RADIUS-Based Policing

First Published: June 25, 2009
Last Updated: November 24, 2010

The RADIUS-Based Policing feature enables the router that is acting as the Intelligent Services Gateway (ISG) to make automatic changes to the policing rate of specific sessions and services.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for RADIUS-Based Policing" section on page 16.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS XE software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for RADIUS-Based Policing

You must configure all traffic classes on the ISG before referencing the classes in policy maps.

You must configure and apply QoS policy maps on the ISG before the ISG can construct and apply an ANCP-based dynamic service policy.

Restrictions for RADIUS-Based Policing

Per-service policing cannot be configured on the class-default class at the parent level of a hierarchical policy. You can configure per-service policing on class-default classes at the child or grandchild level.

Transient policies are not visible in the running-configuration file. Only the original policy configuration is visible.

Parameterized QoS is not supported for IP sessions.

The parameterized Access Control List (pACL) name is limited to 80 characters. The pACL name is formed by concatenating the ACL entries in the RADIUS CoA or Access-Accept message to the ACL name configured on the ISG. If the pACL name exceeds 80 characters the parameterization operation fails and an error message displays. For a CoA message, the ISG also sends a negative Ack (Nack) response to the RADIUS server.

The RADIUS-Based Policing feature is supported only on PPP Termination and Aggregation (PTA) sessions in Cisco IOS Release XE 3.1 and earlier releases; it is supported on L2TP access concentrator (LAC) or L2TP network server (LNS) sessions in Cisco IOS Release XE 3.2 and later releases.

If there is a concatenated service-activation push, QoS policies are applied first and then service activation occurs. If a concatenated service activation fails, any QoS policies applied are not rolled back.

Information About RADIUS-Based Policing

To configure the RADIUS-based policing features supported on the Cisco ASR 1000 Series Aggregation Services Router, you should understand the following topics:

- RADIUS Attributes, page 2
- Parameterized QoS Policy as VSA 1, page 5
- Parameterization of QoS ACLs, page 5

RADIUS Attributes

RADIUS communicates with the ISG device by embedding specific attributes in Access-Accept and change of authentication (CoA) messages. RADIUS-based policing employs this exchange of attributes to activate and deactivate services and to modify the active quality of service (QoS) policy applied to a session.

The following sections describe the RADIUS attributes used in RADIUS-based policing:

- RADIUS Attributes 250 and 252, page 3
- Cisco VSA 1, page 3

RADIUS Attributes 250 and 252

RADIUS uses attribute 250 in Access-Accept messages and attribute 252 in CoA messages to activate and deactivate parameterized services. ISG services are configured locally on the ISG device; RADIUS sends only the service name.

Attributes 250 and 252 have the following syntax for service activation:

Access-Accept Messages

```
250 "Aservice(parameter1=value,parameter2=value,...)"
```

CoA Messages

```
252 0b "service(parameter1=value,parameter2=value,...)"
```

RADIUS uses only Attribute 252 in a CoA message when deactivating a service. RADIUS sends the same information in Attribute 252 that was used for service activation, except that service deactivation uses 0c in the syntax instead of the 0b parameter used for service activation.

CoA Messages

```
252 0xC "service(parameter1=value,parameter2=value,...)"
```

VSA 252 has the above syntax for service deactivation.

Cisco VSA 1

RADIUS uses a vendor-specific attribute (VSA) 1 command to modify the active QoS policy on a session. This VSA has the following format:

```
av-pair = "policy-type=command 9 parameter1 ,...,parametern"
```

Use the following Cisco VSA 1 format to add and remove classes and QoS actions to and from the QoS policy that is currently active on a session:

```
qos-policy-in=add-class(target,(class-list),qos-actions-list)
qos-policy-out=add-class(target,(class-list),qos-actions-list)
qos-policy-in=remove-class(target,(class-list))
qos-policy-out=remove-class(target,(class-list))
```

Before the ISG can construct a policy using the policing parameters specified in the RADIUS message, a QoS policy must be active on the session. If a QoS policy is not active in the specified direction, the ISG does not create the policy.

When implementing the changes specified in the Cisco VSA, the ISG does not make the changes to the originally configured QoS policy on the ISG device. Instead, the ISG copies the active QoS policy for the session and then makes the required changes to the policy copy, which is referred to as a *transient policy*. The originally configured QoS policy on the ISG device is not changed.

The following sections describe the Cisco VSA 1 commands used to automatically modify policing parameters of active policies:

- Add-Class Primitive, page 3
- Remove-Class Primitive, page 5

Add-Class Primitive

To add or modify QoS actions to a traffic class, use the add-class primitive. This attribute has the following format:

```
qos-policy-in=add-class(target,(class-list),qos-actions-list)
qos-policy-out=add-class(target,(class-list),qos-actions-list)
```

- *target* field— indicates the QoS policy to be modified. Currently, the only valid value for this field is **sub**, which indicates the active QoS policy attached to the subscriber session. The Access-Accept or CoA message that includes this attribute must be targeting a subscriber session.
- *class-list* field—A list of class names enclosed in parentheses that identifies the traffic class to which the specified QoS action applies. The class names you specify must be either user-configured class maps or the system-generated class-default class. The order in which you specify the class names indicates the hierarchical level of the class within the QoS policy.

For example, the following class list identifies the class named "voip", which gets added to a nested policy. The VoIP class is configured in a nested child policy that is applied to the parent class-default class.

```
(class-default, voip)
```

ISG Configuration

```
policy-map child
    class voip
        police 8000

policy-map parent
    class class-default
        service-policy child
```

The following class list specifies the voip-2 class, which is configured in a nested policy that is applied to the voip-aggregate class of another nested child policy. The policy containing the voip-aggregate class is in turn nested under the class-default class of the QoS policy attached to the target session.

```
(class-default, voip-aggregate, voip-2)
```

MSQ Configuration

```
policy-map child2
    class voip-2
        police 8000

policy-map child1
    class voip-aggregate
        police 20000
        service-policy child2

policy-map parent
    class class-default
        shape 512000
        service-policy child1
```

The *qos-actions-list* field indicates a QoS action such as police, followed by the action parameters enclosed in parentheses and separated by commas. For example, the following sample configuration specifies the police action and defines the parameters *bps*, *burst-normal*, *burst-max*, *conform-action*, *exceed-action*, and *violate-action*. Parentheses enclose the action parameters.

```
(voip-aggregate police(200000,9216,0,transmit,drop,drop))
```

Note The example above shows a double-parenthesis at the end, because the syntax of the VSA specifies enclosure of the target, class-list, and qos-actions-list in parentheses.

Remove-Class Primitive

To remove traffic classes and QoS actions defined in the active QoS policy on a session, use the remove-class primitive. This attribute has the following format:

```
qos-policy-in=remove-class(target,(class-list))
qos-policy-out=remove-class(target,(class-list))
```

- *target* field—Indicates the QoS policy to be modified. Currently, the only valid value for this field is sub, which indicates the active QoS policy attached to the subscriber session. The Access-Accept or CoA message that includes this attribute must be targeting a subscriber session.
- *class-list* field—A list of class names enclosed in parentheses that identifies the class or classes to be removed. The class names you specify must be either user-configured class maps or the system-generated class-default class. The order in which you specify the class names indicates the hierarchical level of the class within the QoS policy.

For example, the following VSA1 attribute removes the Bronze class and all associated QoS policy actions from the nested child policy that is applied to the parent class-default class:

```
qos-policy-out=remove-class(sub,(class-default,Bronze))
```

When you remove a traffic class from a QoS policy, all of the attributes for the class are also removed. To re-add the class with the same attributes, you must reissue the add-class RADIUS attribute and provide the required parameters and values.

Parameterized QoS Policy as VSA 1

In the current release, multiple complex strings in a CoA message are not supported because they do not display correct behavior of VSA 1, as shown in the next example:

```
vsa cisco 250 S152.1.1.2
vsa cisco generic 252 binary 0b suffix "q-p-out=IPOne1-isg-acct1(1)((c-d,tv)1(10000))"
vsa cisco generic 252 binary 0b suffix "q-p-out=IPOne1-isg-acct(1)((c-d,voip)1(10000))"
```

In the above example:

- All services are enabled on target.
- Parameterized QoS policy in the second command syntax is not echoed in the ISG service.
- Parameterized QoS policy in the first command syntax is echoed.

Parameterization of QoS ACLs

The Parameterization of QoS Access Control Lists (ACLs) feature supports multiple ISG and QoS parameterized services in a single Access-Accept or CoA message. This feature allows the authentication, authorization, and accounting (AAA) device to change parameters dynamically.

How to Configure RADIUS-Based Policing

The RADIUS server determines the new policing rate based on vendor specific attributes (VSAs) configured in a subscriber's user profile on RADIUS and on the ANCP-signaled rate received from the ISG. RADIUS sends the new rate to the ISG in an Access-Accept or CoA message.

After receiving the Access-Accept or CoA message, the ISG copies the original policy map applied to the session and changes the policing rate of the copied, transient policy as indicated by RADIUS. The ISG does not change the shaping rate of the original policy. After changing the transient policy, the ISG applies the transient policy to the subscriber service.

This section contains the following tasks:

- Configuring Per-Service Policing Using RADIUS, page 6
- Verifying RADIUS-Based Policing, page 10

Configuring Per-Service Policing Using RADIUS

To configure per-service policing, perform the following configuration tasks:

- Configuring a Hierarchical QoS Child Policy with Policing, page 6
- Configuring a Hierarchical QoS Parent Policy with Policing, page 8
- Configuring Per-Service Policing on the RADIUS Server, page 9

Configuring a Hierarchical QoS Child Policy with Policing

Use the following procedure to configure a hierarchical QoS Child policy with policing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-name*
5. **shape average** *mean-rate* [[*burst-size*] [*excess-burst-size*]] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*]
6. **police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]
7. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

	Command	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map child`	Creates or modifies a policy map and enters policy-map configuration mode. • *policy-map-name* is the name of the policy map.
Step 4	**class** *class-name* **Example:** `Router(config-pmap)# class voip`	Configures QoS parameters for the traffic class you specify and enters policy-map class configuration mode. • *class-name* is the name of a traffic class you previously configured using the **class-map** command.
Step 5	**shape average** *mean-rate* [[*burst-size*] [*excess-burst-size*]] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*] **Example:** `Router(config-pmap-c)# shape average 10000`	Shapes traffic to the indicated bit rate. • **average** is the maximum number of bits sent out in each interval. Available only on the PRE3. • *mean-rate* is the committed information rate (CIR) in bits per second.
Step 6	**police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*] **Example:** `Router(config-pmap-c)# police 10000`	Configures traffic policing. • *bps* is the average rate in bits per second. Valid values are 8000 to 200000000. • (Optional) *burst-normal* is the normal burst size in bytes. Valid values are 1000 to 51200000. The default normal burst size is 1500 bytes. • (Optional) *burst-max* is the excess burst size in bytes. Valid values are 1000 to 51200000. • **conform-action** *action* is the action to take on packets that conform to the rate limit. • **exceed-action** *action* is the action to take on packets that exceed the rate limit. • (Optional) **violate-action** *action* is the action to take on packets that violate the normal and maximum burst sizes.

	Command	Purpose

Step 7	`exit`
	
	Example:
	`Router(config-pmap-c)# exit`
		Exits policy-map class configuration mode.
		
		Note Repeat steps 1 through 5 for each child policy map you want to create, or repeat steps 2 through 5 for each traffic class you want to define in each policy map. Specify either the **shape** command or the **police** command for a traffic class, but not both commands for the same class. You may also specify other commands for each traffic class such as the **priority**, **set precedence**, and **random-detect** commands. For more information on the commands you can specify for a traffic class, see the *Cisco 10000 Series Router Quality of Service Configuration Guide.*

Police Command Actions

The following are keywords you can use to specify actions in the **police** command:

- **drop**—Drops the packet.
- **set-cos-transmit** *value*—Sets the packet COS value and sends it.
- **set-discard-class-transmit** *value*—Sets the discard class attribute of a packet.
- **set-dscp-transmit** *value*—Sets the IP differentiated services code point (DSCP) value.
- **set-frde-transmit** *value*—Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame.
- **set-mpls-experimental-imposition-transmit** *value*—Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits (0 to 7) in the imposed label headers.
- **set-mpls-experimental-topmost-transmit** *value*—Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces.
- **set-prec-transmit** *value*—Sets the IP precedence value.
- **set-qos-transmit** *value*—Sets the QoS group value.
- **transmit**—Transmits the packet. The packet is not altered.

Configuring a Hierarchical QoS Parent Policy with Policing

Use the following procedure to configure a hierarchical QoS Parent policy with policing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class class-default**
5. **shape average** *mean-rate* [[*burst-size*] [*excess-burst-size*]] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*]
6. **service-policy** *policy-map-name*

7. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config-pmap)# policy-map parent`	Creates or modifies a policy map. • *policy-map-name* is the name of the policy map.
Step 4	**class class-default** **Example:** `Router(config-pmap)# class class-default`	Modifies the class-default traffic class and enters policy-map class configuration mode.
Step 5	**shape average** *mean-rate* [[*burst-size*] [*excess-burst-size*]] [**account** {**qinq** | **dot1q** | **user-defined** *offset*} **aal5** *subscriber-encap*] **Example:** `Router(config-pmap-c)# shape average 10000`	Shapes traffic to the indicated bit rate. • **average** is the maximum number of bits sent out in each interval. Available only on the PRE3. • *mean-rate* is the committed information rate (CIR) in bits per second.
Step 6	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy child`	Applies the child policy map to the parent class-default class. • *policy-map-name* is the name of the child policy map.
Step 7	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.

Configuring Per-Service Policing on the RADIUS Server

To use RADIUS to set the policing rate for a subscriber service, configure the following Cisco VSAs in the service profile on RADIUS:

```
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-list), shape(rate))"
vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-list), police(rate))"
```

When the ISG receives a RADIUS Access-Accept or change of authentication (CoA) message with these VSAs included, the ISG copies the originally configured policy map that is active on the session and changes the policing rate of the traffic class specified in the class-list field. The ISG makes changes only to the transient policy and applies the transient policy to the subscriber service; no changes are made to the original policy map.

Note Per-service policing does not apply to the parent class-default class.

For more information, see the "RADIUS Attributes" section on page 2.

Verifying RADIUS-Based Policing

To verify the configuration of RADIUS-based policing on the ISG, use any of the following commands in privileged EXEC mode.

Command	Displays
`Router# show policy-map interface`	The configuration of all classes configured for all policy maps attached to all interfaces. Also displays the serviced default policy map.
`Router# show policy-map interface` *interface* `[input | output]`	The configuration of all classes configured for all inbound or outbound policy maps attached to the specified interface. *interface* is the name of the interface or subinterface. **input** indicates to display the statistics for the attached inbound policy. **output** indicates to display the statistics for the attached outbound policy. If you do not specify **input** or **output**, the router shows information about all classes that are configured for all inbound and outbound policies attached to the interface you specify.
`Router# show policy-map` *policy-map-name*	The configuration of all of the traffic classes contained in the policy map you specify. *policy-map-name* is the name of the policy map for the configuration information you want to appear. If you do not specify a *policy-map-name*, the command shows the configuration of all policy maps configured on the router.
`Router# show policy-map` *policy-map-name* `class` *class-name*	The configuration of the class you specify. The policy map you specify includes this class. *policy-map-name* is the name of the policy map that contains the class configuration you want to appear. *class-name* is the name of the class whose configuration you want to display. If you do not specify *class-name*, the router displays the configuration of all of the classes configured in the policy map.
`Router# show policy-map session [output | output |`*uid*`]`	The inbound or outbound policy maps configured per session. Also displays the dynamic policy map that is applied to the subscriber session. If you do not specify any arguments, all sessions with configured policy maps display, which might impact performance. **input** indicates inbound policy maps. **output** indicates outbound policy maps. *uid* is the session ID.

Command	Displays
`Router# show running-config`	The running-configuration file, which contains the current configuration of the router, including the default QoS policy.
`Router# show running-config interface interface`	The configuration of the interface you specify that is currently configured in the running-config file, including any service policies attached to the interface.

Configuration Examples for RADIUS-Based Policing

This section provides the following configuration examples:

Adding Parameterization of QoS ACLs: Example

The following example shows how to parameterize the set source IP address and destination IP address parameter, set-src-dst-ip-in-acl, through CoA or Access-Accept messages. The QoS parameterized service is added in the parameterized QoS service RADIUS form:

```
VSA252 0b q-p-out=IPOne(1)((c-d,voip)13(201.10.1.0/28,202.3.20/29))
! The above command activates the service in a CoA message.

vsa cisco generic 1 string
"qos-policy-out=add-class(sub,(class-default,voip),set-src-dst-ip-in-acl(10.10.1.0/28,10.3
.20/29))"
! The above command activates the service in a Access-Accept message.
```

The Cisco ASR 1000 Series Router is configured as follows:

```
ip access-list extended IPOne-acl
 remark Voice-GW
 permit ip host 10.0.1.40 any
!
class-map match-any voip
  match access-group name IPOne-acl
!
class-map type traffic match-any IPOne
 match access-group output name IPOne-acl
 match access-group input name IPOne-acl
 !
!
policy-map type service IPOne
 10 class type traffic IPOne
  accounting aaa list default
 !
!
policy-map output_parent
  class class-default
    police 32000 32000 32000 conform-action transmit exceed-action drop violate-action
drop
  service-policy output_child
  !
!
```

```
policy-map output_child
  class voip
    police 32000 32000 32000 conform-action transmit exceed-action drop violate-action
drop
    !
  !
!
! RADIUS relays the string for service activation. After the VSA is received, a new ACL is
created.
ip access-list extended IPOne-acl-10.10.1.0/28,10.3.20/29
 remark Voice-GW
 permit ip host 10.0.1.40 any
 permit ip 10.10.1.0 0.0.0.15 any
 permit ip any 10.10.1.0 0.0.0.15
 permit ip 10.3.2.0 0.0.0.7 any
 permit ip any 10.3.2.0 0.0.0.7
!
! A new class map is created.
class-map match-any voip-10.10.1.0/28,10.3.20/29
  match access-group name IPOne-acl-10.10.1.0/28,10.3.20/29
!
! The old class is replaced with the new class in the output QoS policy of the subscriber,
along with any other attributes.
```

Adding Parameterization of QoS ACLs with ISG Service accounting

The following example shows how to add QoS accounting by configuring the Intelligent Services Gateway (ISG) accounting service:

```
policy-map type service IPOne
 10 class type traffic IPOne
  accounting aaa list default
 !
 class type traffic default in-out
 !
!
! After the VSA is received, a new traffic class map is created on the service.
class-map type traffic match-any IPOne-10.10.1.0/28,10.3.2.0/29
 match access-group output name IPOne-acl-10.10.1.0/28$10.3.2.0/29
 match access-group input name IPOne-acl-10.10.1.0/28$10.3.2.0/29
!
! A new ISG service is created.
policy-map type service IPOne(tc_in=IPOne-acl-10.10.1.0/28$10.3.2.0/29)
 10 class type traffic IPOne-10.10.1.0/28,10.3.2.0/29
  accounting aaa list default
 !
 class type traffic default in-out
!
```

Setting the Policing Rate Using an Access-Accept Message: Examples

The examples in this section illustrate how to set the policing rate of a traffic class using an access-accept message.

ISG Original Policy

This configuration example uses a RADIUS Access-Accept message to change the policing rate of a traffic class at the child level of a hierarchical policy.

```
class-map match-any Premium
    match access-group name Premium_Dest
!
```

```
policy-map Child
    class Premium
    shape average 5000
!
policy-map Parent
    class class-default
        shape average 10000
        service-policy Child
!
ip access-list extended Premium_Dest
permit ip any 192.168.6.0 0.0.0.255
permit ip any 192.168.5.7 0.0.0.64
```

RADIUS Configuration

The following Cisco VSA is configured in a user profile on RADIUS. This VSA changes the policing rate of the Premium class in the Child policy. The Child policy is applied to the class-default class of the Parent policy.

```
radius subscriber 6
    framed protocol ppp
    service framed
    vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default, Premium),
    police(200000))"
```

RADIUS Access-Accept Message

The ISG receives the following RADIUS Access-Accept message. Notice that the above Cisco VSA configured in the user's profile is present in the Access-Accept message.

```
1d21h: RADIUS: Received from id 1645/3 192.168.1.6:1812, Access-Accept, len 100
1d21h: RADIUS: authenticator 4A 2C F7 05 4B 88 38 64 - DE 60 69 5A 4B EE 43 E1
1d21h: RADIUS: Framed-Protocol [7] 6 PPP [1]
1d21h: RADIUS: Service-Type [6] 6 Framed [2]
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default, Premium),
police(200000))"
1d21h: RADIUS(0000000D): Received from id 1645/3
1d21h: SSS PM [uid:4][65ADE2E8]: SERVICE: Adding Service attachment to event
1d21h: RADIUS/ENCODE(0000000D):Orig. component type = PPoE
1d21h: RADIUS(0000000D): Config NAS IP: 0.0.0.0
1d21h: RADIUS(0000000D): sending
```

ISG Transient Policy

The ISG copies the service policy that is currently applied to the session and creates a transient policy named New_Parent to which it makes the appropriate changes. Based on the Cisco VSA included in the Access-Accept message, the ISG adds the policing rate to the Premium traffic class. The Premium class is configured in the transient New_Child policy, which is applied to the New_Parent class-default class.

```
policy-map New_Child                [New cloned child policy]
    class Premium
        police 200000               [New policing rate]
        shape average 5000
!
policy-map New_Parent               [New cloned parent policy]
    class class-default
        shape average 10000
        service-policy New_Child    [New cloned child policy attached to the new
                                    cloned parent policy]
```

Setting the Policing Rate Using a CoA Message: Examples

The examples in this section illustrate how to set the policing rate of a service using a CoA message.

ISG Original Policy

This configuration example uses a RADIUS CoA message to change the policing rate of a service and is based on the following ISG configuration:

```
policy-map Child
    class Premium
        police 12000
!
policy-map Parent
    class class-default
        shape average 10000
        service-policy Child
```

RADIUS Configuration

The following Cisco VSA is configured in a user's profile on RADIUS. This VSA modifies the Premium class of the Child policy, which is applied to the class-default class of the Parent policy.

```
radius subscriber 1048
    vsa cisco 250 S192.168.1.10
    vsa cisco generic 1 string "qos-policy-out=add-class(sub,(class-default, Premium),
    police(200000))"
```

RADIUS CoA Message

The ISG receives the following RADIUS CoA message. Notice that the above Cisco VSA configured in the user profile is present in the CoA message.

```
1d21h: RADIUS: COA received from id 0 192.168.1.6:1700, CoA Request, len 106
1d21h: COA: 192.168.1.6 request queued
1d21h: RADIUS: authenticator FF A2 6B 63 06 F0 E6 A3 - 0D 04 6C DC 01 0A BE F1
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.10"
1d21h: RADIUS: Vendor, Cisco [26] 68
1d21h: RADIUS: Cisco AVpair [1] 62 "qos-policy-out=add-class(sub,(class-default, Premium),
police(200000))"
1d21h: ++++++ CoA Attribute List ++++++
1d21h: 63C829B0 0 00000009 ssg-account-info(427) 10 S192.168.1.10
1d21h: 63C82A18 0 00000009 qos-policy-out(378) 45 add-class(sub,(class-default, Premium),
police(200000))
1d21h:

ISG#
1d21h: RADIUS(00000000): sending
1d21h: RADIUS(00000000): Send CoA Ack Response to 192.168.1.6:1700 id 0, len 65
1d21h: RADIUS: authenticator 62 B4 B0 1A 90 10 01 01 - F6 C8 CD 17 79 15 C7 A7
1d21h: RADIUS: Vendor, Cisco [26] 18
1d21h: RADIUS: ssg-account-info [250] 12 "S192.168.1.10"
1d21h: RADIUS: Vendor, Cisco [26] 27
1d21h: RADIUS: ssg-account-info [250] 21 "$IVirtual-Access2.2"
```

ISG Transient Policy

The ISG copies the service policy named Parent currently applied to the session and creates a transient copy named New_Parent to which it makes the appropriate changes. Based on the Cisco VSA included in the Access-Accept message, the ISG changes the policing rate of the Premium traffic class from 5000 bps to 200,000 bps. The Premium class is configured in the New_Child policy, which is applied to the New_Parent class-default class.

```
policy-map New_Child                  [New cloned child policy]
    class Premium
        police 200000                 [New policing rate]
!
policy-map New_Parent                 [New cloned parent policy]
    class class-default
        shape average 10000
        service-policy New_Child      [New cloned child policy attached to the new
                                      cloned parent policy]
```

Additional References

The following sections provide references related to the RADIUS-Based Policing feature.

Related Documents

Related Topic	Document Title
ISG commands	*Cisco IOS Intelligent Services Gateway Command Reference*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RADIUS-Based Policing

Table 1 lists the features in this module and provides links to specific configuration information. For information on a feature in this technology that is not documented here, see the Cisco IOS XE Intelligent Services Gateway Features Roadmap.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 1 Feature Information for RADIUS-Based Policing

Feature Name	Releases	Feature Information
ISG: Policy Control: Policy Server: RADIUS-Based Policing	Cisco IOS XE Release 2.4	The RADIUS-Based Policing feature extends ISG functionality to allow the use of a RADIUS server to provide subscriber policy information. In Cisco IOS XE Release 2.4, support was added for the Cisco ASR 1000 Series Router. The following sections provide information about this feature: • "Information About RADIUS-Based Policing" section on page 2 • "How to Configure RADIUS-Based Policing" section on page 6
RADIUS-Based Policing Attribute Modifications	Cisco IOS XE Release 2.4	The RADIUS-Based Policing Attribute Modifications feature allows the RADIUS server to communicate with the ISG by embedding specific attributes in Access-Accept and CoA messages. RADIUS-based shaping and policing employs this exchange of attributes to activate and deactivate services, and to modify the active QoS policy applied to a session. In Cisco IOS XE Release 2.4, support was added for the Cisco ASR 1000 Series Router. The following sections provide information about this feature: • "Information About RADIUS-Based Policing" section on page 2 • "How to Configure RADIUS-Based Policing" section on page 6

Table 1 Feature Information for RADIUS-Based Policing (continued)

Feature Name	Releases	Feature Information
Parameterization of QoS ACLs	Cisco IOS XE Release 2.4	The Parameterization of QoS ACLs feature provides enhancements for QoS ACLs. This feature allows the AAA device to change parameters dynamically. In Cisco IOS XE Release 2.4, support was added for the Cisco ASR 1000 Series Router. The following sections provide information about this feature: • "Information About RADIUS-Based Policing" section on page 2 • "How to Configure RADIUS-Based Policing" section on page 6