Network Working Group
Request for Comments: 4675
Category: Standards Track

P. Congdon
M. Sanchez
Hewlett-Packard Company
B. Aboba
Microsoft Corporation

September 2006

RADIUS Attributes for Virtual LAN and Priority Support

Status of This Memo

Copyright Notice

Abstract

This document proposes additional Remote Authentication Dial-In User Service (RADIUS) attributes for dynamic Virtual LAN assignment and prioritization, for use in provisioning of access to IEEE 802 local area networks. These attributes are usable within either RADIUS or Diameter.

Table of Contents

1. Introduction

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

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 and Diameter 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:

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

RADIUS server
: A RADIUS authentication server is an entity that provides an authentication service to a NAS.

RADIUS proxy
: A RADIUS proxy acts as an authentication server to the NAS, and a RADIUS client to the RADIUS server.

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

The attributes described in this document apply to a single instance of a NAS port, or more specifically an IEEE 802.1Q bridge port. [IEEE-802.1Q], [IEEE-802.1D], and [IEEE-802.1X] do not recognize finer management granularity than "per port". In some cases, such as with IEEE 802.11 wireless LANs, the concept of a "virtual port" is used in place of the physical port. Such virtual ports are typically based on security associations and scoped by station, or Media Access Control (MAC) address.

The attributes defined in this document are applied on a per-user basis and it is expected that there is a single user per port; however, in some cases that port may be a "virtual port". If a NAS implementation conforming to this document supports "virtual ports", it may be possible to provision those "virtual ports" with unique values of the attributes described in this document, allowing multiple users sharing the same physical port to each have a unique set of authorization parameters.

If a NAS conforming to this specification receives an Access-Accept packet containing an attribute defined in this document that it cannot apply, it MUST act as though it had received an Access-Reject. [RFC3576] requires that a NAS receiving a Change of Authorization Request (CoA-Request) reply with a CoA-NAK if the Request contains an unsupported attribute. It is recommended that an Error-Cause attribute with the value set to "Unsupported Attribute" (401) be included in the CoA-NAK. As noted in [RFC3576], authorization changes are atomic so that this situation does not result in session termination and the preexisting configuration remains unchanged. As a result, no accounting packets should be generated.

2. Attributes

2.1. Egress-VLANID

Description

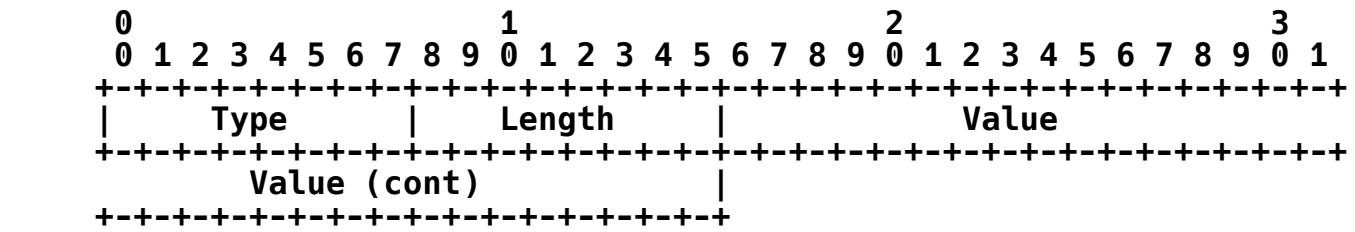
The Egress-VLANID attribute represents an allowed IEEE 802 Egress VLANID for this port, indicating if the VLANID is allowed for tagged or untagged frames as well as the VLANID.

As defined in [RFC3580], the VLAN assigned via tunnel attributes applies both to the ingress VLANID for untagged packets (known as the PVID) and the egress VLANID for untagged packets. In contrast, the Egress-VLANID attribute configures only the egress VLANID for either tagged or untagged packets. The Egress-VLANID attribute MAY be included in the same RADIUS packet as [RFC3580] tunnel attributes; however, the Egress-VLANID attribute is not necessary if it is being used to configure the same untagged VLANID included in tunnel attributes. To configure an untagged VLAN for both ingress and egress, the tunnel attributes of [RFC3580] MUST be used.

Multiple Egress-VLANID attributes MAY be included in Access-Request, Access-Accept, CoA-Request, or Accounting-Request packets; 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

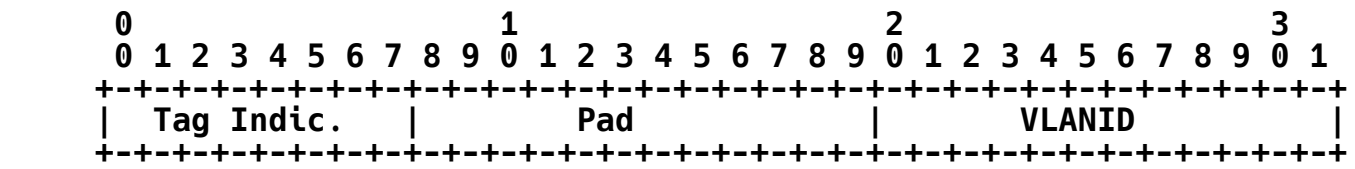
56

Length

6

Value

The Value field is four octets. The format is described below:



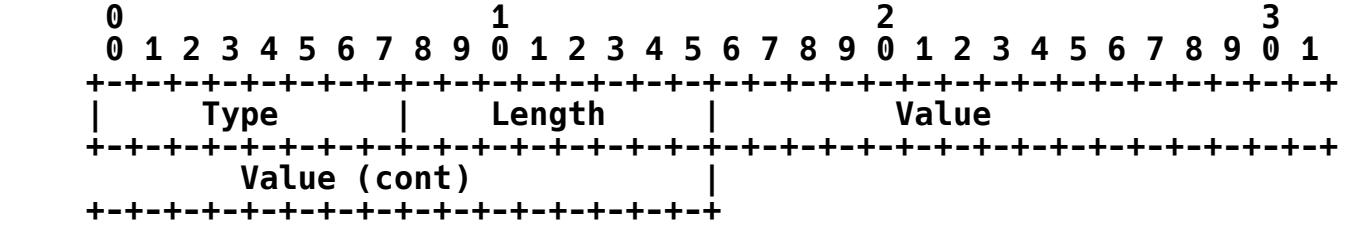
The Tag Indication field is one octet in length and indicates whether the frames on the VLAN are tagged (0x31) or untagged (0x32). The Pad field is 12 bits in length and MUST be 0 (zero). The VLANID is 12 bits in length and contains the [IEEE-802.1Q] VLAN VID value.

2.2. Ingress-Filters

Description

The Ingress-Filters attribute corresponds to the 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, CoA-Request, or Accounting-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

57

Length

6

Value

The Value field is four octets. Supported values include:

1 - Enabled
2 - Disabled

2.3. Egress-VLAN-Name

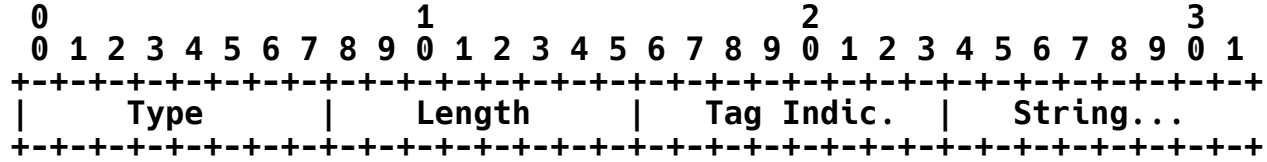
Description

Clause 12.10.2.1.3 (a) in [IEEE-802.1Q] 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 tunnel attributes described in [RFC3580] and the Egress-VLAN-Name attribute both can be used to configure the egress VLAN for untagged packets. These attributes can be used concurrently and MAY appear in the same RADIUS packet. When they do appear concurrently, the list of allowed VLANs is the concatenation of the Egress-VLAN-Name and the Tunnel-Private-Group-ID (81) attributes. The Egress-VLAN-Name attribute does not alter the ingress VLAN for untagged traffic on a port (also known as the PVID). The tunnel attributes from [RFC3580] should be relied upon instead to set the PVID.

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, CoA-Request, or Accounting-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

58

Length

>=4

Tag Indication

The Tag Indication field is one octet in length and indicates whether the frames on the VLAN are tagged (0x31, ASCII '1') or untagged (0x32, ASCII '2'). These values were chosen so as to make them easier for users to enter.

String

The String field is at least one octet in length and contains 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. [IEEE-802.1D] clause 6.3.9 describes the use of remapping:

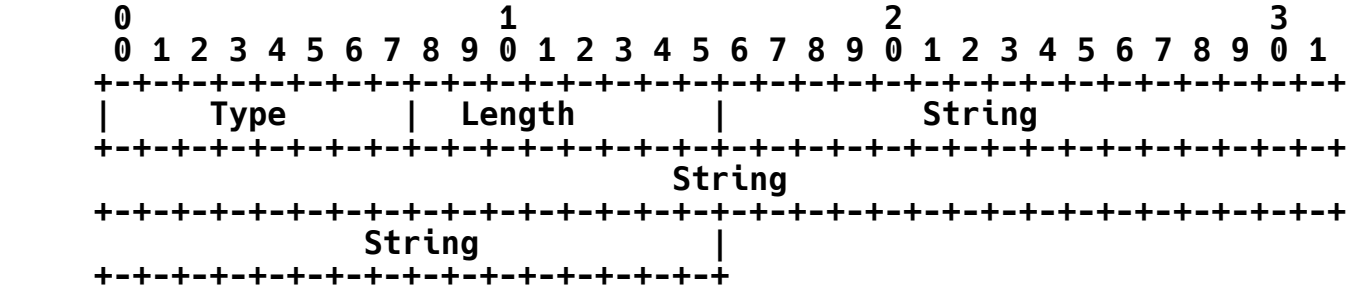
> The ability to signal user priority in IEEE 802 LANs allows user priority to be carried with end-to-end significance across a Bridged Local Area Network. This, coupled with a consistent approach to the mapping of user priority to traffic classes and of user priority to access_priority, allows consistent use of priority information, according to the capabilities of the Bridges and MACs in the transmission path...
>
> Under normal circumstances, user priority is not modified in transit through the relay function of a Bridge; however, network management can control how user priority is propagated. Table 7-1 provides the ability to map incoming user priority values on a per-Port basis. By default, the regenerated user priority is identical to the incoming user priority.

This attribute represents the IEEE 802 prioritization that will be applied to frames arriving at this port. There are eight possible user priorities, according to the [IEEE-802] standard. [IEEE-802.1D] clause 14.6.2.3.3 specifies the regeneration table

as 8 values, each an integer in the range 0-7. The management variables are described in clause 14.6.2.2.

A single User-Priority-Table attribute MAY be included in an Access-Accept or CoA-Request packet; this attribute MUST NOT be sent within an Access-Request, Access-Challenge, Access-Reject, Disconnect-Request, Disconnect-ACK, Disconnect-NAK, CoA-ACK, CoA-NAK or Accounting-Request. Since the regeneration table is only maintained by a bridge conforming to [IEEE-802.1D], this attribute should only be sent to a RADIUS client supporting that specification.

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



Type

59

Length

10

String

The String field is 8 octets in length and includes a table that maps the incoming priority (if it is set -- 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 frame.

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

The [IEEE-802.1D] 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	Acct-Req	#	Attribute
0+	0+	0	0	0+	0+	56	Egress-VLANID
0-1	0-1	0	0	0-1	0-1	57	Ingress-Filters
0+	0+	0	0	0+	0+	58	Egress-VLAN-Name
0	0-1	0	0	0-1	0	59	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

When used in Diameter, the attributes defined in this specification can be used as Diameter attribute-value pair (AVPs) from the Code space 1-255 (RADIUS attribute compatibility space). No additional Diameter Code values are therefore allocated. The data types and flag rules for the attributes are as follows:

		AVP Flag rules				
Attribute Name	Value Type	MUST	MAY	SHLD NOT	MUST NOT	Encr
Egress-VLANID	OctetString	M	P		V	Y
Ingress-Filters	Enumerated	M	P		V	Y
Egress-VLAN-Name	UTF8String	M	P		V	Y
User-Priority-Table	OctetString	M	P		V	Y

The attributes in this specification have no special translation requirements for Diameter to RADIUS or RADIUS to Diameter gateways; they are copied as is, except for changes relating to headers, alignment, and padding. See also [RFC3588] Section 4.1 and [RFC4005] Section 9.

What this specification says about the applicability of the attributes for RADIUS Access-Request packets applies in Diameter to AA-Request [RFC4005] or Diameter-EAP-Request [RFC4072]. What is said about Access-Challenge applies in Diameter to AA-Answer [RFC4005] or Diameter-EAP-Answer [RFC4072] with Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH.

What is said about Access-Accept applies in Diameter to AA-Answer or Diameter-EAP-Answer messages that indicate success. Similarly, what is said about RADIUS Access-Reject packets applies in Diameter to AA-Answer or Diameter-EAP-Answer messages that indicate failure.

What is said about COA-Request applies in Diameter to Re-Auth-Request [RFC4005].

What is said about Accounting-Request applies to Diameter Accounting-Request [RFC4005] as well.

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" has been made by the IANA. The RADIUS attributes are:

56 - Egress-VLANID
57 - Ingress-Filters
58 - Egress-VLAN-Name
59 - User-Priority-Table

6. Security Considerations

This specification describes the use of RADIUS and Diameter for purposes of authentication, authorization, and accounting in IEEE 802 local area networks. RADIUS threats and security issues for this application are described in [RFC3579] and [RFC3580]; security issues encountered in roaming are described in [RFC2607]. For Diameter, the security issues relating to this application are described in [RFC4005] and [RFC4072].

This document specifies new attributes that can be included in existing RADIUS packets, which are protected as described in [RFC3579] and [RFC3576]. In Diameter, the attributes are protected as specified in [RFC3588]. See those documents for a more detailed description.

The security mechanisms supported in RADIUS and Diameter are focused on preventing an attacker from spoofing packets or modifying packets in transit. They do not prevent an authorized RADIUS/Diameter server or proxy from inserting attributes with malicious intent.

VLAN attributes sent by a RADIUS/Diameter 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/Diameter server/proxy.

Similarly, an attacker gaining control of a RADIUS/Diameter server or proxy can modify the user priority table, causing either degradation of quality of service (by downgrading user priority of frames 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", BCP 14, RFC 2119, March 1997.

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

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, 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.

7.2. Informative References

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

[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 (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

[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.

8. Acknowledgements

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

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

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

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

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).