# Configuring ISG Policies for Regulating Network Access

Intelligent Services Gateway (ISG) is a Cisco IOS XE software feature set that provides a structured framework in which edge devices can deliver flexible and scalable services to subscribers. ISG supports the use of policies for governing subscriber session bandwidth and network accessibility. This module provides information about the following methods of regulating session bandwidth and network access: Modular Quality of Service (QoS) command-line interface (CLI) policies and ISG policing.


- Finding Feature Information, on page 1
- Information About ISG Policies for Regulating Network Access, on page 1
- How to Configure ISG Policies for Regulating Network Access, on page 3
- Configuration Examples for ISG Policies for Regulating Network Access, on page 6
- Additional References, on page 7
- Feature Information for ISG Policies for Regulating Network Access, on page 7


# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

# Information About ISG Policies for Regulating Network Access

## Methods of Regulating Network Access

ISG supports the following methods of regulating network access. Each of these methods can be applied to an ISG session and can be dynamically updated.

### Modular QoS CLI (MQC) Policies

QoS policies configured using the MQC are supported for subscriber sessions only. MQC policies cannot be applied to ISG services.

### ISG Policing

ISG policing supports policing of upstream and downstream traffic. ISG policing differs from policing configured using the MQC in that ISG policing can be configured in service profiles to support policing of traffic flows. MQC policies cannot be configured in service profiles. ISG policing can also be configured in user profiles and service profiles to support session policing.

# Overview of ISG Policing

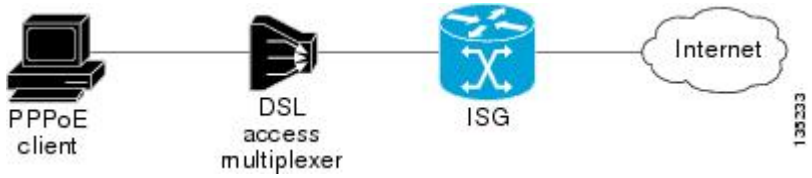
Traffic policing allows you to control the maximum rate of traffic sent or received on an interface. Policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate parameters is sent, whereas traffic that exceeds the parameters is dropped or sent with a different priority.

ISG policing supports policing of upstream and downstream traffic and can be applied to a session or a flow. The following sections describe session-based policing and flow-based policing.

### Session-Based Policing

Session-based policing applies to the aggregate of subscriber traffic for a session. In the figure below, session policing would be applied to all traffic moving from the PPPoE client to ISG and from ISG to the PPPoE client.

***Figure 1: Session-Based Policing***




Session-based policing parameters can be configured on a AAA server in either a user profile or a service profile that does not specify a traffic class. It can also be configured on the router in a service policy map. Session-based policing parameters that are configured in a user profile take precedence over session-based policing parameters configured in a service profile or service policy map.

### Flow-Based Policing

Flow-based policing applies only to the destination-based traffic flows that are specified by a traffic class. In the figure below, flow-based policing would allow you to police the traffic between the PPPoE client and Internet 1 or Internet 2.

*Figure 2: Flow-Based Policing*

Flow-based policing can be configured on a AAA server in a service profile that specifies a traffic class. It can also be configured on the router under a traffic class in a service policy map. Flow-based policing and session-based policing can coexist and operate simultaneously on subscriber traffic.

# How to Configure ISG Policies for Regulating Network Access

## Configuring ISG Policing

### Configuring Policing in a Service Policy Map on the Router

Perform this task to configure ISG policing on the router.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. [*priority*]**class type traffic** *class-map-name*
5. **police input** *committed-rate normal-burst excess-burst*
6. **police output** *committed-rate normal-burst excess-burst*

#### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **policy-map type service** *policy-map-name*<br>**Example:** | Creates or modifies a service policy map, which is used to define an ISG service. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config)# policy-map type service service1` | |
| **Step 4** | [*priority*]**class type traffic** *class-map-name*<br>**Example:**<br>`Router(config-service-policymap)# class type traffic silver` | Associates a previously configured traffic class with the policy map. |
| **Step 5** | **police input** *committed-rate normal-burst excess-burst*<br>**Example:**<br>`Router(config-service-policymap-class-traffic)# police input 20000 30000 60000` | Configures ISG policing of upstream traffic.<br>• These parameters will be used to limit traffic flowing from the subscriber toward the network. |
| **Step 6** | **police output** *committed-rate normal-burst excess-burst*<br>**Example:**<br>`Router(config-service-policymap-class-traffic)# police output 21000 31500 63000` | Configures ISG policing of downstream traffic.<br>• These parameters will be used to limit the traffic flowing from the network toward the subscriber. |

### What to Do Next

You may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

## Configuring Policing in a Service Profile or User Profile on the AAA Server

### SUMMARY STEPS

1. Do one of the following:
   - Add the following Policing vendor-specific attribute (VSA) to the user profile on the AAA server.
   - 26, 9, 250 "QU;*committed-rate*;*normal-burst*;*excess-burst*;D;*committed-rate*;*normal-burst*;*excess-burst*"
   -
   - Add the following Policing VSA to the service profile on the AAA server.

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Do one of the following:<br>• Add the following Policing vendor-specific attribute (VSA) to the user profile on the AAA server.<br>• 26, 9, 250 "QU;*committed-rate*;*normal-burst*;*excess-burst*;D;*committed-rate*;*normal-burst*;*excess-burst*" | Enables ISG policing of upstream and downstream traffic.<br>• If you specify the committed rate and normal burst, excess burst will be calculated automatically.<br>• You can specify upstream or downstream parameters first. |

| | Command or Action | Purpose |
|---|---|---|
| | • <br>• Add the following Policing VSA to the service profile on the AAA server.<br>**Example:**<br>`26,9,251 "Q;committed-rate;normal-burst;excess-burst;D;committed-rate;normal-burst;excess-burst"` | |

### What to Do Next

You may want to configure a method of activating the service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services".

## Verifying ISG Policing

Perform this task to verify ISG policing configuration.

### SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id*| **username** *name*]<br>**Example:**<br>`Router# show subscriber session detailed` | Displays ISG subscriber session information. |

### Examples

The following example shows output for the **show subscriber session** command when policing parameters have been configured in the service profile. The “Config level” field indicates where the policing parameters are configured; in this case, in the service profile.

```
Router# show subscriber session detailed
Current Subscriber Information: Total sessions 2
Unique Session ID: 1
.....
Session inbound features:
```

```
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Service
Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service
.....
```

The following example shows output for the **show subscriber session** command where upstream policing parameters are specified in a user profile and downstream policing parameters are specified in a service profile.

```
Router# show subscriber session all
Current Subscriber Information: Total sessions 2
Unique Session ID: 2
.....
Session inbound features:
Feature: Policing
  Upstream Params:
Average rate = 24000, Normal burst = 4500, Excess burst = 9000
Config level = Per-user  ===========> Upstream parameters are specified in
the user profile.
Session outbound features:
Feature: Policing
  Dnstream Params:
Average rate = 16000, Normal burst = 3000, Excess burst = 6000
Config level = Service ============> No downstream parameters in the user
profile, hence the parameters in the service profile are applied.
.....
```

# Configuration Examples for ISG Policies for Regulating Network Access

## ISG Policing Examples

### Flow-Based Policing Configured in a Service Policy Map Using the CLI

The following example shows the configuration of ISG flow-based policing in a service policy map:

```
class-map type traffic match-any C3
 match access-group in 103
 match access-group out 203
policy-map type service P3
 class type traffic C3
  police input 20000 30000 60000
  police output 21000 31500 63000
```

### Session-Based Policing Configured in a User Profile on a AAA Server

The following example shows policing configured in a user profile:

```
Cisco:Account-Info = "QU;23465;8000;12000;D;64000"
```

### Session-Based Policing Configured in a Service Profile on a AAA Server

The following example shows policing configured in a service profile:

```
Cisco:Service-Info = "QU;16000;D;31000"
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| ISG commands | Cisco IOS Intelligent Services Gateway Command Reference |
| How to configure QoS policies using the MQC | "Applying QoS Features Using MQC" module in the *Quality of Service Configuration Guide* |
| How to configure DBS | "Controlling Subscriber Bandwidth" module in the *Broadband Access Aggregation and DSL Configuration Guide* |

### 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.<br>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.<br>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 ISG Policies for Regulating Network Access

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

*Table 1: Feature Information for Policies for Regulating Network Access*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| ISG: Flow Control: QoS Control: Dynamic Rate Limiting | Cisco IOS XE Release 2.2 | ISG can change the allowed bandwidth of a session or flow by dynamically applying rate-limiting policies. |