Networking Working Group
INTERNET-DRAFT
<draft-ietf-radext-ieee802-00.txt>

10 July 2005

Paul Congdon
Mauricio Sanchez
Hewlett-Packard Company
A. Lior
Bridgewater Systems
F. Adrangi
Intel
Bernard Aboba
Microsoft

VLAN, Priority, and Filtering Attributes

Copyright Notice

Abstract

In certain scenarios it is desirable to limit user access using dynamic VLANs, filters or redirection. This documents proposes additional attributes for this purpose, for use with the Remote Authentication Dial In User Server (RADIUS). The attributes described in this document are expected to be useful in a variety of environments, including enterprise and service provider scenarios.

Table of Contents

1. Introduction..... 3
1.1. Terminology..... 3
1.2. Requirements Language..... 4
2. Overview..... 5
2.1. Capability Advertisement 6
2.2. Attribute Interpretation..... 6
3. RADIUS Authentication..... 7
3.1. Egress-VLANID..... 7
3.2. Ingress-Filters..... 8
3.3. VLAN-Name..... 9
3.4. User-Priority-Table..... 10
3.5. NAS-Filter-Rule..... 11
3.6. QoS-Filter-Rule..... 18
4. RADIUS Accounting..... 19
4.1. Acct-NAS-Filter-Rule..... 19
4.2. Acct-EAP-Auth-Method..... 19
5. Table of Attributes..... 21
6. IANA Considerations..... 21
7. Security Considerations..... 21
7.1. Packet modification or forgery..... 22
7.2. Dictionary Attacks..... 22
7.3. Known Plaintext Attacks..... 22
8. References..... 23
8.1 Normative References..... 23
8.2 Informative References..... 24
Appendix A - Traffic Redirection..... 25
ACKNOWLEDGMENTS..... 29
AUTHORS' ADDRESSES..... 29
Intellectual Property Statement..... 29
Disclaimer of Validity..... 30
Full Copyright Statement 30

1. Introduction

Within the confines of RADIUS authentication, authorization, and accounting (AAA) environments, there is a general dearth of standardized RADIUS attributes to limit user access using dynamic VLANs, filters or redirection.

For example, in IEEE 802.1X [IEEE8021X] environments, which provides "network port authentication" for IEEE 802 [IEEE802] media, including Ethernet [IEEE8023], Token Ring and 802.11 [IEEE80211i] wireless LANS, there exists a strong desire to control authorization beyond just the untagged VLAN parameter based on tunnel attributes in [RFC2868].

This document describes VLAN, filtering and re-direction attributes that may prove useful in IEEE 802.1X and a variety of situations. The attributes defined in this document may be used with RADIUS dynamic authorization [RFC3576].

The Filter-ID attribute defined in [RFC2865] requires the NAS to be pre-populated with the desired filters. This may be difficult to deploy in roaming scenarios where the home realm may not know what filters have been pre-populated by the local operator. The filtering attributes specified in this document enable explicit description of layer 2 and layer 3 filters as well as redirection, and therefore extend the filter language described in [RFC3588].

User traffic redirection is supported with or without tunneling. Tunneling support is provided using the tunnel attributes defined in [RFC2868]. Redirection of traffic in mid-session may break applications.

IEEE 802.1X-2004 [IEEE8021X] provides "network port authentication" for IEEE 802 [IEEE802] media, including Ethernet [IEEE8023], Token Ring and 802.11 wireless LANs [IEEE80211i]. While [RFC3580] enables support for VLAN assignment based on the tunnel attributes defined in [RFC2868], it does not provide support for the full set of VLAN functionality. The VLAN attributes defined in this document provide support within RADIUS analogous to the MIB variables supported in [IEEE-802.1Q]. In addition, this document enables support for a wider range of [IEEE8021X] configuration.

1.1. Terminology

In this document when we refer to Blocking of IP traffic we mean Filtering of IP traffic. Additionally, 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 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.

Hot-lining
: Blocking and redirection of users traffic is known as hot-lining of accounts. In this document, hot-lining is used as the motivation for these attributes and an illustration of how they would be used. However, the attributes may be used together or separately to provide other features.

Port Access Entity (PAE)
: The IEEE8021.X protocol entity associated with a physical or virtual (802.11) Port. A given PAE may support the IEEE8021.X protocol functionality associated with the Authenticator, Supplicant or both.

Redirection
: Refers to an action taken by the NAS to redirect the user's traffic to an alternate location.

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. 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].

An implementation is not compliant if it fails to satisfy one or more of the must or must not requirements for the protocols it implements. An implementation that satisfies all the must, must not, should and should not requirements for its protocols is said to be "unconditionally compliant"; one that satisfies all the must and must not requirements but not all the should or should not requirements for its protocols is said to be "conditionally compliant".

2. Overview

As described in the Introduction section, it may be desirable to a control user's access to network resources (e.g. the Internet) with greater standardized explicitness than what current RADIUS attributes provide. In this section we will examine these requirements in more detail.

Besides IEEE 802.1X networks, there is a corollary need within Internet Service Provider (ISP) environments for standardized authorization attributes. From time to time, an ISP requires to restrict a user's access to the Internet and redirect their traffic to an alternate location. For example, the user maybe on a prepaid plan and all the resources have been used up. In this case the ISP would block the user's access to the Internet and redirect them to a portal where the user can replenish their account. Another example where the ISP would want to restrict access and redirect a user that was involved in some fraudulent behavior. Again the ISP would want to block the user's access to the Internet and redirect to a portal where they can inform the user as to their state and allow them to inform the user of their concerns and potentially rectify the situation.

The ability to block user's traffic is required at service initiation and once service has been established. These

capabilities must also be available across access technologies and

various business scenarios. For example, the ability to block and redirect traffic is required for TCP users, cell phone users, WiFi users. As well, this capability must work whether the user is in their home network or roaming in a visited network which may or may not have a direct roaming relationship with the user's home network.

Blocking access refers to setting up access control rules at the NAS such that when the user initiates IP traffic, the NAS examines the set of rules associated with the service granted to the user. These rules determine what traffic is allowed to proceed through the NAS and what traffic will be blocked. Today this capability is supported in RADIUS and is configurable during service establishment and mid-service via the Filter-Id(11) attribute. To use Filter-Id to control access to network resources the rules need to be configured apriori at each NAS. Filter-Id(11) is used in an Access-Accept to specify the name of the filter rule(s) to apply to this session. To effect a change mid-service (dynamically), the Filter-Id(11) is included in a Change-of-Authorization (COA) packet as described in [RFC3676]. Upon receiving the Filter-Id(11) the NAS starts to apply the rules specified by the Filter-Id(11).

As pointed out by [NASREQ] the use Filter-Id is not roaming friendly and it is recommended that instead one should use NAS-Filter-Rule(TBD) AVP. For this reason, this document introduces NAS-Filter-Rule(TBD) to RADIUS.

2.1. Capability Advertisement

RADIUS does not currently define a method by which a NAS can advertise its capabilities and in many instances, it would be desirable for the home network to know what capabilities are supported by the NAS to ensure proper operational behavior. The attributes defined in this document are intended to be used to enforce policy by the NAS. If a NAS does not recognize these attributes it will most likely ignore them and the desired policy will not be enforced. A method for the NAS advertising the capability to support these attributes would help the RADIUS server understand if the intended policies can be enforced. As a result, the attributes in this document, in particular NAS-Filter-Rule(TBD), can benefit from capability advertisement, if available.

2.2 Attribute Interpretation

Unless otherwise noted in the individual description of an attribute contained herein, a NAS that conforms to this specification and receives an Access-Accept message that contains

an attribute from this document that it does not recognize or

cannot apply MUST interpret this though an Access-Reject had been sent and MUST terminate the session. If accounting is enabled on the NAS, it MUST generate an Accounting-Request(Stop) message upon session termination.

Similarly, if a NAS conforming to this specification receives a CoA message that contains an attribute from this document that it does not recognize or cannot apply, it MUST NOT terminate the session and MUST generate a CoA-NAK packet with ERROR-CAUSE(101) set to "Unsupported Attribute"(401). If accounting is enabled on the NAS, it MUST NOT generate an Accouting-Request(Stop) message in such instances.

3. RADIUS Attributes

This specification introduces seven new RADIUS attributes.

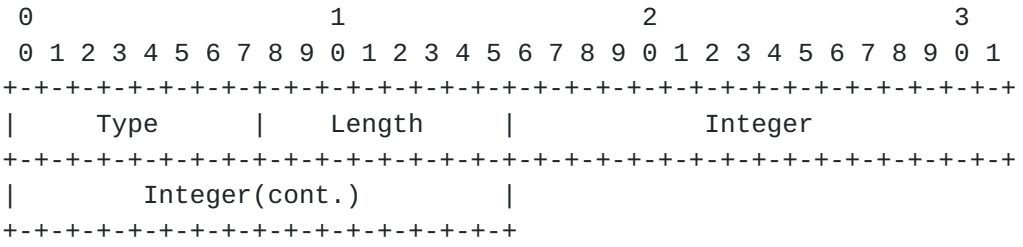
3.1. Egress-VLANID

Description

The Egress-VLANID attribute represents an allowed IEEE 802 Egress VLANID for this port. The Egress-VLANID contains two parts: the first part indicates if the VLANID is allowed for tagged or untagged packets and the second part is the VLANID.

Multiple Egress-VLANID attributes can be delivered in an authentication response; 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

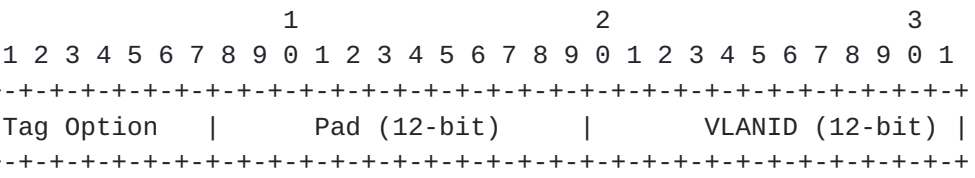
TBD

Length

6

Integer

The Integer field is four octets in length. The format of the Integer field consists of two parts, the first consuming high-order octet and the second consuming the remaining three lower-order octets. The high-order octet field indicates if the VLANID is allowed for tagged or untagged packets. The second part is the 12-bit 802.1Q VLAN VID value that has been padded out to consume the remaining three lower-order octets. A sample encoding follows:



Values for the Tag Option part include:

1 = Tagged

2 = Untagged

Padding bits SHOULD be 0 (zero).

VLANID is the 12-bit 802.1Q-2003 VID value.

3.2. 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-Accept or CoA-Request; this attribute MUST NOT be sent within an Access-Request, Access-Challenge, Access-Reject, or Disconnect-Request.

Type

TBD

Length

6

Integer

The values include:

1 - Enabled
2 - Disabled

3.3. VLAN-Name

Description

Clause 12.10.2.1.3 (a) in [IEEE8021Q] describes the administratively assigned VLAN Name associated with a VLAN ID defined within an 802.1Q bridge. The VLAN-Name attribute represents an allowed VLAN for this port. It works 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 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 VLAN-Name attributes can be delivered in an authentication response; each attribute adds the named VLAN to the list of allowed egress VLANs for the port.

Type

TBD

Length

>= 4

String

The first octet of this string indicates whether the frames on the VLAN are tagged 0x01 or Untagged 0x02. The remaining octets represent the VLAN Name as defined in 802.1Q-2003 clause 12.10.2.1.3 (a). UTF-8 encoded 10646 characters are recommended, but a robust implementation SHOULD support the field as undistinguished octets.

3.4. 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.

Type

TBD

Length

10

String

The table, expressed as an 8 octet string, maps the incoming priority (if one exists - the default is 0) into one of seven regenerated priorities. The format of this attribute is an eight byte octet string, where 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 8021D] specification, Annex G, provides a useful description of traffic type - traffic class mappings.

3.5. NAS-Filter-Rule

Description

The NAS-Filter-Rule attribute is derived from the Diameter IPFilterRule and enables the provisioning of base encapsulation (Layer 2), Internet Protocol (Layer 3-4), and HTTP (Layer 5+)

filter rules and Internet Protocol and HTTP redirect rules on the NAS by the RADIUS server.

When specifying a base encapsulation filter rule, NAS-Filter-Rule processes packets based on the following information that is associated with it:

Direction	(in and/or out)
Base encapsulation type	
Source and destination MAC address	(possibly masked)

When specifying an Internet Protocol filter or tunnel rule, NAS-Filter-Rule processes packets based on the following information that is associated with it:

Direction	(in and/or out)
Source and destination IP address	(possibly masked)
Protocol	
Source and destination port	(lists or ranges)
TCP flags	
IP fragment flag	
IP options	
ICMP types	

When specifying an HTTP filter or redirect rule, NAS-Filter-Rule process packets based on the following information that is associated with it:

HTTP URL	
Source and destination IP address	(possibly masked)

It should be noted that an HTTP filter or redirect rule is only useful with plain-text HTTP and not HTTPS. Redirection or filtering of HTTPS is outside the scope of this document.

As per the requirements of RFC 2865, Section 2.3, if multiple NAS-Filter-Rule attributes are contained within an Access-Request or Access-Accept packet, they MUST be maintained in order. The attributes MUST be consecutive attributes in the packet. RADIUS proxies MUST NOT reorder NAS-Filter-Rule attributes.

The RADIUS server can return multiple NAS-Filter-Rule attributes in an Access-Accept or CoA-Request packet. Where more than one NAS-Filter-Rule attribute is included, it is assumed that the attributes are to be concatenated to form a single filter list. Furthermore, the concatenated filter list must abide to the following rules of precedence and ordering:

1) A flush rule MUST appear before all other rule types.

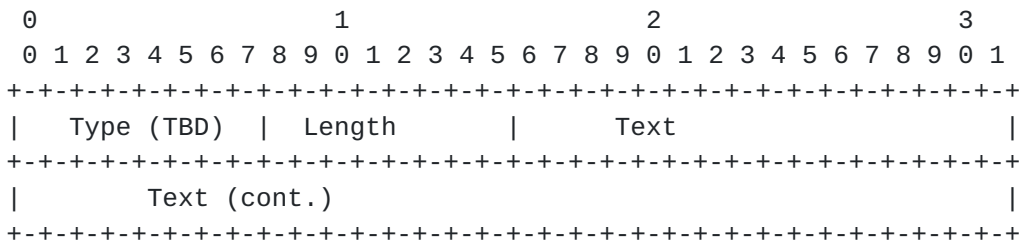
2) Base encapsulation filter rules MUST appear after a flush rule and before IP tunnel, HTTP redirect, IP filter, and/or HTTP filter rules.
3) IP tunnel rules MUST appear after any base encapsulation rules and before any HTTP redirect, IP filter, and/or HTTP filter rules
4) HTTP redirect rules MUST appear after any IP tunnel rules and before any IP filter and/or HTTP filter rules.
5) IP filter rules MUST appear after any HTTP redirect rules and before any HTTP filter rules.
6) HTTP filter rules MUST appear after any other rules.

Rules are evaluated in order, with the first matched rule terminating the evaluation. Each packet is evaluated once. If no rule matches, then packet is dropped (implicit deny all).

When an HTTP redirect rule matches, the NAS shall reply to the HTTP request with an HTTP redirect in accordance with [RFC2616] redirecting traffic to specific URL.

Filter-ID (11) and NAS-Filter-Rule both define how filters are to be applied in the NAS. Both are not intended to be used concurrently and SHOULD NOT appear in the same RADIUS message. Only one type of filtering attribute must be processed. If a Filter-ID (11) is present, then the NAS-Filter-Rule MUST be ignored, if present..

The NAS-Filter-Rule attribute is shown below. The fields are transmitted from left to right:



Type

TBD

Length

>= 3

Text

The text conforms to the following specification:

NAS-Filter-Rule MUST follow the general format:

action [args] dir proto from src to dst [options]

action

permit - Allow packets that match the rule.

deny - Drop packets that match the rule.

redirect - Redirect packets that match the rule.

tunnel - Tunnel packets that match the rule.

flush - Remove all previously assigned filter rules. When flush is specified, it can be followed by other NAS-Filter attributes. This allows for an atomic change of authorization with a single RADIUS message.

args <[redir_cnt] redir_URL|tunnel_id>

For HTTP redirect rules:

redir_cnt Specifies the number of redirect rule matches that should transpire before removing this rule from the active rule set. Upon removal from the active rule set, traffic is no longer evaluated against this rule.

redir_URL An HTTP URL. When the 'redirect' rule matches (src/dst), HTTP requests are redirected to redir_URL address in accordance with [RFC2616] redirection traffic to specific URL.

For IP tunnel rules:

tunnel_id A tunnel id. When the 'tunnel' rule matches, traffic is redirected over the tunnel with the specified tunnel_id. Traffic can only be redirected to or from named tunnels that have been established per [RFC2868] and named

using the Tunnel-Assignment-ID attribute described therein.

dir "in" is from the terminal, "out" is to the terminal, "inout" is from and to the terminal.

proto <l2:<ether2[:val]|rmon_str>> type[:val]|ipprot|ip|http>

For base encapsulation filter rules:

"l2" Prefix on any base encapsulation rule to designate as rule as such.

"ether2" keyword means any Ethernet-II (DIX Ethernet) will match.

ether2:val Used to specify an Ethernet-II type by hexadecimal number, whereby "val" is replaced by desired number. Example: "l2:ether2:0x800" for IP ethertype (0x0800).

"rmon_str" Used to specify base encapsulation per the octet string format defined in [RFC2895], section 4.2. Example: "l2:0.0.0.2.0.0.0.240" for Netbios over LLC.

For IP filter or tunnel rules:

"ip" keyword means any IP protocol will match.

ipprot An IP protocol specified by number.

For HTTP filter or redirect rules:

"http" keyword used to designate rule as of http type.

src, dst <address/mask> [ports]

For base encapsulation filter rules of "l2:ether2" type, <address/mask> may be specified as:

macaddr An Ethernet MAC address with octet values separated by a "-". Example: "00-10-A4-23-19-C0".

macaddr/mask An Ethernet number as above with a mask width of the form "00-10-A4-23-19-C0/24". In this case, all MAC addresses from 00-10-A4-00-00-00 to 00-10-A4-FF-FF-FF will match. The MAC address MUST NOT have bits set beyond the mask. The keyword "any" is 00-00-00-00-00-00/0.

The sense of the match can be inverted by preceding an address with the not modifier

(!), causing all other addresses to be matched instead.

Note: macaddr nor macaddr/mask argument is not used for "l2:rmon" type rules. Also, [ports] optional argument not valid for MAC filter rules.

For IP filter or tunnel rules, the <address/mask> may be specified as:

ipno An IPv4 or IPv6 number in dotted-quad or canonical IPv6 form. Only this exact IP number will match the rule.

ipno/bits An IP number as above with a mask width of the form 1.2.3.4/24. In this case, all IP numbers from 1.2.3.0 to 1.2.3.255 will match. The bit width MUST be valid for the IP version and the IP number MUST NOT have bits set beyond the mask. For a match to occur, the same IP version MUST be present in the packet that was used in describing the IP address. To test for a particular IP version, the bits part can be set to zero. The keyword "any" is 0.0.0.0/0 or the IPv6 equivalent. The keyword "assigned" is the address or set of addresses assigned to the terminal. For IPv4, a typical first rule is often "deny in ip !assigned"

The sense of the match can be inverted by preceding an address with the not modifier (!), causing all other addresses to be matched instead. This does not affect the selection of port numbers.

With the TCP, UDP and SCTP protocols, optional ports may be specified as:

{port/port-port}[,ports[,...]]

The '-' notation specifies a range of ports (including boundaries). Fragmented packets that have a non-zero offset (i.e., not the first fragment) will never match a rule that has one or more port specifications. See the frag option for details on matching fragmented packets.

options

For all rule types other than 'flush', there is an optional argument that can be specified:

Cnt Increments rule hit counter by one every time a packet matches on rule. Counters start with a zero value at session start and are reset back to a zero value every time an authorization change occurs due to a CoA message.

For IP filter or tunnel rules, there are several optional arguments that can be specified:

frag Match if the packet is a fragment and this is not the first fragment of the datagram. frag may not be used in conjunction with either tcpflags or TCP/UDP port specifications.

ipoptions spec

Match if the IP header contains the comma separated list of options specified in spec. The supported IP options are:

ssrr (strict source route), lsrr (loose source route), rr (record packet route) and ts(timestamp). The absence of a particular option may be denoted with a '!'.

tcpoptions spec

Match if the TCP header contains the comma separated list of options specified in spec. The supported TCP options are:

mss (maximum segment size), window (tcp window advertisement), sack (selective ack), ts (rfc1323 timestamp) and cc (rfc1644 t/tcp connection count). The absence of a particular option may be denoted with a '!'.

established

TCP packets only. Match packets that have the RST or ACK bits set.

setup TCP packets only. Match packets that have the SYN bit set but no ACK bit.

tcpflags spec

TCP packets only. Match if the TCP header contains the comma separated list of flags specified in spec. The supported TCP flags are:

fin, syn, rst, psh, ack and urg. The absence of a particular flag may be denoted with a '!'. A rule that contains a tcpflags specification can never match a fragmented packet that has a non-zero offset. See the frag option for details on matching fragmented packets.

icmptypes types
ICMP packets only. Match if the ICMP type is in the list types. The list may be specified as any combination of ranges or individual types separated by commas. Both the numeric values and the symbolic values listed below can be used. The supported ICMP types are:

echo reply (0), destination unreachable (3), source quench (4), redirect (5), echo request(8), router advertisement (9), router solicitation (10), time-to-live exceeded (11), IP header bad (12), timestamp request (13), timestamp reply (14), information request (15), information reply (16), address mask request (17) and address mask reply (18).

Concise syntax statements for each rule type follow:

A NAS-Filter-Rule expressing a flush of all rules MUST follow the syntax:

<flush>

A NAS-Filter-Rule expressing an base encapsulation filter rule MUST follow the syntax:

<permit|deny> <in|out|inout> <l2:<ether2[:val]|rmon_str>> from <address/mask> to <address/mask> [options]

A NAS-Filter-Rule expressing an IP tunnel or filter rule MUST follow the syntax:

<permit|deny|redirect <tunnel <tunnel_id>> <in|out|inout>
<ip|ip_proto> from <address/mask> to <address/mask> [ports]
[options]

A NAS-Filter-Rule expressing a HTTP redirect or filter rule MUST follow the syntax:

<permit|deny|redirect> [redir_cnt] <redir_URL> <in|out|inout>
from <address/mask> to <address/mask> [options]

A NAS that is unable to interpret or apply a deny rule MUST terminate the session. A NAS MAY apply deny rules of its own before the supplied rules, for example to protect the access device owner's infrastructure.

3.6. QoS-Filter-Rule

Description

The QoS-Filter-Rule attribute enables the provisioning of QoS filters on the NAS by the RADIUS server. The QoS-Filter-Rule attribute is defined as follows:

Type

TBD

Length

>=3

Text

The Text field contains a QoS filter, utilizing the syntax defined for the QoSFilterRule derived data type defined in [RFC3588], Section 4.3. Note that this definition contained an error, so that the complete syntax is described in the definition of the QoS-Filter-Rule AVP, defined in [NASREQ].

[Editorial: Is there a need to mention the possibility for attribute fragmentation. Dave N. to provide RFC reference that talks about the fragmentation of an AVP >256 over multiple RADIUS attributes]

The RADIUS server can return multiple QoS-Filter-Rule attributes in an Access-Accept or CoA-Request packet. Where more than one QoS-Filter-Rule Rule attribute is included, it is assumed that the attributes are to be concatenated to form a single QOS filter.

Whereas the maximum allowable message size in [NASREQ] is greater than RADIUS' maximum allowable message size, it is assumed that QOS filters that exceed RADIUS' allowable message size will be broken into multiple QoS-Filter-Rule attributes by the RADIUS server and concatenated back into a single QOS filter by the NAS.

As per the requirements of RFC 2865, Section 2.3, if multiple QoS-Filter-Rule attributes are contained within an Access-Request or Access-Accept packet, they MUST be maintained in order. The attributes MUST be consecutive attributes in the packet. RADIUS proxies MUST NOT reorder QoS-Filter-Rule attributes.

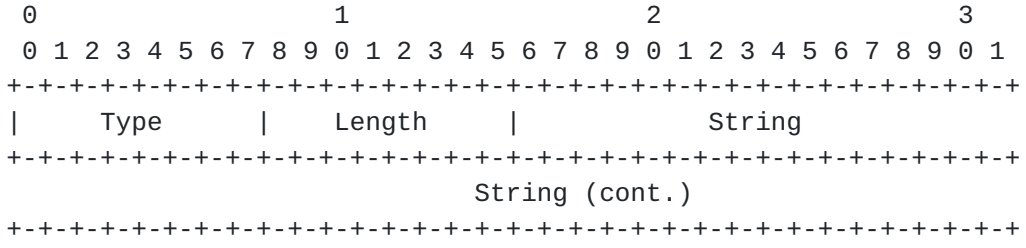
4. RADIUS Accounting

4.1. Acct-NAS-Filter-Rule

Description

Acct-NAS-Filter-Rule enables a RADIUS client to include NAS-Filter-Rule[TODO] rule match counters as part of the accounting message.

The Acct-NAS-Filter-Rule attribute is shown below. The fields are transmitted from left to right:



Type

TBD

Length

>=3

String

The first eight octets of this string are used for a 64-bit value of the rule counter. The remaining octets are used to specify which filter rule the counter value is for. The rule

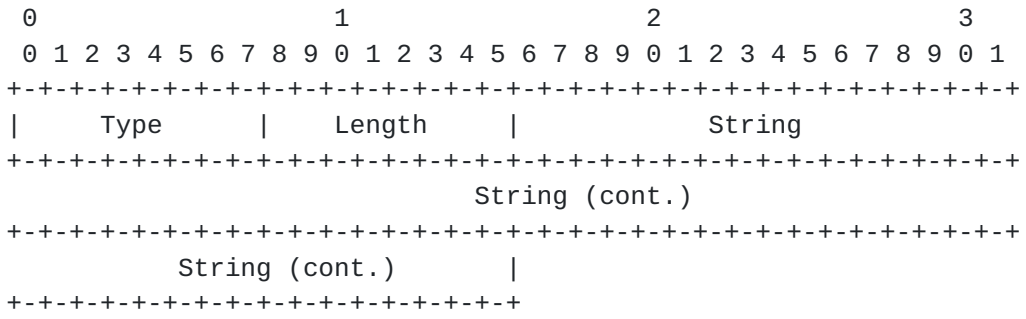
specification MUST conform to the syntax rules specified for NAS-Filter-Rule[TODO].

4.2. Acct-EAP-Auth-Method

Description

Acct-EAP-Auth-Method enables a RADIUS client to include the EAP method utilized within an accounting packet. The semantics of this attribute are identical to that of the Acct-EAP-Auth-Method AVP defined in [DiamEAP], Section 4.1.5. This is a standard RADIUS attribute.

The Acct-EAP-Auth-Method attribute is shown below. The fields are transmitted from left to right:



Type

TBD

Length

10

String

The Value field is eight octets. In case of expanded types defined in [RFC3748] Section 5.7, the least significant 32 bits contain the Vendor-Type field, and the next 24 bits contain the Vendor-Id field and 8 bits reserved data, which SHOULD be zero.

5. 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	0-1	0	0	0-1	TBD	Ingress-Filters
0	0-1	0	0	0-1	TBD	User-Priority-Table
0	0+	0	0	0+	TBD	NAS-Filter-Rule
0	0+	0	0	0+	TBD	QoS-Filter-Rule

Actng-Request	Actng-Response	#	Attribute
0-1	0	TBD	Acct-NAS-Filter-Rule
0-1	0	TBD	Acct-EAP-Auth-Method

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

0	This attribute MUST NOT be present in 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.

6. IANA Considerations

This document uses the RADIUS [RFC2865] namespace, see <http://www.iana.org/assignments/radius-types>. Allocation of seven 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 - User-Priority-Table
TBD - NAS-Filter-Rule
TBD - QoS-Filter-Rule
TBD - Acct-NAS-Filter-Rule
TBD - Acct-EAP-Auth-Method

7. 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], [RFC3576], [RFC3579], and [RFC3580].

Vulnerabilities include:

Packet modification or forgery
Dictionary attacks
Known plaintext attacks
Key management issues

7.1. Packet Modification or Forgery

As noted in [RFC3580], when used with IEEE 802.1X, all RADIUS packets MUST be authenticated and integrity protected. In addition, as described in [RFC3579], 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.

7.2. 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 non-null transform in order to encrypt the RADIUS conversation, as described in [RFC3579], Section 4.2.

7.3. 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 non-null transform, as described in [RFC3579], Section 4.2. In addition, the same RADIUS shared secret MUST NOT used for both IEEE 802.1X authentication and PAP authentication.

8. References

8.1. Normative references

[RFC1321] Rivest, R. and S. Dusse, "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

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

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach P., Berners-Lee T., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

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

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC2867] Zorn, G., Mitton, D. and B. Aboba, "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.

[RFC2895] Bierman, A., Bucci, C., Iddon, R., "Remote Network Monitoring MIB Protocol Identifier Reference", RFC 2895, August 2000

[RFC3162] Aboba, B., Zorn, G. and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[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.

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

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

[IEEE8021X]
IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004, August 2004.

[IEEE802.11i]
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.

8.2. Informative references

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

[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.

[IEEE8021D]
IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, IEEE Std 802.1D-2004, June 2004.

[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.

Appendix A - Traffic Redirection

There are several ways to redirect the user's traffic. Which method will be used depends on the capabilities available at the NAS and Service Provider's preference. This Appendix describes various methods to redirect user traffic by using the new attributes outlined in this document in conjunction with existing attributes, which are:

1) Tunneling; and
2) HTTP Redirection;

For each method we describe how redirection is done at service initiation and mid-session. We also describe how redirection is removed when it is no longer desired.

A.1 Tunneling

User traffic can be redirected by tunneling the user's traffic to an alternate location. Tunneling will typically redirect all of the user's traffic for the Service. When tunneling is used to redirect all the traffic, then filtering may not be necessary.

A.1.1 Service Initiation

Redirect using tunnels at service initiation requires that the RADIUS server send the appropriate [RFC2868] tunnel attributes and NAS-Filter-Rule attributes to the NAS. The [RFC2868] tunnel attributes describe the tunnel endpoint and the type of tunnel to construct. The "tunnel <tunnel_id>" option for the NAS-Filter-Rule allows the specification of a traffic rule for which to redirect traffic to a named tunnel.

A.1.2 Mid-session Tunnel Redirection

Redirection of traffic using tunnels mid-session involves sending the tunnel attributes as per [RFC2868] to the NAS using Change-of-Authorization (CoA) message. The operation is described in [RFC3576]. Careful attention should be paid to the security issues in [RFC3576].

Note that if the session is already tunneled (eg. Mobile-IP) then the CoA message with a new tunnel specification can be sent to the NAS or alternatively the redirection can occur at the tunnel endpoint (the Home Agent) using any one of these methods.

A.1.3 Tunnel Redirection Removal

If the normal mode for the session was to tunnel the session and redirection was sent to the NAS, the RADIUS Server can send the original tunnel attributes to the NAS in a CoA message. The NAS will tear down the tunnel and establish a connection back to the original tunnel endpoint.

However, if the normal mode for the session is not to use tunneling then there is a problem because RADIUS does not have a mechanism whereby it can de-tunnel. Receiving a CoA message without tunnel attributes would not have an effect on an existing tunnel. In order to de-tunnel the session, the RADIUS server has to send the NAS a CoA message with Service-Type(6) set to "Authorize-Only" causing the NAS to perform a re-Authorization. In response to the re-Authorization, the RADIUS server will send an Access-Accept packet without the tunneling information. Upon receiving the corresponding Access-Accept packet the NAS MUST apply the new authorization attributes. If these do not contain tunnel attributes, then the NAS MUST tear down the tunnel.

A.2 HTTP Redirection

Another method of redirection is at the application layer, specifically the HTTP layer. An HTTP aware NAS redirects traffic by issuing an HTTP Redirect response causing the users browser to navigate to an alternate Web Portal.

The same NAS-Filter-Rule(TBD) attribute described above is used to convey the redirection rules to use for HTTP redirection. HTTP redirection rules within the NAS-Filter-Rule attribute supports the encoding of a redirection URL to apply when a rule is matched.

A.2.1 Service Initiation

As with previous call flows, the RADIUS MAY send multiple HTTP redirect or filtering rules within a NAS-Filter-Rule(TBD) attribute to the NAS in the Access-Accept message.

A.2.2 Mid-session HTTP Redirection

If HTTP redirection is required to be applied to a service that has already been started then the RADIUS server can push the redirection rules, and optionally the filter rules, to the NAS within a NAS-Filter-Rule(TBD) attribute using a CoA message. The NAS will then commence to apply the redirection rules and/or the filter rules.

Alternatively, the RADIUS server can request that the NAS re-authorize the session using the procedures defined in [RFC3576]. The RADIUS server responds with an Access-Accept message (with Service-Type(6) set to "Authorize Only" that will contain the redirection and optionally filtering rules within a NAS-Filter-Rule(TBD) attribute.

A.2.3 HTTP Redirection Removal

The RADIUS serve can turn HTTP redirection off mid-session in two way. It can push new redirection rules within a NAS-Filter-Rule(TBD) attribute using a CoA message or it can send the NAS a CoA message requesting it to re-authorize.

When using CoA message to return the redirection and filtering back to "normal," there needs to be either a filter rule (or filter-id) or redirection rule that corresponds to the "normal" state. If normally the session did not have any filter and or redirection rules applied, the RADIUS server can send a NAS-Filter-Rule(TBD) with the action of "flush" in the CoA message. This action will cause all the filter rules and redirection rules previously assigned to the session to be removed.

A.3 Accounting

Every time a session is redirected and every time the redirection is reverted back a new session is created and the old one is terminated. Therefore the NAS MUST generate and Accounting-Request(Stop) for the old session and an Accounting-Request(Start) for the new session.

A.4 Example Scenarios

The following two examples illustrate the user's experience when being redirected.

For the first example assume an IEEE 8021X environment, whereby a user connects to the enterprise LAN and initiates an authentication handshake. As part of the overall authentication process, it is also possible to pass endpoint state such as patch level, virus signature status, etc., all of which can be verified by a back-end server for policy compliancy and alter the authentication and authorization decision. In instances that an end-host is not in compliancy, the NAS may be instructed to limit network access in some fashion (i.e. quarantine) and limit network access to remediation services and a web-based information site. A user may sense degraded network performance and open a web session, which the NAS would redirect to the web-based information site for compliancy status, remediation actions, etc.

For the second example assume an ISP environment, whereby a prepaid user is roaming the net in their hotel room over WiFi is to be Hot-lined because their account has no more funds. The user's Service Provider instructs the NAS to block all traffic, and redirect any port 80 traffic to the Service Provider's Prepaid Portal. Upon detecting that there is no service, the user launches his browser and regardless of which web site is being accessed the browser traffic will arrive at the Prepaid Portal which will then return a page back to the subscriber indicating that he needs to replenish his account.

Acknowledgments

The authors would like to acknowledge Dorothy Stanley of Agere, 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

Avi Lior
Bridgewater Systems Corporation
303 Terry Fox Drive
Suite 100
Ottawa, Ontario K2K 3J1
Canada

Phone: (613) 591-6655
EMail: avi@bridgewatersystems.com
URI: TCP://.bridgewatersystems.com/

Farid Adrangi
Intel Corporation
2111 North East 25th
Hillsboro, Oregon 97124
United States

Phone: (503) 712-1791
EMail: farid.adrangi@intel.com

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

any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

Disclaimer of Validity

Copyright Statement