CHAPTER 15

Service Flow Admission Control for the Cisco CMTS

Revised: February 5, 2007, OL-1467-08

Cisco IOS Release 12.3(21)BC introduces Service Flow Admission Control (SFAC) on the Cisco Cable Modem Termination System. Service Flow Admission Control is supported on the Cisco uBR10012 router with Performance Routing Engines 1 and 2 (PRE1 and PRE2) modules, and the Cisco uBR7246VXR router. This document describes the concepts, advantages, configuration and monitoring capabilities of Service Flow Admission Control on the Cisco CMTS.

Note *Admission Control* is a widely-used term that applies to similarly named features for additional Cisco products and technologies.

One earlier version of Admission Control is introduced in Cisco IOS Release 12.3(13a)BC, and is described in the following document:

- *Admission Control for the Cisco CMTS*

  http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_adm.html

Another distinct version of Admission Control is supported for the Cisco uBR7114 universal broadband router in Cisco IOS 12.1 EC software. This earlier Admission Control feature sets the percentage of upstream channel capacity allowable for the given upstream. Refer to the following document:

- *Cisco uBR7100 Series Software Configuration Guide*

  http://www.cisco.com/en/US/docs/cable/cmts/ubr7100/configuration/guide/scg71ovr.html

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Additional References" section on page 16-43.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Prerequisites for Service Flow Admission Control

Service Flow Admission Control requires the following:

- Cisco IOS Release 12.3(21)BC or later supporting release
- Cisco uBR10012 router with Performance Routing Engine Modules 1 or 2 (PRE1 or PRE2), or the Cisco uBR7246VXR router

Restrictions for Service Flow Admission Control

SFAC in Cisco IOS Release 12.3(21)BC follows these general factors when implementing on the Cisco CMTS:

- Configure SFAC before admitting any static or dynamic service flows. The best option is to have the configuration in place during startup time, or before the interface is up.h
- SFAC in Cisco IOS Release 12.3(21)BC supports the following resource monitoring on the Cisco CMTS:
  - Upstream and downstream bandwidth on the Cisco CMTS
  - CPU utilization and memory resources on the Cisco uBR10012 and Cisco uBR7246VXR router chassis (Cisco uBR10-MC5X20U and Cisco uBR-MC28U broadband processing engines)
- Admission Control does not support Wide Area Network (WAN) bandwidth monitoring for the Cisco uBR10012 router.

Information About Service Flow Admission Control

This section describes DOCSIS 1.1 concepts and configuration options supported on the Cisco CMTS for Service Flow Admission Control.

Overview of Service Flow Admission Control for the Cisco CMTS

SFAC on the Cisco CMTS is a mechanism that gracefully manages service flow admission requests when one or more resources are not available to process and support the incoming service request. Lack of such a mechanism not only causes the new request to fail with unexpected behavior but could potentially cause the flows that are in progress to have quality related problems. SFAC monitors such resources constantly, and accepts or denies requests depending on the resource availability.

SFAC enables you to provide a reasonable guarantee about the Quality of Service (QoS) to subscribers at the time of call admission, and to enable graceful degradation of services when resource consumption approaches critical levels. SFAC reduces the impact of unpredictable traffic demands in circumstances that would otherwise produce degraded QoS for subscribers.

SFAC uses two event types for resource monitoring and management—cable modem registration and dynamic service (voice call) requests. When either of these two events occurs on the Cisco CMTS, SFAC verifies that the associated resources conform to the configured limits prior to admitting and supporting the service call request.

SFAC is not a mechanism to apply QOS to the traffic flows. Scheduling and queuing are some of the mechanisms used for implementing the QOS. The QOS is applied on per packet basis. SFAC checks are performed before the flow is admitted.

SFAC in Cisco IOS Release 12.3(21)BC monitors the following resources on the Cisco CMTS.

- *CPU utilization*—SFAC monitors CPU utilization on the Cisco CMTS, and preserves QoS for existing service flows when new traffic would otherwise compromise CPU resources on the Cisco CMTS.
- *Memory resource utilization (I/O, Processor, and combined total)*—SFAC monitors one or both memory resources and their consumption, and preserves QoS in the same way as with CPU utilization.
- *Bandwidth utilization for upstream and downstream*—SFAC monitors upstream and downstream bandwidth utilization, and associated service classes, whether for data or dynamic service traffic.

Note See also the "Service Flow Admission Control and Cisco CMTS Resources" section on page 16-5.

Note SFAC begins graceful degradation of service when either a critical threshold is crossed, or when bandwidth is nearly consumed on the Cisco CMTS, depending on the resource being monitored.

SFAC enables you to configure major and minor thresholds for each resource on the Cisco CMTS. These thresholds are expressed in a percentage of maximum allowable resource utilization. Alarm traps may be sent each time a minor or major threshold is crossed for a given resource.

For system-level resources, such as CPU and memory utilization, you can configure critical thresholds in addition to the major and minor thresholds. When a critical threshold is crossed, further service requests are gracefully declined until the associated resource returns to a lower threshold level.

For upstream (US) and downstream (DS) channels, you can configure the bandwidth allocation with exclusive and non-exclusive thresholds. These thresholds can be configured for specified DOCSIS traffic types.

- Exclusive bandwidth indicates the percentage of bandwidth that is allocated exclusively for the specified traffic type. This bandwidth may not be shared with any other traffic type.
- Non-exclusive bandwidth indicates the percentage of bandwidth that is configured in addition to the exclusive bandwidth. Non-exclusive bandwidth is also configured for specific DOCSIS traffic types. Non-exclusive bandwidth is not guaranteed, and may be shared with other traffic types.
- The sum of exclusive and non-exclusive thresholds indicates the maximum bandwidth the specified traffic type may use.

This section provides additional information about SFAC with the following topics:

Service Flow Admission Control and Cisco Universal Broadband Routers

Service Flow Admission Control on the Cisco uBR10012 Universal Broadband Router

Cisco IOS Release 12.3(21)BC supports Service Flow Admission Control on the Cisco uBR10012 router and all broadband processing engines.

Service Flow Admission Control on the Cisco uBR7246VXR Universal Broadband Router

Cisco IOS release 12.3(21)BC supports Service Flow Admission Control on the Cisco uBR7246VXR router.

Service Flow Admission Control and Memory Requirements for the Cisco CMTS

Service Flow Admission Control for the Cisco CMTS is a powerful feature that maintains Quality of Service (QoS) on the Cisco CMTS and enforces graceful degradation in service when attempted consumption exceeds resource availability.

Additional memory is required in the Cisco universal broadband router to maintain and store information about various scheduling types, the distribution of upstream or downstream traffic, and associated resource check processes. For complete information about memory requirements and Cisco IOS Release 12.3(21)BC, refer to the corresponding release notes for your product:

- *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC*
  http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html
- *Release Notes for Cisco uBR7200 Series for Cisco IOS Release 12.3 BC*
  http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html

Service Flow Admission Control and Cisco CMTS Resources

Service Flow Admission Control with Cisco IOS Release 12.3(21)BC implements graceful QoS policies for the following resources of the Cisco CMTS:

System-Level Resources—Impact All Cisco CMTS Functions

- CPU utilization on route processor or broadband processing engine (BPE) modules
- I/O memory on route processor or broadband processing engine modules

- Processor memory

Bandwidth-Level Resources—Impact Traffic Per Interface or Per Port

- Downstream DOCSIS 1.1 bandwidth with QoS support on Cisco cable interface line cards or BPEs
- Upstream DOCSIS 1.1 bandwidth with QoS support on Cisco cable interface line cards or BPEs

Cisco IOS release 12.3(21)BC supports the following resources for the following Cisco CMTS routers:

Cisco uBR10012 Router Resources

- Cisco uBR Route Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources with the Cisco MC28U

- Cisco uBR Route Processor
  - CPU Utilization
  - Processor Memory
  - I/O Memory
- Cisco uBR Cable Interface Line Card
  - Downstream Bandwidth
  - Upstream Bandwidth

Cisco uBR7246VXR Router Resources without the Cisco MC28U

- Network Processing Engine
  - CPU Utilization
  - Processor Memory
  - I/O Memory
  - Downstream Bandwidth
  - Upstream Bandwidth

For additional information, refer to the "How to Configure, Monitor and Troubleshoot Service Flow Admission Control" section on page 16-9.

Service Flow Admission Control and CPU Utilization

CPU utilization is defined and monitored either as a five-second or a one-minute average. Both averages cannot be configured at the same time for any given resource. For CPU utilization, you can set minor, major, and critical threshold levels.

For additional information, refer to the "Configuring Service Flow Admission Control Based on CPU Utilization" section on page 16-12.

Service Flow Admission Control and Memory Utilization

Service Flow Admission Control can define up to three different memory options on the Cisco CMTS:

- IO memory - Current available (free) I/O memory
- Processor memory - Current available processor memory
- Both - Combined (IO and processor) memory that are available on the router

Memory resources are similar to CPU utilization, in that you can set minor, major, and critical threshold levels. Memory-based Service Flow Admission Control is supported for memory on the main CPU in Cisco IOS Release 12.3(21)BC, and not for the broadband processing engine line card memory.

For additional information, refer to the "Configuring Service Flow Admission Control Based on Memory Resources" section on page 16-13.

Service Flow Admission Control and Upstream or Downstream Bandwidth Utilization

Service Flow Admission Control allows you to control the bandwidth usage for various DOCSIS traffic types or application types. The application types are defined by the user using a CLI to categorize the service flow.

Categorization of Service Flows

The SFAC feature allows you to allocate the bandwidth based on the application types. Flow categorization allows you to partition bandwidth in up to eight application types or buckets. The composition of a bucket is defined by the command-line interface (CLI), as is the definition of rules to categorize service flows into one of these eight application buckets. Various attributes of the service flow may be used to define the rules.

For flows created by PacketCable, the following attributes may be used:

- the priority of the Packetcable gate associated with the flow (high or normal)

For flows created by PacketCable MultiMedia (PCMM), the following attributes may be used:

- Priority of the gate (0 to 7)
- Application type (0 to 65535)

The scheduling type for Upstream flows uses the following attribute type:

- Service class name

Before a service flow is admitted, it is passed through the categorization routine. Various attributes of the service flow are compared with the user-configured rules. Based on the match, the service flow is labeled with application type, from 1 to 8. The bandwidth allocation is then performed per application type.

Before a service flow is admitted, it is categorized based on its attributes. The flow attributes are compared against CLI-configured rules, one bucket at a time. If a match is found for any one of the rules, the service flow is labeled for that bucket, and no further check is performed.

Bucket 1 rules are scanned first and bucket 8 rules are scanned last. If two different rules match two different buckets for the same service flow, the flow gets categorized under the first match. If no match is found, the flow is categorized as Best Effort (BE) and the bucket with best effort rule is labelled to the flow. By default, the BE bucket is bucket 8.

Thresholds for Upstream or Downstream Bandwidth

SFAC monitors upstream or downstream bandwidth consumption with minor, major, and critical thresholds. SFAC generates alarm traps when bandwidth consumption crosses minor and major thresholds. For additional information, refer to the "How to Configure, Monitor and Troubleshoot Service Flow Admission Control" section on page 16-9.

Exclusive and Non-Exclusive Bandwidth Thresholds

In addition to minor and major thresholds, SFAC also allows configuration of exclusive or non-exclusive thresholds.

- *Exclusive* bandwidth thresholds, for the upstream or downstream bandwidth, define a given percentage of the total (100%) bandwidth, and dedicate it to a specific traffic type.
- *Non-exclusive* bandwidth thresholds can be shared with multiple traffic types. Non-exclusive bandwidth is typically used by Best Effort traffic, yet remains available to other traffic types when required.

When the traffic usage exceeds the exclusive threshold, SFAC checks if there is any non-exclusive bandwidth available. Any new service request is permitted only if sufficient non-exclusive bandwidth is available.

Comparing Service Flow Admission Control with Prior Admission Control

The prior Admission Control feature on the Cisco CMTS was introduced in Cisco IOS Release 12.3(13a)BC. This prior version of Admission Control allows you to set minor, major, exclusive and non-exclusive thresholds. This topic lists changes introduced for SFAC in Cisco IOS Release 12.3(21)BC, and identifies which part of the functionality is changed and which functionality is preserved.

Note The configuration, monitoring, and debugging commands used for the original Admission Control feature are not supported for the Service Flow Admission Control bucket scheme.

- SFAC retains the prior Admission Control concept of thresholds. SFAC enables configuration of major, minor, exclusive and non-exclusive thresholds. However, SFAC is *distinct and unique in that the thresholds are applied per application bucket, numbered 1 to 8.*
- For downstream service flows, the prior Admission Control feature permitted bandwidth allocation for only data and voice traffic, and only PacketCable voice was recognized. SFAC uniquely allows bandwidth allocation per application bucket. As with Admission Control, however, SFAC allocates bandwidth for PacketCable voice by configuring the appropriate rules that apply to the application buckets.
- Upstream bandwidth allocation in SFAC is not based on the scheduling types, such as UGS, RTPS and so forth. SFAC newly handles upstream channels in fashion similar to downstream channels—the upstream channels also support eight application types. You may configure SFAC bandwidth allocation based on the scheduling types. You achieve the same result, however, by defining the appropriate rules to map each scheduling type into one of the eight buckets.
- SFAC monitors and manages Cisco CMTS resources according to the categorization of service flow, in which service flow policies, status and resource management are configured and processed in more categorical fashion, to include support for both PacketCable and PacketCable MultiMedia voice traffic.

- SFAC newly treats upstream and downstream traffic in the same manner and in more uniform fashion than the previous Admission Control feature.
- Exclusive and non-exclusive thresholds define resource management processes of the SFAC feature.
- Service Flow Admission Control introduces enhanced support for the CISCO-CABLE-ADMISSION-CTRL-MIB.

How to Configure, Monitor and Troubleshoot Service Flow Admission Control

This section describes the following configuration, monitoring and troubleshooting procedures for the Service Flow Admission Control (SFAC) feature. Configuration procedures are optional, given default configurations are enabled in Cisco IOS Release 12.3(21)BC. This section presents a sequence of procedures for non-default configurations, monitoring and debugging procedures that apply in default or non-default operations of Service Flow Admission Control.

Primary Configurations for Service Flow Admission Control

- Enabling Service Flow Admission Control for Event Types, page 16-10

  This procedure sets the events that trigger the Admission Control checks on the Cisco CMTS.
- Configuring Service Flow Admission Control Based on CPU Utilization, page 16-12

  This procedure configures threshold levels for CPU utilization. When threshold levels are crossed during an Admission Control check, an alarm is generated or the service is gracefully declined, depending on the level crossed.
- Configuring Service Flow Admission Control Based on Memory Resources, page 16-13

  This procedure configures memory resource types and associated threshold levels for Admission Control on the Cisco CMTS.
- Defining Rules for Service Flow Categorization, page 16-14

  This procedure describes how to configure service flow rules on the Cisco CMTS. This procedure changes default global service flow rule rules. By default, Cisco IOS Release 12.3(21)BC enables the definition of service flows according to application or traffic type, with bucket assignments for a standard set of service flow applications.
- Naming Application Buckets for Service Flow Admission Control, page 16-19

  This procedure enables you to assign alpha-numeric names to six of the eight application buckets that Service Flow Admission Control supports.
- Setting Downstream and Upstream Application Thresholds, page 16-21

  This procedure sets downstream and upstream applications thresholds for Service Flow Admission Control on the Cisco CMTS.
- Preempting High-Priority Emergency 911 Calls, page 16-25

  This procedure enables you to override the default Emergency 911 call preemption functions described in the "Comparing Service Flow Admission Control with Prior Admission Control" section on page 16-8.
- Calculating Upstream and Downstream Bandwidth Utilization, page 16-27

  Provides guidelines for calculating requirements and potential configurations of Service Flow Admission Control and related thresholds and settings.

Monitoring and Troubleshooting Commands for Service Flow Admission Control

- Bandwidth Validity Checks for Service Flow Admission Control, page 16-28

  Provides guidelines for performing validation of configuration and operation.
- Displaying Application Buckets for Service Flow Admission Control, page 16-29

  Describes how to display the application types configured and active.
- Displaying Service Flow Reservation Levels, page 16-30

  Describes how to display the reservation levels configured and active.
- Displaying SFAC Configuration and Status, page 16-31

  Describes how to display service flows, application categorizations, and bandwidth consumption status.
- Debugging Service Flow Admission Control for Different Event Types, page 16-33

  Describes how to debug event type classifications.
- Debugging Service Flow Admission Control for CPU Resources, page 16-34

  Describes how to debug CPU resource configurations.
- Debugging Service Flow Admission Control for Downstream Bandwidth, page 16-36

  Describes how to debug downstream bandwidth settings and operation.
- Debugging Service Flow Admission Control for Upstream Throughput, page 16-37

  Describes how to debug upstream throughput settings and operation.
- Debugging Flow Categorization for Service Flow Admission Control, page 16-38

  Describes how to enable and use **debug** and **show** commands for service flow categorization settings.

Enabling Service Flow Admission Control for Event Types

Service Flow Admission Control can be enabled for one or more of the following events. At least one of these events must be configured for Service Flow Admission Control on the Cisco CMTS prior to the configuration of any additional settings:

- the registration of a cable modem
- the request for a dynamic service, such as a PacketCable or PCMM voice call

Perform these steps to configure either or both event types on the Cisco CMTS.

Prerequisites

Service Flow Admission Control requires that event types, traffic types and CMTS resource thresholds be configured and enabled on the Cisco CMTS. Refer also to the "Prerequisites for Service Flow Admission Control" section on page 16-2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable admission-control event { cm-registration | dynamic-service }**
4. **Ctrl-Z**

DETAILED STEPS

	Command or Action	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	**cable admission-control event** { **cm-registration** | **dynamic-service** }
	
	Example:
	`Router(config)# cable admission-control event cm-registration`
	`Router(config)# cable admission-control event dynamic-service`
		Sets the event type on the Cisco CMTS at which Service Flow Admission Control performs resource monitoring and management. At least one of the following keywords must be used, and both can be set.
		• **cm-registration**—Sets Service Flow Admission Control checks to be performed when a cable modem registers. If there are insufficient resources at the time of registration, the cable modem is allowed to come online.
		• **dynamic-service**—Sets Service Flow Admission Control checks to be performed when a dynamic service such as a voice call is requested.

Step 4	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

Examples

The following example in global configuration mode enables both event types on the Cisco CMTS:

```
Router(config)# cable admission-control event cm-registration
Router(config)# cable admission-control event dynamic-service
```

What to Do Next

Once configured, event types and Service Flow Admission Control event activity on the Cisco CMTS can be reviewed using the following two commands:

- **debug cable admission-control** *options*
- **show cable admission-control**

If the resources to be monitored and managed by Service Flow Admission Control are not yet configured on the Cisco CMTS, refer to the additional procedures in this document for information about their configuration.

Configuring Service Flow Admission Control Based on CPU Utilization

Service Flow Admission Control allows you to configure minor, major and critical thresholds for CPU utilization. The thresholds are specified as percentage of CPU utilization. When the an event such as cable modem registration or dynamic service takes place, and the CPU utilization is greater than the major or minor threshold, an alarm is generated. If it is greater than the critical threshold, the new service is gracefully declined.

Service Flow Admission Control enforces threshold levels in one of two ways. The Cisco CMTS supports both enforcement methods, but both cannot be configured at the same time.

- **cpu-5sec**—This finest-level setting configures the Cisco CMTS to reject new requests when the **cpu-5sec** utilization has exceeded the configured critical threshold. This protects any time-sensitive activities on the router. Service Flow Admission Control takes action on the router when a new request might otherwise exceed the configured CPU threshold level.
- **cpu-avg**—This normal-level setting is a CPU utilization average, enforced by sampling the CPU utilization at much lower frequency and calculating an exponentially weighted average. Service Flow Admission Control takes action on the router when a new service request might otherwise exceed the configured CPU peak threshold level.

Prerequisites

Refer to the "Prerequisites for Service Flow Admission Control" section on page 16-2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable admission-control** {**cpu-5sec** | **cpu-avg** } **minor** *num1* **major** *num2* **critical** *num3*
4. **Ctrl-Z**

DETAILED STEPS

	Command or Action	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.

	Command or Action	Purpose
Step 3	**[no] cable admission-control {cpu-5sec | cpu-avg } minor** *num1* **major** *num2* **critical** *num3* **Example:** `Router# cable admission-control cpu-avg minor 60 major 70 critical 80`	Configures CPU memory thresholds on the Cisco CMTS for Service Flow Admission Control. • **cpu-5sec**—average CPU utilization over a period of five seconds. • **cpu-avg—**average CPU utilization over a period of one minute. • **minor** *num1*—Specifies the minor threshold level, where *num1* is a percentage and can be an integer between 1 and 100. • **major** *num2*—Specifies the major threshold level, where *num2* is a percentage and can be an integer between 1 and 100. • **critical** *num3*—Specifies the critical threshold level, where *num3* is a percentage and can be an integer between 1 and 100. There are no default values for this command. **Note** **cpu-5sec** and **cpu-avg** cannot be configured at the same time.
Step 4	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

Note When the minor value (*num1*) is crossed, then an alarm (trap) is sent. When the major value (*num2*) is crossed, then another alarm (trap) is sent. When the critical value (*num3*) is crossed, then the request is gracefully declined.

Note The threshold counters are set to zero when the resource is re-configured.

Note The minor threshold should be less than the major threshold, and the major threshold must be less than the critical threshold.

Configuring Service Flow Admission Control Based on Memory Resources

Three different memory resource options can be configured on the Cisco CMTS:

- IO memory - Current available (free) I/O memory
- Processor memory - Current available processor memory
- Both - Combined (IO and processor) memory that are available on the router

Memory-based Service Flow Admission Control is supported for memory on the main CPU in Cisco IOS Release 12.3(21)BC, and not for the broadband processing engine line card memory. As with CPU utilization, you can set minor, major, and critical threshold levels.

Prerequisites

Refer to the "Prerequisites for Service Flow Admission Control" section on page 16-2.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **cable admission-control** { **io-mem** | **proc-mem** | **total-memory** } **minor** *num1* **major** *num2* **critical** *num3*
4. **Ctrl-Z**

DETAILED STEPS

	Command or Action	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	[**no**] **cable admission-control** { **io-mem** | **proc-mem** | **total-memory** } **minor** *num1* **major** *num2* **critical** *num3* **Example:** `Router(config)# cable admission-control total-memory minor 60 major 80 critical 90`	Configures CPU memory thresholds on the Cisco router. • **io-mem**—Input/Output memory on the Cisco router • **proc-mem**—Process memory on the Cisco router • **total-memory**—Combined I/O and processor memory on the CMTS • **minor** *num1*—Specifies the minor threshold level, where *num1* is a percentage and can be an integer between 1 and 100. • **major** *num2*—Specifies the major threshold level, where *num2* is a percentage and can be an integer between 1 and 100. • **critical** *num3*—Specifies the critical threshold level, where *num3* is a percentage and can be an integer between 1 and 100. There are no default values for this command. **Note** All three memory threshold levels can and should be configured.
Step 4	**Ctrl-Z** **Example:** `Router(config-if)# Ctrl^Z`	Returns to Privileged EXEC mode.

Note When the minor value (*num1*) is crossed, then an alarm (trap) is sent. When the major value (*num2*) is crossed, then another alarm (trap) is sent. When the critical value (*num3*) is crossed, then the request is gracefully declined.

Note The threshold counters are set to zero when the resource is re-configured.

Defining Rules for Service Flow Categorization

This procedure describes how to configure service flow categorization rules on the Cisco CMTS. This flexible procedure changes default global service flow rules with variations of the **cable application type include** command.

By default, Cisco IOS Release 12.3(21)BC enables the definition of service flows according to application or traffic type, with bucket assignments for a standard set of service flow applications.

Any one or several of these steps or commands may be used, in nearly any combination, to set or re-configure SFAC on the Cisco CMTS.

Note Application rules for Service Flow Admission Control are global configurations, and upstream and downstream bandwidth resources use the same sets of service flow rules.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable application-type** *n* **include packetcable** { **normal** | **priority** }
4. **cable application-type** *n* **include pcmm** { **priority** *gate-priority* | **app-id** *gate-app-id* }
5. **cable application-type** *n* **include scheduling-type** *type*
6. **cable application-type** *n* **include service-class** *service-class-name*
7. **cable application-type** *n* **include BE**
8. **Ctrl-Z**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**cable application-type** *n* **include packetcable** { **normal** | **priority** } **Example:** `Router(config)# cable application-type 5 include packetcable priority`	For PacketCable, this command variation maps PacketCable service flow attributes to the specified bucket. PacketCable service flows are associated with PacketCable gates. The gate can be normal or high-priority. • *n*—Specify the bucket number to which an application is associated, with range from 1 to 8, with 1 as the first in the sequence. • **packetcable**—Specifies PacketCable for the designated bucket, with the associated priority configured with additional keywords. • **normal**—Maps normal PacketCable service flows into the specified application bucket. • **priority**—Maps high-priority PacketCable service flows into the specified application bucket.

	Command or Action	Purpose

Step 4	**cable application-type** *n* **include pcmm** { **priority** *gate-priority* | **app-id** *gate-app-id* }
	
	Example:
	`Router(config)# cable application-type 2 include pcmm priority 7`
	
	`Router(config)# cable application-type 2 include pcmm app-id 152`
		For PCMM, this command variation maps PCMM service flow priority or application to the specified bucket. The PCMM gates are characterized by a priority level and by an application identifier.
		• *n*—Specify the bucket number to which an application is associated, with range from 1 to 8, with 1 as the first in the sequence.
		• **pcmm**—Specifies PCMM for the designated bucket, with the associated priority and applications configured with additional keywords.
		• **priority** *gate-priority*—Designates the priority level for PCMM in this bucket. The priority level can range from 0 to 7.
		• **app-id** *gate-app-id*—Designates the application identifier for PCMM in this bucket. The application identifier can be from 0 to 65535. For each bucket, up to 10 application type rules may be defined.

Step 5	**cable application-type** *n* **include scheduling-type** *type*
	
	Example:
	`Router(config)# cable application-type 1 include scheduling-type ugs`
	
	`Router(config)# cable application-type 1 include scheduling-type ugs-ad`
		For DOCSIS scheduling types, this command variation binds the DOCSIS scheduling types into the designated application bucket. DOCSIS 1.1 specifies the scheduling type to bind QoS parameters to the service flows for upstream traffic.
		• *n*—Specify the bucket number to which an application is associated, with range from 1 to 8, with 1 as the first in the sequence.
		• **scheduling-type**—Keyword applies this command to upstream scheduling types, as further defined with one of the following additional keywords.
		• *type*—Choose one of the DOCSIS scheduling types:
		– **UGS**—Unsolicited Grant Service
		– **UGS-AD**—UGS-AD service
		– **RTPS**—real-time polling service
		– **nRTPS**—non-real-time polling service
		– **BE**—Best Effort

	Command or Action	Purpose
Step 6	**cable application-type** *n* **include service-class** *service-class-name* **Example:** `Router(config)# cable application-type 1 include service-class upstream1`	For service class parameters, this command variation applies a service class name to the service flows, and applies corresponding QoS parameters. • *n*—Specify the bucket number to which an application is associated, with range from 1 to 8, with 1 as the first in the sequence. • **service-class** —Keyword applies this command to the service class being assigned to the designated bucket. • *service-class-name*—Alphanumeric service class name. DOCSIS 1.1 introduced the concept of service classes. A service class is identified by a service class name. A Service Class Name is a string which the CMTS associates with a QOS Parameter Set. One of the objectives of using a service class is to allow the high level protocols to create the service flows with desired QOS parameter set. Using a service class is a convenient way to bind the application with the service flows. The rules provide a mechanism to implement such binding. Note the following factors when using the command in this step: • Service classes are separately configured using the **cable service class** command to define the service flow.b • A named service class may be classified into any application type. • Up to ten service class names may be configured per application types. Attempting to configure more than ten service classes prints an error message. • Using the **no cable traffic-type** command, remove configuration of one of the service class names before adding a new class.

	Command or Action	Purpose
Step 7	`Router(config)#` **cable application-type** *n* **include BE** **Example:** `Router# cable application-type 3 include BE`	For Best Effort service flows, this command variation elaborates on Step 3, and changes the default bucket of 8 for Best Effort service flows with non-zero Committed Information Rate (CIR). These BE service flows are often created during cable modem registration. • *n*—Specify the bucket number to which an application is associated, with range from 1 to 8, with 1 as the first in the sequence. • **BE**—Keyword applies Best Effort CIR to the specified bucket. Note that there is an alternate rule that applies to the Best Effort scheduling type. This rule is applicable only for upstream service flows, as described in an earlier step of this procedure. The BE CIR service flow rule may be applicable to both upstream and downstream. However, in the case of upstream service flows, in most cases, the same service flow may map both the rules.
Step 8	**Ctrl-Z** **Example:** `Router(config)#` **Ctrl^Z** `Router#`	Returns to Privileged EXEC mode.

Examples

The following example maps high-priority PacketCable service flows into application bucket 5.

```
Router(config)# cable application-type 5 include packetcable priority
```

The following example maps normal PacketCable service flows into application bucket 1.

```
Router(config)# cable application-type 1 include packetcable normal
```

The following example maps the specified bucket number with PCMM service flow with a priority of 7, then maps an application identifier of 152 for the same bucket number:

```
Router(config)# cable application-type 2 include pcmm priority 7
Router(config)# cable application-type 2 include pcmm app-id 152
```

The following example maps both UGS and UGS-AD into bucket number 1:

```
Router(config)# cable application-type 1 include scheduling-type ugs
Router(config)# cable application-type 1 include scheduling-type ugs-ad
```

The following example maps the Best Effort CIR flows to bucket 3:

```
Router(config)# cable application-type 3 include BE
```

Troubleshooting Tips

Service Flow Admission Control supports **debug** and **show** commands for monitoring and troubleshooting functions on the Cisco CMTS. Refer to the following procedures:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels

- Debugging Flow Categorization for Service Flow Admission Control

What to Do Next

When rules for Service Flow Admission Control are enabled on the Cisco CMTS, which is the default, those rules can be overridden or re-configured with the steps in this procedure. Once rules are enabled, the application buckets can be named or renamed with the procedure in the "Naming Application Buckets for Service Flow Admission Control" section on page 16-19.

Otherwise, refer to additional non-default procedures in this document, or to the following procedures for monitoring or troubleshooting Service Flow Admission Control on the Cisco CMTS:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels
- Debugging Flow Categorization for Service Flow Admission Control

Naming Application Buckets for Service Flow Admission Control

This procedure enables you to assign alpha-numeric names to six of the eight application buckets that Service Flow Admission Control supports. The default bucket identifiers range from 1 to 8.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable application-type** *n* **name** *bucket-name*
4. **Ctrl-Z**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable application-type** *n* **name** *bucket-name* **Example:** `Router(config)# cable application-type 7 name besteffort`	Assigns an alpha-numeric name for the specified bucket. **Note** This bucket name appears in supporting **show** and **debug** commands along with the default bucket number. • *n*—Specify the bucket number to which the name is applied. The priority sequence of the buckets, according to their original numeration of 1 to 8, still applies, whether the default bucket numbers or customized alpha-numeric names are used. • **name**—Keyword enables bucket renaming to the value specified. • *bucket-name*—Alpha-numeric bucket name to augment the default bucket number and display in **show** commands.
Step 4	**Ctrl-Z** **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Examples

The following example illustrates the use of descriptive names instead of numeration for the associated buckets:

```
Router(config)# cable application-type 2 name video
Router(config)# cable application-type 3 name gaming
```

The change made with this procedure is displayed with the **show application-buckets** command.

Troubleshooting Tips

Service Flow Admission Control supports **debug** and **show** commands for monitoring and troubleshooting functions on the Cisco CMTS. Refer to the following procedures:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels
- Debugging Flow Categorization for Service Flow Admission Control

What to Do Next

The change made with this procedure is displayed with the **show application-buckets** command.

Refer to additional non-default procedures in this document, or to the following procedures for monitoring or troubleshooting Service Flow Admission Control on the Cisco CMTS:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels
- Debugging Flow Categorization for Service Flow Admission Control

Setting Downstream and Upstream Application Thresholds

This procedure sets downstream and upstream applications thresholds for Service Flow Admission Control on the Cisco CMTS. This procedure extends the previous Admission Control commands from earlier Cisco IOS releases to support additional applications in Service Flow Admission Control. The settings in this procedure may be applied in either global or per-interface mode for downstream and upstream applications, and may also be applied in per-upstream fashion if desired.

Precedence of These Configuration Commands

Service Flow Admission Control based on bandwidth can be configured at the interface or global level. For upstream bandwidth, SFAC can be configured at the per-upstream level as well.

For downstream channels, the interface-level thresholds have higher precedence over the global thresholds configured. For upstream ports, the port-level thresholds have higher precedence over interface-level thresholds; and the interface-level thresholds have higher precedence over global thresholds.

As such, if you configure both global and interface-level downstream thresholds, the interface-level thresholds are effective for that interface. In similar fashion, if you configure port-level settings and the interface-level upstream thresholds, the port-level thresholds are effective on that port. The remaining ports, with no port-level thresholds in place, use the interface-level upstream thresholds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. (Optional) **interface cable** { *slot*/*port* | *slot*/*subslot*/*port* }
4. **cable admission-control ds-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* [**non-exclusive** *non-exclusive-percentage*]
5. (Optional) **interface cable** {*slot*/*port* | *slot*/*subslot*/*port*}
6. **cable admission-control us-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* **[non-exclusive** *non-exclusive-percentage*]
7. (Optional) **interface cable** {*slot*/*port* | *slot*/*subslot*/*port*}
8. **cable upstream** *n* **admission-control us-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* **[non-exclusive** *non-exclusive-percentage*]
9. **Ctrl-Z**

DETAILED STEPS

	Command or Action	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.

	Command or Action	Purpose

Step 3	**interface cable** {*slot/port* | *slot/subslot/port*}
	
	Example:
	`Router(config)# interface c5/0/1`
	`Router(config-if)#`
		(Optional). Interface configuration mode implements this feature only for the specified interface. Use global configuration mode in step 4 for global configurations.
		
		If downstream thresholds are configured for the interface, then that configuration supersedes global configuration.
		
		• *slot/port*—Designates the cable interface on the Cisco uBR7246VXR router.
		• *slot/subslot/port*—Designates the cable interface on the Cisco uBR10012 router.

Step 4	**cable admission-control ds-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* [**non-exclusive** *non-exclusive-percentage*] **Example:** `Router(config)# cable admission-control ds-bandwidth bucket-no 1 minor 15 major 25 exclusive 30 non-exclusive 15`	Sets minor, major and exclusive thresholds for downstream voice or data bandwidth for each or all interfaces on the Cisco CMTS. Repeat this step when setting bandwidth for multiple buckets. Global configuration mode implements this feature across the entire Cisco CMTS. Otherwise, use this command in interface configuration mode as per step 3. Bandwidth values are as follows: • **ds-bandwidth—**Sets downstream throughput thresholds. • **bucket-no** *n*—Keyword and variable select the bucket number for which this configuration applies. • *n*—Selects the application bucket number for which this configuration applies. • **minor** *minor-threshold*—Sets the minor alarm threshold. The *minor-threshold* value is a percentage from 1 to 100. • **major** *major-threshold*—Sets the major alarm threshold. The *major-threshold* value is a percentage from 1 to 100. • **exclusive** *exclusive-percentage*—Specifies the percentage of throughput reserved exclusively for this class (voice or data). The *exclusive-percentage* value is an integer between 1 and 100. No other bucket can use this throughput. • **non-exclusive** *non-exclusive-percentage*—(Optional) Specifies the percentage of throughput, over and above the exclusive share, that can be used by this class. The *non-exclusive-percentage* value is an integer between 1 and 100. Because this throughput is non-exclusive, it can be used by other buckets as specified. The **no** form of this command removes downstream bandwidth configuration from the Cisco CMTS: • **no cable admission-control ds-bandwidth**

Step 5	**interface cable** {*slot/port* | *slot/subslot/port*}
	
	Example:
	`Router(config)# interface c5/0/1`
	`Router(config-if)#`
		(Optional). Interface configuration mode implements this feature only for the specified interface. Use global configuration mode for global configurations.
		
		• *slot/port*—Designates the cable interface on the Cisco uBR7246VXR router.
		• *slot/subslot/port*—Designates the cable interface on the Cisco uBR10012 router.

	Command or Action	Purpose
Step 6	**cable admission-control us-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* [**non-exclusive** *non-exclusive-percentage*] **Example:** `Router(config)# cable admission-control us-bandwidth bucket-no 1 minor 10 major 20 exclusive 30 non-exclusive 10`	Configures global or interface-level upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS. If upstream thresholds are configured for the interface, then that configuration supersedes global configuration. • **us-bandwidth**—Specifies that this command is to configure the upstream bandwidth thresholds. • **bucket-no** *n*—Selects the application bucket for which this configuration applies.: • **minor** *minor-threshold*—Sets the minor alarm threshold. The *minor-threshold* value is a percentage from 1 to 100. • **major** *major-threshold*—Sets the major alarm threshold. The *major-threshold* value is a percentage from 1 to 100. • **exclusive** *exclusive-percentage*—Represents the critical threshold for the upstream throughput resource. Specifies the percentage of throughput reserved exclusively for this class. The *exclusive-percentage* value is a range from 1 to 100. No other class can use this bandwidth. • **non-exclusive** *non-exclusive-percentage*—(Optional) Specifies the percentage of bandwidth, over and above the exclusive share, that can be used by this class. The non-exclusive-percentage value is an integer between 1 and 100. Because this bandwidth is non-exclusive, it can be used by other classes as specified.

Step 7	**interface cable** {*slot* | *subslot*} {*slot*/*subslot*/*port*}
	
	Example:
	`Router(config)# interface c5/0/1`
	`Router(config-if)#`
		(Optional). Interface configuration mode implements this feature only for the specified interface. Use global configuration mode for global configurations.
		If downstream thresholds are configured for the interface, then that configuration supersedes global configuration.
		• *slot/port*—Designates the cable interface on the Cisco uBR7246VXR router.
		• *slot/subslot/port*—Designates the cable interface on the Cisco uBR10012 router.

	Command or Action	Purpose
Step 8	**cable upstream** *n* **admission-control us-bandwidth bucket-no** *n* **minor** *minor-threshold* **major** *major-threshold* **exclusive** *exclusive-percentage* **[non-exclusive** *non-exclusive-percentage* **]** **Example:** `Router(config)# cable upstream 1 admission-control us-bandwidth bucket-no 1 minor 10 major 20 exclusive 30 non-exclusive 10`	Configures global or interface-level upstream bandwidth thresholds and exclusive or non-exclusive resources on the Cisco CMTS. If upstream thresholds are configured for the interface, then that configuration supersedes global configuration. • **upstream**—Specifies that this command applies on per-upstream channel basis. • *n*—Specifies the upstream channel number. The traffic type takes the same values as the downstream command. • **us-bandwidth**—Specifies that this command is to configure the upstream bandwidth thresholds. • **bucket-no** *n*—Selects the application bucket for which this configuration applies. • **minor** *minor-threshold*—Sets the minor alarm threshold. The *minor-threshold* value is a percentage from 1 to 100. • **major** *major-threshold*—Sets the major alarm threshold. The *major-threshold* value is a percentage from 1 to 100. • **exclusive** *exclusive-percentage*—Represents the critical threshold for the upstream throughput resource. Specifies the percentage of throughput reserved exclusively for this class. The *exclusive-percentage* value is a range from 1 to 100. No other class can use this bandwidth. • **non-exclusive** *non-exclusive-percentage*—(Optional) Specifies the percentage of bandwidth, over and above the exclusive share, that can be used by this class. The non-exclusive-percentage value is an integer between 1 and 100. Because this bandwidth is non-exclusive, it can be used by other classes as specified.
Step 9	**Ctrl-Z** **Example:** `Router(config)# Ctrl^Z`	Returns to Privileged EXEC mode.

Examples

The following example illustrates the sequence of steps used when setting downstream and upstream application thresholds for the specified bucket in global configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# cable admission-control ds-bandwidth bucket-no 1 minor 15 major 25
exclusive 30 non-exclusive 15
Router(config)# cable admission-control us-bandwidth bucket-no 1 minor 10 major 20
exclusive 30 non-exclusive 10
```

Troubleshooting Tips

Service Flow Admission Control supports **debug** and **show** commands for monitoring and troubleshooting functions on the Cisco CMTS. Refer to the following procedures:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels

- Debugging Flow Categorization for Service Flow Admission Control

What to Do Next

Refer to additional non-default procedures in this document, or to the following procedures for monitoring or troubleshooting Service Flow Admission Control on the Cisco CMTS:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels
- Debugging Flow Categorization for Service Flow Admission Control

Preempting High-Priority Emergency 911 Calls

You may configure SFAC rules and thresholds so that the high-priority voice (911) traffic receives an exclusive share of bandwidth. Because the average call volume for Emergency 911 traffic may not be very high, the fraction of bandwidth reserved for Emergency 911 calls may be small. In the case of regional emergency, the call volume of Emergency 911 calls may surge. In this case, it may be necessary to preempt some of the normal voice traffic to make room for surging Emergency 911 calls.

The Cisco CMTS software preempts one or more normal-priority voice flows to make room for the high-priority voice flows. SFAC provides the command-line interface (CLI) to enable or disable this preemption ability.

SFAC preemption logic follows the following steps:

1. When the first pass of admission control fails to admit a high priority PacketCable flow, it checks if it is possible to admit the flow in another bucket configured for normal PacketCable calls (applicable only if the PacketCable normal and high-priority rules are configured for different buckets). If the bandwidth is available, the call is admitted in the normal priority bucket.
2. If there is no room in normal priority bucket, it preempts a normal priority PacketCable flow and admits the high priority flow in the bucket where the low priority flow was preempted.
3. If there is no normal priority flow that it can preempt, it rejects the admission for high-priority flow. This usually happens when both normal and high-priority buckets are filled with 911 flows.

This preemption is effective only for PacketCable high-priority flows.

When an upstream or downstream low-priority service flow is chosen for preemption, the corresponding service flow for the same voice call in the opposite direction gets preempted as well.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **[no] cable admission-control preempt priority-voice**
4. **Ctrl-Z**

DETAILED STEPS

	Command or Action	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	**[no] cable admission-control preempt priority-voice** **Example:** `Router(config)# no cable admission-control preempt priority-voice`	Changes the default Emergency 911 call preemption functions on the Cisco CMTS, supporting throughput and bandwidth requirements for Emergency 911 calls above all other buckets on the Cisco CMTS. The **no** form of this command disables this preemption, and returns the bucket that supports Emergency 911 calls to default configuration and normal function on the Cisco CMTS.

Step 4	**Ctrl-Z**
	
	Example:
	`Router(config)# Ctrl^Z`
	`Router#`
		Returns to Privileged EXEC mode.

Examples

The following example disables then restores Emergency 911 call preemption on the Cisco CMTS.

```
Router> enable
Router# configure terminal
Router(config)# cable admission-control preempt priority-voice
Router(config)# no cable admission-control preempt priority-voice
Router(config)# Ctrl^Z
Router#
```

Troubleshooting Tips

Service Flow Admission Control supports **debug** and **show** commands for monitoring and troubleshooting functions on the Cisco CMTS. Refer to the following procedures:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels
- Debugging Flow Categorization for Service Flow Admission Control

What to Do Next

Refer to additional non-default procedures in this document, or to the following procedures for monitoring or troubleshooting Service Flow Admission Control on the Cisco CMTS:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels

- Debugging Flow Categorization for Service Flow Admission Control

Calculating Upstream and Downstream Bandwidth Utilization

The Service Flow Admission Control feature maintains a counter for every US and DS channel, and this counter stores the current bandwidth reservation. Whenever a service request is made to create a new service flow, Service Flow Admission Control estimates the bandwidth needed for the new flow, and adds it to the counter. The estimated bandwidth is computed as follows:

- For DS service flows, the required bandwidth is the minimum reservation rate, as specified in the DOCSIS service flow QOS parameters.
- For US flows, the required bandwidth is as follows:
  - For BE flows the required bandwidth is the minimum reservation rate as specified in the DOCSIS service flow QOS parameters.
  - For UGS flows the required bandwidth is grant size times number of grants per second, as per the DOCSIS specification.
  - For RTP and RTPS flows, the required bandwidth is sum of minimum reservation rate as specified in the DOCSIS service flow QOS parameters; and the bandwidth required to schedule the request slots.
  - For UGSAD flows the required bandwidth is sum of bandwidth required for payload (same as UGS flows) and the bandwidth required to schedule to request slots.

In each of the above calculations, Service Flow Admission Control does not account for the PHY overhead. DOCSIS overhead is counted only in the UGS and UGS-AD flows. To estimate the fraction of bandwidth available, the calculation must account for the PHY and DOCSIS overhead, and also the overhead incurred to schedule DOCSIS maintenance messages. Service Flow Admission Control applies a correction factor of 80% to the raw data rate to calculate the total available bandwidth.

Example

The following example describes how the bandwidth calculations are performed for US voice calls.

Consider an US channel with voice calls generated using a G711 codec:

- The channel is 3.2 MHz wide with 16 QAM giving 10.24 MHz of raw data rate.
- The G711 codec generates 64 kbps of voice traffic with 20 ms sampling rate.
- Therefore, each sample payload is 160 bytes. With RTP, UDP and IP, Ethernet and the DOCSIS overhead, the packet size becomes 232 bytes. At 50 samples per second, this translates into 92.8 kbps of data.
- Therefore, for each new call, Service Flow Admission Control adds 92.8 kbps to the current reservation. The total available bandwidth with 80% of raw data rate becomes 8.192 Mbps.

If you configure 70% threshold for UGS traffic on this channel, the bandwidth allocated to voice becomes 8.192 * 0.7, or 5.7344 Mbps. At 92.8 Kbps per call, this allows 62 calls. For 99% threshold, the number of calls permitted increases to 87.

Note that the 80% correction factor is an approximation to account for all the overhead. The exact correction needed depends on several factors, such as raw data rate, PHS option, FEC options, and so forth.

Because UGS packets are a fixed size, the calculation of UGS data rate requirements is straightforward. For other flow types, where the packet size is variable, the actual usage of the channel cannot be predicted. In this example, when the threshold is 99% and the channel is carrying only the voice calls, the scheduler limitation may activate before the Service Flow Admission Control threshold that is set, and no calls may be scheduled after 85 calls.

As a result, the Service Flow Admission Control feature does not guarantee the accuracy of the bandwidth estimation.

Bandwidth Validity Checks for Service Flow Admission Control

Service Flow Admission Control is based on and monitors multiple resources on the Cisco CMTS. You can configure major, minor, exclusive and non-exclusive thresholds for various traffic types. To prevent circumstances in which some Service Flow Admission Control configurations are inconsistent, Service Flow Admission Control first validates the attempted configuration, and if an error is found, Service Flow Admission Control prints an error message and the configuration is not set.

Before setting the threshold limits for a given resource on the Cisco CMTS, Service Flow Admission Control configuration should follow these important guidelines to ensure a valid configuration:

1. For the given resource, the minor threshold should be less than the major threshold, and the major threshold should be less than the exclusive or critical threshold. For example, minor threshold at 45%, major threshold at 65%, and critical threshold at 85%.
2. For downstream and upstream bandwidth, the sum of the exclusive thresholds and the maximum configured non-exclusive threshold should be less than 100%. For example, consider US bandwidth configuration for various buckets. If exclusive thresholds for buckets 1-4 were configured at 15% each, this would mean a total of 60% bandwidth is reserved exclusively for these four buckets. This leaves only 40% for any non-exclusive bandwidth. Therefore, in this case, the maximum non-exclusive thresholds that any bucket can have is 40% (100% - 60%), and should be less than 40%.

Implicit Bandwidth

You may choose not to assign any explicit thresholds to certain buckets. In this case, these buckets assume implicit thresholds. In the previous example, if you do not configure any thresholds for buckets 5-8, then those bukets assume implicit thresholds. Because 60% bandwidth is already reserved by buckets 1-4, buckets 5-8 can share the remaining 40% bandwidth. This 40% bandwidth is treated in a non-exclusive manner. This information displays in supporting **show** commands.

Oversubscription

Oversubscription of a given resource on the Cisco CMTS may be encountered in one of the following ways:

- Consider a situation where voice and data are both given 50% exclusive bandwidth. If a large number of cable modems register with non-zero committed information rate (CIR) service flows, this results in consuming a large fraction of the bandwidth. Because service flows are not rejected during cable modem registration, the data usage may exceed its allocated 50% threshold. This situation is called oversubscription.
- Cable modem registration with CM configuration files with CIR flows may result in oversubscription. As explained above, the admission of CIR flows, even though it violates the admission control policy, can result in oversubscription.
- Enabling SFAC events after the service flows are admitted may result in oversubscription. If the SFAC check is not enabled using the cable admission-control dynamic-service command, this can result in service flows being admitted. If the thresholds are configured, the bandwidth usage may exceed its allocated share.

- Dynamically changing the thresholds can result in oversubscription. You can make changes in dynamic fashion to the threshold levels while the flows are already admitted. If the new threshold is lower than the current reservation for a given bucket, that bucket will oversubscribe its share under the new and lower threshold.
- The service flow handling method may result in oversubscription. The amount of bandwidth exceeding the allocated bandwidth is measured as "oversubscribed bandwidth". The oversubscribed bandwidth is displayed in the "show cable admission-control.." commands. While calculating the available bandwidth for the rest of the buckets, the oversubscribed bandwidth is not taken into consideration. We calculate effective bandwidth as follows:

  Effective bandwidth = current reservation - oversubscribed bandwidth

  For example, referring to the starting scenario with voice and data both given 50% bandwidth, if the data usage reaches 70%, the data bucket oversubscription totals 20%. That is, the effective bandwidth for the data bucket = 70 - 20 = 50%.

  Therefore, while calculating the available bandwidth for voice, full 50% bandwidth is considered available. Note that in this example, if you allow voice utilization to reach 50%, the total reservation becomes 120%. At present the Cisco CMTS platforms do not allow total reservation to exceed 100% of the available bandwidth for downstream channels; only upstream channels may exceed 100% reservation.

Displaying Application Buckets for Service Flow Admission Control

Cisco IOS Release 12.3(21)BC introduces the **show application-buckets** command to display default or customized Service Flow Admission Control settings and status on the Cisco CMTS. This command displays the bucket number and bucket name, if the latter is configured, and the associated rules for each bucket. When multiple rules are applied to one bucket, the rules display in order of priority for that bucket.

Prerequisites

This procedure presumes that SFAC is configured and operational on the Cisco CMTS.

SUMMARY STEPS

1. **enable**
2. **show cable application-type** [**bucket-no** *n*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cable application-type** [**bucket-no** *n*] **Example:** `Router# show application-buckets 5`	Displays rules for any or all buckets supporting Service Flow Admission Control on the Cisco CMTS. The configured rules for any given bucket are displayed in order of precedence in the Rule field. • **bucket-no** *n*—You may specify a specific bucket number on the Cisco CMTS to display parameters for that bucket and no others. Valid range is 1 to 8, or all buckets if no specific bucket is designated.

Examples

The following example illustrates sample output of the **show cable application-type** command.

```
Router# show cable application-type
For bucket 1, Name PktCable
     Packetcable normal priority gates
     Packetcable high priority gates
For bucket 2, Name PCMM-Vid
     PCMM gate app-id = 30
For bucket 3, Name Gaming
     PCMM gate app-id = 40
For bucket 4, Name
For bucket 5, Name
For bucket 6, Name
For bucket 7, Name
For bucket 8, Name HSD
     Best-effort (CIR) flows
```

Troubleshooting Tips

Service Flow Admission Control supports **show** and **debug** commands for troubleshooting functions on the Cisco CMTS. Refer to the following procedures:

- Displaying Service Flow Reservation Levels
- Debugging Flow Categorization for Service Flow Admission Control

What to Do Next

Refer to additional non-default procedures in this document, or to the following procedures for monitoring or troubleshooting Service Flow Admission Control on the Cisco CMTS:

- Displaying Service Flow Reservation Levels
- Debugging Flow Categorization for Service Flow Admission Control

Displaying Service Flow Reservation Levels

Cisco IOS Release 12.3(21)BC introduces a new command to display service flows, application categorizations, and bandwidth consumption on the Cisco CMTS.

Prerequisites

This procedure presumes that SFAC is configured and operational on the Cisco CMTS.

SUMMARY STEPS

1. **enable**
2. **show interface cable** { *slot/port* | *slot/subslot/port* } **admission-control reservation** { **downstream** | **upstream** } *port-no*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show interface cable** { *slot/port* | *slot/subslot/port* } **admission-control reservation** { **downstream** | **upstream** *port-no* } **Example:** `Router# show interface cable 5/1/1 admission-control reservation downstream`	Displays service flows, categorizations, and bandwidth consumption on the Cisco CMTS, for the specified interface, and the specified service flow direction. • *slot/port*—Designates the cable interface on the Cisco uBR7246VXR router. • *slot/subslot/port*—Designates the cable interface on the Cisco uBR10012 router. • **downstream**—Displays downstream service flow information for the designated cable interface. • **upstream** —Displays upstream service flow information for the designated cable interface. The port number may be specified here for more limited display. • *port-no*—Port number to which this designation applies, applicable in the case of upstream ports configured for SFAC.

Examples

The following example illustrates sample output and status of the Service Flow Admission Control feature, and the **show interface cable admission-control reservation** { **downstream** | **upstream** } *port-no* command.

```
Router# show interface cable 5/1/1 admission-control reservation downstream.
SfId   Mac Address       Bucket    Bucket Name         State    Current Reserv
4      0000.cad6.f052       8                         act       0
88     0000.cad6.f052       8                         act       2000
6      0000.cad6.eece       8                         act       0
21     0000.cad6.eece       8                         act       2000
8      0000.cad6.eebe       8                         act       0
24     0000.cad6.eebe       8                         act       2000
10     0000.cadb.30a6       8                         act       0
27     0000.cadb.30a6       8                         act       2000
```

Displaying SFAC Configuration and Status

Cisco IOS Release 12.3(21)BC supports an enhanced command to display service flows, application categorizations, and bandwidth consumption status on the Cisco CMTS.

Prerequisites

This procedure presumes that SFAC is configured and operational on the Cisco CMTS.

SUMMARY STEPS

1. **enable**
2. **show cable admission-control** [**global**] [**interface** *slot/port* | *slot/subslot/port*] [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show cable admission-control** [**global**] [**interface** *slot/port* | *slot/subslot/port*] [**all**] **Example:** `Router#`	Displays the current SFAC configuration and status on the Cisco CMTS, or on a specified interface. • **global**—Optional keyword displays the following information: – Parameters that have been configured for admission control – Number of requests that have crossed minor, major and critical levels for each resource • **interface** *slot/port* | *slot/subslot/port*—Option allows you to display SFAC information for the specified interface or port. This includes the following: – Values for US throughput resources – Values for DS throughput resources – *slot/port*—Designates the cable interface on the Cisco uBR7246VXR router. – *slot/subslot/port*—Designates the cable interface on the Cisco uBR10012 router. • **all**—Displays information for all interfaces configured for SFAC on the Cisco CMTS.

Examples

The following example illustrates further information for the Service Flow Admission Control feature. This example displays threshold levels and current reservation per bucket, and the oversubscribed bandwidth per bucket. Cisco IOS indicates implicitly calculated threshold with asterisk.

```
Router# show cable admission-control interface cable 5/1/1 upstream 0
Interface  Cable5/1/1
Upstream Bit Rate (bits per second) = 4096000
```

```
Resource - Upstream Bandwidth
-----------------------------
Bucket Names  Minor # of  Major # of  Excls # of  Non-Ex Curr. Curr. Conf  # of
No            Level Times Level Times Level Times Level  Resv  Ovrsb Level Rejec
1             5     1312  7     1262  45    0     0      31    0     I    36
2             0     0     0     0     0     0     6*     0     0     I     0
3             0     0     0     0     0     0     6*     0     0     I     0
4             0     0     0     0     0     0     6*     0     0     I     0
5             0     0     0     0     0     0     6*     0     0     I     0
6             0     0     0     0     0     0     6*     0     0     I     0
7             0     0     0     0     0     0     6*     0     0     I     0
8             5     31    7     29    49    11    5      79    25    I     0
```

Troubleshooting Tips

Service Flow Admission Control supports **debug** and **show** commands for monitoring and troubleshooting functions on the Cisco CMTS. Refer to the following procedures:

- Displaying Application Buckets for Service Flow Admission Control
- Debugging Flow Categorization for Service Flow Admission Control

What to Do Next

Refer to additional non-default procedures in this document, or to the following procedures for monitoring or troubleshooting Service Flow Admission Control on the Cisco CMTS:

- Displaying Application Buckets for Service Flow Admission Control
- Debugging Flow Categorization for Service Flow Admission Control
- Debugging Service Flow Admission Control for Different Event Types, page 16-33
- Debugging Service Flow Admission Control for CPU Resources, page 16-34
- Debugging Service Flow Admission Control for Memory Resources, page 16-35
- Debugging Service Flow Admission Control for Downstream Bandwidth, page 16-36
- Debugging Service Flow Admission Control for Upstream Throughput, page 16-37

Debugging Service Flow Admission Control for Different Event Types

Cisco IOS Release 12.3(21)BC supports the debugging of service flow events for SFAC on the Cisco CMTS.

Prerequisites

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

- "Enabling Service Flow Admission Control for Event Types" section on page 16-10

SUMMARY STEPS

1. **enable**
2. **debug cable admission-control event**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control event** **Example:** `Router# debug cable admission-control event`	Enables event-oriented troubleshooting for Service Flow Admission Control. Use the **no** form of this command to disable this debugging.

Examples

The following example illustrates the enablement and displays of the debug cable admission-control event command.

```
Router# debug cable admission-control event
*Sep 12 23:15:22.867: Entering admission control check on PRE and it's a cm-registration
*Sep 12 23:15:22.867: Admission control event check is TRUE
```

What to Do Next

If Service Flow Admission Control checks fail for the event types, refer to the following sections for additional information about events and configuration:

- **debug cable admission-control**
- **show cable admission-control**
- "How to Configure, Monitor and Troubleshoot Service Flow Admission Control" section on page 16-9

Debugging Service Flow Admission Control for CPU Resources

Cisco IOS Release 12.3(21)BC supports the debugging of CPU resources configured for SFAC on the Cisco CMTS.

Prerequisites

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

- "Configuring Service Flow Admission Control Based on CPU Utilization" section on page 16-12

SUMMARY STEPS

1. **enable**
2. **debug cable admission-control cpu**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control cpu** **Example:** `Router# debug cable admission-control cpu`	Enables CPU troubleshooting processes for Service Flow Admission Control. Use the **no** form of this command to disable this debugging.

Examples

The following example illustrates the enablement and displays of the **debug cable admission-control cpu** command.

```
Router# debug cable admission-control cpu
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
```

What to Do Next

If Service Flow Admission Control checks fail for the CPU resources, refer to the followingsections for additional information about CPU utilization thresholds, events and configuration:

- **debug cable admission-control**
- **show cable admission-control**
- "How to Configure, Monitor and Troubleshoot Service Flow Admission Control" section on page 16-9

Debugging Service Flow Admission Control for Memory Resources

Cisco IOS Release 12.3(21)BC supports the debugging of memory resources configured for SFAC on the Cisco CMTS.

Prerequisites

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

- "Configuring Service Flow Admission Control Based on Memory Resources" section on page 16-13

SUMMARY STEPS

1. **enable**
2. **debug cable admission-control cpu**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control cpu** **Example:** `Router# debug cable admission-control memory`	Enables memory troubleshooting processes for Service Flow Admission Control. Use the **no** form of this command to disable this debugging.

Examples

The following example illustrates the enablement and displays of the **debug cable admission-control memory** command.

```
Router# debug cable admission-control memory
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
*Sep 12 23:08:53.255: CPU admission control check succeeded
*Sep 12 23:08:53.255: System admission control check succeeded
```

What to Do Next

If Service Flow Admission Control checks fail for memory resources, refer to the following sections for additional information about memory thresholds, events and configuration:

- **debug cable admission-control**
- **show cable admission-control**
- "How to Configure, Monitor and Troubleshoot Service Flow Admission Control" section on page 16-9

Debugging Service Flow Admission Control for Downstream Bandwidth

Cisco IOS Release 12.3(21)BC supports the debugging of downstream bandwidth resources configured for SFAC on the Cisco CMTS.

Prerequisites

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

- "Setting Downstream and Upstream Application Thresholds" section on page 16-21

SUMMARY STEPS

1. **enable**
2. **debug cable admission-control ds-bandwidth**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control ds-bandwidth** **Example:** `Router# debug cable admission-control ds-bandwidth`	Enables downstream throughput troubleshooting processes for Service Flow Admission Control. Use the **no** form of this command to disable this debugging.

Examples

The following example illustrates the enablement and displays of the **debug cable admission-control ds-bandwidth** command.

```
Router# debug cable admission-control ds-bandwidth
Oct  8 23:29:11: Failed to allocate DS bandwidth for
CM 0007.0e01.1db5 in adding a new service entry
```

What to Do Next

If **debug** commands reveal issues with Service Flow Admission Control settings for the downstream, refer to the following sections for additional information about throughput thresholds, events and configuration:

- **debug cable admission-control**
- **show cable admission-control**
- "How to Configure, Monitor and Troubleshoot Service Flow Admission Control" section on page 16-9

Debugging Service Flow Admission Control for Upstream Throughput

Cisco IOS Release 12.3(21)BC supports the debugging of upstream bandwidth resources configured for SFAC on the Cisco CMTS.

Prerequisites

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

- "Setting Downstream and Upstream Application Thresholds" section on page 16-21

SUMMARY STEPS

1. **enable**
2. **debug cable admission-control us-bandwidth**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control us-bandwidth** **Example:** `Router# debug cable admission-control us-bandwidth`	Enables enable upstream throughput troubleshooting processes for Service Flow Admission Control. Use the **no** form of this command to disable this debugging.

Examples

The following example illustrates the enablement and displays of the **debug cable admission-control us-bandwidth** command.

```
Router# debug cable admission-control us-bandwidth
Router#
Oct  8 23:29:11: Failed to allocate US bandwidth for
CM 0007.0e01.9b45 in adding a new service entry
```

What to Do Next

If **debug** commands reveal issues with Service Flow Admission Control checks for the upstream, refer to the following sections for additional information about throughput thresholds, events and configuration:

- **debug cable admission-control**
- **show cable admission-control**
- "How to Configure, Monitor and Troubleshoot Service Flow Admission Control" section on page 16-9

Debugging Flow Categorization for Service Flow Admission Control

Cisco IOS Release 12.3(21)BC introduces a new **debug** command that accounts for the bucket-flow scheme of Service Flow Admission Control. This **debug** command displays service flow categorization results—when a service flow is classified, the **debug** command displays the application by which it was categorized, along with which rule is matched.

Prerequisites

Default or manual configuration of the following procedure is required for using this **debug** command, with additional SFAC settings presumed, according to your requirements.

- "Defining Rules for Service Flow Categorization" section on page 16-14

SUMMARY STEPS

1. **enable**

2. **debug cable admission-control flow-categorization**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug cable admission-control flow-categorization** **Example:** `Router# debug cable admission-control flow-categorization`	Enables debugging of service flow categorization processes for Service Flow Admission Control. This command displays service flow categorizations currently enabled on the Cisco CMTS. Use the **no** form of this command to disable this debugging.

Examples

Below is a shortened example of the information displayed when the **debug cable admission-control flow-categorization** command is enabled on the Cisco CMTS. This command displays interface-level information.

```
Router# debug cable admission-control flow-categorization

int ca 5/1/1 sfid 55 identified as video pcmm priority 6 matched.
```

Troubleshooting Tips

Service Flow Admission Control supports **debug** and **show** commands for monitoring and troubleshooting functions on the Cisco CMTS. Refer to the following procedures:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels

What to Do Next

Refer to additional non-default procedures in this document, or to the following procedures for monitoring or troubleshooting Service Flow Admission Control on the Cisco CMTS:

- Displaying Application Buckets for Service Flow Admission Control
- Displaying Service Flow Reservation Levels
- "How to Configure, Monitor and Troubleshoot Service Flow Admission Control" section on page 16-9

Configuration Examples for Service Flow Admission Control

This section describes solutions-level examples of the Service Flow Admission Control feature on the Cisco CMTS. This section illustrates the functioning of Service Flow Admission Control in default or non-default but properly operational configurations. This section presumes the proper use of configuration and monitoring procedures and commands described elsewhere in this document.

This section contains the following examples to illustrate Service Flow Admission Control:

- Example of SFAC Configuration Commands, page 16-40
- Example of Service Flow Admission Control for Downstream Traffic, page 16-41
- Example of Prioritizing Emergency 911 Traffic, page 43

Example of SFAC Configuration Commands

In this section of configuration examples, the following SFAC parameters are set on the Cisco CMTS:

- All the packetcable flows are mapped into bucket 1.
- The BE service flows are mapped into bucket 8.

The following configuration commands enable these settings:

- To map the packetcable voice flows, these commands are used:

```
cable application-type 1 include packetcable normal
cable application-type 1 include packetcable priority
cable application-type 1 name PktCable
```

- To map the BE flows into bucket 8, these commands are used.

```
cable application-type 8 name HSD
cable application-type 8 include best-effort
```

- Given the above configurations, you may also control bandwidth allocation to a PCMM streaming video application. The streaming video application is identified by the PCMM application ID 35. The following commands implement this configuration:

```
cable application-type 2 name PCMM-Vid
cable application-type 2 include pcmm app-id 35
```

- These configurations may be verified on the Cisco CMTS using the following **show** commands:

```
Router# show cable application-type
For bucket 1, Name PktCable
     Packetcable normal priority gates
     Packetcable high priority gates
For bucket 2, Name PCMM-Vid
     PCMM gate app-id = 30
For bucket 3, Name Gaming
     PCMM gate app-id = 40
For bucket 4, Name
For bucket 5, Name
For bucket 6, Name
For bucket 7, Name
For bucket 8, Name HSD
     Best-effort (CIR) flows
```

These above configuration examples might be omitted or changed, but the remaining examples in this section presume the above configurations.

Example of Service Flow Admission Control for Downstream Traffic

This example presumes that you have configured the rules according to the commands illustrated at the start of this section. All the voice flows in bucket 1. All the CIR data flows are categorized in bucket 8.

This example illustrates a sample configuration for Service Flow Admission Control with downstream traffic. In this example, if voice traffic exceeds 30% bandwidth consumption, additional voice flows are denied.

- 30% downstream throughput is reserved exclusively for voice traffic.
- Minor and major alarms for voice traffic to be generated at 15% and 25% respectively.

The following Cisco IOS command implements this configuration:

```
Router(config)# cable admission-control ds-bandwidth bucket-no 1 minor 15 major 25
exclusive 30
```

In this example, the voice flows are rejected when the bandwidth usage of the flows exceeds 30%.

In addition, you can allow for some flexibility by allowing flows to exceed their exclusive share, and to consume up to 50% of the total downstream throughput (30% + 20%). The following command accomplishes this:

```
Router(config)# cable admission control downstream bucket-no 1 minor 15 major 25 exclusive
30 non-exclusive 20
```

With this previous command, the bucket 1 flows are rejected when the voice usage exceeds 50% (30% + 20%).

Similarly you can configure data thresholds as follows:

```
Router(config)# cable admission control bucket-no 8 minor 15 major 25 exclusive 50
non-exclusive 10
```

With the configuration commands as above, the following multi-stage scenario illustrates how the lending and borrowing of throughput is achieved in the presence of multiple traffic classes.

Stage I—Initial Throughput Allocations

Assume downstream throughput distribution is as follows:

- Downstream voice threshold is configured at 30%, with current consumption at 20%.
- Downstream data threshold is configured at 50%, with current consumption at 40%.

Table 15-1 summarizes this throughput disribution:

Table 15-1 Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	Exclusive Threshold	Non-exclusive Threshold	% Consumed	% Available
Bucket-no 1 (Voice)	30%	20%	20%	30%
Bucket-no 8 (Data)	50%	10%	40%	20%
Uncategorized Traffic			0%	40% (100% -20% - 40%)

Stage 2—Voice Traffic Exceeds 30% Exclusive Throughput

Now assume conditions change as follows:

- Voice throughput increases to 40%. Voice obtains 10% from the non-exclusive share.

- Data (Best Effort CIR) throughput usage increases to 50%, consuming all exclusive data throughput.
- Bandwidth available for uncategorized traffic shrinks to 30%.

Table 15-2 summarizes this throughput distribution:

Table 15-2 Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	Exclusive Threshold	Non-exclusive Threshold	% Consumed	% Available
Voice	30%	20%	40% (30% + 10%)	10%
Data	50%	10%	50%	10%
Uncategorized Traffic			0%	10% (100% - 40% - 50%)

Step 3—Bandwidth Consumption Increases by 10%

Now assume that data throughput usage increases by 10% for a new consumption total of 60%, and voice usage remains same. This consumes all remaining non-exclusive bandwidth from Best Effort.

Table 15-3 summarizes this throughput distribution:

Table 15-3 Throughput Allocation and Consumption for Stage 1 of this Example

Throughput Type	Exclusive Threshold	Non-exclusive Threshold	% Consumed	% Available
Voice	30%	20%	40% (30% + 10%)	0%
Data	50%	10%	60% (50% + 10%)	0%
Uncategorized Traffic				0% (100%-40%-60%)

Note For the first time in this multi-stage example, bandwidth consumption on the Cisco CMTS has reached 100%, and there is no bandwidth available for uncategorized flows after the events of Stage 3.

Additional References

The following topics provide references related to Service Flow Admission Control for the Cisco CMTS in Cisco IOS Release 2.3(21a)BC or later releases.

Related Documents

Related Topic	Document Title
Cisco IOS Commands for the Cisco CMTS	*Cisco Broadband Cable Command Reference Guide* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
DOCSIS 1.1 Operations for the Cisco CMTS	*DOCSIS 1.1 for the Cisco CMTS* http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html
CISCO-CABLE-ADMISSION-CTRL-MIB for the Cisco Cable Modem Termination System	*Cisco CMTS Universal Broadband Router MIB Specifications Guide* http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/ubrmib3.html

Standards

Standard	Title
CableLabs™ DOCSIS 1.1 specifications	http://www.cablelabs.com/cablemodem
CableLabs™ PacketCable specifications	http://www.cablelabs.com/packetcable
CableLabs™ PacketCable MultiMedia specifications	http://www.cablelabs.com/packetcable/specifications/multimedia.html

MIBs

MIB	MIBs Link
• MIBs for the Cisco Cable Modem Termination System	*Cisco CMTS Universal Broadband Router MIB Specifications Guide* http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html
• MIBs Supporting Cisco IOS	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html