CONTENTS

Per-Session QoS 1
Finding Feature Information 1
Prerequisites for Per-Session QoS 1
Restrictions for Per-Session QoS 2
Restrictions for Per-Session QoS (Cisco 7600 Series Routers) 2
Information About Per-Session QoS 4
Benefits of Per-Session QoS 4
Policy Maps and QoS Features 5
Hierarchical Policy Maps 5
Per-Session QoS and Virtual Templates 5
Per-Session QoS and the ISG Framework 6
Cisco AV Pairs and VSAs 6
How to Configure Per-Session QoS 6
Configuring Per-Session QoS Using a RADIUS Server 7
Adding the Cisco QoS AV Pairs to the Service Profile on the RADIUS Server 7
Prerequisites 7
Defining an ISG Policy Map to Start the QoS Service on the RADIUS Server 8
Reviewing Session Statistics and Verifying the Policy Map Configuration 9
What to Do Next 10
Configuring Per-Session QoS Using the ISG Framework 10
Configuring a Local Service Profile 10
Defining an ISG Policy Map to Start the QoS Service 12
Starting the Session and Verifying the Policy Map Configuration 13
Configuration Examples for Per-Session QoS 14
Example Adding the Cisco QoS AV Pairs to the Service Profile on the RADIUS Server 14
Example Configuring a Local Service Profile 15
Example Defining an ISG Policy Map to Start the QoS Service 15
Examples Verifying the Per-Session QoS Configuration 15
Additional References 17
Per-Session QoS

The Per-Session QoS feature is one of two features bundled with the QoS: Broadband Aggregation Enhancements--Phase 1 feature. The Per-Session QoS feature provides the ability to apply quality of service (QoS) features (such as traffic classification, shaping, queueing, and policing) on a per-session basis. The Per-Session QoS feature can be configured either using a RADIUS server or using the framework available on the Intelligent Service Gateway (ISG).

Note: The Per-Session QoS feature can also be configured using a virtual template (for PPP sessions only). Using a virtual template is considered a "legacy" method but is still an available option for those familiar with virtual templates. For more information about using virtual templates to configure this feature, see the Per-Session QoS and Virtual Templates, page 5.

- Finding Feature Information, page 1
- Prerequisites for Per-Session QoS, page 1
- Restrictions for Per-Session QoS, page 2
- Information About Per-Session QoS, page 4
- How to Configure Per-Session QoS, page 6
- Configuration Examples for Per-Session QoS, page 14
- Additional References, page 17
- Feature Information for Per-Session QoS, page 19

Finding Feature Information

Your software release may not support all the features documented in this module. 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 Table at the end of this document.

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.

Prerequisites for Per-Session QoS

- The PPP or IP sessions are enabled.
Note

This document uses the generic term PPP to cover all protocol types. Examples of protocols include PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA). The specific protocol supported varies by platform. For example, the Cisco 7600 series router does not support PPPoA or PPP over Ethernet over ATM (PPPoEoA). For information about the Cisco 7600 series router, see the Cisco 7600 Series Cisco IOS Configuration Guide for the Cisco IOS release you are using.

- Layer 2 Tunneling Protocol (L2TP) resequencing is disabled.

Note

This prerequisite does not apply to the Cisco 7600 series router. L2TP is not supported on the Cisco 7600 series router.

- Traffic classes and policy maps have been configured with the QoS feature (for example, traffic policing or traffic shaping) to be applied to the network traffic. Depending on the needs of your network, multiple traffic classes and policy maps may be required.

Only if you are using a RADIUS server the following prerequisites apply:

- Authentication, authorization, and accounting (AAA) must be enabled.
- The RADIUS server must be configured.
- The service profile on the RADIUS server must be created.

Restrictions for Per-Session QoS

This feature does not support the following:

- L2TP sequencing.
- Packet dropping (packet discarding). That is, this feature does not allow you to discard packets using the drop command.
- The Multilink PPP (MLPPP) protocol. That is, multi-link bundles are not supported in either a PPP Termination and Aggregation (PTA) configuration or an L2TP configuration.

Note

MLPPP is supported on the Cisco 7600 series router.

- ATM interfaces (that is, PPPoA sessions) for Cisco IOS Release 12.2(33)SRC.
- Restrictions for Per-Session QoS (Cisco 7600 Series Routers), page 2

Restrictions for Per-Session QoS (Cisco 7600 Series Routers)

The following restrictions apply to the Cisco 7600 series router only.

- Queueing features are not supported in the ingress (incoming) direction of a router in an IP session. This means that traffic shaping, priority queueing such as low latency queueing (LLQ), class-based weighted fair queueing (CBWFQ), and weighted random early detection (WRED) are not supported.
Features that can be configured are traffic policing and traffic marking in either the class-default class or any of the user-defined classes, as shown in the following example:

```
policy-map sess_ingress
  class c1
  police 2000000
  set ip precedence 4
  class class-default
  police 5000000
  set ip precedence 1
```

**Note**
This restriction does not apply at the subinterface level in the ingress direction. That is, LLQ and traffic shaping are supported in the ingress direction. CBWFQ and WRED are not supported. For more information, see the "IP Subscriber Awareness over Ethernet" module.

- A policy map (in the egress direction) used in an IP session can have only packet marking enabled in the user-defined class. No other QoS features (for instance, traffic policing, LLQ, WRED, or traffic shaping) can be enabled. This means that the simplified configuration shown below would not be supported.

```
policy-map sess_egress
  class c1
  police/priority/bandwidth/wred/shape
```

The simplified configuration shown below would be supported.

```
policy-map sess_egress
  class c1
  set <name> <value>
```

However, all QoS features can be configured in the class-default class, as illustrated below.

```
policy-map sess_egress
  class class-default
  police/priority/bandwidth/wred/shape/set
```

- A hierarchical policy map (in the egress direction) on a IP session is supported, but the child policy map must be attached to the class class-default of the parent policy map as illustrated in the simplified configuration below.

```
policy-map sess_egress
  class class-default
  <Queueing feature like traffic shaping or bandwidth remaining ratio>
  service-policy child
```

**Note**
None of the restrictions that apply to a “flat” policy map (that is, a policy map not in a hierarchical policy map structure) in the egress or outgoing direction on a session apply to the child policy map. A simplified configuration illustrating this point is shown below.

```
policy-map child
  class voip
  police 9000
  priority level 1
  class iptv
  police 4193000
  priority level 2
  set cos 4
```
Traffic in both the ingress and egress direction can be classified (matched) on the basis of characteristics or attributes such as the following:

- IP precedence value
- Differentiated services code point (DSCP) value
- Class of service (CoS) value and CoS-inner value (of a Layer 2 QinQ packet)
- Access control list (ACL) number
- VLAN and inner-VLAN numbers

Combinations of these characteristics or attributes are allowed with the following restrictions:

- A combination of the CoS-inner setting and ACL number is not supported.
- While the command-line interface (CLI) does allow a configuration that contains two `match cos` commands, the `match-any` keyword must be used with the `class-map` command to make such a configuration meaningful.
- The `match vlan` and `match vlan-inner` commands are supported at the main interface level only.

Traffic in both the ingress and egress direction can be marked on the basis of characteristics or attributes such as the following:

- IP precedence value
- DSCP value
- CoS value
- CoS-inner value (in the egress direction only)

If a `set` command is specified, note the following points:

- Specifying both `set cos 4` and `set cos 5` in the same traffic class causes the `show policy-map` command to display only `set cos 5` in the show command output.
- Specifying both the `set ip prec 5` command and the `set dscp cs6` command in the same class causes the `show policy-map` command to display only `set dscp cs6` in the `show` command output.

**Information About Per-Session QoS**

- **Benefits of Per-Session QoS**, page 4
- **Policy Maps and QoS Features**, page 5
- **Per-Session QoS and Virtual Templates**, page 5
- **Per-Session QoS and the ISG Framework**, page 6
- **Cisco AV Pairs and VSAs**, page 6

**Benefits of Per-Session QoS**

The ability to apply QoS features on a per-session basis helps the Internet service provider (ISP) to adhere to the Service Level Agreement (SLA) established for handling traffic. Applying QoS on a per-session basis provides a higher degree of granularity for managing traffic on the network.
Policy Maps and QoS Features

A policy map specifies the QoS feature to be applied to network traffic. Examples of QoS features that can be specified in a policy map include traffic classification, shaping, queueing, and policing, among others. Each QoS feature is configured using the appropriate QoS commands.

- Hierarchical Policy Maps, page 5

Hierarchical Policy Maps

Policy maps can be configured in a hierarchical structure. That is, policy maps can be configured in levels subordinate to one another. The policy map at the highest level is referred to as the "parent" policy map. A subordinate policy map is referred to as a "child" policy map.

A typical hierarchical policy map structure consists of a parent policy map and one child policy map. Configure the child policy map first; then configure the parent policy map. Both types of policy maps are configured in the same manner.

The parent policy map typically contains one class—the class called class-default. The child policy map can contain multiple classes.

Note Before configuring the policy map, create the traffic classes and specify the match criteria used to classify traffic. To create traffic classes and specify match criteria, use the MQC.

The following restrictions apply to hierarchical policy maps:

- Specify CBWFQ in the child policy map only. CBWFQ cannot be specified in the parent policy map.
- Traffic shaping can be specified in either the parent policy map or the child policy map.

However, for this feature, you must specify traffic shaping in the parent policy map. Specifying traffic shaping in the child policy map is optional.

Note The restrictions related to policy maps and the Cisco 7600 series router are different from those listed above. For more information about the restrictions specific to the Cisco 7600 series router, see the Restrictions for Per-Session QoS (Cisco 7600 Series Routers), page 2.

Per-Session QoS and Virtual Templates

As mentioned earlier, you can configure the Per-Session QoS feature using a virtual template.

Note Using virtual templates to configure the Per-Session QoS feature applies to PPP sessions only.

A virtual template is a logical interface that is configured with generic configuration information for a specific purpose or with configuration information common to specific users, plus router-dependent information. The template takes the form of a list of Cisco IOS interface commands that are applied to virtual access interfaces, as needed.
A virtual template is configured (defined) on an interface. When a session is enabled (that is, when a packet arrives at the interface), the virtual template inherits the QoS features specified in the policy map for use during the session.

After configuring the policy maps (as many as needed) and associating the policy maps with the virtual template on the interface, you may want to verify the configuration. To verify the per-session QoS configuration, use the `show policy-map session [uid uid-number]` command. This command allows you to see whether the policy maps are configured the way that you intended.

**Per-Session QoS and the ISG Framework**

QoS features can be applied on a per-session basis using the ISG framework in a number of ways, including the following:

- Enabling the QoS feature when it is triggered by specific events configured in the ISG policy map (for instance, at the start of a session or at a predetermined expiration interval).
- Using the Change of Authorization (CoA).
- Using the Transparent Auto Logon (TAL).
- Downloading the service profile at the time of authentication.

**Cisco AV Pairs and VSAs**

Cisco AV pairs are part of vendor-specific attributes (VSAs) that allow a policy map to be applied to the router. Cisco AV pairs are a combination of an attribute and a value. The purpose of the Cisco VSA (attribute 26) is to communicate vendor-specific information between the router and the RADIUS server. The Cisco VSA encapsulates vendor-specific attributes that allow vendors such as Cisco to support their own extended attributes.

For this configuration, one of two Cisco AV pairs can be used (formatted as shown below):

- `lcp:interface-config=service-policy output/input <policy name>`
- `ip:sub-qos-policy-in/out=<policy name>`

This Cisco AV pair takes advantage of more recent technology and is the recommended choice. This Cisco AV pair is the one shown in the configuration task and example.

The Cisco AV pair is added to the service profile on the RADIUS server. Each entry establishes an attribute that the user can access.

In a user file, the data to the left of the equal sign (=) is an attribute defined in the dictionary file, and the data to the right of the equal sign is the configuration data.

The Cisco AV pair identifies the policy map that was used to configure the specific QoS features. When the router requests the policy map name (specified in the Cisco AV pair), the policy map is pulled to the router from the RADIUS server when the session is established. The Cisco AV pair applies the appropriate policy map (and, therefore, the QoS feature) directly to the router from the RADIUS server.

**How to Configure Per-Session QoS**

The tasks for configuring per-session QoS vary according to the configuration method that you are using. You can choose to configure the feature either using a RADIUS server or using the ISG framework.
Choose one of the following:

Note
For information about configuring the feature using a virtual template, see the Per-Session QoS and Virtual Templates, page 5.

- Configuring Per-Session QoS Using a RADIUS Server, page 7
- Configuring Per-Session QoS Using the ISG Framework, page 10

Configuring Per-Session QoS Using a RADIUS Server

- Adding the Cisco QoS AV Pairs to the Service Profile on the RADIUS Server, page 7
- Defining an ISG Policy Map to Start the QoS Service on the RADIUS Server, page 8
- Reviewing Session Statistics and Verifying the Policy Map Configuration, page 9

Adding the Cisco QoS AV Pairs to the Service Profile on the RADIUS Server

- Prerequisites, page 7

Prerequisites
Before adding the Cisco QoS AV pairs to the service profile, you must create traffic classes and configure policy maps used to enable the QoS feature you want to use.

SUMMARY STEPS

1. ip:sub-qos-policy-in/out=<policy name>
Defining an ISG Policy Map to Start the QoS Service on the RADIUS Server

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** ip:sub-qos-policy-in/out=<policy name> | Enter the Cisco QoS AV pair for policy maps on the RADIUS server in the service profile. When the router requests the service definition from the RADIUS server, the information in the service profile is used.  
  • Add the Cisco QoS AV pairs to the service profile. |

Example:

cisco-avpair="ip:sub-qos-policy-in=res_ingress"

cisco-avpair="ip:sub-qos-policy-out-res_hsi_voip_parent1"

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. policy-map type control policy-map-name  
4. class type control always event session-start  
5. action-number service-policy type service name service-name  
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |

Example:

Router> enable
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> policy-map type control policy-map-name</td>
<td>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# policy-map type control TEST</td>
<td>• Enter the type and control keywords and the name of the policy map.</td>
</tr>
<tr>
<td><strong>Step 4</strong> class type control always event session-start</td>
<td>Specifies a control class (or event) for which actions may be configured in policy map. Enters control policy-map class control configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-control-policymap)# class type control always event session-start</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> action-number service-policy type service name service-name</td>
<td>Applies the specified service at the start of the session.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-control-policymap-class-control)# 1 service-policy type service name QoS_Service</td>
<td>• Enter the action number, the name keyword, and the name of the service.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-control-policymap-class-control)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Reviewing Session Statistics and Verifying the Policy Map Configuration**

**SUMMARY STEPS**

1. enable
2. show subscriber session uid uid-number
3. show policy-map session uid uid-number
4. exit
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show subscriber session uid <em>uid-number</em></td>
<td>Displays information about subscriber sessions on an ISG by the unique ID.</td>
</tr>
<tr>
<td>Example: Router# show subscriber session uid 401</td>
<td>• Enter the <em>uid</em> keyword and unique identifier.</td>
</tr>
<tr>
<td><strong>Step 3</strong> show policy-map session uid <em>uid-number</em></td>
<td>Displays the information about the session identified by the unique ID.</td>
</tr>
<tr>
<td>Example: Router# show policy-map session uid 401</td>
<td>• Enter the <em>uid</em> keyword and unique identifier.</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>(Optional) Exits privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router# exit</td>
<td>• What to Do Next, page 10</td>
</tr>
</tbody>
</table>

What to Do Next

Proceed to the Configuration Examples for Per-Session QoS, page 14.

Configuring Per-Session QoS Using the ISG Framework

• Configuring a Local Service Profile, page 10
• Defining an ISG Policy Map to Start the QoS Service, page 12
• Starting the Session and Verifying the Policy Map Configuration, page 13

Configuring a Local Service Profile

Before configuring the local service profile, you must create traffic classes and configure policy maps used to enable the QoS feature that you want to use. To create traffic classes and policy maps, use the MQC.
### SUMMARY STEPS

1. enable
2. configure terminal
3. policy-map type service policy-map-name
4. service-policy input policy-map-name
5. service-policy output policy-map-name
6. exit
7. aaa authorization subscriber-service default local group name
8. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** | |
| Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | |
| Router# configure terminal | |
| **Step 3** policy-map type service policy-map-name | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.  
- Enter the `type` and `service` keywords and the name of the policy map. |
| **Example:** | |
| Router(config)# policy-map type service QoS_Service | |
| **Note** | Using the `service` keyword enters service policy-map configuration mode. |
| **Step 4** service-policy input policy-map-name | Attaches the specified policy map to the input interface or input VC.  
- Enter the name of the policy map. |
| **Example:** | |
| Router(config-service-policymap)# service-policy input res_ingress | |
| **Step 5** service-policy output policy-map-name | Attaches the specified policy map to the output interface or output VC.  
- Enter the name of the policy map. |
| **Example:** | |
| Router(config-service-policymap)# service-policy output res_hsi_voip_iptV_parent1 | |
### Defining an ISG Policy Map to Start the QoS Service

**SUMMARY STEPS**

1. enable
2. configure terminal
3. policy-map type control policy-map-name
4. class type control always event session-start
5. action-number service-policy type service name service-name
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

### Step 6 exit

**Example:**

```
Router(config-service-policymap)# exit
```

Returns to global configuration mode.

### Step 7 aaa authorization subscriber-service default local group name

**Example:**

```
Router(config)# aaa authorization subscriber-service default local group group1
```

Specifies one or more authentication, authorization, and accounting (AAA) authorization methods for ISG to use in providing subscriber service.

- Enter the default keyword, the local keyword, the group keyword, and the group name.

**Note** The local keyword must be entered after the default keyword.

### Step 8 end

**Example:**

```
Router(config)# end
```

(Optional) Returns to privileged EXEC mode.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3 policy-map type control policy-map-name</td>
<td>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# policy-map type control TEST</code></td>
<td>• Enter the <em>type</em> and <strong>control</strong> keywords and the name of the policy map.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Using the <strong>control</strong> keyword enters control policy-map configuration mode.</td>
</tr>
<tr>
<td>Step 4 class type control always event session-start</td>
<td>Specifies a control class (or event) for which actions may be configured in an ISG control policy. Enters control policy-map class control configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-control-policymap)# class type control always event session-start</code></td>
<td></td>
</tr>
<tr>
<td>Step 5 action-number service-policy type service name service-name</td>
<td>Activates an ISG service.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-control-policymap-class-control)# 1 service-policy type service name QoS_Service</code></td>
<td>• Enter the action number, the <strong>name</strong> keyword, and the name of the service.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-control-policymap-class-control)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Starting the Session and Verifying the Policy Map Configuration**

**SUMMARY STEPS**

1. enable
2. show subscriber session uid *uid-number*
3. show policy-map session uid *uid-number*
4. exit
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 show subscriber session uid uid-number</td>
<td>(Optional) Displays information about subscriber sessions on an ISG by the unique ID.</td>
</tr>
<tr>
<td></td>
<td>• Enter the uid keyword and unique identifier.</td>
</tr>
<tr>
<td>Example: Router# show subscriber session uid 401</td>
<td></td>
</tr>
<tr>
<td>Step 3 show policy-map session uid uid-number</td>
<td>(Optional) Displays information about the session identified by the unique ID.</td>
</tr>
<tr>
<td></td>
<td>• Enter the uid keyword and unique identifier.</td>
</tr>
<tr>
<td>Example: Router# show policy-map session uid 401</td>
<td></td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>(Optional) Exits privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router# exit</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Examples for Per-Session QoS

- Example Adding the Cisco QoS AV Pairs to the Service Profile on the RADIUS Server, page 14
- Example Configuring a Local Service Profile, page 15
- Example Defining an ISG Policy Map to Start the QoS Service, page 15
- Examples Verifying the Per-Session QoS Configuration, page 15

Example Adding the Cisco QoS AV Pairs to the Service Profile on the RADIUS Server

The following is an example of a service profile in which the Cisco QoS AV pairs have been added. Cisco AV pairs are needed only if you are configuring the Per-Session QoS feature using a RADIUS server.

cisco-avpair = "ip:sub-qos-policy-in-res_ingress"
cisco-avpair = "ip:sub-qos-policy-out-res_hsi_voip_iptv_parent1"
Example Configuring a Local Service Profile

The following is an example of a local service profile configuration. Configuring a local service profile is needed only if you are configuring the Per-Session QoS feature using the ISG framework.

Router> enable
Router# configure terminal
Router(config)# policy-map type service QoS_Service
Router(config-service-policymap)# service-policy input res_ingress
Router(config-service-policymap)# service-policy output res_hsi_voip_iptv_parent1
Router(config-service-policymap)# exit
Router(config)# aaa authorization subscriber-service default local group group1
Router(config)# end

Example Defining an ISG Policy Map to Start the QoS Service

The following is an example an ISG policy map configured to initiate the QoS service at the start of a session.

Router> enable
Router# configure terminal
Router(config)# policy-map type control TEST
Router(config-policymap)# class type control always event session-start
Router(config-policymap-class-control)# 1 service-policy type service name QoS_Service
Router(config-policymap-class-control)# end

Examples Verifying the Per-Session QoS Configuration

The following is an example of the output of the `show subscriber session` command.

Router# show subscriber session uid 2
Unique Session ID: 2
Identifier:
SIP subscriber access type(s): IP
Current SIP options: Req Fwding/Req Fwded
Session Up-time: 00:00:20, Last Changed: 00:00:20

Policy information:
Authentication status: unauthen
Active services associated with session:
name "QoS_Service", applied before account logon
Rules, actions and conditions executed:
subscriber rule-map TEST
  condition always event session-start
    1 service-policy type service name QoS_Service
Session inbound features:
Feature: QoS Policy Map
  Input Policy Map: res_ingress

Session outbound features:
Feature: QoS Policy Map
  Output Policy Map: res_hsi_voip_iptv_parent1

Configuration sources associated with this session:
Service: QoS_Service, Active Time = 00:00:22
Interface: GigabitEthernet3/1/3.100, Active Time = 00:00:22

The following is an example of the output of the show policy-map session command.

Router# show policy-map session uid 2

SSS session identifier 2 -
Service-policy input: res_ingress
Counters last updated 00:00:00 ago

Class-map: voip (match-all)
  126126 packets, 9585576 bytes
  30 second offered rate 1114000 bps, drop rate 1114000 bps
  Match: ip precedence 5
  police:
    cir 9000 bps, bc 1500 bytes
    conformed 40 packets, 3040 bytes; actions:
      transmit
    exceeded 126086 packets, 9582536 bytes; actions:
      drop
    conformed 0 bps, exceed 1114000 bps
QoS Set
  cos 5
  Packets marked 126126

Class-map: class-default (match-any)
  262772 packets, 133488176 bytes
  30 second offered rate 15550000 bps, drop rate 15502000 bps
  Match: any
  police:
    cir 2000000 bps, bc 62500 bytes
    conformed 784 packets, 398272 bytes; actions:
      transmit
    exceeded 261988 packets, 133089904 bytes; actions:
      drop
    conformed 44000 bps, exceed 15502000 bps
QoS Set
  cos 1
  Packets marked 262772
SSS session identifier 2 -
Service-policy output: res_hsi_voip_iptv_parent1

Class-map: class-default (match-any)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
  Queueing
  queue limit 2000 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
  bandwidth remaining ratio 5
  bandwidth remaining 0%
  shape (average) cir 8000000, bc 32000, be 32000
  target shape rate 8000000
Service-policy : hsi_voip_iptv

  queue stats for all priority classes:
priority level 1
queue limit 2 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pktts output/bytes output) 0/0

queue stats for all priority classes:

priority level 2
queue limit 1048 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pktts output/bytes output) 0/0

Class-map: voip (match-all)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 5
Priority: Strict, b/w exceed drops: 0
Priority Level: 1
police:
cir 9000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions: transmit
exceeded 0 packets, 0 bytes; actions: drop
conformed 0 bps, exceed 0 bps
QoS Set
cos 5
Packets marked 0

Class-map: iptv (match-all)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 6
Priority: Strict, b/w exceed drops: 0
Priority Level: 2
police:
cir 4193000 bps, bc 131031 bytes
conformed 0 packets, 0 bytes; actions: transmit
exceeded 0 packets, 0 bytes; actions: drop
conformed 0 bps, exceed 0 bps
QoS Set
cos 4
Packets marked 0

Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any

queue limit 949 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pktts output/bytes output) 0/0
QoS Set
cos 1
Packets marked 0

Additional References
The following sections provide references related to the Per-Session QoS feature.
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td><em>Cisco IOS Quality of Service Solutions Command Reference</em></td>
</tr>
<tr>
<td>QoS features such as traffic classification and traffic policing</td>
<td>&quot;Quality of Service Overview&quot; module</td>
</tr>
<tr>
<td>Class maps, policy maps, hierarchical policy maps, and MQC</td>
<td>&quot;Applying QoS Features Using the MQC” module</td>
</tr>
<tr>
<td>RADIUS servers and AAA</td>
<td>&quot;Configuring Authentication” module</td>
</tr>
<tr>
<td>RADIUS accounting</td>
<td>&quot;Configuring Accounting” module</td>
</tr>
<tr>
<td>ISG policies and session maintenance</td>
<td>&quot;Configuring ISG Policies for Session Maintenance” module</td>
</tr>
<tr>
<td>Classification, policing, and marking on Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC)</td>
<td>&quot;QoS: Classification, Policing, and Marking on LAC” module</td>
</tr>
<tr>
<td>LLQ, traffic shaping, CBWFQ, and WRED support on a 7600 series router</td>
<td>&quot;IP Subscriber Awareness over Ethernet” module</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>
Feature Information for Per-Session QoS

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Per-Session QoS    | 12.2(28)SB 12.2(33)SRC | The Per-Session QoS feature provides the ability to apply quality of service (QoS) features (such as traffic classification, shaping, queueing, and policing) on a per-session basis.  
In Release 12.2(28)SB, this feature was introduced on the Cisco 7200 series router.  
In Release 12.2(33)SRC, support was added for the Cisco 7600 series router. |

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.