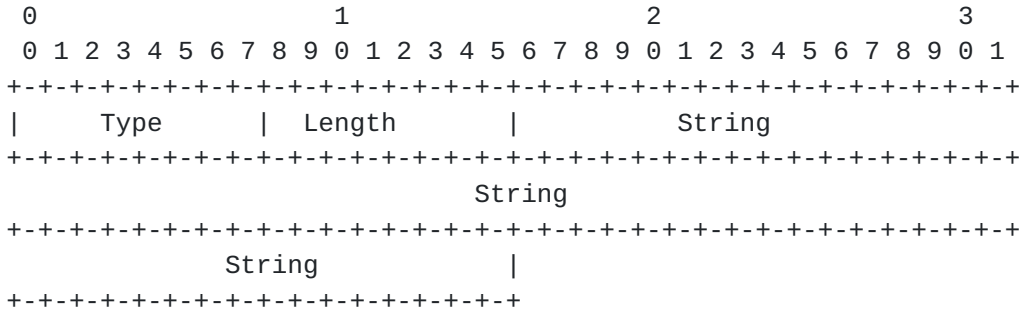
2.4. User-Priority-Table

Description

[IEEE-802.1D] clause 7.5.1 discusses how to regenerate (or re-map) user priority on frames received at a port. This per-port configuration enables a bridge to cause the priority of received traffic at a port to be mapped to a particular priority. The management variables are described in clause 14.6.2.2.

This attribute represents the IEEE 802 prioritization that will be applied to packets arriving at this port. There are eight possible user priorities, according to the [IEEE-802] standard. A single User-Priority-Table attribute MAY be included in an Access-Request, Access-Accept or CoA-Request packet; this attribute MUST NOT be sent within an Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, or CoA-NAK.

The User-Priority-Table attribute is shown below. The fields are transmitted from left to right:



Type

TBD

Length

10

String

The String field is 8 octets in length, and includes a table which maps the incoming priority (if one exists - the default is 0) into one of eight regenerated priorities. The first octet maps to incoming priority 0, the second octet to incoming priority 1, etc. The values in each octet represent the regenerated priority of the packet.

It is thus possible to either remap incoming priorities to more appropriate values; or to honor the incoming priorities; or to override any incoming priorities, forcing them to all map to a single chosen priority.

The [IEEE-8021.D] specification, Annex G, provides a useful description of traffic type - traffic class mappings.

3. Table of Attributes

The following table provides a guide to which attributes may be found in which kinds of packets, and in what quantity.

Access-Request	Access-Accept	Access-Reject	Access-Challenge	CoA-Req	#	Attribute
0+	0+	0	0	0+	TBD	Egress-VLANID
0-1	0-1	0	0	0-1	TBD	Ingress-Filters
0+	0+	0	0	0+	TBD	Egress-VLAN-Name
0-1	0-1	0	0	0-1	TBD	User-Priority-Table

The following table defines the meaning of the above table entries.

0	This attribute MUST NOT be present in the packet.
0+	Zero or more instances of this attribute MAY be present in the packet.
0-1	Zero or one instance of this attribute MAY be present in the packet.

4. Diameter Considerations

Diameter needs to define identical attributes with the same Type values. The attributes should be available as part of the NASREQ application [RFC4005], as well as the Diameter EAP application [RFC4072].

5. IANA Considerations

This specification does not create any new registries.

This document uses the RADIUS [RFC2865] namespace, see <http://www.iana.org/assignments/radius-types>. Allocation of four updates for the section "RADIUS Attribute Types" is requested. The RADIUS attributes for which values are requested are:

TBD - Egress-VLANID
TBD - Ingress-Filters
TBD - Egress-VLAN-Name
TBD - User-Priority-Table

6. Security Considerations

This specification describes the use of RADIUS for purposes of authentication, authorization and accounting in networks supporting [IEEE 802.1X]. Threats and security issues for this application are described in [RFC3579] and [RFC3580]; security issues encountered in roaming are described in [RFC2607].

This document specifies new attributes that can be included in existing RADIUS packets, which are protected as described in [RFC3579] and [RFC3576]. See those documents for a more detailed description.

The security mechanisms described in [RFC3579] and [RFC3576] are focused on preventing an attacker from spoofing packets or modifying packets in transit. They do not prevent an authorized RADIUS server or proxy from inserting attributes with malicious intent.

VLAN attributes sent by a RADIUS server or proxy may enable access to unauthorized VLANs. These vulnerabilities can be limited by performing authorization checks at the NAS. For example, a NAS can be configured to accept only certain VLANIDs from a given RADIUS server/proxy.

Similarly, an attacker gaining control of a RADIUS server or proxy can modify the user priority table, causing either degradation of quality of service (by downgrading user priority of packets arriving

at a port), or denial of service (by raising the level of priority of traffic at multiple ports of a device, oversubscribing the switch or link capabilities).

7. References

7.1. Normative references

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March, 1997.

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

[RFC3575] Aboba, B., "IANA Considerations for RADIUS", RFC 3575, July 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation of ISO 10646", RFC 2607, November 2003.

[RFC4363] Levi, D. and D. Harrington, "Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions", RFC 4363, January 2006.

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

[IEEE-802.1D] IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, IEEE Std 802.1D-2004, June 2004.

[IEEE-802.1Q] IEEE Standards for Local and Metropolitan Area Networks: Draft Standard for Virtual Bridged Local Area Networks, P802.1Q-2003, January 2003.

[IEEE-802.1X] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004, August 2004.

7.2. Informative references

[RFC2607] Aboba, B. and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming", RFC 2607, June 1999.

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D. and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS Support for Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., Roese, J., "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC3580, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4005] Calhoun, P., Zorn, G., Spence, D. and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

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

[IEEE-802.3]
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.

[IEEE-802.11]
Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11-1999, 1999.

[IEEE-802.11i]
Institute of Electrical and Electronics Engineers, "Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", June 2004.

Acknowledgments

The authors would like to acknowledge Joseph Salowey of Cisco, David Nelson of Enterasys, Chuck Black of Hewlett Packard, and Ashwin Palekar of Microsoft.

Authors' Addresses

Paul Congdon
Hewlett Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5662
Roseville, CA 95747

EMail: paul.congdon@hp.com
Phone: +1 916 785 5753
Fax: +1 916 785 8478

Mauricio Sanchez
Hewlett Packard Company
HP ProCurve Networking
8000 Foothills Blvd, M/S 5559
Roseville, CA 95747

EMail: mauricio.sanchez@hp.com
Phone: +1 916 785 1910
Fax: +1 916 785 1815

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

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

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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

Open issues

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

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